ZyWALL 2 Plus

Security Appliance

Support Notes

Version 4.01

September, 2006

ZyXEL

Unleash Networking Power

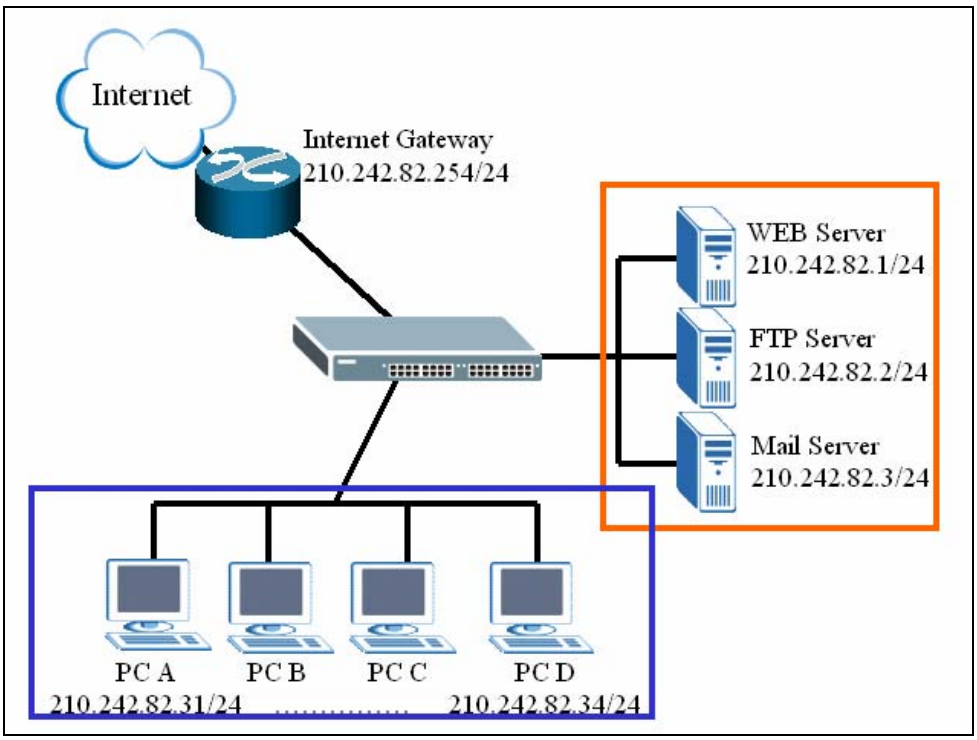
INDEX

Application Notes

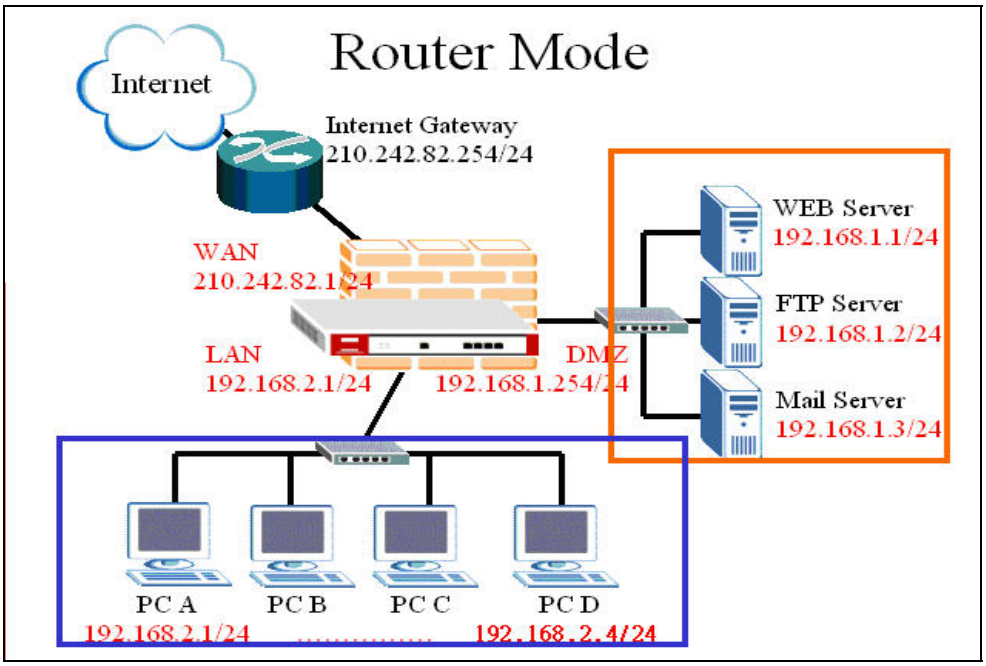
Seamless Incorporation into your network

Using Transparent (Bridge Mode) Firewall

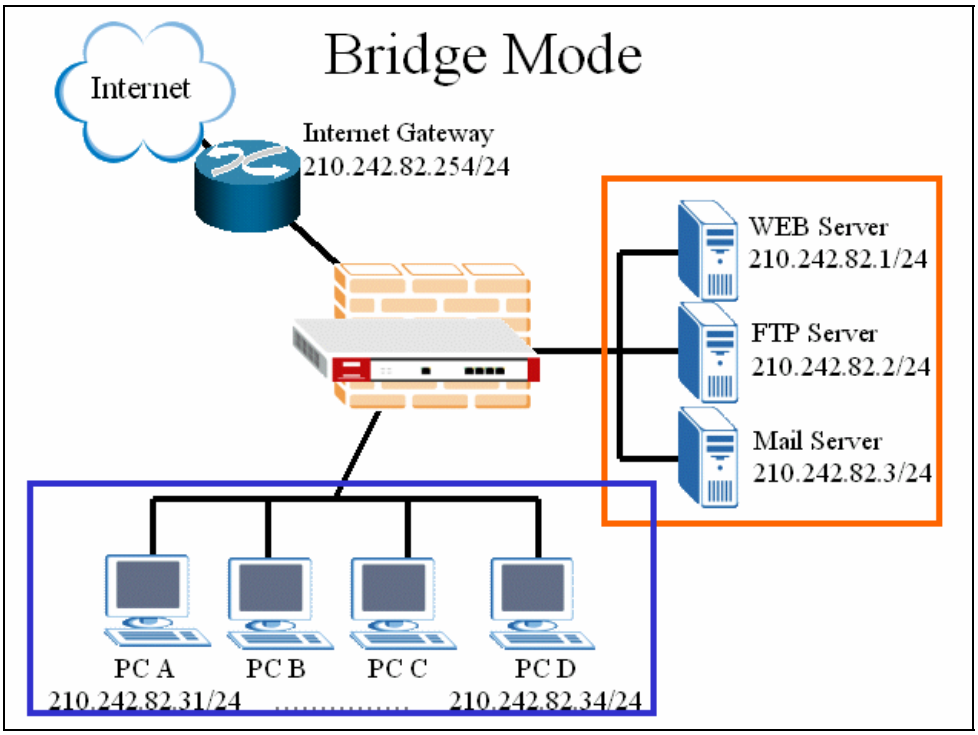
If user wants to insert a firewall into current network, IP setting of hosts and servers may need to change. Following example illustrates an example of current deployment: servers and other hosts sit in the same IP segment.



If a router mode firewall is inserted into existing network, user may need to reassign the IP of all servers and hosts and related setting of applications. However, it may be a huge task to administrators.



Deploying a transparent mode firewall doesn't require any changes of settings on the original network topology. It works as bridge/switch; therefore, all the hosts can communicate with each other as without firewall in between. At the same time, the transparent firewall can check the packets passing through it and block attacks and limit unauthorized access through access control right.

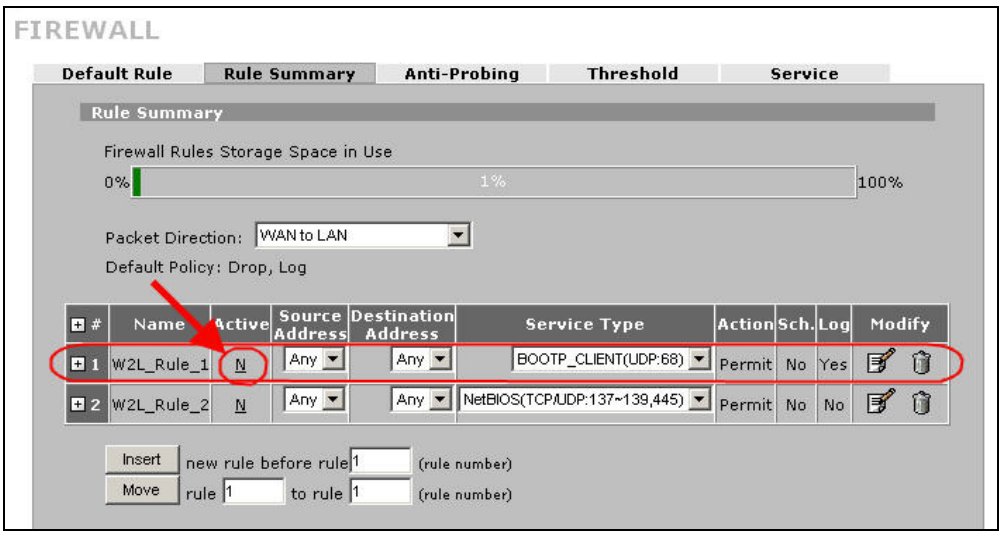


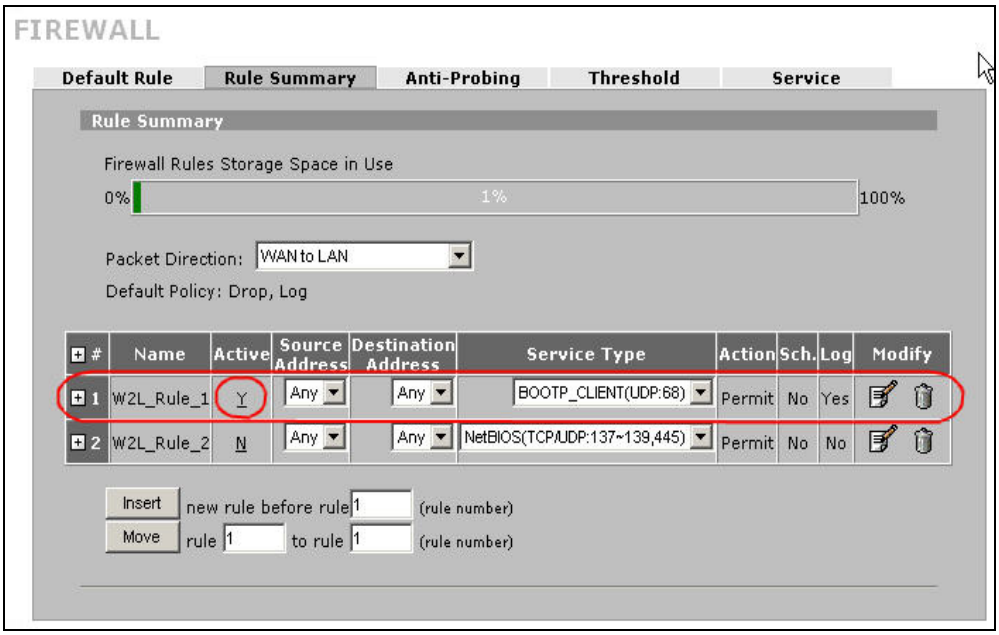
In the following section, we will explain how to configure ZyWALL as bridge firewall. Therefore, all hosts and servers can keep using the same IP as that of current network.

User can configure ZyWALL to act as a router mode firewall or bridge (transparent) firewall. The default is router mode firewall.

Step1. Before changing ZyWALL to bridge mode, if admin wants to make the ZyWALL's LAN PC be able to get DHCP IP address assignment from the DHCP server or the gateway upper than the ZyWALL, there is one firewall rule needs to be activated.

Go to **Firewall** >> **Rule Summary**; choose '**WAN to LAN**' from 'Packet Direction'. You will see a rule to permit the service type, 'BOOTP_CLIENT(UDP:68)', to pass firewall. It's INACTIVE by default. Admin can activate the rule by clicking the '**N**' as following picture. Then the rule will be activated right away.

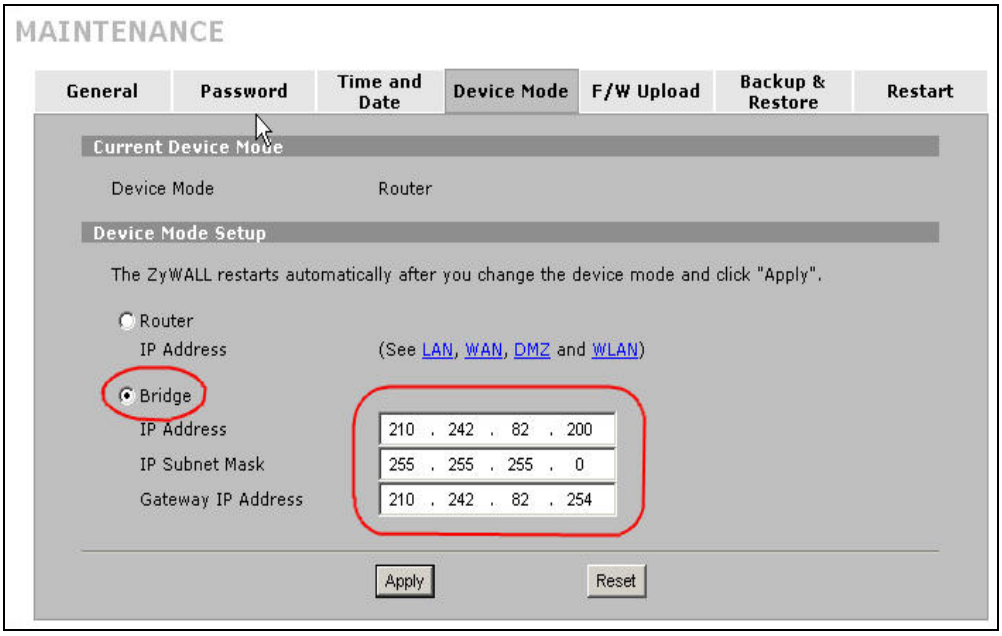


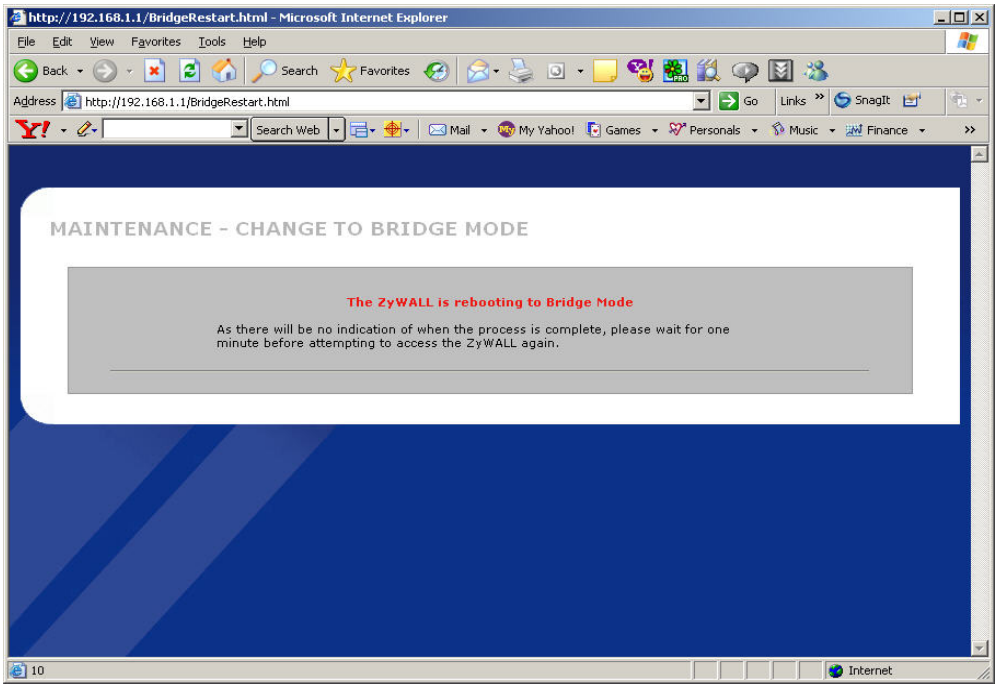


Step2. To change the device mode, go to **MAINTENANCE** >> **Device Mode**. Select '**Bridge**' and

assign a management IP for ZyWALL. The Gateway IP Address is used as next-hop of default route. ZyWALL will restart after applying the change.

(Note: Here we suggest admin to dedicate an IP address to ZyWALL itself at the same subnet as original one (like 210.242.82.X/24 in this example). In this way, admin doesn't need to change his PC's IP address when he wants to access Internet and ZyWALL's web GUI at the same time.)

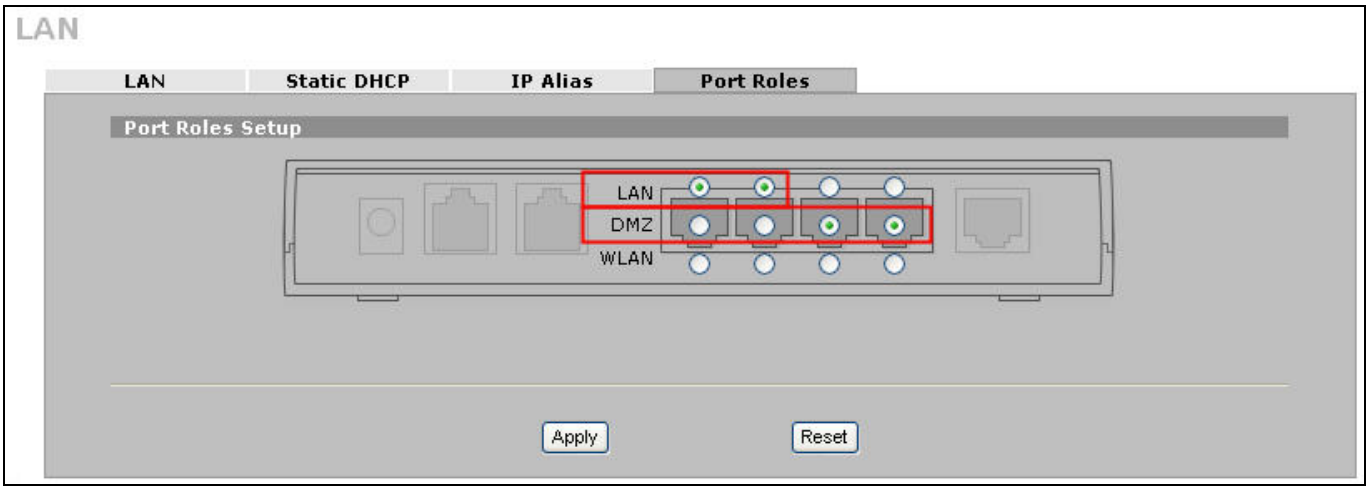




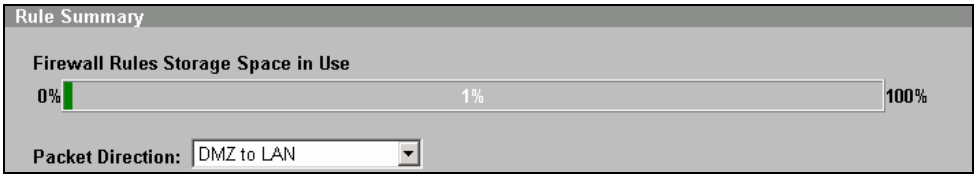
Step3. After rebooting, login ZyWALL's GUI by accessing ZyWALL's management IP address. (Accessing ZyWALL by the PC with a static IP address configured in the same subnet or with an IP from DHCP server (refer to step1 for the pre-configured firewall rule).

Step4. In this example, since we want to apply a DMZ zone for servers. So for ZyWALL 2 Plus which the ports of LAN & DMZ can be configured, user can decide the roles of each port.

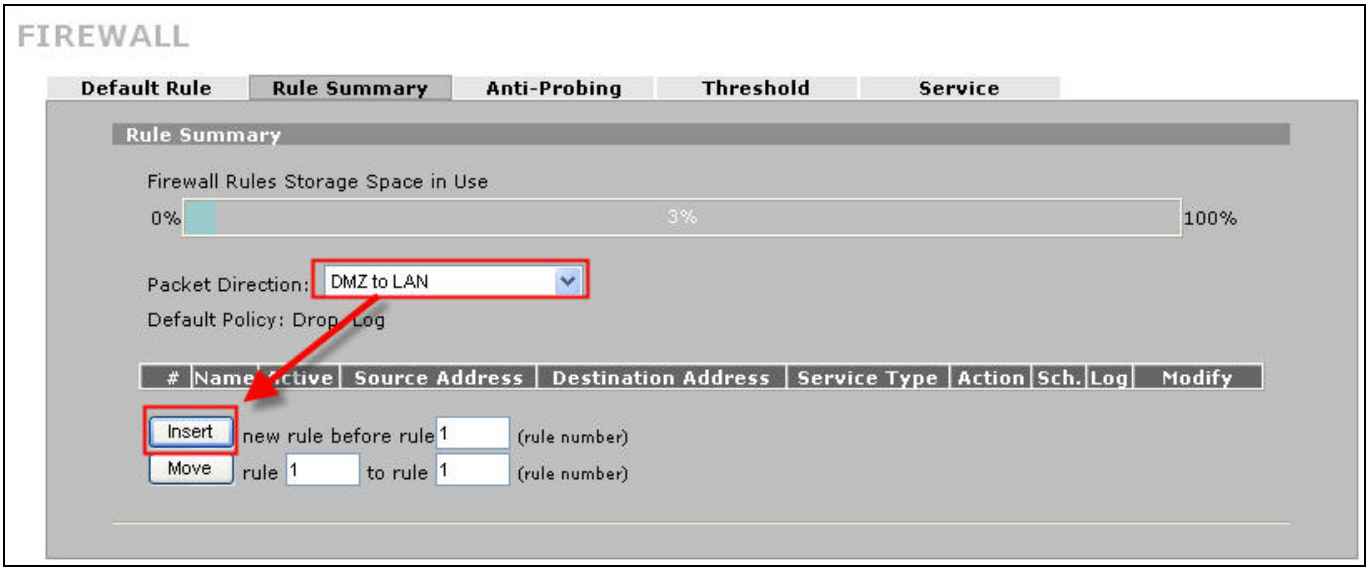
Go to **Network** >> **LAN (or DMZ or WLAN)** >> **Port Roles**. By default, 4 ports are assigned to LAN. In this example, we use port 1 & 2 assigned to LAN and Port 3 & 4 assigned to DMZ as following picture.

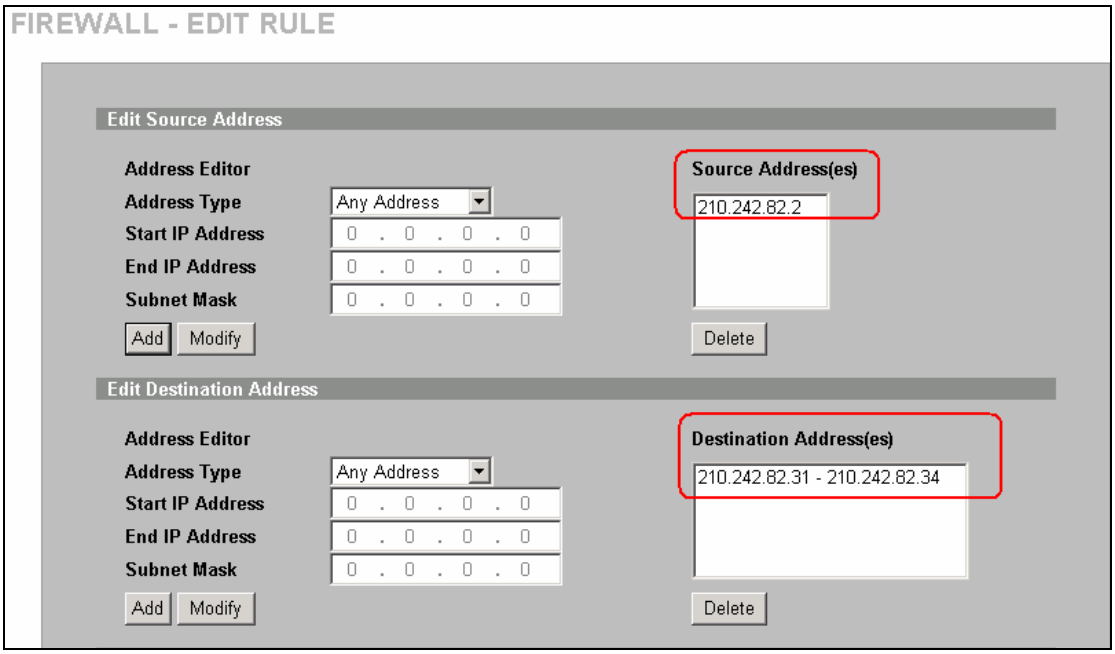


Step5. Furthermore, to configure firewall rule to control the access of your network, go to **SECURITY** >> **FIREWALL** as you do in router mode firewall. For example, user wants to block the access from a FTP server (210.242.82.2) in DMZ zone to LAN hosts (210.242.82.31~34) (Note that they all sits in the same IP segment 210.242.82.0/24). Edit the firewall rule via **Firewall** >> **Rule Summary** and with packet direction: **DMZ to LAN**.



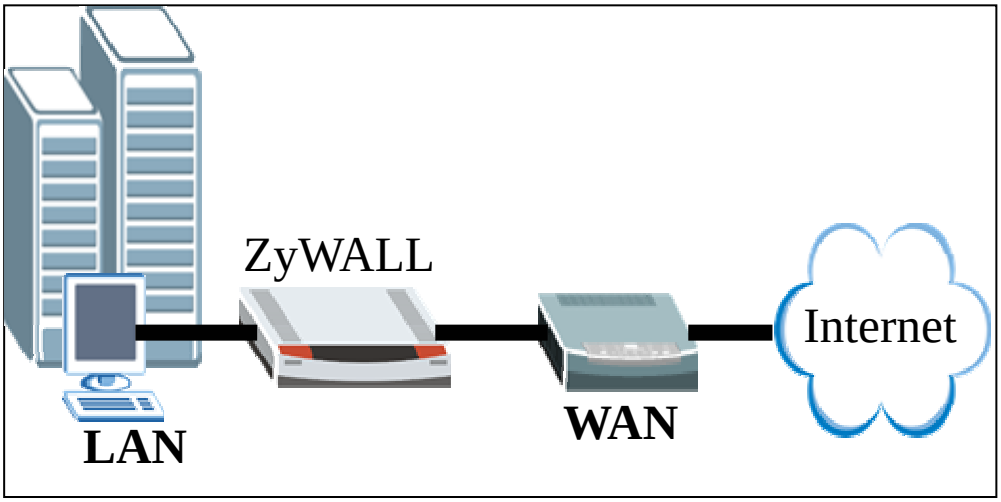
And enter 210.242.82.2 as the source address and 210.242.82.31~34 as destination address. And then select the service and set the action for 'Matched Packet' to
'**BLOCK**'.





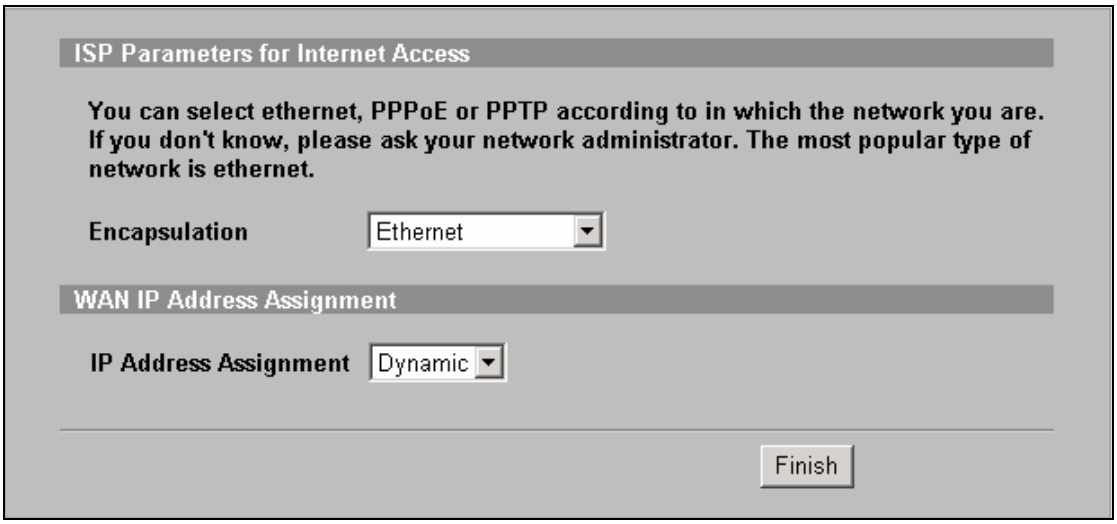
Internet Connection

A typical Internet access application of the ZyWALL is shown below. This section guides you how to configure ZyWALL to gain the Internet access.



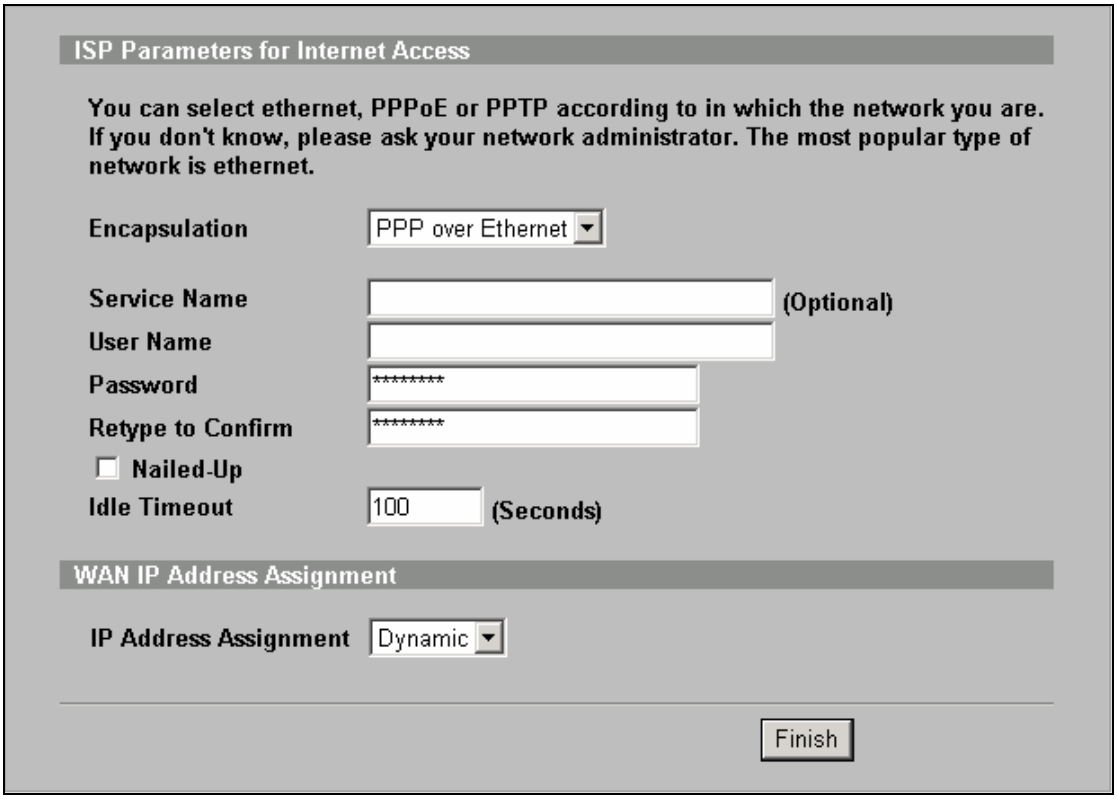
Step1. First of all, Select **Home** menu and click **Internet Access** Wizard to configure your WAN connection. Click "**Internet Access**" under **Home** >> **Wizards for Internet Access Quick Setup**

A pop-up window as below will indicate you to enter **ISP Parameters for Internet Access** .



There are three kinds of encapsulation which are supported by ZyWALL: **Ethernet**, **PPPoE** & **PPTP**. Select the correct encapsulation type from the drop-down menu. The wizards will requests related information needed. These fields vary depending on what you select in the Encapsulation field. Fill them in with the information exactly as given by the ISP or network administrator.

Following picture is an example while PPPoE is selected.



Once the required information is correctly configured, click on the "**Finish**" button to apply the setting and then you have finished configuring Internet Access on WAN link.

DHCP server/client/relay

ZyWALL supports

(1) DHCP client on the WAN port

User can choose either a static IP or a dynamic IP address for WAN port. When choosing dynamic IP, ZyWALL will get a DHCP IP address from ISP or upper layer DHCP server.

(2) DHCP server/relay/none on the LAN ports

ZyWALL supports DHCP server for LAN ports, but also

1. When choosing DHCP setting as 'None', the LAN will NOT assign IP address to the associated hosts. Client PCs need to configure IP address manually.

2. When choosing DHCP setting as a ‘Server’, the LAN will automatically assign IP, subnet, gateway and DNS to the associated clients.

3. When choosing DHCP setting as a ‘Relay’, the LAN will forward the DHCP request to another DHCP server.

Using NAT/Multi-NAT

- What is Multi-NAT?

NAT (Network Address Translation-NAT RFC 1631) is the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and "unmaps" the global IP addresses on incoming packets back into local IP addresses. The IP addresses for the NAT can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. In such case, all incoming connections to your network will be filtered out by the ZyWALL, thus preventing intruders from probing your network.

The SUA feature that the ZyWALL supports previously operates by mapping the private IP addresses to a global IP address. It is only one subset of the NAT. The ZyWALL supports the most of the features of the NAT based on RFC 1631, and we call this feature as 'Multi-NAT'. For more information on IP address translation, please refer to RFC 1631, *The IP Network Address Translator (NAT)*.

- How NAT works

If we define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Address (IGA), see the following figure. The term 'inside' refers to the set of networks that are subject to translation. NAT operates by mapping the ILA to the IGA required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers) and then forwards each packet to the Internet ISP, thus making them appear as if they had come from the NAT system itself (e.g., the ZyWALL router). The ZyWALL keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored.

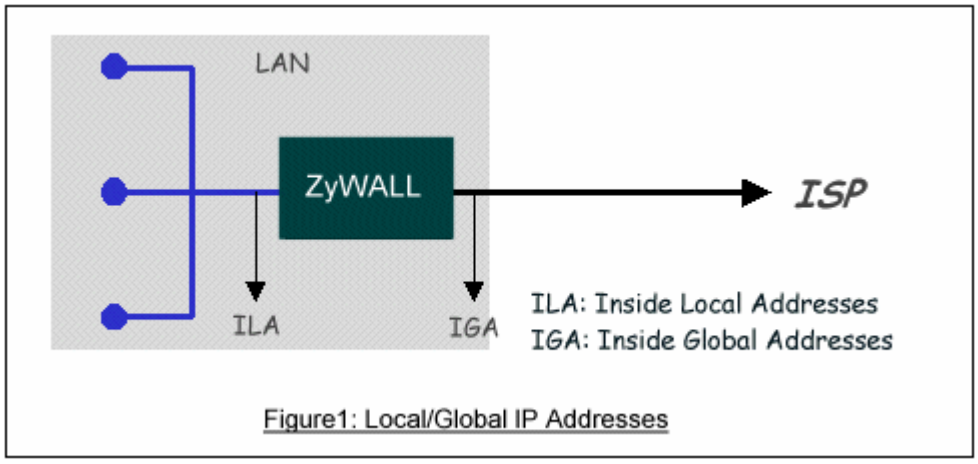


Figure1: Local/Global IP Addresses

- NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

1. **One to One**

In One-to-One mode, the ZyWALL maps one ILA to one IGA.

