

User's Guide

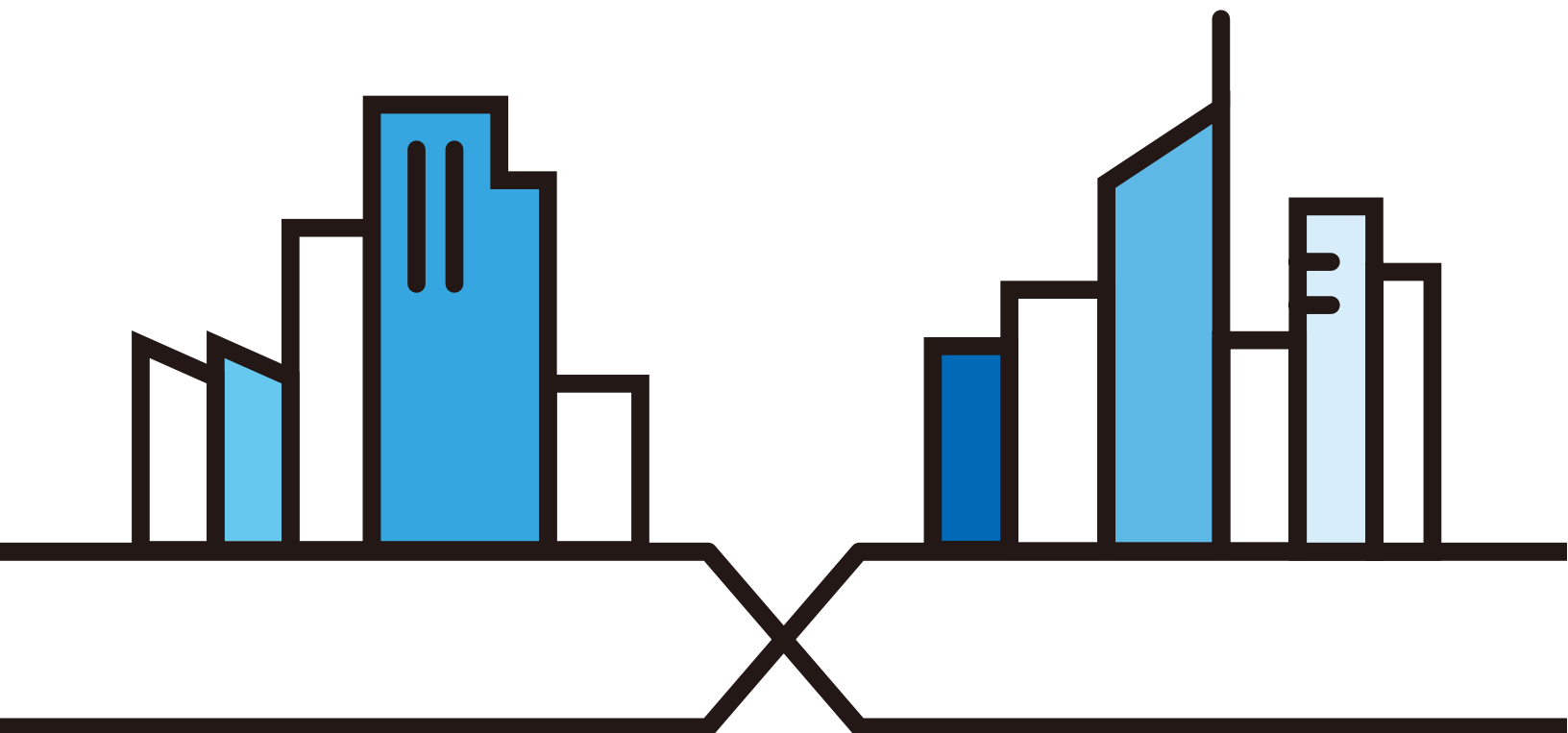
VPN2S

ZyWALL VPN Firewall

Default Login Details

LAN IP Address	http://192.168.1.1
User Name	admin
Password	1234

Version 1.12 Edition 2, 06/2018



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for a series of products. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the VPN2S and access the Web Configurator wizards. It contains information on setting up your network and configuring for Internet access.

- More Information

Go to **support.zyxel.com** to find other information on the VPN2S.



Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this guide.

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











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

Syntax Conventions

- All models in this series may be referred to as the "VPN2S" in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Configuration > Log / Report > Log Settings** means you first click **Configuration** in the navigation panel, then the **Log** sub menu and finally the **Log Settings** tab to get to that screen.

Icons Used in Figures

Figures in this user guide may use the following generic icons. The VPN2S icon is not an exact representation of your device.

VPN2S 	Generic Router 	Wireless Router / Access Point 
Switch 	Firewall 	USB Storage Device 
USB Dongle 	Cell Tower 	Printer 
Server 		

Contents Overview

User's Guide	12
Introducing the VPN2S	13
The Web Configurator	18
Wizard	25
Technical Reference	42
Dashboard	43
WAN/Internet	46
LAN	73
Routing	96
Network Address Translation (NAT)	110
Firewall	126
Security Service	146
VPN	154
Bandwidth Management	190
Network Management	208
System	212
Log / Report	214
Service / License	224
Device Name	226
Host Name List	228
Date / Time	230
User Account	233
USB Storage	236
Diagnostic	240
Firmware Upgrade	244
Backup / Restore	248
Language	250
Restart / Shutdown	251
Troubleshooting	252

Table of Contents

Document Conventions	3
Contents Overview	4
Table of Contents	5
Part I: User's Guide.....	12
Chapter 1	
Introducing the VPN2S.....	13
1.1 Overview	13
1.2 Ways to Manage the VPN2S	13
1.3 Good Habits for Managing the VPN2S	13
1.4 Applications for the VPN2S	14
1.4.1 Internet Access	14
1.4.2 VPN2S's USB Support	15
1.5 LEDs (Lights)	15
1.6 The RESET Button	16
Chapter 2	
The Web Configurator.....	18
2.1 Overview	18
2.1.1 Accessing the Web Configurator	18
2.2 Web Configurator Layout	20
2.2.1 Title Bar	20
2.2.2 Navigation Panel	21
2.2.3 Main Window	23
Chapter 3	
Wizard	25
3.1 Overview	25
3.2 Wizard Basic Setup	26
3.3 Wizard IPsec VPN Setup	30
3.3.1 VPN Express Settings	32
3.3.2 VPN Advanced Settings	34
3.4 Wizard IPv6 Setup	38

Part II: Technical Reference	42
Chapter 4	
Dashboard	43
4.1 Overview	43
4.2 The Dashboard Screen	43
Chapter 5	
WAN/Internet.....	46
5.1 Overview	46
5.1.1 What You Can Do in this Chapter	47
5.1.2 What You Need to Know	47
5.1.3 Before You Begin	49
5.2 The WAN Status Screen	50
5.3 The WAN Setup Screen	50
5.3.1 Internet Connection: Add/Edit	51
5.4 The Mobile Screen	59
5.5 The Port Setting Screen	63
5.6 The Multi-WAN Screen	64
5.6.1 Multi-WAN: Edit	65
5.6.2 How to Configure Multi-WAN for Load Balancing and Failover	66
5.7 The Dynamic DNS screen	67
5.7.1 Dynamic DNS: Add/Edit	68
5.8 Technical Reference	70
Chapter 6	
LAN	73
6.1 Overview	73
6.1.1 What You Can Do in this Chapter	73
6.1.2 What You Need To Know	74
6.1.3 Before You Begin	75
6.2 The LAN Status Screen	75
6.3 The LAN Setup Screen	76
6.3.1 LAN Setup: Edit	77
6.3.2 LAN Setup IPv6: Edit	79
6.4 The Static DHCP Screen	82
6.4.1 Static DHCP: Add/Edit	82
6.5 The Additional Subnet Screen	84
6.6 The Wake on LAN Screen	84
6.6.1 Wake On LAN: Add/Edit	85
6.7 The VLAN / Interface Group Screen	86
6.7.1 VLAN / Interface Group: Add/Edit	87
6.8 The DNS Entry Screen	91

6.9 The DNS Forwarder Screen	91
6.9.1 DNS Forwarder: Add/Edit	92
6.10 Technical Reference	93
6.10.1 LANs, WANs and the VPN2S	93
6.10.2 DHCP Setup	93
6.10.3 DNS Server Addresses	94
6.10.4 LAN TCP/IP	94

Chapter 7

Routing.....96

7.1 Overview	96
7.1.1 What You Can Do in this Chapter	96
7.2 The Routing Status Screen	97
7.3 The Policy Route Screen	103
7.3.1 Policy Route: Add/Edit	104
7.4 The Static Route Screen	106
7.4.1 Static Route: Add/Edit	107
7.5 The RIP Screen	108

Chapter 8

Network Address Translation (NAT).....110

8.1 Overview	110
8.1.1 What You Can Do in this Chapter	110
8.1.2 What You Need To Know	110
8.2 The Port Forwarding Screen	111
8.2.1 Port Forwarding: Add/Edit	113
8.3 The Port Triggering Screen	114
8.3.1 Port Triggering Rule: Add/Edit	116
8.4 The Address Mapping Screen	117
8.4.1 Address Mapping Rule: Add/Edit	118
8.5 The Default Server Screen	119
8.5.1 Default Server: Edit	120
8.6 The ALG Screen	121
8.7 Technical Reference	122
8.7.1 NAT Definitions	122
8.7.2 What NAT Does	122
8.7.3 How NAT Works	123
8.7.4 NAT Application	123

Chapter 9

Firewall.....126

9.1 Overview	126
9.1.1 What You Can Do in this Chapter	126

9.1.2 What You Need to Know	127
9.2 The Firewall Overview Screen	128
9.3 The DoS Screen	128
9.4 The Firewall Rules Screen	129
9.4.1 Firewall Rule: Add/Edit	130
9.5 The Device Service Screen	132
9.5.1 Device Service: Edit	134
9.5.2 Trust Domain: Add/Edit	134
9.6 The Zone Control Screen	135
9.7 The Service Screen	136
9.7.1 Service: Add/Edit	137
9.8 The MAC Filter Screen	138
9.8.1 MAC Filter: Add/Edit	139
9.9 The Certificate Screen	140
9.10 The AAA Server	141
9.10.1 LDAP Server: Add/Edit	142
9.10.2 RADIUS Server: Add/Edit	144

Chapter 10

Security Service.....146

10.1 Overview	146
10.1.1 What You Can Do in This Chapter	146
10.1.2 What You Need to Know	146
10.2 The Content Filter Screen	147
10.2.1 Content Filter: Add/Edit	150

Chapter 11

VPN.....154

11.1 Overview	154
11.2 What You Can Do in this Chapter	154
11.3 What You Need to Know	154
11.4 The VPN Status Screen	157
11.5 The IPsec VPN Screen	158
11.5.1 VPN Gateway: Add/Edit	160
11.5.2 VPN Connection: Add/Edit	166
11.5.3 The Default_L2TP_VPN_GW IPsec VPN Rule	169
11.5.4 PPTP VPN Troubleshooting Tips	170
11.6 The PPTP VPN Screen	171
11.6.1 PPTP VPN Troubleshooting Tips	173
11.7 The L2TP VPN Screen	174
11.7.1 L2TP Setup - Server	174
11.7.2 L2TP Setup - Client	176
11.7.3 L2TP VPN Troubleshooting Tips	177

11.8 The L2TP Client Status Screen	180
11.9 The GRE VPN Screen	181
11.9.1 GRE VPN: Add/Edit	182
11.10 Technical Reference	183
11.10.1 IPsec Architecture	183
11.10.2 Encapsulation	184
11.10.3 IKE Phases	185
11.10.4 Negotiation Mode	186
11.10.5 IPsec and NAT	186
11.10.6 VPN, NAT, and NAT Traversal	187
11.10.7 ID Type and Content	188
11.10.8 Pre-Shared Key	189
11.10.9 Diffie-Hellman (DH) Key Groups	189

Chapter 12

Bandwidth Management190

12.1 Overview	190
12.1.1 What You Can Do in this Chapter	190
12.1.2 What You Need to Know	190
12.2 The General Screen	192
12.3 The Queue Setup Screen	193
12.3.1 QoS Queue: Add/Edit	195
12.4 The Classification Setup Screen	196
12.4.1 QoS Class: Add/Edit	197
12.5 The Policer Setup Screen	200
12.5.1 QoS Policer: Add/Edit	201
12.6 The Shaper Setup Screen	202
12.6.1 QoS Shaper: Add/Edit	203
12.7 Technical Reference	204

Chapter 13

Network Management208

13.1 Overview	208
13.1.1 What You Can Do in This Chapter	208
13.2 The SNMP Screen	208

Chapter 14

System.....212

14.1 Overview	212
14.1.1 What You Can Do in This Chapter	212
14.2 The Scheduler Rule Screen	212
14.2.1 Scheduler Rule: Add/Edit	213

Chapter 15	
Log / Report	214
15.1 Overview	214
15.1.1 What You Can Do in this Chapter	214
15.1.2 What You Need To Know	214
15.2 The Log Viewer Screen	215
15.3 Log Settings	216
15.3.1 Log on USB Settings: Edit	217
15.3.2 System and Email: Edit	219
15.3.3 Remote Server Log Settings: Edit	221
Chapter 16	
Service / License.....	224
16.1 Overview	224
16.2 The License Screen	224
Chapter 17	
Device Name	226
17.1 Overview	226
17.2 The Device Name Screen	226
Chapter 18	
Host Name List.....	228
18.1 Overview	228
18.2 The Host Name List Screen	228
18.2.1 Add Host Name	228
Chapter 19	
Date / Time	230
19.1 Overview	230
19.2 The Date / Time Screen	230
Chapter 20	
User Account.....	233
20.1 Overview	233
20.2 What You Can Do in this Chapter	233
20.3 The User Account Screen	233
20.3.1 Users Account: Add/Edit	234
Chapter 21	
USB Storage	236
21.1 Overview	236
21.1.1 What You Need To Know	236

21.1.2 Before You Begin	237
21.2 The USB Storage Screen	237
21.2.1 Add a USB Share	239
Chapter 22	
Diagnostic.....	240
22.1 Overview	240
22.1.1 What You Can Do in this Chapter	240
22.2 The Network Tools Screen	240
22.3 The Packet Capture Screen	241
Chapter 23	
Firmware Upgrade	244
23.1 Overview	244
23.2 The Firmware Screen	244
23.3 The Mobile Profile Screen	246
Chapter 24	
Backup / Restore	248
24.1 Overview	248
24.2 The Backup / Restore Screen	248
Chapter 25	
Language	250
25.1 Overview	250
25.2 The Language Screen	250
Chapter 26	
Restart / Shutdown.....	251
26.1 Overview	251
26.2 The Restart / Shutdown Screen	251
Chapter 27	
Troubleshooting.....	252
27.1 Power, Hardware Connections, and LEDs	252
27.2 VPN2S Access and Login	253
27.3 Internet Access	254
27.4 USB Device Connection	255
Appendix A Customer Support	256
Appendix B Legal Information	262
Index	266

PART I

User's Guide

CHAPTER 1

Introducing the VPN2S

1.1 Overview

The VPN2S is a VPN firewall with Gigabit Ethernet (GbE) gateway. It has two USB ports that can be used for file sharing or using a 3G/4G dongle for cellular WAN (Internet) backup connections.

Features

- Four GbE Ports for LAN Connection
- Firewall with Secure Network Management
- Secure Access via VPN (IPsec, PPTP, L2TP)

Only use firmware for your VPN2S's specific model. Refer to the label on the bottom of your VPN2S.

1.2 Ways to Manage the VPN2S

Use any of the following methods to manage the VPN2S.

- Web Configurator. This is recommended for everyday management of the VPN2S using a (supported) web browser.

1.3 Good Habits for Managing the VPN2S

Do the following things regularly to make the VPN2S more secure and to manage the VPN2S more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters. The password must have 6-64 printable characters [0-9][a-z][A-Z][!@#\$%*].
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the VPN2S to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the VPN2S. You could simply restore your last configuration.

1.4 Applications for the VPN2S

Here are some example uses for which the VPN2S is well suited.

1.4.1 Internet Access

As a VPN firewall your VPN2S has multiple WAN interfaces, including, 3G/4G and Gigabit Ethernet to share the network traffic load. You can configure multiple WAN load balance and failover rules to distribute traffic amongst the different interfaces.

If you prefer you can also use a 3G/4G dongle for cellular backup WAN (Internet) connections.

Note: If you connect all WAN ports the priority order will be Ethernet WAN port, and USB port.

Computers can connect to the VPN2S's LAN ports.

Figure 1 VPN2S's Internet Access Application

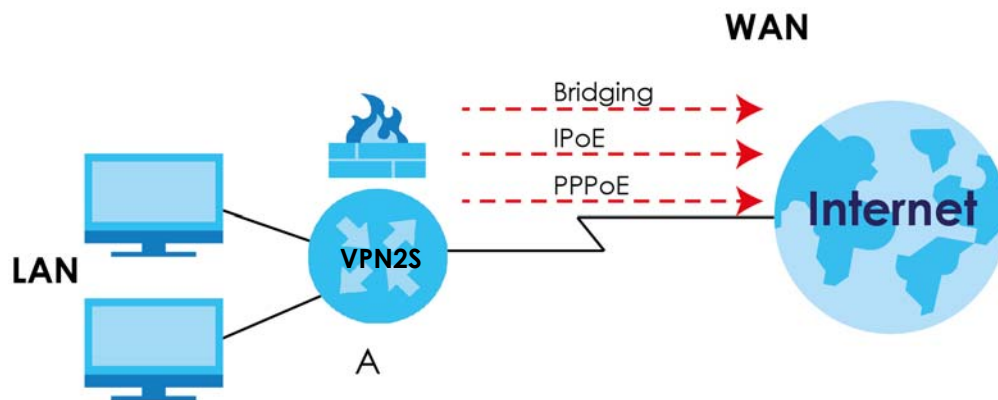
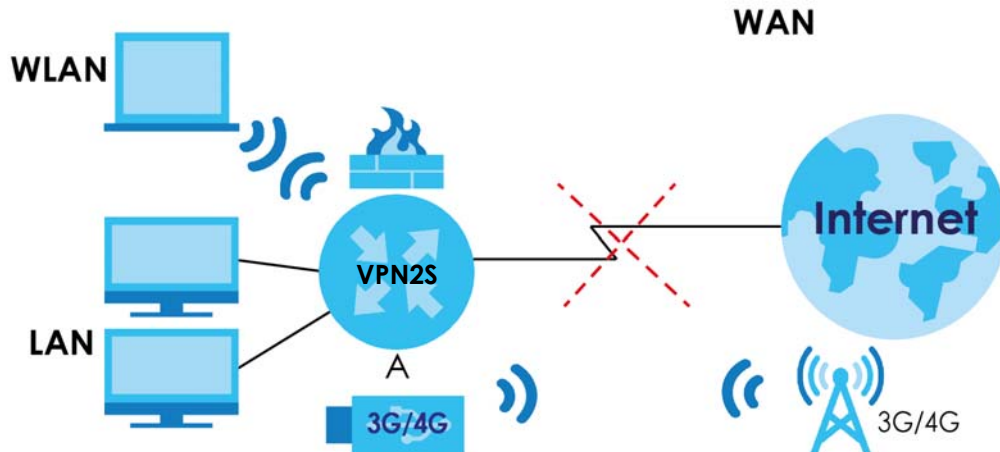


Figure 2 VPN2S's Internet Access Application: 3G/4G WAN Backup



You can also configure IP filtering on the VPN2S for secure Internet access. When the IP filter is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

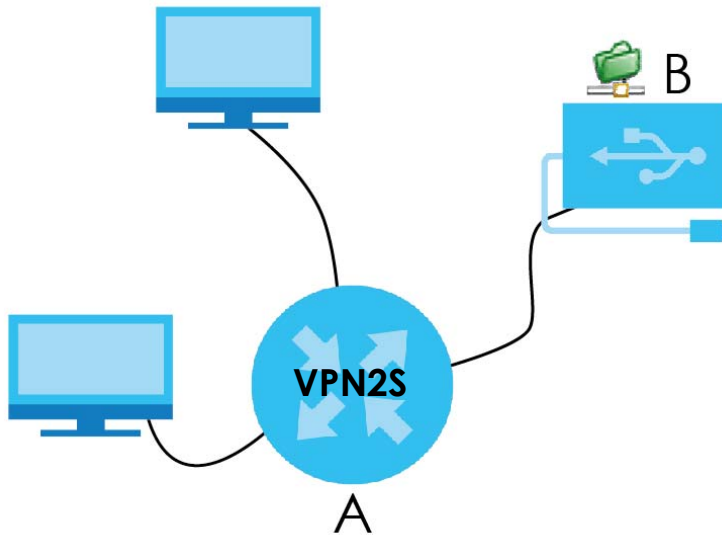
1.4.2 VPN2S's USB Support

Use the **USB** port for file sharing or insert a 3G/4G dongle for cellular backup WAN (Internet) connections.

File Sharing

Use the **USB** port (built-in USB 2.0) to share files on USB memory sticks or USB hard drives (**B**). Use FTP to access the files on the USB device.

Figure 3 USB File Sharing Application

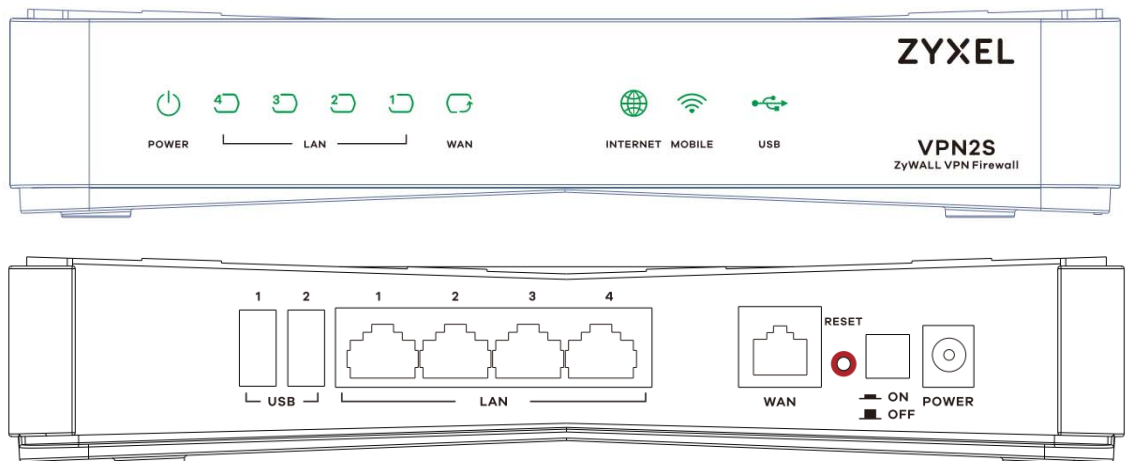


1.5 LEDs (Lights)

This section describes the LEDs on the VPN2S.

The following figure shows the front and rear panels of the VPN2S.

Figure 4 VPN2S Front and Rear Panels



None of the LEDs are on if the VPN2S is not receiving power. The location of the LEDs are highlighted in the figures above.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The VPN2S is receiving power and ready for use.
		Blinking	The VPN2S is self-testing.
	Red	On	The VPN2S detected an error while self-testing, or there is a device malfunction.
		Off	The VPN2S is not receiving power.
LAN	Green	On	The VPN2S has a successful Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The VPN2S is sending or receiving data to/from the LAN.
		Off	The VPN2S does not have an Ethernet connection with the LAN.
WAN	Green	On	The VPN2S has a successful Ethernet connection on the WAN.
		Blinking	The VPN2S is sending or receiving data to/from the WAN.
		Off	There is no Ethernet connection on the WAN.
INTERNET	Green	On	The VPN2S has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used).
		On	The Ethernet WAN port is connected to an Ethernet port but the VPN2S cannot access the Internet. There is an Internet connection problem.
		Off	There is no Internet connection or the gateway is in bridged mode.
MOBILE	Green	On	The VPN2S recognizes a 3G/4G dongle connection in USB port 1/2.
		Off	The VPN2S does not detect a 3G/4G dongle connection in USB port 1/2.
USB	Green	On	The VPN2S recognizes a USB connection in USB port 1/2.
		Off	The VPN2S does not detect a USB connection in USB port 1/2.
ETHERNET LAN 1-4 (On Connector)	Green (Left LED) 1GM	On	The VPN2S has a successful Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The VPN2S is sending or receiving data to/from the LAN.
		Off	The VPN2S does not have an Ethernet connection with the LAN.
	Amber (Right LED) 10-100M	On	The VPN2S has a successful Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The VPN2S is sending or receiving data to/from the LAN.
		Off	The VPN2S does not have an Ethernet connection with the LAN.

1.6 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234".

- 1 Make sure the **POWER** LED is on (not blinking).

- 2 To set the device back to the factory default settings, press the **RESET** button for five seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

CHAPTER 2

The Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 10.0 and later versions, Mozilla Firefox, Google Chrome, and Safari latest versions. The recommended screen resolution is 1024 by 768 pixels.

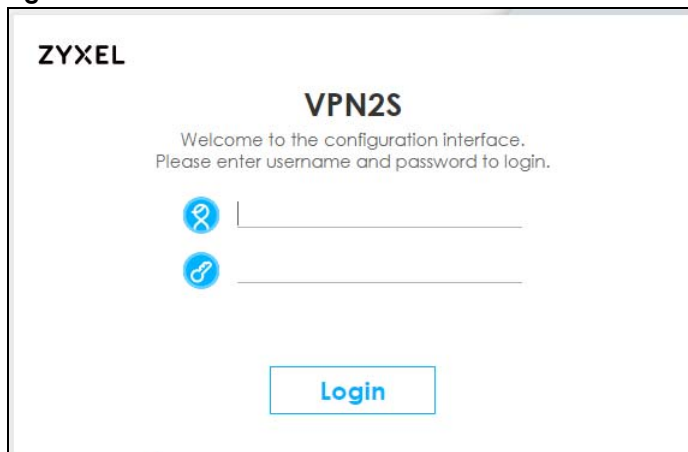
In order to use the web configurator you need to allow:

- Allow pop-up windows from your device (blocked by default in some Internet browsers).
- JavaScript (enabled by default).
- Java permissions (enabled by default).

2.1.1 Accessing the Web Configurator

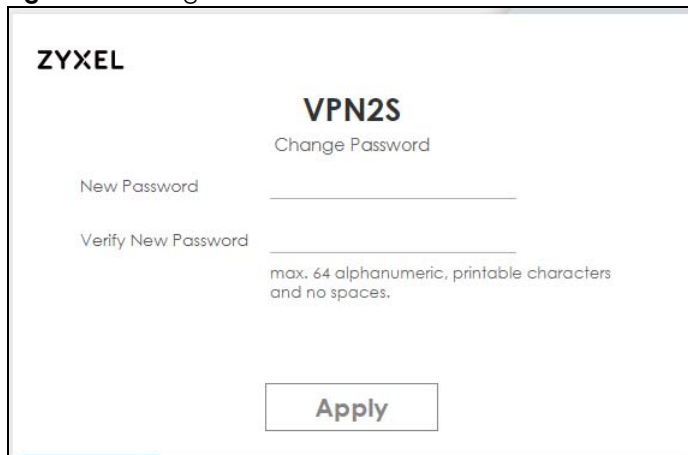
- 1 Make sure your VPN2S hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser. If the VPN2S does not automatically re-direct you to the login screen, go to <http://192.168.1.1>.
- 3 A password screen displays. To access the administrative web configurator and manage the VPN2S, type the default username **admin** and password **1234** in the password screen and click **Login**. If advanced account security is enabled (see [Section 18.3 on page 221](#)) the number of dots that appears when you type the password changes randomly to prevent anyone watching the password field from knowing the length of your password. If you have changed the password, enter your password and click **Login**.

Figure 5 Password Screen



- 4 The following screen displays if you have not yet changed your password from the default. Enter a new password, retype it to confirm and click **Apply**. After changing the password your VPN2S will log out automatically, so you can log in with your new password.

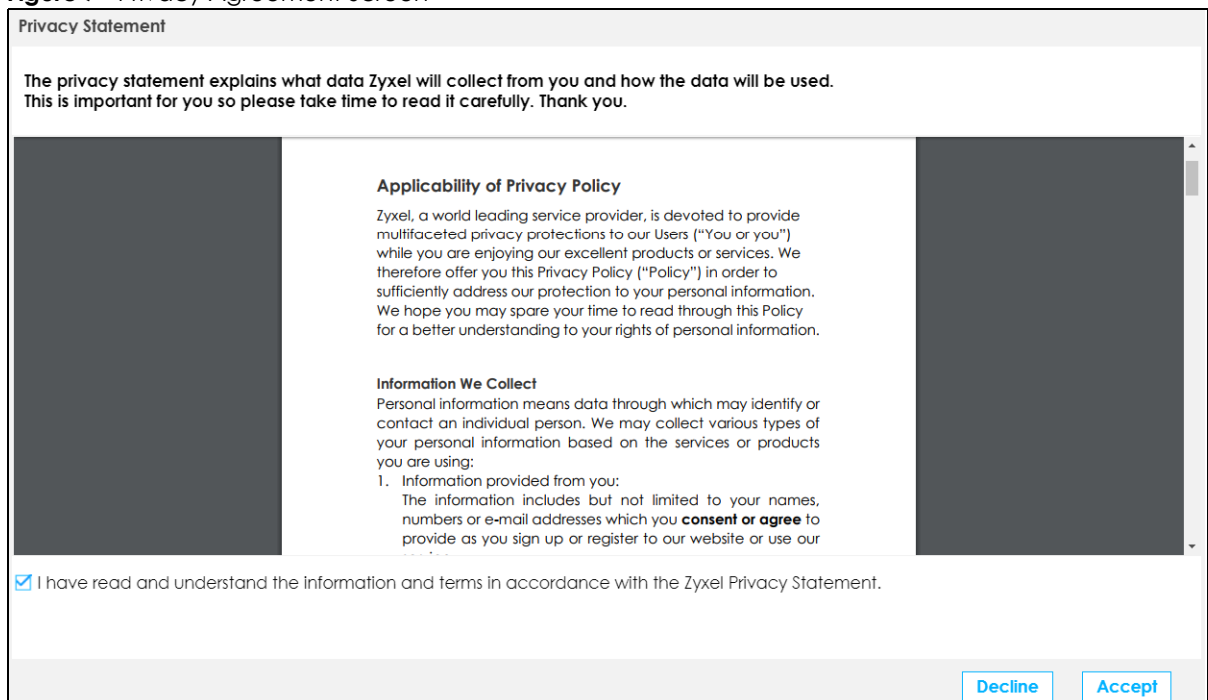
Figure 6 Change Password Screen



The screenshot shows the ZyXEL VPN2S Change Password screen. At the top left is the ZyXEL logo. In the center, it says 'VPN2S' and 'Change Password'. Below this are two input fields: 'New Password' and 'Verify New Password'. To the right of the 'Verify New Password' field, there is a note: 'max. 64 alphanumeric, printable characters and no spaces.' At the bottom center is an 'Apply' button.

- 5 The **Privacy Agreement** screen appears automatically after login. Click on the check box to agree to all the terms and click **Accept**.

Figure 7 Privacy Agreement Screen



The screenshot shows the ZyXEL Privacy Agreement screen. At the top, it says 'Privacy Statement'. Below this, a paragraph states: 'The privacy statement explains what data ZyXel will collect from you and how the data will be used. This is important for you so please take time to read it carefully. Thank you.' The main content area is divided into two columns. The left column is dark gray. The right column contains the text 'Applicability of Privacy Policy' and 'Information We Collect'. Below the text, there is a checkbox with the label 'I have read and understand the information and terms in accordance with the ZyXel Privacy Statement.' At the bottom right are two buttons: 'Decline' and 'Accept'.

- 6 The **Wizard** appears after the **Privacy Agreement** screen. Use the Wizard to configure VPN2S's basic settings. See [Chapter 3 on page 25](#) for more information.
- 7 The **Dashboard** page appears after the **Wizard** set up, here you can view the VPN2S's interface and system information.

2.2 Web Configurator Layout

Figure 8 Screen Layout

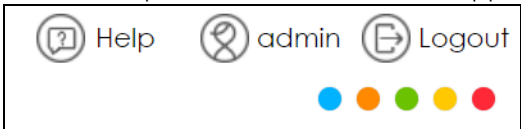


As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window

2.2.1 Title Bar

The title bar provides some icons in the upper right corner.



The icons provide the following functions.

Table 2 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	Help: Click this icon to view a description of the screen you are currently using.
	Logout: Click this icon to log out of the web configurator.
	Click a color from the palette to change the color of your web configurator.

2.2.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure VPN2S features. The following tables describe each menu item.

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Dashboard		Click this to go to the main Web Configurator screen.
Wizard		Use this screen to configure the VPN2S's basic settings. For more information see Chapter 3 on page 25 .
Configuration		
Configuration Site Map		Click this to view a summary of all the available screens in the Configuration menu.
WAN / Internet		
WAN Status	WAN Status	Use this screen to view the WAN ports' status.
WAN Setup		Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections.
Mobile		Use this screen to configure the mobile 3G/4G connection.
Port Setting		Use this screen to set flexible ports as part of LAN or WAN interfaces.
Multi-WAN		Use this screen to configure the multiple WAN load balance and failover rules to distribute traffic among different interfaces.
Dynamic DNS		Use this screen to allow a static hostname alias for a dynamic IP address.
LAN / Home Network		
LAN Status	LAN Status	Use this screen to view the status of all network traffic going through the LAN ports of the VPN2S.
	DHCP Client	Use this screen to view the status of all devices connected to the VPN2S. You can also set screen refresh time to see updates on new devices.
	ARP Table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
	Multicast Status	Use this screen to look at IGMP/MLD group status and traffic statistics.
LAN Setup		Use this screen to configure LAN TCP/IP settings, and other advanced properties.
Static DHCP		Use this screen to assign specific IP addresses to individual MAC addresses.
Additional Subnet		Use this screen to configure IP alias.
Wake on LAN		Use this screen to remotely wake up a hibernating device on the local network.
VLAN / Interface Group		Use this screen to create a new interface group, which is a new LAN bridge interface (subnet).
DNS Entry		Use this screen to view and configure a domain name and DNS routes on the VPN2S.
DNS Forwarder		Use this screen to view and configure domain zone forwarder on the VPN2S.
Routing		
Routing Status		Use this screen to view the IPv4 and IPv6 routing flow.
Policy Route		Use this screen to view and set up policy routes on the VPN2S.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Static Route		Use this screen to view and set up static routes on the VPN2S.
RIP		Use this screen to set up RIP (Routing Information Protocol) settings on the VPN2S.
NAT		
Port Forwarding		Use this screen to make your local servers visible to the outside world.
Port Triggering		Use this screen to change your VPN2S's port triggering settings.
Address Mapping		Use this screen to change your VPN2S's address mapping settings.
Default Server		Use this screen to configure a default server which receives packets from ports that are not specified in the Port Forwarding screen.
ALG		Use this screen to enable or disable NAT ALG and SIP ALG.
Firewall / Security		
Firewall Overview		Use this screen to enable the firewall.
DoS		Use this screen to activate protection against Denial of Service (DoS) attacks.
Firewall Rules		Use this screen to add and view existing firewall rules to the VPN2S.
Device Service		Use this screen to manage the services (such as HTTP and SSH) in the VPN2S.
Zone Control		Use this screen to set the firewall's default actions based on the direction of travel of packets.
Service		Use this screen to add Internet services.
MAC Filter		Use this screen to block or allow traffic from devices of certain MAC addresses to the VPN2S.
Certificate		Use this screen to view a summary list of certificates and manage certificates and certification requests.
AAA Server		Use this screen to manage the list of LDAP and RADIUS servers the VPN2S can use in authenticating users.
Security Service		
Content Filter		Use this screen to control access to specific websites or web content.
VPN		
VPN Status		Use this screen to look at the status of VPN tunnels that are currently established.
IPsec VPN		Use this screen to display and manage IPsec VPN gateways and connections.
PPTP VPN		Use this screen to configure the PPTP VPN settings in the VPN2S.
L2TP VPN		Use this screen to configure L2TP over IPsec tunnels.
L2TP Client Status		Use this screen to view details about the L2TP clients.
GRE VPN		Use this screen to configure the GRE VPN settings in the VPN2S.
Bandwidth Management		
General		Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions.
Queue Setup		Use this screen to configure QoS queues.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Classification Setup		Use this screen to define a classifier.
Policer Setup		Use these screens to configure QoS policers.
Shaper Setup		Use this screen to limit outgoing traffic transmission rate on the selected interface.
Network Management		
SNMP		Use this screen to configure SNMP communities and services.
System		
Scheduler Rule		Use this screen to configure the days and times when a configured restriction (such as User Access control) is enforced.
Log/Report		
Log Viewer		Use this screen to view the system logs on the VPN2S.
Log Settings		Use this screen to change specify settings to recording your logs on the VPN2S.
Maintenance		
Maintenance Site Map		Click this to view a summary of all the available screens in the Maintenance menu.
Service / License		Use this screen to view the status of your licenses and update any license information.
Device Name		Use this screen to give your VPN2S a name.
Host Name List		Use this screen to add connected devices to the VPN2S.
Date / Time		Use this screen to change your VPN2S's time and date.
User Account		Use this screen to manage user accounts, which includes configuring the username, password, retry times, file sharing, captive portal, and customizing the login message.
USB Storage		Use this screen to enable USB storage sharing.
Diagnostic	Network Tools	Use this screen to ping an IP address or trace the route packets take to a host
	Packet Capture	Use this screen to capture packets going through the VPN2S.
Firmware Upgrade		
Firmware		Use this screen to upload firmware to your device.
Mobile Profile		Use this screen to update the mobile profile on the VPN2S.
Backup / Restore		Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
Language		Use this screen to change the VPN2S web configurator's language.
Restart / Shutdown		Use this screen to reboot the VPN2S without turning the power off.

2.2.3 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

If you click **Dashboard** a graphic shows the connection status of the VPN2S's ports. The connected interfaces are in color and disconnected interfaces are gray.

Figure 9 Dashboard Screen

CHAPTER 3

Wizard

3.1 Overview

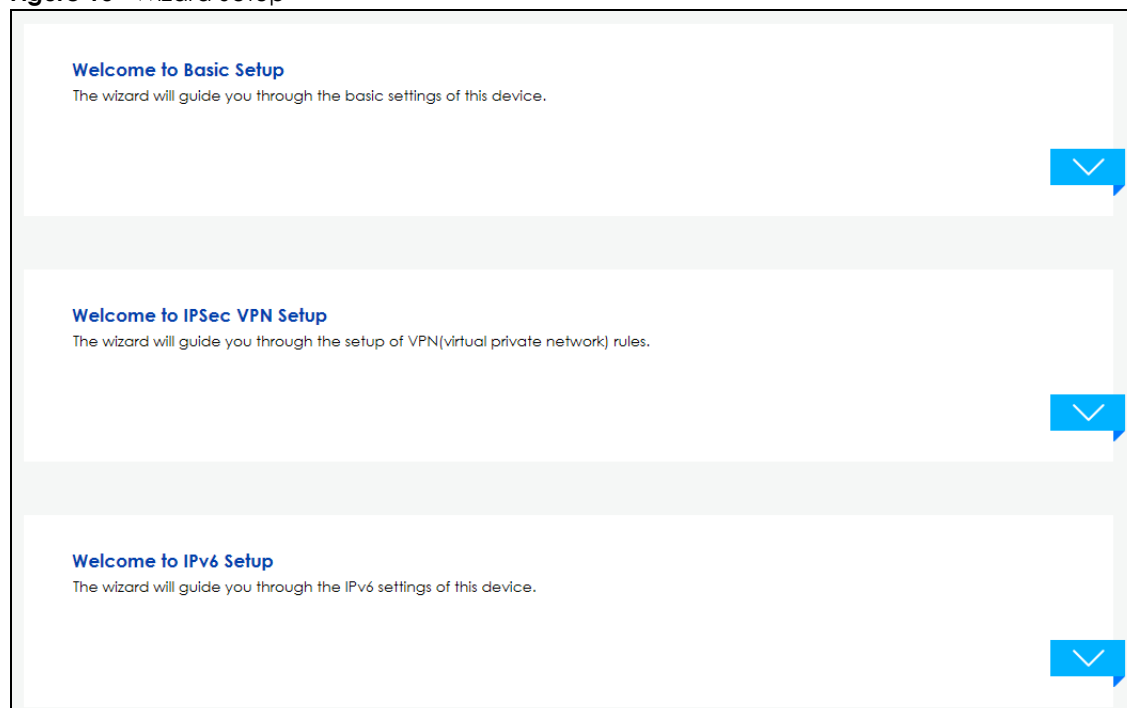
The Web Configurator's quick setup Wizard helps you configure Internet and VPN connection settings. This chapter provides information on configuring the Wizard screens in the Web Configurator. See the feature-specific chapters in this User's Guide for background information.

Before you begin configuring your VPN2S register your device at myZyxel portal and check your current license status.

The Wizard consists of the following setups:

- **Wizard Basic Setup** - Use **Basic Setup** to set up a WAN (Internet) connection. This Wizard creates matching ISP account settings in the VPN2S if you use PPPoE. See [Section 3.2 on page 26](#).
- **Wizard IPsec VPN Setup** - Use **IPsec VPN Setup** to configure an IPsec VPN (Virtual Private Network) rule for a secure connection to another computer or network. See [Section 3.3 on page 30](#).
- **Wizard IPv6 Setup** - Use **IPv6 Setup** to configure the IPv6 settings on your VPN2S. See [Section 3.4 on page 38](#).

Figure 10 Wizard Setup

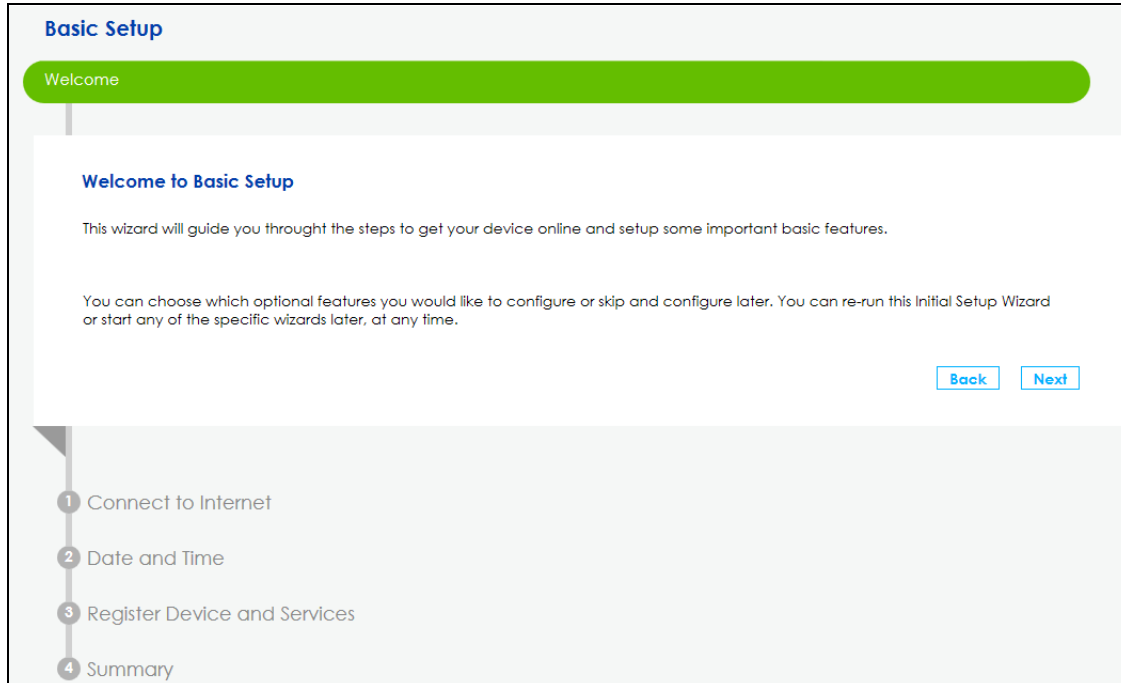


Note: See the technical reference chapters (starting on [page 42](#)) for background information on the features in this chapter.

3.2 Wizard Basic Setup

The **Wizard** appears automatically after you log in the first time. Or you can go to the **Wizard** tab in the navigation panel. Click the **Welcome to Basic Setup** down arrow to configure an interface to connect to the Internet. Click **Next** to continue the Wizard, **Back** to return to the previous screen.

Figure 11 Wizard Basic Setup



- 1 Enter your Internet connection information in this screen. The screen and fields to enter may vary depending on your current connection type and the **Encapsulation** you choose. You can also use this screen to enable the VLAN tag in the VPN2S. Assign it a priority level (**802.1p**) and a **VLAN ID** for traffic through this connection. Click **Next**.

Figure 12 Connect to the Internet

Basic Setup

Welcome → Connect to Internet

Connect to Internet

Type:

Encapsulation:

VLAN

☒ Enable

802.1p:

VLAN ID: ! (1~4094)

[Back](#) [Next](#)

2 Date and Time

3 Register Device and Services

4 Summary

- 2 If you select **PPPoE** as your encapsulation, type the **Username** given to you by your ISP and type the **Password** associated with the user name.

Figure 13 PPP information

Basic Setup

Welcome → Connect to Internet

Connect to Internet

PPP Information

Username: !

Password: !

[Back](#) [Next](#)

2 Date and Time

3 Register Device and Services

4 Summary

- 3 Use this screen to specify which IPv4 address the VPN2S uses to connect to the Internet. If your ISP gave you this information, enter it here. Otherwise select **Obtain an IP Address Automatically**.

Figure 14 IPv4 Address

The screenshot shows the 'Basic Setup' wizard with a green progress bar at the top indicating the current step is 'Connect to Internet'. Below the progress bar, the title 'Connect to Internet' is displayed. Underneath, the 'IPv4 Address' section has two radio button options: 'Obtain an IP Address Automatically' (which is selected) and 'Use the Following IP Address'. The second option is followed by three input fields labeled 'IP Address:', 'Subnet Mask:', and 'Gateway IP:'. At the bottom right of the main content area are 'Back' and 'Next' buttons. On the left side, a vertical list of steps shows '1 Connect to Internet' as the active step, followed by '2 Date and Time', '3 Register Device and Services', and '4 Summary'.

- 4 Choose whether VPN2S gets DNS server addresses from the ISP automatically or uses the DNS server addresses you got from the ISP. A DNS server is used for mapping a domain name to its corresponding IP address and vice versa.

Figure 15 DNS Server

The screenshot shows the 'Basic Setup' wizard with a green progress bar at the top indicating the current step is 'Connect to Internet'. Below the progress bar, the title 'Connect to Internet' is displayed. Underneath, the 'DNS Server' section has two radio button options: 'Obtain DNS Server Address Automatically' (which is selected) and 'Use the Following DNS Server Address'. The second option is followed by two input fields labeled 'DNS Server 1:' and 'DNS Server 2:'. At the bottom right of the main content area are 'Back' and 'Next' buttons. On the left side, a vertical list of steps shows '1 Connect to Internet' as the active step, followed by '2 Date and Time', '3 Register Device and Services', and '4 Summary'.

- 5 Choose the time zone for your device's location. Click **Save**.

Figure 16 Date and Time

The screenshot shows the 'Basic Setup' wizard with a green progress bar indicating the sequence: Welcome → Connect to Internet → Date and Time. The 'Date and Time' section is active, showing a 'Time Zone' dropdown menu set to '(GMT-00:00) Greenwich Mean Time: Edinburgh, London'. At the bottom left, a progress indicator shows steps 3 'Register Device and Services' and 4 'Summary'. 'Back' and 'Next' buttons are located at the bottom right.

- 6 The VPN2S saves your settings and attempts to connect to the Internet. If the VPN2S failed to connect to the Internet or if you want to modify any of the settings you previously configured you can click **Back** or go to the **Configuration > WAN/Internet > WAN Setup** screen. Click **Connection Test** for the VPN2S to try reconnecting with the same settings.

Figure 17 Basic Setup Completed

The screenshot shows the 'Basic Setup' wizard with a green progress bar indicating the sequence: Welcome → Connect to Internet → Date and Time. The 'Connect to Internet' step is completed, showing a diagram of the VPN2S device connected to the Internet with a green checkmark. Below the diagram, it says 'Your Internet connection is working!'. At the bottom left, a progress indicator shows steps 3 'Register Device and Services' and 4 'Summary'. 'Back' and 'Next' buttons are located at the bottom right.

- 7 You can register your device and manage subscription services available for your VPN2S at myZyxel portal for online services.

Figure 18 Register Device and Services

Basic Setup

Welcome → Connect to Internet → Date and Time → Register Device and Services

Register Device and Services

Register Device [Refresh](#)

Registering your device is prerequisite for receiving notifications when new firmware is available and for activation licenses.

Device Registration Status: Not registered

Register your device now [Register](#)

Click "Activate" to go to myZyxel to activate security licenses. Otherwise, press "Skip" to go to the next step.

[Back](#) [Next](#)

4 Summary

- 8 Once you completed the basic setup a summary of your settings displays. Click **Finish** to continue with the Wizard setup.

