ZyWALL 5

Internet Security Appliance

Quick Start Guide

Version 4.02
Edition 1
12/2006

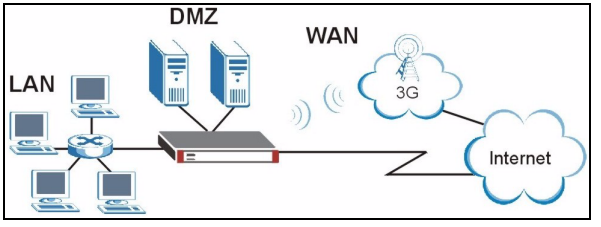
Table of Contents

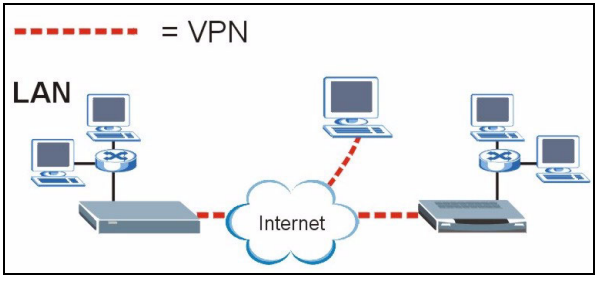
Overview

The ZyWALL 5 is a firewall with VPN, bandwidth management, content filtering, anti-spam, anti-virus, IDP (Intrusion Detection and Protection) and many other features. You can use it as a transparent firewall and not reconfigure your network nor configure the ZyWALL's routing features. When the ZyWALL is in router mode, you can also insert a 3G wireless card to add a second WAN. The ZyWALL increases network security by adding the option to change port roles from LAN to DMZ for use with publicly accessible servers. This guide covers the initial connections and configuration needed to start using the ZyWALL in your network.

See the User's Guide for more information on all features.

You may need your Internet access information.



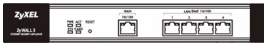


This guide is divided into the following sections.

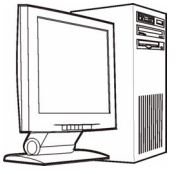
1 Hardware Connections

You need the following.

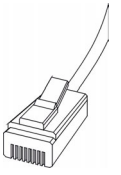
ZyWALL



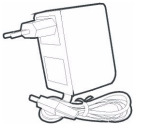
Computer



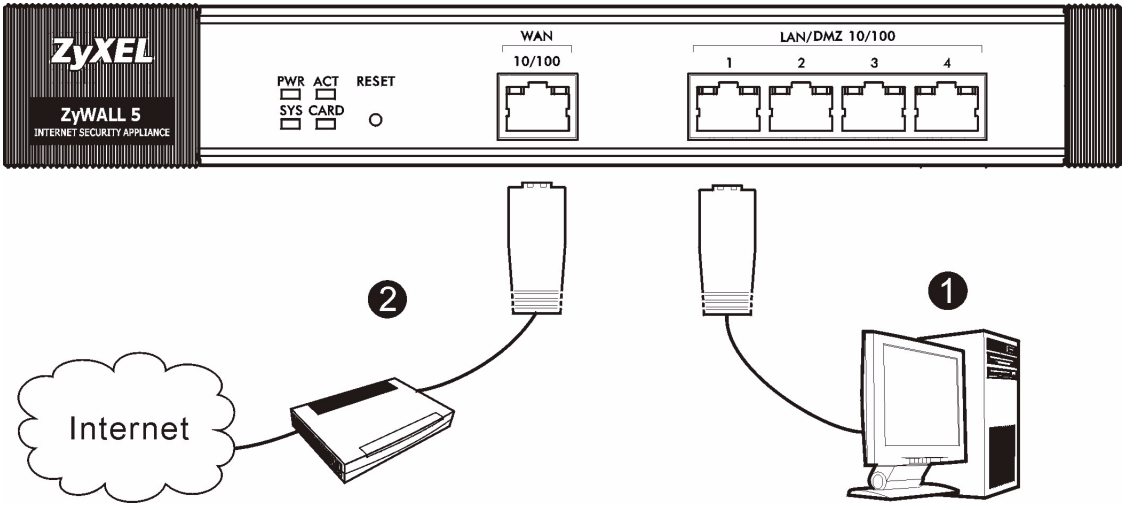
Ethernet Cables



Power Adaptor

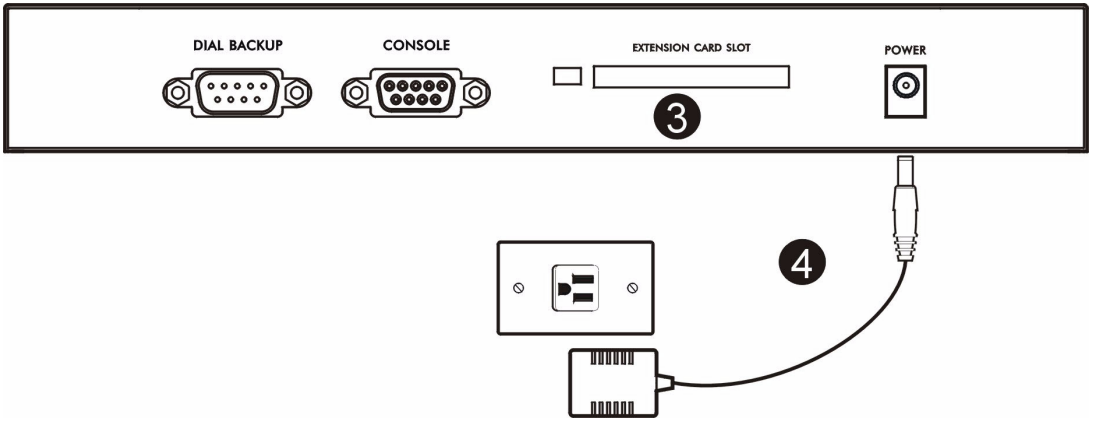


Do the following to make hardware connections for initial setup.



1 Use an Ethernet cable to connect the **LAN/DMZ** port to a computer. If you configure these ports as DMZ ports in the **LAN** or **DMZ** screen through the web configurator, you can also use Ethernet cables to connect public servers (web, e-mail, FTP, etc.) to the **LAN/DMZ** ports.

2 Use another Ethernet cable to connect the **WAN** port to an Ethernet jack with Internet access.



3 Insert the ZyWALL Turbo extension card to use the anti-virus and IDP features or insert a wireless LAN card to use the wireless LAN feature. You can optionally insert a 3G wireless card to access the Internet wirelessly via a 3G network. See the ZyWALL Turbo Card guide for more information about the extension card. See the user's guide about installing a wireless LAN card. At the time of writing, you can only use the Sierra AC850/860 3G wireless card in the ZyWALL.

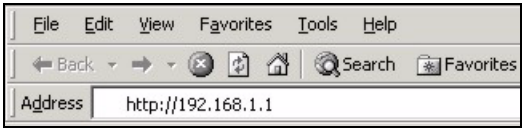
4 Use the included power adaptor to connect the power socket (on the rear panel) to a power outlet.

5 Look at the front panel. The **PWR** LED turns on. The **SYS** LED blinks while performing system testing and then stays on if the testing is successful. The **ACT**, **CARD**, **LAN/DMZ** and **WAN** LEDs turn on and stay on if the corresponding connections are properly made.

2 Accessing the Web Configurator

Use this section to configure the **WAN 1** interface for Internet access.

1 Launch your web browser. Enter **192.168.1.1** (the ZyWALL's default IP address) as the address. If the login screen does not display, see Section 9.1 to set your computer's IP address.



2 Click **Login** (the default password 1234 is already entered).

3 Change the login password by entering a new password and clicking **Apply**.

4 Click **Apply** to replace the ZyWALL's default digital certificate.

5 The **HOME** screen opens.

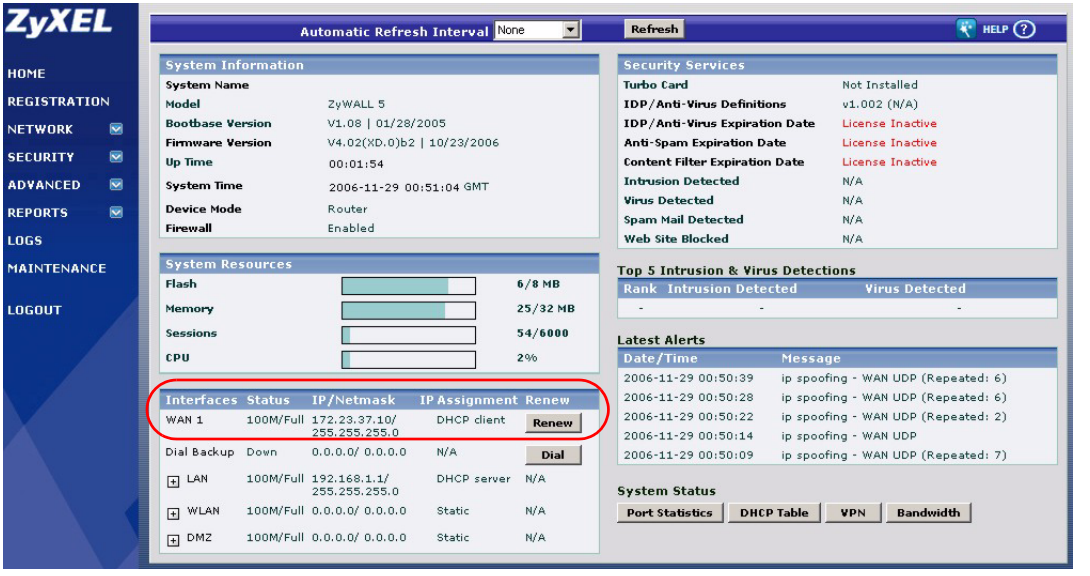
The ZyWALL is in router mode by default. Continue to the next step if you want to use routing features such as NAT, DHCP and VPN.

Go to Section 3 if you prefer to use the ZyWALL as a transparent firewall.

6 Check the network status table. If the **WAN 1** status is *not* **Down** and there is an IP address, go to Section 5.

If the **WAN 1** status is **Down** (or there is not an IP address), click the **Wizard** icon and use Section 4 to configure **WAN 1**.

Use the **NETWORK WAN** screens if you need to configure **WAN 2**. You can also configure load balancing between the WAN connections.

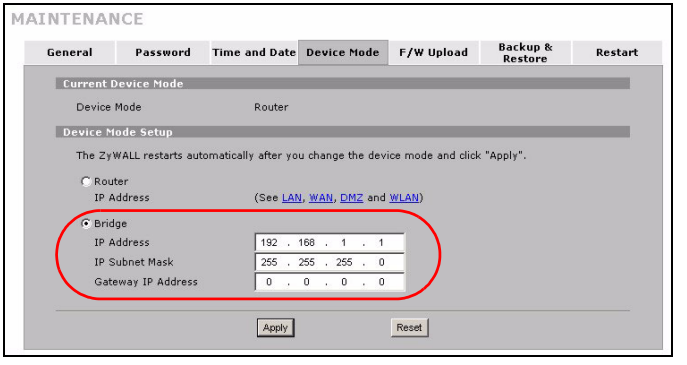


3 Bridge Mode

When you set the ZyWALL to bridge mode, it functions as a transparent firewall. Do the following to set the ZyWALL to bridge mode.

1. Click **MAINTENANCE** in the navigation panel and then **Device Mode**.
2. Select **Bridge** and configure a (static) IP address subnet mask and gateway IP address for the ZyWALL's **LAN**, **WAN**, **DMZ** and **WLAN** interfaces.
3. Click **Apply**. The ZyWALL restarts.

Skip to Section 5 if you have servers that you need to be accessible from the WAN.



4 Internet Access Setup and Product Registration

1. Click the **Wizard** icon ( ) in the **HOME** screen and then the **Internet Access Setup** link to open the Internet access wizard.

Enter the Internet access information exactly as given to you.

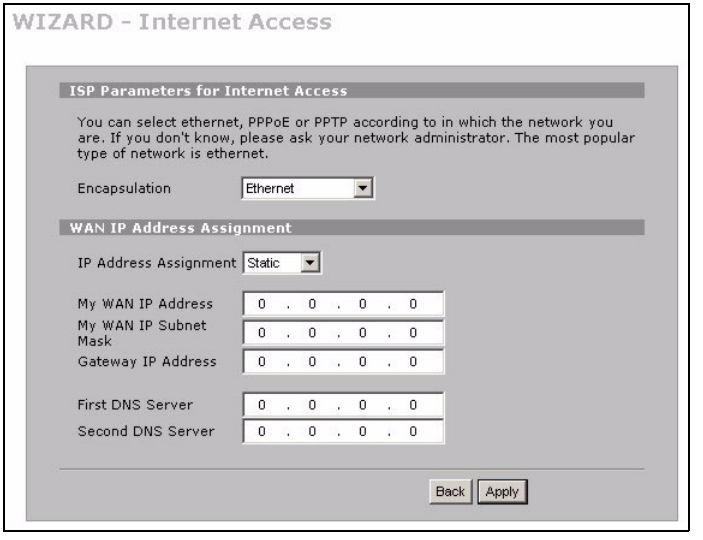
If you were given an IP address to use, select **Static** in the **IP Address Assignment** drop-down list box and enter the information provided.

The fields vary depending on what you select in the **Encapsulation** field. Fill them in with the information provided by the ISP or network administrator.

Click **Apply** when you are done.

- **Ethernet Encapsulation**

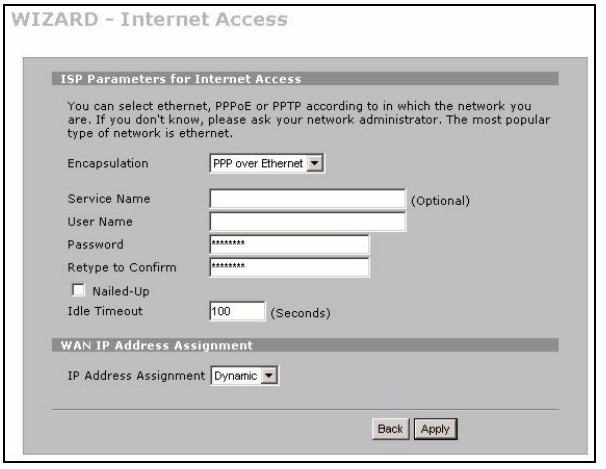
Configure a Roadrunner service in the **NETWORK WAN** screens (use the **WAN** tab).

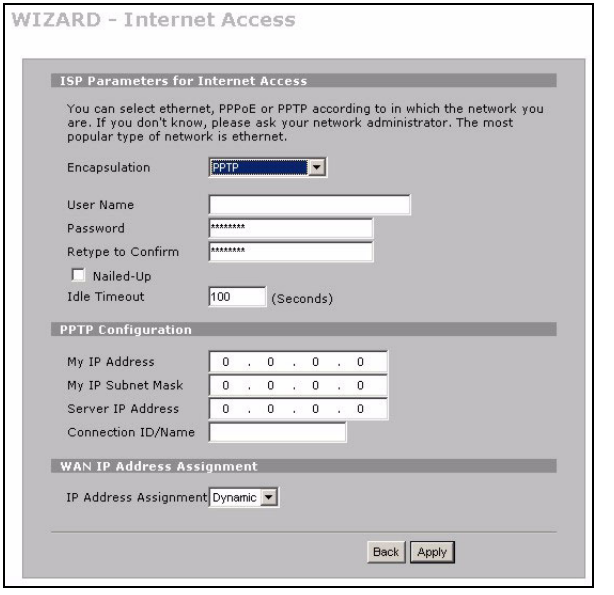


- **PPP over Ethernet or PPTP Encapsulation**

Select **Nailed-Up** when you want your connection up all the time (this could be expensive if your ISP bills you for Internet usage time instead of a flat monthly fee).

To not have the connection up all the time, specify an idle time-out period (in seconds) in **Idle Timeout**.



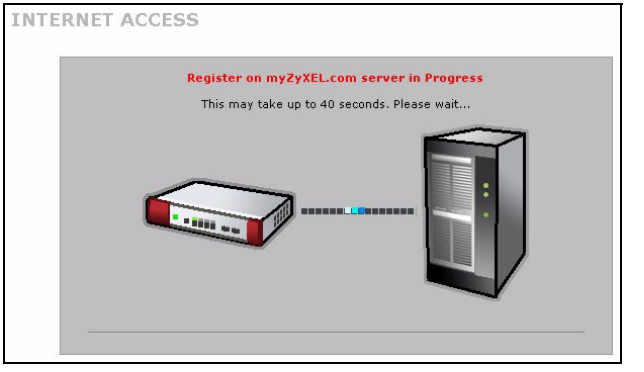


2 Click **Next** to display the screen where you can register your ZyWALL with myZyXEL.com (ZyXEL's online services center) and activate the free content filtering, anti-spam, anti-virus and IDP trial applications. Otherwise, click **Skip** and then **Close** to complete Internet access setup.

Make sure you have installed the ZyWALL Turbo Card before you activate the IDP and anti-virus subscription services.
Turn the ZyWALL off before you install or remove the ZyWALL Turbo Card.

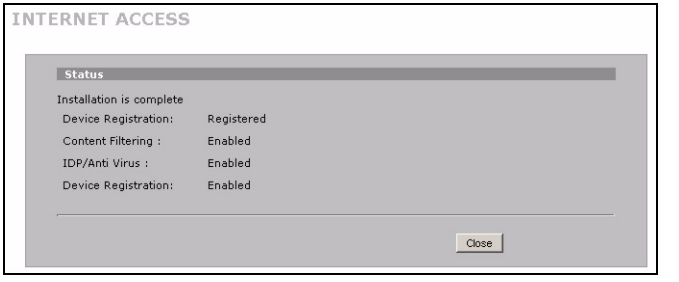
3 If you already have an account at myZyXEL.com, select **Existing myZyXEL.com account** and enter account information. Otherwise, select **New myZyXEL.com account** and fill in the fields below to create a new account and register your ZyWALL. Click **Next**.

4 Wait for the registration progress to finish.



5 The following screen displays if the registration was not successful. Click **Return** to go back to the **Device Registration** screen and check your settings.

6 Click **Close** to leave the wizard screen when the registration and activation are done.



If you want to activate a standard service with your iCard's PIN number (license key), use the **REGISTRATION Service** screen. See the user's guide for details.

5 DMZ

The DeMilitarized Zone (DMZ) allows public servers (web, e-mail, FTP, etc.) to be visible to the outside world and still have firewall protection from DoS (Denial of Service) attacks.

You can assign TCP/IP configuration via DHCP to computers connected to the DMZ ports. Otherwise, configure the computers with static IP addresses (in the same subnet as the DMZ port's IP address) and DNS server addresses. Use the ZyWALL's DMZ IP address as the default gateway.

Do the following to configure the DMZ if the ZyWALL is in routing mode.

You do not need to configure DMZ with bridge mode, skip to Section 7.

1 Click **NETWORK** > **DMZ** in the navigation panel.

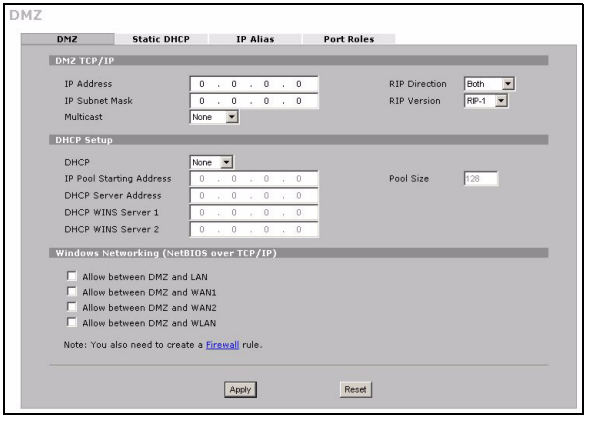
2 Specify an IP address and subnet mask for the DMZ interface.

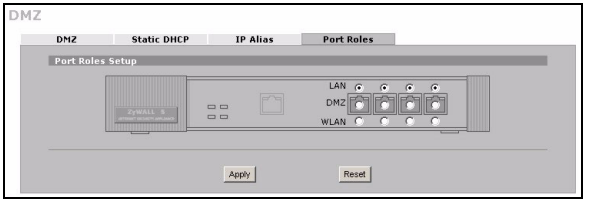
   If you use private IP addresses on the DMZ, use NAT to make the servers publicly accessible (see Section 6).

   A public IP address must be on a separate subnet from the WAN port's public IP address. If you do not configure NAT for the public IP addresses on the DMZ, the ZyWALL routes traffic to the public IP addresses on the DMZ without performing NAT. This may be useful for hosting servers for NAT unfriendly applications.

3 Click **Apply**.

4 By default, **LAN/DMZ** ports 1 to 4 are all LAN ports. To configure a port as a DMZ port, click the **Port Roles** tab, select its radio button next to **DM**Z and click **Apply**.



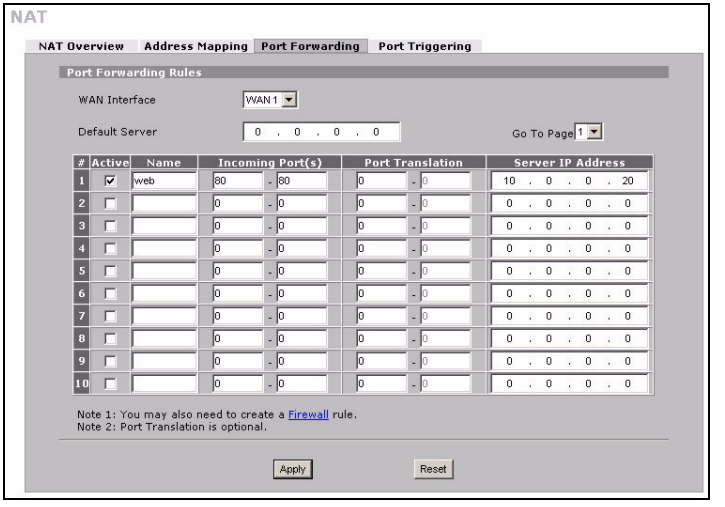


6 NAT

NAT (Network Address Translation - NAT, RFC 1631) means the translation of an IP address in one network to a different IP address in another. You can use the **NAT Address Mapping** screens to have the ZyWALL translate multiple public IP addresses to multiple private IP addresses on your LAN (or DMZ).

The following example allows access from the WAN1 to an HTTP (web) server on the DMZ. The server has a private IP address of 10.0.0.20.

1 Click **ADVANCED** > **NAT** in the navigation panel and then **Port Forwarding**.
2 Select the WAN connection (**WAN1**) for which you want to configure port forwarding rules.
3 Select the **Active** check box.
4 Type a name for the rule.
5 Type the port number that the service uses.
6 Type the HTTP server's IP address.
7 Click **Apply**.



7 Firewall

You can use the ZyWALL without configuring the firewall.

The ZyWALL's firewall is pre-configured to protect your LAN from attacks from the Internet. By default, no traffic can enter your LAN unless a request was generated on the LAN first. The ZyWALL allows access to the DMZ from the WAN or LAN, but blocks traffic from the DMZ to the LAN.

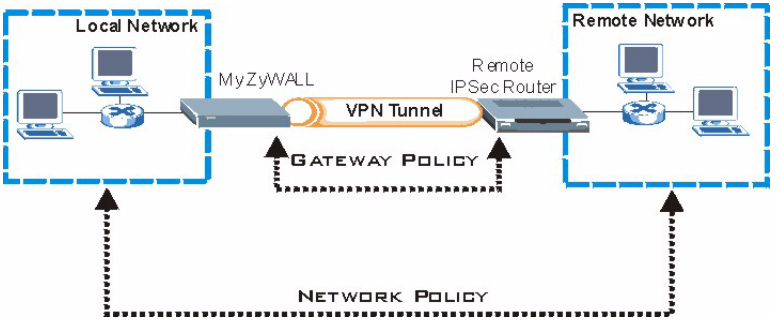
If you are using the ZyWALL in router mode, continue with the next section. For bridge mode, skip to Section 9.

8 VPN Rule Setup

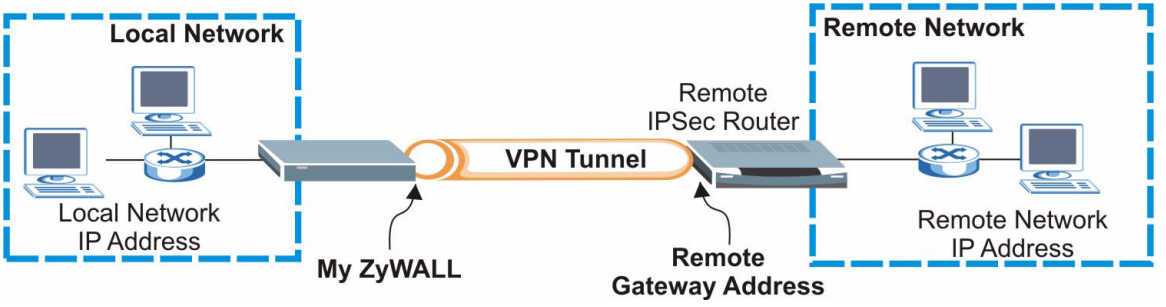
A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network.

A gateway policy identifies the IPSec routers at either end of a VPN tunnel.

A network policy specifies which devices (behind the IPSec routers) can use the VPN tunnel.



This figure helps explain the main fields in the wizard screens.



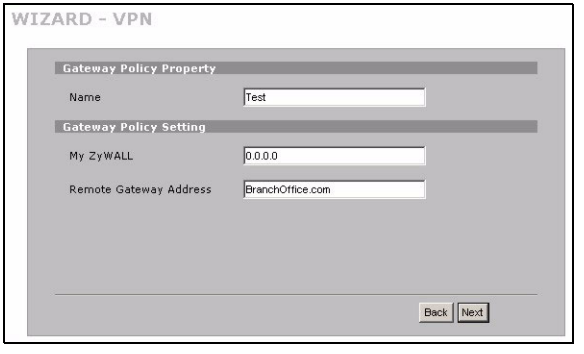
1 Click the **Wizard** icon ( ) in the **HOME** screen and then the **VPN Setup** link to open the VPN wizard.

Your settings are not saved when you click **Back**.

2 Use this screen to configure the gateway policy.

Name: Enter a name to identify the gateway policy.

Remote Gateway Address: Enter the IP address or domain name of the remote IPSec router.



3 Use this screen to configure the network policy.

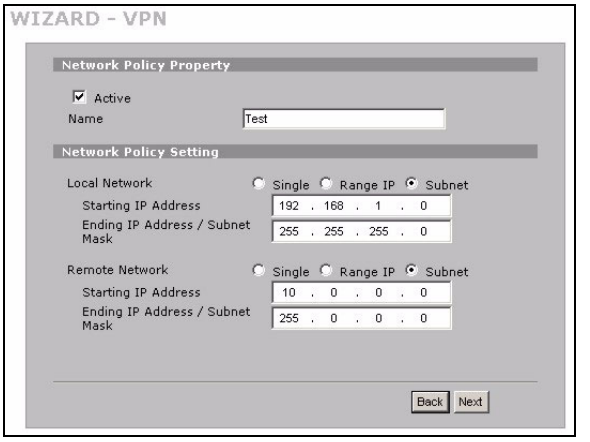
Leave the **Active** check box selected.

Name: Enter a name to identify the network policy.

Select **Single** and enter an IP address for a single IP address.

Select **Range IP** and enter starting and ending IP addresses for a specific range of IP addresses.

Select **Subnet** and enter an IP address and subnet mask to specify IP addresses on a network by their subnet mask.



Make sure that the remote IPSec router uses the same security settings that you configure in the next two screens.

Negotiation Mode: Select **Main Mode** for identity protection. Select **Aggressive Mode** to allow more incoming connections from dynamic IP addresses to use separate passwords.

Multiple SAs (security associations) connecting through a secure gateway must have the same negotiation mode.

Encryption Algorithm: Select **3DES** or **AES** for stronger (and slower) encryption.

Authentication Algorithm: Select **MD5** for minimal security or **SHA-1** for higher security.

Key Group: Select **DH2** for higher security.

SA Life Time: Set how often the ZyWALL renegotiates the IKE SA (minimum 180 seconds). A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.

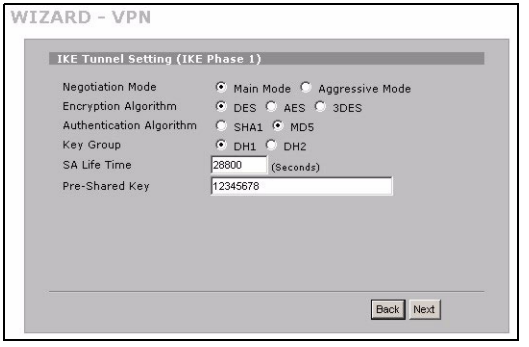
Pre-Shared Key: Use 8 to 31 case-sensitive ASCII characters or 16 to 62 hexadecimal ("0-9", "A-F") characters. Precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key.

Encapsulation Mode: **Tunnel** is compatible with NAT, **Transport** is not.

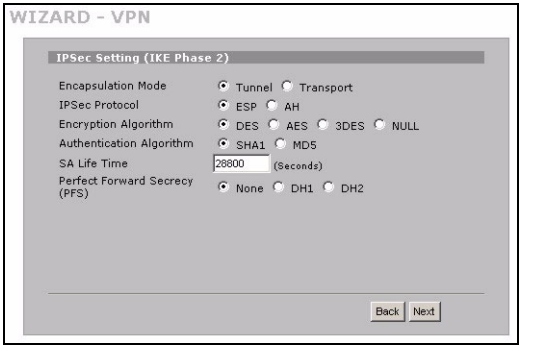
IPSec Protocol: **ESP** is compatible with NAT, **AH** is not.

Perfect Forward Secrecy (PFS): **None** allows faster IPSec setup, but **DH1** and **DH2** are more secure.

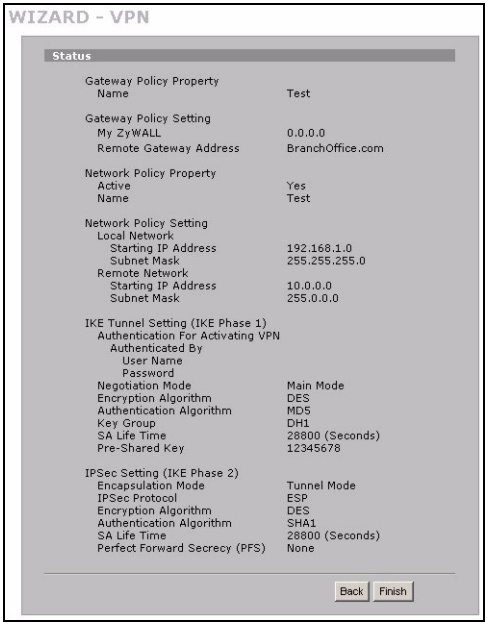
4 Use this screen to configure IKE (Internet Key Exchange) tunnel settings.



5 Use this screen to configure IPSec settings.



6 Check your VPN settings. Click **Finish** to save the settings.



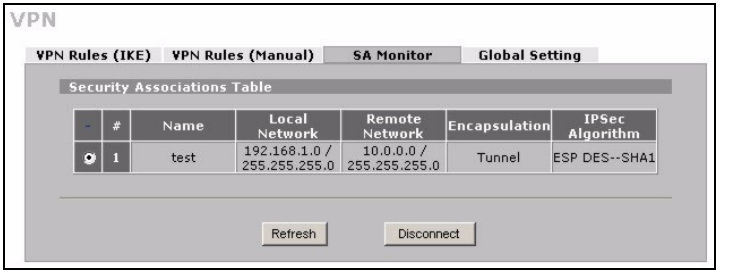
7 Click **Close** in the final screen to complete the VPN wizard setup. Continue with the next section to activate the VPN rule and establish a VPN connection.

8.1 Using the VPN Connection

Use VPN tunnels to securely send and retrieve files, and allow remote access to corporate networks, web servers and e-mail. Services work as if you were at the office instead of connected through the Internet.

For example, the “test” VPN rule allows secure access to an web server on a remote corporate LAN. Enter the server’s IP address (10.0.0.23 in this example) as your browser’s URL. The ZyWALL automatically builds the VPN tunnel when you attempt to use it.

Click **SECURITY** > **VPN** in the navigation panel and then the **SA Monitor** tab to display a list of connected VPN tunnels (the “test” VPN tunnel is up here).



9 Troubleshooting

Problem	Corrective Action
None of the LEDs turn on.	Make sure that you have the power adaptor connected to the ZyWALL and plugged in to an appropriate power source. Check all cable connections.
	If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.
Cannot access the ZyWALL from the LAN.	Check the cable connection between the ZyWALL and your computer or hub. Refer to Section 1 for details.
	Ping the ZyWALL from a LAN computer. Make sure your computer’s Ethernet card is installed and functioning properly. In the computer, click **Start**, (**All) Programs**, **Accessories** and then **Command Prompt**. In the **Command Prompt** window, type "ping" followed by the ZyWALL’s LAN IP address (192.168.1.1 is the default) and then press [ENTER]. The ZyWALL should reply. Otherwise, refer to Section 9.1.
	If you’ve forgotten the ZyWALL’s password, use the **RESET** button. Press the button in for about 10 seconds (or until the **SYS** LED starts to blink), then release it. It returns the ZyWALL to the factory defaults (password is 1234, LAN IP address 192.168.1.1 etc.; see your User’s Guide for details).
	If you’ve forgotten the ZyWALL’s LAN or WAN IP address, you can check the IP address in the SMT via the console port. Connect your computer to the **CONSOLE** port using a console cable. Your computer should have a terminal emulation communications program (such as HyperTerminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no flow control and 9600 bps port speed.
Cannot access the Internet.	Check the ZyWALL’s connection to the Ethernet jack with Internet access. Make sure the Internet gateway device (such as a DSL modem) is working properly.
	Click **WAN** in the navigation panel to verify your settings.

Problem	Corrective Action
Cannot establish a VPN connection	Make sure the ZyWALL and the remote IPSec router use the same VPN settings. Click **VPN** in the navigation panel to configure advanced settings.
	Access a web site to check that you have a successful Internet connection.

9.1 Set Up Your Computer's IP Address

This section shows you how to set up your computer to receive an IP address in Windows 2000, Windows NT and Windows XP. This is ensures that your computer can communicate with your ZyWALL.

1 In Windows XP, click **Start**, **Control Panel**.

In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

2 In Windows XP, click **Network Connections**.

In Windows 2000/NT, click **Network and Dial-up Connections**.

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

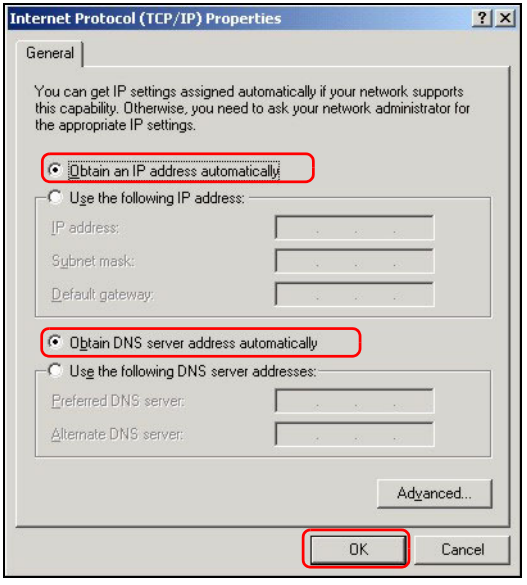
4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Windows XP) and click **Properties**.

5 The **Internet Protocol TCP/IP Properties** screen opens (the **General** tab in Windows XP). Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options.

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

7 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

8 Close the **Network Connections** screen.



Procedure to View a Product's Certification(s)

1 Go to www.zyxel.com.

2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.

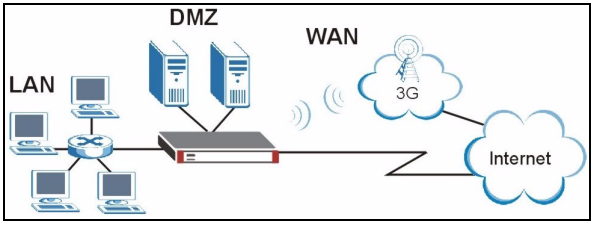
3 Select the certification you wish to view from this page.

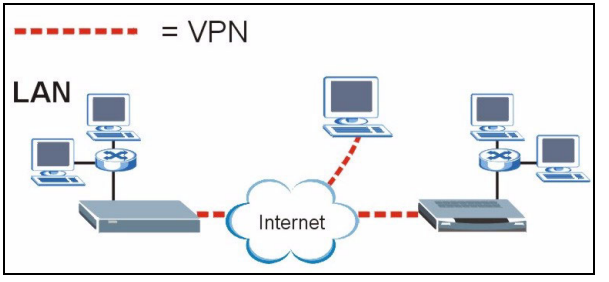
Übersicht

Die ZyWALL 5 ist eine Firewall mit VPN, Bandbreitenmanagement, Content Filtering, Anti-Spam, Anti-Virus, IDP (Intrusion Detection and Protection) und vielen anderen Funktionen. Sie können sie als transparente Firewall verwenden, ohne das Netzwerk neu zu konfigurieren und die Routingfunktionen des Geräts zu konfigurieren. Wenn sich der ZyWALL im Router-Modus befindet, können Sie auch eine 3G-Wireless-Card einsetzen, um ein zweites WAN hinzuzufügen. Die ZyWALL bietet die Möglichkeit, bei der Benutzung öffentlich zugänglicher Server die Portfunktionen zu wechseln (LAN zu DMZ) und erhöht damit die Netzwerksicherheit. In dieser Anleitung finden Sie eine Beschreibung der Anschlüsse und der Konfiguration, die notwendig ist, damit Sie die ZyWALL in Ihrem Netzwerk verwenden können.

Eine ausführliche Beschreibung aller Funktionen finden Sie im Benutzerhandbuch.

Bitte halten Sie die Daten für Ihren Internetzugang bereit.





Diese Anleitung ist in die folgenden Abschnitte aufgeteilt.

1 Anschließen der Hardware

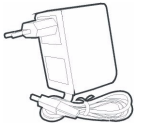
Sie benötigen folgendes:

ZyWALL

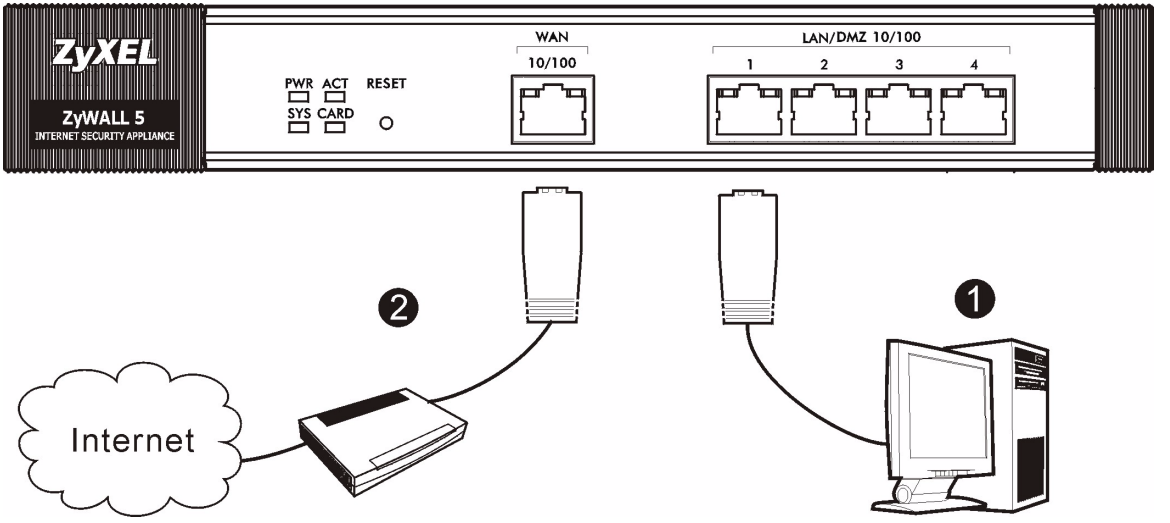
Computer

Ethernetkabel

Netzteil

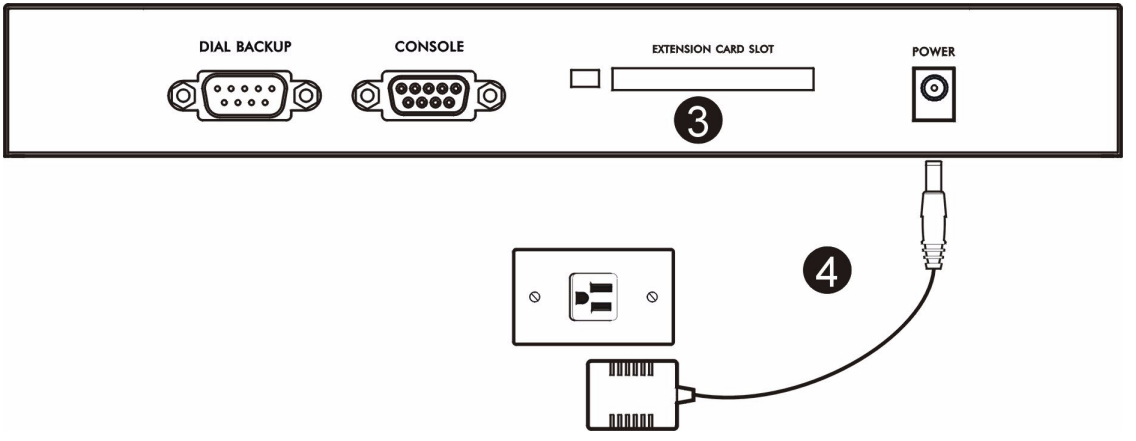


Wenn Sie das Gerät installieren, müssen Sie die Hardwaregeräte folgendermaßen anschließen.



1 Verbinden Sie den **LAN**-/**DMZ**-Port mit einem Ethernet-Kabel mit dem Computer. Wenn Sie diese Ports im **LAN**- oder **DMZ**-Fenster mit dem Web-Konfigurator als DMZ-Ports konfigurieren, können Sie auch mit Ethernetkabeln eine Verbindung von **LAN**-/**DMZ**-Ports zu öffentlichen Servern (Internet, E-Mail, FTP usw.) herstellen.

2 Schließen Sie mit einem anderen Ethernet-Kabel den **WAN**-Port an die Ethernet-Buchse mit Internetzugriff an.



3 Wenn Sie die Antiviren- und IDP-Funktion verwenden möchten, müssen Sie die Erweiterungskarte ZyWALL TURBO einsetzen. Sie können alternativ eine 3G-Wireless-Card einsetzen, um über ein 3G-Netzwerk auf das Internet zuzugreifen. Fur die LAN-Funktion benötigen Sie die Wireless LAN-Karte.

Weitere Informationen zu den Erweiterungskarten erhalten Sie in der Bedienungsanleitung der ZyWALL Turbo Karte. Eine Installationsanleitung fur eine Wireless LAN-Karte finden Sie im Benutzerhandbuch. Zum Zeitpunkt der Drucklegung können Sie im ZyWALL nur die 3G-Wireless-Card Sierra AC850/860 verwenden.

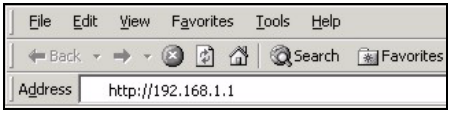
4 Schließen Sie das mitgelieferte Netzteil an der Rückseite der ZyWALL an.

5 Kontrollieren Sie den Systemstart mittels der LEDs an der Frontseite. Die **PWR**-LED beginnt zu leuchten. Während des Systemtests blinkt die **SYS**-LED. Wurde der Test erfolgreich abgeschlossen, bleibt diese Anzeige an. Die LEDs **ACT**, **CARD**, **LAN**/**DMZ** und **WAN** beginnen zu leuchten und bleiben an, wenn die entsprechenden Verbindungen richtig hergestellt wurden.

2 Zugriff auf den Web-Konfigurator

In diesem Abschnitt wird beschrieben, wie die **WAN 1**-Schnittstelle für den Internetzugriff konfiguriert wird.

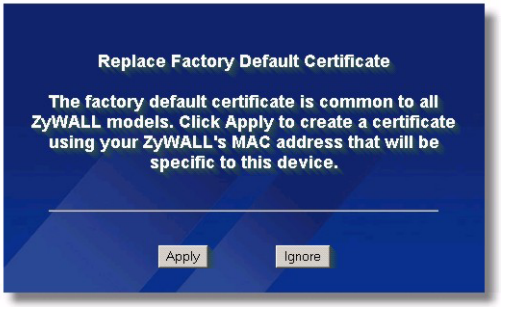
1 Starten Sie Ihren Internetbrowser. Geben Sie als Adresse **192.168.1.1** (die Standard IP-Adresse der ZyWALL) ein.
Wenn das Loginfenster nicht angezeigt wird, lesen Sie in Abschnitt 9.1 nach, wie Sie die IP-Adresse Ihres Computers einstellen können.



2 Klicken Sie auf **Login** (Einloggen) (das Standardpasswort 1234 ist bereits vorgegeben).

3 Ändern Sie das Passwort, indem Sie ein neues Passwort eingeben und auf **Apply** (Übernehmen) klicken.

4 Klicken Sie auf **Apply** (Übernehmen), um das Standarddigitalzertifikat der ZyWALL zu ersetzen.



5 Das Fenster **HOME** wird angezeigt.

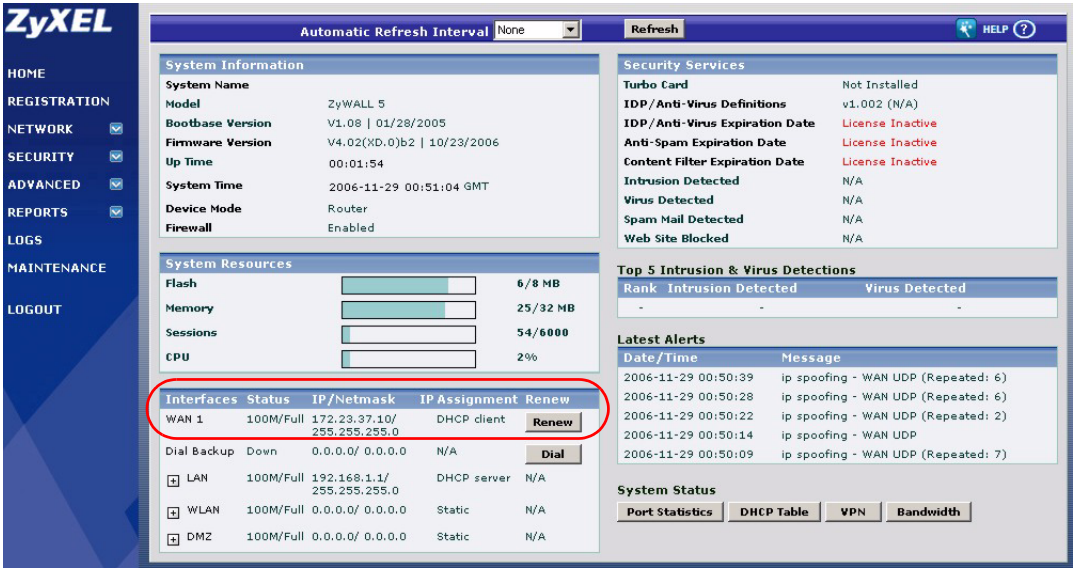
Standardmäßig befindet sich die ZyWALL im Routermodus. Wenn Sie Routingfunktionen wie NAT, DHCP oder VPN verwenden möchten, gehen Sie weiter zum nächsten Schritt.