2. **Many to One**

In Many-to-One mode, the ZyWALL maps multiple ILA to one IGA. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyNOS routers supported (the SUA only option in today's routers).

3. **Many to Many Overload**

In Many-to-Many Overload mode, the ZyWALL maps the multiple ILA to shared IGA.

4. **Many One to One**

In Many One to One, the ZyWALL maps each ILA to unique IGA.

5. **Server**

In Server mode, the ZyWALL maps multiple inside servers to one global IP address. This allows us to specify multiple servers of different types behind the NAT for outside access. Note, if you want to map each server to one unique IGA please use the One-to-One mode.

The following table summarizes these types.

NAT Type	IP Mapping
One-to-One	ILA1<--->IGA1
Many-to-One (SUA/PAT)	ILA1<--->IGA1 ILA2<--->IGA1 ...
Many-to-Many Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA1 ILA4<--->IGA2 ...
Many One-to-One	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA3 ILA4<--->IGA4 ...
Server	Server 1 IP<--->IGA1 Server 2 IP<--->IGA1

- SUA Versus Multi-NAT

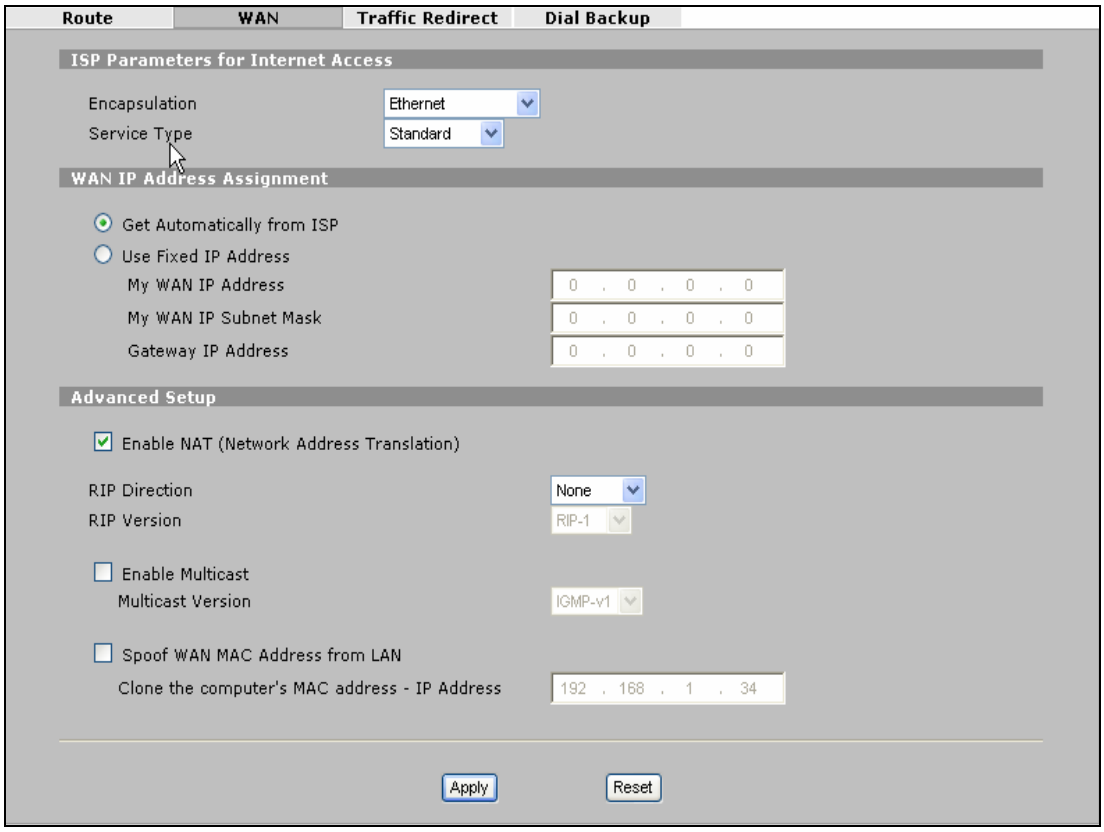
SUA (Single User Account), if you get only one public IP address from your ISP, then you should use SUA. With SUA, PCs on ZyWALL's LAN side can access Internet without further configuration. If you have internal servers to be accessed by remote users on Internet, you need to go to ADVANCED -> SUA/NAT -> SUA Server to setup which service, or port numbers, you would like to forward to which Internal server.

Multi-NAT, if you get multiple public IP addresses from your ISP, then you may use Multi-NAT. With Multi-NAT, you can choose different types of NAT mapping methods to utilize the public IP addresses. You should define each NAT mapping rules clearly in ADVANCED -> SUA/NAT -> Address Mapping, so that internal PCs can access Internet and internal servers can be accessed by remote uses on Internet.

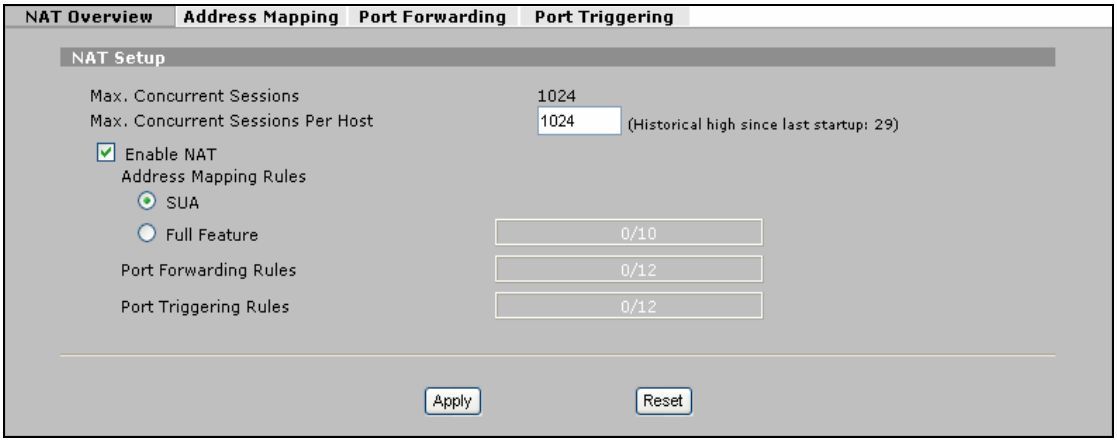
Step 1. Applying NAT in WAN Interface

You can choose the NAT mapping types to either **SUA Only** or **Full Feature** in WAN setup.

NETWORK -> WAN



or ADVANCED -> NAT -> NAT Overview

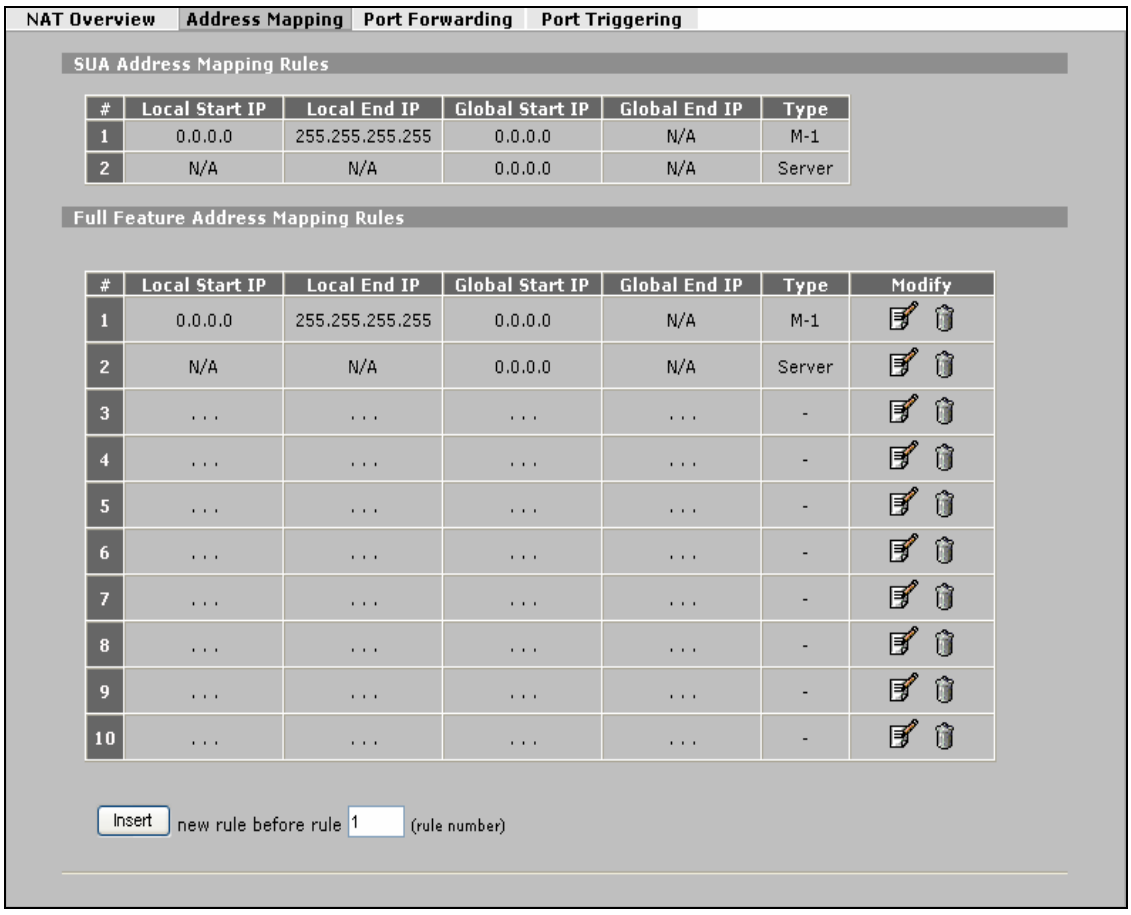


Key Settings

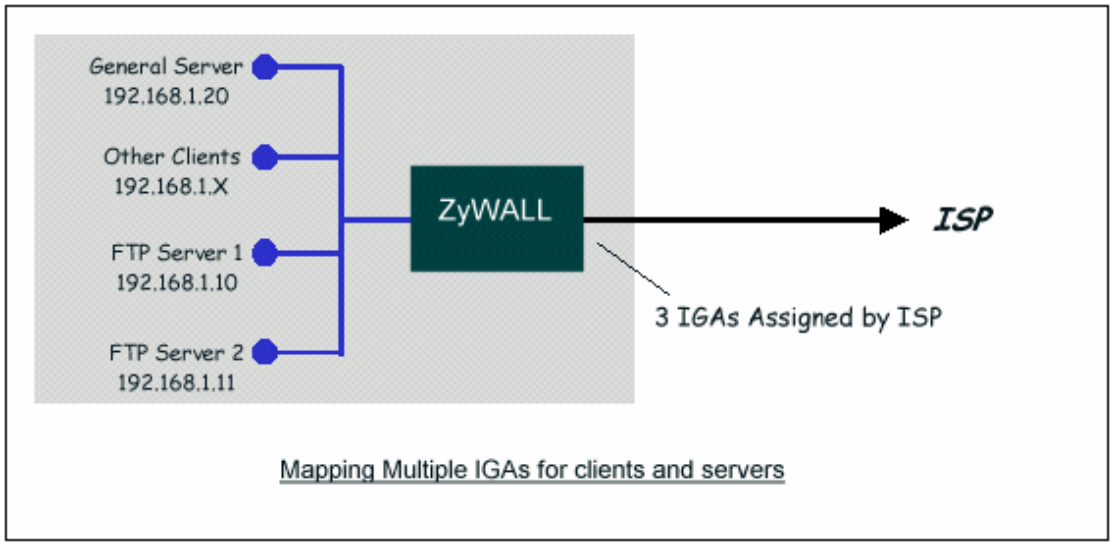
Field	Options	Description
Network Address Translation	**Full Feature**	Set to '**Full Feature**' if there are multiple IP addresses given by ISP and can assigned to your clients.
	Routing	Set to '**Routring**' if you clients use Internet IP addresses and thus do not need NAT function.
	SUA Only	Set this field to '**SUA Only**' if you want all clients share one IP to Internet.

Step 2. Configuring NAT Address Mapping

To configure NAT, go to ADVANCED -> NAT -> Address Mapping



Step 3. Using Multiple Global IP addresses for clients and servers (One-to-One, Many-to-One, Server Set mapping types)

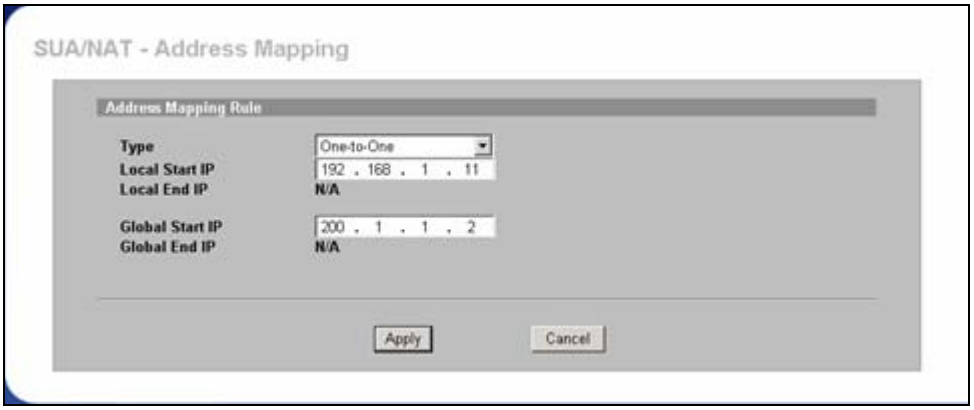


In this case we have 3 IGAs (IGA1, IGA2 and IGA3) from the ISP. We have two very busy internal FTP servers and also an internal general server for the web and mail. In this case, we want to assign the 3 IGAs by the following way using 4 NAT rules.

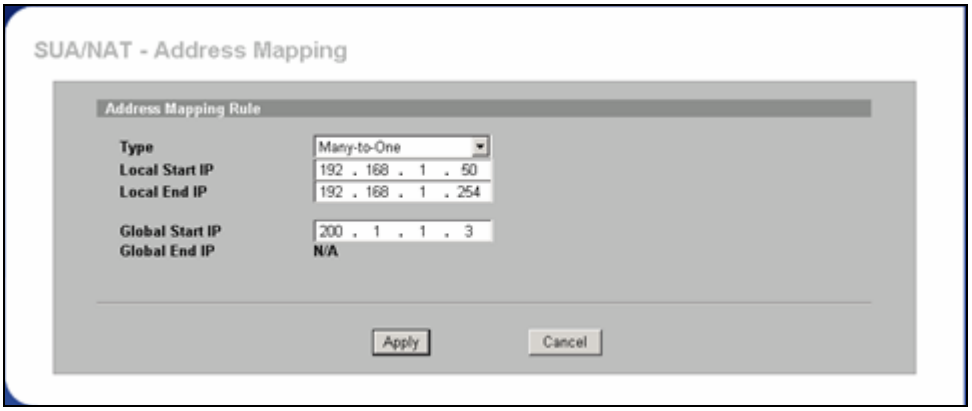
- Rule 1 (One-to-One type) to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.1.1.1).
- Rule 2 (One-to-One type) to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.1.1.2).
- Rule 3 (Many-to-One type) to map the other clients to IGA3 (200.1.1.3).
- Rule 4 (Server type) to map a web server and mail server with ILA3 (192.168.1.20) to IGA3. Type **Server** allows us to specify multiple servers, of different types, to other machines behind NAT on the LAN.

Rule 1 Setup: Select One-to-One type to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.1.1.1).

Rule 2 Setup: Selecting One-to -One type to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.1.1.2).

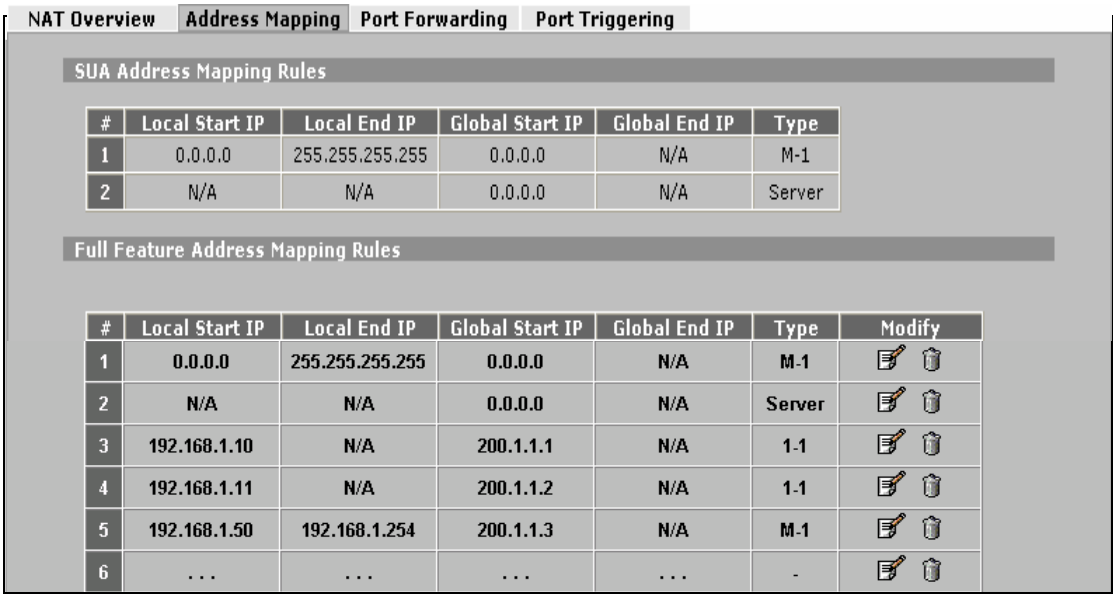


Rule 3 Setup: Select Many-to-One type to map the other clients to IGA3.

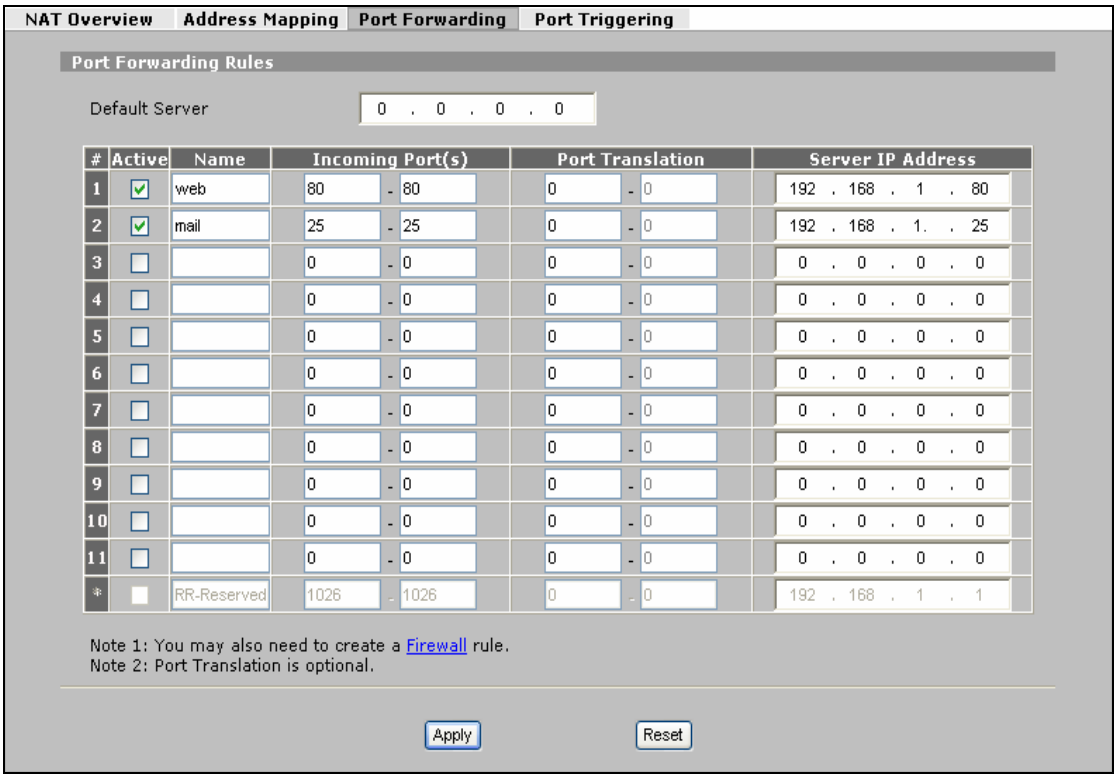


Rule 4 Setup: Select Server type to map our web server and mail server with ILA3 (192.168.1.20) to IGA3.

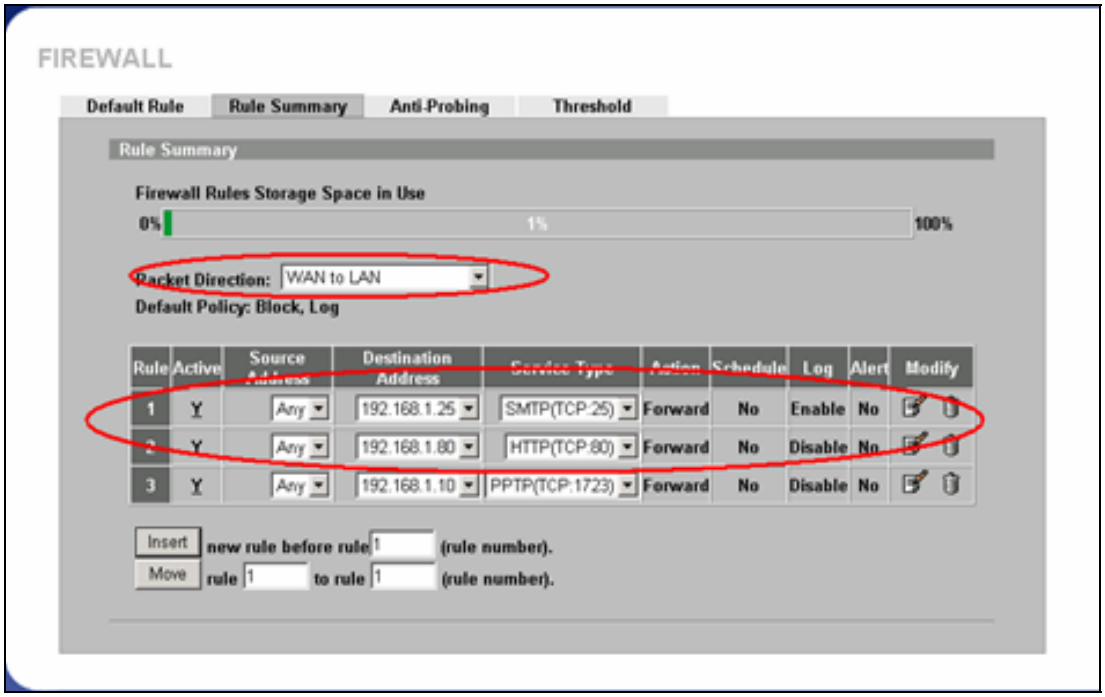
When we have configured all four rules in the rule summary page.



Now we configure all other incoming traffic to go to our web server and mail server in "Port Mapping" page,

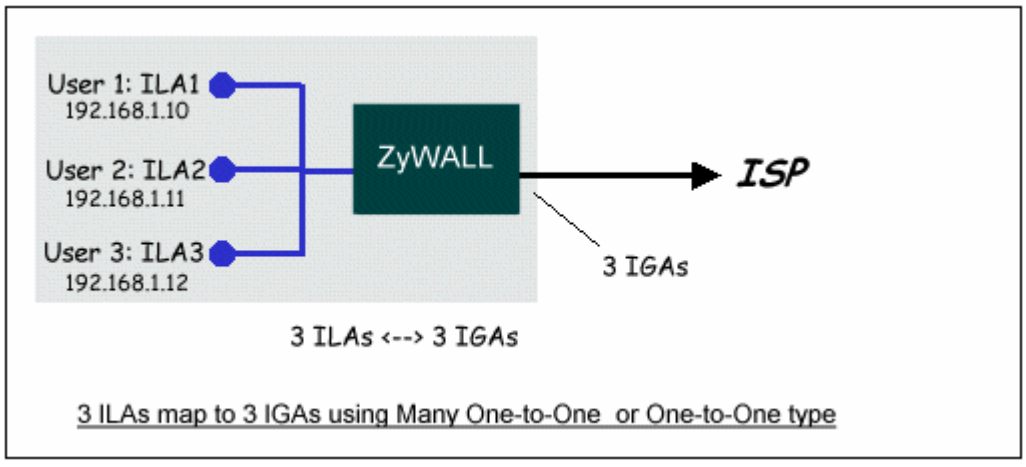


Please note that if you turn on ZyWALL's firewall function, then you should add a firewall rule from WAN to LAN to forward the incoming connections. If you would like to only allow traffic going to the internal server, you should specify server's private IP address in the field of the destination IP address.

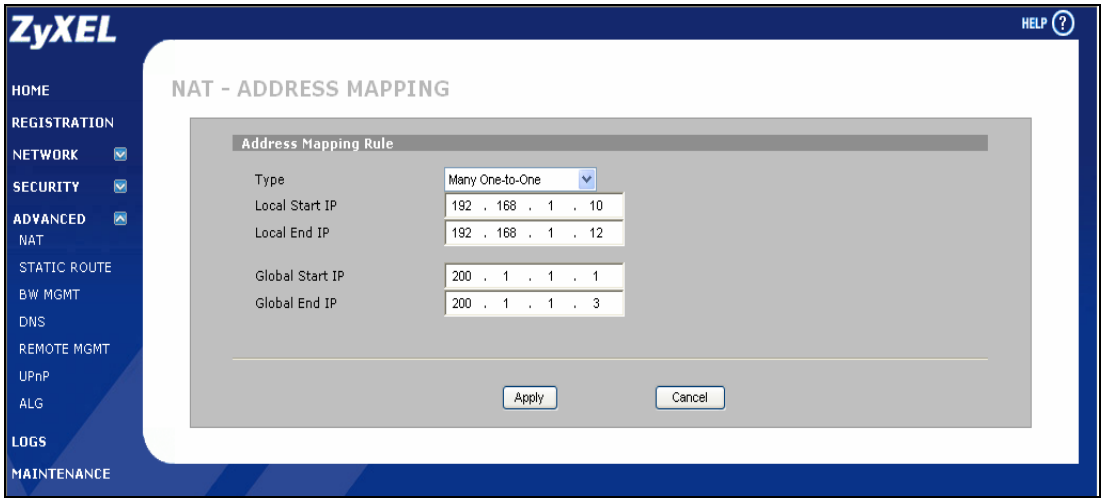


Application for Non NAT Friendly Support

Some servers providing Internet applications such as some mIRC servers do not allow users to login using the same IP address. In this case it is better to use Many One-to-One or One-to-One NAT mapping types, thus each user login to the server is using a unique global IP address. The following figure illustrates this.



One rule configured for using Many One-to-One mapping type is shown below.

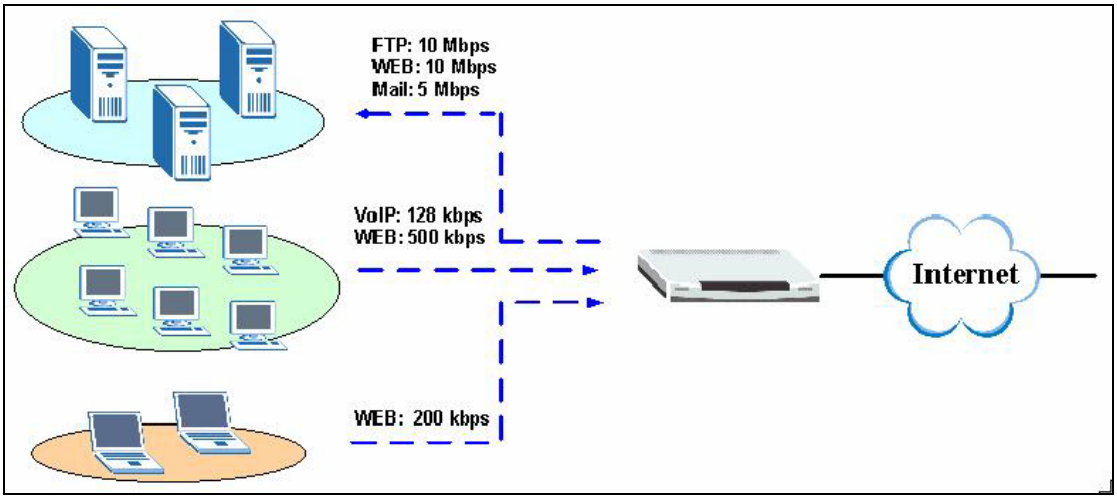


Optimize network performance & availability

Using Bandwidth Management

Why Bandwidth Management (BWM)?

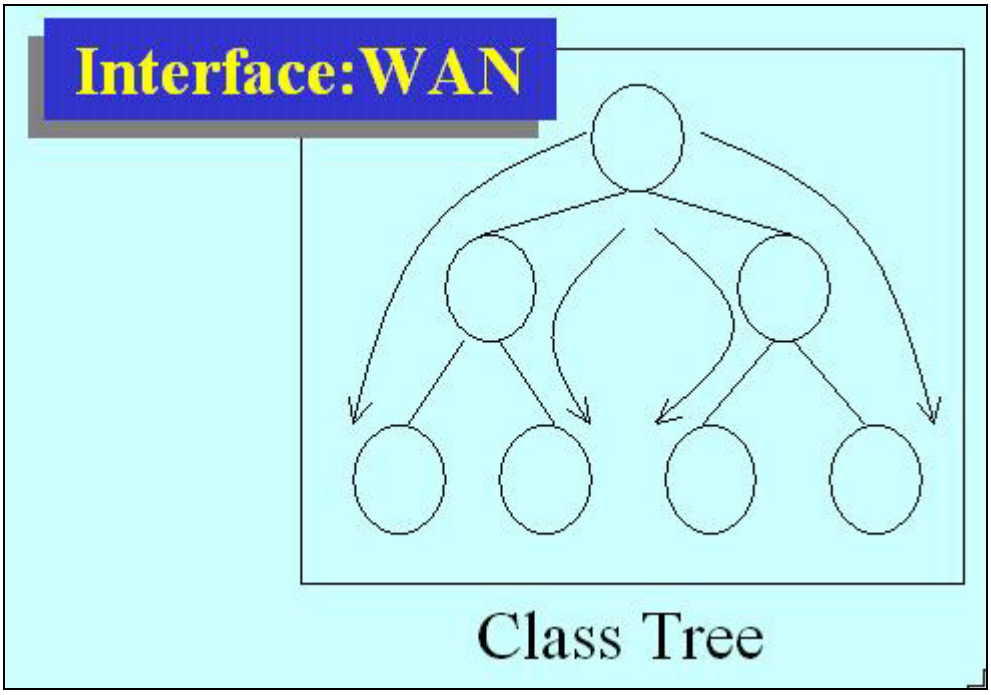
Nowadays, we have many different traffic types for Internet applications. Some traffic may consume high bandwidth, such as FTP (File Transfer Protocol), if you are downloading or uploading files with large size. Some other traffic may not require high bandwidth, but they require stable supply of bandwidth, such as VoIP traffic. The VoIP quality would not be good, if all of the outgoing bandwidth is occupied via FTP. Additionally, chances are that you would like to grant higher bandwidth for some body special that is using specific IP address in your network. All of these are reasons why we need bandwidth management.



How Bandwidth Management in ZyWALL?

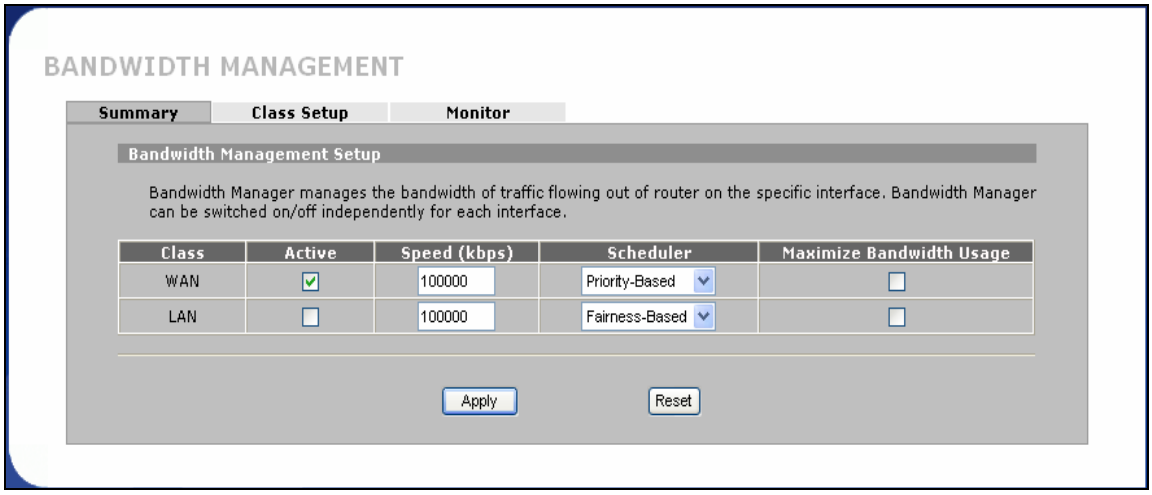
ZyWALL achieves BWM by classifying packets, and control when to send out the classified packets. Bandwidth Management of ZyXEL appliances operates on the IP layer. The major step to configure BWM is defining filter rules by fields of IP header or TCP/UDP port number. Then specify the volume of bandwidth you want to allocate to the filtered traffic. There are two types of BWM in ZyXEL implementations, Full and Lite versions.

Full version: Users can define how they want to classify traffic on each interface. In this version, child-class can borrow bandwidth from parent-class if necessary by **Bandwidth Borrowing**. For classes that need more bandwidth even after bandwidth borrowing, users can also apply **Maximize Bandwidth Usage** from the interface.



Using BWM

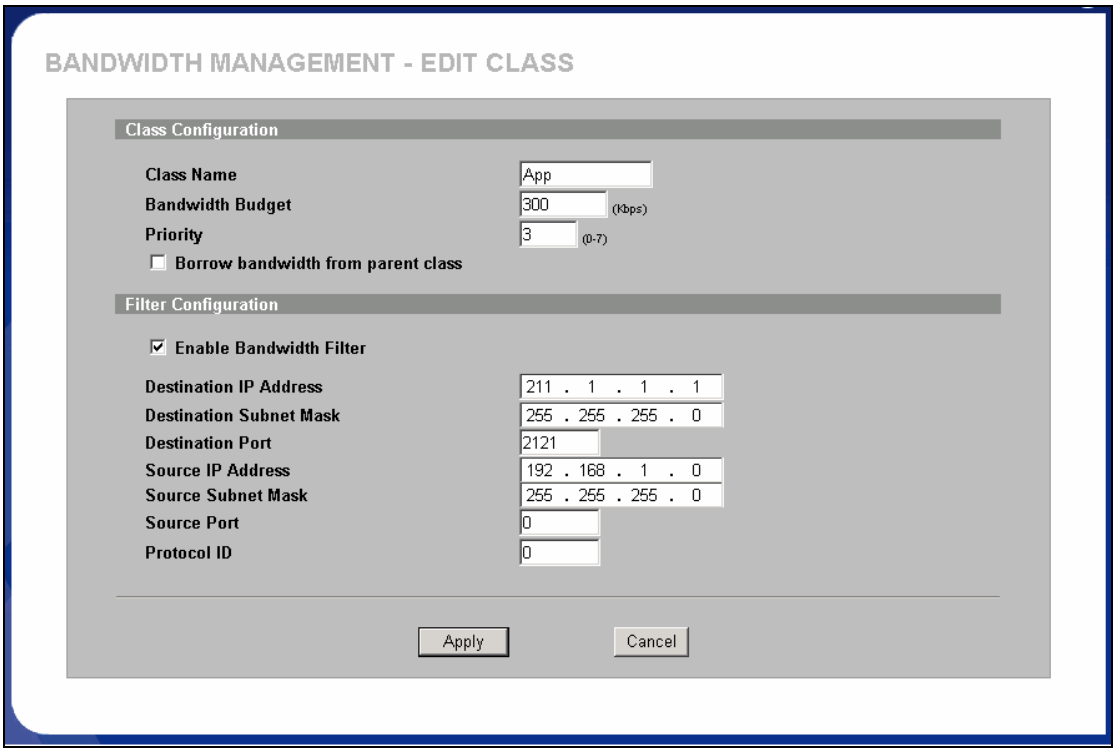
Go to ADVANCED->BW MGMT->Summary, activate bandwidth management on the interface you would like to manage. We enable the BWM function on WAN interface in this example.
Enter the total speed for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class.
Select how you want the bandwidth to be allocated. Priority-Based means bandwidth is allocated via priority, so the traffic with highest priority would be served first, then the second priority is served secondly and so on. If Fairness-Based is chosen, then the bandwidth is allocated by ratio. Which means if A class needs 300 kbps, B class needs 600 kbps, then the ratio of A and B's actual bandwidth is 1:2. So if we get 450 kbps in total, then A would get 150 kbps, B would get 300 kbps.