Figure 19 Summary

Basic Setup

Welcome → Connect to Internet → Date and Time → Register Device and Services → Summary

WAN

IP Address:	172.17.40.14
Subnet Mask:	255.255.252.0
Gateway IP:	172.17.43.254

Time

Time Zone:	(GMT-00:00) Greenwich Mean Time: Edinburgh, London
------------	--

Service License

Device Registration:	Unregistered
Firmware Upgrade:	Not Activated

[Back](#) [Finish](#)

3.3 Wizard IPsec VPN Setup

Click the **IPsec VPN Setup** down arrow to configure a VPN (Virtual Private Network) rule for a secure connection to another computer or network.

Figure 20 Wizard IPsec VPN Setup

The screenshot shows the 'VPN Setup' wizard's 'Welcome' screen. At the top, a green bar contains the text 'Welcome'. Below this, the main heading is 'Welcome to IPsec VPN Setup'. The text below the heading states: 'VPN Setup Wizard will guide you to create a secure, private connection between two sites. Two networks (sites) behind the VPN2S can then communicate securely with each other.' At the bottom right of the main content area are two buttons: 'Back' and 'Next'. On the left side, there is a vertical progress indicator with five steps: 1 Policy, 2 Type, 3 Settings, 4 Summary, and 5 Completed. The first step, '1 Policy', is highlighted with a larger circle and a vertical line through it.

There are two types of VPN policies you can configure in the VPN2S. Select one and click **Next**.

- **Express** - Select **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key as the authentication method. See [Section 3.3.1 on page 32](#).
- **Advanced** - Select **Advanced** to change default settings an/or use certificates instead of a pre-shared key in the VPN rule. See [Section 3.3.2 on page 34](#).

Figure 21 VPN Policy Type

The screenshot shows the 'VPN Setup' wizard's screen for selecting a policy type. At the top, a green bar contains the text 'Welcome ⇒ Policy'. Below this, the main heading is 'Please select the type of VPN policy you wish to setup.' followed by the sub-heading 'Type of VPN policy'. There are two radio button options: 'Express' (which is selected) and 'Advanced'. At the bottom right of the main content area are two buttons: 'Back' and 'Next'. On the left side, there is a vertical progress indicator with five steps: 2 Type, 3 Settings, 4 Summary, and 5 Completed. The second step, '2 Type', is highlighted with a larger circle and a vertical line through it.

3.3.1 VPN Express Settings

The following screens will display if you select **Express** in the previous screen.

- 1 Type the **Rule Name** used to identify this VPN connection (and VPN gateway). Then select the **IKE Version** and **Scenario** that best describes your intended VPN connection. For more information on each label see [Section 11.5 on page 158](#).

Figure 22 VPN Express Settings

VPN Setup

Welcome → Policy → Type

Express Settings

Rule Name: WIZARD_VPN

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Diagram: A site-to-site connection between two networks via the Internet. The left network is connected to a router, and the right network is connected to a router with a 'Static IP' label. The Internet is represented by a cloud.

[Back](#) [Next](#)

Progress bar: 3 Settings, 4 Summary, 5 Completed

- 2 In **My Interface** select the type of encapsulation this connection is to use. Configure a **Secure Gateway** IP as the peer VPN2S's WAN IP address. Type a secure **Pre-Shared Key**. Set **Local Policy** to be the IP address range of the network connected to the VPN2S and **Remote Policy** to be the IP address range of the network connected to the peer VPN2S.

Figure 23 Secure Gateway

VPN Setup

Welcome ⇒ Policy ⇒ Type ⇒ Settings

Express Settings

My Interface: Any

Secure Gateway

Static Address: 1.1.1.1

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 2.2.2.2 / 255.255.255.0

Remote Policy (IP/Mask): 3.3.3.3 / 255.255.255.0

Back Next

4 Summary

5 Completed

- 3 This screen shows a read-only summary of the VPN tunnel's configuration. Click **Save** to apply your changes.

Figure 24 Summary

VPN Setup

Welcome ⇒ Policy ⇒ Type ⇒ Settings ⇒ Summary

Express Settings

Summary

IKE Version: IKEv1

Rule Name: WIZARD_VPN

My Interface: Any

Secure Gateway: 1.1.1.1

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 2.2.2.2/255.255.255.0

Remote Policy (IP/Mask): 3.3.3.3/255.255.255.0

Back Save

5 Completed

- 4 Your VPN2S saves your settings. Now the VPN rule is configured on the VPN2S.

Figure 25 VPN Express Settings Completed

VPN Setup

Welcome → Policy → Type → Settings → Summary

Express Settings

Congratulations. The VPN Access wizard is completed.

IKE Version:	IKEv1
Rule Name:	WIZARD_VPN
My Address:	Any
Secure Gateway:	1.1.1.1
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	2.2.2.2/255.255.255.0
Remote Policy (IP/Mask):	3.3.3.3/255.255.255.0

[Finish](#)

3.3.2 VPN Advanced Settings

The following screens will display if you select **Advanced** in the VPN Policy screen.

- 1 Type the **Rule Name** used to identify this VPN connection (and VPN gateway). Then select the **IKE Version** and the **Scenario** that best describes your intended VPN connection. Then click **Next**. For more information on each label see [Section 11.5 on page 158](#).

Figure 26 VPN Advanced Settings

VPN Setup

Welcome → Policy → Type

Advanced Settings

Rule Name: WIZARD_VPN

IKE Version

☒ IKEv1

☐ IKEv2


Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)



[Back](#) [Next](#)

3 Settings

4 Summary

5 Completed

- 2 Use the following screen to setup **Phase 1 Settings**. Select an **Encryption, Authentication Algorithm**, and **Key Group**, and define how often the VPN2S renegotiates the IKE SA in the **Life Time** field. For more information on each label see [Section 11.5 on page 158](#).

Figure 27 Phase 1 Settings

VPN Setup

Welcome ⇒ Policy ⇒ Type ⇒ Settings

Advanced Settings

Phase 1 Settings

My Interface: Any

Secure Gateway

☒ Static Address: ⓘ
 Negotiation Mode: Main
 Encryption Algorithm: AES128
 Authentication Algorithm: SHA1
 Key Group: DH2
 SA Life Time: 86400 (180 - 3000000 seconds)
☒ NAT Traversal
☒ Dead Peer Detection (DPD)

Authentication Method

☒ Pre-Shared Key: ⓘ
☐ Certificate:

Back Next

4 Summary

5 Completed

- 3 Use the following screen to setup **Phase 2 Settings**. Phase 2 in an IKE uses the SA that was established in phase1 to negotiate Security Associations (SAs) for IPsec. For more information on each label on this screen see [Section 11.5 on page 158](#). Click **Next**.

Figure 28 Phase 2 Settings

The screenshot shows the 'VPN Setup' wizard at the 'Phase 2 Settings' step. A green breadcrumb bar at the top reads 'Welcome ⇒ Policy ⇒ Type ⇒ Settings'. The main content area is titled 'Advanced Settings' and 'Phase 2 Settings'. It contains several configuration fields: 'Encapsulation' (Tunnel), 'Encryption Algorithm' (AES128), 'Authentication Algorithm' (SHA1), 'SA Life Time' (86400 seconds), and 'Perfect Forward Secrecy (PFS)' (DH2). Below these are 'Policy Settings' for 'Local Policy (IP/Mask)' and 'Remote Policy (IP/Mask)', both set to 2.2.2.2 / 255.255.255.0. A 'Property' section has an unchecked 'Nailed UP' checkbox. 'Back' and 'Next' buttons are at the bottom right. A progress indicator on the left shows steps 4 (Summary) and 5 (Completed).

VPN Setup

Welcome ⇒ Policy ⇒ Type ⇒ Settings

Advanced Settings

Phase 2 Settings

Encapsulation: Tunnel

Encryption Algorithm: AES128

Authentication Algorithm: SHA1

SA Life Time: 86400 (180 - 3000000 seconds)

Perfect Forward Secrecy (PFS): DH2

Policy Settings

Local Policy (IP/Mask): 2.2.2.2 / 255.255.255.0

Remote Policy (IP/Mask): 3.3.3.3 / 255.255.255.0

Property

☐ Nailed UP

[Back](#) [Next](#)

4 Summary

5 Completed

- 4 A read-only summary of the VPN tunnel's configuration will display. If you want to save your changes click **Save**; otherwise go **Back** to modify any previous configurations.

Figure 29 Summary

VPN Setup

Welcome → Policy → Type → Settings → Summary

Advanced Settings

Summary

Rule Name:	WIZARD_VPN
IKE Version:	IKEv1
My Interface:	Any
Secure Gateway:	1.1.1.1
Pre-Shared Key:	12345678
Certificate:	
Local Policy (IP/Mask):	2.2.2.2/255.255.255.0
Remote Policy (IP/Mask):	3.3.3.3/255.255.255.0

Phase 1

Negotiation Mode:	Main
Encryption Algorithm:	AES128
Authentication Algorithm:	SHA1
Key Group:	DH2

Phase 2

Encryption:	Tunnel
Encryption Algorithm:	AES128
Authentication Algorithm:	SHA1

[Back](#) [Save](#)

5 Completed

- 5 Your VPN2S saves your settings. Now the rule is configured on the VPN2S. Click **Finish** to exit the **VPN Setup** Wizard.

Figure 30 VPN Advanced Settings Completed

VPN Setup

Welcome ⇒ Policy ⇒ Type ⇒ Settings ⇒ Summary

Advanced Settings

Congratulations. The VPN Access wizard is completed.

Summary

Rule Name:	WIZARD_VPN
Secure Gateway:	1.1.1.1
My Address:	Any
Pre-Shared Key:	12345678
Certificate:	

Phase 1

Negotiation Mode:	Main
Encryption Algorithm:	AES128
Authentication Algorithm:	SHA1
Key Group:	DH2
SA Life Time:	86400
NAT Traversal:	Enable
Dead Peer Detection (DPD):	Enable

Phase 2

Encryption:	Tunnel
Encryption Algorithm:	AES128
Authentication Algorithm:	SHA1
SA Life Time:	86400
Perfect Forward Secrecy (PFS):	DH2

Policy

Local Policy (IP/Mask):	2.2.2.2/255.255.255.0
Remote Policy (IP/Mask):	3.3.3.3/255.255.255.0
Natted UP:	Disable

[Finish](#)

3.4 Wizard IPv6 Setup

Click the **IPv6 Setup** down arrow to configure the IPv6 settings on the VPN2S. Click **Next** to continue the Wizard, **Back** to return to the previous screen.

Figure 31 Wizard IPv6 Setup

The screenshot shows the 'IPv6 Setup' wizard's 'Welcome' screen. At the top, a green bar contains the word 'Welcome'. Below it, a white box with a blue header 'Welcome to IPv6 Setup' contains the text: 'Welcome to IPv6 Wizard. This wizard will help you to configure the VPN2S for IPv6 network environment.' To the right of this box are 'Back' and 'Next' buttons. On the left side, a vertical progress bar shows four steps: 1. Interface Setup (highlighted), 2. WAN setup, 3. LAN Setup, and 4. Summary.

- 6 Select the WAN interface on which you want to have an IPv6 connection. Select **Auto Detection** for the VPN2S to automatically detect the IPv6 Internet connection type, and the Wizard IPv6 setup is completed. If you want to enter a static IPv6 address or obtain it from a DHCP server click **Next**.

Figure 32 Interface Setup

The screenshot shows the 'Interface Setup' screen of the wizard. A green bar at the top says 'Welcome'. The main content area has a blue header 'Interface Setup' and the text 'WAN Interface:' followed by a dropdown menu. A red error icon is next to the dropdown. Below this is an unchecked checkbox labeled 'Auto Detection' and a note: '(Please connect your ethernet cable or telephone cable to auto detect the IPv6 setting via your service provider.)' 'Back' and 'Next' buttons are on the right. The left progress bar shows steps: 2. WAN setup (highlighted), 3. LAN Setup, and 4. Summary.

- 7 If you did not select **Auto Detection** the following screen displays. Use this screen to enter a static IPv6 address assigned by your ISP, and/or obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCP server has priority over the IP address automatically generated by the VPN2S.

Figure 33 WAN Setup

Welcome => Interface Setup

WAN Setup

IPv6 Address

☒ Obtain an IPv6 Address Automatically
☐ Static IPv6 Address

IPv6 Address:
 Prefix Length: (3-128)
 Default Gateway:

IPv6 DNS Server

☒ Obtain IPv6 DNS Info Automatically
☐ Use Following Static IPv6 DNS Address

DNS Server 1:
 DNS Server 2:

Back Next

3 LAN Setup
4 Summary

- 8 Use this screen to configure the LAN IPv6 settings of the VPN2S. Select **Delegate Prefix From WAN** to automatically obtain an IPv6 network prefix from the previously selected interface. Or select **Static** to configure a static IPv6 address for the VPN2S's LAN IPv6 address. Select the type of service that you are registered from your DNS service provider. Click **Next** to save your settings.

Figure 34 LAN Setup

Welcome => Interface Setup => WAN Setup

LAN Setup

Prefix

☒ Delegate Prefix From WAN
☐ Static

Static IPv6 Address Prefix:

IPv6 Address Assignment

☐ Auto Config
☒ DHCP Server

DNS Values

IPv6 DNS Server 1:
 IPv6 DNS Server 2:
 IPv6 DNS Server 3:

Back Next

- 9 A read-only summary of the IPv6 settings will display. Click **Finish** to exit the Wizard IPv6 Setup.

Figure 35 Summary

The screenshot shows a summary screen from a network configuration wizard. At the top, a green breadcrumb bar contains the text "Welcome ⇒ Interface Setup ⇒ WAN Setup ⇒ LAN Setup". Below this, the word "Summary" is displayed in blue. The settings are organized into two sections: "WAN" and "LAN".

WAN	
Address:	None
Gateway IP:	
DNS Server 1:	None
DNS Server 2:	None

LAN	
Address:	None
Mode:	Default PD from WAN
DNS Server 1:	DNS Proxy
DNS Server 2:	DNS Proxy

A blue "Finish" button is located in the bottom right corner of the main content area.

PART II

Technical Reference

CHAPTER 4

Dashboard

4.1 Overview

After you log into the Web Configurator, the **Dashboard** screen appears. This shows the network connection status of the VPN2S and clients connected to it.

You can use the **Dashboard** screen to look at the current status of the VPN2S, system resources, and interfaces (LAN and WAN).

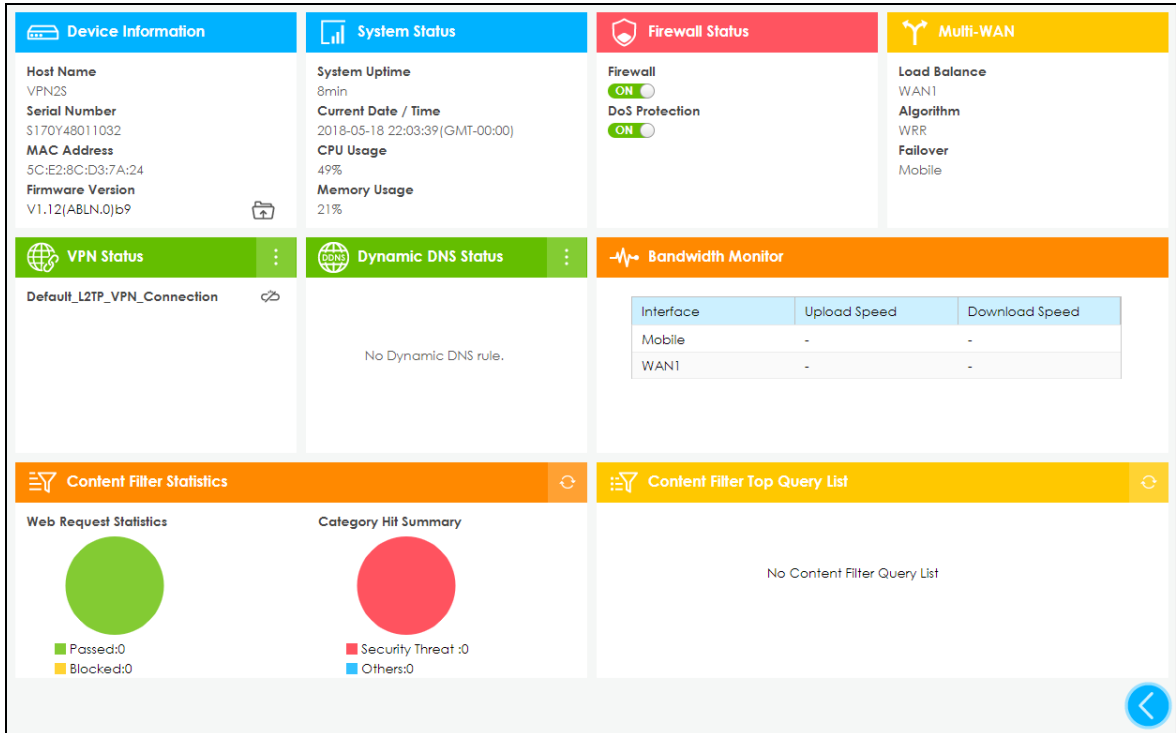
4.2 The Dashboard Screen

Use this screen to view the connections status of the VPN2S. When you click the **Dashboard** tab a network map opens. You can view the number of devices connected to the VPN2S. Click on each interface icon to view details about the VPN2S interfaces.

Figure 36 Dashboard Screen



If you prefer to view the status in a list, click the arrow icon  to show the Dashboard's list view.

Figure 37 Dashboard List View Screen

Each field is described in the following table.

Table 4 Dashboard List View Screen

LABEL	DESCRIPTION
Device Information	
Host Name	This field displays the name used to identify the VPN2S on any network.
Serial Number	This field displays the serial number of this VPN2S. The serial number is used for device tracking and control.
MAC Address	This field displays the MAC address used by the VPN2S.
Firmware Version	This field displays the present firmware version.
System Status	
System Uptime	This field displays how long the VPN2S has been running since it last restarted or was turned on.
Current Date / Time	This field displays the time in the VPN2S. Each time you reload this page, the VPN2S synchronizes the date with the time server.
CPU Usage	This field displays what percentage of the VPN2S's processing capability is currently being used.
Memory Usage	This field displays what percentage of the VPN2S's RAM is currently being used.
Firewall Status	
Firewall	Click the slide button to enable and disable the firewall on the VPN2S.
DoS Protection	Click the slide button to activate protection against DoS attacks.
Multi-WAN	
Load Balance	This shows the active WAN interfaces in the VPN2S.

Table 4 Dashboard List View Screen

LABEL	DESCRIPTION
Algorithm	<p>This field displays the type of load balancing algorithm currently used by the VPN2S.</p> <p>WRR (Weighted Round Robin) to balance the traffic load between interfaces based on their respective weights.</p> <p>LLF (Least Load First) to send new session traffic through the least utilized trunk member.</p> <p>SPILLOVER to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).</p>
Failover	This field displays the passive interfaces used for failover in the VPN2S.
VPN Status	This field displays the VPN2S's VPN connections and if the IP Sec SA is connected or disconnected.
Dynamic DNS Status	This field display the VPN2S's dynamic DNS and the interface each DDNS uses.
Bandwidth Monitor	
Interface	This field displays the name of each interface in the VPN2S.
Upload Speed	This displays interface's current upload link speed.
Download Speed	This displays interface's current download link speed.
Content Filter Statistics	
Web Request Statistics	<p>This displays the number of websites the VPN2S has grant access to versus the websites that have been blocked according to what you have selected in the Configuration > Security Service> Content Filter screen.</p>
Category Hit Summary	<p>This displays the number of requested managed web pages versus the ones with security threat categories you have selected in the Configuration > Security Service> Content Filter screen.</p>
Content Filter Top Query List	This displays the top categories of the web pages accessed by the VPN2S

CHAPTER 5

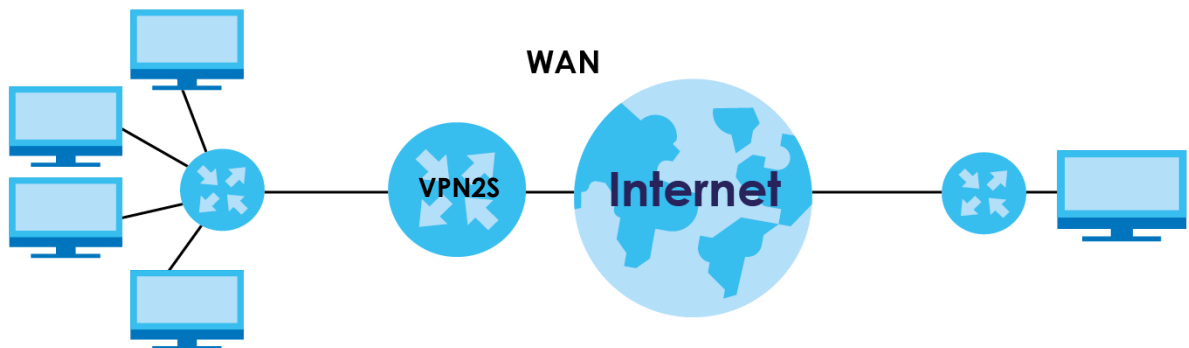
WAN/Internet

5.1 Overview

This chapter discusses the VPN2S's **WAN/Internet** screens. Use these screens to configure your VPN2S for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

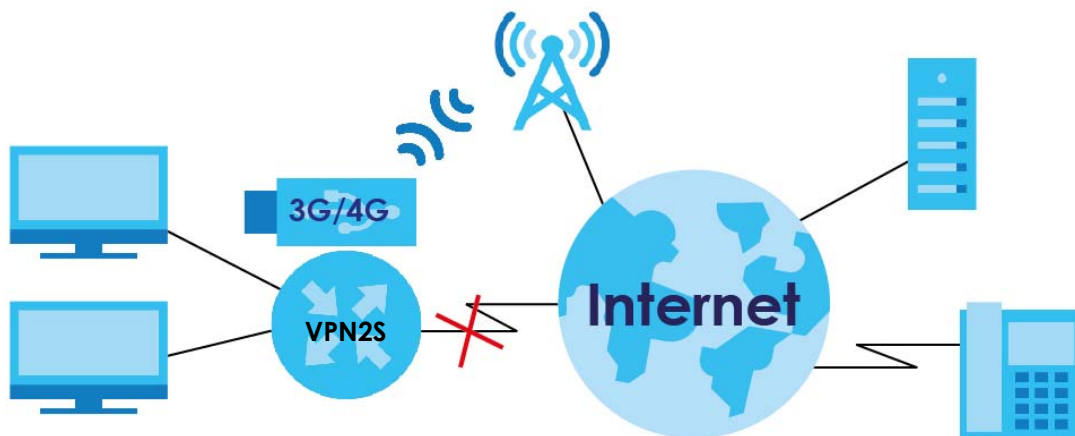
Figure 38 LAN and WAN



3G (third generation)/4G (fourth generation) standards are used for the sending and receiving of voice, video, and data in a mobile environment.

You can attach a 3G/4G wireless adapter to the USB port and set the VPN2S to use this 3G/4G connection as your WAN or a backup when the wired WAN connection fails.

Figure 39 Mobile WAN Connection



5.1.1 What You Can Do in this Chapter

- Use the **WAN Status** screen to view the WAN traffic statistics ([Section 5.3 on page 50](#)).
- Use the **WAN Setup** screen to view, remove or add a WAN interface. You can also configure the WAN settings on the VPN2S for Internet access ([Section 5.3 on page 50](#)).
- Use the **Mobile** screen to configure a 3G/4G WAN connection ([Section 5.4 on page 59](#)).
- Use the **Port Setting** screen to set flexible ports as part of LAN or WAN interfaces. ([Section 5.5 on page 63](#)).
- Use the **Multi-WAN** screen to configure the multiple WAN load balancing and failover rules to distribute traffic among different interfaces ([Section 5.6 on page 64](#)).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the VPN2S ([Section 5.7 on page 67](#)).

Table 5 WAN Setup Overview

LAYER-2 INTERFACE	INTERNET CONNECTION		
CONNECTION	MODE	ENCAPSULATION	CONNECTION SETTINGS
Ethernet	Routing	IPoE/PPPoE	PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
	Bridge	N/A	VLAN and QoS
3G	Nailed Up	PPP/IPoE	Dial string, APN (Access Point Name), IP address, DNS server
	On Demand	PPP/IPoE	Dial string, APN, Maximum idle time out, IP address, DNS server

5.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the VPN2S, which makes it accessible from an outside network. It is used by the VPN2S to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the VPN2S tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es).

3G / 4G

3G (Third Generation)/ 4G(Fourth Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only

allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses. The VPN2S can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

`2001:db8:1a2b:15::1a2f:0/32`

means that the first 32 bits (`2001:db8`) is the subnet prefix.

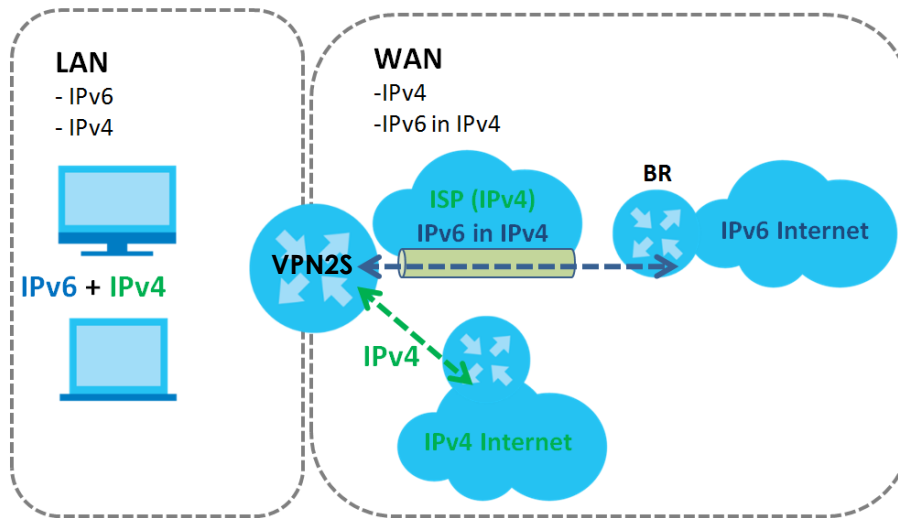
IPv6 Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, `FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000`.

IPv6 Rapid Deployment

Use IPv6 Rapid Deployment (6rd) when the local network uses IPv6 and the ISP has an IPv4 network. When the VPN2S has an IPv4 WAN address and you set **IPv4/IPv6 Mode** to **IPv4 Only**, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

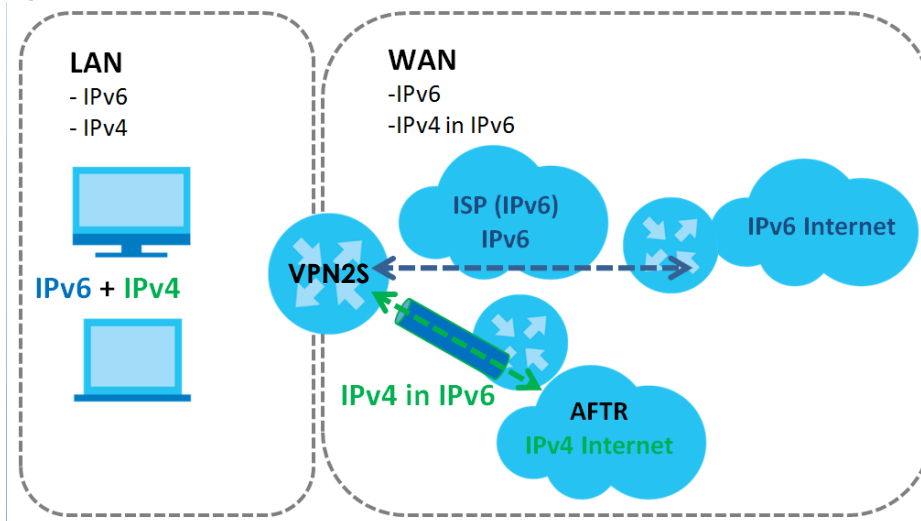
The VPN2S generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router (BR in the figure) to connect to the native IPv6 Internet. The local network can also use IPv4 services. The VPN2S uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 40 IPv6 Rapid Deployment

Dual Stack Lite

Use Dual Stack Lite when local network computers use IPv4 and the ISP has an IPv6 network. When the VPN2S has an IPv6 WAN address and you set **IPv4/IPv6 Mode** to **IPv6 Only**, you can enable Dual Stack Lite to use IPv4 computers and services.

The VPN2S tunnels IPv4 packets inside IPv6 encapsulation packets to the ISP's Address Family Transition Router (AFTR in the graphic) to connect to the IPv4 Internet. The local network can also use IPv6 services. The Router uses its configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 41 Dual Stack Lite

5.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

5.2 The WAN Status Screen

Use this screen to show the number of bytes received and sent on the VPN2S. Click **Configuration > WAN / Internet** to open the **WAN Status** screen.

Figure 42 Configuration > WAN / Internet > WAN Status

WAN Status					
WAN Status					
Refresh					
Name	Status	Tx Bytes	Rx Bytes	Tx Pkts	Rx Pkts
WAN1	Down	0	0	0	0

The following table describes the labels in this screen.

Table 6 Configuration > WAN / Internet > WAN Status

LABEL	DESCRIPTION
Refresh	Click this to update the table.
Name	This displays the name of the WAN interface.
Status	This shows Up if the connection to this interface is up, otherwise it will display Down .
Tx Bytes	This indicates the number of bytes transmitted on this interface.
Rx Bytes	This indicates the number of bytes received on this interface.
Tx Pkts	This indicates the number of transmitted packets on this interface.
Rx Pkts	This indicates the number of received packets on this interface.

5.3 The WAN Setup Screen

Use this screen to change your VPN2S's Internet access settings. Click **Configuration > WAN / Internet > WAN Setup** from the menu. The summary table shows you the configured WAN services (connections) on the VPN2S.

Figure 43 Configuration > WAN / Internet > WAN Setup

#	Status	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP ...	NAT	Default...	IPv6	MLD Proxy
1	ON	WAN1	ETH	Routing	IPoE	-	-	✓	✓	✓	✗	✗

The following table describes the labels in this screen.

Table 7 Configuration > WAN / Internet > WAN Setup

LABEL	DESCRIPTION
Add	Click this button to create a new WAN connection.
Edit	Click Edit to modify the WAN connection.
Remove	Click Remove to delete a WAN connection.
Multiple Entries Turn On	Select one or more WAN connections and click this to enable them. Use the [Shift] or [Ctrl] key to select multiple entries.
Multiple Entries Turn Off	Select one or more WAN connections and click this to disable them. Use the [Shift] or [Ctrl] key to select multiple entries.
#	This is the index number of the WAN connection.
Status	This field displays whether the connection is active or not. A green ON button signifies that this connection is active. A gray OFF button signifies that this connection is not active. Click the slide button to enable and disable the connection.
Name	This is the service name of the connection.
Type	This shows Ethernet connection.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.
802.1p	This indicates the IEEE 802.1p priority level assigned to traffic sent through this connection. This displays N/A when there is no priority level assigned.
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays N/A when there is no VLAN ID number assigned.
IGMP Proxy	This shows whether the VPN2S act as an IGMP proxy (green check mark) or not (red X) on this connection.
NAT	This shows whether NAT is activated (green check mark) or not (red X) for this connection.
Default Gateway	This shows whether the VPN2S use the WAN interface of this connection as the system default gateway (green check mark) or not (red X).
IPv6	This shows whether IPv6 is activated (green check mark) or not (red X) for this connection. IPv6 is not available when the connection uses the bridging service.
MLD Proxy	This shows whether Multicast Listener Discovery (MLD) is activated (green check mark) or not (red X) for this connection. MLD is not available when the connection uses the bridging service.

5.3.1 Internet Connection: Add/Edit

Click **Add** or **Edit** in the **Configuration > WAN / Internet > WAN Setup** screen to configure a WAN connection. The screen varies depending on the interface type, mode, encapsulation, and IPv4/IPv6 mode you select.

5.3.1.1 Routing Mode

Use **Routing** mode if your ISP give you one IP address only and you want multiple computers to share an Internet account.

The screen varies when you select other interface type, encapsulation, and IPv6/IPv4 mode.

Figure 44 WAN / Internet > WAN Setup > Add/Edit: Routing Mode

WAN Setup - Add

General | IPv6

General

☒ Interface Enable

Name:

Type:

Mode:

Encapsulation:

IPv4 / IPv6 Mode:

IPv4 Address

☒ Obtain an IP Address Automatically

☐ Use the Following IP Address

IP Address:

Subnet Mask:

Gateway IP:

Routing Feature

☒ Enable NAT

☐ Enable IGMP Proxy

☒ Apply as Default Gateway

DNS Server

☒ Obtain DNS Server Address Automatically

☐ Use the Following DNS Server Address

DNS Server 1:

DNS Server 2:

DHCP Client Options

Request Options:

☐ Option 43 ☐ Option 120 ☐ Option 121

Send Options:

☒ Option 60

Vendor Class ID:

☒ Option 61

IAID:

DUID Type:

Hardware Type:

Time:

Link-layer Address:

☒ Option 125

VLAN

☒ Enable

802.1p:

VLAN ID:

Interface Parameters

Egress Bandwidth: Kbps

Ingress Bandwidth: Kbps

MTU: (68~1500)

Connectivity Check

☐ Enable Connectivity Check

Check Method:

Check Period: (5 - 600 seconds)

Check Timeout: (1 - 10 seconds)

Check Fail Tolerance: (1 - 10)

☒ Check Default Gateway

☐ Check This Address (Domain Name or IP Address)

WAN MAC Address

☒ Factory Default

☐ Clone the computer MAC address-IP Address

IP Address:

☐ Set MAC Address

MAC Address:

OK Cancel

The following table describes the labels in this screen.

Table 8 WAN Internet > WAN Setup > Add/Edit: Routing Mode

LABEL	DESCRIPTION
General	
Interface Enable	Select this to activate the WAN configuration settings.
Name	Specify a descriptive name for this connection.
Type	This displays Ethernet when the VPN2S transmits data over the Ethernet WAN port.
Mode	Select Routing if your ISP give you one IP address only and you want multiple computers to share an Internet account.
Encapsulation	<p>Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select Routing in the Mode field.</p> <ul style="list-style-type: none"> • PPP over Ethernet (PPPoE): PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. Select this if you have a username and password for Internet access. • IP over Ethernet (IPoE): In this type of Internet connection, IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment.
IPv4/IPv6 Mode	<p>Select IPv4 Only if you want the VPN2S to run IPv4 only.</p> <p>Select IPv4 IPv6 Dualstack to allow the VPN2S to run IPv4 and IPv6 at the same time.</p> <p>Select IPv6 Only if you want the VPN2S to run IPv6 only.</p>
PPP Information	This is available only when you select PPPoE in the Encapsulation field.
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. Click Password Unmask to view the password you entered.
Connection Trigger	Select Auto Connect if you do not want the connection to time out. Select On Demand to specify the time of idle before the connection times out.
Idle Timeout	<p>This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.</p> <p>This field is not configurable if you select Auto Connect.</p>
PPPoE Passthrough	<p>This field is available when you select PPPoE encapsulation.</p> <p>In addition to the VPN2S'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 VPN2S. Each host can have a separate account and a public WAN IP address.</p> <p>PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.</p> <p>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.</p>
IPv4 Address	This is available only when you select IPv4 Only or IPv4 IPv6 Dualstack in the IPv4 / IPv6 Mode field.
Obtain an IP Address Automatically	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. Select this if you have a dynamic IP address.
Use the Following IP Address	Select this option if the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.

Table 8 WAN Internet > WAN Setup > Add/Edit: Routing Mode (continued)

LABEL	DESCRIPTION
Gateway IP Address	Enter the gateway IP address provided by your ISP.
Routing Feature	This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4 / IPv6 Mode field.
Enable NAT	Select this option to activate NAT on this connection.
Enable IGMP Proxy	<p>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.</p> <p>Select this option to have the VPN2S act as an IGMP proxy on this connection. This allows the VPN2S to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.</p>
Apply as Default Gateway	Select this option to have the VPN2S use the WAN interface of this connection as the system default gateway.
DNS Server	This is available only when you select IPv4 Only or IPv4 IPv6 Dualstack in the IPv4 / IPv6 Mode field.
Obtain DNS Server Address Automatically	Select this if you want the VPN2S to use the DNS server addresses assigned by your ISP.
Use the Following DNS Server Address	Select this if you want the VPN2S to use the DNS server addresses you configure manually.
DNS Server 1	Enter the first DNS server address.
DNS Server 2	Enter the second DNS server address.
DHCP Client Options	This is available only when you select IPv4 Only or IPv4 IPv6 Dualstack in the IPv4 / IPv6 Mode field.
Request Options	<ul style="list-style-type: none"> Select Option 43 to have the VPN2S automatically add vendor specific information in the DHCP packets to request the vendor specific options from the DHCP server. Select Option 120 to have the VPN2S get the IP address or a fully-qualified domain name of SIP server from the DHCP server. Select Option 121 to have the VPN2S get static route rules from the DHCP server.
Send Options	
Option 60	Select this and enter the device identity you want the VPN2S to add in the DHCP discovery packets that go to the DHCP server.
Vendor Class ID	Enter the Vendor Class Identifier, such as the type of the hardware or firmware.
Option 61	Select this and enter any string that identifies the device.
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DUID Type	<p>Select DUID-LLT to have the VPN2S use DUID-LLT (DUID Based on Link-layer Address Plus Time) for identification when exchanging DHCPv6 messages. You need to enter the hardware type, a time value and the MAC address of the device.</p> <p>Select DUID-EN to have the VPN2S use DUID-EN (DUID Assigned by Vendor Based upon Enterprise Number) for identification when exchanging DHCPv6 messages. You need to enter the vendor's registered enterprise number.</p> <p>Select DUID-LL to have the VPN2S use DUID-LL (DUID Based on Link-layer Address) for identification when exchanging DHCPv6 messages. You need to enter the device's hardware type and hardware address (MAC address).</p>
Hardware Type	Enter the device's hardware type, assigned by the IANA.
Time	Enter the time that the DUID is generated.

Table 8 WAN Internet > WAN Setup > Add/Edit: Routing Mode (continued)

LABEL	DESCRIPTION
Link-layer Address	Enter the VPN2S's hardware address, that is the MAC address.
Enterprise Number	Enter the vendor's registered private enterprise number. An enterprise number is a unique number that identifies a company.
Identifier	Enter a unique identifier assigned by the vendor.
Option 125	Select this to have the VPN2S automatically generate and add vendor specific parameters in the DHCP discovery packets that go to the DHCP server.
6RD	<p>Enable IPv6 rapid deployment to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.</p> <p>The 6RD (IPv6 rapid deployment) fields display when you set the IPv4 / IPv6 Mode field to IPv4 Only.</p>
Automatically configured by DHCP	<p>Select this to have the VPN2S detect IPv4 address automatically through DHCP.</p> <p>This option is configurable only when you set the method of encapsulation to IPoE.</p>
Manual Configuration	Select this to manually configure an IPv4 address of the relay server.
Service Provider IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's Border Relay router and connecting to the native IPv6 Internet.
IPv4 Mask Length	Enter the subnet mask number (1~32) for the IPv4 network.
Border Relay IPv4 Address	When you select Manual Configuration , specify the relay server IPv4 address.
VLAN	
Enable	Select this option to add the VLAN tag (specified below) to the outgoing traffic through this connection.
802.1p	<p>IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.</p> <p>Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.</p>
VLAN ID	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the VPN2S can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	<p>This is reserved for future use.</p> <p>Enter the maximum amount of traffic, in kilobits per second, the VPN2S can receive from the network through the interface. Allowed values are 0 - 1048576.</p>
MTU	<p>Enter the MTU (Maximum Transfer Unit) size for this traffic.</p> <p>Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the VPN2S divides it into smaller fragments. Allowed values are 68 -1492. Usually, this value is 1500.</p>
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the VPN2S stops routing to the gateway. The VPN2S resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.

Table 8 WAN Internet > WAN Setup > Add/Edit: Routing Mode (continued)

LABEL	DESCRIPTION
Check Method	Select the method that the gateway allows. Select ICMP to have the VPN2S regularly ping the gateway you specify to make sure it is still available. Select TCP to have the VPN2S regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the VPN2S stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check This Address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
WAN MAC Address	
Factory Default	Select this to use the factory default MAC address,
Clone the Computer MAC address-IP Address	Select this to clone the MAC address from a computer on your LAN. Type the IP address of the computer with the MAC address you are cloning.
Set MAC Address	Select this if you know the MAC address you want to use.
OK	Click OK to save your changes back to the VPN2S.
Cancel	Click Cancel to exit this screen without saving.

5.3.1.2 Bridge Mode

Click the **Add** or **Edit** in the **Configuration > WAN / Internet > WAN Setup** screen. Select **Bridge** as the device mode. The screen varies depending on the interface type you select.

Ethernet

If you select **Ethernet** as the interface type, the following screen appears.

Figure 45 WAN / Internet > WAN Setup > Add/Edit: Bridge Mode (Ethernet)

The following table describes the fields in this screen.

Table 9 WAN / Internet > WAN Setup > Add/Edit: Bridge Mode (Ethernet)

LABEL	DESCRIPTION
General	
Interface Enable	Select this to activate the WAN configuration settings.
Name	Enter a service name of the connection.
Type	Select Ethernet to have the VPN2S transmits data over the Ethernet WAN port.
Mode	Select Bridge when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select Bridge , you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
VLAN	
Enable	Select this to add the VLAN Tag (specified below) to the outgoing traffic through this connection.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
VLAN ID	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

5.3.1.3 IPv6

Click the **Add** or **Edit** in the **Configuration > WAN / Internet > WAN Setup** screen. Click the **IPv6** tab to configure an IPv6 WAN interface connection. This screen is available only when you select **IPv6 Only** or **IPv4 IPv6 Dualstack** in the **IPv4 / IPv6 Mode** field of the **WAN Setup > Add/Edit** screen.

Figure 46 WAN / Internet > WAN Setup > IPv6

WAN Setup - Add

General **IPv6**

IPv6 Address

☐ Obtain an IPv6 Address Automatically

☒ Static IPv6 Address

IPv6 Address:

Prefix Length:

Default Gateway:

IPv6 Routing Feature

☐ Enable MLD Proxy

☐ Apply as Default Gateway

IPv6 DNS Server

☐ Obtain IPv6 DNS Info Automatically

☒ Use Following Static IPv6 DNS Address

DNS Server 1:

DNS Server 2:

Tunnel

☒ Enable DS-Lite

DS-Lite Relay Server IP:

OK Cancel

The following table describes the labels in this screen.

Table 10 WAN / Internet > WAN Setup > IPv6

LABEL	DESCRIPTION
IPv6 Address	
Obtain an IPv6 Address Automatically	Select this if you want to have the VPN2S use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Static IPv6 Address	Select this if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the IPv6 address assigned by your ISP.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
Default Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your VPN2S's interface(s). The gateway helps forward packets to their destinations.
IPv6 Routing Feature	
Enable MLD Proxy	Select this check box to have the VPN2S act as an MLD proxy on this connection. This allows the VPN2S to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the VPN2S use the WAN interface of this connection as the system default gateway.
IPv6 DNS Server	
Obtain IPv6 DNS Info Automatically	Select this to have the VPN2S get the IPv6 DNS server addresses from the ISP automatically.
Use Following Static IPv6 DNS Address	Select Static to have the VPN2S use the IPv6 DNS server addresses you configure manually.

Table 10 WAN / Internet > WAN Setup > IPv6

LABEL	DESCRIPTION
DNS Server 1	Enter the first IPv6 DNS server address assigned by the ISP.
DNS Server 2	Enter the second IPv6 DNS server address assigned by the ISP.
Tunnel (This is available only when you select IPv6 Only in the IPv4 / IPv6 Mode field.)	
Enable DS-Lite	Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network.
DS-Lite Relay Server IP	Specify the transition router's IPv6 address.
OK	Click OK to save your changes back to the VPN2S.
Cancel	Click Cancel to exit this screen without saving.

5.4 The Mobile Screen

Use this screen to configure your 3G/4G settings. Click **Configuration > WAN / Internet > Mobile**.

Note: The actual data rate you obtain varies depending on the 3G/4G USB dongle you use, the signal strength to the service provider's base station, and so on.

Figure 47 Configuration > WAN / Internet > Mobile

Mobile

Connection Settings

Card Description:

Username:

Password:

Authentication Type:

PIN:

(The SIM card locks after 3 incorrect attempts.)

Dial String:

APN:

Connection:

Max Idle Timeout: Minute(s) (1 ~ 4320)

IP Address

Obtain an IP Address Automatically

Use the Following IP Address

IP Address:

Subnet Mask:

DNS

Obtain DNS info dynamically

Use the Following DNS Server Address

DNS Server 1:

DNS Server 2:

Connectivity Check

☐ Enable Connectivity Check

Check Method:

Check Period: (5 - 600 seconds)

Check Timeout: (1 - 10 seconds)

Check Fail Tolerance: (1 - 10)

Check Default Gateway

Check This Address (Domain Name or IP Address)

Check Port: (1 - 65535)

Budget Setup

☒ Enable

☐ Time Budget hours per month

☐ Data Budget Mbytes per month

☐ Data Budget kPackets per month

Reset All Budget Counters On : day of month:

Reset Time And Data Budget Counters :

Before Over Budget

If ...

☐ % of time budget

☐ % of data budget (Mbytes)

☐ % of data budget (Packets)

Then ...

☐ Enable Log

Interval: Minute(s)

When Over Budget

Current Connection:

Note:
 Budget Control is an approximate value.

The following table describes the labels in this screen.

Table 11 Configuration > WAN / Internet > Mobile

LABEL	DESCRIPTION
Connection Settings	
Card Description	This field displays the manufacturer and model name of your 3G/4G card if you inserted one in the VPN2S. Otherwise, it displays N/A .
Username	Type the user name (of up to 64 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 64 ASCII printable characters) associated with the user name above.
Authentication Type	Select an authentication type protocol for outgoing connection requests. Select Auto for the VPN2S to accept any protocol when requested by the remote node. Select CHAP to accept only CHAP and PAP for the VPN2S to accept only PAP .
PIN	<p>A PIN (Personal Identification Number) code is a key to a 3G/4G card. Without the PIN code, you cannot use the 3G/4G card.</p> <p>If your ISP enabled PIN code authentication, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the 3G/4G card may be blocked by your ISP and you cannot use the account to access the Internet.</p> <p>If your ISP disabled PIN code authentication, leave this field blank.</p>
Dial string	<p>Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number.</p> <p>For example, *99# is the dial string to establish a GPRS or 3G or 4G connection in Taiwan.</p>
APN	<p>Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method.</p> <p>You can enter up to 32 ASCII printable characters. Spaces are allowed.</p>
Connection	<p>Select Nailed UP if you do not want the connection to time out.</p> <p>Select on Demand if you do not want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.</p>
Max Idle Timeout	This value specifies the time in minutes that elapses before the VPN2S automatically disconnects from the ISP. This field is only available when you select On Demand in the Connection field.
IP Address	
Obtain an IP Address Automatically	Select this option If your ISP did not assign you a fixed IP address.
Use the following static IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected Use the following static IP address .
Subnet Mask	Enter the Subnet Mask provided by your ISP.
DNS	
Obtain DNS info dynamically	Select this to have the VPN2S get the DNS server addresses from the ISP automatically.
Use the Following DNS Server Address	Select this to have the VPN2S use the DNS server addresses you configure manually.
DNS server 1	Enter the first DNS server address assigned by the ISP.
DNS server 2	Enter the second DNS server address assigned by the ISP.

Table 11 Configuration > WAN / Internet > Mobile (continued)

LABEL	DESCRIPTION
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the VPN2S stops routing to the gateway. The VPN2S resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select ICMP to have the VPN2S regularly ping the gateway you specify to make sure it is still available. Select TCP to have the VPN2S regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the VPN2S stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check This Address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field is available when you select TCP in Check Method . Enter the port number to use for a TCP connection check.
Budget Setup	
Enable	Select this option to set a monthly limit for the user account of the installed 3G/4G card. You must insert a 3G/4G card before you enable budget control on the VPN2S. You can set a limit on the total traffic and/or call time. The VPN2S takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this option and specify the amount of time (in hours) that the 3G/4G connection can be used within one month. If you change the value after you configure and enable budget control, the VPN2S resets the statistics.
Data Budget	Select this option and specify the amount of data in Mega bytes or the number of packets that can be transmitted via the 3G/4G connection within one month. Select Download to set a limit on the downstream traffic (from the ISP to the VPN2S). Select Upload to set a limit on the upstream traffic (from the VPN2S to the ISP). Select Download/Upload to set a limit on the total traffic in both directions. If you change the value after you configure and enable budget control, the VPN2S resets the statistics.
Reset All Budget Counters On	Select the last or a specific day of the month to reset all budget counters. If the date you specified is not available in a month, such as 30th or 31th of February, the VPN2S resets the budget on the last day of the month.
Reset Time And Data Budget Counters	Click this button to reset the time and data budgets immediately. The count starts over with the 3G/4G connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart.
Before Over Budget	Enter a number from 1 to 99 in the percentage fields. The VPN2S takes actions when the specified percentage of time budget or data limit is exceeded. If you change the value after you configure and enable budget control, the VPN2S resets the statistics.