Gehen Sie zu Abschnitt 3, wenn Sie die ZyWALL als eine transparente Firewall verwenden möchten.

6 Prüfen Sie die Netzwerkstatus Tabelle. Wenn der Status von **WAN 1** *nicht* **Down** ist und eine IP-Adresse angegeben ist, gehen Sie zu Abschnitt 5.

Wenn der Status bei **WAN 1 Down** ist (oder es keine IP-Adresse gibt), klicken Sie auf das **Assistent**-Symbol, und konfigurieren Sie **WAN 1** gemäß der Beschreibung in Abschnitt 4 **WAN**.

Verwenden Sie das **NETWORK WAN** Fenster, wenn Sie **WAN 2** konfigurieren möchten. Sie können auch ein Load-balancing zwischen den WAN-Anschlüssen konfigurieren.



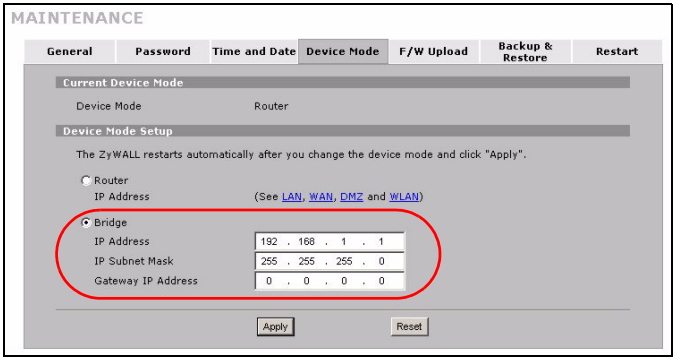
3 Bridge Modus

Wenn Sie bei der ZyWALL den Bridge Modus einstellen, funktioniert sie als transparente Firewall. Bei der ZyWALL wird der Bridge Modus folgendermaßen eingestellt:

1 Klicken Sie in der Navigationsleiste auf **MAINTENANCE** (Wartung) und dann auf **Device Mode** (Gerätemodus).

2 Wählen Sie **Bridge** und konfigurieren Sie eine (statische) IP-Adressen-Subnetmaske und eine Gateway-IP-Adresse für die **LAN-**, **WAN-**, **DMZ- u**nd **WLAN-** Schnittstelle der ZyWALL.

3 Klicken Sie auf **Apply** (Übernehmen). Die ZyWALL wird neu gestartet.



Gehen Sie weiter zu Abschnitt 5, wenn Sie Server haben, auf die Sie vom WAN aus zugreifen müssen.

4 Einrichten des Internetzugriffs und Produktregistrierung

1 Klicken Sie im Startfenster (**HOME**) auf das **Assistent**-Symbol ( ) und dort auf die Verknüpfung **Internet Access Setup** (Einrichten des Internetzugriffs), um den Assistenten zum Einrichten des Internetzugriffs aufzurufen.

Geben Sie die Daten für den Internetzugriff so ein, wie Sie sie von Ihrem Provider erhalten haben.

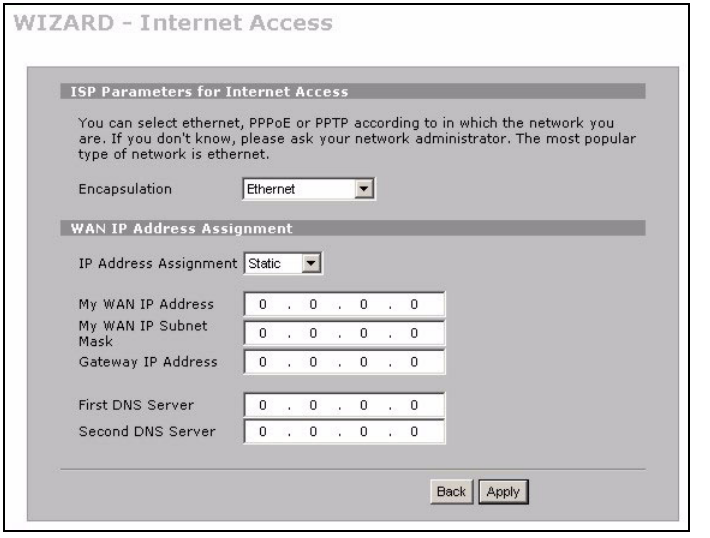
Wenn Ihnen eine feste IP-Adresse gegeben wurde, wählen Sie im Lisenfeld **IP Address Assignment** (IP-Adressenzuweisung) die Option **Static** (Statisch) und geben Sie dort die Daten ein.

Je nachdem, was Sie im Feld **Encapsulation** wählen, sieht die Eingabemaske anders aus. Geben Sie dort die Daten ein, die Sie von Ihrem Internetdienstanbieter oder Netzwerkadministrator erhalten haben.

Wenn Sie die Eingabe beendet haben, klicken Sie auf **Apply** (Übernehmen).

- **Ethernet Encapsulation**

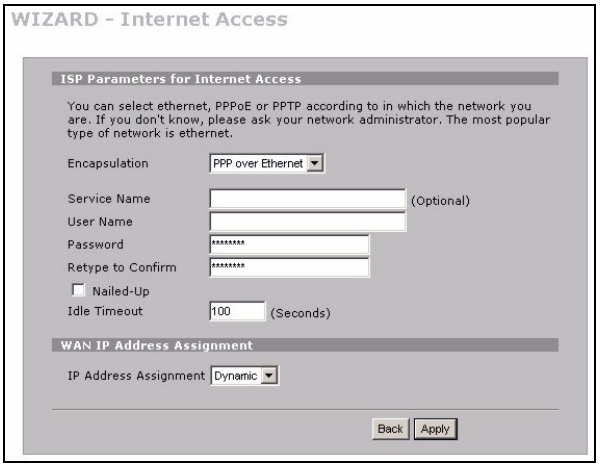
Konfigurieren Sie den Internetzugang in den **NETWORK WAN** (Netzwerk-WAN) Fenstern (auf der Registerkarte **WAN**).

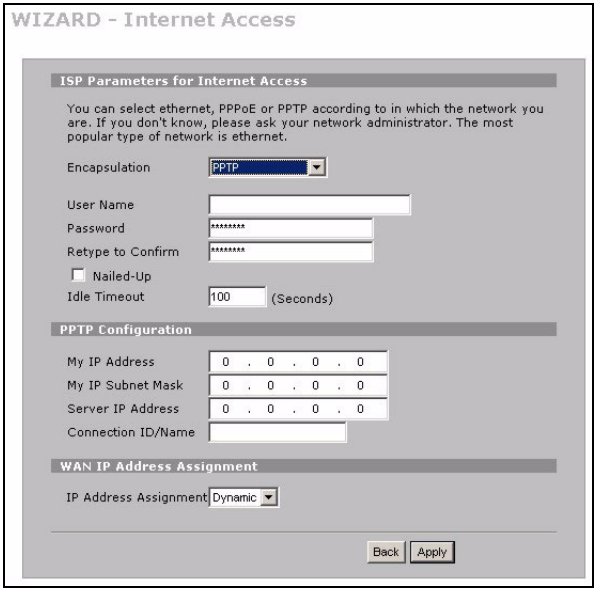


- **PPP over Ethernet or PPTP Encapsulation**

Wählen Sie **Nailed-Up**, wenn die Verbindung dauerhaft aufrecht erhalten werden soll (Aus Kostengründen empfehlen wir diese Option nur wenn Sie eine Flatrate haben).

Wenn die Verbindung nicht dauerhaft stehen soll, tragen Sie bitte den **Idle Timeout** in Sekunden ein.



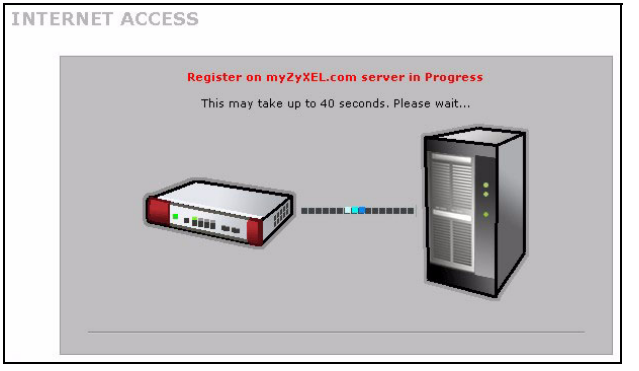


2 Klicken Sie auf **Next** (Weiter), um das Fenster aufzurufen, in dem Sie Ihre ZyWALL bei myZyXEL.com (Online-Servicezentrum von ZyXEL) registrieren und den kostenlosen Inhaltsfilter sowie die Anti-Spam-, Antiviren- und IDP-Testsoftware aktivieren können. Oder Sie klicken auf **Skip** (Überspringen) und dann auf **Close** (Schliessen), um das Einrichten des Internetzugriffs abzuschliessen.

Stellen Sie sicher, dass die ZyWALL Turbo Karte installiert ist, bevor Sie die Abodienste für IDP und die Antivirensoftware aktivieren.
Schalten Sie immer erst die ZyWALL aus, bevor Sie die ZyWALL Turbo Karte einsetzen oder entfernen.

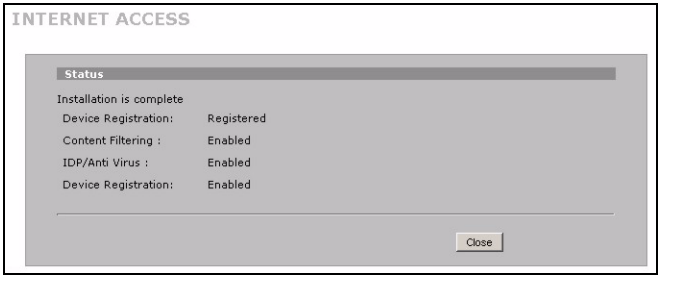
3 Wenn Sie bei myZyXEL.com bereits ein Konto haben, wahlen Sie **Existing myZyXEL.com account** (Bestehendes myZyXEL.com-Konto) und geben Sie die Daten zum Konto ein. Anderenfalls wählen Sie **New myZyXEL.com account** (Neues myZyXEL.com-Konto) und füllen Sie die Felder unten aus, um ein neues Konto zu öffnen und die ZyWALL zu registrieren. Klicken Sie auf **Next** (Weiter).

4 Warten Sie ab, bis die Registrierung abgeschlossen ist. Dies kann einige Minuten dauern.



5 Im folgenden Fenster wird angezeigt, wenn die Registrierung nicht erfolgreich durchgeführt wurde. Klicken Sie auf **Return** (Zuruck), um zum Fenster **Device Registration** (Gerät registrieren) zurückzukehren. Prüfen Sie noch einmal Ihre Einstellungen.

6 Klicken Sie auf **Close** (Schliessen), um nach der Registrierung und Aktivierung den Assistenten zu verlassen.



Wenn Sie mit der PIN-Nummer (Lizenzschlüssel) auf Ihrer iCard einen Standarddienst aktivieren möchten, gehen Sie zum Fenster **REGISTRATION**. Ausführliche Informationen finden Sie im Benutzerhandbuch.

5 DMZ

Die DeMilitarisierte Zone (DMZ) ermöglicht es, dass öffentliche Server (Internet, E-Mail, FTP, usw.) nach außen hin sichtbar sind aber dennoch über Firewallschutz vor DoS-Angriffen verfügen (Denial of Service).

Sie können die TCP/IP-Konfiguration über DHCP den Computern zuweisen, die an die DMZ-Anschlüsse angeschlossen sind. Die Computer werden mit statischen IP-Adressen (in demselben Subnetz wie die IP-Adressen des DMZ-Ports) und DNS-Serveradressen konfiguriert. Verwenden Sie die DMZ-IP-Adresse der ZyWALL als Standardgateway.

Wenn sich die ZyWALL im Routingmodus befindet, wird die DMZ folgendermaßen konfiguriert.

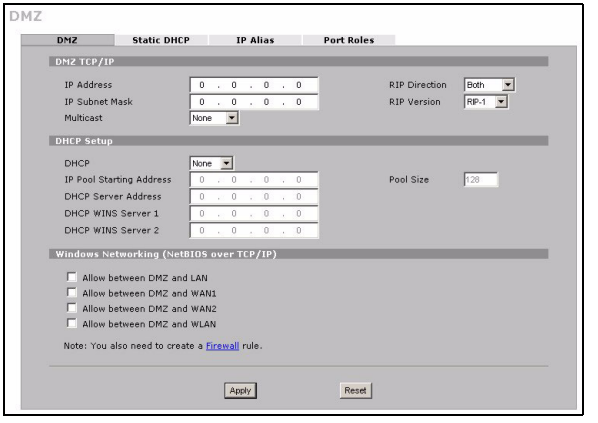
Im Bridge Modus muss die DMZ nicht konfiguriert werden. Gehen Sie weiter zu Abschnitt 7.

1 Klicken Sie in der Navigationsleiste auf **NETWORK** (NETZWERK) > **DMZ**.

2 Geben Sie für die DMZ-Schnittstelle eine IP-Adresse und eine Subnetmaske an.

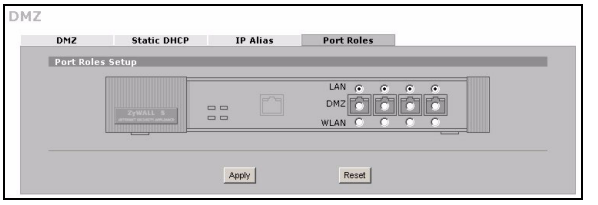
   Wenn Sie in der DMZ private IP-Adressen verwenden, können Sie die Server mit NAT öffentlich zugänglich machen (siehe Abschnitt 6).

   Eine öffentliche IP-Adresse muss sich auf einem anderen Subnetz als dem der öffentlichen IP-Adresse eines WAN-Ports befinden. Wenn Sie das NAT nicht für die öffentlichen IP-Adressen aus der DMZ konfigurieren, leitet die ZyWALL den Datenverkehr ohne NAT zu den öffentlichen IP-Adressen in der DMZ. Diese Funktion kann für die Hostserver bei NAT-feindlichen Anwendungen sehr nützlich sein.



3 Klicken Sie auf **Apply** (Übernehmen).

4 Standardmäßig sind alle **LAN**-/**DMZ**-Ports (1 bis 4) LAN-Ports. Wenn Sie einen Port als DMZ-Port konfigurieren möchten, klicken Sie auf die Registerkarte **Port Roles** (Portfunktionen), wählen Sie das Kontrollfeld neben **DMZ** und klicken Sie auf **Apply** (übernehmen).



6 NAT

NAT (Network Address Translation - NAT, RFC 1631) ist die Übersetzung einer IP-Adresse eines Netzwerks in eine andere IP-Adresse eines anderen Netzwerks. Wenn die ZyWALL mehrere öffentliche IP-Adressen in mehrere private IP-Adressen Ihres LAN (oder Ihrer DMZ) übersetzen soll, verwenden Sie die Fenster **NAT Address Mapping** (NAT-Adressmapping).

Das folgende Beispiel zeigt den Zugriff von einem WAN1- auf einen HTTP-Server (Internet) in der DMZ. Der Server hat die private IP-Adresse 10.0.0.20.

1 Klicken Sie in der Navigationsleiste auf **ADVANCED** (ERWEITERT) > **NAT** und dann auf **Port Forwarding** (Portweiterleitung).

2 Wählen Sie die WAN-Verbindung (**WAN1**) für diejenige Verbindung aus, für die Sie die Anschlussweiterleitungsregeln konfigurieren möchten.

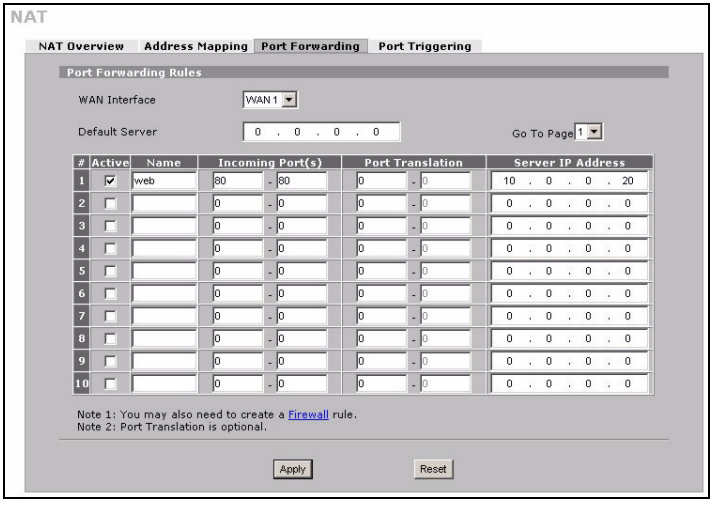
3 Wählen Sie das Kontrollfeld **Active** (Aktiv).

4 Geben Sie eine Bezeichnung für die Regel ein.

5 Geben Sie die Portnummer ein, die der Dienst verwendet.

6 Geben Sie die IP-Adresse des HTTP-Servers ein.

7 Klicken Sie auf **Apply** (Übernehmen).



7 Firewall

Sie können die ZyWALL verwenden, ohne die Firewall zu konfigurieren.

Die Firewall die ZyWALL ist so vorkonfiguriert, dass sie Ihr LAN vor Angriffen aus dem Internet schützt. Bei der Standardeinstellung können keine Daten in Ihr LAN eindringen, wenn nicht zuvor eine Anfrage aus dem LAN gestellt wurde. Die ZyWALL lässt den Zugriff vom WAN oder LAN auf die DMZ zu, blockiert aber den Datenverkehr aus der DMZ zum LAN.

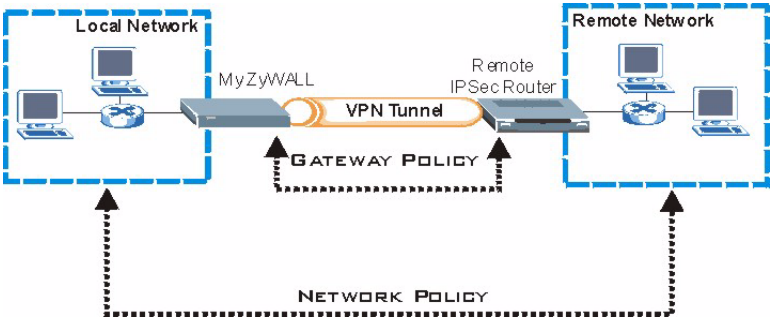
Wenn Sie die ZyWALL im Routermodus verwenden, fahren Sie mit dem nächsten Abschnitt fort. Weiter mit dem Bridge Modus geht es in Abschnitt 9.

8 Einstellen der VPN-Regeln

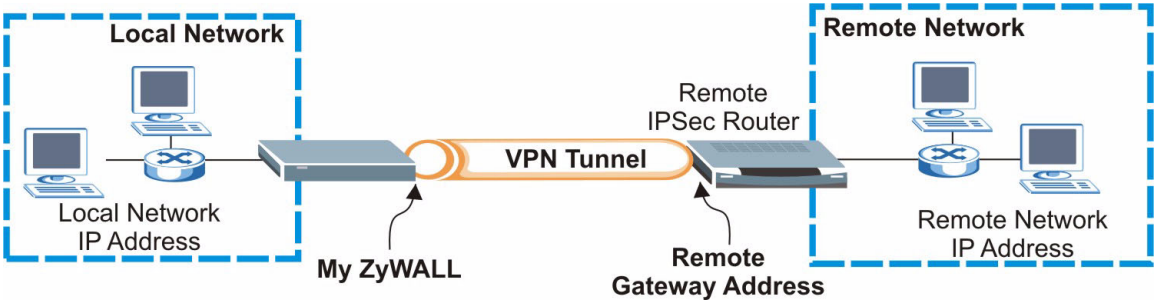
Mit einem VPN-Tunnel (Virtual Private Network) haben Sie eine sichere Verbindung zu anderen Computern oder Netzwerken.

Eine Gateway-Policy identifiziert an jedem Ende eines VPN-Tunnels die IPSec-Router.

In einer Netzwerk-Policy ist festgelegt, welche Geräte (hinter den IPSec-Routern) den VPN-Tunnel benutzen dürfen.



Diese Abbildung soll die Hauptfelder in den Assistentenfenstern erläutern.



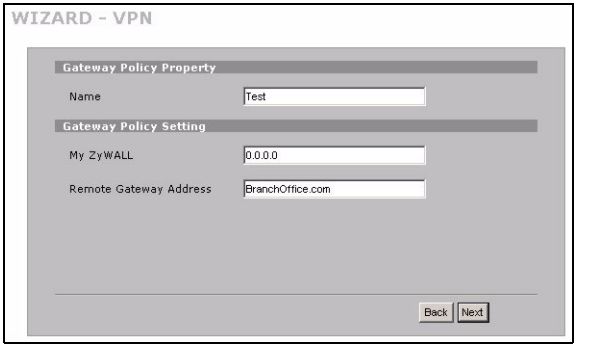
1 Klicken Sie im Startfenster (**HOME**) auf das **Assistent**-Symbol ( ) und dort auf die Verknüpfung **VPN Setup** (VPN Einrichten), um den VPN-Assistenten aufzurufen.

Wenn Sie auf **Back** (Zurück) klicken, werden Ihre Einstellungen nicht gespeichert.

2 In diesem Fenster können Sie die Gateway-Policy konfigurieren.

Name: Geben Sie einen Namen ein, um die Gateway-Policy zu bezeichnen.

Remote Gateway Address: Geben Sie die IP-Adresse oder den Domainnamen des IPSec-Routers ein.



3 In diesem Fenster können Sie die Netzwerk-Policy konfigurieren.

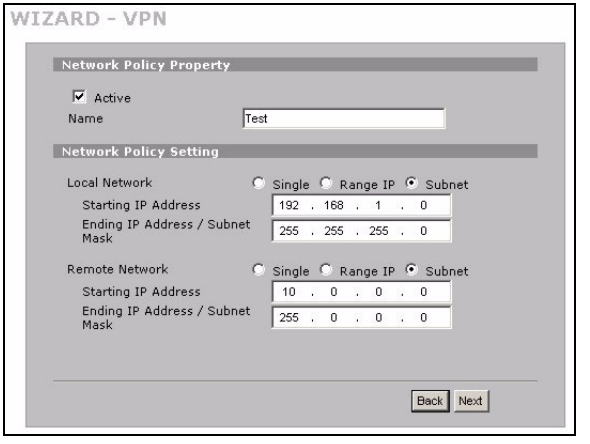
Lassen Sie die Markierung im Kontrollfeld **Active** (Aktiv).

Name: Geben Sie einen Namen für die Netzwerk Policy ein.

Wählen Sie **Single** und geben eine IP-Adresse für eine Host ein.

Wählen Sie **Range IP** (IP-Bereich) und geben Sie die Anfangs- und End-IP eines bestimmten Bereichs von IP-Adressen ein.

Wählen Sie **Subnet** (Subnetz) und geben Sie eine IP-Adresse und eine Subnetmaske ein, um ein bestimmtes Netzwerk anhand ihrer Subnetmaske festzulegen.



Stellen Sie sicher, dass der Remote-IPSec-Router dieselben Sicherheitseinstellungen verwendet, die Sie in den zwei folgenden Fenstern festlegen.

Negotiation Mode: Wählen Sie **Main Mode** für den Identitätsschutz. Wählen Sie **Aggressive Mode**, wenn mehrere eingehende Verbindungen von dynamischen IP-Adressen verschiedene Passwörter benutzen sollen.

Wenn mehrere SAs (Security Associations) durch ein Sicherheitsgateway verbunden sind, müssen diese denselben Negotiation-Modus haben.

Encryption Algorithm (Verschlüsselungsalgorithmus): Wählen Sie **3DES** oder **AES** für eine stärkere Verschlüsselung.

Authentication Algorithm (Authentifizierungsalgorithmus): Wählen Sie **MD5** für eine minimale Sicherheit oder **SHA-1** für eine höhere Sicherheit.

Key Group (Schlüsselgruppe): Wählen Sie **DH2** für eine höhere Sicherheit.

SA Life Time (SA-Dauer): Legen Sie fest, wie oft die ZyWALL die IKE SA wieder verhandelt (mindestens 180 Sekunden). Eine kurze SA-Dauer erhöht die Sicherheit, bei der Verhandlung wird aber vorübergehend der VPN-Tunnel getrennt.

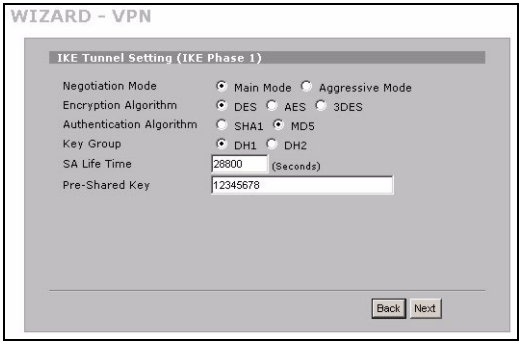
Pre-Shared Key: Geben Sie hier 8 bis 31 ASCII-Zeichen (Groß- und Kleinschreibung beachten) oder 16 bis 62 Hexadezimalzeichen ("0-9", "A-F") ein. Setzen Sie einem Hexadezimalschlüssel ein "0x" (Null x) voran, wird dieses nicht als Teil des 16 bis 32 Zeichen langen Schlüssels betrachtet.

Encapsulation Mode: **Tunnel** ist kompatibel mit NAT, **Transport** nicht.

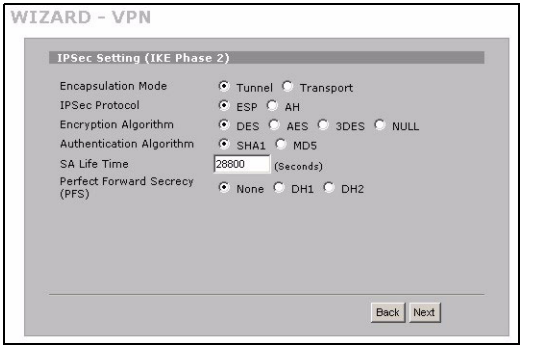
IPSec Protocol: **ESP** ist kompatibel mit NAT, **AH** nicht und AH bietet keine Verschlüsselung.

Perfect Forward Secrecy (PFS): **None** (Keine) ermöglicht einen beschleunigt Phase 2 beim Aufbau des IPSec-Tunnels, **DH1** und **DH2** bieten aber mehr Sicherheit.

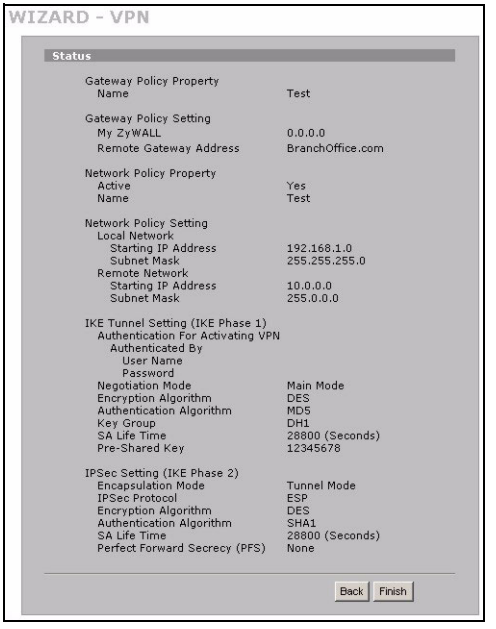
4 In diesem Fenster werden die IKE-Tunneleinstellungen (Internet Key Exchange) konfiguriert.



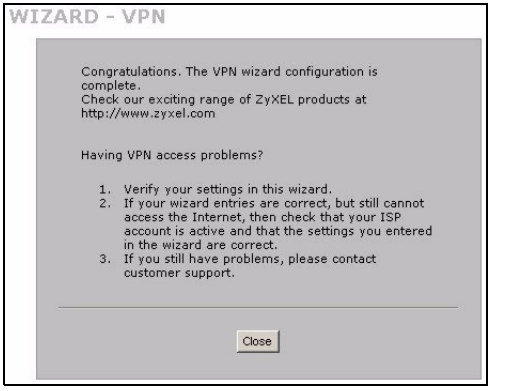
5 In diesem Fenster werden die IPSec-Einstellungen konfiguriert.



6 Prüfen Sie Ihre VPN-Einstellungen. Klicken Sie auf **Finish** (Fertig stellen), um die Einstellungen zu speichern.



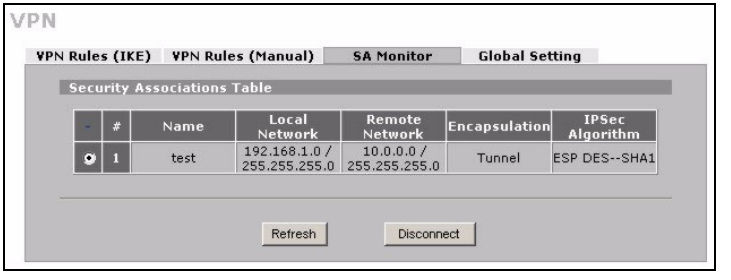
7 Klicken Sie beim letzten Fenster auf **Close** (Schließen), um die Installation mit dem VPN-Assistenten zu beenden. Fahren Sie mit dem nächsten Abschnitt fort, um die VPN-Regel zu aktivieren und eine VPN-Verbindung herzustellen.



8.1 Benutzen der VPN-Verbindung

Mit VPN-Tunneln können Sie Dateien sicher senden und empfangen sowie einen Remotezugriff auf Firmennetzwerke, Internetserver und E-Mails zulassen. Die Dienste funktionieren so, als wären Sie an einem Standort und nicht über das Internet miteinander verbunden.

Zum Beispiel lässt die VPN-Regel “test” einen sicheren Zugriff auf einen Internetserver in einem Remote-Firmen-LAN zu. Geben Sie die IP-Adresse des Servers (in diesem Beispiell 10.0.0.23) als die URL Ihres Browsers ein. Die ZyWALL baut automatisch den VPN-Tunnel auf, wenn Sie den Server benutzen möchten.



Klicken Sie in der Navigationsleiste auf **SECURITY** > **VPN** und dort auf die Registerkarte **SA Monitor**. Dort erscheint eine Liste der aktiven VPN-Tunnel (der VPN-Tunnel “test” ist hier oben).

9 Problembeseitigung

Problem	Lösungsmöglichkeit
Es leuchtet keine der LED-Anzeigen.	Stellen Sie sicher, dass das Netzteil richtig an die ZyWALL und an eine Netzsteckdose angeschlossen wurde. Überprüfen Sie alle Kabelverbindungen.
	Wenn die LEDs auch dann nicht leuchten, besteht möglicherweise ein Hardwareproblem. In diesem Fall sollten Sie sich an Ihren Händler wenden.
Aus dem LAN kann nicht auf die ZyWALL zugegriffen werden.	Überprüfen Sie die Kabelverbindung zwischen der ZyWALL und dem Computer oder Hub. Eine ausführliche Beschreibung finden Sie in Abschnitt 1.
	Versuchen Sie die ZyWALL mit einem Ping von einem LAN-Computer aus zu erreichen. Stellen Sie sicher, dass die Ethernetkarte des Computers installiert ist und einwandfrei funktioniert. Klicken Sie im Computer auf **Start**, (**Alle) Programme**, **Zubehör** und dann auf **Eingabeaufforderung**. Geben Sie im Fenster **Eingabeaufforderung** "ping" gefolgt von der LAN-IP-Adresse der ZyWALL (192.168.1.1 ist die Standardadresse) ein und drücken Sie dann auf [ENTER]. Nun sollte die ZyWALL reagieren. Falls nicht, lesen Sie nach unter Abschnitt 9.1.
	Wenn Sei das ZyWALL-Passwort vergessen haben, drücken Sie die **RESET** -Taste. Drücken Sie etwa 10 Sekunden lang auf die Taste (oder so lange, bis die **SYS-**LED blinkt). Lassen Sie die Taste dann wieder los. Auf diese Weise werden alle Einstellungen der ZyWALL auf ihre Standardwerte zurückgesetzt (Passwort: 1234, LAN-IP-Adresse 192.168.1.1 usw.; Detailinformationen hierzu finden Sie im Benutzerhandbuch).
	Wenn Sie die LAN- oder WAN-IP-Adresse der ZyWALL vergessen haben, können Sie die IP-Adresse über den Konsolenport im SMT einsehen. Schließen Sie Ihren Computer mit einem Konsolenkabel an den Anschluss **CONSOLE** an. Ihr Computer muss über ein Terminalemulationsprogramm (z.B. HyperTerminal) verfügen, das folgendermassen eingestellt ist: Anschlussemulation VT100, keine Parität, 8 Datenbits, 1 Stoppbit, keine Flusskontrolle, Portgeschwindigkeit 9600 bps.
Ein Zugriff auf das Internet ist nicht möglich.	Prüfen Sie den Anschluss der ZyWALL an der Ethernet-Buchse mit Internetzugriff. Stellen Sie sicher, dass das Gerät für den Internetzugriff (zum Beispiel ein DSL-Modem) einwandfrei funktioniert.
	Klicken Sie in der Navigationsleiste auf **WAN** und überprüfen Sie die Einstellungen.
Es kann keine VPN-Verbindung hergestellt werden.	Stellen Sie sicher, dass die ZyWALL und der Remote-IPSec -Router die gleichen VPN-Einstellungen verwenden. Klicken Sie in der Navigationsleiste auf **VPN**, um die erweiterten Einstellungen zu konfigurieren.
	Rufen Sie eine Website auf, um zu überprüfen, ob die Internetverbindung hergestellt werden kann.

9.1 Einrichten der IP-Adresse des Computers

In diesem Abschnitt wird beschrieben, wie Sie Ihren Computer einrichten müssen, damit er bei Windows 2000, Windows NT und Windows XP eine IP-Adresse empfangen kann. Nur auf diese Weise kann Ihr Computer mit der ZyWALL kommunizieren.

1 Klicken Sie bei Windows XP auf **Start**, **Systemsteuerung**.

Klicken Sie bei Windows 2000/NT auf **Start**, **Einstellungen**, **Systemsteuerung**.

2 Klicken Sie bei Windows XP auf **Netzwerkverbindungen**.

Klicken Sie bei Windows 2000/NT auf **Netzwerk und DFÜ-Verbindungen**.

3 Klicken Sie mit der rechten Maustaste auf **LAN-Verbindung** und dann auf **Eigenschaften**.

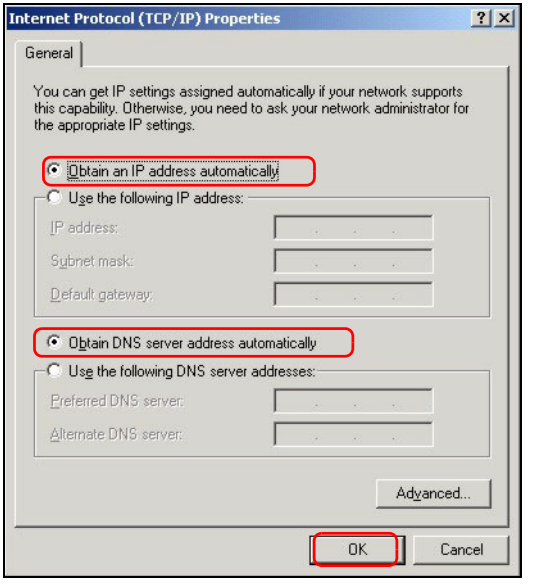
4 Wählen Sie **Internetprotokoll (TCP/IP)** (bei Windows XP auf der Registerkarte **Allgemein**) und klicken Sie auf **Eigenschaften**.

5 Das Fenster **Eigenschaften von Internetprotokoll (TCP/IP)** erscheint (bei Windows XP auf der Registerkarte **Allgemein**). Wählen Sie **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen**.

6 Klicken Sie auf **OK**, um das Fenster **Eigenschaften von Internetprotokolle (TCP/IP)** zu schließen.

7 Klicken Sie auf **Schließen** (bei Windows 2000/NT auf **OK**), um das Fenster **Eigenschaften von LAN-Verbindung** zu schließen.

8 Schließen Sie das Fenster **Netzwerkverbindungen**.



Schritte zum Ansehen der Produktzertifizierung(en)

1 Besuchen Sie www.zyxel.com.

2 Wählen Sie auf der ZyXEL-Homepage aus der Liste der Produkte Ihr Produkt aus.

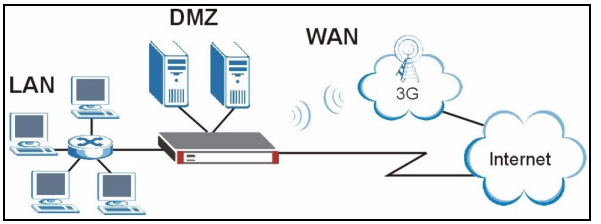
3 Wählen Sie auf dieser die Zertifizierung aus, die Sie gerne angezeigt haben möchten.

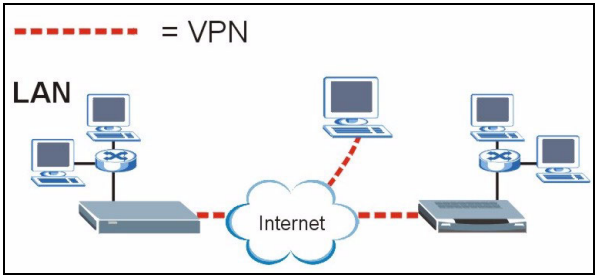
Vista previa

El ZyWALL 5 es un cortafuegos, soporte de VPNs, gestión del ancho de banda, filtrado de contenidos, anti-spam, antivirus, IDP (Intrusion Detection and Protection) y muchas otras características. Puede usarlo como cortafuegos transparente sin reconfigurar su red ni configurar las características de enrutamiento de ZyWALL. Cuando el ZyWALL está en modo router, también puede insertar una tarjeta 3G inalámbrica para añadir una segunda WAN. El ZyWALL aumenta la seguridad de la red añadiendo la opción de cambiar las funciones de los puertos de LAN a DMZ para utilizarlos con servidores de acceso público. Esta guía cubre las conexiones iniciales y configuración necesaria para comenzar a usar el ZyWALL en su red.

Vea la Guía del usuario para más información sobre todas las características.

Puede que necesite su acceso a Internet para más información.





Esta guía está dividida en las siguientes secciones.

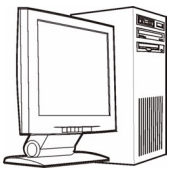
1 Conexiones del hardware
2 Acceso al configurador Web
3 Modo puente (bridge)
4 Configuración del acceso a Internet y registro del producto
5 DMZ
6 NAT
7 Cortafuegos
8 Configuración de reglas VPN
9 Solución de problemas

1 Conexiones del hardware

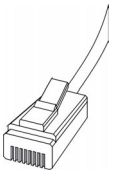
Necesita lo siguiente.

ZyWALL

Ordenador

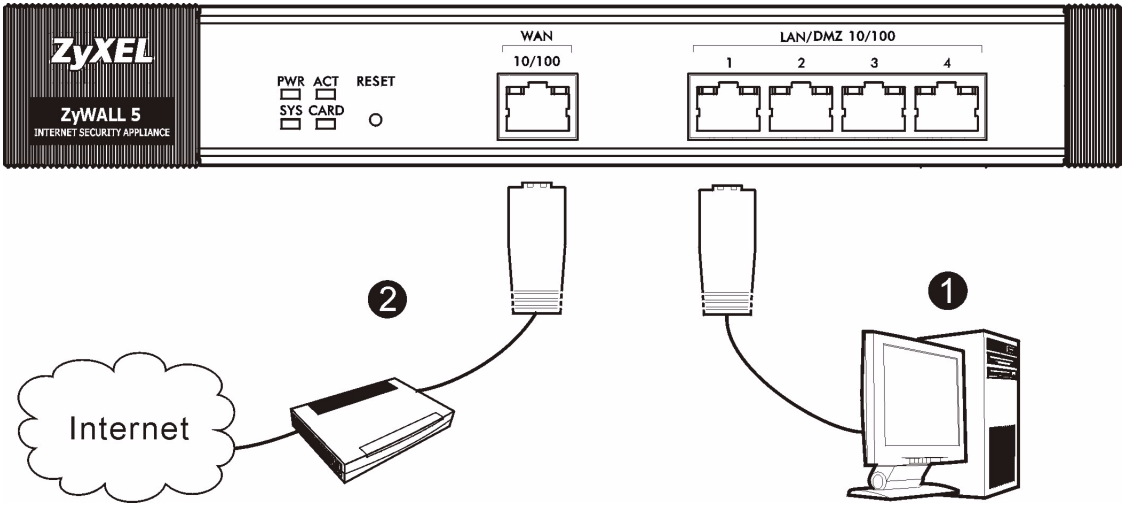


Cables Ethernet



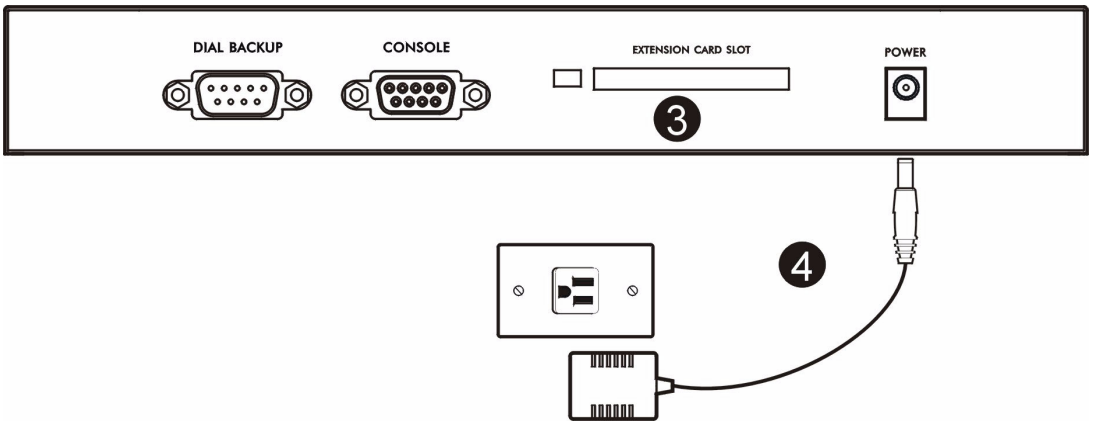
Adaptador de corriente

Realice lo siguiente para crear conexiones de hardware para la configuración inicial.



1 Use un cable Ethernet para conectar el puerto **LAN/DMZ** a un ordenador. Si configura estos puertos como puertos **DMZ** en la pantalla **LAN** o **DMZ** a través del configurador web, también podrá usar cables Ethernet para conectar servidores públicos (web, correo electrónico, FTP, etc.) a los puertos **LAN/DMZ**.

2 Use un cable Ethernet para conectar el puerto **WAN** a un dispositivo Ethernet con acceso a Internet.



3 Inserte la tarjeta de expansion ZyWALL Turbo para utilizar el antivirus y las caracteristicas IDP o inserte una tarjeta LAN inalambrica para utilizar la caracteristica wireless LAN. Puede insertar opcionalmente una tarjeta inalámbrica 3G para acceder a Internet de forma inalámbrica a través de una red 3G. Consulte la guia ZyWALL Turbo Card para mas informacion sobre la tarjeta de expansion. Consulte la guia del usuario para la instalacion de una tarjeta LAN inalambrica. En el momento de la redacción de esta guía, sólo podrá utilizar la tarjeta inalámbrica Sierra AC850/860 3G en el ZyWALL.

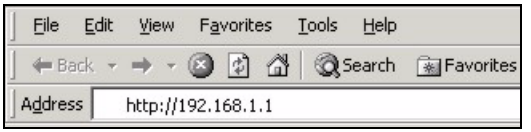
4 Use el adaptador de corriente incluido para conectar el zócalo de alimentación (en el panel posterior) a una toma de corriente.

5 Mire al panel frontal. El LED **PWR** se encenderá. El LED **SYS** parpadeará mientras realiza la prueba del sistema y luego se quedará fijo si la prueba ha tenido éxito. Los LEDs **ACT**, **CARD**, **LAN**/**DMZ** y **WAN** se encenderán y permanecerán encendidos si las conexiones correspondientes se han realizado correctamente.

2 Acceso al configurador Web

Use esta sección para configurar la interfaz **WAN 1** para el acceso a Internet.

1 Abra su explorador de web. Introduzca **192.168.1.1** (la dirección IP predeterminada del ZyWALL) como dirección.
Si no aparece la pantalla de acceso, vea Sección 9.1 para ajustar la dirección IP de su ordenador.



2 Haga clic en **Login** (acceso) (la contraseña predeterminada 1234 ya está introducida).

3 Cambie la contraseña de acceso introduciendo una nueva contraseña y haciendo clic en **Apply** (Aplicar).

4 Haga clic en **Apply** (Aplicar) para reemplazar el certificado digital predeterminado de ZyWALL.

5 Aparecerá la pantalla **HOME** (Inicio).

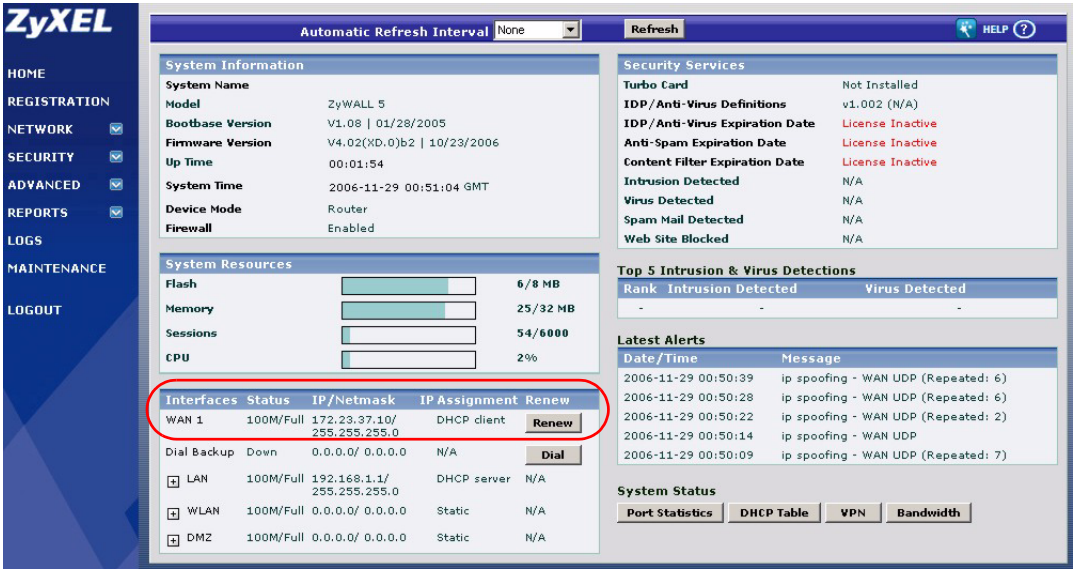
El ZyWALL está en modo router por defecto. Continúe en el siguiente paso si desea usar características de enrutamiento como NAT, DHCP y VPN.

Vaya a Sección 3 si prefiere usar el ZyWALL como cortafuegos transparente.

6 Compruebe la tabla network status (estado de la red). Si el estado de **WAN 1** *no* es **Down** (Caído) y hay una dirección IP, vaya a Sección 5.

Si el estado de **WAN 1** es **Down** (la línea ha caído) (o no hay una dirección IP), haga clic en el icono **Wizard** (Asistente) y utilice la Sección 4 para configurar **WAN 1**.

Use las pantallas **WAN** en **NETWORK** (red) si necesita configurar **WAN 2**. También puede configurar la distribución de carga entre las conexiones WAN.



