

ZyWALL 70

Internet Security Gateway

Quick Start Guide

Version 3.64
3/2005

Table of Contents

ENGLISH	1
DEUTSCH	23
ESPAÑOL	47
FRANÇAIS	71
ITALIANO	95
中文	119

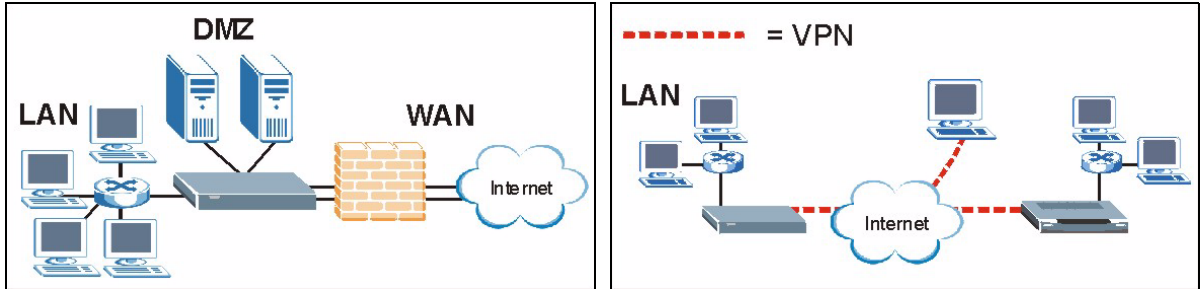


Overview

The ZyWALL 70 is a load-balancing, dual WAN 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. The ZyWALL increases network security by providing DMZ ports 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 | 7 Firewall |
| 2 Accessing the Web Configurator | 8 VPN Rule Setup |
| 3 Bridge Mode | 9 myZyXEL.com Product Registration |
| 4 Internet Access Setup | 10 External Database Content Filtering |
| 5 DNS | 11 Troubleshooting |
| 6 NAT | |

1 Hardware Connections

You need the following.

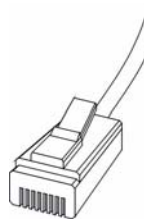
ZyWALL



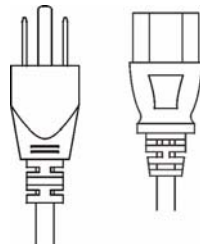
Computer



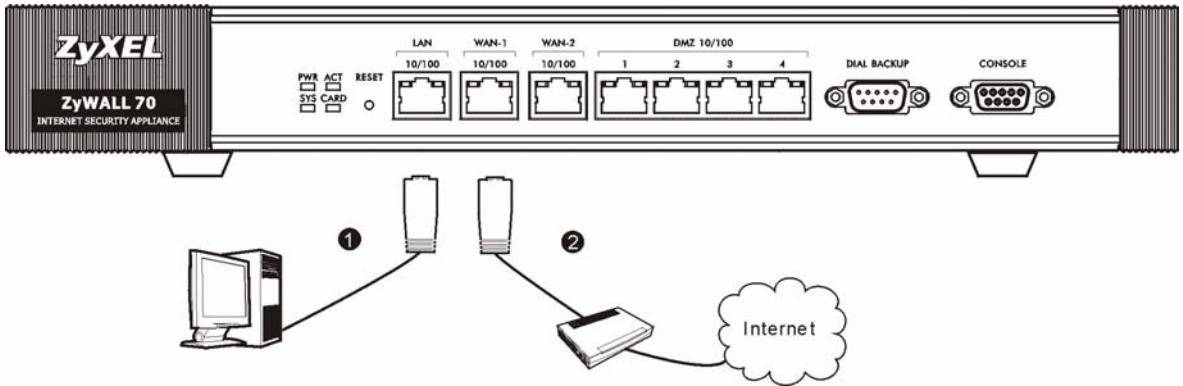
Ethernet Cables



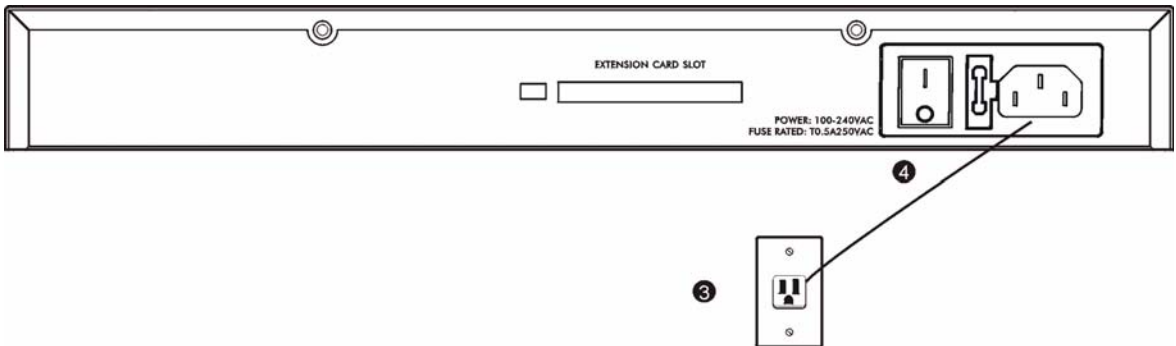
Power Cord



Do the following to make hardware connections for initial setup.



- 1 Use an Ethernet cable to connect the **LAN** port to a computer. You can also use Ethernet cables to connect public servers (web, e-mail, FTP, etc.) to the **DMZ** ports.
- 2 Use another Ethernet cable(s) to connect the **WAN 1** and/or **WAN 2** port to an Ethernet jack with Internet access.

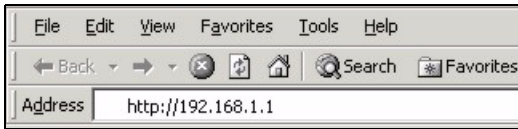


- 3 Use the included power cord to connect the power socket (on the rear panel) to a power outlet
- 4 Push the power switch to the on position and look at the front panel. The **PWR LED** turns on. The **SYS LED** blinks while performing system testing and then stays on if the testing is successful. The **ACT**, **CARD**, **LAN**, **DMZ**, and **WAN** LEDs turn on and stay on if the corresponding connections are properly made.

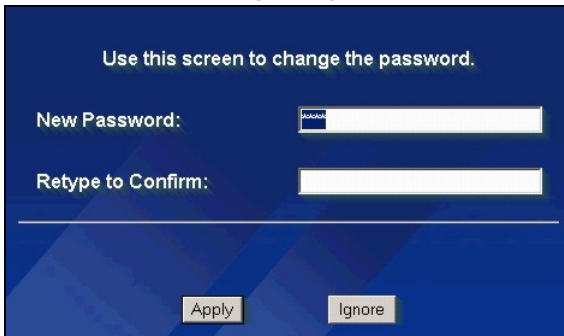
2 Accessing the Web Configurator

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

- 1 Launch your web browser. Enter **192.168.1.1** (the ZyWALL's default IP address) as the address. If the login screen does not display, see [Section 11.1](#) to set your computer's IP address.
- 2 Click **Login** (the default password 1234 is already entered).



- 3 Change the login password by entering a new password and clicking **Apply**.
- 4 Click **Apply** to replace the ZyWALL's default digital certificate.



- 5 The **HOME** screen opens.

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

Go to [Section 3](#) if you prefer to use the ZyWALL as a transparent firewall.

6 Check the **Network Status** table. If the **WAN 1** status is *not Down* and there is an IP address, go to [Section 5](#).

If the **WAN 1** status is **Down** (or there is not an IP address), click **Internet Access** 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 ports.

The screenshot shows the ZyXEL web management interface. The left sidebar contains navigation menus: HOME, NETWORK (LAN, WIRELESS LAN, WAN, DMZ), SECURITY (FIREWALL, CONTENT FILTER, VPN, CERTIFICATES, AUTH SERVER), ADVANCED (NAT, STATIC ROUTE, POLICY ROUTE, BW MGMT, DNS, REMOTE MGMT, UPnP), LOGS, MAINTENANCE, and LOGOUT. The main content area is titled 'HOME' and features 'Wizards for WAN 1 Quick Setup' with buttons for 'Internet Access' and 'VPN'. Below this is 'Device Information' showing system details like name, firmware version, routing protocol, device mode, firewall status, system time, memory usage, sessions, policy, and routes. At the bottom is a 'Network Status' table.

Interface	Status	IP Address	Subnet Mask	DHCP	Renew
WAN 1	Down	0.0.0.0	0.0.0.0	Client	Renew
WAN 2	Down	0.0.0.0	0.0.0.0	Client	Renew

Status: **Ready**

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.

MAINTENANCE

General
Password
Time and Date
Device Mode
F/W Upload
Configuration
Restart

Current Device Mode

Device Mode Router

Device Mode Setup

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

Router
IP Address (See [LAN](#), [WAN](#) and [DMZ](#))

Bridge

IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Gateway IP Address	192 . 168 . 1 . 3

Apply
Reset

4 Internet Access Setup

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.

Note: 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 **Finish** when you are done.

- **Ethernet Encapsulation**

Configure a Roadrunner service in the **NETWORK WAN** screens (use the **WAN 1** tab).

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**.

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

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

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.

Unlike the LAN, the ZyWALL does not assign TCP/IP configuration via DHCP to computers connected to the DMZ ports. 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 **DMZ** in the navigation panel.

- 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.

- Click **Apply**.

The screenshot shows the DMZ configuration interface. The 'DMZ' tab is selected, and the 'IP Alias' sub-tab is active. The 'DMZ TCP/IP' section contains the following fields:

- IP Address:** 10 . 0 . 0 . 1
- IP Subnet Mask:** 255 . 0 . 0 . 0
- RIP Direction:** Both
- RIP Version:** RIP-1
- Multicast:** None

The 'Windows Networking (NetBIOS over TCP/IP)' section contains two checkboxes:

- Allow between DMZ and LAN** (You also need to create a firewall rule!)
- Allow between DMZ and WAN**

At the bottom of the interface are two buttons: **Apply** and **Reset**.

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 WAN to an HTTP (web) server on the DMZ. The server has a private IP address of 10.0.0.20.

- 1 Click **NAT** in the navigation panel and then **Port Forwarding**.
- 2 Select the **Active** check box.
- 3 Type a name for the rule.
- 4 Type the port number that the service uses.
- 5 Type the HTTP server's IP address.
- 6 Click **Apply**.

NAT

NAT Overview
Address Mapping
Port Forwarding
Port Triggering

Port Forwarding Rules

WAN Interface WAN 1

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
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 Firewall

You can use the ZyWALL without configuring the firewall.

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

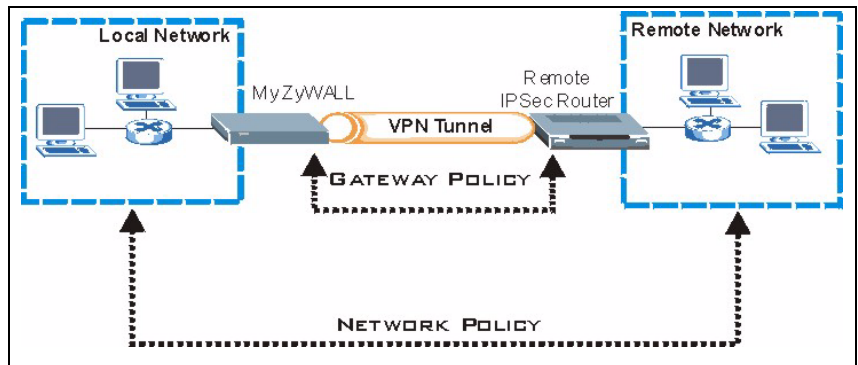
If you are using the ZyWALL in router mode, continue with the next section. For bridge mode, skip to [Section 9](#).

8 VPN Rule Setup

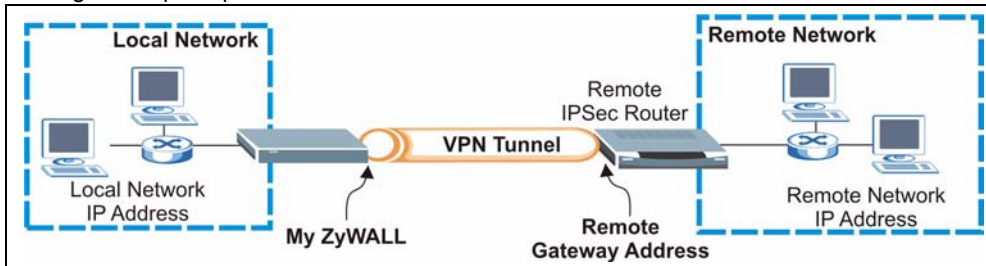
A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network.

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

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



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



1 Click **VPN** in the **HOME** screen (you may need to scroll up to see the link) to open the VPN wizard.

Note: 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.

Gateway Policy Property

Name: Test

Gateway Policy Setting

My ZyWALL: 0.0.0.0

Remote Gateway Address: BranchOffice.com

Next

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.

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

Note: 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.

Note: 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.

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.

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.

Status

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

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)
 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 Secret (PFS) NONE

Back Finish

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.

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 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 **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).

VPN

VPN Rules (IKE) VPN Rules (Manual) SA Monitor Global Setting

Security Associations Table

#	Name	Local Network	Remote Network	Encapsulation	IPSec Algorithm
1	test	192.168.1.0 / 255.255.255.0	10.0.0.0 / 255.0.0.0	Tunnel	ESP DES-SHA1

Refresh Disconnect

9 myZyXEL.com Product Registration

myZyXEL.com is ZyXEL's online services center where you can register your ZyXEL device.

- 1 Go to myZyXEL.com using your web browser.
- 2 Create a new account (if you don't have one already).

Note: You are automatically logged out of your myZyXEL.com account after five minutes of inactivity. Simply log back into your myZyXEL.com account if this happens to you.

Login /

Welcome to myZyXEL.com

What's myZyXEL.com?

myZyXEL.com provides an easy-to-use service management platform where you can manage all your ZyXEL product registrations and services using your personal account.

Please register your account at myZyXEL.com first.

Username:

Password:

Remember Username:

> Forgot Password? [Click here](#)

> If you are not a registered user, [Click here](#)

- 3 After you create an account, you will receive a confirmation e-mail. Click the URL in the e-mail to activate your account.

From: myzyxel-admin@zyxel.com.tw	Sent: Thu 7/15/2004 11:58
To: XXXX@zyxel.com.tw	
Cc:	
Subject: myZyXEL.com Subscription Notice	

Dear Customer,

You have registered a new account at myZyXEL.com.
Here is your login information.

Username : zytest
Password : 123456

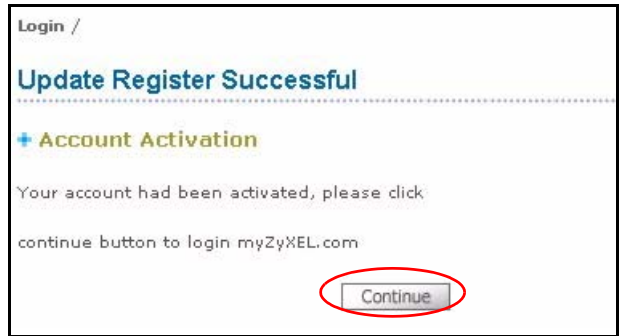
To activate your account, please click the following URL.

URL :
https://www.myzyxel.com/myzyxel/register?hidFunction=LOGIN_REG&hidAction=REG_CONFIRM&ACCOUNT_ID=2099&SUB_CODE=5830326

NOTE: If no action is taken within 3 days, your account will not be valid.
You may register again anytime at myZyXEL.com
(<https://www.myZyXEL.com>).

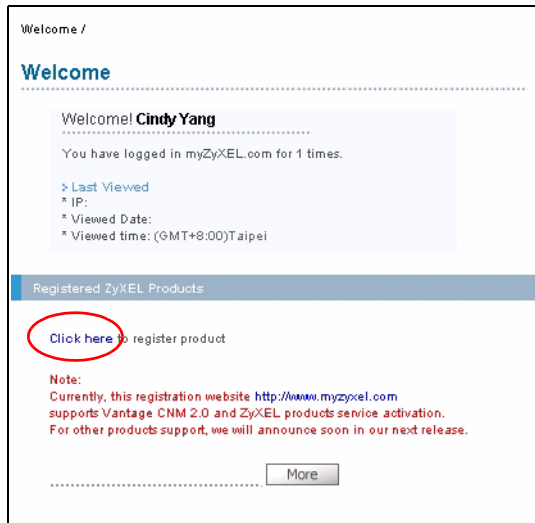
Best Regards,
myzyxel-admin@zyxel.com.tw
ZyXEL Communications Corporation

4 Click **Continue** to go to the myZyXEL.com login screen.



5 Log in.

6 Click the link and register your ZyXEL device.



7 Click **Add**.



- 8 Enter the product serial number in the **Serial Number** field.
- 9 Your device category and model number automatically display in the **Category** and **Model** fields respectively. Otherwise, select the correct ones from the drop-down list boxes.
- 10 Enter the device's MAC address in the **Authentication Code** field (it may already be displayed).
- 11 Enter a descriptive name in the **Friendly Name** field for identification purposes.
- 12 Click **Register**.

Add New Product

To add a new product, please fill in the following fields.
Friendly Name is an alias you give the product to identify it in the product list.

marked by (*) are Required

* Serial Number: Please enter the 10-digit number of the label on the unit. (Upper Case)

* Category:

* Model: Please select your correct category and model. You can find it by your case.

* Authentication Code: > For hardware products, this is the physical MAC address. > For software products, this is a generated number that is displayed after you ins (Upper Case)

* Friendly Name: Please give a name easy to remember for you. Up to 30 characters. It may contain underscore character, other character are not allowed.

- 13 Specify the purchase information and click **Continue**.
- 14 Click **Continue** again to complete the process.

My Products / Product Registration

Product Survey

Product Information

+ Purchase date:

+ You purchased this product from:

15After you have registered your ZyXEL device, you can view its registration details in the **Service Management** screen. The ZyXEL device is now registered, but content filtering is not activated. To activate content filtering, you need to access myZyXEL.com via your device. Continue with the next section.

Service Management

Product Information

zy70cf

Serial Number: S4Z2928704
 Products: ZyWALL 70
 Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

> zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

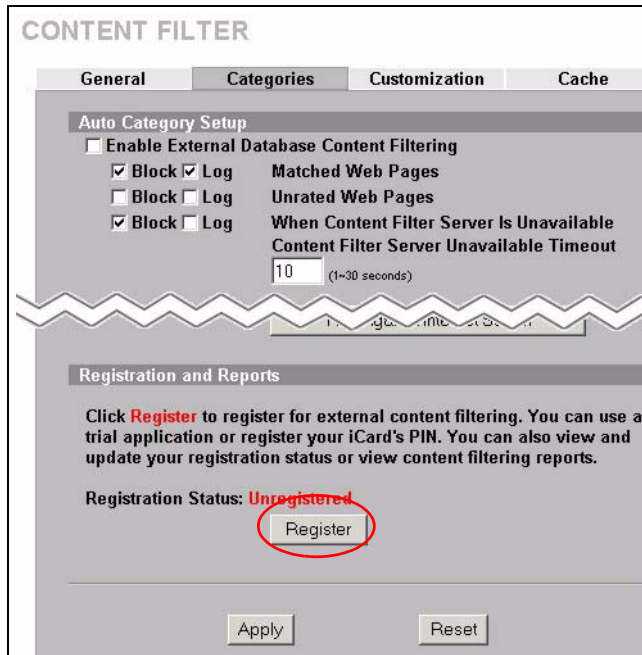
	Service Name	Service Activation	Status	Expiry Date	Remarks
1.	Content Filter	Activate	-	-	

10 External Database Content Filtering

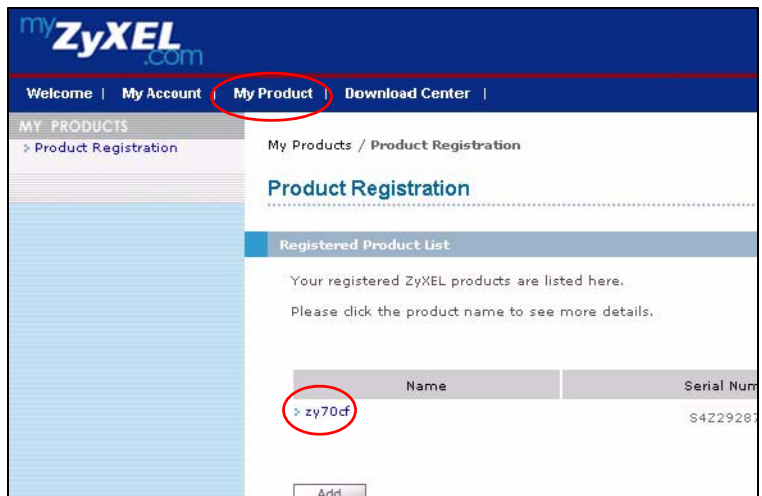
When you register for and enable external database content filtering, your ZyWALL accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL block and/or log access to web sites based on these categories. Register your ZyWALL at myZyXEL.com (see [Section 9](#)) and then do the following to register for external database content filtering.

- 1 In your ZyXEL device's web configurator, click **CONTENT FILTER, Categories** and then the **Register** button.

Note: You must also use the ZyWALL's web configurator **CONTENT FILTER** screens to configure and enable content filtering.



- 2 The myZyXEL.com login screen opens.
- 3 Enter the user name and password from your myZyXEL.com account.
- 4 Click **My Product** in the navigation panel.
- 5 Click the product name link for your device to view its registration details in the **Service Management** screen.



6 Click **Activate** for the content filter service to display the next screen.

My Products / Service Activation

Service Management

Product Information

zy70cf

Serial Number: S422928704
 Products: ZyWALL 70
 Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

	Service Name	Service Activation	Status	Expiry Date	Ren
1	Content Filter	Activate	-	-	

7 If you want to use the trial, click **Submit** under **Content Filtering Trial**. The trial period begins the date you apply.

You cannot apply for a trial if you've already used a trial or registered an iCard's PIN number.

If you purchased an iCard, enter the PIN code exactly as shown on your iCard in the **License Key** (PIN code) field. Select the date when you want your content filtering to start and click **Submit** under **Registration Information**.

My Products / Service Activation

Content Filtering Trial

We offer 30-day free trial for content filtering service.
 If you would like to have a try, please click "submit".

Registration Information

1. Enter the License Key (PIN code) exactly as shown in your iCard.
2. Content filtering begins from the activation date.

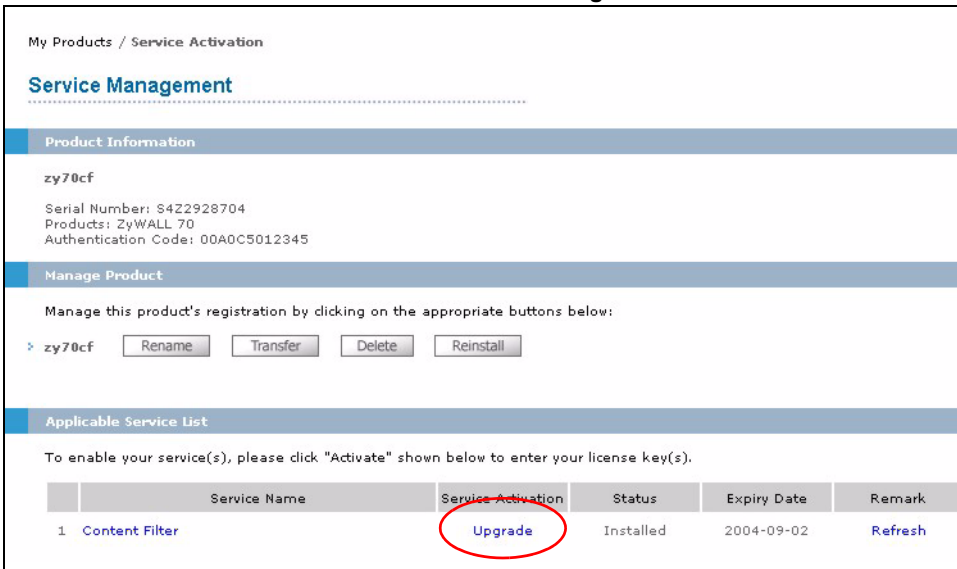
License Key (PIN code) :

Activation Date : - -

8 A screen displays showing you the service is registered. Click **Continue** to proceed to the **Service Management** screen.



9 If you are currently using a trial, you can still register the PIN code from an iCard by clicking **Upgrade** in the **Service Activation** field of the **Service Management** screen.



11 Troubleshooting

Problem	Corrective Action
None of the LEDs turn on.	Make sure that you have the power cord connected to the ZyWALL and plugged in to an appropriate power source. Make sure you have the ZyWALL turned on. Check all cable connections.
	If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.
Cannot access the ZyWALL from the LAN.	Check the cable connection between the ZyWALL and your computer or hub. Refer to Section 1 for details.
	Ping the ZyWALL from a LAN computer. Make sure your computer's Ethernet card is installed and functioning properly.
	In the computer, click Start, (All) Programs, Accessories and then Command Prompt . In the Command Prompt window, type "ping" followed by the ZyWALL's LAN IP address (192.168.1.1 is the default) and then press [ENTER]. The ZyWALL should reply. Otherwise, refer to Section 11.1 .
	If you've forgotten the ZyWALL's password, use the RESET button. Press the button in for about 10 seconds (or until the PWR LED starts to blink), then release it. It returns the ZyWALL to the factory defaults (password is 1234, LAN IP address 192.168.1.1 etc.; see your User's Guide for details).
	If you've forgotten the ZyWALL's LAN or WAN IP address, you can check the IP address in the SMT via the console port. Connect your computer to the CONSOLE port using a console cable. Your computer should have a terminal emulation communications program (such as HyperTerminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no flow control and 9600 bps port speed.
Cannot access the Internet.	Check the ZyWALL's connection to the Ethernet jack with Internet access. Make sure the Internet gateway device (such as a DSL modem) is working properly.
	Click WAN in the navigation panel to verify your settings.
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.