Key Settings:

Active	Check the box to enable BWM on the interface. Note that if you would like to manage traffic from **WAN to LAN**, you should apply BWM on **LAN** interface.
Speed	Enter the total speed to manage on this interface. This value is the budget of the class tree's root.
Scheduler	Choose the principle to allocate bandwidth on this interface. **Priority-Based** allocates bandwidth via priority. **Fairness-Based** allocates bandwidth by ratio.
Maximize Bandwidth Usage	Check this box if you would like to give residuary bandwidth from Interface to the classes who need more bandwidth than configured amount. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class or you want to limit the bandwidth of each class at the configured value. (Please note that to meat the second condition, you should also disable bandwidth borrowing on the class.)

Go to **ADVANCED->BW MGMT->Class Setup**, select the interface on which you would like to setup the Class tree.
Click the radio button besides the **Root Class**, then press **'Add Sub-Class'**

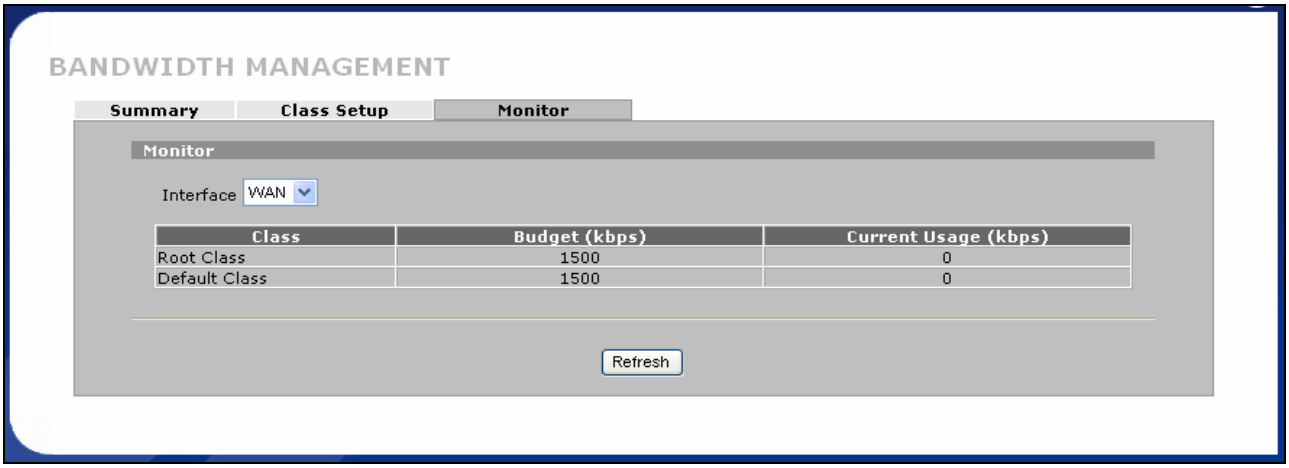


Key Settings:

Class Name	Give this class a name, for example, **'App'**
Bandwidth Budget	Configure the speed you would like to allocate to this class
Priority	Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3.
Bandwidth Borrowing	Check this box if you would like to let this class to borrow bandwidth from it's parents when the required bandwidth is higher than the configured amount. Do not check this if you want to limit the bandwidth of this class at the configured value.(Please note that you should also disable **Maximize Bandwidth Usage** on the interface to meat the condition.)
Enable Bandwidth Filter	Check this to specify the traffic types via IP addresses/Port numbers.
Destination IP Address	Enter the IP address of destination that meats this class.
Destination Subnet Mask	Enter the destination subnet mask.
Destination Port	Enter the destination port number of the traffic.

Source IP Address	Enter the IP address of source that meats this class. Note that for traffic from '**LAN to WAN**', since BWM is before NAT, you should use the IP address before NAT processing.
Source Subnet Mask	Enter the destination subnet mask.
Source Port	Enter the source port number of the traffic.
Protocol ID	Enter the protocol number for the traffic. 1 for ICMP, 6 for TCP or 17 for UDP

After configuration BWM, you can check current bandwidth of the configured traffic in **ADVANCED->BWM MGMT->Monitor.** The values in the column of **Current usage (kbps)** would display the actually number.

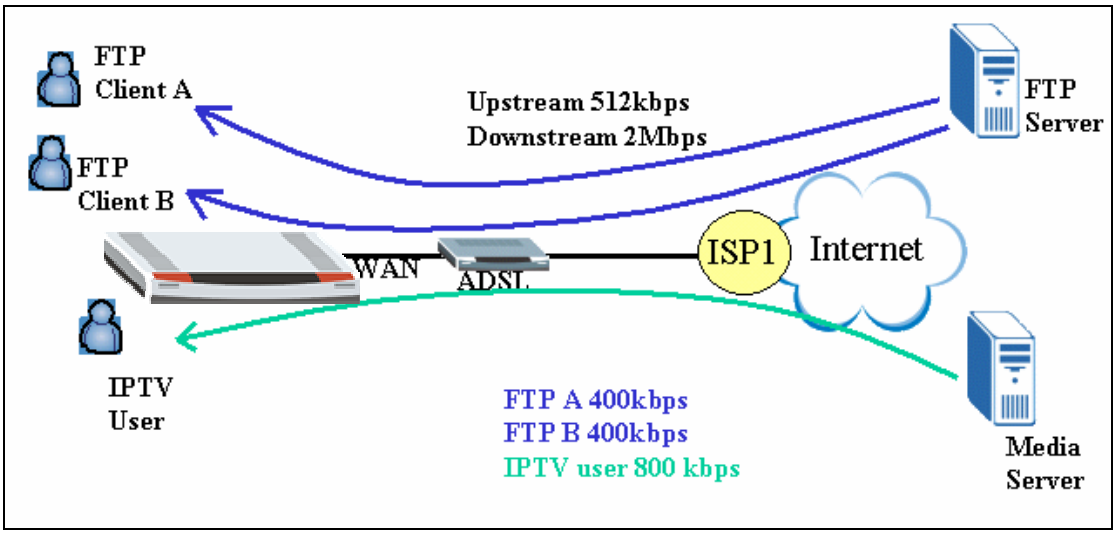


Scenario - Limit bandwidth usage, but when there is residual bandwidth, we hope it can be shared fairly among several active traffic.

Description

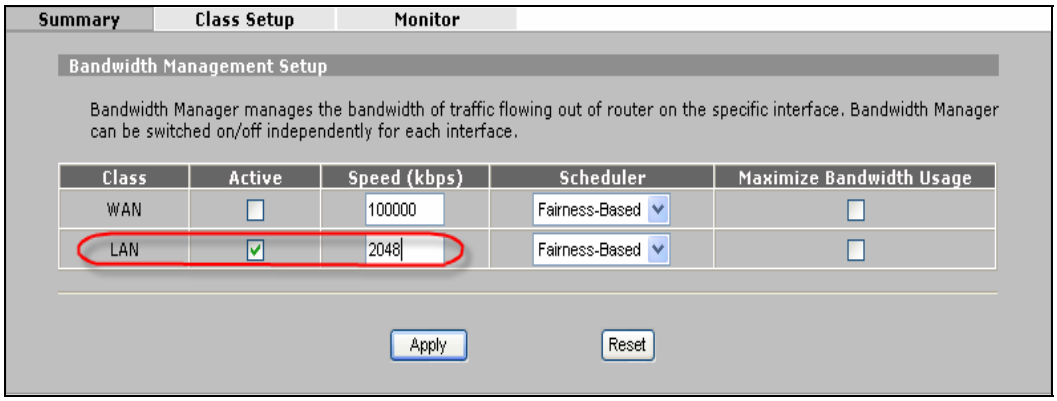
FTP Client A can get 400kbps FTP traffic and FTP Client B can get 800 kbps FTP traffic and IPTV user can retrieve 800 kbps UDP streaming.

LAN Interface: Fairness-based, Speed = 2048kbps
Class 1: Budget = 400kbps, Dest. IP = FTP Client A's IP, Service = FTP, Priority = 3, enable Borrow
Class 2: Budget = 800kbps, Dest. IP = FTP Client B's IP, Service = FTP, Priority = 3, enable Borrow
Class 3: Budget = 800kbps, Dest IP = IPTV Client's IP, Protocol = UDP.

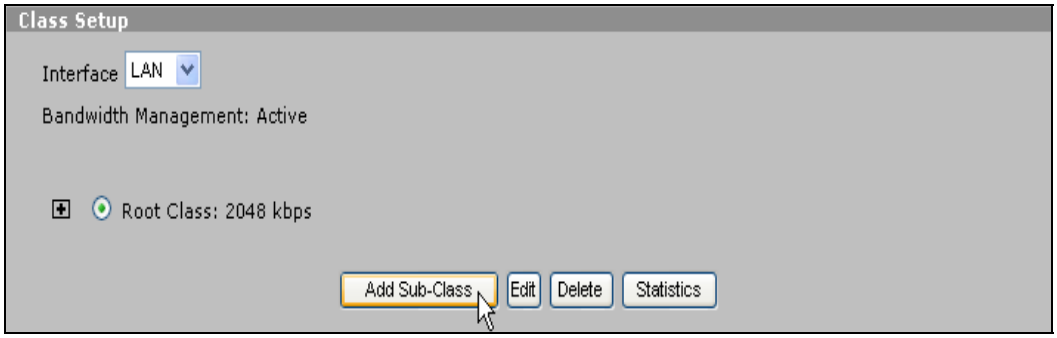


Step1.

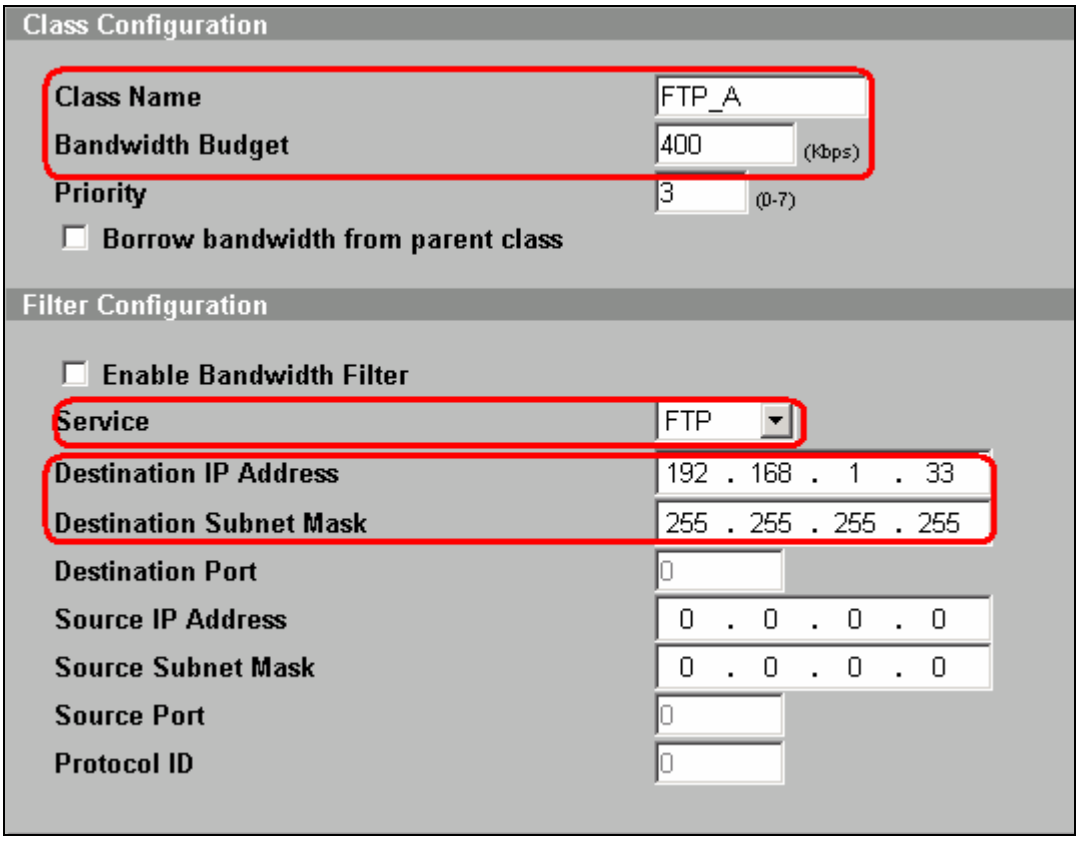
Activate Bandwidth Management on the interface on which you want to control. In this example, it is LAN. Assign 2048Kbps to LAN interface.



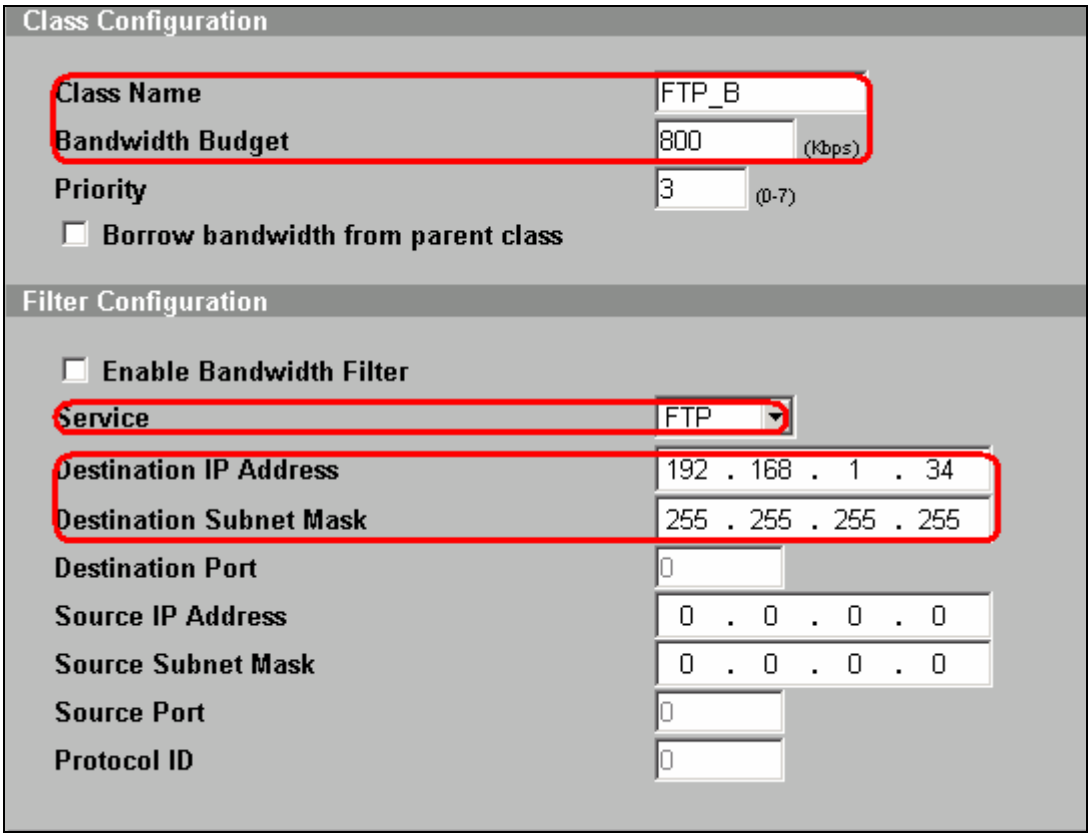
Step2. Go to “Class Setup” and select LAN from the drop-down list of Interface. Click on Root Class and then click on “Add Sub-Class” to create and add a new class under root.



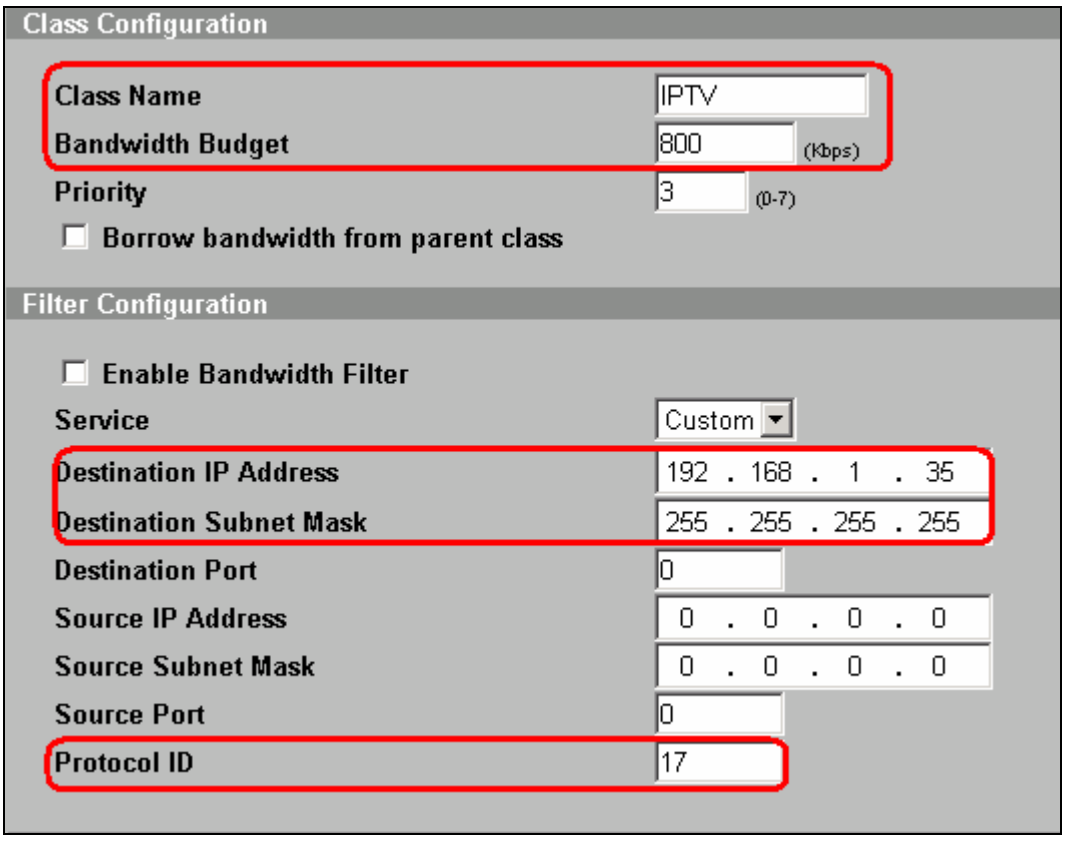
We add a service and allocate 400kbps for FTP and destined to FTP Client A. Select the **Service** as FTP from drop-down list. Input Client A’s IP address as Destination IP Address.



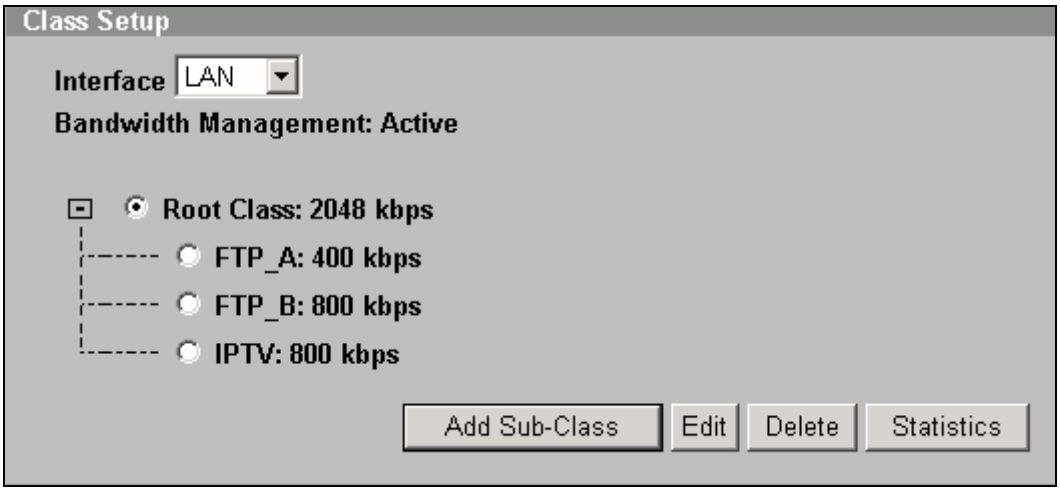
Step3. Add another service and allocate 800kbps for FTP and destined to FTP Client B. Select the **Service** as FTP from drop-down list. Input Client B's IP address as Destination IP Address.



Step4. Add another service and allocate 800kbps for IPTV user and destined to Media traffic to IPTV user. Select the **Service** as Custom from drop-down list and set Protocol IP as 17 (UDP). Input IPTV user's IP address as Destination IP Address.



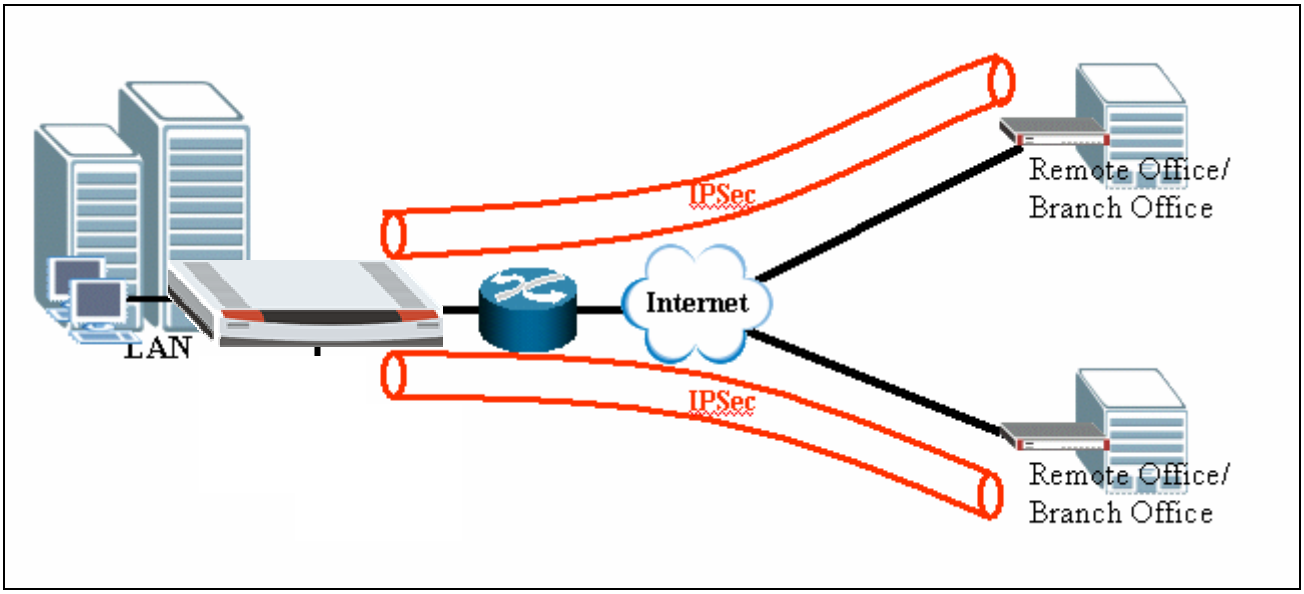
Step 5. Three classes are created for FTP Client A, B & IPTV user as below:



Secure Connections across the Internet

Site-to-Site VPN (Intranet) Scenario

A site-to-site VPN protects the network resources on your protected networks from unauthorized use by users on an unprotected network, such as the public Internet. Site-to-site VPN connects offices in different locations with encryption technology.

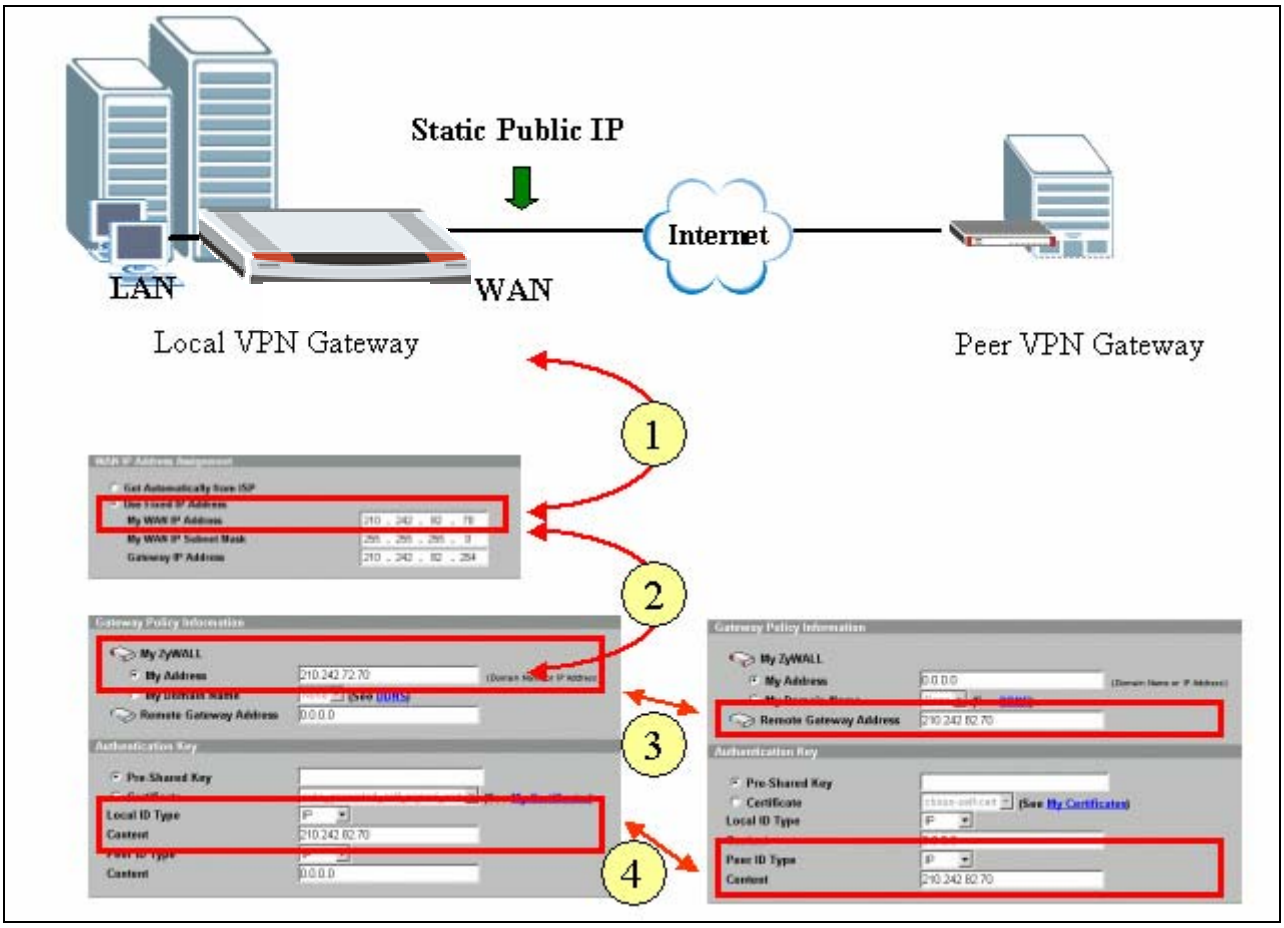


Configure ZyWALLs with Static WAN IP Address

This section describes an example configuration ZyWALL with static WAN IP address.

If ZyWALL is used as Internet gateway and public IP address is assigned on ZyWALL's WAN interface. ZyWALL uses this public WAN IP address for terminating the VPN tunnels from remote VPN gateways.

In following example, local VPN gateway (ZyWALL) uses a static public IP address.



1) Configure the static Public IP address to WAN interface through Network-> WAN-> WAN IP Address Assignment
2) Enter the WAN IP address as My Address in Gateway Policy
3) On peer VPN gateway, use the same IP address as **Remote Gateway Address** in Gateway Policy

On Local VPN gateway, select **IP** as the **Local IP Type** and enter the public WAN IP address as the **content** of identify. One remote VPN peer, select IP as the Peer ID Type and enter the same IP address as the content of identify.

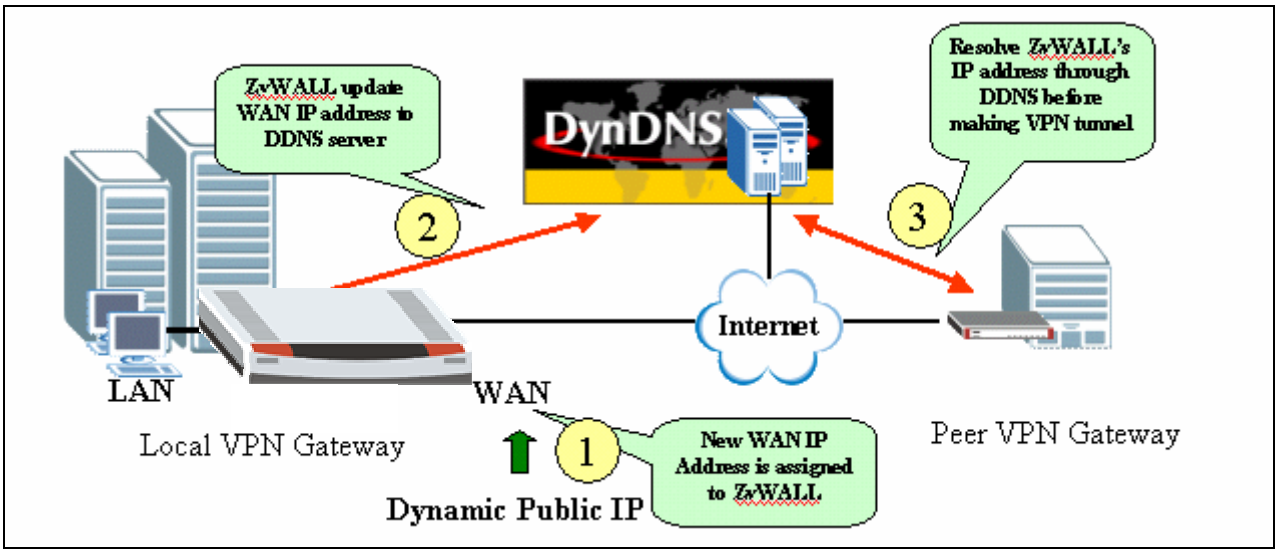
Configure ZyWALL with Dynamic WAN IP Address

This section describes an example configuration ZyWALL with dynamic WAN IP address.

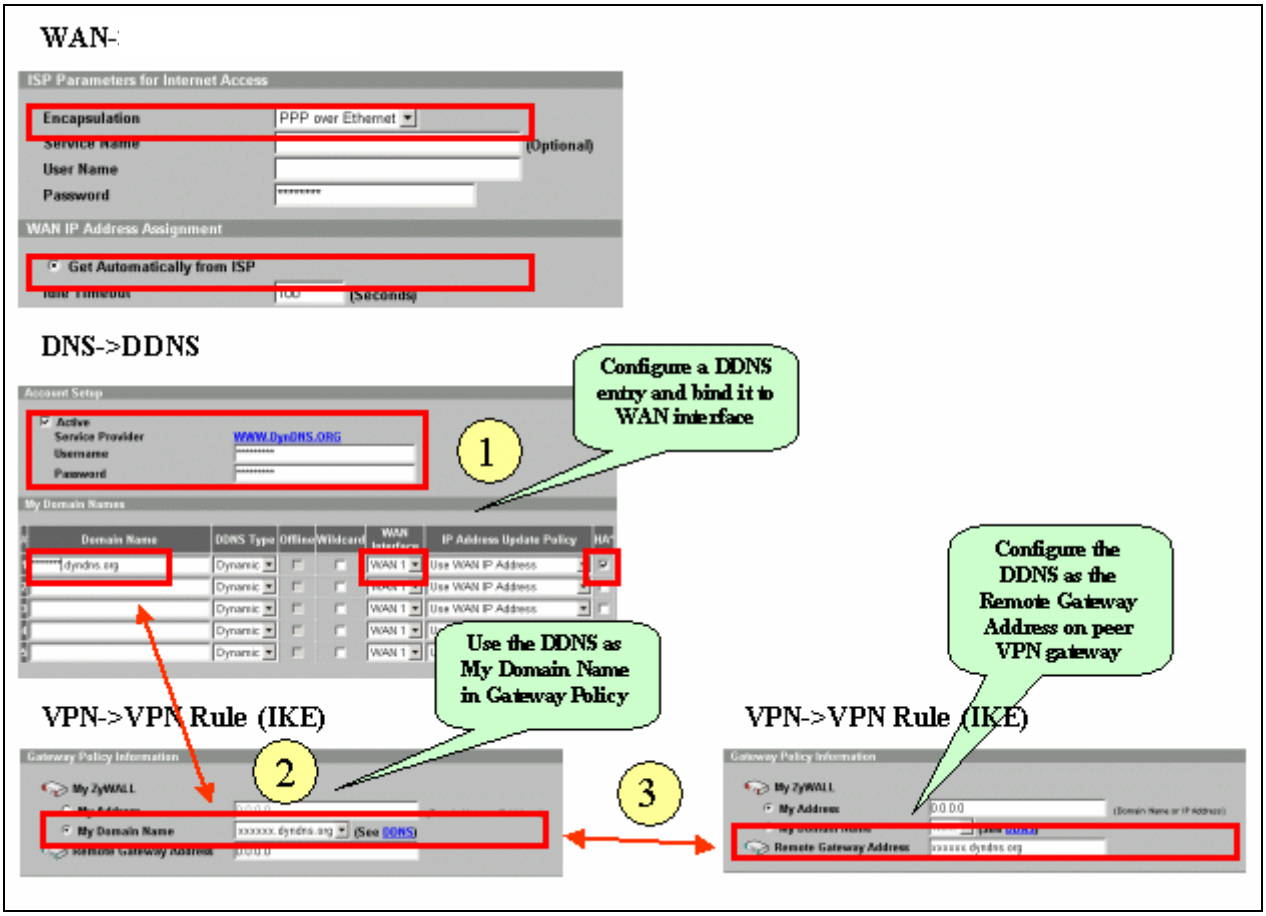
If ZyWALL uses PPPoE or Ethernet/DHCP for its Internet connection, WAN IP address is dynamically assigned by ISP. Since ZyWALL has no idea about its WAN IP address before it is assigned, it is difficult/impossible to use WAN IP Address for My Address in Gateway Policy.

To overcome this problem, **Dynamic DNS** can be used to resolving the VPN gateway. When new IP

address is assigned to ZyWALL's WAN interface, ZyWALL will updates the related record in DDNS server. Therefore the peer VPN gateway can resolve ZyWALL's IP address to make a VPN tunnel.