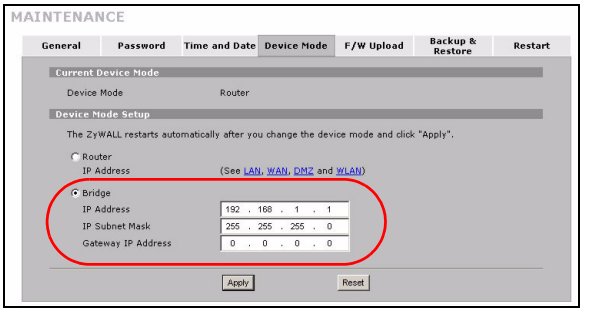
3 Modo puente (bridge)

Cuando configura el ZyWALL en modo puente, funciona como un cortafuegos transparente. Haga lo siguiente para configurar el ZyWALL en este modo bridge.

1 Haga clic en **MAINTENANCE** (Mantenimiento) en el panel de navegación y luego en **Device Mode** (Modo de Dispositivo).

2 Seleccione **Bridge** (Puente) y configure una máscara de subred de dirección IP (estática) y una dirección IP de puerta de enlace para las interfaces **LAN**, **WAN**, **DMZ** y **WLAN** del ZyWALL.

3 Haga clic en **Apply** (Aplicar). El ZyWALL se reiniciará.



Vaya a Sección 5 si tiene servidores que necesitan ser accesibles desde la WAN.

4 Configuración del acceso a Internet y registro del producto

1 Haga clic en el icono **Wizard** (Asistente) ( ) en la pantalla **HOME** (INICIO) y luego en el enlace **Internet Access Setup** (Configuración de acceso a Internet) para abrir el asistente de acceso a Internet.

Introduzca la información del acceso a Internet exactamente como se le ha dado.

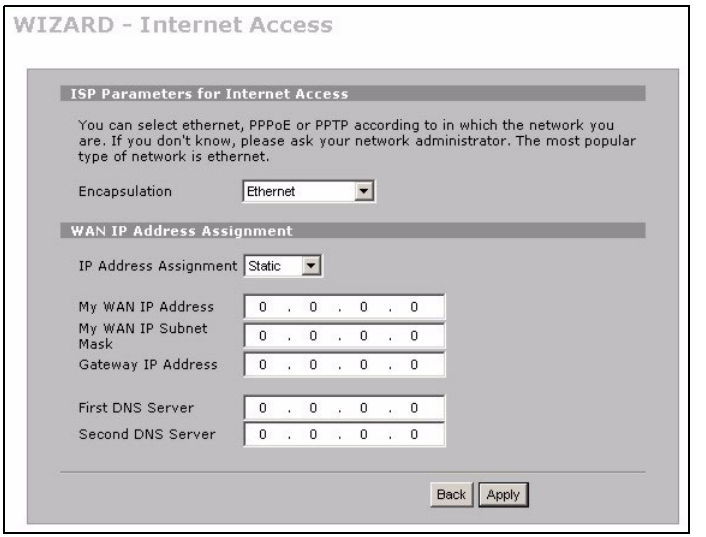
Si se le ha dado una dirección IP para usarla, seleccione **Static** (Estática) en el cuadro desplegable **IP Address Assignment** (Asignación de dirección IP) e introduzca la información facilitada.

Los campos varían dependiendo de lo que seleccione en el campo **Encapsulation** (Encapsulación). Rellénelos con la información facilitada por el ISP o el administrador de redes.

Haga clic en **Apply** (Aplicar) cuando haya terminado.

- **Encapsulación Ethernet**

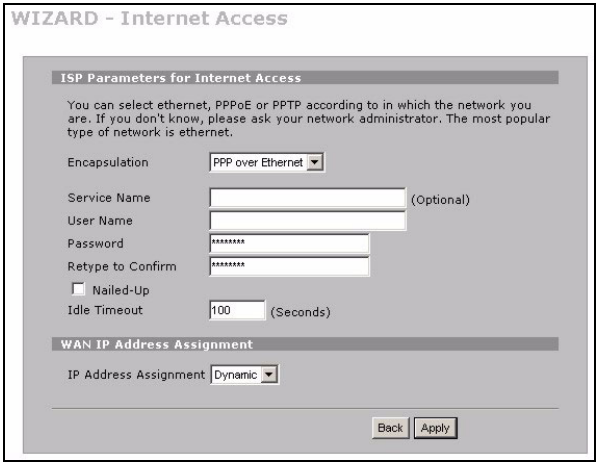
Configure un servicio Roadrunner en las pantallas **WAN** de **NETWORK** (Red) (use la ficha pestaña **WAN**).

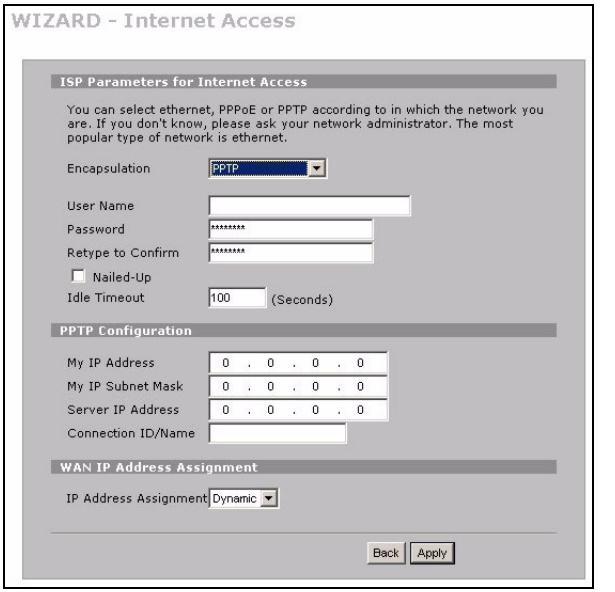


- **Encapsulación PPP sobre Ethernet o PPTP**

Seleccione **Nailed-Up** (Forzada) cuando desee que su conexión esté arriba todo el tiempo (esto puede resultar caro si su ISP le cobra por el tiempo de uso de Internet en lugar de una cuota fija mensual).

Para no tener una conexión arriba todo el tiempo, especifique un período de tiempo en espera (en segundos) en **Idle Timeout (Temporizador de inactividad)**.

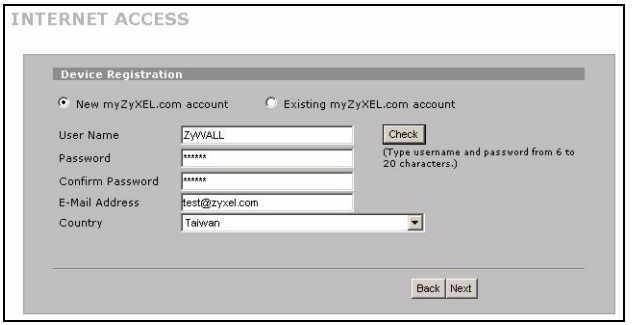




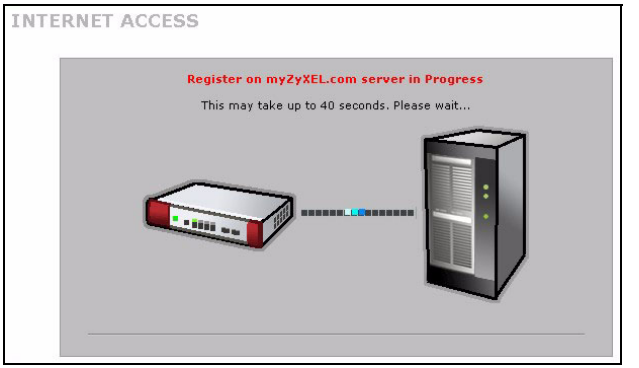
2 Haga clic en **Next** (Siguiente) para mostrar la pantalla donde podra registrar ZyWALL con myZyXEL.com (centro de servicios en linea de ZyXEL) y activar los periodos de prueba de filtrado de contenidos, anti-spam, antivirus e IDP. En caso contrario, haga clic en **Skip** (Saltar) y luego en **Close** (Cerrar) para completar la configuracion de acceso a Internet.

Asegurese de haber instalado el ZyWALL Turbo Card antes de activar los servicios de suscripcion a IDP y antivirus.
Apague el ZyWALL antes de instalar o quitar ZyWALL Turbo Card.

3 Si ya tiene una cuenta en myZyXEL.com, seleccione **Existing myZyXEL.com account** (Cuenta myZyXEL.com existente) e introduzca la informacion de la cuenta. En caso contrario, seleccione **New myZyXEL.com account** (Nueva cuenta myZyXEL.com) y rellene los campos de abajo para crear una nueva cuenta y registrar su ZyWALL. Haga clic en **Next** (Siguiente).

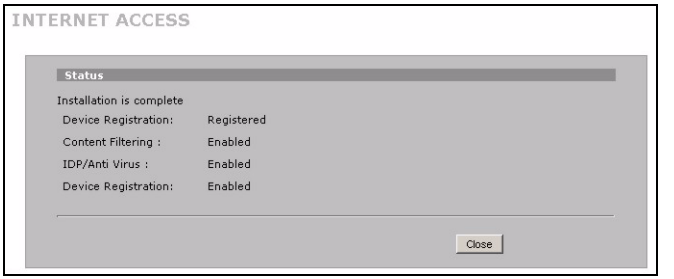


4 Espere a que el progreso del registro finalice.



5 La pantalla siguiente muestra si el registro no ha tenido exito. Haga clic en **Return** (Volver) para regresar a la pantalla **Device Registration** (Registro del dispositivo) y comprobar su configuracion.

6 Haga clic en **Close** (Cerrar) para salir de la pantalla del asistente cuando se hayan realizado el registro y la activacion.



Si desea activar un servicio estandar con el numero de PIN de su iCard (clave de licencia), utilice la pantalla **REGISTRATION Service** (Servicio del REGISTRO). Consulte la guia del usuario para mas detalles.

5 DMZ

La Zona DesMilitarizada (DeMilitarized Zone - DMZ) permite a los servidores públicos (web, correo electrónico, FTP, etc.) estar visibles al mundo exterior teniendo aún protección de cortafuegos contra ataques DoS (Denial of Service -Denegación de Servicio).

Puede asignar la configuración TCP/IP a través de DHCP para los ordenadores conectados a los puertos DMZ. O bien, configure los ordenadores con direcciones IP estáticas (en la misma subred que la dirección IP del puerto DMZ) y direcciones del servidor DNS. Use la dirección IP del ZyWALL como puerta de enlace predeterminada.

Realice lo siguiente para configurar la DMZ si el ZyWALL está en modo de enrutamiento.

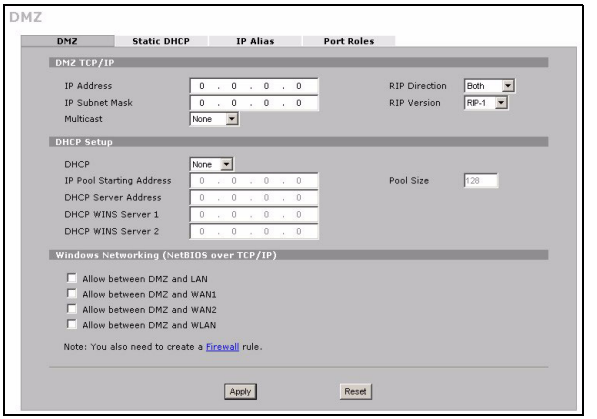
No necesita configurar la DMZ con modo puente, vaya a Sección 7.

1 Haga clic en **NETWORK** (RED) > **DMZ** en el panel de navegación.

2 Especifique una dirección IP y máscara de subred para la interfaz DMZ.

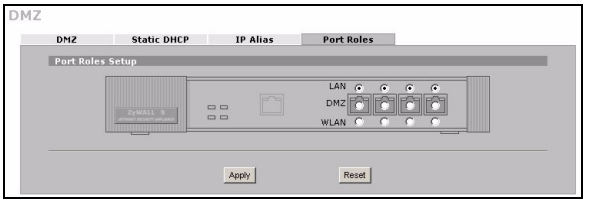
Si usa direcciones IP privadas en la DMZ, use NAT para hacer a los servidores accesibles públicamente (ver Sección 6).

Una dirección IP pública debe estar en una subred separada de las direcciones IP públicas de los puertos WAN. Si no configura NAT para las direcciones IP públicas en la DMZ, el ZyWALL enruta el tráfico a las direcciones IP públicas de la DMZ sin realizar la NAT. Esto puede resultar útil para albergar servidores para aplicaciones hostiles NAT.



3 Haga clic en **Apply** (Aplicar).

4 Por defecto, los puertos **LAN/DMZ** (del 1 al 4) son todos puertos LAN. Para configurar un puerto como puerto DMZ, haga clic en la pestaña **Port Roles** (Función de los puertos), seleccione el botón circular junto a **DMZ** y haga clic en **Apply** (Aplicar).

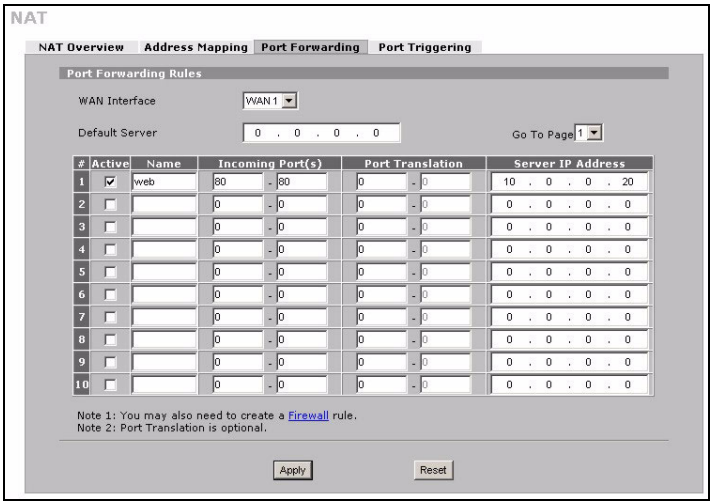


6 NAT

NAT (Network Address Translation (Traducción de Direcciones de Redes) - NAT, RFC 1631) significa la traducción de una dirección IP en una red a una dirección IP diferente en otra. Puede usar las pantallas de **NAT Address Mapping (mapeo de direcciones NAT)** para que el ZyWALL traduzca múltiples direcciones IP públicas a múltiples direcciones IP privadas en su LAN (o DMZ).

El siguiente ejemplo permite el acceso desde la WAN1 a un servidor HTTP (web) en la DMZ. El servidor tiene una dirección IP privada de 10.0.0.20.

1 Haga clic en **ADVANCED** (AVANZADA) > **NAT** en el panel de navegación y luego en **Port Forwarding** (Reenvío de puerto).
2 Seleccione la conexión WAN (**WAN1**) para la que desea configurar las normas de reenvío de puertos.
3 Seleccione la casilla de verificación **Active** (Activa).
4 Escriba un nombre para la regla.
5 Escriba el número que el servicio usa.
6 Escriba la dirección IP del servidor HTTP.
7 Haga clic en **Apply** (Aplicar).



7 Cortafuegos

Puede usar el ZyWALL sin configurar el cortafuegos.

El cortafuegos del ZyWALL está preconfigurado para proteger su LAN de ataques desde Internet. Por defecto, no puede entrar ningún tráfico en su LAN a menos que se haya generado una petición en la LAN antes. El ZyWALL permite el acceso a la DMZ desde la WAN o LAN, pero bloquea el tráfico de la DMZ a la LAN.

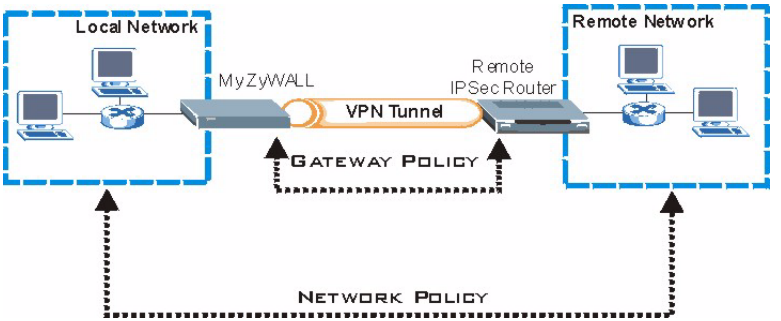
Si usa el ZyWALL en modo enrutador, continúe con la siguiente sección. Para el modo puente, vaya a Sección 9.

8 Configuración de reglas VPN

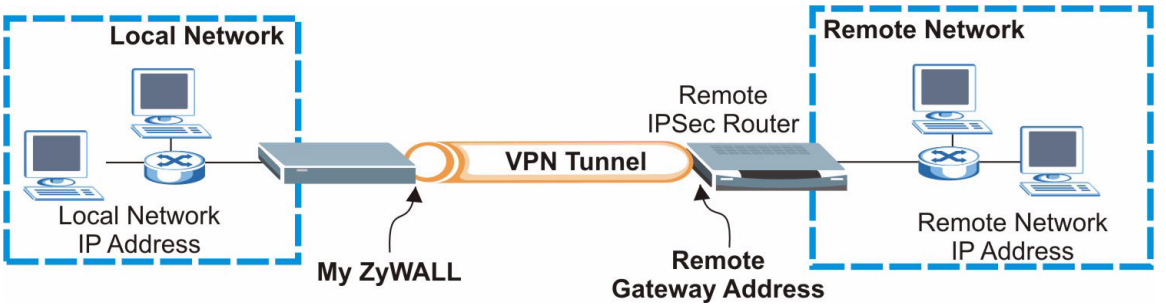
Un túnel VPN (Virtual Private Network - Red Privada Virtual) le ofrece una conexión segura a otro ordenador o red.

Una política de puerta de enlace identifica a los enrutadores IPSec en ambos extremos del túnel VPN.

Una política de red especifica qué dispositivos (detrás de los enrutadores IPSec) pueden usar el túnel VPN.



Esta figura ayuda a explicar los campos principales en las pantallas del asistente.



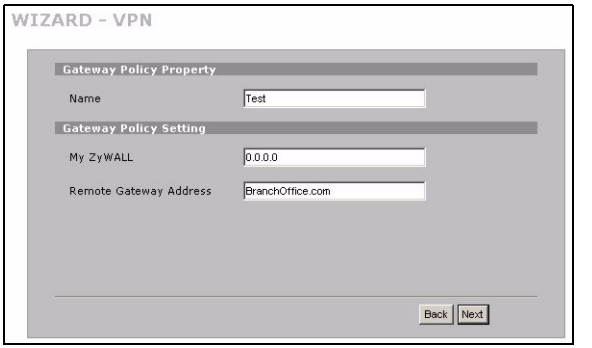
1 Haga clic en el icono **Wizard** (Asistente) ( ) en la pantalla **HOME** (INICIO) y luego en el enlace **VPN Setup** (Configuración VPN) para abrir el asistente VPN.

Su configuración no se grabará cuando haga clic en **Back** (Atrás).

2 Use esta pantalla para configurar la política de la puerta de enlace.

Name (Nombre): Introduzca un nombre para identificar la política de la puerta de enlace.

Remote Gateway Address (Dirección de puerta de enlace remota): Introduzca la dirección IP o nombre del dominio del enrutador IPSec remoto.



3 Use esta pantalla para configurar la política de la red.

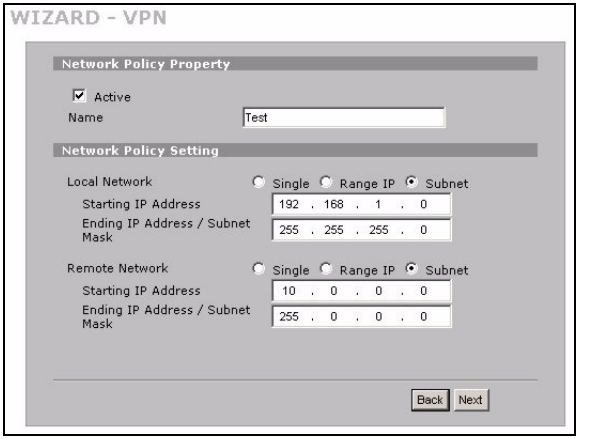
Deje la casilla de verificación **Active** (Activa) seleccionada.

Name (Nombre): Introduzca un nombre para identificar la política de la red.

Seleccione **Single** (Una) e introduzca la dirección IP para una única dirección IP.

Seleccione **Range IP** (Rango IP) e introduzca las direcciones IP inicial y final para un rango específico de direcciones IP.

Seleccione **Subnet** (Subred) e introduzca la dirección IP y la máscara de subred para especificar las direcciones IP en una red por su máscara de subred.



Compruebe que el enrutador IPSec usa la misma configuración de seguridad que la que configurará en las siguientes dos pantallas.

Negotiation Mode (Modo de negociación): Seleccione **Main Mode** (Modo principal) para la protección de la identidad. Seleccione **Aggressive Mode** (Modo agresivo) para permitir que más conexiones entrantes desde direcciones IP dinámicas usen contraseñas separadas.

SAs (asociaciones de seguridad) múltiples conectadas a través de una puerta de enlace segura deben tener el mismo modo de negociación.

Encryption Algorithm (Algoritmo de cifrado): Seleccione **3DES** o **AES** para un cifrado más fuerte (y más lento).

Authentication Algorithm (Algoritmo de autenticación): Seleccione **MD5** para una seguridad mínima o **SHA-1** para una mayor seguridad.

Key Group (Grupo de claves): Seleccione **DH2** para una mayor seguridad.

SA Life Time (Temporizador de SA): Ajuste la frecuencia con que ZyWALL negocia la IKE SA (mínimo 180 segundos). Una vida de SA corta aumenta la seguridad, pero la negociación desconecta temporalmente el túnel VPN.

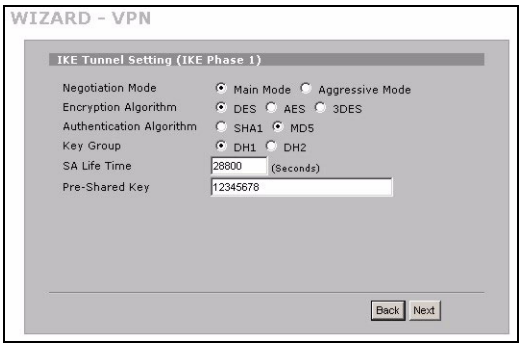
Pre-Shared Key (Clave pre-compartida): Use 8 a 31 caracteres ASCII sensibles a mayúsculas o 16 a 62 caracteres hexadecimales ("0-9", "A-F"). Precede una clave hexadecimal con un "0x" (cero x), que no cuenta como parte del rango de caracteres 16 a 62 para la clave.

Encapsulation Mode (Modo de encapsulación): **Tunnel** (Túnel) es compatible con NAT, **Transport** (Transporte) no lo es.

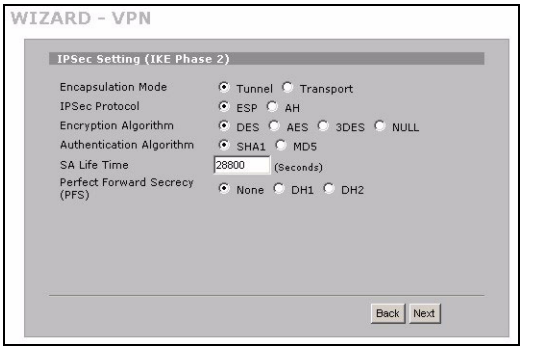
IPSec Protocol (Protocolo IPSec): **ESP** es compatible con NAT, **AH** no lo es.

Perfect Forward Secrecy (PFS): **None** (Ninguno) permite una configuración IPSec más rápida, pero **DH1** y **DH2** son el modo seguro.

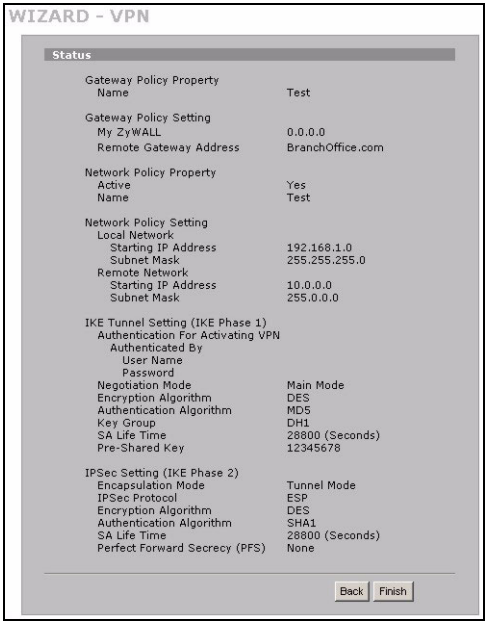
4 Use esta pantalla para establecer la configuración de túnel IKE (Internet Key Exchange - Intercambio de Claves de Internet).



5 Use esta pantalla para establecer la configuración IPSec.



6 Compruebe su configuración VPN. Haga clic en **Finish** (Finalizar) para guardar la configuración.

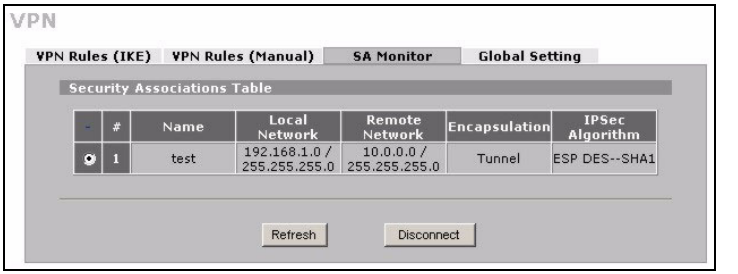


7 Haga clic en **Close** (Cerrar) en la pantalla final para completar la configuración del asistente para VPN. Continúe con la siguiente sección para activar la regla VPN y establecer una conexión VPN.

8.1 Usar la conexión VPN

Use túneles VPN para enviar y recibir archivos con seguridad y permitir el acceso remoto a redes corporativas, servidores de web y correo electrónico. Los servicios funcionan igual que si estuviese en la oficina en lugar de estar conectado a Internet.

Por ejemplo, la regla VPN “test” (prueba) permite un acceso seguro a un servidor web en una LAN corporativa remota. Introduzca la dirección IP del servidor (10.0.0.23 en este ejemplo) como URL en su explorador. El ZyWALL construye automáticamente un túnel VPN cuando intenta usarlo.



Haga clic en **SECURITY** (SEGURIDAD) > **VPN** en el panel de navegación y luego en la ficha **SA Monitor** (monitor SA) para mostrar una lista de los túneles VPN conectados (el túnel VPN “test” (prueba) está aquí).

9 Solución de problemas

Problema	Solución
Ninguno de los LEDs se enciende.	Asegúrese de haber conectado el adaptador de corriente al ZyWALL y si lo ha enchufado en una fuente de alimentación apropiada. Compruebe todas las conexiones de los cables.
	Si los LEDs todavía no se encienden, puede que tenga un problema de hardware. En este caso, debería contactar con su vendedor local.
No se puede acceder al ZyWALL desde la LAN.	Compruebe la conexión de cables entre el ZyWALL y su ordenador o hub. Consulte Sección 1 para más detalles.
	Realice un ping al ZyWALL desde un ordenador LAN. Compruebe que la tarjeta Ethernet de su ordenador esté instalada y funcione correctamente. En el ordenador, haga clic en **Inicio**, (**Todos los) programas**, **Accesorios** y luego en **Símbolo del sistema**. En la ventana del **Símbolo del sistema**, escriba "ping" seguido por la dirección IP LAN del ZyWALL (192.168.1.1 es la predeterminada) y pulse [ENTRAR]. El ZyWALL debería responder. En caso contrario, consulte Sección 9.1.
	Si ha olvidado la contraseña del ZyWALL, use el botón **RESET** . Mantenga pulsado el botón durante unos 10 segundos (o hasta que el LED **SYS** comience a parpadear), a continuación suéltelo. Esto devolverá al ZyWALL la configuración predeterminada de fábrica (la contraseña es 1234, dirección IP LAN 192.168.1.1 etc.; vea la Guía del usuario para más detalles).
	Si ha olvidado la dirección IP LAN o WAN del ZyWALL puede comprobar la dirección IP en la SMT a través del puerto consola SMT. Conecte su ordenador al puerto **CONSOLE** (Consola) usando un cable de consola. Su ordenador debería tener un programa de comunicaciones de emulación de terminales (como HyperTerminal) ajustado a la emulación del terminal VT100, sin paridad, 8 bits de datos, 1 bit de parada, sin flujo de control y una velocidad de puerto de 9600 bps.
No puedo acceder a Internet.	Compruebe la conexión del ZyWALL a la clavija Ethernet con acceso a Internet. Compruebe si el dispositivo de puerta de enlace de Internet (como un módem DSL) funciona correctamente.
	Haga clic en **WAN** en el panel de navegación para verificar su configuración.
No puedo establecer una conexión VPN.	Compruebe si el ZyWALL y el enrutador IPSec usan la misma configuración VPN. Haga clic en **VPN** en el panel de navegación para establecer la configuración avanzada.
	Acceda a un sitio web para comprobar si tiene una conexión a Internet correcta.

9.1 Configurar la dirección IP de su ordenador

Esta sección le explica cómo configurar su ordenador para recibir una dirección IP en Windows 2000, Windows NT y Windows XP. Esto asegura que su ordenador pueda conectarse con su ZyWALL.

1 En Windows XP, haga clic en **Inicio**, **Panel de control**.

En Windows 2000/NT, haga clic en **Inicio**, **Configuración**, **Panel de control**.

2 En Windows XP, haga clic en **Conexiones de red**.

En Windows 2000/NT, haga clic en **Conexiones de red y marcación**.

3 Haga clic con el botón derecho en **Conexión de área local** y haga clic en **Propiedades**.

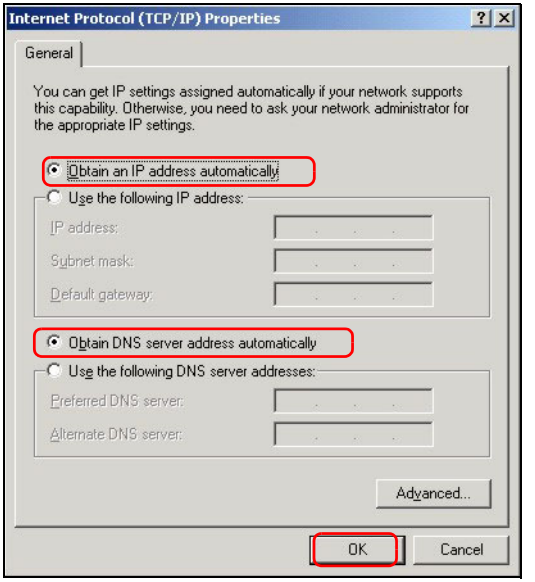
4 Seleccione **Protocolo Internet (TCP/IP)** (en la ficha **General** en Windows XP) y haga clic en **Propiedades**.

5 Se abrirá la pantalla **Propiedades de Protocolo Internet TCP/IP** (la ficha **General** en Windows XP). Seleccione las opciones **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente**.

6 Haga clic en **Aceptar** para cerrar la ventana **Propiedades de Protocolo Internet (TCP/IP)**.

7 Haga clic en **Cerrar** (**Aceptar** en Windows 2000/NT) para cerrar la ventana **Propiedades de conexión de área local**.

8 Cierre la pantalla **Conexiones de red**.



Procedimiento para ver la(s) certificación(es) del producto

1 Vaya a www.zyxel.com.

2 Seleccione su producto de la lista desplegable en la página inicial de ZyXEL para ir a la página de ese producto.

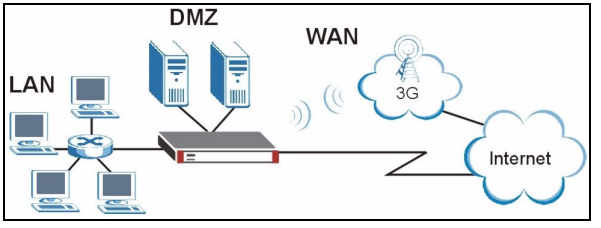
3 Seleccione la certificación que desee visualizar en esta página.

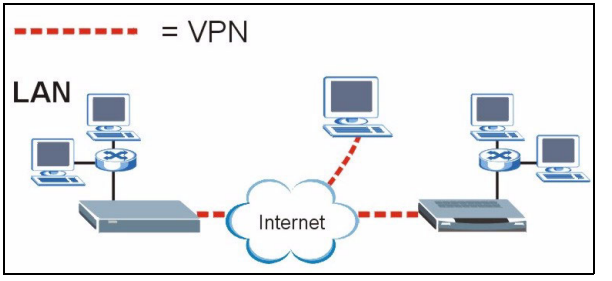
Présentation

Le ZyWALL 5 est un pare-feu avec VPN, gestion de bande passante, filtrage de contenu, antispam, antivirus, détection et protection contre les intrusions (IDP) et de nombreuses autres fonctionnalités. Vous pouvez l'utiliser comme un pare-feu transparent et ne pas reconfigurer votre réseau ni configurer les fonctionnalités de routage du ZyWALL. Quand le ZyWALL est en mode routeur, vous avez aussi la possibilité d'insérer une carte sans fil 3G pour ajouter un second WAN. Le ZyWALL améliore la sécurité du réseau grâce à la possibilité de changer les rôles des ports LAN en DMZ pour utiliser avec des serveurs accessibles au public. Ce guide couvre les connexions initiales et la configuration nécessaire pour commencer à utiliser le ZyWALL dans votre réseau.

Voir le Guide de l'utilisateur pour plus d'informations sur toutes les fonctionnalités.

Vous aurez peut-être besoin de vos informations d'accès à Internet.





Ce guide est divisé en sections comme suit.

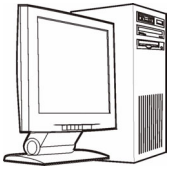
1 Connexions matérielles
2 Accéder au Configurateur Web
3 Mode Pont
4 Installation de l'accès à Internet et inscription du produit
5 DMZ
6 NAT
7 Pare-feu
8 Installation de la règle VPN
9 Dépannage

1 Connexions matérielles

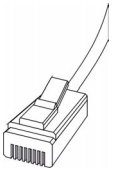
Vous avez besoin des éléments suivants.

ZyWALL

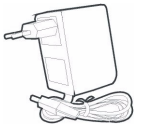
Ordinateur



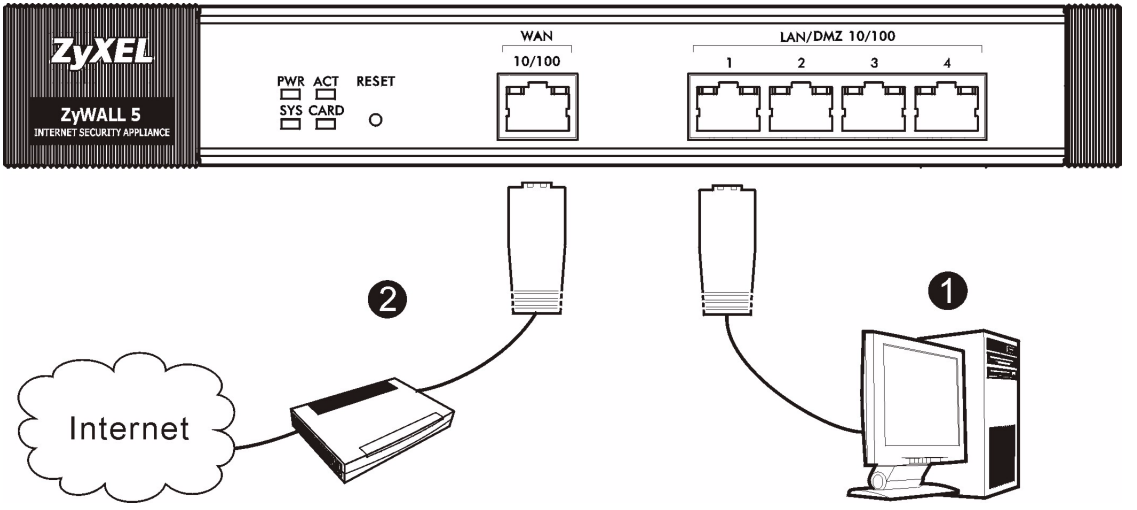
Câbles Ethernet



Adaptateur d'alimentation

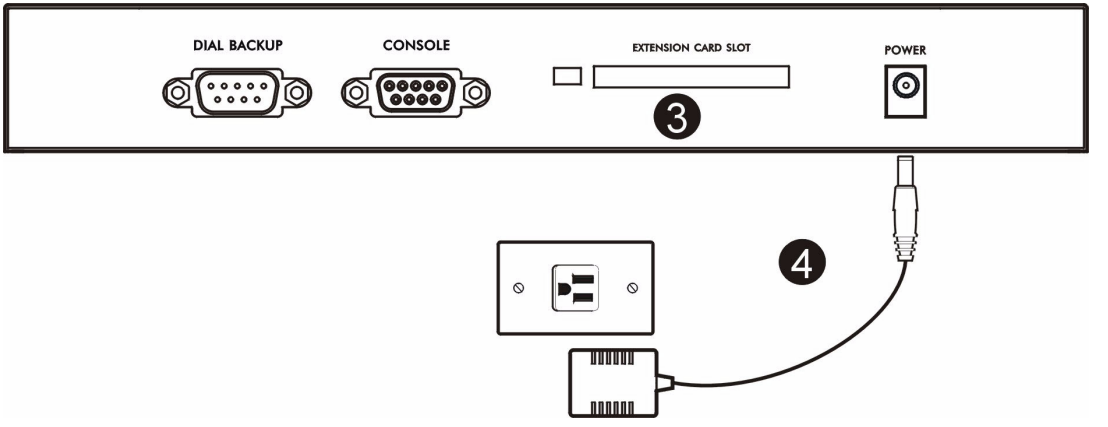


Procédez comme suit pour effectuer les connexions matérielles pour l'installation initiale.



1 Utilisez un câble Ethernet pour connecter le port **LAN/DMZ** à un ordinateur. Si vous configurez ces ports en ports **DMZ** dans l'écran **LAN** ou **DMZ** à l'aide du configurateur web, vous pouvez aussi utiliser les câbles Ethernet pour connecter les serveurs publics (web, e-mail, FTP, etc.) aux ports **LAN/DMZ**.

2 Utilisez un autre (ou d'autres) câble Ethernet pour connecter le port **WAN** à une prise Ethernet avec accès à Internet.



3 Insérez la carte d'extension ZyWALL Turbo pour utiliser les fonctionnalités antivirus et IDP ou insérez une carte LAN sans fil pour utiliser la fonctionnalité LAN sans fil. Vous pouvez aussi insérer une carte sans fil 3G pour accéder à l'Internet sans fil via un réseau 3G. Voir le guide de ZyWALL Turbo Card pour plus d'informations sur la carte d'extension. Voir le guide de l'utilisateur concernant l'installation d'une carte LAN sans fil. Pour l'instant, vous pouvez utiliser une carte 3G Sierra AC850/860 dans le ZyWALL.

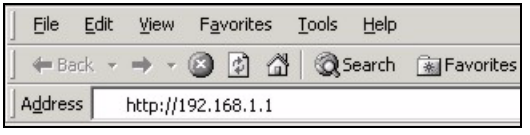
4 Utilisez le adaptateur d'alimentation pour connecter la prise d'alimentation (sur le panneau arrière) à une prise de courant.

5 Regardez le panneau avant. La LED **PWR** s'allume. La LED **SYS** clignote lors du test du système et reste ensuite allumée si le test a réussi. Les LED **ACT**, **CARD**, **LAN**/**DMZ**, et **WAN** s'allument et restent allumées si les connexions correspondantes sont effectuées correctement.

2 Accéder au Configurateur Web

Utilisez cette section pour configurer l'interface **WAN 1** pour l'accès à Internet.

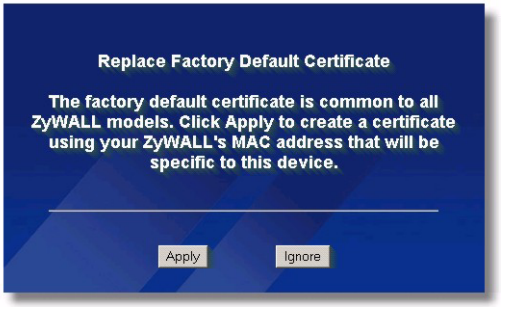
1 Lancez votre navigateur web. Entrez **192.168.1.1** (l'adresse IP par défaut du ZyWALL) comme adresse.
Si l'écran de connexion n'apparaît pas, voyez la Section 9.1 comment définir l'adresse IP de votre ordinateur.



2 Cliquez sur **Login** (Ouverture de session) (le mot de passe par défaut 1234 est déjà entré).

3 Changez le mot de passe d'ouverture de session en entrant un nouveau mot de passe et cliquez sur **Apply** (Appliquer).

4 Cliquez sur **Apply** (Appliquer) pour remplacer le certificat numérique par défaut du ZyWALL.



5 L'écran **HOME** (ACCUEIL) s'ouvre.

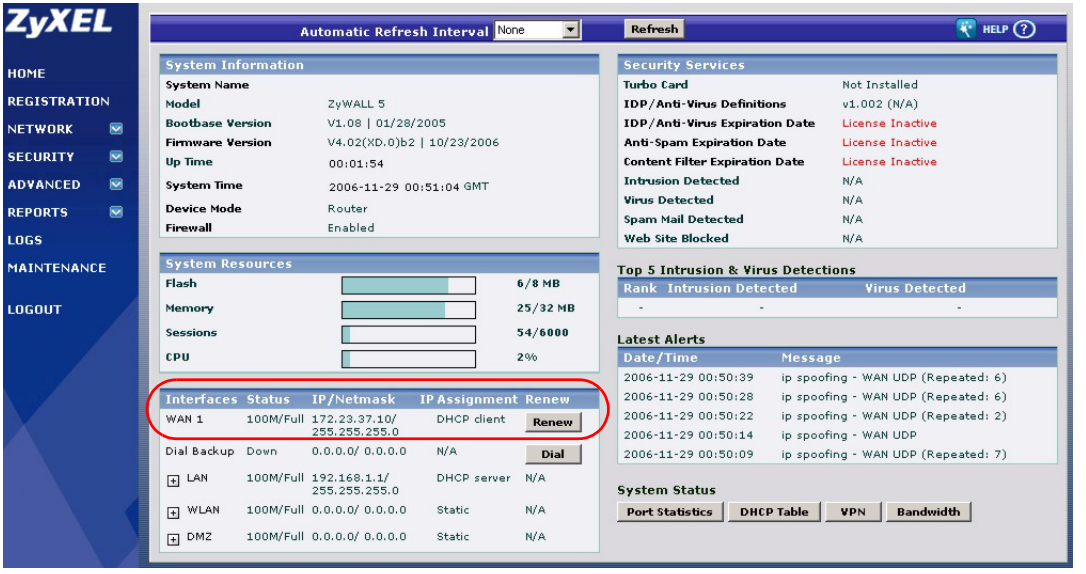
Par défaut, le ZyWALL est en mode routeur. Suivez l'étape suivante si vous voulez utiliser les fonctionnalités de routage telles que NAT, DHCP et VPN.

Allez à la Section 3 si vous préférez utiliser le ZyWALL comme un pare-feu transparent.

6 Reportez-vous au tableau d'network status (Etat du Réseau). Si l'état **WAN 1** n'est *pas* **Down** (Désactivé) et qu'il y a une adresse IP, allez à la Section 5.

Si l'état **WAN 1** est **Down** (Désactivé) (ou qu'il n'y a pas d'adresse IP), cliquez sur l'icône **Wizard** (Assistant) et utilisez la Section 4 pour configurer **WAN 1**.

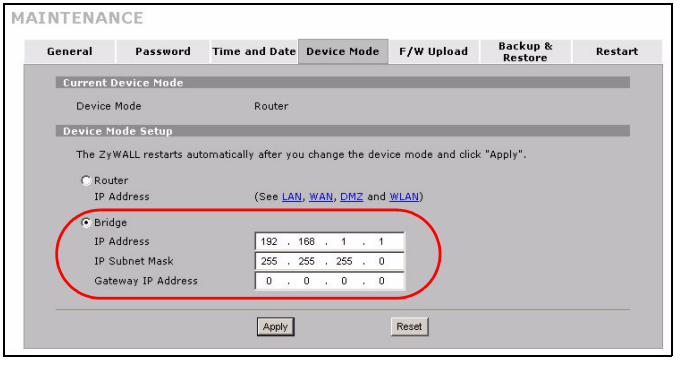
Utilisez les écrans **NETWORK/WAN** si vous devez configurer **WAN 2**. Vous pouvez aussi configurer l'équilibrage de charge entre les connexions WAN.



3 Mode Pont

Quand vous paramétrez le ZyWALL en mode pont, il fonctionne comme un pare-feu transparent. Procédez comme suit pour paramétrer le ZyWALL en mode pont.

1. Cliquez sur **MAINTENANCE** dans le panneau de navigation et ensuite sur le **Device Mode** (Mode Périphérique).
2. Sélectionnez **Bridge** (Pont) et configurez une d'adresse IP (statique) de masque de sous-réseau et une adresse IP de passerelle pour les interfaces **LAN**, **WAN**, **DMZ** et **WLAN** du ZyWALL.
3. Cliquez sur **Apply** (Appliquer). Le ZyWALL redémarre.



Passez à la Section 5 si vous avez des serveurs qui doivent être accessibles à partir du WAN.

4 Installation de l'accès à Internet et inscription du produit

1 Cliquez sur l'icône ( ) **Wizard** (Assistant) dans l'écran **HOME** (ACCUEIL) et ensuite sur le lien **Internet Access Setup** (Installation de l'accès à Internet) pour ouvrir l'assistant d'accès à Internet.

Entrez les informations d'accès à Internet exactement telles qu'elles vous ont été fournies.

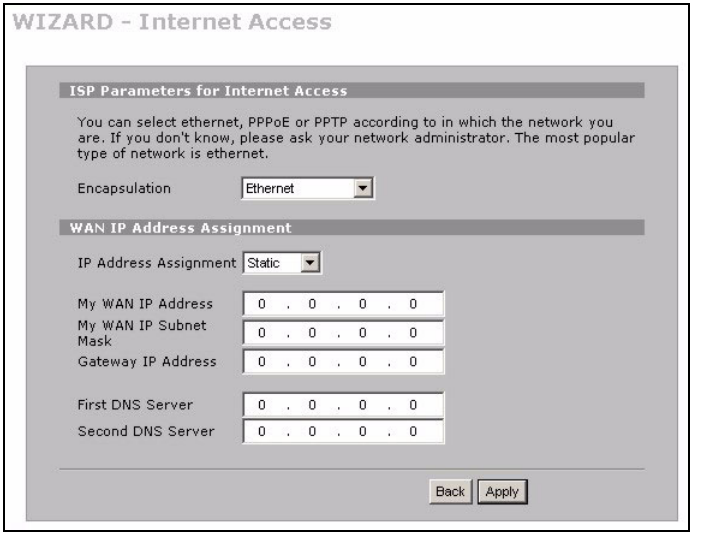
Si vous avez reçu une adresse IP à utiliser, sélectionnez **Static** (Statique) dans la boîte de la liste déroulante d'**IP Address Assignment** (Attribution d'adresse IP) et saisissez les informations fournies.

Les champs varient en fonction de ce que vous sélectionnez dans le champ **Encapsulation**. Remplissez-les avec les informations fournies par l'ISP ou l'administrateur réseau.

Cliquez sur **Finish** (Terminer) quand vous avez terminé.