11.1 Set Up Your Computer's IP Address

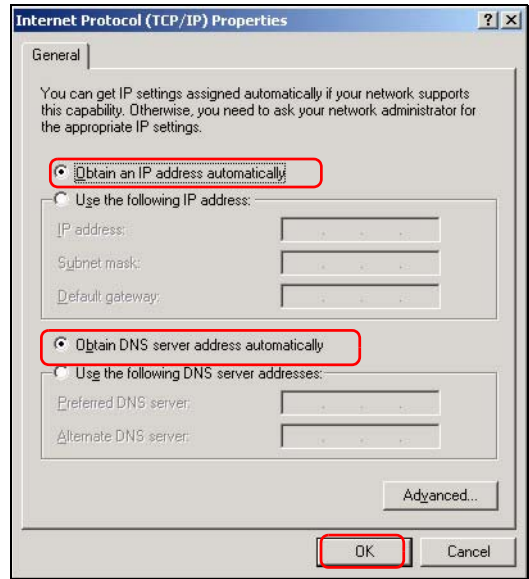
This section shows you how to set up your computer to receive an IP address in Windows 2000, Windows NT and Windows XP. This ensures that your computer can communicate with your ZyWALL.

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.



11.2 Procedure to View a Product's Certification(s)

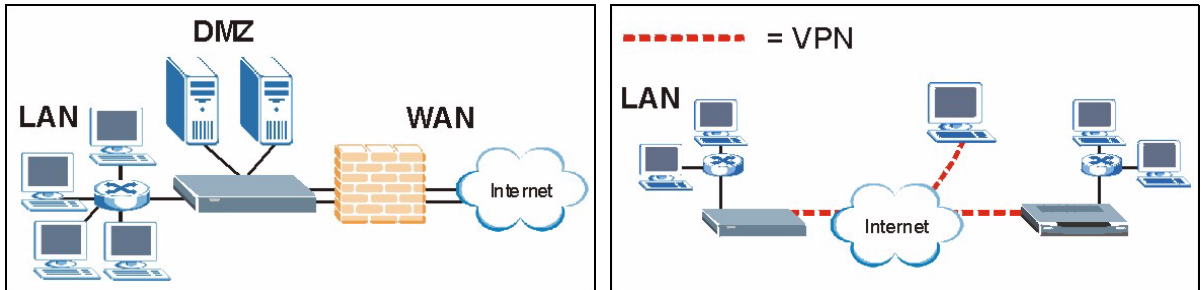
- 1 Go to www.zyxel.com.
- 2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

Übersicht

Die ZyWALL 70 ist eine Load-balancing-, Dual-WAN-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. Die ZyWALL erhöht die Netzwerksicherheit, indem sie DMZ-Ports für die Verwendung öffentlich zugänglicher Server bietet. 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 | 7 Firewall |
| 2 Zugriff auf den Web-Konfigurator | 8 Einstellen der VPN-Regeln |
| 3 Bridge Mode | 9 myZyXEL.com Produktregistrierung |
| 4 Einrichten des Internetzugriffs | 10 Externe Datenbank für den Content Filter |
| 5 DNS | 11 Problembeseitigung |
| 6 NAT | |

1 Anschließen der Hardware

Sie benötigen folgendes:

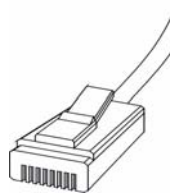
ZyWALL



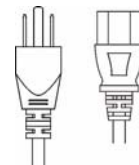
Computer



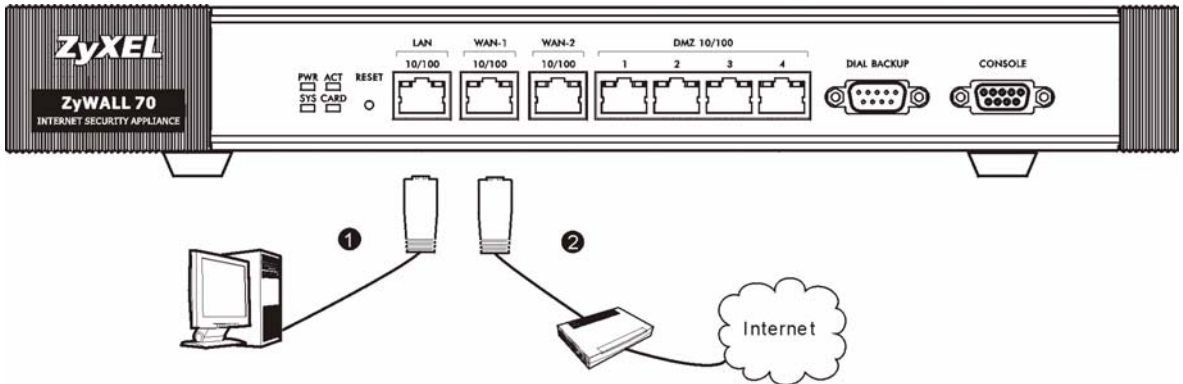
Ethernetkabel



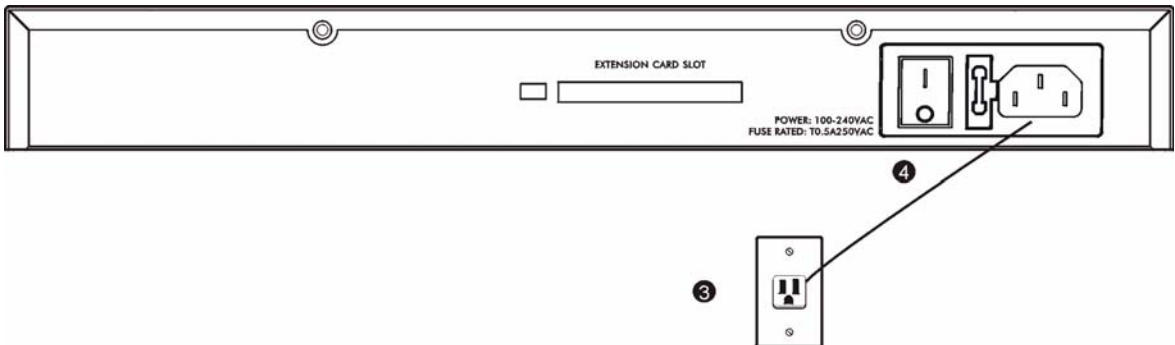
Netzkabel



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



- 1 Verbinden Sie den **LAN**-Port mit einem Ethernet-Kabel mit dem Computer. Mit Ethernet-Kabeln können Sie auch öffentliche Server (Internet, E-Mail, FTP, usw.) an die **DMZ**-Ports anschließen.
- 2 Schließen Sie mit einem anderen Ethernet-Kabel den **WAN 1**- und/oder **WAN 2**-Port an die Ethernet-Buchse mit Internetzugriff an.

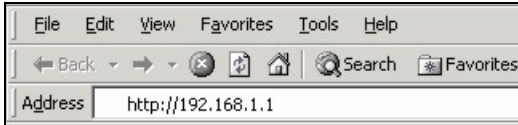


- 3 Schliessen Sie den Netzanschluss des Geräts (an der Rückseite) mit dem mitgelieferten Netzkabel an eine Netzsteckdose an.
- 4 Schalten Sie den Ein/Aus-Schalter in die Position On und sehen Sie sich das vordere Bedienfeld an. Die **PWR-LED** beginnt zu leuchten. Während des Systemtests blinkt die **SYS-LED**. Wurde er Test erfolgreich abgeschlossen, bleibt diese Anzeige an. Die LEDs **ACT**, **CARD**, **LAN**, **DMZ** und **WAN** beginnen zu leuchten und bleiben an, wenn die entsprechenden Verbindungen richtig hergestellt wurden.

2 Zugriff auf den Web-Konfigurator

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

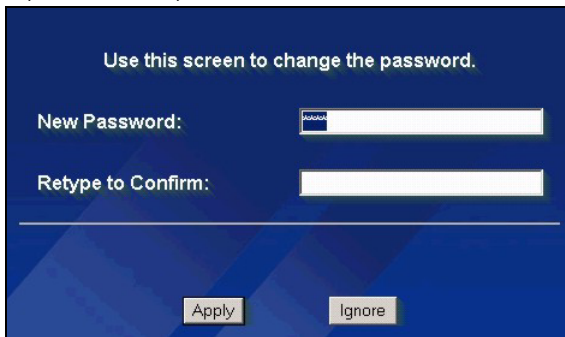
- 1 Starten Sie Ihren Internetbrowser. Geben Sie als Adresse **192.168.1.1** (die IP-Standardadresse des ZyWALL) ein.
Wenn das Loginfenster nicht angezeigt wird, lesen Sie in [Abschnitt 11.1](#) nach, wie Sie die IP-Adresse Ihres Computers einstellen können.



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



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



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



- 5 Das Fenster **HOME** wird angezeigt.

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

Gehen Sie zu [Abschnitt 3](#), wenn Sie die ZyWALL als eine transparente Firewall verwenden möchten.

6 Prüfen Sie die **Netzwerkstatus** tabelle. Wenn der Status von **WAN 1 nicht Down** ist und eine IP-Adresse angegeben ist, gehen Sie zu [Abschnitt 5](#).

Wenn der Status von **WAN 1 Down** ist (oder keine IP-Adresse angegeben ist), klicken Sie auf **Internet Access** (Internetzugriff) und konfigurieren Sie mit [Abschnitt 4 WAN 1](#).

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

ZyXEL HOME HELP ?

HOME

NETWORK
LAN
WIRELESS LAN
WAN
DMZ

SECURITY
FIREWALL
CONTENT FILTER
VPN
CERTIFICATES
AUTH SERVER

ADVANCED
NAT
STATIC ROUTE
POLICY ROUTE
BW MGMT
DNS
REMOTE MGMT
UPnP

LOGS

MAINTENANCE

LOGOUT

HOME

Wizards for WAN 1 Quick Setup

Internet Access VPN

Device Information

System Name:

Firmware Version: V3.64(WM.0)b1 | 12/17/2004

Routing Protocol: IP

Device Mode: Router

Firewall: Enabled

System Time: 2005-01-11 08:27:37 GMT

Memory: 14358K/19173K

Sessions: 5/10000

Policy

Routes: 0/48

Network Status

Interface	Status	IP Address	Subnet Mask	DHCP	Renew
WAN 1	Down	0.0.0.0	0.0.0.0	Client	Renew
WAN 2	Down	0.0.0.0	0.0.0.0	Client	Renew

Status: **Ready**

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** (Brücke) 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.

MAINTENANCE

General
Password
Time and Date
Device Mode
F/W Upload
Configuration
Restart

Current Device Mode

Device Mode	Router
--------------------	--------

Device Mode Setup

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

Router

IP Address (See [LAN](#), [WAN](#) and [DMZ](#))

Bridge

IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Gateway IP Address	192 . 168 . 1 . 3

Apply
Reset

Gehen Sie weiter zu [Abschnitt 5](#), wenn Sie Server haben, auf die Sie vom WAN aus zugreifen müssen.

4 Einrichten des Internetzugriffs

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

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

Hinweis: Je nachdem, was Sie im Feld **Encapsulation** (Verkapselung) 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 **Finish** (fertigstellen).

- **Ethernet Encapsulation**

Konfigurieren Sie einen Roadrunnerdienst in den **NETWORK WAN** (Netzwerk-WAN) Fenstern (auf der Registerkarte **WAN 1**).

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**

Wählen Sie **Nailed-Up**, wenn die Verbindung dauerhaft aufrecht erhalten werden soll (das kann jedoch sehr teuer sein, wenn Ihr Internetdienstanbieter Ihnen die Benutzungsdauer anstelle eines monatlichen Pauschalbetrags in Rechnung stellt).

Wenn die Verbindung nicht dauerhaft stehen soll, müssen Sie bei **Idle Timeout** (Leerlaufausschaltzeit) eine Leerlaufausschaltzeit (in Sekunden) festlegen.

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

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

5 DMZ

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

Anders als beim LAN weist die ZyWALL den an den DMZ-Ports angeschlossenen Computern nicht über DHCP die TCP/IP-Konfiguration zu. 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.

Hinweis: Im Bridge Modus muss die DMZ nicht konfiguriert werden. Gehen Sie weiter zu [Abschnitt 7](#).

- 1 Klicken Sie in der Navigationsleiste auf **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).

The screenshot shows the DMZ configuration window with the following settings:

- DMZ TCP/IP**
 - IP Address: 10 . 0 . 0 . 1
 - IP Subnet Mask: 255 . 0 . 0 . 0
 - RIP Direction: Both
 - RIP Version: RIP-1
 - Multicast: None
- Windows Networking (NetBIOS over TCP/IP)**
 - Allow between DMZ and LAN (You also need to create a firewall rule!)
 - Allow between DMZ and WAN

Buttons: Apply, Reset

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 WAN- 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 **NAT** und dann auf **Port Forwarding** (Portweiterleitung).
- 2 Wählen Sie das Kontrollfeld **Active** (Aktiv).
- 3 Geben Sie eine Bezeichnung für die Regel ein.
- 4 Geben Sie die Portnummer ein, die der Dienst verwendet.
- 5 Geben Sie die IP-Adresse des HTTP-Servers ein.
- 6 Klicken Sie auf **Apply** (Übernehmen).

NAT

NAT Overview
Address Mapping
Port Forwarding
Port Triggering

Port Forwarding Rules

WAN Interface WAN 1

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
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 Firewall

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

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

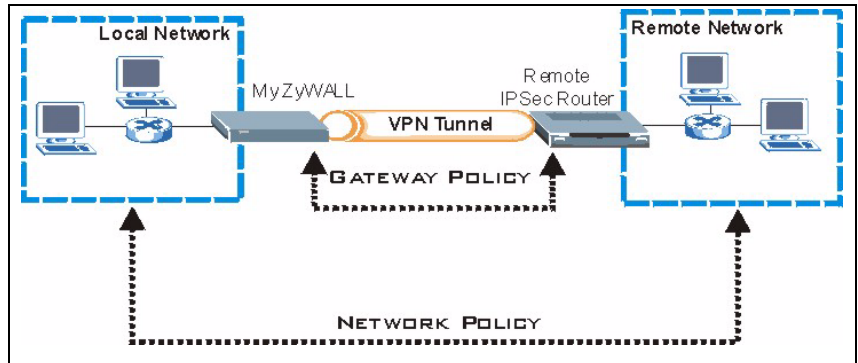
Wenn Sie die ZyWALL im Routermodus verwenden, fahren Sie mit dem nächsten Abschnitt fort. Weiter mit dem Bridge Modus geht es in [Abschnitt 9](#).

8 Einstellen der VPN-Regeln

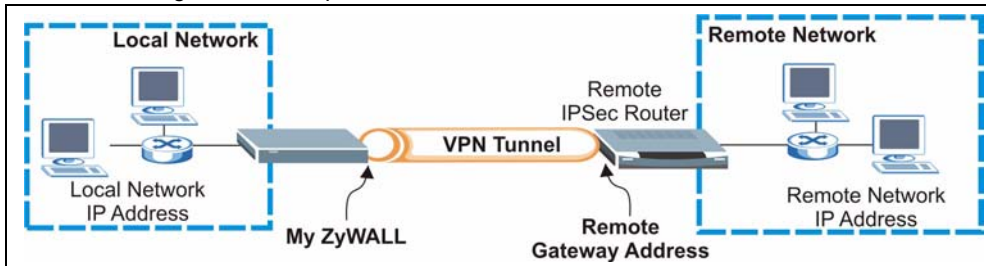
Mit einem VPN-Tunnel (Virtual Private Network) haben Sie eine sichere Verbindung zu anderen Computern oder Netzwerken.

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

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



Diese Abbildung soll die Hauptfelder in den Assistentenfenstern erläutern.



- 1 Klicken Sie im Fenster **HOME** (Anfang) auf **VPN** (möglicherweise müssen Sie die Seite scrollen, um den Link sichtbar zu machen), um den VPN-Assistenten zu öffnen.

Hinweis: 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 (Remote-Gatewayadresse): Geben Sie die IP-Adresse oder den Domainnamen des IPSec-Routers ein.

Gateway Policy Property

Name

Gateway Policy Setting

My ZyWALL

Remote Gateway Address

Next

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

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

Name (Name): Geben Sie einen Namen ein, um die Netzwerk-Policy zu bezeichnen.

Wählen Sie **Single** (Eine) und geben eine IP-Adresse für eine einzelne IP-Adresse 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 die IP-Adressen eines bestimmten Netzwerk anhand ihrer Subnetmaske festzulegen.

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

Back Next

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

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

Hinweis: 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 (und langsamere) 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 (Vorgegebener Schlüssel): 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 (Verkapselungsmodus): **Tunnel** (Tunnel) ist kompatibel mit NAT, **Transport** (Transport) nicht.

IPSec Protocol (IPSec-Protokoll): **ESP** ist kompatibel mit NAT, **AH** nicht.

Perfect Forward Secrecy (PFS): **None** (Keine) ermöglicht ein schnelleres Einrichten des IPSec, **DH1** und **DH2** bieten aber mehr Sicherheit.

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

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 In diesem Fenster werden die IPSec-Einstellungen konfiguriert.

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 Secret (PFS) None DH1 DH2

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

Status	
Gateway Policy Setting	
My ZyWALL	0.0.0.0
Remote Gateway Address	BranchOffice.com
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)	
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 Secret (PFS)	NONE
<input type="button" value="Back"/> <input type="button" value="Finish"/>	

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.

<p>Congratulations. The VPN wizard configuration is complete. Check our exciting range of ZyXEL products at http://www.zyxel.com</p> <p>Having VPN access problems?</p> <ol style="list-style-type: none"> 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. <p style="text-align: center;"><input type="button" value="Close"/></p>
--

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 ihn benutzen möchten.

Klicken Sie in der Navigationsleiste auf **VPN** und dort auf die Registerkarte **SA Monitor**. Dort erscheint eine Liste der angeschlossenen VPN-Tunnel (der VPN-Tunnel "test" ist hier oben).



9 myZyXEL.com Produktregistrierung

myZyXEL.com ist das Online-Servicecenter von ZyXEL, wo Sie Ihr ZyXEL-Produkt registrieren können.

- 1 Gehen Sie mit Ihrem Internetbrowser zu myZyXEL.com.
- 2 Eröffnen Sie ein neues Konto (wenn Sie noch keines besitzen).

Hinweis: Wenn Sie fünf Minuten lang keine Eingaben machen, werden Sie automatisch von Ihrem myZyXEL.com-Konto abgemeldet. Sie können sich dann wieder ganz einfach bei Ihrem myZyXEL.com-Konto anmelden.

myZyXEL.com provides an easy-to-use service management platform where you can manage all your ZyXEL product registrations and services using your personal account. Please register your account at myZyXEL.com first.

Username:

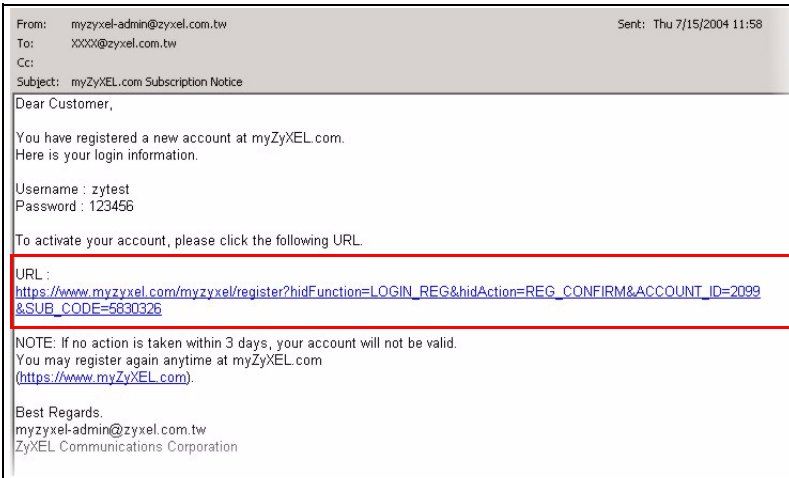
Password:

Remember Username:

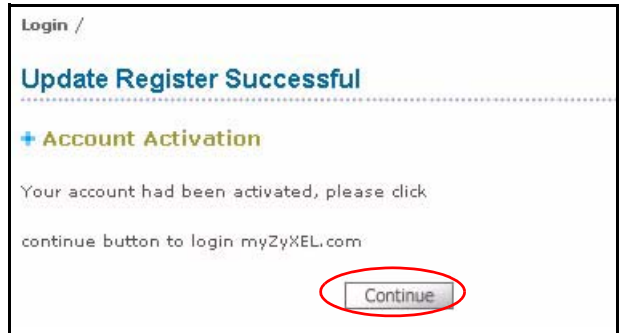
> Forgot Password? [Click here](#)

> If you are not a registered user, [Click here](#)

3 Wenn Sie ein Konto eröffnet haben, erhalten Sie eine E-Mail zur Bestätigung. Klicken Sie auf die in der E-Mail angegebene URL, um das Konto zu aktivieren.



4 Klicken Sie auf **Continue** (Weiter), um das myZyXEL.com-Anmeldefenster aufzurufen.



- 5 Melden Sie sich an.
- 6 Klicken Sie auf den Link und registrieren Sie Ihr ZyXEL-Produkt.

Welcome /

Welcome

Welcome! **Cindy Yang**

You have logged in myZyXEL.com for 1 times.

- > Last Viewed
- * IP:
- * Viewed Date:
- * Viewed time: (GMT+8:00)Taipei

Registered ZyXEL Products

[Click here](#) to register product

Note:
Currently, this registration website <http://www.myzyxel.com> supports Vantage CNM 2.0 and ZyXEL products service activation. For other products support, we will announce soon in our next release.

[More](#)

- 7 Klicken Sie auf **Add** (Hinzufügen).

My Products / Product Registration

Product Registration

Registered Product List

Your registered ZyXEL products are listed here.

Please click the product name to see more details.

Name	Serial Number
------	---------------

[Add](#)

8 Geben Sie in das Feld **Serial Number** (Seriennummer) die Seriennummer des Geräts ein.

9 In den Feldern **Category** (Kategorie) und **Model** (Modell) erscheinen automatisch die Gerätekategorie und die Modellnummern. Wenn nicht, wählen Sie die richtigen Angaben aus den Listenfeldern aus.

10 Geben Sie im Feld **Authentication Code** (Authentifizierungscode) die MAC-Adresse des Geräts ein (möglicherweise wird sie dort schon angezeigt).

11 Geben Sie im Feld **Friendly Name** (freundlicher Name) für Identifikationszwecke eine beschreibende Bezeichnung ein.

12 Klicken Sie auf **Register** (Registrieren).

13 Geben Sie die Kaufdaten ein und klicken Sie auf **Continue** (Fortfahren).

14 Klicken Sie noch einmal auf **Continue** (Fortfahren), um den Vorgang abzuschließen.

Add New Product

To add a new product, please fill in the following fields.
Friendly Name is an alias you give the product to identify it in the product list.

marked by (*) are Required

* Serial Number: Please enter the 10-digit number of the label on the unit. (Upper Case)

* Category: Please select your correct category and model. You can find it by your case.

* Model:

* Authentication Code:
 > For hardware products, this is the physical MAC address.
 > For software products, this is a generated number that is displayed after you ins (Upper Case)

* Friendly Name: Please give a name easy to remember for you. Up to 30 characters. It may contain underscore character, other character are not allowed.

Register

My Products / Product Registration

Product Survey

Product Information

+ Purchase date

+ You purchased this product from

Continue

15Nachdem Sie Ihr ZyXEL-Gerät registriert haben, können Sie sich die Registrierungsdaten im Fenster **Service Management** ansehen.

Das ZyXEL-Gerät ist nun registriert, jedoch ist der Content Filter noch nicht aktiviert. Um den Content Filter zu aktivieren, müssen Sie mit Ihrem Gerät auf die Seite myZyXEL.com zugreifen. Lesen Sie im nächsten Abschnitt weiter.