In following example, local VPN gateway (ZyWALL) uses a dynamic WAN IP address (PPPoE with dynamic IP assignment).



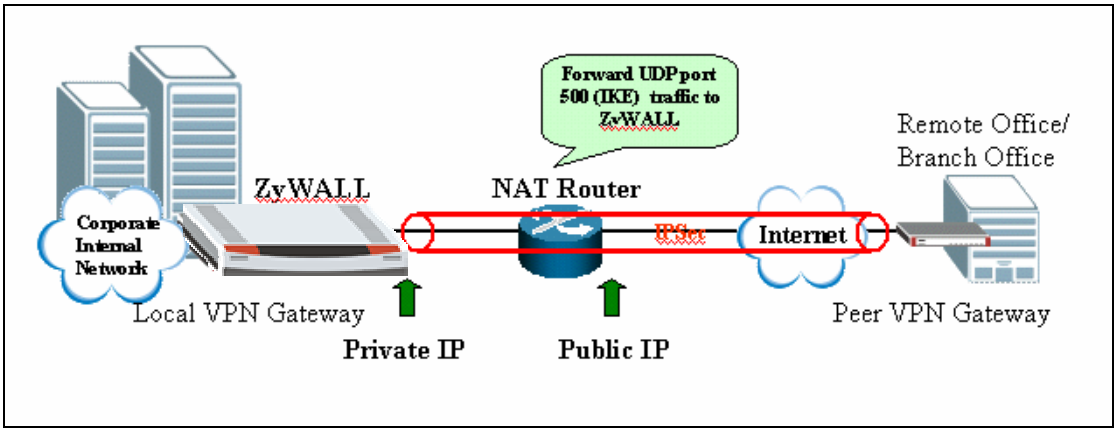
4) Configure the DDNS entry under DNS-> DDNS and bind it to a WAN interface.
5) Under Gateway Policy menu, select the DDNS entry from drop-down list and use it as **My Domain Name.**
6) Configure the DDNS entry in **Remote Gateway Address** on peer VPN gateway.
7) Both **DNS** and **E-mail** can be used as the Local ID & Peer ID for authentication.

Note: If Hi-Available (HA) for incoming VPN HA is necessary, enable the **HA** option while configure the DDNS entry under DNS-> DDNS ZyWALL will update its DDNS entry with another WAN interface when the specified WAN interface is not available. Therefore, the next coming VPN connection will go through second WAN interface.

Configure ZyWALL behind NAT Router

This section describes an example configuration ZyWALL behind NAT Router (Internet Gateway).

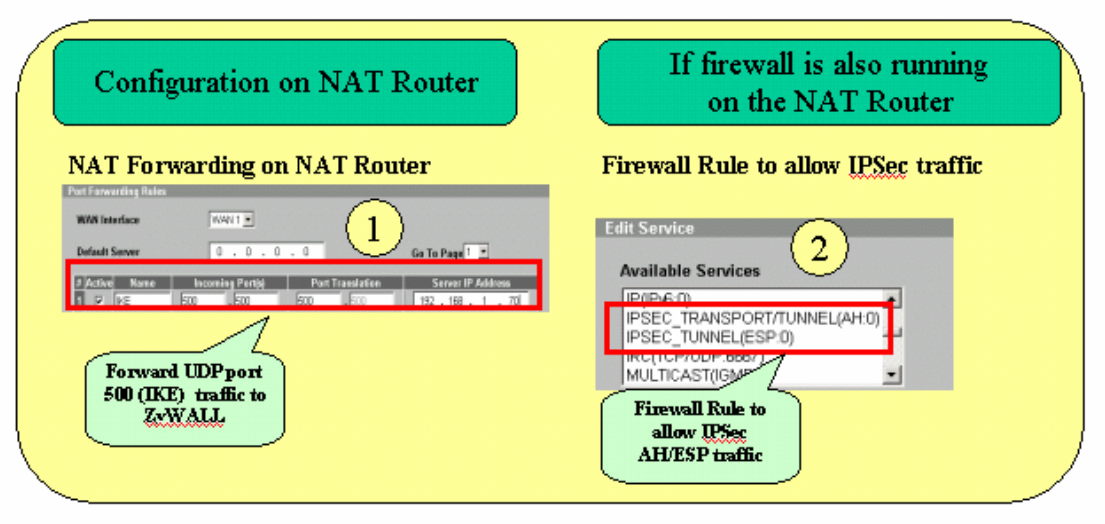
NAT routers sit on the border between private and public (Internet) networks, converting private addresses in each IP packet into legally registered public ones. NAT is commonly supported by Internet access routers that sit at the network edge. However, IPSec is NAT-sensitive protocol which means modification on IPSec traffic may cause failure of VPN connection.



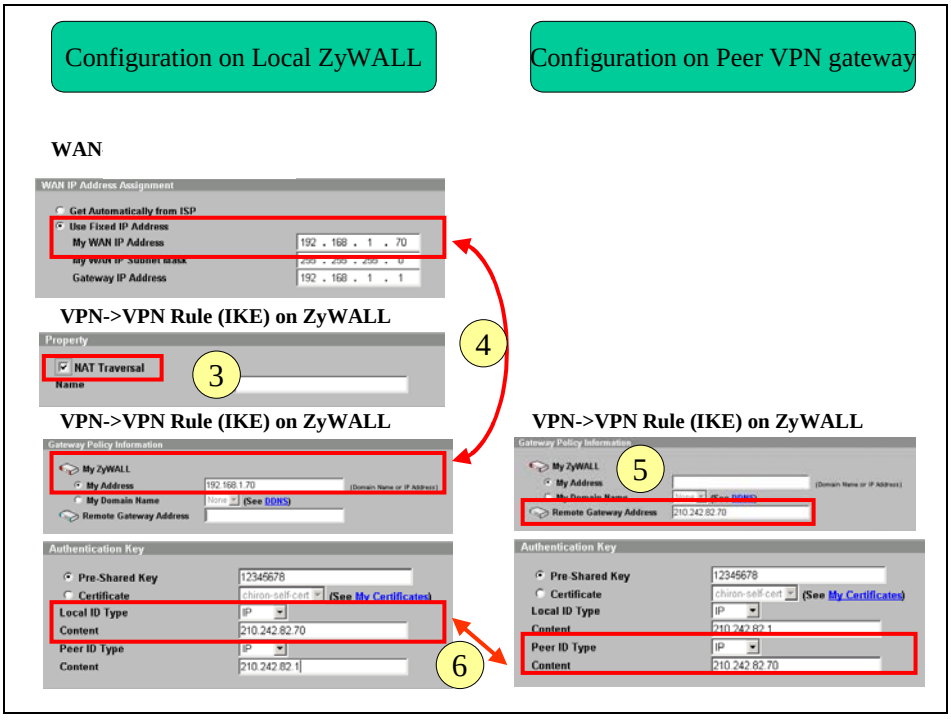
By far the easiest way to combine IPSec and NAT is to completely avoid these problems by locating IPSec endpoints in public address space. This can be accomplished in two ways:
1) Perform NAT on a device located behind IPSec gateway
2) Use an IPSec gateway for both IPSec (VPN) and NAT (Internet Access).

However, in some situation, it is inevitable to locate IPSec gateway in public IP address and it must be

placed behind the NAT router. For example, the NAT router has a different interface (e.g. leased line, ISDN) which are not supported by IPSec gateway. This example gives some guideline for configuring ZyWALL behind NAT router.



1) UDP 500 (IKE) must be forwarded to ZyWALL to accept incoming VPN connection from peer VPN gateway or client.
2) If Firewall is running on the same NAT router, make sure a firewall rule is configured to allow IKE/IPSec (AH/ESP) traffic to pass-through.



3) On ZyWALL, enable "**NAT Traversal**" no matter if the front NAT router supports NAT Traversal (IPSec pass-through) or not. With this option enabled, ZyWALL can detect if it is placed behind NAT when peer VPN entity also support NAT Traversal function. If yes, the IPSec traffic will be

encapsulated in UDP packet to avoid traversal problem on NAT routers.

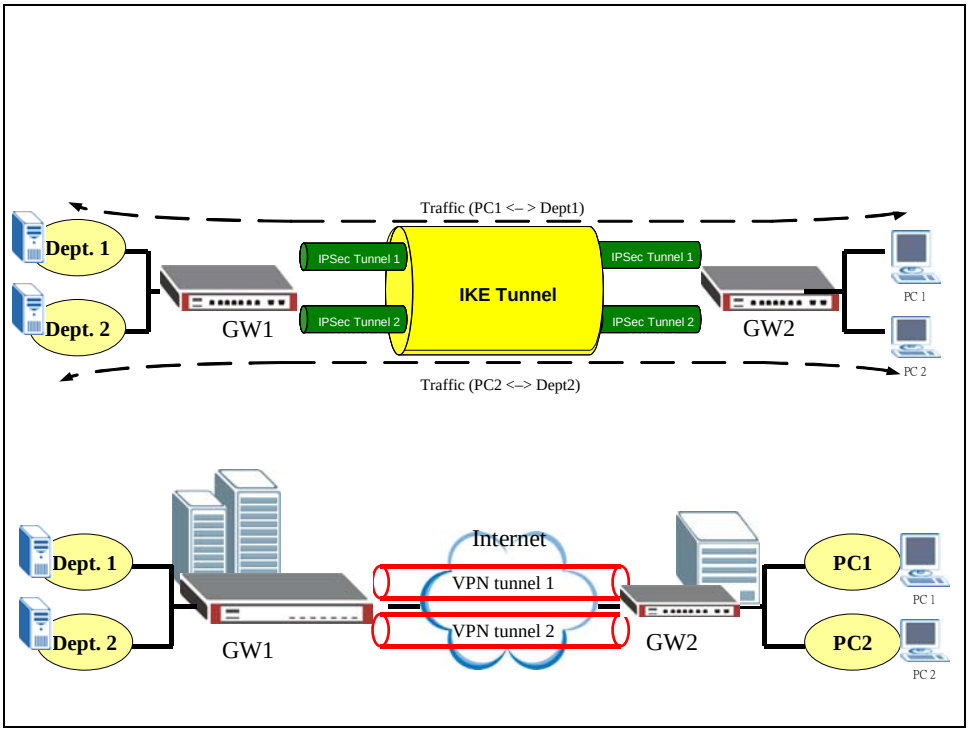
4) Under **VPN->Gateway Policy-> Gateway Policy Information** configure the **private IP address** as "**My Address**" on local ZyWALL gateway (behind NAT router).
5) On peer VPN gateway, use the public **WAN IP address of NAT Router** as the "**Remote Gateway Address**" of Gateway Policy rule.

The ID must be consistent no matter if IP/DNS/EMAIL is used. So long as if the ID Type and content are consistent on both VP entities.

Mapping multiple Network policy to same gateway policy

This section describes an example configuration to map multiple (different) network policies to same gateway policy which is built between two VPN gateways. Different network policies allow user in one network to access multiple destination networks which are not in the continuous range. The other feature of this application is to limit some users to access some specific destination and prevent others from accessing the same network.

In following example, the owner of PC1 belongs to financial department and needs to connect to the financial department (Dept.1) for business sensitive application. PC2 belongs to other group (Dept.2) and need to access Dept.2 .



The configuration goal is to achieve following two:

1) Setup VPN rule to allow PC1 to access Dept.1 through the tunnel between GW1 & GW2
2) Setup VPN rule to allow PC2 to access Dept.2 through the tunnel between GW1 & GW2

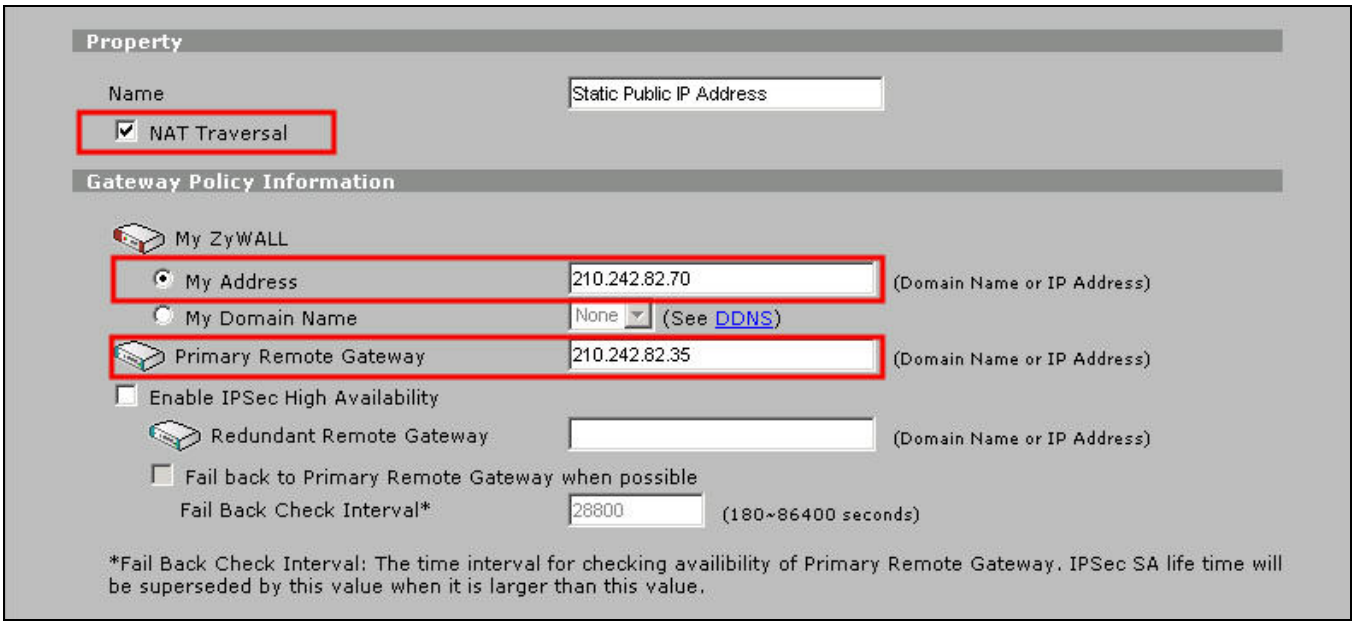
PC1	PC2	GW2	GW1	Dept.1	Dept.2
192.168.35.101	192.168.35.102	WAN 210.242.82.35	WAN 210.242.82.70	192.168.71.0/24	192.168.72.0/24

The following will illustrate how to configure on the GW1:

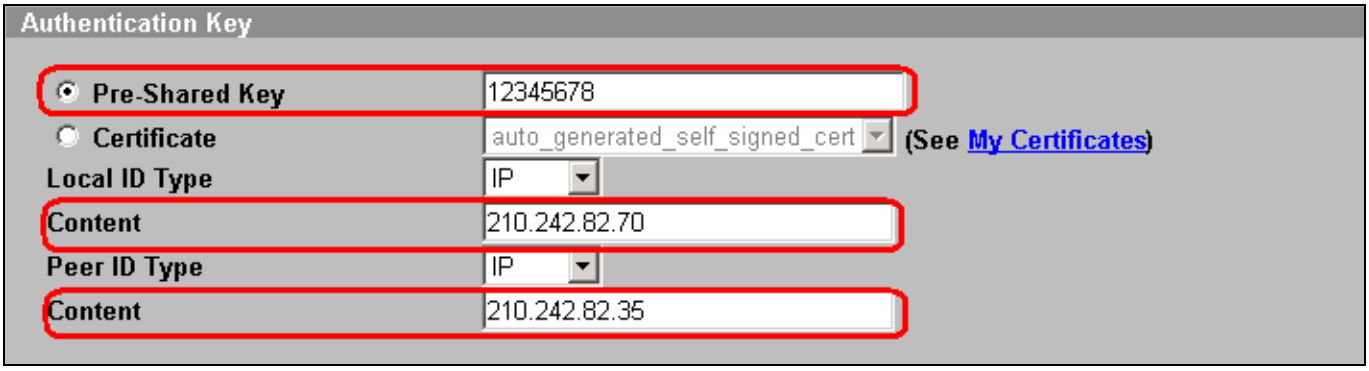
1) Login ZyWALL and click at “VPN”

3) Click on the icon to add a new “gateway policy” of the VPN tunnel

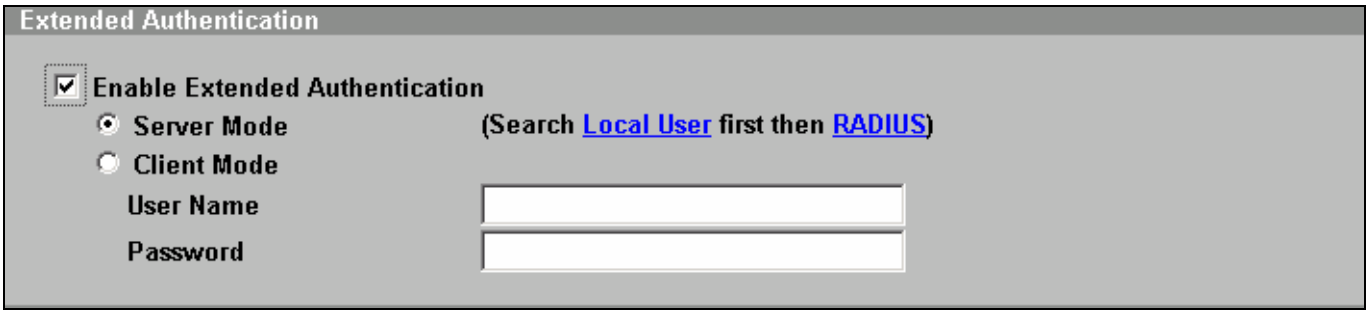
4) Enable “NAT Traversal” and configure the WAN IP as the “My Address” of My ZyWALL and



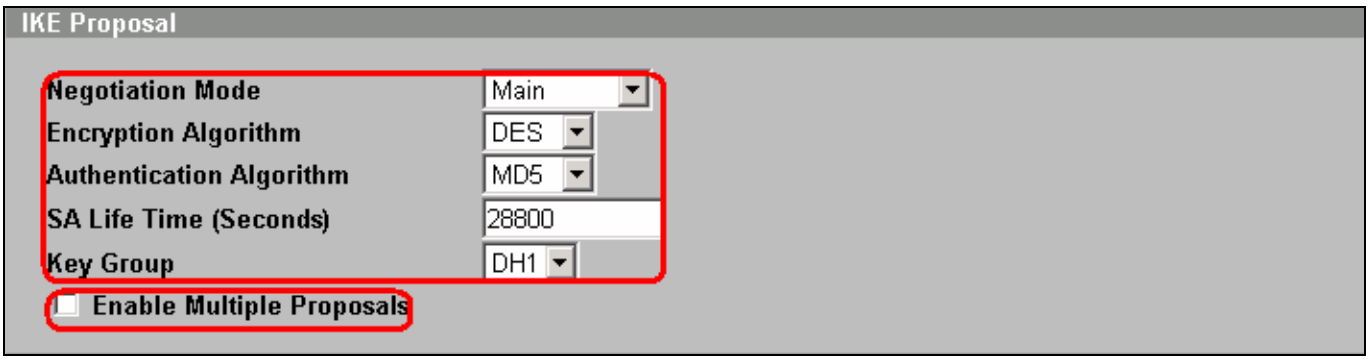
5) Under Authentication Key, “Pre-Shared Key” or “Certificate” can be used as authentication method. For detailed usage of “Pre-Shared Key” and “Certificate”, please refer to XXX. In this example, “Pre-Shared Key” is used and the string “12345678” is used as example.



6) Extended Authentication (xAuth) can be enabled or not depending on your application. For detailed info, you can refer to XXX.

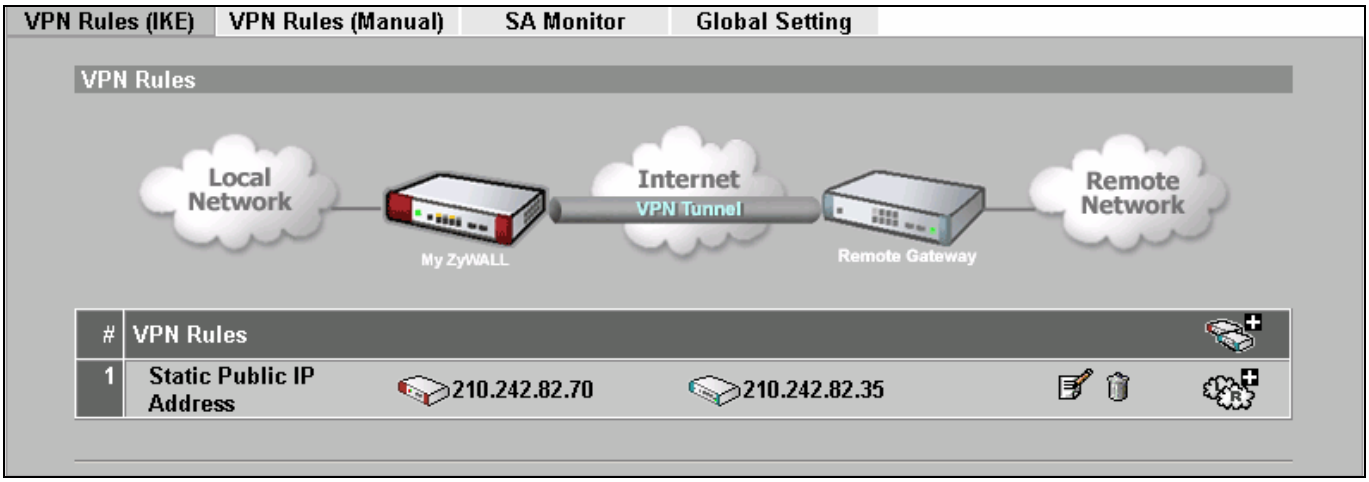


7) Under “IKE Proposal”, select the Encryption and Authentication Algorithm. Note the configuration must be consist on both ZyWALLs (GW1 & GW2)



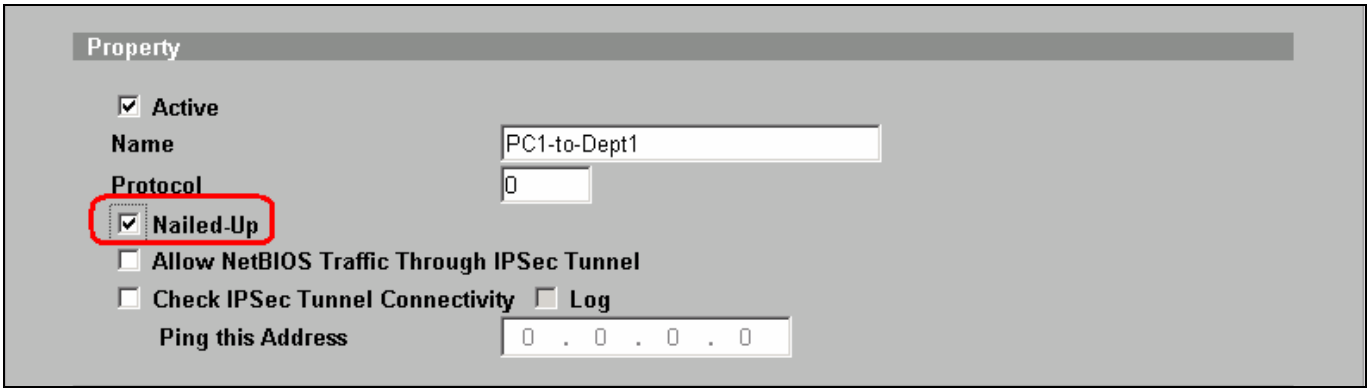
8) Click on “Apply” to save profile

9) The IKE rule will be configured as below:



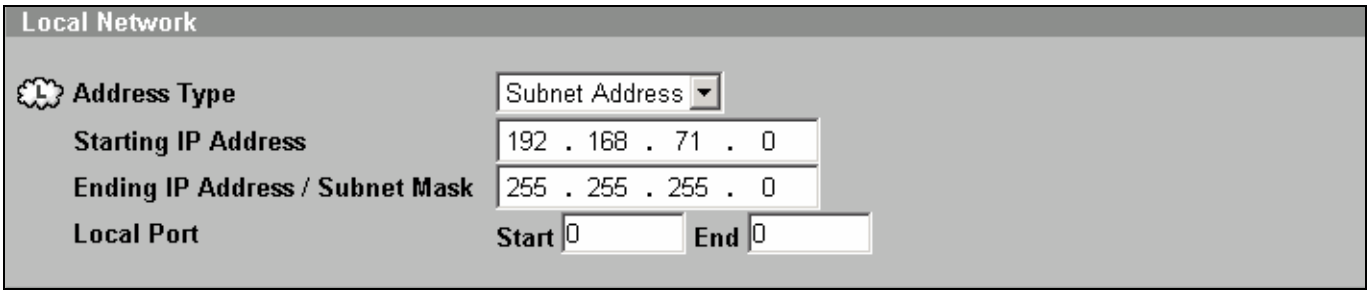
10) Click on the icon to add a new "Network Policy" over the configured Gateway Policy.

11) Activate the profile and name this policy as "PC1-to-Dept1" in this example. Enable "Nailed-Up" option if you need the functionality that will automatically re-initiate a tunnel to a configured peer in the event of SA Lifetime expires, failure on the link.

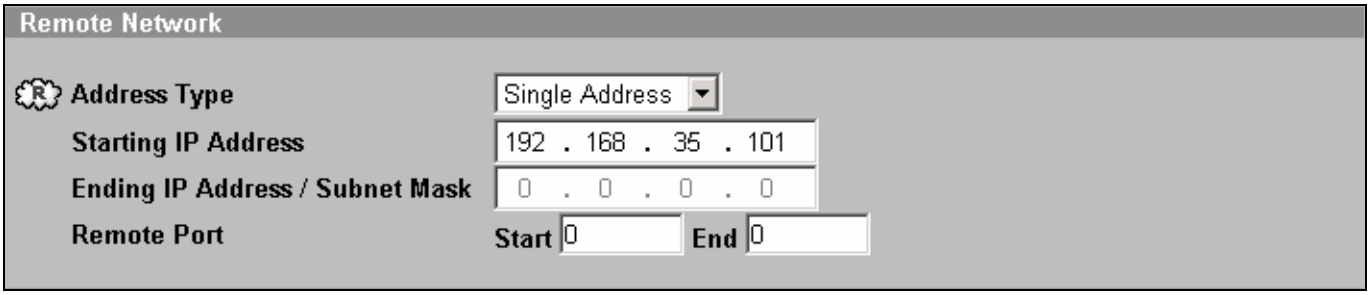


12) This network policy "PC1-to-Dept1" will be mapped to Gateway Policy, "Static Public IP Address" by default. If you need to change to other pre-defined Gateway Policy, you can select from the drop-down list.

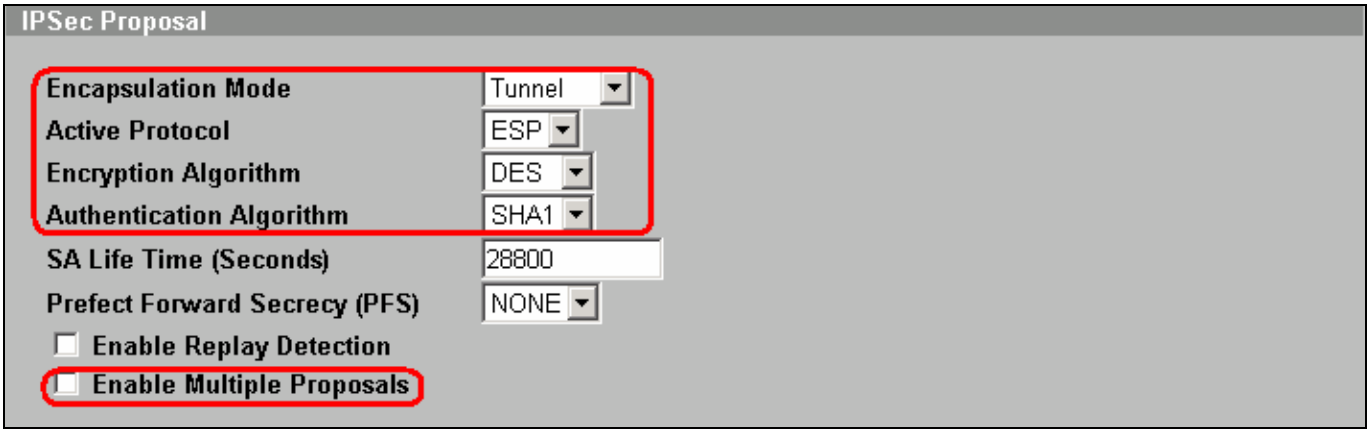
13) Under "Local Network", choose "Subnet" and input "192.168.71.0" and "255.255.255.0" for Dept1 in this example.



14) Under “Remote Network”, choose “Single” and input “192.168.1.101” for PC1 in this example.

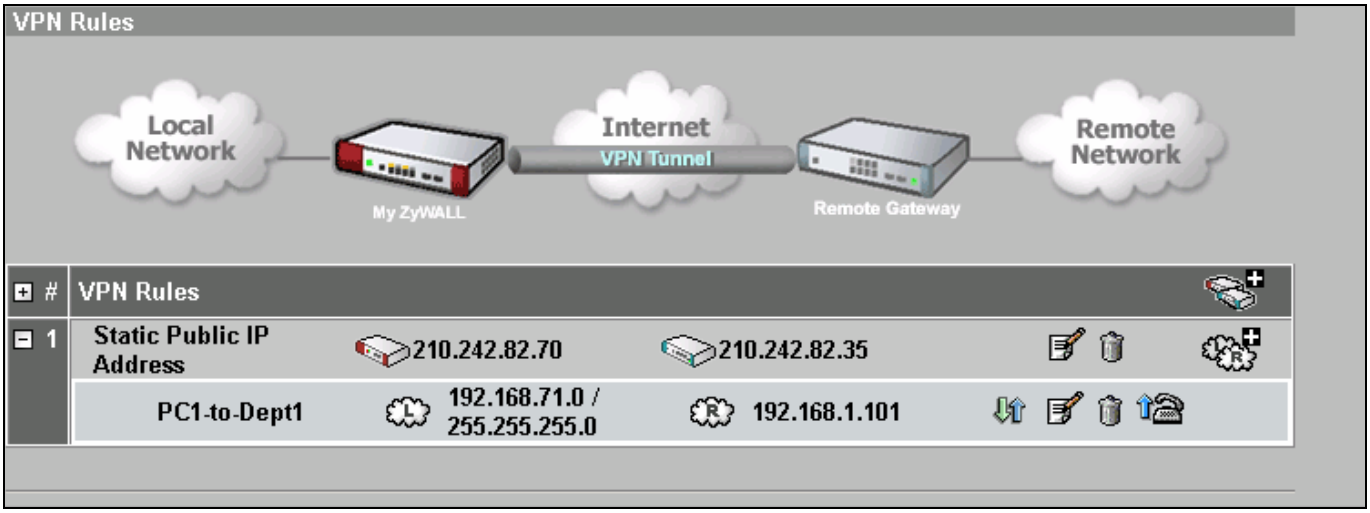


15) Under “IPSec Proposal”, select the Encryption and Authentication Algorithm. Note the configuration must be consist on both ZyWALLs (GW1 & GW2)

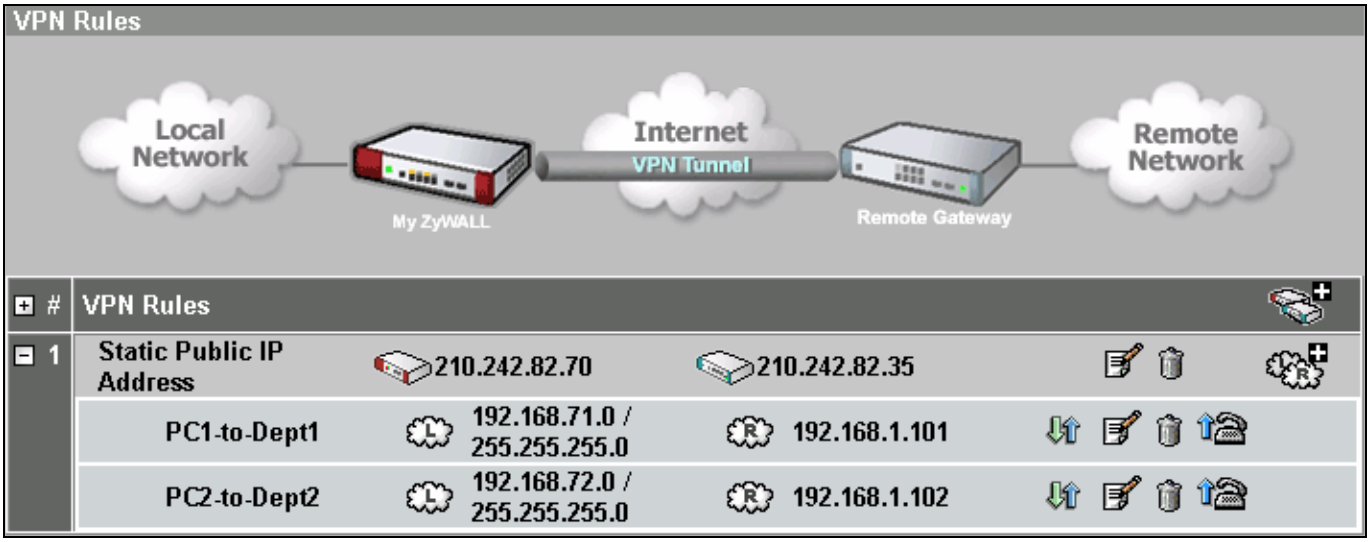


16) Click on “Apply” to save profile

17) The new Network Policy, PC1-to-Dept1 is added to the Gateway Policy.



18) Follow the same procedures as step 10~16 to add 2nd Network Policy, PC2-to-Dept2.



Finish

Using Certificate for Device Authentication

IKE must authenticate the identities of the systems using the Diffie-Hellman algorithm. This process is known as primary authentication. IKE can use two primary authentication methods:

1) Digital Signatures
2) Pre-shared keys

Digital signature and public-key encryption are both based on asymmetric key encryption and require a mechanism for distributing public keys. This is usually done using security certificates and a Public Key Infrastructure (PKI).

If certificate (Digital Signatures) is used for authentication, there are five available types of identity: **IP,**

DNS, E-mail, Subject Name and Any.

