

ZyWALL P1

Security Appliance

Support Notes

Version 4.01

Sep. 2006



INDEX

Application Notes	6
General Application Notes	6
Internet Connection.....	6
Application of Bridge Mode	7
Bridge VPN.....	7
Application of Zero Configuration Mode	15
WAN Encapsulation Detection	15
Network Conflict Detection.....	17
VPN Network Conflict Detection.....	19
Other Enhancement.....	22
Multi-Client Support.....	22
Management FQDN.....	23
FAQ	27
ZyNOS FAQ	27
What is ZyNOS?.....	27
How do I upgrade/backup the ZyNOS firmware by using TFTP client program via LAN?	27
Why can't I make Telnet to ZyWALL from WAN?.....	27
What should I do if I forget the system password?.....	28
How many network users can the NAT support?	28
Product FAQ	28
Will the ZyWALL work with my Internet connection?.....	28
What do I need to use the ZyWALL?	28
What is PPPoE?	28
Does the ZyWALL support PPPoE?	29
How do I know I am using PPPoE?.....	29
Why does my Internet Service Provider use PPPoE?.....	29
How can I configure the ZyWALL?	29
What can we do with ZyWALL?	29
Does ZyWALL support dynamic IP addressing?.....	29
What is the difference between the internal IP and the real IP from my ISP?.....	29
How does e-mail work through the ZyWALL?	30
Is it possible to access a server running behind NAT from the outside Internet? If possible, how?.....	30

What DHCP capability does the ZyWALL support?	30
What network interface does the new ZyWALL series support?.....	30
How does the ZyWALL support TFTP?	30
Can the ZyWALL support TFTP over WAN?.....	31
How can I upload data to outside Internet over the one-way cable?	31
My ZyWALL can not get an IP address from the ISP to connect to the Internet, what can I do?.....	31
What is DDNS?.....	32
When do I need DDNS service?	32
What DDNS servers does the ZyWALL support?	32
What is DDNS wildcard?.....	32
Does the ZyWALL support DDNS wildcard?	32
Can the ZyWALL NAT handle IPSec packets sent by the VPN gateway behind ZyWALL?	33
How do I setup my ZyWALL for routing IPSec packets over NAT?	33
Firewall FAQ	33
What is a network firewall?	33
What makes ZyWALL secure?.....	33
What are the basic types of firewalls?	34
What kind of firewall is the ZyWALL?.....	34
Why do you need a firewall when your router has packet filtering and NAT built-in?.....	35
What is Denials of Service (DoS)attack?.....	35
What is Ping of Death attack?.....	35
What is Teardrop attack?	35
What is SYN Flood attack?.....	35
What is LAND attack?.....	36
What is Brute-force attack?	36
What is IP Spoofing attack?.....	36
How can I protect against IP spoofing attacks?.....	36
IPSec FAQ	37
What is VPN?	37
Why do I need VPN?	38
What are most common VPN protocols?.....	38
What is PPTP?	38
What is L2TP?	38
What is IPSec?	39

What secure protocols does IPSec support?	39
What are the differences between 'Transport mode' and 'Tunnel mode'?.....	39
What is SA?	39
What is IKE?.....	39
What is Pre-Shared Key?	40
What are the differences between IKE and manual key VPN?	40
What is Phase 1 ID for?	40
What are Local ID and Peer ID?.....	40
When should I use FQDN?	41
Is my ZyWALL ready for IPSec VPN?.....	41
What VPN protocols are supported by ZyWALL?	41
What types of encryption does ZyWALL VPN support?.....	41
What types of authentication does ZyWALL VPN support?.....	41
I am planning my ZyWALL-to-ZyWALL VPN configuration. What do I need to know?	42
Will ZyXEL support Secure Remote Management?.....	42
Does ZyWALL VPN support NetBIOS broadcast?.....	42
Is the host behind NAT allowed to use IPSec?	42
How do I configure ZyWALL with NAT for internal servers?.....	43
I am planning my ZyWALL behind a NAT router. What do I need to know?.....	43
How can I keep a tunnel alive?	44
PKI FAQ	44
Basic Cryptography concept.....	44
What is PKI?.....	45
What are the security services PKI provides?.....	45
What are the main elements of a PKI?.....	45
What is a Certification Authority?	45
What is a digital certificate?	46
What are public and private keys, and what is their relationship?.....	46
What are Certificate Policies (CPs)?.....	46
How does a PKI ensure data confidentiality?	46
What is a digital signature?.....	47
How does a digital signature work?.....	47
Does ZyXEL provide CA service?.....	48
What if customers don't have access to CA service, but would like to use PKI function?	48

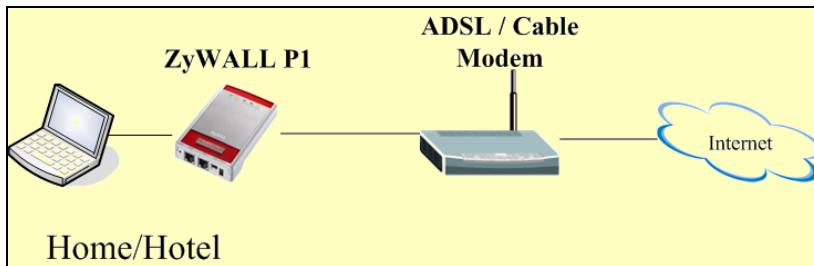
How can I have Self-signed certificate for ZyXEL appliance?	48
Can I create self-signed certificates in addition to the default one?	49
Will Self-signed certificate be erased if I reset to default configuration file?	49
Will certificates stored in ZyXEL appliance be erased if I reset to default configuration file?	49
What can I do prior to reset appliance's configuration?.....	49
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 ?	49

Application Notes

General Application Notes

Internet Connection

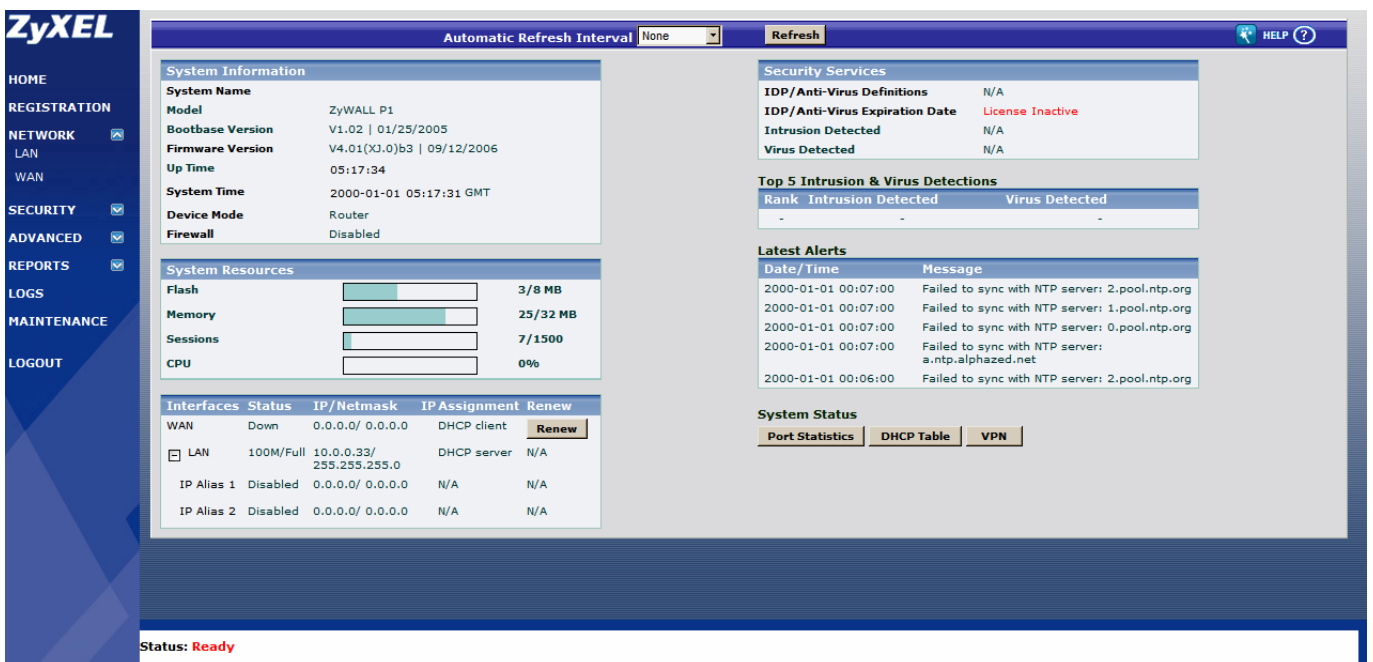
A typical Internet access application of the ZyWALL P1 is shown below. For a teleworker or road warrior, there are some secure settings need to be checked before accessing the Internet.



