ZyWALL P1

Security Appliance

Support Notes

Version 3.64

Mar. 2005

ZyXEL

Unleash Networking Power

INDEX

Application Notes 6
General Application Notes 6
Internet Connection 6
IPSec VPN 8
ZyWALL Application Notes 8
Using xAuth authentication for IPSec VPN Tunneling 12
Using Self-signed Certificate 12
FAQ 23
ZyNOS FAQ 23
What is ZyNOS? 23
How do I upgrade/backup the ZyNOS firmware by using TFTP client program via LAN? 23
Why can't I make Telnet to ZyWALL from WAN? 24
What should I do if I forget the system password? 24
How many network users can the NAT support? 24
Product FAQ 24
What can the USB port on the ZyWALL P1 be use for? 24
Do I need to use the power adapter if I already connected the USB port on the ZyWALL P1 to my PC/Notebook? 25
Can the USB port on the ZyWALL P1 function as an Ethernet port to allow data transmit to or from PC/Notebook? 25
What is the ZyWALL Internet Access Sharing Router? 25
Will the ZyWALL work with my Internet connection? 25
What do I need to use the ZyWALL? 26
What is PPPoE? 26
Does the ZyWALL support PPPoE? 26
How do I know I am using PPPoE? 26
Why does my Internet Service Provider use PPPoE? 26
How can I configure the ZyWALL? 26
What can we do with ZyWALL? 27
Does ZyWALL support dynamic IP addressing? 27
What is the difference between the internal IP and the real IP from my ISP? 27
How does e-mail work through the ZyWALL? 27
Is it possible to access a server running behind NAT from the outside

Internet? If possible, how? 27
What DHCP capability does the ZyWALL support? 28
What are the capability of wireless feature of ZyWALL 28
What is the coverage range of Wireless in ZyWALL? 28
How do I used the reset button, more over what field of parameter will be reset by reset button? 28
What network interface does the new ZyWALL series support? 28
How does the ZyWALL support TFTP? 28
Can the ZyWALL support TFTP over WAN? 28
How can I upload data to outside Internet over the one-way cable? 29
My ZyWALL can not get an IP address from the ISP to connect to the Internet, what can I do? 29
What is BOOTP/DHCP? 29
What is DDNS? 30
When do I need DDNS service? 30
What DDNS servers does the ZyWALL support? 30
What is DDNS wildcard? 30
Does the ZyWALL support DDNS wildcard? 31
Can the ZyWALL NAT handle IPSec packets sent by the VPN gateway behind ZyWALL? 31
How do I setup my ZyWALL for routing IPSec packets over NAT? 31
Firewall FAQ 31
What is a network firewall? 31
What makes ZyWALL secure? 31
What are the basic types of firewalls? 32
What kind of firewall is the ZyWALL? 32
Why do you need a firewall when your router has packet filtering and NAT built-in? 33
What is Denials of Service (DoS)attack? 33
What is Ping of Death attack? 33
What is Teardrop attack? 33
What is SYN Flood attack? 34
What is LAND attack? 34
What is Brute-force attack? 34
What is IP Spoofing attack? 34
What are the default ACL firewall rules in ZyWALL? 34
Is DMZ behind NAT or not, in ZyWALL 100? 35

Can I use both public and private IP addresses on DMZ? 35
Why traffic redirect/static/policy route be blocked by ZyWALL? 35
How can I protect against IP spoofing attacks? 37
IPSec FAQ 38
What is VPN? 38
Why do I need VPN? 38
What are most common VPN protocols? 39
What is PPTP? 39
What is L2TP? 39
What is IPSec? 39
What secure protocols does IPSec support? 39
What are the differences between 'Transport mode' and 'Tunnel mode? 40
What is SA? 40
What is IKE? 40
What is Pre-Shared Key? 40
What are the differences between IKE and manual key VPN? 40
What is Phase 1 ID for? 41
What are Local ID and Peer ID? 41
When should I use FQDN? 41
Is my ZyWALL ready for IPSec VPN? 42
How do I configure ZyWALL VPN? 42
How many VPN connections does ZyWALL support? 42
What VPN protocols are supported by ZyWALL? 42
What types of encryption does ZyWALL VPN support? 42
What types of authentication does ZyWALL VPN support? 42
I am planning my ZyWALL-to-ZyWALL VPN configuration. What do I need to know? 42
Does ZyWALL support dynamic secure gateway IP? 43
What VPN gateway that has been tested with ZyWALL successfully? 43
What VPN software that has been tested with ZyWALL successfully? 44
Will ZyXEL support Secure Remote Management? 44
12. Does ZyWALL VPN support NetBIOS broadcast? 44
Is the host behind NAT allowed to use IPSec? 44
How do I configure ZyWALL with NAT for internal servers? 44
I am planning my ZyWALL behind a NAT router. What do I need to know? 45
Where can I configure Phase 1 ID in ZyWALL? 45

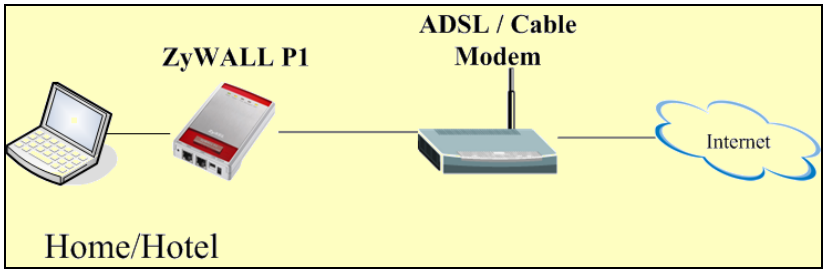
How can I keep a tunnel alive? 46
Single, Range, Subnet, which types of IP address do ZyWALL 10/10II/10W/50/100 support in VPN/IPSec? 46
Does ZyWALL support IPSec pass-through? 46
Can ZyWALL behave as a NAT router supporting IPSec pass through and an IPSec gateway simultaneously? 47
PKI FAQ 47
Basic Cryptography concept 47
What is PKI? 48
What are the security services PKI provides? 48
What are the main elements of a PKI? 48
What is a Certification Authority? 48
What is a digital certificate? 49
What are public and private keys, and what is their relationship? 49
What are Certificate Policies (CPs)? 49
How does a PKI ensure data confidentiality? 49
What is a digital signature? 50
How does a digital signature work? 50
Does ZyXEL provide CA service? 51
What if customers don't have access to CA service, but would like to use PKI function? 51
How can I have Self-signed certificate for ZyXEL appliance? 52
Can I create self-signed certificates in addition to the default one? 52
Will Self-signed certificate be erased if I reset to default configuration file? 52
Will certificates stored in ZyXEL appliance be erased if I reset to default configuration file? 52
What can I do prior to reset appliance's configuration? 52
If I export My Certificates from ZyXEL appliance, save them locally, and then import them back after resetting the configuration file, can I reuse the imported My Certificates ? 52

Application Notes

General Application Notes

Internet Connection

A typical Internet access application of the ZyWALL is shown below. For a small office, there are some components needs to be checked before accessing the Internet.



- **Before you begin**

The ZyWALL is shipped with the following factory default:
1. LAN IP address = 192.168.167.1, subnet mask = 255.255.255.0 (24 bits)
2. DHCP server enabled with IP pool starting from 192.168.167.33
3. Default Web GUI menu password = 1234

- **Setting up the PC (Windows OS)**

1. Ethernet connection

All PCs must have an Ethernet adapter card installed.

- If you only have one PC, connect the PC's Ethernet adapter to the ZyWALL's LAN port with a crossover (red one) Ethernet cable.

2. TCP/IP Installation

You must first install TCP/IP software on each PC before you can use it for Internet access. If you have already installed TCP/IP, go to the next section to configure it; otherwise, follow these steps to install:

- In the **Control Panel/Network** window, click **Add** button.
- In the **Select Network Component Type** windows, select **Protocol** and click **Add**.
- In the **Select Network Protocol** windows, select **Microsoft** from the manufacturers, then select **TCP/IP** from the **Network Protocols** and click **OK**.

3. TCP/IP Configuration

Follow these steps to configure Windows TCP/IP:

- In the **Control Panel/Network** window, click the **TCP/IP** entry to select it and click **Properties** button.
- In the **TCP/IP** Properties window, select **obtain an IP address automatically**.

Note: Do not assign arbitrary IP address and subnet mask to your PCs, otherwise, you will not be able to access the Internet.

- Click the **WINS** configuration tab and select **Disable WINS Resolution**.
- Click the **Gateway** tab. Highlight any installed gateways and click the **Remove** button until there are none listed.
- Click the **DNS Configuration** tab and select **Disable DNS**.
- Click **OK** to save and close the **TCP/IP** properties window
- Click **OK** to close the Network window. You will be prompted to insert your Windows CD or disk. When the drivers are updated, you will be asked if you want to restart the PC. Make sure your ZyWALL is powered on before answering YES to the prompt. Repeat the above steps for each Windows PC on your network.

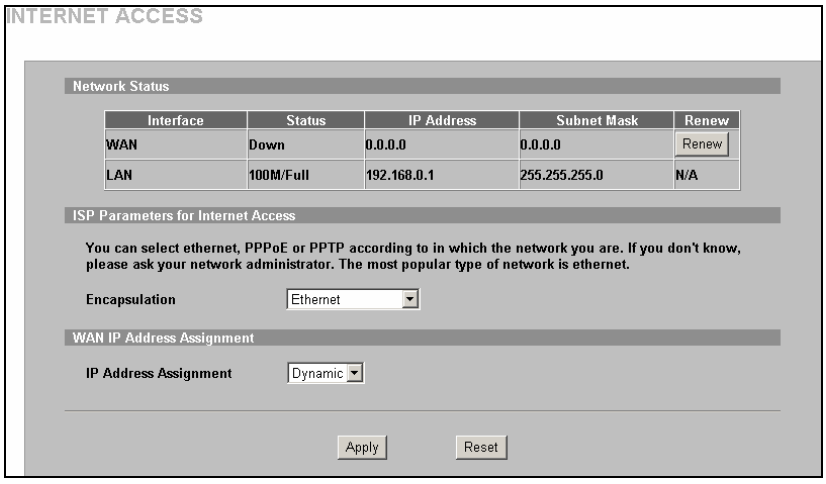
- **Setting up the ZyWALL router**

The following procedure is for the most typical usage of the ZyWALL where you have a single-user account (SUA). The ZyWALL supports embedded web server that allows you to use Web browser to configure it. Before configuring the router using Browser please be sure there is no Telnet or Console login.

1. Retrieve ZyWALL Web

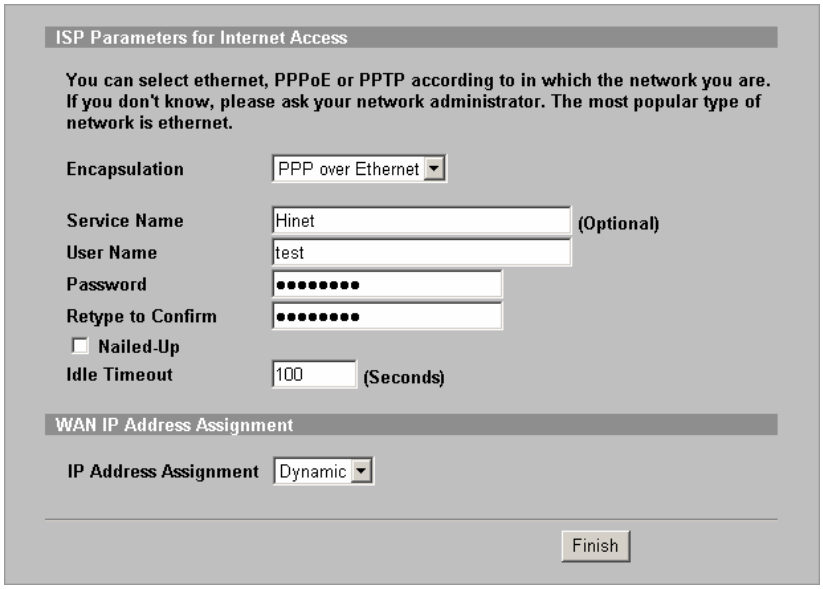
Please enter the LAN IP address of the ZyWALL router in the URL location to retrieve the web screen from the ZyWALL. The default LAN IP of the ZyWALL is 192.168.167.1.

2. Internet Access is the default home page when you first open ZyWALL WEB GUI.



Select Encapsulation type according to your environment. Ex. If you are in a hotel, most likely you would use Ethernet with Dynamic IP address assignment

The Web screen shown below takes PPPoE as the example.