My Products / Service Activation

Service Management

Product Information

zy70cf
 Serial Number: S4Z2928704
 Products: ZyWALL 70
 Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

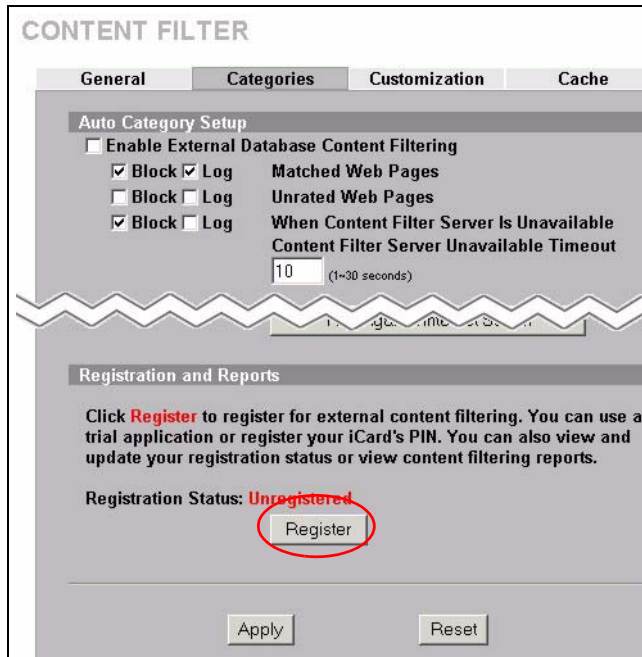
	Service Name	Service Activation	Status	Expiry Date	Remark
1	Content Filter	Activate	-	-	-

10 Externe Datenbank für den Content Filter

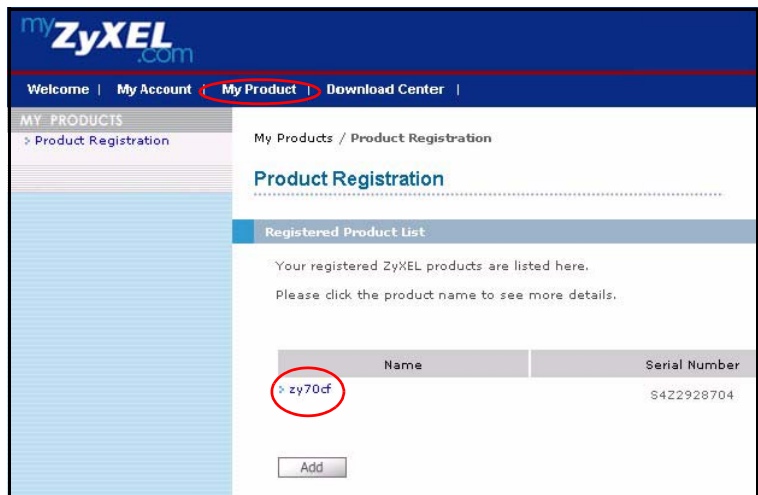
Wenn Sie den Content Filter registrieren und die externe Datenbank für den Content Filter aktivieren, greift die ZyWALL auf eine externe Datenbank zu, die Millionen von nach Inhalt sortierten Websites enthält. Auf der Grundlage dieser Kategorien kann die ZyWALL den Zugriff blockieren und/oder den Zugriff auf diese Websites zulassen. Registrieren Sie Ihre ZyWALL bei myZyXEL.com (siehe [Abschnitt 9](#)) und registrieren Sie dann folgendermaßen die externe Datenbank für den Content Filter.

- 1 Klicken Sie im Web-Konfigurator des ZyXEL-Geräts auf **CONTENT FILTER** (Inhaltsfilter), **Categories** (Kategorien) und dann auf die Taste **Register** (Registrieren).

Hinweis: Um den Content Filter zu konfigurieren, verwenden Sie die Fenster **CONTENT FILTER** (Inhaltsfilter) des ZyWALL-Web-Konfigurators



- 2 Das myZyXEL.com-Loginfenster erscheint.
- 3 Geben Sie den Nutzernamen und das Passwort Ihres myZyXEL.com-Kontos ein.
- 4 Klicken Sie in der Navigationsleiste auf **My Product** (Mein Produkt).
- 5 Klicken Sie auf die Verknüpfung Ihres Produktnamens, um die Registrierungsdaten im Fenster **Service Management** (Service-Management) aufzurufen.



6 Klicken Sie auf **Activate** (Aktivieren), um den Content Filter Dienst auf der nächsten Seite aufzurufen.

My Products / Service Activation

Service Management

Product Information

zy70cf

Serial Number: S4Z2928704
 Products: ZyWALL 70
 Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

> zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

	Service Name	Service Activation	Status	Expiry Date
1	Content Filter	Activate	-	-

7 Wenn Sie einen Testfilter verwenden möchten, klicken Sie bei **Content Filtering Trial** (Content Filter Testversion) auf **Submit** (Senden). Die Testdauer von 30 Tagen beginnt am Tag der Anmeldung.

Sie können keine Testversion anfordern, wenn Sie vorher schon einmal eine Testversion angefordert hatten oder eine PIN-Nummer einer iCard registriert haben.

Wenn Sie eine iCard erworben haben, geben Sie in das Feld **License Key** (PIN-Code) den PIN-Code genau wie auf der iCard an. Geben Sie das Datum ein, an dem der Inhaltsfilter beginnen soll und klicken Sie bei **Registration Information** (Registrierungsdaten) auf **Submit** (Senden).

My Products / Service Activation

Content Filtering Trial

We offer 30-day free trial for content filtering service.
 If you would like to have a try, please click "submit".

Registration Information

1. Enter the License Key (PIN code) exactly as shown in your iCard.
 2. Content filtering begins from the activation date.

> License Key (PIN code) :

> Activation Date : - -

- 8 Eine Meldung teilt Ihnen mit, dass der Dienst registriert wurde. Klicken Sie auf **Continue** (Fortfahren), um das Fenster **Service Management** aufzurufen.

My Products / Service Activation

Apply Standard Version Successful

Your E-mail Address : stanley_king@gfortunenet.com

Effective Period : 2004/07/31 ~ 2005/07/31

Your Name : stanley

Your Region : Taiwan

- 9 Auch wenn Sie gerade mit einer Testversion arbeiten, können Sie den PIN-Code einer iCard registrieren. Klicken Sie dazu im Feld **Service Activation** (Dienstaktivierung) des Fensters **Service Management** auf **Upgrade** (Aktualisieren).

My Products / Service Activation

Service Management

Product Information

zy70cf

Serial Number: S4Z2928704
Products: ZyWALL 70
Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

> zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

	Service Name	Service Activation	Status	Expiry Date	Remark
1	Content Filter	<input type="button" value="Upgrade"/>	Installed	2004-09-02	Refresh

11 Problembeseitigung

Problem	Lösungsmöglichkeit
Es leuchtet keine der LED-Anzeigen.	Stellen Sie sicher, dass das Netzkabel richtig an die ZyWALL und an eine Netzsteckdose angeschlossen wurde. Stellen Sie sicher, dass die ZyWALL eingeschaltet wurde. Überprüfen Sie alle Kabelverbindungen.
	Wenn die LEDs auch dann nicht leuchten, besteht möglicherweise ein Hardwareproblem. In diesem Fall sollten Sie sich an Ihren Händler wenden.
Aus dem LAN kann nicht auf die ZyWALL zugegriffen werden.	Überprüfen Sie die Kabelverbindung zwischen der ZyWALL und dem Computer oder Hub. Eine ausführliche Beschreibung finden Sie in Abschnitt 1 .
	Versuchen Sie die ZyWALL mit einem Ping von einem LAN-Computer aus zu erreichen. Stellen Sie sicher, dass die Ethernetkarte des Computers installiert ist und einwandfrei funktioniert.
	Klicken Sie im Computer auf Start, (Alle) Programme, Zubehör und dann auf Eingabeaufforderung . Geben Sie im Fenster Eingabeaufforderung "ping" gefolgt von der LAN-IP-Adresse der ZyWALL (192.168.1.1 ist die Standardadresse) ein und drücken Sie dann auf [ENTER]. Nun sollte die ZyWALL reagieren. Falls nicht, lesen Sie nach unter Abschnitt 11.1 .
	Wenn Sie das ZyWALL-Passwort vergessen haben, drücken Sie die RESET -Taste. Drücken Sie etwa 10 Sekunden lang auf die Taste (oder so lange, bis die PWR -LED blinkt). Lassen Sie die Taste dann wieder los. Auf diese Weise werden alle Einstellungen der ZyWALL auf ihre Standardwerte zurückgesetzt (Passwort: 1234, LAN-IP-Adresse 192.168.1.1 usw.; Detailinformationen hierzu finden Sie im Benutzerhandbuch).
	Wenn Sie die LAN- oder WAN-IP-Adresse der ZyWALL vergessen haben, können Sie die IP-Adresse über den Konsolenport im SMT einsehen. Schließen Sie Ihren Computer mit einem Konsolenkabel an den Anschluss CONSOLE an . Ihr Computer muss über ein Terminalemulationsprogramm (z.B. HyperTerminal) verfügen, das folgendermassen eingestellt ist: Anschlussemulation VT100, keine Parität, 8 Datenbits, 1 Stoppbit, keine Flusskontrolle, Portgeschwindigkeit 9600 bps.
Ein Zugriff auf das Internet ist nicht möglich.	Prüfen Sie den Anschluss der ZyWALL an der Ethernet-Buchse mit Internetzugriff. Stellen Sie sicher, dass das Gerät für den Internetzugriff (zum Beispiel ein DSL-Modem) einwandfrei funktioniert.
	Klicken Sie in der Navigationsleiste auf WAN und überprüfen Sie die Einstellungen.
Es kann keine VPN-Verbindung hergestellt werden.	Stellen Sie sicher, dass die ZyWALL und der Remote-IPSec -Router die gleichen VPN-Einstellungen verwenden. Klicken Sie in der Navigationsleiste auf VPN , um die erweiterten Einstellungen zu konfigurieren.
	Rufen Sie eine Website auf, um zu überprüfen, ob die Internetverbindung hergestellt werden kann.

11.1 Einrichten der IP-Adresse des Computers

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

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

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

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

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

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

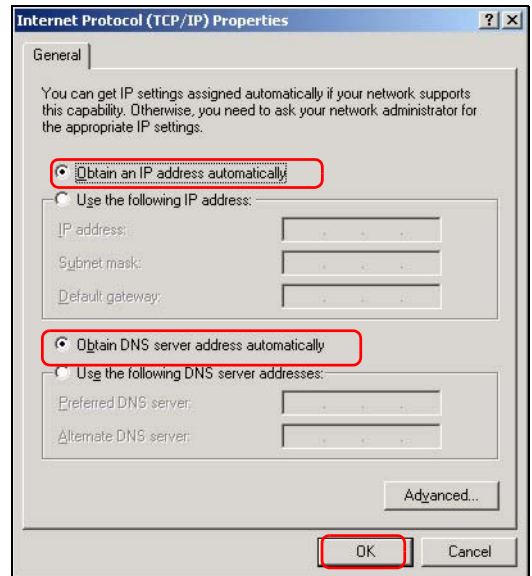
4 Wählen Sie **Internetprotokoll (TCP/IP)** (bei Windows XP auf der Registerkarte **Allgemein**) und klicken Sie auf **Eigenschaften**.

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

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

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

8 Schließen Sie das Fenster **Netzwerkverbindungen**.



11.2 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.

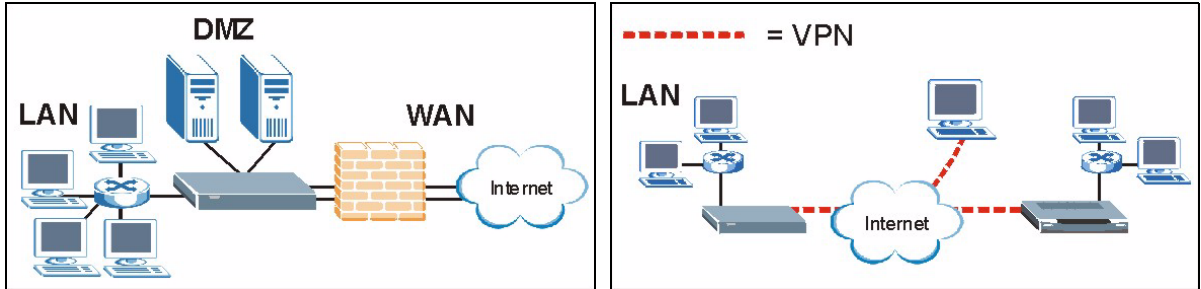
Wählen Sie auf dieser die Zertifizierung aus, die Sie gerne angezeigt haben möchten.

Vista previa

El ZyWALL 70 es un cortafuegos de WAN dual, con balanceo de carga, 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. El ZyWALL aumenta la seguridad de la red ofreciendo puertos DMZ para el uso con servidores públicos de acceso. 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 | 7 Cortafuegos |
| 2 Acceso al configurador Web | 8 Configuración de reglas VPN |
| 3 Modo puente (bridge) | 9 Registro del producto en myZyXEL.com |
| 4 Configuración del acceso a Internet | 10 Filtrado de contenidos |
| 5 DNS | 11 Solución de problemas |
| 6 NAT | |

1 Conexiones del hardware

Necesita lo siguiente.

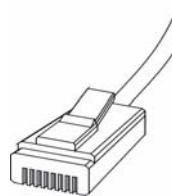
ZyWALL



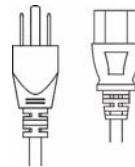
Ordenador



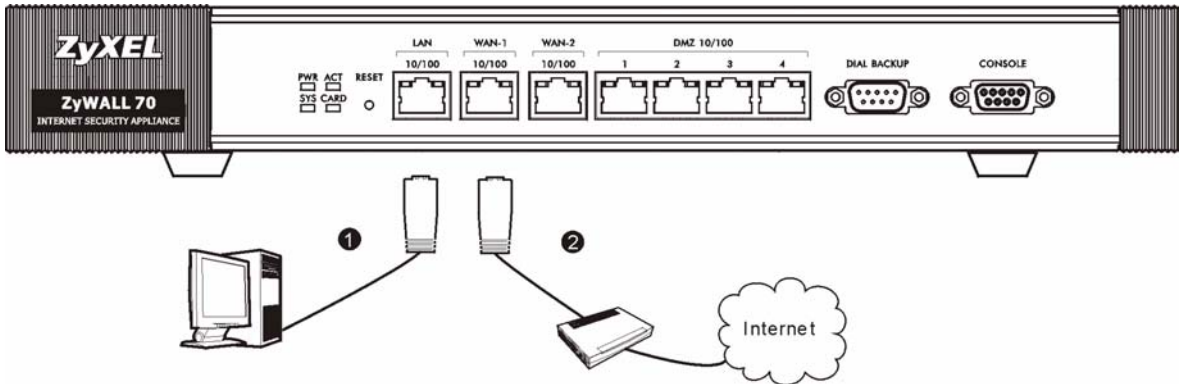
Cables Ethernet



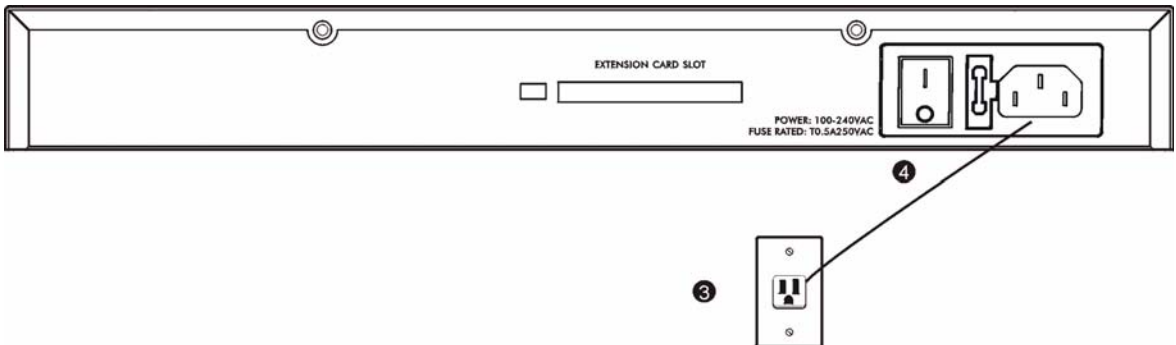
Cable de alimentación



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



- 1 Use un cable Ethernet para conectar el puerto **LAN** a un ordenador. También puede usar cables Ethernet para conectar servidores públicos (web, correo electrónico, FTP, etc.) a los puertos **DMZ**.
- 2 Use otro(s) cable(s) Ethernet para conectar el puerto **WAN 1** y/o **WAN 2** a un dispositivo Ethernet con acceso a Internet.

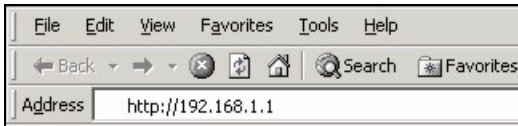


- 3 Use el cable de alimentación incluido para conectar el zócalo de alimentación (en el panel posterior) a una toma de corriente
- 4 Pulse el interruptor de alimentación hasta la posición de encendido y mire al panel frontal. El **LED PWR** se encenderá. El **LED SYS** parpadeará mientras realiza la prueba del sistema y luego se quedará fijo si la prueba ha tenido éxito. Los LEDs **ACT**, **CARD**, **LAN**, **DMZ** y **WAN** se encenderán y permanecerán encendidos si las conexiones correspondientes se han realizado correctamente.

2 Acceso al configurador Web

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

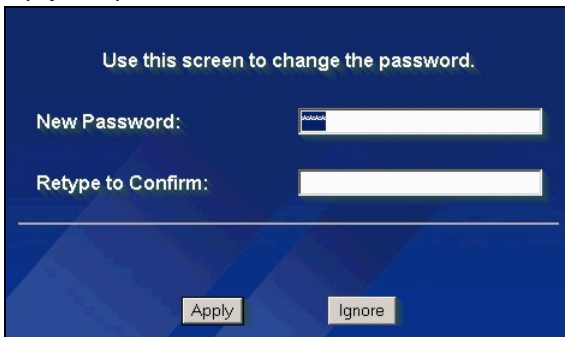
- 1 Abra su explorador de web. Introduzca **192.168.1.1** (la dirección IP predeterminada del ZyWALL) como dirección.
Si no aparece la pantalla de acceso, vea [Sección 11.1](#) para ajustar la dirección IP de su ordenador.



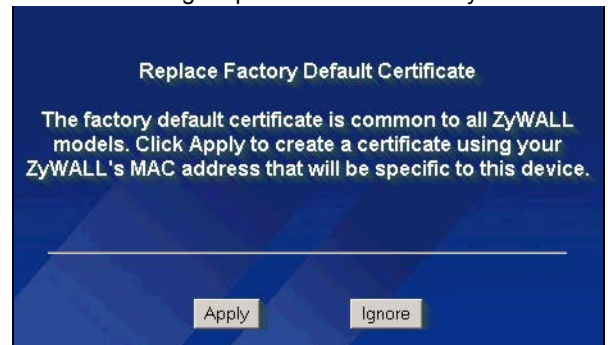
- 2 Haga clic en **Login (acceso)** (la contraseña predeterminada 1234 ya está introducida).



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



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



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

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

Vaya a [Sección 3](#) si prefiere usar el ZyWALL como cortafuegos transparente.

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

Si el estado de la **WAN 1** es **Down (Caído)** (o no hay una dirección IP), haga clic en **Internet Access** (acceso a Internet) y use [Sección 4](#) para configurar **WAN 1**.

Use las pantallas **WAN** en **NETWORK** (red) si necesita configurar **WAN 2**. También puede configurar el balanceo de carga entre los puertos WAN.

ZyXEL HOME HELP ?

HOME

NETWORK
LAN
WIRELESS LAN
WAN
DMZ

SECURITY
FIREWALL
CONTENT FILTER
VPN
CERTIFICATES
AUTH SERVER

ADVANCED
NAT
STATIC ROUTE
POLICY ROUTE
BW MGMT
DNS
REMOTE MGMT
UPnP

LOGS

MAINTENANCE

LOGOUT

HOME

Wizards for WAN 1 Quick Setup

Internet Access VPN

Device Information

System Name:

Firmware Version: V3.64(WM.0)b1 | 12/17/2004

Routing Protocol: IP

Device Mode: Router

Firewall: Enabled

System Time: 2005-01-11 08:27:37 GMT

Memory: 14358K/19473K

Sessions: 5/10000

Policy

Routes: 0/48

Network Status

Interface	Status	IP Address	Subnet Mask	DHCP	Renew
WAN 1	Down	0.0.0.0	0.0.0.0	Client	Renew
WAN 2	Down	0.0.0.0	0.0.0.0	Client	Renew

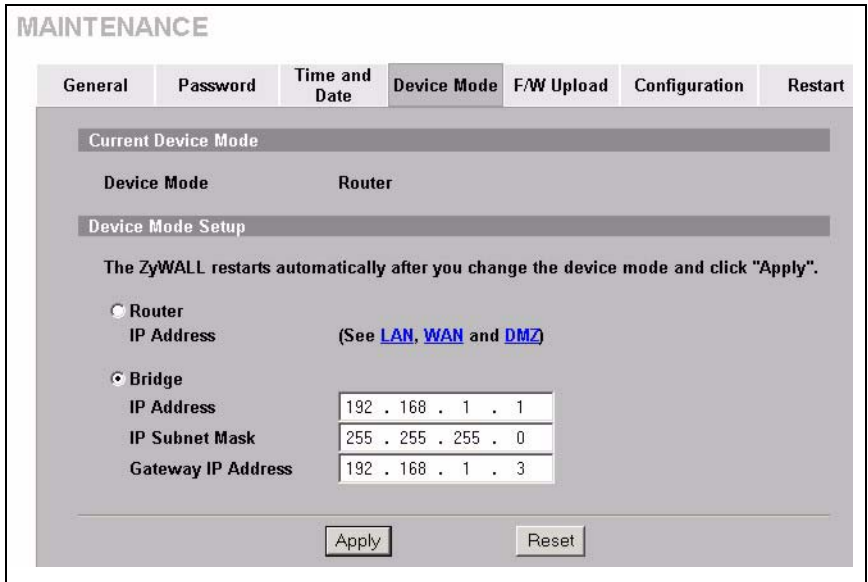
Status: Ready

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

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.

Nota: 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 **Finish (Finalizar)** cuando haya terminado.

- **Encapsulación Ethernet**

Configure un servicio Correcaminos en las pantallas **WAN** de **NETWORK (Red)** (use la ficha **WAN 1**).

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

- **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)**.

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

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

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 - Negación de Servicio).

A diferencia de LAN, el ZyWALL no asigna la configuración TCP/IP a través de DHCP a ordenadores conectados a los puertos DMZ. Configure los ordenadores con direcciones IP estáticas (en la misma subred que la dirección IP del puerto DMZ) y direcciones de 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.

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

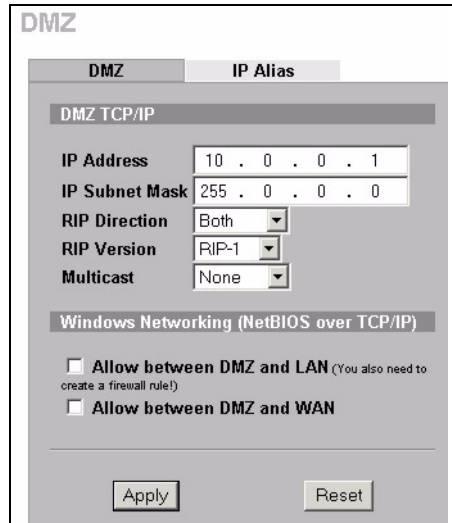
- 1 Haga clic en **DMZ** en el panel de navegación.

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)**.



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 WAN a un servidor HTTP (web) en la DMZ. El servidor tiene una dirección IP privada de 10.0.0.20.

- 1 Haga clic en **NAT** en el panel de navegación y luego en **Port Forwarding (Reenvío de puerto)**.
- 2 Seleccione la casilla de verificación **Active (Activa)**.
- 3 Escriba un nombre para la regla.
- 4 Escriba el número que el servicio usa.
- 5 Escriba la dirección IP del servidor HTTP.
- 6 Haga clic en **Apply (Aplicar)**.

NAT

NAT Overview
Address Mapping
Port Forwarding
Port Triggering

Port Forwarding Rules

WAN Interface WAN 1

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
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 Cortafuegos

Puede usar el ZyWALL sin configurar el cortafuegos.

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

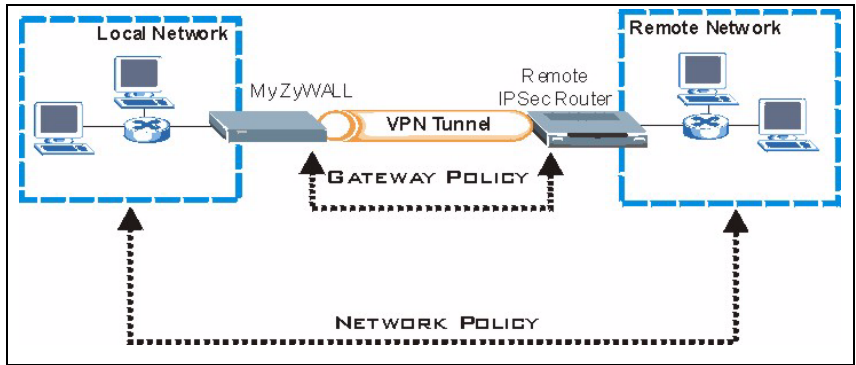
Si usa el ZyWALL en modo enrutador, continúe con la siguiente sección. Para el modo puente, vaya a [Sección 9](#).