- **Before you begin**

The ZyWALL P1 is shipped with the following factory default:

1. LAN IP address = 192.168.167.1, subnet mask = 255.255.255.0/24
2. DHCP server enabled with IP pool starting from 192.168.167.33
3. Default Web GUI menu password = 1234
4. The 4.01 release's new dashboard just looks like this:



Application of Bridge Mode

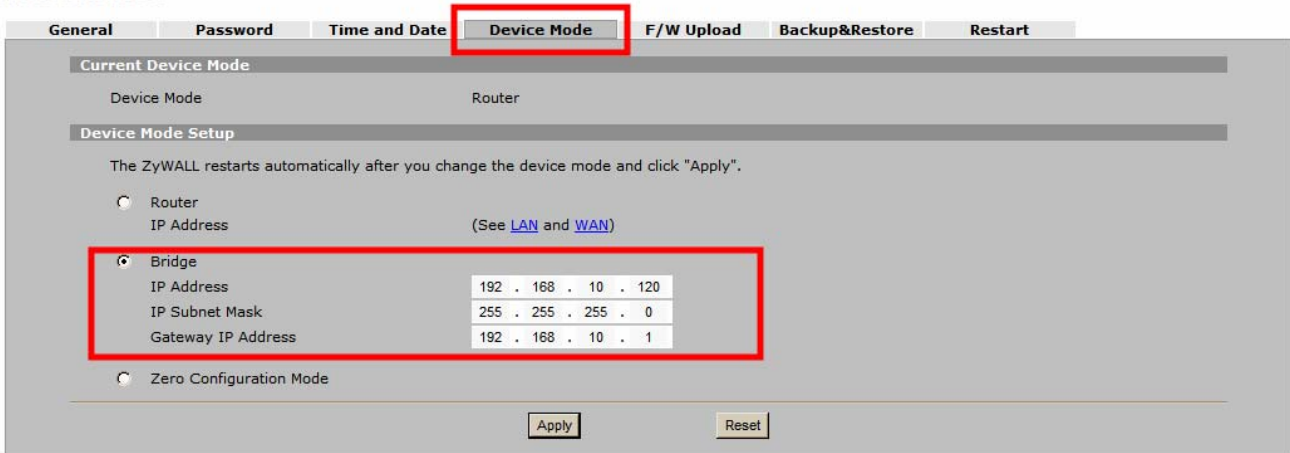
Bridge VPN

The ZyWALL P1 supports three kinds of operation mode: Route 、 Bridge 、 and Zero configuration. In bridge mode, the ZyWALL P1 functions as a transparent firewall (also known as a bridge firewall). The ZyWALL P1 bridges traffic traveling between the ZyWALL P1's two interfaces and still filters and inspects packets. Hence you do not need to change the configuration of your existing network to use the ZyWALL P1 in bridge mode.

In bridge mode, the ZyWALL P1 can not get an IP address from a DHCP server. The LAN and WAN interfaces have the same (static) IP address and subnet mask. You can configure the ZyWALL P1's IP address in order to access the ZyWALL P1 for management. If you connect your computer directly to the ZyWALL P1, you also need to assign your computer a static IP address in the same subnet as the ZyWALL P1's IP address in order to access the ZyWALL P1.

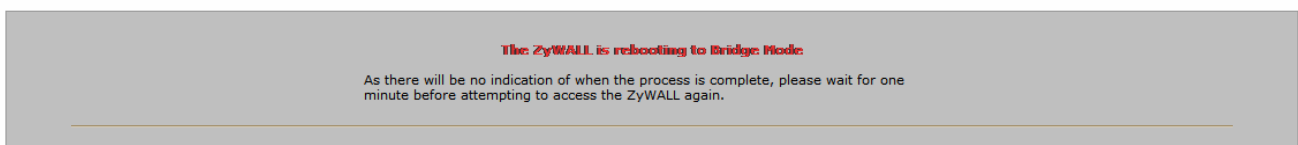
The configuration just likes below:

MAINTENANCE

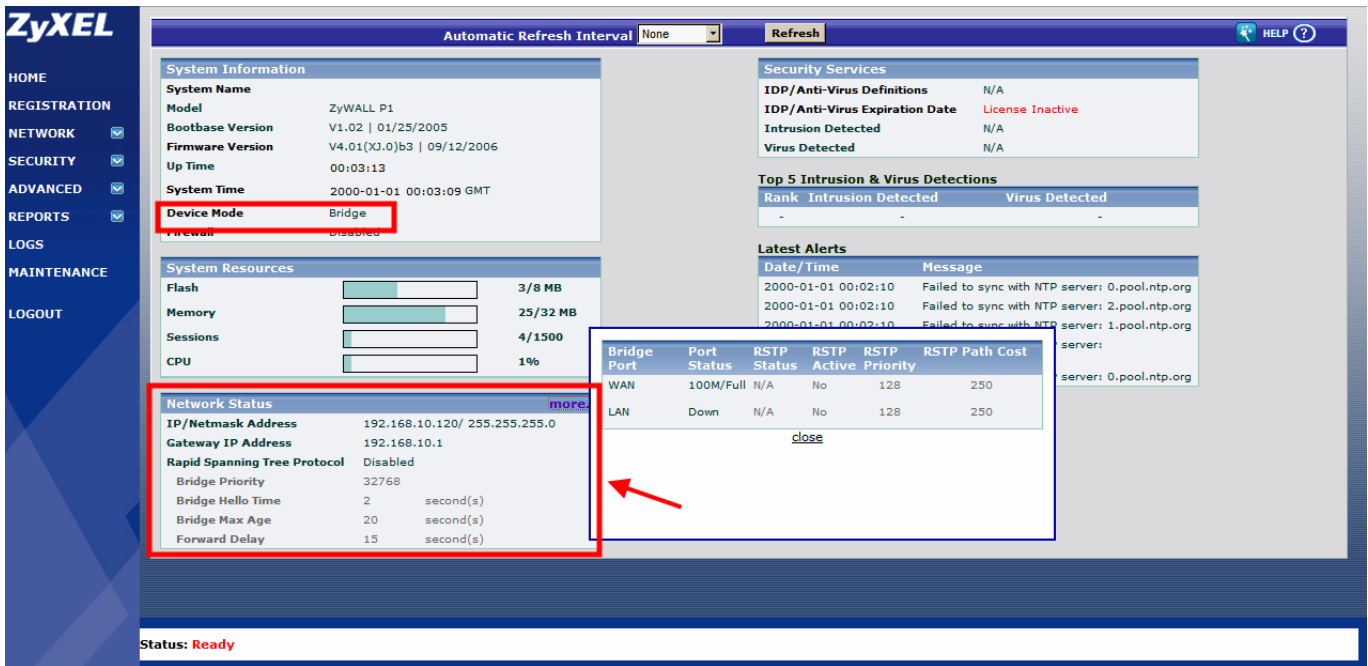


After press the 'Apply' button, the device would reboot and change to the Bridge mode.