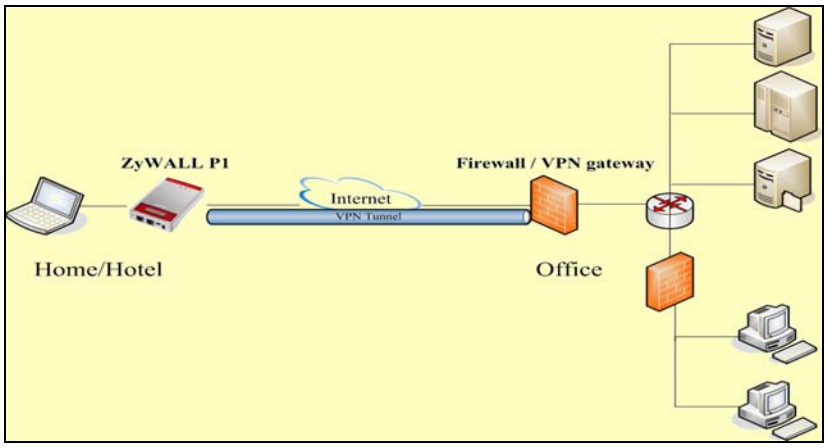


Select "**Dynamic**" if the ISP provides the IP dynamically, otherwise select "**Static**" and enter the static IP given by ISP in the "**IP Address**" field.

IPSec VPN

ZyWALL Application Notes

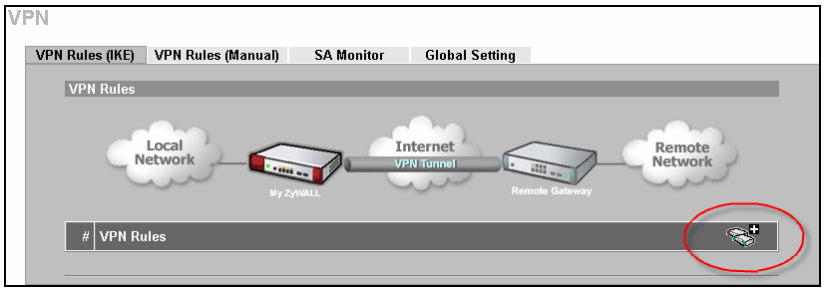
Following section shows how to configure the ZyWALL P1 to establish VPN with an IPSec VPN gateway. The ZyWALL P1 is designed and implemented according to industry IPSec VPN standard, so it should be able to establish VPN with an VPN gateway that follows industry IPSec VPN standard.



Setup ZyWALL VPN

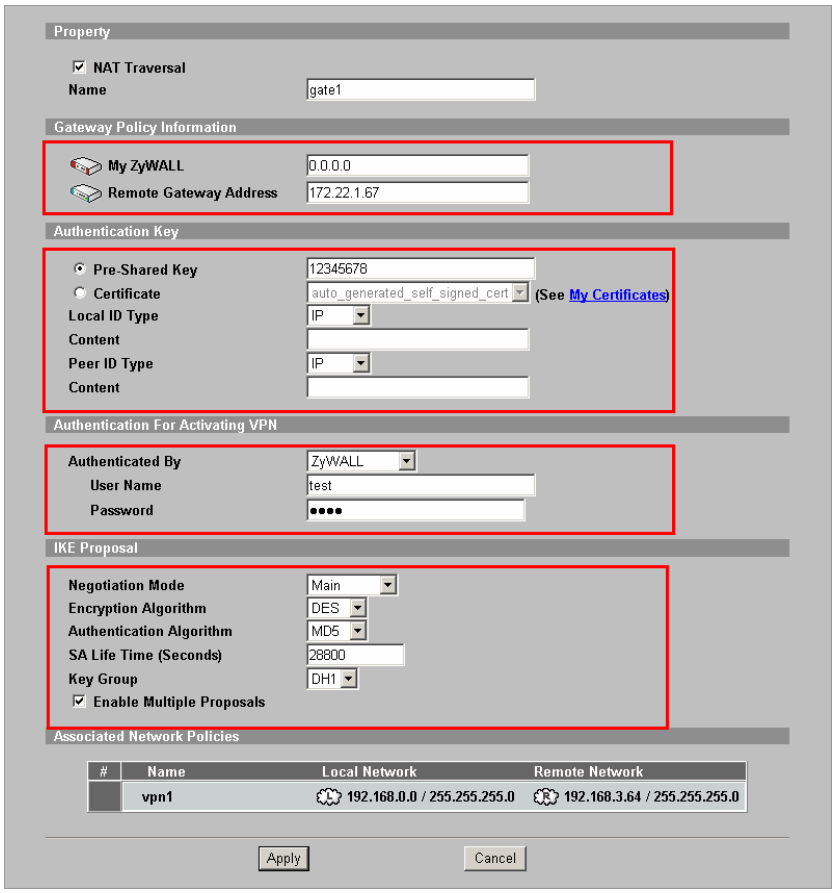
1. Enter ZyWALL GUI using http://192.168.167.1
2. Select **Advanced** menu and you will be asked to key in password to enter ZyWALL advanced configuration mode. Default password is 1234

3. Select **VPN** menu and click + sign to add a new VPN gateway policy.

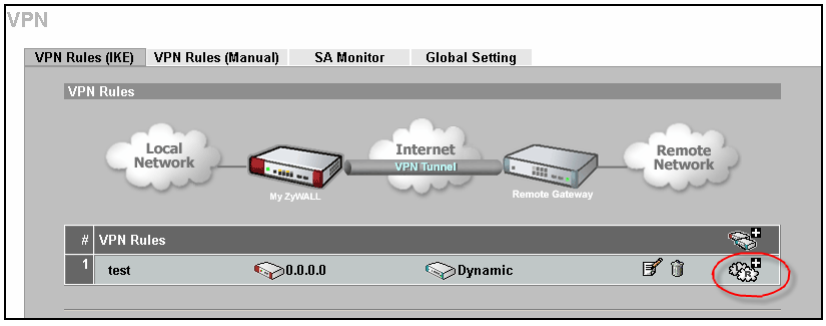


4. Provide a name for this VPN gateway policy
5. Enter ZyWALL P1 **WAN IP** into **My ZyWALL**. (If you are constantly on the move, it's recommended to use a Dynamic VPN rule. IP: 0.0.0.0)

6. Enter the **WAN IP** of office/HQ VPN gateway into **Remote Gateway Address**
7. Configure the **Authentication Key** and **IKE Proposal** according to the IPSec proposal on the VPN gateway of your office/HQ. If office/HQ VPN gateway is using x-auth to authenticate VPN user, then select **Authenticated by: XAUTH server** in **Authentication for Activating VPN.** Otherwise, you may select **Authenticated by: ZyWALL** in **Authentication for Activating VPN** and then provide a set of username and password for authentication purpose.

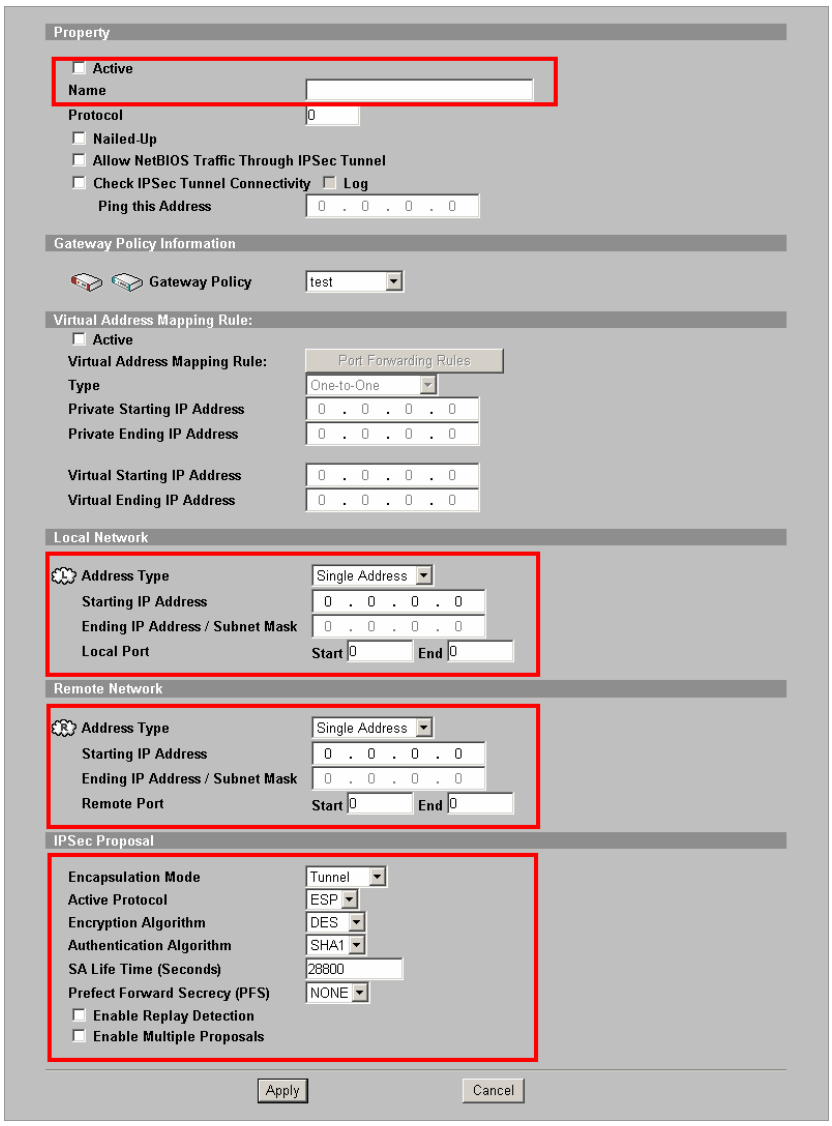


8. After configure a VPN gateway policy, you will need to configure a Network Policy



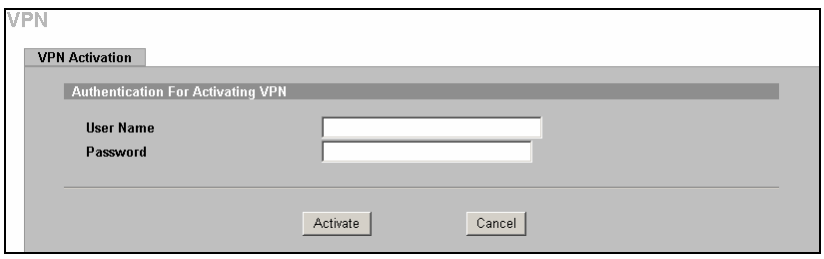
9. Provide a **Name** for this Network Policy
10. Enter ZyWALL P1 LAN subnet address into Local Network. (If you are constantly on the move, it's recommended to use a Dynamic VPN rule. IP: 0.0.0.0)
11. Enter office/HQ subnet address into Remote Network

12. Configure the **IPSec Proposal** according to the IPSec proposal on the VPN gateway of your office/HQ.



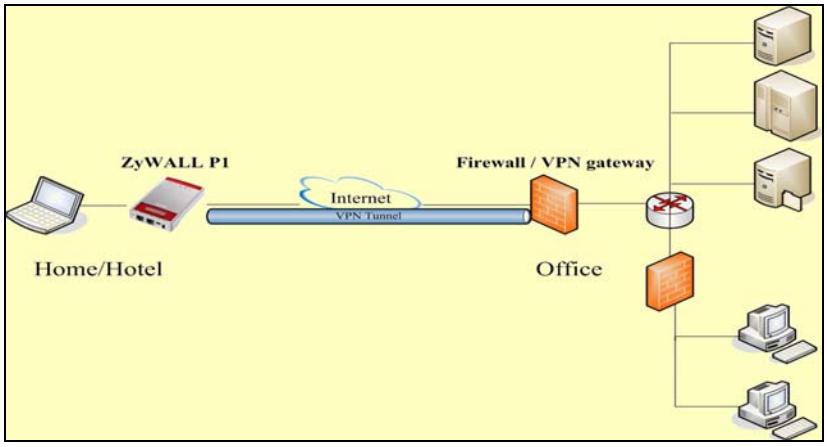
Initiate ZyWALL VPN

You will be ask to provide username/password before you could initiate VPN from ZyWALL P1 Enter the username/password you configured in step 7 in previous section.



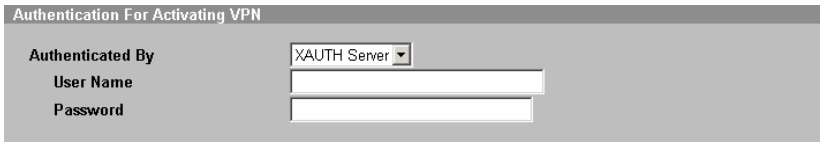
Using xAuth authentication for IPSec VPN Tunneling

xAuth leverages traditional RADIUS authentication method in IPSec/VPN. With xAuth, network administrators can apply user level access control over IPSec VPN.
Managing different pre-shared keys for different mobile users would be a big headache for network administrators. With xAuth, multiple users can shared the same pre-shared key, but their access to central network will be further checked via RADIUS server in central side. Network administrators can utilize their RADIUS server for authentication of IPSec connection.
xAuth is a protocol with client and server architecture. The ZyWALL supports both client and server mode. Between IKE phase 1 and phase 2 negotiations, a client needs to send username & password to server for authentication purpose. Then the server would forward the username & password to RADIUS server for checking. The ZyWALL also provides internal database in server mode. With internal database, administrators do not need to build up the external RADIUS server.



