

ZyWALL 2WG

Internet Security Appliance

Quick Start Guide

Version 4.02
Edition 1
1/2007

Table of Contents	
ENGLISH	1
DEUTSCH	17
ESPAÑOL	33
FRANÇAIS	49
ITALIANO	65
РУССКИЙ	81
SVENSKA	99
简体中文	115
繁體中文	131



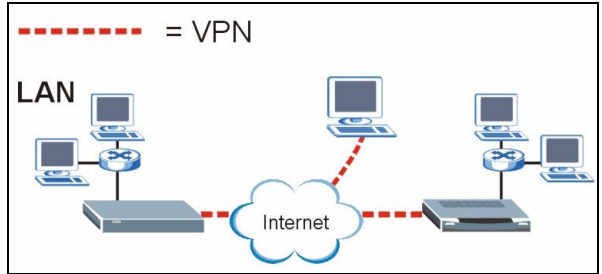
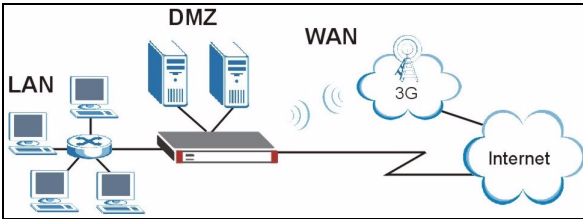
Copyright © 2007. All rights reserved.

Overview

The ZyWALL 2WG is a firewall with VPN, bandwidth management, content filtering 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.



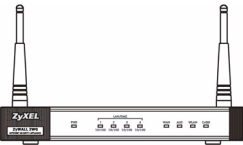
This guide is divided into the following sections.

- | | |
|---|--------------------------|
| 1 Hardware Connections | 6 NAT |
| 2 Accessing the Web Configurator | 7 Firewall |
| 3 Bridge Mode | 8 VPN Rule Setup |
| 4 Internet Access Setup and Product Registration | 9 Troubleshooting |
| 5 DMZ | |

1 Hardware Connections

You need the following.

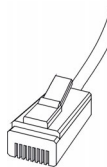
ZyWALL



Computer



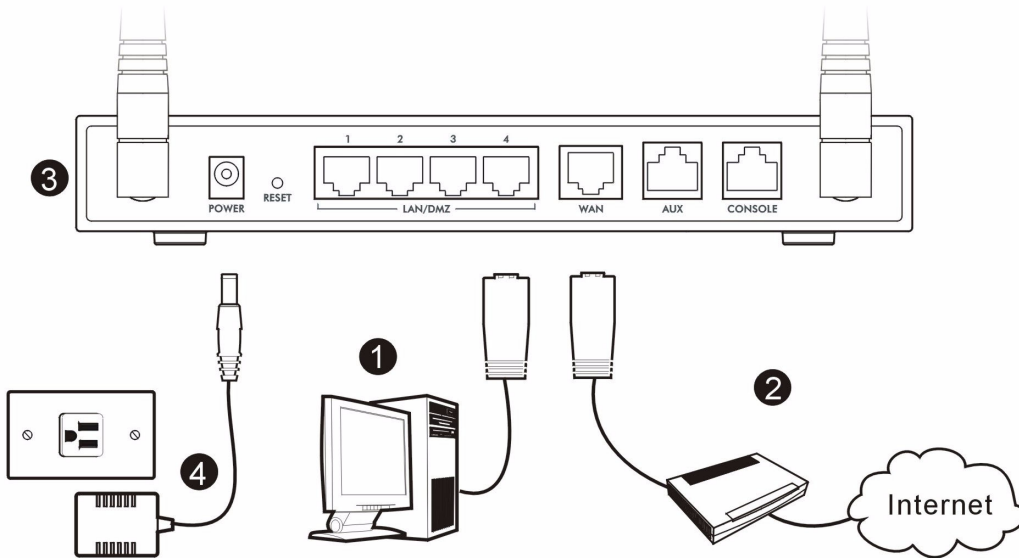
Ethernet Cables



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.

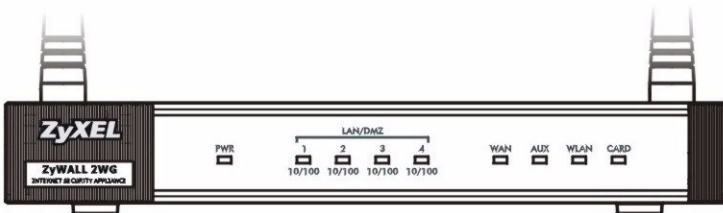


Use the blue console cable if you want to connect the **CONSOLE** port to your computer. Use the black dial backup cable if you want to connect the **AUX** port to an analog modem.

3 Insert a 3G wireless card into the card slot on the side panel to access the Internet wirelessly via a 3G network. 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 **CARD**, **LAN/DMZ** and **WAN** LEDs turn on and stay on if the corresponding connections are properly made.



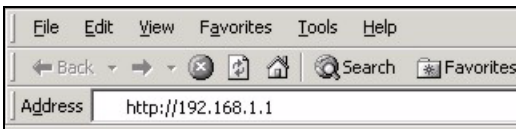


If none of the LEDs are on, check your connections, and inspect your cables for damage. Make sure that you have the power adaptor connected to the ZyWALL and plugged in to an appropriate power source. Make sure the power source is turned on. If the LEDs are still off, contact your local vendor.

2 Accessing the Web Configurator

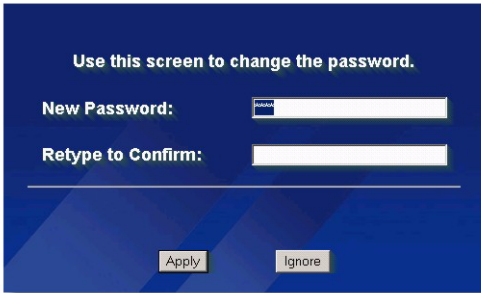
Use this section to configure the **WAN 1** interface for Internet access.

- 1 Launch your web browser. Enter **192.168.1.1** (the ZyWALL's default IP address) as the address.
- 2 Click **Login** (the default password 1234 is already entered).



If the login screen does not display, check your browser's security settings and make sure your computer's Ethernet card is installed and functioning properly. Your computer should be also set to get an IP address automatically from a DHCP server. See Set Up Your Computer's IP Address for more information.

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



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



If you changed the password and have forgotten it, you need to return the ZyWALL to the defaults (password is 1234, LAN IP address is 192.168.1.1, etc.). Press the **RESET** button (on the rear panel) until the **PWR** LED starts to blink, then release it.

5 The **HOME** screen opens.

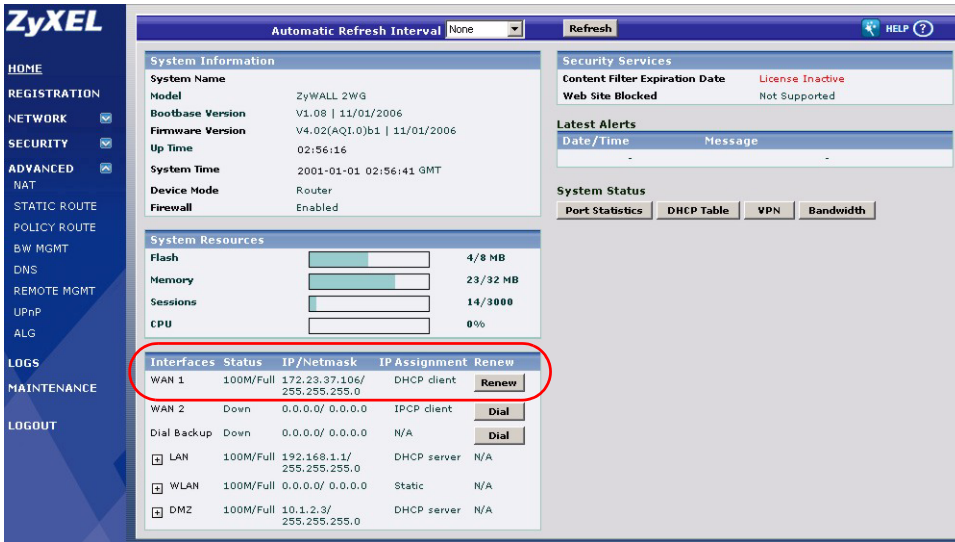
The ZyWALL is in router mode by default. Continue to the next step if you want to use routing features such as NAT, DHCP and VPN.

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.

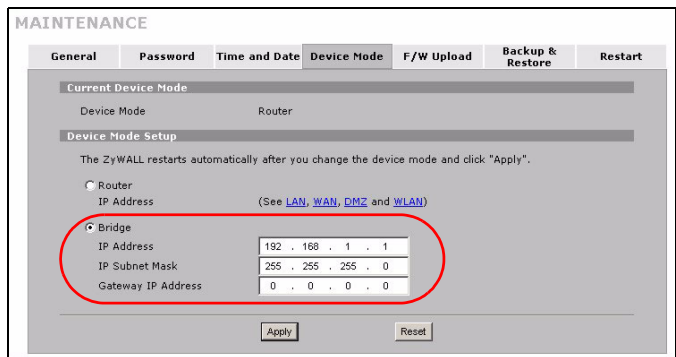


3 Bridge Mode

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).

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation

WAN IP Address Assignment

IP Address Assignment

My WAN IP Address

My WAN IP Subnet Mask

Gateway IP Address

First DNS Server

Second DNS Server

• 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**.

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation: (Optional)

Service Name:

User Name:

Password:

Retype to Confirm:

Nailed-Up

Idle Timeout: (Seconds)

WAN IP Address Assignment

IP Address Assignment:

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation:

User Name:

Password:

Retype to Confirm:

Nailed-Up

Idle Timeout: (Seconds)

PPTP Configuration

My IP Address:

My IP Subnet Mask:

Server IP Address:

Connection ID/Name:

WAN IP Address Assignment

IP Address Assignment:

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 trial application. Otherwise, click **Skip** and then **Close** to complete Internet access setup.

INTERNET ACCESS

Product registration and service activation for free

You can register ZyWALL on <http://www.zyxel.com> and activate "Free Trial" of Content Filtering service on your ZyWALL.

Click "Next" to activate these services for FREE.

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**.

INTERNET ACCESS

Device Registration

New myZyXEL.com account Existing myZyXEL.com account

User Name:

Password: (Type username and password from 6 to 20 characters.)

Confirm Password:

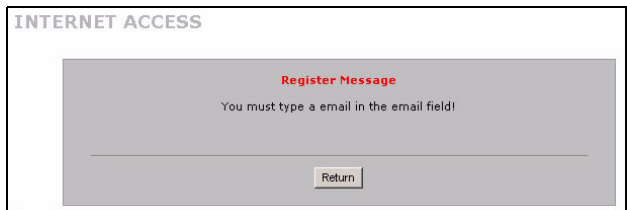
E-Mail Address:

Country:

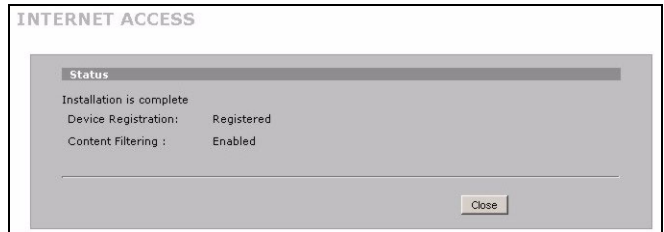
4 Wait for the registration progress to finish.



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.



If you cannot access the Internet via WAN 1, 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.

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.

Note: 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 **DMZ** and click **Apply**.

The screenshot shows the 'DMZ' configuration page with the 'Static DHCP' tab selected. The 'DMZ TCP/IP' section has IP Address, IP Subnet Mask, and Multicast set to 'None'. The 'DHCP Setup' section has DHCP set to 'None', IP Pool Starting Address, DHCP Server Address, and two DHCP WINS Servers all set to '0.0.0.0'. The 'Windows Networking (NetBIOS over TCP/IP)' section has four checkboxes: 'Allow between DMZ and LAN', 'Allow between DMZ and WAN1', 'Allow between DMZ and WAN2', and 'Allow between DMZ and WLAN', all of which are unchecked. There is a note: 'Note: You also need to create a Firewall rule.' and 'Apply' and 'Reset' buttons at the bottom.

The screenshot shows the 'DMZ' configuration page with the 'Port Roles Setup' tab selected. It displays a diagram of the ZyWALL with four ports labeled LAN, DMZ, and WLAN. Each port has a radio button next to it, and the 'DMZ' radio button is selected. There are 'Apply' and 'Reset' buttons at the bottom.

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**.

NAT

NAT Overview Address Mapping **Port Forwarding** Port Triggering

Port Forwarding Rules

WAN Interface:

Default Server: Go To Page:

#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	web	80 - 80	0 - 0	10 . 0 . 0 . 20
2	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
3	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
4	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
5	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
6	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
7	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
8	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
9	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
10	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0

Note 1: You may also need to create a [Firewall](#) rule.
Note 2: Port Translation is optional.

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.

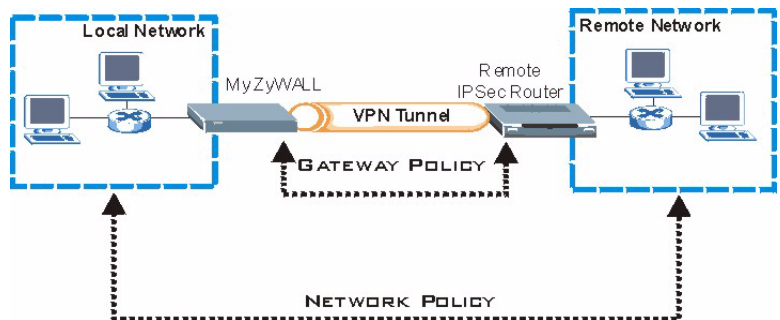
If you are using the ZyWALL in router mode, continue with the next section. For bridge mode, you are done with initial configuration.

8 VPN Rule Setup

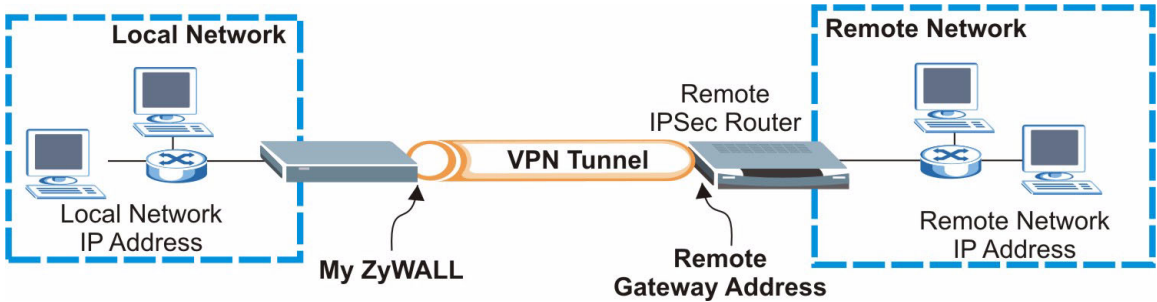
A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network.


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.

WIZARD - VPN

Gateway Policy Property

Name

Gateway Policy Setting

My ZyWALL

Remote Gateway Address

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.

WIZARD - VPN

Network Policy Property

Active
Name:

Network Policy Setting

Local Network: Single Range IP Subnet
Starting IP Address:
Ending IP Address / Subnet Mask:

Remote Network: Single Range IP Subnet
Starting IP Address:
Ending IP Address / 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.

WIZARD - VPN

IKE Tunnel Setting (IKE Phase 1)

Negotiation Mode Main Mode Aggressive Mode

Encryption Algorithm DES AES 3DES

Authentication Algorithm SHA1 MD5

Key Group DH1 DH2

SA Life Time (Seconds)

Pre-Shared Key

5 Use this screen to configure IPSec settings.

WIZARD - VPN

IPsec Setting (IKE Phase 2)

Encapsulation Mode Tunnel Transport

IPsec Protocol ESP AH

Encryption Algorithm DES AES 3DES NULL

Authentication Algorithm SHA1 MD5

SA Life Time (Seconds)

Perfect Forward Secrecy (PFS) None DH1 DH2

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

WIZARD - VPN

Status

Gateway Policy Property Name: Test

Gateway Policy Setting: My ZyWALL, Remote Gateway Address: BranchOffice.com

Network Policy Property Active Name: Yes, Test

Network Policy Setting: Local Network (Starting IP Address: 192.168.1.0, Subnet Mask: 255.255.255.0), Remote Network (Starting IP Address: 10.0.0.0, Subnet Mask: 255.0.0.0)

IKE Tunnel Setting (IKE Phase 1) Authentication For Activating VPN: User Name, Password, Negotiation Mode: Main Mode, Encryption Algorithm: DES, Authentication Algorithm: MD5, Key Group: DH1, SA Life Time: 28800 (Seconds), Pre-Shared Key: 12345678

IPsec Setting (IKE Phase 2) Encapsulation Mode: Tunnel Mode, IPsec Protocol: ESP, Encryption Algorithm: DES, Authentication Algorithm: SHA1, SA Life Time: 28800 (Seconds), Perfect Forward Secrecy (PFS): None

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.

WIZARD - VPN

Congratulations. The VPN wizard configuration is complete.
Check our exciting range of ZyXEL products at <http://www.zyxel.com>

Having VPN access problems?

1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.

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 a 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).

The screenshot shows the ZyWALL VPN SA Monitor interface. At the top, there are tabs for 'VPN Rules (IKE)', 'VPN Rules (Manual)', 'SA Monitor', and 'Global Setting'. The 'SA Monitor' tab is selected. Below the tabs is a 'Security Associations Table' with the following data:

#	Name	Local Network	Remote Network	Encapsulation	IPSec Algorithm
1	test	192.168.1.0 / 255.255.255.0	10.0.0.0 / 255.255.255.0	Tunnel	ESP DES--SHA1

Below the table are two buttons: 'Refresh' and 'Disconnect'.



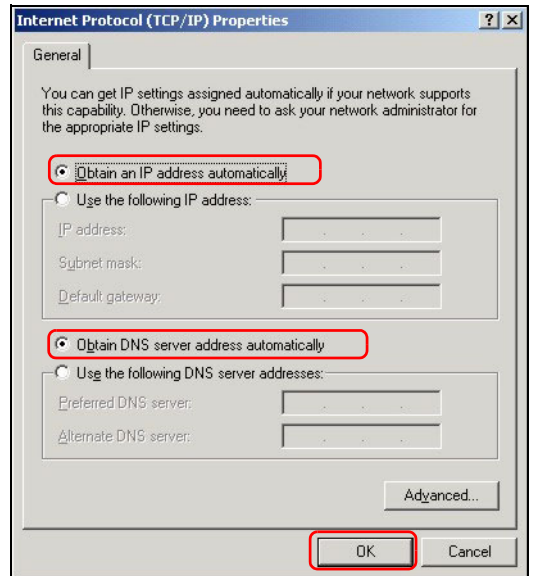
If you cannot establish a VPN connection, make sure the ZyWALL and the remote IPSec router use the same VPN settings. Click **VPN** in the navigation panel to configure advanced settings. Access a web site to check that you have a successful Internet connection.

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 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)

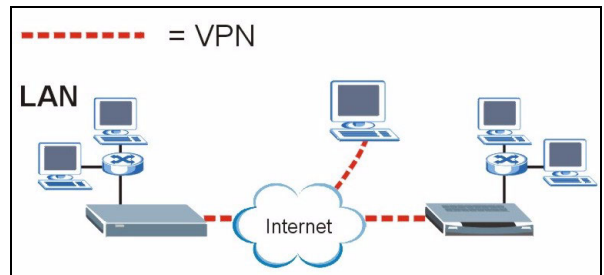
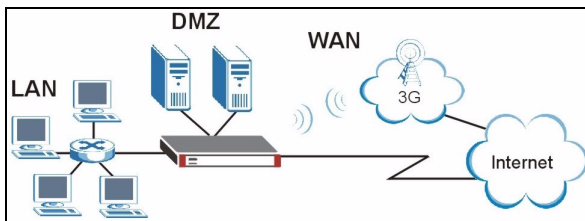
- 1 Go to www.zyxel.com.
- 2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

Übersicht

Die ZyWALL 2WG ist eine Firewall mit VPN, Bandbreitenmanagement, Content Filtering 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 | 6 NAT |
| 2 Zugriff auf den Web-Konfigurator | 7 Firewall |
| 3 Bridge Mode | 8 Einstellen der VPN-Regeln |
| 4 Einrichten des Internetzugriffs und Produktregistrierung | 9 Problembeseitigung |
| 5 DMZ | |

1 Anschließen der Hardware

Sie benötigen folgendes:

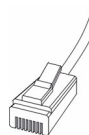
ZyWALL



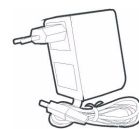
Computer



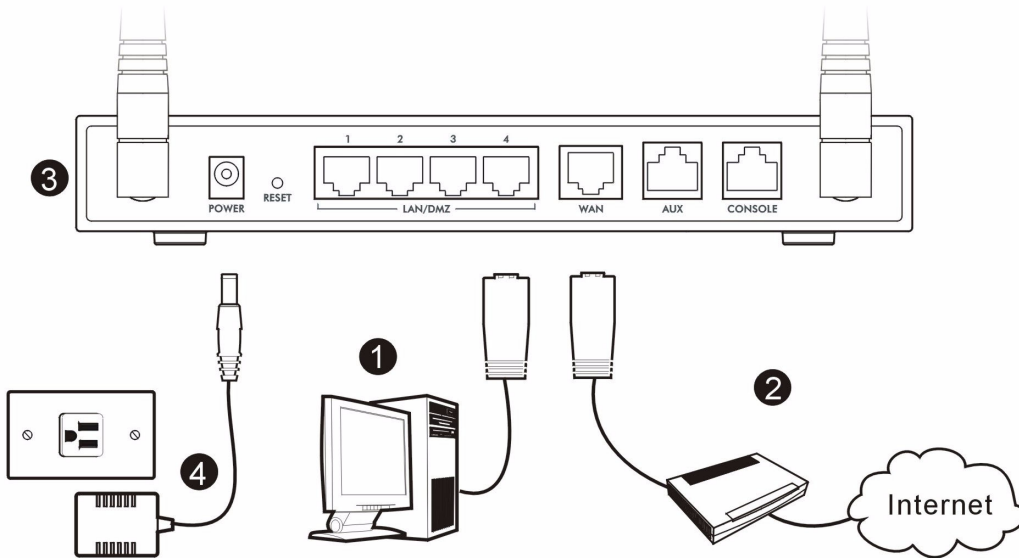
Ethernetkabel



Netzteil



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



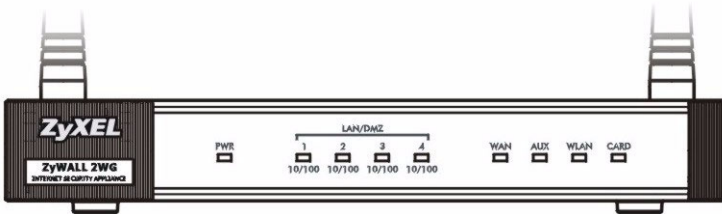
- 1 Verbinden Sie den **LAN-/DMZ**-Port mit einem Ethernet-Kabel mit dem Computer. Wenn Sie diese Ports im **LAN-** oder **DMZ**-Fenster mit dem Web-Konfigurator als DMZ-Ports konfigurieren, können Sie auch mit Ethernetkabeln eine Verbindung von **LAN-/DMZ**-Ports zu öffentlichen Servern (Internet, E-Mail,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



Schließen Sie den Konsolenanschluss **CONSOLE** mit dem blauen Konsolenkabel an den Computer an. Schließen Sie den Anwahlsicherungsanschluss **AUX** mit dem schwarzen Anwahlsicherungskabel an das Analogmodem an.