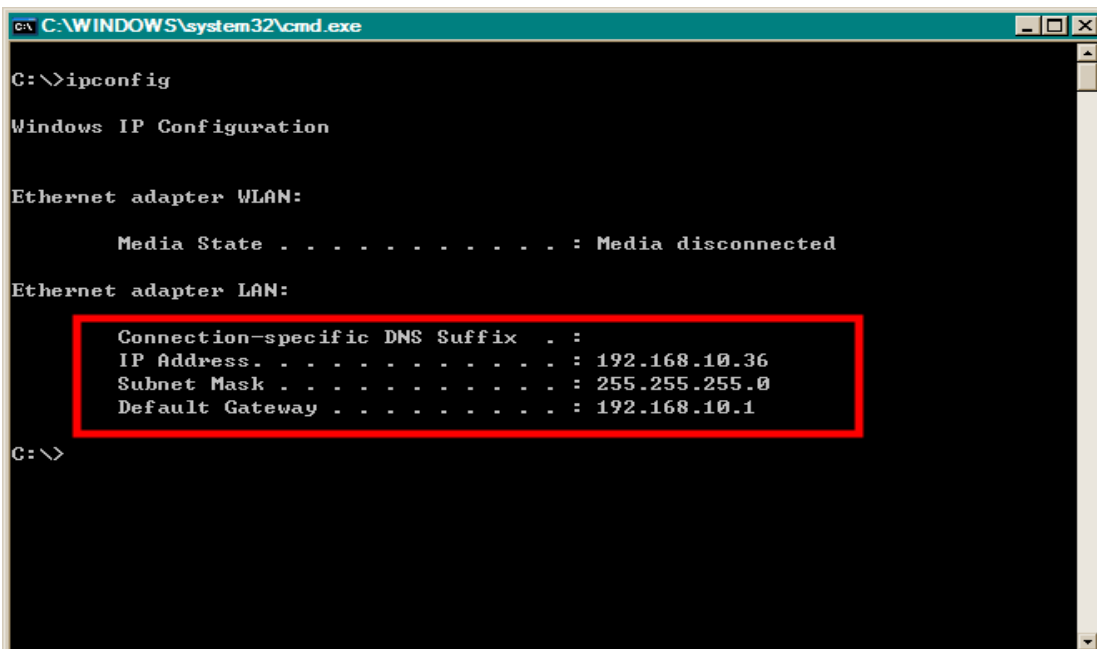
MAINTENANCE - CHANGE TO BRIDGE MODE



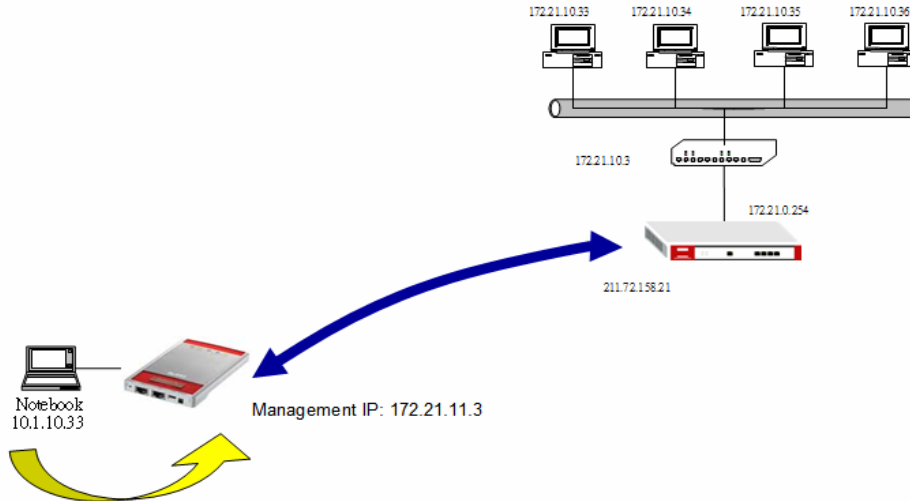
After the device reboot, the dashboard would show the new status about Bridge mode.



The PC/Notebook connects to the ZyWALL P1's LAN would also get the IP address on the same subnet.



Since now ZyWALL P1 is in bridge mode, it would use the IP address of PC/Notebook behind ZyWALL P1 for the VPN secure gateway IP. This is also what we called the “IP Hijack mode”.



Here, for example, using the ZyWALL 1050 as the peer security gateway.

LAN	ZyWALL P1 (Bridge)	ZyWALL 1050	LAN
192.168.10.36	192.168.10.120	WAN: 192.168.10.50 LAN: 192.168.105.1	192.168.105.0/24

Step.1: Setup the ZyWALL P1's Gateway Policy.

VPN - GATEWAY POLICY - EDIT

Property

Name: zw1050

NAT Traversal

Gateway Policy Information

My ZyWALL: 192.168.10.120

Primary Remote Gateway: 192.168.10.50 (Domain Name or IP Address)

Enable IPSec High Availability

Redundant Remote Gateway: (Domain Name or IP Address)

Fall back to Primary Remote Gateway when possible

Fall Back Check Interval*: 26800 (180~86400 seconds)

*Fall Back Check Interval: The time interval for checking availability of Primary Remote Gateway. IPSec SA life time will be superseded by this value when it is larger than this value.

Authentication Key

Pre-Shared Key: 12345678

Certificate: auto_generated_self_signed_cert (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: IP

Content: 0.0.0.0

Extended Authentication

gray-out

Enable Extended Authentication

Server Mode (Search Local User first then RADIUS)

Client Mode

Authenticated By: XAUTH Server

User Name:

Password:

IKE Proposal

Negotiation Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

SA Life Time (Seconds): 28800

Key Group: DH1

Enable Multiple Proposals

Associated Network Policies

#	Name	Local Network	Remote Network
	zw1050VPN	192.168.10.36	192.168.105.0 / 255.255.255.0

Apply Cancel

Step.2: Setup the ZyWALL P1's Network Policy

VPN - NETWORK POLICY - EDIT

Property

Active
Name: zw1050VPN
Protocol: 0
 Nailed-Up
 Check IPSec Tunnel Connectivity Log
Ping this Address: 0 . 0 . 0 . 0

Gateway Policy Information

Gateway Policy: zw1050

Virtual Address Mapping Rule:

Active
Virtual Address Mapping Rule: Port Forwarding Rules
Type: One-to-One
Private Starting IP Address: 0 . 0 . 0 . 0
Private Ending IP Address: 0 . 0 . 0 . 0
Virtual Starting IP Address: 0 . 0 . 0 . 0
Virtual Ending IP Address: 0 . 0 . 0 . 0

Local Network

Address Type: Single Address
Starting IP Address: 192 . 168 . 10 . 36
Ending IP Address / Subnet Mask: 0 . 0 . 0 . 0
Local Port: Start 0 End 0

Remote Network

Address Type: Subnet Address
Starting IP Address: 192 . 168 . 105 . 0
Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0
Remote Port: Start 0 End 0

IPSec Proposal

Encapsulation Mode: Tunnel
Active Protocol: ESP
Encryption Algorithm: DES
Authentication Algorithm: MD5
SA Life Time (Seconds): 28800
Perfect Forward Secrecy (PFS): NONE
 Enable Replay Detection
 Enable Multiple Proposals

Apply Cancel

Step.3: Setup the ZyWALL 1050's VPN Gateway

ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway > Edit > #1

VPN Gateway

VPN Gateway Name: Remote-Dialup

IKE Phase 1

Negotiation Mode: Main

Proposal:

#	Encryption	Authentication	
1	DES	MD5	

Key Group: DH1

SA Life Time (Seconds): 28800 <180 - 3000000>

NAT Traversal

Dead Peer Detection (DPD)

Property

My Address:

- Interface: ge2 DHCP client -- 192.168.10.50/255.255.255.0
- Domain Name:

Secure Gateway Address:

1. 0.0.0.0
2. 0.0.0.0

← for Remote-Dialup case

Authentication Method

Pre-Shared Key: 12345678

Certificate: (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: IP

Content: 0.0.0.0

Extended Authentication

Enable Extended Authentication

Server Mode: default

Client Mode:

User Name:

Password:

OK Cancel

Message Ready

Step.4: Setup the ZyWALL 1050's Connection Setting

ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Connection > Edit > #1

VPN Connection

Connection Name: Remote-Dialup

VPN Gateway

Name: Remote-Dialup
ge2 Remote-Dialup

Phase 2

Active Protocol: ESP
Encapsulation: Tunnel
Proposal:

#	Encryption	Authentication	
1	DES	MD5	<input type="button" value="Delete"/>

SA Life Time (Seconds): 28800 (180 - 3000000)
Perfect Forward Secrecy (PFS): none

Policy

Policy Enforcement

Local policy: LAN_SUBNET SUBNET, 192.168.105.0/24
Remote policy: Remote-Subnet SUBNET, 0.0.0.0/0

Property

Nailed-Up
 Enable Replay Detection
 Enable NetBIOS broadcast over IPSec

Inbound/Outbound traffic NAT

Outbound Traffic

Source NAT

Source: NONE
Destination: NONE
SNAT: NONE

Inbound Traffic

Source NAT

Source: NONE
Destination: NONE
SNAT: NONE

Destination NAT

#	Original IP	Mapped IP	Protocol	Original Port	Mapped Port	
---	-------------	-----------	----------	---------------	-------------	--

Message: Ready.