To use xAuth on the above scenario, you will need to configure the VPN gateway at the office to function as xAuth server and the ZyWALL P1 to act as xAuth client.

In the VPN Gateway Policy page, you will see authentication for activating VPN selection. Select Authenticated by XAUTH Server if your office VPN gateway uses xAuth protocol to authentication VPN user.

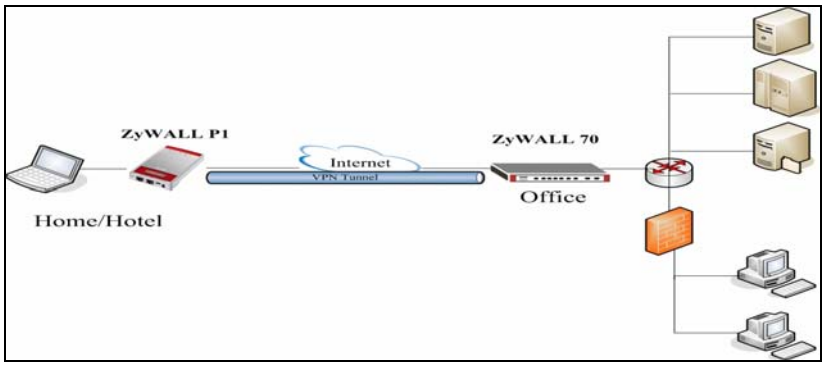


Using Self-signed Certificate

This example displays how to use PKI feature in VPN function of ZyXEL appliance. Through PKI function, users can achieve party identification when doing VPN/IPSec negotiation. For customers who don't have CA

service support in their environment but would like to use PKI feature, ZyWALL provides self-signed certificates to achieve this. As the name indicates, a self-signed certificate is a certificate signed by the device (ZyWALL) its self. Each ZyWALL device has its own self-signed certificate by factory default. When you reset to default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created at the first boot up time.

To utilize self-signed certificates in VPN negotiation, the procedures are as following,

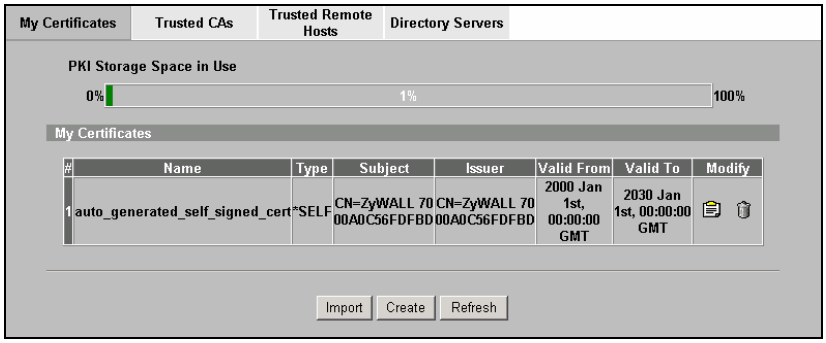


LAN	ZyWALL 70	ZyWALL P1	LAN
10.1.133.0/24	LAN: 10.1.133.1 WAN: 192.168.1.35	LAN: 192.168.167.1 WAN:192.168.1.36	192.168.167.0/24

Step 1. Export Self-signed certificate from ZyWALL 70 & Import it to ZyWALL P1

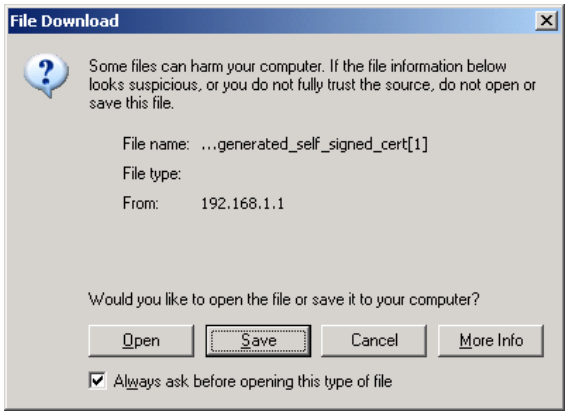
1. ZyWALL keeps its own Self-signed certificate by default. But the factory default Self-signed certificates are the same on all ZyWALL models. To make the self-signed certificate unique for this device, you should replace the factory default certificate by pressing the Apply button in the following page at the first time you login to ZyWALL.

2. Go to ZyWALL 70, SECURITY->CERTIFICATES->My Certificates.

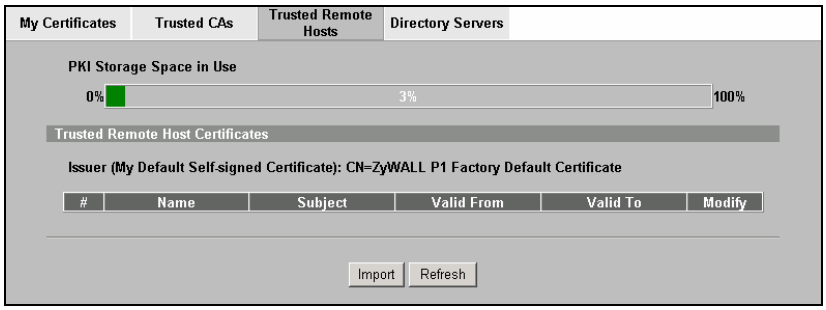


3. Click Export button.

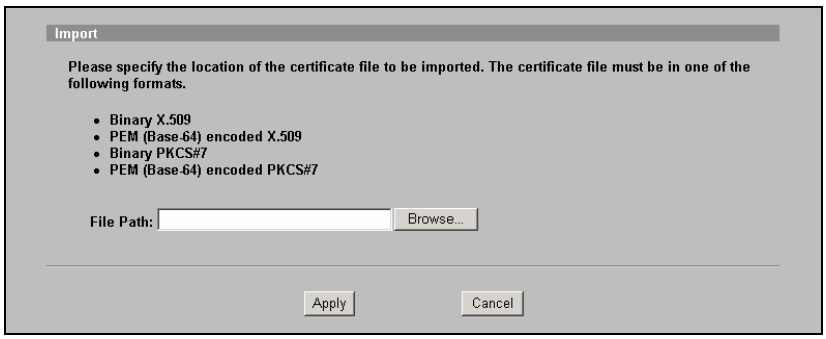
4. A **File Download** window will be popped out. Click **Save** button. And specify the location to save the exported certificate.



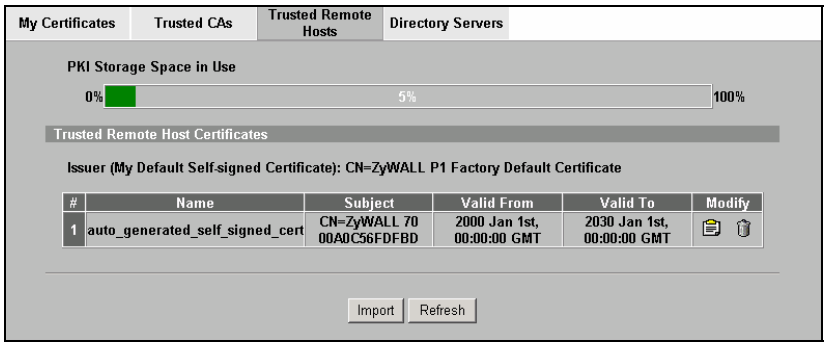
5. Go to ZyWALL P1, **SECURITY->CERTIFICATES->Trusted Remote Hosts** -> click **Import** button.



6. Specify file path where ZyWALL 70's self-signed certificate exported. Then click **Apply** button.



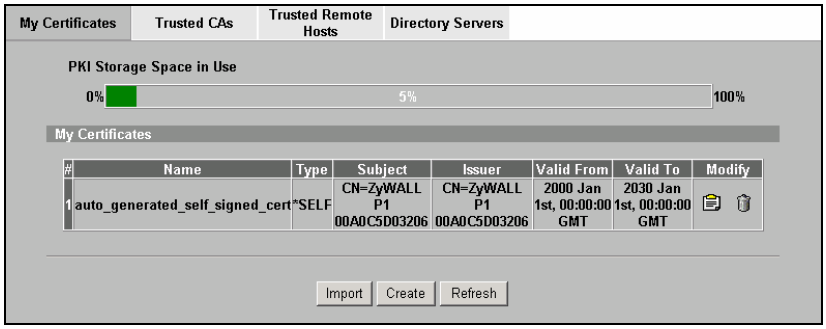
7. After the file is transferred to ZyWALL P1. You can see ZyWALL 70's self-signed certificate in **Trusted Remote Hosts** tab.



Step 2. Export Self-signed certificate from ZyWALL P1 & Import it to ZyWALL 70

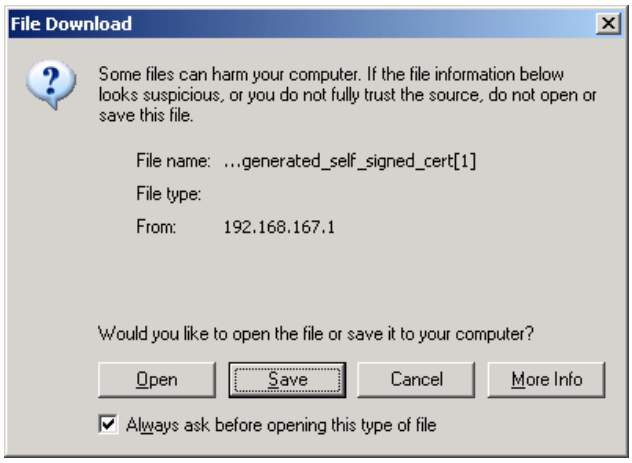
1. ZyWALL keeps its own Self-signed certificate by default. But the factory default Self-signed certificates are the same on all ZyWALL models. To make the self-signed certificate unique for this device, you should replace the factory default certificate by pressing the **Apply** button in the following page at the first time you login to ZyWALL.

1. Go to ZyWALL P1, SECURITY->CERTIFICATES->My Certificates.

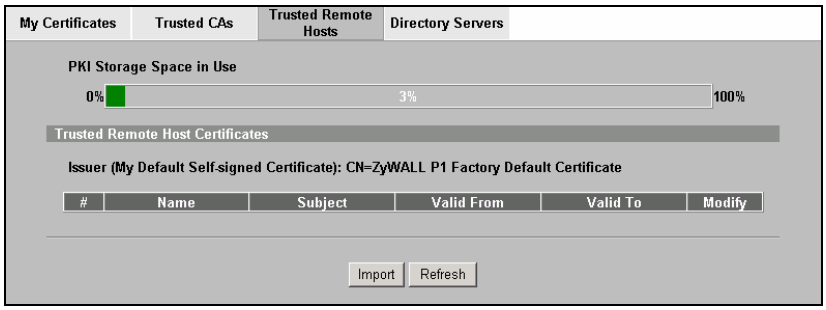


2. Click Export button.

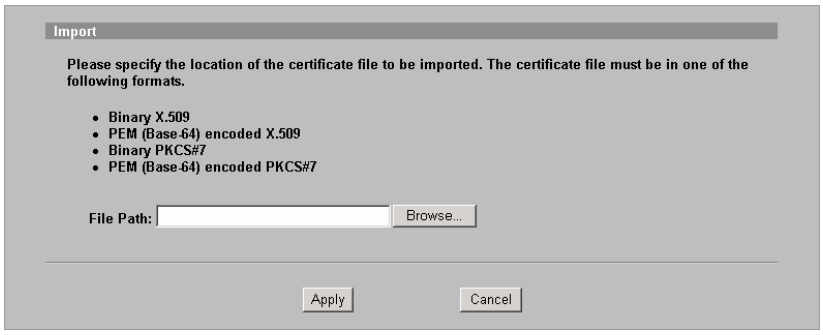
3. A **File Download** window will be popped out. Click **Save** button. And specify the location to save the exported certificate.



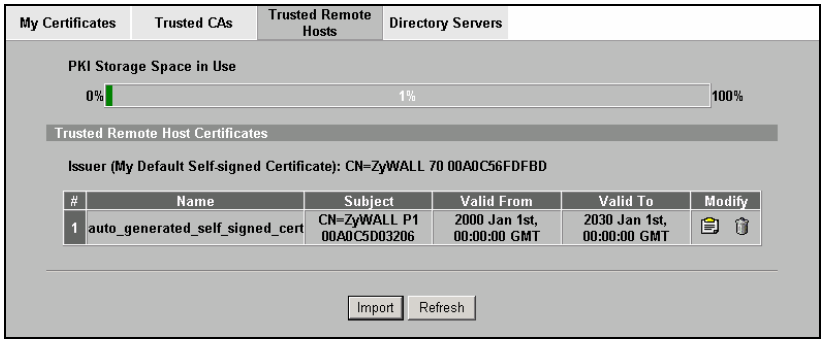
4. Go to ZyWALL 70, **VPN** -> **Trusted Remote Hosts** -> click **Import** button.