- 3 Wenn Sie das Internet über UMTS erreichen wollen, setzen Sie Ihre 3G Karte in den seitlichen Kartenslot ein. 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. Die LEDs **CARD**, **LAN/DMZ** und **WAN** beginnen zu leuchten und bleiben an, wenn die entsprechenden Verbindungen richtig hergestellt wurden.

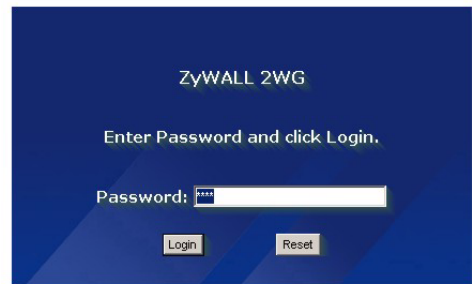
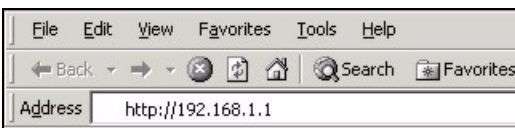


- ? Wenn keine der LEDs leuchtet, prüfen Sie noch einmal, ob alle Kabelverbindungen richtig gesteckt wurden und ob die Kabel unbeschädigt sind. Stellen Sie sicher, dass der Netzadapter richtig an das ZyWALL-Gerät und an eine Netzsteckdose angeschlossen wurde. Stellen Sie sicher, dass das Gerät eingeschaltet ist. Wenn die LEDs immer noch nicht leuchten, wenden Sie sich an Ihren Fachhändler

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





Wenn das Anmeldefenster nicht angezeigt wird, prüfen Sie die Sicherheitseinstellungen Ihres Browsers, und stellen Sie sicher, dass die im Computer installierte Ethernet-Karte richtig funktioniert.

Außerdem muss der Computer so eingerichtet sein, dass er eine IP-Adresse automatisch von einem DHCP-Server bezieht. Weitere Informationen dazu finden Sie unter Einrichten der IP-Adresse des Computers.

- 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.



Wenn Sie das Kennwort vergessen haben sollten, müssen Sie das ZyWALL-Gerät auf die Standardeinstellungen zurücksetzen (Kennwort: ?1234, LAN-IP-Adresse: ?192.168.1.1, usw.). Drücken Sie so lange auf die **RESET**-Taste (an der Rückseite des Geräts) bis die **PWR**-LED blinkt, und lassen Sie die Taste dann wieder los.

- 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](#).

Um **WAN 2** zu konfigurieren, benötigen Sie die **NETWORK WAN**-Fenster. Sie können auch ein Load-balancing zwischen den WAN-Anschlüssen konfigurieren.

The screenshot shows the ZyXEL web interface. On the left is a navigation menu with options like HOME, REGISTRATION, NETWORK, SECURITY, ADVANCED, NAT, STATIC ROUTE, POLICY ROUTE, BW MGMT, DNS, REMOTE MGMT, UPnP, ALG, LOGS, MAINTENANCE, and LOGOUT. The main content area is titled 'Automatic Refresh Interval None' and includes a 'Refresh' button. It is divided into several sections: System Information, Security Services, Latest Alerts, System Status, System Resources, and a table of Interfaces. The 'Interfaces' table is circled in red and contains the following data:

Interfaces	Status	IP/Netmask	IP Assignment	Renew
WAN 1	100M/Full	172.23.37.106/ 255.255.255.0	DHCP client	Renew
WAN 2	Down	0.0.0.0/ 0.0.0.0	IPCP client	Dial
Dial Backup	Down	0.0.0.0/ 0.0.0.0	N/A	Dial
LAN	100M/Full	192.168.1.1/ 255.255.255.0	DHCP server	N/A
WLAN	100M/Full	0.0.0.0/ 0.0.0.0	Static	N/A
DMZ	100M/Full	10.1.2.3/ 255.255.255.0	DHCP server	N/A

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- und WLAN-** Schnittstelle der ZyWALL.
- 3 Klicken Sie auf **Apply** (Übernehmen). Die ZyWALL wird neu gestartet.


The screenshot shows the 'MAINTENANCE' section of the ZyXEL web interface, specifically the 'Device Mode' tab. The 'Current Device Mode' is set to 'Router'. The 'Device Mode Setup' section shows the 'Bridge' mode selected. The configuration fields for Bridge mode are circled in red:

IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Gateway IP Address	0 . 0 . 0 . 0

Buttons for 'Apply' and 'Reset' are visible at the bottom of the configuration area.

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 Listenfeld **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**).

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation Ethernet ▾

WAN IP Address Assignment

IP Address Assignment Static ▾

My WAN IP Address 0 . 0 . 0 . 0

My WAN IP Subnet Mask 0 . 0 . 0 . 0

Gateway IP Address 0 . 0 . 0 . 0

First DNS Server 0 . 0 . 0 . 0

Second DNS Server 0 . 0 . 0 . 0

Back Apply

• 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.

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation:

Service Name: (Optional)

User Name:

Password:

Retype to Confirm:

Nailed-Up

Idle Timeout: (Seconds)

WAN IP Address Assignment

IP Address Assignment:

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation:

User Name:

Password:

Retype to Confirm:

Nailed-Up

Idle Timeout: (Seconds)

PPTP Configuration

My IP Address:

My IP Subnet Mask:

Server IP Address:

Connection ID/Name:

WAN IP Address Assignment

IP Address Assignment:

2 Klicken Sie auf **Next** (Weiter), um das Fenster aufzurufen, in dem Sie Ihr ZyWALL mit myZyXEL.com (ZyXELs Online-Servicezentrum) registrieren den kostenlosen Test des Webcontent-Filters zu aktivieren. Oder Sie klicken auf **Skip** (Überspringen) und dann auf **Close** (Schliessen), um das Einrichten des Internetzugriffs abzuschliessen.

INTERNET ACCESS

Product registration and service activation for free

You can register ZyWALL on <http://www.zyxel.com> and activate "Free Trial" of Content Filtering service on your ZyWALL.

Click "Next" to activate these services for FREE.

3 Wenn Sie bei myZyXEL.com bereits ein Konto haben, wählen 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).

INTERNET ACCESS

Device Registration

New myZyXEL.com account Existing myZyXEL.com account

User Name:

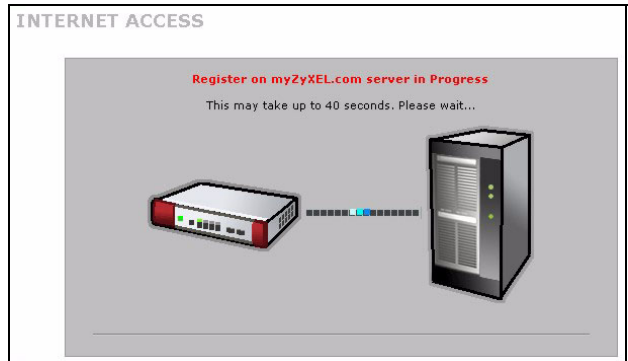
Password: (Type username and password from 6 to 20 characters.)

Confirm Password:

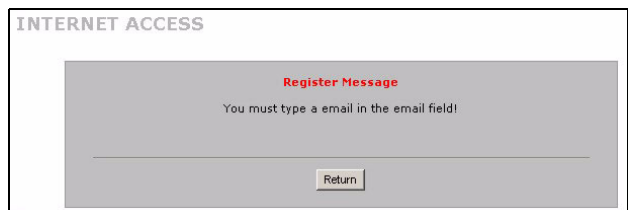
E-Mail Address:

Country:

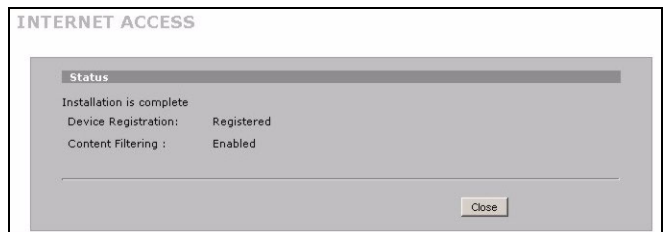
4 Warten Sie ab, bis die Registrierung abgeschlossen ist. Dies kann einige Minuten dauern.



5 Im folgenden Fenster wird angezeigt, wenn die Registrierung nicht erfolgreich durchgeführt wurde. Klicken Sie auf **Return** (Zurück), 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.



Wenn Sie nicht über WAN 1 auf das Internet zugreifen können, prüfen Sie die Verbindung des ZyWALL-Geräts zum Ethernet-Anschluss mit Internet-Zugriff. Stellen Sie sicher, dass die Verbindung zum Internet (zum Beispiel DSL Modem) einwandfrei arbeitet. Klicken Sie in der Navigationsleiste auf **WAN** und überprüfen Sie die Einstellungen.

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 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).

The screenshot shows the 'NAT Port Forwarding Rules' configuration page. At the top, there are tabs for 'NAT Overview', 'Address Mapping', 'Port Forwarding', and 'Port Triggering'. The 'Port Forwarding Rules' section is active. Below it, the 'WAN Interface' is set to 'WAN1' and the 'Default Server' is '0.0.0.0'. A 'Go To Page' dropdown is set to '1'. A table lists 10 rules. Rule 1 is active and named 'web', with incoming port 80 and server IP 10.0.0.20. Rules 2-10 are inactive. At the bottom, there are 'Apply' and 'Reset' buttons. Two notes are present: 'Note 1: You may also need to create a Firewall rule.' and 'Note 2: Port Translation is optional.'

#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	web	80 - 80	0 - 0	10 . 0 . 0 . 20
2	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
3	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
4	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
5	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
6	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
7	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
8	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
9	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
10	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0

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.

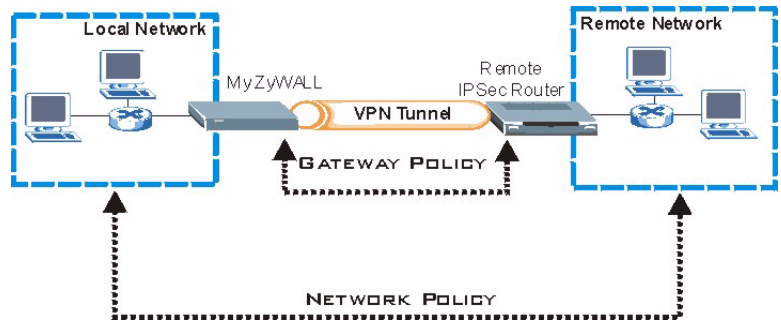
Wenn Sie die ZyWALL im Routermodus verwenden, fahren Sie mit dem nächsten Abschnitt fort. Für den Bridge-Modus, reicht die Erstkonfiguration.

8 Einstellen der VPN-Regeln

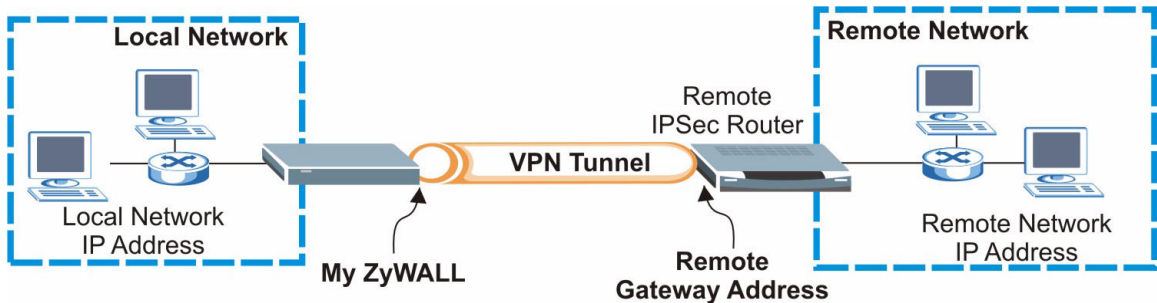
Mit einem VPN-Tunnel (Virtual Private Network) haben Sie eine sichere Verbindung zu anderen Computern oder Netzwerken.

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.

The screenshot shows the 'WIZARD - VPN' configuration window, specifically the 'IKE Tunnel Setting (IKE Phase 1)' section. The settings are as follows:

- Negotiation Mode: Main Mode Aggressive Mode
- Encryption Algorithm: DES AES 3DES
- Authentication Algorithm: SHA1 MD5
- Key Group: DH1 DH2
- SA Life Time: 28800 (Seconds)
- Pre-Shared Key: 12345678

At the bottom right, there are 'Back' and 'Next' buttons.

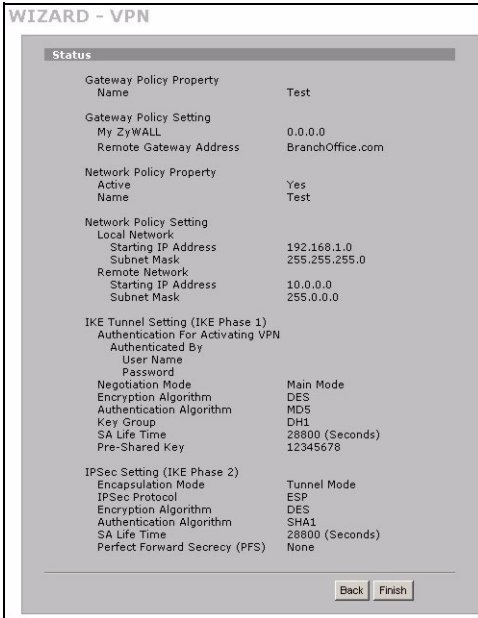
- 5 In diesem Fenster werden die IPSec-Einstellungen konfiguriert.

The screenshot shows the 'WIZARD - VPN' configuration window, specifically the 'IPSec Setting (IKE Phase 2)' section. The settings are as follows:

- Encapsulation Mode: Tunnel Transport
- IPSec Protocol: ESP AH
- Encryption Algorithm: DES AES 3DES NULL
- Authentication Algorithm: SHA1 MD5
- SA Life Time: 28800 (Seconds)
- Perfect Forward Secrecy (PFS): None DH1 DH2

At the bottom right, there are 'Back' and 'Next' buttons.

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



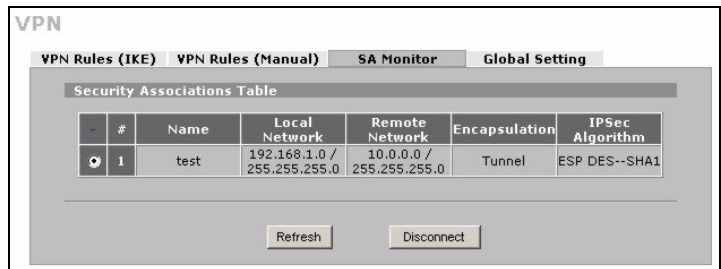
7 Klicken Sie beim letzten Fenster auf **Close** (Schließen), um die Installation mit dem VPN-Assistenten zu beenden. Fahren Sie mit dem nächsten Abschnitt fort, um die VPN-Regel zu aktivieren und eine VPN-Verbindung herzustellen.



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 Beispiel 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).



Wenn Sie keine VPN-Verbindung herstellen können, 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.

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**.

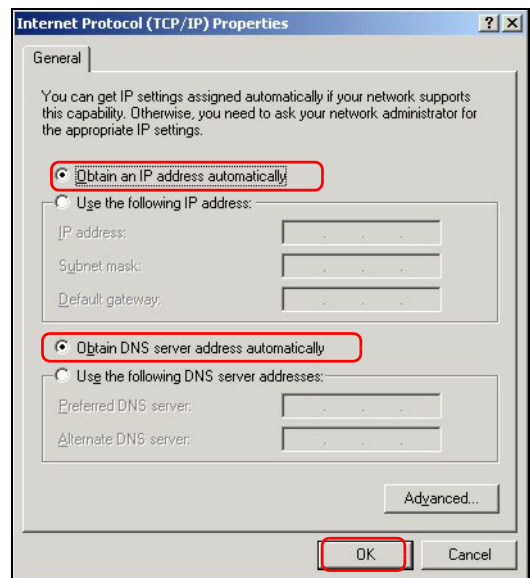
- 4 Wählen Sie **Internetprotokoll (TCP/IP)** (bei Windows XP auf der Registerkarte **Allgemein**) und klicken Sie auf **Eigenschaften**.

- 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)

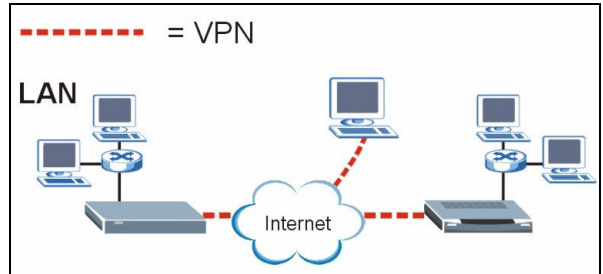
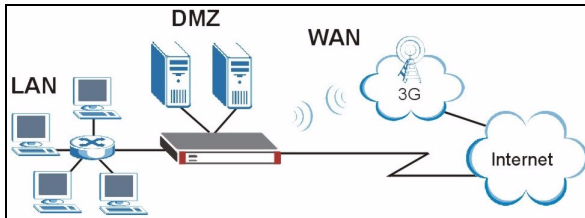
- 1** Besuchen Sie www.zyxel.com.
- 2** Wählen Sie auf der ZyXEL-Homepage aus der Liste der Produkte Ihr Produkt aus.
- 3** Wählen Sie auf dieser die Zertifizierung aus, die Sie gerne angezeigt haben möchten.

Vista previa

El ZyWALL 2WG es un cortafuegos, soporte de VPNs, gestión del ancho de banda, filtrado de contenidos 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 | 6 NAT |
| 2 Acceso al configurador Web | 7 Cortafuegos |
| 3 Modo puente (bridge) | 8 Configuración de reglas VPN |
| 4 Configuración del acceso a Internet y registro del producto | 9 Solución de problemas |
| 5 DMZ | |

1 Conexiones del hardware

Necesita lo siguiente.

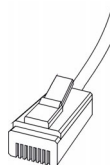
ZyWALL



Ordenador



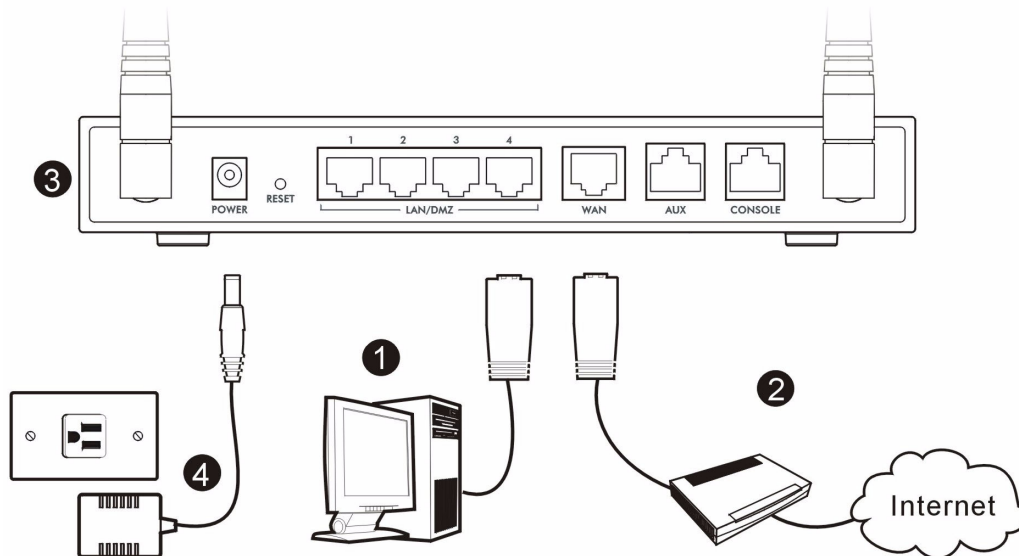
Cables Ethernet



Adaptador de corriente



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



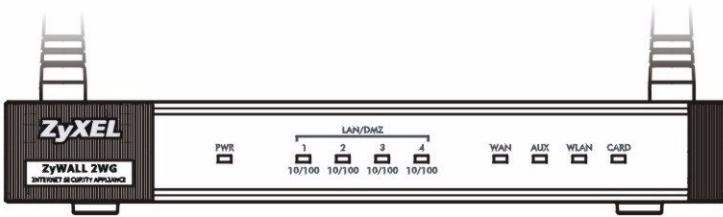
- 1 Use un cable Ethernet para conectar el puerto **LAN/DMZ** a un ordenador. Si configura estos puertos como puertos **DMZ** en la pantalla **LAN** o **DMZ** a través del configurador web, también podrá usar cables Ethernet para conectar servidores públicos (web, correo electrónico, FTP, etc.) a los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



Utilice el cable de consola azul si desea conectar el puerto **CONSOLA** a su ordenador. Utilice el cable de dial backup (apoyo de marcado) si desea conectar el puerto **AUX** a un módem analógico.

- 3 Introduzca una tarjeta inalámbrica 3G en el slot situado en el panel lateral para acceder a Internet inalámbricamente a través de una red 3G. En el momento de escribir redacción, 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. Los LEDs **CARD**, **LAN/DMZ** y **WAN** se encenderán y permanecerán encendidos si las conexiones correspondientes se han realizado correctamente.

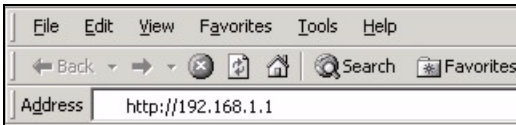


- ?** Si ninguno de los LEDs está encendido, verifique sus conexiones y compruebe si los cables están dañados. Asegúrese de haber conectado el adaptador de alimentación al ZyWALL y de haberlo enchufado en una fuente de alimentación apropiada. Compruebe que la fuente de alimentación esté encendida. Si los LEDs continúan apagados, contacte con su vendedor local.

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.



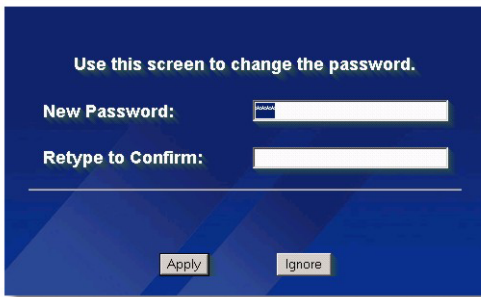
- 2 Haga clic en **Login** (acceso) (la contraseña predeterminada 1234 ya está introducida).





Si la pantalla de acceso no aparece, compruebe la configuración de seguridad de su explorador y asegúrese de que su tarjeta Ethernet esté instalada y funcionando correctamente.
Su ordenador también debería estar configurado para obtener automáticamente una dirección IP desde un servidor DHCP. Consulte Configurar la dirección IP de su ordenador para más información.

- 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.