Step.5: Dial the connection from Remote side (must from remote side), then you could see the tunnel is built from the ZyWALL P1 to the ZyWALL 1050 but using the host's IP address.

VPN

VPN Rules (IKE) SA Monitor Global Setting

VPN Rules

Local Network My ZyWALL Internet VPN Tunnel Remote Gateway Remote Network

Zero Configuration VPN Rules

Activating VPN Rule : zw1050VPN

#	VPN Rules	Local IP	Remote IP	Actions
1	zw1050	192.168.10.120	192.168.10.50	[Edit] [Delete] [Refresh]
	zw1050VPN	192.168.10.36	192.168.105.0 / 255.255.255.0	[Add] [Edit] [Delete] [Refresh]

ZyWALL 1050 > Configuration > Network > IPSec VPN > SA Monitor

VPN Connection VPN Gateway Concentrator SA Monitor

Current IPSec Security Associations

#	Name	Encapsulation	Policy	Algorithm	Up Time	Timeout	Inbound (Bytes)	Outbound (Bytes)	Actions
1	Remote-Dialup	Tunnel	192.168.105.0/24<->192.168.10.36	DES/MD5	2028	26802	0	0	[Refresh]

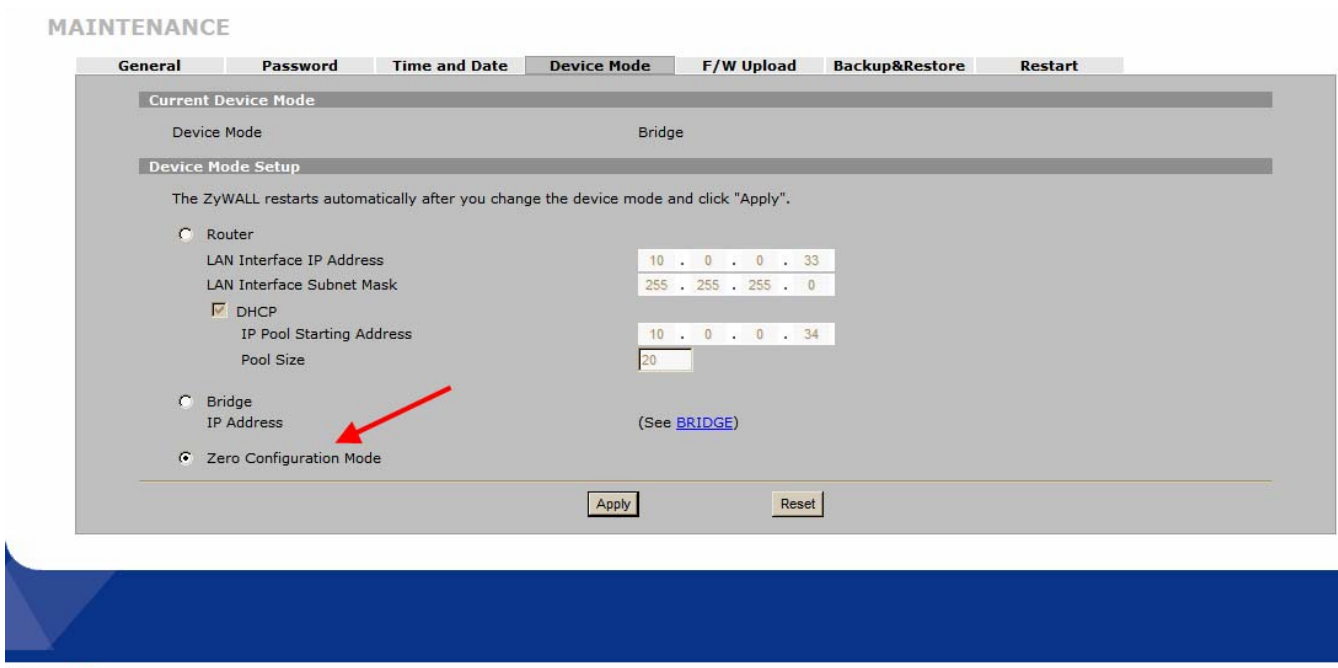
Refresh

192.168.10.36 is host's IP address instead of ZyWALL P1's

Application of Zero Configuration Mode

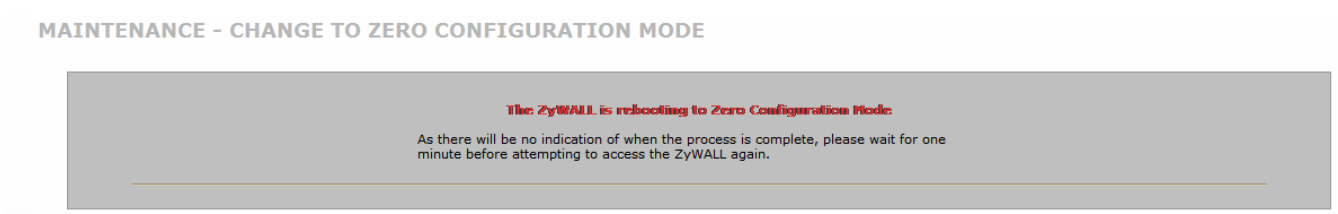
WAN Encapsulation Detection

On ZyWALL P1 4.01 release, it supports a new operation mode called “Zero Configuration Mode”. When you change to the Zero Configuration mode, it would configure the ZyWALL P1’s most settings automatically. This is very useful and easily for travelers or telecommuters usage.

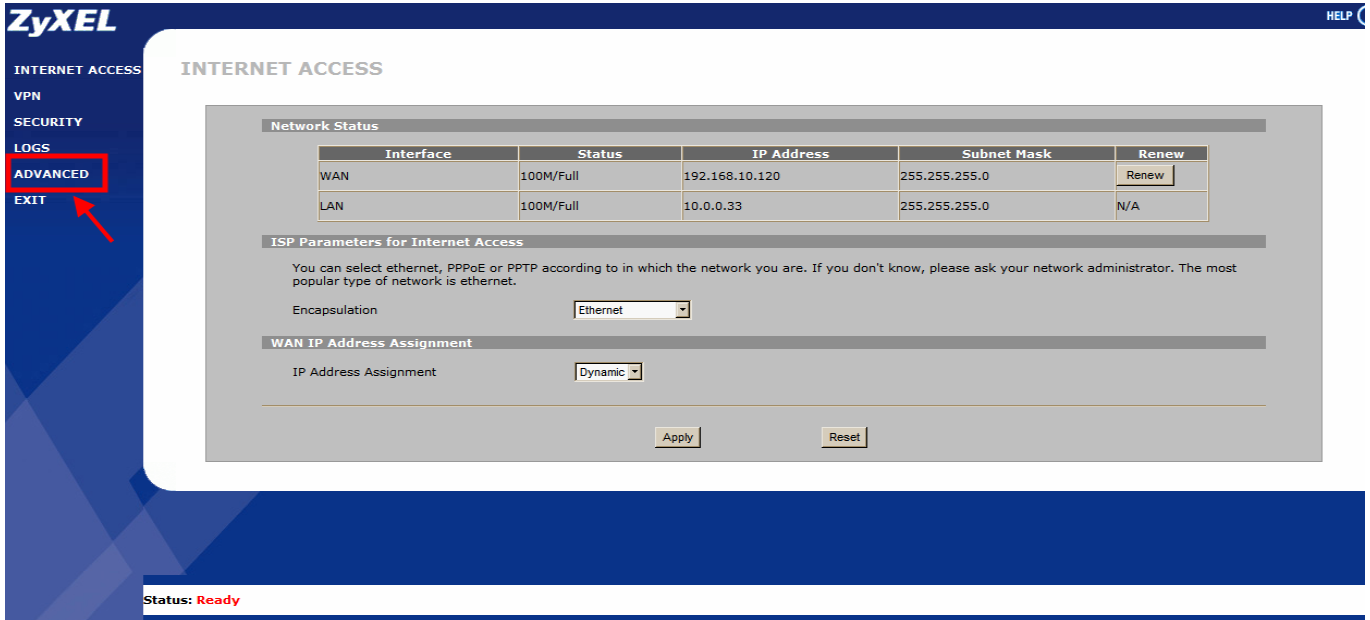


Status: Ready

After press the Apply button, the device will show it just changes to the Zero Configuration Mode.