5. Specify file path where ZyWALL A's self-signed certificate exported. Then click **Apply** button.

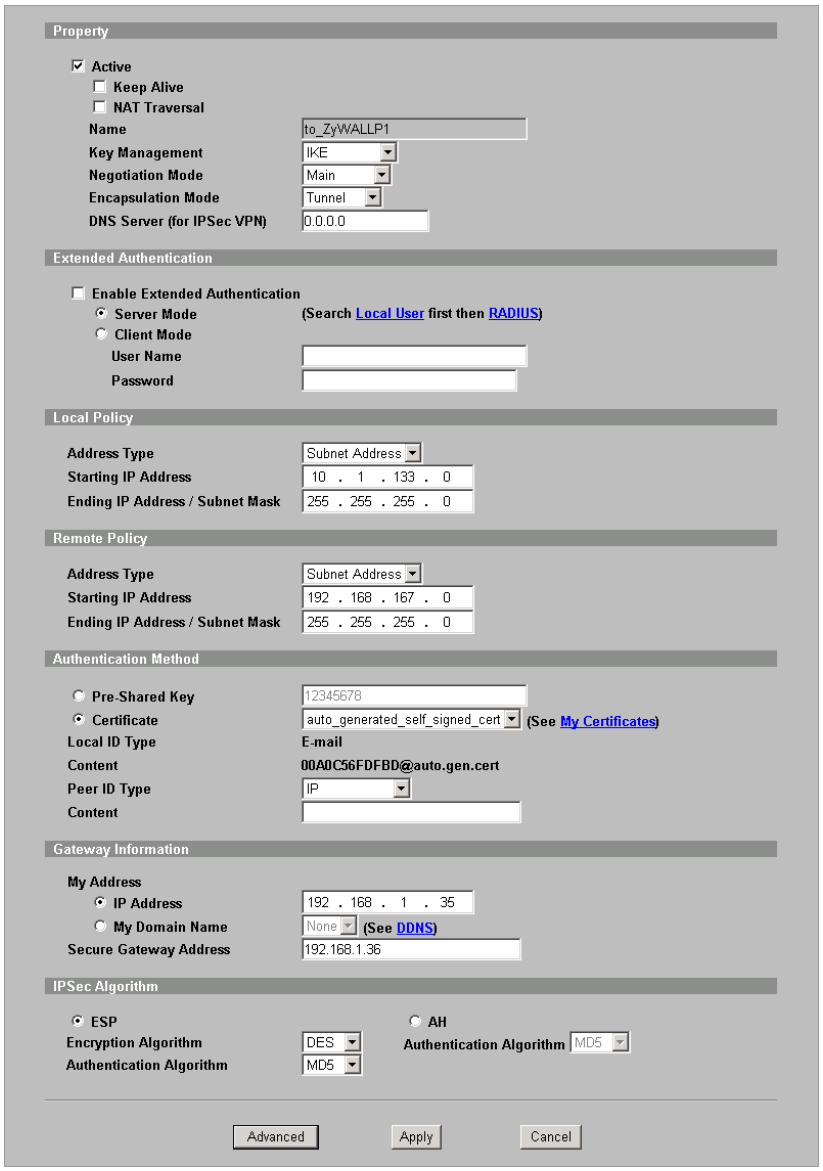


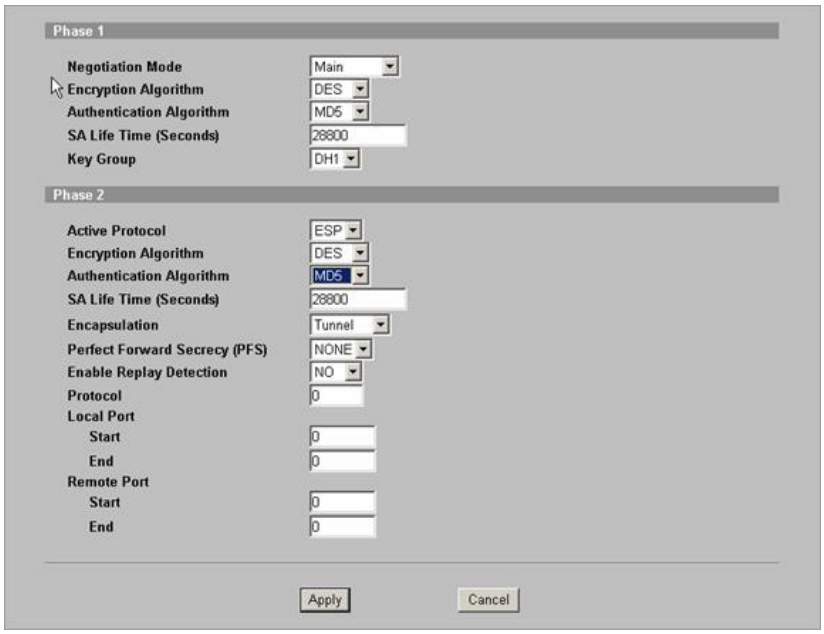
6. After the file is transferred to ZyWALL 70. You can see ZyWALL P1's self-signed certificate in **Trusted Remote Hosts** tab.



Step 3. Using Certificate in VPN on ZyWALL 70

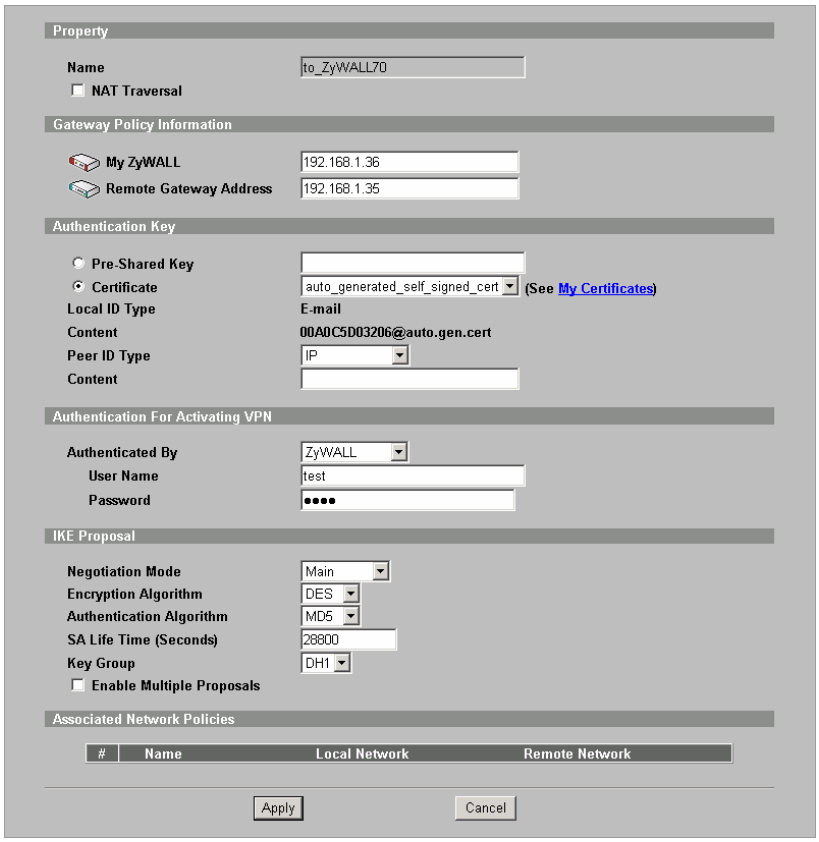
1. Check **Active** to activate the VPN rule.
2. Input this VPN rule a Name, such as **to_ZyWALLP1**.
3. Specify Local network IP address. Address Type=**Subnet Address**, Starting IP Address=**10.1.133.0**, Ending IP Address/Subnet Mask=**255.255.255.0**.
4. Specify Remote network IP address. Address Type=**Subnet Address**, Starting IP Address=**192.168.167.0**, Ending IP Address/Subnet Mask=**255.255.255.0**.
5. In Authentication Key, select Certificate, and choose **auto_generated_self_signed_cert**.



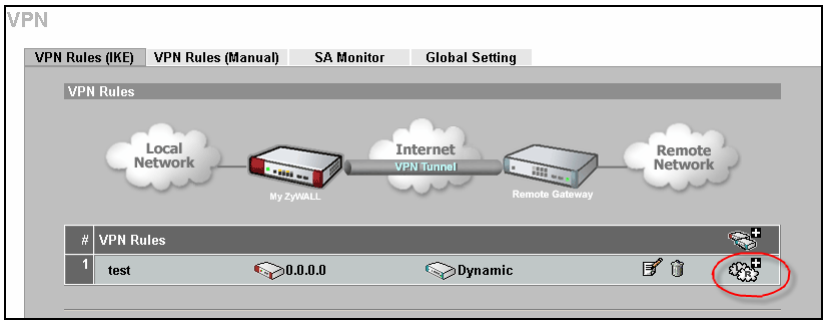


Step 4. Using Certificate in VPN on ZyWALL P1

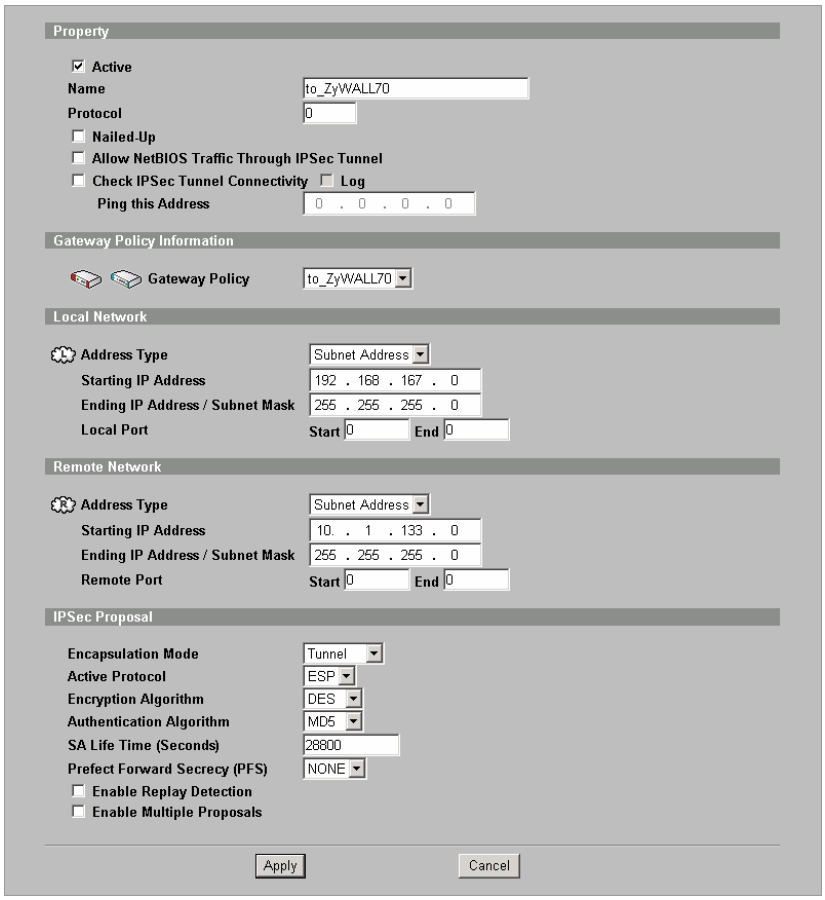
1. Provide a name for this VPN gateway policy (to_ZyWALL70)
2. Enter ZyWALL P1 **WAN IP** into **My ZyWALL**. (192.168.1.36/255.255.255.0)
3. Enter the **WAN IP** of ZyWALL 70 VPN gateway into **Remote Gateway Address** (192.168.1.35/255.255.255.0)
4. Configure the **Authentication Key: select Certificate** and **IKE Proposal** according to the IPSec proposal on the VPN gateway of ZyWALL 70. Select **Authenticated by: ZyWALL** in **Authentication for Activating VPN** and then provide a set of username and password for authentication purpose.



5. After configure a VPN gateway policy, you will need to configure a Network Policy



6. Provide a **Name** for this Network Policy (to_ZyWALL70)
7. Enter ZyWALL P1 LAN subnet address into Local Network. (192.168.167.1/255.255.255.0)
8. Enter ZyWALL 70 subnet address into Remote Network. (10.1.133.0/255.255.255.0)
9. Configure the **IPSec Proposal** according to the IPSec proposal on the VPN gateway of the ZyWALL 70



FAQ

ZyNOS FAQ

What is ZyNOS?