Depending how certificates are generated, it can be classified into three methods:

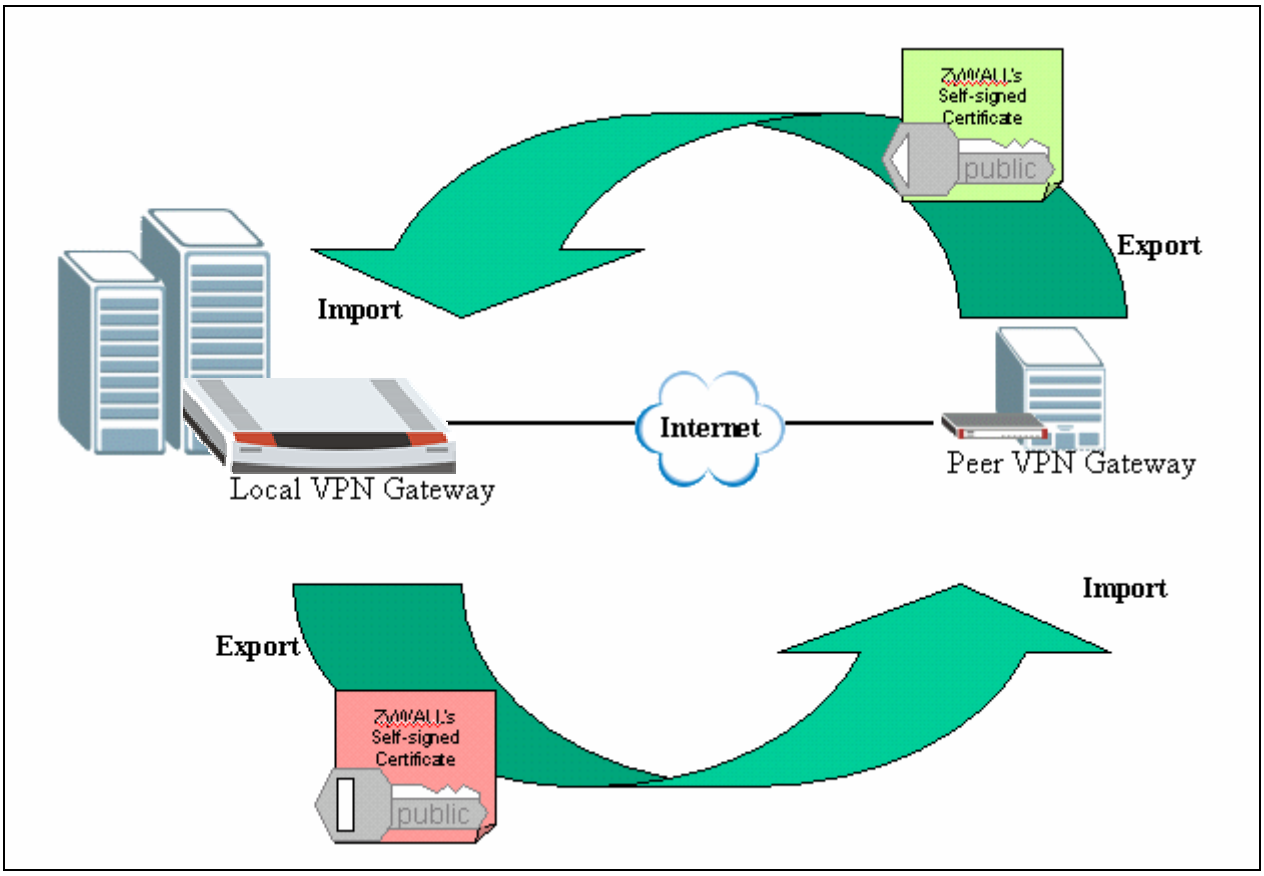
1) Using Self-signed Certificates (both entities must be ZyXEL IPSec gateway)
2) Online Enroll Certificates
3) Offline Enroll Certificates

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.

Using Self-signed Certificates

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) itself.

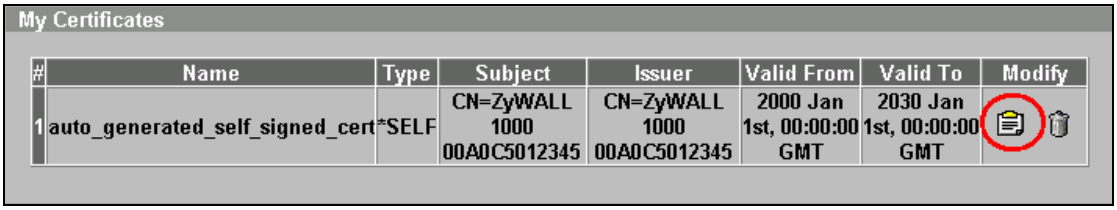
ZyWALL has the feature to sign itself a so-called self-signed certificate which can be imported to other ZyWALL for authentication. This feature allows users to use certificate without CA. The certificate must be exchanged and imported into **Trusted Remote Hosts** before making a VPN connection.



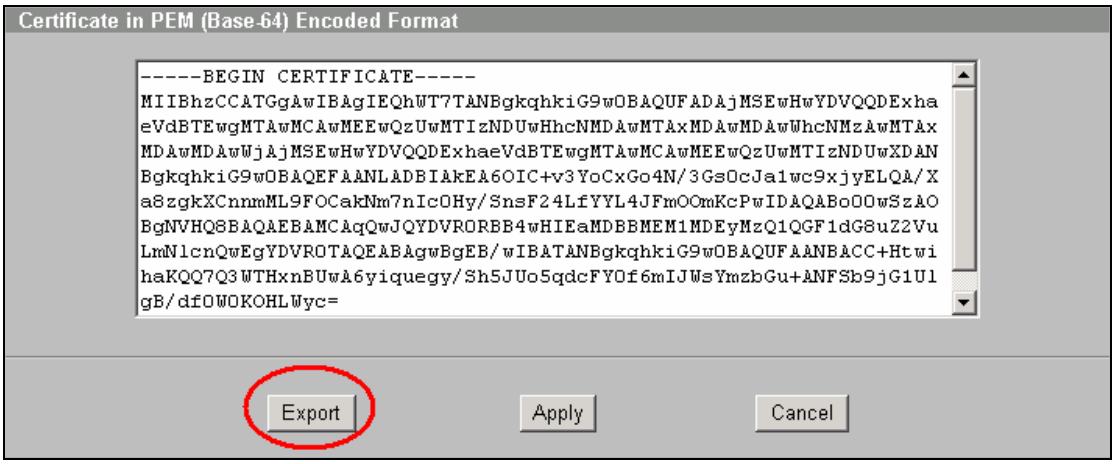
The factory default self-signed certificates are the same on all ZyWALL models. It is not secure to use the default self-signed certificate. To make the self-signed certificate unique for this device, you should replace the factory default certificate by pressing the Apply button in the following page at the first time you login to ZyWALL.

If you reset ZyWALL to default configuration file, the original self-signed certificate is also erased, and a new self-signed certificate should be created at the first boot up time.

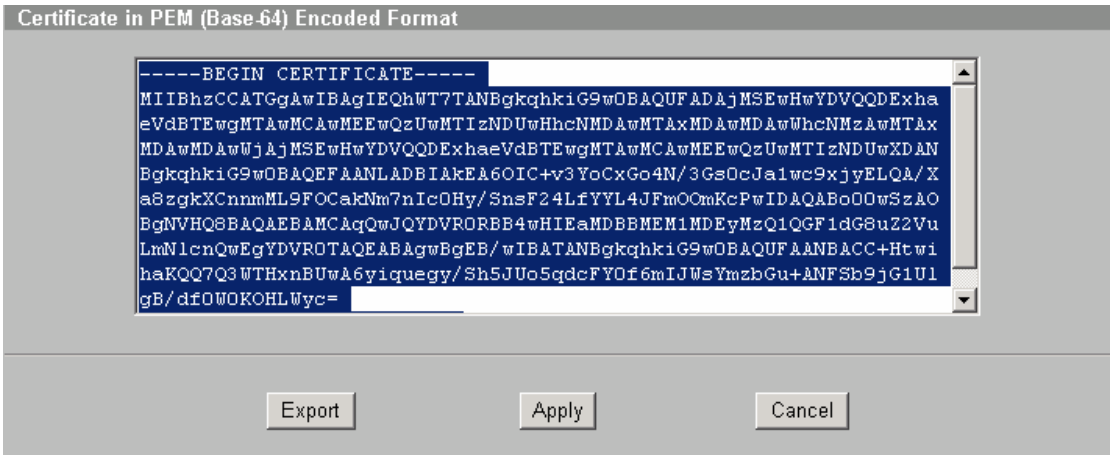
To use self-signed certificate, go to ZyWALL **CERTIFICATES->My Certificates** and export ZyWALL's certificate.



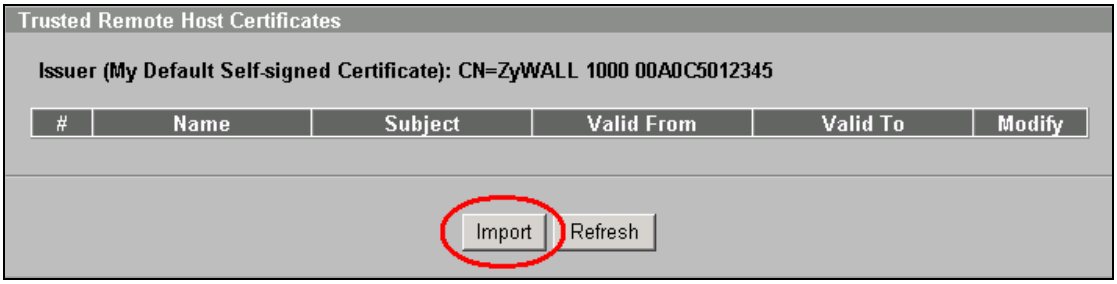
1) Press "Export" to save the ZyWALL self-signed certificate to local computer in **Binary X.509** format.



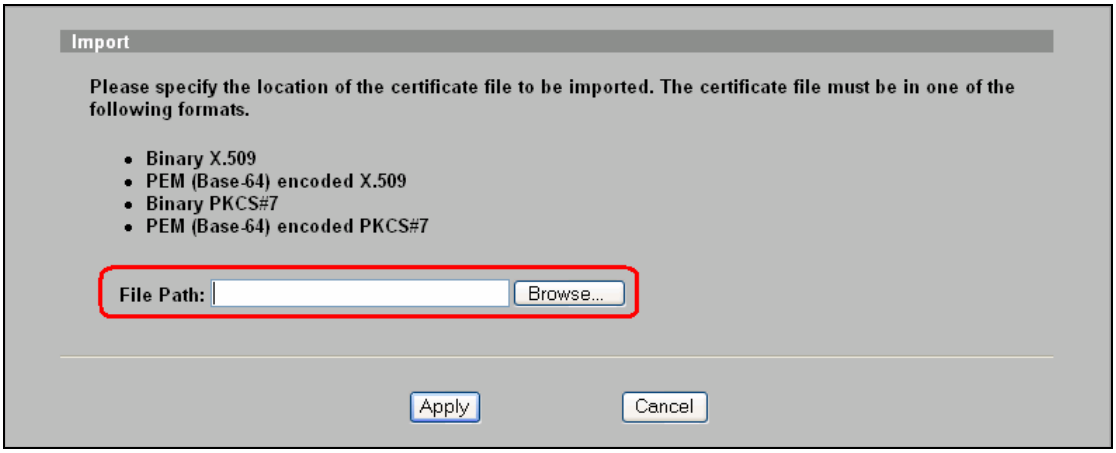
2) Or mark the certificate in **PEM (Base-64) Encoded Format** and then copy to a test editor (e.g. Notepad) and then save to you local computer in **PEM (Base-64) Encoded** Format.

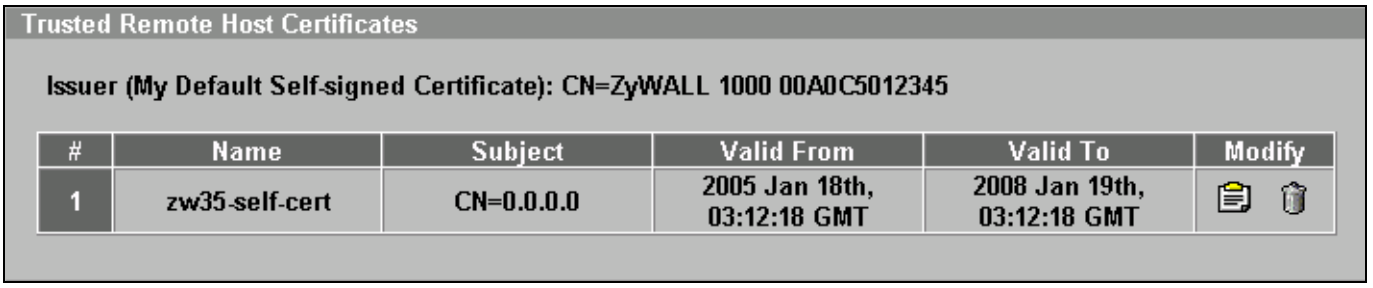


Then import the certificate to the other ZyWALL VPN gateway. Go to the other ZyWALL and click "Import" button under **CERTIFICATES->Trusted Remote Hosts**



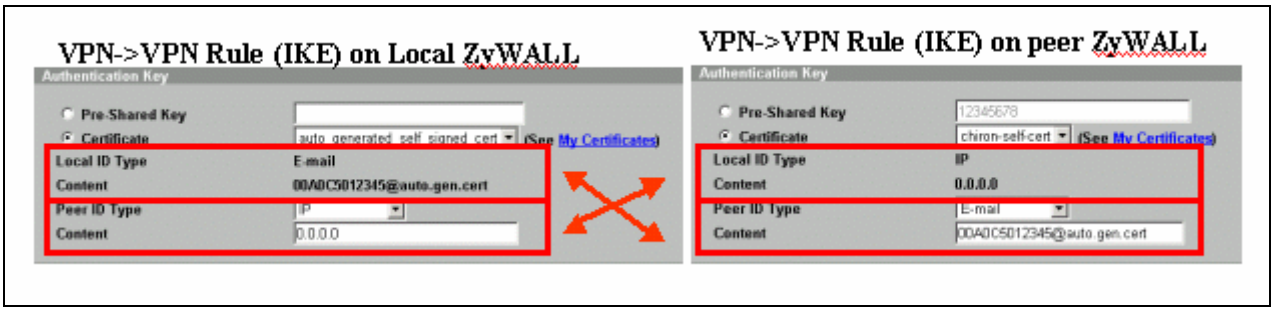
Select the certificate from local computer.





When you configure VPN rule with certificate, select Certificate under VPN-> Gateway Policy. Select My Certificate from the drop-down list. When (My) certificate is selected, ZyWALL will show what is the Local ID Type and Content in my certificate. You must configure the same setting on peer ZyWALL and vise versal.

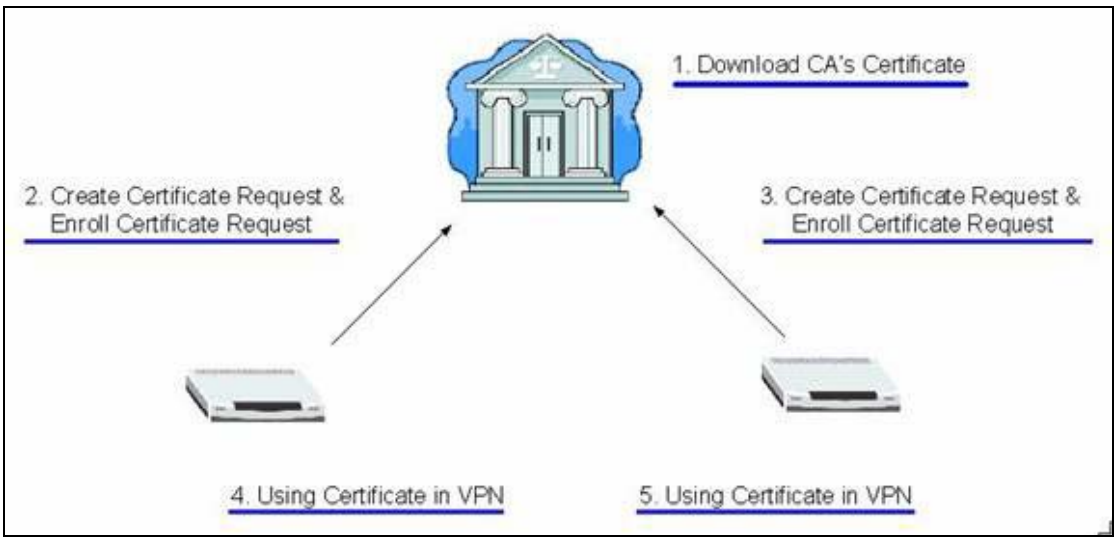
For example, on Local ZyWALL, the Local ID Type is E-mail and content is 00A0C5012345@auto.gen.cert. Therefore, configure Peer ID Type and content on peer ZyWALL.



Online Enroll Certificates

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. With online enrollment, ZyWALL firstly create certification request locally, then send certification request to trusted CA (Certificate Authority)

servers, and finally get a certificate for further usage. ZyWALL supports both SCEP and CMP protocols as methods of online enrollment. Both SCEP and CMP online enrollment protocols provide secure mechanisms to transmit ZyWALL's certification request securely over Internet. In this example, we adopt SCEP protocol to enroll certificates.

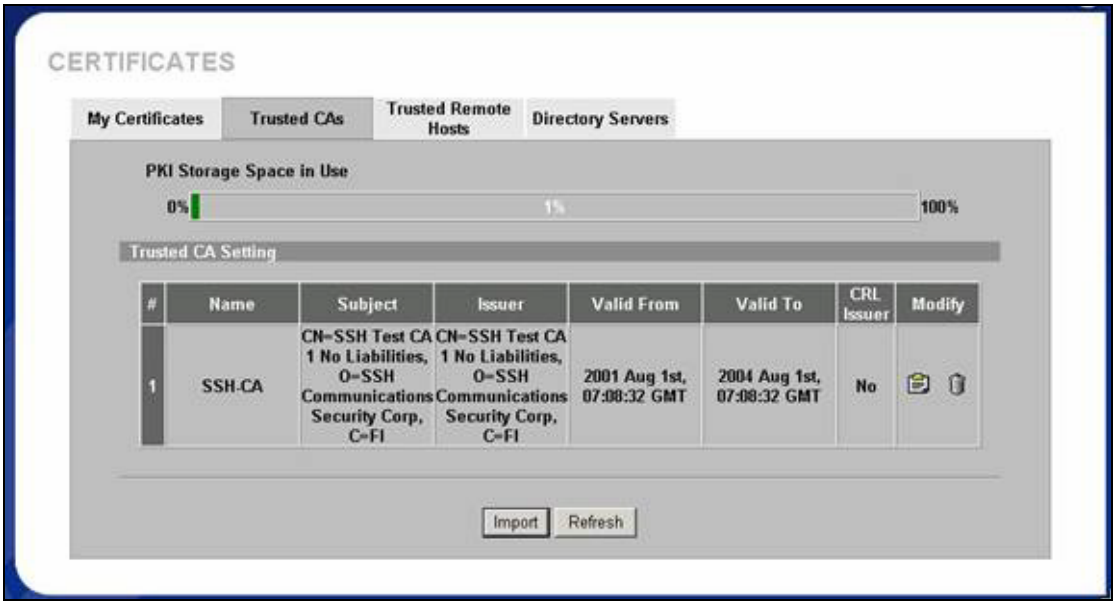


LAN 1	ZyWALL A	ZyWALL B	LAN 2
10.1.133.0/24	LAN: 10.1.133.1 WAN: 192.168.1.35	LAN: 192.168.2.1 WAN:192.168.1.36	192.168.2.0/24

Step 1. Download CA server's Certificate

The most critical part for online certification request would be we need to send the certification request over Internet, which is an insecure environment. To prevent certification request from being modified or eavesdropped, we need to download CA server's certificate in the first step. When ZyWALL delivers the certification requests, the public key in CA server's certificate will be used to protect the data.

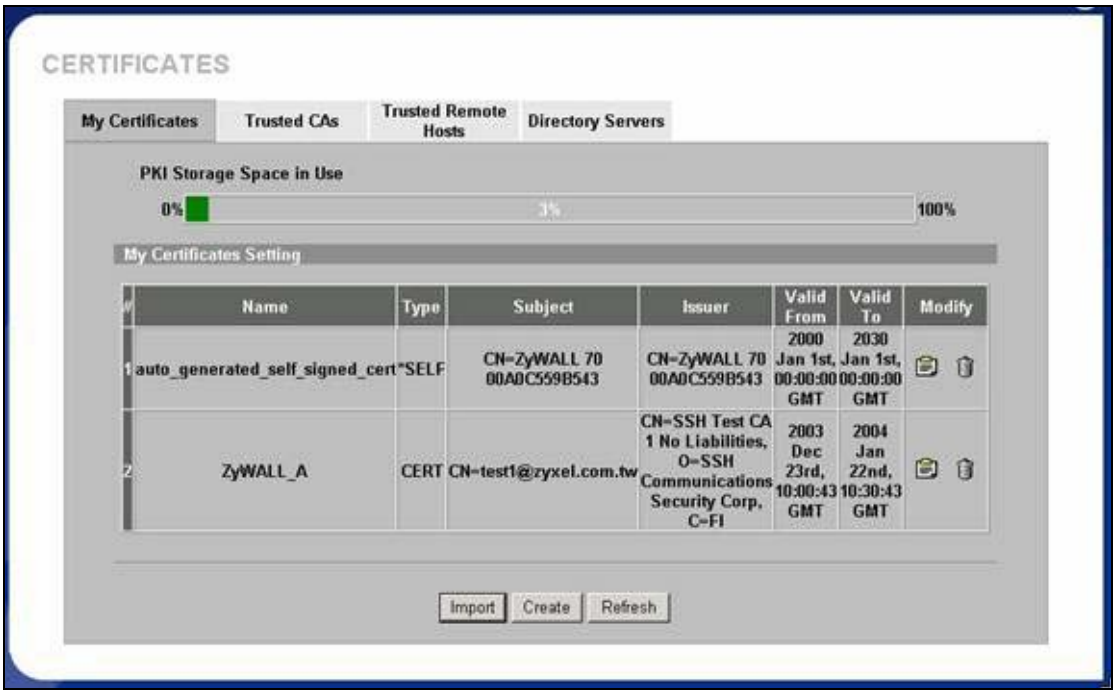
You may need to access CA server's WEB interface or contact the administrator to get CA's certificate. Then you can go to SECURITY->CERTIFICATES->Trusted CAs to import the downloaded certificate.



Step 2. Create certificate request and enroll certificate request on ZyWALL A

1. Input a name, for this Certificate so you can identify this Certificate later.
2. In Subject Information, give this certificate a Common Name by either Host IP Address, Host Domain Name or E-Mail address. Organizational Unit, Organization, Country are optional fields, you are free to either enter them or not.
3. Finally, specify the key length.
4. Select **Create a certification request and enroll for a certificate immediately online.**
5. Specify the Enrollment Protocol to **Simple Certificate Enrollment Protocol (SCEP)**.
6. In the "CA Server's Address" field, input the URL to access CA server, for example, http://1.1.1.1:8080/scep/
7. Choose the previously downloaded CA server's certificate from the drop down list.
8. Input user name and password if necessary.
9. Then click **Apply**.

After pressing the **Apply** button, ZyWALL would create the certification request and send it to the CA server for enrollment. It may take one minutes to complete the whole process. After CA server agrees to issue the corresponding certificate, you will find a newly enrolled certificate in **My Certificates**.



Step 3. Create certificate request and enroll certificate request on ZyWALL B

1. Input a name, for this Certificate so you can identify this Certificate later.

2. In Subject Information, give this certificate a Common Name by either Host IP Address, Host Domain Name or E-Mail address. Organizational Unit, Organization, Country are optional fields, you are free to either enter them or not.

3. Finally, specify the key length.

4. Select **Create a certification request and enroll for a certificate immediately online.**

5. Specify the Enrollment Protocol to **Simple Certificate Enrollment Protocol (SCEP)**.

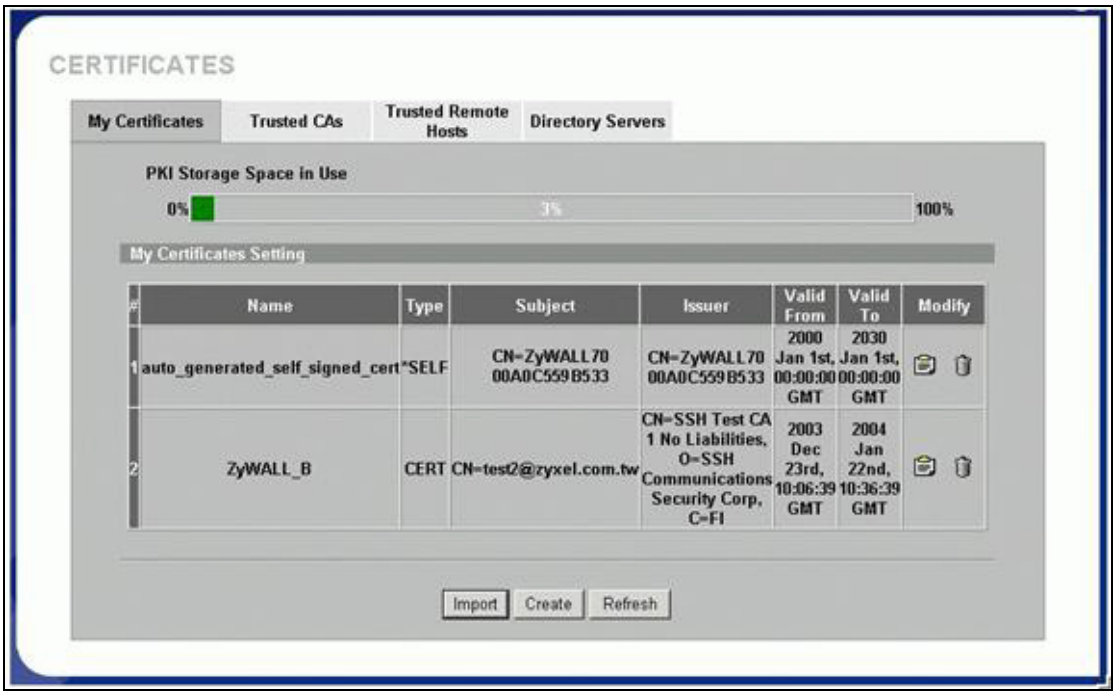
6. In the "CA Server's Address" field, input the URL to access CA server, for example, http://1.1.1.1:8080/scep/

7. Choose the previously downloaded CA server's certificate from the drop down list.

8. Input user name and password if necessary.

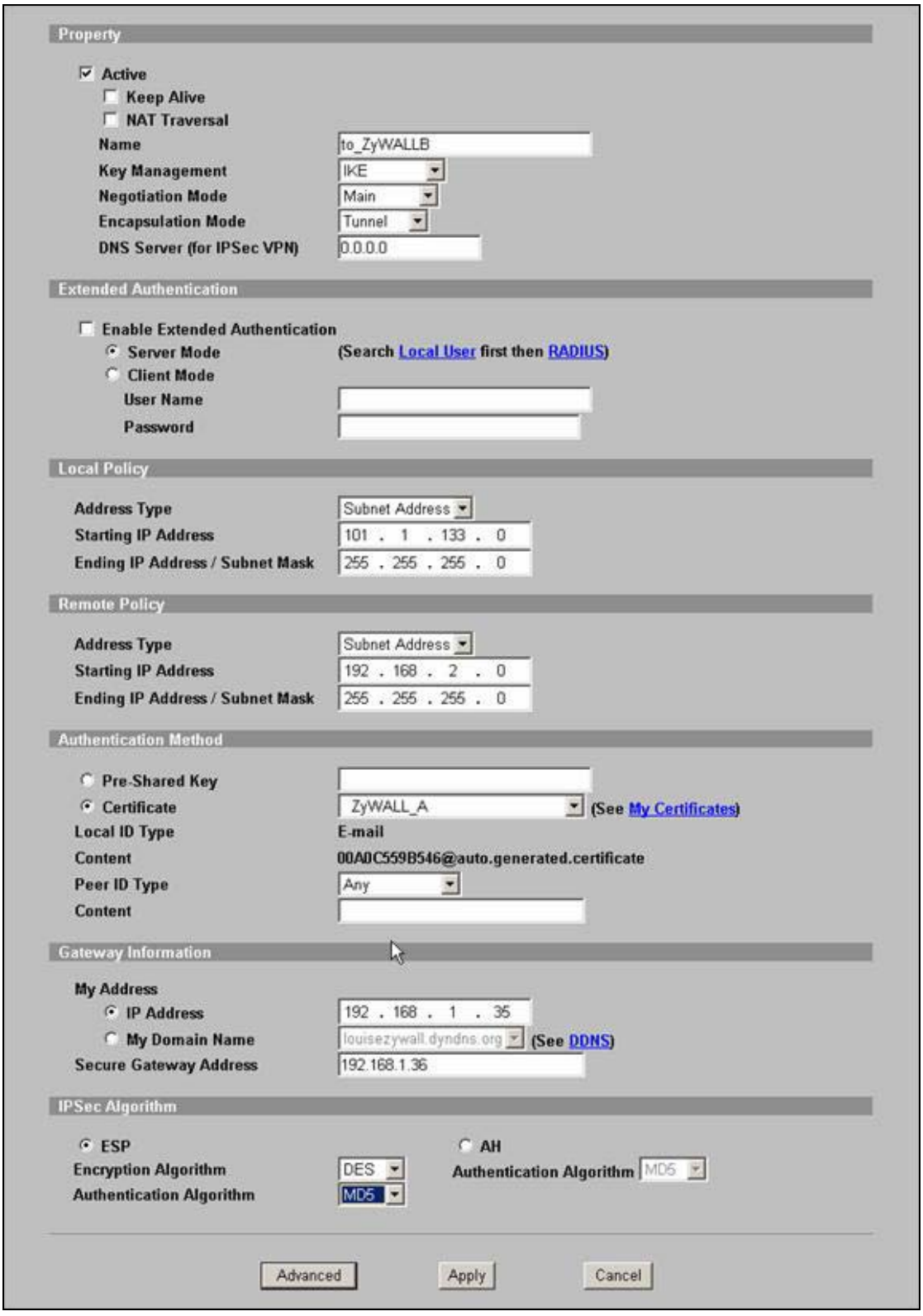
9. Then click **Apply**.

After pressing the **Apply** button, ZyWALL would create the certification request and send it to the CA server for enrollment. After CA server agrees to issue the corresponding certificate, ZyWALL will receive it automatically, and you will find a newly enrolled certificate in **My Certificates**.

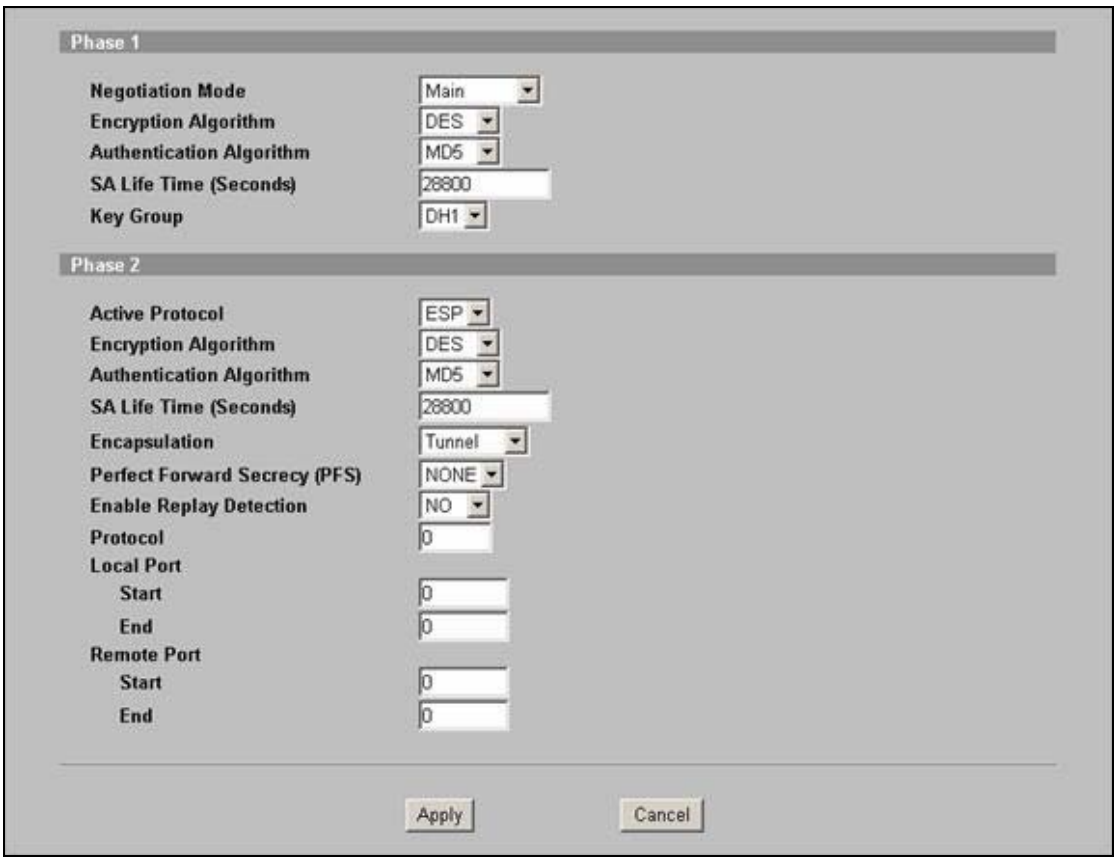


Step 4. Using Certificate in VPN on ZyWALL A

1. Activate the rule
2. Give this VPN rule a name "**toZyWALL_B**"
3. Select Key Management to "**IKE**"
4. Select Negotiation Mode to "**Main**"
5. Edit Local: Address Type="**Subnet Address**", Starting IP Address="**10.1.33.0**", End IP Address/Subnet Mask="**255.255.255.0**"
6. Edit Remote: Address Type="**Subnet Address**", Starting IP Address="**192.168.2.0**", End IP Address/Subnet Mask="**255.255.255.0**"
7. Authentication Key, Select **Certificate**, and choose certificate you enrolled for this device from drop down list.
8. Fill in My IP address= "**192.168.1.35**"
9. Peer ID type= **"ANY"**
10. Secure Gateway Address= "**192.168.1.36**"
11. Encapsulation Mode="**Tunnel**"
12. Leave other options as default.