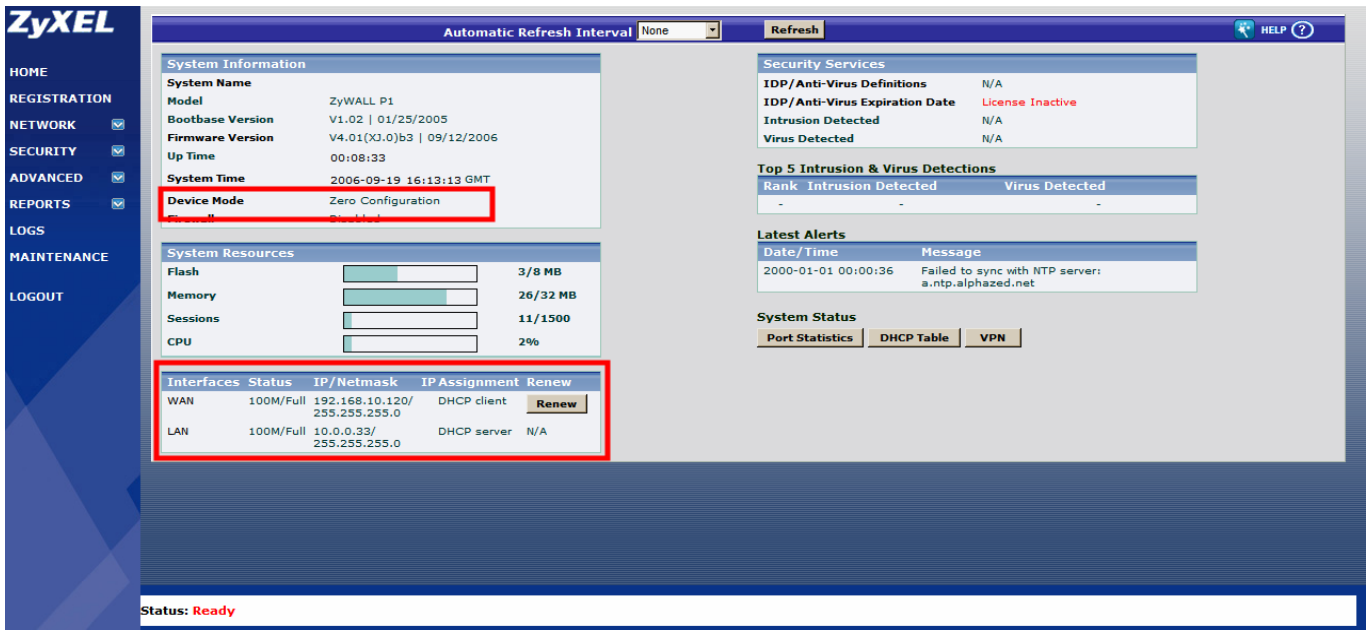
After device reboot, you would see a totally different view of the dashboard. It just gives you a brief view, and you could get more details by clicking the “Advanced”.



This is the Advance page and you would feel it quite similar the Router or Bridge mode’s GUI.

If the device is in the Zero Configuration Mode, it will detect the WAN link encapsulation type automatically. Currently, the ZyWALL P1 could detect PPPoE and DHCP network environment exactly. When the WAN link is up, the device will send DHCP-Discover and PPPoE Active Discovery Initiation (PADI) packet to examine whether there is a DHCP server or a PPPoE server in the WAN link. If there is a DHCP server, the DHCP server will send a DHCP-Offer packet to reply the device’s DHCP-Discover packet. If there is a PPPoE server, the PPPoE server will send a PPPoE Active Discovery Offer (PADO) packet to reply the device’s PADI packet.

If the device sends probing packet many times and still get no response, the WAN network configurations might be static IP or PPTP



Network Conflict Detection

Hence the most usage of ZyWALL P1 is for Teleworker or Road warrior, it is a big chance that the LAN setting conflicts with WAN setting that got from the Hotel or Partner's office. To keep user's Internet access and VPN access, when the WAN configuration conflicts with the LAN configuration in the Zero Configuration Mode, the device will re-write LAN DHCP/Static DHCP configurations, IP alias configurations, NAT over IPSEC configurations and NAT over IPSEC port forwarding rules.

Let's see how the ZyWALL P1 works:

Step.1: You just power on the ZyWALL P1 and do not plug the WAN connect yet.

The screenshot shows the ZyWALL P1 web management interface. At the top, there is a navigation bar with 'Automatic Refresh Interval' set to 'None' and a 'Refresh' button. The main content area is divided into several sections:

- System Information:** Lists details such as System Name (ZyWALL P1), Model, Bootbase Version (V1.02), Firmware Version (V4.01), Up Time (00:31:20), and System Time (2006-09-19 16:36:00 GMT). The 'Device Mode' is highlighted with a red box and set to 'Zero Configuration'.
- System Resources:** Displays progress bars for Flash (3/8 MB), Memory (26/32 MB), Sessions (26/1500), and CPU (1%).
- Interfaces:** A table with columns for Interfaces, Status, IP/Netmask, IP Assignment, and Renew. The WAN interface is 'Down' with IP 0.0.0.0/0.0.0.0. The LAN interface is '100M/Full' with IP 192.168.10.83/255.255.255.0. A red box highlights this table, and a red arrow points to it with the text 'WAN is down and the LAN subnet is 192.168.10.x'.
- Security Services:** Shows 'IDP/Anti-Virus Definitions' as N/A and 'IDP/Anti-Virus Expiration Date' as 'License Inactive'.
- Top 5 Intrusion & Virus Detections:** A table with columns for Rank, Intrusion Detected, and Virus Detected, all showing dashes.
- Latest Alerts:** A table with columns for Date/Time and Message. One alert is shown: '2000-01-01 00:00:36 Failed to sync with NTP server: a.ntp.alphazed.net'.
- System Status:** Includes buttons for 'Port Statistics', 'DHCP Table', and 'VPN'.

At the bottom left, the status is indicated as 'Status: Ready'.