Table 11 Configuration > WAN / Internet > Mobile (continued)

LABEL	DESCRIPTION
Enable Log	Select this to activate the logging function at the interval you set in the Interval field.
Interval	Enter the time interval (in minutes) at which the VPN2S creates log messages.
When Over Budget	Specify the actions the VPN2S takes when the time or data limit is exceeded.
Current connection	Select Keep to maintain the existing 3G/4G connection or Drop to disconnect it when the data transmission is over the set budget.
Apply	Click Apply to save your changes back to the VPN2S.
Reset	Click Reset to return to the previous configuration.

5.5 The Port Setting Screen

Click **Configuration > WAN / Internet > Port Setting** to display the following screen. Use the **Port Setting** screen to set the VPN2S flexible ports as part of the **LAN** or **WAN** interfaces. This creates a hardware connection between physical ports at the layer 2 (data link, MAC address level).

Note the following if you are configuring from a computer connected to a **LAN** or **WAN** port and change the port's role:

- A port's IP address varies as its role changes. Make sure your computer's IP address is in the same subnet as the VPN2S's **LAN** or **WAN** IP address.
- Use the appropriate **LAN** or **WAN** IP address to access the VPN2S.

Figure 48 Configuration > WAN / Internet > Port Setting

The physical Ethernet ports are shown at the bottom and the Ethernet interfaces are shown at the bottom of the screen. Use the radio buttons to select for which interface (network) you want to use each physical port. For example, select a port's **LAN** radio button to use the port as part of the **LAN** interface. The port will use the VPN2S's **LAN** IP address and MAC address.

Note: You will notice when Port 4 is WAN, Port 5 can only be WAN, this is because Port 5 has a better performance as WAN and Port 4 works as failover.

Click **Apply** to save your changes and apply them to the VPN2S.

Click **Reset** to change the port groups to their current configuration (last-saved values).

5.6 The Multi-WAN Screen

Use the **Multi-WAN** screen to configure the multiple WAN load balance and failover rules to distribute traffic among different interfaces. This helps to increase overall network throughput and reliability. Load balancing divides traffic loads between multiple interfaces. This allows you to improve quality of service and maximize bandwidth utilization for multiple ISP links.

You can only configure one rule for each interface. Click **Configuration > WAN / Internet > Multi-WAN** to display the following screen.

Figure 49 Configuration > WAN / Internet > Multi-WAN

Multi-WAN

Configuration

☐ Disconnect Connections Before Falling Back

System Default

[Edit](#)

#	Name	Algorithm
1	SYSTEM_DEFAULT_WAN_TRUNK	WRR

Page 1 of 1 | Show 20 items | Displaying 1 - 1 of 1

[Apply](#) [Reset](#)

The following table describes the labels in this screen.

Table 12 Configuration > WAN / Internet > Multi-WAN

LABEL	DESCRIPTION
Configuration	
Disconnect Connections Before Falling Back	Select this to terminate existing connections on an interface which is set to passive mode when any interface set to active mode in the same trunk comes back up.
System Default	The VPN2S automatically adds all external interfaces into the pre-configured system default SYSTEM_DEFAULT_WAN_TRUNK . You cannot delete it.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the label to identify the trunk.
Algorithm	This field displays the load balancing method the trunk is set to use.
Apply	Click Apply to save your changes to the VPN2S.
Reset	Click Reset to return the screen to its last-saved settings.

5.6.1 Multi-WAN: Edit

Select an existing multi-WAN and click **Edit** in the **Multi-WAN** screen to configure it.

Figure 50 Multi-WAN: Edit

Multi-WAN - Edit

Name:

Load Balancing Algorithm:

#	Member	Mode	Weight
1	WAN1	Active	1
2	Mobile	Passive	1

Page 1 of 1 | Show 20 items | Displaying 1 - 2 of 2

The following table describes the labels in this screen.

Table 13 Multi-WAN: Edit

LABEL	DESCRIPTION
Name	This field displays the label to identify the trunk.
Load Balancing Algorithm	<p>Select a load balancing method to use from the drop-down list box.</p> <p>Select Weighted Round Robin to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the VPN2S chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions.</p> <p>Select Least Load First to send new session traffic through the least utilized trunk member.</p> <p>Select Spillover to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).</p>
Load Balancing Index(es)	<p>This field is available if you selected to use the Least Load First or Spillover method.</p> <p>Select Outbound, Inbound, or Outbound + Inbound to set the traffic to which the VPN2S applies the load balancing method. Outbound means the traffic traveling from an internal interface (ex. LAN) to an external interface (ex. WAN). Inbound means the opposite.</p>
	The table lists the trunk's member interfaces. You can add, edit, remove, or move entries for user configured trunks.
Add	Click this to add a member interface to the trunk. Select an interface and click Add to add a new member interface after the selected member interface.
Edit	Select an entry and click Edit to modify the entry's settings.
Remove	To remove a member interface, select it and click Remove .
Move	To move an interface to a different number in the list, click the Move icon. In the field that appears, specify the number to which you want to move the interface.
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	Click this table cell and select an interface to be a group member.

Table 13 Multi-WAN: Edit (continued)

LABEL	DESCRIPTION
Mode	Click this table cell and select Active to have the VPN2S always attempt to use this connection. Select Passive to have the VPN2S only use this connection when all of the connections set to active are down. You can only set one of a group's interfaces to passive mode.
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. This ratio determines how much traffic the VPN2S assigns to each member interface. The higher an interface's weight is (relative to the weights of the interfaces), the more sessions that interface should handle.
Ingress Bandwidth	This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the VPN2S is to allow to come in through the interface per second. Note: You can configure the bandwidth of an interface in the corresponding interface edit screen.
Egress Bandwidth	This field displays with the least load first or spillover load balancing algorithm. It displays the maximum number of kilobits of data the VPN2S is to send out through the interface per second. Note: You can configure the bandwidth of an interface in the corresponding interface edit screen.
Total Bandwidth	This field displays with the spillover load balancing algorithm. It displays the maximum number of kilobits of data the VPN2S is to send out and allow to come in through the interface per second. Note: You can configure the bandwidth of an interface in the corresponding interface edit screen.
Spillover	This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the VPN2S sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started. The VPN2S uses the group member interfaces in the order that they are listed.
OK	Click OK to save your changes back to the VPN2S.
Cancel	Click Cancel to exit this screen without saving.

5.6.2 How to Configure Multi-WAN for Load Balancing and Failover

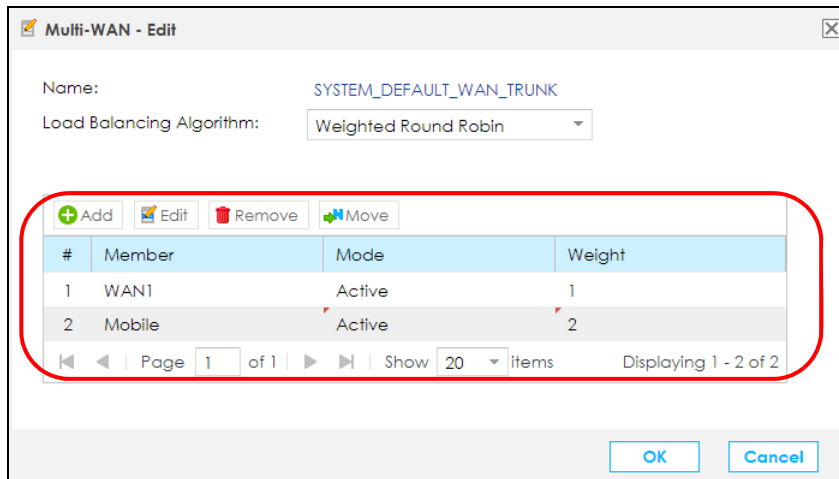
This example shows you how to configure multi-WAN for three WAN connections: an Ethernet WAN connection and a 3G/4G (mobile) WAN connection. The available bandwidth for the Ethernet WAN connection is 3 Mbps.

As these two wired WAN connections have different bandwidths, you can set multi-WAN to send traffic over these WAN connections in a 3:2 ratio. Most 3G/4G WAN connections charge the user for the amount of data sent, so you can set multi-WAN to send traffic over the 3G/4G WAN connection only if all other WAN connections are unavailable.

5.6.2.1 Configuring Multi-WAN

- 1 Click **Configuration > WAN / Internet > Multi-WAN > Edit**. By default, all available WAN connections on the VPN2S are in active mode with a weight of 1, except for the mobile WAN connection which is set to passive mode.

- 2 Select the Ethernet WAN (**WAN1**) connection and click **Edit**. Change the weight field to **1** and change **Mobile**'s weight to **2**. Click the **OK** button.



- 3 You have finished the configuration. When both the Ethernet WAN and Mobile connections are up, the VPN2S will send traffic over these two connections in a 3:2 ratio. When only one of these two connections are up, the VPN2S will use that connection exclusively. Only when both of these two connections are down will the VPN2S use the mobile WAN connection.

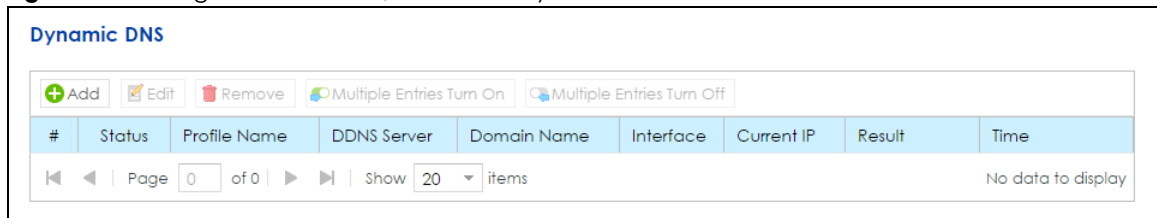
5.6.2.2 What Can Go Wrong?

- There can only be one WAN connection configured as passive mode at a time. If there is already a WAN connection configured as passive mode, you will not be able to add or edit another WAN connection in passive mode until the first WAN connection is changed to active mode or deleted.
- The VPN2S will automatically add newly created WAN connections (from the **WAN / Internet > WAN Setup** screen) to the multi-WAN configuration as active mode with a weight of 1. If you are creating a new WAN connection for other purposes (such as exclusive VPN use), you will need to delete that WAN connection from the multi-WAN configuration. Deleting a WAN connection from the multi-WAN screen does not delete the WAN connection from the **WAN Setup** page.
- A WAN connection can only be listed once in the multi-WAN configuration table.

5.7 The Dynamic DNS screen

Use this screen to change your VPN2S's DDNS. Click **Configuration > WAN / Internet > Dynamic DNS**. The screen appears as shown.

Figure 51 Configuration > WAN / Internet > Dynamic DNS



The following table describes the labels in this screen.

Table 14 Configuration > WAN / Internet > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS	
Add	Click this to add a dynamic DNS.
Edit	Select an entry and click Edit to modify the dynamic DNS's settings.
Remove	To remove an Dynamic DNS, select it and click Remove .
Multiple Entries Turn On	Select one or more dynamic DNS entries and click this to enable them.
Multiple Entries Turn Off	Select one or more dynamic DNS entries and click this to disable them.
#	This is the number of an individual dynamic DNS.
Status	This field displays whether the dynamic DNS is active or not. A green ON button signifies that this dynamic DNS is active. A gray OFF button signifies that this dynamic DNS is not active.
Profile Name	This field displays the descriptive profile name for this entry.
DDNS Server	This shows your Dynamic DNS service provider.
Domain Name	This shows the domain name assigned to your VPN2S by your Dynamic DNS provider.
Interface	This field displays the interface to use for updating the IP address mapped to the domain name.
Current IP	This shows the IP address your Dynamic DNS provider has currently associated with the Profile Name.
Result	Accept - displays when DDNS profile was updated to server successfully. Not Accept - displays when DDNS profile is there was a problem during sync process. Login Fail - displays when a DDNS profile is incorrect and it failed
Time	This shows the last time the IP address the Dynamic DNS provider has associated with the profile name was updated.

5.7.1 Dynamic DNS: Add/Edit

Click **Add** or select an existing dynamic DNS and click **Edit** in the **Dynamic DNS** screen to configure it.

Figure 52 Dynamic DNS: Add/Edit

Dynamic DNS - Add

☐ Enable

General Settings

Profile Name:

DDNS Type:

DDNS Account

Username:

Password:

DDNS Settings

Domain Name:

Primary Binding Address:

Interface:

☐ Enable Wildcard Option

☐ Enable off line Option (only applies to custom DNS)

OK Cancel

The following table describes the labels on this screen.

Table 15 Dynamic DNS: Add/Edit

LABEL	DESCRIPTION
Enable	Select Enable to use this dynamic DNS.
General	
Profile Name	When you are adding a dynamic DNS entry, type a descriptive name for this DDNS entry in the VPN2S. You may use 1-32 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
DDNS Type	Select your Dynamic DNS service provider from the drop-down list box.
DDNS Account	
Username	Type the user name used when you registered your domain name. You can use up to 32 alphanumeric characters and the underscore. Spaces are not allowed.
Password	Type the password provided by the DDNS provider. You can use up to 32 alphanumeric characters and the underscore. Spaces are not allowed.
DDNS Settings	
Domain Name	Type the domain name you registered. You can use up to 256 alphanumeric characters.
Primary Binding Address	
Interface	Select the interface to use for updating the IP address mapped to the domain name.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard. Enable the wildcard feature to alias subdomains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.
Enable off line Option (only applies to custom DNS)	This option applies for custom DNS. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.

Table 15 Dynamic DNS: Add/Edit

LABEL	DESCRIPTION
OK	Click OK to save your changes back to the VPN2S and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

5.8 Technical Reference

The following section contains additional technical information about the VPN2S features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The VPN2S can work in bridge mode or routing mode. When the VPN2S is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

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 VPN2S (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the VPN2S does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

Multicast

IP packets are transmitted in either one of two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

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. 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. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of

all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the VPN2S queries all directly connected networks to gather group membership. After that, the VPN2S periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of `www.zyxel.com` is `204.217.0.2`. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The VPN2S can get the DNS server addresses in the following ways.

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- 2 If your ISP dynamically assigns the DNS server IP addresses (along with the VPN2S's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as `"/x"` where `x` is a number. For example,

`2001:db8:1a2b:15::1a2f:0/32`

means that the first 32 bits (`2001:db8`) is the subnet prefix.

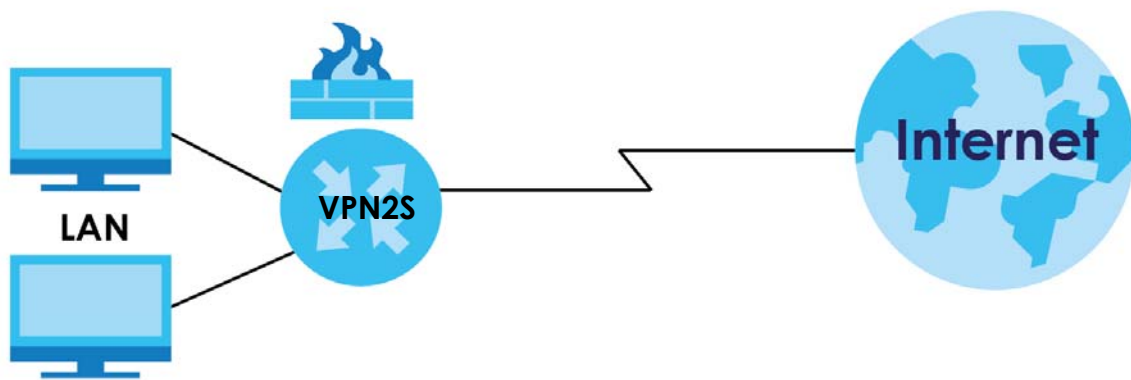
CHAPTER 6

LAN

6.1 Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is usually located in one immediate area such as a building or floor of a building.

Use the LAN screens to help you configure a LAN DHCP server and manage IP addresses.



6.1.1 What You Can Do in this Chapter

- Use the **LAN Status** screen to show the status of interfaces currently connected to the VPN2S ([Section 6.2 on page 75](#)).
- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings of your VPN2S ([Section 6.2 on page 75](#)).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses ([Section 6.4 on page 82](#)).
- Use the **Additional Subnet** screen to configure IP alias ([Section 6.5 on page 84](#)).
- Use the **Wake on LAN** screen to remotely turn on a device on the network ([Section 6.6 on page 84](#)).
- Use the **VLAN / Interface Group** screen to create multiple networks on the VPN2S ([Section 6.7 on page 86](#)).
- Use the **DNS Entry** screen to view, configure or remove DNS routes ([Section 6.8 on page 91](#)).
- Use the **DNS Forwarder** screen to view and configure domain zone forwarder on the VPN2S ([Section 6.9 on page 91](#)).

6.1.2 What You Need To Know

6.1.2.1 About LAN

IP Address

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 Mask

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.

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your VPN2S an IP address, subnet mask, DNS and other routing information when it's turned on.

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a networking device before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **LAN Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The VPN2S supports the IPCP DNS server extensions through the DNS proxy feature.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **LAN Setup** screen.

RADVD (Router Advertisement Daemon)

When an IPv6 host sends a Router Solicitation (RS) request to discover the available routers, RADVD with Router Advertisement (RA) messages in response to the request. It specifies the minimum and maximum intervals of RA broadcasts. RA messages containing the address prefix. IPv6 hosts can be generated with the IPv6 prefix an IPv6 address.

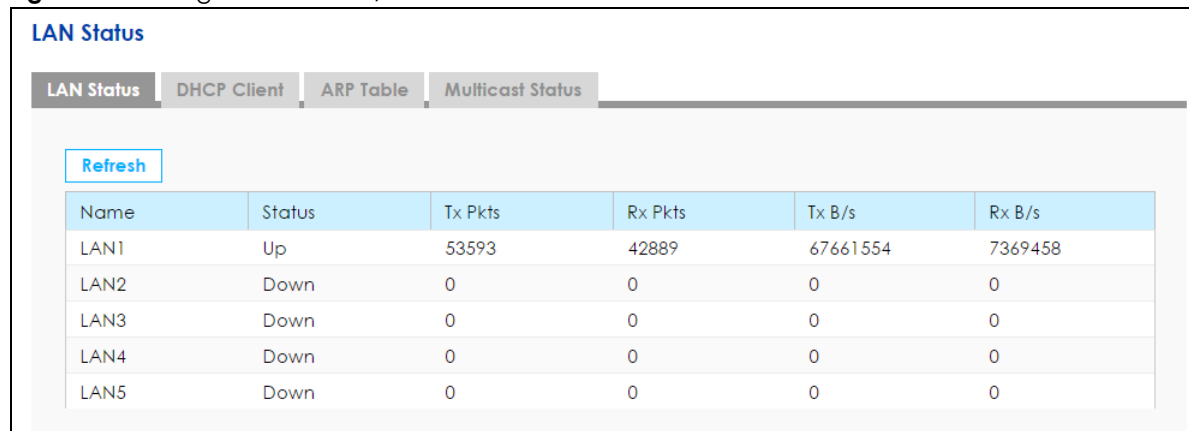
6.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

6.2 The LAN Status Screen

Use the LAN Status Screen to view the status of all interfaces connected to the VPN2S, details about DHCP clients. Click on **Configuration > LAN / Home Network > LAN Status** to open the following screen. The tables change depending on the table you click on.

Figure 53 Configuration > LAN / Home Network > LAN Status



The screenshot shows the 'LAN Status' screen with a title bar and four tabs: 'LAN Status', 'DHCP Client', 'ARP Table', and 'Multicast Status'. The 'LAN Status' tab is selected. Below the tabs is a 'Refresh' button. A table displays the status of five LAN interfaces (LAN1 to LAN5).

Name	Status	Tx Pkts	Rx Pkts	Tx B/s	Rx B/s
LAN1	Up	53593	42889	67661554	7369458
LAN2	Down	0	0	0	0
LAN3	Down	0	0	0	0
LAN4	Down	0	0	0	0
LAN5	Down	0	0	0	0

The following table describes the labels in the screen.

Table 16 Configuration > LAN / Home Network > LAN Status

LABEL	DESCRIPTION
Refresh	Click this to update the table.
LAN Status	Click this to show the interfaces currently connected to the VPN2S.
Name	This shows the name of the LAN interface.
Status	This shows Up if the VPN2S detect a connection through this port. Otherwise it shows Down .
Tx Pkts	This is the number of transmitted packets on this port.
Rx Pkts	This is the number of received packets on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
DHCP Client	Click this to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses.
#	This field is a sequential value, and it is not associated with a specific entry.
Device Name	This field displays the name used to identify this device on the network (the computer name). The VPN2S learns these from the DHCP client requests. "None" shows here for a static DHCP entry.

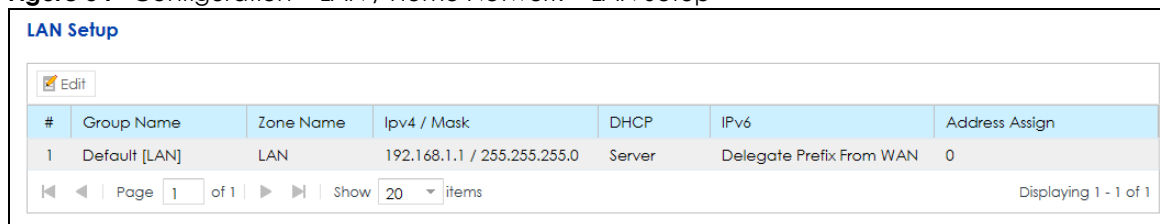
Table 16 Configuration > LAN / Home Network > LAN Status

LABEL	DESCRIPTION
IP Address	This field displays the DHCP client's IP address.
MAC Address	This field displays the MAC address to which the IP address is currently assigned or for which the IP address is reserved.
ARP Table	
Click this to view IP-to-MAC address mapping(s).	
#	This is the ARP table entry number.
IP Address	This is the learned IPv4 or IPv6 IP address of a device connected to a port.
MAC Address	This is the MAC address of the device with the listed IP address.
Interface	This is the interface used by the ARP entry.
Multicast Status	
Click this to look at the current list of multicast groups the VPN2S has joined and which ports have joined it.	
#	This is the multicast status table entry number.
Type	This is the protocol used by the interface.
Interface	This field displays the name of an interface on the VPN2S that belongs to an IGMP multicast group.
Multicast Group	This field displays the name of the IGMP multicast group to which the interface belongs.
Host	This shows the clients that are part of this multicast group.

6.3 The LAN Setup Screen

Use this screen to set the Local Area Network IP address and subnet mask of your VPN2S. Click **Configuration > LAN / Home Network** to open the **LAN Setup** screen.

Figure 54 Configuration > LAN / Home Network > LAN Setup



The screenshot shows the 'LAN Setup' screen with an 'Edit' button. Below it is a table with the following data:

#	Group Name	Zone Name	Ipv4 / Mask	DHCP	IPv6	Address Assign
1	Default [LAN]	LAN	192.168.1.1 / 255.255.255.0	Server	Delegate Prefix From WAN	0

At the bottom of the table, there is a pagination bar showing 'Page 1 of 1', 'Show 20 items', and 'Displaying 1 - 1 of 1'.

The following table describes the labels in this screen.

Table 17 Configuration > LAN / Home Network > LAN Setup

LABEL	DESCRIPTION
Edit	Select an entry and click Edit to modify it.
#	This field is a sequential value, and it is not associated with a specific entry.
Group Name	This field shows the interface group name.
Zone Name	This field shows the security zone (LAN , WLAN , DMZ , or EXTRA) in which the LAN interface is included.
IPv4 / Mask	This field displays the LAN IPv4 address assigned to your VPN2S and the subnet mask of your network in dotted decimal notation.

Table 17 Configuration > LAN / Home Network > LAN Setup

LABEL	DESCRIPTION
DHCP	This shows whether the VPN2S acts as DHCP Server or DHCP Relay agent. It shows Disable if the DHCP server has been stopped in the VPN2S.
IPv6	This shows the IPv6 prefix and prefix length you configured when you enable IPv6 on the LAN interface and set
Address Assign	<p>This field displays 1 when the IPv6 address is assigned using IPv6 stateful autoconfiguration (DHCPv6) or 0 when the VPN2S uses IPv6 stateless autoconfiguration.</p> <ul style="list-style-type: none"> Stateless: The VPN2S send IPv6 prefix information in router advertisements periodically and in response to router solicitations. Stateful: The DHCPv6 server is enabled to have the VPN2S act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.

6.3.1 LAN Setup: Edit

In **Configuration > LAN / Home Network** screen select an entry and click **Edit** to open the following screen.

Figure 55 LAN Setup: Edit > General / IPv4

LAN Setup

General / IPv4 | IPv6

General

Group Name: Default [LAN]

Zone: LAN

IPv4 / IPv6 Mode: IPv4 IPv6 Dualstack

IPv4 Address Setting

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

IGMP Snooping

☒ Enable IGMP Snooping

IGMP Mode: ☒ Standard Mode ☐ Blocking Mode

DHCP Setting

DHCP Mode: DHCP Server

Beginning IP Address: 192.168.1.2

Ending IP Address: 192.168.1.254

Lease Time: 1 Day 0 Hour 0 Minute(s)

DNS Server 1: DNS Proxy

DNS Server 2: DNS Proxy

DHCP Option Setup

TFTP Server Name(option 66):

Bootfile Name(option 67):

TFTP Server Address(option 150):

OK Cancel

The following table describes the fields in this screen.

Table 18 LAN Setup: Edit > General / IPv4

LABEL	DESCRIPTION
General	
Group Name	Select the interface group name for which you want to configure LAN settings. See Section 6.7 on page 86 for how to create a new interface group/VLAN.
Zone	Select the security zone (LAN , WLAN , DMZ , or EXTRA) in which to include the LAN interface. A newly created local network (interface group) belongs to the LAN zone by default.
IPv4 / IPv6 Mode	Select IPv4 only if you want the VPN2S to run IPv4 only. Select IPv4 IPv6 Dualstack to allow the VPN2S to run IPv4 and IPv6 at the same time.
IPv4 Address Setting	
IP Address	Enter the LAN IP address you want to assign to your VPN2S in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your VPN2S automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
IGMP Snooping	
Enable IGMP Snooping	Select the check box to allow the VPN2S to passively learn multicast group.
IGMP Mode	Select Standard Mode to have the VPN2S forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select Blocking Mode to have the VPN2S block all unknown multicast packets from the WAN.
DHCP Setting	
DHCP Mode	Select DHCP Server to have the VPN2S act as a DHCP server. Select DHCP Relay to have the VPN2S act as a DHCP relay agent and forward DHCP request to the DHCP server you specify. Select DHCP Disable to stop the DHCP server on the VPN2S.
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Lease Time	This is the period of time DHCP-assigned addresses use. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. This field is only available when you select DHCP Server in the DHCP Mode field.
DNS Server 1	Specify the IP address of the first DNS server for the DHCP clients to use. Use one of the following ways to specify the IP address. DNS Proxy - the clients use the IP address of the VPN2S LAN interface. The VPN2S redirects clients' DNS queries to a DNS server for resolving domain names. Static - enter a static IP address. From Wan Interface - select the WAN interface that receives the DNS server address from its DHCP server.

Table 18 LAN Setup: Edit > General / IPv4 (continued)

LABEL	DESCRIPTION
DNS Server 2	Specify the IP address of the secondary DNS server for the DHCP clients to use. Use one of the following ways to specify the IP address. DNS Proxy - the clients use the IP address of the VPN2S LAN interface. The VPN2S redirects clients' DNS queries to a DNS server for resolving domain names. Static - enter a static IP address. From Wan Interface - select the WAN interface that receives the DNS server address from its DHCP server.
Remote DHCP Server	Enter the DHCP server's address so the VPN2S forwards DHCP requests to this address. This field is only available when you select DHCP Relay .
DHCP Option Setup	These fields display when you select DHCP Server in the DHCP Mode field. You may need to configure them when you have VoIP phones on your LAN.
TFTP Server Name (option 66)	Enter the name of a TFTP server to assign it to the DHCP clients.
Bootfile Name (option 67)	Enter the name of a bootfile to assign it to the DHCP clients.
TFTP Server Address (option 150)	Enter the IP address of a TFTP server to assign it to the DHCP clients.
OK	Click OK to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

6.3.2 LAN Setup IPv6: Edit

Click the **IPv6** tab in **Configuration > LAN / Home Network > LAN Setup > Edit** to configure IPv6 LAN settings on the VPN2S. This screen is available only when you select **IPv4 IPv6 Dualstack** in the **IPv4 / IPv6 Mode** field of the **LAN Setup > Edit > General / IPv4** screen.

Figure 56 LAN Setup: Edit > IPv6

LAN Setup - Edit

General / IPv4 / **IPv6**

Link Local Address

Static IPv6 Address Prefix: FE80::

Link Local Address Type: ☐ Manual ☒ EUI-64

LAN Identifier: 1e74:0dff:fe8:2380

IP Address: FE80::1e74:0dff:fe8:2380

Address Setting

☒ Delegate Prefix From WAN WAN1

☐ Static

LAN Global Identifier Type: ☐ Manual ☒ EUI-64

LAN Identifier: 1e74:0dff:fe8:2380

Router Advertisement State

LAN Address Assign Setup: Stateless / Auto

LAN DNS Assign Setup: From DHCPv6 Server

DHCPv6 Setting

DHCPv6 Status: DHCPv6 Server

IPv6 Start Address: 0:0:0:2

IPv6 End Address: 0:0:0:ffff

IPv6 Domain Name:

DNS Values

IPv6 DNS Server 1: DNS Proxy

IPv6 DNS Server 2: DNS Proxy

IPv6 DNS Server 3: DNS Proxy

Note:
The LAN IPv6 Identifier cannot be abbreviated. Please enter the complete address.
For example: Please enter '0:0:0:2' instead of '::2' or '2'

OK Cancel

The following table describes the labels in this screen.

Table 19 Configuration > LAN / Home Network > LAN Setup: Edit > IPv6

LABEL	DESCRIPTION
Link Local Address	
Static IPv6 Address Prefix	This shows the static IPv6 address prefix used to represent the VPN2S network address.
Link Local Address Type	Select EUI-64 to give clients a 64-bit Extended Unique Identifier (EUI) to link locally without DHCP. Select Manual to manually enter an interface ID for the LAN interface's global IPv6 address.
LAN Identifier	Enter an interface ID for the LAN interface's global IPv6 address.
IP address	This field shows an IPv6 address created using the Static IPv6 Address Prefix and the LAN Identifier you input.
Address Setting	
Delegate Prefix From WAN	Select this option and a WAN interface with IPv6 enabled to automatically obtain an IPv6 network prefix from the service provider or an uplink router through the specified WAN interface.

Table 19 Configuration > LAN / Home Network > LAN Setup: Edit > IPv6

LABEL	DESCRIPTION
Static	Select this option to configure a fixed IPv6 address for the VPN2S's LAN interface. Note: This fixed address is for local hosts to access the Web Configurator only as the global LAN IPv6 address might be changed by your ISP any time. This address is not the routing gateway's address for LAN IPv6 hosts.
Static IPv6 Address Prefix	Enter the address prefix to represent the VPN2S's static LAN IPv6 address.
Prefix Length	If you select Static , enter the IPv6 prefix length that the VPN2S uses to generate the LAN IPv6 address. An IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.
LAN Global Identifier Type	Select EUI-64 to allow clients to assign themselves a 64-bit Extended Unique Identifier (EUI) without DHCP. Select Manual if you want to enter the LAN identifier the clients use.
LAN Identifier	Enter the LAN identifier clients use without DHCP.
IP Address	This field shows an IPv6 address created using the Static IPv6 Address Prefix and the LAN Identifier you input.
Route Advertisement State	
LAN Address Assign Setup	Select how you want to obtain an IPv6 address: <ul style="list-style-type: none"> • Stateless / Auto: The VPN2S uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the VPN2S send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. • Stateful / DHCP: The VPN2S uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the VPN2S act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.
LAN DNS Assign Setup	Select how the VPN2S provide DNS server and domain name information to the clients: <ul style="list-style-type: none"> • From Router Advertisement: The VPN2S provides DNS information through router advertisements. • From DHCPv6 Server: The VPN2S provides DNS information through DHCPv6.
DHCPv6 Setting	
DHCPv6 Status	This shows the status of the DHCPv6. DHCPv6 Server displays if you configured the VPN2S to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.
IPv6 Start Address	If DHCPv6 is enabled, specify the first IPv6 address in the pool of addresses that can be assigned to DHCPv6 clients.
IPv6 End Address	If DHCPv6 is enabled, specify the last IPv6 address in the pool of addresses that can be assigned to DHCPv6 clients.
IPv6 Domain Name	If DHCPv6 is enabled, specify the domain name to be assigned to DHCPv6 clients.
DNS Values	
IPv6 DNS Server 1-3	Select From WAN Interface if your ISP dynamically assigns IPv6 DNS server information. Select Static if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the VPN2S passes to the DHCP clients. Select DNS Proxy if you have the DNS proxy service. The VPN2S redirects clients' DNS queries to a DNS server for resolving domain names.

Table 19 Configuration > LAN / Home Network > LAN Setup: Edit > IPv6

LABEL	DESCRIPTION
OK	Click OK to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

6.4 The Static DHCP Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

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.

Use this screen to change your VPN2S's static DHCP settings. Click **Configuration > LAN / Home Network > Static DHCP** to open the following screen.

Figure 57 Configuration > LAN / Home Network > Static DHCP

Static DHCP

#	Status	MAC Address	IP Address
1	<input type="radio"/> OFF	00:a0:c5:01:23:45	192.168.1.99
2	<input checked="" type="radio"/> ON	C0:35:DF:E6:78:23	192.168.1.100

Page 1 of 1
 20 items
 Displaying 1 - 2 of 2

The following table describes the labels in this screen.

Table 20 Network Setting > LAN > Static DHCP

LABEL	DESCRIPTION
Add	Click this to add a new static DHCP entry.
Edit	Click Edit to configure a static DHCP entry.
Remove	Click Remove to delete a static DHCP entry.
Multiple Entries Turn On	Select one or more static DHCP entry and click this to enable them.
Multiple Entries Turn Off	Select one or more static DHCP entry and click this to disable them.
#	This is the index number of the DHCP entry.
Status	This field displays whether the entry is active. Click the slide button to turn on or turn off the entry.
MAC Address	This field displays the MAC address of a computer on the LAN.
IP Address	This field displays the IP address relative to the MAC address field listed above.

6.4.1 Static DHCP: Add/Edit

If you click **Add** in the **Static DHCP** screen or **Edit** next to a static DHCP entry, the following screen displays.

Figure 58 Static DHCP: Add/Edit

Static DHCP Configuration

☐ Enable

Group Name: Default [LAN]

Select Device Info: Manual Input

MAC Address:

IP Address:

Note:
Release / renew your device's IP Address or disconnect / reconnect from the router to receive a new IP Address.

OK Cancel

The following table describes the labels in this screen.

Table 21 Static DHCP: Add/Edit

LABEL	DESCRIPTION
Static DHCP Configuration	
Enable	Select this to activate the rule.
Group Name	Select the interface group name for which you want to configure static DHCP settings. See Section 6.7 on page 86 for how to create a new interface group.
Select Device Info	If you select Manual Input , you can manually type in the MAC address and IP address of a computer on your LAN. You can also choose the name of a computer from the drop list and have the MAC Address and IP Address auto-detected.
MAC Address	If you select Manual Input , enter the MAC address of a computer on your LAN.
IP Address	If you select Manual Input , enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

6.5 The Additional Subnet Screen

Use the **Additional Subnet** screen to configure IP alias.

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The VPN2S supports multiple logical LAN interfaces via its physical Ethernet interface with the VPN2S itself as the gateway for the LAN network. When you use IP alias, you can also configure firewall rules to control access to the LAN's logical network (subnet).

Click **Configuration > LAN / Home Network > Additional Subnet** to display the screen shown next.

Figure 59 Configuration > LAN / Home Network > Additional Subnet

The following table describes the labels in this screen.

Table 22 Configuration > LAN / Home Network > Additional Subnet

LABEL	DESCRIPTION
General	
Group Name	Select the interface group name for which you want to configure the IP alias settings. See Section 6.7 on page 86 for how to create a new interface group. A newly created local network (interface group) belongs to the LAN zone by default.
IP Alias Setup	
Enable	Select the check box to configure a LAN network for the VPN2S.
IP Address	Enter the IP address of your VPN2S in dotted decimal notation.
Subnet Mask	Your VPN2S 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 VPN2S.
Apply	Click Apply to save your changes.
Reset	Click Reset to return the screen to its last-saved settings.

6.6 The Wake on LAN Screen

Use this screen to turn on a device on the LAN network. To use this feature, the remote device must also support Wake On LAN.

You need to know the MAC address of the LAN device. It may be on a label on the device or in its documentation.

Figure 60 Configuration > LAN / Home Network > Wake on LAN

The following table describes the labels in this screen.

Table 23 Configuration > LAN / Home Network > Wake on LAN

LABEL	DESCRIPTION
Add	Click this to add a new device to Wake on LAN.
Remove	Select a static DHCP entry and click Remove to delete it.
Wake Up	Select a device and click this to enable the Wake on LAN feature.
#	This field is a sequential value, and it is not associated with any entry.
Description	This field shows a descriptive name for a device on the LAN network.
MAC Address	This field shows the MAC address for a device on the LAN network.

6.6.1 Wake On LAN: Add/Edit

Use this screen to add a device and turn it on using Wake on LAN. Click **Edit** to open the following screen.

Figure 61 Wake On LAN: Edit

The following table describes the labels in this screen.

Table 24 Configuration > LAN / Home Network > Wake on LAN

LABEL	DESCRIPTION
Wake From	
Manual Type MAC	Select this to enter the MAC address of the device to turn it on remotely.
Host Name List	Select this to look at the list of hosts connected to the VPN2S.
Host Name List	This is drop-down list that shows the IP addresses that can be found in the VPN2S's LAN Site Host list, see Section 16.2 on page 216 . Select a host and it will then automatically update the Description and MAC address fields.
Get MAC Address From IP	If you selected Manual Type MAC you can enter a device's IP address and click Get to obtain its MAC address.
Description	Enter a descriptive name for the device you want to turn on.
MAC Address	Enter the MAC address of the device to turn it on. A MAC address consists of six hexadecimal character pairs.
Add New Host to Profile	Select this check box to add this Host to the LAN Site Host list in the Maintenance > LAN Site Host Name screen, see Section 16.2 on page 216 .

6.7 The VLAN / Interface Group Screen

Use Interface Group to create multiple networks on the VPN2S. You can manually add a LAN interface to a new group. Alternatively, you can have the VPN2S automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the LAN screen to configure the private IP addresses the DHCP server on the VPN2S assigns to the clients in the default and/or user-defined groups. If you set the VPN2S to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups.

Click **Configuration > LAN / Home Network > VLAN / Interface Group** to open the following screen.

Figure 62 Configuration > LAN / Home Network > VLAN / Interface Group

VLAN / Interface Group				
<div> + Add Edit Remove </div>				
#	Mode	Group Name	LAN Interface	Criteria
1	VLAN	Default [LAN]	LAN1,LAN2,LAN3,LAN4	
<div> ◀ ▶ Page 1 of 1 Show 20 items <div>Displaying 1 - 1 of 1</div> </div>				

The following table describes the labels on this screen.

Table 25 Configuration > LAN / Home Network > VLAN / Interface Group

LABEL	DESCRIPTION
VLAN/ Interface Group	
Add	Click Add to create a new interface group.
Edit	Click Edit to configure an interface group.
Remove	Click Remove to delete an interface group.

Table 25 Configuration > LAN / Home Network > VLAN / Interface Group

LABEL	DESCRIPTION
#	This shows the index number of the interface group.
Mode	This shows VLAN when this is a VLAN group. This shows Interface Group when this is an interface group.
Group Name	This shows the descriptive name of the group.
LAN Interface	This shows the LAN interfaces in the group.
Criteria	This shows the filtering criteria for the group.

6.7.1 VLAN / Interface Group: Add/Edit

If you click **Add** in the **VLAN / Interface Group** screen or select an existing group and click **Edit** the screen displays as shown below.

The screen varies depending on whether you create a **VLAN Group** or an **Interface Group**.

Figure 63 VLAN / Interface Group: Add/Edit (VLAN Group)

VLAN / Interface Group - Add

VLAN / Interface Group

Group Name:

Mode

☒ VLAN

☐ Interface Group (To Bridge / Bundle WAN Interfaces)

802.1p:

802.1q: (1~4094)

VLAN Port Membership

#	Interface	Member	TX Tagged
1	LAN1	<input type="checkbox"/>	<input type="checkbox"/>
2	LAN2	<input type="checkbox"/>	<input type="checkbox"/>
3	LAN3	<input type="checkbox"/>	<input type="checkbox"/>
4	LAN4	<input type="checkbox"/>	<input type="checkbox"/>

Automatically Add Clients With The Following DHCP Vendor IDs

#	Criteria	Wildcard Support
No data to display		

Page 0 of 0 | Show 20 items

Figure 64 VLAN / Interface Group: Add/Edit (Interface Group)

VLAN / Interface Group - Add

VLAN / Interface Group
Group Name:

Mode
☒ VLAN
☐ Interface Group (To Bridge / Bundle WAN Interfaces)

802.1p:
802.1q: (1~4094)

VLAN Port Membership

#	Interface	Member	TX Tagged
1	LAN1	<input type="checkbox"/>	<input type="checkbox"/>
2	LAN2	<input type="checkbox"/>	<input type="checkbox"/>
3	LAN3	<input type="checkbox"/>	<input type="checkbox"/>
4	LAN4	<input type="checkbox"/>	<input type="checkbox"/>

Automatically Add Clients With The Following DHCP Vendor IDs

#	Criteria	Wildcard Support
No data to display		

OK Cancel

The following table describes the labels in this screen.

Table 26 VLAN / Interface Group > Add/Edit

LABEL	DESCRIPTION
VLAN / Interface Group	
Group Name	Enter the descriptive name of the VLAN or Interface Group. You can enter up to 65 characters. You can use numbers, letters, hyphens (-) and underscores(_). Spaces are not allowed.
Mode	
VLAN	Click this check box to create a VLAN group.
Interface Group (To Bridge / Bundle WAN Interfaces)	Click this check box to create an interface group.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC layer frame that contains bits to define class of service. Select the IEEE 802.1p priority (from 0 to 7) to add to traffic the VPN2S sends through tagged member ports of this group. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 1 to 4094) for traffic through tagged member ports of this group. A VLAN ID cannot be assigned to more than one group.
VLAN Port Membership	
#	This shows the index number of the interface.

Table 26 VLAN / Interface Group > Add/Edit

LABEL	DESCRIPTION
Interface	This shows the VPN2S LAN interfaces.
Member	Select this check box to add the LAN interface to the group. Clear the Tagged check box to add the LAN interface as an untagged member port. A LAN interface can be added as an untagged member port of at most one group. Ethernet LAN interfaces that have already been added as an untagged member port of another group will have this check box disabled. It is still possible to add these LAN interfaces to the group as tagged member ports.
TX Tagged	Select this check box to add the LAN interface to the group as a tagged member port.
VLAN Group(s)	
Add	Click this to add a new VLAN group.
Remove	Select a VLAN group and click this to delete it.
#	This shows the index number of the VLAN group.
802.1q	This shows the VLAN ID number (from 1 to 4094) for traffic through tagged member ports of this group. A VLAN ID cannot be assigned to more than one group.
Interfaces	This shows the LAN ports included in the VLAN group and if traffic leaving the port will be tagged with the VLAN ID.
WAN Interface Used In This Group	
Add	Click this to add a new WAN interface for an interface group.
Remove	Select a WAN interface and click this to delete it.
WAN Type	This field displays the current WAN connection type.
WAN Interface	This field displays the current WAN interface.
Automatically Add Clients With The Following DHCP Vendor IDs	Click Add to identify LAN hosts to add to the interface group by criteria such as the type of the hardware or firmware.
Add	Click this to add a new rule.
Edit	Select a rule and click this to modify it.
Remove	Select a rule and click this to delete it.
#	This shows the index number of the rule.
Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
Wildcard Support	This shows if wildcard on DHCP option 60 is enabled.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

6.7.1.1 Add WAN Interface Used In This Group

Click **Add** in the **WAN Interface Used In This Group** table to display the following screen.

Figure 65 WAN Interface Use In This Group: Add

The screenshot shows a dialog box titled "WAN Interface Used In This Group - Add". Inside the dialog, there are two labels with corresponding dropdown menus: "WAN Type:" and "WAN Interface:". Both dropdown menus are currently set to "Mobile". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

The following table describes the labels in this screen.

Table 27

LABEL	DESCRIPTION
WAN Type	Select the current WAN connection type.
WAN Interface	Select the current WAN interface.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

6.7.1.2 Add Clients With The Following DHCP Vendor IDs

Click **Add** in the **Clients With The Following DHCP Vendor IDs** table to display the following screen.

Figure 66 Clients With The Following DHCP Vendor IDs: Add

The following table describes the labels in this screen.

Table 28 Clients With The Following DHCP Vendor IDs: Add

LABEL	DESCRIPTION
Criteria	
DHCP Option 60	Select this to enter STB's Vendor Class Identifiers (DHCP Option 60). Type the class vendor ID you want the VPN2S to add in the DHCP Discovery packets that go to the DHCP server in the Vendor Class ID field.
Enable Wildcard	Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60.
DHCP Option 61	Click this to enter the Identity Association Identifier (IAD Option 61) of the matched traffic such as the MAC address of the device. Type the DHCP Unique Identifier (DUID) you want the VPN2S to add in the DHCP Discovery packets that go to the DHCP server.
DHCP Option 125	Click this to enter the vendor specific information of the matched traffic, such as the Enterprise Number , Manufacture OUI , Serial Number and Product Class of the device.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

6.8 The DNS Entry Screen

Use this screen to view and configure DNS routes on the VPN2S. Click **Configuration > LAN / Home Network > DNS Entry** screen.

Figure 67 Configuration > LAN / Home Network > DNS Entry

#	Host Name	IP Address
No data to display		

The following table describes the labels in this screen.

Table 29 Configuration > LAN / Home Network > DNS Entry

LABEL	DESCRIPTION
Add	Click this to create a new DNS rule.
Edit	Click Edit to modify a DNS rule.
Remove	Click Remove to delete an existing DNS rule.
#	This is the index number of the rule.
Host Name	This indicates the host or domain name.
IP Address	This indicates the IP address assigned to this computer.

6.9 The DNS Forwarder Screen

A domain zone forwarder contains a DNS server's IP address. The VPN2S can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. 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. Use this screen to create domain zone forwarder records. Click **Configuration > LAN / Home Network > DNS Forwarder** to open the following screen.

Figure 68 Configuration > LAN / Home Network > DNS Forwarder

#	Domain Name	Mode	DNS Server	Interface
No data to display				

The following table describes the labels in this screen.

Table 30 Configuration > LAN / Home Network > DNS Forwarder

LABEL	DESCRIPTION
Add	Click this to add a domain zone forwarder record.
Edit	Select an existing domain zone forwarder record and click Edit to modify it.
Remove	Click this to delete a domain zone forwarder record.
#	This is the index number of the domain zone entry.
Domain Name	This shows the domain zone.
Mode	This shows whether the DNS server is user-designed or from the ISP.
DNS Server	If the Mode is User Defined Address , this field displays the IP address of the DNS server.
Interface	This shows the interface through which the VPN2S sends DNS queries to a DNS server.

6.9.1 DNS Forwarder: Add/Edit

If you click **Add** in the **DNS Forwarder** screen or select a domain zone forwarder record and click **Edit**, the following screen displays.

Figure 69 DNS Forwarder: Add/Edit

The following table describes the labels in this screen.

Table 31 Configuration > LAN / Home Network > DNS Forwarder

LABEL	DESCRIPTION
Domain Name	Enter the domain zone in this field. A domain zone is a fully qualified domain name without the host. For example, *.zyxel.com.tw is a wildcard domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the VPN2S looks up a domain name that ends in zyxel.com.tw domain name, it can send a query to the recorded name server IP address.
DNS Server	
DNS Server From ISP	Select DNS Server(s) from ISP if your ISP dynamically assigns DNS server information. You also need to select an interface through which the ISP provides the DNS server IP address(es). The interface should be activated and set to be a DHCP client.
DNS Server	Select DNS Server if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Use the Interface field to select the interface through which the VPN2S sends DNS queries to a DNS server.