ZyNOS is ZyXEL's proprietary Network Operating System. It is the platform on all ZyWALL routers that delivers network services and applications. It is designed in a modular fashion so it is easy for developers to add new features. New ZyNOS software upgrades can be easily downloaded from our FTP sites as they become available.

How do I upgrade/backup the ZyNOS firmware by using TFTP client program via LAN?

The ZyWALL allows you to transfer the firmware from/to ZyWALL by using TFTP program via LAN.

The procedure for uploading ZyNOS via TFTP is as follows.

- Use the TELNET client program in your PC to login to your ZyWALL.
- Enter CI command **'sys stdio 0'** in menu 24.8 to disable console idle timeout
- To upgrade firmware, use TFTP client program to put firmware in file **'ras'** in the ZyWALL. After data transfer is finished, the ZyWALL will program the upgraded firmware into FLASH ROM and reboot itself.
- To backup your firmware, use the TFTP client program to get file **'ras'** from the ZyWALL.
-

Why can't I make Telnet to ZyWALL from WAN?

There are three reasons that Telnet from WAN is blocked.

1. When the firewall is turned on, all connections from WAN to LAN are blocked by the default ACL rule. To enable Telnet from WAN, you must turn the firewall off or create a firewall rule to allow Telnet connection from WAN. The WAN-to-LAN ACL summary will look like as shown below.

Source IP= Telnet host
Destination IP= ZyWALL's WAN IP
Service= TCP/23
Action=Forward

2. You have disabled Telnet service
3. Telnet service is enabled but your host IP is not the trusted secure host entered. In this case, the error message *'Client IP is not allowed!'* is appeared on the Telnet screen.

What should I do if I forget the system password?

In case you forget the system password, you need to upload ROMFILE to reset the device to factory default. After uploading ROMFILE, the default system password is '1234'.

How many network users can the NAT support?

The ZyWALL does not limit the number of the users but the number of the sessions. The ZyWALL P1 supports 2048 sessions. You can see the NAT sessions utilization bar at the HOME menu of ZyWALL P1 Web GUI

Product FAQ

What can the USB port on the ZyWALL P1 be use for?

The USB port on the ZyWALL P1 allows you to power up the ZyWALL P1 using a PC or Notebook with USB connector.

Do I need to use the power adapter if I already connected the USB port on the ZyWALL P1 to my PC/Notebook?

Under normal circumstance, the power transmits from PC/Notebook via USB port should be enough to let the ZyWALL P1 function properly.
However, if you see all LEDs on the ZyWALL P1 are blinking; this is an indication that the power from USB isn't enough for the ZyWALL P1. You may need to use the power adapter to provide additional power to the ZyWALL P1. This could happen when the USB controller on your PC/Notebook does not follow standard USB spec.

Can the USB port on the ZyWALL P1 function as an Ethernet port to allow data transmit to or from PC/Notebook?

No, the USB port on the ZyWALL P1 only allows power to transmit from PC/Notebook.

What is the ZyWALL Internet Access Sharing Router?

The ZyWALL series fulfills a range of application environments, from small and medium businesses, SOHO, or Telecommuters, to home user or education applications. The ZyWALL series provides a robust Firewall to protect your network, and the IPSec VPN function allows you to create a secure connection for e-business. ZyWALL's design helps users to save expenses, minimize maintenance, and simultaneously provide a high quality networking environment.
The ZyWALL series is a robust solution complete with everything needed for providing Internet access to multiple workstations through your cable or ADSL modem. It is the most simple and affordable solution for multiple and instant broadband Internet access router with 802.11 wireless support.

Will the ZyWALL work with my Internet connection?

The ZyWALL is designed to be compatible with most network environment (cable or xDSL modems). Most external Cable and xDSL modems use an Ethernet port to connect to your computer so the ZyWALL can be place between the computer and the External modem. As long as your Internet Access device has an Ethernet port, you can use the ZyWALL. Besides, if your ISP supports PPPoE you can also use the ZyWALL, because PPPoE had been supported in the ZyWALL.

What do I need to use the ZyWALL?

You need an xDSL modem or cable modem with an Ethernet port to use the ZyWALL. The ZyWALL has two Ethernet ports: LAN port and WAN port. You should connect the computer to the LAN port and connect the external modem to the WAN port. If the ISP uses PPPoE Authentication you need the user account to enter in the ZyWALL.

What is PPPoE?

PPPoE stands for Point-to-Point Protocol over Ethernet that is an IETF draft standard specifying how a computer interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) to achieve access to the high-speed data networks via a familiar PPP dialer such as 'Dial-Up Networking' user interface. PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

Does the ZyWALL support PPPoE?

Yes. The ZyWALL supports PPPoE since ZyNOS 2.50.

How do I know I am using PPPoE?

PPPoE requires a user account to login to the provider's server. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check your ISP or the information sheet given by the ISP. Please choose PPPoE as the encapsulation type in the ZyWALL if you are using PPPoE service provided by your ISP.

Why does my Internet Service Provider use PPPoE?

PPPoE emulates a familiar Dial-Up connection. It allows your ISP to provide services using their existing network configuration over the broadband connections. Besides, PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

How can I configure the ZyWALL?

- Telnet remote management- CLI command line
- Web browser- web server embedded for easy configurations

What can we do with ZyWALL?

Browse the World Wide Web (WWW), send and receive individual e-mail, and up/download data on the internet. These are just a few of many benefits you can enjoy when you put the whole office on-line with the ZyWALL Internet Access Sharing Router.

Does ZyWALL support dynamic IP addressing?

The ZyWALL supports both static and dynamic IP address from ISP.

What is the difference between the internal IP and the real IP from my ISP?

Internal IPs is sometimes referred to as virtual IPs. They are a group of up to 255 IPs that are used and recognized internally on the local area network. They are not intended to be recognized on the Internet. The real IP from ISP, instead, can be recognized or pinged by another real IP on the internet. The ZyWALL Internet Access Sharing Router works like an intelligent router that route between the virtual IP and the real IP.

How does e-mail work through the ZyWALL?

It depends on what kind of IP you have: Static or Dynamic. If your company has a domain name, it means that you have a static IP address. Suppose your company's e-mail address is xxx@mycompany.com. Joe and Debbie will be able to send e-mail through ZyWALL Internet Access Sharing Router using jane@mycompany.com and debbie@mycompany.com respectively as their e-mail addresses. They will be able to retrieve their individual private and secure e-mail, if they have been assigned the proper access right.
If your company does not have a domain name, it means that your ISP provides you with a dynamic IP address. Suppose your company's e-mail address is mycompany@ispname.com. Jane and John will be able to send e-mail through ZyWALL Internet Access Sharing Router using "jane"<mycompany@ispname.com> and "john"<mycompany@ispname.com> respectively as their e-mail addresses. Again, they will be able to retrieve their individual private and secured e-mail, if they have been assigned the proper access right.

Is it possible to access a server running behind NAT from the outside Internet? If possible, how?

Yes, it is possible because ZyWALL delivers the packet to the local server by looking up to a NAT server table. Therefore, to make a local server accessible to the outsider, the port number and the internal IP address of the server must be configured in NAT menu.

What DHCP capability does the ZyWALL support?

The ZyWALL supports DHCP client on the WAN port and DHCP server on the LAN port. The ZyWALL's DHCP client allows it to get the Internet IP address from ISP automatically. The ZyWALL's DHCP server allows it to automatically assign IP and DNS addresses to the clients on the local LAN.

What are the capability of wireless feature of ZyWALL

Wireless in ZyWALL series support embedded 802.1x MD5/CHAP authentication of 32 clients.

What is the coverage range of Wireless in ZyWALL?

The coverage range typically is 50m~80m indoor, 150m~300m outdoor. The actual range may very depend on environment, as to obstacles and walls, RF interference, in the environment.

How do I used the reset button, more over what field of parameter will be reset by reset button?

You can used a sharp pointed object insert it into the little reset hole beside the power connector. Press down the reset button and hold down for approx 10 second, the unit will be reset. When the reset button is pressed the device's all parameter will be reset back to factory default.
The default IP address is 192.168.1.1, Password 1234, ESSID Wireless.

What network interface does the new ZyWALL series support?

The new ZyWALL series support auto MDX/MDIX 10/100M Ethernet LAN/WAN port to connect to the computer on LAN and 10/100M Ethernet to connect to the external cable or xDSL modem on WAN.

How does the ZyWALL support TFTP?

In addition to the direct console port connection, the ZyWALL supports the uploading/download of the firmware and configuration file using TFTP (Trivial File Transfer Protocol) over LAN.

Can the ZyWALL support TFTP over WAN?

Although TFTP should work over WAN as well, it is not recommended because of the potential data corruption problems.

How can I upload data to outside Internet over the one-way cable?

A workaround is to use an alternate path for your upstream path, such as a dial-up connection to an Internet service provider. So, if you can find another way to get your upstream packets to the Internet you will still be able to receive downstream packets via ZyWALL.

My ZyWALL can not get an IP address from the ISP to connect to the Internet, what can I do?

Currently, there are various ways that ISPs control their users. That is, the WAN IP is provided only when the user is checked as an authorized user. The ISPs currently use three ways:

1. Check if the 'MAC address' is valid
2. Check if the 'Host Name' is valid, e.g., @home

If you are not able to get the Internet IP from the ISP, check which authentication method your ISP uses and troubleshoot the problem as described below.

1. Your ISP checks the 'MAC address'

Some ISPs only provide an IP address to the user with an authorized MAC address. This authorized MAC can be the PC's MAC which is used by the ISP for the authentication. So, if a new network card is used or the ZyWALL is attached to the cable modem directly, the ISP will reject the DHCP discovery from this MAC, thus no IP is assigned by the ISP.
The ZyWALL supports to clone the MAC from the first PC the ISP installed to be its WAN MAC. To clone the MAC from the PC you need to enter that PC's IP in WAN menu of the ZyWALL web configurator.

2. Your ISP checks the 'Host Name'

Some ISPs take advantage of the 'host name' message in a DHCP packet such as @home to do the authentication. When first installing, the ISP's tech people configure the host name as the 'Computer Name' of the PC in the 'Networking' settings. When the ZyWALL is attached to the cable modem to connect to the ISP, we should configure this host name in the ZyWALL's system (menu 1).

What is BOOTP/DHCP?

BOOTP stands for Bootstrap Protocol. DHCP stands for Dynamic Host Configuration Protocol. Both are mechanisms to dynamically assign an IP address for a TCP/IP client by the server. In this case, the ZyWALL

Internet Access Sharing Router is a BOOTP/DHCP server. Win95 and WinNT clients use DHCP to request an internal IP address, while WFW and WinSock clients use BOOTP. TCP/IP clients may specify their own IP or utilize BOOTP/DHCP to request an IP address.

What is DDNS?

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet. To use the service, you must first apply an account from several free Web servers such as WWW.DYNDNS.ORG.
Without DDNS, we always tell the users to use the WAN IP of the ZyWALL to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the ZyWALL, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the ZyWALL.
When the ISP assigns the ZyWALL a new IP, the ZyWALL updates this IP to DDNS server so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

When do I need DDNS service?

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address we can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname. Whenever the ISP assigns you a new IP, the ZyWALL sends this IP to the DDNS server for its updates.

What DDNS servers does the ZyWALL support?

The DDNS servers the ZyWALL supports currently is WWW.DYNDNS.ORG where you apply the DNS from and update the WAN IP to.

What is DDNS wildcard?

Some DDNS servers support the wildcard feature which allows the hostname, *.yourhost.dyndns.org, to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful when there are multiple servers inside and you want users to be able to use things such as www.yourhost.dyndns.org and still reach your hostname.

Does the ZyWALL support DDNS wildcard?

Yes, the ZyWALL supports DDNS wildcard that WWW.DynDNS.ORG supports. When using wildcard, you simply enter yourhost.dyndns.org in the Host field in Network/WAN/DDNS menu.

Can the ZyWALL NAT handle IPSec packets sent by the VPN gateway behind ZyWALL?

Yes, the ZyWALL's NAT can handle IPSec ESP Tunneling mode. We know when packets go through NAT, NAT will change the source IP address and source port for the host. To pass IPSec packets, NAT must understand the ESP packet with protocol number 50, replace the source IP address of the IPSec gateway to the router's WAN IP address. However, NAT should not change the source port of the UDP packets which are used for key managements. Because the remote gateway checks this source port during connections, the port thus is not allowed to be changed.

How do I setup my ZyWALL for routing IPSec packets over NAT?

For outgoing IPSec tunnels, no extra setting is required. For forwarding the inbound IPSec ESP tunnel, A 'Default' server set in menu 15 is required. It is because NAT makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. So, to make an internal server for outside access, we must specify the service port and the LAN IP of this server in Menu 15. Thus NAT is able to forward the incoming packets to the requested service behind NAT and the outside users access the server using the ZyWALL's WAN IP address. So, we have to configure the internal IPSec as a default server (unspecified service port) in menu 15 when it acts a server gateway.

Firewall FAQ

What is a network firewall?