8 Configuración de reglas VPN

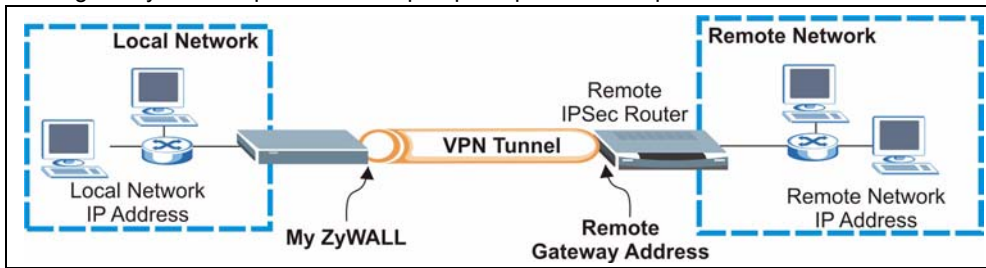
Un túnel VPN (Virtual Private Network - Red Privada Virtual) le ofrece una conexión segura a otro ordenador o red.

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

Una política de red específica 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 **VPN** en la pantalla **HOME (Inicio)** (puede que necesite desplazar arriba para ver el enlace) para abrir el asistente para VPN.

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

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

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

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

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

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

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.

Gateway Policy Property

Name: Test

Gateway Policy Setting

My ZyWALL: 0.0.0.0

Remote Gateway Address: BranchOffice.com

Next

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

Nota: 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.

Nota: 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).

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 esta pantalla para establecer la configuración IPSec.

IPSec Setting (IKE Phase 2)

Encapsulation Mode Tunnel Transport

IPSec Protocol ESP AH

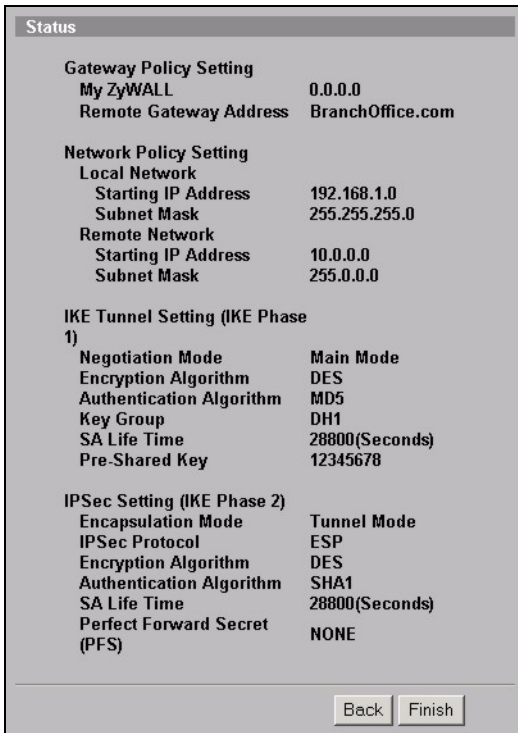
Encryption Algorithm DES AES 3DES NULL

Authentication Algorithm SHA1 MD5

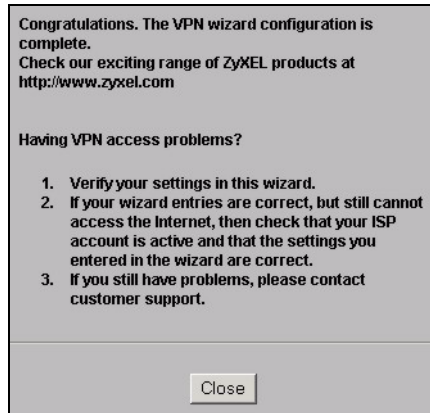
SA Life Time (Seconds)

Perfect Forward Secret (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.

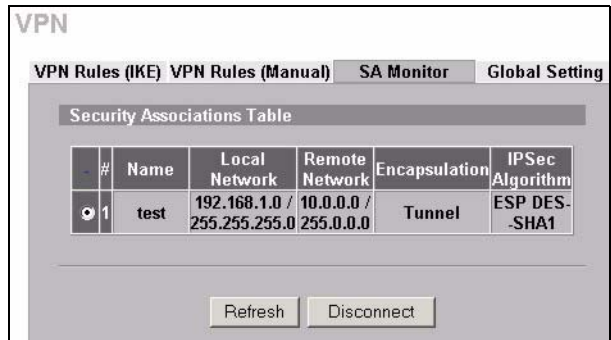


8.1 Usar la conexión VPN

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

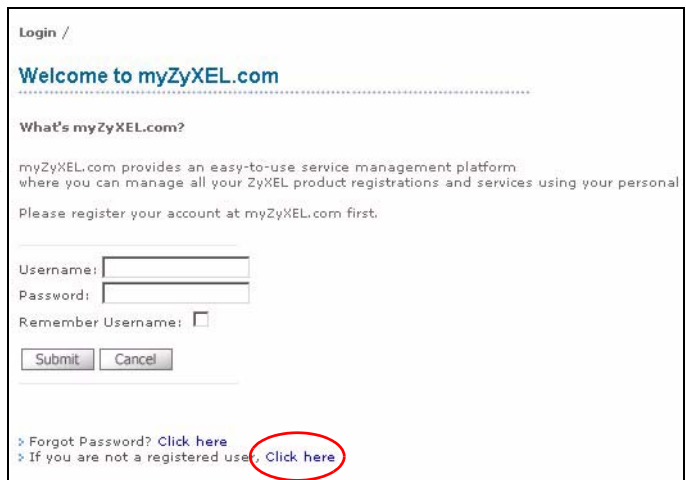


9 Registro del producto myZyXEL.com

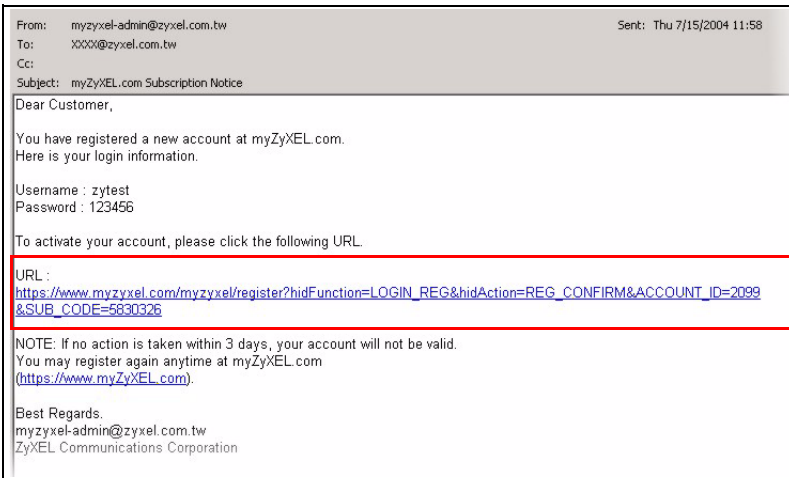
myZyXEL.com es el centro de servicios en línea de ZyXEL donde podrá registrar su dispositivo ZyXEL.

- 1 Vaya a myZyXEL.com usando su explorador.
- 2 Cree una nueva cuenta (si todavía no tiene una).

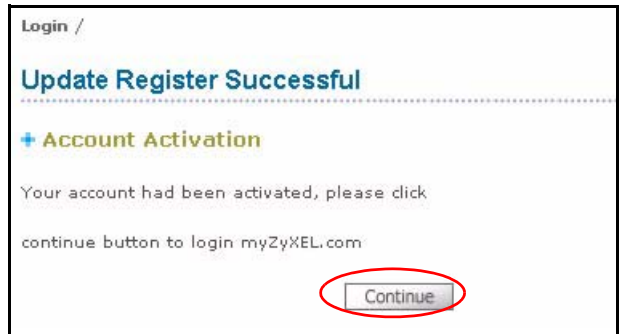
Nota: Saldrá automáticamente de la cuenta myZyXEL.com tras cinco minutos de inactividad. Simplemente vuelva a entrar en su cuenta myZyXEL.com si esto ocurre.



3 Tras crear una cuenta, recibirá un correo electrónico de confirmación. Haga clic en la URL del correo electrónico para activar su cuenta.

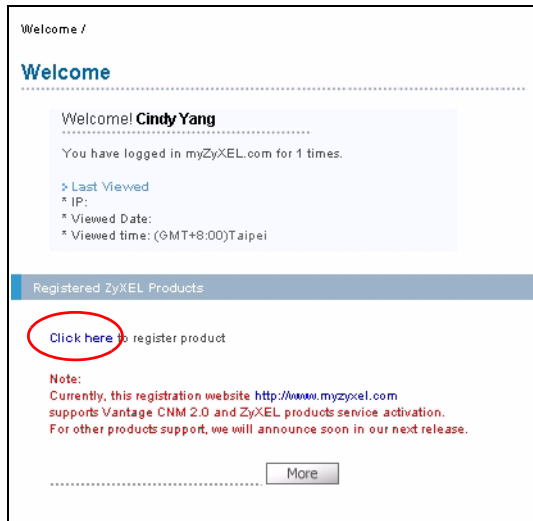


4 Haga clic en **Continue (Continuar)** para ir a la pantalla de acceso de myZyXEL.com.



5 Acceda.

6 Haga clic en el enlace y registre su dispositivo ZyXEL.



7 Haga clic en **Add (Agregar)**.



- 8 Introduzca el número de serie del producto en el campo **Serial Number (Número de serie)**.
- 9 La categoría del dispositivo y número de modelo aparecen automáticamente en los campos **Category (Categoría)** y **Model (Modelo)** respectivamente. En caso contrario, seleccione los correctos de los cuadros de listas desplegables.
- 10 Introduzca la dirección MAC del dispositivo en el campo **Authentication Code (Código de autenticación)** (puede que ya se vea).
- 11 Introduzca un nombre de descripción en el campo **Friendly Name (Nombre amigable)** para la identificación.
- 12 Haga clic en **Registrar**.
- 13 Especifique la información de compra y haga clic en **Continuar**.
- 14 Haga clic en **Continuar** de nuevo para completar el proceso.

Add New Product

To add a new product, please fill in the following fields.
Friendly Name is an alias you give the product to identify it in the product list.

marked by (*) are Required

* Serial Number: Please enter the 10-digit number of the label on the unit. (Upper Case)

* Category: Please select your correct category and model. You can find it by your case.

* Model:

* Authentication Code:
 > For hardware products, this is the physical MAC address.
 > For software products, this is a generated number that is displayed after you ins (Upper Case)

* Friendly Name: Please give a name easy to remember for you. Up to 30 characters. It may contain underscore character, other character are not allowed.

My Products / Product Registration

Product Survey

Product Information

+ Purchase date

+ You purchased this product from

15Tras haber registrado el dispositivo ZyXEL, podrá ver los detalles de su registro en la pantalla **Service Management (Administración del servicio)**.

El dispositivo ZyXEL ya está registrado, pero la filtración de contenidos no está activada. Para activar la filtración de contenidos, deberá acceder a myZyXEL.com a través de su dispositivo. Continúe con la siguiente sección.

The screenshot shows the 'Service Management' page for a ZyXEL device. It is divided into three main sections:

- Product Information:** Displays the device ID 'zy70cf', Serial Number 'S422928704', Product 'ZyWALL 70', and Authentication Code '00A0C5012345'.
- Manage Product:** Instructs the user to manage registration via buttons: 'Rename', 'Transfer', 'Delete', and 'Reinstall'.
- Applicable Service List:** A table listing services available for activation. The 'Content Filter' service is listed with an 'Activate' link.

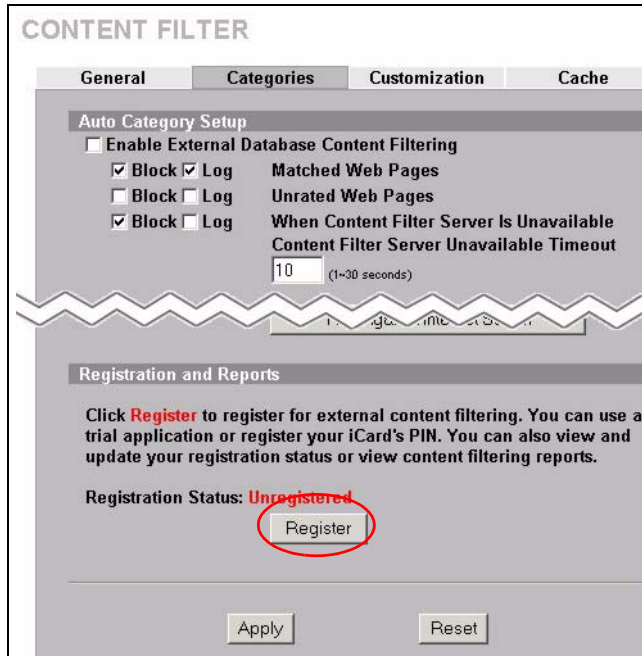
	Service Name	Service Activation	Status	Expiry Date	Remark
1	Content Filter	Activate	-	-	-

10 Filtrado de contenidos

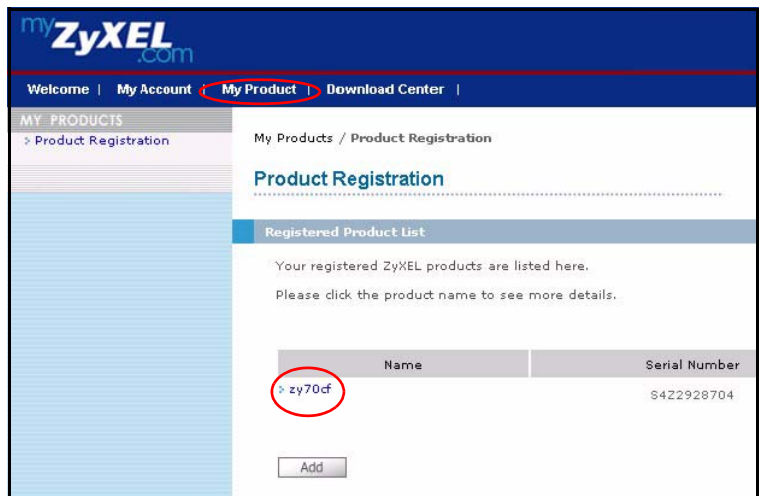
Cuando registre y active la filtración de contenidos de la base de datos externa, su ZyWALL accederá a una base de datos externa que tiene millones de sitios web clasificados según su contenido. Puede que el ZyWALL bloquee y/o acceda a los sitios web basándose en estas categorías. Registre su ZyWALL en myZyXEL.com (ver [Sección 9](#)) y luego realice lo siguiente para registrarse para la filtración de contenidos de la base de datos externa.

- 1 En el configurador web del dispositivo ZyXEL, haga clic en el botón **CONTENT FILTER (Filtro de contenidos)**, **Categories (Categorías)** y luego en **Register (Registrar)**.

Nota: Puede usar las pantallas **CONTENT FILTER (Filtro de contenidos)** del configurador web del ZyWALL para configurar y activar el filtrado de contenidos.



- 2 Se abrirá la pantalla de acceso a myZyXEL.com.
- 3 Introduzca el nombre de usuario y contraseña de su cuenta myZyXEL.com.
- 4 Haga clic en **My Product (Mi producto)** en el panel de navegación.
- 5 Haga clic en el enlace del nombre del producto de su dispositivo para ver sus detalles de registro en la pantalla **Service Management (Administración del servicio)**.



6 Haga clic en **Activate (Activar)** para que el servicio de filtro de contenidos aparezca en la siguiente pantalla.

My Products / Service Activation

Service Management

Product Information

zy70cf

Serial Number: S4Z2928704
 Products: ZyWALL 70
 Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

> zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

	Service Name	Service Activation	Status	Expiry Date
1	Content Filter	<input type="button" value="Activate"/>	-	-

7 Si desea usar la versión de prueba, haga clic en **Submit (Enviar)** en **Content Filtering Trial (Prueba de filtrado de contenidos)**. El período de prueba comienza desde la fecha en que aplique.

No puede aplicar una prueba si ya ha usado un número PIN de iCard de prueba o registrado.

Si ha comprado una iCard, introduzca el código PIN exactamente como aparece en su iCard en el campo **License Key (Clave de licencia)** (código PIN). Seleccione la fecha cuando desea que la filtración de sus contenidos comience y haga clic en **Submit (Enviar)** en **Registration Information (Información del registro)**.

My Products / Service Activation

Content Filtering Trial

We offer 30-day free trial for content filtering service.
 If you would like to have a try, please click "submit".

Registration Information

1. Enter the License Key (PIN code) exactly as shown in your iCard.
2. Content filtering begins from the activation date.

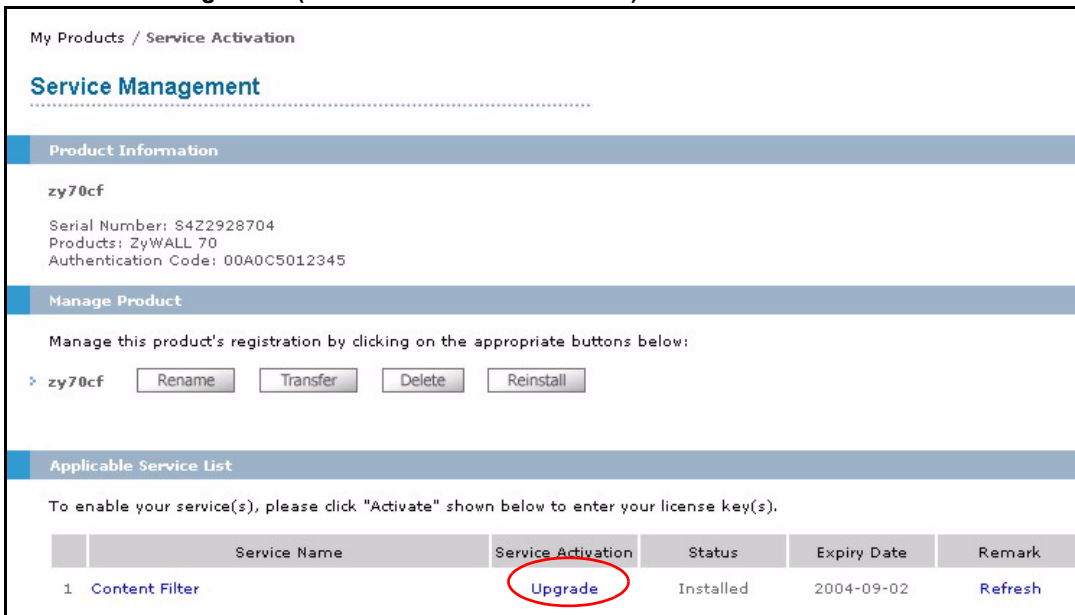
> License Key (PIN code) :

> Activation Date : - -

- 8 Aparecerá una pantalla mostrando que el servicio se ha registrado. Haga clic en **Continue (Continuar)** para ir a la pantalla **Service Management (Administración del servicio)**.



- 9 Si actualmente está usando una prueba, todavía puede registrar el código PIN de una iCard haciendo clic en **Upgrade (Actualizar)** en el campo **Service Activation (Activación del servicio)** en la pantalla **Service Management (Administración del servicio)**.



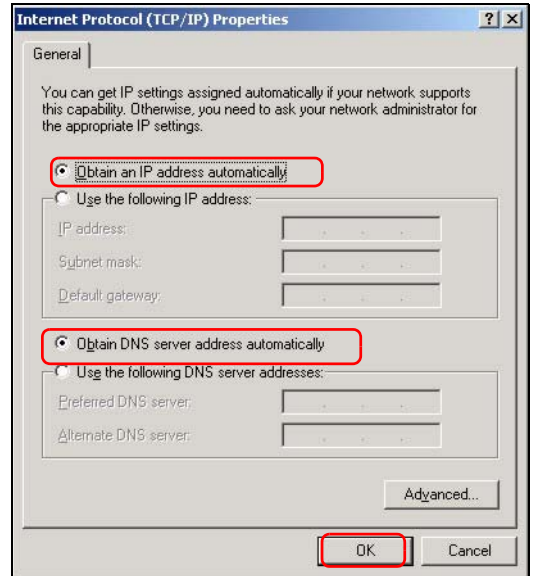
11 Solución de problemas

Problema	Solución
Ninguno de los LEDs se enciende.	Asegúrese de haber conectado el cable de alimentación al ZyWALL y si lo ha enchufado en una fuente de alimentación apropiada. Compruebe que el ZyWALL está encendido. Compruebe todas las conexiones de los cables.
	Si los LEDs todavía no se encienden, puede que tenga un problema de hardware. En este caso, debería contactar con su vendedor local.
No se puede acceder al ZyWALL desde la LAN.	Compruebe la conexión de cables entre el ZyWALL y su ordenador o hub. Consulte Sección 1 para más detalles.
	Realice un ping al ZyWALL desde un ordenador LAN. Compruebe que la tarjeta Ethernet de su ordenador esté instalada y funcione correctamente. En el ordenador, haga clic en Inicio , (Todos los programas , Accesorios y luego en Símbolo del sistema . En la ventana del Símbolo del sistema , escriba "ping" seguido por la dirección IP LAN del ZyWALL (192.168.1.1 es la predeterminada) y pulse [ENTRAR]. El ZyWALL debería responder. En caso contrario, consulte Sección 11.1 .
	Si ha olvidado la contraseña del ZyWALL, use el botón RESET . Mantenga pulsado el botón durante unos 10 segundos (o hasta que el LED PWR comience a parpadear), a continuación suéltelo. Esto devolverá al ZyWALL la configuración predeterminada de fábrica (la contraseña es 1234, dirección IP LAN 192.168.1.1 etc.; vea la Guía del usuario para más detalles).
	Si ha olvidado la dirección IP LAN o WAN del ZyWALL puede comprobar la dirección IP en la SMT a través del puerto consola SMT. Conecte su ordenador al puerto CONSOLE (Consola) usando un cable de consola. Su ordenador debería tener un programa de comunicaciones de emulación de terminales (como HyperTerminal) ajustado a la emulación del terminal VT100, sin paridad, 8 bits de datos, 1 bit de parada, sin flujo de control y una velocidad de puerto de 9600 bps.
No puedo acceder a Internet.	Compruebe la conexión del ZyWALL a la clavija Ethernet con acceso a Internet. Compruebe si el dispositivo de puerta de enlace de Internet (como un módem DSL) funciona correctamente.
	Haga clic en WAN en el panel de navegación para verificar su configuración.
No puedo establecer una conexión VPN	Compruebe si el ZyWALL y el enrutador IPsec usan la misma configuración VPN. Haga clic en VPN en el panel de navegación para establecer la configuración avanzada.
	Acceda a un sitio web para comprobar si tiene una conexión a Internet correcta.

11.1 Configurar la dirección IP de su ordenador

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

- 1 En Windows XP, haga clic en **Inicio, Panel de control**.
En Windows 2000/NT, haga clic en **Inicio, Configuración, Panel de control**.
- 2 En Windows XP, haga clic en **Conexiones de red**.
En Windows 2000/NT, haga clic en **Conexiones de red y marcación**.
- 3 Haga clic con el botón derecho en **Conexión de área local** y haga clic en **Propiedades**.
- 4 Seleccione **Protocolo Internet (TCP/IP)** (en la ficha **General** en Windows XP) y haga clic en **Propiedades**.
- 5 Se abrirá la pantalla **Propiedades de Protocolo Internet TCP/IP** (la **ficha General** en Windows XP). Seleccione las opciones **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente**.
- 6 Haga clic en **Aceptar** para cerrar la ventana **Propiedades de Protocolo Internet (TCP/IP)**.
- 7 Haga clic en **Cerrar (Aceptar** en Windows 2000/NT) para cerrar la ventana **Propiedades de conexión de área local**.
- 8 Cierre la pantalla **Conexiones de red**.



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

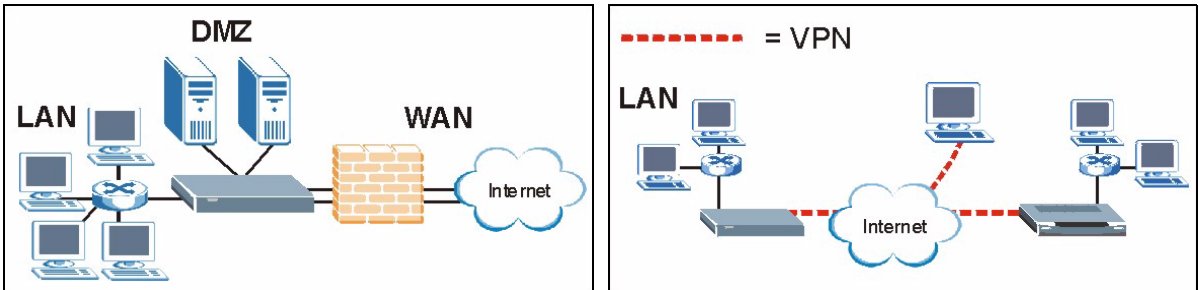
- 1 Vaya a www.zyxel.com.
- 2 Seleccione su producto de la lista desplegable en la página inicial de ZyXEL para ir a la página de ese producto.
- 3 Seleccione la certificación que desee visualizar en esta página.

Présentation

Le ZyWALL 70 est un pare-feu double WAN à équilibrage de charge 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. Le ZyWALL améliore la sécurité du réseau en offrant des ports DMZ à utiliser avec les 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 | 7 Pare-feu |
| 2 Accéder au Configurateur Web | 8 Installation de la règle VPN |
| 3 Mode Pont | 9 Enregistrement du produit sur myZyXEL.com |
| 4 Installation de l'accès à Internet | 10 Filtrage du contenu à partir d'une base données externe |
| 5 DNS | 11 Dépannage |
| 6 NAT | |

1 Connexions matérielles

Vous avez besoin des éléments suivants.