Si ha cambiado la contraseña y la ha olvidado, necesitará devolver al ZyWALL a sus valores predeterminados (la contraseña es 1234, la dirección IP de la LAN es 192.168.1.1, etc.). Presione el botón **RESET** (del panel posterior) hasta que el LED **PWR** comience a parpadear, luego suéltelo.

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

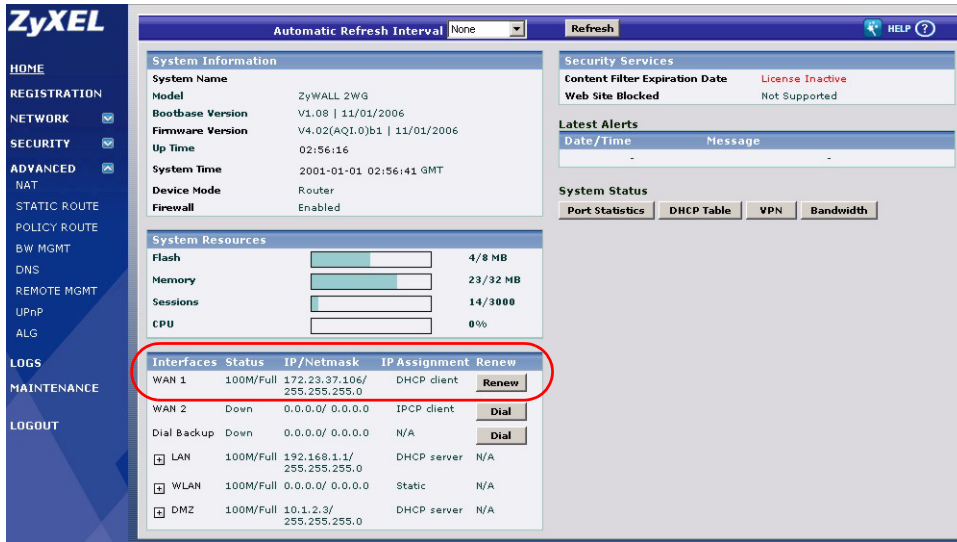
El ZyWALL está en modo router por defecto. Continúe en el siguiente paso si desea usar características de enrutamiento como NAT, DHCP y VPN.

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**.

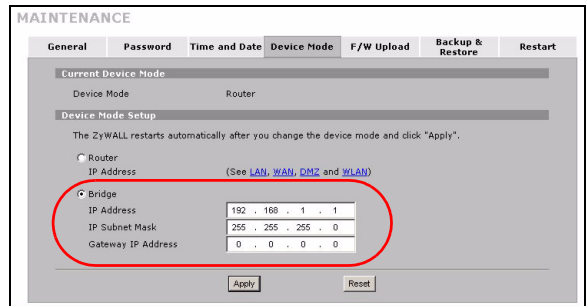
Use las pantallas **WAN** en **NETWORK** (red) si necesita configurar **WAN 2**. También puede configurar la distribución de carga entre las conexiones WAN.



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)**.

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation (Optional)

Service Name

User Name

Password

Retype to Confirm

Nailed-Up

Idle Timeout (Seconds)

WAN IP Address Assignment

IP Address Assignment

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation

User Name

Password

Retype to Confirm

Nailed-Up

Idle Timeout (Seconds)

PPTP Configuration

My IP Address

My IP Subnet Mask

Server IP Address

Connection ID/Name

WAN IP Address Assignment

IP Address Assignment

2 Haga clic en **Next (Siguiente)** para mostrar la pantalla donde podrá registrar ZyWALL con myZyXEL.com (centro de servicios en línea de ZyXEL) y activar la aplicación gratuita de prueba de filtrado de contenidos. En caso contrario, haga clic en **Skip (Saltar)** y luego en **Close (Cerrar)** para completar la configuración de acceso a Internet.

INTERNET ACCESS

Product registration and service activation for free

You can register ZyWALL on <http://www.zyxel.com> and activate "Free Trial" of Content Filtering service on your ZyWALL.

Click "Next" to activate these services for FREE.

3 Si ya tiene una cuenta en myZyXEL.com, seleccione **Existing myZyXEL.com account** (Cuenta myZyXEL.com existente) e introduzca la información 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)**.

INTERNET ACCESS

Device Registration

New myZyXEL.com account Existing myZyXEL.com account

User Name

Password (Type username and password from 6 to 20 characters.)

Confirm Password

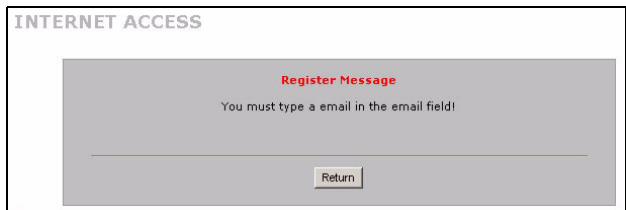
E-Mail Address

Country

4 Espere a que el progreso del registro finalice.



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



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



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.



Si no puede acceder a Internet a través de WAN 1, 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.

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.



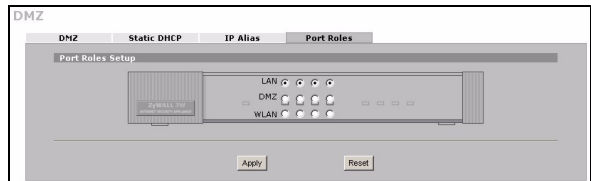
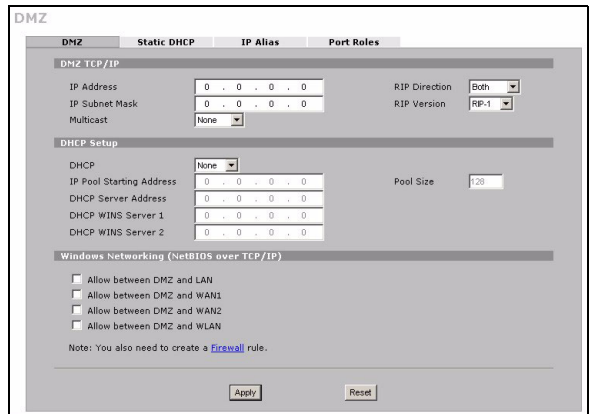
No necesita configurar la DMZ con modo puente, vaya a [Sección 7](#).

- 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).

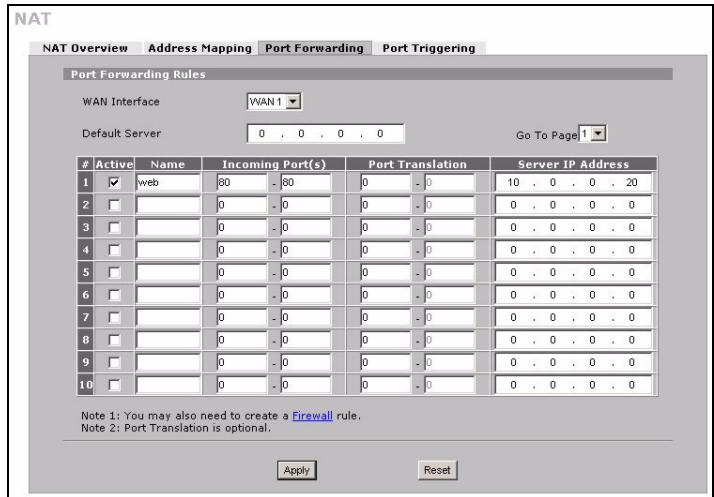


6 NAT

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.

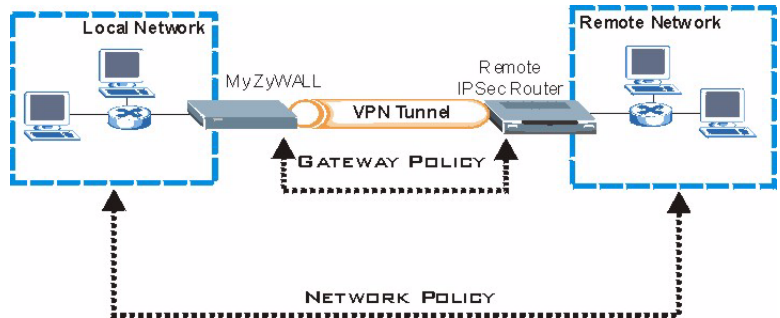
Si usa el ZyWALL en modo enrutador, continúe con la siguiente sección. Para el modo puente, habrá finalizado con la configuración inicial.

8 Configuración de reglas VPN

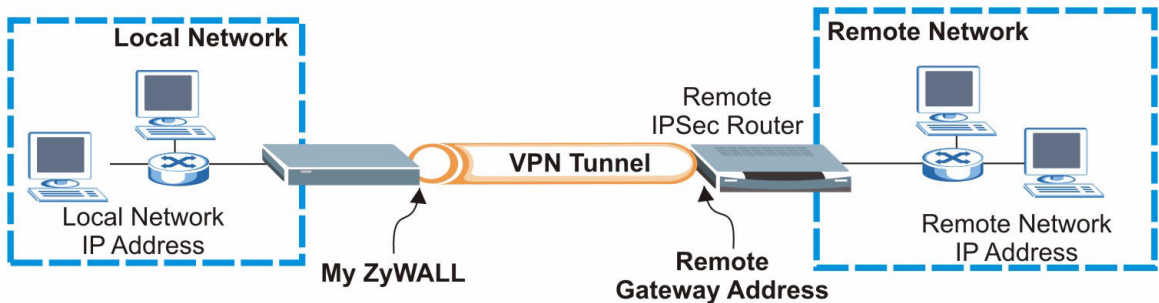
Un túnel VPN (Virtual Private Network - Red Privada Virtual) le ofrece una conexión segura a otro ordenador o red.

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.

WIZARD - VPN

Gateway Policy Property

Name: Test

Gateway Policy Setting

My ZyWALL: 0.0.0.0

Remote Gateway Address: BranchOffice.com

Back Next

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.

WIZARD - VPN

Network Policy Property

Active

Name: Test

Network Policy Setting

Local Network: Single Range IP Subnet

Starting IP Address: 192 . 168 . 1 . 0

Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0

Remote Network: Single Range IP Subnet

Starting IP Address: 10 . 0 . 0 . 0

Ending IP Address / Subnet Mask: 255 . 0 . 0 . 0

Back Next



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.

WIZARD - VPN

IKE Tunnel Setting (IKE Phase 1)

Negotiation Mode: Main Mode Aggressive Mode

Encryption Algorithm: DES AES 3DES

Authentication Algorithm: SHA1 MD5

Key Group: DH1 DH2

SA Life Time: (Seconds)

Pre-Shared Key:

WIZARD - VPN

IPSec Setting (IKE Phase 2)

Encapsulation Mode: Tunnel Transport

IPSec Protocol: ESP AH

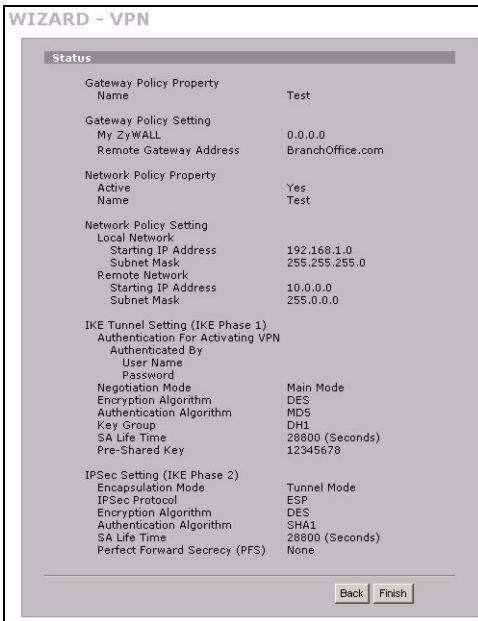
Encryption Algorithm: DES AES 3DES NULL

Authentication Algorithm: SHA1 MD5

SA Life Time: (Seconds)

Perfect Forward Secrecy (PFS): None DH1 DH2

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



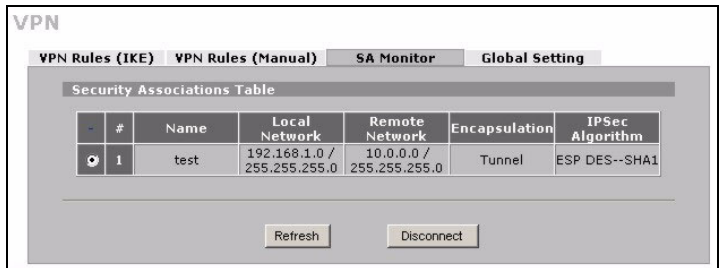
7 Haga clic en **Close** (Cerrar) en la pantalla final para completar la configuración del asistente para VPN. Continúe con la siguiente sección para activar la regla VPN y establecer una conexión VPN.



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).



Si no puede establecer una conexión VPN, compruebe si el ZyWALL y el router IPsec utilizan 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.

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**.

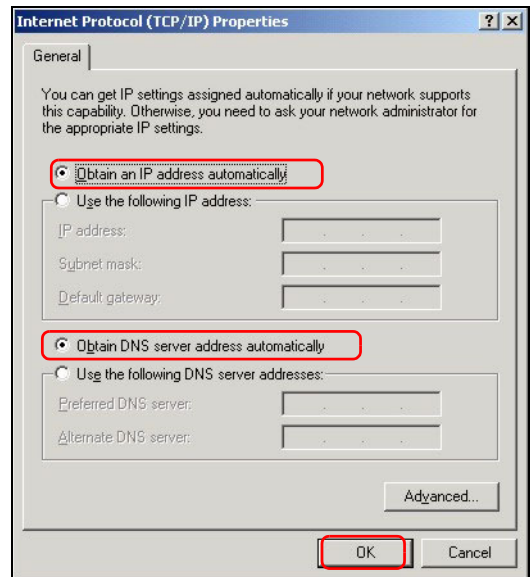
4 Seleccione **Protocolo Internet (TCP/IP)** (en la ficha **General** en Windows XP) y haga clic en **Propiedades**.

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

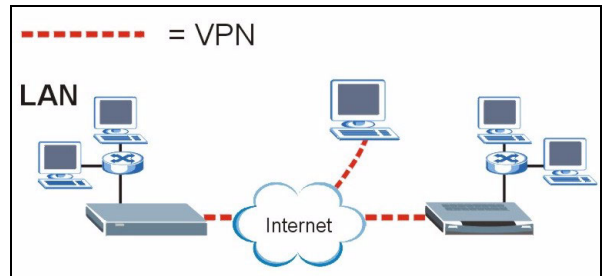
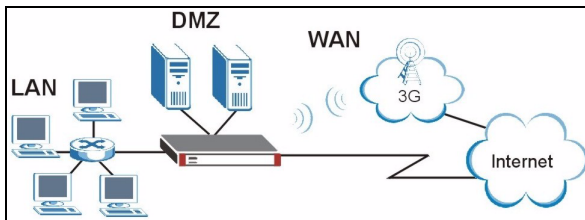
- 1** Vaya a www.zyxel.com.
- 2** Seleccione su producto de la lista desplegable en la página inicial de ZyXEL para ir a la página de ese producto.
- 3** Seleccione la certificación que desee visualizar en esta página.

Présentation

Le ZyWALL 2WG est un pare-feu avec VPN, gestion de bande passante, filtrage de contenu 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 | 6 NAT |
| 2 Accéder au Configurateur Web | 7 Pare-feu |
| 3 Mode Pont | 8 Installation de la règle VPN |
| 4 Installation de l'accès à Internet et inscription du produit | 9 Dépannage |
| 5 DMZ | |

1 Connexions matérielles

Vous avez besoin des éléments suivants.

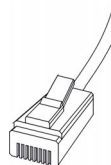
ZyWALL



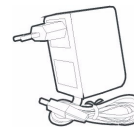
Ordinateur



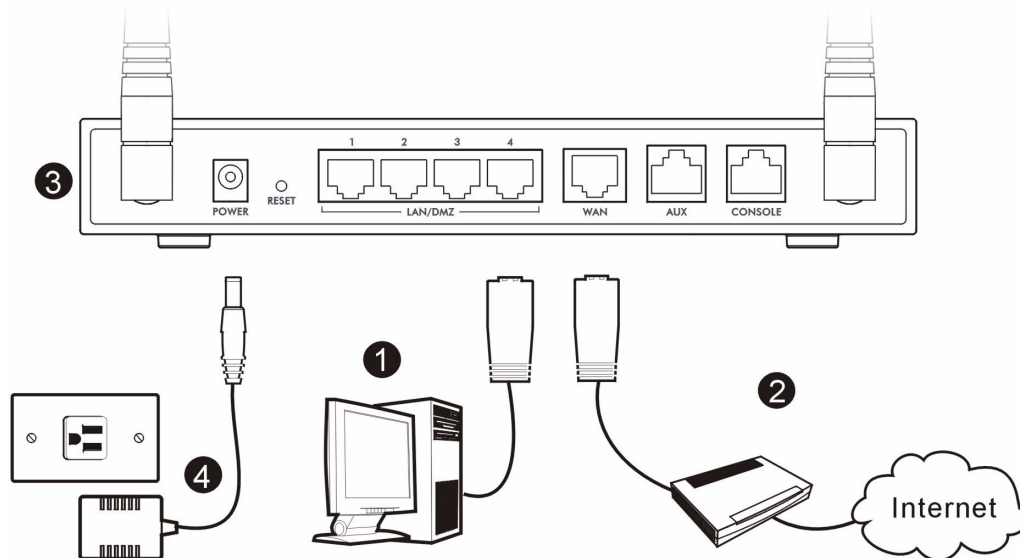
Câbles Ethernet



Adaptateur d'alimentation



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



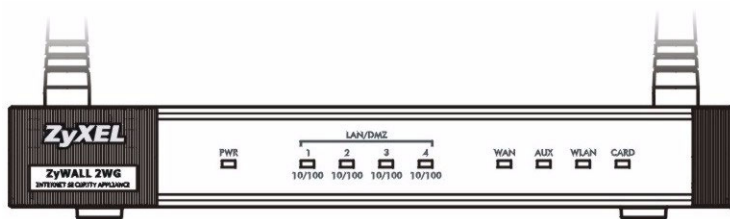
- 1 Utilisez un câble Ethernet pour connecter le port **LAN/DMZ** à un ordinateur. Si vous configurez ces ports en ports **DMZ** dans l'écran **LAN** ou **DMZ** à l'aide du configurateur web, vous pouvez aussi utiliser les câbles Ethernet pour connecter les serveurs publics (web, e-mail, FTP, etc.) aux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



Utilisez le câble de console bleu si vous voulez connecter le port **CONSOLE** à votre ordinateur. Utilisez le câble d'accès direct secouru noir si vous voulez connecter le port **AUX** à un modem analogique.

- 3 Insérez une carte sans fil 3G dans la fente prévu à cette effet sur le côté de l'appareil afin de pouvoir accéder à l'Internet sans fil via un réseau 3G. 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. Les LED **CARD**, **LAN/DMZ**, et **WAN** s'allument et restent allumées si les connexions correspondantes sont effectuées correctement.

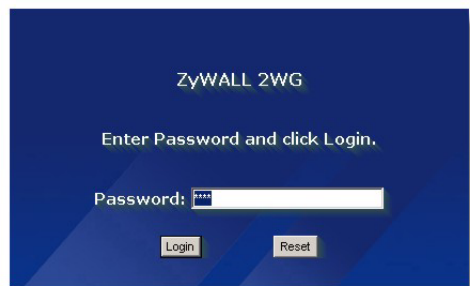
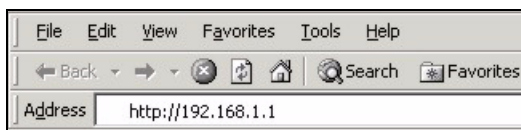


- ? Si aucune des LED n'est allumée, vérifiez vos connexions, et vérifiez si vos câbles ne sont pas endommagés. Vérifiez que l'adaptateur d'alimentation est connecté au ZyWALL et branché dans une prise de courant appropriée. Vérifiez que l'alimentation est sous tension. Si les LED sont toujours éteintes, contactez votre vendeur.

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



- ?** Si l'écran d'ouverture de session ne s'affiche pas, vérifiez les paramètres de sécurité de votre navigateur et assurez-vous que la carte Ethernet de votre ordinateur est installée et fonctionne correctement.
- Votre ordinateur doit aussi être paramétré de façon à obtenir automatiquement une adresse IP depuis un serveur DHCP. Consultez Paramétrez l'adresse IP de votre ordinateur pour plus d'informations.

- 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.

Use this screen to change the password.

New Password:

Retype to Confirm:

Apply Ignore

Replace Factory Default Certificate

The factory default certificate is common to all ZyWALL models. Click Apply to create a certificate using your ZyWALL's MAC address that will be specific to this device.

Apply Ignore

- ?** Si vous avez changé le mot de passe et que vous l'avez oublié, vous devez rétablir le ZyWALL à son paramétrage par défaut (le mot de passe est 1234, l'adresse IP LAN est 192.168.1.1, etc.). Appuyez sur le bouton **RESET** (RÉINITIALISER) (sur le panneau arrière) jusqu'à ce que la LED **PWR** se mette à clignoter, puis relâchez-le.

- 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 (RÉSEAU) WAN** si vous devez configurer **WAN 2**. Vous pouvez aussi configurer l'équilibrage de charge entre les connexions WAN.

The screenshot shows the ZyXEL web management interface. On the left is a navigation menu with options like HOME, REGISTRATION, NETWORK, SECURITY, ADVANCED, NAT, STATIC ROUTE, POLICY ROUTE, BW MGMT, DNS, REMOTE MGMT, UPnP, ALG, LOGS, MAINTENANCE, and LOGOUT. The main content area is titled 'Automatic Refresh Interval None' and includes a 'Refresh' button. It is divided into several sections: System Information, Security Services, Latest Alerts, System Status, System Resources, and Interfaces. The 'Interfaces' section contains a table with the following data:

Interfaces	Status	IP/Netmask	IP Assignment	Renew
WAN 1	100M/Full	172.23.37.106/ 255.255.255.0	DHCP client	Renew
WAN 2	Down	0.0.0.0/ 0.0.0.0	IPCP client	Dial
Dial Backup	Down	0.0.0.0/ 0.0.0.0	N/A	Dial
LAN	100M/Full	192.168.1.1/ 255.255.255.0	DHCP server	N/A
WLAN	100M/Full	0.0.0.0/ 0.0.0.0	Static	N/A
DMZ	100M/Full	10.1.2.3/ 255.255.255.0	DHCP server	N/A

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.


The screenshot shows the 'MAINTENANCE' section of the ZyXEL web management interface. The 'Device Mode' tab is selected, showing the current device mode as 'Router'. Below this, the 'Device Mode Setup' section is visible. It includes a note: 'The ZyWALL restarts automatically after you change the device mode and click "Apply".' There are two radio buttons: 'Router' (unselected) and 'Bridge' (selected). Under the 'Bridge' mode, the following fields are visible and highlighted with a red circle:

IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Gateway IP Address	0 . 0 . 0 . 0

At the bottom of the configuration area, there are 'Apply' and 'Reset' buttons.

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**).

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation

WAN IP Address Assignment

IP Address Assignment

My WAN IP Address

My WAN IP Subnet Mask

Gateway IP Address

First DNS Server

Second DNS Server

• 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).