A firewall is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an un-trusted network. The firewall can be thought of two mechanisms. One to block the traffic, and the other to permit traffic.

What makes ZyWALL secure?

The ZyWALL is pre-configured to automatically detect and thwart Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND attack, IP Spoofing, etc. It also uses stateful packet inspection to determine if an inbound connection is allowed through the firewall to the private LAN. The ZyWALL supports Network Address Translation (NAT), which translates the private local addresses to one or

multiple public addresses. This adds a level of security since the clients on the private LAN are invisible to the Internet.

What are the basic types of firewalls?

Conceptually, there are three types of firewalls:

1. Packet Filtering Firewall
2. Application-level Firewall
3. Stateful Inspection Firewall

Packet Filtering Firewalls generally make their decisions based on the header information in individual packets. This header information includes the source, destination addresses and ports of the packets.

Application-level Firewalls generally are hosts running proxy servers, which permit no traffic directly between networks, and which perform logging and auditing of traffic passing through them. A proxy server is an application gateway or circuit-level gateway that runs on top of general operating system such as UNIX or Windows NT. It hides valuable data by requiring users to communicate with secure systems by mean of a proxy. A key drawback of this device is performance.

Stateful Inspection Firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also 'inspect' the session data to assure the integrity of the connection and to adapt to dynamic protocols. The flexible nature of Stateful Inspection firewalls generally provides the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support.

What kind of firewall is the ZyWALL?

1. The ZyWALL's firewall inspects packets contents and IP headers. It is applicable to all protocols, that understands data in the packet is intended for other layers, from network layer up to the application layer.
2. The ZyWALL's firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
3. The ZyWALL's firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
4. The ZyWALL's firewall is fast. It uses a hashing function to search the matched session cache instead of going through every individual rule for a packet.

5. The ZyWALL's firewall provides email service to notify you for routine reports and when alerts occur.

Why do you need a firewall when your router has packet filtering and NAT built-in?

With the spectacular growth of the Internet and online access, companies that do business on the Internet face greater security threats. Although packet filter and NAT restrict access to particular computers and networks, however, for the other companies this security may be insufficient, because packets filters typically cannot maintain session state. Thus, for greater security, a firewall is considered.

What is Denials of Service (DoS)attack?

Denial of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.
There are four types of DoS attacks:

1. Those that exploits bugs in a TCP/IP implementation such as Ping of Death and Teardrop.
2. Those that exploits weaknesses in the TCP/IP specification such as SYN Flood and LAND Attacks.
3. Brute-force attacks that flood a network with useless data such as Smurf attack.
4. IP Spoofing

What is Ping of Death attack?

Ping of Death uses a 'PING' utility to create an IP packet that exceeds the maximum 65535 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang, or reboot.

What is Teardrop attack?

Teardrop attack exploits weakness in the reassemble of the IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original packet except that it contains an offset field. The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

What is SYN Flood attack?

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

What is LAND attack?

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

What is Brute-force attack?

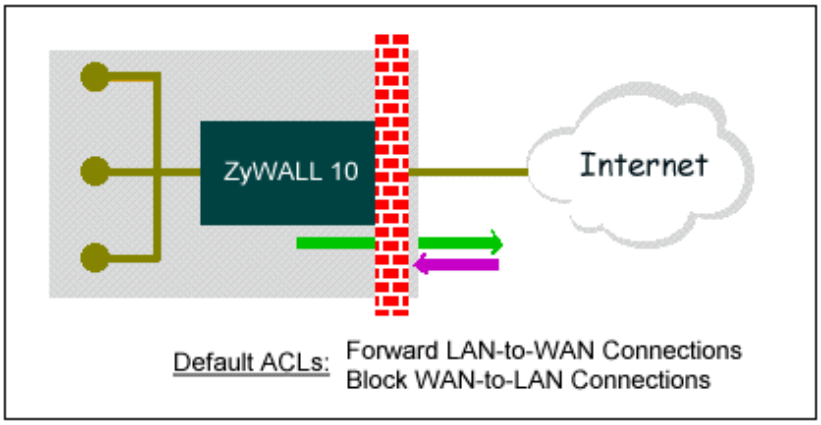
A Brute-force attack, such as 'Smurf' attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker flood a destination IP address of each packet is the broadcast address of the network; the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request packet, the resulting ICMP traffic will not only clog up the 'intermediary' network, but will also congest the network of the spoofed source IP address, known as the 'victim' network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

What is IP Spoofing attack?

Many DoS attacks also use IP Spoofing as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP Spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall.

What are the default ACL firewall rules in ZyWALL?

There are two default ACLs pre-configured in the ZyWALL, one allows all connections from LAN to WAN and the other blocks all connections from WAN to LAN except of the DHCP packets.



Is DMZ behind NAT or not, in ZyWALL 100?

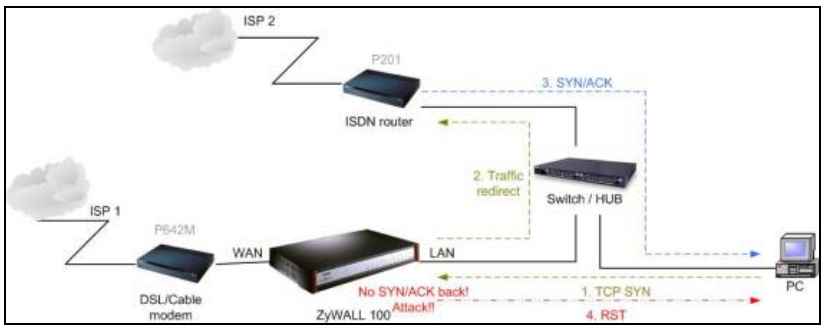
Basically DMZ is behind NAT. But there is one exception. If you use Full Feature as NAT type, and there is no NAT mapping for systems on DMZ. Then NAT will not take effect in this case.

Can I use both public and private IP addresses on DMZ?

- Yes, you can. To achieve this, you have to use IP alias to separate the DMZ interface into 2 logical segments, one for private IP, and the other for public IP.
- Then you have to use Full Feature as NAT type in Menu 4.
- Set NAT mapping for private IP addresses in Menu 15.1.
- Note that in this case, NAT will not take care IP addresses without NAT mapping. So private IP address could be sent out by ZyWALL due to users' incaution.

Why traffic redirect/static/policy route be blocked by ZyWALL?

ZyWALL is an ideal secure gateway for all data passing between the Internet and the LAN/DMZ. For some reasons (load balance or backup line), users may want traffic to be re-routed to another Internet access devices while still be protected by ZyWALL. In such case, the network topology is the most important issue. Here is a common example that people mis-deploy the LAN traffic redirect and static route.



The above figure indicates the "**triangle route**" topology. It works fine if you turn off firewall function on ZyWALL box. However, if you turn on firewall, your connection will be blocked by firewall because of the following reason.

Step 1. Being the default gateway of PC, ZyWALL will receive all "outgoing" traffic from PC.

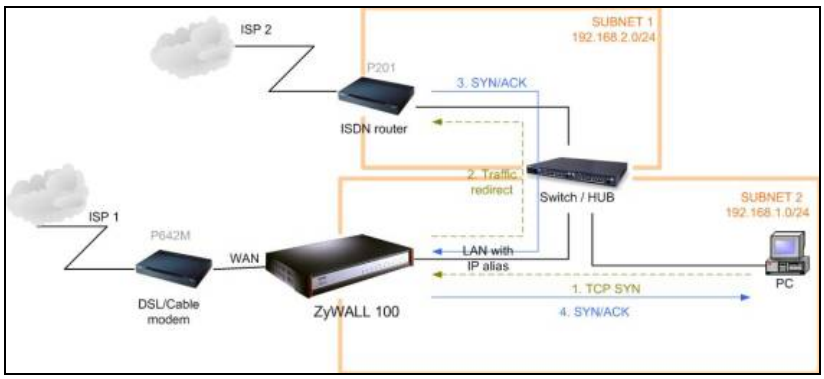
Step 2. And because of **Static route/Traffic Redirect/Policy Routing**, ZyWALL forwards the traffic to another gateway (ISDN/Router) which is in **the same segment** as ZyWALL's LAN.

Step 3. However the return traffic won't go back to ZyWALL, in stead, the "another gateway (ISDN/Router)" will send back the traffic to PC directly. Because the gateway (say, P201) and the PC are in the same segment.

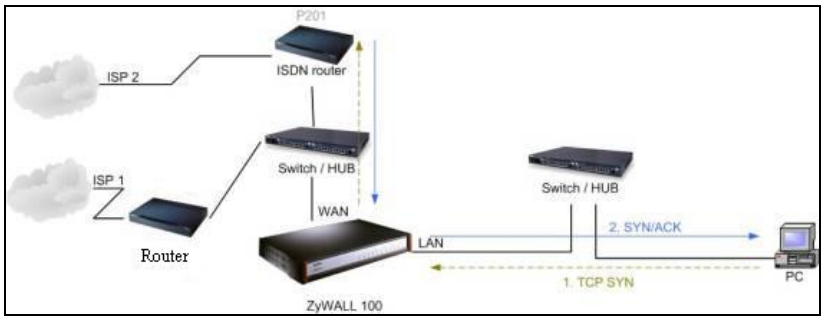
When firewall is turned on, ZyWALL will check the outgoing traffic by ACL and create dynamic sessions to allow return traffic to go back. To achieve Anti-DoS, ZyWALL will send RST packets to the PC and the peer since it never receives the TCP SYN/ACK packet. Thus the connection will always be reset by ZyWALL.

Solutions.

(A) Deploying your second gateway in IP alias segment is a better solution. In this way, your connection can be always under control of firewall. And thus there won't be Triangle Route problem.



(B) Deploying your second gateway on WAN side.



(C) To resolve this conflict, we add an option for users to allow/disallow such **Triangle Route** topology in both CI command and Web configurator. You can issue this command, "**sys firewall ignore triangle all on**", to allow firewall bypass triangle route checking. In Web GUI, you can find this option in firewall setup page.

But we would like to notify that if you allow Triangle Route, any traffic will be easily injected into the protected network through the unprotected gateway. In fact, it's a security hole in your protected network.

How can I protect against IP spoofing attacks?

The ZyWALL's firewall will automatically detect the IP spoofing and drop it if the firewall is turned on. If the firewall is not turned on we can configure a filter set to block the IP spoofing attacks. The basic scheme is as follows:

For the input data filter:

- Deny packets from the outside that claim to be from the inside
- Allow everything that is not spoofing us

Filter rule setup:

- Filter type =TCP/IP Filter Rule
- Active =Yes
- Source IP Addr =a.b.c.d
- Source IP Mask =w.x.y.z
- Action Matched =Drop
- Action Not Matched =Forward

Where a.b.c.d is an IP address on your local network and w.x.y.z is your netmask:

For the output data filters:

- Deny bounce back packet
- Allow packets that originate from us

Filter rule setup:

- Filter Type =TCP/IP Filter Rule
- Active =Yes
- Destination IP Addr =a.b.c.d
- Destination IP Mask =w.x.y.z
- Action Matched =Drop
- Action No Matched =Forward

Where a.b.c.d is an IP address on your local network and w.x.y.z is your net mask.

IPSec FAQ

What is VPN?

A VPN gives users a secure link to access corporate network over the Internet or other public or private networks without the expense of lease lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

Why do I need VPN?

There are some reasons to use a VPN. The most common reasons are because of security and cost.

Security

1). Authentication
With authentication, VPN receiver can verify the source of packets and guarantee the data integrity.
2). Encryption
With encryption, VPN guarantees the confidentiality of the original user data.

Cost

1). Cut long distance phone charges
Because users typically dial the their local ISP for VPN, thus, long distance phone charge is reduced than making a long direct connection to the remote office.

2).Reducing number of access lines
Many companies pay monthly charges for two types access lines: (1) high-speed links for their Internet access and (2) frame relay, ISDN Primary Rate Interface or T1 lines to carry data. A VPN may allow a company to carry the data traffic over its Internet access lines, thus reducing the need for some installed lines.

What are most common VPN protocols?

There are currently three major tunneling protocols for VPNs. They are Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and Internet Protocol Security (IPSec).

What is PPTP?

PPTP is a tunneling protocol defined by the PPTP forum that allows PPP packets to be encapsulated within Internet Protocol (IP) packets and forwarded over any IP network, including the Internet itself. The PPTP is supported in Windows NT and Windows 98 already. For Windows 95, it needs to be upgraded by the Dial-Up Networking 1.2 upgrade.

What is L2TP?

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

What is IPSec?

IPSec is a set of IP extensions developed by IETF (Internet Engineering Task Force) to provide security services compatible with the existing IP standard (IPv.4) and also the upcoming one (IPv.6). In addition, IPSec can protect any protocol that runs on top of IP, for instance TCP, UDP, and ICMP. The IPSec provides cryptographic security services. These services allow for authentication, integrity, access control, and confidentiality. IPSec allows for the information exchanged between remote sites to be encrypted and verified. You can create encrypted tunnels (VPNs), or just do encryption between computers. Since you have so many options, IPSec is truly the most extensible and complete network security solution.