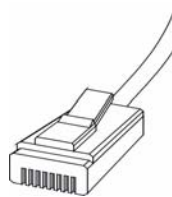
ZyWALL



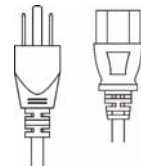
Ordinateur



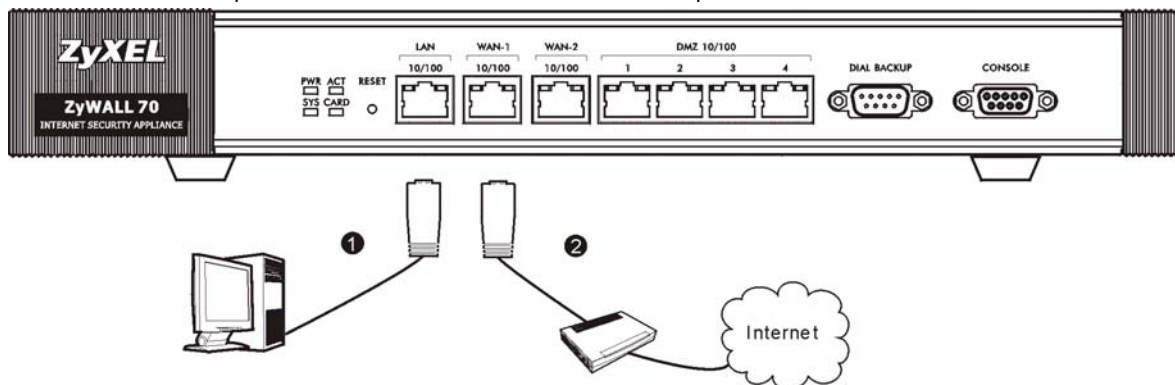
Câbles Ethernet



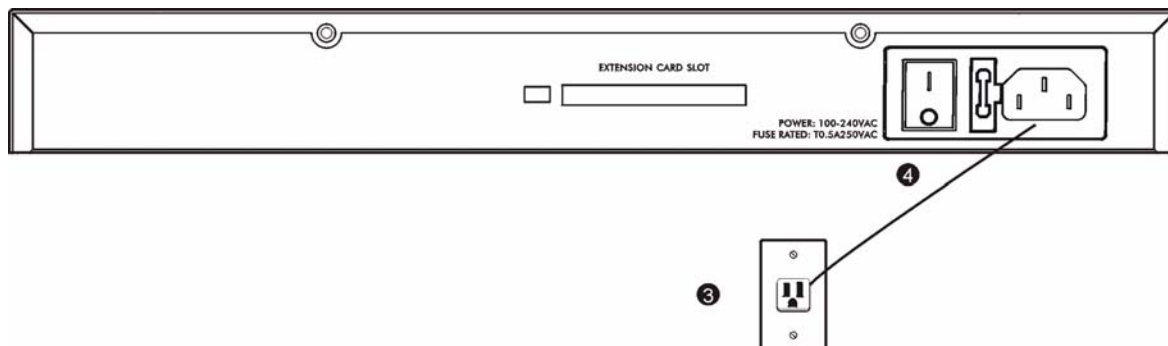
Cordon d'alimentation



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



- 1 Utilisez un câble Ethernet pour connecter le port **LAN** à un ordinateur. Vous pouvez aussi utiliser les câbles Ethernet pour connecter les serveurs publics (web, e-mail, FTP, etc.) aux ports **DMZ**.
- 2 Utilisez un autre (ou d'autres) câble(s) Ethernet pour connecter le port **WAN 1** et/ou **WAN 2** à une prise Ethernet avec accès à Internet.

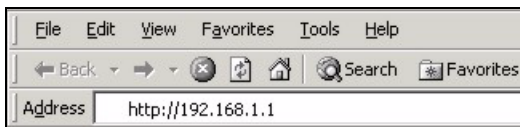


- 3 Utilisez le cordon d'alimentation pour connecter la prise d'alimentation.
- 4 Mettez le commutateur d'alimentation sur la position allumé et regardez le panneau avant. La **LED PWR** s'allume. La **LED SYS** clignote lors du test du système et reste ensuite allumée si le test a réussi. Les **LED ACT, CARD, LAN, DMZ, et WAN** s'allument et restent allumées si les connexions correspondantes sont effectuées correctement.

2 Accéder au Configurateur Web

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

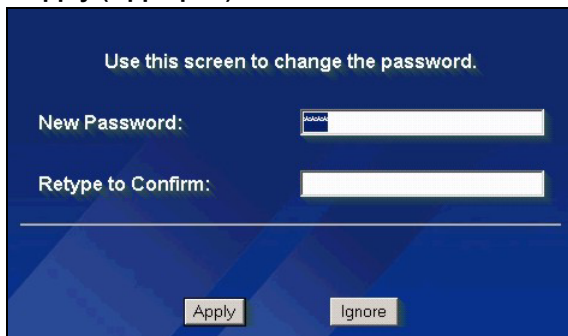
- 1 Lancez votre navigateur web. Entrez **192.168.1.1** (l'adresse IP par défaut du ZyWALL) comme adresse.
Si l'écran de connexion n'apparaît pas, voyez [la Section 11.1](#) comment définir l'adresse IP de votre ordinateur.



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



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



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



- 5 L'écran **HOME (ACCUEIL)** s'ouvre.

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

Allez à [la Section 3](#) si vous préférez utiliser le ZyWALL comme un pare-feu transparent.

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

Si l'état **WAN 1** est **Désactivé** (ou s'il n'y a pas d'adresse IP), cliquez sur **Accès Internet** et passez à la [Section 4](#) pour configurer **WAN 1**.

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

ZyXEL HOME HELP ?

HOME

NETWORK
LAN
WIRELESS LAN
WAN
DMZ

SECURITY
FIREWALL
CONTENT FILTER
VPN
CERTIFICATES
AUTH SERVER

ADVANCED
NAT
STATIC ROUTE
POLICY ROUTE
BW MGMT
DNS
REMOTE MGMT
UPnP

LOGS

MAINTENANCE

LOGOUT

Wizards for WAN 1 Quick Setup

Internet Access VPN

Device Information

System Name:
Firmware Version: V3.64(WM.0)b1 | 12/17/2004
Routing Protocol: IP
Device Mode: Router
Firewall: Enabled
System Time: 2005-01-11 08:27:37 GMT
Memory: 14358K/19473K
Sessions: 5/10000
Policy
Routes: 0/48

Network Status

Interface	Status	IP Address	Subnet Mask	DHCP	Renew
WAN 1	Down	0.0.0.0	0.0.0.0	Client	Renew
WAN 2	Down	0.0.0.0	0.0.0.0	Client	Renew

Status: Ready

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 **Mode Périphérique**.
- 2 Sélectionnez **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 **Appliquer**. Le ZyWALL redémarre.

Passez à la [Section 5](#) si vous avez des serveurs qui doivent être accessibles à partir du WAN.

MAINTENANCE

General	Password	Time and Date	Device Mode	F/W Upload	Configuration	Restart
---------	----------	---------------	-------------	------------	---------------	---------

Current Device Mode

Device Mode	Router
--------------------	--------

Device Mode Setup

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

Router

Bridge

IP Address	(See LAN , WAN and DMZ)
IP Address	<input type="text" value="192 . 168 . 1 . 1"/>
IP Subnet Mask	<input type="text" value="255 . 255 . 255 . 0"/>
Gateway IP Address	<input type="text" value="192 . 168 . 1 . 3"/>

4 Installation de l'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 **Statique** dans la boîte de la liste déroulante d'**Attribution d'adresse IP** et saisissez les informations fournies.

Remarque: 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 **Terminer** quand vous avez terminé.

- **Encapsulation Ethernet**

Configurer un service Roadrunner dans les écrans du **NETWORK WAN** (utilisez l'onglet **WAN 1**).

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 **Délai d'inactivité** (Idle Timeout).

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

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

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).

Contrairement au LAN, le ZyWALL n'attribue pas de configuration TCP/IP via DHCP aux ordinateurs connectés aux ports DMZ. 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.

Remarque: Vous n'avez pas besoin de configurer DMZ avec le mode pont, sautez à [la Section 7](#).

- 1 Cliquez **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 **Appliquer**.

The screenshot shows the DMZ configuration window. The 'DMZ' tab is selected, and the 'IP Alias' sub-tab is active. The 'DMZ TCP/IP' section contains the following fields and values:

- IP Address: 10 . 0 . 0 . 1
- IP Subnet Mask: 255 . 0 . 0 . 0
- RIP Direction: Both
- RIP Version: RIP-1
- Multicast: None

The 'Windows Networking (NetBIOS over TCP/IP)' section has two checkboxes:

- Allow between DMZ and LAN (You also need to create a firewall rule!)
- Allow between DMZ and WAN

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

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 **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 WAN à un serveur HTTP (web) sur le DMZ. Le serveur possède une adresse IP privée de 10.0.0.20.

- 1 Cliquez sur **NAT** dans le panneau de navigation et ensuite sur **Réacheminement de Port**.
- 2 Sélectionnez la case à cocher **Active**.
- 3 Tapez un nom pour la règle.
- 4 Tapez le numéro de port que le service utilise.
- 5 Tapez l'adresse IP du serveur HTTP.
- 6 Cliquez sur **Appliquer**.

NAT

NAT Overview
Address Mapping
Port Forwarding
Port Triggering

Port Forwarding Rules

WAN Interface WAN 1

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
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.

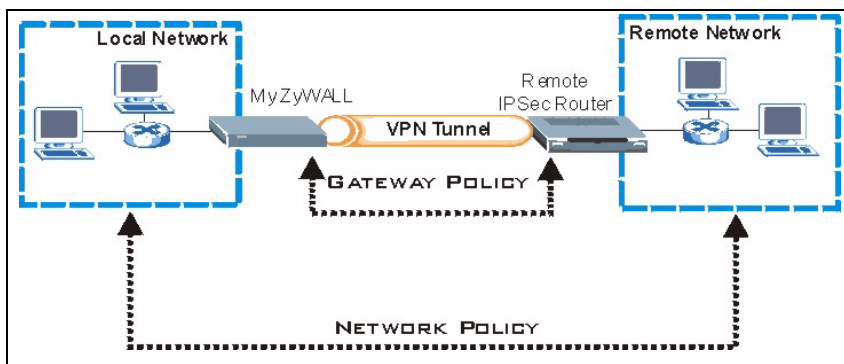
Si vous utilisez le ZyWALL en mode routeur, suivez la section suivante. Pour le mode pont, passez à [la Section 9](#).

8 Installation de la règle VPN

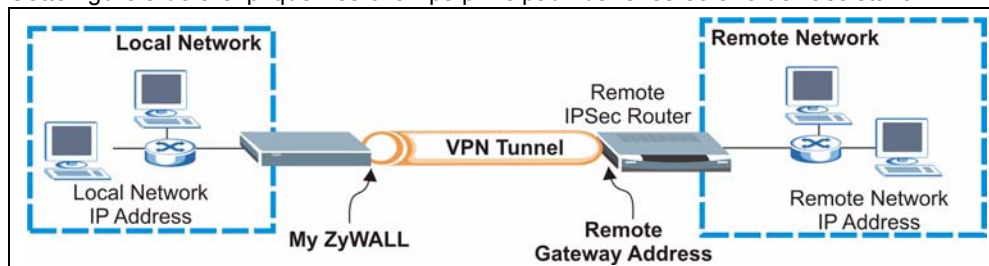
Un tunnel VPN (Virtual Private Network) vous offre une connexion sécurisée à un autre ordinateur ou réseau.

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

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



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



- 1 Cliquez sur **VPN** dans l'écran d'**ACCUEIL** (vous devrez peut-être faire défiler vers le haut pour voir les liens) pour ouvrir l'assistant VPN.

Remarque: Vos paramètres ne sont pas enregistrés quand vous cliquez sur **Retour**.

2 Utilisez cet écran pour configurer la stratégie de passerelle.

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

Adresse de passerelle distante : Entrez l'adresse IP ou le nom de domaine du routeur IPsec distant.

The screenshot shows two configuration screens for a Gateway Policy. The top screen, titled "Gateway Policy Property", has a "Name" field containing "Test". The bottom screen, titled "Gateway Policy Setting", has a "My ZyWALL" field containing "0.0.0.0" and a "Remote Gateway Address" field containing "BranchOffice.com". A "Next" button is located at the bottom right of the second screen.

3 Utilisez cet écran pour configurer la stratégie de réseau.

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

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

Sélectionnez **Unique** et entrez une adresse IP pour une adresse IP unique.

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

Sélectionnez **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.

The screenshot shows two configuration screens for a Network Policy. The top screen, titled "Network Policy Property", has a checked "Active" checkbox and a "Name" field containing "Test". The bottom screen, titled "Network Policy Setting", has radio buttons for "Local Network" and "Remote Network", each with options for "Single", "Range IP", and "Subnet". For the "Local Network", "Single" is selected, with "Starting IP Address" set to "192 . 168 . 1 . 0" and "Ending IP Address / Subnet Mask" set to "255 . 255 . 255 . 0". For the "Remote Network", "Subnet" is selected, with "Starting IP Address" set to "10 . 0 . 0 . 0" and "Ending IP Address / Subnet Mask" set to "255 . 0 . 0 . 0". "Back" and "Next" buttons are at the bottom right.

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

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

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

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

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

Groupe de clés : Sélectionnez **DH2** pour avoir une sécurité plus élevée.

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.

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.

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

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

Confidentialité de transmission parfaite (PFS) : **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).

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 Utilisez cet écran pour configurer les paramètres IPSec.

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 Secret (PFS) None DH1 DH2

- 6 Vérifiez vos paramètres VPN. Cliquez sur **Terminer** pour enregistrer les paramètres.

Status	
Gateway Policy Setting	
My ZyWALL	0.0.0.0
Remote Gateway Address	BranchOffice.com
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)	
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 Secret (PFS)	NONE
<input type="button" value="Back"/> <input type="button" value="Finish"/>	

- 7 Cliquez sur **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.

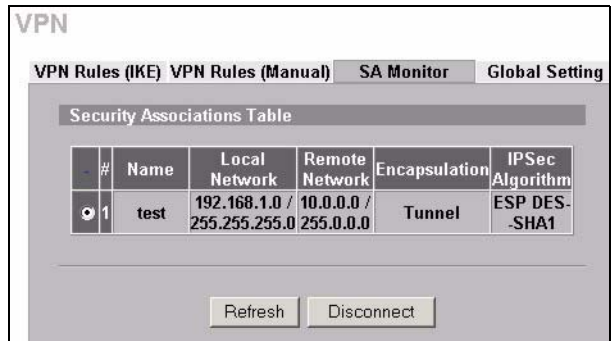
<p>Congratulations. The VPN wizard configuration is complete. Check our exciting range of ZyXEL products at http://www.zyxel.com</p> <p>Having VPN access problems?</p> <ol style="list-style-type: none"> 1. Verify your settings in this wizard. 2. If your wizard entries are correct, but still cannot access 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. <p style="text-align: center;"><input type="button" value="Close"/></p>

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

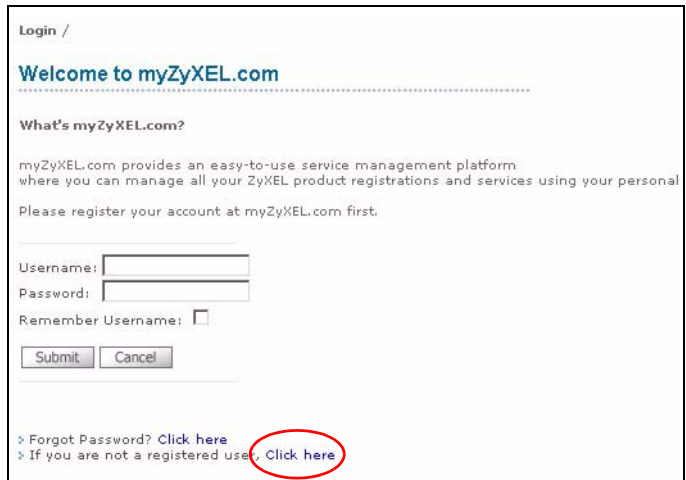


9 Enregistrement du produit sur myZyXEL.com

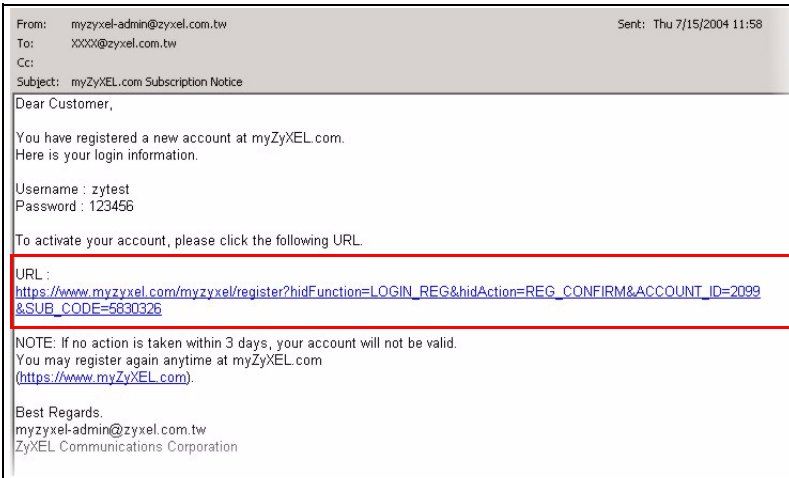
myZyXEL.com est le centre de services en ligne de ZyXEL où vous pouvez enregistrer votre matériel ZyXEL.

- 1 Allez à myZyXEL.com à l'aide de votre navigateur web.
- 2 Créez un nouveau compte (si vous n'en avez pas déjà un).

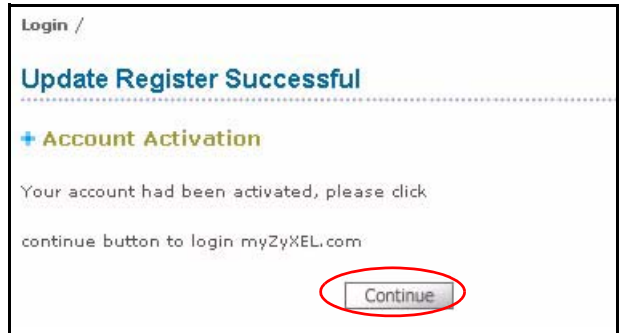
Remarque: Vous êtes automatiquement déconnecté de votre compte myZyXEL.com au bout de cinq minutes d'inactivité. Réouvrez simplement une session dans votre compte myZyXEL.com si cela vous arrive.



3 Après avoir créé un compte, vous recevrez un e-mail de confirmation. Cliquez sur l'URL dans l'e-mail pour activer votre compte.



4 Cliquez sur **Continuer** pour aller à l'écran de connexion de myZyXEL.com.



- 5 Ouvrez une session.
- 6 Cliquez sur le lien et enregistrez votre matériel ZyXEL.

Welcome /

Welcome

Welcome! **Cindy Yang**

You have logged in myZyXEL.com for 1 times.

- > Last Viewed
- * IP:
- * Viewed Date:
- * Viewed time: (GMT+8:00)Taipei

Registered ZyXEL Products

[Click here](#) to register product

Note:
Currently, this registration website <http://www.myzyxel.com> supports Vantage CNM 2.0 and ZyXEL products service activation. For other products support, we will announce soon in our next release.

[More](#)

- 7 Cliquez sur **Ajouter**.

My Products / Product Registration

Product Registration

Registered Product List

Your registered ZyXEL products are listed here.

Please click the product name to see more details.

Name	Serial Number
------	---------------

[Add](#)

- 8 Saisissez le numéro de série du produit dans le champ du **numéro de série**.
- 9 Votre numéro de catégorie et de modèle de votre matériel s'affiche automatiquement dans les champs **Catégorie** et **Modèle** respectivement. Sinon, sélectionnez les bons dans les boîtes de listes déroulantes.
- 10 Entrez l'adresse MAC du matériel dans le champ **Code d'authentification** (il est peut-être déjà affiché).
- 11 Entrez un nom de description dans le champ **Nom convivial** pour les besoins d'identification.
- 12 Cliquez sur **Enregistrer**.
- 13 Spécifiez les informations d'achat et cliquez sur **Continuer**.
- 14 Cliquez à nouveau sur **Continuer** pour terminer le processus.

Add New Product

Add New Product

To add a new product, please fill in the following fields.
Friendly Name is an alias you give the product to identify it in the product list.

marked by (*) are Required

* Serial Number:	Please enter the 10-digit number of the label on the unit. (Upper Case)
<input type="text"/>	
* Category:	
<input type="text" value="-- Select --"/>	
* Model:	Please select your correct category and model. You can find it by your case.
<input type="text" value="-- Select --"/>	
* Authentication Code:	> For hardware products, this is the physical MAC address. > For software products, this is a generated number that is displayed after you ins (Upper Case)
<input type="text"/>	
* Friendly Name:	Please give a name easy to remember for you. Up to 30 characters. It may conta underscore character, other character are not allowed.
<input type="text"/>	

My Products / Product Registration

Product Survey

Product Information

+ Purchase date

+ You purchased this product from

15Après avoir enregistré votre matériel ZyXEL, vous pouvez visualiser ses informations d'enregistrement dans l'écran de **gestion de service**.

Le matériel ZyXEL est maintenant enregistré, mais le filtrage de contenu n'est pas activé. Pour activer le filtrage de contenu, vous devez accéder à myZyXEL.com via votre matériel. Continuer par la section suivante.

My Products / Service Activation

Service Management

Product Information

zy70cf
 Serial Number: S42Z928704
 Products: ZyWALL 70
 Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

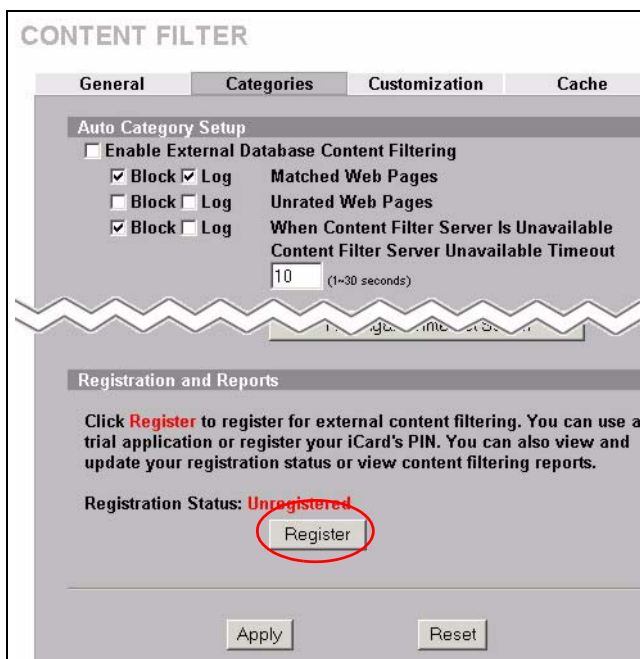
	Service Name	Service Activation	Status	Expiry Date	Remark
1	Content Filter	Activate	-	-	-

10 Filtrage du contenu à partir d'une base données externe

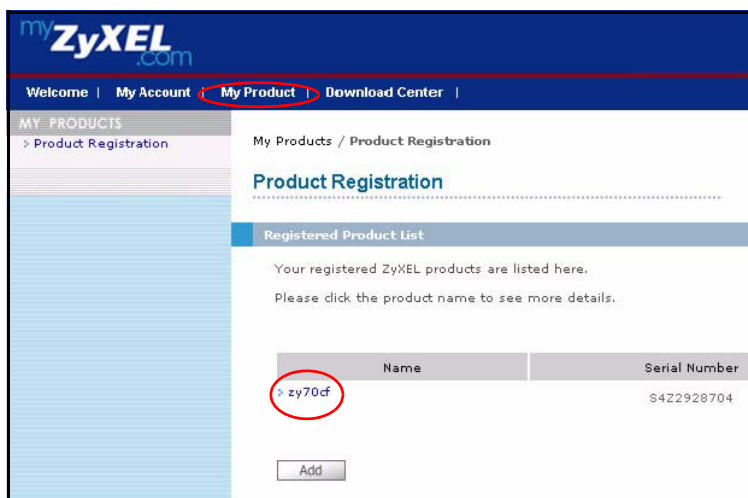
Quand vous enregistrez et que vous activez un filtrage de contenu à partir d'une base données externe, votre ZyWALL accède à une base de données externe ayant des millions de sites web classés par catégories suivant leur contenu. Le ZyWALL peut bloquer et/ou accéder aux sites web en fonction de ces catégories. Enregistrez votre ZyWALL à myZyXEL.com (voir [la Section 9](#) et procédez comme suit pour inscrire à un filtrage de contenu à partir d'une base données externe.

- 1 Dans le configurateur web de votre matériel ZyXEL, cliquez sur **FILTRE DE CONTENU** (CONTENT FILTER), **Catégories** et ensuite sur le bouton **Enregistrer**.