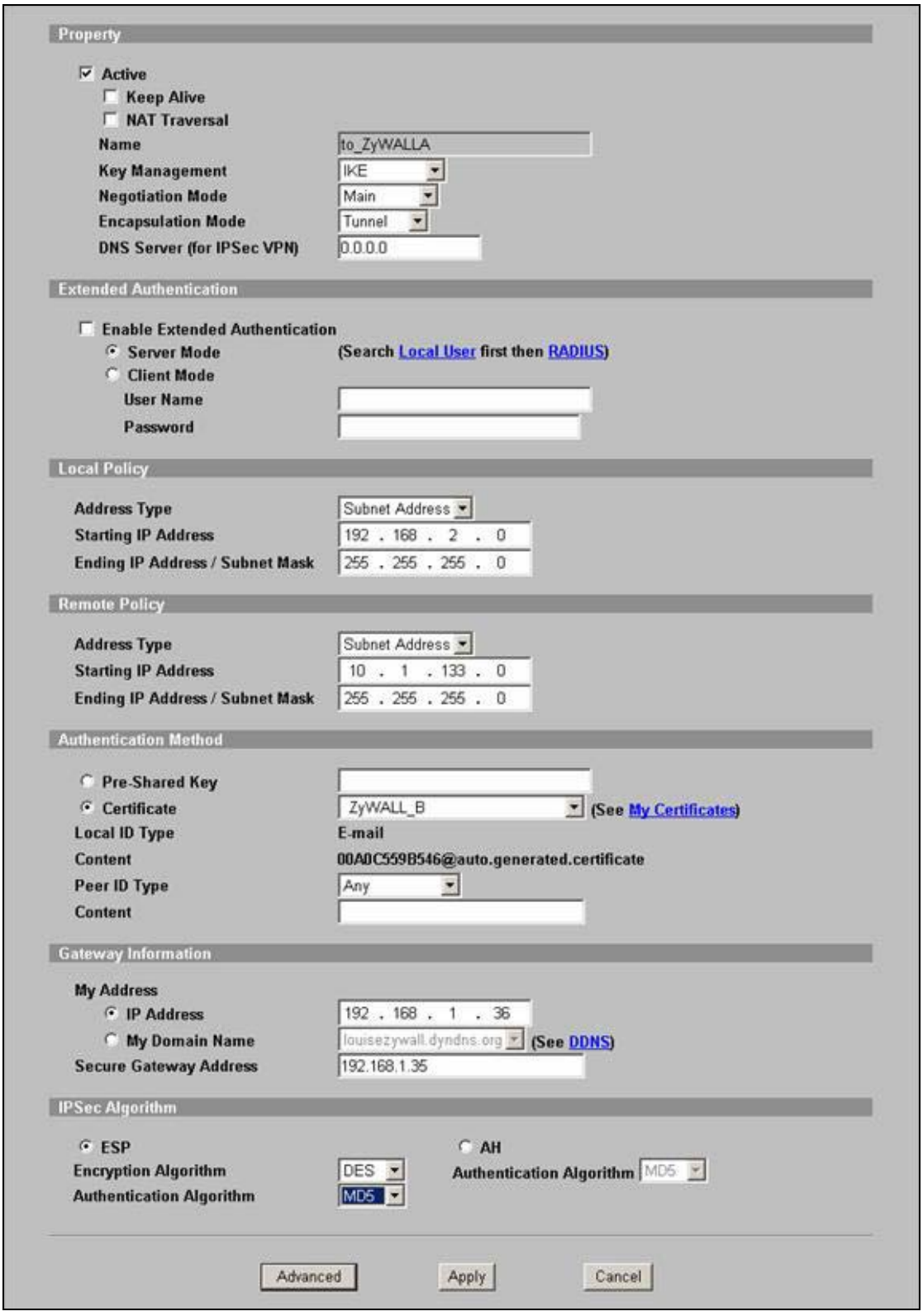


13. You can check detailed settings by clicking Advanced button.

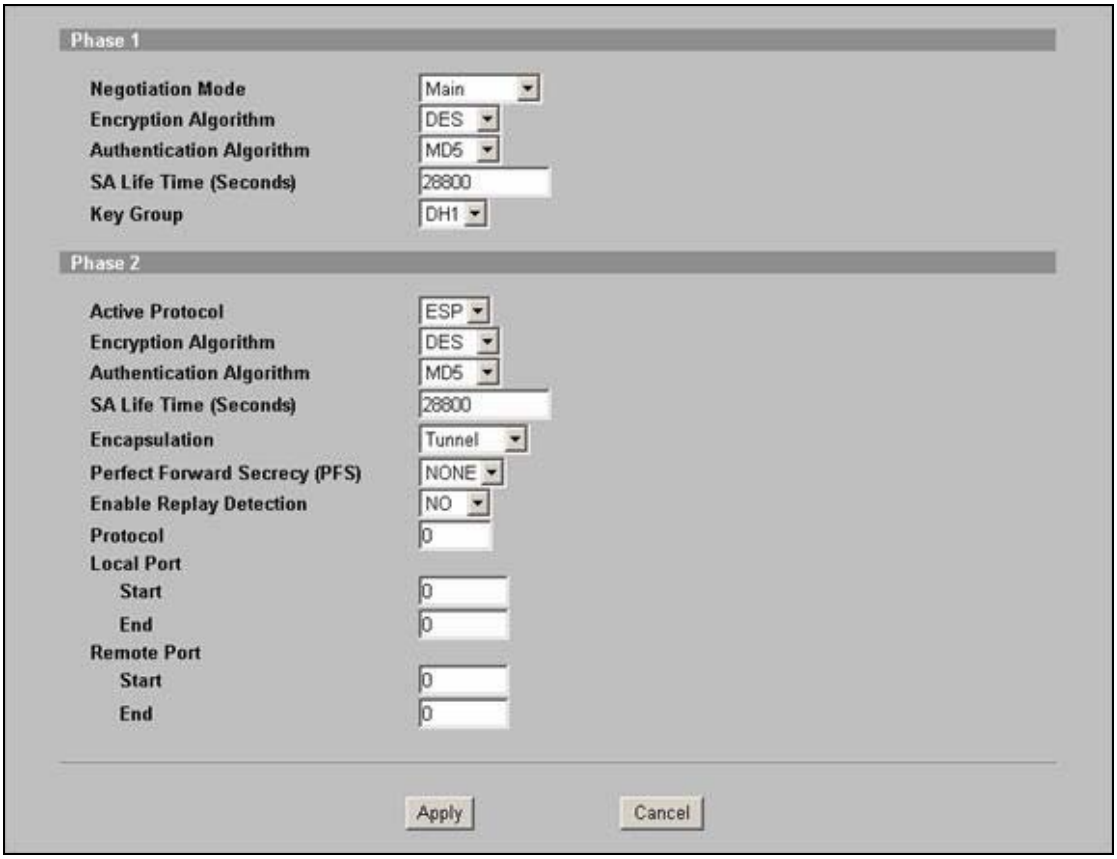


Step 5. Using Certificate in VPN on ZyWALL B

1. Activate the rule
2. Give this VPN rule a name "toZyWALL_A"
3. Select Key Management to "IKE"
4. Select Negotiation Mode to "Main"
5. Edit Local: Address Type="Subnet Address", Starting IP Address="192.168.2.0", End IP Address/Subnet Mask="255.255.255.0"
6. Edit Remote: Address Type="Subnet Address", Starting IP Address="10.1.33.0", End IP Address/Subnet Mask="255.255.255.0"
7. Authentication Key, Select Certificate, and choose certificate you enrolled for this device from drop down list.
8. Fill in My IP address= "192.168.1.36"
9. Peer ID type= "ANY".
10. Secure Gateway Address= "192.168.1.35"
11. Encapsulation Mode="Tunnel"
12. Leave other options as default.

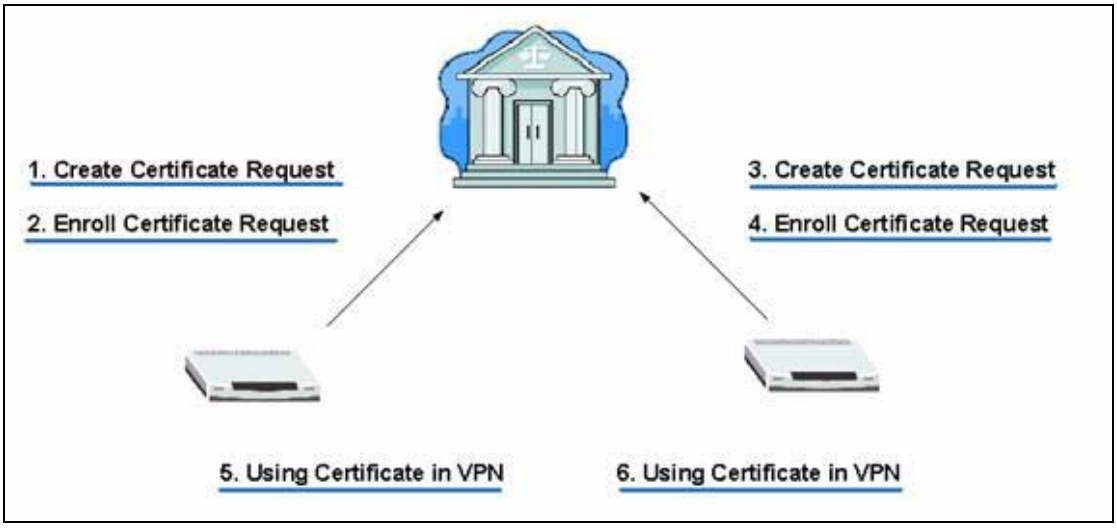


13. You can check detailed settings by clicking Advanced button.



Offline Enroll Certificates

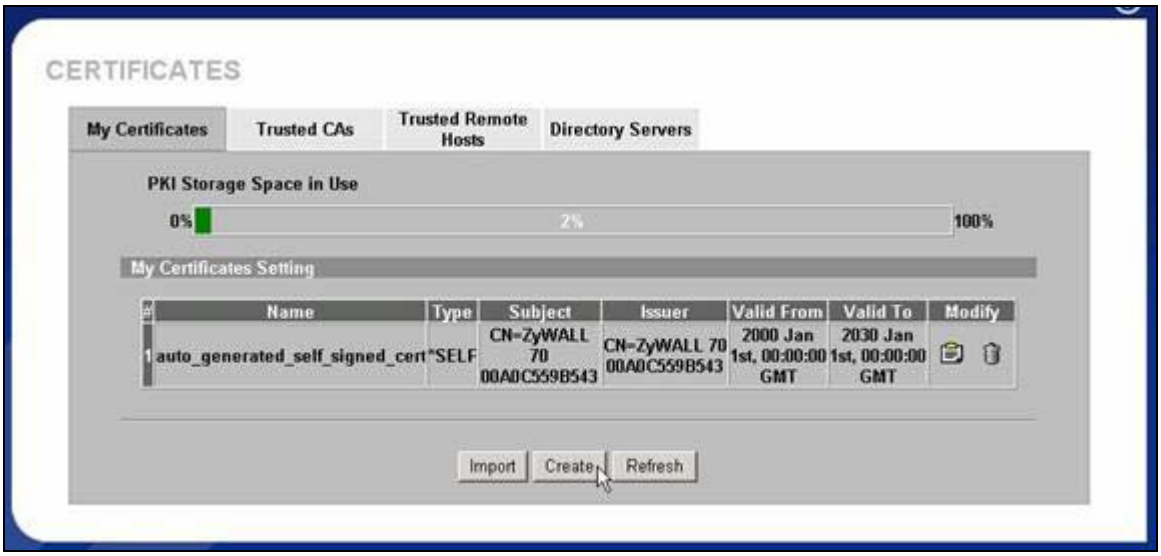
In this guide, we describe how ZyWALL devices, both ZyWALL A and ZyWALL B as IPSec/VPN tunnel end points, authenticate each other through PKI. We use CA (Certificate Authority) service provided by Windows 2000 server in this example. The whole procedure includes



LAN 1	ZyWALL A	ZyWALL B	LAN 2
10.1.133.0/24	LAN: 10.1.133.1 WAN: 192.168.1.35	LAN: 192.168.2.1 WAN:192.168.1.36	192.168.2.0/24

Step 1. Create Certificate Request on ZyWALL A

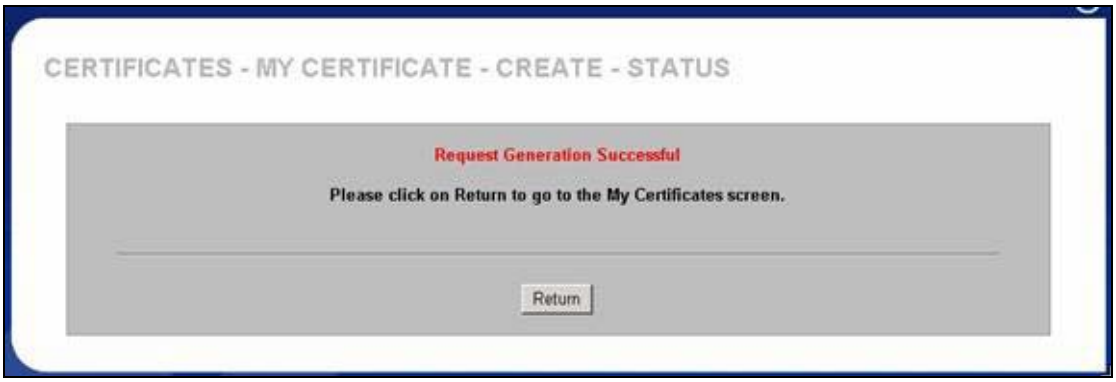
1. Go to **VPN->My Certificates** -> Click **Create** button.



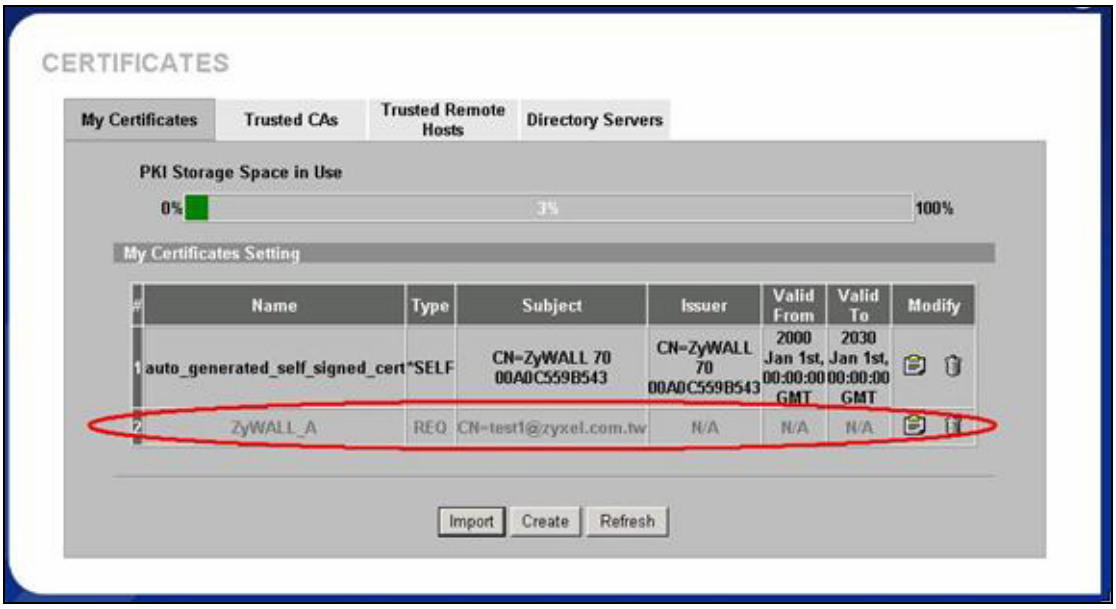
2. Input a name, for this Certificate so you can identify this Certificate later. In Subject Information, give this certificate a Common Name by either Host IP Address, Host Domain Name or E-Mail address. Organizational Unit, Organization, Country are optional fields, you are free to either enter them or not. Finally, specify the key length and select Create a certification request and save it locally for later manual enrollment.

3. Wait for 1-2 minutes until "Request Generation Successful" displays. During this period, ZyWALL is working on creation of private, public key pair, and certificate request.

4. After creating certificate request, ZyWALL would return Successful Message.

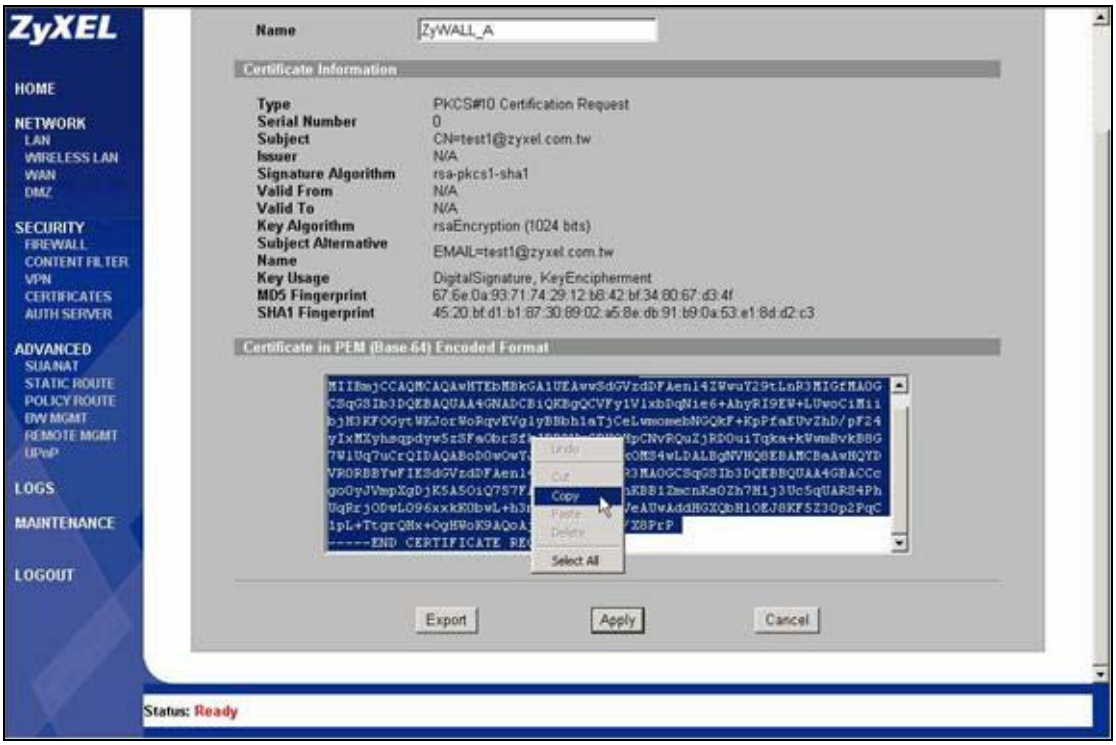


5. In **My Certificates** tab, you can get a new entry in grey color. This is the **Certificate Request** you just created. Click **Details** to export the request.



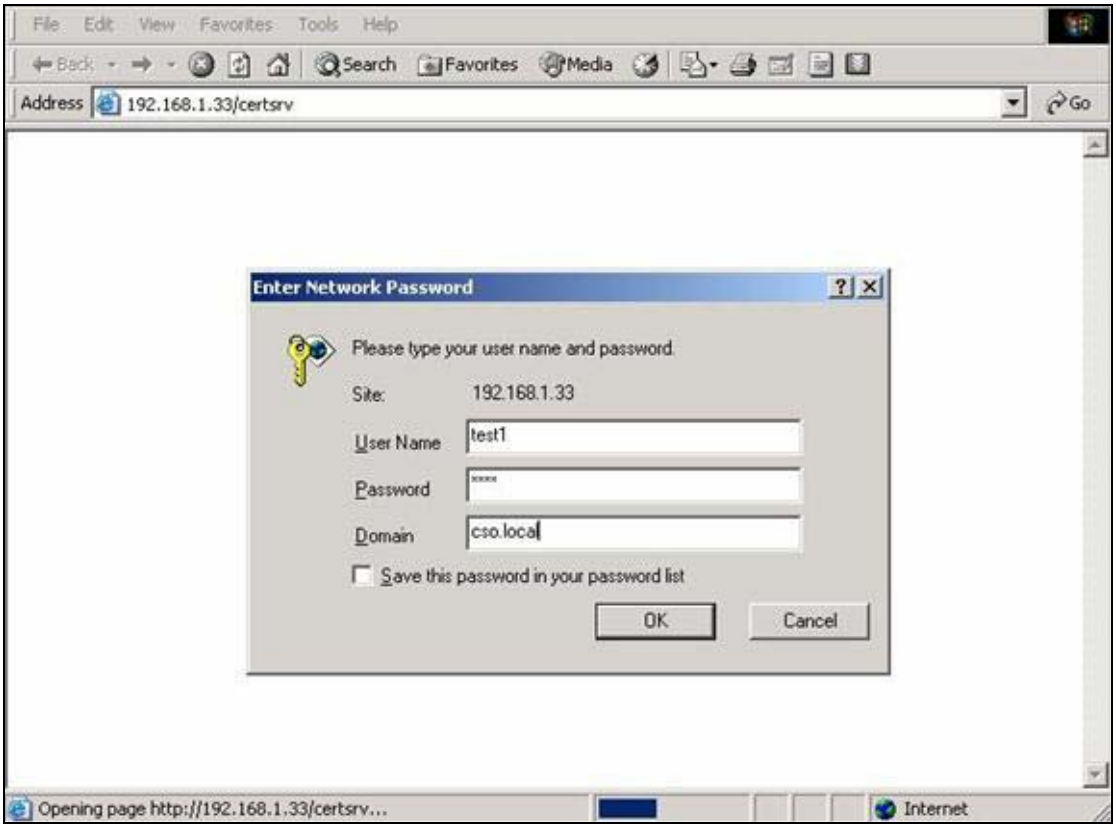
Step 2. Enroll Certificate Request

1. Copy the content of Certificate in PEM Encoded Format, by selecting all of the content, then right click your mouse, and select **Copy**. Keep your copy in clipboard for later paste.

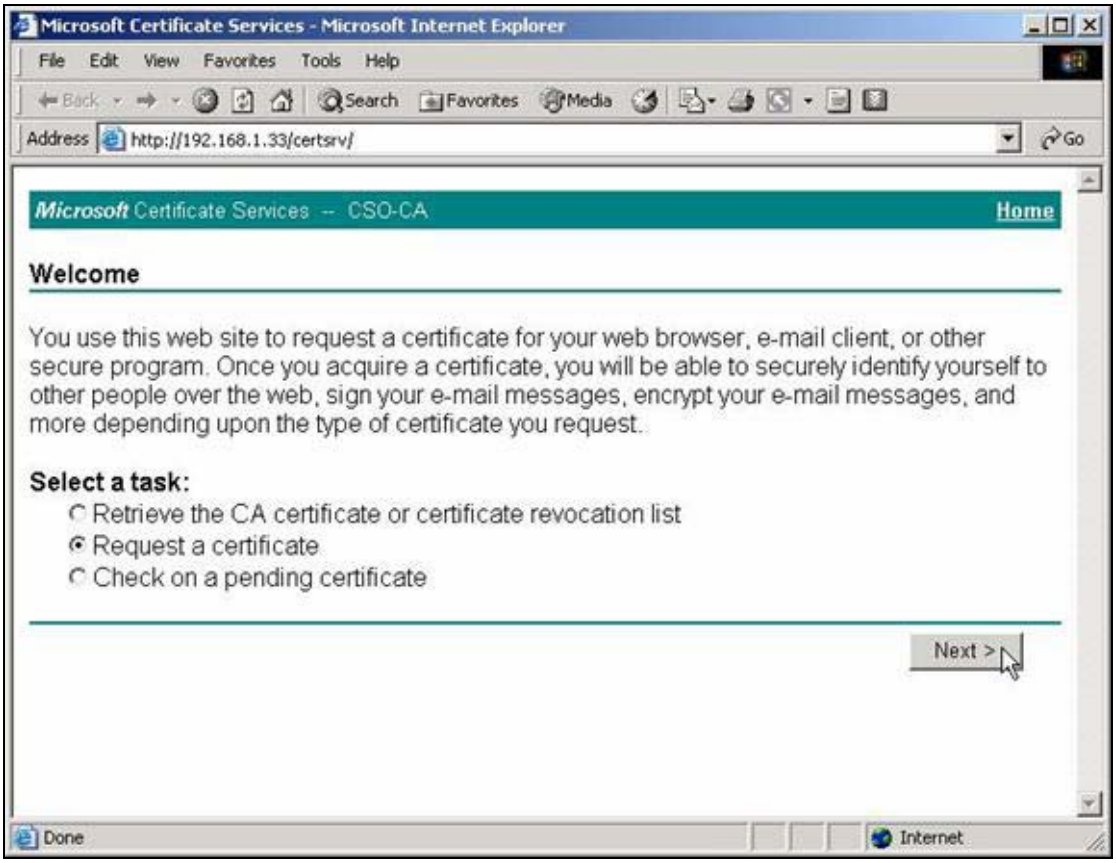


In this support note, we utilize certificate enrollment service from Microsoft Windows 2000 CA server. The enrollment procedure of your CA server may be different, you may need to check your CA service provider for details.For how to setup Windows 2000 CA server, users may refer to http://www.microsoft.com.

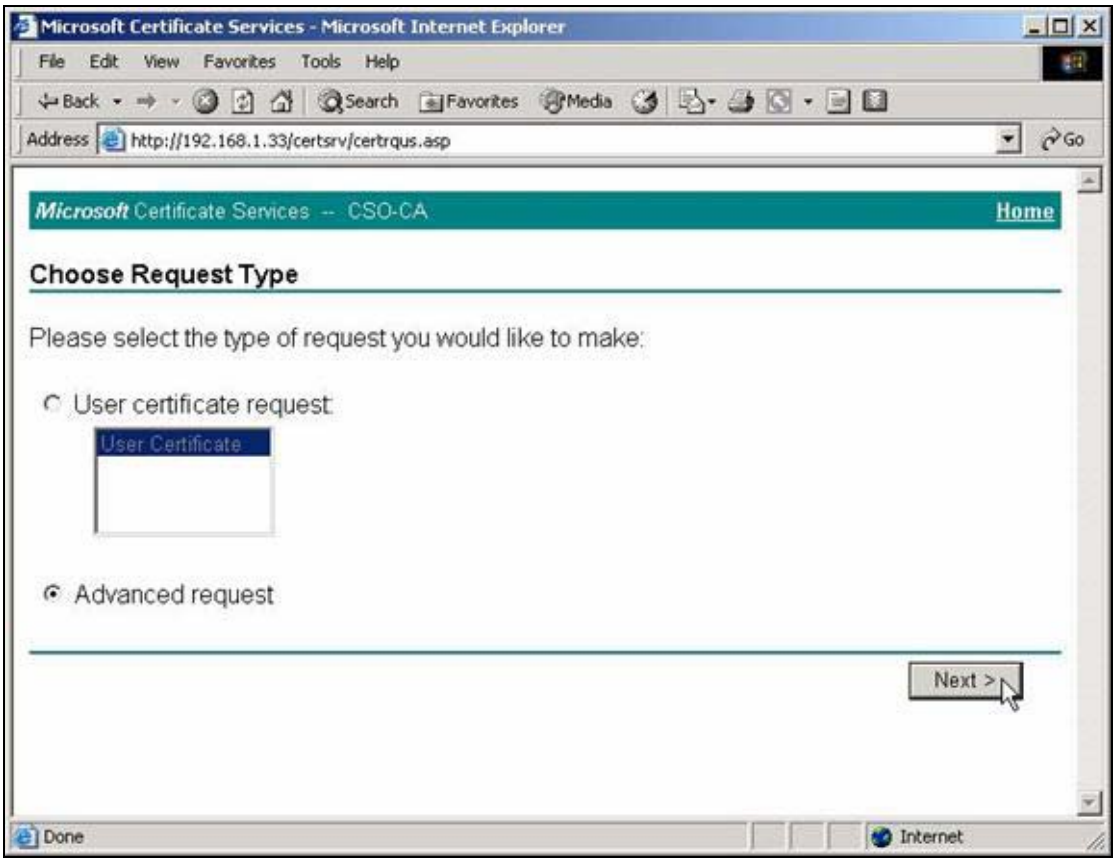
2. Issue the URL to access the CA server, type in User Name/Password/Domain fields.



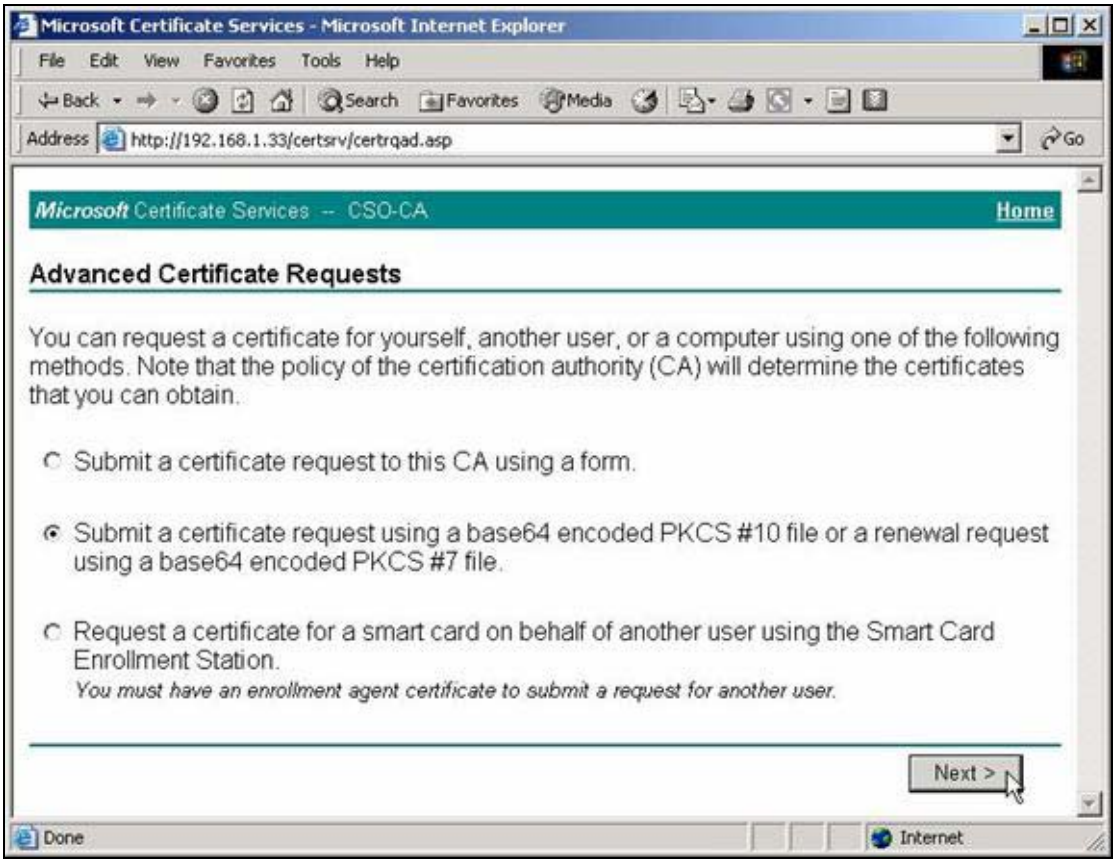
3, Select **Request a Certificate**, then press **Next>** button.



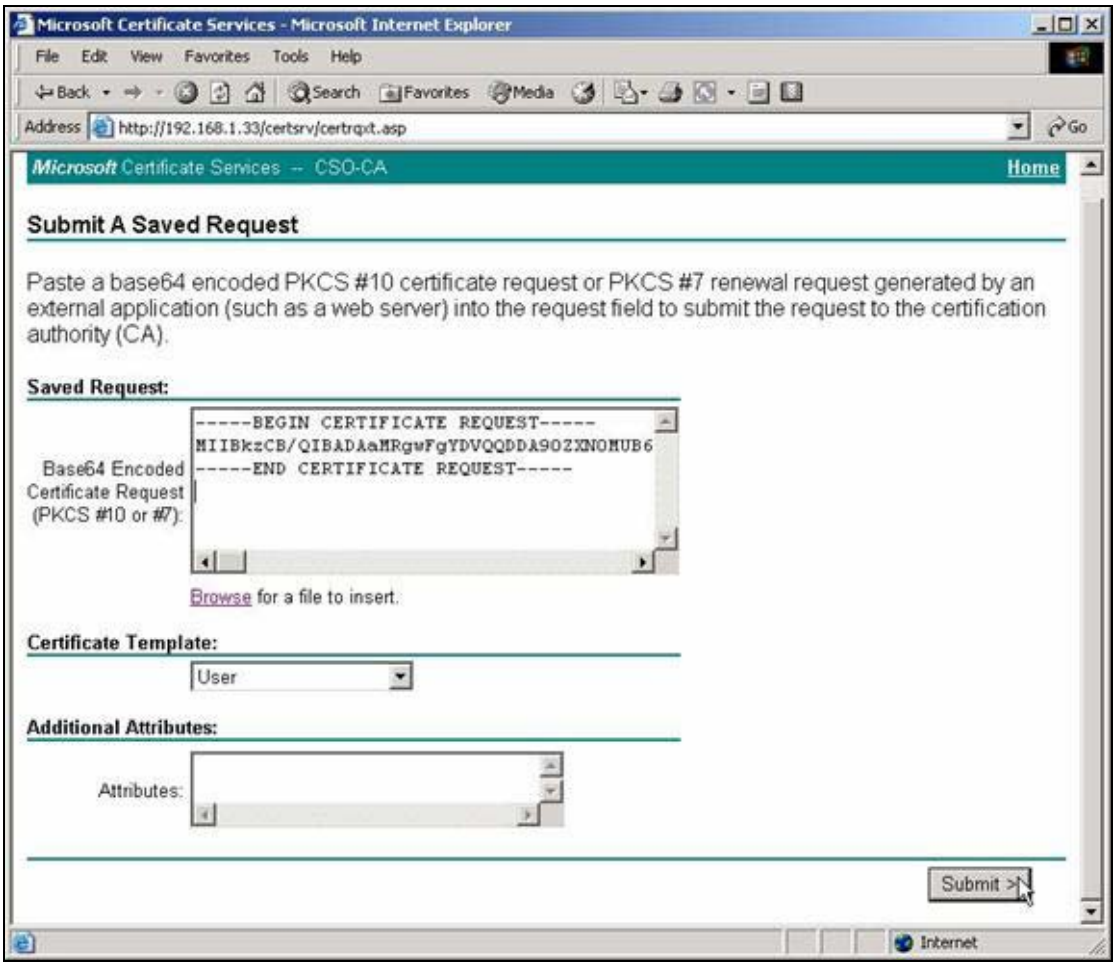
4. Choose **Advanced request**, the press **Next>** button.



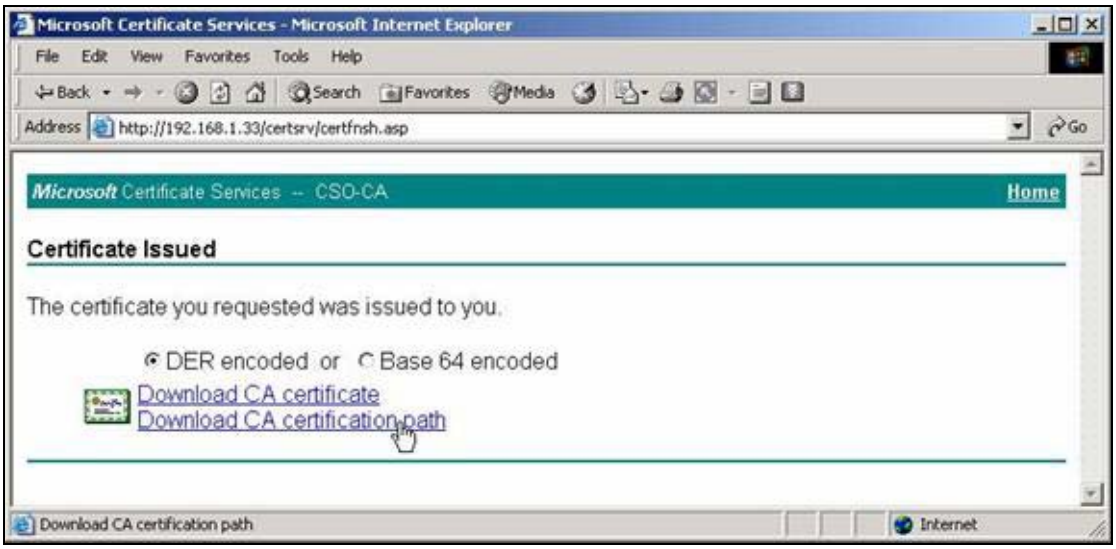
5. Choose "Submit a certificate request using a base64...", then press Next> button.