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation (Optional)

Service Name (Optional)

User Name

Password

Retype to Confirm

Nailed-Up

Idle Timeout (Seconds)

WAN IP Address Assignment

IP Address Assignment

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation

User Name

Password

Retype to Confirm

Nailed-Up

Idle Timeout (Seconds)

PPTP Configuration

My IP Address

My IP Subnet Mask

Server IP Address

Connection ID/Name

WAN IP Address Assignment

IP Address Assignment

2 Cliquez sur **Next** (Suivant) pour afficher l'écran où vous pouvez inscrire votre ZyWALL avec myZyXEL.com (Centre de services en ligne de ZyXEL) et activer l'application d'évaluation gratuite de filtrage de contenu. Vous pouvez aussi cliquer sur **Skip** (Passer) et ensuite sur **Close** (Fermer) pour terminer l'installation de l'accès à Internet.

INTERNET ACCESS

Product registration and service activation for free

You can register ZyWALL on <http://www.zyxel.com> and activate "Free Trial" of Content Filtering service on your ZyWALL.

Click "Next" to activate these services for FREE.

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).

INTERNET ACCESS

Device Registration

New myZyXEL.com account Existing myZyXEL.com account

User Name

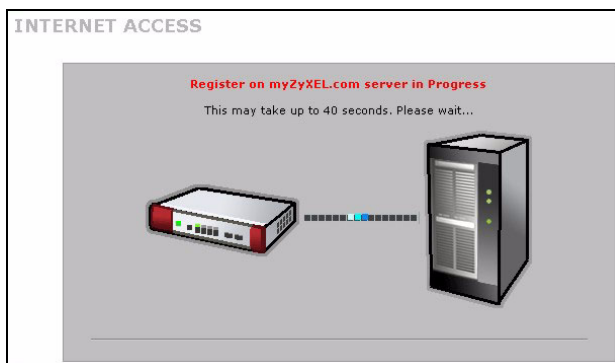
Password (Type username and password from 6 to 20 characters.)

Confirm Password

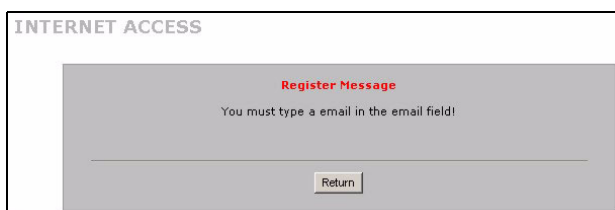
E-Mail Address

Country

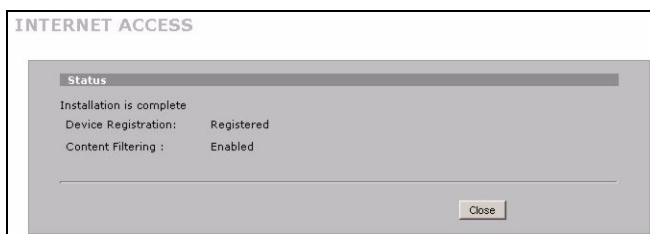
4 Attendez que l'enregistrement soit terminé.



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.



Si vous n'arrivez pas à accéder à Internet via WAN 1, vérifiez la connexion du ZyWALL à la prise Ethernet avec accès Internet. Vérifiez que le périphérique de passerelle Internet (un modem DSL par exemple) fonctionne correctement. Cliquez sur **WAN** dans le panneau de navigation pour vérifier vos paramètres.

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).

The screenshot shows the 'DMZ TCP/IP' configuration page. It includes fields for IP Address (0.0.0.0), IP Subnet Mask (0.0.0.0), and Multicast (None). There are also dropdown menus for RIP Direction (Both) and RIP Version (RP-1). The DHCP Setup section includes a DHCP dropdown (None), IP Pool Starting Address (0.0.0.0), DHCP Server Address (0.0.0.0), and DHCP WINS Server 1 and 2 (0.0.0.0). The Pool Size is set to 20. The Windows Networking (NetBIOS over TCP/IP) section has four checkboxes: Allow between DMZ and LAN, Allow between DMZ and WAN1, Allow between DMZ and WAN2, and Allow between DMZ and WLAN. A note states: 'Note: You also need to create a Firewall rule.' There are 'Apply' and 'Reset' buttons at the bottom.

The screenshot shows the 'Port Roles Setup' page. It features a diagram with four ports: LAN, DMZ, and WLAN. The DMZ port is selected with a radio button. There are 'Apply' and 'Reset' buttons at the bottom.

6 NAT

NAT (Network Address Translation - NAT, RFC 1631) permet la conversion d'une 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).

NAT

NAT Overview | Address Mapping | Port Forwarding | Port Triggering

Port Forwarding Rules

WAN Interface: WAN1

Default Server: 0 . 0 . 0 . 0

Go To Page: 1

#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	web	80 - 80	0 - 0	10 . 0 . 0 . 20
2	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
3	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
4	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
5	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
6	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
7	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
8	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
9	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
10	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0

Note 1: You may also need to create a [Firewall](#) rule.
Note 2: Port Translation is optional.

Apply Reset

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 DMZ vers le LAN.

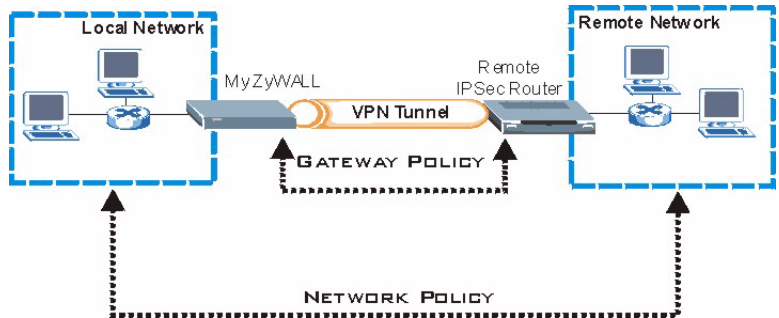
Si vous utilisez le ZyWALL en mode routeur, suivez la section suivante. Pour le mode pont, vous en avez terminé avec la configuration initiale.

8 Installation de la règle VPN

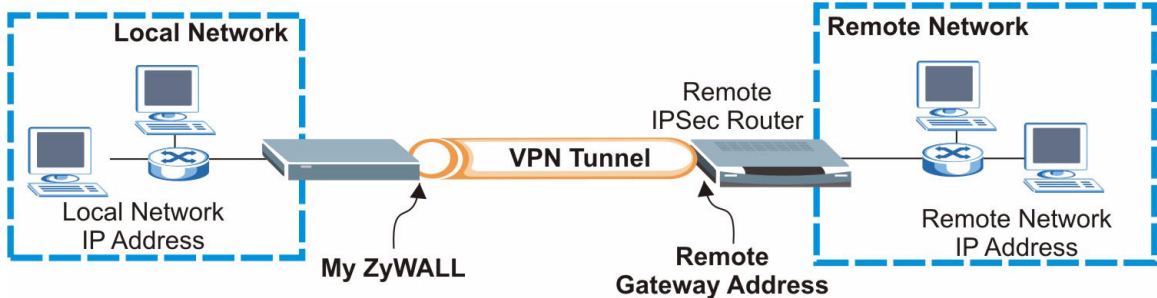
Un tunnel VPN (Virtual Private Network) vous offre une connexion sécurisée à un autre ordinateur ou réseau.

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.

WIZARD - VPN

Gateway Policy Property

Name

Gateway Policy Setting

My ZyWALL

Remote Gateway Address

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.

WIZARD - VPN

Network Policy Property

Active

Name

Network Policy Setting

Local Network Single Range IP Subnet

Starting IP Address

Ending IP Address / Subnet Mask

Remote Network Single Range IP Subnet

Starting IP Address

Ending IP Address / Subnet Mask



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.

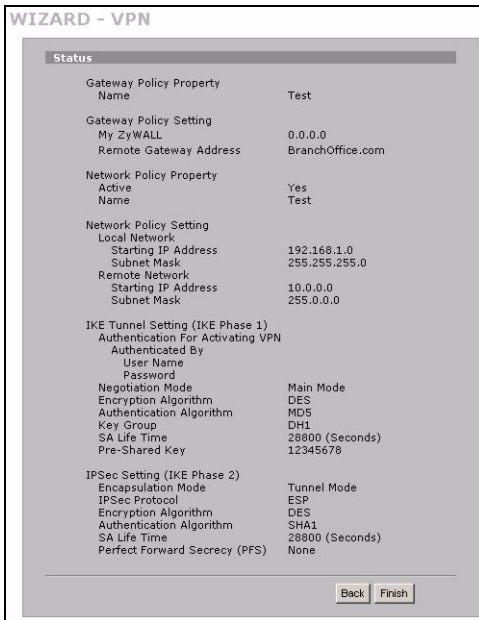
- 4 Utilisez cet écran pour configurer les paramètres IKE (Internet Key Exchange-Echange de clé Internet).

The screenshot shows the 'WIZARD - VPN' configuration interface, specifically the 'IKE Tunnel Setting (IKE Phase 1)' screen. It features several radio button options for Negotiation Mode (Main Mode selected), Encryption Algorithm (DES selected), Authentication Algorithm (SHA1 selected), and Key Group (DH1 selected). The SA Life Time is set to 28800 seconds, and the Pre-Shared Key is 12345678. 'Back' and 'Next' buttons are at the bottom.

- 5 Utilisez cet écran pour configurer les paramètres IPSec.

The screenshot shows the 'WIZARD - VPN' configuration interface, specifically the 'IPSec Setting (IKE Phase 2)' screen. It features radio button options for Encapsulation Mode (Tunnel selected), IPSec Protocol (ESP selected), Encryption Algorithm (DES selected), and Authentication Algorithm (SHA1 selected). The SA Life Time is set to 28800 seconds, and Perfect Forward Secrecy (PFS) is set to None. 'Back' and 'Next' buttons are at the bottom.

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



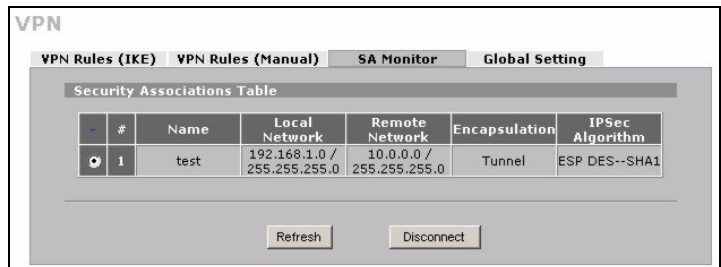
7 Cliquez sur **Close** (Fermer) dans l'écran final pour terminer l'installation de l'assistant de VPN. Suivez la section suivante pour activer la règle VPN et établir une connexion VPN.



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.



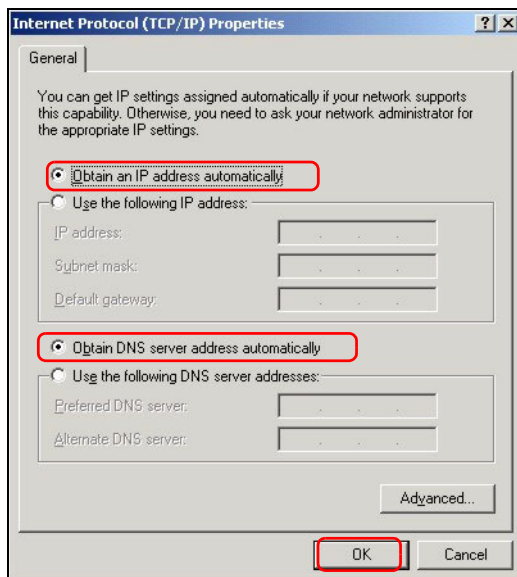
Cliquez sur **SECURITY** (SÉCURITÉ) > **VPN** dans le panneau de navigation et ensuite sur l'onglet du **SA Monitor** (Moniteur SA) pour afficher une liste de tunnel VPN connectés (le tunnel VPN "test" est là).

? Si vous ne pouvez pas établir de connexion VPN, vérifiez que le ZyWALL et le routeur IPsec distant utilisent 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.

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 **Start** (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 address 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

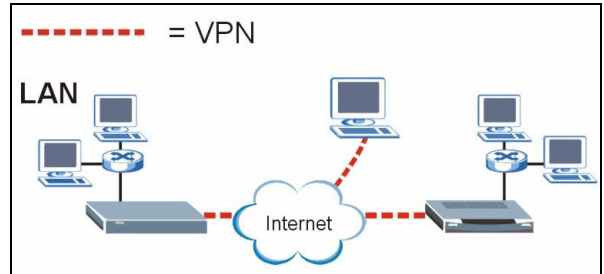
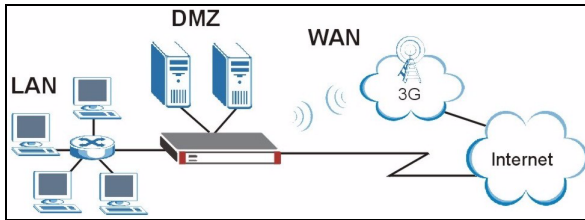
- 1** Allez à www.zyxel.com.
- 2** Sélectionnez votre produit dans la boîte de la liste déroulante dans la page d'accueil de ZyXEL pour aller à la page de ce produit.
- 3** Sélectionnez la certification que vous désirez consulter dans cette page.

Cenni generali

ZyWALL 2WG è un firewall con funzionalità di dotato di funzioni di VPN, gestione della larghezza di banda, filtraggio dei contenuti 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.



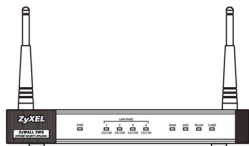
Questa guida è suddivisa nelle seguenti sezioni:

- 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:

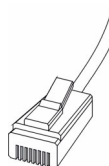
ZyWALL



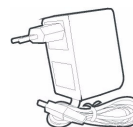
Computer



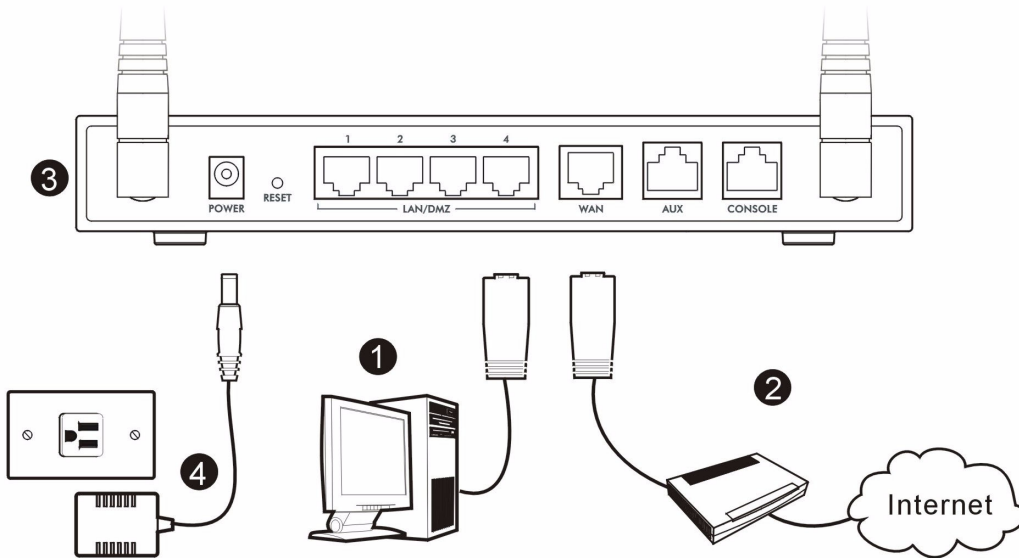
Cavi Ethernet



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.

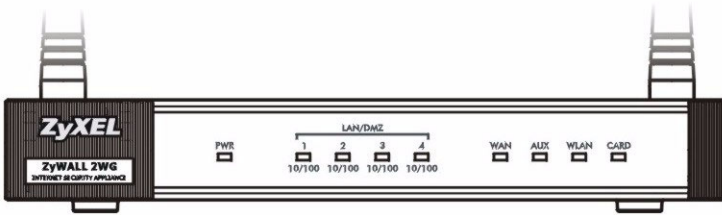


Utilizzare il cavo di console blu se si desidera collegare la porta **CONSOLE** al computer. Utilizzare il cavo di backup per composizione nero se si desidera collegare la porta **AUX** a un modem analogico.

3 Per accedere a Internet senza fili tramite una rete 3G, inserire una scheda wireless 3G nell'apposito slot situato sul pannello laterale. 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. I LED **CARD**, **LAN/DMZ** e **WAN** si accendono e restano accesi se i corrispondenti collegamenti sono stati eseguiti correttamente.

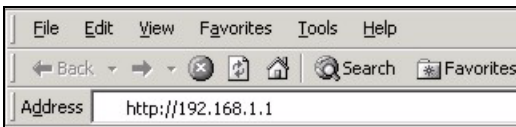


- ? Se nessuno dei LED è acceso, verificare i collegamenti e controllare che i cavi non presentino alcun danno. Assicurarsi di aver collegato l'alimentatore allo ZyWALL e a una sorgente di alimentazione appropriata. Assicurarsi che la sorgente di alimentazione sia attiva. Se i LED restano ancora spenti, contattare il rivenditore locale.

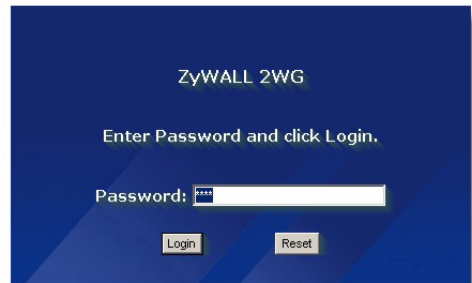
2 Accesso allo strumento di configurazione Web

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.

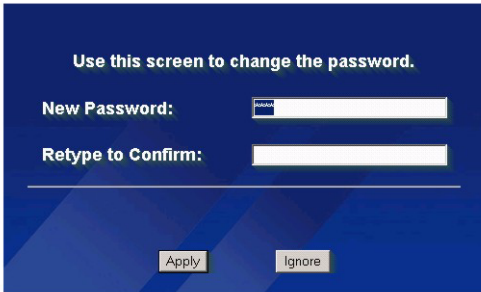


- 2 Fare clic su **Login** (accedi) (la password predefinita 1234 è già immessa).



- ? Se non viene visualizzata la schermata di login, controllare le impostazioni di sicurezza del browser e verificare che la scheda Ethernet del computer sia installata e correttamente funzionante.
Il computer deve inoltre ottenere automaticamente un indirizzo IP da un server DHCP. Per ulteriori informazioni, vedere Impostare l'indirizzo IP del computer.

- 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.



Use this screen to change the password.

New Password:

Retype to Confirm:

Apply Ignore



Replace Factory Default Certificate

The factory default certificate is common to all ZyWALL models. Click Apply to create a certificate using your ZyWALL's MAC address that will be specific to this device.

Apply Ignore

? Se si è modificata la password e la si è dimenticata, è necessario riportare lo ZyWALL alle impostazioni predefinite (la password è 1234, l'indirizzo IP LAN è 192.168.1.1, e così via). Tenere premuto il pulsante **RESET** (dietro l'unità) finché il LED **PWR** non inizia a lampeggiare, quindi rilasciarlo.

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.

The screenshot shows the ZyXEL web interface. On the left is a navigation menu with options like HOME, REGISTRATION, NETWORK, SECURITY, ADVANCED, NAT, STATIC ROUTE, POLICY ROUTE, BW MGMT, DNS, REMOTE MGMT, UPnP, ALG, LOGS, MAINTENANCE, and LOGOUT. The main content area is titled 'Automatic Refresh Interval None' and includes a 'Refresh' button. It is divided into several sections: 'System Information' (Model: ZyWALL 2WG, Bootbase Version: V1.08, Firmware Version: V4.02(AQI.0)b1, Up Time: 02:56:16, System Time: 2001-01-01 02:56:41 GMT, Device Mode: Router, Firewall: Enabled), 'Security Services' (Content Filter Expiration Date: License Inactive, Web Site Blocked: Not Supported), 'Latest Alerts' (empty table), and 'System Status' (Port Statistics, DHCP Table, VPN, Bandwidth). Below these is a 'System Resources' section with progress bars for Flash (4/8 MB), Memory (23/32 MB), Sessions (14/3000), and CPU (0%). At the bottom is a table of 'Interfaces' with columns for Name, Status, IP/Netmask, IP Assignment, and Renew. The 'WAN 1' row is highlighted with a red circle.

Interfaces	Status	IP/Netmask	IP Assignment	Renew
WAN 1	100M/Full	192.23.37.106/ 255.255.255.0	DHCP client	Renew
WAN 2	Down	0.0.0.0/ 0.0.0.0	IPCP client	Dial
Dial Backup	Down	0.0.0.0/ 0.0.0.0	N/A	Dial
LAN	100M/Full	192.168.1.1/ 255.255.255.0	DHCP server	N/A
WLAN	100M/Full	0.0.0.0/ 0.0.0.0	Static	N/A
DMZ	100M/Full	10.1.2.3/ 255.255.255.0	DHCP server	N/A

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.

The screenshot shows the 'MAINTENANCE' page with the 'Device Mode' tab selected. The 'Current Device Mode' is 'Router'. The 'Device Mode Setup' section includes a note: 'The ZyWALL restarts automatically after you change the device mode and click "Apply"'. There are two radio buttons: 'Router' (selected) and 'Bridge'. The 'Bridge' option is circled in red. Below it, the 'IP Address' is set to '192 . 168 . 1 . 1', the 'IP Subnet Mask' is '255 . 255 . 255 . 0', and the 'Gateway IP Address' is '0 . 0 . 0 . 0'. There are 'Apply' and 'Reset' buttons at the bottom.

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**).

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation

WAN IP Address Assignment

IP Address Assignment

My WAN IP Address

My WAN IP Subnet Mask

Gateway IP Address

First DNS Server

Second DNS Server

• PPP over Ethernet oppure incapsulamento PPTP

Selezionare **Nailed-Up** (riconnesione) 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).

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation (Optional)

Service Name

User Name

Password

Retype to Confirm

Nailed-Up

Idle Timeout (Seconds)

WAN IP Address Assignment

IP Address Assignment

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation

User Name

Password

Retype to Confirm

Nailed-Up

Idle Timeout (Seconds)

PPTP Configuration

My IP Address

My IP Subnet Mask

Server IP Address

Connection ID/Name

WAN IP Address Assignment

IP Address Assignment

2 Fare clic su **Next** (avanti) per visualizzare la schermata in cui è possibile registrare lo ZyWALL in myZyXEL.com (il centro servizi online di ZyXEL) e attivare l'applicazione di valutazione gratuita per il filtraggio dei contenuti. Altrimenti fare clic su **Skip** (ignora) e quindi su **Close** (chiudi) per completare la configurazione dell'accesso a Internet.

INTERNET ACCESS

Product registration and service activation for free

You can register ZyWALL on <http://www.zyxel.com> and activate "Free Trial" of Content Filtering service on your ZyWALL.

Click "Next" to activate these services for FREE.

3 Se si dispone già di un account su myZyXEL.com, selezionare **Existing myZyXEL.com account** (account esistente) e immettere le informazioni relative all'account. Altrimenti 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).

INTERNET ACCESS

Device Registration

New myZyXEL.com account Existing myZyXEL.com account

User Name (Type username and password from 6 to 20 characters.)