Remarque: Vous devez aussi utiliser les écrans **FILTRE DE CONTENU** (CONTENT FILTER) du configurateur web du ZyWALL pour configurer et activer le filtrage de contenu.



- 2 L'écran de connexion de myZyXEL.com s'ouvre.
- 3 Entrez le nom d'utilisateur et le mot de passe de votre compte myZyXEL.com.
- 4 Cliquez **Mon Produit** dans le panneau de navigation.
- 5 Cliquez sur le lien du nom du produit pour votre matériel pour voir ses informations d'enregistrement dans l'écran de **Gestion de Service**.



6 Cliquez sur **Activer** pour le service de filtrage de contenu pour afficher l'écran suivant.

My Products / Service Activation

Service Management

Product Information

zy70cf

Serial Number: S4Z2928704
 Products: ZyWALL 70
 Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

> zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

	Service Name	Service Activation	Status	Expiry Date
1	Content Filter	Activate	-	-

7 Si vous voulez utiliser l'évaluation, cliquez sur **Envoyer** sous **Evaluation du filtrage de contenu**. La période d'évaluation commence à la date à laquelle vous vous inscrivez.

Vous ne pouvez pas vous inscrire à une évaluation si vous avez déjà utilisé une évaluation ou enregistré un numéro PIN d'iCard.

Si vous avez acheté une iCard, entrez le code PIN exactement comme indiqué sur votre iCard dans le champ **Clé de Licence** (code PIN). Sélectionnez la date quand vous voulez que votre filtrage de contenu commence et cliquez sur **Envoyer** sous **Informations d'enregistrement**.

My Products / Service Activation

Content Filtering Trial

We offer 30-day free trial for content filtering service.
 If you would like to have a try, please click "submit".

Registration Information

1. Enter the License Key (PIN code) exactly as shown in your iCard.
2. Content filtering begins from the activation date.

> License Key (PIN code) :

> Activation Date : - -

- 8 Un écran apparaît vous indiquant que le service est enregistré. Cliquez sur **Continuer** pour aller à l'écran de **Gestion de Service**.

My Products / Service Activation

Apply Standard Version Successful

Your E-mail Address : stanley_king@gfortunenet.com

Effective Period : 2004/07/31 ~ 2005/07/31

Your Name : stanley

Your Region : Taiwan

- 9 Si vous utilisez actuellement une version d'évaluation, vous pouvez quand même enregistrer le code PIN à partir d'une iCard en cliquant sur **Mise à niveau** dans le champ **Activation du Service** de l'écran **Gestion du Service**.

My Products / Service Activation

Service Management

Product Information

zy70cf

Serial Number: S4Z2928704
Products: ZyWALL 70
Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

> zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

	Service Name	Service Activation	Status	Expiry Date	Remark
1	Content Filter	<input type="button" value="Upgrade"/>	Installed	2004-09-02	Refresh

11 Dépannage

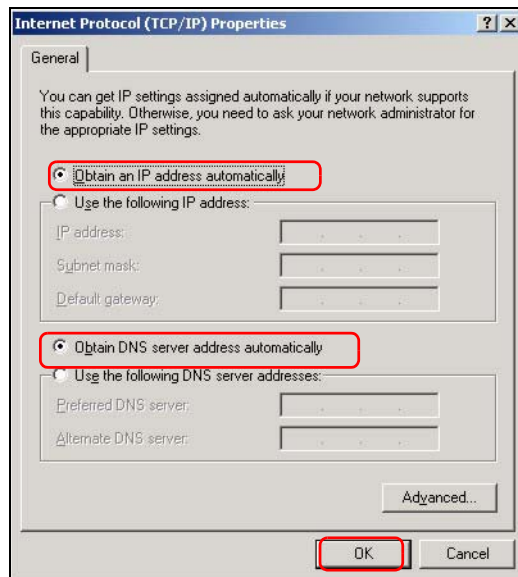
problème	ACTION CORRECTIVE
Aucune LED ne s'allume.	Vérifiez que votre cordon d'alimentation est connecté au ZyWALL et branché dans une prise de courant appropriée. Vérifiez que le ZyWALL est allumé. Vérifiez toutes les connexions câblées.
	Si les LED ne s'allument toujours pas, cela signifie que vous avez peut-être un problème matériel. Dans ce cas-là, vous devez contacter votre revendeur local.
Impossible d'accéder au ZyWALL à partir du LAN.	Vérifiez la connexion câblée entre le ZyWALL et votre ordinateur ou hub. Reportez-vous à la Section 1 pour les détails.
	Envoyez un signal Ping au ZyWALL à partir d'un ordinateur du LAN. Vérifiez que la carte Ethernet de votre ordinateur est installée et fonctionne correctement.
	Dans l'ordinateur, cliquez sur Démarrer, (Tous) Programmes, Accessoires et ensuite sur Invite de Commande . Dans la fenêtre Invite de Commande , tapez "ping" suivi de l'adresse IP LAN du ZyWALL (192.168.1.1 est l'adresse par défaut) et appuyez ensuite sur [ENTER]. Le ZyWALL devrait répondre. Sinon, reportez-vous à la Section 11.1 .
	Si vous avez oublié le mot de passe du ZyWALL, utilisez le bouton RESET . Appuyez sur le bouton pendant environ 10 secondes (jusqu'à ce que la LED PWR commence à clignoter), puis relâchez-le. Cela rétablit le ZyWALL à ses paramètres par défaut d'usine (le mot de passe est 1234, adresse IP LAN 192.168.1.1 etc.; voir votre Guide de l'utilisateur pour les détails).
	Si vous avez oublié l'adresse IP LAN ou WAN du ZyWALL, vous pouvez vérifier l'adresse IP dans le SMT via le port de la console. Connectez votre ordinateur au port CONSOLE à l'aide d'un câble de console. Votre ordinateur doit avoir un programme de communication d'émulation de terminal (tel qu'HyperTerminal) paramétré sur l'émulation de terminal VT100, pas de parité, 8 bits de données, 1 bit de stop, pas de contrôle de flux et une vitesse de port de 9600 bps.
Impossible d'accéder à Internet.	Vérifiez la connexion du ZyWALL à la prise Ethernet avec l'accès Internet. Vérifiez que le périphérique de passerelle Internet (tel qu'un modem DSL) fonctionne correctement.
	Cliquez sur WAN dans le panneau de navigation pour vérifier vos paramètres.
Impossible d'établir une connexion VPN	Vérifiez que le ZyWALL et le routeur IPsec distant utilise les mêmes paramètres VPN. Cliquez sur VPN dans le panneau de navigation pour configurer les paramètres avancés.
	Accédez à un site web pour vérifier que vous avez une connexion Internet qui fonctionne.

11.1 Paramétrez l'adresse IP de votre ordinateur

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

1 Dans Windows XP, cliquez sur **Démarrer, Panneau de configuration**.

- Dans Windows 2000/NT, cliquez sur **Démarrer, Paramètres, Panneau de configuration**.
- 2 Dans Windows XP, cliquez sur **Connexion réseau**.
Dans Windows 2000/NT, cliquez sur **Connexions réseau et accès à distance**.
 - 3 Cliquez avec le bouton droit de la souris sur **Connexion de réseau local** et cliquez sur **Propriétés**.
 - 4 Sélectionnez **Protocole Internet (TCP/IP)** (dans l'onglet **Général** dans Windows XP) et cliquez sur **Propriétés**.
 - 5 L'écran de **Propriétés TCP/IP de protocole Internet** s'ouvre (**onglet Général** dans Windows XP). Sélectionnez les options **Obtenir automatiquement une adresse IP** et **Obtenir automatiquement une adresse de serveur DNS**.
 - 6 Cliquez sur **OK** pour fermer la fenêtre de **Propriétés (TCP/IP) de protocole Internet**.
 - 7 Cliquez sur **Fermer (OK** dans Windows 2000/NT) pour fermer la fenêtre de **Propriétés de connexion au réseau local**.
 - 8 Fermez l'écran de **Connexion réseau**.



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

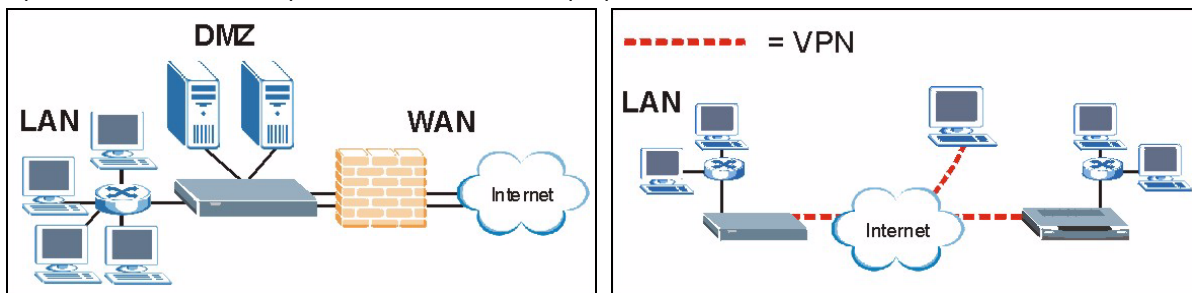
- 1 Allez à www.zyxel.com.
- 2 Sélectionnez votre produit dans la boîte de la liste déroulante dans la page d'accueil de ZyXEL pour aller à la page de ce produit.
- 3 Sélectionnez la certification que vous désirez consulter dans cette page.

Cenni generali

ZyWALL 70 è un firewall con funzionalità di Load Balancing, a doppia WAN, 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. ZyWALL aumenta la sicurezza della rete offrendo porte DMZ da utilizzare per 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 | 7 Firewall |
| 2 Accesso allo strumento di configurazione Web | 8 Configurazione delle regole di VPN |
| 3 Modalità Bridge | 9 Registrazione del prodotto su myZyXEL.com |
| 4 Configurazione dell'accesso a Internet | 10 Filtraggio dei contenuti mediante database esterno |
| 5 DNS | 11 Risoluzione dei problemi |
| 6 NAT | |

1 Collegamenti hardware

È necessario disporre dei seguenti componenti:

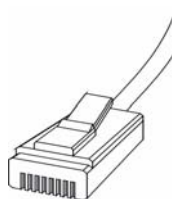
ZyWALL



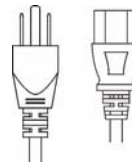
Computer



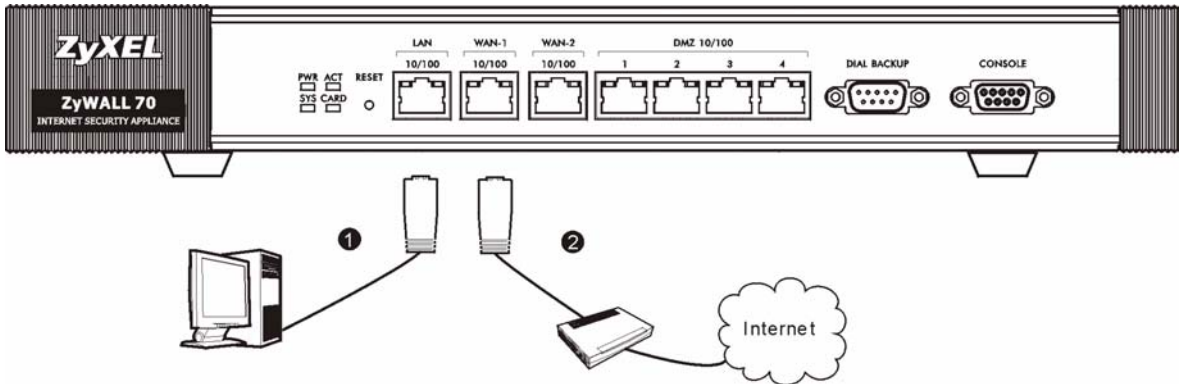
Cavi Ethernet



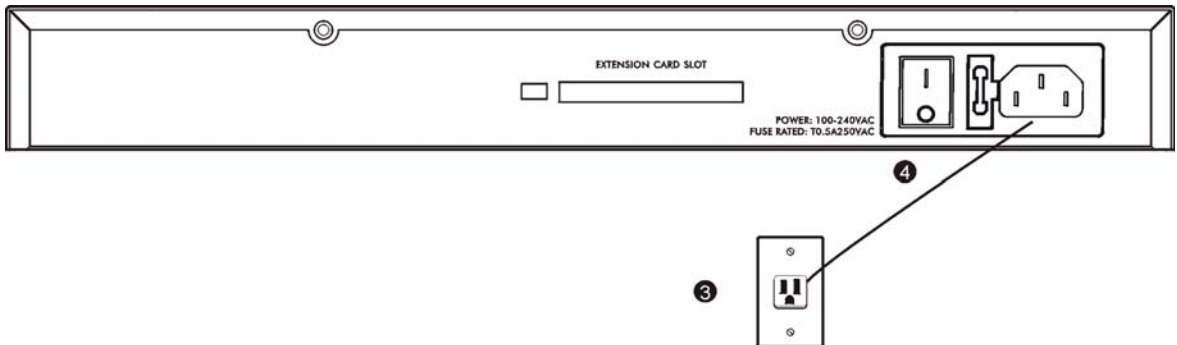
Cavo di alimentazione



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



- 1 Utilizzare un cavo Ethernet per collegare la porta **LAN** a un computer. È possibile utilizzare cavi Ethernet anche per collegare server pubblici (Web, E-mail, FTP, ecc.) alle porte **DMZ**.
- 2 Utilizzare altri cavi Ethernet per collegare la porta **WAN 1** e/o **WAN 2** a un jack Ethernet con accesso a Internet.

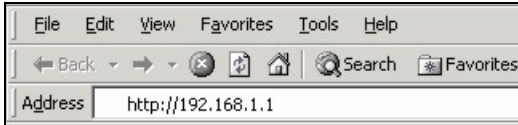


- 3 Utilizzare il cavo di alimentazione fornito a corredo per collegare la presa di alimentazione (situata dietro all'apparecchio) a una presa elettrica.
- 4 Posizionare l'interruttore di accensione sulla posizione **ACCESO** e analizzare il pannello frontale. Il **LED PWR** si accende. Il **LED SYS** lampeggia mentre viene eseguito il test del sistema e quindi resta acceso in caso di test riuscito. I **LED ACT, CARD, LAN, DMZ** e **WAN** si accendono e restano accesi se i corrispondenti collegamenti sono stati eseguiti correttamente.

2 Accesso allo strumento di configurazione Web

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

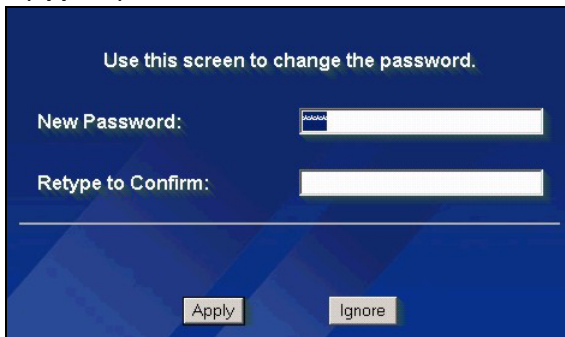
- 1 Avviare il browser. Immettere **192.168.1.1** (l'indirizzo IP predefinito dello ZyWALL) nella barra dell'indirizzo.
Se non viene visualizzata la schermata di accesso, vedere [Sezione 11.1](#) per impostare l'indirizzo IP del proprio computer.



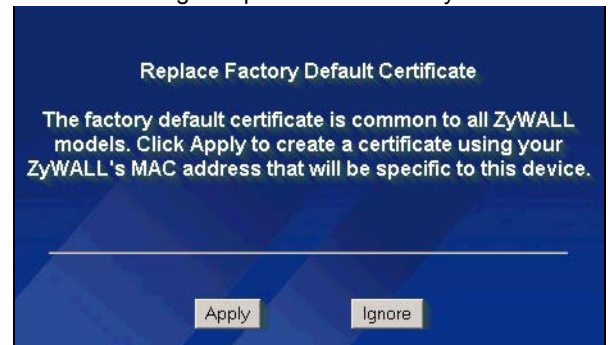
- 2 Fare clic su **Login** (accedi)(la password predefinita 1234 è già immessa).



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



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



- 5 Si apre la schermata **HOME**.

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

Passare a [Sezione 3](#) se si preferisce utilizzare lo ZyWALL come firewall trasparente.

6 Controllare la tabella **Network Status** (stato della rete). Se lo stato della **WAN 1** è **not Down** (non disattivata) ed è presente un indirizzo IP, passare a [Sezione 5](#).

Se lo stato della **WAN 1** è **Down** (disattivata) (oppure se non è presente un indirizzo IP), fare clic su **Internet Access** (accesso a Internet) e utilizzare [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 porte WAN.

ZyXEL HOME HELP ?

HOME

NETWORK
LAN
WIRELESS LAN
WAN
DMZ

SECURITY
FIREWALL
CONTENT FILTER
VPN
CERTIFICATES
AUTH SERVER

ADVANCED
NAT
STATIC ROUTE
POLICY ROUTE
BW MGMT
DNS
REMOTE MGMT
UPnP

LOGS

MAINTENANCE

LOGOUT

Wizards for WAN 1 Quick Setup

Internet Access VPN

Device Information

System Name:

Firmware Version: V3.64(WM.0)b1 | 12/17/2004

Routing Protocol: IP

Device Mode: Router

Firewall: Enabled

System Time: 2005-01-11 08:27:37 GMT

Memory: 14358K/19473K

Sessions: 5/10000

Policy

Routes: 0/48

Network Status

Interface	Status	IP Address	Subnet Mask	DHCP	Renew
WAN 1	Down	0.0.0.0	0.0.0.0	Client	Renew
WAN 2	Down	0.0.0.0	0.0.0.0	Client	Renew

Status: Ready

3 Modalità Bridge

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

- 1 Fare clic su **MAINTENANCE** (manutenzione) nel pannello di navigazione, quindi su **Device Mode** (modalità dispositivo).
- 2 Selezionare **Bridge** e immettere un indirizzo IP (statico), una subnet mask e un indirizzo IP del gateway per le interfacce **LAN, WAN, DMZ** e **WLAN** dello ZyWALL.
- 3 Fare clic su **Apply** (applica). Lo ZyWALL si riavvia.

Passare a [Sezione 5](#) se si dispone di server che occorre rendere accessibili dalla WAN.

MAINTENANCE

General	Password	Time and Date	Device Mode	F/W Upload	Configuration	Restart
---------	----------	---------------	-------------	------------	---------------	---------

Current Device Mode

Device Mode: Router

Device Mode Setup

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

Router

IP Address: (See [LAN](#), [WAN](#) and [DMZ](#))

Bridge

IP Address:

IP Subnet Mask:

Gateway IP Address:

4 Configurazione dell'accesso 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.

Nota: 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 **Finish (fine)** una volta terminata la configurazione.

- **Incapsulamento Ethernet**

Configurare un servizio Roadrunner nelle schermate **NETWORK WAN (WAN di rete)** (utilizzare la scheda **WAN 1**).

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)**.

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

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

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).

Differentemente dalla LAN, lo ZyWALL non assegna una configurazione TCP/IP via DHCP ai computer connessi alle porte DMZ. 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.

Nota: Non è necessario configurare la DMZ con la modalità bridge; passare a [Sezione 7](#).

- 1 Fare clic su **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).

The screenshot shows the DMZ configuration window. The 'DMZ' tab is selected, and the 'IP Alias' sub-tab is active. The 'DMZ TCP/IP' section contains the following settings:

- IP Address: 10 . 0 . 0 . 1
- IP Subnet Mask: 255 . 0 . 0 . 0
- RIP Direction: Both
- RIP Version: RIP-1
- Multicast: None

The 'Windows Networking (NetBIOS over TCP/IP)' section contains two checkboxes:

- Allow between DMZ and LAN (You also need to create a firewall rule!)
- Allow between DMZ and WAN

At the bottom of the window, there are two buttons: 'Apply' and 'Reset'.

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 WAN a un server HTTP (Web) sulla DMZ. L'indirizzo IP privato del server è 10.0.0.20.

- 1 Fare clic su **NAT** nel pannello di navigazione, quindi su **Port Forwarding (inoltro delle porte)**.
- 2 Selezionare la casella di controllo **Active (attiva)**.
- 3 Digitare un nome per la regola.
- 4 Digitare il numero di porta utilizzata dal servizio.
- 5 Digitare l'indirizzo IP del server HTTP.
- 6 Fare clic su **Apply (applica)**.

NAT

NAT Overview
Address Mapping
Port Forwarding
Port Triggering

Port Forwarding Rules

WAN Interface WAN 1

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
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 Firewall

È possibile utilizzare lo ZyWALL senza dover configurare il firewall.

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

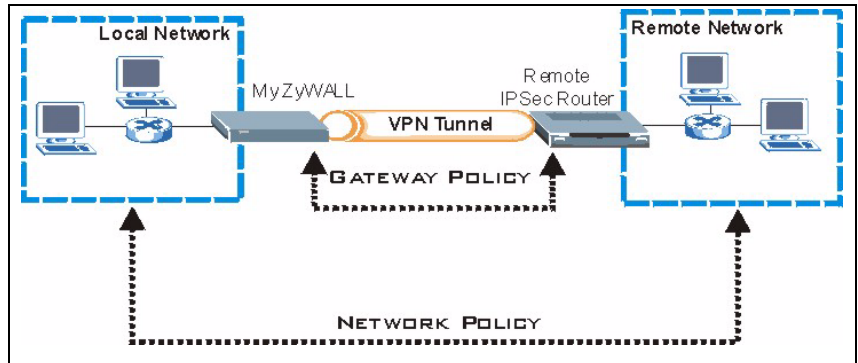
Se si utilizza lo ZyWALL in modalità router, continuare con la prossima sezione. Per la modalità bridge, passare a [Sezione 9](#).

8 Configurazione delle regole di VPN

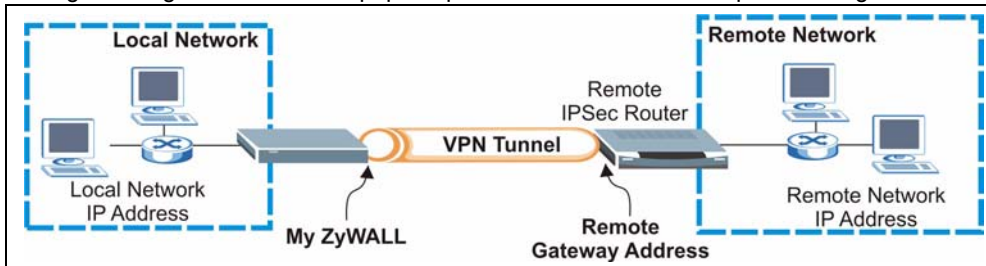
Un tunnel VPN (Virtual Private Network, rete privata virtuale) offre una connessione sicura a un altro computer o rete.

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

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



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



- 1 Per aprire la procedura guidata di impostazione della VPN, fare clic su **VPN** nella schermata **HOME** (potrebbe essere necessario scorrere la pagina per vedere il collegamento).

Nota: 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.

Gateway Policy Property

Name

Gateway Policy Setting

My ZyWALL

Remote Gateway Address

Next

3 Utilizzare questa schermata per configurare il criterio di rete.

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

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

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

Selezionare **Range IP (IP della gamma)** e immettere gli indirizzo IP iniziale 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.

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

Back Next

Nota: 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.

Nota: 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 'IKE Tunnel Setting (IKE Phase 1)' window. It contains the following configuration options:

- 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 Utilizzare questa schermata per configurare le impostazioni IPSec.

The screenshot shows the 'IPSec Setting (IKE Phase 2)' window. It contains the following configuration options:

- 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 Secret (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.

Status	
Gateway Policy Setting	
My ZyWALL	0.0.0.0
Remote Gateway Address	BranchOffice.com
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)	
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 Secret (PFS)	NONE
<input type="button" value="Back"/> <input type="button" value="Finish"/>	

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.

<p>Congratulations. The VPN wizard configuration is complete. Check our exciting range of ZyXEL products at http://www.zyxel.com</p> <p>Having VPN access problems?</p> <ol style="list-style-type: none"> 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. <p style="text-align: center;"><input type="button" value="Close"/></p>

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 **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”).

The screenshot shows the 'SA Monitor' tab in the VPN configuration interface. It displays a 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 / 255.0.0.0	Tunnel	ESP DES-SHA1

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

9 Registrazione del prodotto su myZyXEL.com

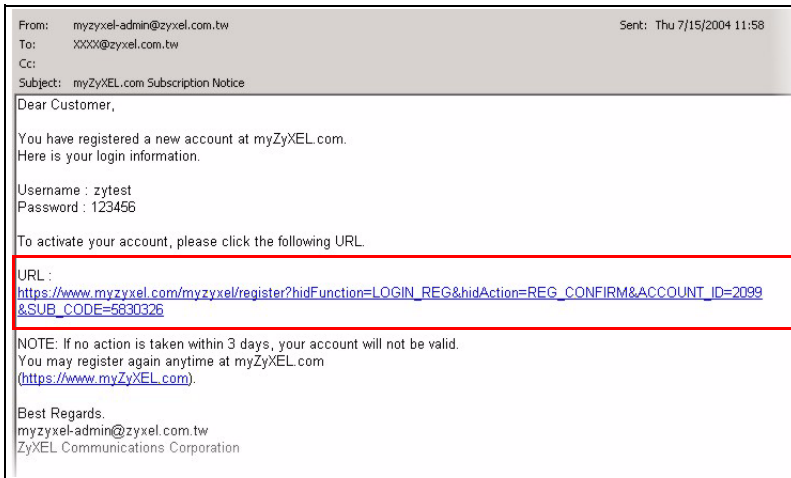
myZyXEL.com è un centro servizi online di ZyXEL dove l'utente può registrare il proprio dispositivo ZyXEL.