Table 31 Configuration > LAN / Home Network > DNS Forwarder

LABEL	DESCRIPTION
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

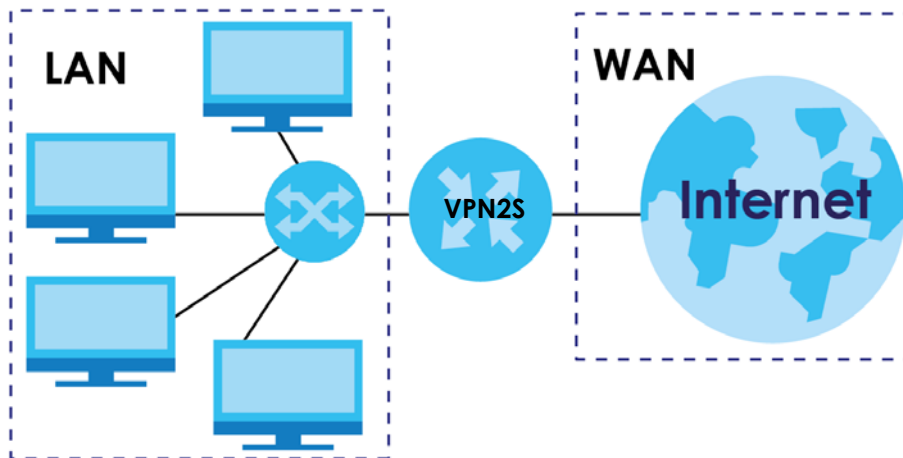
6.10 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

6.10.1 LANs, WANs and the VPN2S

The actual physical connection determines whether the VPN2S ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 70 LAN and WAN IP Addresses



6.10.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the VPN2S as a DHCP server or disable it. When configured as a server, the VPN2S provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The VPN2S is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

6.10.3 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The VPN2S supports the IPCP DNS server extensions through the DNS proxy feature.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

6.10.4 LAN TCP/IP

The VPN2S has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so do computers on a LAN share one common network number.

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 and you must enable the Network Address Translation (NAT) feature of the VPN2S. 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. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your VPN2S, 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 VPN2S 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 VPN2S 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, for example, only between your two branch offices, 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.

Note: 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".

CHAPTER 7

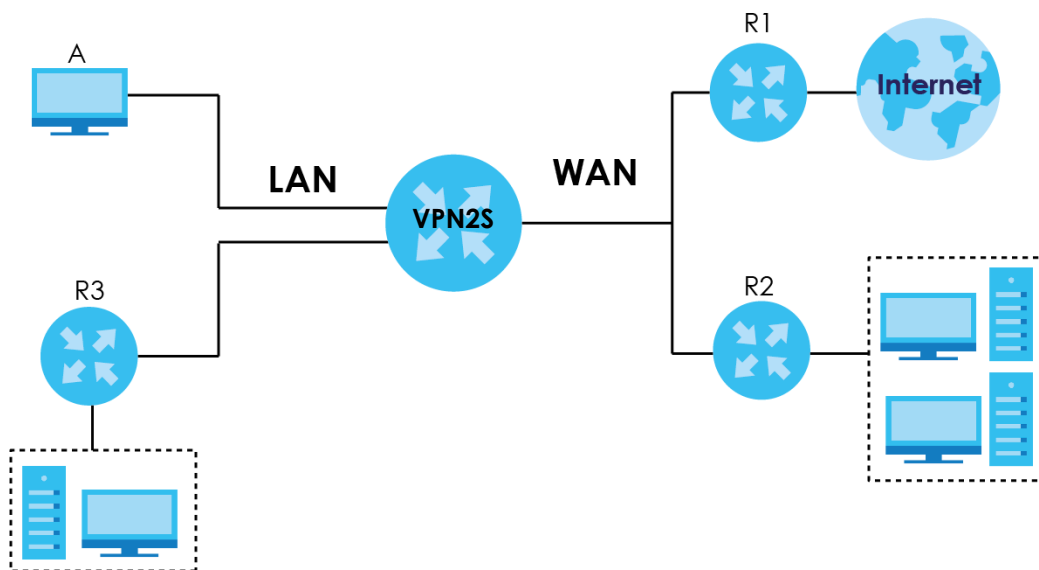
Routing

7.1 Overview

The VPN2S usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the VPN2S send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the VPN2S's LAN interface. The VPN2S routes most traffic from **A** to the Internet through the VPN2S's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 71 Example of Routing Topology



7.1.1 What You Can Do in this Chapter

- Use the **Routing Status** screen to view the IPv4 and IPv6 routing flow([Section 7.2 on page 97](#)).
- Use the **Policy Route** screen to configure policy routing on the VPN2S ([Section 7.3 on page 103](#)).
- Use the **Static Route** screen to view and set up static routes on the VPN2S ([Section 7.4 on page 106](#)).
- Use the **RIP** screen to set up RIP settings on the VPN2S ([Section 7.5 on page 108](#)).

7.2 The Routing Status Screen

The **Routing Status** screen allows you to view the current routing flow and quickly link to specific routing settings. Click a function box in the **Routing Flow** section, the related routes (activated) will display in the Routing Table section. To access this screen, click **Configuration > Routing > Routing Status**.

Note: Once a packet matches the criteria of a routing rule, the VPN2S takes the corresponding action and does not perform any further flow checking.

Figure 72 Configuration > Routing > Routing Status (IPsec)

Routing Status

Routing Flow

IPsec

Note:
If you want to configure IPsec, please go to [IPsec](#).

#	VPN Connection	Local Policy	Remote Policy
Page 0 of 0 Show 20 items No data to display			

Figure 73 Configuration > Routing > Routing Status (Direct Route)

Routing Status

Routing Flow

Direct Route

Destination	Subnet Mask	Interface
192.168.1.0	255.255.255.0	Default [LAN]

Page 0 of 0 | Show 20 items | Displaying 1 - 1 of 1

Figure 74 Configuration > Routing > Routing Status (Policy Route)

Routing Status

Routing Flow

Policy Route

Note:
If you want to configure Policy Route, please go to [Policy Route](#).

IPv4 Routing Table

#	Name	Source IP	Source Port	Destination IP	Destination ...	Protocol	Next-Hop
Page 0 of 0 Show 20 items No data to display							

IPv6 Routing Table

#	Name	Source IP	Source Port	Destination IP	Destination ...	Protocol	Next-Hop
Page 0 of 0 Show 20 items No data to display							

Figure 75 Configuration > Routing > Routing Status (L2TP Server)

Routing Status

Routing Flow

L2TP Server

Note:
If you want to configure L2TP Server, please go to [L2TP Server](#).

#	Destination	Username	Host Name
Page 0 of 0 Show 20 items No data to display			

Figure 76 Configuration > Routing > Routing Status (PPTP Route)

Routing Status

Routing Flow

PPTP Route

Note:
If you want to configure PPTP Route, please go to [PPTP Route](#).

#	Destination	Username	Host Name
Page 0 of 0 Show 20 items No data to display			

Figure 77 Configuration > Routing > Routing Status (GRE VPN)

Routing Status

Routing Flow

GRE VPN

Note:
If you want to configure GRE Tunnel, please go to [GRE VPN](#).

#	Tunnel Name	Destination IP	Subnet Mask	Interface
Page 0 of 0 Show 20 items No data to display				

Figure 78 Configuration > Routing > Routing Status (Static Route)

Routing Status

Routing Flow

Static Route

Note:
If you want to configure Static Route, please go to [Static Route](#).

IPv4 Routing Table

#	Name	Destination IP	Gateway IP	Interface
Page 0 of 0 Show 20 items No data to display				

IPv6 Routing Table

#	Name	Destination IP	Gateway IP	Interface
Page 0 of 0 Show 20 items No data to display				

Figure 79 Configuration > Routing > Routing Status (Dynamic Route (RIP))

Routing Status

Routing Flow

Dynamic Route(RIP)

Note:
If you want to configure Dynamic Route(RIP), please go to [Dynamic Route\(RIP\)](#).

#	Destination IP	Gateway IP	Interface	Protocol	Metric
Page 0 of 0 Show 20 items No data to display					

Figure 80 Configuration > Routing > Routing Status (Multi-WAN)

Routing Status

Routing Flow

Multi-WAN

Note:
If you want to configure Multi-WAN, please go to [Multi-WAN](#).

Name: `SYSTEM_DEFAULT_WAN_TRUNK`

Load Balancing Algorithm: `Weighted Round Robin`

#	Member	Mode	Weight
1	WAN1	Active	1
2	Mobile	Passive	1

Page 0 of 0 | Show 20 items | Displaying 1 - 2 of 2

Figure 81 Configuration > Routing > Routing Status (Main Table)

Routing Status

Routing Flow

Main Table

IPv4 Routing Table

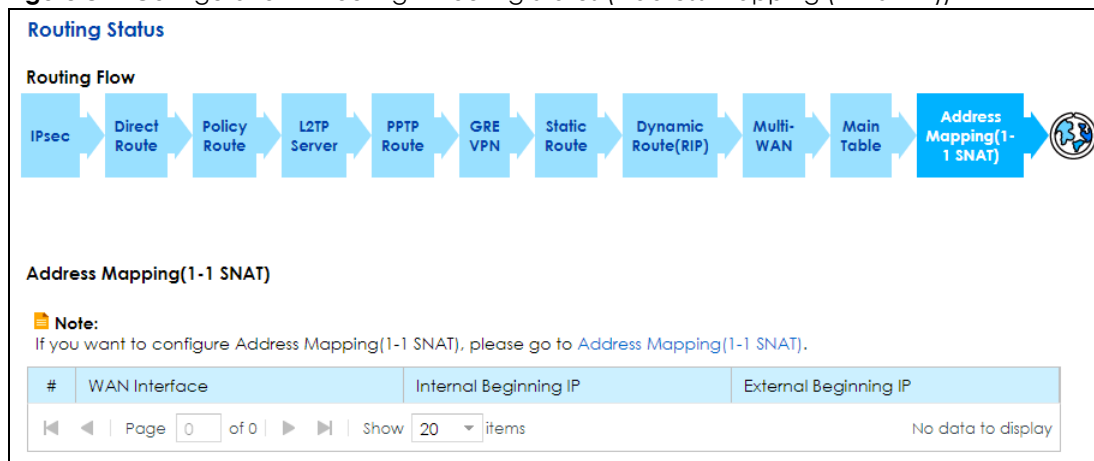
Destination IP	Gateway IP	Subnet Mask	Flag	Metric	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	Default [LAN]

Page 0 of 0 | Show 20 items | Displaying 1 - 1 of 1

IPv6 Routing Table

Destination IP	Gateway IP	Flag	Metric	Interface
fd00::5ee2:8cff:fed3:7a24...	::	U	1024	Default [LAN]
fd00::/64	::	U	1024	Default [LAN]
fd00::5ee2:8cff:fed3:7a24...	::	U	256	Default [LAN]
fd00::/64	::	U	1024	Default [LAN]
fd00:0:0:ffff::/64	::	U	1024	Default [LAN]
fe80::/64	::	U	256	Default [LAN]
fe80::/64	::	U	256	Default [LAN]
ff00::/8	::	U	256	Default [LAN]
ff00::/8	::	U	256	Default [LAN]

Page 0 of 0 | Show 20 items | Displaying 1 - 9 of 9

Figure 82 Configuration > Routing > Routing Status (Address Mapping (1-1 SNAT))

The following table describes the labels in this screen.

Table 32 Configuration > Routing > Routing Status

LABEL	DESCRIPTION
Routing Flow	This section shows you the flow of how the VPN2S determines where to route a packet. Click a function box to display the related settings in the next section.
	This section shows the corresponding settings according to the function box you click in the Routing Flow section.
The following fields are available if you click IPsec in the Routing Flow section.	
#	This is the IPsec VPN policy index number.
VPN Connection	This field displays the identification name for this VPN policy.
Local Policy	This field displays the local policy.
Remote Policy	This field displays the remote policy.
The following fields are available if you click Direct Route in the Routing Flow section.	
Destination	This is the destination IP address of a route.
Subnet Mask	This is the subnet mask of a route.
Interface	This is the name of an interface associated with the route.
The following fields are available if you click Policy Route in the Routing Flow section.	
#	This is the number of an individual policy route.
Name	This field displays the descriptive name of the policy route.
Source IP	This is the name of the source IP address (group) object. Any means all IP addresses.
Destination IP	This is the name of the destination IP address (group) object. Any means all IP addresses.
Source Port	This displays the port (0-65535) the source IP address(es) are using in this policy route rule.
Destination Port	This displays the port (0-65535) the destination IP address(es) are using in this policy route rule.
Protocol	This shows the kind of protocol used by this policy route rule (TCP , UDP or None).
Next-Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel, outgoing interface or trunk.
The following fields are available if you click L2TP Server and PPTP Route in the Routing Flow section.	
#	This is the PPTP/L2TP VPN policy index number.
Destination	This is the original destination IP address(es) to which the packets are transmitted.

Table 32 Configuration > Routing > Routing Status

LABEL	DESCRIPTION
Username	This field displays the client's login name for this connection.
Host Name	This is the client's host name of this connection.
The following fields are available if you click GRE VPN in the Routing Flow section.	
#	This is the GRE VPN policy index number.
Tunnel Name	This field displays the identification name for this GRE VPN policy.
Destination IP	This field displays the destination IP address of the GRE tunnel.
Subnet Mask	This field displays the IP network subnet mask of the GRE remote subnet.
Interface	This field displays the WAN interface this GRE VPN policy uses.
The following fields are available if you click Static Route in the Routing Flow section.	
#	This is the number of an individual static route.
Name	This field displays the descriptive name of the static route.
Destination IP	This is the destination IP address. Any means all IP addresses.
Subnet Mask / Prefix Length	This parameter specifies the IP network subnet mask and prefix length of the final destination.
Gateway IP	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface used for this static route.
The following fields are available if you click Dynamic Route (RIP) in the Routing Flow section.	
#	This is the number of an individual dynamic route.
Destination	This indicates the destination IP address of this route.
Gateway IP	This indicates the IP address of the gateway that helps forward this route's traffic.
Interface	This indicates the name of the interface through which the route is forwarded.
Protocol	This shows the kind of protocol used by this route rule (TCP , UDP or None).
Metric	This is the route's priority among the displayed routes.
The following fields are available if you click Multi-WAN in the Routing Flow section.	
Name	This is the name to identify the trunk.
Load Balancing Algorithm	This shows the load balancing method used by the trunk.
Load Balancing Index(es)	This field appears when the load balancing algorithm is Lead Load First or Spillover . This shows the traffic to which the VPN2S applies the load balancing method.
#	This field is a sequential value, and it is not associated with any interface.
Member	This field displays the member interface of the trunk.
Mode	This field displays Active when the VPN2S always attempt to use this connection. Displays Passive to have the VPN2S only use this connection when all of the connections set to active are down.
Weight	This field displays with the weighted round robin load balancing algorithm.
Egress Bandwidth	This field appears when the load balancing algorithm is Lead Load First or Spillover . This shows the maximum amount of data (in Kb) sent through the interface per second.
Spillover	This field appears when the load balancing algorithm is Spillover . This shows the maximum amount of data (in Kb) to send through the interface before using another interface.
The following fields are available if you click Main Table in the Routing Flow section	
Destination	This indicates the destination IPv4 address or IPv6 address and prefix of this route.

Table 32 Configuration > Routing > Routing Status

LABEL	DESCRIPTION
Gateway IP	This indicates the IPv4 or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of the IPv4 route.
Flag	<p>This indicates the route status.</p> <p>U-Up: The route is up.</p> <p>UC-Up Cache: The route is up and it is a cache entry.</p> <p>I-Reject: The route is blocked and will force a route lookup to fail.</p> <p>G-Gateway: The route uses a gateway to forward traffic.</p> <p>H-Host: The target of the route is a host.</p> <p>R-Reinstate: The route is reinstated for dynamic routing.</p> <p>D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect.</p> <p>M-Modified (redirect): The route is modified from a routing daemon or redirect.</p>
Metric	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost". This is the route's priority among the displayed routes.
Interface	This indicates the name of the interface through which the route is forwarded.
The following fields are available if you click Address Mapping (1-1 SNAT) in the Routing Flow section	
#	This is the index number of the rule.
WAN Interface	This shows the WAN interface through which the address mapping is forwarded.
Internal beginning IP	This is the starting Inside Local IP Address (ILA).
External Beginning IP	This is the starting Inside Global IP Address (IGA).

7.3 The Policy Route Screen

Click **Configuration > Routing** to open the Policy Route screen. Use this screen to see the configured policy routes and turn policy routing based bandwidth management on or off.

A policy route defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria can include the user name, source address and incoming interface, destination address, schedule, IP protocol (ICMP, UDP, TCP, etc.) and port.

The actions that can be taken include:

- Routing the packet to a different gateway, outgoing interface, VPN tunnel, or trunk.
- Limiting the amount of bandwidth available and setting a priority for traffic.

IPPR follows the existing packet filtering facility of RAS in style and in implementation. If you enabled IPv6 you can also configure policy routes used for your IPv6 networks on this screen.

Figure 83 Configuration > Routing > Policy Route

Policy Route

IPv4 Routing Table

#	Status	Name	Source IP	Destination IP	Sou...	Des...	Pro...	Next-Hop
1	ON	policy1	192.168.1.100/...	Any	Any	Any	TCP	WAN1

Page 1 of 1
 20 items
 Displaying 1 - 1 of 1

IPv6 Routing Table

#	Status	Name	Source IP	Destination IP	Sou...	Des...	Pro...	Next-Hop
---	--------	------	-----------	----------------	--------	--------	--------	----------

Page 0 of 0
 20 items
 No data to display

The following table describes the labels in this screen.

Table 33 Configuration > Routing > Policy Route

LABEL	DESCRIPTION
IPv4 / IPv6 Routing Table	
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an existing entry, select it and click Remove .
#	This is the number of an individual policy route.
Status	<p>This field displays whether the policy route is active or not. A green ON button signifies that this route is active. A gray OFF button signifies that this route is not active.</p> <p>Click the slide button to enable and disable the policy router.</p>
Name	This field displays the descriptive name of the policy route.
Source IP	This is the source IP address(es) from which the packets are sent. Any means all IP addresses.
Destination IP	This is the destination IP address(es) to which the packets are transmitted. Any means all IP addresses.
Source Port	This displays the port(0-65535) the source IP address(es) are using in this policy route rule.
Destination Port	This displays the port(0-65535) the destination IP address(es) are using in this policy route rule.
Source MAC	This displays the source MAC address. Blank space means all MAC addresses.
Destination MAC	This displays the destination MAC address. Blank space means all MAC addresses.
Protocol	This shows the kind of protocol used by this policy route rule (TCP , UDP or None).
Next Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel, outgoing interface or trunk.

7.3.1 Policy Route: Add/Edit

Click **Add** in the **Policy Route** screen or click the **Edit**. Use this screen to configure the required information for a policy route.

Figure 84 Policy Route: Add/Edit

Policy Route - Add

Configuration

☒ Enable

Policy Name:

Order:

Criteria

Source

Address:

IP Address:

Subnet Mask:

MAC Address:

Source Port ☒ Any (1-65535)

Destination

Address:

IP Address:

Subnet Mask:

MAC Address:

Destination Port ☒ Any (1-65535)

Protocol:

Next-Hop

WAN Interface:

Advanced

☐ Disable this policy rule automatically while the selected next-hop is unreachable.

OK Cancel

The following table describes the labels in this screen.

Table 34 Policy Route: Add/Edit (Sheet 1 of 2)

LABEL	DESCRIPTION
Configuration	
Enable	Select this to activate the policy route.
Policy Name	Enter a descriptive name for the policy. It should begin with a letter and cannot exceed 31 characters [0-9][A-Z] [a-z][_].
Order	Select an existing number for where you want to put this policy route to move the policy route to the number you selected after clicking OK . Ordering your rules is important because the VPN2S applies the rules in the order that you specify.
Criteria	
Source	Use this section to configure where the packets are coming from in this policy route.
Address	Select Any if the policy route will receive packets from all IP addresses. Select IP Address to specify the source IP address. Otherwise, select Subnet to specify the source subnet mask.
IP Address	Enter a source IP address object from which the packets are sent.
Subnet Mask	Enter a subnet mask address object from which the packets are sent.
MAC Address	Enter a MAC address object from which the packets are sent.
Source Port	Enter the port number (1-65535) from which the packets are sent. The VPN2S applies the policy route to the packets sent from the corresponding service port. Any means all service ports.
Destination	Use this section to configure where the packets are going from in this policy route.

Table 34 Policy Route: Add/Edit (Sheet 2 of 2)

LABEL	DESCRIPTION
Address	Select Any if the policy route packets will go to all IP addresses. Otherwise select IP Address to specify the destination IP address, or select Subnet to specify the destination subnet mask.
IP Address	Enter a source IP address object to which the packets go.
Subnet Mask	Enter a subnet mask address object to which the packets go.
MAC Address	Enter a MAC address object to which the packets go.
Destination Port	Enter the port number (1-65535) to which the packets go. The VPN2S applies the policy route to the packets that go to the corresponding service port. Any means all service ports.
Protocol	Select TCP or UDP if you want to specify a protocol for the policy route. Otherwise select None .
Next-Hop	
WAN Interface	Select the WAN interface to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface).
Advanced	
Disable this policy rule automatically while the selected next-hop is unreachable	Select this if you want the VPN2S to disable a policy rule if next-hop is unreachable.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

7.4 The Static Route Screen

Use this screen to view and configure the static route rules on the VPN2S. Click **Configuration > Routing > Static Route** to open the following screen.

Figure 85 Configuration > Routing > Static Route

Static Route

IPv4 Routing Table

+ Add
Edit
Remove
Multiple Entries Turn On
Multiple Entries Turn Off

#	Status	Name	Destination IP	Subnet Mask / Prefix L...	Gateway IP	Interface
1	ON	Route1	10.2.3.0	255.255.255.0	10.1.2.3	WAN1

Page 1 of 1
Show 20 items
Displaying 1 - 1 of 1

IPv6 Routing Table

+ Add
Edit
Remove
Multiple Entries Turn On
Multiple Entries Turn Off

#	Status	Name	Destination IP	Subnet Mask / Prefix L...	Gateway IP	Interface
---	--------	------	----------------	---------------------------	------------	-----------

Page 0 of 0
Show 20 items
No data to display

The following table describes the labels in this screen.

Table 35 Configuration > Routing > Static Route

LABEL	DESCRIPTION
IPv4 / IPv6 Routing Table	
Add	Click this to configure a new static route.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the static route's settings. Click the slide button to enable and disable the static router.
Remove	To remove an existing static route, select it and click Remove .
Multiple Entries Turn On	Select one or more static routes and click this to enable them.
Multiple Entries Turn Off	Select one or more static route and click this to disable them.
#	This is the index number of the static route.
Status	This field displays whether the static route is active or not. A green ON button signifies that this static route is active. A gray OFF button signifies that this static route is not active.
Name	This is the name that describes or identifies this route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask / Prefix Length	This parameter specifies the IP network subnet mask and prefix length of the final destination.
Gateway IP	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface used for this static route.

7.4.1 Static Route: Add/Edit

Use this screen to add or edit a static route. Click **Add new static route** in the **Routing** screen or the **Edit** icon next to the static route you want to edit. The screen shown next appears.

Figure 86 Static Route: Add/Edit

Static Route - Add

☒ Enable

Route Name: !

Destination IP: !

Subnet Mask:

☒ Use Gateway IP Address

Gateway IP: !

Use Interface:

OK Cancel

The following table describes the labels in this screen.

Table 36 Routing: Add/Edit

LABEL	DESCRIPTION
Enable	This field allows you to activate/deactivate this static route. Select this to enable the static route. Clear this to disable this static route without having to delete the entry.
Route Name	Enter a descriptive name for the static route.
Destination IP Address	Enter the IPv4 or IPv6 network address of the final destination.
Subnet Mask	Enter the IP subnet mask here. If you are using IPv4 and 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.
Prefix Length	Enter the IPv6 prefix length that specifies how many most significant bits (starting from the left) in the address compose the network address.
Use Gateway IP Address	The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. Select this if you want to use the gateway IP address.
Gateway IP	Enter the IP address of the gateway.
Use Interface	Select the WAN interface you want to use for this static route.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

7.5 The RIP Screen

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

Click **Configuration > Routing > RIP** to open the **RIP** screen.

Figure 87 Configuration > Routing > RIP

RIP

WAN Ports

#	Interface	Version	Operation	Enabled
1	Default [LAN]	RIPv2	Active	<input type="checkbox"/>
2	VLAN123 [LAN]	RIPv2	Active	<input type="checkbox"/>

LAN Ports

#	Interface	Version	Operation	Enabled
1	Default [LAN]	RIPv2	Active	<input type="checkbox"/>
2	VLAN123 [LAN]	RIPv2	Active	<input type="checkbox"/>

RIP Routing Rule List

#	Interface	Routing Rule List	Deny
1	WAN1	172.21.40.0 / 255.255.252.0	<input type="checkbox"/>
2	Default [LAN]	192.168.1.0 / 255.255.255.0	<input type="checkbox"/>
3	VLAN123	192.168.5.0 / 255.255.255.0	<input type="checkbox"/>

Note:
RIP cannot be configured when NAT is enabled.

[Apply](#) [Reset](#)

The following table describes the labels in this screen.

Table 37 Configuration > Routing > RIP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the VPN2S sends (it recognizes both formats when receiving). RIP version RIPv1 is universally supported but RIP version RIPv2 carries more information. RIP version RIPv1 is probably adequate for most networks, unless you have an unusual network topology.
Operation	Select Passive to have the VPN2S update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select Active to have the VPN2S advertise its route information and also listen for routing updates from neighboring routers.
Enabled	Select the check box to activate the settings.
Routing Rule List	This shows the destination IP address and subnet mask of the routing entries.
Deny	Select the check box to deny routing entries to report (send out) through the interfaces.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

CHAPTER 8

Network Address Translation (NAT)

8.1 Overview

This chapter discusses how to configure NAT on the VPN2S. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

8.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network ([Section 8.2 on page 111](#)).
- Use the **Port Triggering** screen to add and configure the VPN2S's trigger port settings ([Section 8.3 on page 114](#)).
- Use the **Address Mapping** screen to configure the VPN2S's address mapping settings ([Section 8.4 on page 117](#)).
- Use the **Default Server** screen to configure a default server ([Section 8.5 on page 119](#)).
- Use the **ALG** screen to enable and disable the NAT and SIP (VoIP) ALG in the VPN2S ([Section 8.6 on page 121](#)).

8.1.2 What You Need To Know

Inside/Outside

Inside/outside denotes where a host is located relative to the VPN2S, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

External/Internal

External/Internal denotes the IP address of a host in a packet as the packet traverses a router, for example, the internal address refers to the IP address of a host when the packet is in the local network, while the external address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See [Section 8.7 on page 122](#) for advanced technical information on NAT.

8.2 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

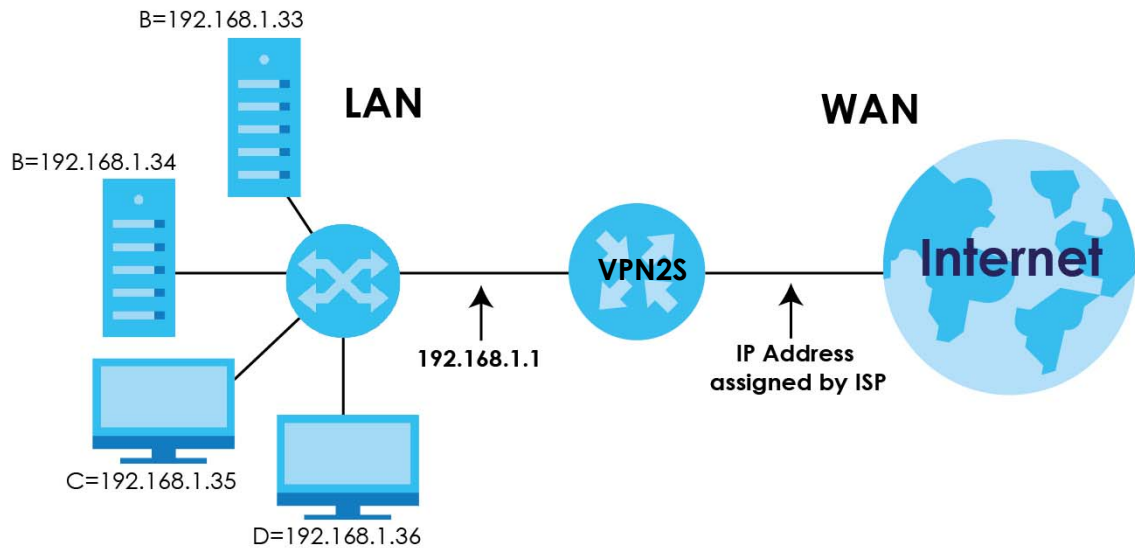
You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 88 Multiple Servers Behind NAT Example

Click **Configuration > NAT > Port Forwarding** to open the following screen.

Figure 89 Configuration > NAT > Port Forwarding

Port Forwarding

[+ Add](#) [Edit](#) [Remove](#)

#	Status	Firewall	Service...	Protocol	WAN In...	WAN IP	Startin...	Ending...	LAN IP ...	Transla...	Transla...
<div> <div>◀ ▶</div> <div>Page 0 of 0</div> <div>Show 20 items</div> <div>No data to display</div> </div>											

Note
The TCP port is reserved for TR069 connection request port.

The following table describes the fields in this screen.

Table 38 Configuration > NAT > Port Forwarding

LABEL	DESCRIPTION
Add	Click this to add a new rule.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the rule's settings.
Remove	To remove an existing rule, select it and click Remove .
#	This is the index number of the rule.
Status	This field displays whether the rule is active or not. A green ON button signifies that this rule is active. A gray OFF button signifies that this rule is not active. Click the slide button to turn on or turn off the rule.
Firewall	This shows a firewall exception icon if there is an exception filter rule on the VPN2S firewall for this port forwarding rule, otherwise this field is empty.
Service Name	This shows the service's name.
Protocol	This shows the IP protocol supported by this virtual server, whether it is TCP , UDP , or TCP/UDP .
WAN Interface	This shows the WAN interface through which the service is forwarded.
WAN IP	This field displays the incoming packet's destination IP address.
Starting Port	This is the first external port number that identifies a service.

Table 38 Configuration > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
Ending Port	This is the last external port number that identifies a service.
LAN IP Address	This is the service's internal IP address.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.

8.2.1 Port Forwarding: Add/Edit

Click **Add** in the **Port Forwarding** screen or select an existing rule and click **Edit** to open the following screen.

Figure 90 Port Forwarding: Add/Edit

The following table describes the labels in this screen.

Table 39 Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Enable	Clear the check box to inactivate the rule. Select the check box to activate it.
Add Exception to Firewall	Select this option to create an incoming filter rule in the Firewall to allow the packets.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
Protocol	Select the protocol supported by this virtual server. Choices are TCP , UDP , or TCP/UDP .
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
From WAN Side	

Table 39 Port Forwarding: Add/Edit (continued)

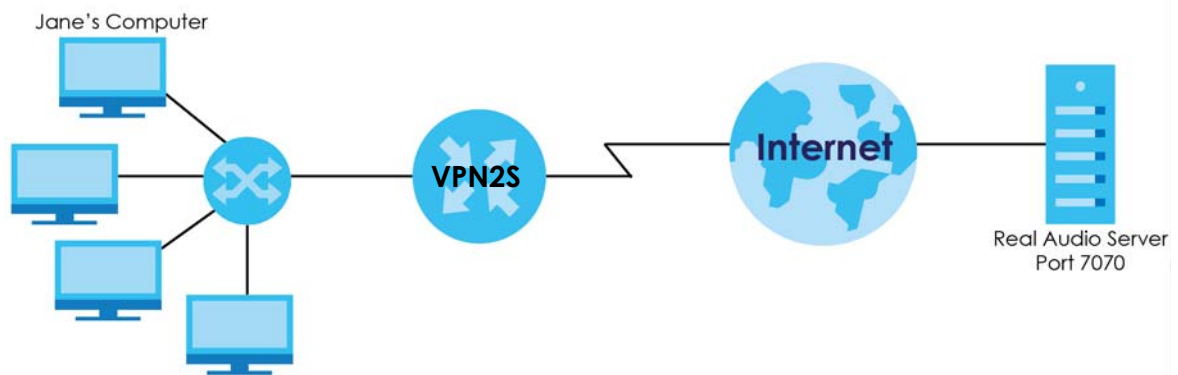
LABEL	DESCRIPTION
WAN IP	Enter the WAN IP address for which the incoming service is destined. If the packet's destination IP address doesn't match the one specified here, the port forwarding rule will not be applied.
Port Mapping Type	Select Port if you only want to enter the starting port. Select Ports if you want to enter both starting and ending ports (1-65535).
Starting Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the End Port field. To forward a series of ports, enter the start port number here and the end port number in the End Port field.
Ending Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the Start Port field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the Start Port field above.
To LAN Side	
LAN IP Address	Enter the inside IP address of the virtual server here.
Translation Start Port	Enter the port number to which you want the VPN2S to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	This shows the last port of the translated port range.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

8.3 The Port Triggering Screen

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The VPN2S records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the VPN2S's WAN port receives a response with a specific port number and protocol ("open" port), the VPN2S forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

Figure 91 Trigger Port Forwarding Process: Example

- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the VPN2S to record Jane's computer IP address. The VPN2S associates Jane's computer IP address with the "open" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The VPN2S forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The VPN2S times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Configuration > NAT > Port Triggering** to open the following screen. Use this screen to view your VPN2S's trigger port settings.

Figure 92 Configuration > NAT > Port Triggering

Port Triggering

+ Add
Edit
Remove
Multiple Entries Turn On
Multiple Entries Turn Off

#	Status	Service N...	WAN Inter...	Trigger Sta...	Trigger En...	Trigger Pr...	Open Sta...	Open End...	Open Pro...
<div> ◀ ▶ Page 0 of 0 Show 20 items No data to display </div>									

The following table describes the labels in this screen.

Table 40 Network Setting > NAT > Port Triggering

LABEL	DESCRIPTION
Add	Click this to create a new rule.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the rule's settings.
Remove	To remove an existing rule, select it and click Remove .
Multiple Entries Turn On	Select one or more rules and click this to enable them.
Multiple Entries Turn Off	Select one or more rules and click this to disable them.
#	This is the index number of the rule.

Table 40 Network Setting > NAT > Port Triggering (continued)

LABEL	DESCRIPTION
Status	This field displays whether the rule is active or not. A green ON button signifies that this rule is active. A gray OFF button signifies that this rule is not active. Click the slide button to turn on or turn off the rule.
Service Name	This field displays the name of the service used by this rule.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the VPN2S to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.
Trigger Protocol	This is the trigger transport layer protocol.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The VPN2S forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Protocol	This is the open transport layer protocol.

8.3.1 Port Triggering Rule: Add/Edit

This screen lets you create new port triggering rules. Click **Add** in the **Port Triggering** screen or select a rule and click **Edit** to open the following screen.

Figure 93 Port Triggering: Add/Edit

Port Triggering - Add

☒ Enable

Service Name: !

WAN Interface: ADSL

Trigger

Protocol: TCP

Starting Port: ! (1-65535)

Ending Port: ! (1-65535)

Open

Protocol: TCP

Starting Port: ! (1-65535)

Ending Port: ! (1-65535)

OK Cancel

The following table describes the labels in this screen.

Table 41 Port Triggering: Configuration Add/Edit

LABEL	DESCRIPTION
Enable	Select the check box to activate this rule.
Service Name	Enter a name to identify this rule. It should begin with a letter and cannot exceed 20 characters [0-9][A-Z] [a-z][_-.].
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger	
Protocol	Select the transport layer protocol from TCP , UDP , or TCP/UDP .
Starting Port	The trigger port is a port (or a range of ports) that causes (or triggers) the VPN2S to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers (1-65535).
Ending Port	Type a port number or the ending port number in a range of port numbers (1-65535).
Open	
Protocol	Select the transport layer protocol from TCP , UDP , or TCP/UDP .
Starting Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The VPN2S forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers (1-65535).
Ending Port	Type a port number or the ending port number in a range of port numbers (1-65535).
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

8.4 The Address Mapping Screen

Use this screen to change your VPN2S's address mapping settings. Ordering your rules is important, because the VPN2S applies the rules in the order that you specify. When a rule matches the current packet, the VPN2S takes the corresponding action and the remaining rules are ignored.

Click **Configuration > NAT > Address Mapping** to display the following screen.

Figure 94 Configuration > NAT > Address Mapping

Address Mapping

+ Add Edit Remove

#	Type	WAN Interface	Internal Beginning IP	Internal Ending IP	External Beginning IP	External Ending IP
No data to display						

Note:
Address mapping rule sets do not have priority above each other, and might not give the desired result if the IP ranges overlap.

The following table describes the fields in this screen.

Table 42 Configuration > NAT > Address Mapping

LABEL	DESCRIPTION
Add	Click this to create a new address mapping rule.
Edit	Double-click an address mapping rule or select it and click Edit to open a screen where you can modify the rule's settings.
Remove	To remove an existing address mapping rule, select it and click Remove .
#	This is the index number of the rule.
Type	<p>This is the address mapping type.</p> <p>One-to-One: This 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.</p> <p>Many-to-One / Source NAT: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (that is, PAT, port address translation), the VPN2S's Single User Account feature that previous routers supported only.</p> <p>Many-to-Many: This mode maps multiple local IP addresses to shared global IP addresses.</p>
WAN Interface	This shows the WAN interface through which the address mapping is forwarded.
Internal Beginning IP	This is the starting Inside Local IP Address (ILA).
Internal Ending IP	This is the ending Inside Local IP Address (ILA). This field is blank for One-to-One mapping types.
External Beginning 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. You can only do this for the Many-to-One mapping type.
External Ending IP	This is the ending Inside Global IP Address (IGA). This field is blank for One-to-One and Many-to-One mapping types.

8.4.1 Address Mapping Rule: Add/Edit

To add or edit an address mapping rule, click **Add** or select a rule and click **Edit** icon in the **Address Mapping** screen to display the screen shown next.

Figure 95 Address Mapping: Add/Edit

Address Mapping - Add

Type: One-to-One

WAN Interface: ADSL

Internal

Beginning IP Address:

Ending IP Address:

External

Beginning IP Address:

Ending IP Address:

OK Cancel

The following table describes the fields in this screen.

Table 43 Address Mapping: Add/Edit

LABEL	DESCRIPTION
Type	Choose the IP/port mapping type from one of the following. One-to-One: This mode maps one internal IP address to one external IP address. Note that port numbers do not change for the One-to-one NAT mapping type. Many-to-One / Source NAT: This mode maps multiple internal IP addresses to one external IP address. This is equivalent to SUA (that is, PAT, port address translation), the VPN2S's Single User Account feature that previous routers supported only. Many-to-Many: This mode maps multiple internal IP addresses to shared external IP addresses.
WAN Interface	Select the WAN interface through which the service is forwarded.
Internal	
Beginning IP Address	Enter the starting Inside Local IP Address (ILA).
Ending IP Address	Enter the ending Inside Local IP Address (ILA). This field is blank for One-to-One mapping types.
External	
Beginning IP Address	Enter the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the Many-to-One / Source NAT mapping type.
Ending IP Address	Enter the ending Inside Global IP Address (IGA). This field is blank for One-to-One and Many-to-One mapping types.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

8.5 The Default Server Screen

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in the **NAT Port Forwarding Setup** screen. Click **Configuration > NAT > Default Server** to open the following screen.

Figure 96 Configuration > NAT > Default Server

The screenshot shows the 'Default Server' configuration screen. At the top, there is a title 'Default Server' and an 'Edit' button. Below this is a table with two columns: '#', 'WAN Interface', and 'Default Server Address'. The table contains three rows of data:

#	WAN Interface	Default Server Address
1	Mobile	
2	WAN1	
3	L2TP	

At the bottom of the screen, there is a pagination control showing 'Page 1 of 1', a 'Show 20 items' dropdown, and a status 'Displaying 1 - 3 of 3'.

The following table describes the labels in this screen.

Table 44 Configuration > NAT > Default Server

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the default server's IP address.
#	This is the index number of the WAN interface.
WAN Interface	This shows the name of the interface group that was created in the Configuration > LAN / Home Network > VLAN / Interface Group screen.
Default Server Address	This shows the IP address of the default server.

8.5.1 Default Server: Edit

This screen lets you edit interface groups. Select an interface and click **Edit** to open the following screen.

Figure 97 Default Server: Edit

#	WAN Interface	Default Server Address
1	Mobile	
2	WAN1	
3	L2TP	

Page 1 of 1 | Show 20 items | Displaying 1 - 3 of 3

The following table describes the fields in this screen.

Table 45 Default Server: Edit

LABEL	DESCRIPTION
WAN Interface	This shows the name of the interface group that was created in the Configuration > LAN / Home Network > VLAN / Interface Group screen. The host must be in the same VLAN as the selected VLAN / Interface Group .
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the NAT Port Forwarding screen. Note: If you do not assign a Default Server Address , the VPN2S discards all packets received for ports that are not specified in the NAT Port Forwarding screen.
OK	Click OK to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

8.6 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the VPN2S registers with the SIP register server, the SIP ALG translates the VPN2S's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your VPN2S is behind a SIP ALG.

Use this screen to enable and disable the NAT, SIP (VoIP) and/or RTSP ALG in the VPN2S. To access this screen, click **Configuration > NAT > ALG**.

Figure 98 Configuration > NAT > ALG

ALG

- ☒ NAT ALG
 - ☒ FTP ALG
 - ☒ TFTP ALG
 - ☒ RTSP ALG
 - ☐ SIP ALG
 - ☐ H.323 ALG
 - ☐ PPTP ALG

The following table describes the fields in this screen.

Table 46 Configuration > NAT > ALG

LABEL	DESCRIPTION
NAT ALG	Enable this to make sure applications such as FTP and file transfer in IM applications work correctly with port-forwarding and address-mapping rules.
FTP ALG	Turn on the FTP ALG to detect FTP (File Transfer Program) traffic and help build FTP sessions through the VPN2S's NAT.
TFTP ALG	Turn on the TFTP ALG to detect TFTP (Trivial File Transfer Protocol) traffic and help build TFTP sessions through the VPN2S's NAT.
RTSP ALG	Enable this to have the VPN2S detect RTSP traffic and help build RTSP sessions through its NAT. The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SIP ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
H.323 ALG	Turn on the H.323 ALG to detect H.323 traffic (used for audio communications) and help build H.323 sessions through the VPN2S's NAT.
PPTP ALG	Turn on the PPTP ALG to detect PPTP (Point-to-point Tunneling Protocol) traffic and help build PPTP sessions through the VPN2S's NAT.
Apply	Click Apply to save your changes.
Reset	Click Reset to return the screen to its last-saved settings.

8.7 Technical Reference

This part contains more information regarding NAT.

8.7.1 NAT Definitions

Inside/outside denotes where a host is located relative to the VPN2S, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 47 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

8.7.2 What NAT Does

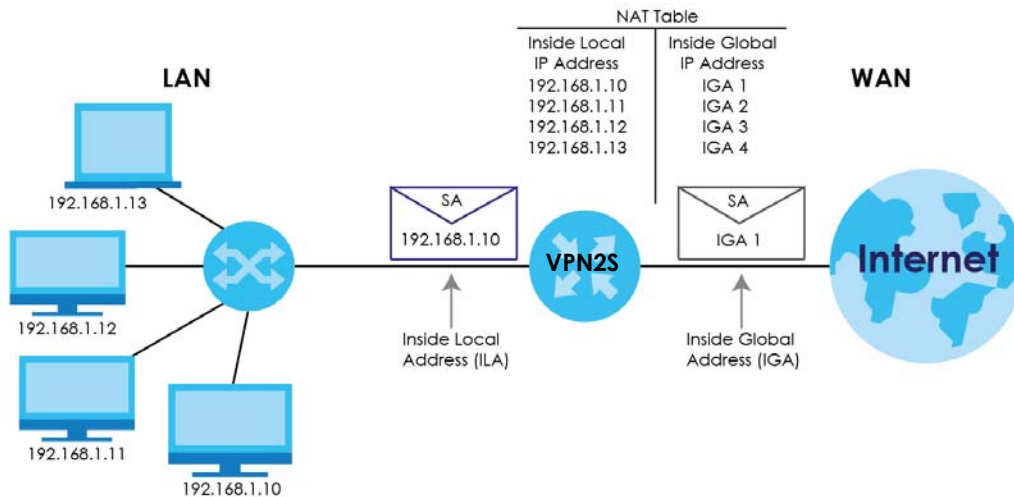
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your VPN2S filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

8.7.3 How NAT Works

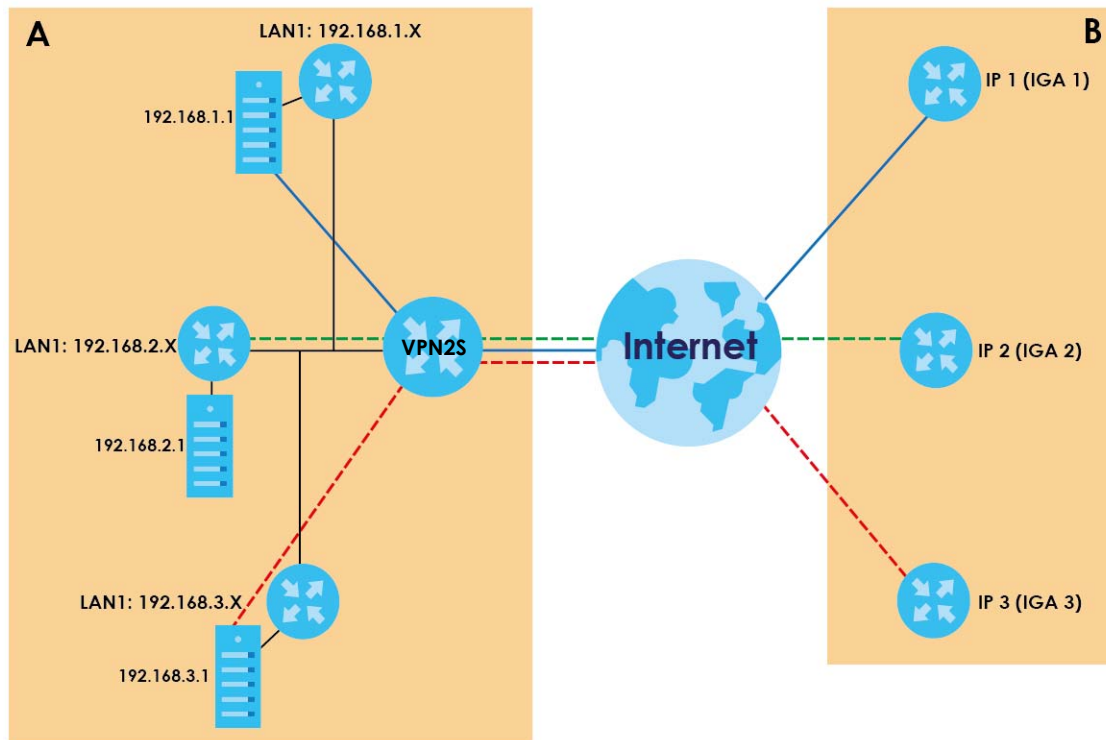
Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The VPN2S keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 99 How NAT Works



8.7.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the VPN2S can communicate with three distinct WAN networks.