What secure protocols does IPSec support?

There are two protocols provided by IPSec, they are AH (Authentication Header, protocol number 51) and ESP (Encapsulated Security Payload, protocol number 50).

What are the differences between 'Transport mode' and 'Tunnel mode?

The IPSec protocols (AH and ESP) can be used to protect either an entire IP payload or only the upper-layer protocols of an IP payload. Transport mode is mainly for an IP host to protect the data generated locally, while tunnel mode is for security gateway to provide IPSec service for other machines lacking of IPSec capability.
In this case, Transport mode only protects the upper-layer protocols of IP payload (user data). Tunneling mode protects the entire IP payload including user data.
There is no restriction that the IPSec hosts and the security gateway must be separate machines. Both IPSec protocols, AH and ESP, can operate in either transport mode or tunnel mode.

What is SA?

A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

What is IKE?

IKE is short for Internet Key Exchange. Key Management allows you to determine whether to use IKE (ISAKMP) or manual key configuration to set up a VPN.
There are two phases in every IKE negotiation- phase 1 (Authentication) and phase 2 (Key Exchange). Phase 1 establishes an IKE SA and phase 2 uses that SA to negotiate SAs for IPSec.

What is Pre-Shared Key?

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called 'Pre-shared' because you have to share it with another party before you can communicate with them over a secure connection.

What are the differences between IKE and manual key VPN?

The only difference between IKE and manual key is how the encryption keys and SPIs are determined.

- For IKE VPN, the key and SPIs are negotiated from one VPN gateway to the other. Afterward, two VPN gateways use this negotiated keys and SPIs to send packets between two networks.
- For manual key VPN, the encryption key, authentication key (if needed), and SPIs are predetermined by the administrator when configuring the security association.

IKE is more secure than manual key, because IKE negotiation can generate new keys and SPIs randomly for the VPN connection.

What is Phase 1 ID for?

In IKE phase 1 negotiation, IP address of remote peer is treated as an indicator to decide which VPN rule must be used to serve the incoming request. However, in some application, remote VPN box or client software is using an IP address dynamically assigned from ISP, so ZyWALL needs additional information to make the decision. Such additional information is what we call phase 1 ID. In the IKE payload, there are local and peer ID field to achieve this.

What are Local ID and Peer ID?

Local ID and Peer ID are used in IKE phase 1 negotiation. It’s in FQDN(Fully Qualified Domain Name) format, IKE standard takes it as one type of Phase 1 ID.
Phase 1 ID is identification for each VPN peer. The type of Phase 1 ID may be IP/FQDN (DNS)/User FQDN (E-mail). The content of Phase 1 ID depends on the Phase 1 ID type. The following is an example for how to configure phase 1 ID.

ID type	Content
IP	202.132.154.1
DNS	www.zyxel.com
E-mail	support@zyxel.com.tw

Please note that, in ZyWALL, if "DNS" or "E-mail" type is chosen, you can still use a random string as the content, such as "this_is_zywall". It's not neccessary to follow the format exactly.
By default, ZyWALL takes IP as phase 1 ID type for itself and it's remote peer. But if its remote peer is using DNS or E-mail, you have to adjust the settings to pass phase 1 ID checking.

When should I use FQDN?

If your VPN connection is ZyWALL to ZyWALL, and both of them have static IP address, and there is no NAT router in between, you can ignore this option. Just leave Local/Peer ID type as IP, and then skip this option.
If either side of VPN tunneling end point is using dynamic IP address, you may need to configure ID for the one with dynamic IP address. And in this case, "Aggressive mode" is recommended to be applied in phase 1 negotiation.

Is my ZyWALL ready for IPSec VPN?

IPSec VPN is available for ZyWALL since ZyNOS V3.50. It is free upgrade, no registration is needed. By upgrading the firmware and also configurations (romfile) to ZyNOS V3.50, the IPSec VPN capability is ready in your ZyWALL. You then can configure VPN via web configurator. Please download the firmware from our web site.

How do I configure ZyWALL VPN?

You can configure ZyWALL for VPN using Web configurator. ZyWALL 1 supports Web only.

How many VPN connections does ZyWALL support?

ZyWALL 1 supports 1 VPN connection. ZyWALL 10 supports 10 VPN connections. ZyWALL 50 supports 50 tunnels. ZyWALL 100 supports 100 tunnels.

What VPN protocols are supported by ZyWALL?

All ZyWALL series support ESP (protocol number 50) and AH (protocol number 51).

What types of encryption does ZyWALL VPN support?

ZyWALL supports 56-bit DES and 168-bit 3DES.

What types of authentication does ZyWALL VPN support?

VPN vendors support a number of different authentication methods. ZyWALL VPN supports both SHA1 and MD5.
AH provides authentication, integrity, and replay protection (but not confidentiality). Its main difference with ESP is that AH also secures parts of the IP header of the packet (like the source/destination addresses), but ESP does not.
ESP can provide authentication, integrity, replay protection, and confidentiality of the data (it secures everything in the packet that follows the header). Replay protection requires authentication and integrity (these two go always together). Confidentiality
(encryption) can be used with or without authentication/integrity. Similarly, one could use authentication/integrity with or without confidentiality.

I am planning my ZyWALL-to-ZyWALL VPN configuration. What do I need to know?

First of all, both ZyWALL must have VPN capabilities. Please check the firmware version, V3.50 or later has the VPN capability.
If your ZyWALL is capable of VPN, you can find the VPN options in **Advanced>VPN** tab.
For configuring a 'box-to-box VPN', there are some tips:

1. If there is a NAT router running in the front of ZyWALL, please make sure the NAT router supports to pass through IPSec.
2. In NAT case (either run on the frond end router, or in ZyWALL VPN box), only IPSec ESP tunneling mode is supported since NAT against AH mode.
3. **Source IP/Destination IP**-- Please do not number the LANs (local and remote) using the same exact range of private IP addresses. This will make VPN destination addresses and the local LAN addresses are indistinguishable, and VPN will not work.
4. **Secure Gateway IP Address** -- This must be a public, routable IP address, private IP is not allowed. That means it can not be in the 10.x.x.x subnet, the 192.168.x.x subnet, nor in the range 172.16.0.0 - 172.31.255.255 (these address ranges are reserved by internet standard for private LAN numberings behind NAT devices). It is usually a static IP so that we can pre-configure it in ZyWALL for making VPN connections. If it is a dynamic IP given by ISP, you still can configure this IP address after the remote ZyWALL is on-line and its WAN IP is available from ISP.

Does ZyWALL support dynamic secure gateway IP?

If the remote VPN gateways uses dynamic IP, we enter **0.0.0.0** as the **Secure Gateway IP Address** in ZyWALL. In this case, the VPN connection can only be initiated from dynamic side to fixed side in order to update its dynamic IP to the fixed side. However, if both gateways use dynamic IP addresses, it is no way to establish VPN connection at all.

What VPN gateway that has been tested with ZyWALL successfully?

We have tested ZyWALL successfully with the following third party VPN gateways.

- Cisco 1720 Router, IOS 12.2(2)XH, IP/ADSL/FW/IDS PLUS IPSEC 3DES
- NetScreen 5, ScreenOS 2.6.0r6
- SonicWALL SOHO 2
- WatchGuard Firebox II
- ZyXEL ZyWALL 100
- Avaya VPN
- Netopia VPN
- III VPN

What VPN software that has been tested with ZyWALL successfully?

We have tested ZyWALL successfully with the following third party VPN software.

- SafeNet Soft-PK, 3DES edition
- Checkpoint Software
- SSH Sentinel, 1.4
- SecGo IPSec for Windows
- F-Secure IPSec for Windows
- KAME IPSec for UNIX
- Nortel IPSec for UNIX
- Intel VPN, v. 6.90
- FreeS/WAN for Linux
- SSH Remote ISAKMP Testing Page, (http://isakmp-test.ssh.fi/cgi-bin/nph-isakmp-test)
- Windows 2000, Windows XP IPSec

Will ZyXEL support Secure Remote Management?

Yes, we will support it and we are working on it currently.

12. Does ZyWALL VPN support NetBIOS broadcast?

Yes, the ZyWALL does support NetBIOS broadcast over VPN.

Is the host behind NAT allowed to use IPSec?

NAT Condition	Supported IPSec Protocol
VPN Gateway embedded NAT	AH tunnel mode, ESP tunnel mode
VPN client/gateway behind NAT*	ESP tunnel mode
NAT in Transport mode	None

* The NAT router must support IPSec pass through. For example, for ZyWALL NAT routers, IPSec pass through is supported since ZyNOS 3.21. The default port and the client IP have to be specified in NAT menu Server Setup.

How do I configure ZyWALL with NAT for internal servers?

Generally, without IPSec, to configure an internal server for outside access, we need to configure the server private IP and its service port in NAT Server Table.

However, if both NAT and IPSec is enabled in ZyWALL, the edit of the table is necessary only if the connection is a non-secure connections. For secure connections, none NAT server settings are required since private IP is reachable in the VPN case.

For example:

host----ZyWALL(NAT)----ADSL Modem----Internet----Secure host
\
\
Non-secure host

I am planning my ZyWALL behind a NAT router. What do I need to know?

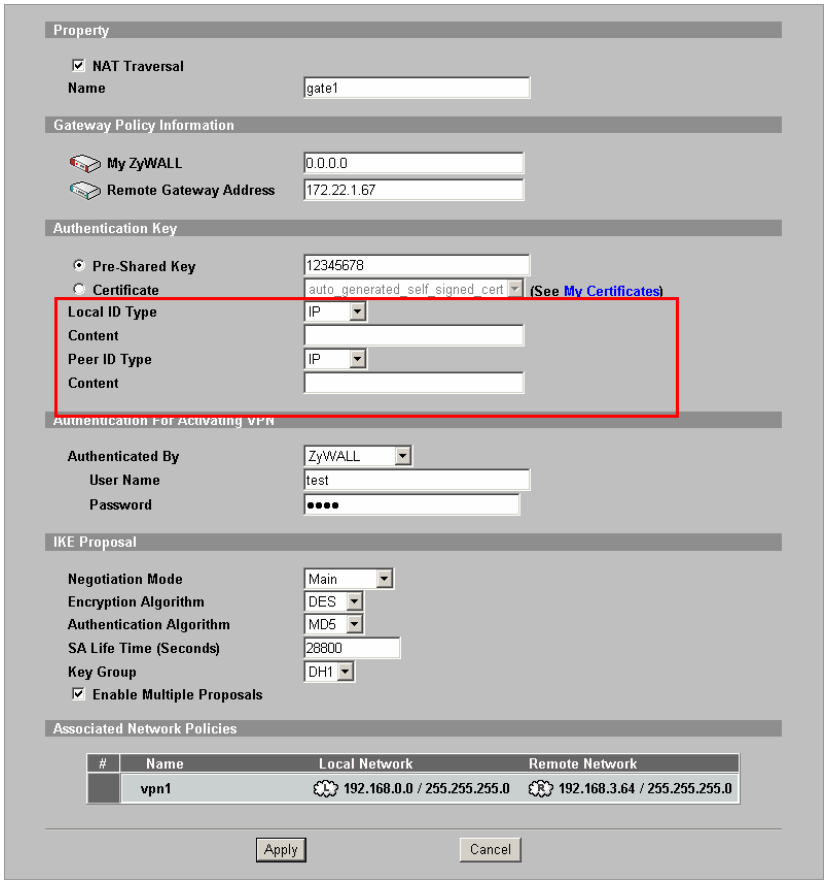
Some tips for this:

1. The NAT router must support to pass through IPSec protocol. Only ESP tunnel mode is possible to work in NAT case. In the NAT router is ZyWALL NAT router supporting IPSec pass through, default port and the ZyWALL WAN IP must be configured in NAT Server Table.
2. WAN IP of the NAT router is the tunneling endpoint for this case, not the WAN IP of ZyWALL.
3. If firewall is turned on in ZyWALL, you must forward **IKE** port in Internet interface.
4. If NAT are also enabled in ZyWALL, NAT server is required for non-secure connections, NAT server is not required for secure connections and the physical private IP is used.

For example:
host----ZyWALL----NAT Router----Internet----Secure host
\
\
Non-secure host

Where can I configure Phase 1 ID in ZyWALL?

Phase 1 ID can be configured in VPN setup menu as following..



How can I keep a tunnel alive?

To keep a tunnel alive, you can check "**Nailed-up**" option when configuring your VPN tunnel. With this option, the ZyWALL will keep IPSec tunnel up at all time. With "**Nailed-up**", the ZyWALL will try to establish whenever tunnel is terminated due to any unknown reason.

Single, Range, Subnet, which types of IP address do ZyWALL 10/10II/10W/50/100 support in VPN/IPSec?