- **Encapsulation Ethernet**

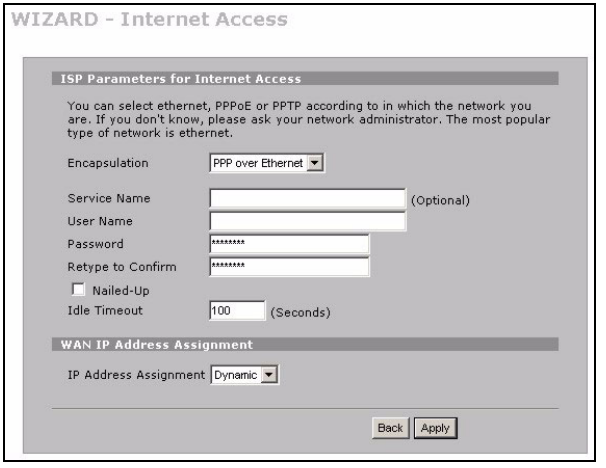
Configurer un service Roadrunner dans les écrans du **NETWORK WAN** (utilisez l'onglet **WAN**).

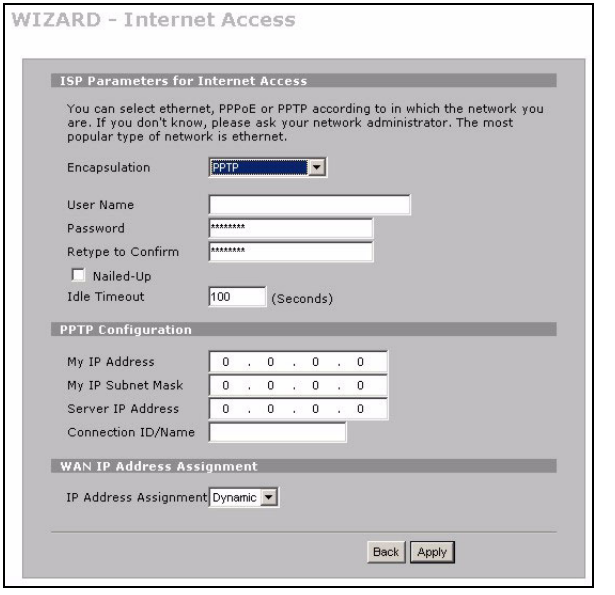


- **PPP over Ethernet ou PPTP Encapsulation**

Sélectionnez **Nailed-Up** quand vous voulez que votre connexion soit toujours active (cela peut être cher si votre ISP vous facture pour votre temps d'utilisation à la place d'un abonnement mensuel).

Pour ne pas avoir la connexion constamment active, spécifiez un délai d'inactivité (en secondes) dans **Idle Timeout** (Délai d'inactivité).



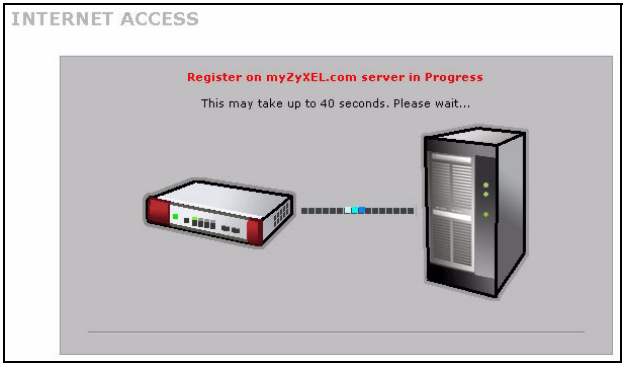


2 Cliquez sur **Next** (Suivant) pour afficher l'écran où vous pourrez inscrire votre ZyXEL sur MyZyXEL.com (Centre de services en ligne de ZyXEL) et activer les applications d'évaluation gratuites de filtrage de contenu, antispam, antivirus et IDP. Vous pouvez aussi cliquer sur **Skip** (Passer) et ensuite sur **Close** (Fermer) pour terminer l'installation de l'accès à Internet.

Vérifiez que vous avez installé le ZyWALL Turbo Card avant d'activer les services d'abonnement IDP et antivirus.
Eteignez le ZyWALL avant d'installer ou de retirer le ZyWALL Turbo Card.

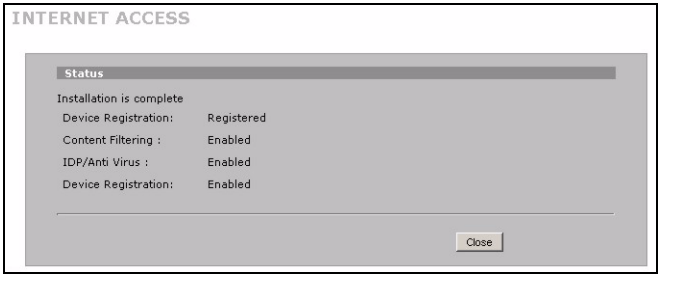
3 Si vous avez déjà un compte sur myZyXEL.com, sélectionnez **Existing myZyXEL.com account** (Quitter mon compte myZyXEL.com) et entrer les informations du compte. Vous pouvez aussi sélectionner **New myZyXEL.com account** (Nouveau compte myZyXEL.com) et remplir les champs ci-dessous pour créer un compte et enregistrer votre ZyWALL. Cliquez sur **Next** (Suivant).

4 Attendez que l'enregistrement soit terminé.



5 Les écrans suivants s'affichent si l'enregistrement a échoué. Cliquez sur **Return** (Retour) pour retourner à l'écran **Device Registration** (Inscription matériel) et vérifier vos paramètres.

6 Cliquez sur **Close** (Fermer) pour quitter l'assistant quand l'inscription et l'action sont effectuées.



Si vous voulez activer un service standard avec le numéro PIN de votre iCard (clé de licence), utilisez l'écran de **REGISTRATION Service** (Service d'INSCRIPTION). Voir le guide de l'utilisateur pour les détails.

5 DMZ

La Zone Démilitarisée (DMZ) permet aux serveurs publics (web, e-mail, FTP, etc.) d'être visible au monde extérieur et avoir cependant une protection pare-feu contre les attaques DoS (Denial of Service).

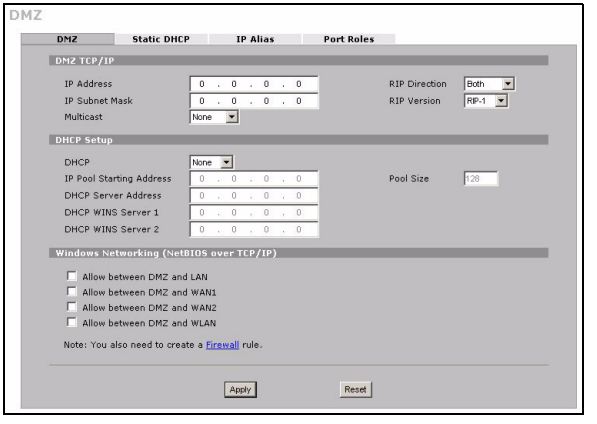
Vous pouvez attribuer la configuration TCP/IP via DHCP aux ordinateurs connectés aux ports DMZ. Autrement, configurez les ordinateurs avec des adresses IP statiques (dans le même sous-réseau que les adresses IP des ports DMZ) et les adresses de serveur DNS. Utilisez l'adresse IP DMZ du ZyWALL comme passerelle par défaut.

Procédez comme suit pour configurer le DMZ si le ZyWALL est en mode routage.

Vous n'avez pas besoin de configurer DMZ avec le mode pont, sautez à la Section 7.

1 Cliquez **NETWORK** (RÉSEAU) > **DMZ** dans le panneau de navigation.

2 Spécifiez une adresse IP et un masque de sous-réseau pour l'interface DMZ.

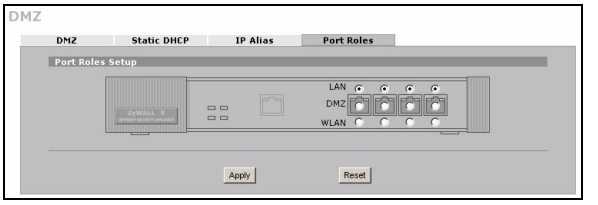


Si vous utilisez des adresses IP privées sur le DMZ, utilisez NAT pour rendre les serveurs accessibles au public (voir la Section 6).

Une adresse IP publique doit se trouver sur un sous-réseau séparé de l'adresse IP publique du port WAN. Si vous ne configurez pas NAT pour les adresses IP publiques sur le DMZ, le ZyWALL dirige le trafic vers les adresses IP publiques sur le DMZ sans effectuer de NAT. Cela peut être utile pour héberger des serveurs pour des applications non conviviales avec NAT.

3 Cliquez sur **Apply** (Appliquer).

4 Par défaut, les ports **LAN/DMZ** 1 à 4 sont tous des ports LAN. Pour configurer un port en port DMZ, cliquez sur l'onglet de **Port Roles** (Rôle des Ports), sélectionnez la case à côté de **DMZ** et cliquez sur **Apply** (Appliquer).



6 NAT

NAT (Network Address Translation - NAT, RFC 1631) permet la conversion d'un adresse IP dans un réseau en une adresse IP différente dans un autre. Vous pouvez utiliser les écrans de **NAT Address Mapping** (Mappage d'Adresse NAT) pour que le ZyWALL convertisse plusieurs adresses IP publiques en plusieurs adresses IP privées sur votre LAN (ou DMZ).

L'exemple suivant permet l'accès depuis le WAN1 à un serveur HTTP (web) sur le DMZ. Le serveur possède une adresse IP privée de 10.0.0.20.

1 Cliquez sur **ADVANCED** (AVANCÉ) > **NAT** dans le panneau de navigation et ensuite sur **Port Forwarding** (Réacheminement de Port).

2 Sélectionnez la connexion WAN (**WAN1**) pour laquelle vous voulez configurer les règles de réacheminement de port.

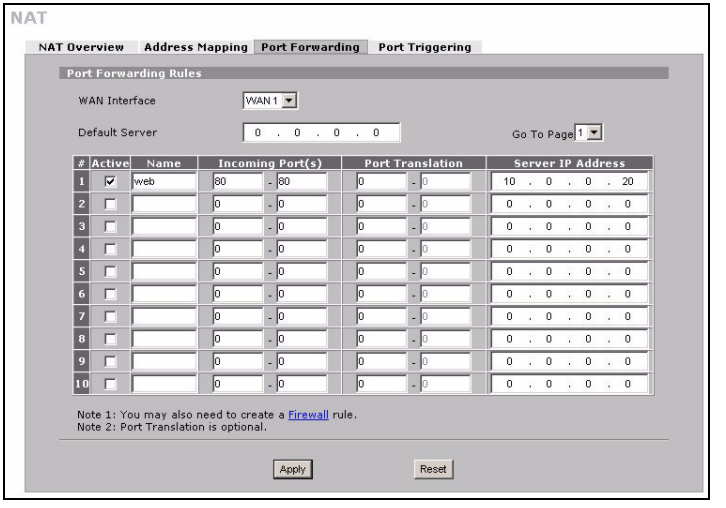
3 Sélectionnez la case à cocher **Active**.

4 Tapez un nom pour la règle.

5 Tapez le numéro de port que le service utilise.

6 Tapez l'adresse IP du serveur HTTP.

7 Cliquez sur **Apply (**Appliquer).



7 Pare-feu

Vous pouvez utiliser le ZyWALL sans configurer le pare-feu.

Le pare-feu du ZyWALL est préconfiguré pour protéger votre LAN contre les attaques provenant d'Internet. Par défaut, aucun trafic ne peut pénétrer dans votre LAN à moins qu'une requête ne soit tout d'abord générée sur le LAN. Le ZyWALL permet l'accès au DMZ depuis le WAN ou LAN, mais bloque le trafic provenant du DMZvers le LAN.

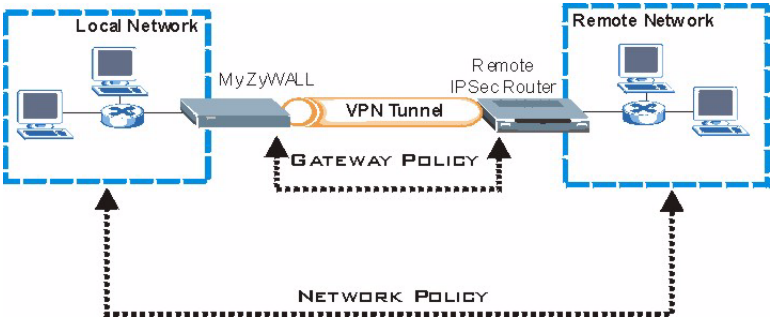
Si vous utilisez le ZyWALL en mode routeur, suivez la section suivante. Pour le mode pont, passez à la Section 9.

8 Installation de la règle VPN

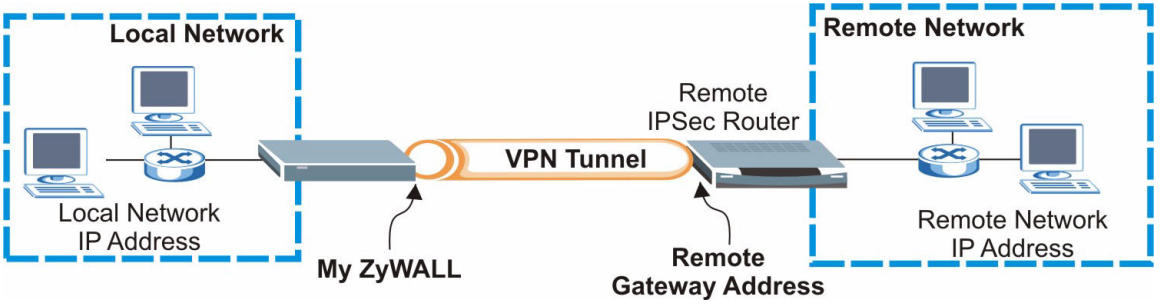
Un tunnel VPN (Virtual Private Network) vous offre une connexion sécurisée à un autre ordinateur ou réseau.

Une stratégie de passerelle identifie les routeurs IPSec aux extrémités d'un tunnel VPN.

Une stratégie de réseau spécifie les périphériques (derrière les routeurs IPSec) pouvant utiliser le tunnel VPN.



Cette figure aide à expliquer les champs principaux dans les écrans de l'assistant.



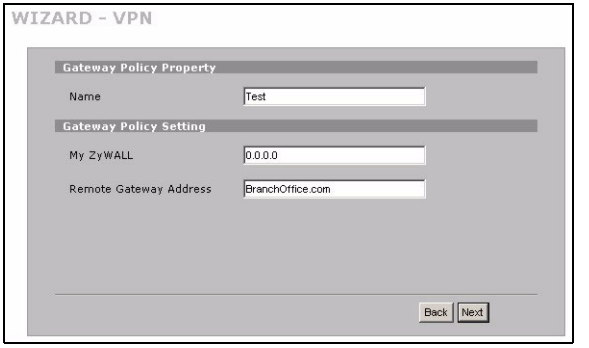
1 Cliquez sur l'icône ( ) **Wizard** (Assistant) dans l'écran **HOME** (ACCUEIL) et ensuite sur le lien **VPN Setup** (Installation du VPN) pour ouvrir l'assistant du VPN.

Vos paramètres ne sont pas enregistrés quand vous cliquez sur **Back** (Retour).

2 Utilisez cet écran pour configurer la stratégie de passerelle.

Name (Nom): Entrez un nom pour identifier la stratégie de passerelle.

Remote Gateway Address (Adresse de passerelle distante): Entrez l'adresse IP ou le nom de domaine du routeur IPSec distant.



3 Utilisez cet écran pour configurer la stratégie de réseau.

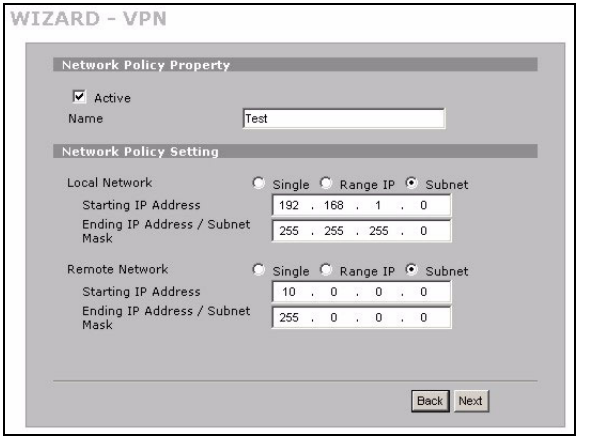
Laissez la case à cocher **Active** sélectionnée.

Name (Nom): Entrez un nom pour identifier la stratégie de réseau.

Sélectionnez **Single** (Unique) et entrez une adresse IP pour une adresse IP unique.

Sélectionnez **Range IP** (Plage d'IP) et saisissez les adresses IP de début et de fin pour une plage d'adresses IP spécifique.

Sélectionnez **Subnet** (Sous-réseau) et saisissez une adresse IP et un masque de sous-réseau pour spécifier les adresses IP sur le réseau par leur masque de sous-réseau.



Vérifiez que le routeur IPSec distant utilise les mêmes paramètres de sécurité que ceux que vous configurez dans les deux écrans suivants.

Negotiation Mode (Mode de négociation): Sélectionnez **Main Mode** (Mode Principal) pour la protection d'identité. Sélectionnez le **Aggressive Mode** (Mode Agressif) pour permettre à plus de connexions entrantes à partir des adresses IP dynamiques d'utiliser des mots de passe séparés.

Plusieurs SAs (associations de sécurité) se connectant via une passerelle de sécurité doivent avoir le même mode de négociation.

Encryption Algorithm (Algorithme de cryptage): Sélectionnez **3DES** ou **AES** pour bénéficier d'un cryptage plus puissant (et plus lent).

Authentication Algorithm (Algorithme d'authentification): Sélectionnez **MD5** pour la sécurité minimale ou **SHA-1** pour une sécurité plus élevée.

Key Group (Groupe de clés): Sélectionnez **DH2** pour avoir une sécurité plus élevée.

SA Life Time (Durée de vie SA): Définissez la fréquence à laquelle le ZyWALL renégocie l'IKE SA (minimum 180 secondes). Une durée de vie de SA courte augmente la sécurité, mais la renégociation déconnecte temporairement le tunnel VPN.

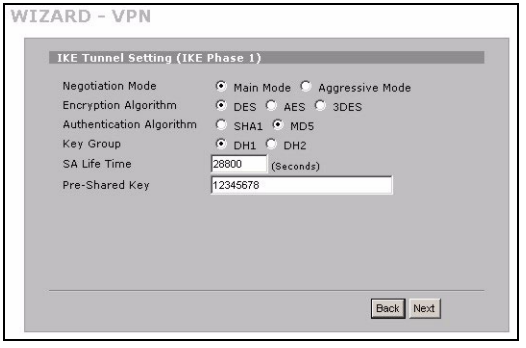
Pre-Shared Key (Clé prépartagée): Utilisez 8 à 31 caractères ASCII sensibles à la casse ou 16 à 62 caractères hexadécimaux ("0-9", "A-F"). Faites précéder une clé hexadécimale par un "0x" (zéro x), qui n'est pas compté comme faisant partie de la plage de 16 à 62 caractères pour la clé.

Encapsulation Mode (Mode d'encapsulation): **Tunnel** est compatible avec NAT, **Transport** ne l'est pas.

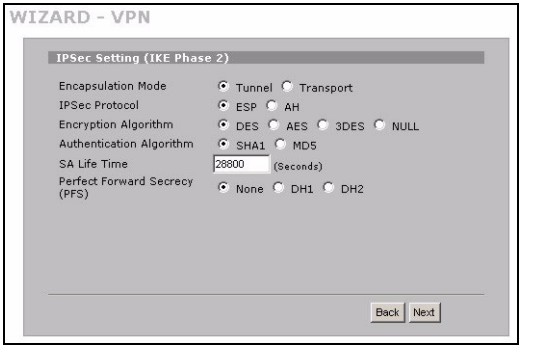
IPSec Protocol (Protocole IPSec): **ESP** est compatible avec NAT, **AH** ne l'est pas.

Perfect Forward Secrecy (Confidentialité de transmission parfaite) **(PFS)**: **None** (Aucune) permet une configuration IPSec plus rapide, mais **DH1** et **DH2** sont plus sécurisés.

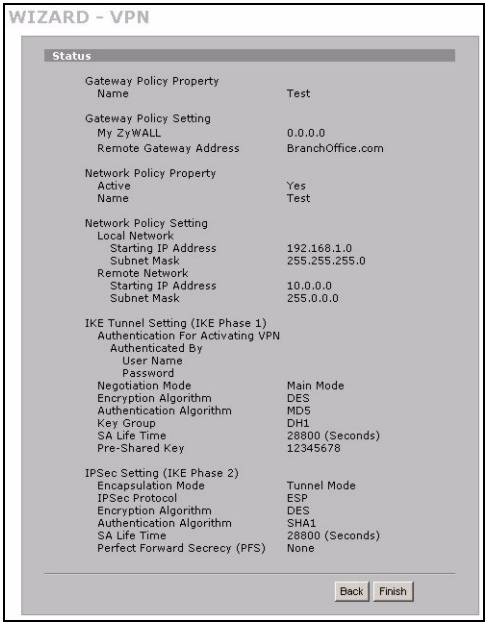
4 Utilisez cet écran pour configurer les paramètres IKE (Internet Key Exchange-Echange de clé Internet).



5 Utilisez cet écran pour configurer les paramètres IPSec.



6 Vérifiez vos paramètres VPN. Cliquer sur **Finish** (Terminer) pour enregistrer les paramètres.

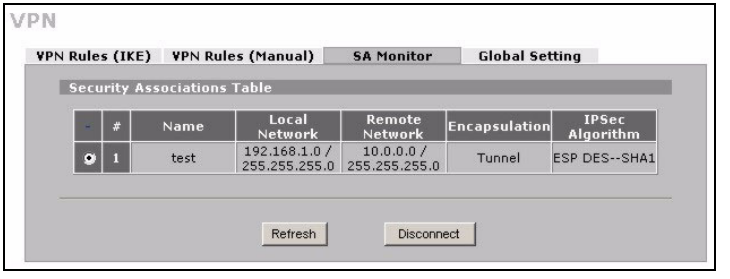


7 Cliquez sur **Close** (Fermer) dans l'écran final pour terminer l'installation de l'assistant de VPN. Suivez la section suivante pour activer la règle VPN et établir une connexion VPN.

8.1 Utiliser la Connexion VPN

Utilisez les tunnels VPN pour envoyer et recevoir de manière sécurisée, et permettre l'accès à distance aux réseaux d'entreprise, serveurs web et e-mail. Les services fonctionnent comme si vous étiez au bureau au lieu d'être connecté à Internet.

Par exemple, la règle VPN “test” permet un accès sécurisé à un serveur web sur un LAN d'entreprise distant . Entrez l'adresse IP du serveur (10.0.0.23 dans cet exemple) comme votre URL de navigateur. Le ZyWALL construit automatiquement le tunnel VPN quand vous tentez de l'utiliser.



Cliquez sur **SECURITY** (SÉCURITÉ) > **VPN** dans le panneau de navigation et ensuite sur l'onglet du **SA Monitor** (Moniteur SA) pour afficher une liste de tunnel VPN connectés (le tunnel VPN “test” est là).

9 Dépannage

Problème	Action Corrective
Aucune LED ne s'allume.	Vérifiez que votre adaptateur d'alimentation est connecté au ZyWALL et branché dans une prise de courant appropriée. Vérifiez toutes les connexions câblées.
	Si les LED ne s'allument toujours pas, cela signifie que vous avez peut-être un problème matériel. Dans ce cas-là, vous devez contacter votre revendeur local.
Impossible d'accéder au ZyWALL à partir du LAN.	Vérifiez la connexion câblée entre le ZyWALL et votre ordinateur ou hub. Reportez-vous à la Section 1 pour les détails.
	Envoyez un signal Ping au ZyWALL à partir d'un ordinateur du LAN. Vérifiez que la carte Ethernet de votre ordinateur est installée et fonctionne correctement. Dans l'ordinateur, cliquez sur **Start** (Démarrer), **(All** (Tous)**) Programs** (Programmes), **Accessories** (Accessoires) et ensuite sur **Command Prompt** (Invite de Commande). Dans la fenêtre **Command Prompt** (Invite de Commande), tapez "ping" suivi de l'adresse IP LAN du ZyWALL (192.168.1.1 est l'adresse par défaut) et appuyez ensuite sur [ENTER]. Le ZyWALL devrait répondre. Sinon, reportez-vous à la Section 9.1.
	Si vous avez oublié le mot de passe du ZyWALL, utilisez le bouton **RESET**. Appuyez sur le bouton pendant environ 10 secondes (jusqu'à ce que la LED **SYS** commence à clignoter), puis relâchez-le. Cela rétablit le ZyWALL à ses paramètres par défaut d'usine (le mot de passe est 1234, adresse IP LAN 192.168.1.1 etc.; voir votre Guide de l'utilisateur pour les détails).
	Si vous avez oublié l'adresse IP LAN ou WAN du ZyWALL, vous pouvez vérifier l'adresse IP dans le SMT via le port de la console. Connectez votre ordinateur au port **CONSOLE** à l'aide d'un câble de console. Votre ordinateur doit avoir un programme de communication d'émulation de terminal (tel qu'HyperTerminal) paramétré sur l'émulation de terminal VT100, pas de parité, 8 bits de données, 1 bit de stop, pas de contrôle de flux et une vitesse de port de 9600 bps.
Impossible d'accéder à Internet.	Vérifiez la connexion du ZyWALL à la prise Ethernet avec l'accès Internet. Vérifiez que le périphérique de passerelle Internet (tel qu'un modem DSL) fonctionne correctement.
	Cliquez sur **WAN** dans le panneau de navigation pour vérifier vos paramètres.
Impossible d'établir une connexion VPN.	Vérifiez que le ZyWALL et le routeur IPSec distant utilise les mêmes paramètres VPN. Cliquez sur **VPN** dans le panneau de navigation pour configurer les paramètres avancés.
	Accédez à un site web pour vérifier que vous avez une connexion Internet qui fonctionne.

9.1 Paramétrez l'adresse IP de votre ordinateur

Cette section vous indique comment paramétrer votre ordinateur pour recevoir une adresse IP dans Windows 2000, Windows NT et Windows XP. Cela permet à votre ordinateur de communiquer avec votre ZyWALL.

1 Dans Windows XP, cliquez sur **Start** (Démarrer), **Control Panel** (Panneau de configuration).

Dans Windows 2000/NT, cliquez sur **Strart** (Démarrer), **Settings** (Paramètres), **Control Panel** (Panneau de configuration).

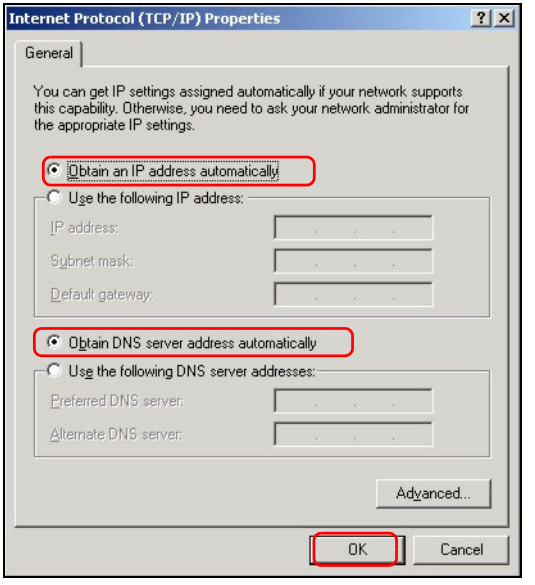
2 Dans Windows XP, cliquez sur **Network Connections** (Connexion réseau).

Dans Windows 2000/NT, cliquez sur **Network and Dial-up Connection** (Connexions réseau et accès à distance).

3 Cliquez avec le bouton droit de la souris sur **Local Area Connection** (Connexion de réseau local) et cliquez sur **Properties** (Propriétés).

4 Sélectionnez **Protocole Internet (TCP/IP)** (dans l'onglet **General** (Général) dans Windows XP) et cliquez sur **Properties** (Propriétés).

5 L'écran de **Propriétés TCP/IP de protocole Internet** s'ouvre (l'onglet **General** (Général) dans Windows XP). Sélectionnez les options **Obtain an IP address automatically** (Obtenir automatiquement une adresse IP) et **Obtain DNS server adress automatically** (Obtenir automatiquement une adresse de serveur DNS).



6 Cliquez sur **OK** pour fermer la fenêtre de **Internet protocol Properties** (Propriétés (TCP/IP) de protocole Internet).

7 Cliquez sur **Close** (Fermer) (**OK** dans Windows 2000/NT) pour fermer la fenêtre de **Local Area Connection Properties** (Propriétés de connexion au réseau local).

8 Fermez l'écran de **Network Connections** (Connexion réseau).

Procédure pour Afficher la (les) certification(s) d'un produit

1 Allez à www.zyxel.com.

2 Sélectionnez votre produit dans la boîte de la liste déroulante dans la page d'accueil de ZyXEL pour aller à la page de ce produit.

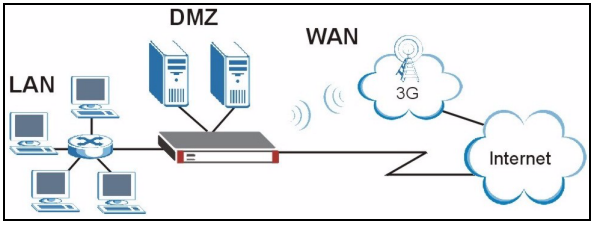
3 Sélectionnez la certification que vous désirez consulter dans cette page.

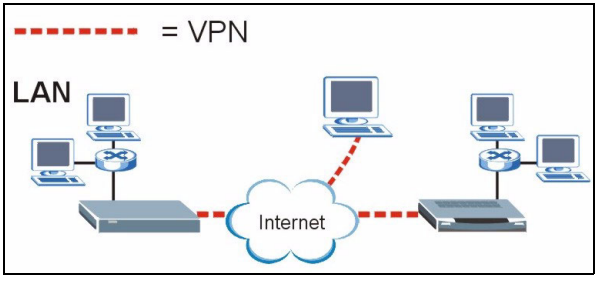
Cenni generali

ZyWALL 5 è un firewall con funzionalità di dotato di funzioni di VPN, gestione della larghezza di banda, filtraggio dei contenuti, antispam, antivirus, IDP (Intrusion Detection and Protection) e molto altro. È possibile utilizzarlo come firewall trasparente ed evitare di riconfigurare la propria rete e di configurare le funzionalità di routing dello ZyWALL. Quando lo ZyWALL è in modalità router, è anche possibile inserire una scheda wireless 3G per aggiungere una seconda WAN. ZyWALL aumenta la sicurezza della rete prevedendo la possibilità di variare le regole relative alle porte dalla LAN alla DMZ per l'uso di server accessibili pubblicamente. La presente guida illustra i collegamenti e la configurazione iniziale necessari per iniziare a utilizzare lo ZyWALL nella propria rete.

Vedere la Guida dell'utente per maggiori informazioni su tutte le funzioni.

È possibile che occorre reperire le informazioni sul proprio accesso a Internet.





Questa guida è suddivisa nelle seguenti sezioni:

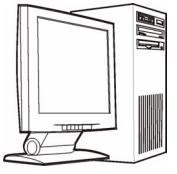
1 Collegamenti hardware
2 Accesso allo strumento di configurazione Web
3 Modalità Bridge
4 Configurazione dell'accesso a Internet e Registrazione del prodotto
5 DMZ
6 NAT
7 Firewall
8 Configurazione delle regole di VPN
9 Risoluzione dei problemi

1 Collegamenti hardware

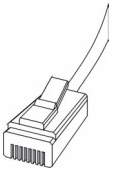
È necessario disporre dei seguenti componenti:

ZyWALL

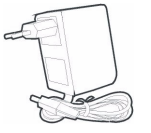
Computer



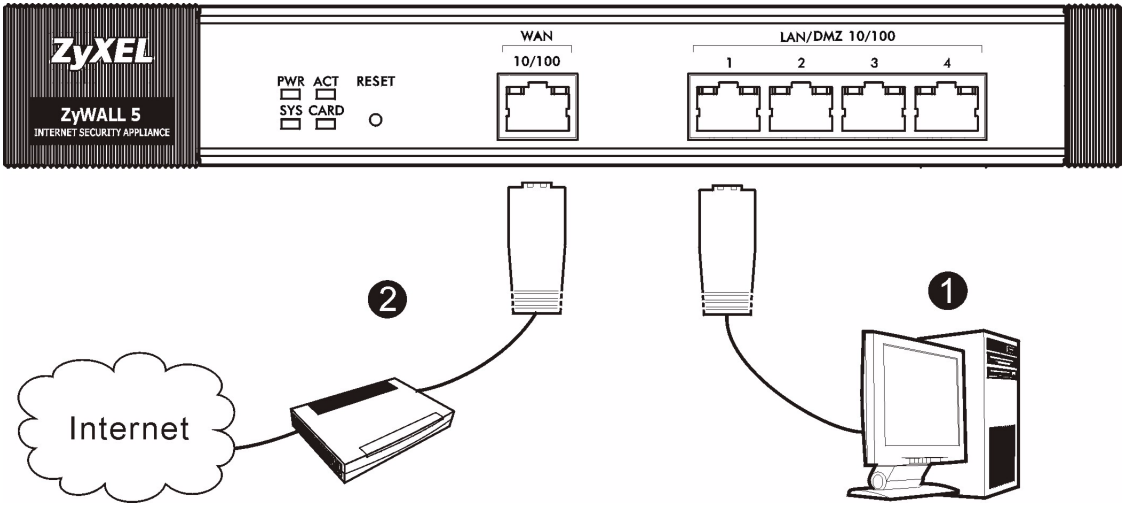
Cavi Ethernet



Adattatore di alimentazione

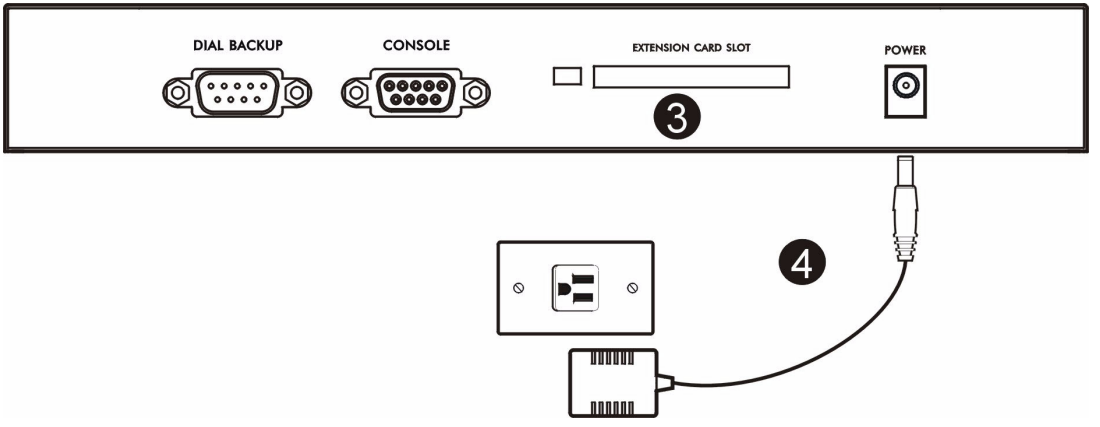


Di seguito sono illustrati i collegamenti hardware per l'installazione iniziale.



1 Utilizzare un cavo Ethernet per collegare la porta **LAN/DMZ** a un computer. Se si configurano queste porte come porte **DMZ** nelle schermate relative alla **LAN** o alla **DMZ** nello strumento di configurazione Web, è anche possibile utilizzare i cavi Ethernet per collegare server pubblici (Web, e-mail, FTP, ecc.) alle porte **LAN/DMZ**.

2 Utilizzare un cavo Ethernet per collegare la porta **WAN** a un jack Ethernet con accesso a Internet.



3 Inserire la scheda di espansione ZyWALL Turbo per utilizzare le funzionalità di antivirus e IDP (rilevazione e protezione dalle intrusioni) oppure inserire una scheda LAN wireless per utilizzare la funzionalità LAN. È in opzione possibile inserire una scheda wireless 3G per accedere a Internet senza fili tramite una rete 3G. Vedere la guida del ZyWALL Turbo Card per ulteriori informazioni sulla scheda di espansione. Vedere la

guida dell'utente per informazioni sull'installazione di una scheda LAN wireless. Nell'istante in cui scriviamo, è possibile utilizzare solo la scheda wireless Sierra AC850/860 3G nello ZyWALL.

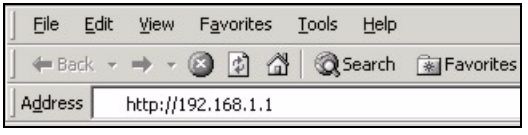
4 Utilizzare il adattatore di alimentazione fornito a corredo per collegare la presa di alimentazione (situata dietro all'apparecchio) a una presa elettrica.

5 Analizzare il pannello frontale. Il LED **PWR** si accende. Il LED **SYS** lampeggia mentre viene eseguito il test del sistema e quindi resta acceso in caso di test riuscito. I LED **ACT**, **CARD**, **LAN/DMZ** e **WAN** si accendono e restano accesi se i corrispondenti collegamenti sono stati eseguiti correttamente.

2 Accesso allo strumento di configurazione Web

Questa sezione spiega come configurare l'interfaccia **WAN 1** per l'accesso a Internet.

1 Avviare il browser. Immettere **192.168.1.1** (l'indirizzo IP predefinito dello ZyWALL) nella barra dell'indirizzo.
Se non viene visualizzata la schermata di accesso, vedere Sezione 9.1 per impostare l'indirizzo IP del proprio computer.



2 Fare clic su **Login** (accedi) (la password predefinita 1234 è già immessa).

3 Cambiare la password di accesso immettendo una nuova password e facendo clic su **Apply** (applica).

4 Fare clic su **Apply** (applica) per sostituire il certificato digitale predefinito dello ZyWALL.

5 Si apre la schermata **HOME**.

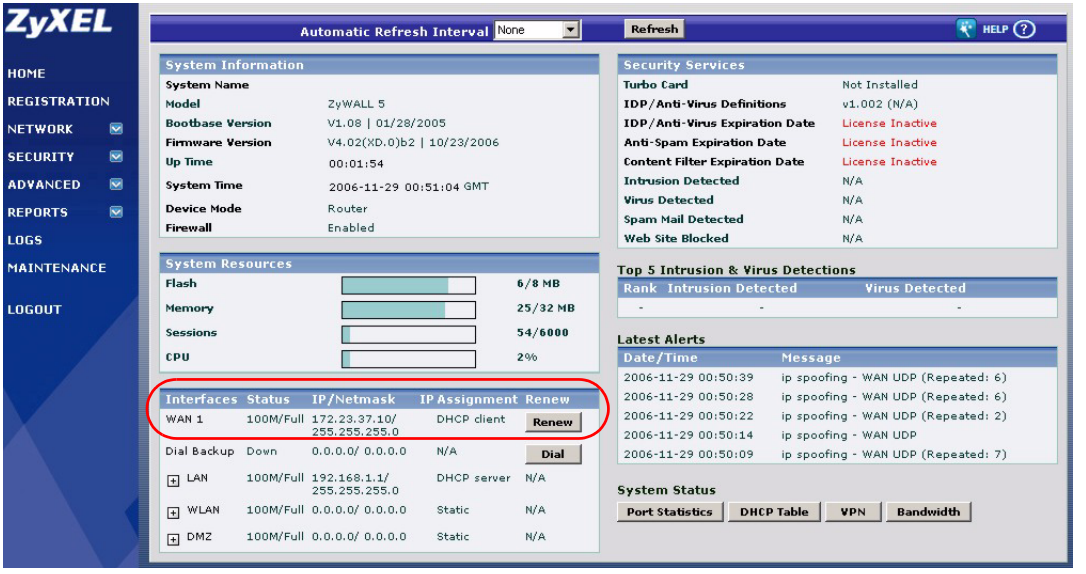
Per impostazione predefinita, lo ZyWALL è in modalità router. Continuare dal passo successivo se si desidera utilizzare funzionalità di routing quali NAT, DHCP e VPN.

Passare a Sezione 3 se si preferisce utilizzare lo ZyWALL come firewall trasparente.

6 Controllare la tabella network status (stato della rete). Se lo stato della **WAN 1** è *not* **Down** (disattivata) ed è presente un indirizzo IP, passare a Sezione 5.

Se lo stato **WAN 1** è **Down** (e se non c'è un indirizzo IP), fare clic sull'icona **Wizard** (procedura guidata) e consultare la Sezione 4 per configurare la **WAN 1**.

Utilizzare le schermate di **NETWORK WAN** (WAN della rete) se occorre configurare lo **WAN 2**. È anche possibile configurare il load balancing (bilanciamento del carico) tra le connessioni WAN.



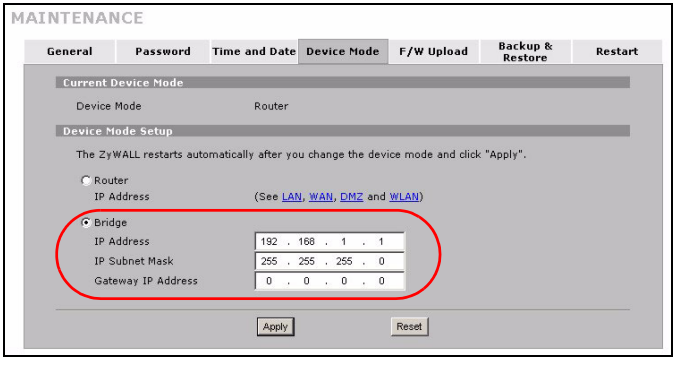
3 Modalità Bridge

Quando si imposta lo ZyWALL in modalità Bridge, esso funziona come un firewall trasparente. La procedura illustrata di seguito consente di impostare lo ZyWALL in modalità Bridge.

1 Fare clic su **MAINTENANCE** (manutenzione) nel pannello di navigazione, quindi su **Device Mode** (modalità dispositivo).

2 Selezionare **Bridge** e immettere un indirizzo IP (statico), una subnet mask e un indirizzo IP del gateway per le interfacce **LAN**, **WAN**, **DMZ** e **WLAN** dello ZyWALL.

3 Fare clic su **Apply** (applica). Lo ZyWALL si riavvia.



Passare a Sezione 5 se si dispone di server che occorre rendere accessibili dalla WAN.

4 Configurazione dell'accesso a Internet

1 Fare clic sull'icona **Wizard** (procedura guidata) ( ) nella schermata **HOME** e quindi sul link **Internet Access Setup** (configurazione accesso a Internet) per aprire la connessione guidata a Internet.

Immettere le informazioni e i parametri Internet esattamente come sono stati forniti.

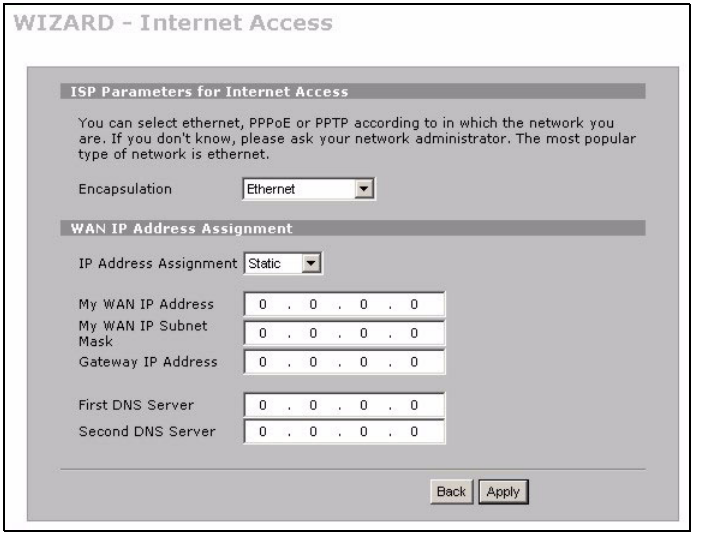
Se è stato fornito un indirizzo IP da utilizzare, selezionare **Static** (statico) nell'elenco di riepilogo **IP Address Assignment** (assegnazione indirizzo IP) e immettere le informazioni fornite.

I campi variano a seconda di quanto viene selezionato nel campo **Encapsulation** (incapsulamento). Compilare i campi con le informazioni fornite dall'ISP o dall'amministratore di rete.

Fare clic su **Apply** (applica) una volta terminata la configurazione.

- **Incapsulamento Ethernet**

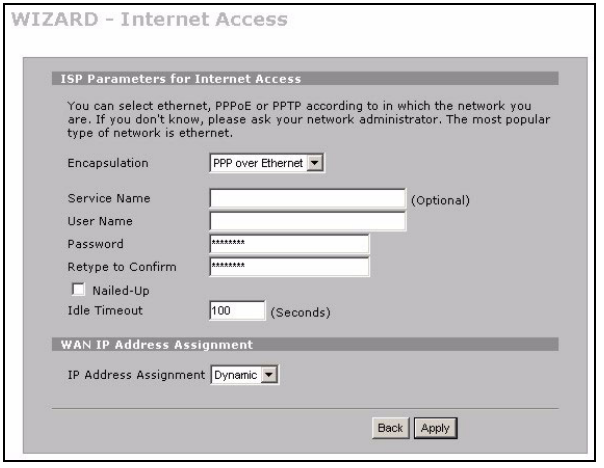
Configurare un servizio Roadrunner nelle schermate **NETWORK WAN** (WAN di rete) (utilizzare la scheda **WAN**).



- **PPP over Ethernet oppure incapsulamento PPTP**

Selezionare **Nailed-Up** (riconnessione) quando si desidera che la connessione sia sempre attiva (questa opzione potrebbe rivelarsi costosa se il proprio ISP applica una tariffazione a tempo dell'accesso a Internet piuttosto che un costo mensile fisso).

Per non avere sempre attiva la connessione, specificare il tempo di timeout di inattività (in secondi) nel campo **Idle Timeout** (timeout di inattività).

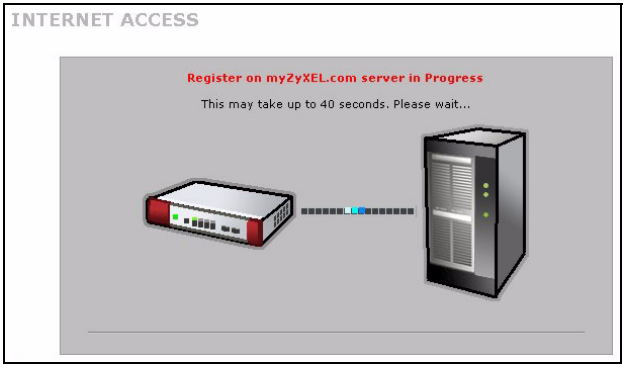


2 Fare clic su **Next** (avanti) per visualizzare la schermata in cui e possibile registrare lo ZyWALL sul sito myZyXEL.com (centro di assistenza online ZyXEL) e attivare i servizi filtraggio dei contenuti, antispam, antivirus e IDP gratuiti in versione di valutazione. Altrimenti fare clic su **Skip** (ignora) e quindi su **Close** (chiudi) per completare la configurazione dell'accesso a Internet.

Verificare di aver installato il ZyWALL Turbo Card prima di attivare i servizi di sottoscrizione IDP e antivirus.
Spegnere lo ZyWALL prima di installare o rimuovere ZyWALL Turbo Card.