Step.2: When plug the WAN connect, it would do the WAN Encapsulation Diction automatically. Then the ZyWALL P1 will get an IP address via DHCP as 192.168.10.x. Bump! The conflict happens! The ZyWALL P1's LAN Led would start to flash and the PC starts to acquire the new IP address.

```
C:\WINDOWS\system32\cmd.exe
Media State . . . . . : Media disconnected

Ethernet adapter LAN:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 192.168.10.34
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.83

C:\>ipconfig

Windows IP Configuration

Ethernet adapter WLAN:

    Media State . . . . . : Media disconnected

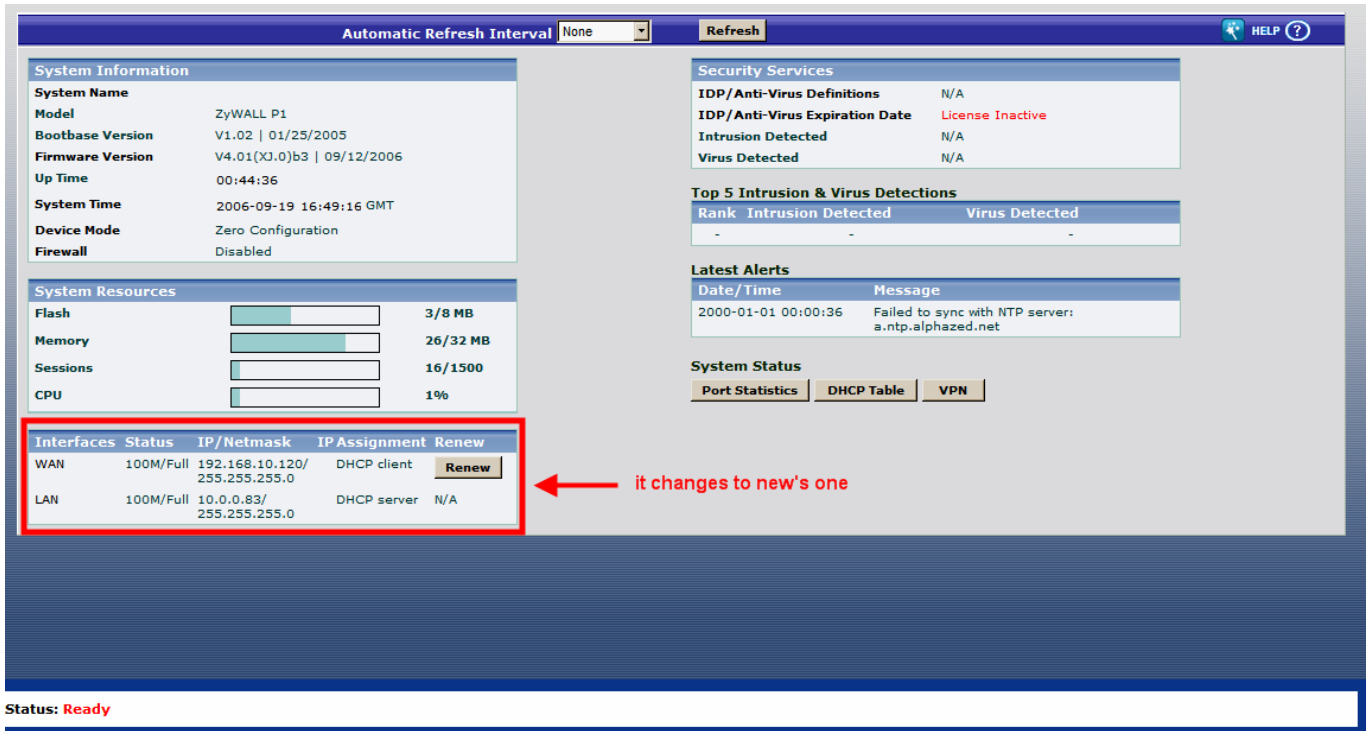
Ethernet adapter LAN:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 10.0.0.34
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.83

C:\>
```

The screenshot shows a Windows command prompt window. The user has run the 'ipconfig' command. The output shows the configuration for the LAN interface. The IP address is 192.168.10.34, the subnet mask is 255.255.255.0, and the default gateway is 192.168.10.83. A red box highlights this information. Below, the output for the WLAN interface is shown, with a red arrow pointing from the LAN output to the WLAN output. The WLAN interface is also shown with a red box highlighting its configuration: IP address 10.0.0.34, subnet mask 255.255.255.0, and default gateway 10.0.0.83.

Step.3: From the dashboard, you could see the WAN IP is 192.168.10.120, and the LAN subnet changes from 192.168.10.x to 10.0.0.x. Thus, this method could help the users to solve the network conflict problem automatically.



VPN Network Conflict Detection

For mobile users, it has high probability that the subnets of different client are the same (especially the system Administrator did not change the default setting so each ZyWALL P1 using same setting on it). To prevent the conflict situation, the ZyWALL P1 supports NAT over IPSec only in the Zero Configuration mode. And it only supports the SNAT that translates local network to another network.

It is work as shown as below:

Step.1: Setup the VPN tunnel as what we did on previous 'Bridge VPN' Chapter.

VPN

VPN Rules (IKE) SA Monitor Global Setting

VPN Rules

Local Network My ZyWALL Internet VPN Tunnel Remote Gateway Remote Network

Zero Configuration VPN Rules

Activating VPN Rule : zw1050VPN

#	VPN Rules	192.168.10.120	192.168.10.50	
1	zw1050	192.168.10.120	192.168.10.50	
	zw1050VPN	10.0.0.0 / 255.255.255.0	192.168.105.0 / 255.255.255.0	

Step.2: So far you could see the policy is from 10.0.0.0/24 to 192.168.105.0/24.

VPN

VPN Rules (IKE) SA Monitor Global Setting

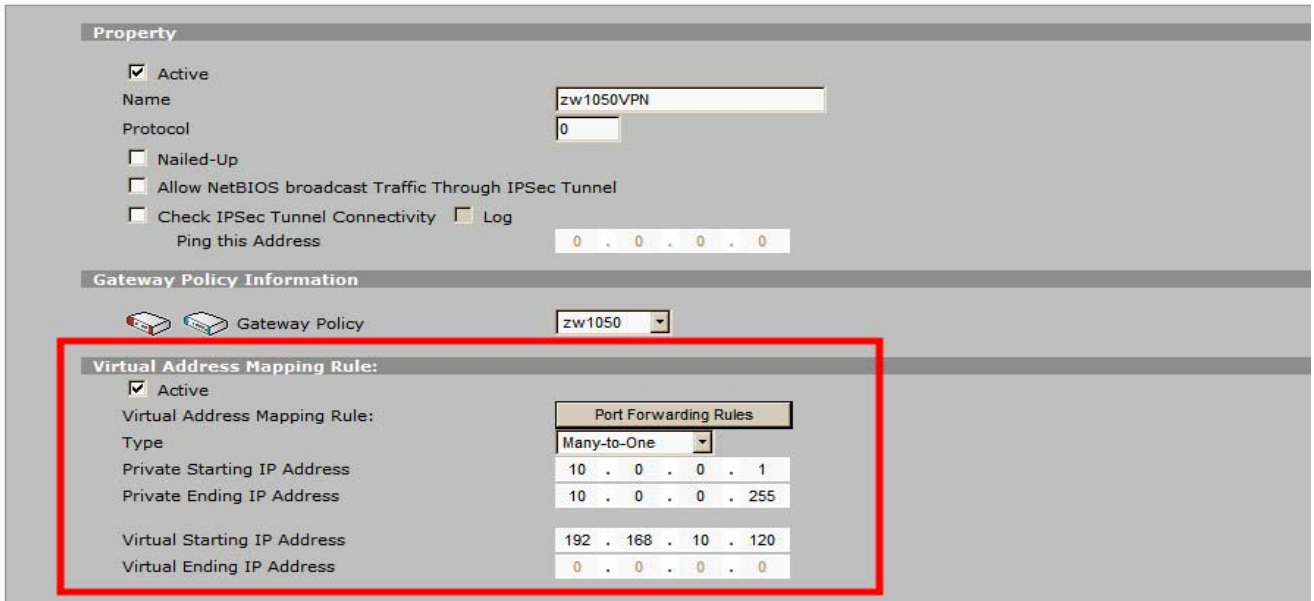
Security Associations Table

#	Name	Local Network	Remote Network	Encapsulation	IPSec Algorithm
1	zw1050VPN	10.0.0.0 / 255.255.255.0	192.168.105.0 / 255.255.255.0	Tunnel	ESP DES--MD5

Refresh Disconnect

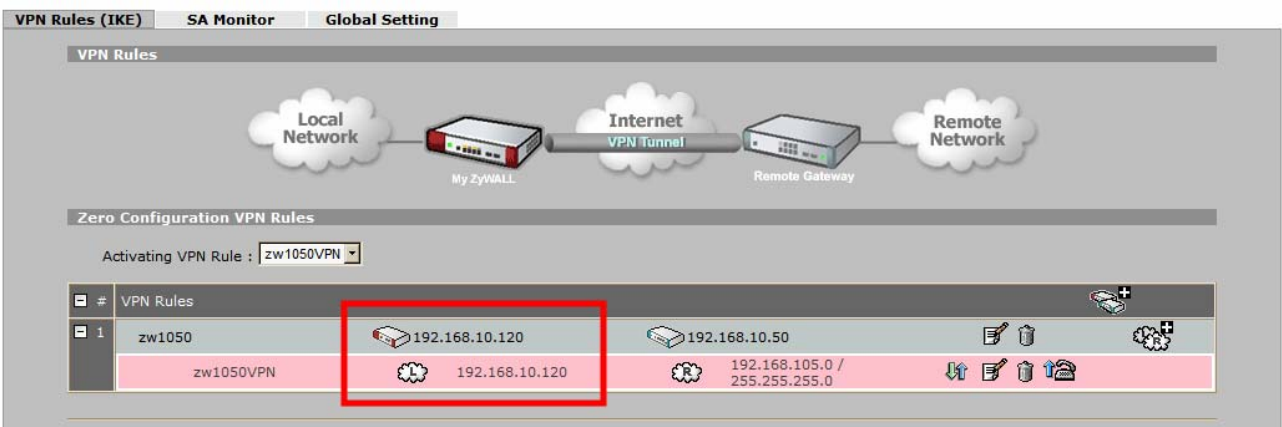
Step.3: Then we configure the Virtual Address Mapping Rule to use the security gateway's – the ZyWALL P1- IP address instead of the Local subnet (10.0.0.0/24) setting.