6. Right click your mouse, then paste the certificate request you get in step 2.1.

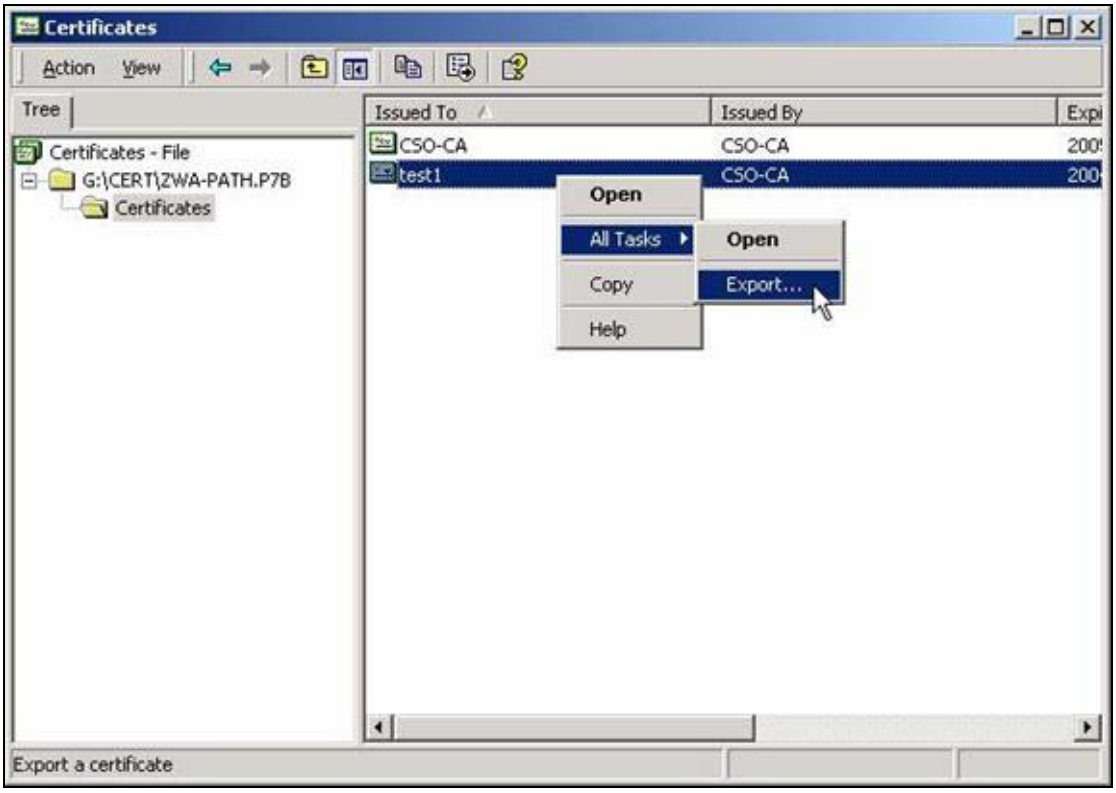


7. Click "Download CA certification path"



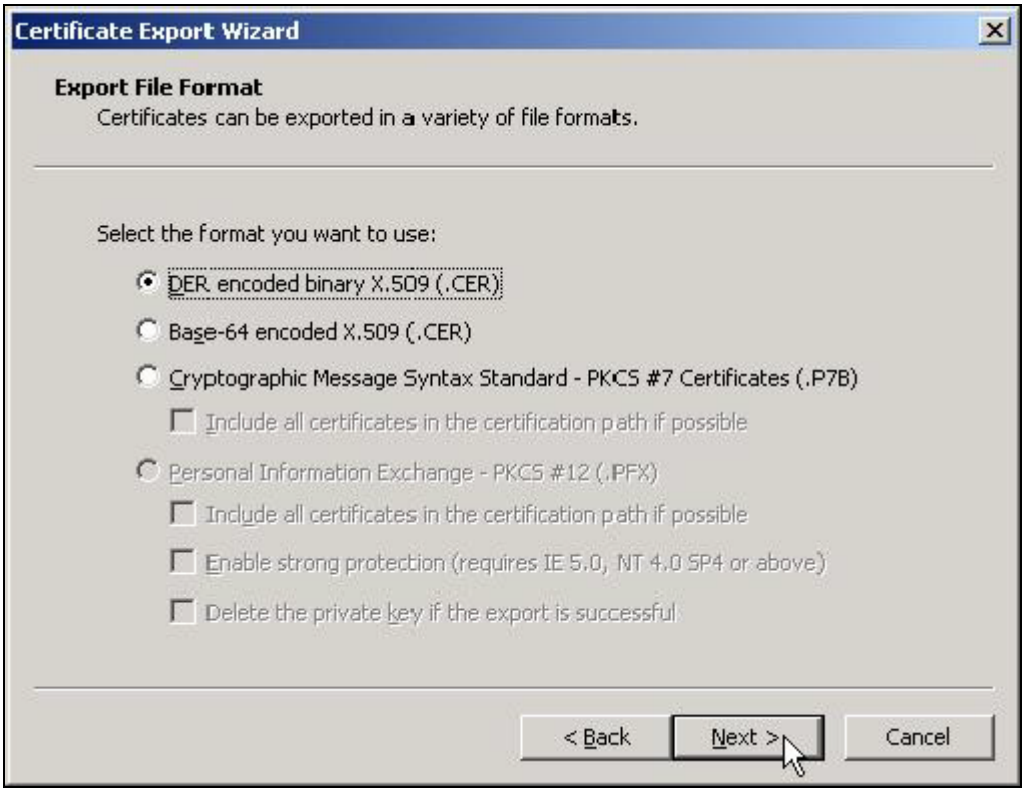
8. A file download would pop out, press Save button, and choose the local folder you would like to store the certification path.

9. Double click the saved file, Select **Certificates**, right click the Certificate, choose **All Tasks-> Export...**

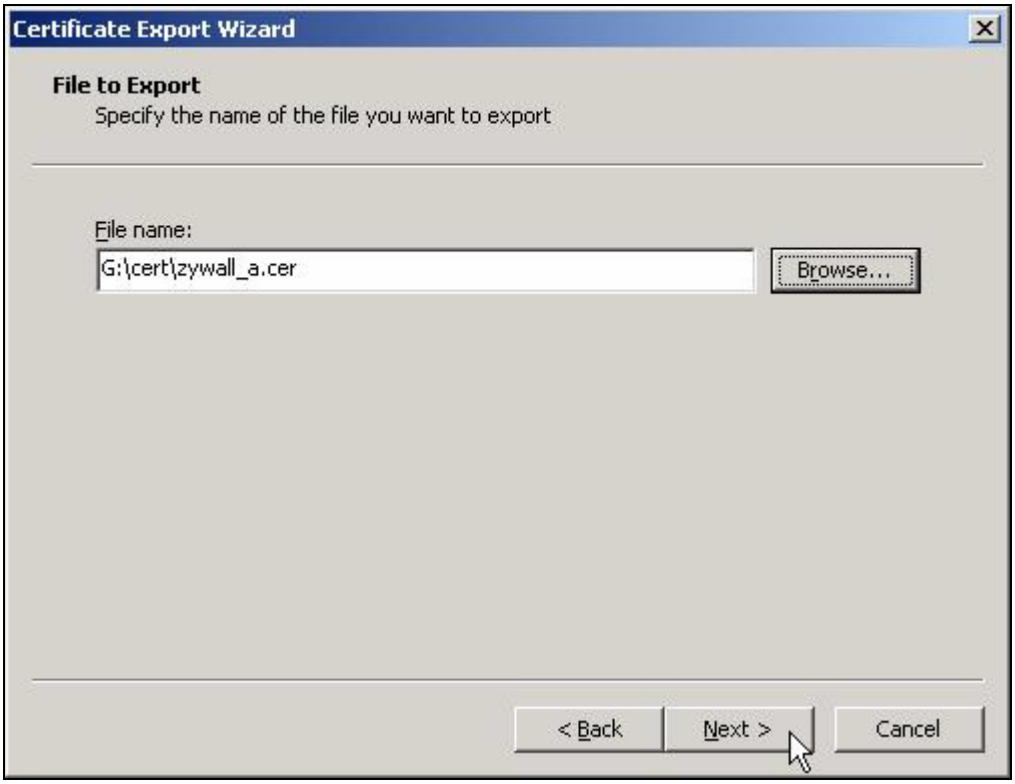


10. Certificate Export Wizard would be popped up, then press **Next>**.

11. Choose DER encoded binary X.509(.CER), then press Nxet>,



12. Specify the path to store your exported Certificate.

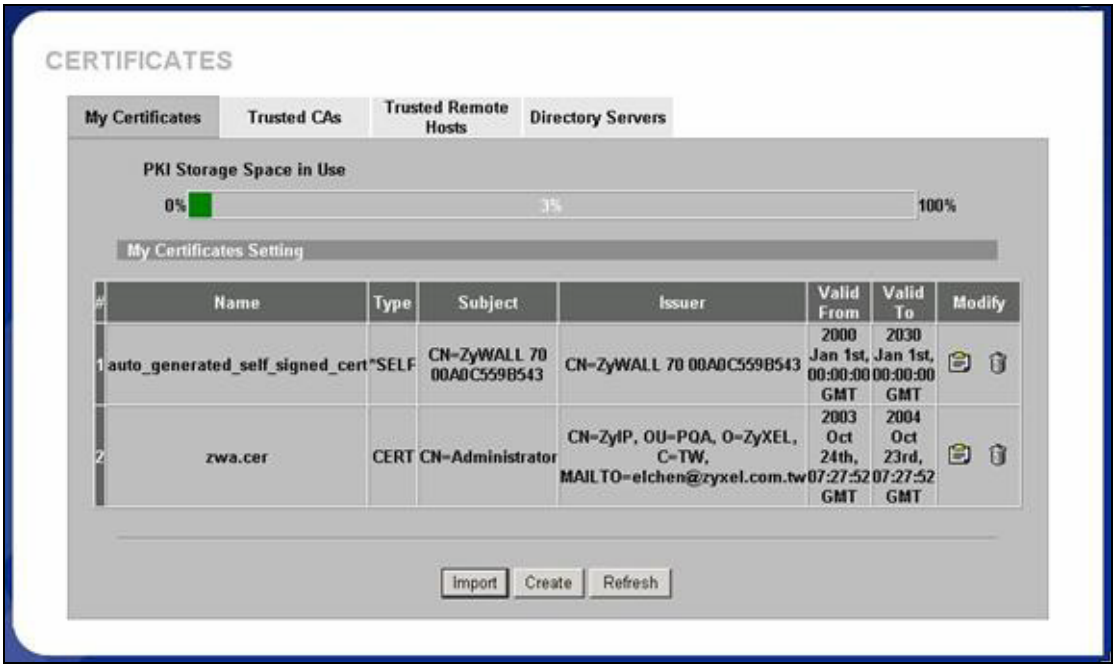


13. Click **Finish**.

14. Go to ZyWALL WEB GUI -> VPN -> My Certificates -> click **Import** button.

15. Click **Browse...** button to find the location you stored ZyWALL's certificate then press **Apply** button.

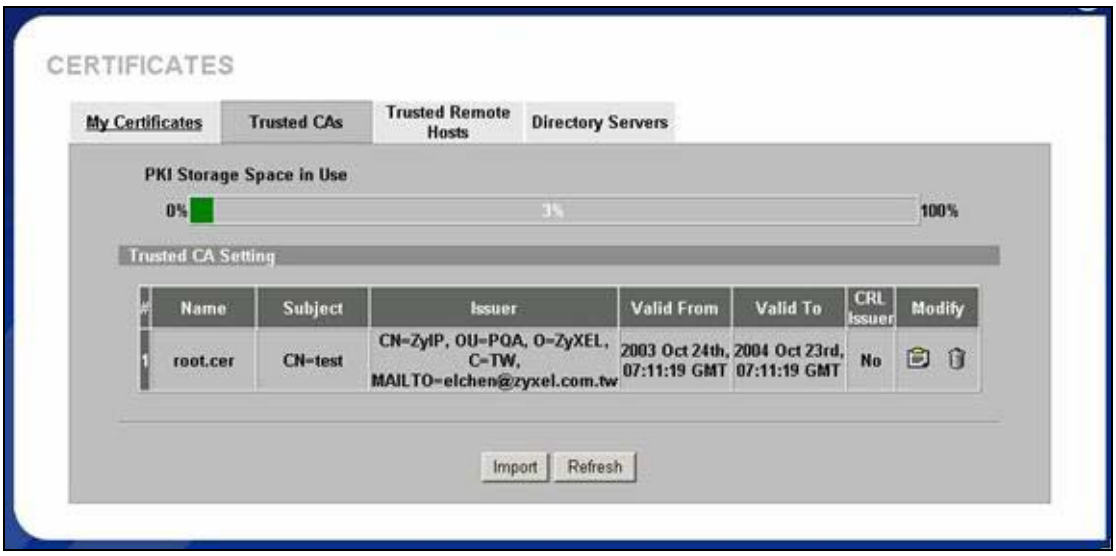
16. After a while, if you see the gray entry turns to a black one, then it means the import of ZyWALL's certificate is successful.



17. Repeat the same procedure from 9 to 13, to export CA's certificate. Note that you may get more than one CA server's certificate, it's not necessary to export all of the CA server's certificates, you can double click ZyWALL's certificate, such as zywall_a.cert.cert in this example, and select Certification Path to view the nearest CA server's name, and then - export that CA server's certificate.

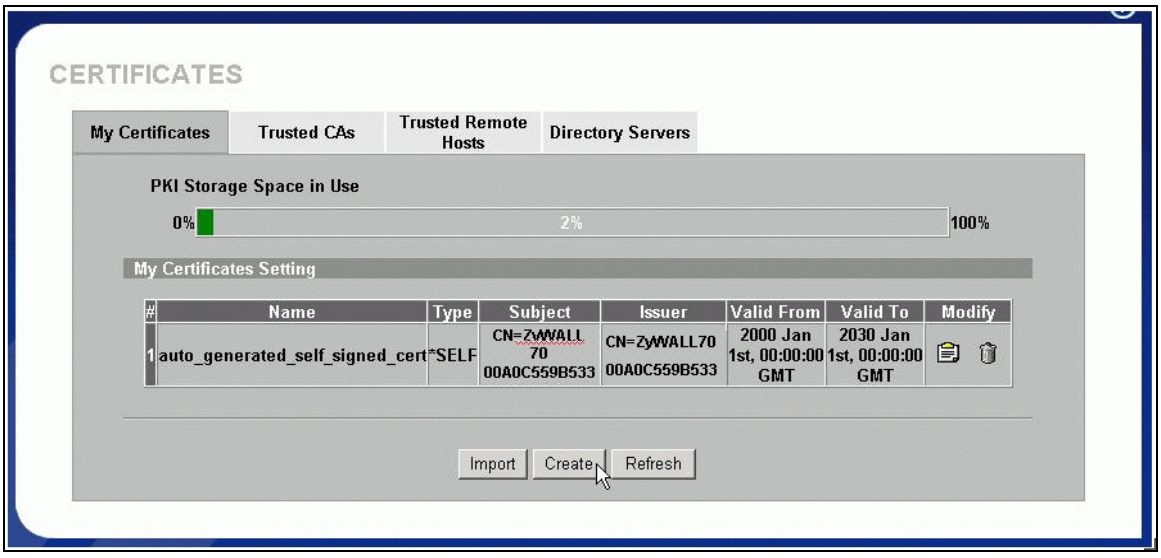
Import the saved CA server's certificate. Click Browse... button, and then select the location.

After import CA's certificate, you will get this display.



Step 3. Create Certificate Request on ZyWALL_B

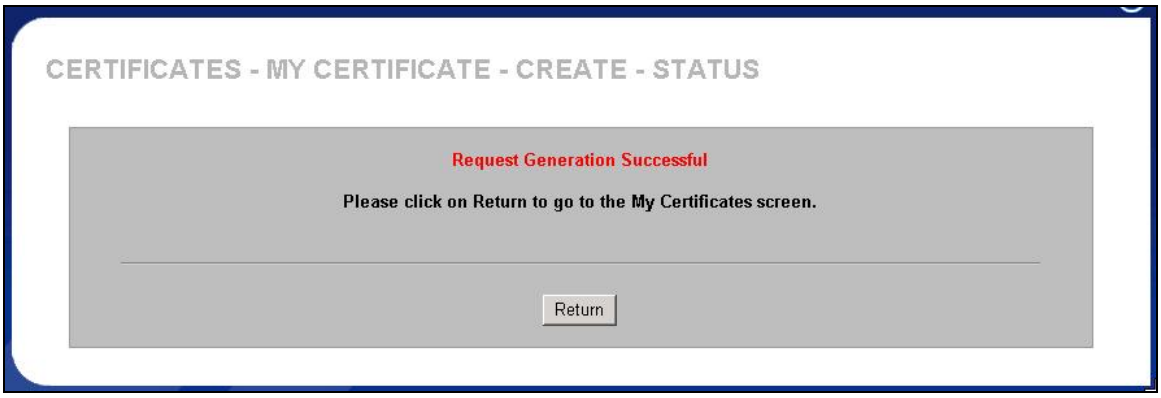
1. Go to **VPN->My Certificates** -> Click **Create** button.



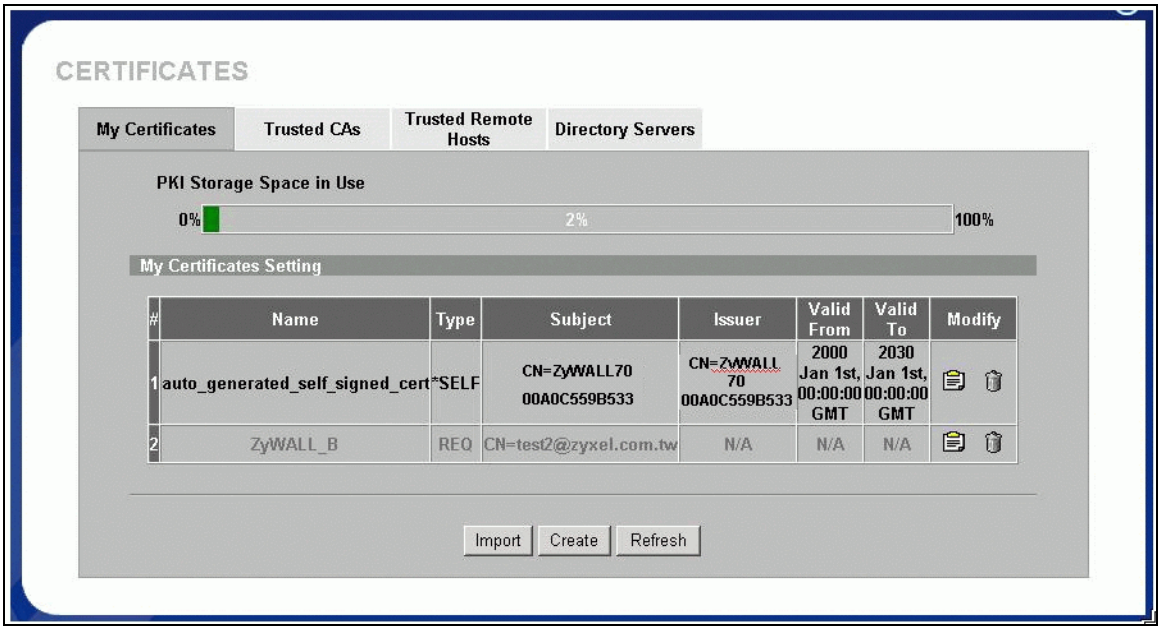
2. Input a name, for this Certificate so you can identify this Certificate later. In Subject Information, give this certificate a Common Name by either Host IP Address, Host Domain Name or E-Mail address. Organizational Unit, Organization, Country are optional fields, you are free to either enter them or not. Finally, specify the key length and select Create a certification request and save it locally for later manual enrollment.

3. Wait for 1-2 minutes until "**Request Generation Successful**" displays. During this period, ZyWALL is working on creation of private, public key pair, and certificate request.

4. After creating certificate request, ZyWALL would return Successful Message.

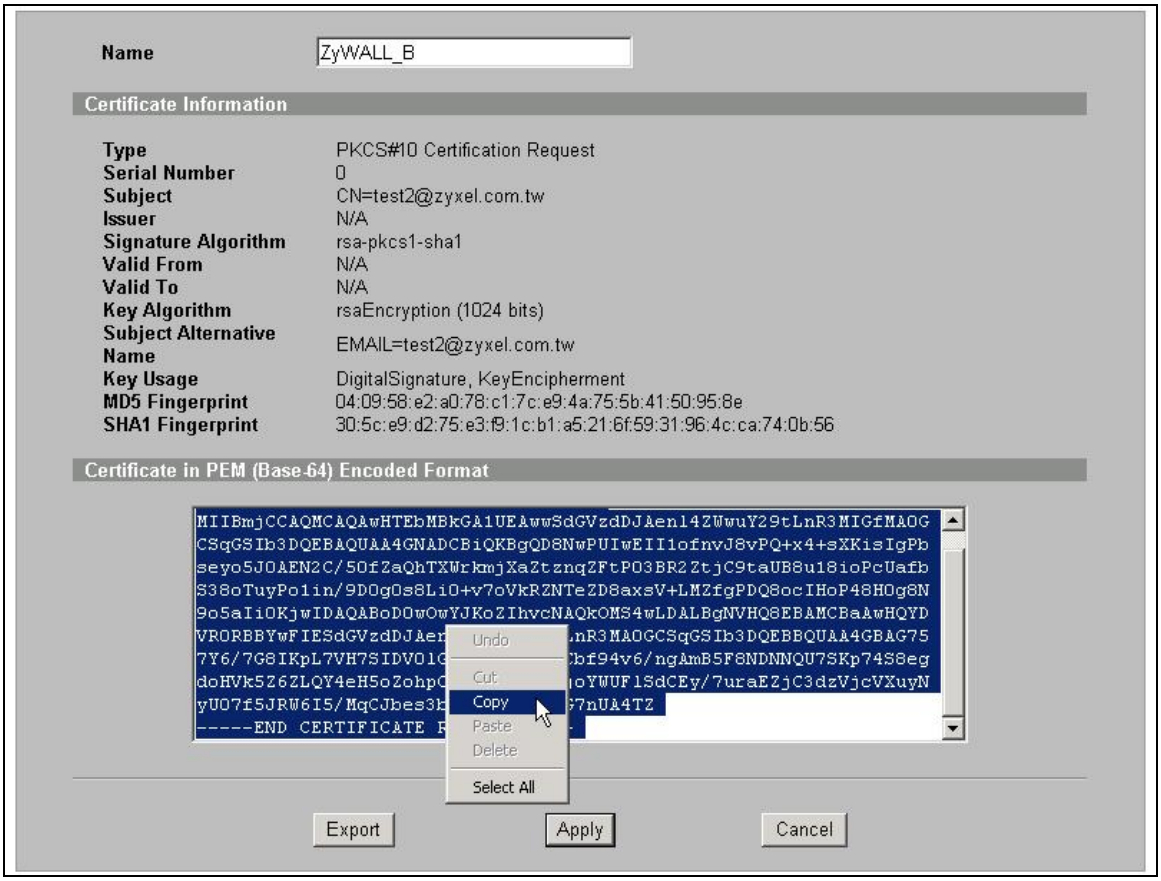


5. In **My Certificates** tab, you can get a new entry in grey color. This is the **Certificate Request** you just created. Click **Details** to export the request.



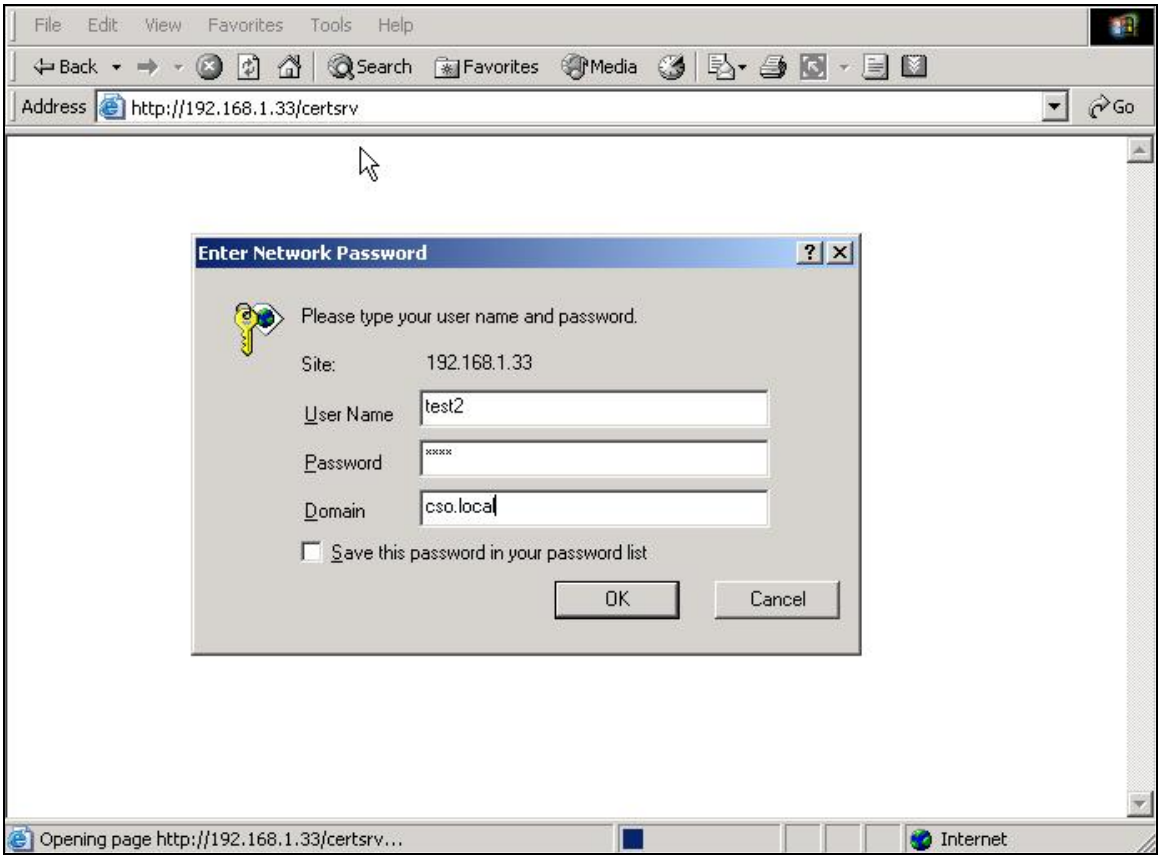
Step 4. Enroll Certificate Request on ZyWALLB

1. Copy the content of Certificate in PEM Encoded Format, by selecting all of the content, then right click your mouse, and select **Copy**. Keep your copy in clipboard for later paste.

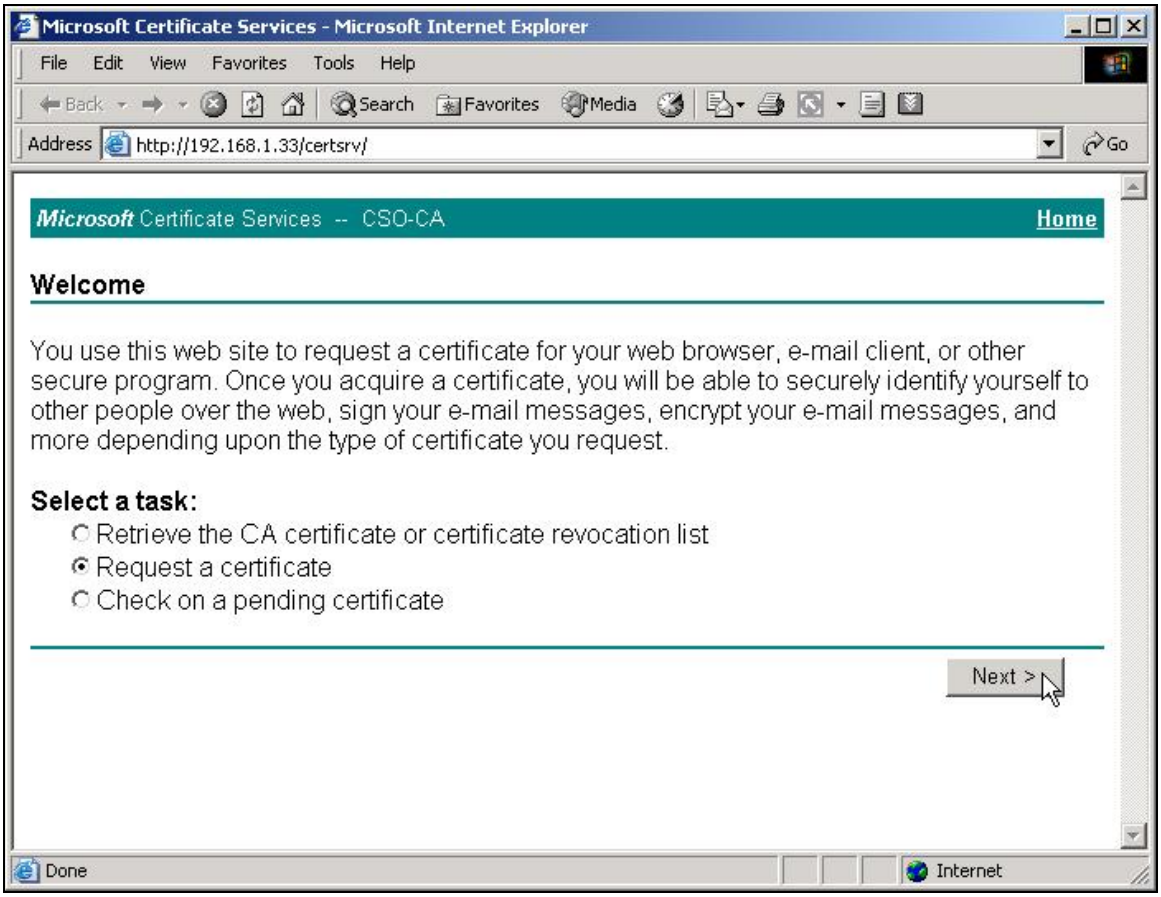


In this support note, we utilize certificate enrollment service from **Microsoft Windows 2000 CA server**. The enrollment procedure of your CA server may be different, you may need to check your CA service provider for details.For how to setup Windows 2000 CA server, users may refer to http://www.microsoft.com.

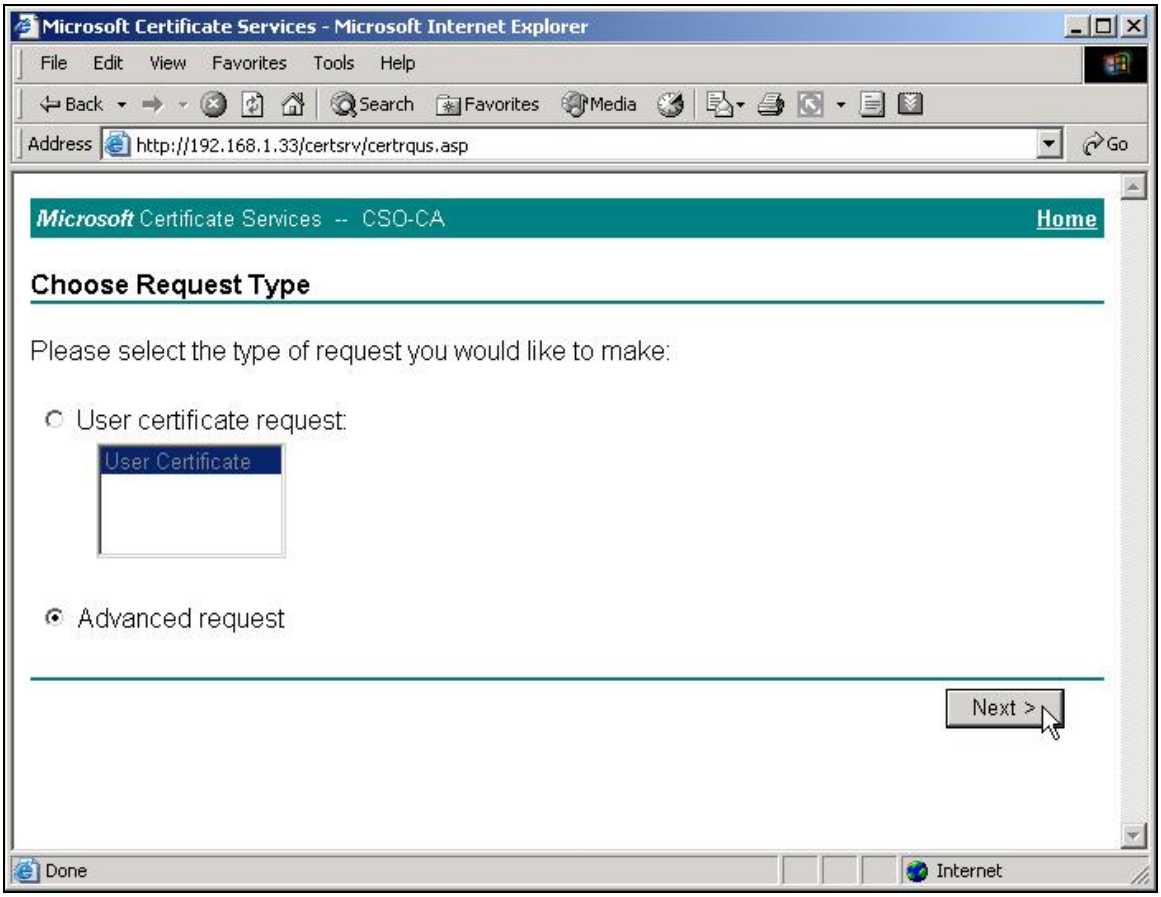
2. Issue the URL to access the CA server, type in User Name/Password/Domain fields.



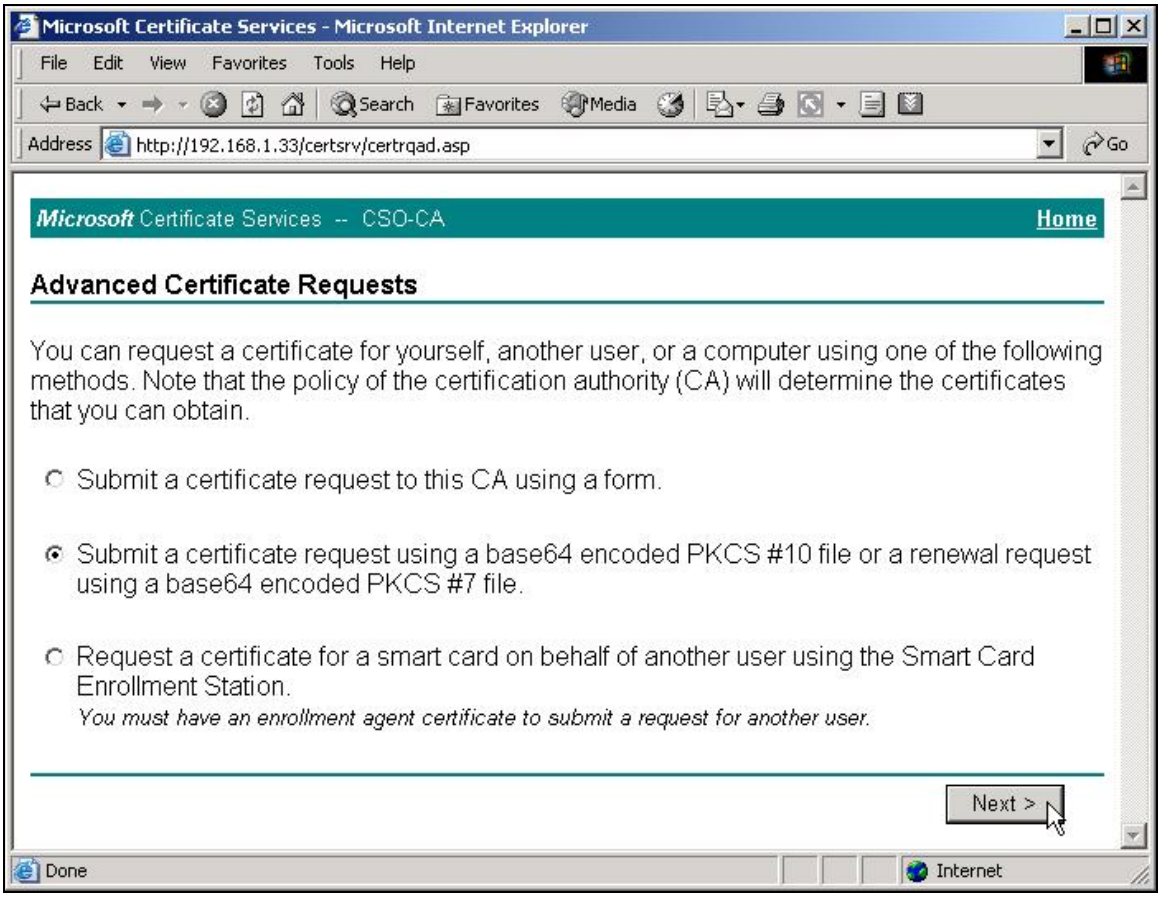
3, Select **Request a Certificate**, then press **Next>** button.