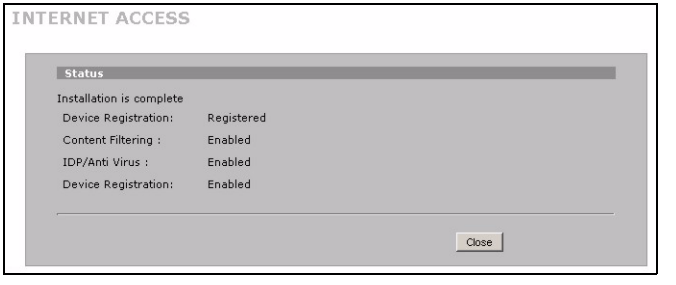
3 Se si dispone gia di un account su myZyXEL.com, selezionare **Existing myZyXEL.com account** (account esistente) e immettere le informazioni relative all'account. Altrimento selezionare **New myZyXEL.com account** (nuovo account) e compilare i campi sotto per creare un nuovo account e registrarsi su ZyWALL. Fare clic su **Next** (avanti).

4 Attendere il completamento del processo di registrazione.



5 La seguente schermata indica se la registrazione non ha avuto esito positivo. Fare clic su **Return** (torna) per tornare alla schermata **Device Registration** (registrazione dispositivo) e controllare le impostazioni.

6 Fare clic su **Close** (chiudi) per chiudere la procedura guidata una volta terminata la registrazione e l'attivazione.



Se si desidera attivare un servizio standard con il proprio numero PIN (chiave di licenza) di iCard, utilizzare la schermata **REGISTRATION Service** (servizio di registrazione). Vedere la guida utente per i dettagli.

5 DMZ

Una zona demilitarizzata (DMZ, DeMilitarized Zone) consente a server pubblici (Web, E-mail, FTP, ecc.) di essere visibili al mondo esterno e di continuare ad avere una protezione firewall contro attacchi DoS (Denial of Service).

È possibile assegnare una configurazione TCP/IP via DHCP ai computer connessi alle porte DMZ. In alternativa, configurare i computer con indirizzi IP statici (nella stessa subnet dell'indirizzo IP della porta DMZ) e con indirizzi dei server DNS. Utilizzare l'indirizzo IP DMZ dello ZyWALL come gateway predefinito.

La procedura seguente consente di configurare la DMZ se lo ZyWALL è in modalità routing.

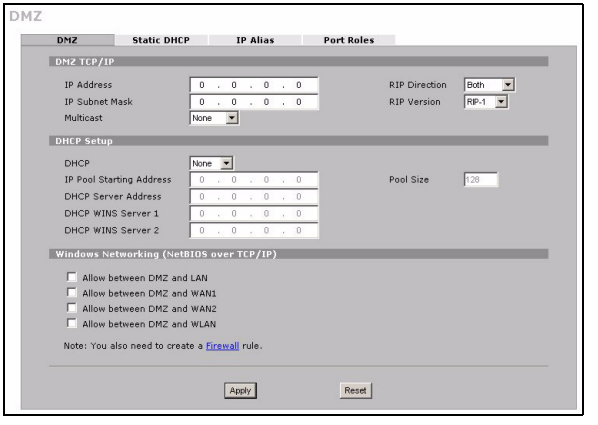
Non è necessario configurare la DMZ con la modalità bridge; passare a Sezione 7.

1 Fare clic su **NETWORK** (RETE) > **DMZ** nel pannello di navigazione.

2 Specificare un indirizzo IP e una subnet mask per l'interfaccia DMZ.

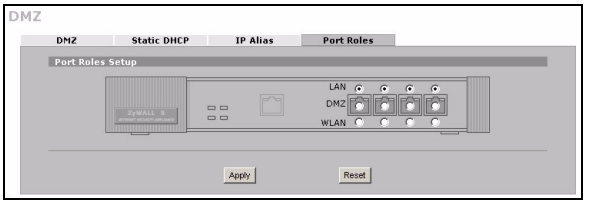
   Se si utilizzano indirizzi IP privati sulla DMZ, utilizzare la funzione NAT per rendere i server accessibili pubblicamente (vedere Sezione 6).

   Un indirizzo IP pubblico deve trovarsi su una subnet separata rispetto all'indirizzo IP pubblico della porta WAN. Se non si configura la funzione NAT per gli indirizzi IP pubblici sulla DMZ, lo ZyWALL instrada il traffico verso gli indirizzi IP pubblici sulla DMZ senza eseguire il NAT. Questo potrebbe essere utile per l'hosting di server per eseguire il NAT di applicazioni non di semplice configurazione.



3 Fare clic su **Apply** (applica).

4 Per impostazione predefinita, le porte **LAN/DMZ** dalla 1 alla 4 sono tutte porte LAN. Per configurare una porta come porta DMZ, fare clic sulla scheda **Port Roles** (regole delle porte), selezionare il pulsante di opzione accanto alla scelta **DMZ** e fare clic su **Apply** (applica).

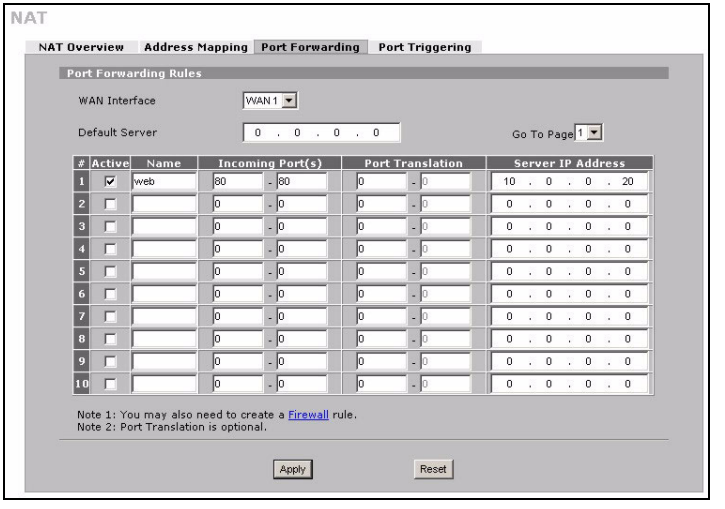


6 NAT

Il processo di NAT (Network Address Translation, traslazione degli indirizzi di rete; NAT, RFC 1631) consente di tradurre un indirizzo IP di una rete in un differente indirizzo IP in un'altra rete. È possibile utilizzare le schermate **NAT Address Mapping** (mappatura indirizzi di NAT) per configurare lo ZyWALL per tradurre più indirizzo IP pubblici in più indirizzi IP privati che si trovano sulla propria LAN (o DMZ).

Il seguente esempio consente di abilitare l'accesso dalla WAN1 a un server HTTP (Web) sulla DMZ. L'indirizzo IP privato del server è 10.0.0.20.

1 Fare clic su **ADVANCED** (AVANZATO) > **NAT** nel pannello di navigazione, quindi su **Port Forwarding** (inoltro delle porte).
2 Selezionare una connessione WAN (**WAN1**) per la quale si desidera configurare le regole di forward delle porte.
3 Selezionare la casella di controllo **Active** (attiva).
4 Digitare un nome per la regola.
5 Digitare il numero di porta utilizzata dal servizio.
6 Digitare l'indirizzo IP del server HTTP.
7 Fare clic su **Apply** (applica).



7 Firewall

È possibile utilizzare lo ZyWALL senza dover configurare il firewall.

Il firewall dello ZyWALL è preconfigurato per proteggere la LAN da attacchi provenienti da Internet. Per impostazione predefinita, nessun traffico dati può entrare nella LAN, a meno che non è stata prima generata una richiesta proveniente dalla LAN. Lo ZyWALL consente di accedere alla DMZ dalla WAN o dalla LAN, ma blocca il traffico dalla DMZ alla LAN.

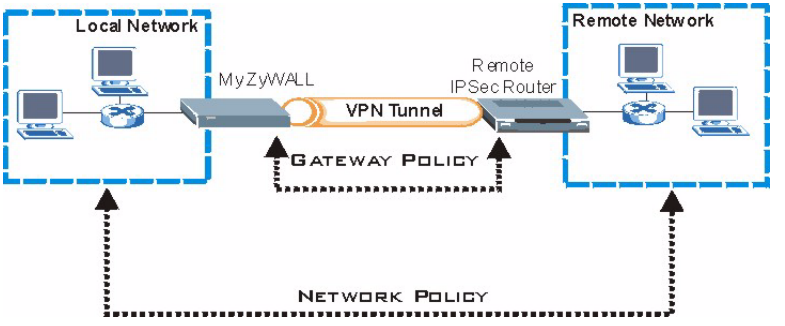
Se si utilizza lo ZyWALL in modalità router, continuare con la prossima sezione. Per la modalità bridge, passare a Sezione 9.

8 Configurazione delle regole di VPN

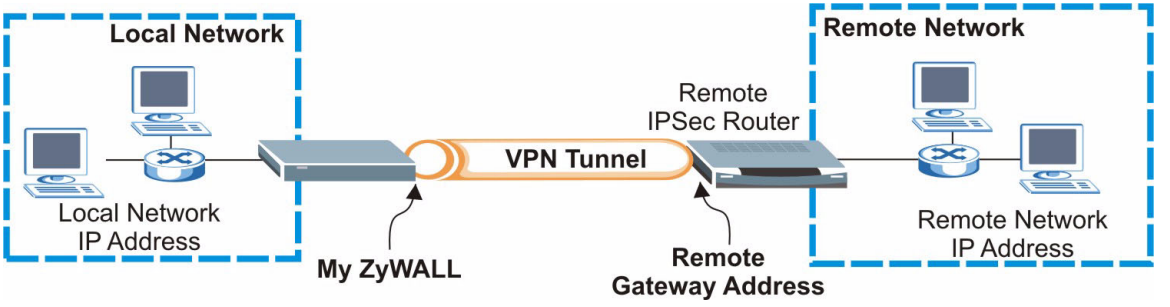
Un tunnel VPN (Virtual Private Network, rete privata virtuale) offre una connessione sicura a un altro computer o rete.

Un criterio di gateway identifica i router IPSec a entrambe le estremità di un tunnel VPN.

Un criterio di rete specifica quali dispositivi (dietro i router IPSec) possono utilizzare il tunnel VPN.



La seguente figura illustra i campi principali nelle schermate della procedura guidata.



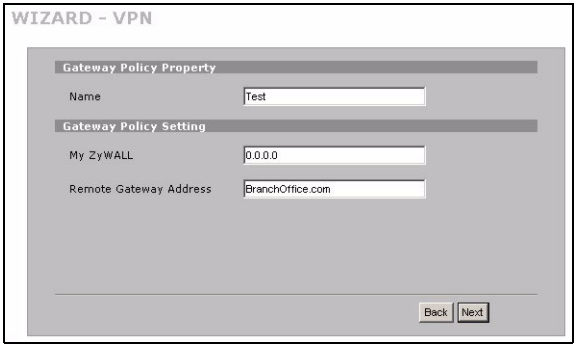
1 Fare clic sull'icona **Wizard** (procedura guidata) ( ) nella schermata **HOME** e quindi sul link **VPN Setup** (configurazione VPN) per aprire la connessione guidata a VPN.

Le impostazioni non vengono salvate quando si fa clic su **Back** (Indietro).

2 Utilizzare questa schermata per configurare il criterio di gateway.

Name (nome): immettere un nome per identificare il criterio di gateway.

Remote Gateway Address (indirizzo gateway remoto): immettere l'indirizzo IP o il nome di dominio del router IPSec remoto.



3 Utilizzare questa schermata per configurare il criterio di rete.

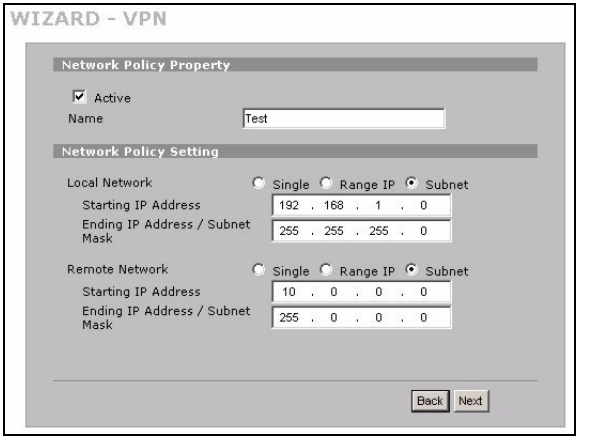
Lasciare la casella di controllo **Active** (attiva) selezionata.

Name (nome): immettere un nome per identificare il criterio di rete.

Selezionare **Single** (singolo) e immettere un indirizzo IP per un unico indirizzo IP.

Selezionare **Range IP** (IP della gamma) e immettere gli indirizzo IP iniziare e finale di una gamma di indirizzi IP specifica.

Selezionare **Subnet** e immettere un indirizzo IP e una subnet mask che specifichino gli indirizzi IP su una rete mediante la loro subnet mask.



Assicurarsi che il router IPSec remoto utilizzi le stesse impostazioni di sicurezza configurate nelle prossime due schermate.

Negotiation Mode (modalità di negoziazione): selezionare **Main Mode** (modalità principale) come protezione dell'identità. Selezionare **Aggressive Mode** (modalità aggressiva) per consentire a più connessioni in ingresso provenienti da indirizzi IP dinamici di utilizzare password separate.

Più SA (Security Association, associazioni di protezione) che si connettono attraverso un gateway sicuro devono avere la stessa modalità di negoziazione.

Encryption Algorithm (algoritmo di crittografia): selezionare **3DES** o **AES** per una crittografia più forte (ma più lenta).

Authentication Algorithm (algoritmo di autenticazione): selezionare **MD5** per una sicurezza minima oppure **SHA-1** per una sicurezza maggiore.

Key Group (gruppo di chiavi): selezionare **DH2** per una maggiore sicurezza.

SA Life Time (tempo di vita SA): imposta quanto spesso lo ZyWALL negozia la SA IKE (minimo 180 secondi). Un tempo di vita di SA breve aumenta la sicurezza, ma la negoziazione disconnette temporaneamente il tunnel VPN.

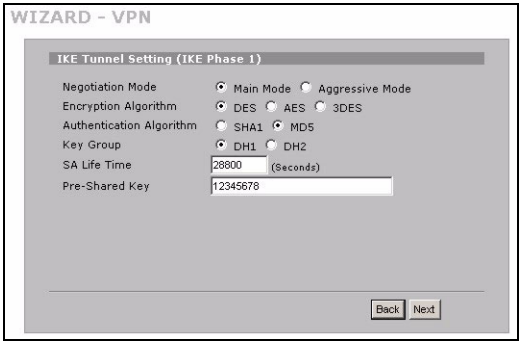
Pre-Shared Key (chiave pre-condivisa): utilizzare da 8 a 31 caratteri ASCII (con differenziazione tra maiuscole e minuscole) oppure da 16 a 62 caratteri esadecimali ("0-9", "A-F"). Precedere una chiave esadecimale con uno "0x" (zero x), il quale non viene conteggiato come parte della gamma di caratteri da 16 a 62 per la chiave.

Encapsulation Mode (modalità di incapsulamento): **Tunnel** è compatibile con la funzione NAT, **Transport** (trasporto) non lo è.

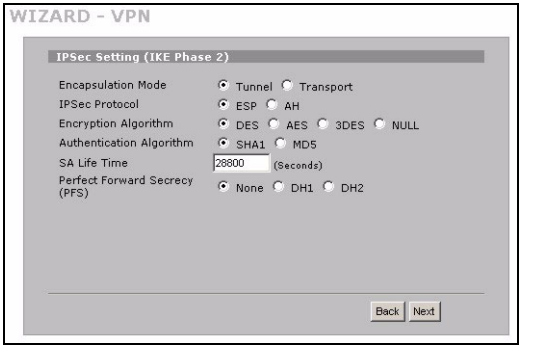
IPSec Protocol (protocollo IPSec): **ESP** è compatibile con NAT, **AH** non lo è.

Perfect Forward Secrecy (PFS): **None** (nessuno) consente una configurazione IPSec più rapida, ma **DH1** e **DH2** sono più sicuri.

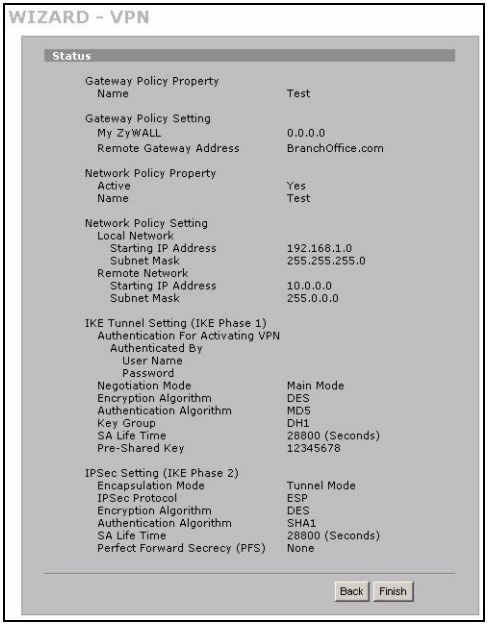
4 Utilizzare questa schermata per configurare le impostazioni del tunnel IKE (Internet Key Exchange, scambio chiavi Internet).



5 Utilizzare questa schermata per configurare le impostazioni IPSec.



6 Verificare le impostazioni della VPN. Fare clic su **Finish** (fine) per salvare le impostazioni.

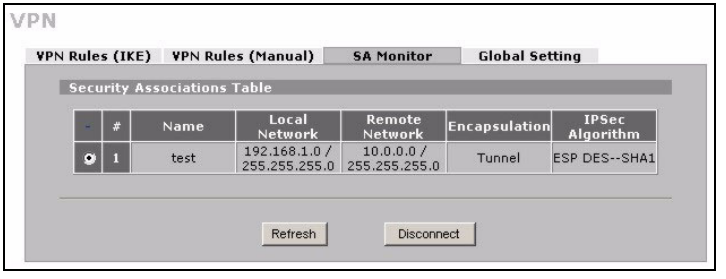


7 Fare clic su **Close** (chiudi) nella schermata finale per completare l'installazione guidata della VPN. Continuare con la prossima sezione per attivare la regola VPN e stabilire una connessione VPN.

8.1 Uso della connessione VPN

Utilizzare i tunnel VPN per inviare e ricevere in maniera sicura file e per consentire un accesso remoto alle reti aziendali, server Web ed e-mail. I servizi funzioneranno come se ci si trovasse connessi direttamente dall'ufficio invece che da Internet.

Ad esempio, la regola di VPN “test” consente un accesso sicuro a un server Web che si trova sulla LAN aziendale remota. Immettere l'indirizzo IP del server (10.0.0.23 in questo esempio) come URL nel browser. Lo ZyWALL crea automaticamente il tunnel VPN quando si tenta di utilizzarlo.



Fare clic su **SECURITY** (PROTEZIONE) > **VPN** nel pannello di navigazione e quindi sulla scheda **SA Monitor** (monitor SA) per visualizzare un elenco dei tunnel VPN connessi (nell'esempio è attivo il tunnel VPN “test”).

9 Risoluzione dei problemi

Problema	Azione correttiva
Nessuno dei LED è acceso.	Assicurarsi di aver collegato il adattatore di alimentazione allo ZyWALL e a una sorgente di alimentazione appropriata. Controllare tutti i collegamenti dei cavi.
	Se i LED continuano a non accendersi, potrebbe esserci un guasto hardware. In questo caso, è opportuno rivolgersi al rivenditore locale.
Impossibile accedere allo ZyWALL dalla LAN.	Controllare il collegamento dei cavi tra lo ZyWALL e il computer o l'hub. Vedere Sezione 1 per i dettagli.
	Eseguire il ping dello ZyWALL da un computer della LAN., Assicurarsi che la scheda Ethernet del computer sia installata e correttamente funzionante. Nel computer, fare clic su **Start**, **(Tutti i) Programmi**, **Accessori** e quindi **Prompt dei comandi**. Nella finestra **Prompt dei comandi**, digitare "ping" seguito dall'indirizzo IP LAN dello ZyWALL (192.168.1.1 è l'indirizzo predefinito) e quindi premere [Invio]. Lo ZyWALL dovrebbe rispondere. In caso contrario, vedere Sezione 9.1.
	Se si è dimenticata la password dello ZyWALL, utilizzare il pulsante **RESET**. Premere il pulsante per circa 10 secondi (oppure finché il LED **SYS** non inizia a lampeggiare), quindi rilasciarlo. Questa operazione riporta lo ZyWALL ai valori predefiniti (la password è 1234, l'indirizzo IP LAN è 192.168.1.1, e così via; vedere la Guida dell'utente per i dettagli).
	Se si dimentica l'indirizzo IP della WAN o della LAN dello ZyWALL, è possibile controllare l'indirizzo IP nello SMT via porta console. Collegare il computer alla porta **CONSOLE** utilizzando un cavo console. Il computer dovrebbe disporre di un programma di comunicazione di emulazione terminale (come ad esempio HyperTerminal); impostare l'emulazione di terminale VT100, nessuna parità, 8 bit di dati, 1 bit di stop, nessun controllo di flusso e velocità della porta pari a 9600 bps.
Impossibile accedere a Internet.	Controllare il collegamento dello ZyWALL al jack Ethernet con accesso a Internet. Assicurarsi che il dispositivo gateway verso Internet (quale ad esempio un modem DSL) funzioni correttamente.
	Fare clic su **WAN** nel pannello di navigazione per verificare le impostazioni.
Impossibile stabilire una connessione VPN.	Assicurarsi lo ZyWALL e il router IPSec remoto utilizzi le stesse impostazioni VPN. Fare clic su **VPN** nel pannello di navigazione per configurare le impostazioni avanzate.
	Accedere a un sito Web per verificare che si dispone di una connessione a Internet valida.

9.1 Impostare l'indirizzo IP del computer

Questa sezione spiega come configurare il computer per ricevere un indirizzo IP in Windows 2000, Windows NT e Windows XP. In questo modo ci si assicura che il computer possa comunicare con lo ZyWALL.

1 In Windows XP, fare clic su **Start**, **Pannello di controllo**.

In Windows 2000/NT, fare clic su **Start**, **Impostazioni**, **Pannello di controllo**.

2 In Windows XP, fare clic su **Connessioni di rete**.

In Windows 2000/NT, fare clic su **Reti e connessioni remote**.

3 Fare clic con il pulsante destro del mouse su **Connessione alla rete locale** e scegliere **Proprietà**.

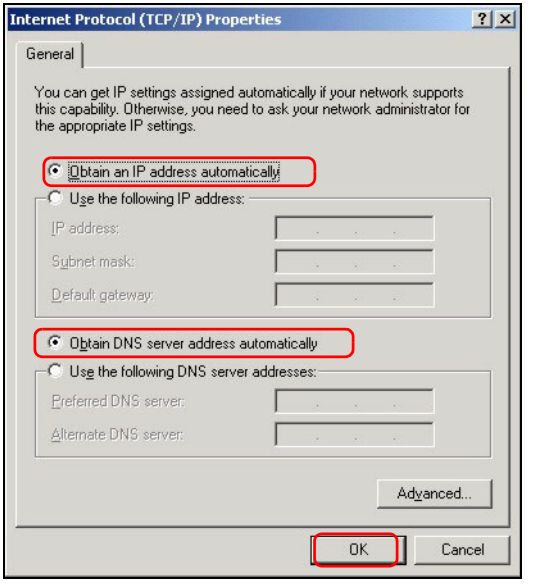
4 Selezionare **Protocollo Internet (TCP/IP)** (sotto la scheda **Generale** in Windows XP) e fare clic su **Proprietà**.

5 Si apre la schermata **Protocollo Internet TCP/IP - Proprietà** (la scheda **Generale** in Windows XP). Selezionare le opzioni **Ottieni automaticamente un indirizzo IP** e **Ottieni automaticamente l'indirizzo del server DNS**.

6 Fare clic su **OK** per chiudere la finestra **Protocollo Internet (TCP/IP) - Proprietà**.

7 Fare clic su **Chiudi** (**OK** in Windows 2000/NT) per chiudere la finestra **Connessione alla rete locale - Proprietà**.

8 Chiudere la schermata **Connessioni di rete**.



Procedura per visualizzare le certificazioni di un prodotto

1 Aprire la pagina www.zyxel.com.

2 Selezionare il prodotto dall'elenco di riepilogo a discesa nella Home Page di ZyXEL per passare alla pagina del prodotto in questione.

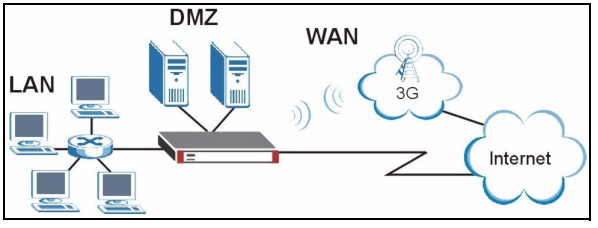
3 Selezionare da questa pagina la certificazione che si desidera visualizzare.

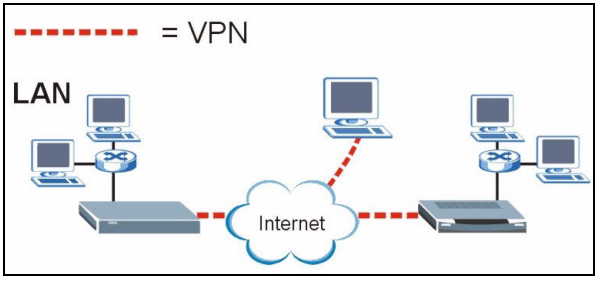
Обзор

Устройство ZyWALL 5 представляет собой межсетевой экран с функциями виртуальной частной сети, управления пропускной способностью, фильтрацией контента, защиты от спама, защиты от вирусов, IDP (Intrusion Detection and Protection - Обнаружение и защита от вторжения) и другими. Устройство можно использовать как прозрачный межсетевой экран, при этом не требуется изменять конфигурацию сети или проводить настройку параметров маршрутизатора ZyWALL. Когда ZyWALL находится в режиме маршрутизатора, то вы также можете вставить беспроводную сетевую 3G карту для добавления второй ГВС. ZyWALL повышает уровень безопасности сети с помощью изменения ролевых имен портов при передаче трафика от локальной сети к DMZ (DeMilitarized Zone - демилитаризованная зона), где устанавливаются общедоступные серверы. Данное руководство содержит информацию по первоначальному подключению и настройке ZyWALL.

Дополнительную информацию обо всех функциях устройства см. в Техническом руководстве.

Вам потребуются учетные данные для подключения к Интернету.





Данное руководство включает следующие разделы.

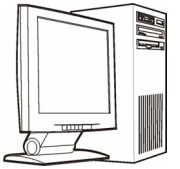
1 Подключение оборудования
2 Доступ к Web-конфигуратору
3 Режим межсетевого моста
4 Настройка доступа в Интернет и регистрация изделия
5 DMZ
6 Трансляция сетевых адресов
7 Межсетевой экран
8 Настройка правил виртуальной частной сети (VPN)
9 Поиск и устранение неисправностей

1 Подключение оборудования

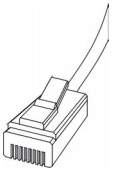
Вам потребуется следующее оборудование.

ZyWALL

Компьютер

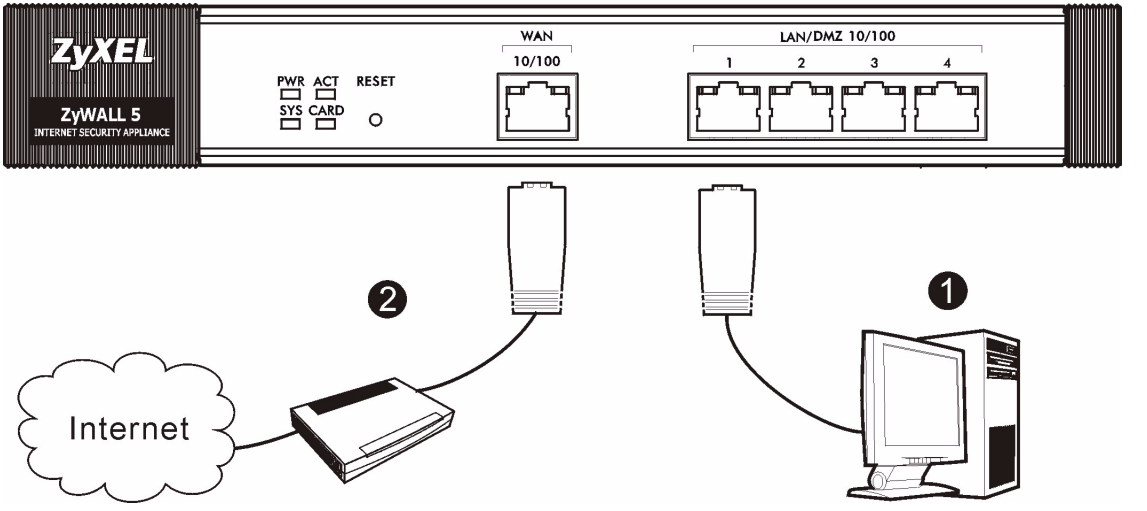


Кабели Ethernet



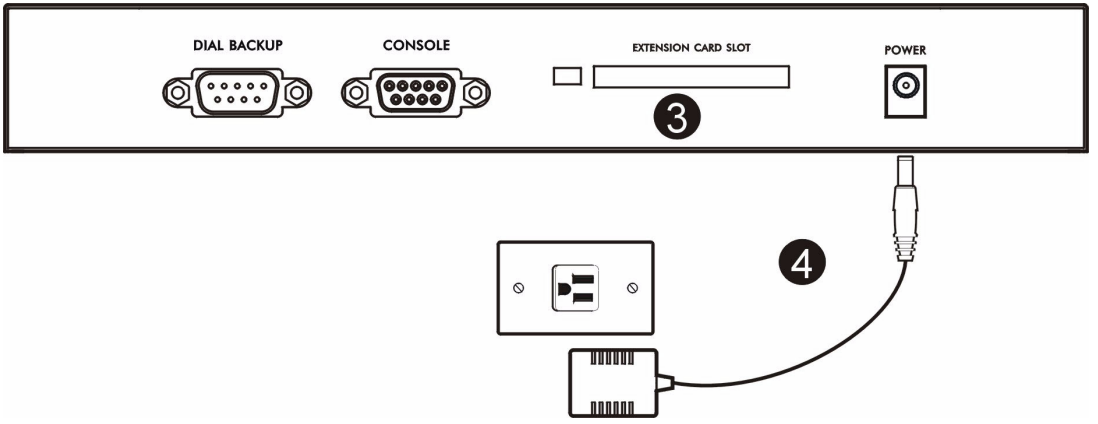
Адаптер питания

Для подключения оборудования выполните следующие действия.



1 Для подключения портов **LAN/DMZ** к компьютеру используется кабель Ethernet. Если в Web-конфигураторе эти порты настроены как порты **DMZ** в окне **LAN** или **DMZ**, для подключения общедоступных серверов (web-сервер, почтовый сервер, FTP-сервер и др.) к портам **LAN/DMZ** можно также использовать кабель Ethernet.

2 С помощью другого кабеля Ethernet подключите порт **WAN** в розетку Ethernet, с которой имеется доступ в Интернет.



3 Установите карту расширения ZyWALL Turbo, чтобы использовать функции защиты от вирусов и IDP, или установите беспроводной адаптер для подключения к беспроводной сети. Вы можете дополнительно вставить беспроводную сетевую 3G карту для беспроводного доступа в Интернет через сеть 3G. Дополнительную информацию по карте расширения см. в руководстве по ZyWALL Turbo. Информацию по установке беспроводной сетевой карты см. в Техническом руководстве. На момент написания руководства вместе с ZyWALL. можно использовать только беспроводную сетевую карту Sierra AC850/860 3G.

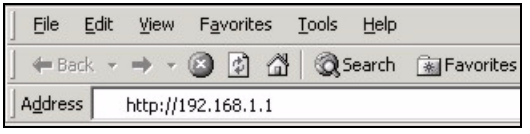
4 Подключите разъем питания на задней панели к розетке сети электропитания с помощью адаптера питания, входящего в комплект поставки.

5 Посмотрите на переднюю панель. Светодиод **PWR** горит. Светодиод **SYS** мигает, пока выполняется тестирование системы и затем, если тестирование прошло успешно, горит постоянно. Светодиоды **ACT**, **CARD**, **LAN/DMZ** и **WAN** горят, если правильно выполнены соответствующие соединения.

2 Доступ к Web-конфигуратору

В этом разделе описывается настройка интерфейса **WAN 1** для доступа в Интернет.

1 Запустите Web-обозреватель. Введите адрес **192.168.1.1** (IP-адрес ZyWALL по умолчанию). Если окно регистрации не отображается, см. Раздел 9.1 для установки IP-адреса компьютера.



2 Щелкните **Login** (Вход) (пароль по умолчанию 1234 уже введен).

3 Измените пароль по умолчанию, введя новый пароль и щелкнув по кнопке **Apply** (Применить).

4 Щелкните по кнопке **Apply** (Применить), чтобы заменить цифровой сертификат ZyWALL по умолчанию.

5 Открывается окно **HOME** (ДОМАШНЯЯ СТРАНИЦА).

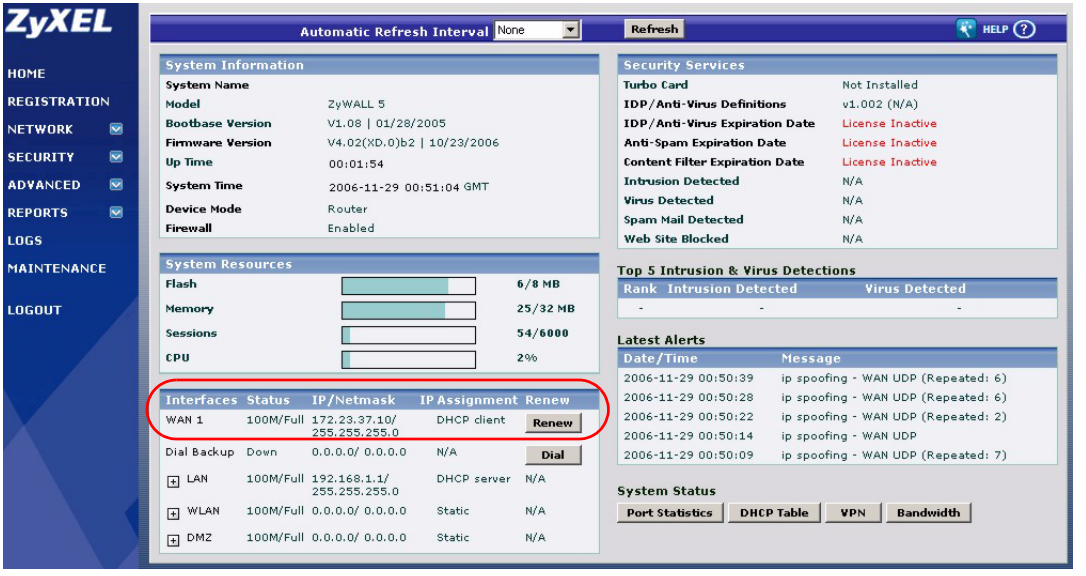
По умолчанию в ZyWALL установлен режим маршрутизатора. Если вы хотите использовать функции маршрутизации, такие как NAT, DHCP и VPN, переходите к следующему шагу.

Если ZyWALL будет использоваться в качестве прозрачного межсетевого экрана, переходите к Раздел 3.

6 Проверьте таблицу Network Status (Статус сети). Если статус порта **WAN 1** *не* **Down** (не подключен) и установлен IP-адрес, см. Раздел 5.

Если **WAN 1** (ГВС1) находится в состоянии **Down** (Откл.) (или для нее не установлен IP-адрес), щелкните на значке **Wizard** (Мастер) и настройте **WAN 1** (ГВС1) при помощи Раздел 4.

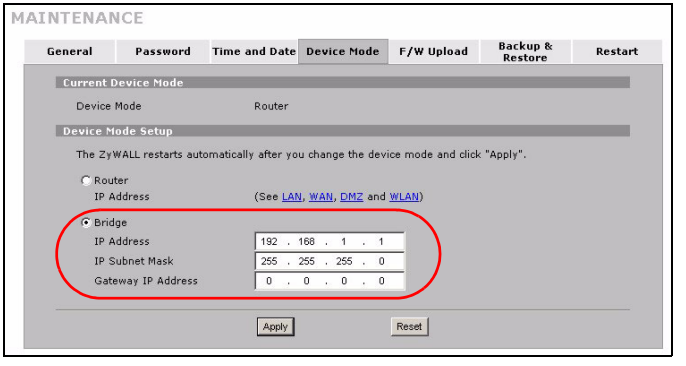
Для настройки порта **WAN 2** используются окна **WAN** в разделе **NETWORK** (СЕТЬ). Вы также можете установить распределение разгрузки между разъемами ГВС.



3 Режим межсетевого моста

Если в ZyWALL установлен режим межсетевого моста, устройство функционирует как прозрачный межсетевой экран. Для установки режима межсетевого моста ZyWALL выполните следующие действия.

1. В Панели навигации щелкните **MAINTENANCE** (ОБСЛУЖИВАНИЕ) и затем **Device Mode** (Режим устройства).
2. Выберите **Bridge** (Мост) и установите статический IP-адрес, маску подсети и IP-адрес шлюза для интерфейсов **LAN**, **WAN**, **DMZ** и **WLAN**.
3. Щелкните **Apply** (Применить). ZyWALL перезагрузится.



Если имеются серверы, которые должны быть доступны из глобальной сети, см. Раздел 5.

4 Настройка доступа в Интернет и регистрация изделия

1 Щелкните на значке **Wizard** (Мастер) ( ) в окне **HOME** (ДОМАШНЯЯ), а затем на ссылке **Internet Access Setup** (Настройка доступа к Интернет), чтобы открыть мастер настройки.

Введите учетные данные для подключения к Интернету.

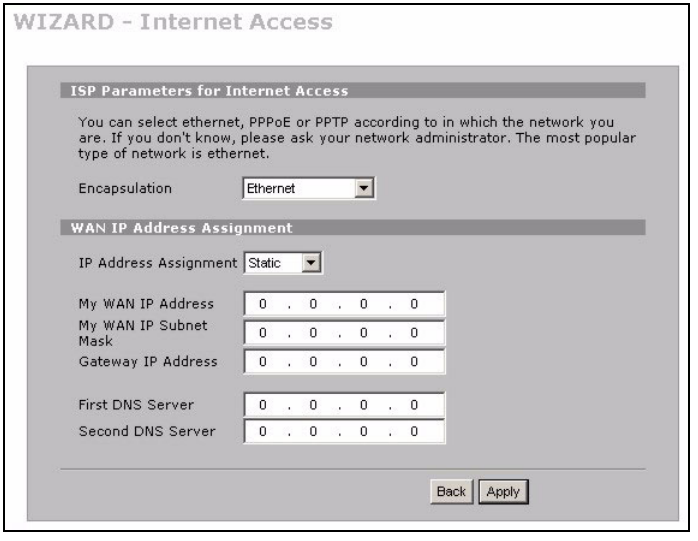
Если вам назначен статический IP-адрес, выберите **Static** (Статический) в раскрывающемся списке **IP Address Assignment** (Назначение IP-адреса) и введите предоставленные вам параметры.

Заполняемые поля могут различаться в зависимости значения, установленного в поле **Encapsulation** (Инкапсуляция). Введите параметры, предоставленные Интернет-провайдером или сетевым администратором.

По окончании щелкните **Apply** (Применить).

- **Инкапсуляция Ethernet**

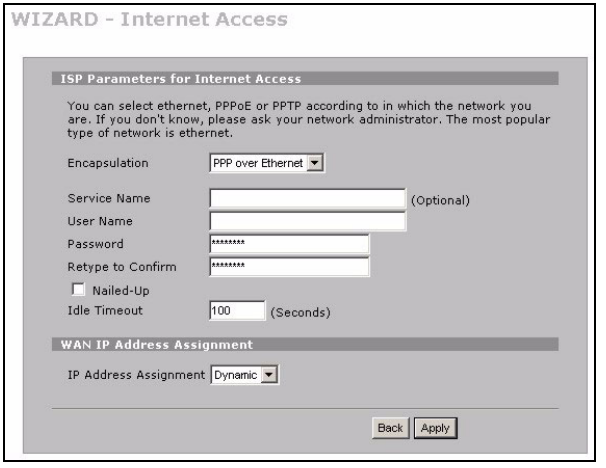
Настройте службу Roadrunner с помощью окон **WAN** в разделе **NETWORK** (СЕТЬ) (закладка **WAN**).

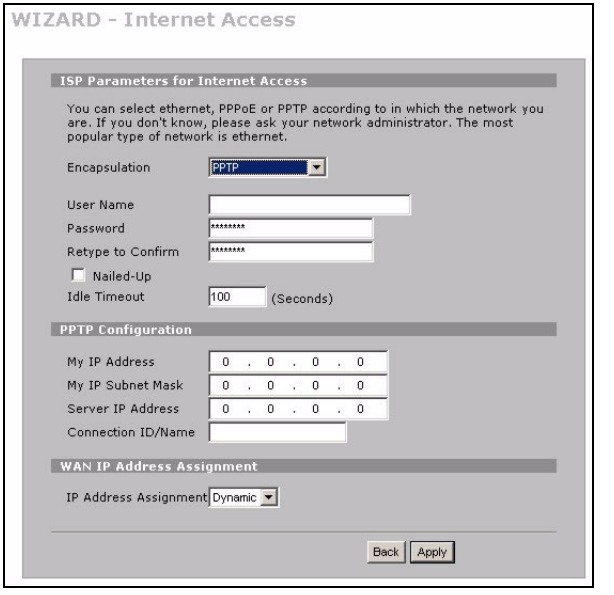


- **PPP поверх Ethernet или инкапсуляция PPTP**

Выберите **Nailed-Up** (Постоянное), если вы хотите иметь постоянное соединение (такое соединение может быть достаточно дорогим, если Интернет-провайдер берет плату за время использования Интернет, а не использует установленный месячный тариф).

Чтобы не поддерживать постоянное соединение, введите интервал времени простоя (в секундах) в поле **Idle Timeout** (Время простоя).





2 Щелкните **Next** (Далее) для отображения окна, которое используется для регистрации ZyWALL на сайте myZyXEL.com (центр обслуживания ZyXEL) и активирования фильтрации контента, защиты от спама, защиты от вирусов и испытательных версии приложений IDP. В другом случае, щелкните **Skip** (Пропустить) и затем **Close** (Закрыть) для завершения настройки доступа в Интернет.

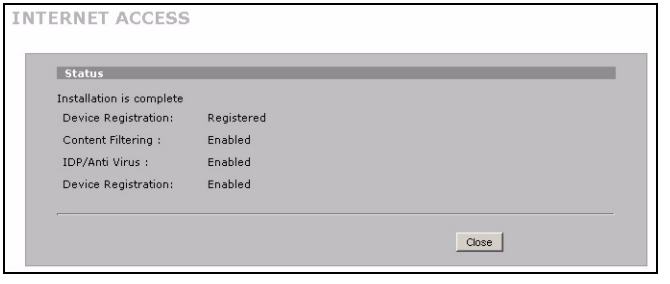
Прежде чем активировать подписку на защиту от вирусов и IDP, установите ZyWALL Turbo Card.
При установке или извлечении карты ZyWALL Turbo Card отключите питание ZyWALL.

3 Если вы уже регистрировались на сайте myZyXEL.com, выберите **Existing myZyXEL.com account** (Существующие учетные данные myZyXEL.com) и введите параметры учетных данных. В другом случае, выберите **New myZyXEL.com account** (Новые учетные данные myZyXEL.com) и заполните поля, расположенные ниже, для создания новых учетных данных и регистрации ZyWALL. Щелкните по кнопке **Next** (Далее).

4 Подождите, пока завершится процесс регистрации.

5 Если регистрация не выполнена, появляется следующее окно. Щелкните **Return** (Вернуться) для возврата к окну **Device Registration** (Регистрация устройства) и проверьте настройки.

6 Щелкните **Close** (Закрыть), чтобы закрыть окно Мастера после выполнения регистрации и активирования служб.



Для активации стандартной службы с номером PIN вашей карточки (лицензионный ключ) используется окно **REGISTRATION Service** (Служба РЕГИСТРАЦИИ). Подробнее см. в Техническом руководстве.

5 DMZ

DMZ (DeMilitarized Zone - демилитаризованная зона) позволяет внешним пользователям обращаться к общедоступным серверам (web-север, почтовый сервер, FTP-сервер и др.) и обеспечивает защиту серверов посредством межсетевого экрана от внешних атак DoS (Denial of Service - отказ от обслуживания).

Вы можете назначить конфигурацию TCP/IP через DHCP для компьютеров, подключенных к портам DMZ. Или, по другому, вы можете назначить компьютерам статические IP-адреса (в той же подсети, что и IP-адрес порта DMZ) и адреса серверов DNS. IP-адрес порта DMZ в ZyWALL используется в качестве шлюза по умолчанию.

Для настройки DMZ, если ZyWALL находится в режиме маршрутизации, выполните следующее.

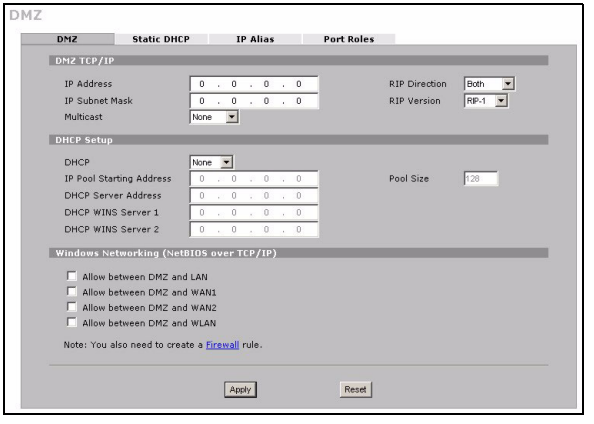
Настройка DMZ в режиме межсетевого моста не требуется, см. далее Раздел 7.

1 В Панели навигации щелкните **NETWORK** (СЕТЬ) > затем **DMZ**.

2 Введите IP-адрес и маску подсети для интерфейса DMZ.

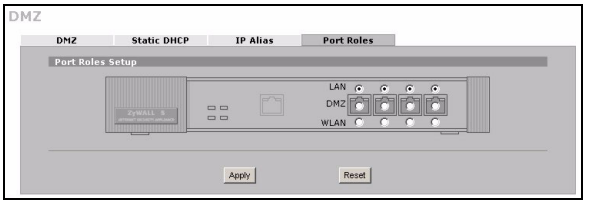
   Если используется частный IP-адрес для DMZ, то чтобы сделать серверы доступными для всех пользователей, необходимо использовать NAT (см. Раздел 6).

   Общедоступный IP-адрес должен находиться в подсети, отличной от общедоступного IP-адреса порта WAN. Если функция NAT для общедоступных IP-адресов для DMZ не настроена, ZyWALL направляет трафик на общедоступные IP-адреса в DMZ без применения NAT. Это используется для хост-серверов с приложениями, несовместимыми с NAT.



3 Щелкните **Apply** (Применить).

4 По умолчанию порты **LAN/DMZ** с 1-го по 4-ый являются портами локальной сети. Чтобы настроить порт как DMZ, щелкните закладку **Port Roles** (Ролевые имена портов), установите переключатель рядом с **DMZ** и щелкните **Apply** (Применить).