Figure 100 NAT Application With IP Alias

Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

Table 48 Services and Port Numbers

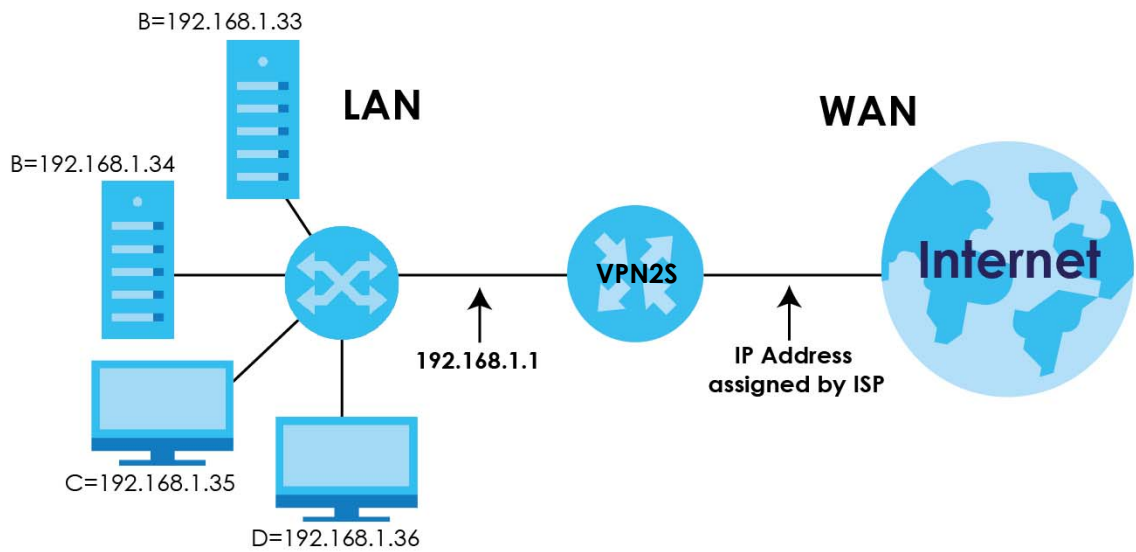
SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the

example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 101 Multiple Servers Behind NAT Example



CHAPTER 9

Firewall

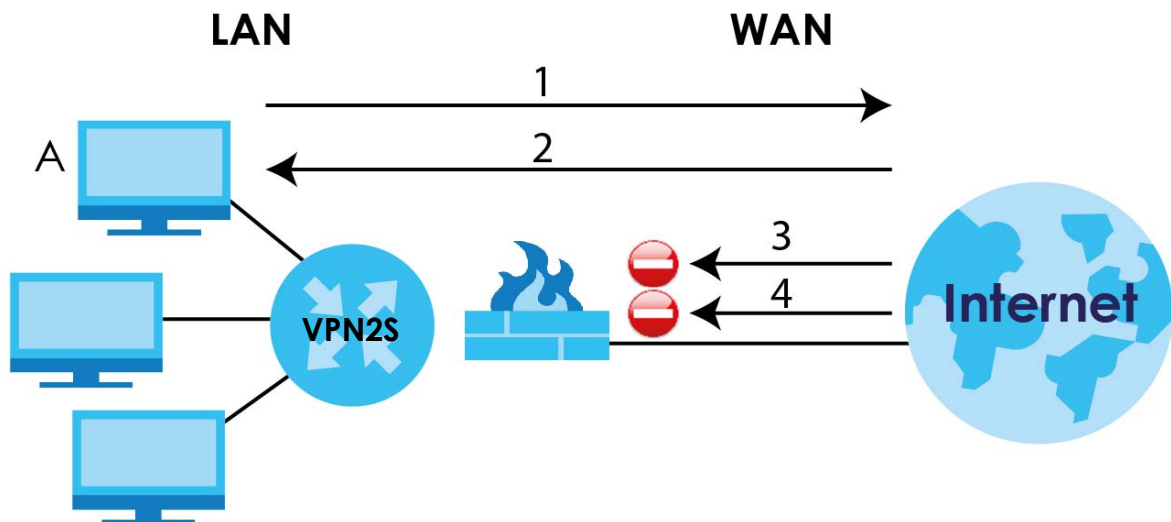
9.1 Overview

This chapter shows you how to enable and configure the VPN2S's security settings. Use the firewall to protect your VPN2S and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 102 Default Firewall Action



9.1.1 What You Can Do in this Chapter

- Use the **Firewall Overview** screen to activate the firewall feature on the VPN2S ([Section 9.2 on page 128](#)).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks ([Section 9.3 on page 128](#)).
- Use the **Firewall Rules** screen to view the configured firewall rules and add, edit or remove incoming/outgoing filtering rules ([Section 9.4 on page 129](#)).
- Use the **Device Service** screen to configure through which interfaces, which services can access the VPN2S ([Section 9.5 on page 132](#)).

- Use the **Zone Control** screen to set the firewall's default actions based on the direction of travel of packets ([Section 9.6 on page 135](#)).
- Use the **Service** screen to add or remove predefined Internet services and configure firewall rules ([Section 9.7 on page 136](#)).
- Use the **MAC Filter** screen to allow LAN clients access to the VPN2S ([Section 9.8 on page 138](#)).
- Use the **Certificate** screen to generate certification requests and import the VPN2S signed certificates ([Section 9.9 on page 140](#)).
- Use the **AAA Server** screen to provide access control to your network ([Section 9.10 on page 141](#)).

9.1.2 What You Need to Know

SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The VPN2S is pre-configured to automatically detect and thwart all known DoS attacks.

DDoS

A DDoS attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

Certification Authority

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. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the VPN2S to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

AAA Servers Supported by the VPN2S

The following lists the types of authentication server the VPN2S supports.

- Local user database

The VPN2S uses the built-in local user database to authenticate administrative users logging into the VPN2S's Web Configurator or network access users logging into the network through the VPN2S.

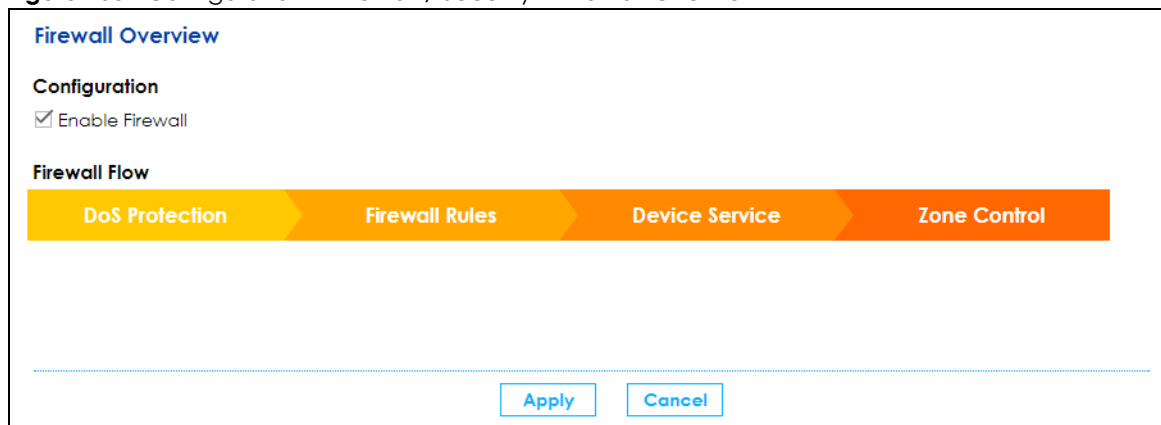
- RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

9.2 The Firewall Overview Screen

Use this screen to enable the firewall on the VPN2S. Click **Configuration > Firewall / Security > Firewall Overview** to display the **General** screen.

Figure 103 Configuration > Firewall / Security > Firewall Overview



Click the check box to activate the firewall feature on the VPN2S, then click **Apply** to save your changes. You can also use the **Firewall Flow** to go through the VPN2S's firewall features.

9.3 The DoS Screen

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

Click **Configuration > Firewall / Security > DoS** to display the following screen. Click the **DoS Protection Blocking** check box to activate protection against DoS attacks. Then click **Apply** to save your settings.

Figure 104 Configuration > Firewall / Security > DoS

DoS

Firewall Flow

DoS Protection Firewall Rules Device Service Zone Control

Configuration

☒ DoS Protection Blocking

Note:
Enable the Firewall to activate DoS.

Apply Reset

9.4 The Firewall Rules Screen

This screen displays a list of the configured firewall rules. Note the order in which the rules are listed, ordering your rules is important because the VPN2S applies the rules in the order that you specify. Click **Configuration > Firewall / Security > Firewall Rules** to display in the following screen.

Figure 105 Configuration > Firewall / Security > Firewall Rules

Firewall Rules

Firewall Flow

DoS Protection Firewall Rules Device Service Zone Control

Status

Firewall Status IPv4 Enable , IPv6 Enable

Rules Storage Space Usage 1 / 500

Firewall Rules

Status: (No Selection) From: (No Selection) To: (No Selection) IP: (No Selection) Show

+ Add Edit Remove Multiple Entries Turn On Multiple Entries Turn Off

# ↑	Status	Name	Sourc...	From	To	IP Ver...	Sourc...	Destin...	Service	Sche...	Action	Log
1	OFF	Firewall-1	Manual	LAN	WAN	4	Any	Any	ALL	-	Accept	✓

Page 1 of 1 Show 20 items Displaying 1 - 1 of 1

Note:
If a Firewall Rule is created that results in loss of management (e.g. Reject Any to Router) the unit must be restored to factory defaults.

The following table describes the labels in this screen.

Table 49 Configuration > Firewall / Security > Firewall Rules

LABEL	DESCRIPTION
Status	
Firewall Status	This shows IPv4 Enable , IPv6 Enable when the firewall is enabled, otherwise it shows Disable . You can change this in the Firewall Overview screen (Section 9.2 on page 128).

Table 49 Configuration > Firewall / Security > Firewall Rules

LABEL	DESCRIPTION
Rules Storage Space Usage	This bar shows the percentage of the VPN2S's space that has been used. If the usage is almost full, you may need to remove an existing filter rule before you create a new one.
Firewall Rules	
Status	Select Enable to view all active firewall rules, or Disable to view all inactivate firewall rules.
From	Select the source security zone of traffic to which the rule applies.
To	Select the destination security zone of traffic to which the rule applies.
IP	Select v4 to filter IPv4 address firewall rules or v6 for IPv6 addresses firewall rules.
Show	Click this button to search the firewall rules with the filters you used.
Add	Click this to create a new rule. Select a rule and click Add to create a new rule after the selected entry.
Edit	Double-click a rule or select it and click Edit to open a screen where you can modify the rule's settings.
Remove	To remove an existing rule, select it and click Remove .
Multiple Entries Turn On	Select one or more rules and click this to enable them.
Multiple Entries Turn Off	Select one or more rules and click this to disable them.
#	This is the index number of the rule.
Status	This field displays whether the firewall rule is active or not. A green ON button signifies that this firewall rule is active. A gray OFF button signifies that this firewall rule is not active. Click the slide button to turn on or turn off the rule.
Name	This displays the descriptive name of the rule.
Source Type	This displays Manual when you create firewall rules on this screen. This displays Auto when you have added an exception to the Firewall in the NAT > Port Forwarding screen, see Section 8.2.1 on page 113 .
From	This displays the source security zone of traffic to which the rule applies.
To	This displays the destination security zone of traffic to which the rule applies.
IP version	This displays 4 if the rule applies to IPv4 addresses or 6 if it applies to IPv6 addresses.
Source IP	This displays the source IP addresses to which this rule applies. Any means all IP addresses.
Destination IP	This displays the destination IP addresses to which this rule applies. Any means all IP addresses.
Service	This displays the transport layer protocol that defines the service and the direction of traffic to which this rule applies.
Schedule	This field displays the scheduler rule used for this firewall rule.
Action	This displays whether the rule allows packets (Accept), silently discards packets (Drop), or discards packets and sends an ICMP destination-unreachable packet to the sender (Reject).
Log	This displays whether the VPN2S logs when it performs the ACL rule's selected action on the traffic traveling between the two zones.

9.4.1 Firewall Rule: Add/Edit

Click **Add** or select a firewall rule and click **Edit** to open the following screen.

Figure 106 Firewall Rules: Add/Edit

The following table describes the labels in this screen.

Table 50 Firewall Rules: Add/Edit

LABEL	DESCRIPTION
Enable	Select this to turn on the firewall rule.
Logging	Select this to have the VPN2S log when it performs the firewall rule's selected action on the traffic traveling between the two zones.
Name	Enter a descriptive name of up to 16 alphanumeric characters, not including spaces. You must enter the filter name to add a firewall rule.
Description (Optional)	Enter a description to help you identify the purpose of the firewall rule.
Order	Select an existing number for where you want to put this firewall rule to move the firewall rule to the number you selected after clicking OK . Ordering your rules is important because the VPN2S applies the rules in the order that you specify.
Direction	Use the From and To define the direction of travel of packets to which to apply this firewall rule. Select from which zone the packets come in and to which zone they are destined. For example, From LAN To WAN means packets traveling from a computer or subnet on the LAN zone to the WAN zone. From Any means traffic coming from the WAN, LAN, WLAN, DMZ, and EXTRA zones (but not the ROUTER zone). To Any (excl. Router) means traffic going to the WAN, LAN, WLAN, DMZ, and EXTRA zones (but not the ROUTER zone). EXTRA is a local zone to use as needed depending on your network topology. To ROUTER applies to traffic that destined for the VPN2S. Use this to control which computers can manage the VPN2S.
IP Type	Select the type of IP you want to apply this firewall rule (IPv4 or IPv6).
Select Source Device	Select the source device to which the firewall rule applies. If you select Specific Address IP , enter the source IP address in the field below.

Table 50 Firewall Rules: Add/Edit

LABEL	DESCRIPTION
Source IP	Enter the source IP address, or select Any to apply firewall rule to any source IP addresses.
Select Destination Device	Select the destination device to which the firewall rule applies. If you select Specific Address IP , enter the source IP address in the field below.
Destination IP	If you do not select Any , enter the destination IP address in this field.
Select Service	Select the transport layer protocol that defines your customized port from the drop-down list box. The specific protocol rule sets you add in the Configuration > Firewall / Security > Service > Add screen display in this list.
Protocol	This field is displayed only when you select Any in Select Service . Choose the IP port (ALL , TCP , UDP , ICMP , or ICMP6) that defines your customized port from the drop-down list box.
Policy	Use the drop-down list box to select whether to discard (DROP), deny and send an ICMP destination-unreachable message to the sender of (REJECT) or allow the passage of (ACCEPT) packets that match this rule.
Enable Rate Limit	Select this check box to set a limit on the upstream/downstream transmission rate for the specified protocol. Specify how many packet(s) per Minute or Second the transmission rate is.
Scheduler Rules	Select a scheduler rule for this firewall rule form the drop-down list box. The scheduler rules available are the ones you create in the Configuration > Firewall / Security > Scheduler Rule screen.
OK	Click OK to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

9.5 The Device Service Screen

Use this screen to configure through which interfaces, which services can access the VPN2S. You can also specify the port numbers the services must use to connect to the VPN2S.

Use the **Trust Domain** section in this screen to view a list of public IP addresses which are allowed to access the VPN2S through the services configured above.

Click **Configuration > Firewall / Security > Device Service** to open the following screen.

Figure 107 Configuration > Firewall / Security > Device Service

Device Service

Firewall Flow

DoS Protection Firewall Rules **Device Service** Zone Control

Service List

Service	Description	LAN Interfaces	WAN Interfaces	Trust Domain	Port
HTTP	Device Service	✓		✗	80
HTTPS	Device Service	✓	WAN1	✗	443
SNMP	Device Service	✓		✗	161
SSH	Device Service	✓		✗	22
TELNET	Device Service	✓		✗	23
ICMP	Ping Response	✓		✗	-
FTP	Firmware Upgrade/USB Storage Sharing	✓		✗	21
PPTP	VPN	✗		✗	1723

Trust Domain

IP Address	Subnet Mask / Prefix Length
------------	-----------------------------

Certificate

HTTPS Certificate:

The following table describes the labels in this screen.

Table 51 Configuration > Firewall / Security > Device Service

LABEL	DESCRIPTION
Service List	
Edit	Select a service control and click Edit to modify it.
Service	This is the service you may use to access the VPN2S.
Description	This shows a description of the service.
LAN Interfaces	This shows a check icon if the service is allowed access to the VPN2S from the LAN.
WAN Interfaces	This shows the interfaces this service is allowed access to the VPN2S from the WAN.
Trust Domain	This shows a check icon if the service is allowed access to the VPN2S from the Trust Domain.
Port	This field displays the server port number for the service.
Trust Domain	
Add	Click this to add a trusted host IP address.
Remove	Click this to remove the trusted IP address.
IP Address	This field shows a trusted host IP address.
Subnet Mask / Prefix Length	This shows the prefix length that specifies how many most significant bits are in the trusted host IP address.
Certificate	
HTTPS Certificate	Select a certificate the HTTPS server (the VPN2S) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the Certificates screen.

Table 51 Configuration > Firewall / Security > Device Service

LABEL	DESCRIPTION
Apply	Click Apply to save your changes.
Reset	Click Reset to restore your previously saved settings.

9.5.1 Device Service: Edit

Double click a **Service** or select one and click **Edit** to open the following screen.

Figure 108 Device Service: Edit

The following table describes the labels in this screen.

Table 52 Device Service: Edit

LABEL	DESCRIPTION
Service	This is the service you may use to access the VPN2S.
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.
Trust Domain	Click the check box if the services is allowed access to the VPN2S from the trust domain.
LAN Interface	Click the check box if the services are allowed access to the VPN2S from the LAN.
WAN Interface	Click the check box if the services are allowed access to the VPN2S from all WAN connections, or specify the interfaces individually.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

9.5.2 Trust Domain: Add/Edit

Use this screen to configure a public IP address which is allowed to access the VPN2S. Double click an **IP Address** or select one and click **Edit** to open the following screen.

Figure 109 Trust Domain: Add/Edit

Add Trust Domain

Enter the IP address and prefix length of the management station permitted to access the local management services, and click "OK".

IP Address [/Prefix Length (optional)]:

The following table describes the labels in this screen.

Table 53 Trust Domain: Add/Edit

LABEL	DESCRIPTION
IP Address [/Prefix Length (optional)]	Enter a public IPv4 IP address which is allowed to access the service on the VPN2S from the WAN. You can also enter the prefix length of the IP address.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

9.6 The Zone Control Screen

Use this screen to set the firewall's default actions. Firewall rules are grouped based on the direction of travel of packets to which they apply.

Click **Configuration > Firewall / Security > Zone Control** to display the following screen.

Figure 110 Configuration > Firewall > Security > Zone Control

Zone Control

Firewall Flow

DoS Protection Firewall Rules Device Service **Zone Control**

Status

Firewall Status IPv4 Enable , IPv6 Enable

Zone Control

From ▶	WAN		LAN		WLAN		DMZ		EXTRA	
To ▼	Permit	Log	Permit	Log	Permit	Log	Permit	Log	Permit	Log
WAN	--	--	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN	<input type="checkbox"/>	<input type="checkbox"/>	--	--	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WLAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	--	--	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	--	--	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EXTRA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	--	--
ROUTER	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Note:

- Existing network connections may be disconnected after applying Zone Control configuration. Please reconnect if necessary.
- Communication within the same zone (except WAN) is always permitted.
- If disallowing any zone to Router, hosts on that zone may need to be set static LAN and DNS IP addresses.

The following table describes the labels in this screen.

Table 54 Configuration > Firewall / Security > Zone Control

LABEL	DESCRIPTION
Status	
Firewall Status	This shows IPv4 Enable , IPv6 Enable when the firewall is enabled, otherwise it shows Disable . You can change this in the Firewall Overview screen (Section 9.2 on page 128).
Zone Control	
From/To	<p>The firewall rules are grouped by the direction of packet travel and their zones (WAN, LAN, WLAN, DMZ, EXTRA and ROUTER). By default, the firewall allows passage of packets traveling in the same zone (a LAN to a LAN, a WAN to a WAN). Here are some example descriptions of the directions of travel.</p> <p>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.</p> <p>You can define the EXTRA zone to include the VPN connection. The Router zone can only be controlled in ingress direction "to" because it is reserved for the router's CPU. However, packets sent from the router zone are always permitted. For example, if your packet come from a LAN zone and is going to the Router zone. The VPN2S will apply the firewall rules to the LAN packets if you did not click the Permit check box.</p> <p>When Permit box is unchecked and Log box is checked, it means the "dropped" packets will be logged. When both Permit and Log boxes are checked, it means the "permitted" packets will be logged.</p>
Permit	Click the check box Permit to allow the passage of the packets.
Log	Click the check box Log to create a log when an action from Firewall rule is taken.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

9.7 The Service Screen

You can configure customized services and port numbers in the **Service** screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website.

Click **Configuration > Firewall / Security > Service** to display the following screen.

Figure 111 Configuration > Firewall / Security > Service

Service

+ Add Edit Remove

#	Name	Description	Protocol/Protocol Number
1	AH	The IPSEC AH (Authentication Header) tunneling protocol uses this servi...	Other: 51
2	BOOTP_CLIENT	DHCP Client.	UDP: Any Port-->68
3	BOOTP_SERVER	DHCP Server.	UDP: Any Port-->67
4	DNS	Domain Name Server, a service that matches web names (for exampl...	UDP: Any Port-->53
5	ESP	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses...	Other: 50
6	FTP-command	File Transfer Program, a program to enable fast transfer of files, includin...	TCP: Any Port-->21
7	FTP-data	File Transfer Program, a program to enable fast transfer of files, includin...	TCP: Any Port-->20
8	H.323	NetMeeting uses this protocol.	TCP: Any Port-->1720
9	HTTP	Hyper Text Transfer Protocol - a client/server protocol for the world wid...	TCP: Any Port-->80
10	HTTPS	HTTPS is a secured http session often used in e-commerce.	TCP: Any Port-->443

Page 1 of 4 Show 10 items Displaying 1 - 10 of 32

Note:
 1. If a protocol rule is removed, related Firewall Rules will be also removed.
 2. The maximum number of protocol rules is 64.

The following table describes the labels in this screen.

Table 55 Configuration > Firewall / Security > Service

LABEL	DESCRIPTION
Add	Click this to add a new service.
Edit	Click this to modify an existing service,
Remove	Click this to remove a service,
#	This is the index number of the service.
Name	This is the name of your customized service.
Description	This is the description of your customized service.
Protocol/ Protocol Number	This shows the IP protocol (TCP , UDP , ICMP , or TCP/UDP) and the port number or range of ports that defines your customized service. Other and the protocol number displays if the service uses another IP protocol.

9.7.1 Service: Add/Edit

Use this screen to add a customized service rule that you can use in the firewall's ACL rule configuration. Click **Add** or select an existing service rule and click **Edit** in the **Service** screen to display the following screen.

Figure 112 Service: Add/Edit

Service - Add

Name: !

Description:

Protocol: Other ▼

Protocol Number: (0-255)

OK Cancel

The following table describes the labels in this screen.

Table 56 Service: Add/Edit

LABEL	DESCRIPTION
Name	Enter a unique name (up to 32 printable English keyboard characters, including spaces) for your customized port.
Description	Enter a description for your customized port.
Protocol	Choose the IP protocol (TCP , UDP , ICMP , Other , or ICMPv6) that defines your customized port from the drop-down list box. Select Other to be able to enter a protocol number. Select ICMPv6 to be able to select a packet type.
Source/ Destination Port	These fields are displayed if you select TCP or UDP as the IP port. Select Single to specify one port only or Range to specify a span of ports that define your customized service. If you select Any , the service is applied to all ports. Type a single port number or the range of port numbers that define your customized service.
ICMPv6 Type	Select an ICMPv6 packet type.
Protocol Number	This field is displayed if you select Other as the protocol. Enter the protocol number of your customized port.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

9.8 The MAC Filter Screen

You can configure the VPN2S to permit access to clients based on their MAC addresses in the **MAC Filter** screen. 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.

Click **Configuration > Firewall / Security > MAC Filter** to open the following screen.

Figure 113 Configuration > Firewall / Security > MAC Filter

MAC Filter

General Settings

☐ Enable

MAC address List

+ Add Edit Remove Multiple Entries Turn On Multiple Entries Turn Off

Status	Host Name	MAC Address
No data to display		

Page 0 of 0 Show 20 items

Note:
Only devices listed here are granted access to the network.

Apply Reset

The following table describes the labels in this screen.

Table 57 Configuration > Firewall / Security > MAC Filter

LABEL	DESCRIPTION
General	
Enable	Select Enable to activate the MAC filter function.
MAC Address List	
Add	Click this to create a new MAC filter rule. Select a rule and click Add to create a new rule after the selected entry.
Edit	Double-click a MAC filter rule or select it and click Edit to open a screen where you can modify the rule's settings.
Remove	To remove an existing MAC filter rule, select it and click Remove .
Multiple Entries Turn On	Select one or more MAC filter rules and click this to enable them.
Multiple Entries Turn Off	Select one or more MAC filter rules and click this to disable them.
Status	This field displays whether the MAC filter rule is active or not. A green ON button signifies that this MAC filter rule is active. A gray OFF button signifies that this MAC filter rule is not active. Click the slide button to turn on or turn off the rule.
Host Name	This field displays host name of the LAN clients that are allowed access to the VPN2S.
MAC Address	This field displays the MAC addresses of the LAN clients that are allowed access to the VPN2S in these address fields.
Apply	Click Apply to save your changes.
Reset	Click Reset to restore your previously saved settings.

9.8.1 MAC Filter: Add/Edit

Click **Add** or select an existing MAC filter rule and click **Edit** to display the following screen.

Figure 114 MAC Filter: Add/Edit

The following table describes the labels in this screen.

Table 58 MAC Filter: Add/Edit

LABEL	DESCRIPTION
Enable	Select this to enable the MAC filter rule. The rule will not be applied if Enable is not selected.
Host Name	Enter the host name of the LAN clients that are allowed access to the VPN2S.
MAC Address	Enter the MAC addresses of the LAN clients that are allowed access to the VPN2S in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.

Table 58 MAC Filter: Add/Edit

LABEL	DESCRIPTION
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

9.9 The Certificate Screen

The VPN2S can use certificates (also called digital IDs) to authenticate users. 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. Click **Configuration > Firewall / Security > Certificate** to open the following screen.

Figure 115 Configuration > Firewall / Security > Certificate

The following table describes the labels in this screen.

Table 59 Configuration > Firewall / Security > Certificate

LABEL	DESCRIPTION
My Certificate Settings / Trusted CA Settings	
Add	Click this to create a new certificate. Select a rule and click Add to create a new certificate after the selected entry.
Remove	To remove an existing certificate, select it and click Remove .
More Information	Select a certificate and click More Information to view all details about the certificate.
Import	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the VPN2S.
#	This is the index number of the rule.
Name	This field displays the descriptive name used to identify this certificate. It is recommended that you give each certificate a unique name.

Table 59 Configuration > Firewall / Security > Certificate

LABEL	DESCRIPTION
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.
Type	This field displays general information about the certificate. It displays Self when the certificate is self-signed. It displays Import when the certificate used is imported.
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.
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.

9.10 The AAA Server

You can use a AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a RADIUS server. Use the AAA Server screens to create and manage objects that contain settings for using AAA servers. Click **Configuration > Firewall / Security > AAA Server** to open the following screen.

Figure 116 Configuration > Firewall / Security > AAA Server

AAA Server

LDAP Server Summary

+ Add Edit Remove

#	Name	Server Address	Base DN
Page 0 of 0 Show 5 items No data to display			

RADIUS Server Summary

+ Add Edit Remove

#	Name	Server Address
Page 0 of 0 Show 5 items No data to display		

The following table describes the labels in this screen.

Configuration > Firewall / Security > AAA Server

LABEL	DESCRIPTION
LDAP Server Summary	
Add	Click this to create a new server. Select a rule and click Add to create a new server after the selected entry.
Edit	Double-click a server or select it and click Edit to open a screen where you can modify the server's settings.
Remove	To remove an existing server, select it and click Remove .
#	This field displays the index number.

Configuration > Firewall / Security > AAA Server

LABEL	DESCRIPTION
Name	This field displays the name of the LDAP server entry.
Server Address	This field displays the address of the LDAP server.
Base DN	This field displays the domain name of the LDAP server.
RADIUS Server Summary	
Add	Click this to create a new server. Select a rule and click Add to create a new server after the selected entry.
Edit	Double-click a server or select it and click Edit to open a screen where you can modify the server's settings.
Remove	To remove an existing server, select it and click Remove .
#	This field displays the index number.
Name	This field displays the name of the RADIUS server entry.
Server Address	This field displays the address of the RADIUS server.

9.10.1 LDAP Server: Add/Edit

Click **Add** icon or select a server and click **Edit** to display the following screen. Use this screen to create a new LDAP entry or edit an existing one.

Figure 117 LDAP Server: Add/Edit

LDAP - Add

General Settings

Name: !

Description: (Optional)

Server Settings

Server Address: ! (IP or FQDN)

Backup Server Address: (IP or FQDN) (Optional)

Port: (1-65535)

Base DN: !

☐ Use SSL

Search time limit: (1-300 seconds)

☒ Case-sensitive User Names

Server Authentication

Bind DN:

Password:

Retype to Confirm:

User Login Settings

Login Name Attribute:

Alternative Login Name Attribute: (Optional)

Group Membership Attribute:

OK Cancel

The following table describes the labels in this screen.

Table 60 LDAP Server: Add/Edit

LABEL	DESCRIPTION
General Settings	
Name	Enter a descriptive name for identification purposes. It cannot exceed 64 characters [0-9][A-Z] [a-z][_].
Description	Enter the description of each server, if any. You can use up to 128 printable ASCII characters.
Server Settings	
Server Address	Enter an IP address or Fully-Qualified Domain Name (FQDN) of the LDAP authentication server.
Backup Server Address	If the LDAP server has a backup authentication server, enter its IP address or FQDN here.
Port	Specify the port number on the LDAP server to which the VPN2S sends authentication requests. Enter a number between 1 and 65535.
Base DN	Specify the directory (up to 127 alphanumerical characters). For example, o=Zyxel, c=US. This is only for LDAP .
Use SSL	Select Use SSL to establish a secure connection to the LDAP server(s).
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the VPN2S disconnects from the LDAP server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the LDAP server(s) or the LDAP server(s) is down.
Case-sensitive User Names	Select this if the server checks the case of the user names.
Server Authentication	
Bind DN	Specify the bind DN for logging into the LDAP server. Enter up to 127 alphanumerical characters. For example, cn=zyxelAdmin specifies zyxelAdmin as the user name.
Password	If required, enter the password (up to 15 alphanumerical characters) for the VPN2S to bind (or log in) to the AD or LDAP server.
Retype to Confirm	Retype your new password for confirmation.
User Login Settings	
Login Name Attribute	Enter the type of identifier the users are to use to log in. For example "name" or "e-mail address".
Alternative Login Name Attribute	If there is a second type of identifier that the users can use to log in, enter it here. For example "name" or "e-mail address".
Group Membership Attribute	An LDAP server defines attributes for its accounts. Enter the name of the attribute that the VPN2S is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create a ext-group-user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management".
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

9.10.2 RADIUS Server: Add/Edit

Click **Add** icon or select a server and click **Edit** to display the following screen. Use this screen to create a new RADIUS entry or edit an existing one.

Figure 118 RADIUS Server: Add/Edit

RADIUS - Add

General Settings

Name: ⓘ

Description: (Optional)

Server Settings

Server Address: ⓘ (IP or FQDN)

Authentication Port: (1-65535)

Backup Server Address: (IP or FQDN) (Optional)

Backup Authentication Port: (1-65535) (Optional)

Timeout: (1-300 seconds)

NAS IP Address: (IP Address)

☒ Case-sensitive User Names

Server Authentication

Key: ⓘ

User Login Settings

Group Membership Attribute: 11

OK Cancel

The following table describes the labels in this screen.

Table 61 RADIUS Server: Add/Edit

LABEL	DESCRIPTION
General Settings	
Name	Enter a descriptive name (up to 64 alphanumeric characters) for identification purposes.
Description	Enter the description of each server, if any. You can use up to 128 printable ASCII characters.
Server Settings	
Server Address	Enter the IP address or FQDN of the RADIUS authentication server.
Authentication Port	Specify the port number on the RADIUS server to which the VPN2S sends authentication requests. Enter a number between 1 and 65535.
Backup Server Address	If the RADIUS server has a backup authentication server, enter its IP address or FQDN here.
Backup Authentication Port	Specify the port number on the RADIUS server to which the VPN2S sends authentication requests. Enter a number between 1 and 65535.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the VPN2S disconnects from the RADIUS server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.

Table 61 RADIUS Server: Add/Edit

LABEL	DESCRIPTION
NAS IP Address	If the RADIUS server requires the VPN2S to provide the Network Access Server IP address attribute with a specific value, enter it here.
Case-sensitive User Names	Select this if the server checks the case of the user names.
Server Authentication	
Key	Enter a password (up to 32 characters) as the key to be shared between the external authentication server and the VPN2S. The key is not sent over the network. This key must be the same on the external authentication server and the VPN2S.
User Login Settings	
Group Membership Attribute	A RADIUS server defines attributes for its accounts. Select the name and number of the attribute that the VPN2S is to check to determine to which group a user belongs. If it does not display, select User Defined and specify the attribute's number.
OK	Click OK to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

CHAPTER 10

Security Service

10.1 Overview

This chapter describes the VPN2S's **Configuration > Content Filter** screens. Use these screens to configure your VPN2S's content filtering to control access to specific web sites or web content.

10.1.1 What You Can Do in This Chapter

Use the **Content Filter** screen to set up content filtering profiles, and manage black and white list ([Section 10.2 on page 147](#)).

10.1.2 What You Need to Know

Content Filtering

Content filtering allows you to block certain web features. It can also block access to specific categories of web site content. You can create different content filter policies for different addresses, schedules, users and content filter profiles. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages during the workday and another policy that lets him access them after work.

Content Filtering Policies

A content filtering policy allows you to do the following.

- Use schedule objects to define when to apply a content filter profile.
- Use address to define to whose web access to apply the content filter profile.
- Apply a content filter profile that you have custom-tailored.

Content Filtering Profiles

A content filtering profile conveniently stores your custom settings for the following features.

- Category-based Blocking

The VPN2S can block access to particular categories of web site content, such as pornography or racial intolerance.

Content Filtering Configuration Guidelines

When the VPN2S receives an HTTP request, the content filter searches for a policy that matches the source address and time (schedule). The content filter checks the policies in order (based on the policy numbers). When a matching policy is found, the content filter allows or blocks the request depending on

the settings of the filtering profile specified by the policy. Some requests may not match any policy. The VPN2S allows the request if the default policy is not set to block. The VPN2S blocks the request if the default policy is set to block.

External Web Filtering Service

When you register for and enable the external web filtering service, your VPN2S accesses an external database that has millions of web sites categorized based on content. You can have the VPN2S block, block and/or log access to web sites based on these categories.

HTTPS Domain Filter

HTTPS Domain Filter works with the Content Filter category feature to identify HTTPS traffic and take appropriate action. HTTPS Domain Filter identifies the URL and matches it to a category. For example, if the URL is 'www.facebook.com' and it's not allowed, then HTTPS Domain Filter identifies the domain name and it will block it.

10.2 The Content Filter Screen

Click **Configuration > Security Service > Content Filter** to open the following screen. Use this screen to enable content filtering, view and manage your list of content filter policies. You can create a common list of white/black (allowed/blocked) web site addresses.

Figure 119 Configuration > Security Service > Content Filter

Content Filter

General Settings

☐ Enable Content Filter

☐ Enable HTTPS Domain Filter for HTTPS traffic

Content Filter Category Service Timeout: seconds (1~60)

Message to display when a site is blocked

Denied Access Message:

Redirect URL:

Profile Management

[+ Add](#) [Edit](#) [Remove](#) [Multiple Entries Turn On](#) [Multiple Entries Turn Off](#)

# ↑	Status	Name	Description	Source	IP Address	Subnet Mask
1	<input type="radio"/> OFF	boss	boss	Any	-	-
2	<input type="radio"/> OFF	Employee	Employee	Any	-	-
3	<input type="radio"/> OFF	Adult	Adult	Any	-	-
4	<input type="radio"/> OFF	Teen	Teen	Any	-	-

◀ ◁ Page of 1 ▷ ▶ Show items Displaying 1 - 4 of 4

White list

[+ Add](#) [Edit](#) [Remove](#)

#	White list
---	------------

◀ ◁ Page of 0 ▷ ▶ Show items No data to display

Black list

[+ Add](#) [Edit](#) [Remove](#)

#	Black list
---	------------

◀ ◁ Page of 0 ▷ ▶ Show items No data to display

[Apply](#) [Reset](#)

The following table describes the fields in this screen.

Table 62 Configuration > Security Service > Content Filter

LABEL	DESCRIPTION
General Settings	
Enable Content Filter	Select this check box to have the VPN2S collect category-based content filtering statistics.
Enable HTTPS Domain Filter for HTTPS traffic	Select this check box to have the VPN2S block HTTPS web pages.
Content Filter Category Service Timeout	Specify the allowable time period in seconds for accessing the external web filtering service's server.
Message to display when a site is blocked	

Table 62 Configuration > Security Service > Content Filter (continued)

LABEL	DESCRIPTION
Denied Access Message	<p>Enter a message to be displayed when content filter blocks access to a web page.</p> <p>Use up to 127 characters (0-9a-zA-Z;/?:@&=+\$\._!~*()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator".</p> <p>It is also possible to leave this field blank if you have a URL specified in the Redirect URL field. In this case if the content filter blocks access to a web page, the VPN2S just opens the web page you specified without showing a denied access message.</p>
Redirect URL	<p>Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message.</p> <p>Use "http://" or "https://" followed by up to 255 characters (0-9a-zA-Z;/?:@&=+\$\._!~*()%,"). For example, http://192.168.1.17/blocked access.</p>
Profile Management	
Add	Click Add to create a new content filter profile.
Edit	Click Edit to make changes to a content filter profile.
Remove	Click Remove to delete a content filter profile.
Multiple Entries On	Select one or more content filter profiles and click this to enable them.
Multiple Entries Off	Select one or more content filter profiles and click this to disable them.
#	<p>This column lists the index numbers of the content filter profile.</p> <p>Note: The order of the content filter profiles in the list is important since they are applied in the same order they are listed.</p>
Status	This field displays whether the content filter profile is active or not. A green ON button signifies that this profile is active. A gray OFF button signifies that this profile is not active.
Name	This field displays the names of the content filter profile rule.
Description	This field displays the description of the content filter profile rule.
Source	This field displays Any when this content filter profile rule applies to all users connected to the VPN2S. Otherwise, it displays IP Address or Subnet if it only applies to a specific IP address or subnet mask.
IP Address	This field displays the IP address for which this content filter profile applies.
Subnet Mask	This field displays the subnet mask for which this content filter profile applies.
White list	This is a common list of good (allowed) web site addresses.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to be able to delete it.
#	This displays the index number of the trusted web sites.
White list	<p>This column displays the trusted web sites already added.</p> <p>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", and so on. You can also enter just a top level domain. For example, enter *.com to allow all .com domains.</p> <p>Use up to 127 characters (0-9a-z-). The casing does not matter.</p>
Black list	This is a common list of bad (blocked) web site addresses.
Add	Click this to create a new entry.

Table 62 Configuration > Security Service > Content Filter (continued)

LABEL	DESCRIPTION
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to be able to delete it.
#	This displays the index number of the forbidden web sites.
Black list	<p>This list displays the forbidden web sites already added.</p> <p>Enter host names such as www.badsite.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are also blocked. For example, entering "*.badsite.com" also blocks "www.badsite.com", "partner.badsite.com", "press.badsite.com", and do on. You can also enter just a top level domain. For example, enter *.com to block all .com domains.</p> <p>Use up to 127 characters (0-9a-z-). The casing does not matter.</p>

10.2.1 Content Filter: Add/Edit

Click **Add** or select a content filter profile and click **Edit** to open the following screen.

Figure 120 Content Filter: Add/Edit

Content Filter - Add

General Settings

☐ Enable

Profile Name: !

Description: (Optional)

Order:

Policy Rule

Source:

IP Address:

Subnet Mask:

Scheduler Rule:

Test Web Site Category

URL to test:

[Test Against Content Filter Category Server](#)

Category

Security:

Adult:

Social Media:

Recreation:

Technology:

Public:

Unrated Web Pages:

Category Server Is Unavailable:

Managed Categories

Note
Checked items will be blocked after you click "OK".

Security

☐ Anonymizers ☐ Malware

☐ Phishing & Fraud ☐ Botnets

☐ Network Errors ☐ Spam Sites

☐ Compromised ☐ Parked Domains

Adult

☐ Nudity ☐ Pornography/Sexually Explicit

☐ Cults ☐ Illegal Drugs

☐ Violence ☐ Child Abuse Images

☐ Criminal Activity ☐ Gambling

☐ Weapons ☐ Sex Education

☐ School Cheating ☐ Alcohol/Tobacco

☐ Hate & Intolerance ☐ Tasteless

Social Media

☐ Social Networking ☐ Dating & Personals

☐ Instant Messaging ☐ Chat

☐ Forums & Newsgroups

Recreation

☐ Entertainment ☐ Games

☐ Sports ☐ Shopping

☐ Peer to Peer ☐ Advertisements & Pop-Ups

☐ Streaming Media & Downloads ☐ Restaurants & Dining

☐ Travel ☐ News

☐ Search Engines/Portals ☐ Fashion & Beauty

☐ Arts ☐ Leisure & Recreation

☐ Greeting Cards ☐ Image Sharing

Technology

☐ Hacking ☐ Information Security

☐ Private IP Addresses ☐ Download Sites

☐ Personal Sites ☐ Illegal Software

☐ Web-based Email ☐ Computers & Technology

☐ Translators

Public

☐ Religion ☐ Business

☐ Health & Medicine ☐ Transportation

☐ Finance ☐ Government

☐ Real Estate ☐ General

☐ Education ☐ Job Search

☐ Non-profits & NGOs ☐ Politics

The following table describes the labels in this screen.

Table 63 Content Filter: Add/Edit

LABEL	DESCRIPTION
General Settings	
Enable	Select the check box to activate this content filter profile.
Profile Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character can only be letters. This value is case-sensitive.
Description	Enter a description for the content filtering profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-). This field is optional.
Order	Select the order in which you want to apply this content filter profile, being 1 the highest priority. Note: The order of the content filter profiles in the list is important since they are applied in the same order they are listed.
Policy Rule	
Source	Select Any to apply this content filter profile to all users connected to the VPN2S. Otherwise, specify the IP Address and/or Subnet on which you want to apply this content filter profile.
IP Address	Enter the IP address for which this content filter profile applies.
Subnet Mask	Enter the subnet mask for which this content filter profile applies.
Scheduler Rule	Select Any to apply this policy rule without time restrictions. Otherwise, select one of the scheduler rules created in Configuration > System > Scheduler Rule screen.
Test Web Site Category	
URL to test	You can check which category a web page belongs to. Enter a web site URL in the text box.
Test Against Content Filter Category Server	Click this button to see the category recorded in the external content filter server's database for the web page you specified.
Category	
Note: This feature will only be applied to the VPN2S, when its content filter license is activated.	
Security	Select Block to prevent users from accessing webpages that match the Security category. Select Allow to grant users to access them. Select User Defined to manually select the items blocked in the Managed Categories section. If you already selected the items, then this automatically changes to User Defined .
Adult	Select Block to prevent users from accessing webpages that match the Adult category. Select Allow to allow users to access them. Select User Defined to manually select the items blocked in the Managed Categories section. If you already selected the items, then this automatically changes to User Defined .

Table 63 Content Filter: Add/Edit

LABEL	DESCRIPTION
Social Media	<p>Select Block to prevent users from accessing webpages that match the Social Media category.</p> <p>Select Allow to grant users to access them.</p> <p>Select User Defined to manually select the items blocked in the Managed Categories section. If you already selected the items, then this automatically changes to User Defined.</p>
Recreation	<p>Select Block to prevent users from accessing webpages that match the Recreation category.</p> <p>Select Allow to grant users to access them.</p> <p>Select User Defined to manually select the items blocked in the Managed Categories section. If you already selected the items, then this automatically changes to User Defined.</p>
Technology	<p>Select Block to prevent users from accessing webpages that match the Technology category.</p> <p>Select Allow to grant users to access them.</p> <p>Select User Defined to manually select the items blocked in the Managed Categories section. If you already selected the items, then this automatically changes to User Defined.</p>
Public	<p>Select Block to prevent users from accessing webpages that match the Public category.</p> <p>Select Allow to grant users to access them.</p> <p>Select User Defined to manually select the items blocked in the Managed Categories section. If you already selected the items, then this automatically changes to User Defined.</p>
Unrated Web Pages	<p>Select Block to prevent users from accessing web pages that the external database content filtering has not categorized. Otherwise, select Allow to grant users to access them.</p> <p>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 screen along with the category of the blocked web page.</p>
Category Server Is Unavailable	<p>Select Block to block access to any requested web page if the external content filtering database is unavailable. The following are possible causes:</p> <ul style="list-style-type: none"> • There is no response from the external content filtering server within the time period specified in the Content Filter Server Unavailable Timeout field. • The VPN2S is not able to resolve the domain name of the external content filtering database. • 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").
Managed Categories	<p>These are categories of web pages based on their content. Select web page items to be included within each category to control access to specific types of Internet content.</p> <p>Note: This feature will only be applied to the VPN2S, when its content filter license is activated.</p>
OK	Click OK to save your changes back to the VPN2S.
Cancel	Click Cancel to exit this screen without saving your changes.

CHAPTER 11

VPN

11.1 Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

11.2 What You Can Do in this Chapter

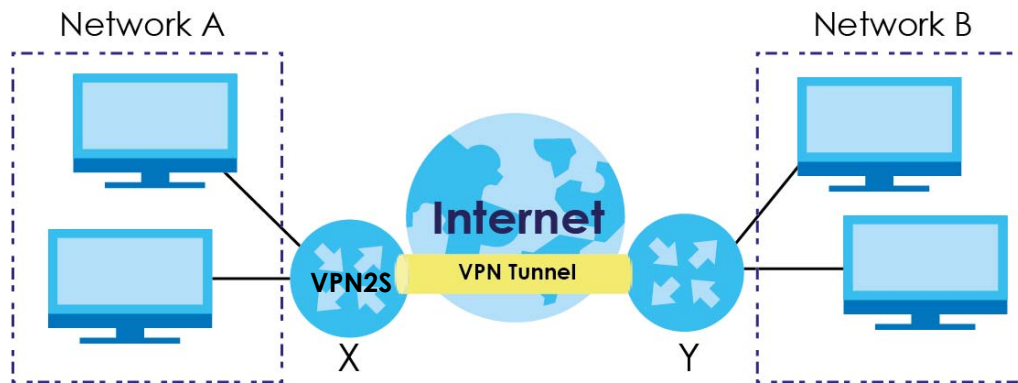
- Use the **VPN Status** screen to look at the VPN tunnels currently established in the VPN2S ([Section 11.4 on page 157](#)).
- Use the **IPsec VPN** screen to display and manage active IPsec VPN connections ([Section 11.5 on page 158](#)).
- Use the **PPTP VPN** screen to configure the PPTP VPN settings in the VPN2S ([Section 11.6 on page 171](#)).
- Use the **L2TP VPN** screen to configure the VPN2S's L2TP VPN settings ([Section 11.7 on page 174](#)).
- Use the **L2TP Client Status** screen to view connection details for L2TP clients ([Section 11.8 on page 180](#)).
- Use the **GRE VPN** screen to configure the GRE VPN settings in the VPN2S ([Section 11.9 on page 181](#)).

11.3 What You Need to Know

IPsec VPN

Internet Protocol Security (IPsec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPsec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

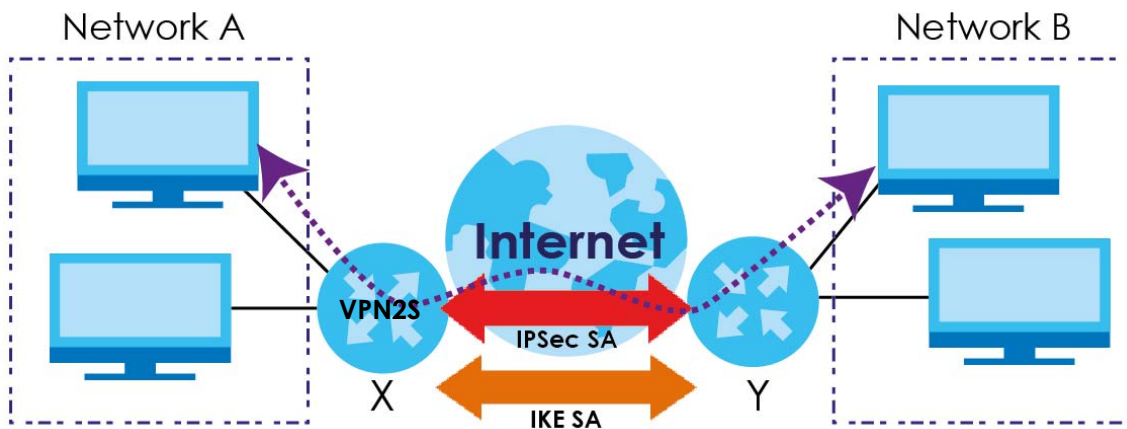
The following figure provides one perspective of a VPN tunnel.

Figure 121 IPsec VPN: Overview

The VPN tunnel connects the VPN2S (**X**) and the remote IPsec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the VPN2S and the remote IPsec router will use.

The first phase establishes an Internet Key Exchange (IKE) SA between the VPN2S and remote IPsec router. The second phase uses the IKE SA to securely establish an IPsec SA through which the VPN2S and remote IPsec router can send data between computers on the local network and remote network. The following figure illustrates this.

Figure 122 VPN: IKE SA and IPsec SA

In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPsec SA. The IPsec SA is established securely using the IKE SA that routers **X** and **Y** established first.

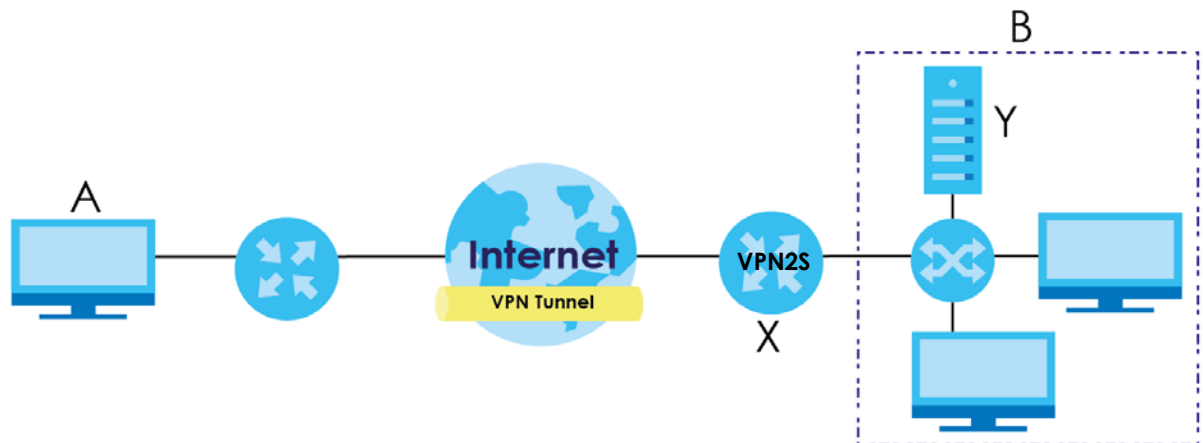
PPTP VPN

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 VPN using TCP/IP-based networks. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

PPTP sets up two sessions and uses Generic Routing Encapsulation (GRE, RFC 2890) to transfer information between the computers. It is convenient and easy-to-use, but you have to make sure that firewalls support both PPTP sessions.