VPN - NETWORK POLICY - EDIT



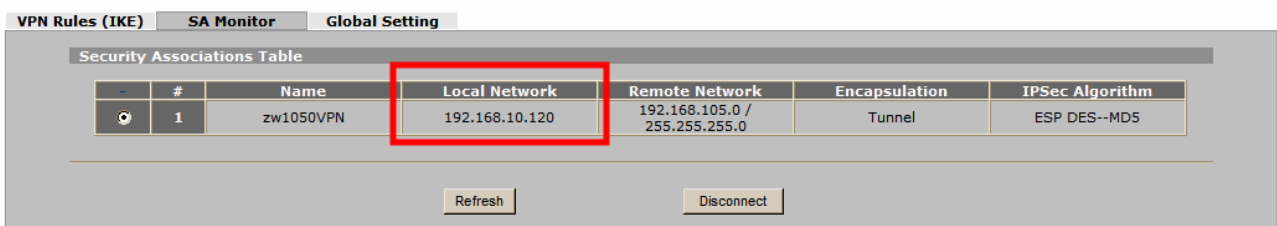
Step.4: After that, you could see the policy change from 10.0.0.0 to 192.168.10.120.

VPN



Step.5: After the VPN tunnel establish successfully, the SA also shows the policy from both sides is 192.168.10.120 and 192.168.105.0/24.

VPN



Other Enhancement

Multi-Client Support

On previous version, the ZyWALL P1 only supports one DHCP client behind it.

On ZyWALL P1 4.01 release, it supports multi-client now. You could configure this by setting the DHCP pool size.

LAN

LAN		Static DHCP	MAC Filter
LAN TCP/IP			
IP Address	10 . 0 . 0 . 83	RIP Direction	Both
IP Subnet Mask	255 . 255 . 255 . 0	RIP Version	RIP-1
Multicast	None		
DHCP Setup			
DHCP	Server	Pool Size	80
IP Pool Starting Address	10 . 0 . 0 . 1		
DHCP WINS Server 1	0 . 0 . 0 . 0		
DHCP WINS Server 2	0 . 0 . 0 . 0		
DNS Servers Assigned by DHCP Server			
First DNS Server	From ISP	172 . 23 . 5 . 2	
Second DNS Server	From ISP	192 . 168 . 10 . 1	
Third DNS Server	From ISP	0 . 0 . 0 . 0	
Windows Networking (NetBIOS over TCP/IP)			
<input type="checkbox"/> Allow between LAN and WAN			
Note: You also need to create a Firewall rule.			
		Apply	Reset

Status: Configuration updated successfully

Management FQDN

If the user wants to manage the ZyWALL P1, he can easily to access it just by typing the domain name, like “http://myZywallP1.com”. Then the DNS client will send the DNS query to the DNS server. The ZyWALL P1 would check every DNS query packet and if it finds a packet is queried the configured FQDN, myZywallP1.com, it will hijack the DNS server and return response to the client. Then the client can connect to the device using the IP address. It also very easily for System Administrator to manage these ZyWALL P1 even users change the management IP address.

It only supports the query coming from LAN side. And it only supports the DNS query, the inverse query is not supported.

Step.1: Enable and setup the FQDN you want to use.

MAINTENANCE

The screenshot shows the 'MAINTENANCE' page with several tabs: General, Password, Time and Date, Device Mode, F/W Upload, Backup&Restore, and Restart. The 'General' tab is selected, showing the 'General Setup' section. In this section, the 'Enable Management FQDN' checkbox is checked and highlighted with a red box. Below it, the 'Management FQDN' field contains the text 'myzywallp1.com'. Other fields include 'System Name', 'Domain Name', and 'Administrator Inactivity Timer' (set to 0). Below the 'General Setup' section is the 'DNS Servers Used by System' section, which has three rows for 'First DNS Server', 'Second DNS Server', and 'Third DNS Server'. Each row has a dropdown menu set to 'From ISP' and a corresponding IP address field. The IP addresses are 172.23.5.2, 192.168.10.1, and 0.0.0.0 respectively. At the bottom of the page are 'Apply' and 'Reset' buttons.

Step.2: After this setting, you could access the device by access this FQDN.

http://myzywallp1.com/rpBascSys.html

Google

INTERNET ACCESS

Network Status

Interface	Status	IP Address	Subnet Mask	Renew
WAN	100M/Full	192.168.10.120	255.255.255.0	<input type="button" value="Renew"/>
LAN	100M/Full	10.0.0.83	255.255.255.0	N/A

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

Step.3: Use ping to check the result, And it just like what we set before.

```
C:\WINDOWS\system32\cmd.exe
Password: ****
Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
ras> exit

Connection to host lost
C:\>ping myzywallp1.com

Pinging myzywallp1.com [10.0.0.83] with 32 bytes of data:
Reply from 10.0.0.83: bytes=32 time<1ms TTL=254
Reply from 10.0.0.83: bytes=32 time<1ms TTL=254
Reply from 10.0.0.83: bytes=32 time<1ms TTL=254

Ping statistics for 10.0.0.83:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\>
```


Step.4: Now change the IP address from 10.0.0.83 to 10.0.0.50.

LAN

LAN TCP/IP

IP Address	10 . 0 . 0 . 50	RIP Direction	Both
IP Subnet Mask	255 . 255 . 255 . 0	RIP Version	RIP-1
Multicast	None		

DHCP Setup

DHCP	Server	Pool Size	20
IP Pool Starting Address	10 . 0 . 0 . 1		
DHCP WINS Server 1	0 . 0 . 0 . 0		
DHCP WINS Server 2	0 . 0 . 0 . 0		

DNS Servers Assigned by DHCP Server

First DNS Server	From ISP	172 . 23 . 5 . 2
Second DNS Server	From ISP	192 . 168 . 10 . 1
Third DNS Server	From ISP	0 . 0 . 0 . 0

Windows Networking (NetBIOS over TCP/IP)

Allow between LAN and WAN

Note: You also need to create a [Firewall](#) rule.

Apply Reset

Step.5: You still could access the ZyWALL P1 by this FQDN.

* sometimes your PC/Notebook catch the old records will cause the update fail.

To solve this you could type “arp -d” or renew the interface to manually update the ARP table.

http://myzywallp1.com/rpBasicSys.html

INTERNET ACCESS

Network Status

Interface	Status	IP Address	Subnet Mask	Renew
WAN	100M/Full	192.168.10.120	255.255.255.0	Renew
LAN	100M/Full	10.0.0.50	255.255.255.0	N/A