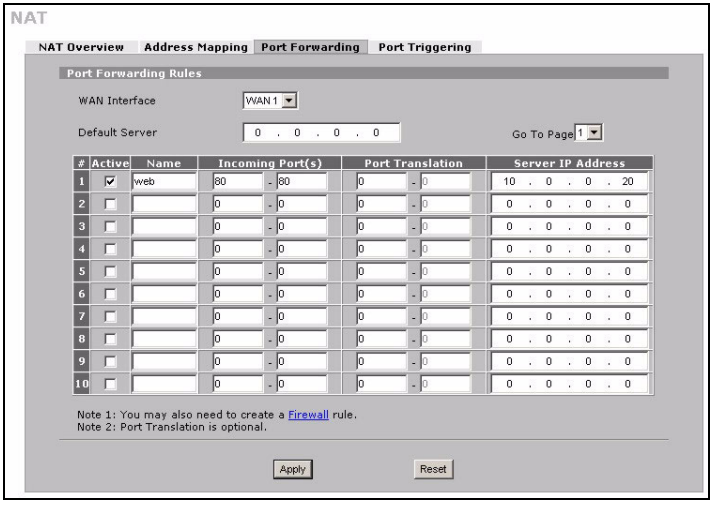


6 NAT

NAT (Network Address Translation - трансляция сетевых адресов NAT, RFC 1631) выполняет преобразование IP-адреса одной сети в отличный IP-адрес другой сети. Окна **NAT Address Mapping** (Преобразование адресов NAT) используются для настройки ZyWALL на преобразование нескольких общедоступных IP-адресов в частные IP-адреса вашей локальной сети (или DMZ).

В следующем примере разрешается доступ из глобальной сети к серверу HTTP (web-сервер) в DMZ. Этот сервер имеет частный IP-адрес 10.0.0.20.

1 В Панели навигации щелкните **ADVANCED** (ДОПОЛНИТЕЛЬНО) > затем **NAT** и затем **Port Forwarding** (Переадресация портов).
2 Выберите соединение ГВС (**WAN1**) (ГВС1) для которого вы хотите настроить правила переадресации порта.
3 Установите флажок **Active** (Включить).
4 Введите имя правила.
5 Введите номер порта, который используется службой.
6 Введите IP-адрес HTTP-сервера.
7 Щелкните **Apply** (Применить).



7 Межсетевой экран

ZyWALL можно использовать, не выполняя настройку межсетевого экрана.

Параметры межсетевого экрана ZyWALL предустановлены так, чтобы обеспечивать защиту локальной сети от атак из сети Интернет. По умолчанию трафик в локальную сеть не пропускается, пока сначала от нее не поступит запрос. ZyWALL разрешает доступ к DMZ из глобальной сети или локальной сети, но блокирует трафик от DMZ в локальную сеть.

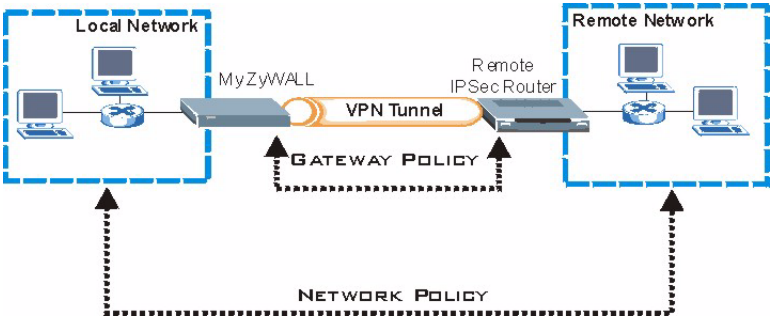
Если ZyWALL находится в режиме маршрутизации, переходите к следующему разделу. Для настройки режима межсетевого моста см. Раздел 9.

8 Настройка правил виртуальной частной сети (VPN)

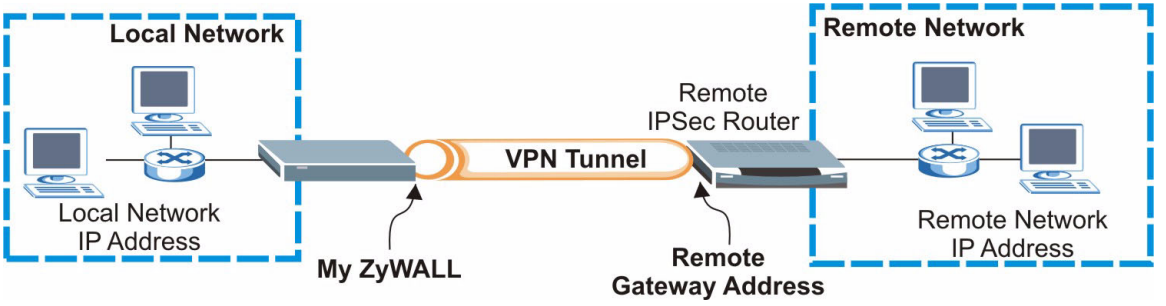
Туннель VPN (Virtual Private Network - виртуальная частная сеть) обеспечивает защищенное соединение к другому компьютеру или сети.

Стратегия шлюза определяет маршрутизаторы IPSec на каждом конце туннеля VPN.

Сетевая политика определяет устройства (за маршрутизаторами IPSec), которые могут использовать туннель VPN.



Следующая схема объясняет основные поля в окнах Мастера.



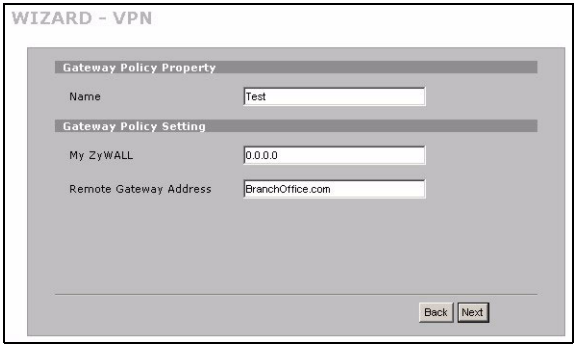
1 Щелкните на значке **Wizard** (Мастер) ( ) в окне **HOME** (ДОМАШНЯЯ), а затем на ссылке **VPN Setup** (Настройка VPN), чтобы открыть мастер настройки.

Если щелкнуть **Back** (Назад), настройки не сохраняются.

2 Это окно используется для настройки стратегии шлюза.

Name (Имя): Введите имя для идентификации стратегии шлюза.

Remote Gateway Address (Адрес удаленного шлюза): Введите IP-адрес или доменное имя удаленного маршрутизатора IPSec.



3 Это окно используется для настройки политики сети.

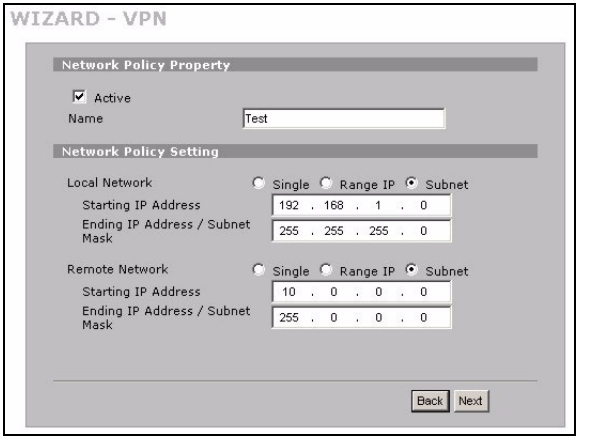
Флажок **Active** (Включить) должен быть установлен.

Name (Имя): Введите имя для идентификации политики сети.

Выберите **Single** (Один) и введите IP-адрес.

Выберите **Range IP** (Диапазон IP) и введите начальный и конечный IP адреса для конкретного диапазона IP-адресов.

Выберите **Subnet** (Подсеть) и введите IP-адрес и маску подсети для определения IP-адресов в сети по маске подсети.



Убедитесь, что удаленный маршрутизатор IPSec использует те же настройки безопасности, что будут настроены в следующих двух окнах.

Negotiation Mode (Режим согласования): Выберите **Main Mode** (Основной режим) для защиты конфиденциальности. Выберите **Aggressive Mode** (Рискованный режим), чтобы разрешить множество входящих подключений с динамическими IP-адресами и различными паролями.

Несколько безопасных соединений, подключаемых через шлюз системы безопасности должны иметь одинаковый режим согласования.

Encryption Algorithm (Алгоритм шифрования): Выберите **3DES** или **AES** для более надежного (или менее) шифрования.

Authentication Algorithm (Алгоритм аутентификации): Выберите **MD5** для минимального уровня безопасности или **SHA-1** для максимального.

Key Group (Ключевая группа): Выберите **DH2** для минимального уровня безопасности.

SA Life Time (Время существования защищенного соединения): Установите, как часто ZyWALL выполняет согласование защищенного соединения по протоколу IKE (минимум 180 секунд). Малое время соединения увеличивает уровень безопасности, но при процедуре согласования туннель VPN временно не доступен.

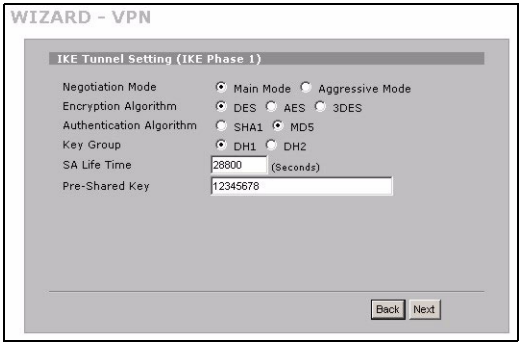
Pre-Shared Key (Предварительно согласованный ключ): Используется от 8 до 31 символа ASCII с учетом регистра или от 16 до 62 шестнадцатеричных символов ("0-9", "A-F"). Перед шестнадцатеричным ключом введите "0x" (ноль x), эти символы не считаются частью ключа из 16 - 62 символов.

Encapsulation Mode (Режим инкапсуляции): Режим **Tunnel** (Туннель) совместим с NAT, режим **Transport** (Транспорт) не совместим.

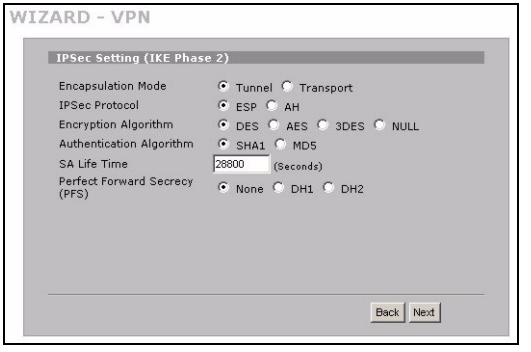
IPSec Protocol (Протокол IPSec): **ESP** совместим с NAT, **AH** не совместим.

Perfect Forward Secrecy (PFS) (Идеальная прямая безопасность): **None** (Нет) позволяет быструю настройку IPSec, но **DH1** и **DH2** повышают уровень безопасности.

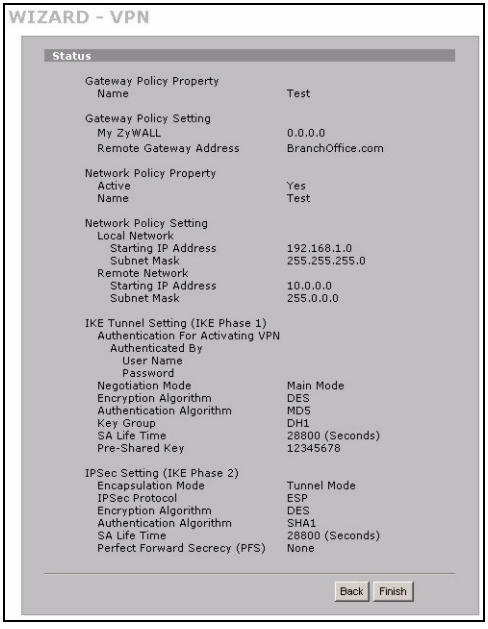
4 Это окно используется для настройки параметров туннеля IKE (Internet Key Exchange - протокол обмена ключами).



5 Это окно используется для настройки параметров IPSec.



6 Проверьте настройки VPN. Щелкните **Finish** (Готово) для сохранения настроек.

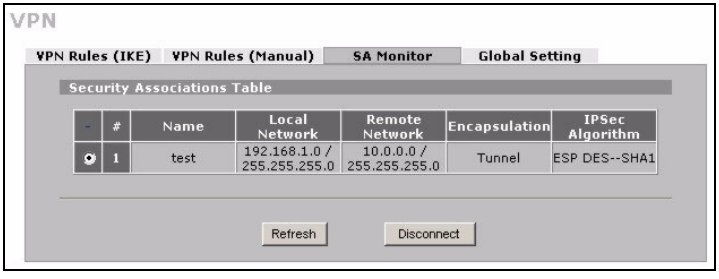


7 В последнем окне щелкните **Close** (Закрыть) для завершения работы Мастера настройки VPN. Для включения правила VPN и установления соединения VPN переходите к следующему разделу.

8.1 Использование соединения VPN

Туннели VPN используются для защищенной отправки и поиска файлов, а также разрешения удаленного доступа к корпоративным сетям, web-серверам и почтовым серверам. Эти службы будут работать так, как если бы вы находились в офисе, а не подключались через Интернет.

Например, правило VPN “test” разрешает защищенный доступ к web-серверу в удаленной корпоративной локальной сети. Введите IP-адрес сервера (10.0.0.23 в данном примере) в поле URL вашего браузера. ZyWALL автоматически создаст туннель VPN, когда вы попытаетесь его использовать.



В Панели навигации щелкните **SECURITY** (БЕЗОПАСНОСТЬ) > затем **VPN** и затем закладку **SA Monitor** (Монитор защищенного соединения) для отображения списка подключенных туннелей VPN (здесь установлен туннель VPN с именем “test”).

9 Поиск и устранение неисправностей

Неисправность	Способы устранения
Не горит ни один светодиод.	Убедитесь, что адаптер питания подключен к ZyWALL и к соответствующему источнику питания. Проверьте кабельные соединения.
	Если светодиоды все еще не горят, возможно, существует аппаратная неисправность. В этом случае следует связаться с поставщиком.
Отсутствует доступ к ZyWALL из локальной сети.	Проверьте кабельное соединение между ZyWALL и компьютером или концентратором. Подробнее см. Раздел 1.
	Протестируйте соединение ZyWALL с сетевым компьютером с помощью команды "ping". Убедитесь, что в компьютере установлена карта Ethernet и она работает нормально. В компьютере щелкните **Start** (Пуск), (**All**) **Programs** ((Все) программы), **Accessories** (Стандартные) и затем **Command Prompt** (Командная строка). В окне **Command Prompt** (Командная строка) введите "ping", затем IP-адрес ZyWALL в локальной сети (по умолчанию 192.168.1.1) и нажмите [ENTER]. ZyWALL должен ответить. В другом случае, см. Раздел 9.1.
	Если вы забыли пароль ZyWALL, нажмите кнопку **RESET**. Нажимайте кнопку в течение 10 секунд (или пока светодиод **SYS** не начнет мигать), затем отпустите кнопку. Эта операция возвращает параметры ZyWALL к заводским настройкам по умолчанию (пароль - 1234, IP-адрес в локальной сети - 192.168.1.1 и т. д.; подробнее см. в Техническом руководстве).
	Если вы забыли IP-адрес ZyWALL в локальной или глобальной сети, можно посмотреть IP-адрес в системной консоли при подключении через консольный порт. Подключите компьютер к порту **CONSOLE** с помощью консольного кабеля. На вашем компьютере должна быть установлена коммуникационная программа эмуляции терминала (например, HyperTerminal) с настроенной эмуляцией терминала VT100, без контроля четности, 8 бит данных, 1 стоп-бит, без управления потоком данных и скоростью порта 9600 бит/с.
Невозможно получить доступ в Интернет.	Проверьте соединение между ZyWALL и розеткой Ethernet, с которой имеется доступ в Интернет. Убедитесь, что устройство шлюза Интернет (например, модем DSL) работает нормально.
	В Панели навигации щелкните **WAN** для проверки параметров.
Невозможно установить соединение VPN.	Убедитесь, что ZyWALL и удаленный маршрутизатор IPSec используют одинаковые настройки VPN. В Панели навигации щелкните **VPN** для дополнительных настроек.
	Перейдите на какой-нибудь Web-сайт, чтобы проверить подключение к Интернету.

9.1 Установка IP-адреса компьютера

В этом разделе описывается, как настроить компьютер на получение IP-адреса в операционной системе Windows 2000, Windows NT и Windows XP. Выполнение этой операции гарантирует, что компьютер сможет взаимодействовать с ZyWALL.

1 В Windows XP щелкните **Start** (Пуск), **Control Panel** (Панель управления).

В Windows 2000/NT щелкните **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления).

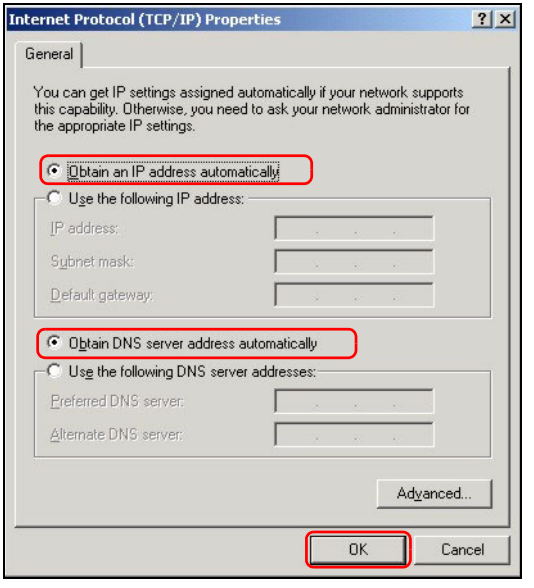
2 В Windows XP щелкните **Network Connections** (Сетевые подключения).

В Windows 2000/NT щелкните **Network and Dial-up Connections** (Сеть и удаленный доступ к сети).

3 Щелкните правой кнопкой мыши **Local Area Connection** (Подключение по локальной сети) и затем **Properties** (Свойства).

4 Выберите **Internet Protocol (TCP/IP)** (Протокол Интернета (TCP/IP)) (на закладке **General** (Общие) в WinXP) и щелкните **Properties** (Свойства).

5 Откроется окно **Internet Protocol TCP/IP Properties** (Свойства: Протокол Интернета (TCP/IP) (закладка **General** (Общие) в Windows XP). Выберите **Obtain an IP address automatically** (Получать IP-адрес автоматически) и **Obtain DNS server address automatically** (Получать адрес сервера DNS автоматически).



6 Щелкните **OK**, чтобы закрыть окно **Internet Protocol (TCP/IP) Properties** (Свойства: Протокол Интернета (TCP/IP)).

7 Щелкните **Close** (Закрыть) (**OK** в Windows 2000/NT), чтобы закрыть окно **Local Area Connection Properties** (Свойства подключения по локальной сети).

8 Закройте окно **Network Connections** (Сетевые подключения).

Порядок просмотра сертификата(ов) на изделие

1 Перейдите на сайт www.zyxel.ru.

2 Выберите изделие из раскрывающегося списка на домашней странице ZyXEL для перехода на страницу, посвященную этому изделию.

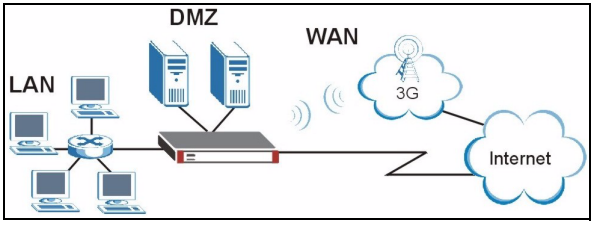
3 Выберите сертификат для просмотра.

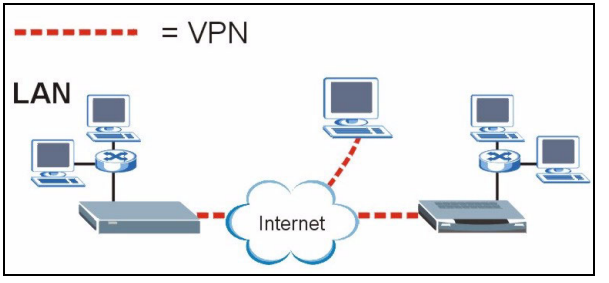
Översikt

ZyWALL 5 är en brandvägg med VPN, bandbreddshantering, innehållsfiltrering, anti-spam, anti-virus, IDP (Intrusion Detection and Protection) och många andra funktioner. Du kan använda den som en transparent brandvägg utan att behöva omkonfigurera ditt nätverk eller konfigurera ZyWALL:s routingfunktioner. När ZyWALL befinner sig i router-läge, kan du även sätta in ett trådlöst 3G-kort för att lägga till ett andra WAN. Din ZyWALL ökar nätverkssäkerheten genom att lägga till möjligheten att ändra portar från LAN till DMZ för användning av servrar med offentlig åtkomst. Denna guide omfattar de initiala anslutningar och konfiguration som krävs för att du ska kunna börja använda din ZyWALL i ditt nätverk.

Se manualen för mer information om alla funktioner.

Eventuellt behöver du ha tillgång till uppgifterna för din Internet anslutning.





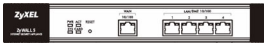
Denna guide är indelad i följande avsnitt.

1 Maskinvaruanslutningar
2 Åtkomst till webbkonfigurator
3 Bryggläge
4 Inställning av Internet-åtkomst och produktregistrering
5 DMZ
6 NAT
7 Brandvägg
8 Inställning av VPN-regel
9 Felsökning

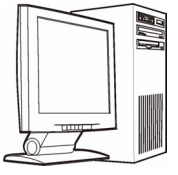
1 Maskinvaruanslutningar

Du behöver följande.

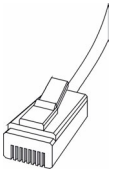
ZyWALL



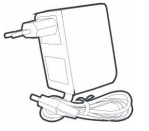
Dator



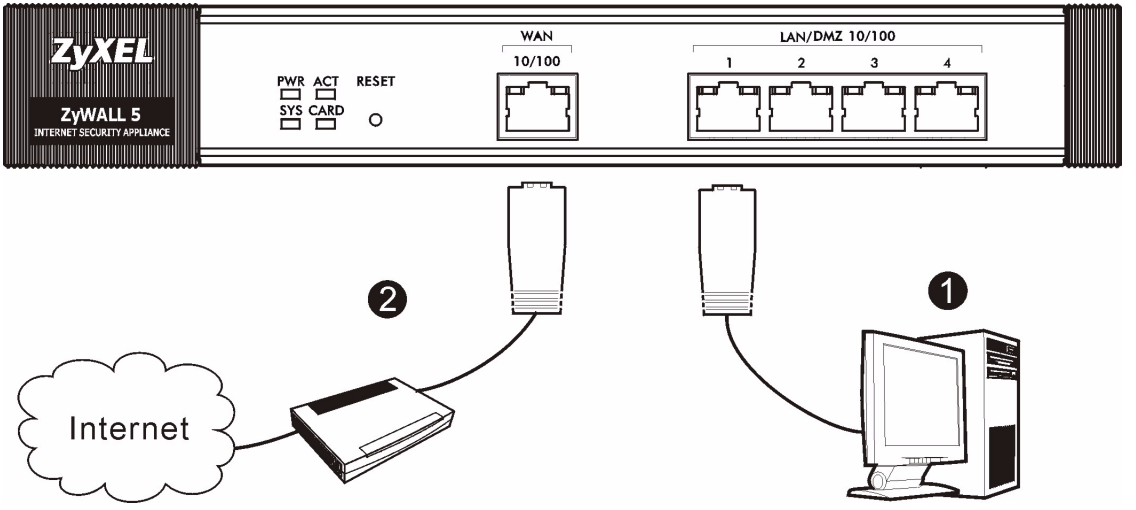
Nätverkskablar



Strömadapter

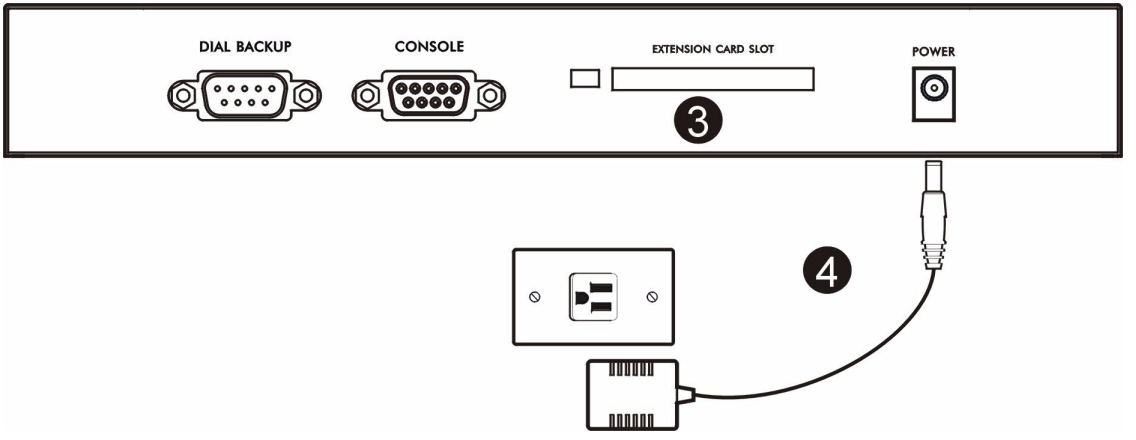


Gör följande för att utföra maskinvaruanslutningar för initial inställning.



1 Använd en Ethernet-kabel för att ansluta **LAN/DMZ**-porten till en dator. Om du konfigurerar dessa portar som DMZ-portar i **LAN** eller **DMZ**-menyn genom webbkonfiguratorn, kan du även använda Nätverkskablar för att ansluta offentliga servrar (webb, e-post, FTP osv) till **LAN/DMZ**-portarna.

2 Använd en annan Ethernet-kabel för att ansluta **WAN**-porten till en Internet-anslutning med Internet-åtkomst.



3 Sätt i ZyWALL Turbo-kortet för att använda anti-virus- och IDP-funktionerna eller sätt i ett trådlöst LAN-kort för att använda den trådlösa LAN-funktionen. Om du vill kan du sätta in ett trådlöst 3G-kort för att få trådlös åtkomst till Internet via ett 3G-nätverk. Se guiden till ZyWALL Turbo-kort för mer information. Se manualen angående installation av ett trådlöst LAN-kort. När detta skrivs kan du bara använda Sierra AC850/860 trådlöst 3G-kort i ZyWALL.

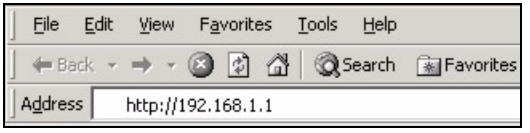
4 Använd den medföljande strömadaptern för att ansluta strömanslutningen (på bakpanelen) till ett eluttag.

5 Titta på frontpanelen. Indikatorlampan **PWR** tänds. Indikatorlampan **SYS** blinkar medan systemtest utförs och förblir därefter tänd om testet lyckats. Indikatorlamporna **ACT**, **CARD**, **LAN/DMZ** och **WAN** tänds och fortsätter att lysa om motsvarande anslutningar är rätt utförda.

2 Åtkomst till webbkonfigurator

Använd detta avsnitt för att konfigurera **WAN 1**-gränssnittet för Internet-åtkomst.

1 Öppna din webbläsare. Ange **192.168.1.1** (ZyWALL:s standard-IP-adress) som adress. Om inloggningsmenyen inte visas, se Avsnitt 9.1 för att ange din dators IP-adress.



2 Klicka på **Login** (standardlösenordet 1234 är redan angivet).

3 Ändra inloggningslösenordet genom att ange ett nytt lösenord och klicka på **Apply**.

4 Klicka på **Apply** för att ersätta ZyWALL:s digitala standardcertifikat.

5 Menyn **HOME** öppnas.

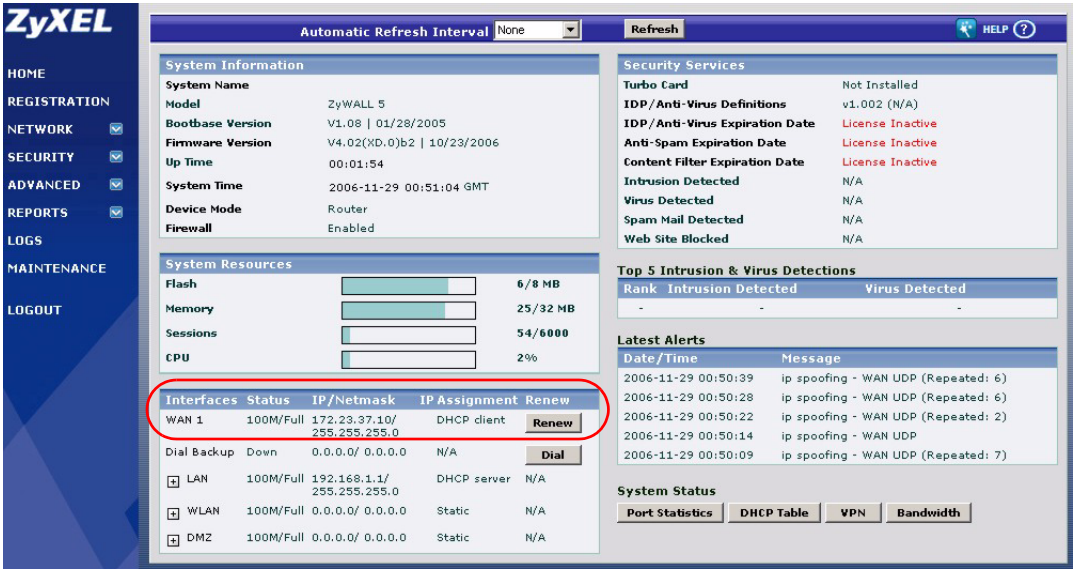
Din ZyWALL befinner sig i routerläge som standard. Fortsätt till nästa steg om du vill använda routingfunktioner som t ex NAT, DHCP och VPN.

Gå till Avsnitt 3 om du föredrar att använda din ZyWALL som en transparent brandvägg.

6 Kontrollera tabellen Network Status (nätverksstatus). Om **WAN 1**-status *inte är* **Down** och det finns en IP-adress, gå till Avsnitt 5.

Om status för **WAN 1** är **Down** (nere) (eller om IP-adress saknas), klicka på ikonen **Wizard** (guide) och använd Avsnitt 4 för att konfigurera **WAN 1**.

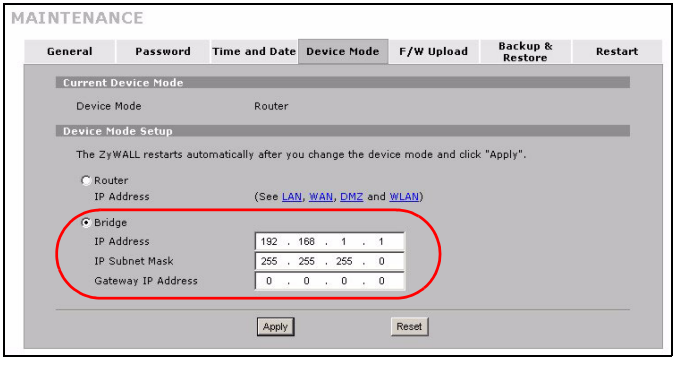
Använd **NETWORK WAN** -skärmarna om du måste konfigurera **WAN 2**. Du kan även konfigurera belastningsbalansering mellan WAN-anslutningarna.



3 Bryggläge

När du ställer in din ZyWALL i bryggläge, fungerar den som en transparent brandvägg. Gör följande för att ställa in ZyWALL på bryggläge.

1. Klicka på **MAINTENANCE** (underhåll) i navigationspanelen och klicka sedan på **Device Mode** (enhetsläge).
2. Välj **Bridge** (brygga) och konfigurera en (statisk) IP-adress subnetmask och gateway-IP-adress för ZyWALL:s **LAN-**, **WAN-**, **DMZ-** och **WLAN-**gränssnitt.
3. Klicka på **Apply**. ZyWALL startar om.



Gå direkt till Avsnitt 5 om du har servrar som måste kunna kommas åt från WAN-sidan.

4 Inställning av Internet-åtkomst och produktregistrering

1 Klicka på ikonen **Wizard** ( ) (guide) på skärmen **HOME** (hem) och klicka därefter på länken **Internet Access Setup** (inställning av Internet-anslutning) för att öppna guiden för Internet-anslutning.

Ange Internet-åtkomstinformationen exakt som du fått den.

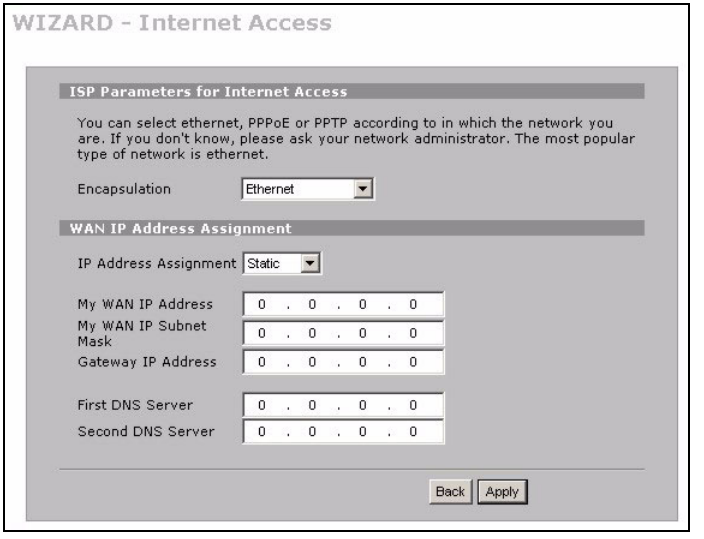
Om du fick en IP-adress som ska användas, välj **Static** i rullgardinslistrutan **IP Address Assignment** och ange den information du fått.

Fälten varierar beroende på vad du väljer i fältet **Encapsulation**. Fyll i den information du fått av din ISP eller nätverksadministratör.

Klicka på **Apply** när du är klar.

- **Ethernet-inkapsling**

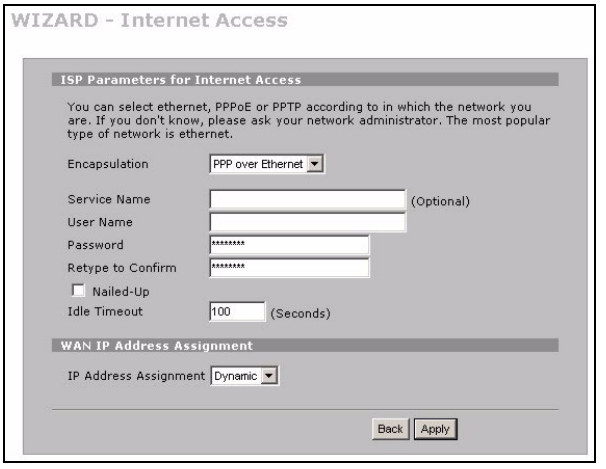
Konfigurera en Roadrunner-tjänst på menyn **NETWORK**, och sedan **WAN**.

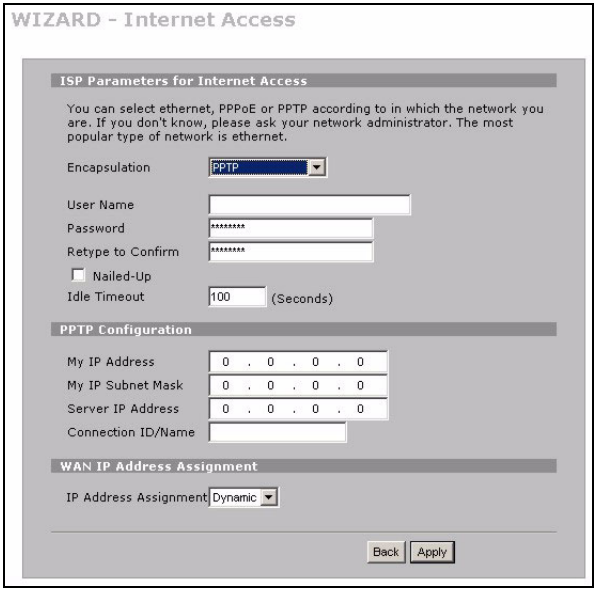


- **PPP over Ethernet eller PPTP**

Välj **Nailed-Up** när du vill att anslutningen ska vara aktiv jämt.

Om du inte vill att anslutningen ska vara aktiv jämt, specificera en timeout-period efter inaktivitet (i sekunder) i **Idle Timeout**.



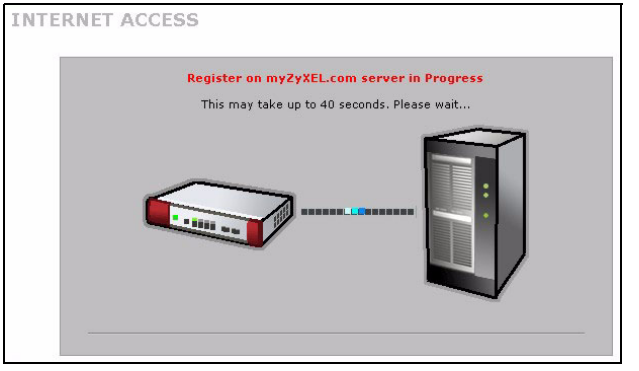


2 Klicka på **Next** för att visa menyn där du kan registrera din ZyWALL hos myZyXEL.com (ZyXEL:s online-servicecenter) och aktivera avgiftsfri innehållsfiltrering, anti-spam, anti-virus och IDP-testprogram. I annat fall klickar du på **Skip** och sedan på **Close** för att slutföra inställningen av Internet-åtkomst.

Kontrollera att du har installerat ZyWALL Turbo-kortet innan du aktiverar IDP- och anti-virus-prenumerationstjänster. Mer information om Turbokortet hittar du på www.zyxel.se.
Stäng av din ZyWALL innan du installerar eller tar bort ZyWALL Turbo-kortet.

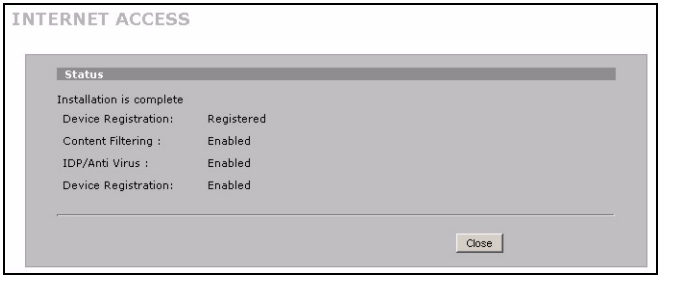
3 Om du redan har ett konto hos myZyXEL.com, välj **Existing myZyXEL.com account** och ange din kontoinformation. I annat fall väljer du **New myZyXEL.com account** och fyller i fälten nedan för att skapa ett nytt konto och registrera din ZyWALL. Klicka på **Next**.

4 Vänta tills registreringsprocessen är slutförd.



5 Följande meny visar om registreringen lyckades. Klicka på **Return** för att gå tillbaka till menyn **Device Registration** och kontrollera dina inställningar.

6 Klicka på **Close** för att lämna guidemenyen när registrering och aktivering är klar.



Om du vill aktivera en standardtjänst med ditt iCards PIN-nummer (licensnyckel), använd menyen **REGISTRATION Service**. Se manualen för mer information.

5 DMZ

DMZ (DeMilitarized Zone) låter offentliga servrar (webb, e-post, FTP osv) vara synliga för omvärlden och ändå vara brandväggsskyddade mot DoS-attacker (Denial of Service).

Du kan tilldela TCP/IP-konfiguration via DHCP till datorer anslutna till DMZ-portarna.Konfigurera annars datorerna med statiska IP-adresser (i samma subnet som DMZ-portarnas IP-adress) och DNS-serveradresser. Använd ZyWALL:s DMZ-IP-adress som standardgateway.

Gör följande för att konfigurera DMZ om ZyWALL befinner sig i routingläge.

Du behöver inte konfigurera DMZ med bryggläge, gå direkt till Avsnitt 7.

1 Klicka på **NETWORK** > **DMZ** i navigationspanelen.

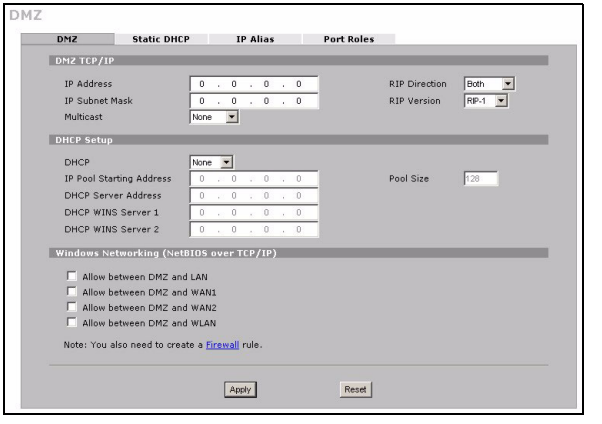
2 Specificera en IP-adress och subnetmask för DMZ-gränssnittet.

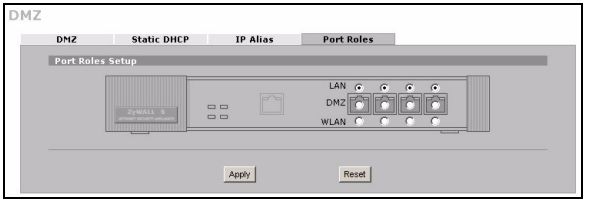
   Om du använder privata IP-adresser på DMZ, använd NAT för att göra servarna offentligt åtkomliga (se Avsnitt 6).

   En offentlig IP-adress måste vara på ett separat subnet från WAN-portens offentliga IP-adress. Om du inte konfigurerar NAT för offentliga IP-adresser på DMZ, dirigerar ZyWALL trafiken till den offentliga IP-adresserna på DMZ utan att utföra NAT. Detta kan vara praktiskt för värdservrar för NAT-fientliga tillämpningar.

3 Klicka på **Apply**.

4 Som standard är alla **LAN/DMZ**-portar 1 till 4 LAN-portar. För att konfigurera en port som en DMZ-port, klicka på fliken **Port Roles**, välj dess radioknapp funktion bredvid **DM**Z och klicka på **Apply**.



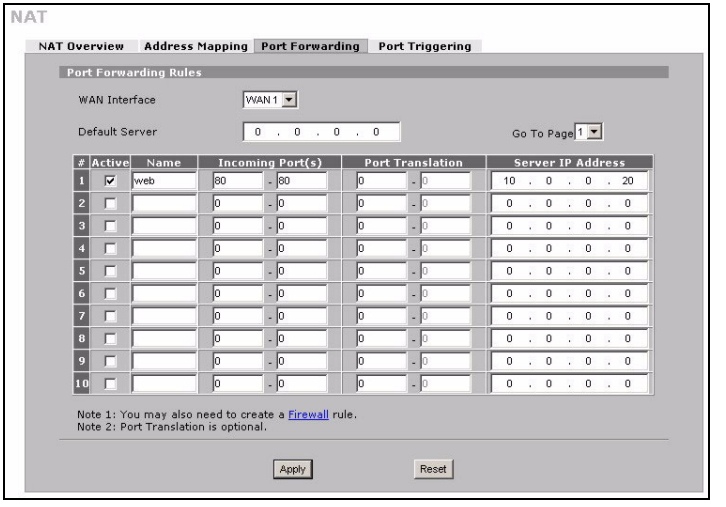


6 NAT

NAT (Network Address Translation - NAT, RFC 1631) innebär översättning av en IP-adress i ett nätverk till en annan IP-adress i ett annat. Du kan använda menyerna **NAT** > **Address Mapping** för att låta ZyWALL översätta flera offentliga IP-adresser till flera privata IP-adresser på ditt LAN (eller DMZ).

Följande exempel möjliggör åtkomst från WAN1 till en HTTP-server (webb) på DMZ. Servern har en privat IP-adress på 10.0.0.20.

1 Klicka på **ADVANCED** > **NAT** i navigationspanelen och sedan på **Port Forwarding**.
2 Välj den WAN-anslutning (**WAN1**) för vilken du vill konfigurera regler för portforwarding.
3 Välj kryssrutan **Active**.
4 Ange ett Name på regeln.
5 Ange det portnummer som tjänsten använder.
6 Ange HTTP-serverns IP-adress.
7 Klicka på **Apply**.



7 Brandvägg

Du kan använda din ZyWALL utan att konfigurera brandväggen.

ZyWALL:s brandvägg är förkonfigurerad att skydda ditt LAN från attacker från Internet. Som standard kan ingen trafik komma in i ditt LAN såvida inte en begäran först genererats från LAN sidan. ZyWALL tillåter åtkomst till DMZ från WAN eller LAN, men blockerar trafik från DMZ till LAN.

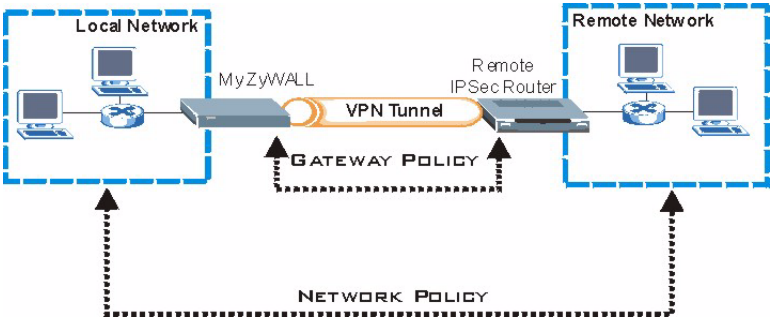
Om du använder din ZyWALL i routerläge, fortsätt med nästa avsnitt. För bryggläge, gå direkt till Avsnitt 9.

8 Inställning av VPN-regel

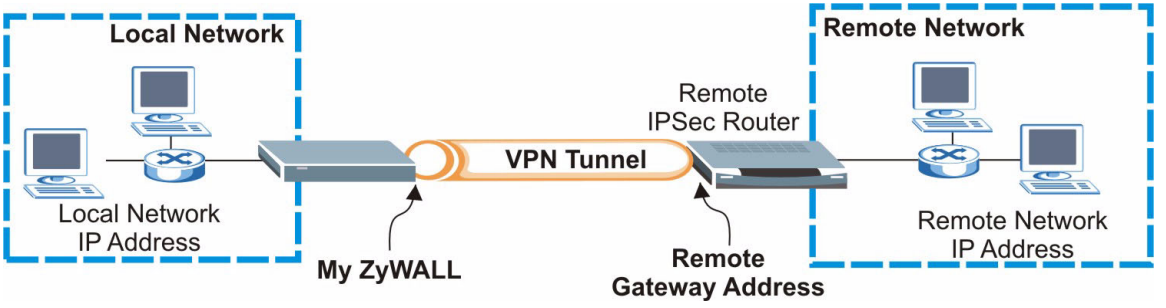
En VPN-tunnel (Virtual Private Network) ger dig en säker anslutning till en annan dator eller ett annat nätverk.

En gatewaypolicy identifierar IPSec-routrar i endera änden av en VPN-tunnel.

En nätverkspolicy specificerar vilka enheter (bakom IPSec-routrarna) som kan använda VPN-tunneln.



Denna figur hjälper dig att förstå huvudfälten i guidemenyarna.



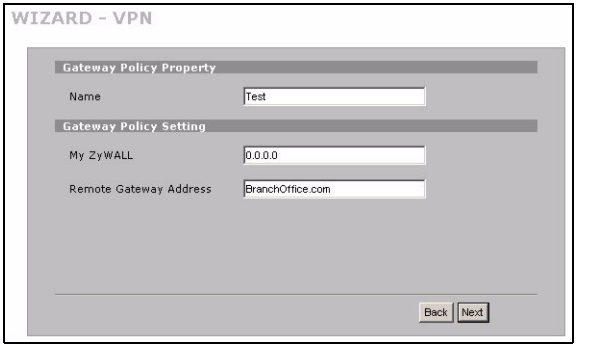
1 Klicka på ikonen **Wizard** ( ) (guide) på skärmen **HOME** (hem) och klicka därefter på länken **VPN Setup** (VPN-inställning) för att öppna VPN-guiden.