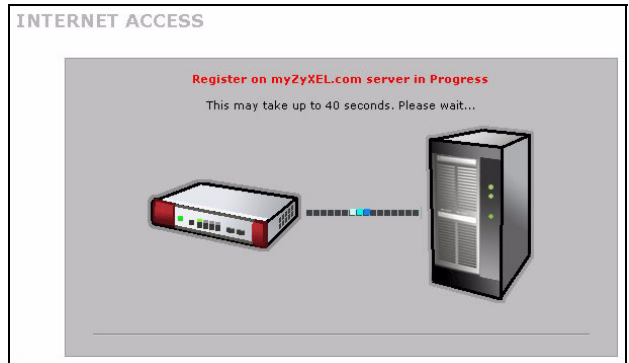
Password

Confirm Password

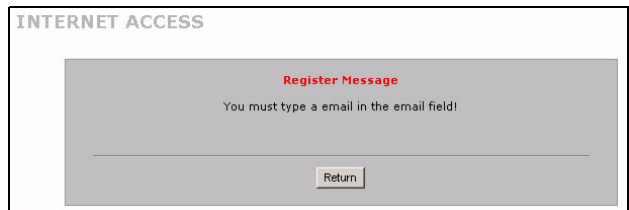
E-Mail Address

Country

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.



7



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.



Se non è possibile accedere a Internet via WAN 1, 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.

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 indirizzi 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** (inoltre 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).

NAT

NAT Overview | Address Mapping | **Port Forwarding** | Port Triggering

Port Forwarding Rules

WAN Interface:

Default Server: Go To Page:

#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	web	80 - 80	0 - 0	10 . 0 . 0 . 20
2	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
3	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
4	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
5	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
6	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
7	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
8	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
9	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
10	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0

Note 1: You may also need to create a [Firewall](#) rule.
Note 2: Port Translation is optional.

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.

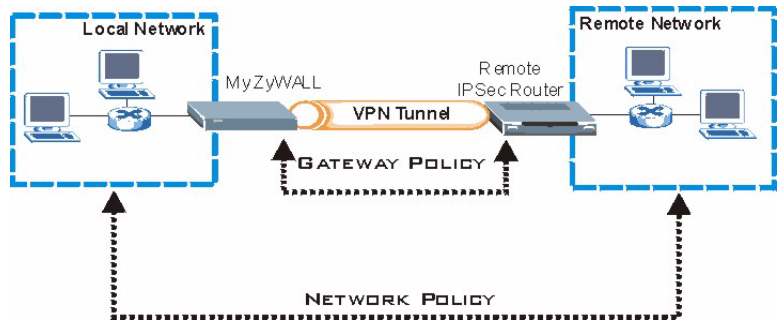
Se si utilizza lo ZyWALL in modalità router, continuare con la prossima sezione. Per la modalità bridge, è valida la configurazione iniziale.

8 Configurazione delle regole di VPN

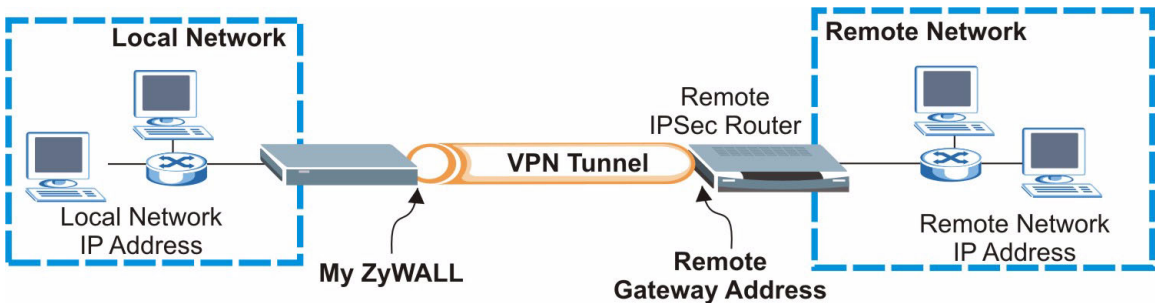
Un tunnel VPN (Virtual Private Network, rete privata virtuale) offre una connessione sicura a un altro computer o rete.

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.

WIZARD - VPN

Gateway Policy Property

Name

Gateway Policy Setting

My ZyWALL

Remote Gateway Address

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 indirizzi 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.

WIZARD - VPN

Network Policy Property

Active

Name

Network Policy Setting

Local Network Single Range IP Subnet

Starting IP Address

Ending IP Address / Subnet Mask

Remote Network Single Range IP Subnet

Starting IP Address

Ending IP Address / 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).

The screenshot shows the 'WIZARD - VPN' configuration interface. The title bar reads 'WIZARD - VPN'. Below it, the main heading is 'IKE Tunnel Setting (IKE Phase 1)'. The configuration options are as follows:

- Negotiation Mode: Main Mode Aggressive Mode
- Encryption Algorithm: DES AES 3DES
- Authentication Algorithm: SHA1 MD5
- Key Group: DH1 DH2
- SA Life Time: 26800 (Seconds)
- Pre-Shared Key: 12345678

At the bottom right, there are 'Back' and 'Next' buttons.

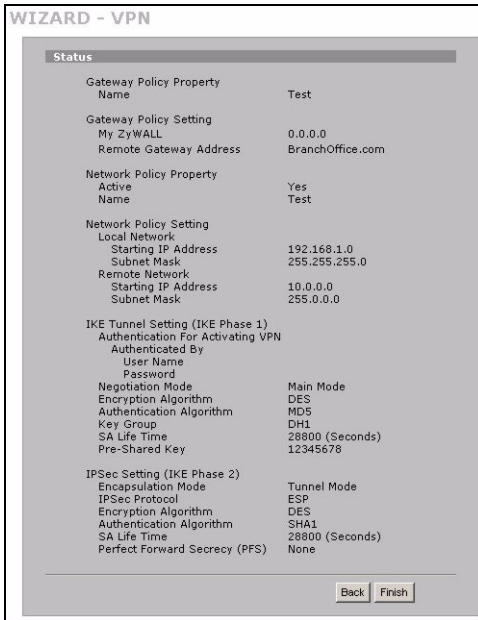
- 5 Utilizzare questa schermata per configurare le impostazioni IPSec.

The screenshot shows the 'WIZARD - VPN' configuration interface. The title bar reads 'WIZARD - VPN'. Below it, the main heading is 'IPSec Setting (IKE Phase 2)'. The configuration options are as follows:

- Encapsulation Mode: Tunnel Transport
- IPSec Protocol: ESP AH
- Encryption Algorithm: DES AES 3DES NULL
- Authentication Algorithm: SHA1 MD5
- SA Life Time: 26800 (Seconds)
- Perfect Forward Secrecy (PFS): None DH1 DH2

At the bottom right, there are 'Back' and 'Next' buttons.

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



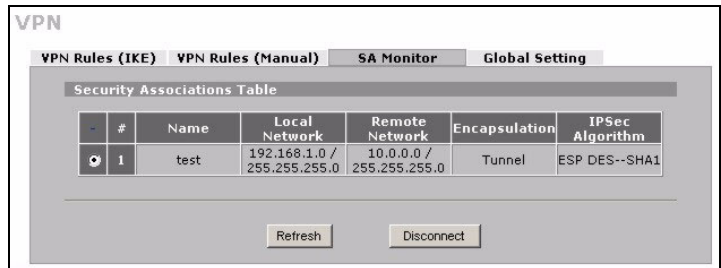
7 Fare clic su **Close** (chiudi) nella schermata finale per completare l'installazione guidata della VPN. Continuare con la prossima sezione per attivare la regola VPN e stabilire una connessione VPN.



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").



Se non è possibile 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.

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**.

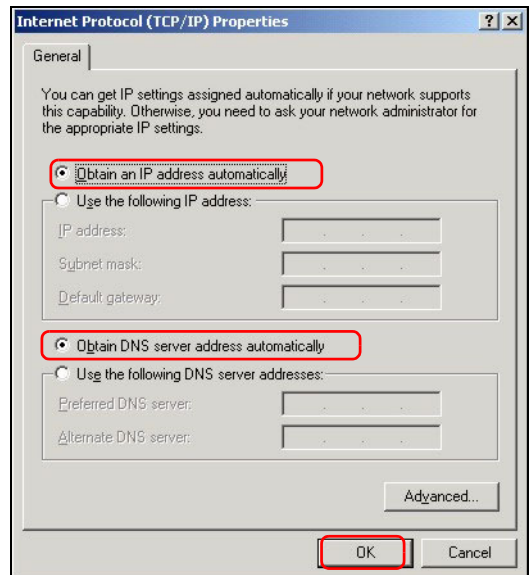
4 Selezionare **Protocollo Internet (TCP/IP)** (sotto la scheda **Generale** in Windows XP) e fare clic su **Proprietà**.

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

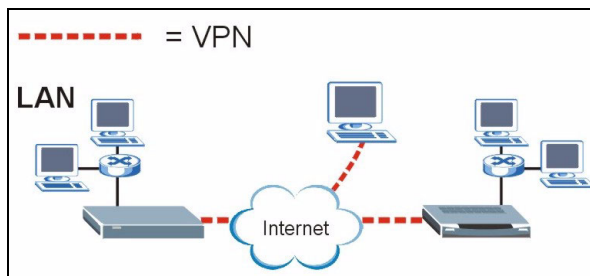
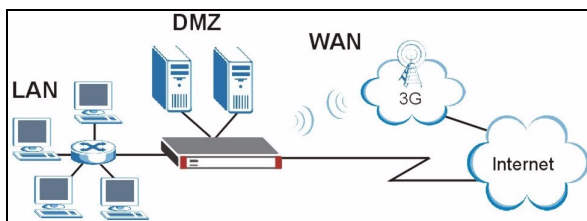
- 1** Aprire la pagina www.zyxel.com.
- 2** Selezionare il prodotto dall'elenco di riepilogo a discesa nella Home Page di ZyXEL per passare alla pagina del prodotto in questione.
- 3** Selezionare da questa pagina la certificazione che si desidera visualizzare.

Обзор

Устройство ZyWALL 2WG представляет собой межсетевой экран с функциями виртуальной частной сети, управления пропускной способностью, фильтрацией контента 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.



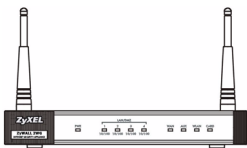
Данное руководство включает следующие разделы.

- 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.

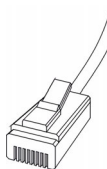
ZyWALL



Компьютер



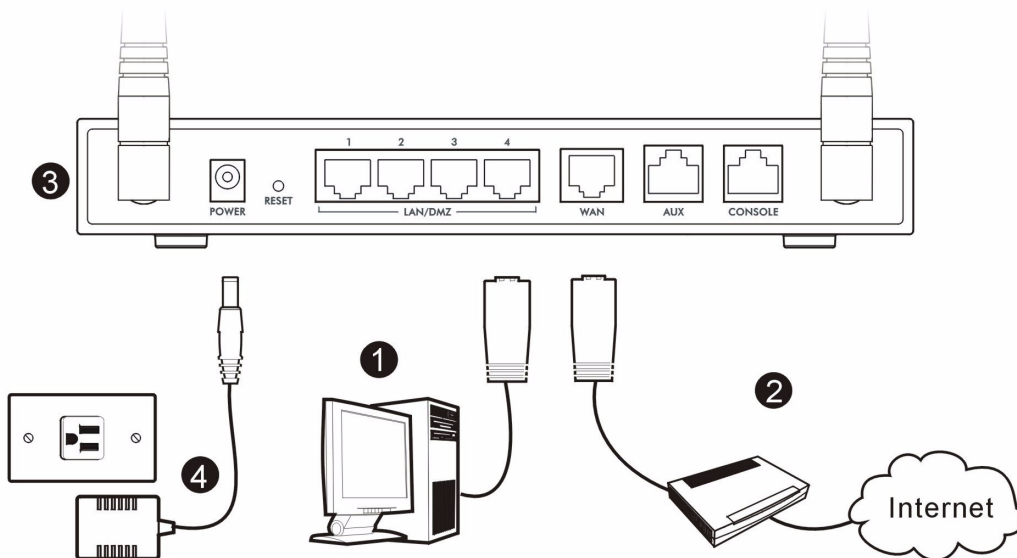
Кабели Ethernet



Адаптер питания



Для подключения оборудования выполните следующие действия.



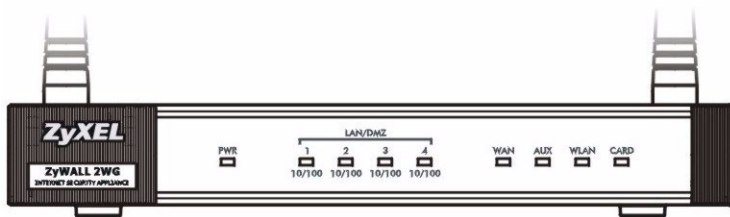
1 Для подключения портов **LAN/DMZ** к компьютеру используется кабель Ethernet. Если в Web-конфигураторе эти порты настроены как порты **DMZ** в окне **LAN** или **DMZ**, для подключения общедоступных серверов (web-сервер, почтовый сервер, FTP-сервер и др.) к портам **LAN/DMZ** можно также использовать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

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



Если вы хотите подключить к своему компьютеру порт **CONSOLE** (КОНСОЛЬ), то используйте синий кабель консоли. Если вы хотите подключить порт **AUX** к аналоговому модему, то используйте черный запасной кабель.

- 3 Для подключения к беспроводной сети 3G вставьте беспроводную карту 3G в слот на боковой панели. 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. Светодиоды **CARD**, **LAN/DMZ** и **WAN** горят, если правильно выполнены соответствующие соединения.

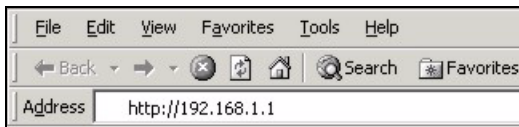


- ?** Если ни один из индикаторов не загорается, то проверьте подключение оборудования и целостность кабелей. Убедитесь, что вы подключили к ZyWALL блок питания верного типа и включили его в подходящий источник электропитания. Убедитесь, что сетевое питание включено. Если индикаторы все еще не горят, то обратитесь к вашему местному поставщику.

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).

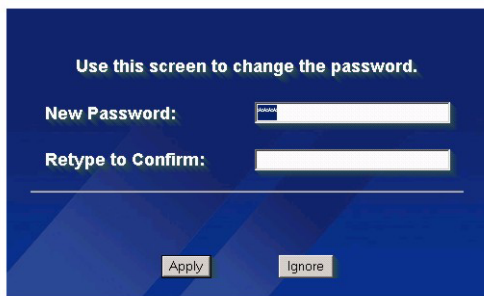


- 2 Щелкните **Login** (Вход) (пароль по умолчанию 1234 уже введен).



? Если экран входа в систему не появляется, то проверьте настройки безопасности вашего браузера и нормальную работу сетевой Ethernet карты вашего компьютера. На вашем компьютере также должно быть включено автоматическое получение IP-адреса с DHCP-сервера. Для получения дополнительной информации смотрите раздел [Установка IP-адреса компьютера](#).

- 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.





Если вы изменили пароль, а затем его забыли, то необходимо вернуть ZyWALL к заводским настройкам по умолчанию (пароль - 1234, IP адрес ЛВС 192.168.1.1 и т.д.). Нажмите на кнопку **RESET** (СБРОС) (на задней панели) до тех пор, пока не начнет мигать индикатор **PWR** (ПИТАНИЕ), а затем отпустите ее.

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

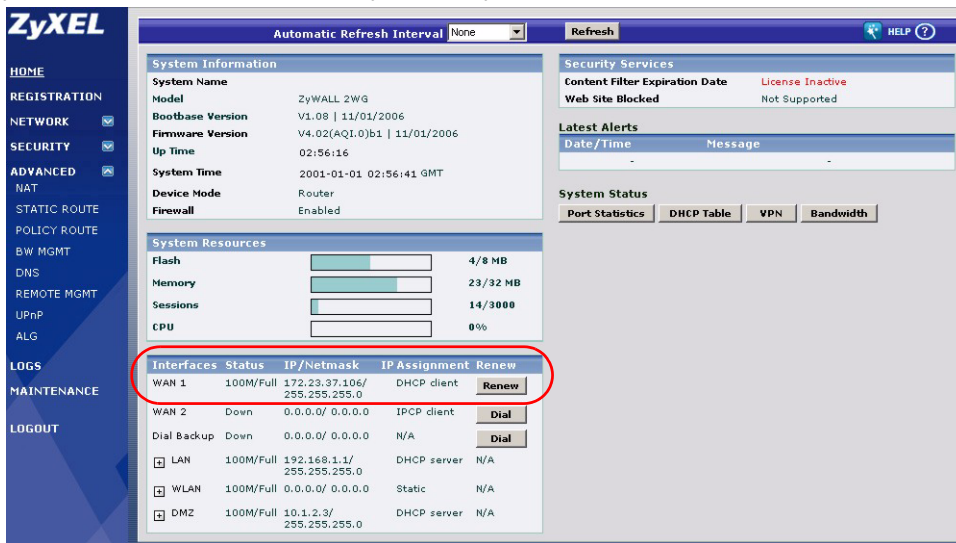
По умолчанию в ZyWALL установлен режим маршрутизатора. Если вы хотите использовать функции маршрутизации, такие как NAT, DHCP и VPN, переходите к следующему шагу.

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](#).

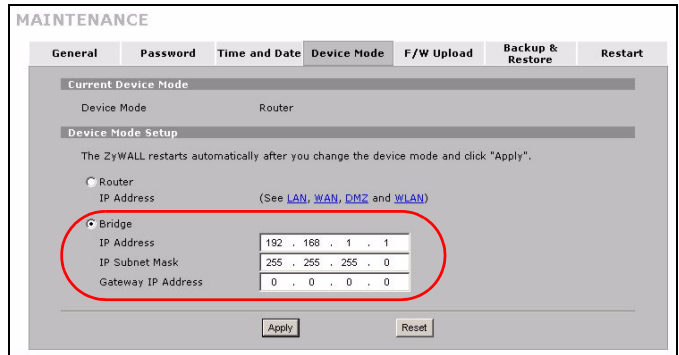
Для настройки порта **WAN 2** используются окна **WAN** в разделе **NETWORK** (СЕТЬ). Вы также можете установить распределение разгрузки между разъемами ГВС.



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**).

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation

WAN IP Address Assignment

IP Address Assignment

My WAN IP Address

My WAN IP Subnet Mask

Gateway IP Address

First DNS Server

Second DNS Server

- **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).

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation (Optional)

Service Name

User Name

Password

Retype to Confirm

Nailed-Up

Idle Timeout (Seconds)

WAN IP Address Assignment

IP Address Assignment

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation

User Name

Password

Retype to Confirm

Nailed-Up

Idle Timeout (Seconds)

PPTP Configuration

My IP Address

My IP Subnet Mask

Server IP Address

Connection ID/Name

WAN IP Address Assignment

IP Address Assignment

2 Щелкните кнопку **Next** (Далее), чтобы вызвать окно, в котором вы можете зарегистрировать ваш ZyWALL на сайте myZyXEL.com (центр онлайн обслуживания компании ZyXEL) и активировать бесплатный фильтр содержания пробное приложение. В другом случае, щелкните **Skip** (Пропустить) и затем **Close** (Закреть) для завершения настройки доступа в Интернет.

INTERNET ACCESS

Product registration and service activation for free

You can register ZyWALL on <http://www.zyxel.com> and activate "Free Trial" of Content Filtering service on your ZyWALL.

Click "Next" to activate these services for FREE.

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).

INTERNET ACCESS

Device Registration

New myZyXEL.com account Existing myZyXEL.com account

User Name (Type username and password from 6 to 20 characters.)

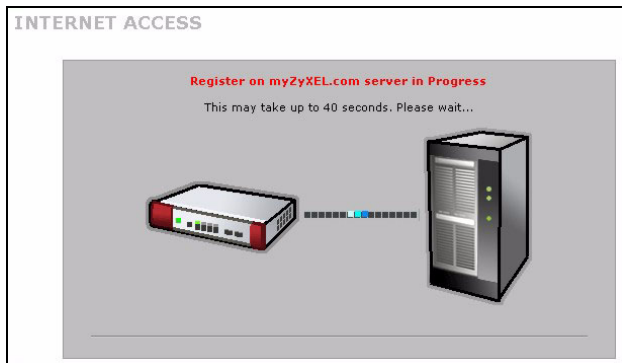
Password

Confirm Password

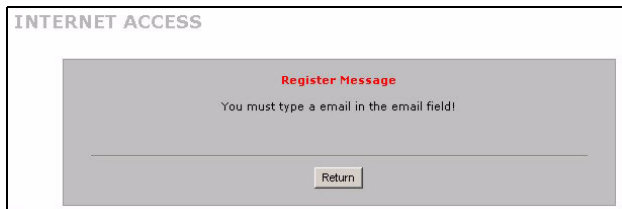
E-Mail Address

Country

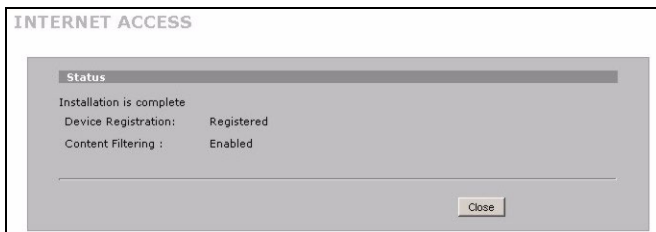
4 Подождите, пока завершится процесс регистрации.



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** (Закреть), 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.



Если вы не можете войти в Интернет через ГВС 1, то проверьте подключение ZyWALL к разъему Ethernet через который происходит доступ в Интернет. Убедитесь в нормальной работе шлюзового устройства (такого как модем DSL). Щелкните на кнопке **WAN** (ГВС) на панели навигации, чтобы проверить ваши настройки.

5 DMZ

DMZ (DeMilitarized Zone - демилитаризованная зона) позволяет внешним пользователям обращаться к общедоступным серверам (web-сервер, 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.



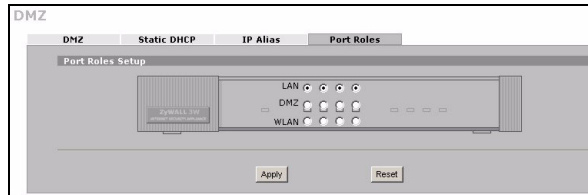
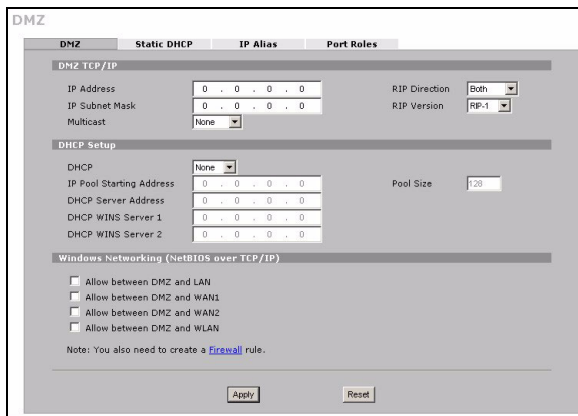
Настройка DMZ в режиме межсетевого моста не требуется, см. далее [Раздел 7](#).