- 1 Aprire myZyXEL.com utilizzando il browser.
- 2 Creare un nuovo account (se non se ne ha già uno).

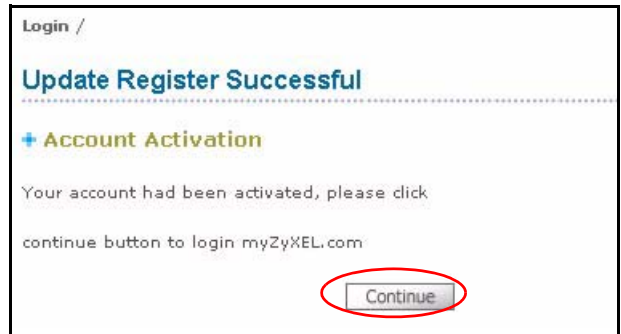
Nota: L'account su myZyXEL.com viene automaticamente disconnesso dopo cinque minuti di inattività. Se ciò accade è sufficiente eseguire nuovamente l'accesso a myZyXEL.com.

The screenshot shows the login page for myZyXEL.com. It includes a 'Login /' header, a 'Welcome to myZyXEL.com' message, and a 'What's myZyXEL.com?' section. Below this is a registration prompt: 'myZyXEL.com provides an easy-to-use service management platform where you can manage all your ZyXEL product registrations and services using your personal information. Please register your account at myZyXEL.com first.' The registration form contains fields for 'Username:' and 'Password:', a 'Remember Username:' checkbox, and 'Submit' and 'Cancel' buttons. At the bottom, there are two links: 'Forgot Password? Click here' and 'If you are not a registered user, Click here', with the latter link circled in red.

3 Dopo aver creato un account, si riceverà una e-mail di conferma. Fare clic sull'URL presente nell'e-mail per attivare l'account.



4 Fare clic su **Continue (continua)** per passare alla schermata di accesso di myZyXEL.com.



- 5 Eseguire l'accesso (login).
- 6 Fare clic sul link e registrare il dispositivo ZyXEL.

Welcome /

Welcome

Welcome! **Cindy Yang**

You have logged in myZyXEL.com for 1 times.

- > Last Viewed
- * IP:
- * Viewed Date:
- * Viewed time: (GMT+8:00)Taipei

Registered ZyXEL Products

[Click here](#) to register product

Note:
Currently, this registration website <http://www.myzyxel.com> supports Vantage CNM 2.0 and ZyXEL products service activation. For other products support, we will announce soon in our next release.

[More](#)

- 7 Fare clic su **Add** (aggiungi).

My Products / Product Registration

Product Registration

Registered Product List

Your registered ZyXEL products are listed here.

Please click the product name to see more details.

Name	Serial Number
------	---------------

[Add](#)

- 8 Immettere il numero di serie del prodotto nel campo **Serial Number (numero di serie)**.
- 9 La categoria del dispositivo e il numero del modello vengono automaticamente visualizzati nei campi **Category (categoria)** e **Model (modello)**, rispettivamente. In caso contrario, selezionare le voci corrette dagli elenchi di riepilogo a discesa.
- 10 Immettere l'indirizzo MAC del dispositivo nel campo **Authentication Code (codice di autenticazione)** (potrebbe già essere visualizzato).
- 11 Immettere un nome descrittivo nel campo **Friendly Name (nome descrittivo)**, a scopo di identificazione.
- 12 Fare clic su **Register (registra)**.
- 13 Specificare le informazioni sull'acquisto e fare clic su **Continue (continua)**.
- 14 Fare nuovamente clic su **Continue (continua)** per completare il processo.

Add New Product

Add New Product

To add a new product, please fill in the following fields.
Friendly Name is an alias you give the product to identify it in the product list.

marked by (*) are Required

* Serial Number:	<input type="text"/>	Please enter the 10-digit number of the label on the unit. (Upper Case)
* Category:	<input type="text" value="-- Select --"/>	
* Model:	<input type="text" value="-- Select --"/>	Please select your correct category and model. You can find it by your case.
* Authentication Code:	<input type="text"/>	> For hardware products, this is the physical MAC address. > For software products, this is a generated number that is displayed after you ins (Upper Case)
* Friendly Name:	<input type="text"/>	Please give a name easy to remember for you. Up to 30 characters. It may conta underscore character, other character are not allowed.

My Products / Product Registration

Product Survey

Product Information

+ Purchase date

+ You purchased this product from

15 Dopo aver registrato il dispositivo ZyXEL, è possibile visualizzare i relativi dettagli di registrazione nella schermata **Service Management (gestione del servizio)**.

Il dispositivo ZyXEL è ora registrato, ma il filtraggio dei contenuti non è attivato. Per attivare il filtraggio dei contenuti è necessario accedere a myZyXEL.com utilizzando il dispositivo stesso. Continuare con la prossima sezione.

My Products / Service Activation

Service Management

Product Information

zy70cf
 Serial Number: S4Z2928704
 Products: ZyWALL 70
 Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

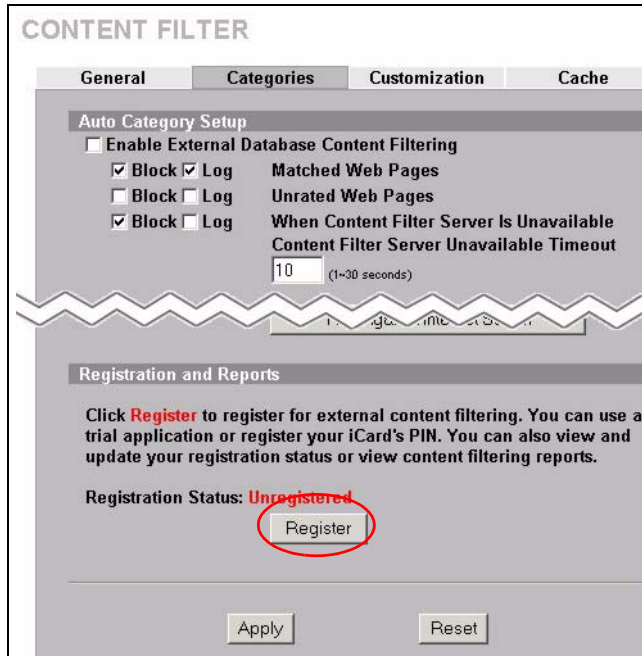
	Service Name	Service Activation	Status	Expiry Date	Remark
1	Content Filter	Activate	-	-	-

10 Filtraggio dei contenuti mediante database esterno

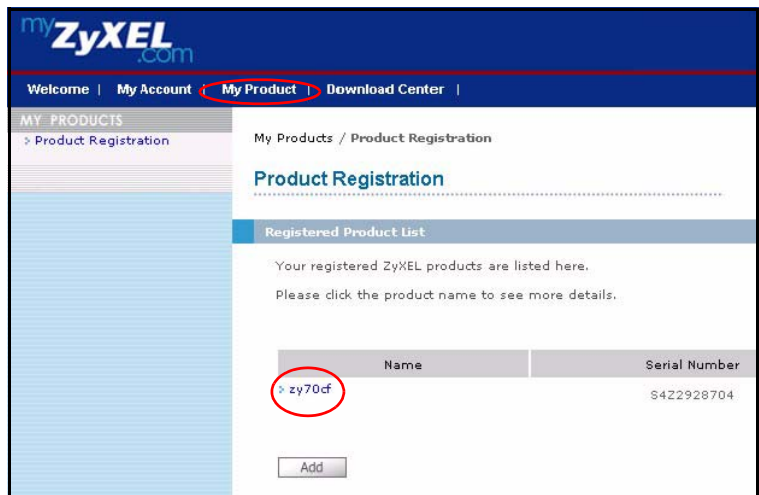
Quando si registra e si attiva il filtraggio dei contenuti mediante database esterno, lo ZyWALL accede a un database esterno contenente milioni di siti Web divisi per categorie sulla base del loro contenuto. È possibile fare in modo che lo ZyWALL blocchi e/o registri l'accesso ai siti Web basandosi su tali categorie. Registrare lo ZyWALL su myZyXEL.com (vedere [Sezione 9](#)), quindi effettuare la seguente registrazione per attivare il filtraggio dei contenuti mediante database esterno.

- 1 Nello strumento di configurazione Web dello ZyXEL, fare clic su **CONTENT FILTER (filtraggio contenuti)**, **Categories (categorie)** e quindi sul pulsante **Register (registra)**.

Nota: Le schermate **CONTENT FILTER (filtraggio contenuti)** dello strumento di configurazione Web dello ZyWALL devono essere utilizzate anche per configurare e attivare il filtraggio dei contenuti.



- 2 Si apre la schermata di accesso a myZyXEL.com.
- 3 Immettere il nome utente e la password dell'account di myZyXEL.com.
- 4 Fare clic su **My Product (il mio prodotto)** nel pannello di navigazione.
- 5 Fare clic sul link del nome del prodotto per visualizzare i dettagli di registrazione del dispositivo nella schermata **Service Management (gestione del servizio)**.



6 Fare clic su **Activate (attiva)** per visualizzare la schermata successiva del servizio di filtraggio dei contenuti.

My Products / Service Activation

Service Management

Product Information

zy70cf

Serial Number: S4Z2928704
 Products: ZyWALL 70
 Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

> zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

	Service Name	Service Activation	Status	Expiry Date
1	Content Filter	<input type="button" value="Activate"/>	-	-

7 Se si desidera utilizzare la versione di valutazione, fare clic su **Submit (invia)** in **Content Filtering Trial (valutazione filtraggio contenuti)**. Il periodo di valutazione inizia dalla data di invio.

Non è possibile avviare una valutazione se si è già effettuata la valutazione o si è eseguita la registrazione di un numero PIN di iCard.

Se si è acquistata una iCard, immettere il codice PIN visibile sulla iCard senza errori nel campo **License Key (chiave di licenza)** (codice PIN). Selezionare la data in cui si desidera che il filtraggio contenuti inizi e fare clic su **Submit (invia)** in **Registration Information (informazioni di registrazione)**.

My Products / Service Activation

Content Filtering Trial

We offer 30-day free trial for content filtering service.
 If you would like to have a try, please click "submit".

Registration Information

1. Enter the License Key (PIN code) exactly as shown in your iCard.
 2. Content filtering begins from the activation date.

> License Key (PIN code) :

> Activation Date : - -

- 8 Appare una schermata che indica che il servizio è stato registrato. Fare clic su **Continue (continua)** per procedere alla schermata **Service Management (gestione del servizio)**.

My Products / Service Activation

Apply Standard Version Successful

Your E-mail Address : stanley_king@gfortunenet.com

Effective Period : 2004/07/31 ~ 2005/07/31

Your Name : stanley

Your Region : Taiwan

- 9 Si sta attualmente utilizzando una versione di valutazione, è ancora possibile registrare il codice PIN di una iCard facendo clic su **Upgrade (aggiorna)** nel campo **Service Activation (attivazione del servizio)** della schermata **Service Management (gestione del servizio)**.

My Products / Service Activation

Service Management

Product Information

zy70cf

Serial Number: S4Z2928704
Products: ZyWALL 70
Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

> zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

	Service Name	Service Activation	Status	Expiry Date	Remark
1	Content Filter	<input type="button" value="Upgrade"/>	Installed	2004-09-02	Refresh

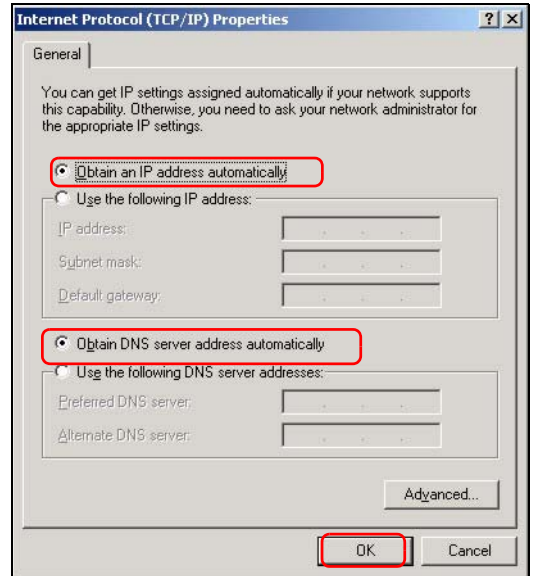
11 Risoluzione dei problemi

Problema	Azione correttiva
Nessuno dei LED è acceso.	Assicurarsi di aver collegato il cavo di alimentazione allo ZyWALL e a una sorgente di alimentazione appropriata. Assicurarsi che lo ZyWALL sia acceso. Controllare tutti i collegamenti dei cavi.
	Se i LED continuano a non accendersi, potrebbe esserci un guasto hardware. In questo caso, è opportuno rivolgersi al rivenditore locale.
Impossibile accedere allo ZyWALL dalla LAN.	Controllare il collegamento dei cavi tra lo ZyWALL e il computer o l'hub. Vedere Sezione 1 per i dettagli.
	Eseguire il ping dello ZyWALL da un computer della LAN., Assicurarsi che la scheda Ethernet del computer sia installata e correttamente funzionante. Nel computer, fare clic su Start, (Tutti i) Programmi, Accessori e quindi Prompt dei comandi . Nella finestra Prompt dei comandi , digitare "ping" seguito dall'indirizzo IP LAN dello ZyWALL (192.168.1.1 è l'indirizzo predefinito) e quindi premere [Invio]. Lo ZyWALL dovrebbe rispondere. In caso contrario, vedere Sezione 11.1 .
	Se si è dimenticata la password dello ZyWALL, utilizzare il pulsante RESET . Premere il pulsante per circa 10 secondi (oppure finché il LED PWR non inizia a lampeggiare), quindi rilasciarlo. Questa operazione riporta lo ZyWALL ai valori predefiniti (la password è 1234, l'indirizzo IP LAN è 192.168.1.1, e così via; vedere la Guida dell'utente per i dettagli).
	Se si dimentica l'indirizzo IP della WAN o della LAN dello ZyWALL, è possibile controllare l'indirizzo IP nello SMT via porta console. Collegare il computer alla porta CONSOLE utilizzando un cavo console. Il computer dovrebbe disporre di un programma di comunicazione di emulazione terminale (come ad esempio HyperTerminal); impostare l'emulazione di terminale VT100, nessuna parità, 8 bit di dati, 1 bit di stop, nessun controllo di flusso e velocità della porta pari a 9600 bps.
Impossibile accedere a Internet.	Controllare il collegamento dello ZyWALL al jack Ethernet con accesso a Internet. Assicurarsi che il dispositivo gateway verso Internet (quale ad esempio un modem DSL) funzioni correttamente.
	Fare clic su WAN nel pannello di navigazione per verificare le impostazioni.
Impossibile stabilire una connessione VPN	Assicurarsi lo ZyWALL e il router IPsec remoto utilizzi le stesse impostazioni VPN. Fare clic su VPN nel pannello di navigazione per configurare le impostazioni avanzate.
	Accedere a un sito Web per verificare che si dispone di una connessione a Internet valida.

11.1 Impostare l'indirizzo IP del computer

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

- 1 In Windows XP, fare clic su **Start, Pannello di controllo**.
In Windows 2000/NT, fare clic su **Start, Impostazioni, Pannello di controllo**.
- 2 In Windows XP, fare clic su **Connessioni di rete**.
In Windows 2000/NT, fare clic su **Reti e connessioni remote**.
- 3 Fare clic con il pulsante destro del mouse su **Connessione alla rete locale** e scegliere **Proprietà**.
- 4 Selezionare **Protocollo Internet (TCP/IP)** (sotto la scheda **Generale** in Windows XP) e fare clic su **Proprietà**.
- 5 Si apre la schermata **Protocollo Internet TCP/IP - Proprietà** (la scheda **Generale** in Windows XP). Selezionare le opzioni **Otteni automaticamente un indirizzo IP** e **Otteni 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**.



11.2 Procedura per visualizzare le certificazioni di un prodotto

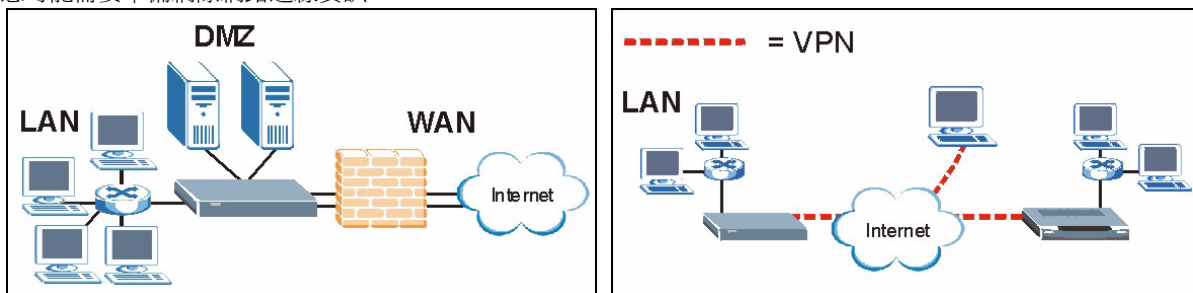
- 1 Aprire la pagina www.zyxel.com.
- 2 Selezionare il prodotto dall'elenco di riepilogo a discesa nella Home Page di ZyXEL per passare alla pagina del prodotto in questione.
- 3 Selezionare da questa pagina la certificazione che si desidera visualizzare.

概觀

ZyWALL 70 是負載平衡的雙 WAN 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 70 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。ZyWALL 提供公用存取伺服器使用的 DMZ 連接埠，更增加了網路的安全性。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、如下。

- | | |
|--------------|--------------------|
| 1 硬體連線 | 7 防火牆 |
| 2 存取網路組態設定程式 | 8 VPN 規則設定 |
| 3 橋接模式 | 9 myZyXEL.com 產品註冊 |
| 4 網際網路存取設定 | 10 外部資料庫內容過濾 |
| 5 DNS | 11 疑難排解 |
| 6 NAT | |

1 硬體連線

您需要以下裝備。

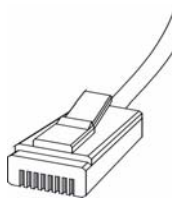
ZyWALL



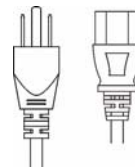
電腦



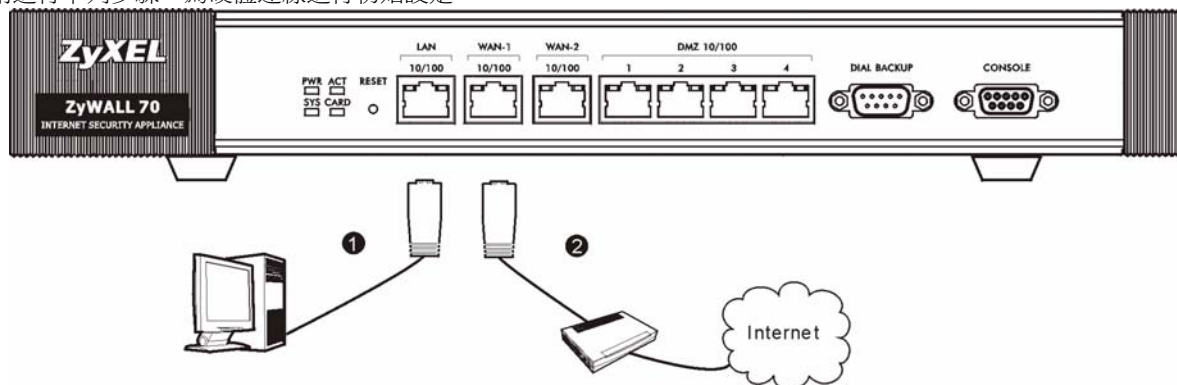
乙太網路線



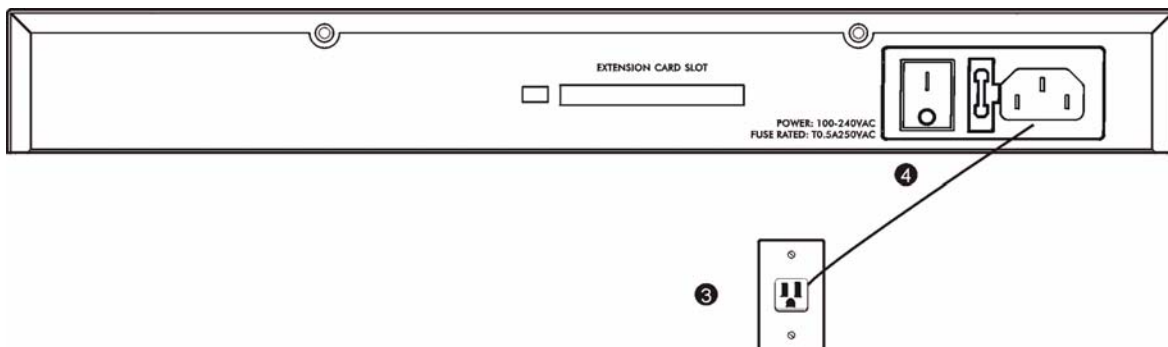
電源線



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 連接埠和電腦。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 DMZ 連接埠。
- 2 使用另一條乙太網路線，將 WAN 1 和 / 或 WAN 2 連接埠連接到可以存取網際網路的乙太網路插孔。

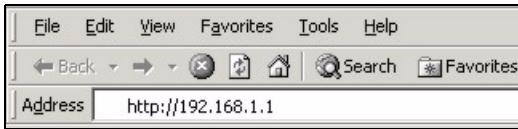


- 3 使用所附的電源線，為電源插槽（位於後方面板）接上電源。
- 4 將電源開關打開，並觀察前方面板。PWR LED 指示燈會亮起。SYS LED 指示燈會在執行系統測試時閃爍，測試成功時燈光會持續亮著。ACT、CARD、LAN、DMZ 和 WAN LED 指示燈會在相關連接正確時亮起並持續亮著。

2 存取網路組態設定程式

您可以使用本節中的資訊設定 **WAN 1** 介面的網際網路存取。

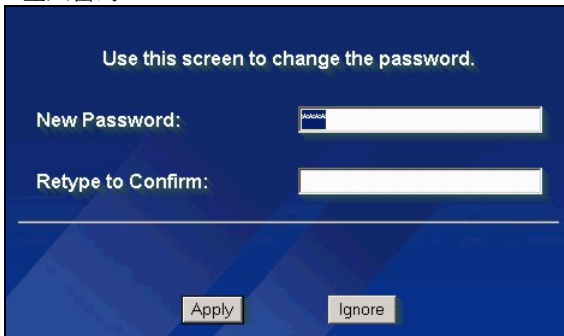
- 1 啟動網頁瀏覽器。輸入位址 **192.168.1.1** (ZyWALL 的預設 IP 位址)。
如果沒有顯示登入畫面，請參閱[章節 11.1](#)，設定電腦的 IP 位址。



- 2 按一下 **Login (登入)** (已經輸入預設的密碼 1234)。



- 3 輸入新的密碼，然後按一下 **Apply (套用)**，變更登入密碼。



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



- 5 會開啓 **HOME** 畫面。

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

如果要將 ZyWALL 做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 (無法運作) (或沒有顯示 IP 位址)，請按一下 **Internet Access** (網際網路存取) 並使用**章節 4** 的資訊設定 WAN 1。

使用 NETWORK WAN 畫面，可以設定 WAN 2。您也可以設定 WAN 連接埠之間的負載平衡。

The screenshot shows the ZyXEL web interface with the following sections:

- HOME**
- NETWORK**
 - LAN
 - WIRELESS LAN
 - WAN
 - DMZ
- SECURITY**
 - FIREWALL
 - CONTENT FILTER
 - VPN
 - CERTIFICATES
 - AUTH SERVER
- ADVANCED**
 - NAT
 - STATIC ROUTE
 - POLICY ROUTE
 - BW MGMT
 - DNS
 - REMOTE MGMT
 - UPnP
- LOGS**
- MAINTENANCE**
- LOGOUT**

The main content area is titled **HOME** and contains:

- Wizards for WAN 1 Quick Setup**
 - Internet Access** (circled in red)
 - VPN
- Device Information**
 - System Name:
 - Firmware Version: V3.64(WM.0)b1 | 12/17/2004
 - Routing Protocol: IP
 - Device Mode: Router
 - Firewall: Enabled
 - System Time: 2005-01-11 08:27:37 GMT
 - Memory: 14358K/19473K
 - Sessions: 5/10000
 - Policy
 - Routes: 0/48
- Network Status**

Interface	Status	IP Address	Subnet Mask	DHCP	Renew
WAN 1	Down	0.0.0.0	0.0.0.0	Client	Renew
WAN 2	Down	0.0.0.0	0.0.0.0	Client	Renew

At the bottom, the status is **Status: Ready**.