Dina inställningar sparas inte om du klickar på **Back**.

2 Använd denna meny för att konfigurera gatewaypolicyn.

Name: Ange ett Name för att identifiera gatewaypolicyn.

Remote Gateway Address: Ange IP-adress eller domännamn för fjärr-IPSec-routern.



3 Använd denna meny för att konfigurera nätverkspolicyn.

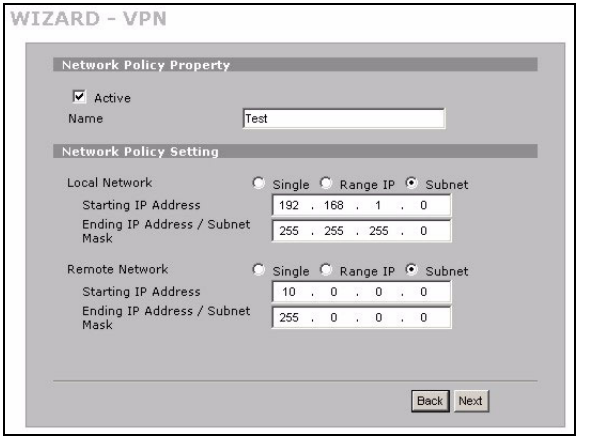
Låt kryssrutan **Active** förbli markerad.

Name: Ange ett Name för att identifiera nätverkspolicyn.

Välj **Single** och ange en IP-adress för en enda IP-adress.

Välj **Range IP** och ange inledande och avslutande IP-adresser för ett specifikt intervall av IP-adresser.

Välj **Subnet** och ange en IP-adress och subnetmask för att specificera IP-adresser på ett nätverk genom deras subnetmask.



Kontrollera att fjärr-IPSec-routern använder samma säkerhetsinställningar som du konfigurerar i de följande två menyarna.

Negotiation Mode (Förhandlingsläge): Välj **Main Mode** för identitetsskydd. Välj **Aggressive Mode** för att tillåta fler inkommande anslutningar från dynamiska IP-adresser för att använda separata lösenord.

Anslutning med flera SA:s (säkerhetsassociationer) genom en säker gateway måste ha samma förhandlingsläge.

Encryption Algorithm (Krypteringsalgoritm): Välj **3DES** eller **AES** för starkare (och långsammare) kryptering.

Authentication Algorithm (Autenticeringsalgoritm): Välj **MD5** för minimal säkerhet eller **SHA-1** för högre säkerhet.

Key Group (Nyckelgrupp): Välj **DH2** för högre säkerhet.

SA Life Time (SA-livstid): Ställ in hur ofta din ZyWALL omförhandlar IKE SA (minimum 180 sekunder). En kort SA-livstid ökar säkerheten, men omförhandling kopplar tillfälligt bort VPN-tunneln.

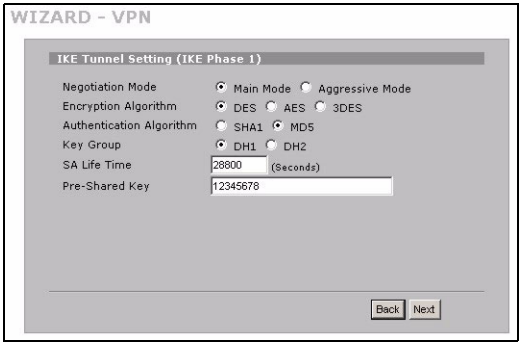
Pre-Shared Key (Fördelad nyckel): Använd 8 till 31 skiftlägeskänsliga ASCII-tecken eller 16 till 62 hexadecimala ("0-9", "A-F") tecken. Föregå en hexadecimal nyckel med "0x" (noll x), som inte räknas som en del av 16-62 teckenintervallet för nyckeln.

Encapsulation Mode (Inkapslingsläge): **Tunnel** är kompatibel med NAT, **Transport** är det inte.

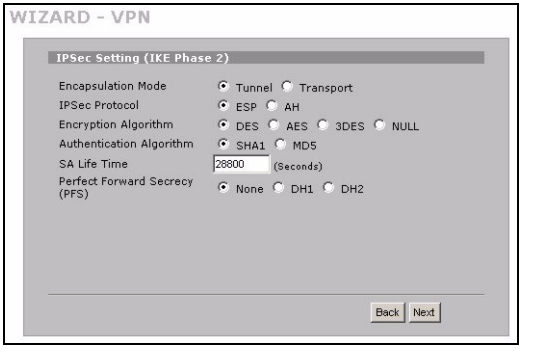
IPSec Protocol (IPSec-protokoll): **ESP** är kompatibel med NAT, **AH** är det inte.

PFS (Perfect Forward Secrecy): **None** (ingen) tillåter snabbare IPSec-inställning, men **DH1** och **DH2** är mer säkra.

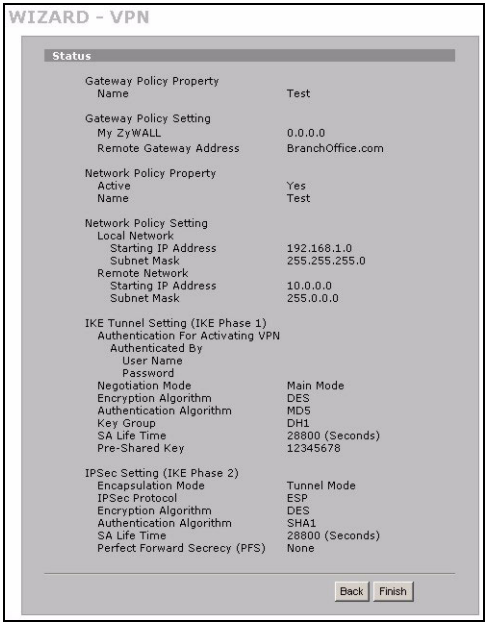
4 Använd denna meny för att konfigurera IKE (Internet Key Exchange) -tunnelinställningar.



5 Använd denna meny för att konfigurera IPSec-inställningar.



6 Kontrollera dina VPN-inställningar. Klicka på **Finish** för att spara inställningarna.

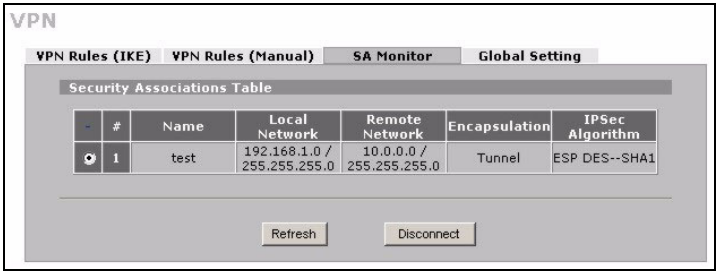


7 Klicka på **Close** i slutmenyen för att slutföra VPN-guideinställningen. Fortsätt med nästa avsnitt för att aktivera VPN-regeln och upprätta en VPN-anslutning.

8.1 Använda VPN-anslutningen

Använd VPN-tunnlar för att säkert skicka och hämta filer, och tillåta fjärråtkomst till bolagsnätverk, webbservrar och e-post. Tjänsterna fungerar som om du satt på kontoret i stället för att vara ansluten via Internet.

Till exempel tillåter “test” VPN-regeln säker åtkomst till en webbserver på ett fjärr-bolags-LAN. Ange serverns IP-adress (10.0.0.23 i detta exempel) som din webbläsares URL. ZyWALL bygger automatiskt upp VPN-tunneln när du försöker använda den.



Klicka på **SECURITY** > **VPN** i navigationspanelen och klicka sedan på fliken **SA Monitor** för att visa en lista över anslutna VPN-tunnlar (“test” VPN-tunneln finns här).

9 Felsökning

Problem	Åtgärd
Ingen indikatorlampa tänds.	Kontrollera att strömadaptern är ansluten till din ZyWALL och ansluten till en lämplig strömkälla. Kontrollera alla kablar.
	Om indikatorlamporna fortfarande inte tänds, kan du stå inför ett maskinvaruproblem. I sådant fall bör du kontakta din lokala återförsäljare.
Det går inte att få åtkomst till ZyWALL från LAN.	Kontrollera kablarna mellan din ZyWALL och din dator eller switch. Se Avsnitt 1 för mer information.
	Pinga ZyWALL från en LAN-dator. Kontrollera att datorns Ethernet-kort är installerat och fungerar som det ska. I datorn, klicka på **Start**, (**All**) **Programs**, **Tillbehör** och sedan **Kommandotolken**. I fönstret **Command Prompt**, skriv in "ping" följt av ZyWALL:s LAN IP-adress (192.168.1.1 är standard) och tryck sedan på [ENTER]. ZyWALL ska svara. I annat fall, se Avsnitt 9.1.
	Om du glömt din ZyWALL:s lösenord, använd knappen **RESET**. Tryck på knappen i ungefär 10 sekunder (eller tills indikatorlampan **SYS** börjar blinka), och släpp sedan upp den. Detta återställer alla fabriksvärden för ZyWALL (lösenord är 1234, LAN IP-adress 192.168.1.1 osv; se manualen för mer information).
	Om du har glömt din ZyWALL:s LAN eller WAN IP-adress, kan du kontrollera IP-adressen i SMT via konsolporten. Anslut din dator till porten **CONSOLE** med en seriekabel. Din dator ska ha ett terminalemuleringskommunikationsprogram (som t ex HyperTerminal) inställt på VT100 terminalemulering, ingen paritet, 8 databitar, 1 stoppbit, ingen flödeskontroll och 9600 bps porthastighet.
Det går inte att ansluta till Internet.	Kontrollera din ZyWALL:s anslutning till Ethernet-anslutningen med Internet. Kontrollera att Internet-gatewayenheten (t ex ett ADSL-modem) fungerar som den ska.
	Klicka på **WAN** i navigationspanelen för att verifiera dina inställningar.
Det går inte att upprätta en VPN-anslutning.	Kontrollera att din ZyWALL och fjärr-IPSec-routern använder samma VPN-inställningar. Klicka på **VPN** i navigationspanelen för att konfigurera avancerade inställningar.
	Öppan en webbsida för att kontrollera att din Internet-anslutning fungerar.

9.1 Ställa in datorns IP-adress

Detta avsnitt beskriver hur du ställer in din dator för att ta emot en IP-adress i Windows 2000, Windows NT och Windows XP. Detta säkerställer att din dator kan kommunicera med ZyWALL.

1 I Windows XP, klicka på **Start**, **Kontrollpanelen**.

I Windows 2000/NT, klicka på **Start**, **Inställningar**, **Kontrollpanelen**.

2 I Windows XP, klicka på **Nätverksanslutningar**.

I Windows 2000/NT, klicka på **Nätverk och uppringda anslutningar**.

3 Högerklicka på **LAN-anslutning** och klicka sedan på **Egenskaper**.

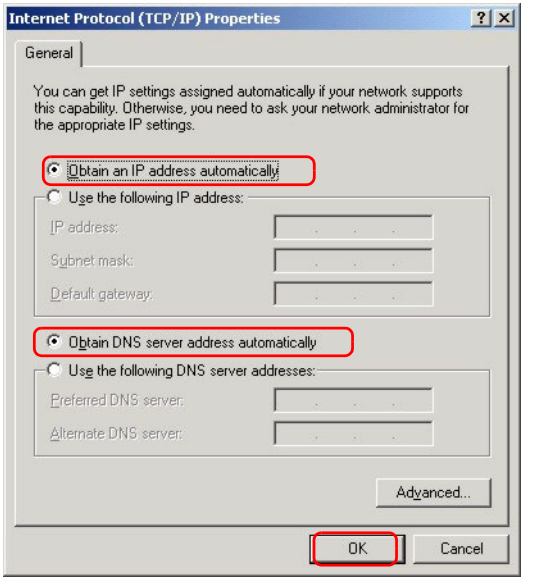
4 Välj **Internetprotokoll (TCP/IP)** (under fliken **Allmänt** i Windows XP) och klicka på **Egenskaper**.

5 Fönstret**Internetprotokoll TCP/IP Egenskaper** öppnas (fliken **Allmänt** i Windows XP). Välj alternativen **Skaffa IP-adress automatiskt** och **Skaffa DNS-serveradress automatiskt**.

6 Klicka på **OK** för att stänga fönstret **Internetprotokoll (TCP/IP) Egenskaper**.

7 Klicka på **Stäng** (**OK** i Windows 2000/NT) för att stänga fönstret **LAN-anslutning Egenskaper**.

8 Stäng menyen **Nätverksanslutningar**.



Procedur för att visa en produkts certifikat

1 Gå till www.zyxel.com.

2 Välj din produkt från rullgardinslistrutan på ZyXEL:s hemsida för att gå till denna produkts sida.

3 Välj det certifikat du vill titta på från denna sida.

Kundsupport

Ha följande information tillhands när du kontaktar kundsupporten.

- Produktmodell och serienummer.
- Garantiinformation.
- Datum då du tog emot din enhet.
- En kortfattad beskrivning av problemet och de åtgärder du vidtagit för att lösa det.

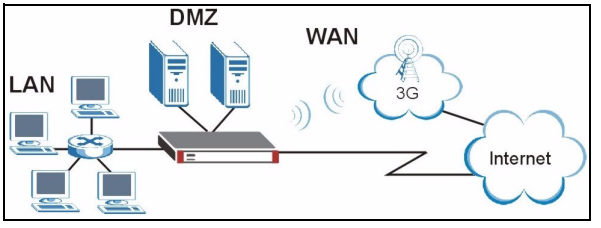
Se www.support.zyxel.se för ytterligare guider.

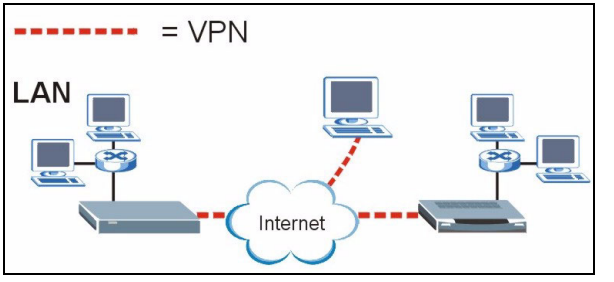
概述

ZyWALL 5 是状态监听型硬件防火墙，具备了虚拟私有网络（VPN）、带宽管理、内容过滤、防垃圾邮件、防病毒、入侵检测与防护（Intrusion detection and Protection, IDP）和多种其他功能。您可以将 ZyWALL 5 当作透明模式防火墙使用，而无须重设网路或设置 ZyWALL 的路由功能。当 ZyWALL 为路由器模式时，可插入 3G 无线网卡，新增第二个广域网。ZyWALL 增加了选项，能让您将端口角色从 LAN 更改为公用访问服务器可以使用的 DMZ，增强了网络的安全性。本手册的内容包括开始在网络中使用 ZyWALL 时，需要进行的初始连接和设置等相关信息。

请参阅 《用戶手册》，获取所有功能的详细信息。

您可能需要准备互联网连接信息。





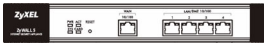
本手册的章节如下。

1 硬件连接
2 访问网络状态设置程序
3 桥接模式
4 互联网访问设置以及产品注册
5 DMZ
6 NAT
7 防火墙
8 VPN 规则设置
9 故障排除

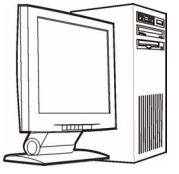
1 硬件连接

您需要以下设备。

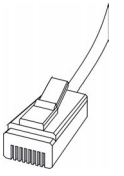
ZyWALL



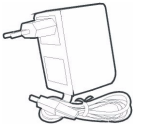
电脑



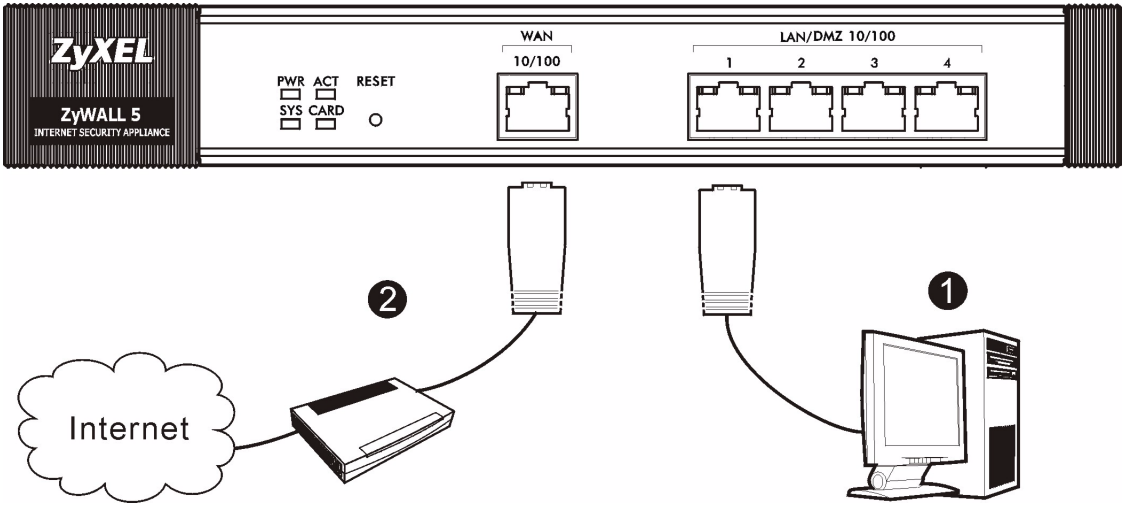
以太网连接线



电源适配器

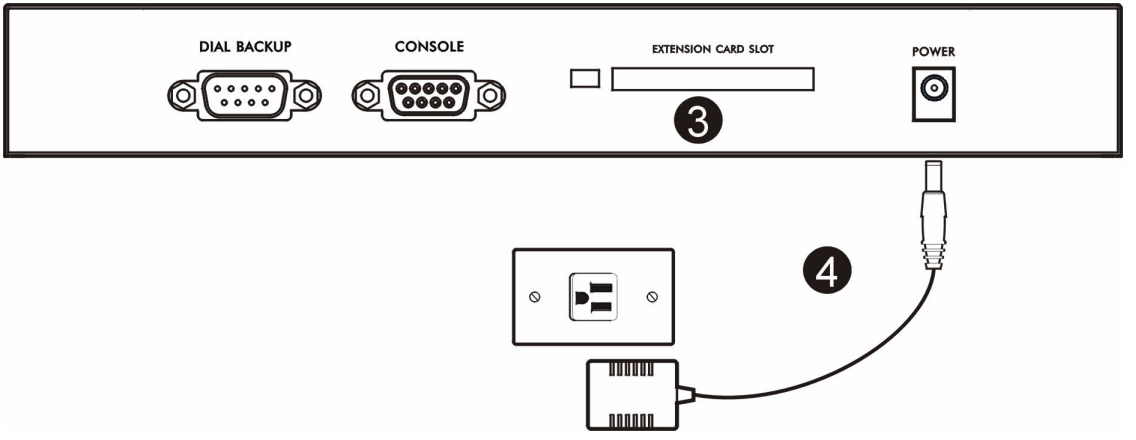


请执行下列步骤，为硬件连接进行初始设置。



1 使用以太网连接线连接 **LAN/DMZ** 连接端口和电脑。如果您通过网络状态配置程序，在 **LAN** 或 **DMZ** 屏幕中将这些端口配置为 DMZ 端口，则您也可以使用以太网连接线，将公用服务器（网络、电子邮件、FTP 等）连接到 **LAN/DMZ** 端口。

2 使用其他以太网连接线，将 **WAN** 端口连接到可以访问互联网的以太网接口。



3 插入 ZyWALL Turbo 扩展卡使用防病毒与入侵检测与防护（IDP）功能，或插入无线网卡使用无线网络功能。您可以选择插入 3G 无线网卡，通过 3G 网络接入因特网。如需更多有关扩展卡的信息，请参阅 ZyWALL Turbo 卡简介。若要安装无线网卡，请参阅用戶手册。 在撰写本文时，ZyWALL 仅能使用 Sierra AC850/860 3G 无线网卡。

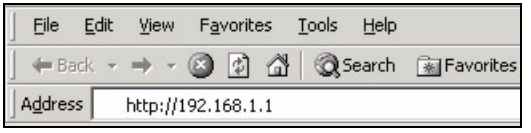
4 使用所附的电源适配器，为电源插槽（位于后方面板）接上电源。

5 观察前方面板。**PWR** 指示灯会亮起。**SYS** 指示灯会在执行系统测试时闪烁，测试成功时灯光会持续亮着。**ACT**、**CARD**、**LAN/DMZ** 和 **WAN** 指示灯会在相关连接正确时亮起并持续亮着。

2 访问网络状态设置程序

您可以使用本节中的信息来设置 **WAN 1** 接口的互联网访问。

1 启动网页浏览器。输入地址 **192.168.1.1**（ZyWALL 的默认 IP 地址）。
如果没有显示登录画面，请参阅章节 9.1，设置电脑的 IP 地址。



2 单击 **Login**（登录）（已经输入默认密码 **1234**）。

3 输入新的密码，然后单击 **Apply**（应用），更改登录密码。

4 单击 **Apply**（应用），取代原来 ZyWALL 的默认数字认证信息。

5 此时会打开 **HOME** 页面。

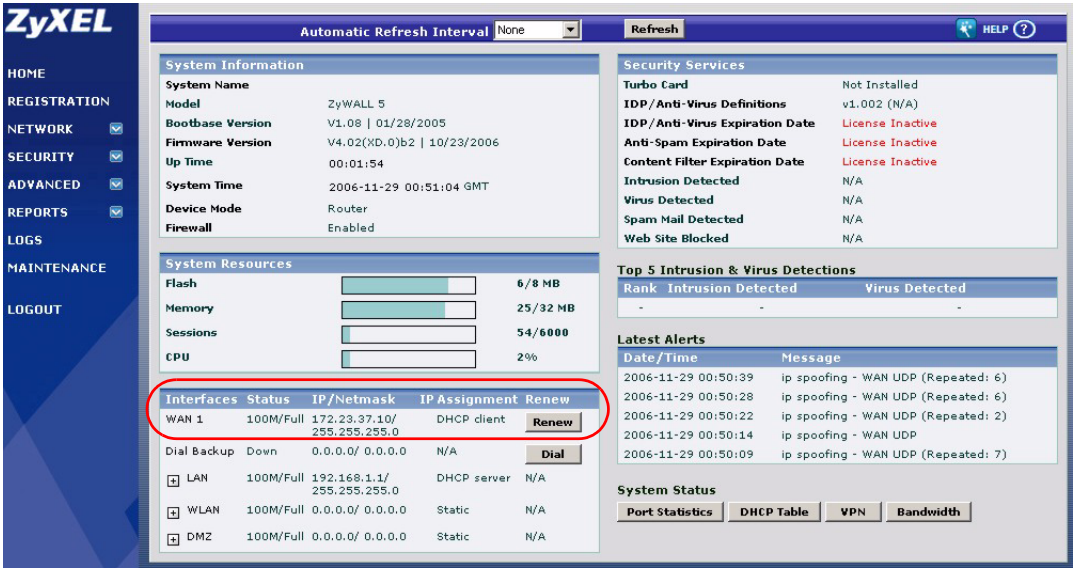
ZyWALL 默认会使用路由器模式。如果想要使用 NAT、DHCP 和 VPN 之类的路由功能，请继续下个步骤。

如果要将 ZyWALL 作为透明模式防火墙使用，请跳至章节 3。

6 查看 Network Status（网络状态）表格。如果 **WAN 1** 的状态并非 **Down**（无法运行），且表上显示了 IP 地址，请跳至章节 2。

如果 WAN 1 状态为 **Down**（关闭）（或没有显示 IP 地址），则按下 Wizard（向导）图示，并使用章节 4 的信息来设置 **WAN 1** 。

使用 **NETWORK WAN** 页面　可以设置 **WAN 2**　您也可以设定广域网联机之间的负载平衡。



3 桥接模式

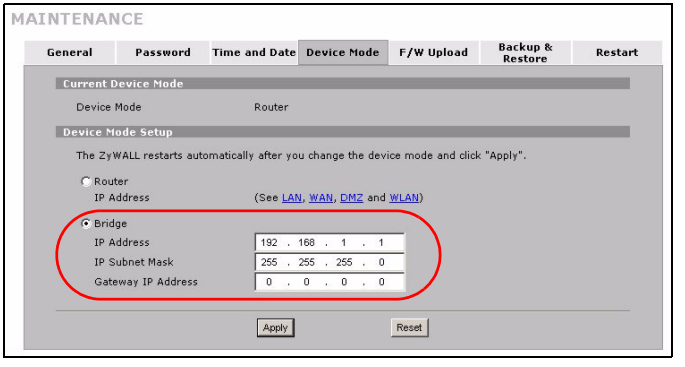
当您将 ZyWALL 设为桥接模式时，其功能即为透明模式防火墙。请进行下列步骤，将 ZyWALL 设为桥接模式。

1 单击导航面板上的 **MAINTENANCE**（维护），然后单击 **Device Mode**（设备模式）。

2 选取 **Bridge**（桥接），并为 ZyWALL 的 **LAN**、**WAN**、**DMZ** 和 **WLAN** 接口设置（静态）IP 地址子网掩码和网关 IP 地址。

3 单击 **Apply**（应用）。ZyWALL 会重新启动。

如果需要从 WAN 访问服务器，请跳至章节 2。



4 互联网访问设置以及产品注册

1 按下 HOME（首页）画面中的 Wizard（向导）图示（ ），再按下 Internet Access Setup（因特网接入设定）链接，启动因特网接入向导。

输入您的互联网访问信息。

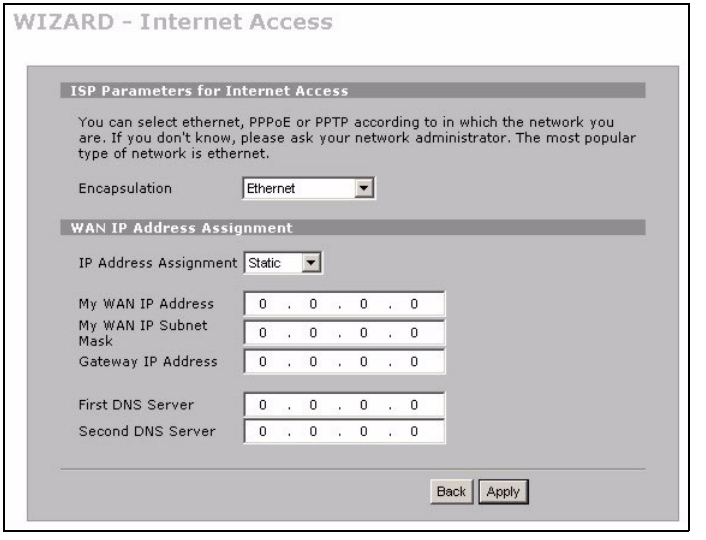
如果 ISP 为您提供了 IP 地址，请在 **IP Address Assignment**（IP 地址设置）下拉列表框中选取 **Static**（静态），然后输入提供的信息。

视您在 **Encapsulation**（封装）栏位中选取的项目而定，需要填入的栏位也会有所不同。请在这些栏位中填入 ISP 或网络管理员提供的信息。请在这些栏位中填入 ISP 或网络管理员提供的信息。

完成后，请单击 **Apply**（应用）。

- **Ethernet（以太网）封装**

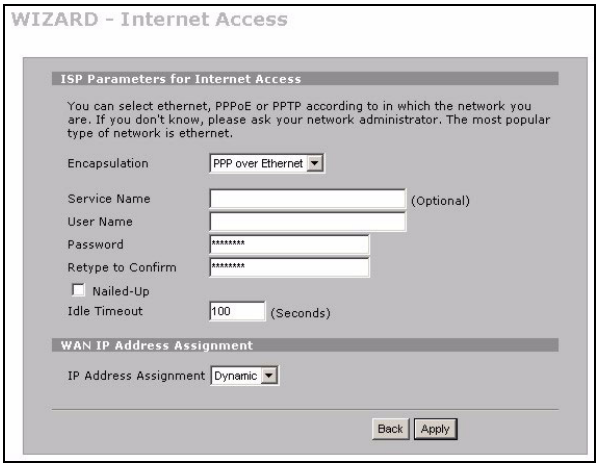
在 **NETWORK WAN** 页面中设置 Roadrunner 服务（使用 **WAN** 选项卡）。

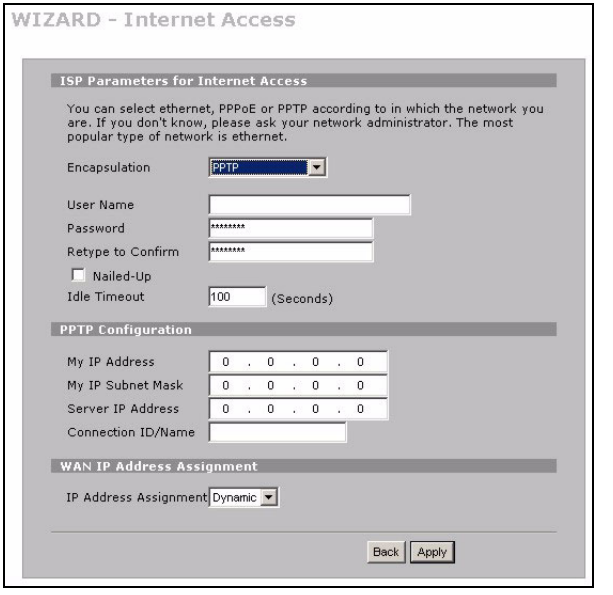


- **PPP over Ethernet 或 PPTP 封装**

如果您希望保持连接不中断，请选中 **Nailed-Up**（固定连接）（如果您的 ISP 是计算网络使用时间收费，而非收取固定月费，选这个选项可能会较为昂贵）。

如果不想一直保持连接状态，请在 **Idle Timeout**（闲置超时）中指定闲置等候时间（单位为秒）。





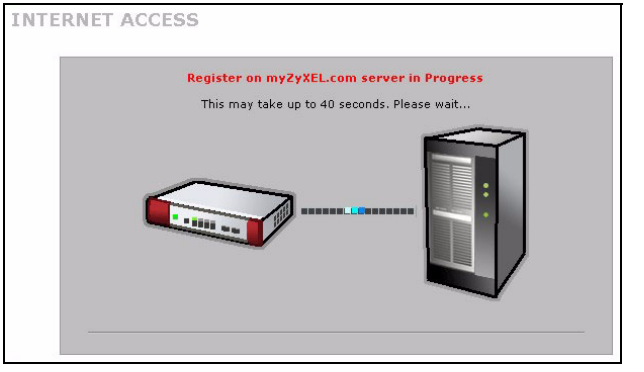
2 单击 **Next**（下一步）显示 **myZyXEL.com**（ZyXEL 在线服务中心）页面，您可在此进行 ZyWALL 产品的注册，激活具有内容过滤、防垃圾邮件、防病毒和入侵检测与防护功能的免费试用。若单击 **Skip**（跳过）再单击 **Close**（关闭），则结束网络连接建立。

在启用入侵检测与防护和防病毒订购服务之前，请确定您已安装 ZyWALL Turbo 卡。

在安装或移除 ZyWALL Turbo 卡 之前，请先关闭 ZyWALL。

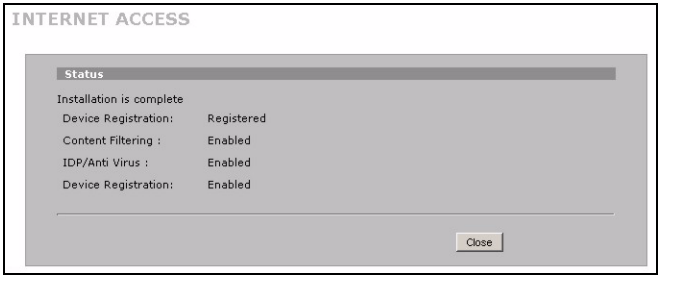
3 如果您有 myZyXEL.com 帐号，请选 **Existing myZyXEL.com account**（现有的 myZyXEL.com 帐号），再输入帐号信息。若无 myZyXEL.com 帐号，则选 **New myZyXEL.com account**（新的 myZyXEL.com 帐号），再填写下列栏位以建立新帐号并进行产品注册。单击 **Next**（下一步）。

4 等待注册完成。



5 如果注册失败则会显示下列画面。单击 **Return**（返回），回到 **Device Registration**（产品注册）页面，检查您的设置。

6 如果成功完成注册与产品启用，则单击 **Close**（关闭），离开向导屏幕。



若要使用 iCard 的 PIN 密码（授权识别码）启用标准服务，请使用 **REGISTRATION Service**（注册服务）屏幕。如需相关详细信息，请参阅使用手册。

5 DMZ

非军事网络区（DMZ）会让外部可以看见公用服务器（网络、电子邮件、FTP 等），但仍在防火墙的保护之下，不会受到 DoS（拒绝服务）攻击。

您可以通过 DHCP 将 TCP/IP 设置配置为连接至 DMZ 端口的电脑。或者，也可以为电脑设置静态 IP 地址（与 DMZ 端口的 IP 地址位于同一子网络）及 DNS 服务器地址。使用 ZyWALL 的 DMZ IP 地址作为默认网关。

如果 ZyWALL 处于路由模式，请执行下列步骤，设置 DMZ。

在桥接模式中不需要设置 DMZ，可以直接跳至章节 7。

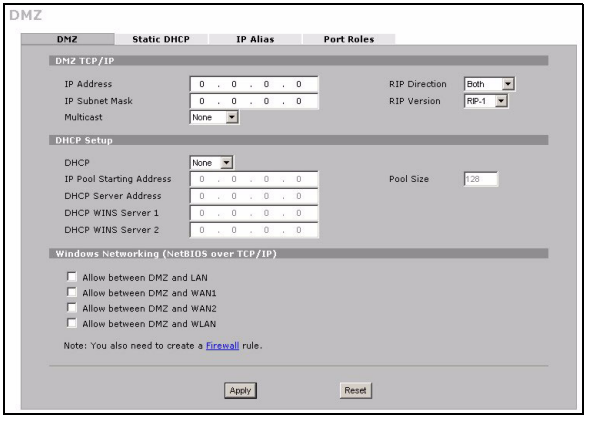
1 单击导航面板上的 **NETWORK**（网络）> **DMZ**。

2 为 DMZ 接口指定 IP 地址和子网掩码。

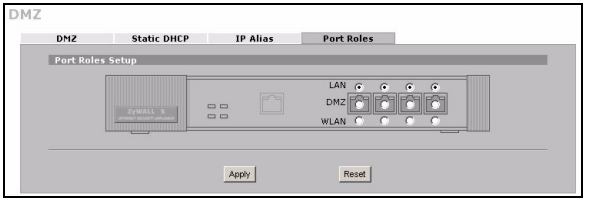
如果您在 DMZ 上使用私有 IP 地址，请使用 NAT，开放服务器公用访问（请参阅章节 6）。

公有 IP 地址必须和 WAN 端口的公有 IP 地址位于不同的子网络。如果您没有为 DMZ 上的公有 IP 地址设置 NAT，ZyWALL 会将流量路由传送到 DMZ 上的公有 IP 地址，而不会执行 NAT。对于不适合使用 NAT 的应用程式而言，这项功能在管理服务器方面非常有用。

3 单击 **Apply**（应用）。



4 默认情况下，**LAN/DMZ** 端口 1 到 4 都是 LAN 端口。要将端口配置为 DMZ 端口，请单击 **Port Roles（端口角色）**选项卡，选择 DMZ 旁边的单选按钮，然后单击 **Apply （应用）**。

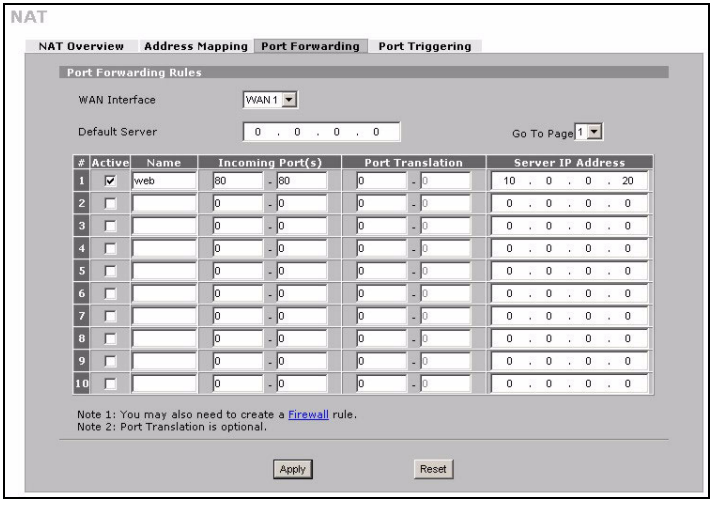


6 NAT

NAT（网络地址转换 - NAT，RFC 1631）代表从某个网络 IP 地址转换为其他网络的不同 IP 地址。您可以使用 **NAT Address Mapping**（NAT 地址映射）配置页面，设置 ZyWALL 在您的 LAN（或 DMZ）上将多个公共 IP 地址转换为多个私有 IP 地址。

在下面的例子中，会允许从 WAN 1 访问 DMZ 上的 HTTP（网络）服务器，而服务器的私有 IP 地址为 10.0.0.20。

1 单击导航面板上的 **ADVANCED**（高级）> **NAT**，然后选中 **Port Forwarding**（端口转发）。
2 选中欲设定连接端口转发规则的广域网联机（WAN1）。
3 选中 **Active**（启用）复选框
4 输入规则名称。
5 输入服务所使用的端口号。
6 输入 HTTP 服务器的 IP 地址。
7 单击 **Apply**（应用）。



7 防火墙

您可以不设置防火墙，直接使用 ZyWALL。

ZyWALL 的防火墙是预先设置的，可以保护 LAN 避免来自互联网的攻击。默认情况下，除非要求先在 LAN 上产生，否则不会有任何传输进入 LAN。ZyWALL 会允许从 WAN 或 LAN 访问 DMZ，但会封锁从 DMZ 到 LAN 的传输。

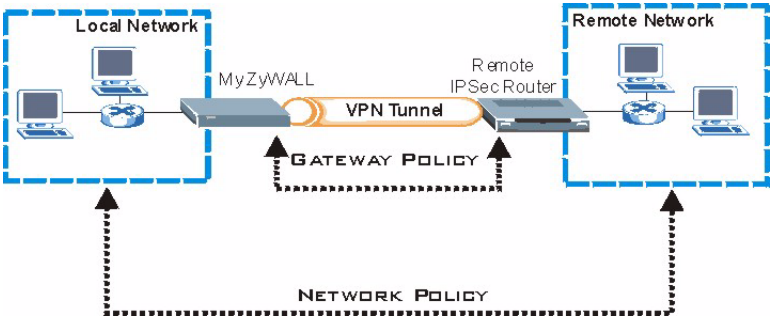
如果您以路由器模式使用 ZyWALL，请继续下一节的步骤。如果您使用桥接模式，请跳至章节 9。

8 VPN 规则设置

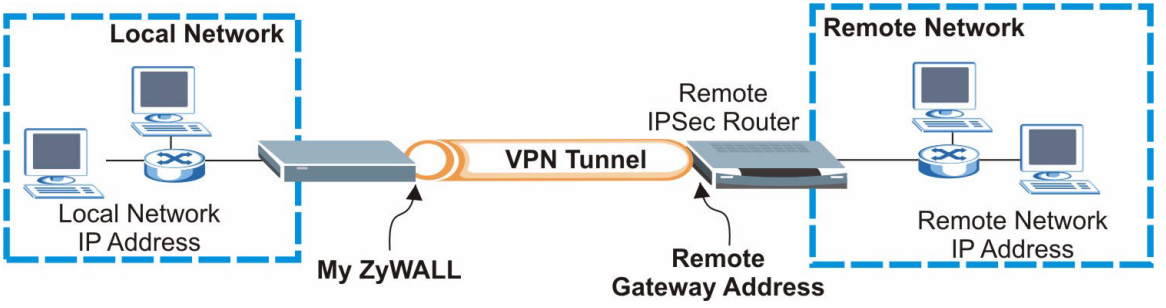
VPN（虚拟专用网络）通道可以让您安全的连接到其他电脑或网络。

网关规则会辨认 VPN 通道两端的 IPSec 路由器。

网络规则会指定哪些装置（位于 IPSec 路由器之后）能使用 VPN 通道。



下图会说明向导页面中出现的主要栏位。



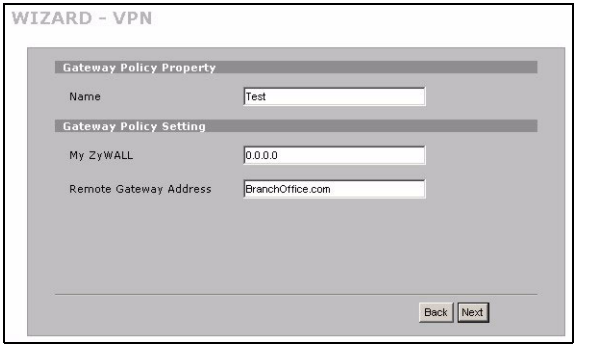
1 按下 HOME（首页）画面中的 Wizard（向导）图示（ ），再按下 VPN Setup（VPN 设定）链接，启动 VPN 向导。

如果您单击 **Back**（上一步），将不会保存您的设置。

2 您可以在这个页面中设置网关规则。

Name（名称）：为网关规则输入辨识名称。

Remote Gateway Address（远程网关地址）：输入远程 IPSec 路由器的 IP 地址或网络名称。



3 您可以在这个页面中设置网络规则。

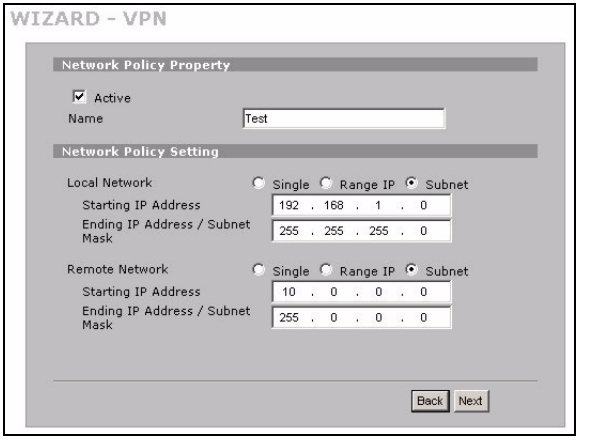
让 **Active**（启用）复选框保持选中状态。

Name（名称）：为网关规则输入辨识名称。

选中 **Single**（单一），并输入单一 IP 地址的 IP 地址。

选中 **Range IP**（IP 地址范围），并输入特定 IP 地址范围的起始和结束 IP 地址。

选中 **Subnet**（子网络），并输入 IP 地址和子网掩码，以子网掩码指定网络上的 IP 地址。



请确保远程 IPSec 路由器使用的设置，和您在下面两个画面中的安全性设置相同。

Negotiation Mode（协商模式）：选中 **Main Mode**（主要模式）可以提供身份识别保护功能。选中 **Aggressive Mode**（主动模式）可以允许较多来自动态 IP 地址的连入连接使用个别密码。

通过安全性网关连接的多重 SA（安全性关联）必须使用相同的协商模式。

Encryption Algorithm（加密算法）：选中 **3DES** 或 **AES** 会使用较安全（且速度较慢）的加密。

Authentication Algorithm（验证算法）：选中 **MD5** 会使用较低的安全性，**SHA-1** 的安全性则较高。

Key Group（密钥组）：选中 **DH2** 会使用较高的安全性。

SA Life Time（SA 时限）：设置 ZyWALL 重新协商 IKE SA 的频率（最低频率 180 秒）。较短的 SA 时限可以提高安全性，但协商会暂时中断 VPN 通道连接。

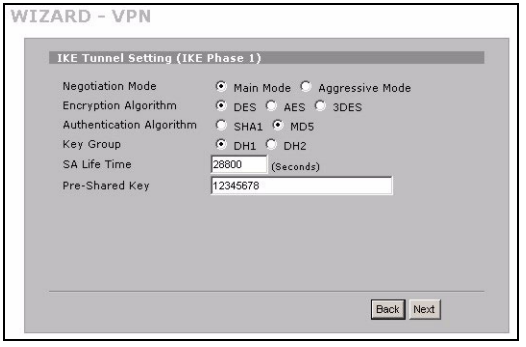
Pre-Shared Key（预共享密钥）：使用 8 到 31 个区分大小写的 ASCII 字符或 16 到 62 个十六进位（"0-9"，"A-F"）字符。在十六进位密钥之前加上 "0x"，而 "0x" 不包括在密钥的 16 到 62 个字符范围内。

Encapsulation Mode（封装模式）：**Tunnel**（通道）可与 NAT 同时应用，而 **Transport**（传输）则不可。

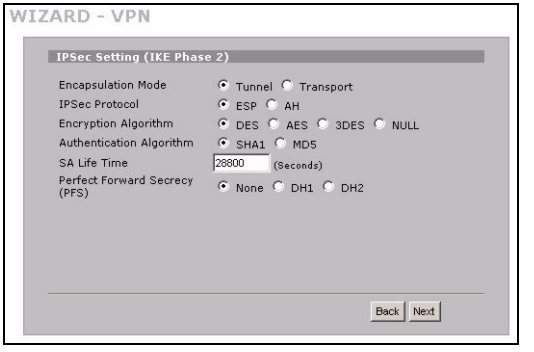
IPSec Protocol（IPSec 通信协议）：**ESP** 可与 NAT 同时应用，而 **AH** 则不可。

Perfect Forward Secrecy (PFS)（PFS- 完全转发安全）：选中 **None**（无）则让 IPSec 设置较快完成，但 **DH1** 和 **DH2** 较为安全。

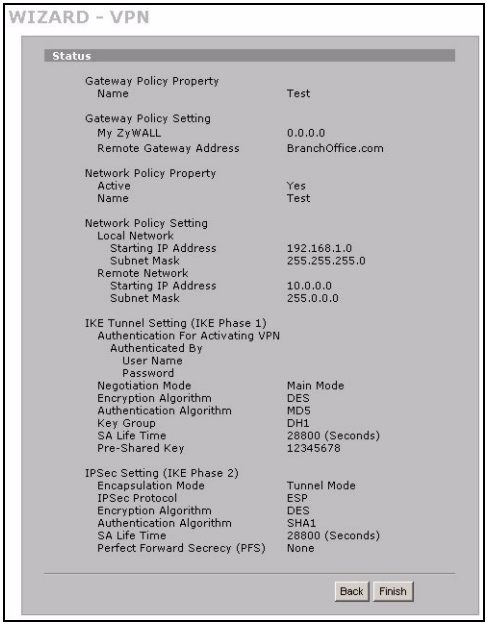
4 您可以在此页面中设置 IKE（互联网密钥交换）通道设置。



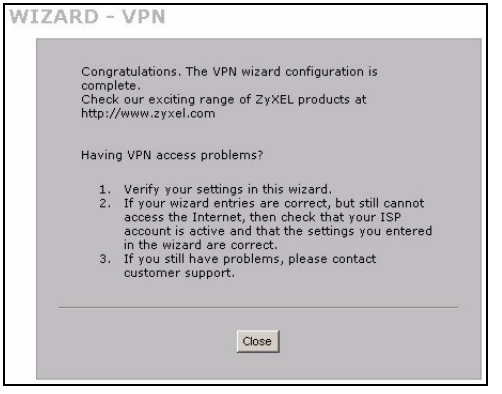
5 您可以在此页面中设置 IPSec。



6 检查 VPN 设置。单击 **Finish**（完成）保存设置。



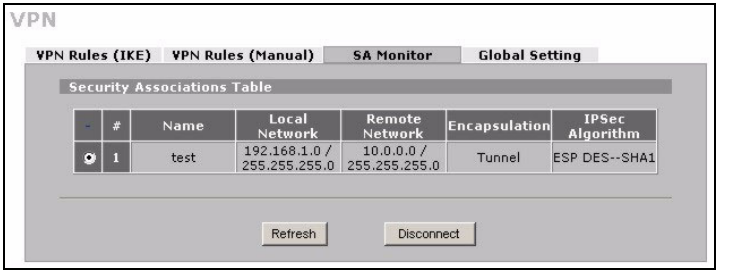
7 单击最后页面中的 **Close**（关闭），完成 VPN 向导的设置。 继续下一节的步骤，启用 VPN 规则并建立 VPN 连接。