PPTP works on a client-server model and is suitable for remote access applications. For example, an employee (**A**) can connect to the PPTP VPN gateway (**X**) as a PPTP client to gain access to the company network resources from outside the office. When you connect to a remote network (**B**) through a PPTP VPN, all of your traffic goes through the PPTP VPN gateway (**X**).

Figure 123 PPTP VPN Example

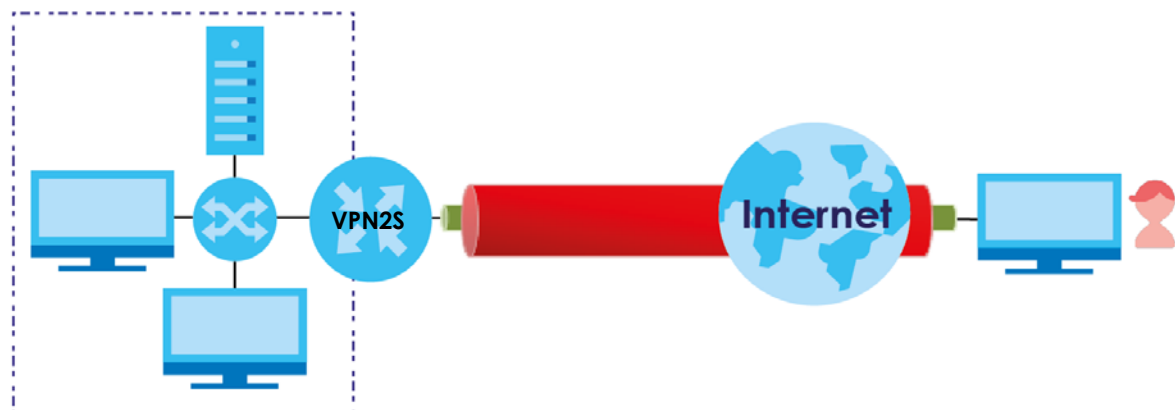


L2TP VPN

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPsec VPN tunnel is established first and then an L2TP tunnel is built inside it.

L2TP VPN lets remote users use the L2TP and IPsec client software included with their computers' operating systems to securely connect to the network behind the VPN2S. The remote users do not need their own IPsec gateways or VPN client software.

Figure 124 L2TP VPN Overview



GRE VPN

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. User is able to create a GRE tunnel to solve the problems faced when trying to form VPNs across the Internet by encapsulating the IP header with private addressing using an outer IP header that use public addressing.

11.4 The VPN Status Screen

Use this screen to look at the VPN tunnels that are currently established. To access this screen, click **Configuration > VPN > VPN Status**.

Figure 125 Configuration > VPN > VPN Status

VPN Status

IPsec VPN

Disconnect Refresh

#	Name	Policy	My Address	Secure Gateway	Up Time	Timeout
No data to display						

Page 0 of 0 Show 5 items

PPTP VPN

Disconnect Refresh

#	Username	Host Name	Assigned IP	Public IP
No data to display				

Page 0 of 0 Show 5 items

L2TP VPN

Disconnect Refresh

#	Username	Host Name	Assigned IP	Public IP
No data to display				

Page 0 of 0 Show 5 items

GRE VPN

Refresh

#	Tunnel Name	WAN Interface	Local IP Address	Remote Peer IP Address
No data to display				

Page 0 of 0 Show 5 items

The following table describes the labels in this screen.

Table 64 Configuration > VPN > VPN Status

LABEL	DESCRIPTION
IPsec VPN	
Disconnect	Select a VPN policy and click Disconnect to disable it.
Refresh	Click this to renew the table.
#	This is the IPsec VPN policy index number.
Name	This field displays the identification name for this VPN policy.
Policy	This field displays the local policy and the remote policy, respectively.

Table 64 Configuration > VPN > VPN Status

LABEL	DESCRIPTION
My Address	This field displays the interface the VPN gateway uses.
Secure Gateway	This field displays the peer gateway address of the IPsec router with which you are making the VPN connection.
Up Time	This field displays the period of time the VPN tunnel has been up.
Timeout	This field displays the timeout period before the VPN2S disconnects from this VPN tunnel.
PPTP VPN / L2TP VPN	
Disconnect	Select a VPN client connection and click this to disable it.
Refresh	Click this to renew the table.
#	This is the PPTP/L2TP VPN policy index number.
Username	This field displays the client's login name for this connection.
Host Name	This is the client's host name of this connection.
Assigned IP	This is the local point-to-point IP address assigned to the client.
Public IP	This is the client's public IP address for this connection.
GRE VPN	
Refresh	Click this to renew the table.
#	This is the GRE VPN policy index number.
Tunnel Name	This field displays the identification name for this GRE VPN policy.
WAN Interface	This field displays the WAN interface this GRE VPN policy uses.
Local IP Address	This displays the WAN interface IP address.
Remote Peer IP Address	This displays an IP address of the remote device terminating the GRE VPN tunnel.

11.5 The IPsec VPN Screen

Click **Configuration > VPN > IPsec VPN** to open the following screen.

Use **Gateway Configuration** to manage the VPN2S's VPN gateway policies. A VPN gateway specifies the IPsec routers at either end of a VPN tunnel and the IKE SA settings (phase 1 settings). You can also activate and deactivate each VPN gateway.

Use **Connection Configuration** to specify which IPsec VPN gateway an IPsec VPN connection policy uses, which devices behind the IPsec routers can use the VPN tunnel, and the IPsec SA settings (phase 2 settings). You can also activate or deactivate and connect or disconnect each VPN connection (each IPsec SA).

Figure 126 Configuration > VPN > IPsec VPN

IPsec VPN

DPD Timeout: (10-3600)

DPD Attempts: (3-10)

Gateway Configuration

[+ Add](#) [Edit](#) [Remove](#)

#	Status	Name	My Address	Secure Gateway	VPN Connection	IKE Version
1	<input type="radio"/> OFF	Default_L2TP_VP...	Interface: Any	Dynamic	Default_L2TP_VP...	IKEv1

◀ ◁ | Page of 1 | ▷ ▶ | Show items | Displaying 1 - 1 of 1

Connection Configuration

[+ Add](#) [Edit](#) [Remove](#) [Connect](#) [Disconnect](#)

#	Status	Tun...	...	Name	VPN Gateway	Policy	Application Scen...
1	<input type="radio"/> OFF			Default_L2TP_VP...	Default_L2TP_VP...	//	Remote Access (...)

◀ ◁ | Page of 1 | ▷ ▶ | Show items | Displaying 1 - 1 of 1

[Apply](#) [Reset](#)

The following table describes the labels in this screen.

Table 65 Configuration > VPN > IPsec VPN

LABEL	DESCRIPTION
DPD Timeout	Use Dead Peer Detection (DPD) so the VPN2S makes sure the remote IPsec router is there before it transmits data through the IKE SA. The remote IPsec router must support DPD. Enter the number of seconds for DPD Timeout . The VPN2S sends a message to the remote IPsec router. If the remote IPsec router responds, the VPN2S keeps the tunnel up.
DPD Attempts	If the remote IPsec router does not respond, enter how many attempts the VPN2S should make before it shuts down the tunnel. Note: If you enabled Nailed Up in the VPN > IPsec VPN > VPN Connection screen, the VPN2S shuts down the tunnel and will automatically establish a new tunnel.
Gateway Configuration	
Add	Click this to configure a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an existing entry, select it and click Remove .
#	This field displays the VPN gateway index number.
Status	This field displays whether the IPsec VPN gateway is active or not. A green ON button signifies that this IPsec VPN gateway is active. A gray OFF button signifies that this IPsec VPN gateway is not active.
Name	This field displays the identification name for this VPN gateway.
My Address	This field displays the interface the VPN gateway uses.
Secure Gateway	This field displays the peer gateway address of the IPsec router with which you are making the VPN connection.
VPN Connection	This field displays which VPN connection use this gateway.

Table 65 Configuration > VPN > IPsec VPN

LABEL	DESCRIPTION
IKE Version	This field displays the IKE Version the VPN gateway uses.
Connection Configuration	
Add	Click this to configure a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an existing entry, select it and click Remove .
Connect	To connect an IPsec SA, select it and click Connect .
Disconnect	To disconnect an IPsec SA, select it and click Disconnect .
#	This field displays the VPN connection index number.
Status	This field displays whether the IPsec VPN connection is active or not. A green ON button signifies that this IPsec VPN connection is active. A gray OFF button signifies that this IPsec VPN connection is not active.
Tunnel	This shows a lit up globe if the VPN tunnel is connected or and a gray globe when it is disconnected.
Full Tunnel	This field displays whether the VPN2S sends packets through the VPN tunnel or not.
Name	This field displays the identification name for this VPN policy.
VPN Gateway	This field displays the VPN gateway the VPN connection uses.
Encapsulation	This field displays the type of encapsulation the IPsec SA uses,
Algorithm	This field displays the encryption algorithm used in the IKE SA.
Policy	This field displays the remote and local policy.
Application Scenario	<p>This field is read-only and shows the scenario that the VPN2S supports.</p> <p>Site-to-site - The remote IPsec router needs to have a static IP address or a domain name. This VPN2S can initiate the VPN tunnel.</p> <p>Site-to-site with Dynamic Peer - Choose this if the remote IPsec router has a dynamic IP address. Only the remote IPsec router can initiate the VPN tunnel.</p> <p>Remote Access (Server Role) - Choose this to allow incoming connections from IPsec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.</p> <p>Remote Access (Client Role) - Choose this to connect to an IPsec server. This VPN2S is the client (dial-in user) and can initiate the VPN tunnel.</p>
Apply	Click Apply to save your changes.
Reset	Click Reset to restore your previously saved settings.

11.5.1 VPN Gateway: Add/Edit

Click **Add** to create a new VPN gateway policy. You can also double click a VPN gateway policy or select one and click **Edit** to go to the following screen.

Figure 127 VPN Gateway: Add/Edit

+ Gateway Configuration - Add

General Settings

☐ Enable

VPN Gateway Name:

IKE Version: IKEv1

Gateway Settings

My Address

☒ Interface Any

☐ Domain Name / IP

Peer Gateway Address

☐ Static Address

Primary:

Secondary:

☒ Dynamic Address

Authentication

☒ Pre-Shared Key ☐ unmasked

☐ Certificate Default (See Local Certificates)

Advanced

Local ID Type:	IPv4
Content:	<input type="text" value="0.0.0.0"/>
Peer ID Type:	IPv4
Content:	<input type="text" value="0.0.0.0"/>

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 seconds)

Negotiation Mode by Initiator: Aggressive

Advanced

Proposal:	<div style="display: flex; justify-content: space-between; align-items: center;"> Add Edit Remove </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e1f5fe;"> <th>#</th> <th>Encryption</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1</td> <td>AES128</td> </tr> </tbody> </table>	#	Encryption	1	AES128	<div style="display: flex; justify-content: space-between; align-items: center;"> Add Edit Remove </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e1f5fe;"> <th>#</th> <th>Authentication</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1</td> <td>SHA1</td> </tr> </tbody> </table>	#	Authentication	1	SHA1
#	Encryption									
1	AES128									
#	Authentication									
1	SHA1									
Key Group:	DH2									
<input checked="" type="checkbox"/> NAT Traversal <input checked="" type="checkbox"/> Dead Peer Detection (DPD)										

X-Auth

X-Auth

☐ Enable Extended Authentication

☒ Server Mode local

OK
Cancel

The following table describes the labels in this screen.

Table 66 VPN Gateway: Add/Edit

LABEL	DESCRIPTION
General Settings	
Enable	Select the check box to activate this VPN gateway policy.

Table 66 VPN Gateway: Add/Edit

LABEL	DESCRIPTION
VPN Gateway Name	<p>Enter a name used to identify this VPN gateway.</p> <p>The VPN Gateway Name of an IPsec rule must be unique and cannot be changed once it has been created.</p>
IKE Version	<p>Select IKEv1 or IKEv2. IKEv1 applies to IPv4 traffic only. IKEv2 applies to both IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely. See Section 11.3 on page 154 for more information on IKEv1 and IKEv2.</p>
Gateway Settings	
My Address	<p>Select how the IP address of the VPN2S in the IKE SA is defined.</p> <p>If you select Interface, select the Ethernet interface, WWAN interface, virtual Ethernet interface. The IP address of the VPN2S in the IKE SA is the IP address of the interface.</p> <p>If you select Domain Name / IP, enter the domain name or the IP address of the VPN2S. The IP address of the VPN2S in the IKE SA is the specified IP address or the IP address corresponding to the domain name. 0.0.0.0 is not generally recommended as it has the VPN2S accept IPsec requests destined for any interface address on the VPN2S.</p>
Peer Gateway Address	<p>Select how the IP address of the remote IPsec router in the IKE SA is defined.</p> <p>Select Static Address to enter the domain name or the IP address of the remote IPsec router. You can provide a Secondary IP address or domain name for the VPN2S to try if it cannot establish an IKE SA with the first one.</p> <p>Enter a Secondary IP address, if the connection to the Primary address goes down and the VPN2S changes to using the secondary connection, the VPN2S will reconnect to the primary address when it becomes available again and stop using the secondary connection. Users will lose their VPN connection briefly while the VPN2S changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection. In the Fallback Check Interval field, set how often to check if the primary address is available.</p> <p>Select Dynamic Address if the remote IPsec router has a dynamic IP address (and does not use DDNS).</p>
Authentication	<p>Note: The VPN2S and remote IPsec router must use the same authentication method to establish the IKE SA.</p>
Pre-Shared Key	<p>Select this to have the VPN2S and remote IPsec router use a pre-shared key (password) to identify each other when they negotiate the IKE SA. Type the pre-shared key in the field to the right. The pre-shared key can be</p> <ul style="list-style-type: none"> • 8 - 32 keyboard characters except (=) equals sign, (-) dash, (/) slash, (\) backslash, or (",') quotation marks. • 8 - 32 pairs of hexadecimal (0-9, A-F) characters, preceded by "0x". <p>If you want to enter the key in hexadecimal, type "0x" at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in "0123456789ABCDEF" is in ASCII format. If you use hexadecimal, you must enter twice as many characters since you need to enter pairs.</p> <p>The VPN2S and remote IPsec router must use the same pre-shared key.</p> <p>Select unmasked to see the pre-shared key in readable plain text.</p> <p>Note: All remote access application scenario of IPsec rules must use the same pre-shared key.</p>

Table 66 VPN Gateway: Add/Edit

LABEL	DESCRIPTION
Certificate	<p>In order to use Certificate for IPsec authentication, you need to add new host certificates in the Firewall / Security > Certificate screen.</p> <p>Select this to have the VPN2S and remote IPsec router use certificates to authenticate each other when they negotiate the IKE SA. Then select the certificate the VPN2S uses to identify itself to the remote IPsec router.</p> <p>This certificate is one of the certificates in Certificate. If this certificate is self-signed, import it into the remote IPsec router. If this certificate is signed by a CA, the remote IPsec router must trust that CA.</p> <p>Note: The IPsec routers must trust each other's certificates.</p> <p>The VPN2S uses one of its Trusted CA to authenticate the remote IPsec router's certificate. The trusted certificate can be a self-signed certificate or that of a trusted CA that signed the remote IPsec router's certificate.</p>
Advanced	
Local ID Type	<p>This field is read-only if the VPN2S and remote IPsec router use certificates to identify each other. Select which type of identification is used to identify the VPN2S during authentication. Choices are:</p> <p>IPv4 - the VPN2S is identified by an IP address.</p> <p>DNS - the VPN2S is identified by a domain name.</p> <p>Email Address - the VPN2S is identified by the string specified in the Content field.</p> <p>My Address - the VPN2S is identified by the IP address specified in the My Address field.</p>
Content	<p>This field is read-only if the VPN2S and remote IPsec router use certificates to identify each other. Type the identity of the VPN2S during authentication. The identity depends on the Local ID Type.</p> <p>IPv4 - type an IP address. This is not recommended in the following situations:</p> <ul style="list-style-type: none"> • There is a NAT router between the VPN2S and remote IPsec router. • You want the remote IPsec router to be able to distinguish between IPsec SA requests that come from IPsec routers with dynamic WAN IP addresses. <p>In these situations, use a different IP address, or use a different Local ID Type.</p> <p>DNS - type the fully qualified domain name (FQDN). This value is only used for identification and can be any string that matches the peer ID string.</p> <p>Email Address - the VPN2S is identified by the string you specify here; you can use up to 63 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.</p>
Peer ID Type	<p>Select which type of identification is used to identify the remote IPsec router during authentication. Choices are:</p> <p>IPv4 - the remote IPsec router is identified by an IP address.</p> <p>DNS - the remote IPsec router is identified by a domain name.</p> <p>Email Address - the remote IPsec router is identified by the string specified in this field.</p> <p>Any - the VPN2S does not check the identity of the remote IPsec router. If the VPN2S and remote IPsec router use certificates, there is one more choice.</p>

Table 66 VPN Gateway: Add/Edit

LABEL	DESCRIPTION
Content	<p>This field is disabled if the Peer ID Type is Any. Type the identity of the remote IPsec router during authentication. The identity depends on the Peer ID Type.</p> <p>If the VPN2S and remote IPsec router do not use certificates,</p> <p>IPv4 - type an IP address; see the note at the end of this description.</p> <p>DNS - type the fully qualified domain name (FQDN). This value is only used for identification and can be any string that matches the peer ID string.</p> <p>Email Address - the remote IPsec router is identified by the string you specify here; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.</p> <p>Note: If Peer ID Type is IPv4, please read the rest of this section.</p> <p>If you type 0.0.0.0, the VPN2S uses the IP address specified in the Secure Gateway Address field. This is not recommended in the following situations:</p> <ul style="list-style-type: none"> • There is a NAT router between the VPN2S and remote IPsec router. • You want the remote IPsec router to be able to distinguish between IPsec SA requests that come from IPsec routers with dynamic WAN IP addresses. <p>In these situations, use a different IP address, or use a different Peer ID Type.</p>
Phase 1 Settings	<p>Phase 1 Encryption and Authentication can have up to 3 algorithm pairs. You cannot use phase 1 Encryption, Authentication, and Key Group pairs that already exist in other enabled IPsec rules.</p> <p>When the default IPsec rule Default_L2TP_VPN_GW is enabled, if you want to add a new Remote Access IPsec rule, you can use phase 1 Encryption, Authentication, and Key Group pair 3DES and SHA1 or 3DES and SHA256, or any algorithm combination with DH1 or DH5.</p>
SA Life Time	<p>Define the length of time before an IKE or IPsec SA automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds.</p> <p>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.</p>
Negotiation Mode by Initiator	<p>Select the negotiation mode to use to negotiate the IKE SA. Choices are:</p> <p>Main - this encrypts the VPN2S's and remote IPsec router's identities but takes more time to establish the IKE SA.</p> <p>Aggressive - this is faster but does not encrypt the identities. The VPN2S and the remote IPsec router must use the same negotiation mode.</p> <p>Note: This field is only available when you select IKEv1 in the IKE Version field.</p>
Advanced	
Proposal	Use this section to manage the encryption algorithm and authentication algorithm pairs the VPN2S accepts from the remote IPsec router for negotiating the IKE SA.
Add	Click this to add phase 1 Encryption and Authentication .
Edit	Select an entry and click the Edit to modify it.
Remove	Select an entry and click Remove to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.

Table 66 VPN Gateway: Add/Edit

LABEL	DESCRIPTION
Encryption	<p>Select which key size and encryption algorithm to use in the IKE SA. Choices are:</p> <p>3DES - a 168-bit key with the DES encryption algorithm</p> <p>AES128 - a 128-bit key with the AES encryption algorithm</p> <p>AES192 - a 192-bit key with the AES encryption algorithm</p> <p>AES256 - a 256-bit key with the AES encryption algorithm</p> <p>The VPN2S and the remote IPsec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.</p>
#	This is the Authentication index number.
Authentication	<p>Select which hash algorithm to use to authenticate packet data in the IPsec SA. Choices are SHA1, SHA256, and SHA512.</p> <p>The remote IPsec router must use the same authentication algorithm.</p>
Key Group	<p>Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are:</p> <p>None - disable DHx.</p> <p>DH2 - use a 1024-bit random number.</p> <p>DH5 - use a 1536-bit random number.</p> <p>DH14 - use a 2048-bit random number.</p> <p>The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.</p>
NAT Traversal	<p>Select this if any of these conditions are satisfied.</p> <ul style="list-style-type: none"> This IKE SA might be used to negotiate IPsec SAs that use ESP as the active protocol. There are one or more NAT routers between the VPN2S and remote IPsec router, and these routers do not support IPsec pass-thru or a similar feature. <p>The remote IPsec router must also enable NAT traversal, and the NAT routers have to forward packets with UDP port 500 and UDP 4500 headers unchanged.</p> <p>This field applies for IKEv1 only. NAT Traversal is always performed when you use IKEv2.</p>
Dead Peer Detection (DPD)	<p>Select this check box if you want the VPN2S to make sure the remote IPsec router is there before it transmits data through the IKE SA. The remote IPsec router must support DPD. If there has been no traffic for at least 15 seconds, the VPN2S sends a message to the remote IPsec router. If the remote IPsec router responds, the VPN2S transmits the data. If the remote IPsec router does not respond, the VPN2S shuts down the IKE SA.</p> <p>If the remote IPsec router does not support DPD, see if you can use the VPN connection connectivity check.</p> <p>This field applies for IKEv1 only. Dead Peer Detection (DPD) is always performed when you use IKEv2.</p>
X Auth / Extended Authentication Protocol	This part of the screen displays X-Auth when using IKEv1 and Extended Authentication Protocol when using IKEv2 .
X-Auth	This displays when using IKEv1 . When different users use the same VPN tunnel to connect to the VPN2S (telecommuters sharing a tunnel for example), use X-auth to enforce a user name and password check. This way even though telecommuters all know the VPN tunnel's security settings, each still has to provide a unique user name and password.

Table 66 VPN Gateway: Add/Edit

LABEL	DESCRIPTION
Enable Extended Authentication	When multiple IPsec routers use the same VPN tunnel to connect to a single VPN tunnel (telecommuters sharing a tunnel for example), use extended authentication to enforce a user name and password check. This way even though they all know the VPN tunnel's security settings, each still has to provide a unique user name and password. Select the check box if one of the routers (the VPN2S or the remote IPsec router) verifies a user name and password from the other router using the local user database and/or an external server.
Allowed Auth Method	This displays when using IKEv2 . Select the authentication method, which specifies how the VPN2S authenticates this information.
Server Mode	Select this if the VPN2S authenticates the user name and password from the remote IPsec router. You also have to select the AAA server to use for authentication if you use IKEv1 .
AAA Method	This displays when using IKEv2 . Select the AAA server to use to authenticate the user name and password from the remote IPsec router.
Client Mode	Select this radio button if the VPN2S provides a username and password to the remote IPsec router for authentication. You also have to provide the Username and the Password .
Username	This field is required if the VPN2S is in Client Mode for extended authentication. Type the user name the VPN2S sends to the remote IPsec router. The user name can be 1-64 ASCII characters. It is case-sensitive, but spaces are not allowed.
Password	This field is required if the VPN2S is in Client Mode for extended authentication. Type the password the VPN2S sends to the remote IPsec router. The password can be 4-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Retype to Confirm	Type the exact same password again here to make sure an error was not made when typing it originally.
OK	Click OK to save your settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

11.5.2 VPN Connection: Add/Edit

Click **Add** to create a new VPN Connection. You can also double click a VPN Connection or select one and click **Edit** to go to the following screen.

Figure 128 VPN Connection: Add/Edit

Connection Configuration - Add

General Settings

☐ Enable

Connection Name: !

☐ Nailed UP

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway: !

Policy

Local policy

IP Address Type:

Network: !

Netmask: !

Remote policy

IP Address Type:

Network: !

Netmask: !

☐ Full tunnel (Force all traffic to cross the VPN tunnel to the remote site)

Phase 2 Settings

SA Life Time: (180 - 3000000seconds)

Advanced

Encapsulation:

Proposal

#	Encryption
1	AES128

#	Authentication
1	SHA1

Perfect Forward Secrecy (PFS):

OK Cancel

The following table describes the labels in this screen.

Table 67 VPN Connection: Add/Edit

LABEL	DESCRIPTION
General Settings	
Enable	Select the check box to activate this VPN connection.
Connection Name	Type the name used to identify this IPsec SA. You may use 1-48 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Nailed Up	Select this if you want the VPN2S to automatically renegotiate the IPsec SA when the SA life time expires.
VPN Gateway	

Table 67 VPN Connection: Add/Edit

LABEL	DESCRIPTION
Application Scenario	<p>Select the scenario that best describes your intended VPN connection.</p> <p>Site-to-site - Choose this if the remote IPsec router has a static IP address or a domain name. This VPN2S can initiate the VPN tunnel.</p> <p>Site-to-site with Dynamic Peer - Choose this if the remote IPsec router has a dynamic IP address. Only the remote IPsec router can initiate the VPN tunnel.</p> <p>Remote Access (Server Role) - Choose this to allow incoming connections from IPsec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.</p> <p>Remote Access (Client Role) - Choose this to connect to an IPsec server. This VPN2S is the client (dial-in user) and can initiate the VPN tunnel.</p>
VPN Gateway	Select the VPN gateway this VPN connection is to use.
Policy	
Local policy	Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the remote IPsec device.
Remote Policy	Type the IP address of a computer behind the remote IPsec device. You can also specify a subnet. This must match the local IP address configured on the remote IPsec device.
Full Tunnel	Select this check box if you need the VPN2S to send packets through the VPN Tunnel.
Phase 2 Settings	
SA Life Time	Type the maximum number of seconds the IPsec SA can last. Shorter life times provide better security. The VPN2S automatically negotiates a new IPsec SA before the current one expires, if there are users who are accessing remote resources.
Advanced	
Encapsulation	<p>Select which type of encapsulation the IPsec SA uses. Choices are:</p> <p>Tunnel - this mode encrypts the IP header information and the data.</p> <p>Transport - this mode only encrypts the data.</p> <p>The VPN2S and remote IPsec router must use the same encapsulation.</p>
Proposal	Use this section to manage the encryption algorithm and authentication algorithm pairs the VPN2S accepts from the remote IPsec router for negotiating the IPsec SA.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.

Table 67 VPN Connection: Add/Edit

LABEL	DESCRIPTION
Encryption	<p>This field is applicable when the Active Protocol is ESP. Select which key size and encryption algorithm to use in the IPsec SA. Choices are:</p> <p>None - no encryption key or algorithm</p> <p>3DES - a 168-bit key with the DES encryption algorithm</p> <p>AES128 - a 128-bit key with the AES encryption algorithm</p> <p>AES192 - a 192-bit key with the AES encryption algorithm</p> <p>AES256 - a 256-bit key with the AES encryption algorithm</p> <p>The VPN2S and the remote IPsec router must both have at least one proposal that uses the same encryption and the same key.</p> <p>Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.</p>
Authentication	<p>Select which hash algorithm to use to authenticate packet data in the IPsec SA. Choices are SHA1, SHA256, and SHA512.</p> <p>The VPN2S and the remote IPsec router must both have a proposal that uses the same authentication algorithm.</p>
Perfect Forward Secrecy (PFS)	<p>Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are:</p> <p>DH2 - enable PFS and use a 1024-bit random number</p> <p>DH5 - enable PFS and use a 1536-bit random number</p> <p>DH14 - enable PFS and use a 2048-bit random number</p> <p>PFS changes the root key that is used to generate encryption keys for each IPsec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.</p>
OK	Click OK to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

11.5.3 The Default_L2TP_VPN_GW IPsec VPN Rule

A default IPsec VPN rule (**Default_L2TP_VPN_GW**) is predefined. It can be edited but cannot be removed. This rule is used for L2TP VPN exclusively and is disabled by default.

The following table lists the default settings for the **Default_L2TP_VPN_GW** IPsec VPN.

Table 68 Default settings for **Default_L2TP_VPN_GW**

GENERAL		AUTHENTICATION	
Enabled	No	Pre-Shared Key	none
Nailed-up	No	Certificate	none
NAT Traversal	Yes	Local ID Type	IP
Application Scenario	Remote Access	Content	0.0.0.0
My Address	Any	Remote ID Type	Any
PHASE 1		PHASE 2	
Life time	86400	Life time	3600
Negotiation Mode	Main	Tunnel Mode	ESP

Table 68 Default settings for **Default_L2TP_VPN_GW** (continued)

GENERAL		AUTHENTICATION	
Encryption	3DES AES192 AES256	Encryption	3DES AES192 AES256
Authentication	SHA1 SHA256 SHA512	Authentication	SHA1 SHA256 SHA512
Key Group	DH2	Perfect Forward Secrecy (PFS)	No
Dead Peer Detection (DPD)	Yes	Encapsulation	Transport
XAUTH	No		

11.5.4 PPTP VPN Troubleshooting Tips

This section lists the common troubleshooting tips for PPTP VPN.

- 1 A PPTP client device (such as a PC, smart phone, tablet) cannot connect to the VPN2S.

TIP: This could be due to one of the following reasons:

- a. The client device is not connected to the Internet successfully.

Action: Check the client device's Internet connection.

- b. Incorrect server address configured on the client device.

- (1) If the **Local WAN Interface** is “Any”:

From the VPN2S's GUI, click **Status**. The client device should be configured with one of the WAN interface IP addresses.

- (2) If the **Local WAN Interface** is an interface (IP address shown to the right):

Use that IP address for the client device to connect.

- c. The WAN interface which the VPN2S's PPTP VPN is using is not connected.

Action: From the VPN2S's GUI, click **Status**. Check if the WAN interface the client device is connected has an IP address present.

- d. The PPTP VPN is not enabled.

Action: From the VPN2S's GUI, click **VPN > PPTP VPN**. Check **Enable** check box and click **Apply**.

- e. PPTP is not configured correctly on the client device.

Action: Check the PPTP VPN configuration on the client device.

- f. The client entered an incorrect username or password.

Action: From the VPN2S's GUI, click **Maintenance > User Account**. The client should use one of the accounts to make the connection.

g. The VPN2S has already reached the maximum number of concurrent PPTP VPN connections.

Action: There are too many clients connected. Wait a while and then retry.

- 2 A PPTP client is disconnected unexpectedly.

Tip: A PPTP connection will be dropped when one of the followings occurs on the VPN2S:

a. The client has no activity for a period of time.

b. The client loses connectivity to the VPN2S for a period of time.

c. PPTP VPN is disabled on the VPN2S.

d. When any one of these configuration changes is applied on the VPN2S: WAN interface used for PPTP VPN, IP address pool, access group.

e. The VPN2S's WAN interface on which the PPTP connection is established is disconnected.

- 3 A PPTP client is connected successfully but cannot access the local host or server behind the VPN2S.

Tip: This may be caused by one of the followings:

a. The local host or server is disconnected.

b. The access group is not configured correctly. From the VPN2S's GUI, go to **VPN > PPTP VPN** to check. Note that all local hosts are by default accessible unless access group is configured.

c. **IP Address Pool** for PPTP VPN conflicts with any WAN, LAN, DMZ, WLAN, or L2TP VPN subnet configured on the VPN2S. Note that the **IP Address Pool** for PPTP VPN has a 24-bit netmask and should not conflict with any others listed above even if they are not in use.

- 4 A PPTP client is connected successfully but cannot browse the Internet.

Tip: From the VPN2S's GUI, click **VPN > PPTP VPN**. Check if **DNS Server** is configured. A client cannot browse the Internet without DNS resolved. Note that when a new DNS server is configured, the client must disconnect then reconnect in order for the new DNS Server to take effect.

- 5 An Android device cannot connect to the VPN2S's PPTP VPN.

Tip: Devices running an Android OS older than version 4.1 have issues with PPTP/MPPE encryption. Avoid using devices that run an Android OS older than version 4.1 for PPTP VPN connection.

11.6 The PPTP VPN Screen

Use this screen to configure settings for a Point to Point Tunneling Protocol (PPTP) server.

Click **Configuration > VPN > PPTP VPN** to open the following screen.

Figure 129 Configuration > VPN > PPTP VPN

PPTP VPN

PPTP Setup

☐ Enable

IP Address Pool: - (Subnet Mask :255.255.255.0)

Access LAN Group (Optional)

Group 1 IP Address: Subnet Mask:

Group 2 IP Address: Subnet Mask:

Note

1. Firewall /Security > Device Service must be configured to allow PPTP VPN access from the WAN.
 2. The maximum number of IP address is limited to 32.
 3. Each PPTP connection will use two IP addresses from the IP Address Pool. The maximum number of concurrent PPTP connections is 16.
 4. The IP Address Pool has a 24-bit netmask and should not conflict with any WAN, LAN, DMZ, WLAN, or L2TP VPN subnet even if they are not in use.
 5. Modifying Local WAN Interface, IP Address Pool, Access LAN Group will disconnect all existing PPTP VPN connections.
 6. If no Access LAN Group is configured, by default all LAN groups can be accessed.

Keep Alive Timer: (1-180)

DNS Server 1 (Optional):

DNS Server 2 (Optional):

WINS Server (Optional):

Note

1. A modification in the Keep Alive Timer will not take effect until you restart the PPTP VPN.
 2. A modification in the DNS Server and WINS Server will be applied to new PPTP VPN connections only.

The following table describes the labels in this screen.

Table 69 Configuration > VPN > PPTP VPN

LABEL	DESCRIPTION
PPTP Setup	
Enable	Use this field to turn the VPN2S's PPTP VPN function on or off.
IP Address Pool	Enter the pool of IP addresses that the VPN2S uses to assign to the PPTP VPN clients. Note: This is with a 24-bit netmask and should not conflict with any configured WAN, LAN, DMZ, WLAN, or L2TP VPN subnet even if they are not in use.
Access LAN Group (optional)	Specify up to 2 LAN groups (subnets) which a PPTP VPN client is allowed to access. If none is specified, all LAN groups can be accessed. Enter the IP address and Subnet Mask for the LAN group(s).
Keep Alive Timer	The VPN2S sends a Hello message after waiting this long without receiving any traffic from the remote user. The VPN2S disconnects the VPN tunnel if the remote user does not respond.
Preferred DNS Server (Optional)	Specify the IP addresses of DNS servers to assign to the remote users. You can choose from one of the DNS servers from the list, or choose User Defined to enter the static IP addresses for the first and second DNS servers manually.
Alternative DNS Server (Optional)	Specify the second DNS server address.

Table 69 Configuration > VPN > PPTP VPN

LABEL	DESCRIPTION
WINS Server (Optional)	The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. Type the IP addresses of up to two WINS servers to assign to the remote users.
Apply	Click Apply to save your changes back to the VPN2S.
Reset	Click Reset to restore your previous settings.

11.6.1 PPTP VPN Troubleshooting Tips

This section lists the common troubleshooting tips for PPTP VPN.

- 1 A PPTP client device (such as a PC, smart phone, tablet) cannot connect to the VPN2S.

TIP: This could be due to one of the following reasons:

- a. The client device is not connected to the Internet successfully.

Action: Check the client device's Internet connection.

- b. Incorrect server address configured on the client device.

(1) If the **Local WAN Interface** is "**Any**":

(2) If the **Local WAN Interface** is an interface (IP address shown to the right):

Use that IP address for the client device to connect.

- c. The WAN interface which the VPN2S's PPTP VPN is using is not connected.

Action: From the VPN2S's GUI, click **Status**. Check if the WAN interface the client device is connected has an IP address present.

- d. The PPTP VPN is not enabled.

Action: From the VPN2S's GUI, click **VPN > PPTP VPN**. Check **Enable** check box and click **Apply**.

- e. PPTP is not configured correctly on the client device.

Action: Check the PPTP VPN configuration on the client device.

- f. The client entered an incorrect username or password.

Action: From the VPN2S's GUI, click **Maintenance > User Account**. The client should use one of the accounts to make the connection.

- g. The VPN2S has already reached the maximum number of concurrent PPTP VPN connections.

Action: There are too many clients connected. Wait a while and then retry.

- 2 A PPTP client is disconnected unexpectedly.

Tip: A PPTP connection will be dropped when one of the followings occurs on the VPN2S:

- a. The client has no activity for a period of time.
- b. The client loses connectivity to the VPN2S for a period of time.
- c. PPTP VPN is disabled on the VPN2S.
- d. When any one of these configuration changes is applied on the VPN2S: WAN interface used for PPTP VPN, IP address pool, access group.
- e. The VPN2S's WAN interface on which the PPTP connection is established is disconnected.

- 3 A PPTP client is connected successfully but cannot access the local host or server behind the VPN2S.

Tip: This may be caused by one of the followings:

- a. The local host or server is disconnected.
- b. The access group is not configured correctly. From the VPN2S's GUI, go to **VPN > PPTP VPN** to check. Note that all local hosts are by default accessible unless access group is configured.
- c. **IP Address Pool** for PPTP VPN conflicts with any WAN, LAN, DMZ, WLAN, or L2TP VPN subnet configured on the VPN2S. Note that the **IP Address Pool** for PPTP VPN has a 24-bit netmask and should not conflict with any others listed above even if they are not in use.

- 4 A PPTP client is connected successfully but cannot browse the Internet.

Tip: From the VPN2S's GUI, click **VPN > PPTP VPN**. Check if **DNS Server** is configured. A client cannot browse the Internet without DNS resolved. Note that when a new DNS server is configured, the client must disconnect then reconnect in order for the new DNS Server to take effect.

- 5 An Android device cannot connect to the VPN2S's PPTP VPN.

Tip: Devices running an Android OS older than version 4.1 have issues with PPTP/MPPE encryption. Avoid using devices that run an Android OS older than version 4.1 for PPTP VPN connection.

11.7 The L2TP VPN Screen

Click **Configuration > VPN > L2TP VPN** to open the following screen. Use this screen to configure the VPN2S L2TP VPN settings.

11.7.1 L2TP Setup - Server

The following screen displays when you select **Server** in the **Type** field.

Figure 130 Configuration > VPN > L2TP VPN > Server

L2TP VPN

L2TP Setup

Type: Server

☐ Enable

IPsec: Default_L2TP_VPN_Connection(WAN Interface: Any)

IP Address Pool: 10.8.1.33 - 10.8.1.64 (Subnet Mask :255.255.255.0)

Access LAN Group (Optional)

Group 1	IP Address:	<input type="text"/>	Subnet Mask:	<input type="text"/>
Group 2	IP Address:	<input type="text"/>	Subnet Mask:	<input type="text"/>

Note:

1. The maximum number of IP address is limited to 32.
2. Each L2TP connection will use two IP addresses from the IP Address Pool. The maximum number of concurrent L2TP connections is 16.
3. The IP Address Pool has a 24-bit netmask and should not conflict with any WAN, LAN, DMZ, WLAN, or L2TP VPN subnet even if they are not in use.
4. Modifying Local WAN Interface, IP Address Pool, Access LAN Group will disconnect all existing L2TP VPN connections.
5. If no Access LAN Group is configured, by default all LAN groups can be accessed.

Keep Alive Timer: 60 (1-180)

DNS Server 1 (Optional): None

DNS Server 2 (Optional): None

WINS Server (Optional):

Note:

1. A modification in the Keep Alive Timer will not take effect until you restart the L2TP VPN.
2. A modification in the DNS Server and WINS Server will be applied to new L2TP VPN connections only.

Apply Reset

The following table describes the fields in this screen.

Table 70 Configuration > VPN > L2TP VPN > Server

LABEL	DESCRIPTION
L2TP Setup	
Type	Select Server to have the VPN2S Series act as a L2TP VPN server . Also, the screen varies depending on which option you select here.
Enable	Select the check box to enable the VPN2S's L2TP VPN function as a server.
IPsec	
IP Address Pool	Enter the pool of IP addresses that the VPN2S uses to assign to the L2TP VPN clients. Note: These addresses use a 24-bit netmask and should not conflict with any WAN, LAN, DMZ, WLAN, or PPTP VPN subnet even if they are not in use.
Access LAN Group (optional)	Specify up to 2 LAN groups (subnets) which a L2TP VPN client is allowed to access. If none is specified, all LAN groups can be accessed. Enter the IP address and Subnet Mask for the LAN group(s).
Keep Alive Timer	The VPN2S sends a Hello message after waiting this long without receiving any traffic from the remote user. The VPN2S disconnects the VPN tunnel if the remote user does not respond.
DNS Server 1 (Optional)	Specify the IP addresses of DNS servers to assign to the remote users. You can choose from one of the DNS servers from the list, or choose User Defined to enter the static IP addresses for the first and second DNS servers manually.
DNS Server 2 (Optional)	Specify the second DNS server address.
WINS Server (Optional)	The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. Type the IP addresses of up to two WINS servers to assign to the remote users.

Table 70 Configuration > VPN > L2TP VPN > Server

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the VPN2S.
Reset	Click Reset to restore your previous settings.

11.7.2 L2TP Setup - Client

The following screen displays when you select **Client** in the **Type** field.

Figure 131 Configuration > VPN > L2TP VPN > Client

L2TP VPN

L2TP Setup

Type: Client

☐ Enable

☒ Default Route Enable

☐ Nailed-up Enable

Nailed-up Period: 60 (10-180 seconds)

Server IP Address or Name: (L2TP/IPsec inactive)

IPsec(Default_L2TP_VPN_Connection) Disabled

Management IP Address: (Optional)

Local Host Name: SBG3310 (up to 64 characters)

☐ Tunnel Auth

Tunnel Secret: (4-64 characters, excluding '^=')

PPP Setup

☐ MPPE Enable

Auth Type: ☒ PAP ☒ CHAP

Username:

Password:

Interface Group NAT Setup

Default [LAN] 192.168.1.1/255.255.255.0 ☐ None ☐ NAT ☒ Address Mapping

Apply Reset

The following table describes the labels in this screen.

Table 71 Configuration > VPN > L2TP VPN > Client

LABEL	DESCRIPTION
Type	Select Client to have the VPN2S act as a L2TP VPN client. Also, the screen varies depending on which option you select here.
Enable	Select the check box to enable the VPN2S's L2TP VPN function as a client.
Default Route Enable	Select the check box to use the L2TP VPN connection as the system default route.
Nailed-up Enable	Select this if you want the VPN2S to automatically reconnect when the L2TP VPN connection is down. The attempt to reconnect will continue until the L2TP VPN connection is up again.
Nailed-up Period	Enter a value in seconds for the VPN2S to wait before re-initiating L2TP VPN connections. The valid range for the period is 10-180 seconds.
Server IP Address or Name	Enter the IP address or domain name of the LNS (L2TP Network Server).

Table 71 Configuration > VPN > L2TP VPN > Client

LABEL	DESCRIPTION
Management IP Address	Enter the VPN2S's public routable IP address for management purposes, and an administrator will be able to reach the VPN2S via L2TP VPN connection and the address input here.
Local Host Name	Enter the L2TP local host name.
Tunnel Auth	When performing tunnel authentication on the LNS (L2TP Network Server), please select the check box to enable tunnel authentication, and enter a valid Tunnel Secret in the next column.
Tunnel Secret	Enter a valid Tunnel Secret consisting of 4-64 characters, and the following special characters are not allowed: '/\=".
PPP Setup	
MPPE Enable	Click the check box to use MPPE, Microsoft Point to Point Encryption. It enables 40-bit encryption as well as 128-bit encryption. Note: PPP CHAP must be enabled as well.
Auth Type	Select PAP or/and CHAP as your authentication method(s). PAP (Password Authentication Protocol) - The L2TP server will crosscheck the username and password sent by the client with the database for authentication purposes. CHAP (Challenge Handshake Authentication Protocol) - When it's enabled, MS-CHAP and MS-CHAP-v2 are both supported. Also, CHAP needs to be enabled if you wish to activate MPPE.
Username	Enter the username for PPP authentication. It must be consistent with the configuration made on LNS (L2TP Network Server). Otherwise the L2TP VPN connection will not be established.
Password	Enter the password for PPP authentication. It must be consistent with the configuration made on LNS (L2TP Network Server). Otherwise the L2TP VPN connection will not be established.
Interface Group NAT Setup	
Default	Select None , NAT , or Address Mapping to apply to the L2TP VPN connection. None - NAT is not applied to the L2TP VPN connection. NAT - Select this option to turn on the NAT function on the VPN connection. Address Mapping - Select this option to apply the specified address mapping rule(s) to the VPN connection. The address mapping rules are configured using the Configuration > NAT > Address Mapping screen.
Apply	Click Apply to save your changes back to the VPN2S.
Reset	Click Reset to restore your previous settings.

11.7.3 L2TP VPN Troubleshooting Tips

This section lists the common troubleshooting tips for L2TP VPN.

- 1 A L2TP client device (such as a PC, smart phone, tablet) cannot connect to the VPN2S.

TIP: This could be due to one of the following reasons:

- a. The client device is not connected to the Internet successfully.

Action: Check the client device's Internet connection.

b. Incorrect server address configured on the client device.

Action: From the VPN2S's GUI, click **VPN > IPsec VPN**.

(1) If the **Local Gateway Address** for **Default_L2TP_VPN_GW** is set to **"Any"**:

(2) If the **Local Gateway Address** for **Default_L2TP_VPN_GW** is an IP address:

Use that IP address for the client device to connect.

c. The WAN interface which the VPN2S's L2TP VPN is using is not connected.

Action: From the VPN2S's GUI, click **Status**. Check if the WAN interface used by L2TP VPN is connected.

d. The client device has an incorrect IPsec pre-shared key configured.

Action: From the VPN2S's GUI, click **VPN > L2TP VPN**. The client device should use the same pre-shared key.

e. The L2TP VPN is not fully enabled.

Action: From the VPN2S's GUI,

(1) Click **VPN > L2TP VPN**. Select the **Enable** check box and click **Apply**.

(2) Click **VPN > L2TP VPN**. Select the **Enable** check box and click **Apply**.

f. L2TP or IPsec is not configured correctly on the client device.

Action: Check the L2TP VPN configuration on the client device.

g. The client entered an incorrect user name or password.

Action: From the VPN2S's GUI, click **Maintenance > User Account**. The client should use one of the accounts to make the connection.

h. The VPN2S exceeds the maximum number of concurrent L2TP VPN connections.

Action: There are too many clients connected. Wait a while and then retry.

- 2** A windows L2TP client fails to connect to the VPN2S with an "invalid certificate" message.

Tip: Windows sometimes may show this error even if the client device has been configured with a correct pre-shared key for authentication. This usually happens at the first connection attempt after a new connection profile is created. Reconfigure the pre-shared key on the client Windows device and retry the connection.

- 3** An L2TP client device cannot reconnect after it is disconnected.

Tip: If a client reconnects right after it is disconnected, the reconnection may fail. Wait 60 seconds before reconnecting.

- 4** An L2TP client is disconnected unexpectedly.

Tip: An L2TP connection will be dropped when one of the followings occurs on the VPN2S:

- (1) Client has no activity for a period of time.
- (2) Client loses connectivity to the VPN2S for a period of time.
- (3) Any IPsec VPN configuration change is applied on the VPN2S.
- (4) Either **Default_L2TP_VPN_GW** IPsec configuration or L2TP VPN is disabled on the VPN2S.
- (5) When any one of these configuration changes is applied on the VPN2S: WAN Interface used for L2TP VPN, IP Address Pool, Access Group.
- (6) The VPN2S WAN interface on which the L2TP connection established is disconnected.

- 5 An L2TP client is connected successfully but cannot access the local host or server behind the VPN2S.

Tip: This may be caused by one of the followings:

- (1) The local host or server is disconnected.
- (2) The Access Group is not configured correctly. From the VPN2S's GUI, go to the **VPN > L2TP VPN** screen to check. Note that all local hosts are by default accessible unless Access Group is configured.
- (3) **IP Address Pool** for L2TP VPN is conflicting with any WAN, LAN, DMZ, WLAN, or PPTP VPN subnet configured on the VPN2S. Note that **IP Address Pool** for L2TP VPN has 24-bit netmask and should not conflict with any others listed above even if they are not in use.

- 6 An L2TP client is connected successfully but cannot browse Internet.

Tip: From the VPN2S's GUI, click **VPN > L2TP VPN**. Check if DNS Server is configured. A client cannot browse Internet without DNS resolved. Note that when a new DNS Server is configured, the client must disconnect then reconnect in order for the new DNS Server to take effect.

- 7 The L2TP client can no longer connect to VPN2S after the **Encryption** or **Authentication** for the **Default_L2TP_VPN_GW** IPsec VPN rule is changed.