ISP Parameters for Internet Access

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

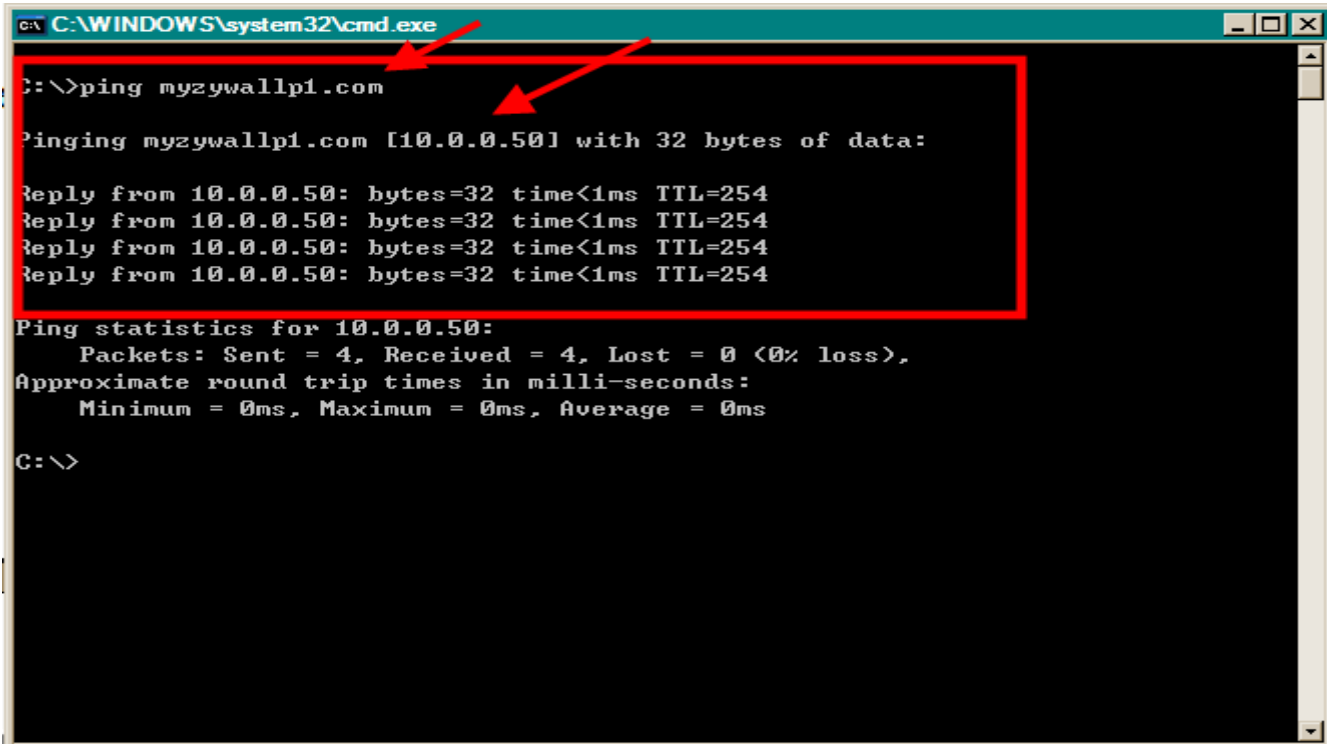
Encapsulation: Ethernet

WAN IP Address Assignment

IP Address Assignment: Dynamic

Apply Reset

Step.6: But when you ping the FQDN, you would see it have already change to the new IP address.



```
C:\WINDOWS\system32\cmd.exe
C:\>ping myzywallp1.com

Pinging myzywallp1.com [10.0.0.50] with 32 bytes of data:

Reply from 10.0.0.50: bytes=32 time<1ms TTL=254
Reply from 10.0.0.50: bytes=32 time<1ms TTL=254
Reply from 10.0.0.50: bytes=32 time<1ms TTL=254
Reply from 10.0.0.50: bytes=32 time<1ms TTL=254

Ping statistics for 10.0.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

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' 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 press the RESET button more than ten seconds to reset the device to factory default. After that, 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

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 **P**oint-to-**P**oint **P**rotocol over **E**thernet 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 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 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 <http://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 500, 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 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. 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) 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.

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 itsInternet 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 runson 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 necessary to follow the format exactly.

By default, ZyWALL takes IP as phase 1 ID type for itself and its 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 a 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.

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:

If there is a NAT router running in the front of ZyWALL, please make sure the NAT router supports to pass through IPsec.

In NAT case (either run on the front end router, or in ZyWALL VPN box), only IPsec ESP tunneling mode is supported since NAT against AH mode.

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.

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.

Will ZyXEL support Secure Remote Management?

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

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:

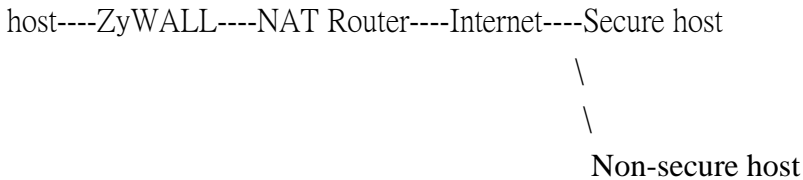
The NAT router must support to pass through IPSec protocol. Only ESP tunnel mode is possible to work in NAT case. In the NAT router is ZyWALL NAT router supporting IPSec pass through, default port and the ZyWALL WAN IP must be configured in NAT Server Table.

WAN IP of the NAT router is the tunneling endpoint for this case, not the WAN IP of ZyWALL.

If firewall is turned on in ZyWALL, you must forward **IKE** port in Internet interface.

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:



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.

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 that 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.

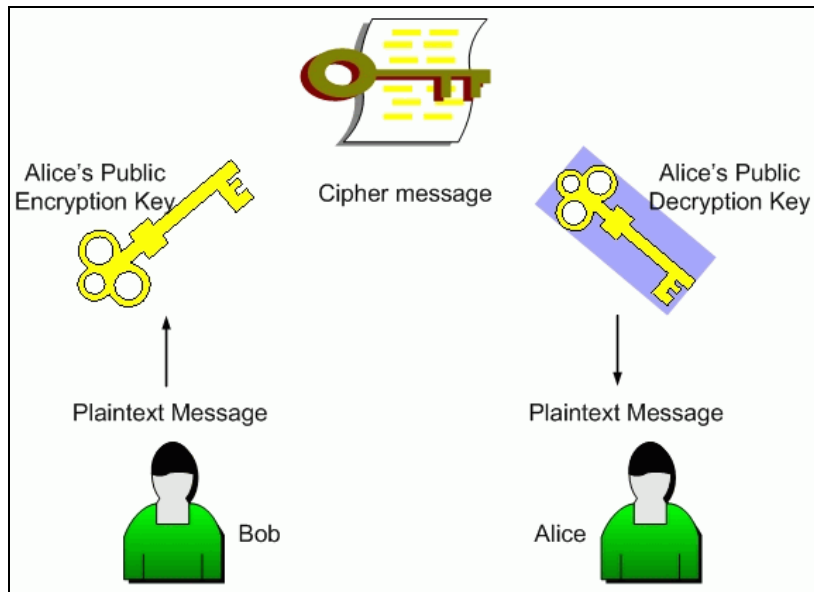
What are Certificate Policies (CPs)?

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.

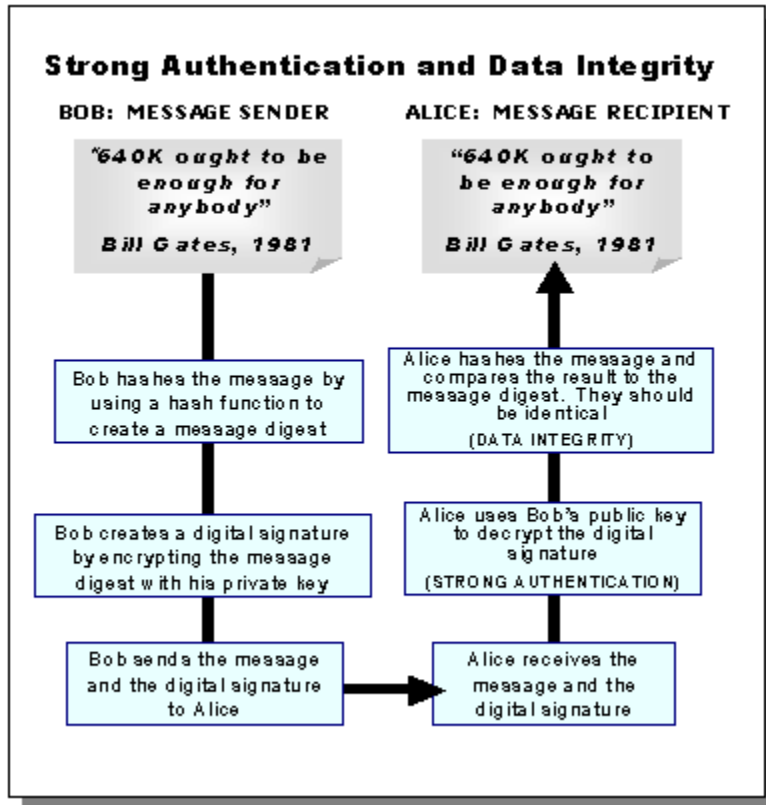
How does a digital signature work?

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.