8.1 使用 VPN 连接

使用 VPN 通道安全地传送和获取文件，并允许远程访问公司网络、网页服务器和电子邮件。服务的运行会和您在办公室的状况一样，不会像是通过互联网连接进行的。

例如，"test"（测试）VPN 规则可以让您安全地访问远程公司 LAN 上的网页服务器。将服务器的 IP 地址（在此范例中为 10.0.0.23）输入浏览器的 URL。ZyWALL 会在您尝试使用 VPN 通道时，自动建立 VPN 连接。



单击导航面板上的 **SECURITY**（安全）> **VPN**，然后选中 **SA Monitor**（SA 监视器）选项卡，显示连接的 VPN 通道列表（可以在这里找到"test" VPN 通道）。

9 故障排除

问题	解决方法
LED 全部不亮。	请确保已经将电源线接到 ZyWALL 设备上，且接上了适当的电源。检查所有网线是否正确连接。
	如果 LED 指示灯仍然不亮，则可能是硬件发生问题。如果是这种情况，请联系当地的供应商。
无法从 LAN 访问 ZyWALL。	检查 ZyWALL 和电脑或集线器之间的缆线连接。请参阅 章节 1，获得详细信息。
	从 LAN 电脑上 ping ZyWALL。请确认电脑上安装了以太网卡，且网卡能够正常工作。 在电脑中，单击**开始**、**（所有程序）程序集**、**附件**，然后单击**命令提示符**。在**命令提示符**窗口中，输入"ping"再输入 ZyWALL 的 LAN IP 地址（默认为 192.168.1.1），然后按 ENTER。ZyWALL 设备应该会有响应。如果仍然没有响应，请参阅 章节 9.1。
	如果忘记了 ZyWALL 的密码，请使用 **RESET**（重设）按钮。按住此按钮约 10 秒（或按住直到 **SYS** LED 指示灯亮起）后放开。按下此按钮会将 ZyWALL 还原为默认值（密码为 1234，而 LAN IP 地址为 192.168.1.1 等，请参阅《用户手册》，获得详细信息）。
	如果忘记了 ZyWALL 的 LAN 或 WAN IP 地址，可以通过管理设置端口（Console Port）检查 SMT 中的 IP 地址。使用控制台线缆（Console Port）将电脑连接到 **CONSOLE** 端口。您的电脑必须具有终端模拟通讯程式（例如超级终端），并进行以下设置：VT100 终端仿真模式、无同位、 8 数据位、 1 停止位、无数据流控制，以及端口速度 9600 bps。
无法访问互联网。	检查 ZyWALL 是否正确连接到可以访问互联网的以太网接口。确保互联网网关设备（例如 DSL 调制解调器）运行正常。
	单击导航面板上的 **WAN**，确认您的设置。

问题	解决方法
无法建立 VPN 连接。	确保 ZyWALL 和远程 IPSec 路由器使用相同的 VPN 设置。单击导航面板上的 VPN，进行高级设置。
	尝试访问某个网站，检查互联网连接是否正常。

9.1 设置电脑的 IP 地址

本节会说明如何在 Windows 2000、Windows NT 和 Windows XP 中，设置电脑接收 IP 地址。此项工作可以确保您的电脑能和 ZyWALL 设备通讯。

1 在 Windows XP 中，单击**开始**，然后单击**控制面板**。

在 Windows 2000/NT 中，依次按下**开始**、**设置**和**控制面板**。

2 在 Windows XP 中，单击**网络连接**。

在 Windows 2000/NT 中，单击**网络和拨号连接**。

3 在**本地连接**上单击鼠标右键，然后单击**属性**。

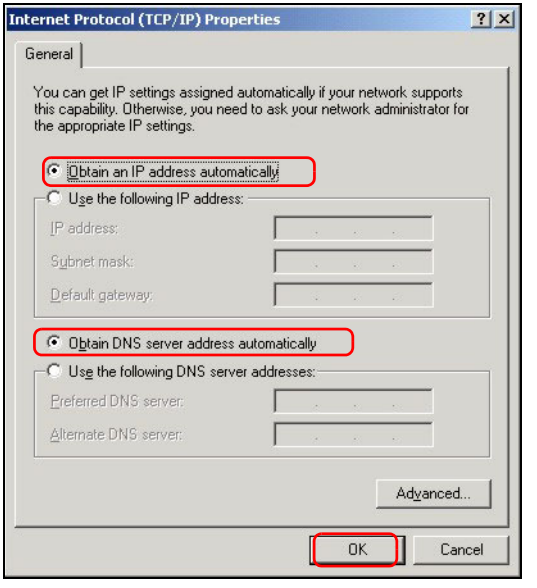
4 选中 **Internet Protocol (TCP/IP)**（在 Win XP 中位于**常规**选项卡上），然后单击**属性**。

5 此时会打开 **Internet Protocol TCP/IP 属性**窗口（在Win XP 中位于**常规**选项卡上）。选中**自动获得 IP 地址**和**自动获得 DNS 服务器地址**选项。

6 单击**确定**，关闭 **Internet Protocol (TCP/IP) 属性**窗口。

7 单击**关闭**（在 Windows 2000/NT 中为**确定**），关闭**本地连接属性**窗口。

8 关闭**本地连接**窗口。



查看产品认证信息步骤

1 访问 http://www.zyxel.cn/ 网站。

2 在合勤科技（ZyXEL）首页上的下拉列表框中选中所需的产品，跳至该产品的页面。

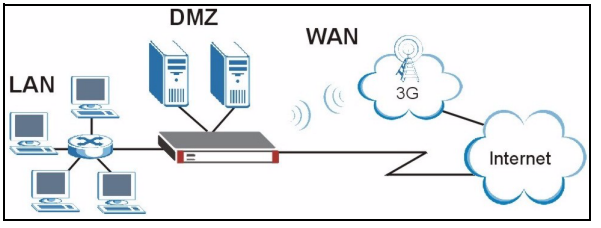
3 在页面中选中要查看的认证信息。

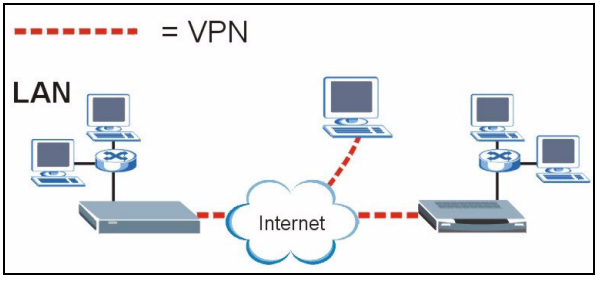
概觀

ZyWALL 5 是防火牆，具備了虛擬私有網路 (VPN)、頻寬管理、內容過濾、防垃圾郵件、防病毒、入侵偵測與防護（Intrusion detection and Protection, IDP）和多種其他功能。 您可以將 ZyWALL 5 當作透通模式防火牆使用，而無須重設網路或設定 ZyWALL 的路由功能。 當 ZyWALL 爲路由器模式時，您也可以插入 3G 無線網卡，新增第二個 WAN（廣域網路）。 ZyWALL 增加了選擇，能讓您將連接埠角色由 LAN 變爲公用存取伺服器可以使用的 DMZ，加強網路的安全性。本手冊的內容包括了開始在網路中使用 ZyWALL 時，所需進行的初始連線和設定等相關資訊。

請參閱《使用手冊》，取得所有功能的詳細資訊。

您可能需要準備網際網路連線資訊。



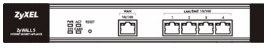


本手冊的章節如下。

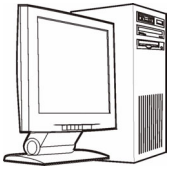
1 硬體連線

您需要以下裝備。

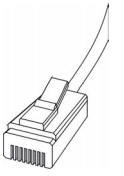
ZyWALL



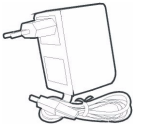
電腦



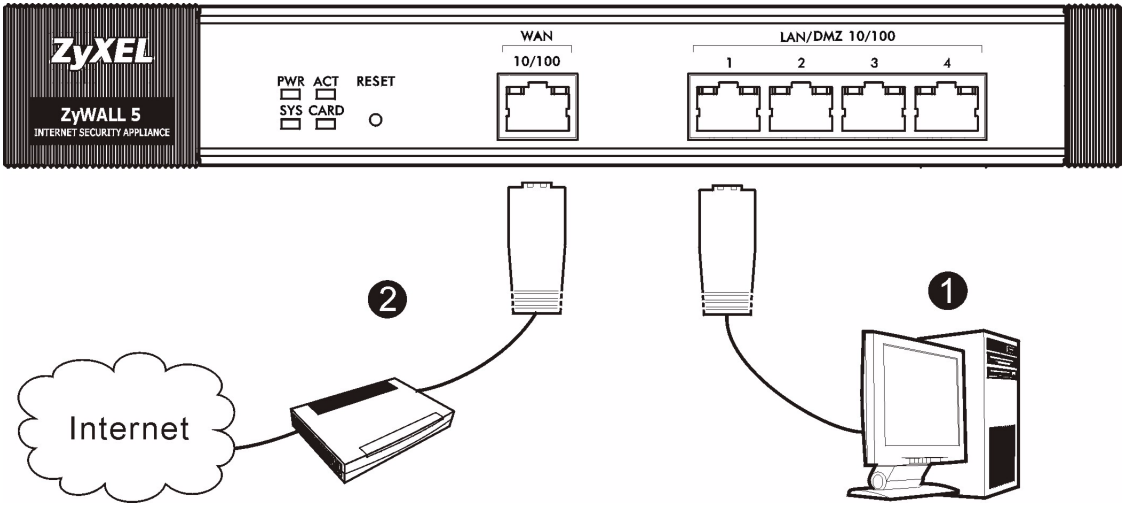
乙太網路線



電源供應器

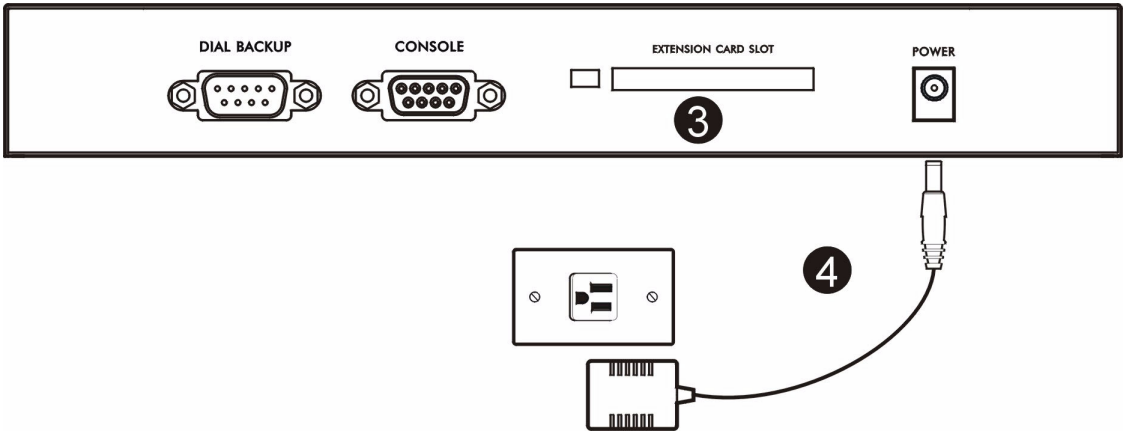


請進行下列步驟，爲硬體連線進行初始設定。



1 使用乙太網路線連接 **LAN/DMZ** 連接埠和電腦。如果您透過網路組態設定程式，在 **LAN** 或 **DMZ** 畫面中將這些連接埠設定爲 **DMZ** 連接埠，您也可以使用乙太網路線，將公用伺服器（網路、電子郵件、FTP 等）連接到 **LAN/DMZ** 連接埠。

2 使用另一條乙太網路線，將 **WAN** 連接埠連接到可以存取網際網路的乙太網路插孔。



3 插入 ZyWALL Turbo 擴充卡使用防毒與 IDP 功能，或插入無線網卡使用無線網路功能。您可以選擇插入 3G 無線網卡，透過 3G 網路接取網際網路。如需更多關於擴充卡的資訊，請參閱 ZyWALL Turbo 卡簡介。若要安裝無線網卡，請參閱使用手冊。在本文撰寫時，ZyWALL 僅能使用 Sierra AC850/860 3G 無線網卡。

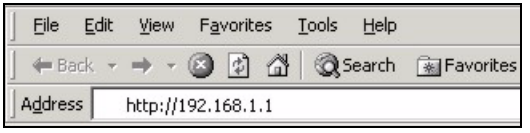
4 使用所附的電源供應器，爲電源插槽（位於後方面板）接上電源。

5 觀察前方面板。**PWR** 指示燈會亮起。**SYS** 指示燈會在在執行系統測試時閃爍，測試成功時燈光會持續亮著。**ACT**、**CARD**、**LAN/DMZ** 和 **WAN** 指示燈會在相關連接正確時亮起並持續亮著。

2 存取網路組態設定程式

您可以使用本節中的資訊設定 **WAN 1** 介面的網際網路存取。

1 啓動網頁瀏覽器。輸入位址 **192.168.1.1**（ZyWALL 的預設 IP 位址）。
如果沒有顯示登入畫面，請參閱章節 9.1，設定電腦的 IP 位址。



2 按一下 **Login**（登入）（已經輸入預設的密碼 1234）。

3 輸入新的密碼，然後按一下 **Apply**（套用），變更登入密碼。

4 按一下 **Apply**（套用），取代原本 ZyWALL 的預設數位檢定資訊。

5 會開啓 **HOME** 畫面。

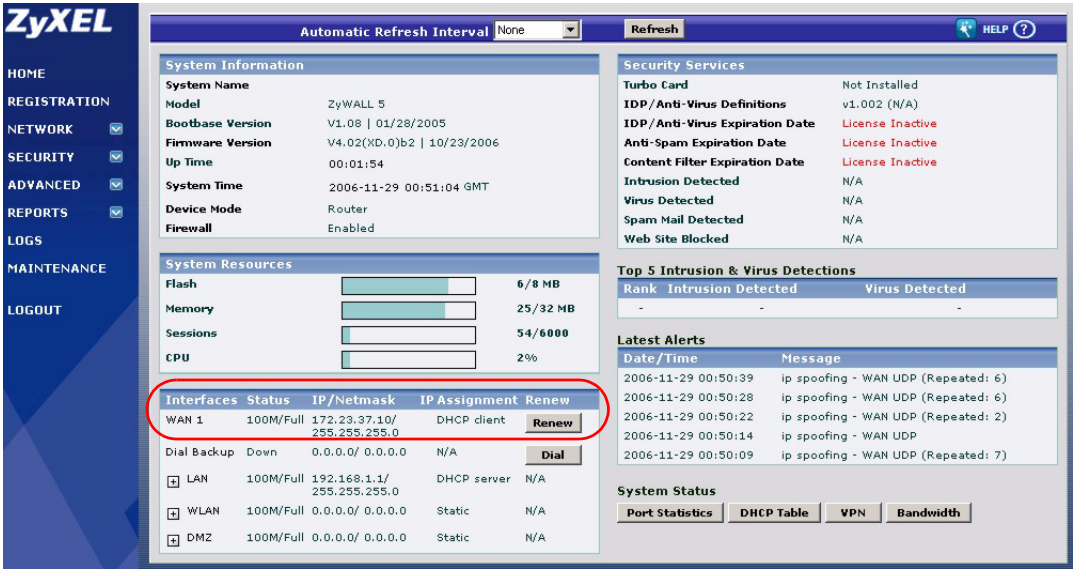
ZyWALL 預設會使用路由器模式。如果想要使用 NAT、DHCP 和 VPN 之類的路由功能，請繼續下個步驟。

如果要將 ZyWALL 做爲透通模式防火牆使用，請移至章節 3。

6 查看 Network Status（網路狀態）表格。如果 **WAN 1** 的狀態*並非* **Down**（無法運作），且表上顯示了 IP 位址，請移至章節 5。

如果 **WAN 1** 狀態爲 **Down**（關閉）（或沒有 **IP** 位址），按一下 **Wizard**（精靈）圖示，使用章節 4 的資訊設定 **WAN 1**。

如果需要設定 **WAN 2**，請使用 **NETWORK WAN** 畫面。您也可以設定 WAN(廣域網路) 連線之間的負載平衡。

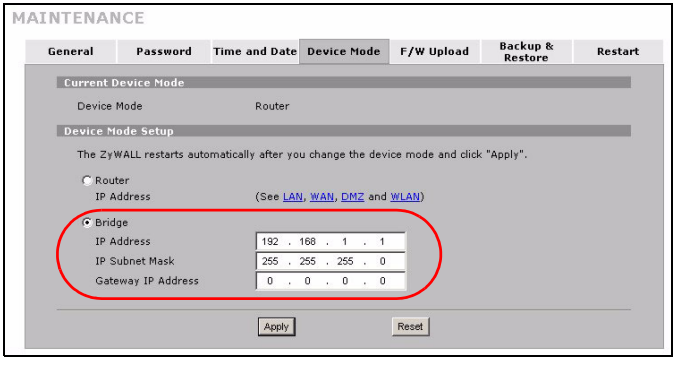


3 橋接模式

當您將 ZyWALL 設爲橋接模式時，其功能即爲透通模式防火牆。請進行下列步驟，將 ZyWALL 設爲橋接模式。

1 按一下導覽面板上的 **MAINTENANCE**（維護），然後按一下 **Device Mode**（裝置模式）。
2 選取 **Bridge**（橋接），並爲 ZyWALL 的 **LAN**、**WAN**、**DMZ** 和 **WLAN** 介面設定（靜態）IP 位址子網路遮罩和閘道 IP 位址。
3 按一下 **Apply**（套用）。ZyWALL 會重新啓動。

如果需要從 WAN 存取伺服器，請跳至章節 5。



4 網際網路存取設定以及產品註冊

1 按一下 **HOME**（首頁）畫面中的 **Wizard**（精靈）圖示 ()，再按一下 **Internet Access Setup**（網際網路接取設定）連結，開啓網際網路接取精靈。

確實輸入您的網際網路存取資訊。

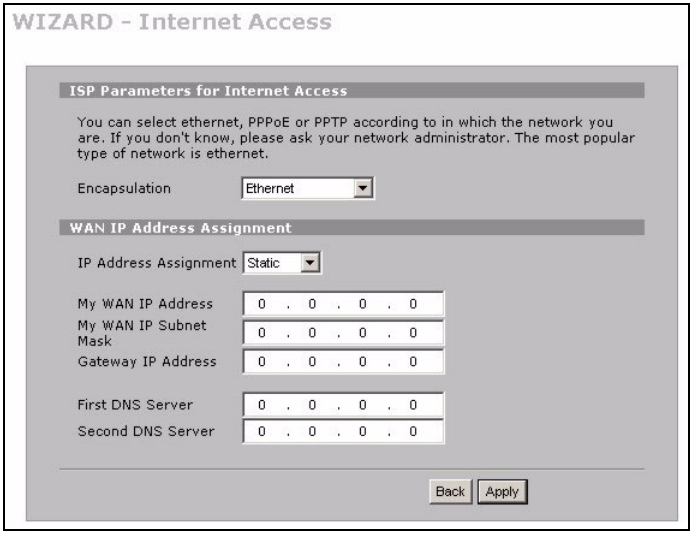
如果 ISP 有提供您 IP 位址，請在 **IP Address Assignment**（IP 位址設定）下拉式清單方塊中選取 **Static**（靜態），然後輸入提供的資訊。

視您在 **Encapsulation**（封裝）欄位中選取的項目而定，需要填入的欄位也會有所不同。請在這些欄位中填入 ISP 或網路管理員提供的資訊。

完成後，請按一下 **Apply**（套用）。

- **Ethernet（乙太網路）封裝**

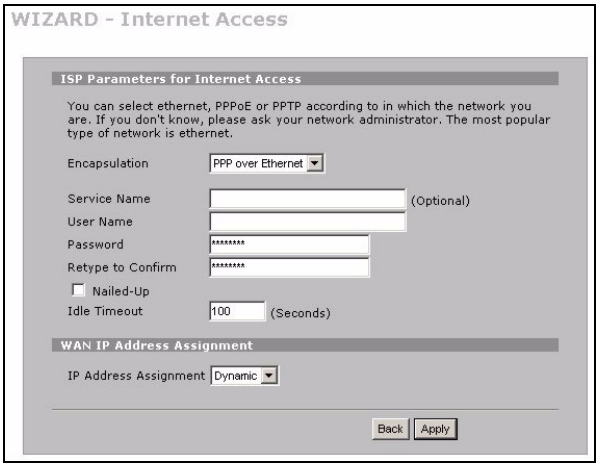
在 **NETWORK WAN** 畫面中設定 Roadrunner 服務（使用 **WAN** 標籤）。

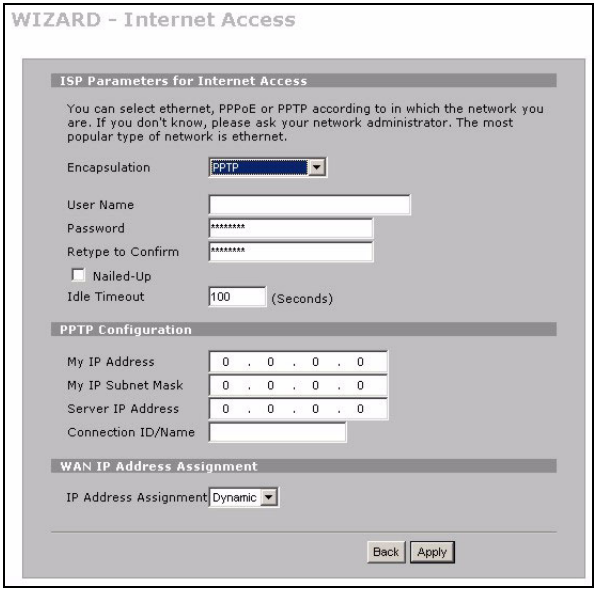


- **PPP over Ethernet 或 PPTP 封裝**

如果您希望保持連線不中斷，請選取 **Nailed-Up**（固定連線）（如果您的 ISP 是計算網路使用時間收費，而非收取固定月費，選這個選項可能會較爲昂貴）。

如果不想一直保持連線狀態，請在 **Idle Timeout**（閒置等候時間）中指定閒置等候時間（單位爲秒）。





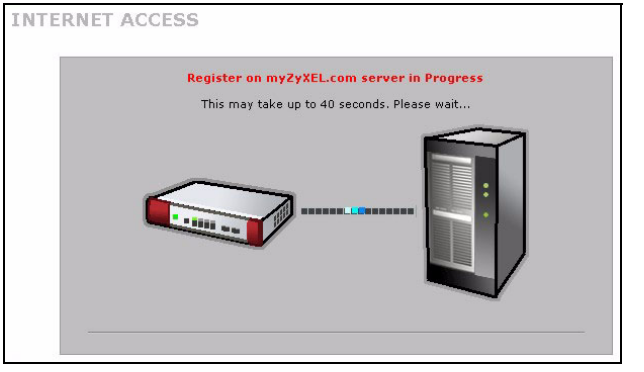
2 按一下 **Next**（下一步）顯示 myZyXEL.com（ZyXEL 線上服務中心）頁面，您可在此進行 ZyWALL 產品的註冊，啓用具有內容過濾、防垃圾郵件、防病毒和 IDP 功能的免費試用。若按 **Skip**（跳過）再按 **Close**（關閉），則結束網路連線建立。

在啓用 IDP 和防毒訂購服務之前，請確定您已安裝 ZyWALL Turbo 卡。

在安裝或移除 ZyWALL Turbo 卡之前，請先關閉 ZyWALL。

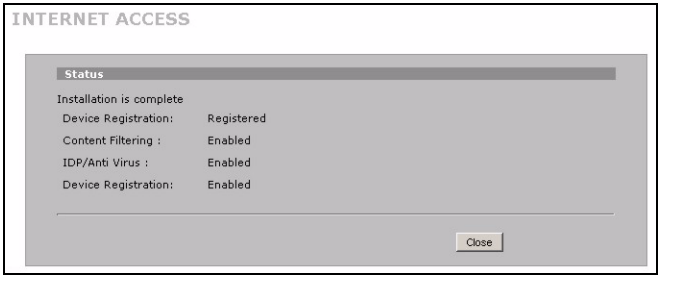
3 如果您有 myZyXEL.com 帳號，請選取 **Existing myZyXEL.com account**（現有的 myZyXEL.com 帳號），再輸入帳號資訊。若無 myZyXEL.com 帳號，則選取 **New myZyXEL.com account**（新的 myZyXEL.com 帳號），再填寫下列欄位以建立新帳號並進行產品註冊。按一下 **Next**（下一步）。

4 等待註冊完成。



5 如果註冊失敗會顯示下列畫面。按一下 **Return**（返回），回到 **Device Registration**（產品註冊）畫面，檢查您的設定。

6 如果成功完成註冊與產品啓用，則按一下 **Close**（關閉），離開精靈畫面。



若要利用 iCard 的 PIN 密碼（授權識別碼）啓用標準服務，請利用 **REGISTRATION Service**（註冊服務）畫面。如需相關詳細資料，請參閱使用手冊。

5 DMZ

非軍事網域區 (DMZ) 會讓外部可以看見公用伺服器（網路、電子郵件、FTP 等），但仍在防火牆的保護之下，不會受到 DoS（拒絕服務）攻擊。

您可以透過 DHCP 將 TCP/IP 設定指派給連接到 DMZ 連接埠的電腦。或者，也可以爲電腦設定靜態 IP 位址（與 DMZ 埠的 IP 位址位於同一子網路）及 DNS 伺服器位址。使用 ZyWALL 的 DMZ IP 位址做爲預設閘道。

如果 ZyWALL 處於路由模式，請進行下列步驟，設定 DMZ。

在橋接模式中不需要設定 DMZ，可以直接跳至章節 7。

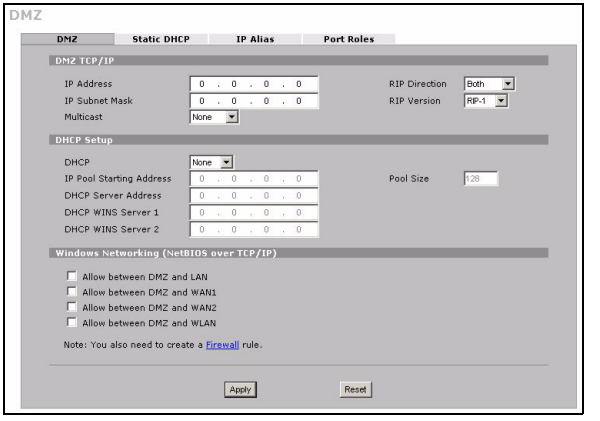
1 按一下導覽面板上的 **NETWORK**（網路）> **DMZ**。

2 爲 DMZ 介面指定 IP 位址和子網路遮罩。

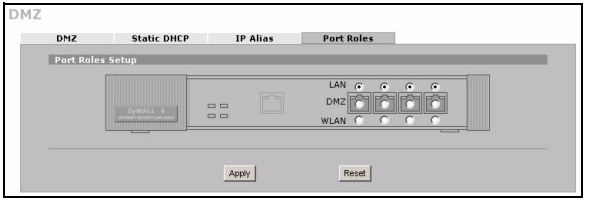
如果您在 DMZ 上使用私人 IP 位址，請使用 NAT，開放伺服器公用存取（請參閱章節 6）。

公開的 IP 位址必須和 WAN 連接埠的公開 IP 位址位於不同的子網路。如果您沒有爲 DMZ 上的公開 IP 位址設定 NAT，ZyWALL 會將流量路由傳送到 DMZ 上的公開 IP 位址，而不會執行 NAT。對於不適合使用 NAT 的應用程式而言，這項功能在管理伺服器方面非常有用。

3 按一下 **Apply**（套用）。



4 依照預設，**LAN/DMZ** 連接埠 1 到 4 都是 l LAN 連接埠。如果要將連接埠設爲 DMZ 連接埠，請按一下 **Port Roles**（連接埠角色）標籤，選取 **DMZ** 旁邊的圓形按鈕，然後按一下 **Apply**（套用）。

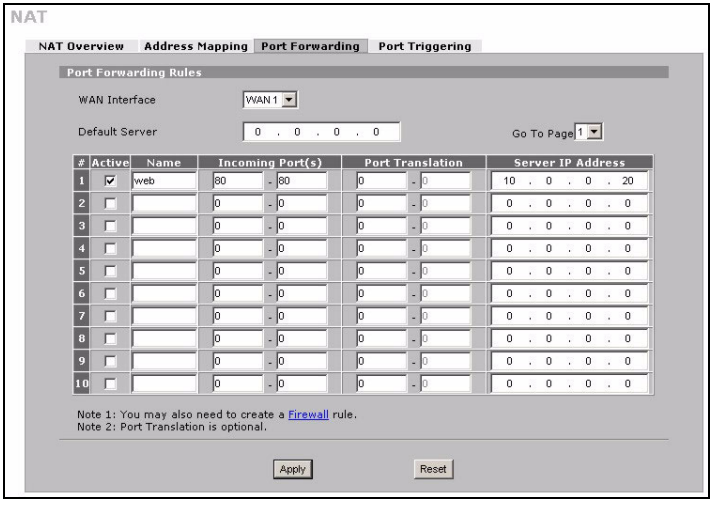


6 NAT

NAT（網路位址轉譯 - NAT，RFC 1631）代表從某個網路 IP 位址轉譯爲另一個網路的不同 IP 位址。您可以使用 **NAT Address Mapping**（NAT 位址對應）畫面，設定 ZyWALL 在您的 LAN（或 DMZ）上將多個公開 IP 位址轉譯爲多個私人 IP 位址。

在下面的例子中，會允許從 WAN1 存取 DMZ 上的 HTTP（網路）伺服器， 而伺服器的私人 IP 位址爲 10.0.0.20。

1 按一下導覽面板上的 **ADVANCED**（進階）> **NAT**，然後選取 **Port Forwarding**（連接埠轉遞）。
2 選取您要用來設定連接埠轉遞規則的廣域網路連線（**WAN1**）。
3 選取 **Active**（啓用）核取方塊。
4 輸入規則名稱。
5 輸入服務所使用的連接埠號碼。
6 輸入 HTTP 伺服器的 IP 位址。
7 按一下 **Apply**（套用）。



7 防火牆

您可以不設定防火牆，直接使用 ZyWALL。

ZyWALL 的防火牆是預先設定的，可以保護 LAN 免於受到來自網際網路的攻擊。依照預設，除非需求先在 LAN 上產生，否則不會有任何傳輸進入 LAN。ZyWALL 會允許從 WAN 或 LAN 存取 DMZ，但會封鎖從 DMZ 到 LAN 的傳輸。

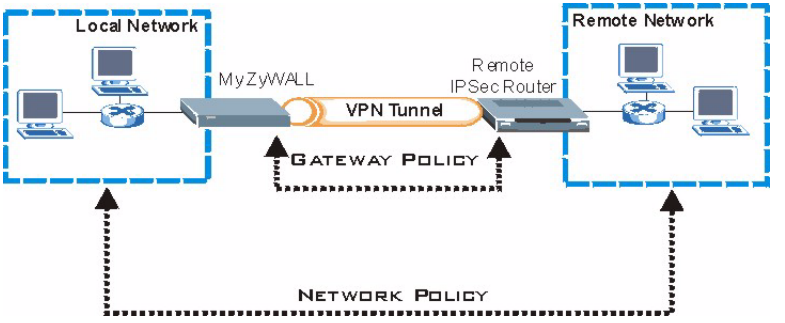
如果您以路由器模式使用 ZyWALL，請繼續下一節的步驟。如果您使用橋接模式，請跳至章節 9。

8 VPN 規則設定

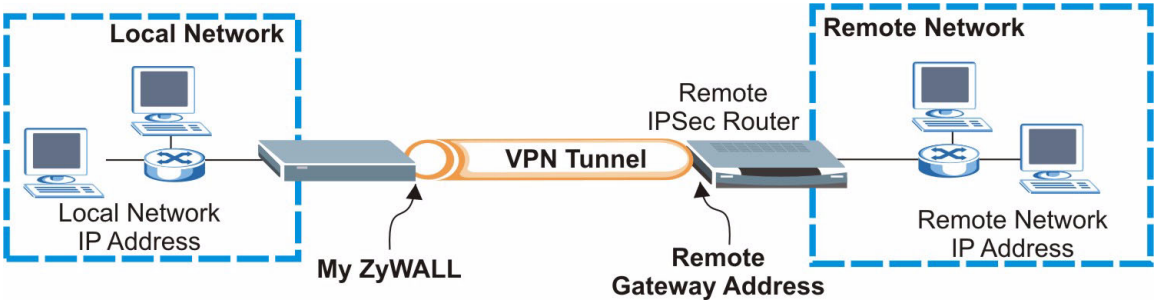
VPN（虛擬私有網路）通道可以讓您安全的連線到另一部電腦或網路。

閘道原則會辨識 VPN 通道兩端的 IPSec 路由器。

網路原則會指定哪些裝置（位於 IPSec路由器之後）能使用VPN通道。



下圖會說明精靈畫面中出現的主要欄位。



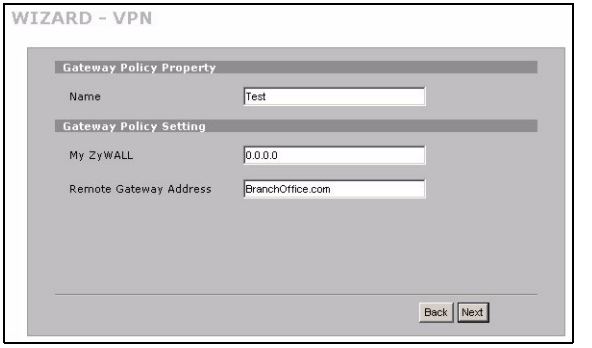
1 按一下 **HOME**（首頁）畫面中的 **Wizard**（精靈）圖示 ( ) ，再按一下 **VPN Setup**（VPN 設定）連結，開啓 VPN 精靈。

如果您按下 **Back**（上一步），將不會儲存您的設定。

2 您可以在這個畫面中設定閘道原則。

Name（名稱）：爲閘道原則輸入辨識名稱。

Remote Gateway Address（遠端閘道位址）:輸入遠端 IPSec 路由器的 IP 位址或網域名稱。



3 您可以在這個畫面中設定網路原則。

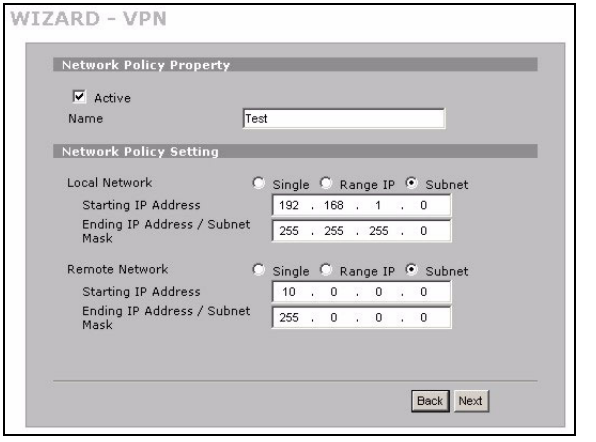
讓 **Active**（啓用）核取方塊保持選取狀態。

Name（名稱）：爲網路原則輸入辨識名稱。

選取 **Single**（單一），並輸入單一 IP 位址的 IP 位址。

選取 **Range IP**（IP 位址範圍），並輸入特定 IP 位址範圍的起始和結束 IP 位址。

選取 **Subnet**（子網路），並輸入 IP 位址和子網路遮罩，以子網路遮罩指定網路上的 IP 位址。



請確認遠端 IPSec 路由器使用的設定，和您在下面兩個畫面中的安全性設定相同。

Negotiation Mode（交涉模式）: 選取 **Main Mode**（主要模式）可以提供身份識別保護功能。選取 **Aggressive Mode**（主動模式）可以允許較多來自動態 IP 位址的連入連線使用個別密碼。

透過安全性閘道連線的多重 SA（安全性關聯）必須使用同樣的交涉模式。

Encryption Algorithm（加密演算法）：選取 **3DES** 或 **AES** 會使用較安全（且速度較慢）的加密。

Authentication Algorithm（驗證演算法）：選取 **MD5** 會使用較低的安全性，**SHA-1** 的安全性則較高。.

Key Group（金鑰組）：選取 **DH2** 會使用較高的安全性。

SA Life Time（SA 時限）:設定 ZyWALL 新交涉 IKE SA 的頻率（最低頻率 180 秒）。較短的 SA 時限可以增進安全性，但交涉會暫時中斷 VPN 通道連線。

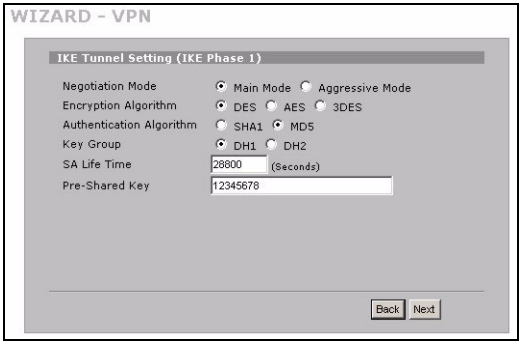
Pre-Shared Key（預先共用金鑰）：使用8到31個區分大小寫的ASCII字元或16到62個十六進位（"0-9"，"A-F"）字元。在十六進位金鑰之前加上 "0x"，而 "0x" 不包括在金鑰的 16 到 62 個字元範圍內。

Encapsulation Mode（封裝模式）：**Tunnel**（通道）與 NAT 相容，而 **Transport**（傳輸）則否。

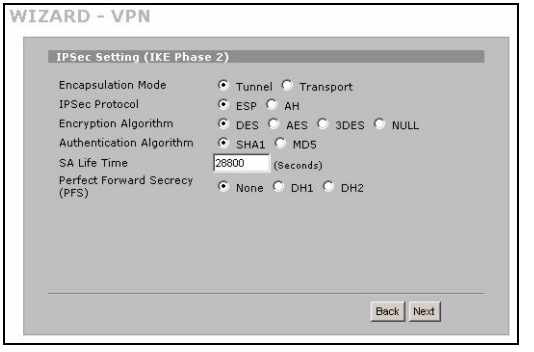
IPSec Protocol（IPSec 通訊協定）：**ESP** 與 NAT 相容，而 **AH** 則否。

Perfect Forward Secrecy (PFS)（完整向前保密）：選取 **None**（無）可以讓 IPSec 設定較快完成，但 **DH1** 和 **DH2** 較爲安全。

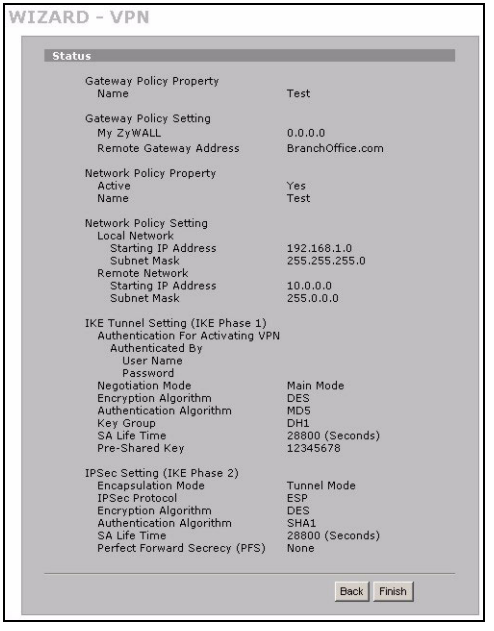
4 您可以在這個畫面中設定IKE（網際網路金鑰交換）通道設定。



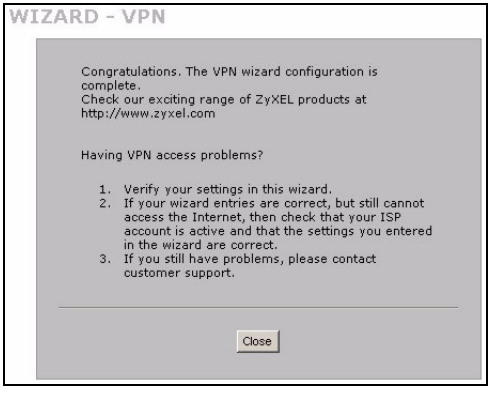
5 您可以在這個畫面中設定 IPSec 設定。



6 檢查 VPN 設定。按一下 **Finish**（完成）儲存設定。



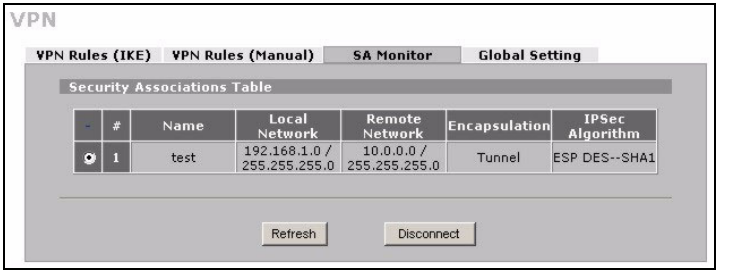
7 按一下最後的畫面中的 **Close**（關閉），完成 VPN 精靈的設定。 繼續下一節的步驟，啓用 VPN 規則並建立 VPN 連線。



8.1 使用 VPN 連線

使用 VPN 通道安全地傳送和擷取檔案，並允許遠端存取公司網路、網頁伺服器和電子郵件。服務的運作會和您在辦公室的狀況一樣，不會像是透過網際網路連線進行的。

例如，"test"（測試）VPN 規則可以讓您安全 地存取遠端公司 LAN 上的網頁伺服器。將伺服器的 IP 位址（在這個範例中爲 10.0.0.23）輸入爲瀏覽器的 URL。ZyWALL 會在您嘗試使用 VPN 通道時，自動加以建立。



按一下導覽面板上的 **SECURITY**（安全）> **VPN**，然後選取 **SA Monitor**（SA 監視器）標籤，顯示連接的 VPN 通道清單（"test" VPN 通道可以在這裡找到）。

9 疑難排解

問題	修正動作
指示燈全部不亮。	請確認已經將電源供應器接到 ZyWALL 裝置上，且接上了適當的電源。檢查所有纜線是否正確連接。
	如果指示燈仍然不亮，可能是硬體發生問題。如果是這種情況，請聯絡當地的供應商。
無法從 LAN 存取 ZyWALL。	檢查 ZyWALL 和電腦或集線器之間的纜線連接。請參閱章節 1，取得詳細資訊。
	從 LAN 電腦上 ping ZyWALL。請確認電腦上安裝了乙太網路卡，且網路卡能夠正常運作。 在電腦中，按一下**開始**、**（所有程式）程式集**、**附屬應用程式**，然後按一下**命令提示字元**。在**命令提示字元**視窗中，輸入 "ping" 再輸入 ZyWALL 的 LAN IP 位址（預設爲 192.168.1.1），然後按一下 ENTER。ZyWALL 裝置應該會有回應。如果仍然沒有回應，請參閱章節 9.1。
	如果忘記了 ZyWALL 的密碼，請使用 **RESET**（重設）按鈕。按住這個按鈕約 10 秒（或按住直到 **SYS** 指示燈亮起）後放開。按下這個按鈕會將 ZyWALL 還原爲預設值（密碼爲 1234，而 LAN IP 位址爲 192.168.1.1 等，請參閱《使用手冊》，取得詳細資訊）。
	如果忘記了 ZyWALL 的 LAN 或 WAN IP 位址，可以透過管理設定連接埠（Console Port）檢查 SMT 中的 IP 位址。使用終端機線（Console Cable）將電腦接到 **CONSOLE** 連接埠。您的電腦必須具有終端機模擬通訊程式（例如超級終端機），並做以下設定：VT100 終端機模擬模式、無同位、8 資料位元、1 停止位元、無流量控制，以及連接埠速度 9600 bps。
無法存取網際網路。	檢查 ZyWALL 是否正確連接可以存取網際網路的乙太網路插孔。確認網際網路閘道裝置（例如 DSL 數據機）運作正常。
	按一下導覽面板上的 **WAN**，確認您的設定。

問題	修正動作
無法建立 VPN 連線。	確認 ZyWALL 和遠端 IPSec 路由器使用同樣的 VPN 設定。按一下導覽面板上的 **VPN**，進行進階設定。
	試著存取某個網站，檢查網際網路連線是否正常。

9.1 設定電腦的 IP 位址

本節會說明如何在 Windows 2000、Windows NT 和 Windows XP 中，設定電腦接收 IP 位址。這項作業可以確保您的電腦能和 ZyWALL 裝置通訊。

1 在 Windows XP 中，按一下**開始**，然後按一下**控制台**。

在 Windows 2000/NT 中，依序按下**開始**、**設定**和**控制台**。

2 在 Windows XP 中，按一下**網路連線**。

在 Windows 2000/NT 中，按一下**網路和撥號連線**。

3 在**區域連線**上按一下滑鼠右鍵，然後按**內容**。

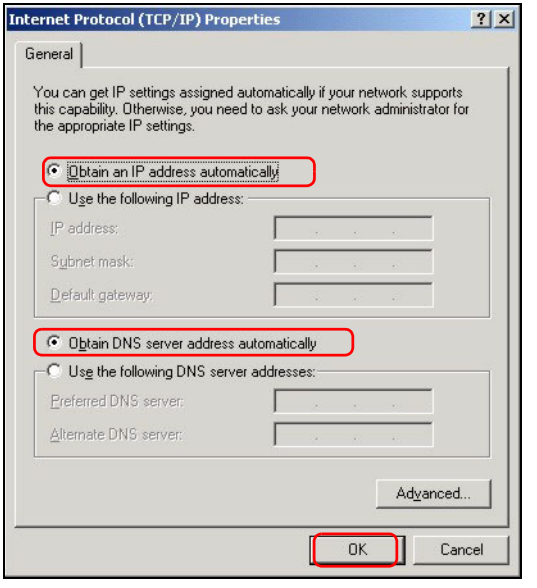
4 選取 **Internet Protocol (TCP/IP)**（在 **Win XP** 中位於**一般**索引標籤上），然後按一下**內容**。

5 **Internet Protocol TCP/IP 內容**畫面會開啓（在 Win XP 中位於**一般**索引標籤上）。選取**自動取得 IP 位址**和**自動取得 DNS 伺服器位址**選項。

6 按一下**確定**，關閉 **Internet Protocol (TCP/IP) 內容**視窗。

7 按一下**關閉**（在 Windows 2000/NT 中爲**確定**），關閉**區域連線內容**視窗。

8 關閉**網路連線**畫面。



檢視產品檢定資訊步驟

1 到 http://www.zyxel.com.tw/ 網站。

2 在合勤科技（ZyXEL）首頁上的下拉式清單方塊中選取所要的產品，移至該產品的頁面。

3 在頁面中選取要檢視的檢定資訊。