Tip: A user usually do not need change the default **Encryption** or **Authentication** algorithms in the **Default_L2TP_VPN** IPsec VPN rule. The default **Encryption** and **Authentication** algorithms should support the built-in L2TP/IPsec client software in the popular operating systems (Windows (XP, Vista, 7), Android, and iOS).

Refer to [Table 67 on page 167](#) for the default setting of the **Default_L2TP_VPN_GW** IPsec VPN rule.

As a reference, [Table 72 on page 179](#) lists the IPsec proposals provided by a built-in L2TP client in the popular operating systems during IPsec phase 1 negotiation. The first proposal that can be supported by the phase 1 setting in the **Default_L2TP_VPN_GW** IPsec VPN rule will be accepted by the VPN2S. The algorithms in red in [Table 72 on page 179](#) indicate the ones that will be accepted based on [Table 68 on page 169](#).

Table 72 Phase 1 IPsec proposals provided by the built-in L2TP client in popular operating systems (Encryption/Authentication/Key Group)

	WINDOWS XP	WINDOWS VISTA	WINDOWS 7	IOS 5.1	ANDROID 4.1
1	3DES/SHA1/DH15	3DES/SHA1/DH15	AES/SHA1/DH15	AES/SHA1/DH2	AES/SHA1/DH2
2	3DES/SHA1/DH2	3DES/SHA1/DH2	3DES/SHA1/DH15	AES/MD5/DH2	AES/MD5/DH2
3	3DES/MD5/DH2		3DES/SHA1/DH2	3DES/SHA1/DH2	3DES/SHA1/DH2

Table 72 Phase 1 IPsec proposals provided by the built-in L2TP client in popular operating systems (Encryption/Authentication/Key Group)

	WINDOWS XP	WINDOWS VISTA	WINDOWS 7	IOS 5.1	ANDROID 4.1
4	DES/SHA1/DH1			3DES/MD5/DH2	3DES/MD5/DH2
5	DES/MD5/DH1				DES/SHA1/DH2
6					DES/MD5/DH2

After phase 1 tunnel is established, IPsec phase 2 negotiations begin. [Table 73 on page 180](#) lists the IPsec phase 2 proposals provided by a built-in L2TP client in the popular operating systems. The first proposal that can be supported by the phase 2 setting in the **Default_L2TP_VPN_GW** IPsec VPN rule will be accepted by the VPN2S. The algorithms in red in [Table 73 on page 180](#) indicate the ones that will be accepted based on [Table 68 on page 169](#).

Table 73 Phase 2 IPsec proposals provided by the built-in L2TP client in popular operating systems (Tunnel Mode/Encryption/Authentication) [Encapsulation = Transport]

	WINDOWS XP	WINDOWS VISTA	WINDOWS 7	IOS 5.1	ANDROID 4.1
1	ESP/3DES/MD5 ESP/3DES/SHA1	ESP/AES/SHA1	ESP/AES/SHA1	ESP/AES/SHA1 ESP/AES/MD5 ESP/3DES/SHA1 ESP/3DES/MD5	ESP/AES/SHA1 ESP/AES/MD5 ESP/3DES/SHA1 ESP/3DES/MD5 ESP/DES/SHA1 ESP/DES/MD5
2	AH/-/SHA1 and ESP/3DES/-	ESP/3DES/SHA1	ESP/3DES/SHA1		
3	AH/-/MD5 and ESP/3DES/-	AH/-/SHA1 and ESP/AES/-	ESP/DES/SHA1		
4	AH/-/SHA1 and ESP/3DES/SHA1	AH/-/SHA1 and ESP/3DES/-	ESP/-/SHA1		
5	AH/-/MD5 and ESP/3DES/MD5	AH/-/SHA1 and ESP/3DES/SHA1	AH/-/SHA1		
6	ESP/DES/MD5 ESP/ DES/SHA1	ESP/-/SHA1			
		AH/-/SHA1			

11.8 The L2TP Client Status Screen

Use the **L2TP Client Status** screen to view details about the L2TP clients. Click **Configuration > VPN > L2TP Client Status** to open the following screen.

Figure 132 Configuration > VPN > L2TP Client Status

L2TP Client Status

L2TP Status Updated in 12 seconds

Status	Up Time	Server Name	Server WAN IP	Client WAN IP	Server L2TP IP	Client L2TP IP
	00:00:00					

Last disconnection: L2TP VPN in Server Mode [05/12/17 06:09:22]

L2TP Statistics

Rx Data Packets	Rx Data Bytes	Rx Err...	Tx Data Packets	Tx Data Bytes	Tx Errors
0	0	0	0	0	0

The following table describes the labels in this screen.

Table 74 Configuration > VPN > L2TP Client Status

LABEL	DESCRIPTION
L2TP Status	
Status	This field displays whether the L2TP VPN is active or not. A yellow bulb signifies that this VPN is active. A gray bulb signifies that this VPN is not active.
Up Time	This field displays the period of time this connection has been up.
Server Name	This field displays the name of the L2TP Network Server.
Server WAN IP	This field displays the WAN IP address of the L2TP Network Server.
Client WAN IP	This field displays the WAN IP address of the L2TP client.
Server L2TP IP	This field displays the assigned L2TP IP address of the L2TP network server.
Client L2TP IP	This field displays the assigned L2TP IP address of the L2TP client.
L2TP Statistics	
Rx Data Packets	This indicates the number of packets received in this L2TP connection.
Rx Data Bytes	This indicates the number of bytes received in this L2TP connection.
Rx Errors	This indicates the number of received packet errors in this L2TP connection.
Tx Data Packets	This indicates the number of packets transmitted in this L2TP connection.
Tx Data Bytes	This indicates the number of bytes transmitted in this L2TP connection.
Tx Errors	This indicates the number of transmitted packet errors in this L2TP connection.

11.9 The GRE VPN Screen

Use the **GRE VPN** screen to configure the Generic Routing Encapsulation (GRE) VPN settings. GRE VPN can encase network layer protocols inside a VPN tunnel. However, GRE VPN does not use encryption like IPsec VPN, so it is not as secure. Click **Configuration > VPN > GRE VPN** to open the following screen.

Figure 133 Configuration > VPN > GRE VPN

GRE VPN

#	Status	Tunnel Name	WAN Interface	Local IP Address	Remote Peer IP Address
<div> ◀ ▶ Page 0 of 0 ▶ Show 20 items </div> <div style="text-align: right;">No data to display</div>					

The following table describes the labels in this screen.

Table 75 Configuration > VPN > GRE VPN

LABEL	DESCRIPTION
Add	Click this to configure a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an existing entry, select it and click Remove.
Multiple Entries On	Select one or more GRE VPN policies, and click this to enable them.
Multiple Entries Off	Select one or more GRE VPN policies, and click this to disable them.
#	This column lists the index numbers of the GRE VPN connection.
Status	This field displays whether the GRE VPN connection is active or not. A green ON button signifies that this GRE VPN connection is active. A gray OFF button signifies that this GRE VPN connection is not active.
Tunnel Name	This field displays the identification name for this GRE VPN policy.
WAN Interface	This field displays the WAN interface this GRE VPN policy uses.
Local IP Address	This displays the WAN interface IP address.
Remote Peer IP Address	This displays an IP address of the remote device terminating the GRE VPN tunnel.

11.9.1 GRE VPN: Add/Edit

Click **Add** to create a new GRE VPN. You can also double click an existing GRE VPN or select one and click **Edit** to go to the following screen.

Figure 134 GRE VPN: Add/ Edit

The following table describes the labels in this screen.

Table 76 GRE VPN > Add / Edit

LABEL	DESCRIPTION
Enable	Select this check box to activate this GRE VPN connection.
Tunnel Name	Specify an identification name for this GRE VPN connection.
Interface IP Address	Specify an IPv4 IP address for the GRE VPN connection.

Table 76 GRE VPN > Add / Edit

LABEL	DESCRIPTION
Interface Subnet Mask	Specify a subnet mask for the interface IP address the GRE VPN connection.
Local WAN Interface	Select the WAN interface used to establish this VPN connection.
Remote Peer IP Address	Specify an IP address of the remote peer to which you are connecting through the GRE VPN tunnel.
Ping Remote Target	Specify an IP address to ping behind the GRE VPN connection.
Routing	
Destination Subnet	Specify the destination IP address of this GRE VPN connection.
Destination Subnet Mask	Specify the IP network subnet mask of the GRE remote subnet.
OK	Click OK to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

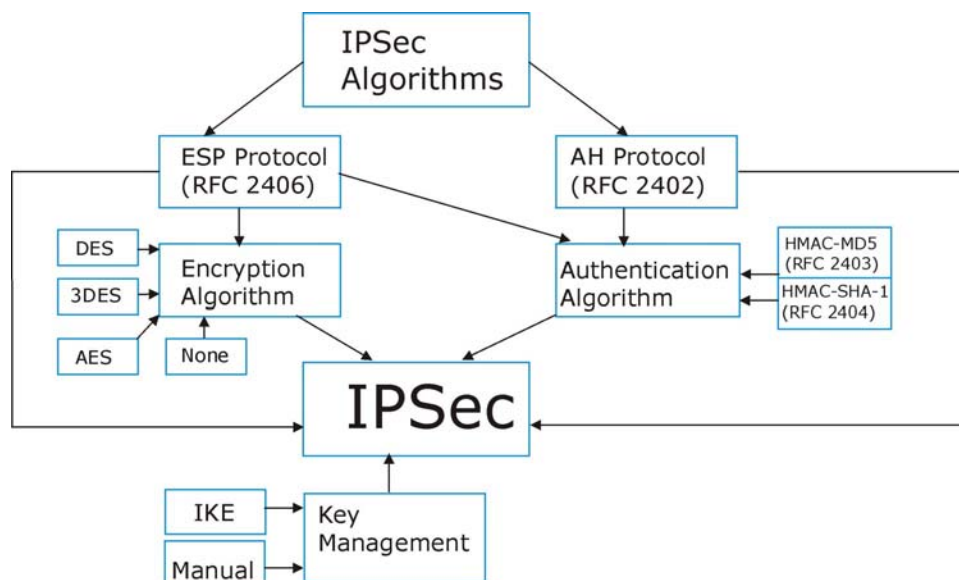
11.10 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

11.10.1 IPsec Architecture

The overall IPsec architecture is shown as follows.

Figure 135 IPsec Architecture



IPsec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404), provide an authentication mechanism for the **AH** and **ESP** protocols.

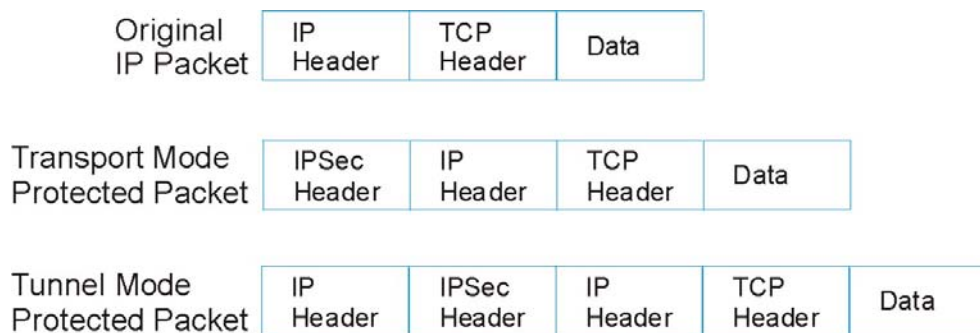
Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

11.10.2 Encapsulation

The two modes of operation for IPsec VPNs are **Transport** mode and **Tunnel** mode. At the time of writing, the VPN2S supports **Tunnel** mode only.

Figure 136 Transport and Tunnel Mode IPsec Encapsulation



Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. 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.

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

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **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. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

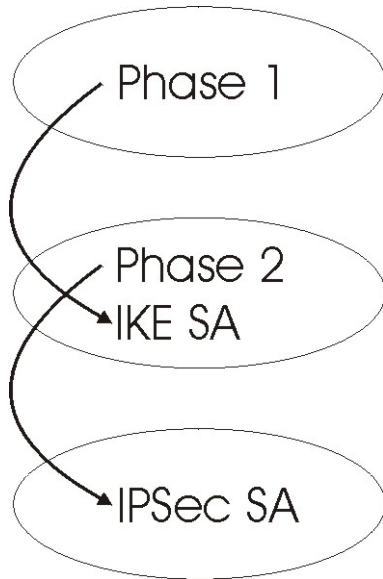
- **Outside header:** The outside IP header contains the destination IP address of the VPN gateway.

- **Inside header:** The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

11.10.3 IKE Phases

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.

Figure 137 Two Phases to Set Up the IPsec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPsec SA is already established, the IPsec SA stays connected.

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPsec SA lifetime. This field allows you to determine how long the IPsec SA should stay up before it times out. The VPN2S automatically renegotiates the IPsec SA if there is traffic when the IPsec SA lifetime period expires. If an IPsec SA times out, then the IPsec router must renegotiate the SA the next time someone attempts to send traffic.

11.10.4 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **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 known by the responder and both parties want to use pre-shared key authentication.

11.10.5 IPsec and NAT

Read this section if you are running IPsec on a host computer behind the VPN2S.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPsec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPsec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPsec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 77 VPN and NAT

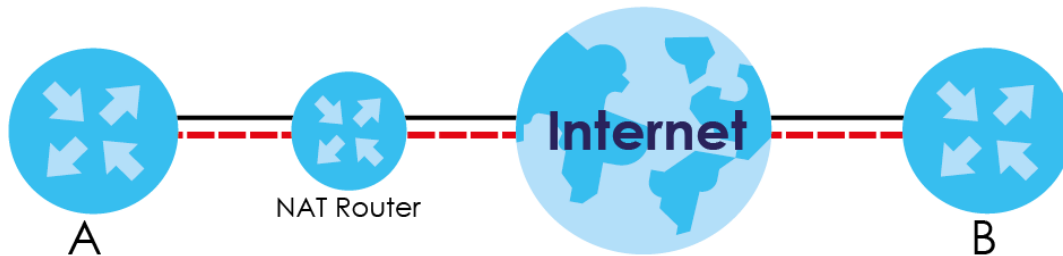
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

11.10.6 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPsec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPsec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the VPN2S's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPsec routers.

Figure 138 NAT Router Between IPsec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPsec routers because the NAT router changes the header of the IPsec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPsec packet. The NAT router forwards the IPsec packet with the UDP port 500 header unchanged. In the above figure, when IPsec router **A** tries to establish an IKE SA, IPsec router **B** checks the UDP port 500 header, and IPsec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPsec endpoints.
- Set the NAT router to forward UDP port 500 to IPsec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 78 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

Y* - This is supported in the VPN2S if you enable NAT traversal.

11.10.7 ID Type and Content

With aggressive negotiation mode (see [Section 11.10.4 on page 186](#)), the VPN2S identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the VPN2S to distinguish between multiple rules for SAs that connect from remote IPsec routers that have dynamic WAN IP addresses.

Regardless of the ID type and content configuration, the VPN2S does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see [Section 11.10.4 on page 186](#)), the ID type and content are encrypted to provide identity protection. In this case the VPN2S can only distinguish between different incoming SAs that connect from remote IPsec routers that have dynamic WAN IP addresses. The VPN2S can distinguish incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and eight key groups when you configure a VPN rule (see [Section 11.6 on page 171](#)). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 79 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer.
FQDN	Type a domain name (up to 31 characters) by which to identify this VPN2S.
User-FQDN	Type an e-mail address (up to 31 characters) by which to identify this VPN2S.
	The domain name or e-mail address that you use in the Local ID Content field is used for identification purposes only and does not need to be a real domain name or e-mail address.

11.10.7.1 ID Type and Content Examples

Two IPsec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two VPN2Ss in this example can complete negotiation and establish a VPN tunnel.

Table 80 Matching ID Type and Content Configuration Example

VPN2S A	VPN2S B
Local ID type: User-FQDN	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Remote ID type: IP	Remote ID type: E-mail
Remote ID content: 1.1.1.2	Remote ID content: tom@yourcompany.com

The two VPN2Ss in this example cannot complete their negotiation because VPN2S B's **Local ID type** is **IP**, but VPN2S A's **Remote ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 81 Mismatching ID Type and Content Configuration Example

VPN2S A	VPN2S B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.2

Table 81 Mismatching ID Type and Content Configuration Example

VPN2S A	VPN2S B
Remote ID type: User-FQDN	Remote ID type: IP
Remote ID content: aa@yahoo.com	Remote ID content: 1.1.1.0

11.10.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see [Section 11.10.3 on page 185](#) for more on IKE phases). It is called “pre-shared” because you have to share it with another party before you can communicate with them over a secure connection.

11.10.9 Diffie-Hellman (DH) Key Groups

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. 768-bit, 1024-bit 1536-bit, 2048-bit, and 3072-bit 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.

CHAPTER 12

Bandwidth Management

12.1 Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

Configure QoS on the VPN2S to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

- 1 Configure classifiers to sort traffic into different flows.
- 2 Assign priority and define actions to be performed for a classified traffic flow.

The VPN2S assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

This chapter contains information about configuring QoS and editing classifiers.

12.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth ([Section 12.2 on page 192](#)).
- The **Queue Setup** screen lets you configure QoS queue assignment ([Section 12.3 on page 193](#)).
- The **Classification Setup** screen lets you add, edit or delete QoS classifiers ([Section 12.4 on page 196](#)).
- The **Policer Setup** screen lets you add, edit or delete QoS policers ([Section 12.5 on page 200](#)).
- The **Shaper Setup** screen lets you limit outgoing traffic transmission rate on the selected interface ([Section 12.6 on page 202](#)).

12.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

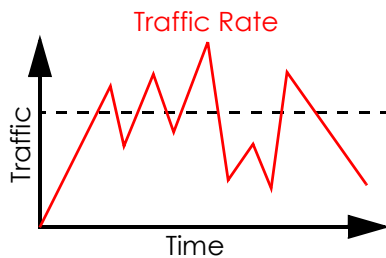
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

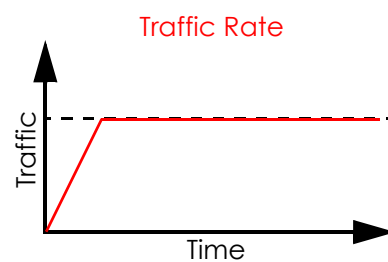
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Your VPN2S uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



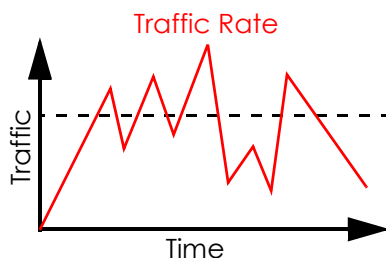
(Before Traffic Shaping)



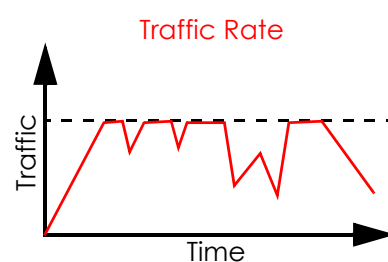
(After Traffic Shaping)

Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.



(Before Traffic Policing)



(After Traffic Policing)

The VPN2S supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Marker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See [Section 12.7 on page 204](#) for more information on each metering algorithm.

12.2 The General Screen

Click **Configuration > Bandwidth Management > General** to open the screen as shown next.

Use this screen to enable or disable QoS and set the upstream bandwidth. See [Section 12.1 on page 190](#) for more information.

Figure 139 Configuration > Bandwidth Management > General

General

General Settings

☐ Enable

WAN Managed Upstream Bandwidth: (kbps) (0,1000~1048576), 0:Not limit

LAN Managed Downstream Bandwidth: (kbps) (0,1000~1048576), 0:Not limit

Upstream Traffic Priority Assigned By:

Note:

1. You can assign the upstream bandwidth manually.
2. If the field is empty, the CPE sets the value automatically.
3. If QoS is enabled, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier.
4. If the WAN Managed Upstream Bandwidth is greater than the current WAN interface linkup rate, then the WAN Managed Upstream Bandwidth will become current WAN interface linkup rate.

Session Control

Default Session per Host: (0~8192), 0:Not limit

The following table describes the labels in this screen.

Table 82 Configuration > Bandwidth Management > General

LABEL	DESCRIPTION
Enable	Select the Enable check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	<p>Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps.</p> <p>You can set this number higher than the interfaces' actual transmission speed.</p> <p>You can also set this number lower than the interfaces' actual transmission speed. This will cause the VPN2S to not use some of the interfaces' available bandwidth.</p> <p>If you leave this field blank, the VPN2S automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed.</p>

Table 82 Configuration > Bandwidth Management > General (continued) (continued)

LABEL	DESCRIPTION
LAN Managed Downstream Bandwidth	<p>Enter the amount of downstream bandwidth for the LAN interfaces (including WLAN) that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the WAN interfaces' actual transmission speed. For example, set the LAN managed downstream bandwidth to 100000 kbps if you use a 100 Mbps wired Ethernet WAN connection.</p> <p>You can also set this number lower than the WAN interfaces' actual transmission speed. This will cause the VPN2S to not use some of the interfaces' available bandwidth.</p> <p>If you leave this field blank, the VPN2S automatically sets this to the LAN interfaces' maximum supported connection speed.</p>
Upstream traffic priority Assigned by	<p>Select how the VPN2S assigns priorities to various upstream traffic flows.</p> <ul style="list-style-type: none"> • None: Disables auto priority mapping and has the VPN2S put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority. • Ethernet Priority: Automatically assign priority based on the IEEE 802.1p priority level. • IP Precedence: Automatically assign priority based on the first three bits of the TOS field in the IP header. • Packet Length: Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, internet gaming, or other real-time packets are usually small while larger packets are usually best effort • data packets like file transfers.
Session Control	
Default Session per Host	<p>Enter a session limit for each host.</p> <p>Use the field to set a common limit to the number of concurrent NAT/firewall sessions each client device can have.</p> <p>If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.</p>
Apply	Click Apply to save your changes.
Reset	Click Reset to restore your previously saved settings.

12.3 The Queue Setup Screen

Click **Configuration > Bandwidth Management > Queue Setup** to open the screen as shown next.

Use this screen to configure QoS queue assignment.

Figure 140 Configuration > Bandwidth Management > Queue Setup

Queue Setup							
<div> + Add Edit Remove Multiple Entries Turn On Multiple Entries Turn Off </div>							
...	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit(kbps)
1		Default queue	WAN	8	1	DT	0
2		PriQ1	WAN	1	1	DT	0
3		PriQ2	WAN	2	1	DT	0
4		PriQ3	WAN	3	1	DT	0
5		PriQ4	WAN	4	1	DT	0
6		PriQ5	WAN	5	1	DT	0
7		PriQ6	WAN	6	1	DT	0
8		PriQ7	WAN	7	1	DT	0
<div> ◀ ◀ Page 1 of 1 ▶ ▶ Show 20 Items <div>Displaying 1 - 8 of 8</div> </div>							

The following table describes the labels in this screen.

Table 83 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add	Click this button to create a new queue entry.
Edit	Double-click a queue entry or select it and click Edit to open a screen where you can modify the queue's settings.
Remove	To remove an existing queue entry, select it and click Remove . Note that subsequent rules move up by one when you take this action.
Multiple Entries Turn On	Select a queue and click this to enable it.
Multiple Entries Turn Off	Select a queue and click this to disable it.
#	This is the index number of the queue entry.
Status	<p>This field displays whether the queue is active or not. A green ON button signifies that this queue is active. A gray OFF button signifies that this queue is not active.</p> <p>Click the slide button to turn on or turn off the queue.</p>
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the VPN2S's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	<p>This shows the queue management algorithm used for this queue.</p> <p>Queue management algorithms determine how the VPN2S should handle packets when it receives too many (network congestion).</p>
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.

12.3.1 QoS Queue: Add/Edit

Click **Add** or select an existing queue and click **Edit** icon in the **Queue Setup** screen to configure a queue.

Figure 141 Queue Setup: Add/Edit

The following table describes the labels in this screen.

Table 84 Queue Setup: Add/Edit

LABEL	DESCRIPTION
Enable	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue. You can use up to 31 alphanumeric characters, it must begin with a letter. The valid characters are [0-9][a-z] [A-Z][_]. This field is not configurable if you are editing an existing queue.
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 8) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the VPN2S divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Dropping Algorithm	This field displays Drop Tail (DT) . Drop Tail (DT) is a simple queue management algorithm that allows the VPN2S buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

12.4 The Classification Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the VPN2S forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Configuration > Bandwidth Management > Classification Setup** to open the following screen.

Figure 142 Configuration > Bandwidth Management > Classification Setup

#	Status	Class Name	Classification Criteria	DSCP Mark	802.1P Mark	VLAN ID T...	To Queue
1	<input type="radio"/> OFF	class1	From Intf: LAN Ether Type: NA	Unchange	Unchange	Unchange	Default queue

Navigation: Add, Edit, Remove, Multiple Entries Turn On, Multiple Entries Turn Off. Page 1 of 1. Show 20 items. Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 85 Configuration > Bandwidth Management > Classification Setup

LABEL	DESCRIPTION
Add	Click this to create a new classifier.
Edit	Double-click a classifier or select it and click Edit to open a screen where you can modify the classifier's settings.
Remove	To remove an existing classifier, select it and click Remove . Note that subsequent rules move up by one when you take this action.
Multiple Entries Turn On	Select one or more classifier and click this to enable them.
Multiple Entries Turn Off	Select one or more classifier and click this to disable them.
#	This field displays the order in which this classifier is applied.
Status	This field displays whether the classifier is active or not. A green ON button signifies that this classifier is active. A gray OFF button signifies that this classifier is not active. Click the slide button to turn on or turn off the classifier.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.

12.4.1 QoS Class: Add/Edit

Click **Add** in the **Classification Setup** screen or the **Edit** icon next to a classifier to open the following screen.

Figure 143 Classification Setup: Add/Edit

Classification Setup - Add

Classification Setup

☒ Enable

Class Name:

Order:

Basic Criteria Configuration

From Interface:

Ether Type:

Source Criteria Configuration

☒ Address: Subnet Mask: ☐ Exclude

☐ Starting Port: 1~65535 Ending Port: 1~65535 ☐ Exclude

☒ MAC Address: MAC Mask: ☐ Exclude

Destination Criteria Configuration

☒ Address: Subnet Mask: ☐ Exclude

☐ Starting Port: 1~65535 Ending Port: 1~65535 ☐ Exclude

☒ MAC Address: MAC Mask: ☐ Exclude

Other Criteria Configuration

☒ Service: ☐ Exclude

☒ IP Protocol: ☐ Exclude

☒ DHCP: ☐ Exclude

☒ Packet Length: ~ ☐ Exclude

☒ DSCP Code: (0~63) ☐ Exclude

☐ 802.1P: ☐ Exclude

☐ VLAN ID: ☐ Exclude

☒ TCP ACK ☐ Exclude

DSCP Marking:

VLAN ID:

802.1P Marking:

Class Routing

Forward Interface:

Outgoing Queue

To Queue:

The following table describes the labels in this screen.

Table 86 Classification Setup: Add/Edit

LABEL	DESCRIPTION
Classification Setup	
Enable	Select this to enable this classifier.

Table 86 Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Class Name	Enter a descriptive name for the classifier. You can use up to 31 alphanumeric characters, it must begin with a letter. The valid characters are [0-9][a-z] [A-Z][_].
Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking OK . Ordering your classifiers is important because the VPN2S applies the classifiers in the order that you specify.
Basic Criteria Configuration	
From Interface	If you want to classify the traffic by an ingress interface, select an interface from the From Interface drop-down list box.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select IP , you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select 802.1Q , you can configure an 802.1p priority level.
Source Criteria Configuration	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask.
Starting Port	Enter the starting port of the source.
Ending Port	Enter the ending port of the source,
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination Criteria Configuration	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask.
Starting Port	Enter the starting port of the source.
Ending Port	Enter the ending port of the source,
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Other Criteria Configuration	

Table 86 Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Service	<p>This field is available only when you select IP in the Ether Type field.</p> <p>This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields.</p>
IP Protocol	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select the protocol (service type) from TCP, UDP, ICMP or IGMP. If you select User defined, enter the protocol (service type) number.</p>
DHCP	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select a DHCP option.</p> <p>If you select Vendor Class ID (DHCP Option 60), enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.</p> <p>If you select Client ID (DHCP Option 61), enter the Identity Association Identifier (IAD Option 61) of the matched traffic such as the MAC address of the device.</p> <p>If you select User Class ID (DHCP Option 77), enter a string that identifies the user's category or application type in the matched DHCP packets.</p> <p>If you select Vendor Specific Info (DHCP Option 125), enter the vendor specific information of the matched traffic, such as the Enterprise Number, Manufacture OUI, Serial Number and Product Class of the device.</p>
Packet Length	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.</p>
DSCP Code	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.</p>
802.1P	<p>This field is available only when you select 802.1Q in the Ether Type field.</p> <p>Select this option and select a priority level (between 0 and 7) from the drop-down list box.</p> <p>"0" is the lowest priority level and "7" is the highest.</p>
VLAN ID	<p>This field is available only when you select 802.1Q in the Ether Type field.</p> <p>Select this option and specify a VLAN ID number.</p>
TCP ACK	<p>This field is available only when you select IP in the Ether Type field.</p> <p>If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.</p>
Exclude	<p>Select this option to exclude the packets that match the specified criteria from this classifier.</p>
DSCP Marking	<p>This field is available only when you select IP in the Ether Type field.</p> <p>If you select Mark, enter a DSCP value with which the VPN2S replaces the DSCP field in the packets.</p> <p>If you select Unchange, the VPN2S keep the DSCP field in the packets.</p>
VLAN ID	<p>If you select Remark, enter a VLAN ID number with which the VPN2S replaces the VLAN ID of the frames.</p> <p>If you select Remove, the VPN2S deletes the VLAN ID of the frames before forwarding them out.</p> <p>If you select Add, the VPN2S treat all matched traffic untagged and add a second VLAN ID.</p> <p>If you select Unchange, the VPN2S keep the VLAN ID in the packets.</p>
802.1P Marking	<p>Select a priority level with which the VPN2S replaces the IEEE 802.1p priority field in the packets.</p> <p>If you select Unchange, the VPN2S keep the 802.1p priority field in the packets.</p>

Table 86 Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Class Routing	
Forward Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select Unchange , the VPN2S forward traffic of this class according to the default routing table.
Outgoing Queue	
To Queue	Select a queue that applies to this class. You should have configured a queue in the Queue Setup screen already.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

12.5 The Policer Setup Screen

Use this screen to configure QoS policers that allow you to limit the transmission rate of incoming traffic. Click **Configuration > Bandwidth Management > Policer Setup**. The screen appears as shown.

Figure 144 Configuration > Bandwidth Management > Policer Setup

The following table describes the labels in this screen.

Table 87 Network Setting > QoS > Policer Setup

LABEL	DESCRIPTION
Add	Click this to create a new policer.
Edit	Double-click a policer or select it and click Edit to open a screen where you can modify the policer's settings.
Remove	To delete an existing policer, select it and click Remove . Note that subsequent rules move up by one when you take this action.
Multiple Entries Turn On	Select one or more policers and click this to enable them.
Multiple Entries Turn Off	Select one or more policers and click this to disable them.
#	This is the index number of the policer.
Status	This field displays whether the policer is active or not. A green ON button signifies that this policer is active. A gray OFF button signifies that this policer is not active. Click the slide button to turn on or turn off the policer.
Name	This field displays the descriptive name of this policer.
Regulated Classes	This field displays the name of a QoS classifier.
Meter Type	This field displays the type of QoS metering algorithm used in this policer.

Table 87 Network Setting > QoS > Policer Setup (continued)

LABEL	DESCRIPTION
Rule	These are the rates and burst sizes against which the policer checks the traffic of the member QoS classes.
Action	This shows the how the policer has the VPN2S treat different types of traffic belonging to the policer's member QoS classes.

12.5.1 QoS Policer: Add/Edit

Click **Add** in the **Policer Setup** screen or select a policer and click **Edit** next to a policer to show the following screen.

Figure 145 Policer Setup: Add/Edit

The following table describes the labels in this screen.

Table 88 Policer Setup: Add/Edit

LABEL	DESCRIPTION
Policer Setting	
Enable	Select the check box to activate this policer.
Name	Enter the descriptive name of this policer. You can use up to 31 alphanumeric characters, it must begin with a letter. The valid characters are [0-9] [a-z] [A-Z] [-].

Table 88 Policer Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Meter Type	<p>This shows the traffic metering algorithm used in this policer.</p> <p>The Simple Token Bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to b bytes which is also the bucket size.</p> <p>The Single Rate Three Color Marker (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS).</p>
Committed Rate	Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic.
Committed Burst Size	<p>Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured.</p> <p>This is the maximum size of the (first) token bucket in a traffic metering algorithm.</p>
Excess Burst Size	Specify the burst size of packet bursts above which the VPN2S will perform the non-conforming action.
Conforming Action	<p>Specify what the VPN2S does for packets within the committed rate and burst size (green-marked packets).</p> <ul style="list-style-type: none"> • Pass: Send the packets without modification. • DSCP Mark: Change the DSCP mark value of the packets. Enter the DSCP mark value to use.
Partial Conforming Action	<p>Specify what the VPN2S does for packets that exceed the committed rate and burst size but are within the excess burst size or peak rate and burst size (yellow-marked packets).</p> <ul style="list-style-type: none"> • Drop: Discard the packets. • Pass: Send the packets without modification. • DSCP Mark: Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network.
Non-Conforming Action	<p>Specify what the VPN2S does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets).</p> <ul style="list-style-type: none"> • Drop: Discard the packets. • DSCP Mark: Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network.
Regulated Classes Member Setting	
Available Member	<p>Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier.</p> <p>Highlight a QoS classifier in the Available box and use the → button to move it to the Member box.</p> <p>To remove a QoS classifier from the Member box, select it and use the ← button.</p>
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

12.6 The Shaper Setup Screen

This screen shows that you can use the token bucket algorithm to allow a certain amount of large bursts while keeping a limit for processing outgoing traffic at the average rate. Click **Configuration > Bandwidth Management > Shaper Setup**. The screen appears as shown:

Figure 146 Configuration > Bandwidth Management > Shaper Setup

The following table describes the labels in this screen.

Table 89 Configuration > Bandwidth Management > Shaper Setup

LABEL	DESCRIPTION
Add	Click this to create a new shaper.
Edit	Double-click a shaper or select it and click Edit to open a screen where you can modify the shaper's settings.
Remove	To remove an existing shaper, select it and click Remove . Note that subsequent rules move up by one when you take this action.
Multiple Entries Turn On	Select one or more shapers and click this to enable them.
Multiple Entries Turn Off	Select one or more shapers and click this to disable them.
#	This is the index number of the entry.
Status	This field displays whether the shaper is active or not. A green ON button signifies that this shaper is active. A gray OFF button signifies that this shaper is not active. Click the slide button to turn on or turn off the shaper.
Outgoing Interface	This shows the name of the VPN2S's interface through which traffic in this shaper applies.
Rate Limit (kbps)	This shows the average rate limit of traffic bursts for this shaper.

12.6.1 QoS Shaper: Add/Edit

Click **Add** in the **Shaper Setup** screen or select a shaper and click **Edit** to show the following screen.

Figure 147 Shaper Setup: Add/Edit

The following table describes the labels in this screen.

Table 90 Shaper Setup: Add/Edit

LABEL	DESCRIPTION
Enable	Select the check box to activate this shaper.
Outgoing Interface	Select the VPN2S's interface through which traffic in this shaper applies.
Rate Limit	Enter the average rate limit of traffic bursts for this shaper.

Table 90 Shaper Setup: Add/Edit

LABEL	DESCRIPTION
OK	Click this button to save your changes to the VPN2S.
Cancel	Click this button to exit this screen without saving.

12.7 Technical Reference

The following section contains additional technical information about the VPN2S features described in this chapter.

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 91 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)
---------------	-----------------

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

Automatic Priority Queue Assignment

If you enable QoS on the VPN2S, the VPN2S can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the VPN2S. On the VPN2S, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 92 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	

Table 92 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to b bytes which is also the bucket size, so the bucket can hold up to b tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the VPN2S stops transmitting until enough tokens are generated.
- If not enough tokens are available, the VPN2S treats the packet in either one of the following ways:
 - In traffic shaping:
 - Holds it in the queue until enough tokens are available in the bucket.
 - In traffic policing:
 - Drops it.
 - Transmits it but adds a DSCP mark. The VPN2S may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface's capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.
- If there are not enough tokens in the CBS bucket, the VPN2S checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

Two Rate Three Color Marker

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green. The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.
- If the PBS bucket has enough tokens, the VPN2S checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

CHAPTER 13

Network Management

13.1 Overview

This chapter describes the VPN2S's **Configuration > Network Management** screens. Use these screens to configure your VPN2S's SNMP.

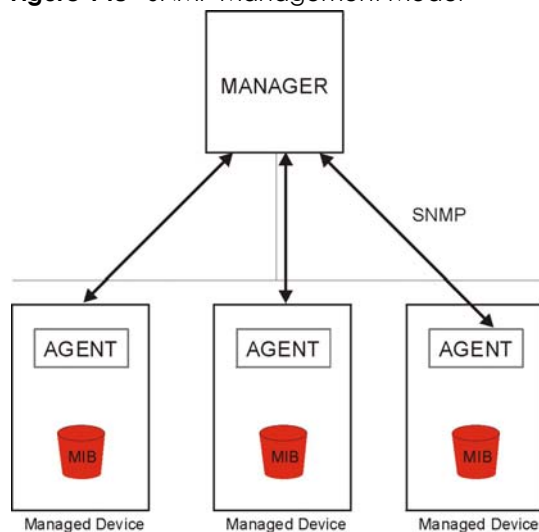
13.1.1 What You Can Do in This Chapter

Use the **SNMP** screen to configure the VPN2S's SNMP settings ([Section 13.2 on page 208](#))

13.2 The SNMP Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your VPN2S supports SNMP agent functionality, which allows a manager station to manage and monitor the VPN2S through the network. The VPN2S supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 148 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the VPN2S). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

Click **Configuration > Network Management > SNMP** to open the following screen. Use this screen to configure the VPN2S SNMP settings.

Figure 149 Configuration > Network Management > SNMP

The following table describes the fields in this screen.

Table 93 Configuration > Network Management > SNMP

LABEL	DESCRIPTION
SNMP Agent	Select the check box to allow a manager station to manage and monitor the VPN2S through the network via SNMP.
Get Community	Enter 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	Enter the Trap Community , which is the password sent with each trap to the SNMP manager.
System Name	Enter the system name of the VPN2S.
System Location	Specify the geographic location of the VPN2S.
System Contact	Enter the name of the person in charge of the VPN2S.
Trap Destination	Type the IP address of the station to send your SNMP traps to.

Table 93 Configuration > Network Management > SNMP (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the VPN2S.
Reset	Click Reset to restore your previously saved settings.

CHAPTER 14

System

14.1 Overview

This chapter describes the VPN2S's **Configuration > System** screens. Use these screens to configure your scheduler rules.

14.1.1 What You Can Do in This Chapter

Use the **Scheduler Rule** screen to view, add, or edit time schedule rules. ([Section 14.2 on page 212](#))

14.2 The Scheduler Rule Screen

Use the **Scheduler Rule** screen to define time periods and days during which the VPN2S performs scheduled rules of certain features (such as a Firewall). Click **Configuration > System > Scheduler Rule** to open this screen.

Figure 150 Configuration > System > Scheduler Rule

#	Rule Name	Days	Time	Description
---	-----------	------	------	-------------

The following table describes the fields in this screen.

Table 94 Configuration > System > Scheduler Rule

LABEL	DESCRIPTION
Add	Click this to create a new scheduler rule. Select a rule and click Add to create a new rule after the selected entry.
Edit	Double-click a scheduler rule or select it and click Edit to open a screen where you can modify the rule's settings.
Remove	To remove an existing scheduler rule, select it and click Remove . Note: You cannot delete a scheduler rule once it is applied to a certain feature.
#	This is the index number of the rule.
Rule Name	This is the name of the rule.
Days	This shows the day(s) on which this rule is enabled. Green days show when the rule is enabled, Gray days show when the rule is disabled.

Table 94 Configuration > System > Scheduler Rule

LABEL	DESCRIPTION
Time	This shows the period of time on which this rule is enabled.
Description	This shows the description of this rule.

14.2.1 Scheduler Rule: Add/Edit

Click **Add** in the **Scheduler Rule** screen, or select a rule and click **Edit** to open the following screen. Use this screen to configure a restricted access schedule.

Figure 151 Scheduler Rule: Add/Edit

Scheduler Rule - Add

Rule Name: !

Description:

Days: ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Time of Day Range: From: To: (hh:mm)

OK Cancel

The following table describes the labels in this screen.

Table 95 Scheduler Rule: Add/Edit

LABEL	DESCRIPTION
Rule Name	Enter a name (up to 31 printable characters English keyboard characters, not including spaces) for this schedule.
Description	Enter a description for this scheduler rule.
Days	Select the check boxes for the days that you want the VPN2S to perform this scheduler rule.
Time of Day Range	Enter the time period of each day, in 24-hour format, during which the rule will be enforced.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

CHAPTER 15

Log / Report

15.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the VPN2S log and then display the logs or have the VPN2S send them to an administrator (as e-mail) or to a syslog server.

15.1.1 What You Can Do in this Chapter

- Use the **Log Viewer** screen to see the system logs ([Section 15.2 on page 215](#)).
- Use the **Log Settings** screen to specify settings for recording log messages and alerts, e-mailing them, storing them on a connected USB storage device, and sending them to remote syslog servers([Section 15.3 on page 216](#)).

15.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Alerts and Logs

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. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 96 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.

Table 96 Syslog Severity Levels

CODE	SEVERITY
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.

15.2 The Log Viewer Screen

Use the Log viewer screen to see the system logs. Click **Configuration > Log / Report > Log Viewer** to open the **following** screen.

Figure 152 Configuration > Log / Report > Log Viewer

The screenshot shows the Log Viewer interface. At the top left is a 'Hide Filter' button. Below it are filter settings for Display (All Logs), Source IP, Source Interface (Any), Protocol (any), Priority (any), Destination IP, Destination Interface (Any), and Keyword. There are Search and Reset buttons. Below the filters are three action buttons: Email Log Now, Refresh, and Clear Log. The main area is a table with columns: #, Time, Priority, Category, Message, Source, Destination, and Note. The table contains five rows of log entries, all with 'error' priority and 'myZyxel...' category, stating 'Device registration has failed: Can't find token.' The bottom of the screen shows pagination: Page 1 of 103, Show 5 items, and Displaying 1 - 5 of 512.

The following table describes the fields in this screen.

Table 97 Configuration > Log / Report > Log Viewer

LABEL	DESCRIPTION
Show (Hide) Filter	Click this button to show or hide the filter settings. If the filter settings are hidden only Display filter is available. If the filter settings are shown, the Display , Priority , Source Address , Destination IP Address , Source Interface , Destination Interface , Protocol , Keyword , Search and Reset fields are available.
Display	Select the type of log message(s) you want to view. You can also view All Logs at one time, or you can view the Debug Log .
Priority	This displays when you show the filter. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: any , emerg , alert , crit , error , warn , notice , and info , from highest priority to lowest priority. This field is read-only if the Display field is set to Debug Log .
Source IP	This displays when you show the filter. Type the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.
Source Interface	This displays when you show the filter. Type the source interface of the incoming packet that generated the log message.

Table 97 Configuration > Log / Report > Log Viewer

LABEL	DESCRIPTION
Protocol	This displays when you show the filter. Select a service protocol whose log messages you would like to see.
Destination IP	This displays when you show the filter. Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Destination Interface	This displays when you show the filter. Type the interface of the destination of the incoming packet when the log message was generated.
Keyword	Type a keyword of the policy service available from VPN2S to search for a log.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.
Reset	Click this to return the filters to its original settings.
Email Log Now	Click this to send the log file(s) to the E-mail address you specify in the Log Settings screen.
Refresh	Click this to renew the log screen.
Clear Log	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Priority	This field displays the priority of the log message. It has the same range of values as the Priority field above.
Category	This field displays type of logs to display.
Messages	This field states the reason for the log.
Source	This field displays the source IP address and the port number in the event that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Note	This field displays any additional information about the log message.

15.3 Log Settings

The **Log Settings** screen controls log messages and alerts. A log message stores the information for viewing or regular e-mailing later, and an alert is e-mailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The **Log Settings Edit** screens control what information the VPN2S saves in each log. You can also specify which log messages to e-mail for the system log, and where and how often to e-mail them. These screens also set for which events to generate alerts and where to email the alerts.

To access this screen click **Configuration > Log / Report > Log Settings**.

Figure 153 Configuration > Log / Report > Log Settings

Log Settings

#	Status	Name	Log Format	Summary
1	<input type="radio"/> OFF	USB	Internal	USB Status: None
2	<input type="radio"/> OFF	System and Email	Internal	E-mail Server Email Mail Server: Mail Subject: Send From: Send Log to: Send Alert to: Schedule: Send log when full.
3	<input type="radio"/> OFF	Remote	VRPT/Syslog	Server Address: Log Facility: Local 1

Page of 1

 items
 Displaying 1 - 3 of 3

The following table describes the labels in this screen.

Table 98 Configuration > Log / Report > Log Settings

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify it.
Multiple Entries Turn On	Select one or more entries and click this to enable them.
Multiple Entries Turn Off	Select one or more entries and click this to disable them.
#	This field is a sequential value, and it is not associated with a specific log.
Status	This field displays whether the log setting is active or not. A green ON signifies that this log setting is active. A gray OFF signifies that this log setting is not active. Click the slide button to turn on or turn off the entry.
Name	This field displays the type of log setting entry (system log, logs stored on a USB storage device connected to the VPN2S, or one of the remote servers).
Log Format	This field displays the format of the log. Internal - system log; you can view the log on the View Log tab. VRPT/Syslog - Zyxel's Vantage Report, syslog-compatible format. CEF/Syslog - Common Event Format, syslog-compatible format.
Summary	This field is a summary of the settings for each log.
Apply	Click Apply to save your changes.
Reset	Click Reset to restore your previously saved settings.

15.3.1 Log on USB Settings: Edit

The **Edit Log on USB Settings** screen controls the detailed settings for saving logs to a connected USB storage device. Go to the **Log Settings** screen (see [Section 15.3 on page 216](#)), and double-click the **USB** setting or select it and click **Edit** to open the following screen.

Figure 154 Configuration > Log / Report > Log Settings > Edit (USB)

USB Log Setting - Edit

USB Log Setting
☒ Enable

Log Settings

Selection ▾

#	Log Category ↑	Selection ✗ ✓ ●
1	AAA Server	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
2	ADP	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
3	Bandwidth Management	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
4	Built-in Service	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
5	Connectivity Check	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
6	Default	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
7	DHCP	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
8	Firewall	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
9	Free Radius	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
10	IKE	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
11	Interface	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
12	IPsec	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
13	L2TP	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
14	Load Balance	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>

OK Cancel

The following table describes the labels in this screen.

Table 99 Configuration > Log / Report > Log Settings > Edit (USB)

LABEL	DESCRIPTION
USB Log Setting	
Enable	Select the check box to turn on the USB Log Setting.
Log Settings	
Selection	Use the Selection drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not send the remote server logs for any log category. enable normal logs (green check mark) - send the remote server log messages and alerts for all log categories. enable normal logs and debug logs (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific entry.
Log Category	This field displays each category of messages. The Default category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each Log Category (except All Logs; see below). Choices are: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - log regular information and alerts from this category enable normal logs and debug logs (yellow check mark) - log regular information, alerts, and debugging information from this category

Table 99 Configuration > Log / Report > Log Settings > Edit (USB)

LABEL	DESCRIPTION
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

15.3.2 System and Email: Edit

The **Log Settings Edit** screen controls the detailed settings for each log in the system log (which includes the e-mail profiles). Double-click a log setting or select it and click **Edit** to open the following screen.

Figure 155 Configuration > Log / Report > Log Settings > Edit (System and Email)

Email Server - Edit

Email Server

☒ Enable

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Server Port: ☒ TLS Security

Security:

Mail Subject:

Alert Mail Subject:

Send From: (Email Address)

Send Log to: (Email Address)

Send Alerts to: (Email Address)

Sending Log:

Day for Sending Log:

Time for Sending Log:

☒ SMTP Authentication

Username:

Password:

Retype to Confirm:

Log Consolidation

☒ Enable

Log Consolidation Interval (seconds): (10 - 600)

Log Settings

☒ System Log ☐ Email Server

#	Log Category ↑	System Log	Email Server
1	AAA Server	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>
2	ADP	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>

OK Cancel

The following table describes the labels in this screen.

Table 100 Configuration > Log / Report > Log Settings > Edit (System and Email)

LABEL	DESCRIPTION
E-mail Server	
Enable	Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the Log Settings section.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.