- 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).

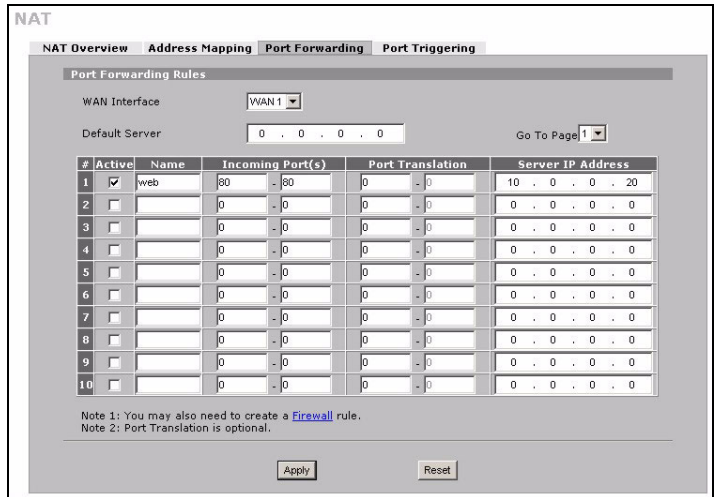


6 NAT

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.

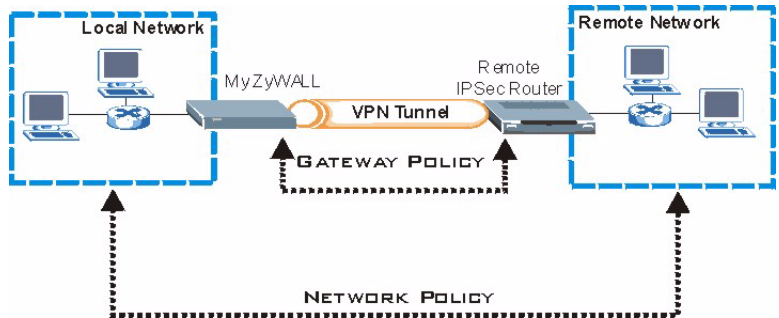
Если ZyWALL находится в режиме маршрутизации, переходите к следующему разделу. В режиме моста вы будете работать с начальной конфигурацией.

8 Настройка правил виртуальной частной сети (VPN)

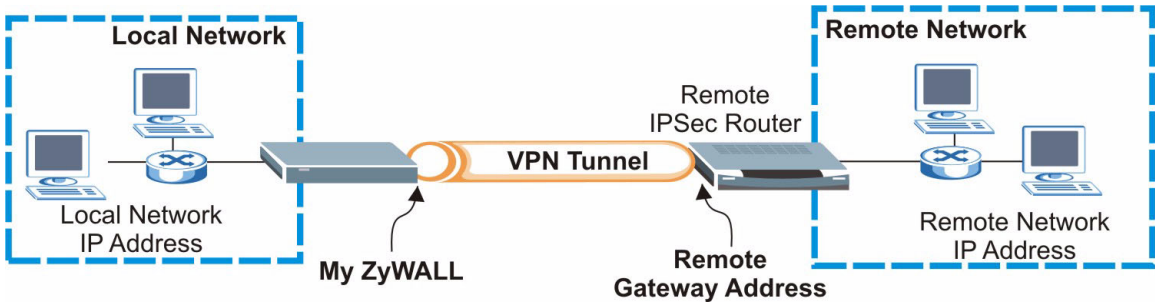
Туннель VPN (Virtual Private Network - виртуальная частная сеть) обеспечивает защищенное соединение к другому компьютеру или сети.

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.



- 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.

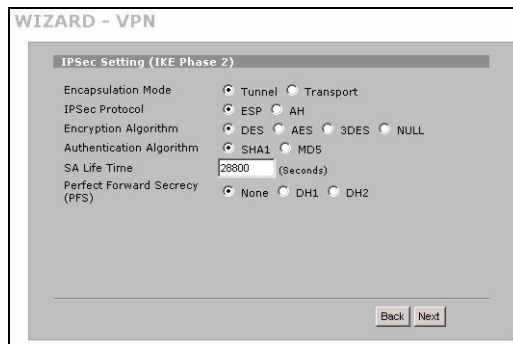
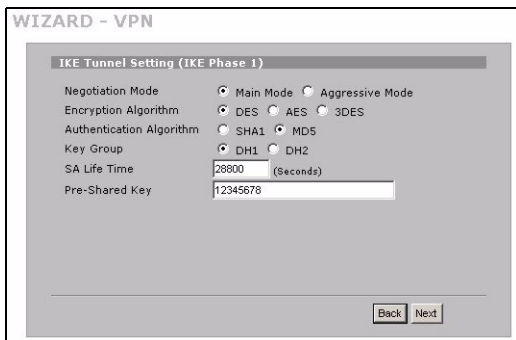
Encapsulation Mode (Режим инкапсуляции): Режим **Tunnel** (Туннель) совместим с NAT, режим **Transport** (Транспорт) не совместим.

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

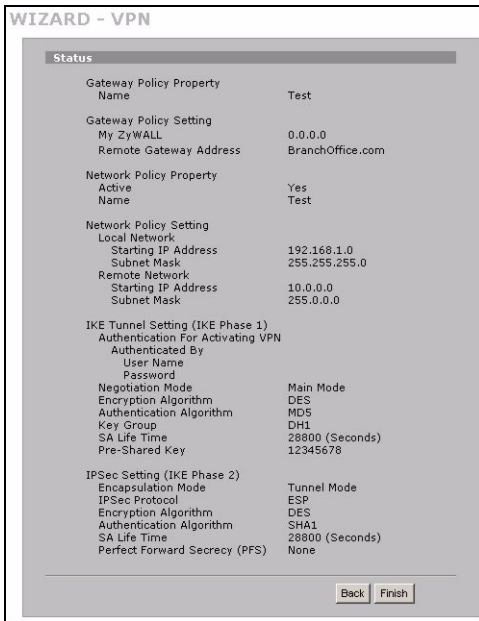
Perfect Forward Secrecy (PFS) (Идеальная прямая безопасность): **None** (Нет) позволяет быструю настройку IPSec, но **DH1** и **DH2** повышают уровень безопасности.

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

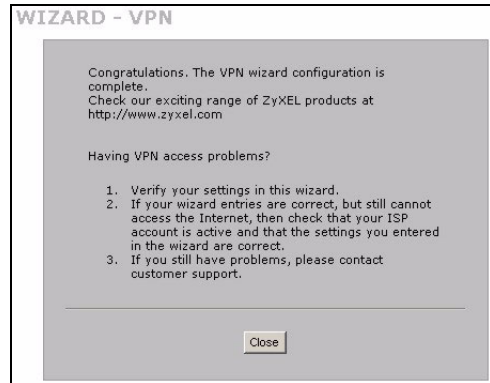
5 Это окно используется для настройки параметров IPSec.



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



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

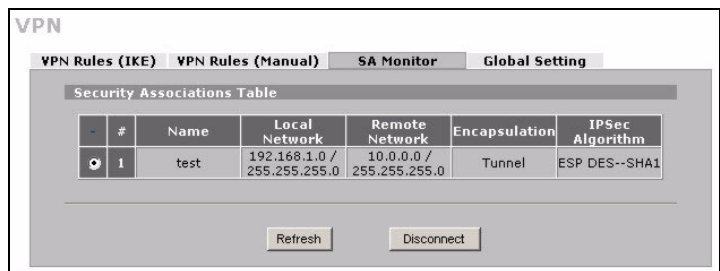


8.1 Использование соединения VPN

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”).

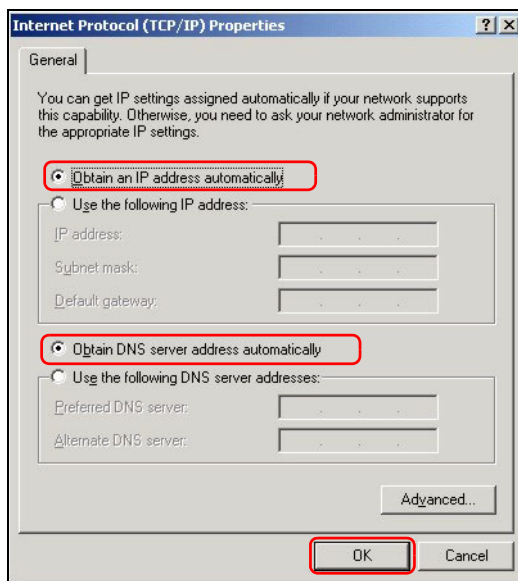


? Если вы не можете установить соединение VPN, то убедитесь, что ZyWALL и удаленный маршрутизатор IPSec используют одинаковые настройки VPN. Щелкните на кнопке **VPN** (ГВС) на панели навигации, чтобы установить расширенные настройки. Посетите какой-либо веб-сайт, чтобы проверить успешное подключение к Интернет

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** (Закреть) (**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

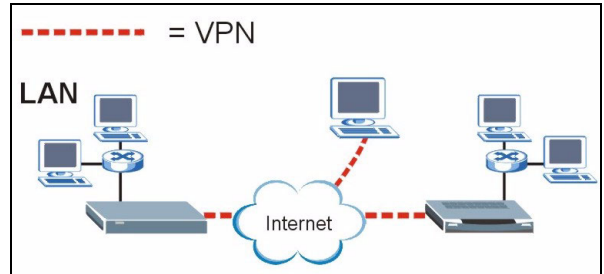
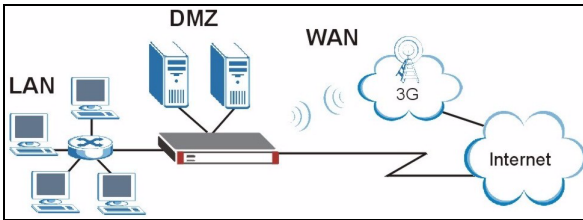
- 1 Перейдите на сайт www.zyxel.ru.
- 2 Выберите изделие из раскрывающегося списка на домашней странице ZyXEL для перехода на страницу, посвященную этому изделию.
- 3 Выберите сертификат для просмотра.

Översikt

ZyWALL 2WG är en brandvägg med VPN, bandbreddshantering, innehållsfiltrering 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.

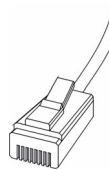
ZyWALL



Dator



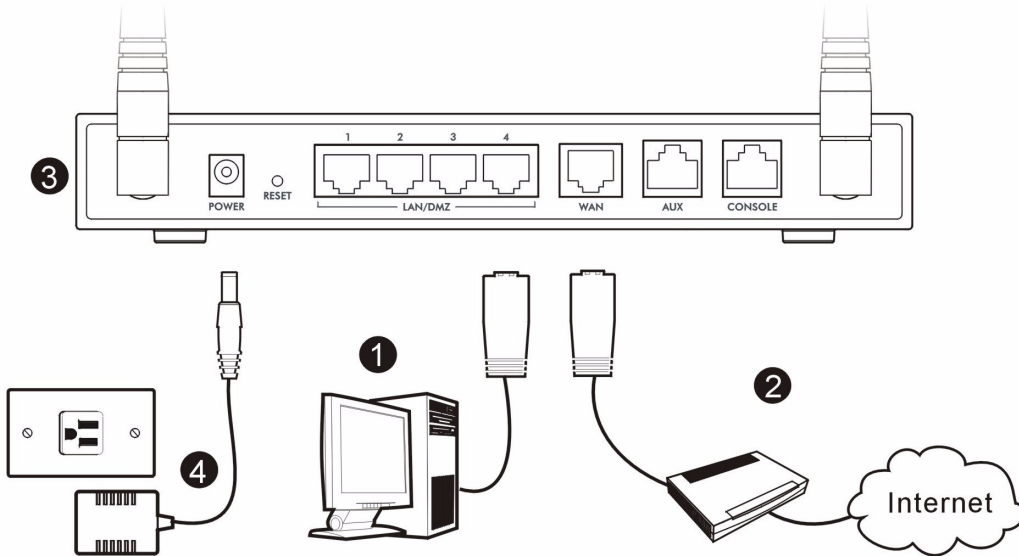
Nätverkskablar



Strömadapter



Gör följande för att utföra maskinvaruanslutningar för initial inställning.



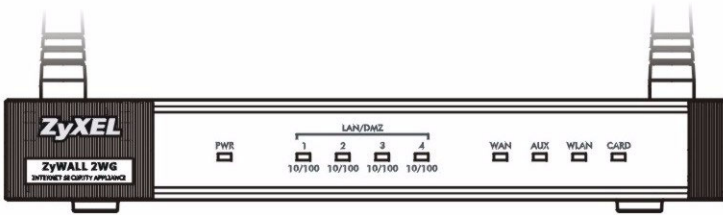
- 1 Använd en Ethernet-kabel för att ansluta **LAN/DMZ**-porten till en dator. Om du konfigurerar dessa portar som DMZ-portar i **LAN** eller **DMZ**-menyn genom webbkonfiguratoren, kan du även använda Nätverkskablar för att ansluta offentliga servrar (webb, e-post, FTP osv) till **LAN/DMZ**-portarna.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



Använd den blå konsolkabeln om du vill ansluta **CONSOLE**-porten till datorn. Använd den svarta dial-backupkabeln om du vill ansluta **AUX**-porten till ett analogt modem.

- 3 Anslut ett 3G kort i PCMCIA ingången på produktens baksida för att få möjlighet att ansluta via ett 3G nät. 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. Indikatorlamporna **CARD**, **LAN/DMZ** och **WAN** tänds och fortsätter att lysa om motsvarande anslutningar är rätt utförda.

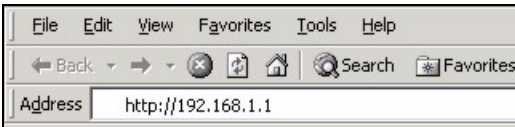


- ? Om inga LED-lampor lyser, kontrollera anslutningarna samt kontrollera att kablarna inte är skadade. Kontrollera att strömadaptern är ansluten till ZyWALL och ansluten till en lämplig strömkälla. Kontrollera att kraftkällan är påslagen. Tag kontakt med den lokala återförsäljaren om LED-lamporna fortfarande inte lyser.

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.

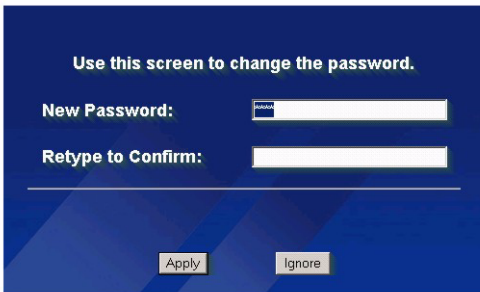


- 2 Klicka på **Login** (standardlösenordet 1234 är redan angivet).



- ? Om inloggningskärmen inte visas, kontrollera webbläsarens säkerhetsinställningar och kontrollera att datorns Ethernetkort är installerat och fungerar som det ska. Datorn ska även vara inställd att automatiskt få en IP-adress från en DHCP-server. Se Ställa in datorns IP-adress för mer information.

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



Use this screen to change the password.

New Password:

Retype to Confirm:

Apply Ignore

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



Replace Factory Default Certificate

The factory default certificate is common to all ZyWALL models. Click Apply to create a certificate using your ZyWALL's MAC address that will be specific to this device.

Apply Ignore

? Om du har bytt lösenord och glömt det, måste du återställa ZyWALL till grundinställningarna (lösenordet är 1234, LAN IP-adressen är 192.168.1.1, etc.). Tryck på **RESET** -knappen (på baksidan) tills **PWR** LED-lampan börjar blinka. Släpp därefter knappen.

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.

The screenshot shows the ZyXEL web interface. On the left is a navigation menu with options like HOME, REGISTRATION, NETWORK, SECURITY, ADVANCED, NAT, STATIC ROUTE, POLICY ROUTE, BW MGMT, DNS, REMOTE MGMT, UPnP, ALG, LOGS, MAINTENANCE, and LOGOUT. The main content area is titled 'Automatic Refresh Interval None' and has a 'Refresh' button. It is divided into several sections:

- System Information:** Model: ZyWALL 2WG, Bootbase Version: V1.08 | 11/01/2006, Firmware Version: V4.02(AQI.0)b1 | 11/01/2006, Up Time: 02:56:16, System Time: 2001-01-01 02:56:41 GMT, Device Mode: Router, Firewall: Enabled.
- System Resources:** Flash: 4/8 MB, Memory: 23/32 MB, Sessions: 14/3000, CPU: 0%.
- Interfaces:** A table with columns: Interfaces, Status, IP/Netmask, IP Assignment, Renew.

Interfaces	Status	IP/Netmask	IP Assignment	Renew
WAN 1	100M/Full	172.23.37.106/ 255.255.255.0	DHCP client	Renew
WAN 2	Down	0.0.0.0/ 0.0.0.0	IPCP client	Dial
Dial Backup	Down	0.0.0.0/ 0.0.0.0	N/A	Dial
LAN	100M/Full	192.168.1.1/ 255.255.255.0	DHCP server	N/A
WLAN	100M/Full	0.0.0.0/ 0.0.0.0	Static	N/A
DMZ	100M/Full	10.1.2.3/ 255.255.255.0	DHCP server	N/A
- Security Services:** Content Filter Expiration Date: License Inactive, Web Site Blocked: Not Supported.
- Latest Alerts:** Table with Date/Time and Message columns.
- System Status:** Buttons for Port Statistics, DHCP Table, VPN, and Bandwidth.

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.

The screenshot shows the 'MAINTENANCE' page with tabs for General, Password, Time and Date, Device Mode, F/W Upload, Backup & Restore, and Restart. The 'Device Mode' tab is active, showing 'Current Device Mode' as Router. Under 'Device Mode Setup', there is a note: 'The ZyWALL restarts automatically after you change the device mode and click "Apply".' There are two radio buttons: 'Router' (selected) and 'Bridge'. The 'Bridge' mode is highlighted with a red circle. Below it, the following fields are visible:

- IP Address: 192 . 168 . 1 . 1
- IP Subnet Mask: 255 . 255 . 255 . 0
- Gateway IP Address: 0 . 0 . 0 . 0

Buttons for 'Apply' and 'Reset' are at the bottom.

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 uppgifterna för din Internet anslutning 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**.

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation

WAN IP Address Assignment

IP Address Assignment

My WAN IP Address

My WAN IP Subnet Mask

Gateway IP Address

First DNS Server

Second DNS Server

- **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**.

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation (Optional)

Service Name

User Name

Password

Retype to Confirm

Nailed-Up

Idle Timeout (Seconds)

WAN IP Address Assignment

IP Address Assignment

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation

User Name

Password

Retype to Confirm

Nailed-Up

Idle Timeout (Seconds)

PPTP Configuration

My IP Address

My IP Subnet Mask

Server IP Address

Connection ID/Name

WAN IP Address Assignment

IP Address Assignment

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

INTERNET ACCESS

Product registration and service activation for free

You can register ZyWALL on <http://www.zyxel.com> and activate "Free Trial" of Content Filtering service on your ZyWALL.

Click "Next" to activate these services for FREE.

- 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**.

INTERNET ACCESS

Device Registration

New myZyXEL.com account Existing myZyXEL.com account

User Name

Password

Confirm Password

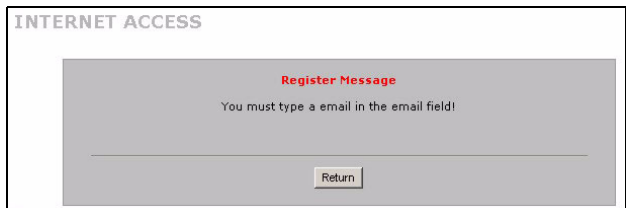
E-Mail Address

Country

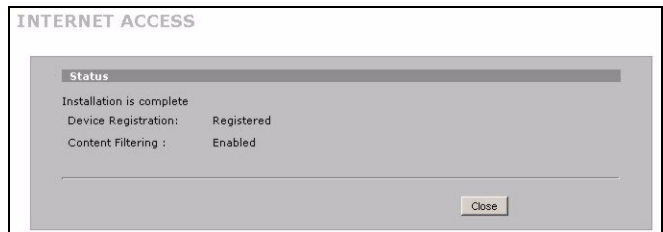
4 Vänta tills registreringsprocessen är slutförd.



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 menyn **REGISTRATION Service**. Se manualen för mer information.



Om du inte kommer åt Internet via WAN 1, kontrollera ZyWALL:s anslutning till Ethernetkontakten med Internetåtkomst. Kontrollera att Internet-gatewayenheten (t ex ett DSL-modem) fungerar som den ska. Klicka på **WAN** i navigationspanelen för att verifiera dina inställningar.

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 serverna 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 värdserverar 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 **DMZ** 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**.

NAT

NAT Overview Address Mapping **Port Forwarding** Port Triggering

Port Forwarding Rules

WAN Interface: WAN1

Default Server: 0 . 0 . 0 . 0 Go To Page: 1

#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	web	80 - 80	0 - 0	10 . 0 . 0 . 20
2	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
3	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
4	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
5	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
6	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
7	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
8	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
9	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
10	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0

Note 1: You may also need to create a [Firewall](#) rule.
Note 2: Port Translation is optional.

Apply Reset

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.

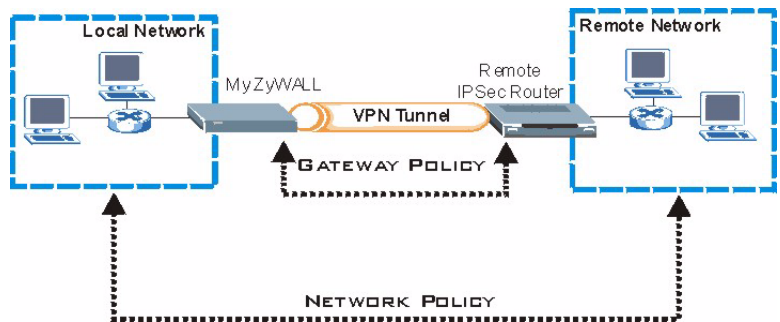
Om du använder din ZyWALL i routerläge, fortsatt med nästa avsnitt. För bryggläge, är du färdig med den initiala konfigurationen.

8 Inställning av VPN-regel

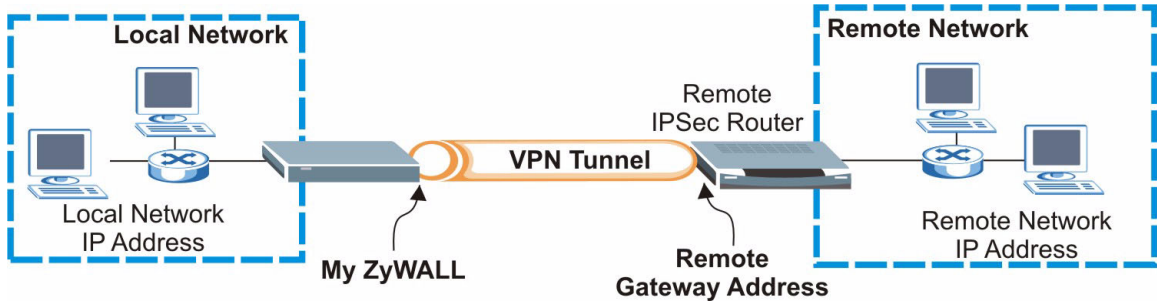
En VPN-tunnel (Virtual Private Network) ger dig en säker anslutning till en annan dator eller ett annat nätverk.