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](#)。

MAINTENANCE

General
Password
Time and Date
Device Mode
F/W Upload
Configuration
Restart

Current Device Mode

Device Mode	Router
--------------------	--------

Device Mode Setup

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

Router
 IP Address (See [LAN](#), [WAN](#) and [DMZ](#))

Bridge

IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Gateway IP Address	192 . 168 . 1 . 3

4 網際網路存取設定

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。

注意：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 **Finish (完成)**。

? Ethernet (乙太網路) 封裝

在 NETWORK WAN 畫面中設定 Roadrunner 服務 (使用 WAN 1 標籤)。

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)。

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

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

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。

和 LAN 不同的是, ZyWALL 不會透過 DHCP 將 TCP/IP 設定指派給連接到 DMZ 連接埠的電腦。請使用靜態 IP 位址設定電腦 (DMZ 連接埠的 IP 位址位於同個子網路) 和 DNS 伺服器位址。使用 ZyWALL 的 DMZ IP 位址做為預設閘道。

如果 ZyWALL 處於路由模式, 請進行下列步驟, 設定 DMZ。

注意: 在橋接模式中不需要設定 DMZ, 可以直接跳至[章節 7](#)。

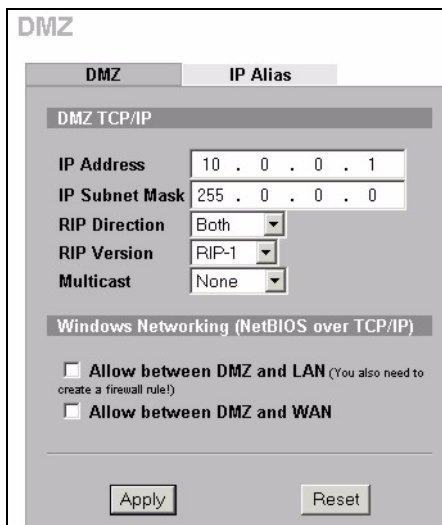
- 1 按一下導覽面板上的 **DMZ**。

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）。



The screenshot shows the DMZ configuration page with the following settings:

DMZ	
DMZ	IP Alias
DMZ TCP/IP	
IP Address	10 . 0 . 0 . 1
IP Subnet Mask	255 . 0 . 0 . 0
RIP Direction	Both
RIP Version	RIP-1
Multicast	None
Windows Networking (NetBIOS over TCP/IP)	
<input type="checkbox"/> Allow between DMZ and LAN (You also need to create a firewall rule!)	
<input type="checkbox"/> Allow between DMZ and WAN	
Apply Reset	

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 WAN 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 **NAT**，然後選取 **Port Forwarding (連接埠轉遞)**。
- 2 選取 **Active (啓用)** 核取方塊。
- 3 輸入規則名稱。
- 4 輸入服務所使用的連接埠號碼。
- 5 輸入 HTTP 伺服器的 IP 位址。
- 6 按一下 **Apply (套用)**。

The screenshot shows the NAT configuration page with the 'Port Forwarding' tab selected. It displays a table of Port Forwarding Rules. The first rule is named 'Web' and is active. The WAN interface is set to 'WAN 1' and the default server IP is '0.0.0.0'. Below the table are two notes and 'Apply' and 'Reset' buttons.

#	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
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.

Buttons: Apply, Reset

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，除非要求先在 LAN 上產生，否則不會有任何傳輸進入 LAN。ZyWALL 會允許從 WAN 或 LAN 存取 DMZ，但會封鎖從 DMZ 到 LAN 的傳輸。

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

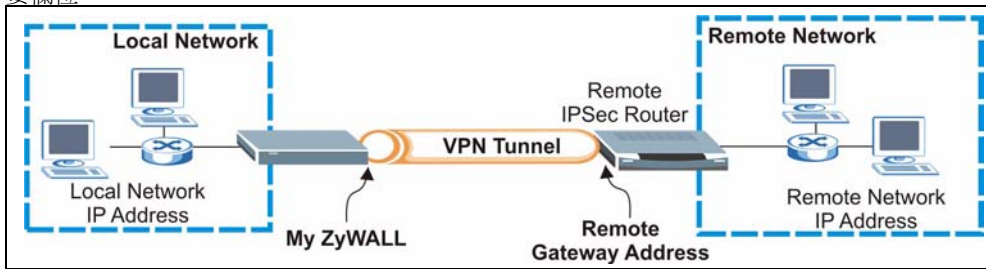
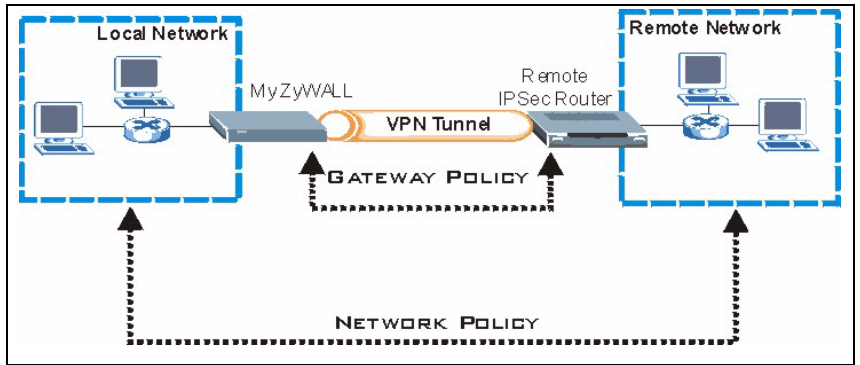
8 VPN 規則設定

VPN（虛擬私有網路）通道可以讓您安全的連線到另一部電腦或網路。

開道原則會辨識 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** 畫面中的 **VPN**（您可能需要向上捲動才能看到連結），開啓 VPN 精靈。

注意： 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)： 為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。



Gateway Policy Property	
Name	Test
Gateway Policy Setting	
My ZyWALL	0.0.0.0
Remote Gateway Address	BranchOffice.com
Next	

3 您可以在這個畫面中設定網路原則。

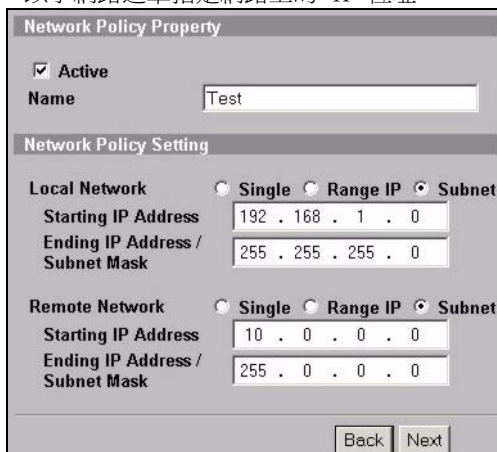
讓 **Active (啓用)** 核取方塊保持選取狀態。

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。



Network Policy Property	
<input checked="" type="checkbox"/> Active	
Name	Test
Network Policy Setting	
Local Network	<input type="radio"/> Single <input type="radio"/> Range IP <input checked="" type="radio"/> Subnet
Starting IP Address	192 . 168 . 1 . 0
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0
Remote Network	<input type="radio"/> Single <input type="radio"/> Range IP <input checked="" type="radio"/> Subnet
Starting IP Address	10 . 0 . 0 . 0
Ending IP Address / Subnet Mask	255 . 0 . 0 . 0
Back Next	

注意：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 (交渉模式)：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。

注意：透過安全性閘道連線的多重 SA (安全性關聯) 必須使用同樣的交渉模式。

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 重新交渉 IKE SA 的頻率 (最低頻率 180 秒)。較短的 SA 時限可以增進安全性，但交渉會暫時中斷 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。

5 您可以在這個畫面中設定 IPSec 設定。

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

Back Next

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 Secret (PFS) None DH1 DH2

Back Next

6 檢查 VPN 設定。按一下 **Finish (完成)** 儲存設定。

Status

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

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)
 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 Secret (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。

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 **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)。

VPN

VPN Rules (IKE) VPN Rules (Manual) SA Monitor Global Setting

Security Associations Table

#	Name	Local Network	Remote Network	Encapsulation	IPSec Algorithm
1	test	192.168.1.0 / 255.255.255.0	10.0.0.0 / 255.0.0.0	Tunnel	ESP DES-SHA1

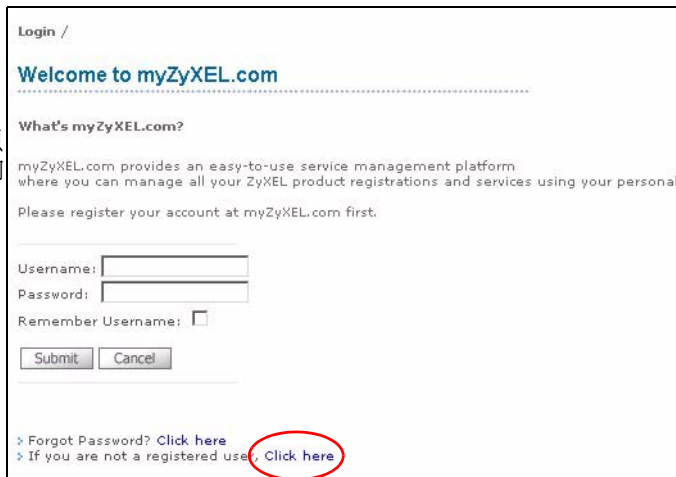
Refresh Disconnect

9 myZyXEL.com 產品註冊

myZyXEL.com 是 ZyXEL 的線上服務中心，您可以在這裡註冊您的 ZyXEL 裝置。

- 1 使用瀏覽器到 myZyXEL.com。
- 2 建立新帳戶（如果還沒有帳戶）。

注意：如果超過 5 分鐘沒有活動，您會自動從 myZyXEL.com 帳戶登出。此時只要重新登入您的 myZyXEL.com 帳戶即可。



Login /

Welcome to myZyXEL.com

What's myZyXEL.com?

myZyXEL.com provides an easy-to-use service management platform where you can manage all your ZyXEL product registrations and services using your personal account.

Please register your account at myZyXEL.com first.

Username:

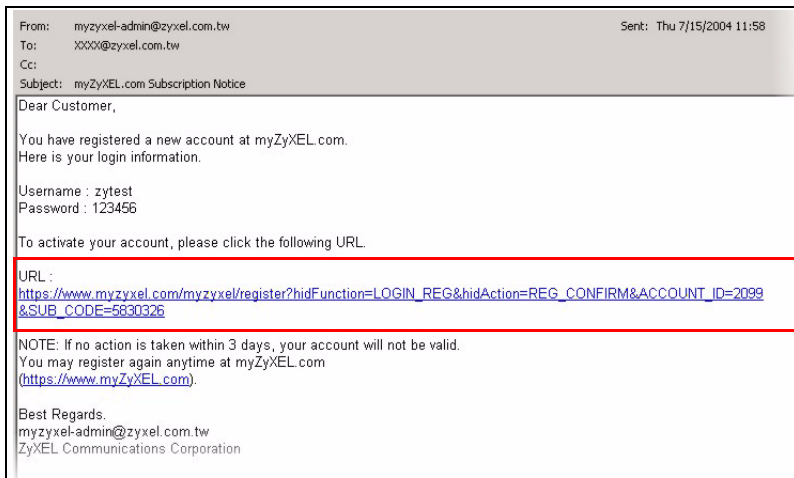
Password:

Remember Username:

> Forgot Password? [Click here](#)

> If you are not a registered user, [Click here](#)

- 3 帳戶建立後，您會收到確認電子郵件。請按一下電子郵件中的 URL，啟用您的帳戶。



From: myzyxel-admin@zyxel.com.tw Sent: Thu 7/15/2004 11:58

To: XXXX@zyxel.com.tw

Cc:

Subject: myZyXEL.com Subscription Notice

Dear Customer,

You have registered a new account at myZyXEL.com.
Here is your login information.

Username : zytest
Password : 123456

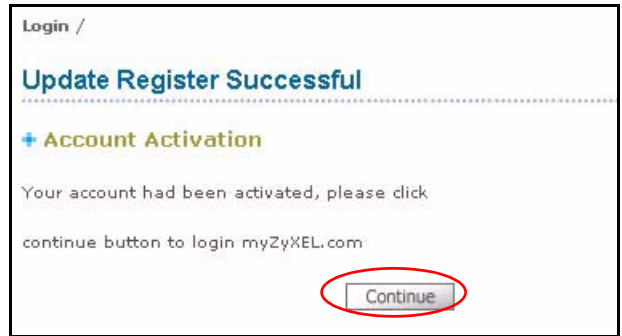
To activate your account, please click the following URL.

URL :
https://www.myzyxel.com/myzyxel/register?hidFunction=LOGIN_REG&hidAction=REG_CONFIRM&ACCOUNT_ID=2099&SUB_CODE=5830326

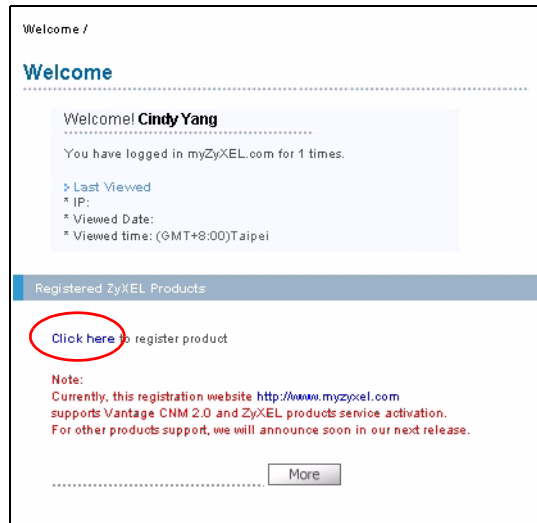
NOTE: If no action is taken within 3 days, your account will not be valid.
You may register again anytime at myZyXEL.com
(<https://www.myZyXEL.com>).

Best Regards,
myzyxel-admin@zyxel.com.tw
ZyXEL Communications Corporation

- 4 按一下 **Continue (繼續)**，會開啓 myZyXEL.com 登入畫面。



- 5 登入帳戶。
6 按一下連結並註冊您的 ZyXEL 裝置。



- 7 按一下 **Add (新增)**。



- 8 在 **Serial Number (序號)** 欄位中輸入產品序號。
- 9 您的裝置類別和型號會自動分別顯示在 **Category (類別)** 和 **Model (型號)** 欄位中。如果沒有顯示，請從下拉式清單方塊中選取正確的類別和型號。
- 10 在 **Authentication Code (驗證碼)** 欄位中輸入裝置的 MAC 位址 (欄位中可能已經顯示這項資訊)。
- 11 在 **Friendly Name (易記名稱)** 欄位中輸入描述性的名稱以方便識別。
- 12 按一下 **Register (註冊)**。

Add New Product

To add a new product, please fill in the following fields.
Friendly Name is an alias you give the product to identify it in the product list.

marked by (*) are Required

* Serial Number: Please enter the 10-digit number of the label on the unit. (Upper Case)

* Category: Please select your correct category and model. You can find it by your case.

* Model:

* Authentication Code: > For hardware products, this is the physical MAC address.
> For software products, this is a generated number that is displayed after you ins (Upper Case)

* Friendly Name: Please give a name easy to remember for you. Up to 30 characters. It may contain underscore character, other character are not allowed.

Register

- 13 填寫購買資訊，然後按一下 **Continue (繼續)**。
- 14 再按一下 **Continue (繼續)**，完成這個程序。

My Products / Product Registration

Product Survey

Product Information

+ Purchase date:

+ You purchased this product from:

Continue

15 為您的 ZyXEL 裝置註冊後，您可以在 **Service Management (服務管理)** 畫面中檢視裝置的註冊資訊。

現在 ZyXEL 裝置已經註冊，但內容過濾功能尚未啟用。要啟用內容過濾功能，您需要透過您的裝置存取 myZyXEL.com。請繼續下一節的步驟。

My Products / Service Activation

Service Management

Product Information

zy70cf
 Serial Number: S422928704
 Products: ZyWALL 70
 Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

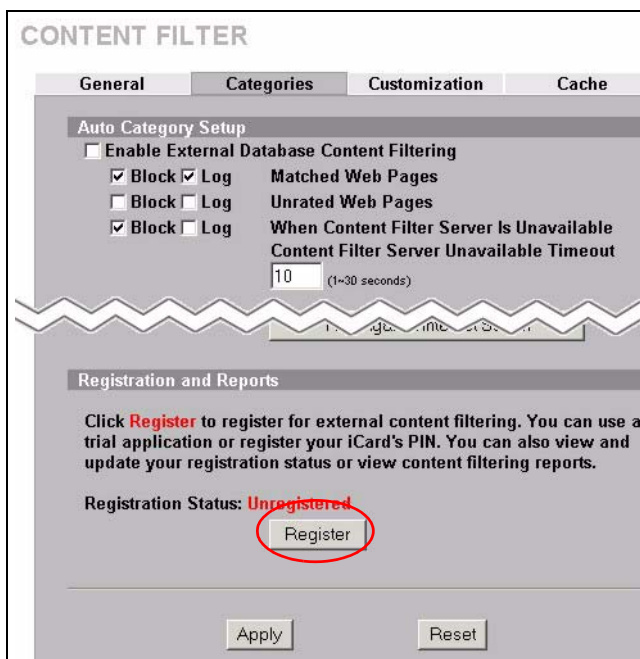
	Service Name	Service Activation	Status	Expiry Date	Remark
1	Content Filter	Activate	-	-	-

10 外部資料庫內容過濾

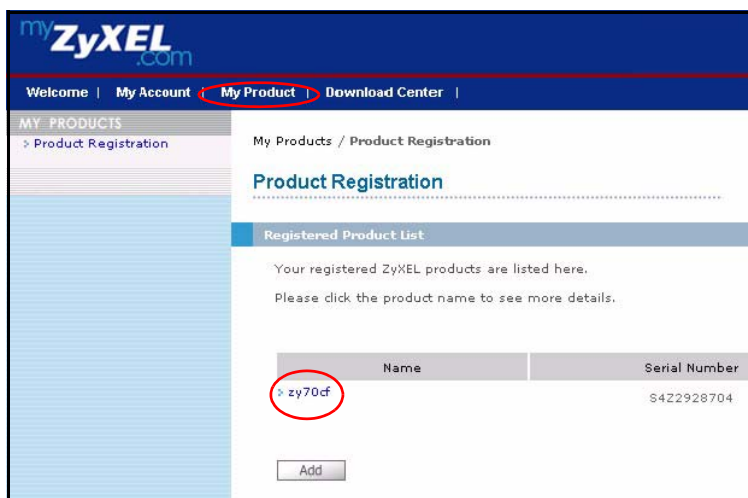
當您註冊並啟用外部資料庫內容過濾時，ZyWALL 會存取依照內容分類數百萬個網站的資料庫。您可以設定 ZyWALL 依照這些類別封鎖和 / 或記錄網站的存取。在 myZyXEL.com 註冊您的 ZyWALL 裝置（請參閱[章節 9](#)），然後進行下列步驟，註冊外部資料庫內容過濾。

- 1 在 ZyXEL 裝置的網路組態設定程式中，按一下 **CONTENT FILTER** (內容過濾)，然後選 **Categories** (類別)，再按下 **Register** (註冊) 按鈕。

注意： 您也必須在 ZyWALL 的網路組態設定程式 **CONTENT FILTER** (內容過濾) 畫面中設定並啟用內容過濾。



- 2 myZyXEL.com 登入畫面會開啓。
- 3 輸入您 myZyXEL.com 帳戶的使用者名稱和密碼。
- 4 按一下導覽面板上的 **My Product** (我的產品)。
- 5 按一下裝置的產品名稱連結，在 **Service Management** (服務管理) 畫面中檢視註冊資訊。



6 按一下 **Activate (啓用)**，顯示內容過濾服務的下個畫面。

My Products / Service Activation

Service Management

Product Information

zy70cf

Serial Number: S4Z2928704
Products: ZyWALL 70
Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

> zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

	Service Name	Service Activation	Status	Expiry Date
1	Content Filter	Activate	-	-

7 如果您想要試用服務，請按一下 **Content Filtering Trial (內容過濾試用)** 下的 **Submit (送出)**。試用期間會從您申請服務的日期開始。

如果您已經在使用試用服務，或已經註冊 iCard 的 PIN 碼，就不能申請試用。

如果您已經購買了 iCard，請在 **License Key (註冊識別碼)** (PIN 碼) 欄位中確實輸入 iCard 上的 PIN 碼。選取內容過濾服務的開始日期，然後按下 **Registration Information (註冊資訊)** 下的 **Submit (送出)**。

My Products / Service Activation

Content Filtering Trial

We offer 30-day free trial for content filtering service.
If you would like to have a try, please click "submit".

Registration Information

1. Enter the License Key (PIN code) exactly as shown in your iCard.
2. Content filtering begins from the activation date.

> License Key (PIN code) :

> Activation Date : - -

- 8 會顯示畫面，說明您已經註冊服務。按一下 **Continue** (繼續)，移至 **Service Management** (服務管理) 畫面。

My Products / Service Activation

Apply Standard Version Successful

Your E-mail Address : stanley_king@gfortunenet.com

Effective Period : 2004/07/31 ~ 2005/07/31

Your Name : stanley

Your Region : Taiwan

Continue

- 9 如果您正在使用試用服務，還是可以註冊 iCard 的 PIN 碼，方法是按一下 **Service Management** (服務管理) 畫面中 **Service Activation** (服務啟動) 欄位中的 **Upgrade** (更新)。

My Products / Service Activation

Service Management

Product Information

zy70cf

Serial Number: S4Z2928704
Products: ZyWALL 70
Authentication Code: 00A0C5012345

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

> zy70cf

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

	Service Name	Service Activation	Status	Expiry Date	Remark
1	Content Filter	Upgrade	Installed	2004-09-02	Refresh

11 疑難排解

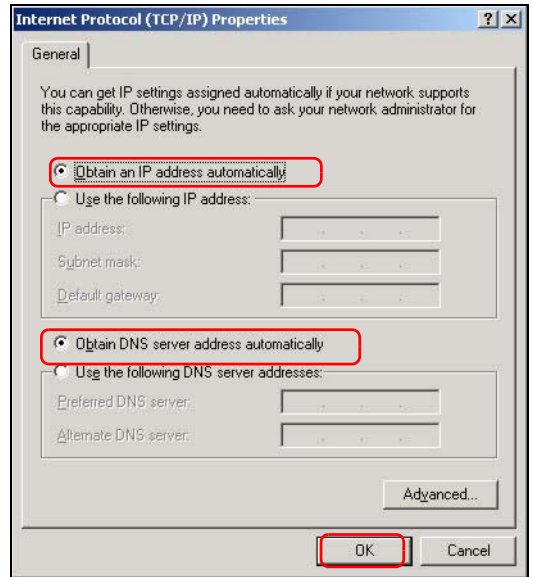
問題	修正動作
LED 全部不亮。	<p>請確認已經將電源線接到 ZyWALL 裝置上，且接上了適當的電源。確認開啓了 ZyWALL 裝置。檢查所有纜線是否正確連接。</p> <p>如果 LED 指示燈仍然不亮，可能是硬體發生問題。如果是這種情況，請聯絡當地的供應商。</p>
無法從 LAN 存取 ZyWALL。	<p>檢查 ZyWALL 和電腦或集線器之間的纜線連接。請參閱 章節 1，取得詳細資訊。</p> <p>從 LAN 電腦上 ping ZyWALL。請確認電腦上安裝了乙太網路卡，且網路卡能夠正常運作。在電腦中，按一下開始、(所有程式) 程式集、附屬應用程式，然後按一下命令提示字元。在命令提示字元視窗中，輸入 "ping" 再輸入 ZyWALL 的 LAN IP 位址 (預設為 192.168.1.1)，然後按一下 ENTER。ZyWALL 裝置應該會有回應。如果仍然沒有回應，請參閱 章節 11.1。</p> <p>如果忘記了 ZyWALL 的密碼，請使用 RESET (重設) 按鈕。按住這個按鈕約 10 秒 (或按住直到 PWR LED 指示燈亮起) 後放開。按下這個按鈕會將 ZyWALL 還原為預設值 (密碼為 1234，而 LAN IP 位址為 192.168.1.1 等，請參閱《使用手冊》，取得詳細資訊)。</p> <p>如果忘記了 ZyWALL 的 LAN 或 WAN IP 位址，可以透過管理設定連接埠 (Console Port) 檢查 SMT 中的 IP 位址。使用終端機線 (Console Cable) 將電腦接到 CONSOLE 連接埠。您的電腦必須具有終端機模擬通訊程式 (例如超級終端機)，並做以下設定：VT100 終端機模擬模式、無同位、8 資料位元、1 停止位元、無流量控制，以及連接埠速度 9600 bps。</p>
無法存取網際網路。	<p>檢查 ZyWALL 是否正確連接可以存取網際網路的乙太網路插孔。確認網際網路閘道裝置 (例如 DSL 數據機) 運作正常。</p> <p>按一下導覽面板上的 WAN，確認您的設定。</p>
無法建立 VPN 連線。	<p>確認 ZyWALL 和遠端 IPSec 路由器使用同樣的 VPN 設定。按一下導覽面板上的 VPN，進行進階設定。</p> <p>試著存取某個網站，檢查網際網路連線是否正常。</p>

11.1 設定電腦的 IP 位址

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

- 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**。
- 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**。
- 在**區域連線**上按一下滑鼠右鍵，然後按**內容**。
- 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。