The mentioned ZyWALL series support all of the types. In other words, you can specify a single PC, a range of PCs or even a network of PCs to utilize the VPN/IPSec service.

Does ZyWALL support IPSec pass-through?

Yes, ZyWALL can support IPSec pass-through. ZyWALL series don't only support IPSec/VPN gateway, it can also be a NAT router supporting IPSec pass-through.
If the VPN connection is initiated from the security gateway behind ZyWALL, no configuration is necessary for neither NAT nor Firewall.

If the VPN connection is initiated from the security gateway outside of ZyWALL, NAT port forwarding and Firewall forwarding are necessary.
To configure NAT port forwarding, please go to WEB interface, **Setup/ "NAT",** put the secure gateway's IP address in default server.
To configure Firewall forwarding, please go to WEB interface, **Setup/Firewall**, select Packet Direction to **WAN to LAN**, and create a firewall rule the forwards IKE(UDP:500).

Can ZyWALL behave as a NAT router supporting IPSec pass through and an IPSec gateway simultaneously?

No, ZyWALL can't support them simultaneously. You need to choose either one. If ZyWALL is to support IPSec pass through, you have to disable the VPN function on ZyWALL. To disable it, you can either deactivate each VPN rule or issue a CI command, "IPSec switch off".

PKI FAQ

Basic Cryptography concept

Encryption and decryption are two major operations involved in cryptography. Whenever we would like to send some secret over an insecure media, such as Internet, we may encrypt the secret before sending it out. The receiver thus needs the corresponding decryption key to recover the encrypted secrete. We need to have keys for both encryption and decryption. The key used to encrypt data is called the encryption key, and the key for decryption is called the decryption key.
Cryptography can be categorized into two types, *symmetric* and *asymmetric* cryptography. For symmetric cryptography, the encryption key is the same with the decryption. Otherwise, we the cryptography as asymmetric.
Symmetric cryptography, such as DES, 3DES, AES, is normally used for data transmission, since it requires less computation power than asymmetric cryptography. The task of privately choosing a key before communicating, however, can be problematic. Applications in real case may use asymmetric cryptography for to protect distribution of keys (symmetric), and uses symmetric cryptography for data transmission.
Asymmetric cryptography solves the key exchange problem by defining an algorithm which uses two keys, each of which can be used to encrypt a message. If one key is used to encrypt a message, then the other must be used to decrypt it. This makes it possible to receive secure messages by simply publishing one key (the public key) and keeping the other secret (the private key).

What is PKI?

PKI is acronym of Public Key Infrastructure. A PKI is a comprehensive system of policies, processes, and technologies working together to enable users of the Internet to exchange information securely and confidentially. Public Key Infrastructures are based on the use of cryptography – the scrambling of information by a mathematical formula and a virtual key so that it can only be decoded by an authorized party using a related key.
A PKI uses pairs of cryptographic keys provided by a trusted third party known as a Certification Authority (CA). Central to the workings of a PKI, a CA issues digital certificates that positively identify the holder's identity. A Certification Authority maintains accessible directories of valid certificates, and a list of certificates it has revoked.

What are the security services PKI provides?

PKI brings to the electronic world the security and confidentiality features provided by the physical documents, hand-written signatures, sealed envelopes and established trust relationships of traditional, paper-based transactions. These features are:
Confidentiality: Ensures than only intended recipients can read files.
Data Integrity: Ensures that files cannot be changed without detection.
Authentication: Ensures that participants in an electronic transaction are who they claim to be.
Non-repudiation: Prevents participants from denying involvement in an electronic transaction.

What are the main elements of a PKI?

A PKI includes:
A Certification Authority
Digital certificates
Mathematically related key pairs, each comprising a private key and a public key
These elements work within a formal structure defined by:
Certificate Policies
A Certification Practice Statement.

What is a Certification Authority?

A Certification Authority is a trusted third party that verifies the identity of an applicant registering for a digital certificate. Once a Certification Authority is satisfied as to the authenticity of an applicant's identity, it issues that person a digital certificate binding his or her identity to a public key. (Digital certificates are also issued to organizations and devices, but we will focus on people for the purposes of

this discussion.)

What is a digital certificate?

An electronic credential that vouches for the holder's identity, a digital certificate has characteristics similar to those of a passport – it has identifying information, is forgery-proof, and is issued by a trusted third party. Digital certificates are published in on-line directories. Typically, a digital certificate contains:
The user's distinguished name (a unique identifier)
The issuing Certification Authority's distinguished name
The user's public key
The validity period
The certificate's serial number
The issuing Certification Authority's digital signature is for verifying the information in the digital certificate.

What are public and private keys, and what is their relationship?

A PKI uses asymmetric cryptography to encrypt and decrypt information. In asymmetric cryptography, encryption is done by a freely available public key, and decryption is done by a closely guarded private key. Although the public and private keys in a particular key pair are mathematically related, it is impossible to determine one key from the other. Each key in an asymmetric key pair performs a function that only the other can undo.

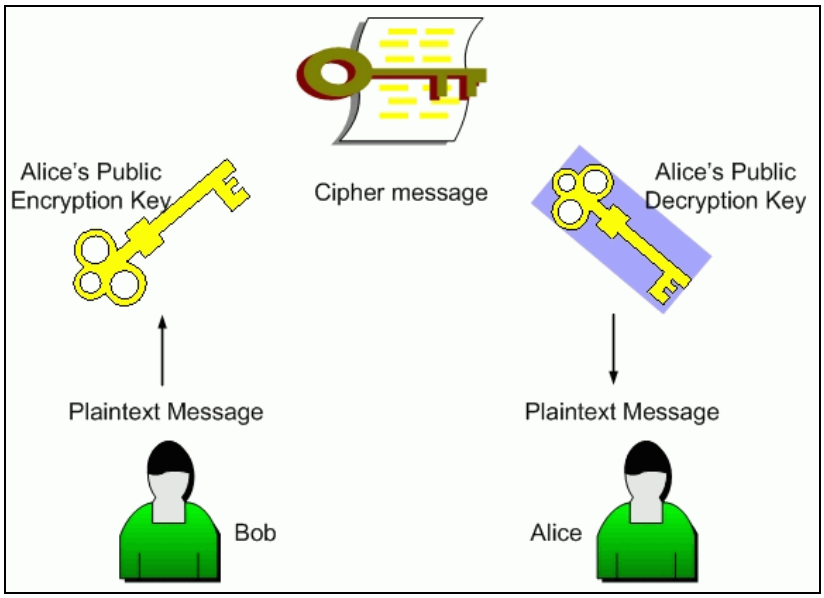
What are Certificate Policies (CPs)?

Certification Authorities issue digital certificates that are appropriate to specific purposes or applications. For example, in the Government of Canada Public Key Infrastructure, digital certificates for data confidentiality are different from those used for digital signatures. Certificate Policies describe the rules governing the different uses of these certificates.

How does a PKI ensure data confidentiality?

Users' public keys are published in an accessible directory. A person wishing to send an encrypted message uses the recipient's public key to scramble the information in the message. Only the recipient's private key can decrypt the message.
So, if Bob wants to send a confidential message to Alice, his PKI software finds Alice's public key in the directory where it is published, and he uses it to encrypt his message. When Alice receives the encrypted

message, she uses her private key to decrypt it. Because Alice keeps her private key secret, Bob can be assured that, even if his message were to be intercepted, only Alice can read it.



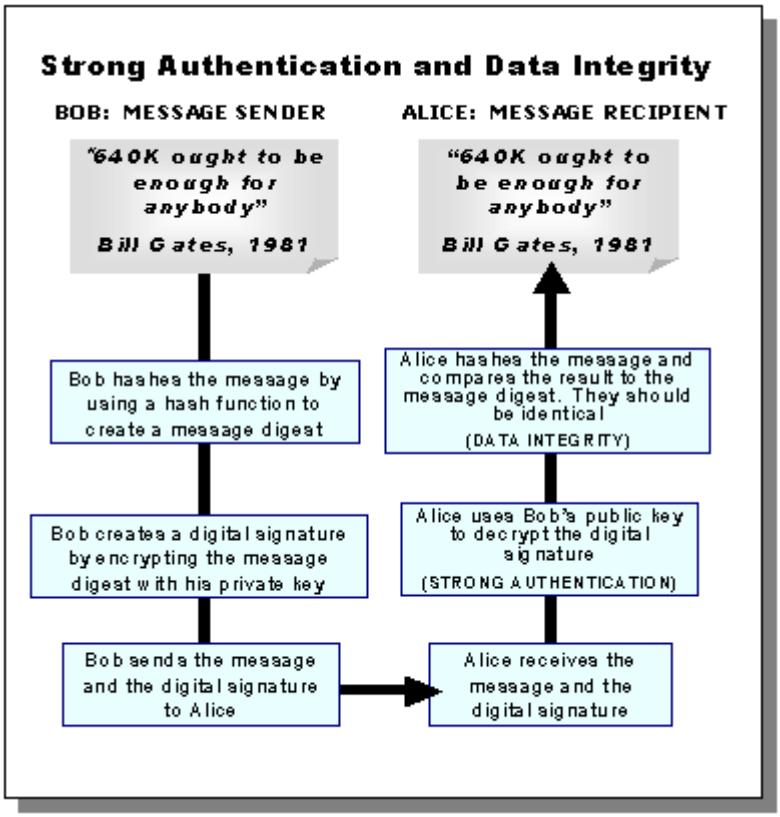
What is a digital signature?

Not to be confused with a digitized signature (a scan of a hand-written signature), a digital signature can be used with either encrypted or unencrypted messages to confirm the sender's identity and ensure the recipient that the message content has not been changed in transmission. Digital signatures incorporate the characteristics of hand-written signatures in that they can only be generated by the signer, are verifiable, and cannot easily be imitated or repudiated.

How does a digital signature work?

Suppose that the famous Bob and Alice wish to correspond electronically. Bob wants to assure Alice that he originated the electronic message, and that its contents have not been tampered with. He does so by signing the message with a digital signature.
When Bob clicks on the digital signature option on his e-mail application, special software applies a mathematical formula known as a hash function to the message, converting it to a fixed-length string of characters called a message digest. The digest acts as a "digital fingerprint" of the original message. If the original message is changed in any way, it will not produce the same message digest when the hash function is applied. Bob's software then encrypts the message digest with his private key, producing a digital signature of the message. He transmits the message and digital signature to Alice.
Alice uses Bob's public key to decrypt the digital signature, revealing the message digest. Since only Bob's public key can decrypt the digital signature, she is able to verify that Bob was the sender of the

message. This verification process also tells Alice's software which hash function was used to create the message digest of Bob's original message. To verify the message content, Alice's software applies the hash function to the message she received from Bob. The message digests should be identical. If they are, Alice knows the message has not been changed and she is assured of its integrity. (If Bob had wanted to ensure the confidentiality of his message, he could have encrypted it with Alice's public key before applying the hash function to the message.)
The best thing about all these encryption, decryption, verifying and authenticating processes is that special software does them all transparently, so that Bob and Alice receive the assurances they need without having actually to engage in computations themselves.



Does ZyXEL provide CA service?

No, ZyXEL doesn't maintain CA service for customers, customers need to find CA server (trusted 3rd party) in order to use PKI functionality on ZyWALL.

What if customers don't have access to CA service, but would like to use PKI function?

ZyXEL VPN solution provides a mechanism called "self-signed" Certificate. If you don't have access CA service, but would like to use PKI function, please use the self-signed Certificate. Check here for how to

configure it.

How can I have Self-signed certificate for ZyXEL appliance?

Each ZyXEL appliance would provide a Self-signed certificate along with default configuration file. You can check content of Self-signed certificate in WEB GUI.

Can I create self-signed certificates in addition to the default one?

Yes, you can create self-signed certificates of your own by selecting self-signed category when creating My Certificates.

Will Self-signed certificate be erased if I reset to default configuration file?

Yes, the original Self-signed certificate will be erased. But ZyXEL appliance will create a new self-signed certificate at it's first boot-up time after resetting the configuration. But the new self-signed certificate is different from the original one. So users also need to export the new self-signed certificate to appliance's peer if they would like to use PKI for VPN.

Will certificates stored in ZyXEL appliance be erased if I reset to default configuration file?

Yes, My Certificates, Trusted CAs' Certificates, and Trusted Remote's Certificates will be totally erased after erasing configuration files. Users need to enroll My Certificates and import Trusted CA's certificates & Trusted Remote's certificates again.

What can I do prior to reset appliance's configuration?

You can export Trusted CA's certificates and Trusted Remote's certificates before resetting configuration to the local computer. Then import them back to ZyXEL appliance.

If I export My Certificates from ZyXEL appliance, save them locally, and then import them back after resetting the configuration file, can I reuse the imported My Certificates ?

No, you can't reuse them. Each certificate stored in My Certificates has corresponding private key. When you erase the configuration, the corresponding private keys are also deleted. So you can't reuse the certificates by importing them afterward.