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 guidemenyerna.



- 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 gatewaypolicyen.

Name: Ange ett Name för att identifiera gatewaypolicyen.

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

WIZARD - VPN

Gateway Policy Property

Name

Gateway Policy Setting

My ZyWALL

Remote Gateway Address

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.

WIZARD - VPN

IKE Tunnel Setting (IKE Phase 1)

Negotiation Mode Main Mode Aggressive Mode

Encryption Algorithm DES AES 3DES

Authentication Algorithm SHA1 MD5

Key Group DH1 DH2

SA Life Time (Seconds)

Pre-Shared Key

5 Använd denna meny för att konfigurera IPSec-inställningar.

WIZARD - VPN

IPSec Setting (IKE Phase 2)

Encapsulation Mode Tunnel Transport

IPSec Protocol ESP AH

Encryption Algorithm DES AES 3DES NULL

Authentication Algorithm SHA1 MD5

SA Life Time (Seconds)

Perfect Forward Secrecy (PFS) None DH1 DH2

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

WIZARD - VPN

Status

Gateway Policy Property Name	Test
Gateway Policy Setting My ZyWALL	0.0.0.0
Remote Gateway Address	BranchOffice.com
Network Policy Property Active	Yes
Network Policy Property Name	Test
Network Policy Setting Local Network	
Starting IP Address	192.168.1.0
Subnet Mask	255.255.255.0
Remote Network	
Starting IP Address	10.0.0.0
Subnet Mask	255.0.0.0
IKE Tunnel Setting (IKE Phase 1)	
Authentication For Activating VPN	
Authenticated By User Name	
Password	
Negotiation Mode	Main Mode
Encryption Algorithm	DES
Authentication Algorithm	MD5
Key Group	DH1
SA Life Time	28800 (Seconds)
Pre-Shared Key	12345678
IPSec Setting (IKE Phase 2)	
Encapsulation Mode	Tunnel Mode
IPSec Protocol	ESP
Encryption Algorithm	DES
Authentication Algorithm	SHA1
SA Life Time	28800 (Seconds)
Perfect Forward Secrecy (PFS)	None

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.

WIZARD - VPN

Congratulations. The VPN wizard configuration is complete. Check our exciting range of ZyxEL products at <http://www.zyxel.com>

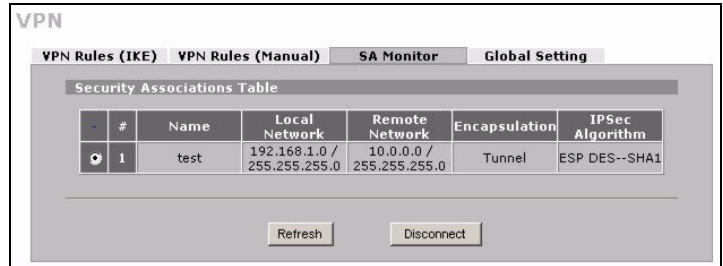
Having VPN access problems?

1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.

8.1 Använda VPN-anlutningen

Använd VPN-tunnlar för att säkert skicka och hämta filer, och tillåta fjärråtkomst till bolagsnätverk, webbserverar 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.



The screenshot shows the ZyWALL VPN configuration page. At the top, there are tabs for 'VPN Rules (IKE)', 'VPN Rules (Manual)', 'SA Monitor', and 'Global Setting'. The 'SA Monitor' tab is selected, displaying the 'Security Associations Table'. The table has the following data:

#	Name	Local Network	Remote Network	Encapsulation	IPSec Algorithm
1	test	192.168.1.0 / 255.255.255.0	10.0.0.0 / 255.255.255.0	Tunnel	ESP DES--SHA1

Below the table are two buttons: 'Refresh' and 'Disconnect'.

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).



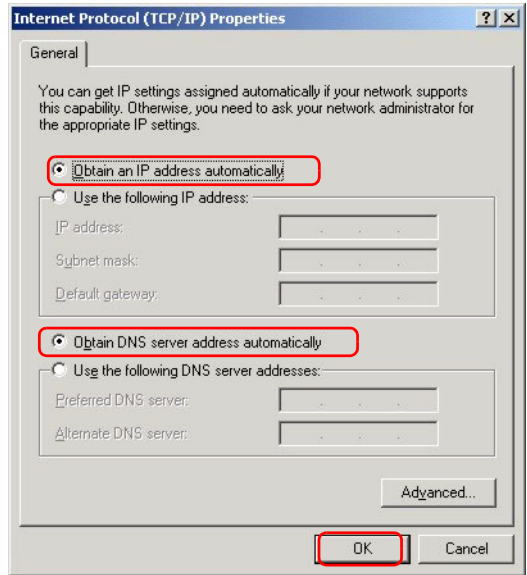
Om du inte kan etablera en VPN-anlutning, kontrollera att ZyWALL och fjärrroutern IPSec använder samma VPN-inställningar. Klicka på **VPN** i navigationspanelen för att konfigurera avancerade inställningar. Öppna en webbsida för att kontrollera att din Internet-anlutning fungerar.

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 uppbringda 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 alternativet **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 menyn **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.

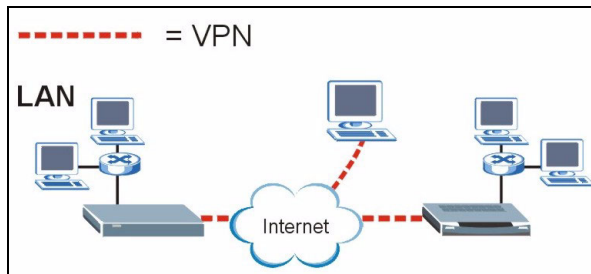
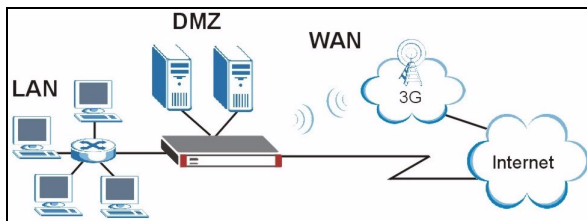
Se www.support.zyxel.se för ytterligare guider.

概述

ZyWALL 2WG 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、内容过滤和多种其他功能。您可以将 ZyWALL 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《用户手册》，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。



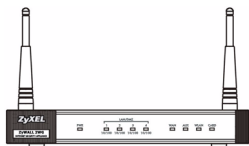
本手册的章节如下。

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

1 硬件连接

您需要以下设备。

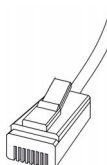
ZyWALL



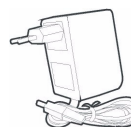
电脑



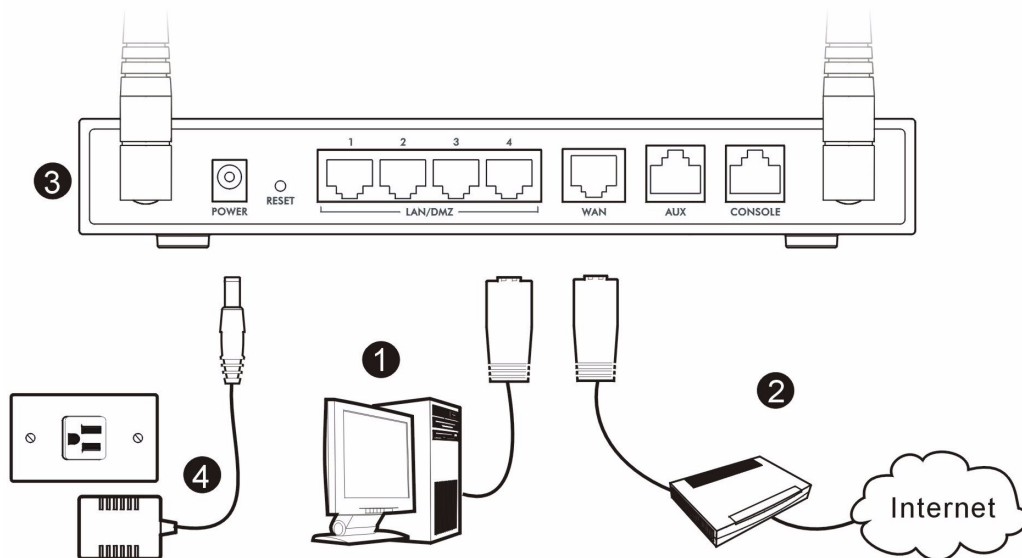
以太网连接线




电源适配器



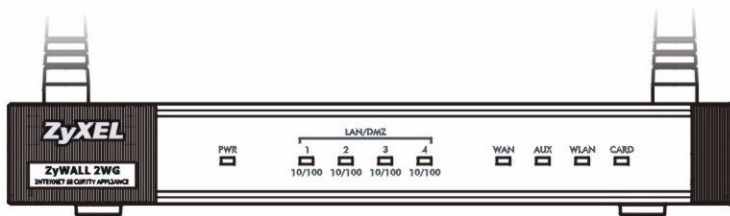
请执行下列步骤，为硬件连接进行初始设置。



- 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。

 若要将 CONSOLE 端口连接至您的电脑，请使用蓝色控制台线路。若要将 AUX 端口连接至模拟
调制解调器，请使用黑色拨号备份线路。

- 3 将 3G 无线网卡插入侧面板上的卡片插槽，通过 3G 网络接入因特网。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。CARD、LAN/DMZ 和 WAN 指示灯会在相关连接正确时亮起并持续亮着。

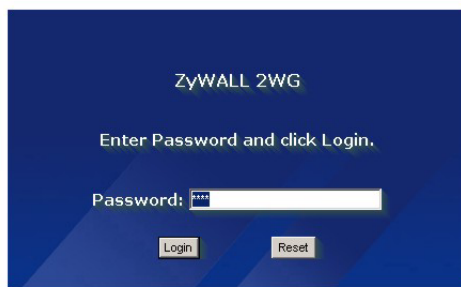
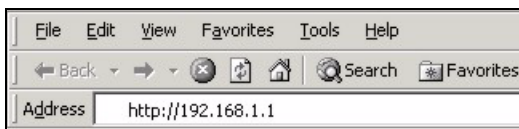


- ?** 如果 LED 指示灯全部不亮，请查看连接，检查电缆是否受损。确保已将电源适配器连接至 ZyWALL 并且插入适当的电源插座。确保电源已开启。如果 LED 指示灯还是没有亮，请联络当地的供应商。

2 访问网络状态设置程序

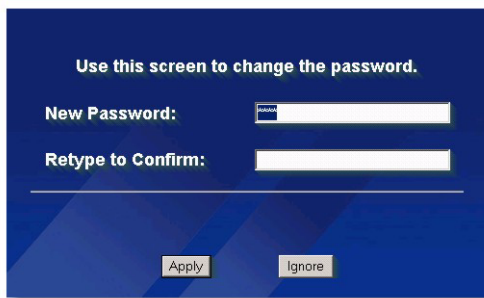
您可以使用本节中的信息来设置 WAN 1 接口的互联网访问。

- 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，设置电脑的 IP 地址。
- 2 单击 **Login** (登录) (已经输入默认密码 **1234**)。



- ?** 若未显示登录屏幕，请检查浏览器的安全设置，确保以太网网卡已经插入电脑且运行正常。此外，电脑也应配置为从 DHCP 服务器获取 IP 地址。请参考「设置电脑的 IP 地址」一节，获取详细信息。

- 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。





如果您更改了密码但却不幸忘记，则需将 ZyWALL 恢复至预设设置（密码是 1234，局域网 IP 地址为 192.168.1.1 等）。按住 **RESET**（重设）按钮（位于后面板）直到 **PWR LED** 指示灯开始闪烁再松开。

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。

如果需要配置 **WAN 2**，请使用 **NETWORK WAN** 屏幕。您也可以设定广域网联机之间的负载平衡。

The screenshot shows the ZyWALL web interface. The left sidebar contains navigation menus: HOME, REGISTRATION, NETWORK, SECURITY, ADVANCED, NAT, STATIC ROUTE, POLICY ROUTE, BW MGMT, DNS, REMOTE MGMT, UPnP, ALG, LOGS, MAINTENANCE, and LOGOUT. The main content area is titled 'Automatic Refresh Interval' and includes a 'Refresh' button and a 'HELP ?' icon. The 'System Information' section displays details such as System Name (ZyWALL 2WG), Model, Bootbase Version (V1.08), Firmware Version (V4.02), Up Time (02:56:16), System Time (2001-01-01 02:56:41 GMT), Device Mode (Router), and Firewall (Enabled). The 'System Resources' section shows progress bars for Flash (4/8 MB), Memory (23/32 MB), Sessions (14/3000), and CPU (0%). The 'Interfaces Status' table is circled in red and contains the following data:

Interfaces	Status	IP/Netmask	IP Assignment	Renew
WAN 1	100M/Full	172.23.37.106/ 255.255.255.0	DHCP client	Renew
WAN 2	Down	0.0.0.0/ 0.0.0.0	IPCP client	Dial
Dial Backup	Down	0.0.0.0/ 0.0.0.0	N/A	Dial
LAN	100M/Full	192.168.1.1/ 255.255.255.0	DHCP server	N/A
WLAN	100M/Full	0.0.0.0/ 0.0.0.0	Static	N/A
DMZ	100M/Full	10.1.2.3/ 255.255.255.0	DHCP server	N/A

The 'Security Services' section shows 'Content Filter Expiration Date' as 'License Inactive' and 'Web Site Blocked' as 'Not Supported'. The 'Latest Alerts' section is empty. The 'System Status' section includes buttons for 'Port Statistics', 'DHCP Table', 'VPN', and 'Bandwidth'.

3 桥接模式

当您 **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。


The screenshot shows the 'MAINTENANCE' page with the 'Device Mode' tab selected. Under 'Current Device Mode', 'Router' is currently selected. In the 'Device Mode Setup' section, 'Bridge' is selected. The 'IP Address' field is set to '192 . 168 . 1 . 1', 'IP Subnet Mask' is '255 . 255 . 255 . 0', and 'Gateway IP Address' is '0 . 0 . 0 . 0'. A red circle highlights these three fields. There are 'Apply' and 'Reset' buttons at the bottom.

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）。

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation

WAN IP Address Assignment

IP Address Assignment

My WAN IP Address

My WAN IP Subnet Mask

Gateway IP Address

First DNS Server

Second DNS Server

- 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）。

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation:

Service Name: (Optional)

User Name:

Password:

Retype to Confirm:

Nailed-Up

Idle Timeout: (Seconds)

WAN IP Address Assignment

IP Address Assignment:

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation:

User Name:

Password:

Retype to Confirm:

Nailed-Up

Idle Timeout: (Seconds)

PPTP Configuration

My IP Address:

My IP Subnet Mask:

Server IP Address:

Connection ID/Name:

WAN IP Address Assignment

IP Address Assignment:

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，启用具有内容过滤功能的免费试用软件。若单击 **Skip**（跳过）再单击 **Close**（关闭），则结束网络连接建立。

INTERNET ACCESS

Product registration and service activation for free

You can register ZyWALL on <http://www.zyxel.com> and activate "Free Trial" of Content Filtering service on your ZyWALL.

Click "Next" to activate these services for FREE.

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）。

INTERNET ACCESS

Device Registration

New myZyXEL.com account Existing myZyXEL.com account

User Name:

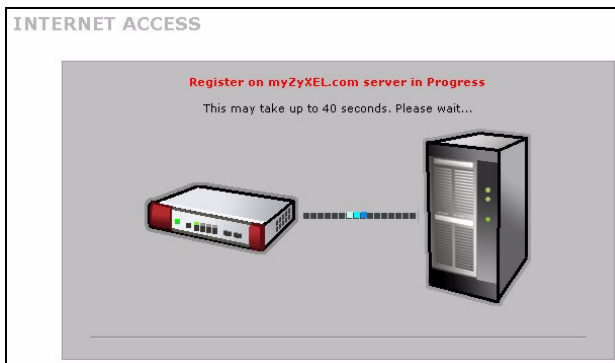
Password: (Type username and password from 6 to 20 characters.)

Confirm Password:

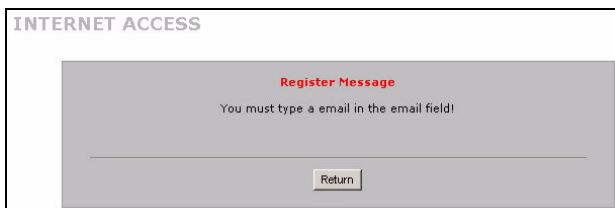
E-Mail Address:

Country:

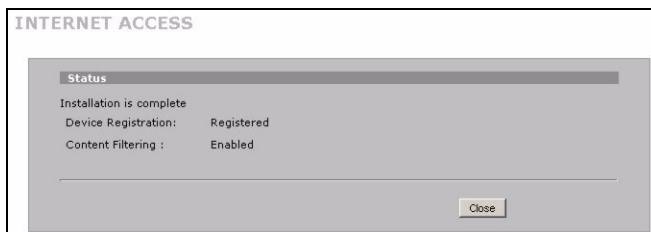
4 等待注册完成。




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。

? 如果您无法通过 WAN 1 访问互联网，请检查 ZyWALL 至以太网端口（具有网络连接功能）的连接。确保互联网网关设备（例如 DSL 调制解调器）运行正常。按一下导航面板上的 **WAN** 以确认您的配置。

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）**。

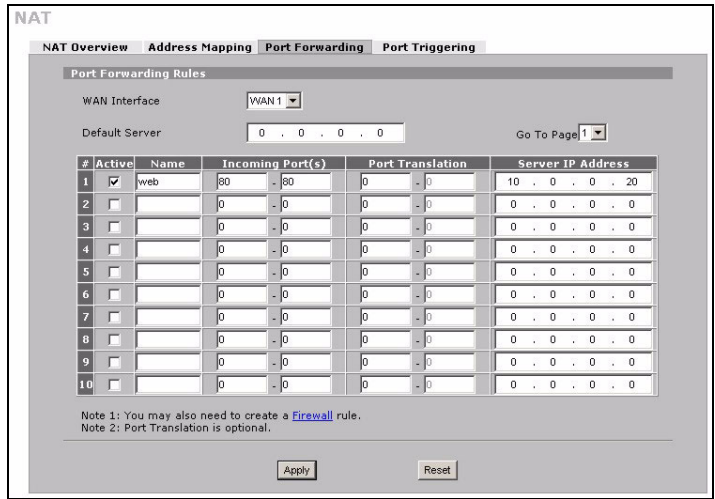
- 4 默认情况下，LAN/DMZ 端口 1 到 4 都是 LAN 端口。要将端口配置为 DMZ 端口，请单击 **Port Roles（端口角色）** 选项卡，选择 DMZ 旁边的单选按钮，然后单击 **Apply（应用）**。

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。

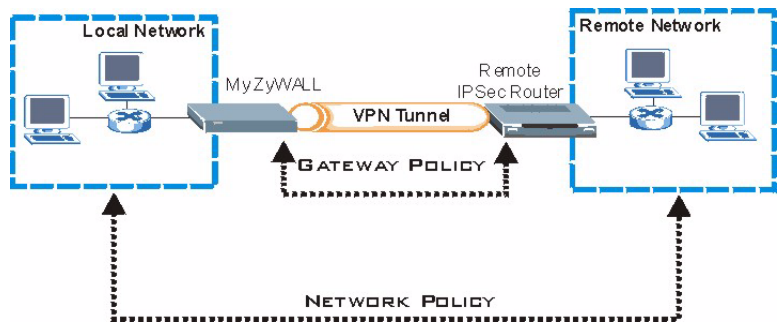
如果您以路由器模式使用 ZyWALL，请继续下一节的步骤。如果您使用桥接模式，则只需初始配置即可。

8 VPN 规则设置

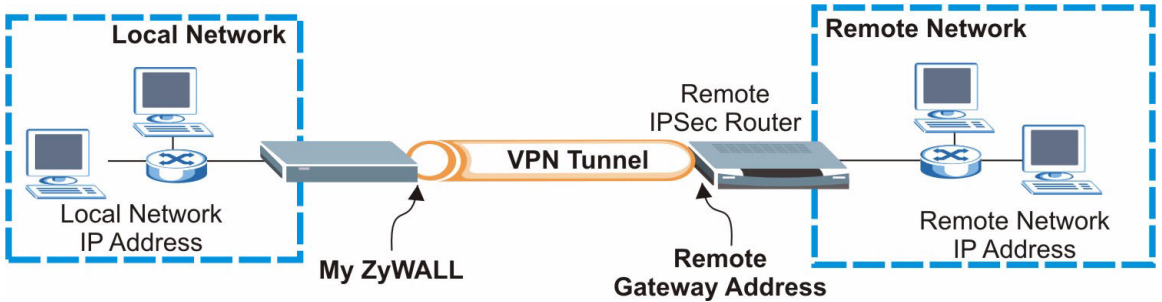
VPN (虚拟专用网络) 通道可以让您安全的连接到其他电脑或网络。

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。

WIZARD - VPN

Gateway Policy Property

Name

Gateway Policy Setting

My ZyWALL

Remote Gateway Address

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。

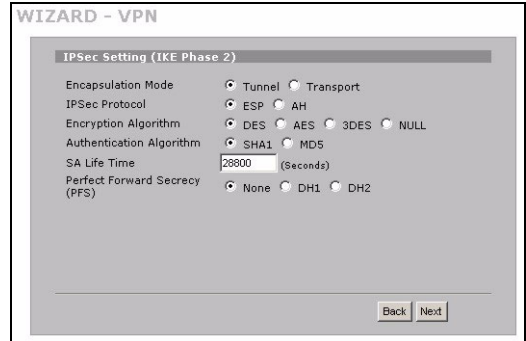
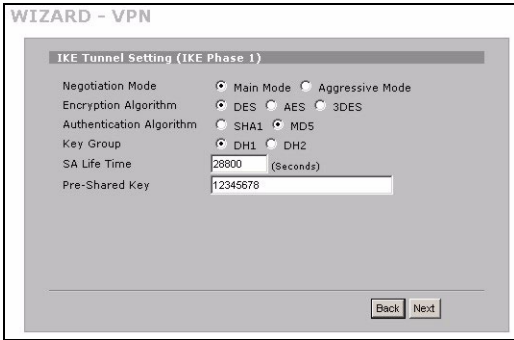
Pre-Shared Key（预共享密钥）：使用 8 到 31 个区分大小写的 ASCII 字符或 16 到 62 个十六进位（“0-9”，“A-F”）字符。在十六进位密钥之前加上“0x”，而“0x”不包括在密钥的 16 到 62 个字符范围内。

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

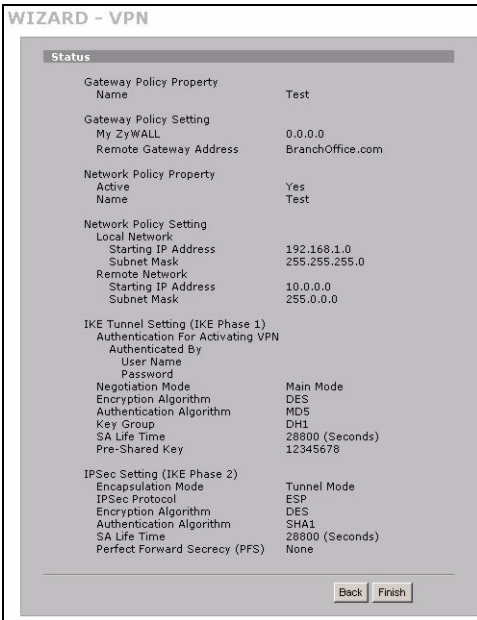
IPsec Protocol（IPsec 通信协议）：**ESP** 可与 NAT 同时应用，而 **AH** 则不可。