Table 100 Configuration > Log / Report > Log Settings > Edit (System and Email)

LABEL	DESCRIPTION
TLS Security	Select the check box if you want encrypted communications between the mail server and the VPN2S.
Security	Select SSL/TLS to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Select STARTTLS to upgrade a plain text connection to a secure connection using SSL/TLS.
Mail Subject	Type the subject line for the outgoing e-mail.
Alert Mail Subject	Type the subject line for the outgoing alert e-mail.
Send From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Send Log to	Type the e-mail address to which the outgoing e-mail is delivered.
Send Alerts to	Type the e-mail address to which alerts are delivered.
Sending Log	Select how often log information is e-mailed. Choices are: When Full, Hourly and When Full, Hourly and When Full, Daily and When Full , and Weekly and When Full .
Day for Sending Log	This field is available if the log is e-mailed weekly. Select the day of the week the log is emailed.
Time for Sending Log	This field is available if the log is e-mailed weekly, daily or hourly. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
Username	This box is effective when you select the SMTP Authentication check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the SMTP Authentication check box. Type the password to provide to the SMTP server when the log is e-mailed.
Retype to Confirm	Type the password again to make sure that you have entered is correctly.
Log Consolidation	
Enable	Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified Log Consolidation Interval . In the Log Viewer tab, the text "[count=x]", where x is the number of original log messages, is appended at the end of the Message field, when multiple log messages were aggregated.
Log Consolidation Interval (seconds)	Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text "[count=x]", where x is the number of original log messages, appended at the end of the Message field.
Log Settings	
System Log	Use the System Log drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. enable normal logs (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the VPN2S will e-mail logs to them. enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information for all categories. The VPN2S does not e-mail debugging information, even if this setting is selected.

Table 100 Configuration > Log / Report > Log Settings > Edit (System and Email)

LABEL	DESCRIPTION
E-mail Server	<p>Use the E-Mail Server drop-down list to change the settings for e-mailing logs to e-mail server for all log categories.</p> <p>Using the System Log drop-down list to disable all logs overrides your e-mail server settings.</p> <p>enable normal logs (green check mark) - e-mail log messages for all categories to e-mail server.</p> <p>enable alert logs (red exclamation point) - e-mail alerts for all categories to e-mail server.</p>
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the Log Viewer tab. The Default category includes debugging messages generated by open source software.
System Log	<p>Select which events you want to log by Log Category. There are three choices:</p> <p>disable all logs (red X) - do not log any information from this category</p> <p>enable normal logs (green check mark) - create log messages and alerts from this category</p> <p>enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information from this category; the VPN2S does not e-mail debugging information, however, even if this setting is selected.</p>
E-mail Server	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in E-Mail Server . The VPN2S does not e-mail debugging information, even if it is recorded in the System log.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

15.3.3 Remote Server Log Settings: Edit

The **Log Settings Edit** screen controls the detailed settings for each log in the remote server (syslog). Go to the **Log Settings** screen ([Section 15.3 on page 216](#)), select a remote server and click **Edit**.

Figure 156 Configuration > Log / Report > Log Settings > Edit (Remote)

Remote Server - Edit

Log Settings for Remote Server

☐ Enable

Log Format: VRPT/Syslog

Server Address: Server

Log Facility: Local 1

Log Settings

Selection

#	Log Category ↑	Selection
1	AAA Server	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
2	ADP	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
3	Bandwidth Management	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
4	Built-in Service	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
5	Connectivity Check	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
6	Default	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
7	DHCP	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
8	Firewall	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
9	Free Radius	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
10	IKE	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
11	Interface	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
12	IPsec	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
13	L2TP	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
14	Load Balance	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>

OK Cancel

The following table describes the labels in this screen.

Table 101 Configuration > Log / Report > Log Settings > Edit (Remote)

LABEL	DESCRIPTION
Log Settings for Remote Server	
Enable	Select this check box to send log information according to the information in this section. You specify what kinds of messages are included in log information in the Log Settings section.
Log Format	This field displays the format of the log information. It is read-only. VRPT/Syslog - Zyxel's Vantage Report, syslog-compatible format. CEF/Syslog - Common Event Format, syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Log Settings	

Table 101 Configuration > Log / Report > Log Settings > Edit (Remote)

LABEL	DESCRIPTION
Selection	<p>Use the Selection drop-down list to change the log settings for all of the log categories.</p> <p>disable all logs (red X) - do not send the remote server logs for any log category.</p> <p>enable normal logs (green check mark) - send the remote server log messages and alerts for all log categories.</p> <p>enable normal logs and debug logs (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.</p>
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the Log Viewer tab. The Default category includes debugging messages generated by open source software.
Selection	<p>Select what information you want to log from each Log Category (except All Logs; see below). Choices are:</p> <p>disable all logs (red X) - do not log any information from this category</p> <p>enable normal logs (green check mark) - log regular information and alerts from this category</p> <p>enable normal logs and debug logs (yellow check mark) - log regular information, alerts, and debugging information from this category</p>
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

CHAPTER 16

Service / License

16.1 Overview

Use the **Service / License** screen to display the status of your service registrations. To activate or extend a standard service subscription, purchase an iCard and enter the iCard's PIN number (license key) at myZyxel.com.

16.2 The License Screen

Click **Maintenance > Service / License** to open the following screen.

Figure 157 Maintenance > Service / License

Service / License

Service / License Status

#	Service	Status	Registration Type	Expiration Date	Count
1	Firmware Upgrade Status	Not Activat...			N/A

◀ ◀ Page 1 of 1 ▶ ▶ Show 20 items Displaying 1 - 1 of 1

Service / License Refresh

[Service License Refresh](#)

Note
Update the device license information from the myZyXEL.com server. If you want to activate a license, go to portal.myzyxel.com

The following table describes the labels on this screen.

Table 102 Maintenance > Service / License

LABEL	DESCRIPTION
Service / License Status	
#	This is the entry's position in the list.
Service	This lists the services that are available on the VPN2S.
Status	This field displays the status of your service registration. Not Activated displays if you have not successfully registered and activated the service. Expired displays if your subscription to the service has expired. Licensed displays if you have successfully registered the VPN2S and activated the service.
Registration Type	This field displays whether you applied for a trial application (Trial) or registered a service with your iCard's PIN number (Standard). This field is blank when a service is not activated. It always displays Standard for a default service.

Table 102 Maintenance > Service / License

LABEL	DESCRIPTION
Expiration Date	This field displays the date your service expires. This field is blank when a service does not expire.
Count	This field displays the maximum number of users that may connect to the VPN2S at the same time or how many managed APs the VPN2S can support with your current license. It displays 0 if this field does not apply to a service.
Service / License Refresh	
Service License Refresh	Click this button to renew service license information (such as the registration status and expiration day).

CHAPTER 17

Device Name

17.1 Overview

Use the **Device Name** screen to change the VPN2S's name in the network.

17.2 The Device Name Screen

Click **Maintenance > Device Name** to view the following screen.

Figure 158 Maintenance > Device Name

Device Name

General Settings

Host Name:

Domain Name:

Device Information

Serial Number: S170Y48011032

MAC Address: 5C:E2:8C:D3:7A:24

The following table describes the labels in this screen.

Table 103 Maintenance > Device Name

LABEL	DESCRIPTION
General Settings	
Host Name	Enter a descriptive name to identify your VPN2S. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes (-) underscores (_) and periods (.) are accepted.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long.
Device Information	
Serial Number	This displays the serial number of the VPN2S.
MAC Address	This displays the MAC address of the VPN2S.

Table 103 Maintenance > Device Name

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the VPN2S.
Reset	Click Reset to renew this screen.

CHAPTER 18

Host Name List

18.1 Overview

Use the **Host Name List** screen to add connected devices to the VPN2S's host list. Configure these devices to turn on with the **Wake on LAN** screen, see [Section 6.6 on page 84](#).

18.2 The Host Name List Screen

Click **Maintenance > Host Name List** to view the following screen. Use this screen to view and manage the clients that you added to the host list.

Figure 159 Maintenance > Host Name List

#	Description	MAC Address
1	test	00:A0:C5:01:23:86
2	172.16.3.254	00:00:5e:00:01:02

The following table describes the labels in this screen.

Table 104 Maintenance > Host Name List

LABEL	DESCRIPTION
Add	Click Add to create a new host.
Remove	Select a host and click Remove to delete it.
#	This is the index number of the host.
Description	This field displays a descriptive name for the host.
MAC Address	This field displays the host's MAC Address.

18.2.1 Add Host Name

Click **Add** to create a new host. The screen appears as shown.

Figure 160 Maintenance > Host Name List: Add

The following table describes the labels in this screen.

Table 105 Maintenance > Host Name List: Add

LABEL	DESCRIPTION
Refer To	<p>Select MAC Filter List if you want to select the devices that you added in the MAC Filter List.</p> <p>Select ARP Table to view the IPv4 or IPv6 devices that are connected to an VPN2S's port,</p> <p>Select Manual Type MAC to enter the MAC address of the host device manually. You can also enter a device's IP address and click Get to obtain its MAC address.</p>
Member List	Select a member device from the drop-down list.
Get MAC Address From IP	Enter the IP address of a device connected to the VPN2S, click Get and the VPN2S will automatically obtain the MAC address of the device with this IP address.
Description	Enter a description for this host.
MAC Address	Enter the host's MAC address, This field is configured automatically if you enter the device's IP address in the Get MAC Address From IP field and click Get .
OK	Click OK to save your changes back to the VPN2S.
Cancel	Click Cancel to exit this screen without saving.

CHAPTER 19

Date / Time

19.1 Overview

This chapter shows you how to configure system related settings, such as system time and the daylight saving setup.

19.2 The Date / Time Screen

To change your VPN2S's time and date, click **Maintenance > Date / Time**. The screen appears as shown. Use this screen to configure the VPN2S's time based on your local time zone.

Figure 161 Maintenance > Date / Time

Date / Time

Current Date / Time

Current Time: 03:30:05 (GMT-00:00) Greenwich Mean Time: Edinburgh, London
 Current Date: 2017-10-26

Time and Date Setup

Time Protocol: SNTP (RFC-1769)
 Time Server 1: pool.ntp.org
 Time Server 2: Other time.nist.gov
 Time Server 3: None
 Time Server 4: None
 Time Server 5: None

Time Zone Setup

Time Zone: (GMT-00:00) Greenwich Mean Time: Edinburgh, London

Daylight Saving Setup

☒ Enable

Start

Month: March
 Day: ☐ 12 ☒ Second Sunday
 Time: 02 : 00

End

Month: November
 Day: ☐ 1 ☒ First Sunday
 Time: 02 : 00

Apply Reset

The following table describes the labels in this screen.

Table 106 Maintenance > Date / Time

LABEL	DESCRIPTION
Current Date / Time	
Current Time	This field displays the time of your VPN2S. Each time you reload this page, the VPN2S synchronizes the time with the time server.
Current Date	This field displays the date of your VPN2S. Each time you reload this page, the VPN2S synchronizes the date with the time server.
Time and Date Setup	
Time Protocol	This displays the protocol currently used by your VPN2S to obtain date and time.
Time Server (1-5)	Select an NTP time server from the drop-down list box. Otherwise, select Other and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select None if you don't want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	

Table 106 Maintenance > Date / Time

LABEL	DESCRIPTION
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving Setup	Daylight Saving time 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.
Enable	Select Enable if you use Daylight Saving time.
Start	<p>Configure the day and time when Daylight Saving time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The Time field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to Second, Sunday, the month to March and the time to 02:00 in the Time field.</p> <p>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 set the day to Last, Sunday and the month to March. The time you select in the Time field depends on your time zone. In Germany for instance, you would select 02:00 in the Time field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End	<p>Configure the day and time when Daylight Saving time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The Time field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the first Sunday of November. 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 set the day to First, Sunday, the month to November and the time to 02:00 in the Time field.</p> <p>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 set the day to Last, Sunday, and the month to October. The time you select in the Time field depends on your time zone. In Germany for instance, you would select 02:00 in the Time field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click Apply to save your changes back to the VPN2S.
Reset	Click Reset to restore your previously saved settings.

CHAPTER 20

User Account

20.1 Overview

Use the **User Account** screen to manage user accounts, which includes configuring the username, password, retry times, and users timeout period.

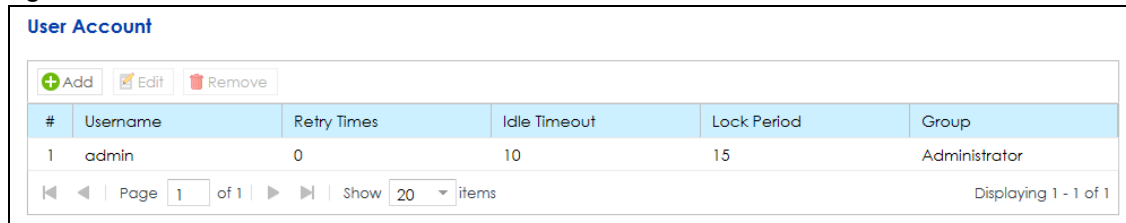
20.2 What You Can Do in this Chapter

Use the **User Account** screen to view and manage all user accounts ([Section 20.3 on page 233](#)).

20.3 The User Account Screen

Click **Maintenance > User Account** to open the following screen.

Figure 162 Maintenance > User Account



User Account					
+ Add Edit Remove					
#	Username	Retry Times	Idle Timeout	Lock Period	Group
1	admin	0	10	15	Administrator

Page 1 of 1
 Show 20 items
 Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 107 Maintenance > User Account

LABEL	DESCRIPTION
Add	Click this to configure a new user account.
Edit	Select an existing user account and click this to modify its settings.
Remove	Click this to delete a user account.
#	This is the index number of the user.
Username	This field displays the name of the user.
Retry Times	This field indicates how many times a user can re-enter his/her account information before the VPN2S locks the user out.
Idle Timeout	This field indicates the number of minutes that the system can idle before being logged out.

Table 107 Maintenance > User Account (continued)

LABEL	DESCRIPTION
Lock Period	This field indicates the number of minutes for the lockout period. A user cannot log into the VPN2S during the lockout period, even if he/she enters correct account information. An account will be locked if the account password is entered incorrectly too many times. You can specify how many times a password can be re-entered in the Retry Times field.
Group	This field displays the login account type of the user. Different login account types have different privilege levels. The web configurator screens and privileges vary depending on which account type you use to log in.

20.3.1 Users Account: Add/Edit

Use this screen to add or edit a users account. Click **Add** in the **User Account** screen or the select an existing user account and click **Edit**. The screen shown next appears.

Figure 163 Users Configuration: Add/Edit

The screenshot shows a web-based configuration window titled "User Account - Add". It contains several input fields with associated labels and help text:

- Username:** An empty text box with a red error icon to its right.
- Group:** A dropdown menu currently showing "Administrator".
- Password:** An empty text box with a red error icon to its right.
- Verify Password:** An empty text box with a red error icon to its right.
- Retry Times:** A text box containing "0", with help text "(0~5), 0 : Not limit".
- Idle Timeout:** A text box containing "5", with help text "Minute(s) (1~60)".
- Lock Period:** A text box containing "15", with help text "Minute(s) (15~90)".

At the bottom right of the window are "OK" and "Cancel" buttons.

The following table describes the labels in this screen.

Table 108 Users Configuration: Add/Edit

LABEL	DESCRIPTION
User Name	This field is read-only if you are editing the user account. Enter a descriptive name for the user account. The user name can be up to 15 alphanumeric characters (0-9, A-Z, a-z, -, _ with no spaces). With advanced account security enabled, the user names must be a minimum length of six characters and include both letters and numbers.
Group	This field is read-only if you are editing the user account. Select a type of login account. The web configurator screens and privileges vary depending on which account type you use to log in. Administrator accounts can configure the VPN2S while User accounts can only view some status information. Users logged in with either type of account can access the Internet.
Password	Specify the password associated to this account. The password can be 6 to 15 alphanumeric characters (0-9, A-Z, a-z, -, _ with no spaces), not containing the user name. It must contain both letters and numbers. The characters are displayed as asterisks (*) in this field.
Verify Password	Enter the exact same password that you just entered in the above field.

Table 108 Users Configuration: Add/Edit (continued)

LABEL	DESCRIPTION
Retry Times	<p>The VPN2S can lock a user out if you use a wrong user name or password to log in the VPN2S.</p> <p>Enter up to how many times a user can re-enter his/her account information before the VPN2S locks the user out.</p>
Idle Timeout	Enter the number of minutes that the system can idle before being logged out.
Lock Period	Enter the number of minutes for the lockout period. A user cannot log into the VPN2S during the lockout period, even if he/she enters correct account information.
OK	Click OK to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

CHAPTER 21

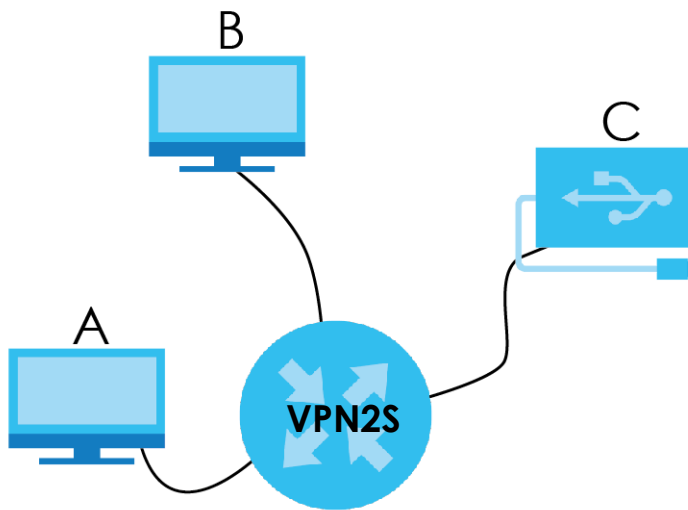
USB Storage

21.1 Overview

Use the USB Storage screen to share files on a USB memory stick or hard drive connected to your VPN2S with users on your network.

The following figure is an overview of the VPN2S's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the VPN2S.

Figure 164 File Sharing Overview



21.1.1 What You Need To Know

The following terms and concepts may help as you read this chapter.

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the VPN2S is given a folder, called a "share". If a USB hard drive connected to the VPN2S has more than one partition, then each partition will be allocated a share. You can also configure a "share" to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your VPN2S supports File Allocation Table (FAT) and FAT32.

Common Internet File System

The VPN2S uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the VPN2S. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

21.1.2 Before You Begin

Make sure the VPN2S is connected to your network and turned on.

- 1 Connect the USB device to one of the VPN2S's USB port. Make sure the VPN2S is connected to your network.
- 2 The VPN2S detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the VPN2S, see the troubleshooting for suggestions.

21.2 The USB Storage Screen

Use this screen to set up file sharing through the VPN2S. The VPN2S's LAN users can access the shared folder (or share) from the USB device inserted in the VPN2S. To access this screen click **Maintenance > USB Storage**.

Figure 165 Maintenance > USB Storage

USB Storage

Configuration

☒ Enable USB Storage Sharing

USB Information

#	Volume	Capacity	Used Space
1	usb1_sda1	3840 MB	1221 MB

Page 1 of 1 | Show 20 items | Displaying 1 - 1 of 1

Share Directory List

#	Status	Share Name	Share Path	Share Description	Allowed User
1	ON	Test	/mnt/usb1_sda1/Test		admin

Page 1 of 1 | Show 20 items | Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 109 Maintenance > USB Storage

LABEL	DESCRIPTION
Configuration	
Enable USB Storage Sharing	Click the check box to activate file sharing through the VPN2S.
USB Information	
This section is available only when a USB device is connected and detected by the VPN2S.	
#	This is the index number of the USB.
Volume	This is the volume name the VPN2S gives to an inserted USB device.
Capacity	This is the total available memory size (in megabytes) on the USB device.
Used Space	This is the memory size (in megabytes) already used on the USB device.
Share Directory List	
This table is available when you connect a USB to the VPN2S.	
Add	Click Add to create a new share.
Edit	Select a share and click Edit to modify it.
Remove	Select a share and click Remove to delete it.
Multiple Entries Turn On	Select one or more shares and click this to enable them.
Multiple Entries Turn Off	Select one or more shares and click this to disable them.
#	This is the index number of the share.
Status	<p>This field displays whether the share is active or not. A green ON button signifies that this share is active. A gray OFF button signifies that this share is not active.</p> <p>Click the slide button to turn on or turn off the share.</p>
Share Name	This field displays the name of the file you shared.
Share Path	This field displays the location in the USB of the file you shared.
Share Description	This field displays a description of the file you shared.
Allowed User	<p>This field displays which username(s) can access this share (Admin or any username added in the Maintenance > User Account screen). This field will be empty if the file is Public and anybody connected to the VPN2S can access it.</p>

Table 109 Maintenance > USB Storage

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the VPN2S.
Reset	Click Reset to restore your previously saved settings.

21.2.1 Add a USB Share

If a USB is connected to the USB port in the VPN2S you can view the **Share Directory List** table. Click **Add** to add a shared file to the VPN2S's network. The following screen will display.

Figure 166 USB Storage: Add

The following table describes the labels in this screen.

Table 110 USB Storage: Add

LABEL	DESCRIPTION
Volume	Select the name of the USB where the file you want to share is located.
Share Path	Select a file drop-down list to share.
Description	Enter a descriptive name for this file.
Access Level	Select Security if you want to specify the user names that can access this file. Select Public so anyone connected to the VPN2S can access this file.
Allowed User	This option displays when you select Security in Access Level . Select the check box of the user names you want to grant access to this file.
OK	Click OK to save your changes back to the VPN2S.
Cancel	Click Cancel to exit this screen without saving.

CHAPTER 22

Diagnostic

22.1 Overview

The **Diagnostic** screens display information to help you identify problems with the VPN2S.

22.1.1 What You Can Do in this Chapter

- The **Network Tools** screen lets you ping an IP address or trace the route packets take to a host ([Section 22.2 on page 240](#)).
- The **Packet Capture** screen to capture packets going through the VPN2S ([Section 22.3 on page 241](#)).

22.2 The Network Tools Screen

Use this screen to ping, traceroute, or nslookup an IP address. Click **Maintenance > Diagnostic > Network Tools** to open the screen shown next.

Figure 167 Maintenance > Diagnostic > Network Tools

The screenshot shows the 'Network Tools' screen. At the top, the title 'Network Tools' is in blue. Below it is a 'Result' section with a large text area containing '-info-'. The main section is titled 'Ping / TraceRoute Test' and contains three rows of controls: 'Bound Interface:' with a dropdown menu showing 'LAN (br0)', 'IPv4 / IPv6 Mode:' with radio buttons for 'IPv4' (selected) and 'IPv6', and 'Address / Domain Name:' with a text input field. To the right of the input field are two buttons: 'Ping' and 'TraceRoute'. Below this is a 'Name Service Lookup' section with 'Domain Name:' and a text input field, followed by an 'Nslookup' button.

The following table describes the fields in this screen.

Table 111 Maintenance > Diagnostic > Network Tools

LABEL	DESCRIPTION
Ping / TraceRoute Test	
Bound Interface	Choose a connected interface from the drop-down list (LAN, WAN) to perform the ping/tracer route test.
IPv4 / IPv6 Mode	Select IPv4 if you want to ping and IPv4 address. Select IPv6 if you want to ping an IPv6 address.
Address	Type the URL or IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection.
Ping	Click this to ping the IP address that you entered.
TraceRoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified computer.
Name Service lookup	
Domain name	Type a domain name in this field for the name service lookup.
Nslookup	Click this button to perform a DNS lookup on the IP address of a computer you enter.

22.3 The Packet Capture Screen

Use this screen to capture network traffic going through the VPN2S's interfaces. Studying these packet captures may help you identify network problems. Click **Maintenance > Diagnostic > Packet Capture** to open the packet capture screen.

Note: New capture files overwrite existing files of the same name. Change the File Suffix field's setting to avoid this.

Figure 168 Maintenance > Diagnostic > Packet Capture

Packet Capture

Status: USB not found

Interface: Any

File Name: .pcap

Setting

☒ Capture Until Stop

☐ Count Packet packet(s)

☐ Capture Duration seconds

☐ Capture File Size MB

Filter

☐ Host IP Source IP

☐ Host Port Port 0

Protocol Type

☐ ICMP

☐ IGMP

☐ ARP

☐ TCP

☐ UDP

The following table describes the labels in this screen.

Table 112 Maintenance > Diagnostic > Packet Capture

LABEL	DESCRIPTION
Status	<p>This displays USB not found if there is no USB detected in the port.</p> <p>This displays Ready when the USB is ready for capture.</p> <p>This displays Unmount USB to confirm you can remove your USB drive safely.</p> <p>This displays Capturing when the packet is in process of being captured.</p> <p>This displays Completed when the packet capture process is finished.</p>
Interface	Enabled interfaces appear under Interface . Select interfaces for which to capture packets.
File Name	Enter the label that identifies the file. The file name format is interface name-file suffix.pcap.
Setting	

Table 112 Maintenance > Diagnostic > Packet Capture

LABEL	DESCRIPTION
Capture Until Stop	<p>Click this check box to have the VPN2S capture packets according to the settings configured here.</p> <p>You can configure the VPN2S while a packet capture is in progress although you cannot modify the packet capture settings.</p> <p>The VPN2S's throughput or performance may be affected while a packet capture is in progress.</p> <p>After the VPN2S finishes the capture it saves a separate capture file for each selected interface. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space. Once the flash storage space is full, adding more packet captures will fail.</p>
Count Packet	Specify a maximum number of individual packet for each capture files. After a packet capture file reaches this number, the VPN2S won't start another capture.
Capture Duration	Set a time limit in seconds for the capture. The VPN2S stops the capture and generates the capture file when either this period of time has passed.
Capture File Size	Specify a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the VPN2S won't start another capture, but replaces the existing packet capture file.
Filter	
Host IP	Select a host IP address object for which to capture packets.
Host Port	Specify the port number or port range of traffic to capture.
Protocol Type	Select the protocol of traffic for which to capture packets.
Start Capture	After applying the desired filters click Start Capture for the VPN2S to capture network traffic on the interfaces.
Stop Capture	Click Stop Capture so the VPN2S ends the capture process.
Check Status	Click Check Status to refresh the USB status in Status .
Unmount USB	Click Unmount USB to remove your USB drive safely.

CHAPTER 23

Firmware Upgrade

23.1 Overview

This chapter explains how to upload new firmware package, to update USB 3G/4G dongle support, to your VPN2S. You can download new firmware releases and USB 3G/4G dongle support packages from your nearest Zyxel FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Only use firmware for your device's specific model. Refer to the label on the bottom of your VPN2S.

23.2 The Firmware Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the VPN2S while firmware upload is in progress!

Figure 169 Maintenance > Firmware Upgrade

Firmware Upgrade

Firmware Status

#	Status	Model	Version	Released Date	Upgrade
1	Running	VPN2S	V1.12[ABLN.0]b9	2018-05-19 3:55:51	

Cloud Firmware Information

Note
Register your device at portal.myzyxel.com to receive automatic notifications of firmware update.

Latest Version: [Check Now](#)

Released Date:

Release Note: [Release Notes Document](#)

Firmware Upgrade Service Status

Service Status: [Not Activated](#)

The following table describes the labels in this screen.

Table 113 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Firmware Status	
#	This is a sequential value, and it is not associated with the entry.
Status	This indicates whether the firmware is Running , or not running but already uploaded to the VPN2S and is on Standby . It displays N/A if there is no firmware uploaded to that system space.
Model	This shows the model name of this Zyxel device.
Version	This is the VPN2S's present firmware version.
Released Date	This shows the date the present firmware was released.
Upgrade	Click the Upgrade icon to open a new screen, where you Browse the location of the .bin file you want to Upload to the VPN2S. Remember that you must decompress compressed (.zip) files before you can upload them. The upgrade process may take up to two minutes. Note: Do not turn off the VPN2S while firmware upgrade is in progress.
Cloud Firmware Information	
Latest Version	This is the firmware's latest version. Click Check Now for the VPN2S to check for new firmware releases.
Released Date	This is the date that the latest version of the firmware was created.
Release Note	This is a comment associated with the latest firmware.
Firmware Upgrade License Status	
Service / License Status	This is the current status of the license.

After you see the firmware updating screen, wait two minutes before logging into the VPN2S again.

Figure 170 Firmware Uploading

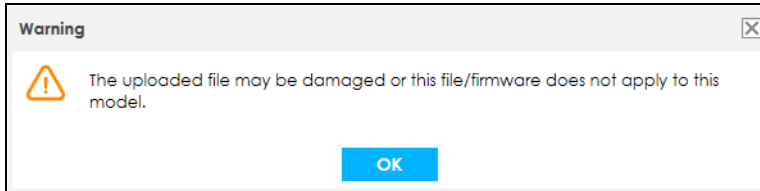


The VPN2S automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 171 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 172 Error Message

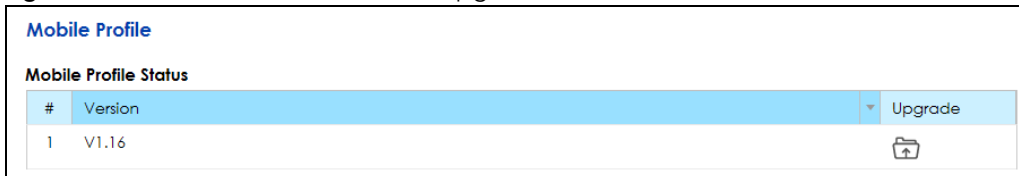
23.3 The Mobile Profile Screen

Use this screen to update the mobile profile on the VPN2S. The mobile profile is a WWAN package that contains configuration to identify and activate the supported 3G/4G USB dongles.

Note: To update the supported 3G/4G USB dongle list, download the latest mobile profile from the ZyXEL website and upload it to the VPN2S.

Click **Maintenance > Firmware Upgrade > Mobile Profile** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes.

Do NOT turn off the VPN2S while profile upload is in progress!

Figure 173 Maintenance > Firmware Upgrade > Mobile Profile

The following table describes the labels in this screen.

Table 114 Maintenance > Firmware Upgrade > Mobile Profile

LABEL	DESCRIPTION
Mobile Profile Status	
#	This is a sequential value, and it is not associated with the entry.

Table 114 Maintenance > Firmware Upgrade > Mobile Profile

LABEL	DESCRIPTION
Version	This is the version of the VPN2S's present mobile profile.
Upgrade	<p>Click the Upgrade icon to open a new screen, where you Browse the location of the file you want to Upload to the VPN2S.</p> <p>Note: Do not turn off the VPN2S while profile upgrade is in progress.</p>

CHAPTER 24

Backup / Restore

24.1 Overview

The **Backup / Restore** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

24.2 The Backup / Restore Screen

Click **Maintenance > Backup / Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 174 Maintenance > Backup / Restore

Backup / Restore

Backup Configuration
Click Backup to save the current configuration of your system to your computer.

[Backup](#)

Restore Configuration
You can save the current settings in a backup file on your computer, or restore previous settings from a backup file. You can also reset the device back to its factory default state.

File Path: [Browse](#) [Upload](#)

Back to Factory Default Settings
Click Reset to clear all user-entered configuration information and return to factory default settings. After resetting, the

- LAN IP address will be 192.168.1.1
- DHCP will be reset to default setting

[Reset](#)

Backup Configuration

Backup Configuration allows you to back up (save) the VPN2S's current configuration to a file on your computer. Once your VPN2S 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.

Click **Backup** to save the VPN2S's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your VPN2S.

Table 115 Restore Configuration

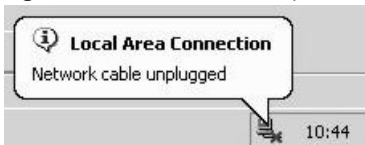
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Choose File to find it.
Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.

Do not turn off the VPN2S while configuration file upload is in progress.

After the VPN2S configuration has been restored successfully, the login screen appears. Login again to restart the VPN2S.

The VPN2S automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

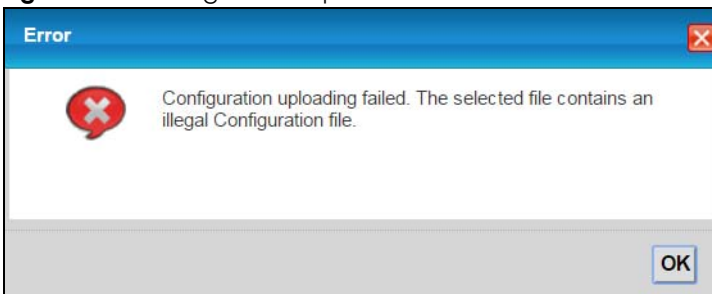
Figure 175 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Backup / Restore** screen.

Figure 176 Configuration Upload Error



Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the VPN2S to its factory defaults. The following warning screen appears.

CHAPTER 25

Language

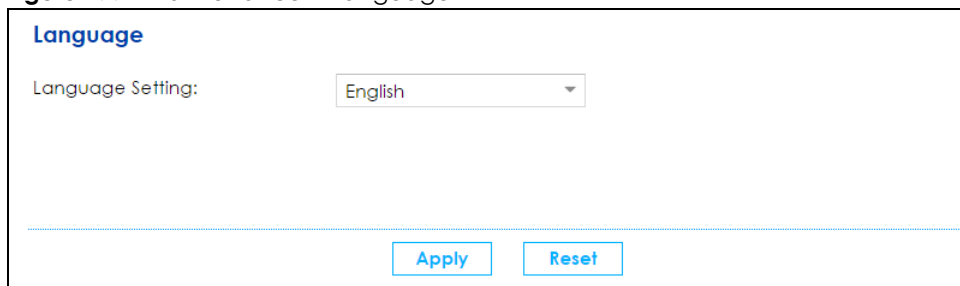
25.1 Overview

Use the **Language** screen to change the language in which the screen are displayed in the web configurator.

25.2 The Language Screen

Click **Maintenance > Language** to open the following screen.

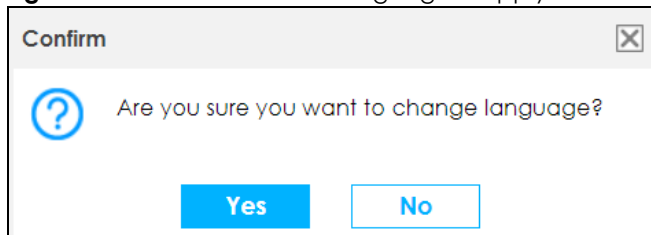
Figure 177 Maintenance > Language



The screenshot shows the 'Language' screen. At the top, the title 'Language' is in blue. Below it, the text 'Language Setting:' is followed by a dropdown menu currently set to 'English'. At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

Select the language of your preference and click **Apply** to save your changes to the VPN2S. The following screen will display. After clicking **Yes** the VPN2S will automatically change all the screens to the selected language.

Figure 178 Maintenance > Language > Apply



The screenshot shows a 'Confirm' dialog box. It has a title bar with a close button (X). Inside, there is a question mark icon and the text 'Are you sure you want to change language?'. At the bottom, there are two buttons: 'Yes' and 'No'.

CHAPTER 26

Restart / Shutdown

26.1 Overview

Use this screen to restart the device. Restart is different to reset; restart returns the device to its default configuration.

26.2 The Restart / Shutdown Screen

System restart allows you to reboot the VPN2S remotely without turning the power off. You may need to do this if the VPN2S hangs, for example.

Click **Maintenance > Restart / Shutdown**. Click **Restart** to have the VPN2S reboot. This does not affect the VPN2S's configuration. If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot.

Figure 179 Maintenance > Restart / Shutdown



CHAPTER 27

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [VPN2S Access and Login](#)
- [Internet Access](#)
- [USB Device Connection](#)

27.1 Power, Hardware Connections, and LEDs

[The VPN2S does not turn on. None of the LEDs turn on.](#)

- 1 Make sure the VPN2S is turned on.
- 2 Make sure you are using the power adaptor or cord included with the VPN2S.
- 3 Make sure the power adaptor or cord is connected to the VPN2S and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the VPN2S off and on.
- 5 If the problem continues, contact the vendor.

[One of the LEDs does not behave as expected.](#)

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.5 on page 15](#).
- 2 Check the hardware connections.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the VPN2S off and on.
- 5 If the problem continues, contact the vendor.

27.2 VPN2S Access and Login

I forgot the IP address for the VPN2S.

- 1 The default LAN IP address is 192.168.1.1.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the VPN2S by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the VPN2S (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 1.6 on page 16](#).

I forgot the password.

- 1 The default admin password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 1.6 on page 16](#).

I cannot see or access the **Login** screen in the web configurator.

- 1 Make sure you are using the correct IP address.
 - The default IP address is [192.168.1.1](#).
 - If you changed the IP address ([Section 6.2 on page 75](#)), use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the VPN2S](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 1.5 on page 15](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
- 4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Configuration > Firewall / Security > Device Service**).
- 5 Reset the device to its factory defaults, and try to access the VPN2S with the default IP address. See [Section 1.6 on page 16](#).
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the VPN2S using another service, such as Telnet. If you can access the VPN2S, check the remote management settings and firewall rules to find out why the VPN2S does not respond to HTTP.

I can see the [Login](#) screen, but I cannot log in to the VPN2S.

- 1 Make sure you have entered the password correctly. The default admin password is **1234**. The field is case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using Telnet to access the VPN2S. Log out of the VPN2S in the other session, or ask the person who is logged in to log out.
- 3 Turn the VPN2S off and on.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 27.1 on page 252](#).

I cannot Telnet to the VPN2S.

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

27.3 Internet Access

I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and [Section 1.5 on page 15](#).
- 2 Make sure you entered your ISP account information correctly in the **Configuration > WAN / Internet > WAN Setup** or **Mobile** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.

- 3 Disconnect all the cables from your device and reconnect them.
- 4 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the VPN2S), but my Internet connection is not available anymore.

- 1 Your session with the VPN2S may have expired. Try logging into the VPN2S again.
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and [Section 1.5 on page 15](#).
- 3 Turn the VPN2S off and on.
- 4 If the problem continues, contact your ISP.

27.4 USB Device Connection

The VPN2S fails to detect my USB device.

- 1 Disconnect the USB device.
- 2 Reboot the VPN2S.
- 3 If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
- 4 Re-connect your USB device to the VPN2S.

APPENDIX A

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See <http://www.zyxel.com/homepage.shtml> and also http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml for the latest information.

Please have the following information ready when you contact an office.

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)

Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com>

Asia

China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

India

- Zyxel Technology India Pvt Ltd
- <http://www.zyxel.in>

Kazakhstan

- Zyxel Kazakhstan
- <http://www.zyxel.kz>

Korea

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- Zyxel Philippines
- <http://www.zyxel.com.ph>

Singapore

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com/tw/zh/>

Thailand

- Zyxel Thailand Co., Ltd
- <http://www.zyxel.co.th>

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

Europe

Austria

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

Belarus

- Zyxel BY
- <http://www.zyxel.by>

Belgium

- Zyxel Communications B.V.
- <http://www.zyxel.com/be/nl/>
- <http://www.zyxel.com/be/fr/>

Bulgaria

- Zyxel България
- <http://www.zyxel.com/bg/bg/>

Czech Republic

- Zyxel Communications Czech s.r.o
- <http://www.zyxel.cz>

Denmark

- Zyxel Communications A/S
- <http://www.zyxel.dk>

Estonia

- Zyxel Estonia
- <http://www.zyxel.com/ee/et/>

Finland

- Zyxel Communications
- <http://www.zyxel.fi>

France

- Zyxel France
- <http://www.zyxel.fr>

Germany

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

Hungary

- Zyxel Hungary & SEE
- <http://www.zyxel.hu>

Italy

- Zyxel Communications Italy
- <http://www.zyxel.it/>

Latvia

- Zyxel Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

Lithuania

- Zyxel Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

Netherlands

- Zyxel Benelux
- <http://www.zyxel.nl>

Norway

- Zyxel Communications
- <http://www.zyxel.no>

Poland

- Zyxel Communications Poland
- <http://www.zyxel.pl>

Romania

- Zyxel Romania
- <http://www.zyxel.com/ro/ro>

Russia

- Zyxel Russia
- <http://www.zyxel.ru>

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

Spain

- Zyxel Communications ES Ltd
- <http://www.zyxel.es>

Sweden

- Zyxel Communications
- <http://www.zyxel.se>

Switzerland

- Studerus AG

- <http://www.zyxel.ch/>

Turkey

- Zyxel Turkey A.S.
- <http://www.zyxel.com.tr>

UK

- Zyxel Communications UK Ltd.
- <http://www.zyxel.co.uk>

Ukraine

- Zyxel Ukraine
- <http://www.ua.zyxel.com>

Latin America

Argentina

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Brazil

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

Ecuador

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Middle East

Israel

- Zyxel Communication Corporation
- <http://il.zyxel.com/homepage.shtml>

Middle East

- Zyxel Communication Corporation
- <http://www.zyxel.com/me/en/>

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- <http://www.zyxel.com/us/en/>

Oceania

Australia

- Zyxel Communications Corporation
- <http://www.zyxel.com/au/en/>

Africa

South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

APPENDIX B

Legal Information

Copyright

Copyright © 2018 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

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.

Regulatory Notice and Statement

UNITED STATES of AMERICA



The following information applies if you use the product within USA area.

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference, and
 - (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
 - Reorient or relocate the receiving antenna
 - Increase the separation between the devices
 - Connect the equipment to an outlet other than the receiver's
 - Consult a dealer or an experienced radio/TV technician for assistance

CANADA

The following information applies if you use the product within Canada area

Industry Canada ICES statement

CAN ICES-3 (B)/NMB-3(B)

EUROPEAN UNION



The following information applies if you use the product within the European Union.

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
 - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
 - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Environment Statement**ErP (Energy-related Products)**

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣





安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸
 - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
 - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝、使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Trademarks

ZyNOS (Zyxel Network Operating System) and ZON (Zyxel One Network) are registered trademarks of Zyxel Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those licenses, please contact support@zyxel.com.tw to get it.

Index

A

- activation
 - SIP ALG [121](#)
- address groups
 - and content filtering [146](#)
- address objects
 - and content filtering [146](#)
- administrator password [19](#)
- AH [183](#)
- algorithms [183](#)
- applications
 - Internet access [14](#)
- applications, NAT [123](#)
- and schedules [146](#)
- and user groups [146](#)
- and users [146](#)
- by category [146](#), [147](#)
- default policy [146](#)
- policies [146](#)
- copyright [262](#)
- CoS [204](#)
- CoS technologies [191](#)
- customer support [256](#)

B

- backup
 - configuration [248](#)
- blinking LEDs [16](#)
- broadcast [71](#)

C

- Canonical Format Indicator See CFI
- certifications [263](#)
 - viewing [265](#)
- CFI [71](#)
- client list [82](#)
- configuration
 - backup [248](#)
 - reset [249](#)
 - restoring [249](#)
 - static route [107](#), [234](#)
- contact information [256](#)
- content filtering [146](#)
 - and address groups [146](#)
 - and address objects [146](#)

D

- Dashboard [43](#)
- DDoS [127](#)
- default server address [120](#)
- Denials of Service, see DoS
- DH [189](#)
- DHCP [74](#), [93](#)
- Differentiated Services, see DiffServ [204](#)
- Diffie-Hellman key groups [189](#)
- DiffServ [204](#)
 - marking rule [205](#)
- disclaimer [262](#)
- DMZ [119](#)
- DNS [74](#), [94](#)
- DNS server address assignment [72](#)
- Domain Name [124](#)
- Domain Name System, see DNS
- Domain Name System. See DNS.
- DoS [127](#)
- DS field [205](#)
- DS, dee differentiated services
- DSCP [204](#)
- Dynamic Host Configuration Protocol, see DHCP

E

ECHO [124](#)
Encapsulation [70](#)
 MER [70](#)
 PPP over Ethernet [70](#)
encapsulation [47](#), [184](#)
ESP [183](#)

F

file sharing [15](#)
Finger [124](#)
firewalls [126](#)
 add protocols [136](#)
 DDoS [127](#)
 DoS [127](#)
 LAND attack [127](#)
 Ping of Death [127](#)
 SYN attack [127](#)
firmware [244](#)
forwarding ports [111](#)
FTP [124](#)

H

HTTP [124](#)

I

ID type and content [188](#)
IEEE 802.1Q [71](#)
IGA [122](#)
IGMP [71](#)
 version [71](#)
IKE phases [185](#)
ILA [122](#)
Inside Global Address, see IGA
inside header [185](#)
Inside Local Address, see ILA
Internet

 wizard setup [26](#)
Internet access [14](#)
 wizard setup [26](#)
Internet Key Exchange [185](#)
Internet Protocol Security. See IPsec.
Internet Protocol version 6 [48](#)
Internet Service Provider, see ISP
IP address [74](#), [94](#)
 ping [240](#)
 private [95](#)
 WAN [47](#)
IP Address Assignment [70](#)
IP alias
 NAT applications [124](#)
IPsec [154](#)
 algorithms [183](#)
 architecture [183](#)
 NAT [186](#)
IPsec. See also VPN.
IPv6 [48](#)
 addressing [48](#), [72](#)
 prefix [48](#), [72](#)
 prefix delegation [49](#)
 prefix length [48](#), [72](#)
ISP [47](#)

L

L2TP VPN [156](#)
LAN [73](#)
 client list [82](#)
 DHCP [74](#), [93](#)
 DNS [74](#), [94](#)
 IP address [74](#), [76](#), [94](#)
 subnet mask [74](#), [94](#)
LAND attack [127](#)
Layer 2 Tunneling Protocol Virtual Private Network, see L2TP VPN [156](#)
login [18](#)
 passwords [18](#), [19](#)
logs [214](#)

M

Management Information Base (MIB) [209](#)
managing the device
 good habits [13](#)
MTU (Multi-Tenant Unit) [71](#)
multicast [71](#)

N

NAT [110, 112, 122](#)
 applications [123](#)
 IP alias [124](#)
 example [123](#)
 global [122](#)
 IGA [122](#)
 ILA [122](#)
 inside [122](#)
 IPsec [186](#)
 local [122](#)
 outside [122](#)
 port forwarding [111](#)
 port number [124](#)
 services [124](#)
 SIP ALG [121](#)
 activation [121](#)
 traversal [187](#)
NAT example [125](#)
negotiation mode [186](#)
Network Address Translation, see NAT
NNTP [124](#)

O

outside header [184](#)

P

passwords [18, 19](#)
Per-Hop Behavior, see PHB [205](#)
PHB [205](#)
Ping of Death [127](#)

Point-to-Point Tunneling Protocol [124](#)
POP3 [124](#)
port forwarding [111](#)
ports [16](#)
PPP over Ethernet, see PPPoE
PPPoE [47, 70](#)
 Benefits [70](#)
PPTP [124](#)
prefix delegation [49](#)
pre-shared key [189](#)
private IP address [95](#)
product registration [265](#)
protocol [47](#)

Q

QoS [190, 204](#)
 marking [191](#)
 setup [190](#)
 tagging [191](#)
 versus CoS [190](#)
Quality of Service, see QoS

R

registration
 product [265](#)
reset [16, 249](#)
restart [251](#)
restoring configuration [249](#)
RFC 1058. See RIP.
RFC 1389. See RIP.
RFC 3164 [214](#)
RIP [108](#)
router features [14](#)
Routing Information Protocol. See RIP

S

schedules
 and content filtering [146](#)

security associations. See VPN.

Security Parameter Index, see SPI

Services [124](#)

setup

static route [107, 234](#)

Simple Network Management Protocol, see SNMP

Single Rate Three Color Marker, see srTCM

SIP ALG [121](#)

activation [121](#)

SMTP [124](#)

SNMP [124, 208, 209](#)

agents [208](#)

Get [209](#)

GetNext [209](#)

Manager [208](#)

managers [208](#)

MIB [209](#)

Set [209](#)

Trap [209](#)

versions [208](#)

SNMP trap [124](#)

SPI [127](#)

srTCM [207](#)

static route [96](#)

configuration [107, 234](#)

example [96](#)

static VLAN

status [43](#)

status indicators [16](#)

subnet mask [74, 94](#)

SYN attack [127](#)

syslog

protocol [214](#)

severity levels [214](#)

system

firmware [244](#)

passwords [18, 19](#)

reset [16](#)

status [43](#)

T

Tag Control Information See TCI

Tag Protocol Identifier See TPID

TCI

The [47](#)

TPID [71](#)

trademarks [265](#)

transport mode [184](#)

trTCM [207](#)

tunnel mode [184](#)

Two Rate Three Color Marker, see trTCM

U

unicast [71](#)

upgrading firmware [244](#)

USB features [15](#)

user groups

and content filtering [146](#)

users

and content filtering [146](#)

V

VID

Virtual Local Area Network See VLAN

Virtual Private Network. See VPN.

VLAN [71](#)

Introduction [71](#)

number of possible VIDs

priority frame

static

VLAN ID [71](#)

VLAN Identifier See VID

VLAN tag [71](#)

VPN [154](#)

established in two phases [155](#)

IPsec [154](#)

local network [155](#)

remote IPsec router [155](#)

remote network [155](#)

security associations (SA) [155](#)

VPN. See also IKE SA, IPsec SA.

W

WAN

Wide Area Network, see WAN [46](#)

warranty [265](#)

note [265](#)

web configurator [18](#)

login [18](#)

passwords [18, 19](#)

wizard setup

Internet [26](#)

Z

Zone Control [135](#)