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。



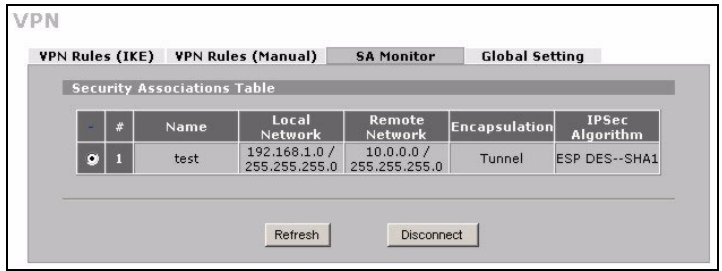
- 7 单击最后页面中的 **Close** (关闭), 完成 VPN 向导的设置。继续下一节的步骤, 启用 VPN 规则并建立 VPN 连接。



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）。



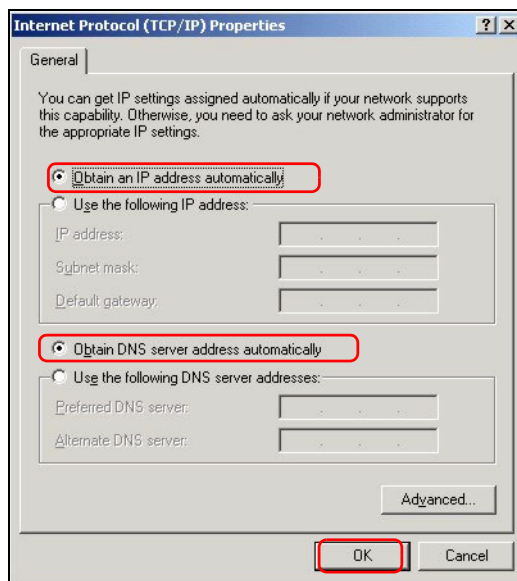
如果无法建立 VPN 连接，请确保 ZyWALL 与远程 IPSec 路由器使用的 VPN 配置相同。按一下导航面板上的 **VPN** 以配置高级设置。请访问任一网站，以确认您是否已成功连接到互联网。

设置电脑的 IP 地址

本节将说明如何在 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 Windows 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

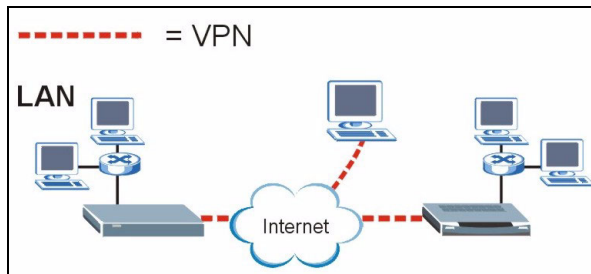
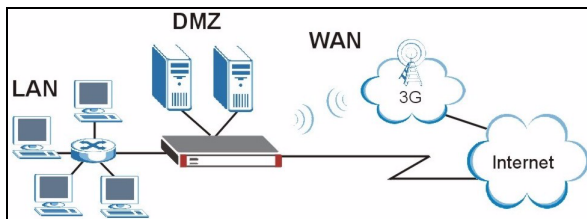
- 1 访问 <http://www.zyxel.cn/> 网站。
- 2 在合勤科技（ZyXEL）首页上的下拉列表框中选中所需的产品，跳至该产品的页面。
- 3 在页面中选中要查看的认证信息。

概觀

ZyWALL 2WG 是防火牆，具備了虛擬私有網路 (VPN)、頻寬管理、內容過濾和多種其他功能。您可以將 ZyWALL 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 為路由器模式時，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 變為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。



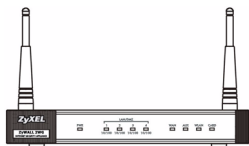
本手冊的章節如下。

- | | |
|------------------|------------|
| 1 硬體連線 | 6 NAT |
| 2 存取網路組態設定程式 | 7 防火牆 |
| 3 橋接模式 | 8 VPN 規則設定 |
| 4 網際網路存取設定以及產品註冊 | 9 疑難排解 |
| 5 DMZ | |

1 硬體連線

您需要以下裝備。

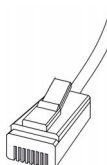
ZyWALL



電腦



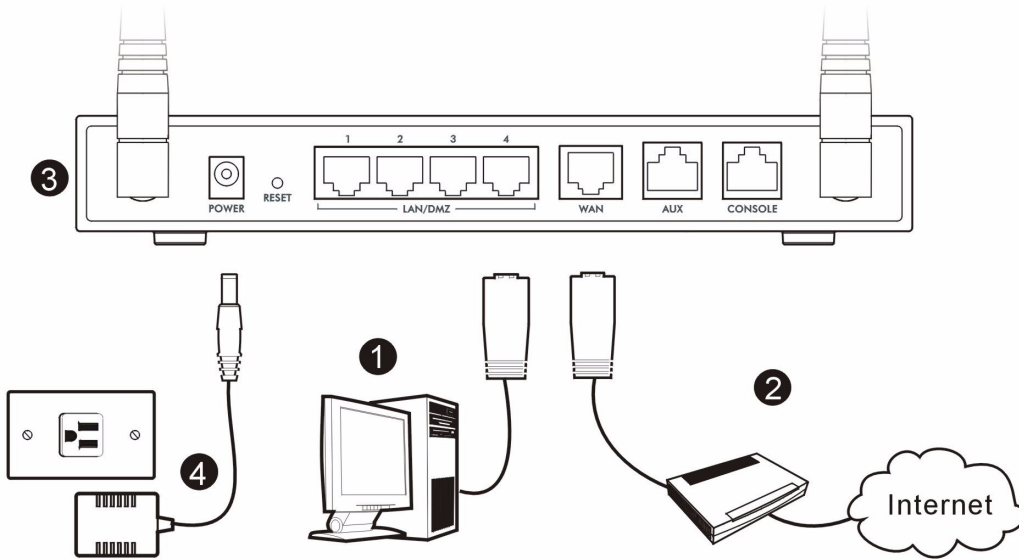
乙太網路線



電源供應器




請進行下列步驟，為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為 **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。

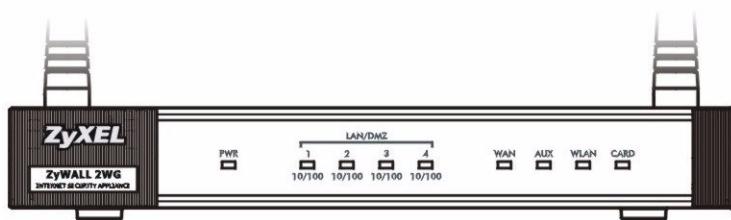
2 使用另一條乙太網路線，將 **WAN** 連接埠連接到可以存取網際網路的乙太網路插孔。

 若要將 **CONSOLE** 埠連接至您的電腦，請使用藍色終端機線。若要將 **AUX** 埠連接至類比數據機，請使用黑色撥接備援線。

3 將 3G 無線網卡插入側邊面板上的卡片插槽，透過 3G 網路接取網際網路。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，為電源插槽（位於後方面板）接上電源。

- 5 觀察前方面板。**PWR** 指示燈會亮起。**CARD**、**LAN/DMZ** 和 **WAN** 指示燈會在相關連接正確時亮起並持續亮著。

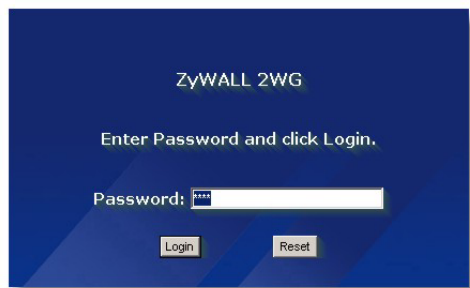
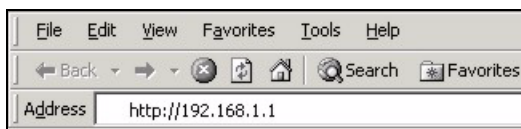


- ? 如果 LED 指示燈全部不亮，請查看連線，檢查電纜是否受損。確認您已經將電源轉接器連接至 ZyWALL 並且插入適當的電源插座。確認電源已經開啓。如果 LED 指示燈還是沒有亮，請聯絡當地的供應商。

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 啟動網頁瀏覽器。輸入位址 **192.168.1.1** (ZyWALL 的預設 IP 位址)。
- 2 按一下 **Login** (登入) (已經輸入預設的密碼 1234)。



- ? 若未顯示登入畫面，請檢查瀏覽器的安全設定，確認乙太網路卡已經插入電腦且運作正常。此外，電腦也應設定為自 DHCP 伺服器取得 IP 位址。請參閱「設定電腦的 IP 位址」一節，取得詳細資訊。

- 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。



? 如果您變更了密碼卻不幸忘記，則需將 ZyWALL 恢復至預設設定（密碼是 1234，區域網路 IP 位址為 192.168.1.1 等）。按住 **RESET**（重設）按鈕（位在後面板）直到 **PWR LED** 指示燈開始閃爍才放開。

- 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 做為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** 狀態為 **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。

The screenshot shows the ZyXEL web management interface. The left sidebar contains navigation options: HOME, REGISTRATION, NETWORK, SECURITY, ADVANCED, NAT, STATIC ROUTE, POLICY ROUTE, BW MGMT, DNS, REMOTE MGMT, UPnP, ALG, LOGS, MAINTENANCE, and LOGOUT. The main content area is divided into several sections:

- System Information:** Model (ZyWALL 2WG), Bootbase Version (V1.08), Firmware Version (V4.02), Up Time (02:56:16), System Time (2001-01-01 02:56:41 GMT), Device Mode (Router), and Firewall (Enabled).
- System Resources:** Flash (4/8 MB), Memory (23/32 MB), Sessions (14/3000), and CPU (0%).
- Interfaces Table:** A table with columns for Interface, Status, IP/Netmask, IP Assignment, and Renew. The 'WAN 1' row is highlighted with a red circle.

Interfaces	Status	IP/Netmask	IP Assignment	Renew
WAN 1	100M/Full	172.23.37.106/ 255.255.255.0	DHCP client	Renew
WAN 2	Down	0.0.0.0/ 0.0.0.0	IPCP client	Dial
Dial Backup	Down	0.0.0.0/ 0.0.0.0	N/A	Dial
LAN	100M/Full	192.168.1.1/ 255.255.255.0	DHCP server	N/A
WLAN	100M/Full	0.0.0.0/ 0.0.0.0	Static	N/A
DMZ	100M/Full	10.1.2.3/ 255.255.255.0	DHCP server	N/A
- Security Services:** Content Filter Expiration Date (License Inactive) and Web Site Blocked (Not Supported).
- Latest Alerts:** A table with Date/Time and Message columns.
- System Status:** Buttons for Port Statistics, DHCP Table, VPN, and Bandwidth.

3 橋接模式

當您將 ZyWALL 設為橋接模式時，其功能即為透通模式防火牆。請進行下列步驟，將 ZyWALL 設為橋接模式。

- 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)，並為 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 會重新啟動。

如果需要從 WAN 存取伺服器，請跳至 [章節 5](#)。


The screenshot shows the Maintenance page with the Device Mode tab selected. The 'Current Device Mode' is Router. The 'Device Mode Setup' section shows the Bridge mode selected. The IP Address field is highlighted with a red circle and contains the value 192.168.1.1. The IP Subnet Mask field contains 255.255.255.0 and the Gateway IP Address field contains 0.0.0.0.

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** (網際網路存取設定) 連結，開啟網際網路存取精靈。

確實輸入您的網際網路存取資訊。

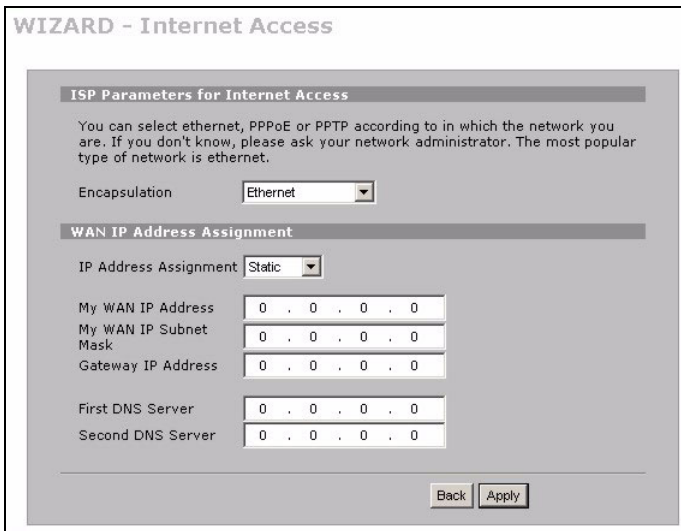
如果 ISP 有提供您 IP 位址，請在 **IP Address Assignment** (IP 位址設定) 下拉式清單方塊中選取 **Static** (靜態)，然後輸入提供的資訊。

 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)。



WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation: Ethernet

WAN IP Address Assignment

IP Address Assignment: Static

My WAN IP Address: 0 . 0 . 0 . 0

My WAN IP Subnet Mask: 0 . 0 . 0 . 0

Gateway IP Address: 0 . 0 . 0 . 0

First DNS Server: 0 . 0 . 0 . 0

Second DNS Server: 0 . 0 . 0 . 0

Back Apply

- **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為昂貴)。

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（單位為秒）。

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation:

Service Name: (Optional)

User Name:

Password:

Retype to Confirm:

Nailed-Up

Idle Timeout: (Seconds)

WAN IP Address Assignment

IP Address Assignment:

WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation:

User Name:

Password:

Retype to Confirm:

Nailed-Up

Idle Timeout: (Seconds)

PPTP Configuration

My IP Address:

My IP Subnet Mask:

Server IP Address:

Connection ID/Name:

WAN IP Address Assignment

IP Address Assignment:

- 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。

INTERNET ACCESS

Product registration and service activation for free

You can register ZyWALL on <http://www.zyxel.com> and activate "Free Trial" of Content Filtering service on your ZyWALL.

Click "Next" to activate these services for FREE.

- 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）。

INTERNET ACCESS

Device Registration

New myZyXEL.com account Existing myZyXEL.com account

User Name: (Type username and password from 6 to 20 characters.)

Password:

Confirm Password:

E-Mail Address:

Country:

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。

? 如果您無法透過 **WAN 1** 存取網際網路，請檢查 **ZyWALL** 至乙太網路插孔 (具有網路連線功能) 的連線。確認網路閘道裝置 (例如 **DSL** 數據機) 運作正常。按一下導覽面板上的 **WAN** 以確認您的設定。

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，也可以為電腦設定靜態 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 位址做為預設開道。

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 為 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。如果您沒有為 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)**。

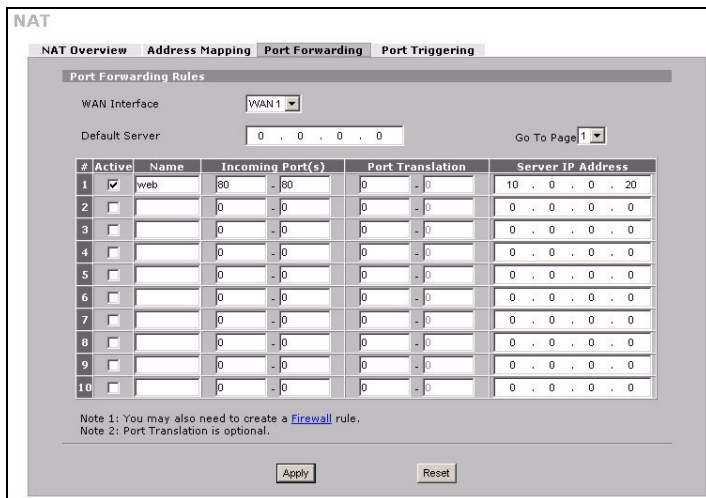
- 4 依照預設，LAN/DMZ 連接埠 1 到 4 都是 LAN 連接埠。如果要將連接埠設為 DMZ 連接埠，請按一下 **Port Roles (連接埠角色)** 標籤，選取 DMZ 旁邊的圓形按鈕，然後按一下 **Apply (套用)**。

6 NAT

NAT(網路位址轉譯 - NAT, RFC 1631) 代表從某個網路 IP 位址轉譯為另一個網路的不同 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 位址轉譯為多個私人 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 位址為 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。

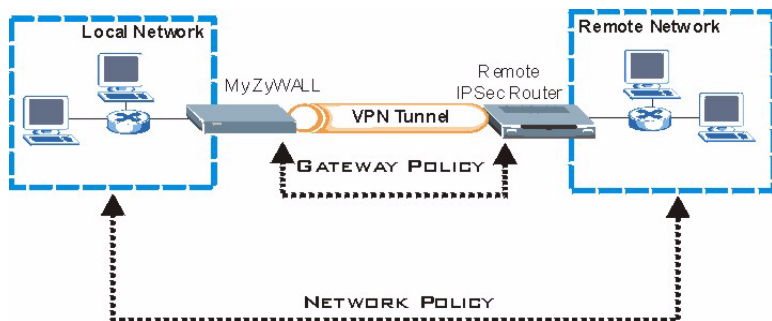
如果您以路由器模式使用 ZyWALL，請繼續下一節的步驟。若為橋接器模式，您已完成初始設定。

8 VPN 規則設定

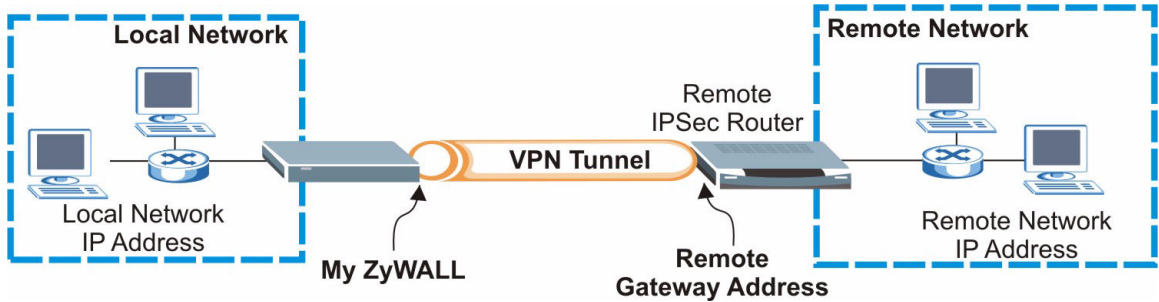
VPN（虛擬私有網路）通道可以讓您安全的連線到另一部電腦或網路。

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。

WIZARD - VPN

Gateway Policy Property

Name

Gateway Policy Setting

My ZyWALL

Remote Gateway Address

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) : 為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** 較為安全。

- 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。

WIZARD - VPN

IKE Tunnel Setting (IKE Phase 1)

Negotiation Mode: Main Mode Aggressive Mode

Encryption Algorithm: DES AES 3DES

Authentication Algorithm: SHA1 MD5

Key Group: DH1 DH2

SA Life Time: 28800 (Seconds)

Pre-Shared Key: 12345678

Back Next

- 5 您可以在這個畫面中設定 IPsec 設定。

WIZARD - VPN

IPsec Setting (IKE Phase 2)

Encapsulation Mode: Tunnel Transport

IPsec Protocol: ESP AH

Encryption Algorithm: DES AES 3DES NULL

Authentication Algorithm: SHA1 MD5

SA Life Time: 28800 (Seconds)

Perfect Forward Secrecy (PFS): None DH1 DH2

Back Next

- 6 檢查 VPN 設定。按一下 **Finish** (完成) 儲存設定。

WIZARD - VPN

Status

Gateway Policy Property Name: Test

Gateway Policy Setting
My ZyWALL: 0.0.0.0
Remote Gateway Address: BranchOffice.com

Network Policy Property
Active: Yes
Name: Test

Network Policy Setting
Local Network
Starting IP Address: 192.168.1.0
Subnet Mask: 255.255.255.0
Remote Network
Starting IP Address: 10.0.0.0
Subnet Mask: 255.0.0.0

IKE Tunnel Setting (IKE Phase 1)
Authentication For Activating VPN
Authenticated By: User Name, Password
Negotiation Mode: Main Mode
Encryption Algorithm: DES
Authentication Algorithm: MD5
Key Group: DH1
SA Life Time: 28800 (Seconds)
Pre-Shared Key: 12345678

IPsec Setting (IKE Phase 2)
Encapsulation Mode: Tunnel Mode
IPsec Protocol: ESP
Encryption Algorithm: DES
Authentication Algorithm: SHA1
SA Life Time: 28800 (Seconds)
Perfect Forward Secrecy (PFS): None

Back Finish

- 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, 啟用 VPN 規則並建立 VPN 連線。

WIZARD - VPN

Congratulations. The VPN wizard configuration is complete.
Check our exciting range of ZyXEL products at <http://www.zyxel.com>

Having VPN access problems?

1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.

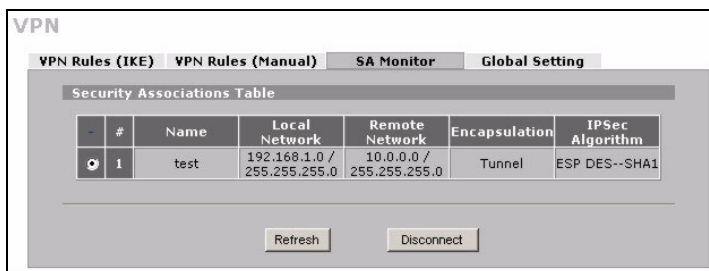
Close

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 and 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 (在這個範例中為 10.0.0.23) 輸入為瀏覽器的 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)。



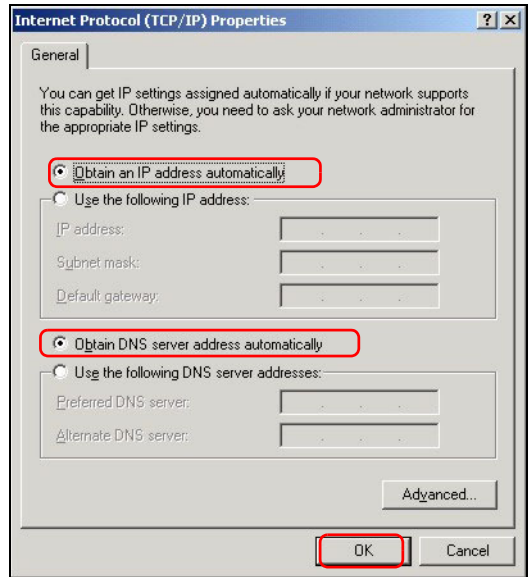
如果無法建立 VPN 連線，請確認 ZyWALL 與遠端 IPSec 路由器使用的 VPN 設定相同。按一下導覽面板上的 **VPN** 以設定進階設定。請存取任一網站，以確定您是否已經成功連線至網際網路。

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 中為確定），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。