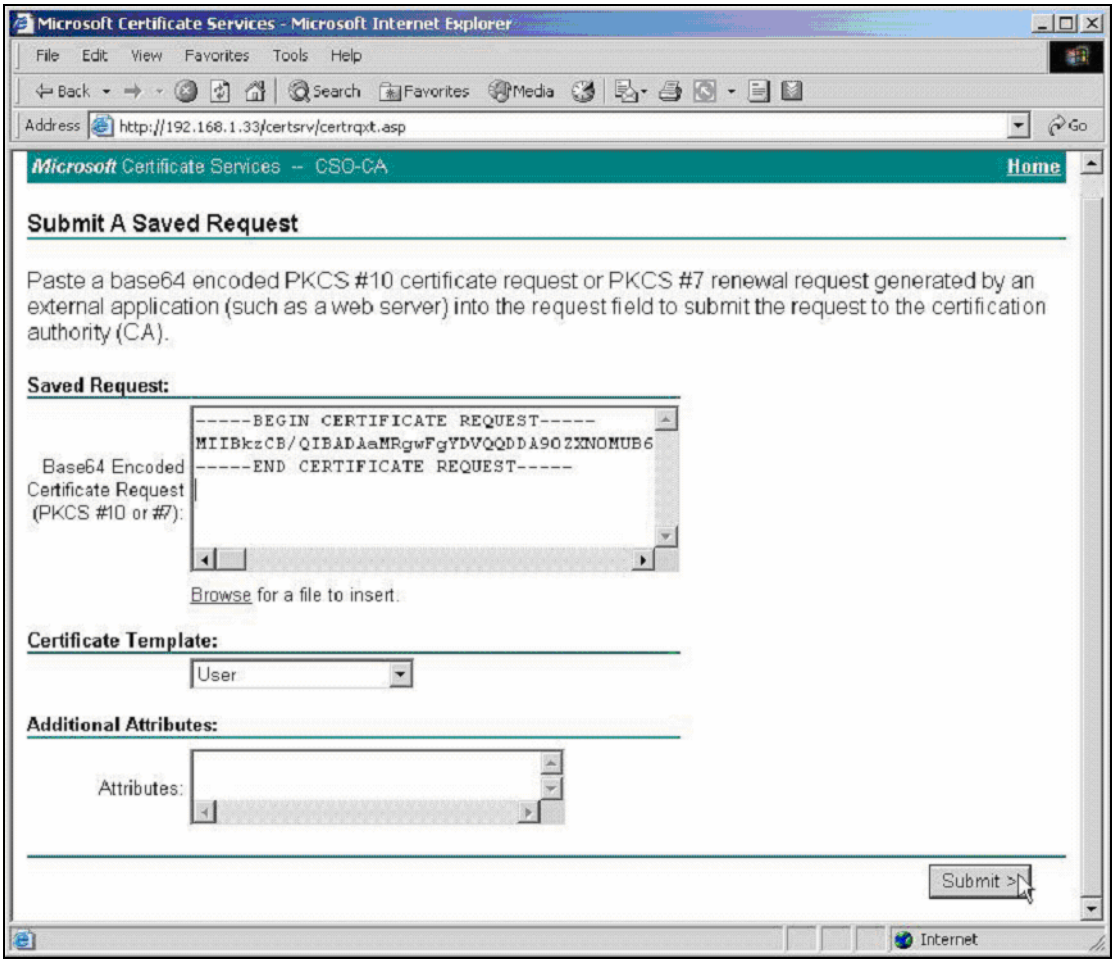
4. Choose **Advanced request**, the press **Next>** button.



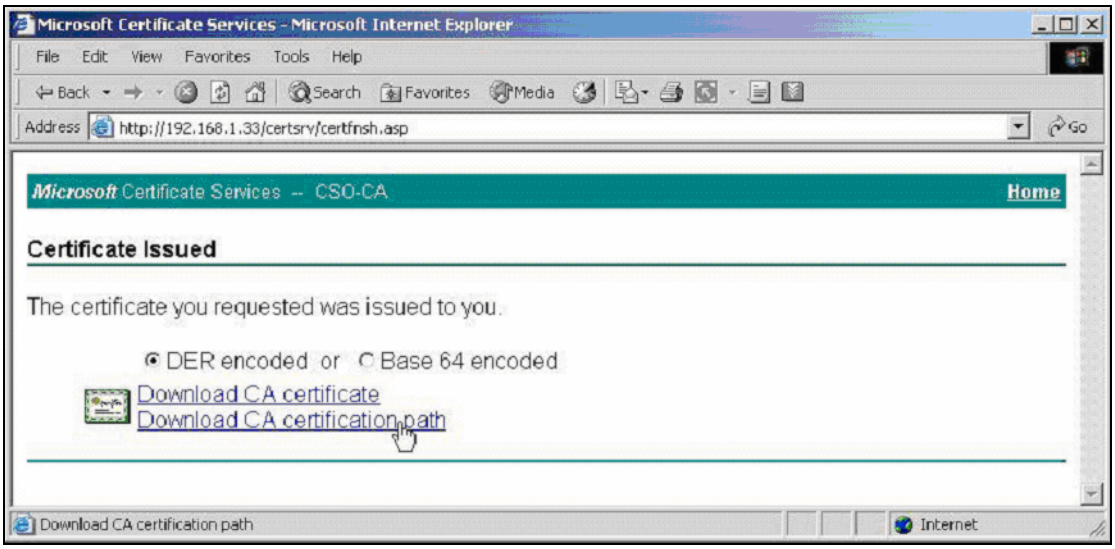
5. Choose "Submit a certificate request using a base64...", then press Next> button.



6. Right click your mouse, then paste the certificate request you get in step 4.1.

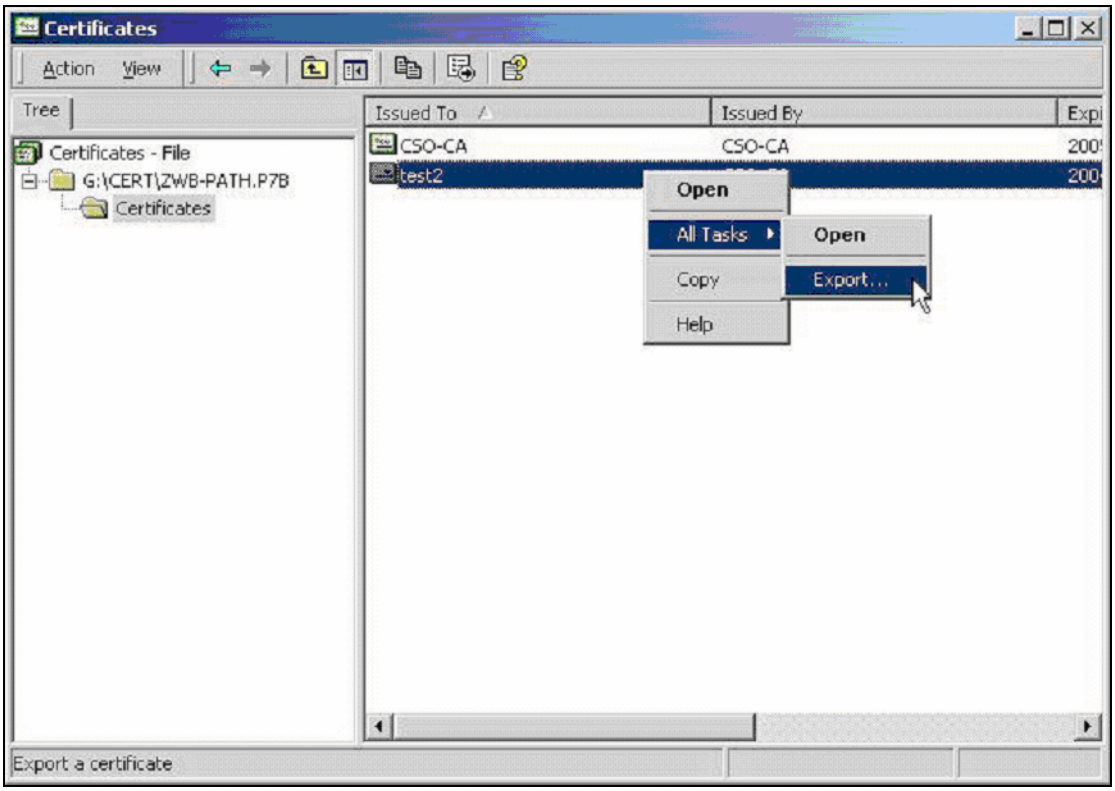


7. Click "Download CA certification path"



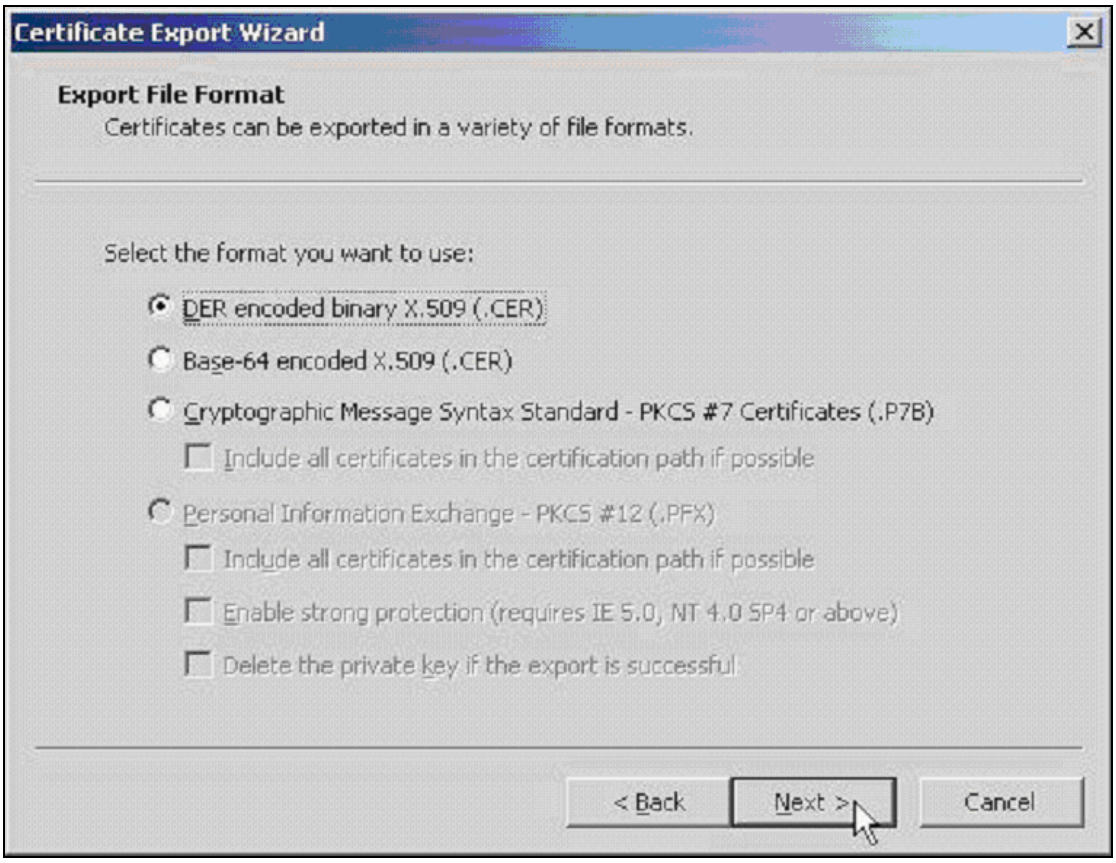
8. A file download would pop out, press Save button, and choose the local folder you would like to store the certification path.

9. Double click the saved file, Select **Certificates**, right click the Certificate, choose **All Tasks-> Export...**

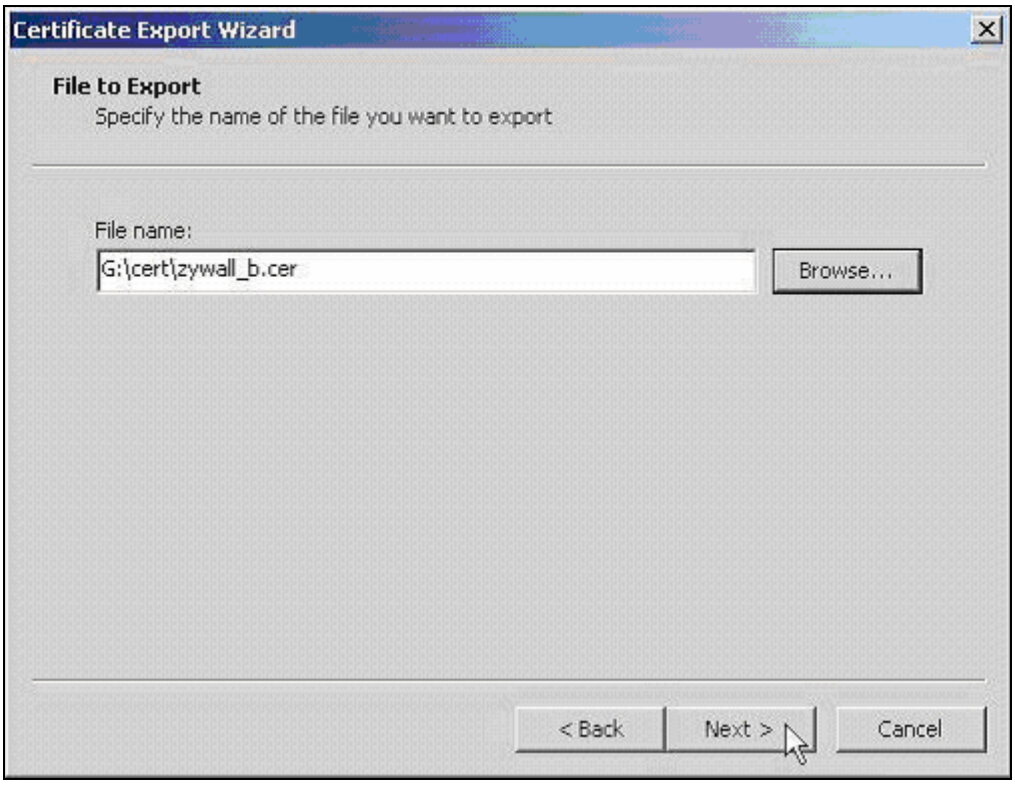


10. Certificate Export Wizard would be popped up, then press **Next>**.

11. Choose **DER encoded binary X.509(.CER)**, then press **Nxet>**,

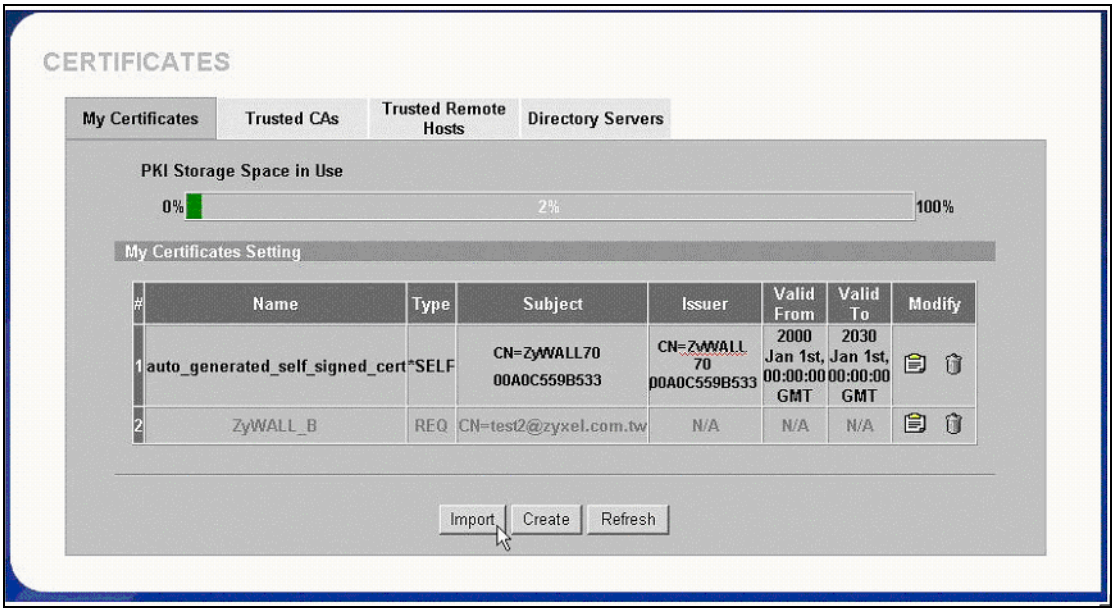


12. Specify the path to store your exported Certificate.

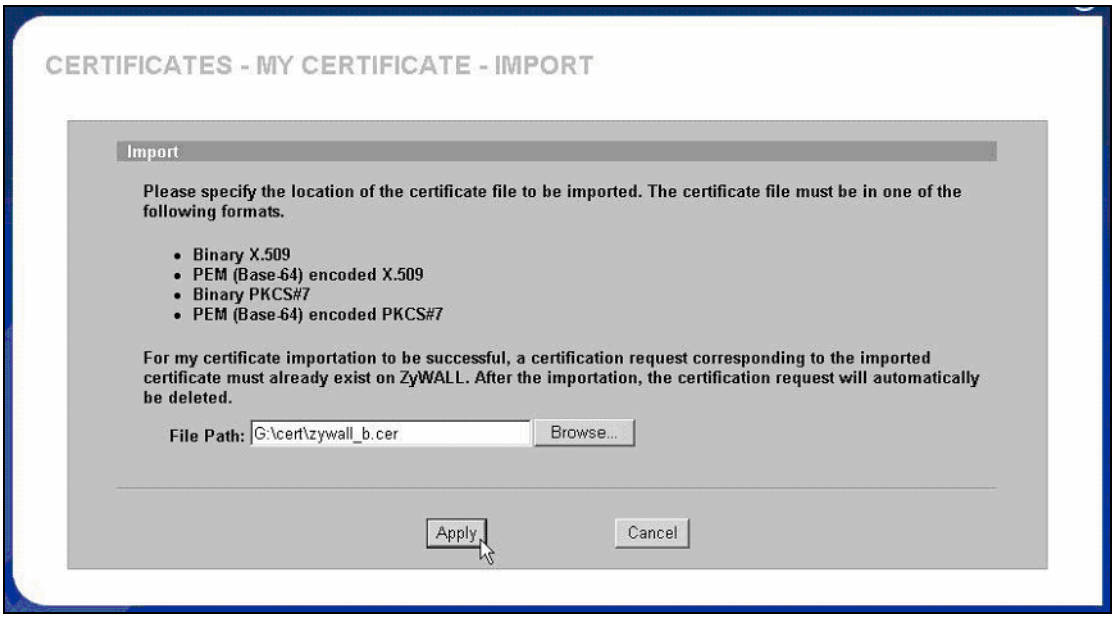


13. Click **Finish**.

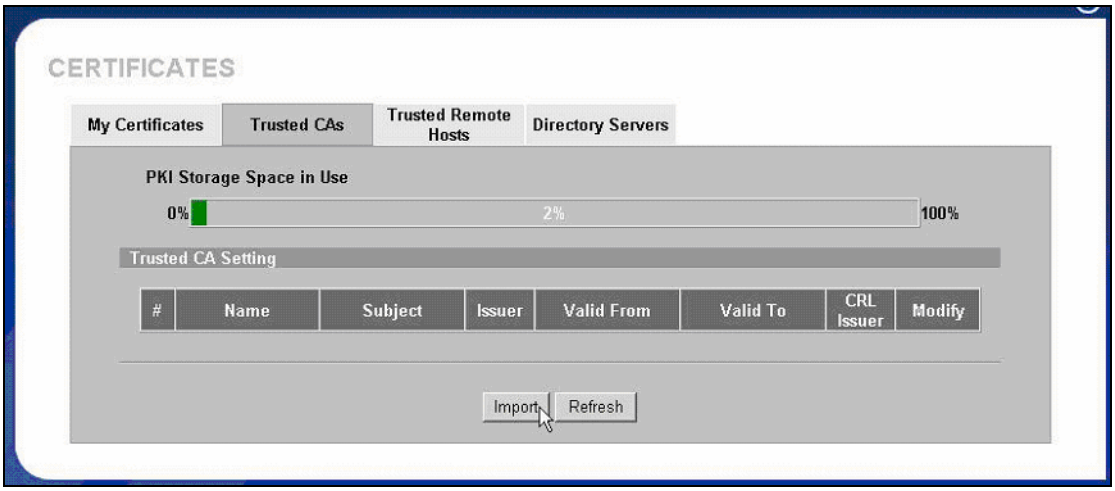
14. Go to ZyWALL WEB GUI -> VPN -> My Certificates -> click **Import** button.



15. Click **Browse...** button to find the location you stored ZyWALL's certificate then press **Apply** button.

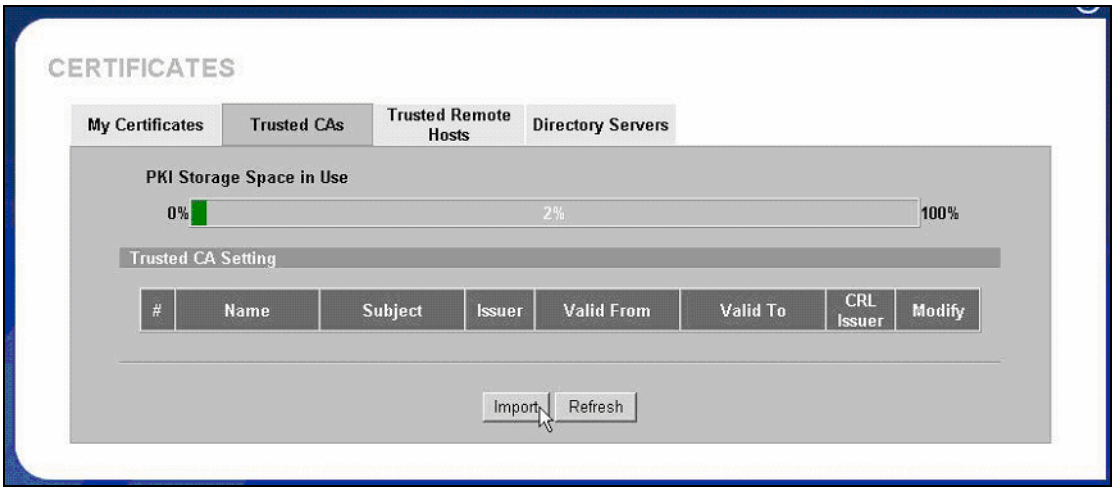


16. After a while, if you see the gray entry turns to a black one, then it means the import of ZyWALL's certificate is successful.

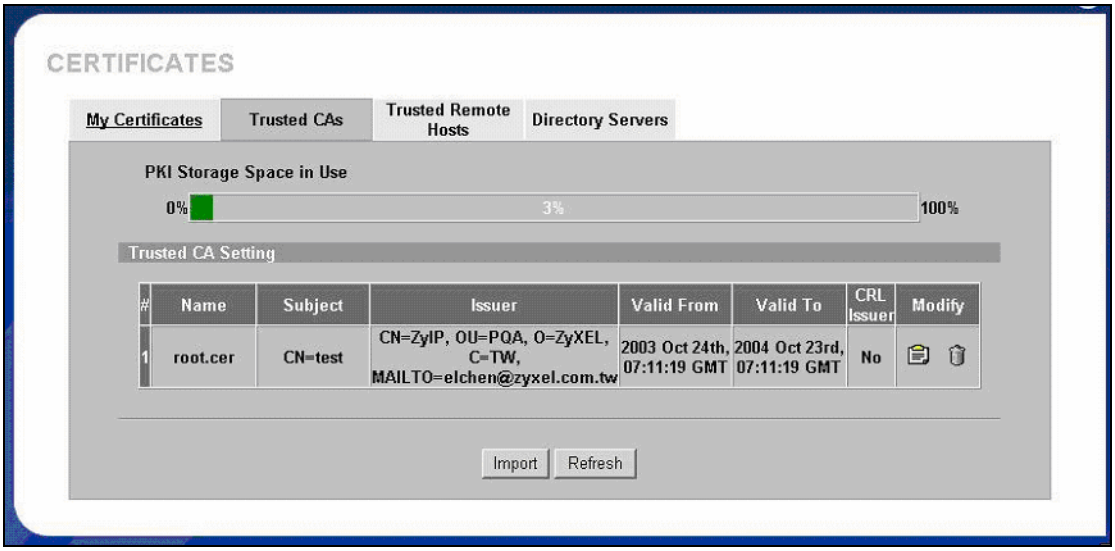


17. Repeat the same procedure from 9 to 13, to export CA's certificate. Note that you may get more than one CA server's certificate, it's not necessary to export all of the CA server's certificates, you can double click ZyWALL's certificate, such as zywall_a.cert.cert in this example, and select **Certification Path** to view the nearest CA server's name, and then - export that CA server's certificate.

Import the saved CA server's certificate. Click **Browse...** button, and then select the location.



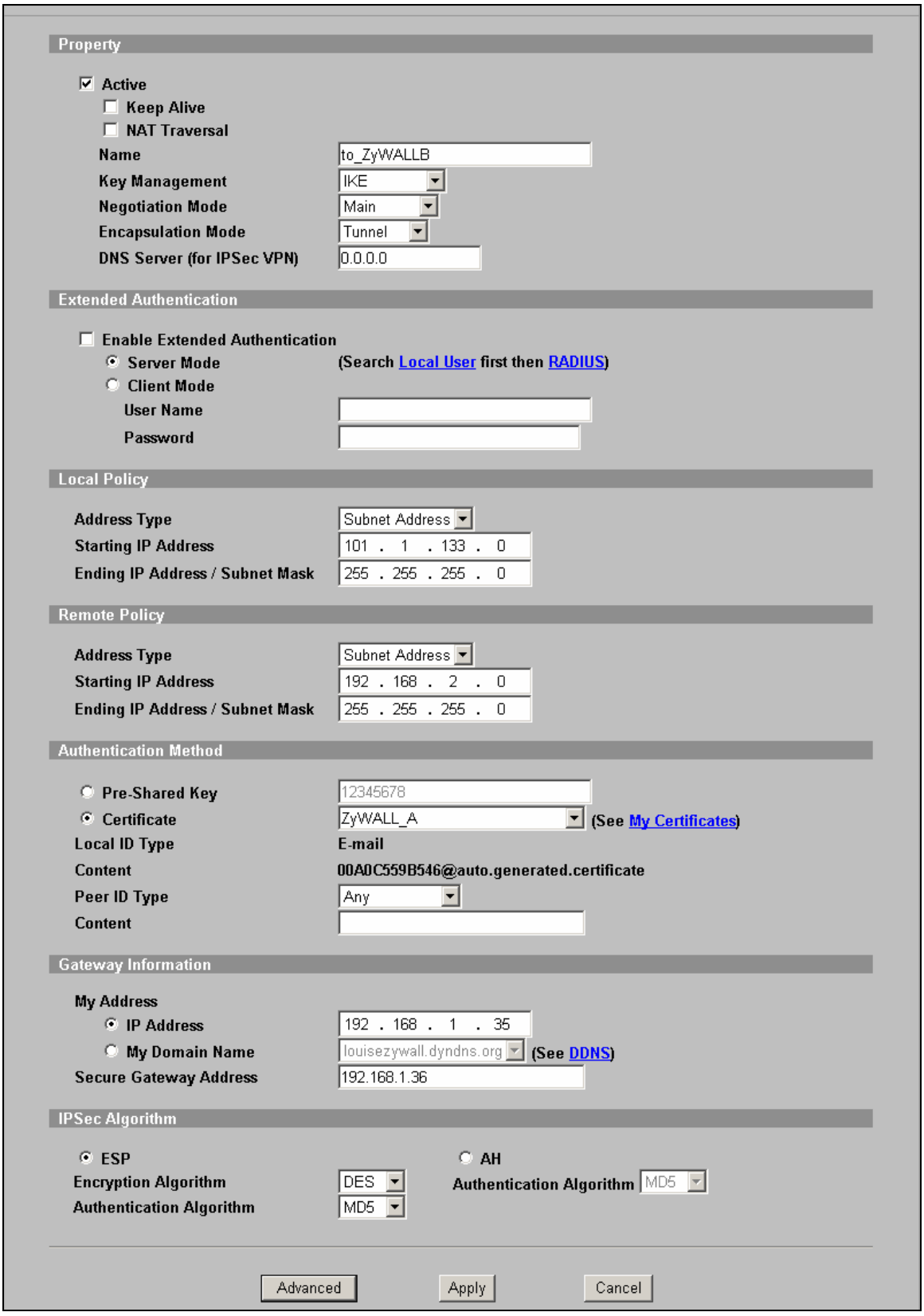
18. After import CA's certificate, you will get this display.



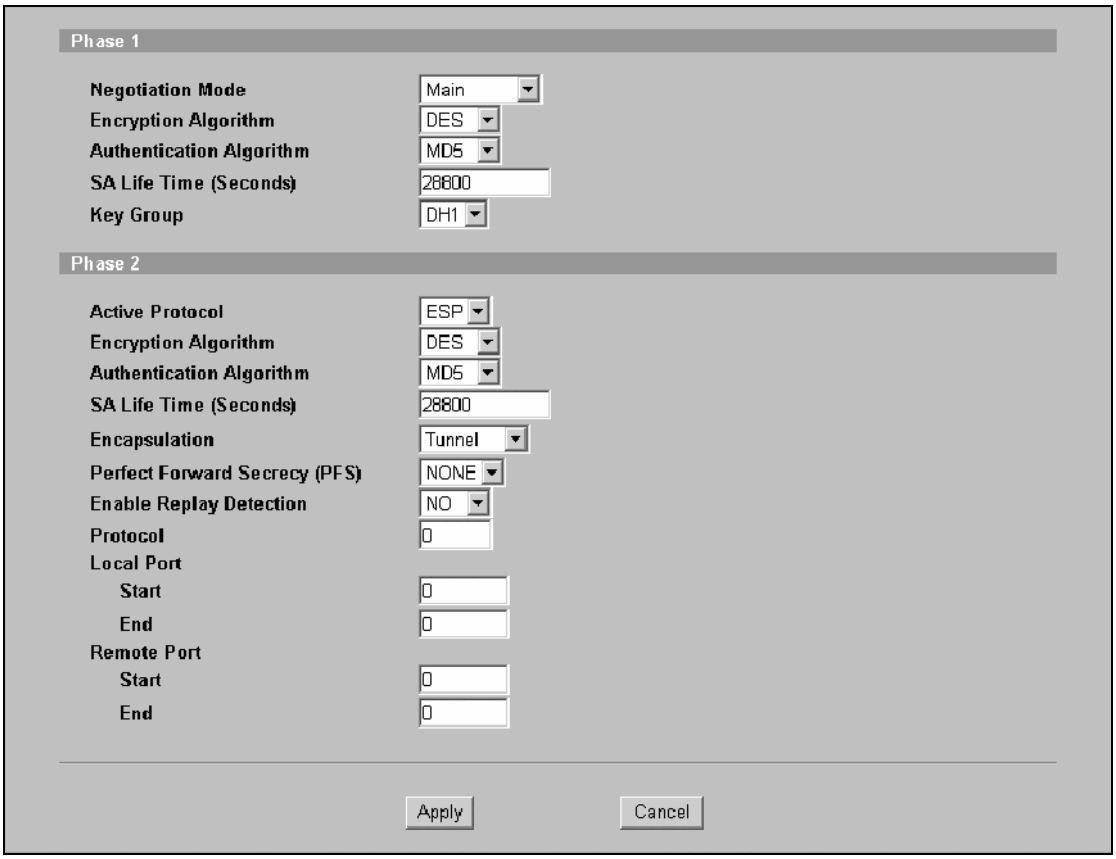
Step 5. Using Certificate in VPN on ZyWALL A

1. Activate the rule
2. Give this VPN rule a name "toZyWALL_B"
3. Select Key Management to "IKE"
4. Select Negotiation Mode to "Main"
5. Edit Local: Address Type="Subnet Address", Starting IP Address="10.1.33.0", End IP Address/Subnet Mask="255.255.255.0"
6. Edit Remote: Address Type="Subnet Address", Starting IP Address="192.168.2.0", End IP Address/Subnet Mask="255.255.255.0"
7. Authentication Key, Select Certificate, and choose certificate you enrolled for this device from drop down list.
8. Fill in My IP address= "192.168.1.35"

9. Peer ID type= "ANY".
10. Secure Gateway Address= "192.168.1.36"
11. Encapsulation Mode="Tunnel"
12. Leave other options as default.

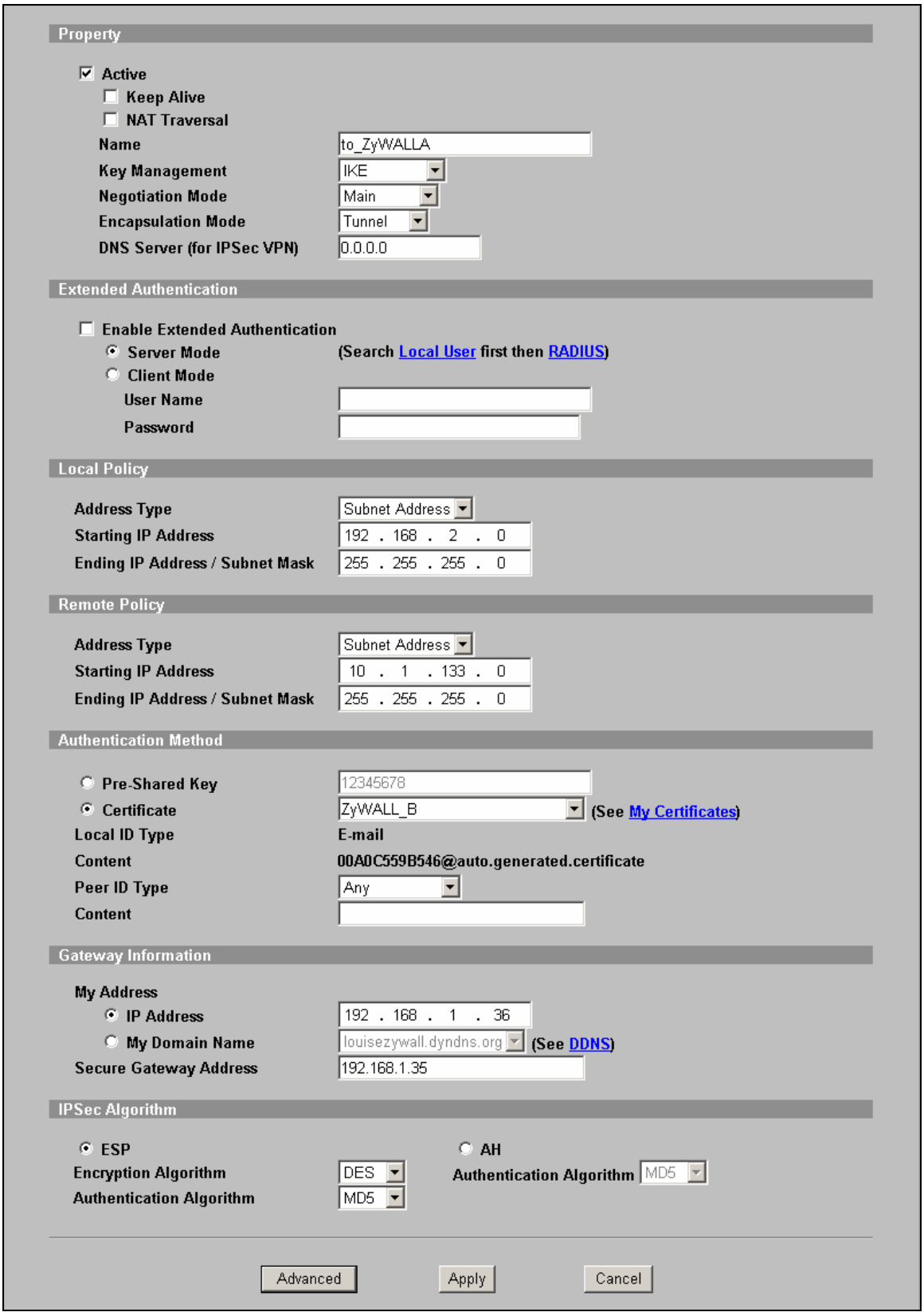


13. You can check detailed settings by clicking Advanced button.

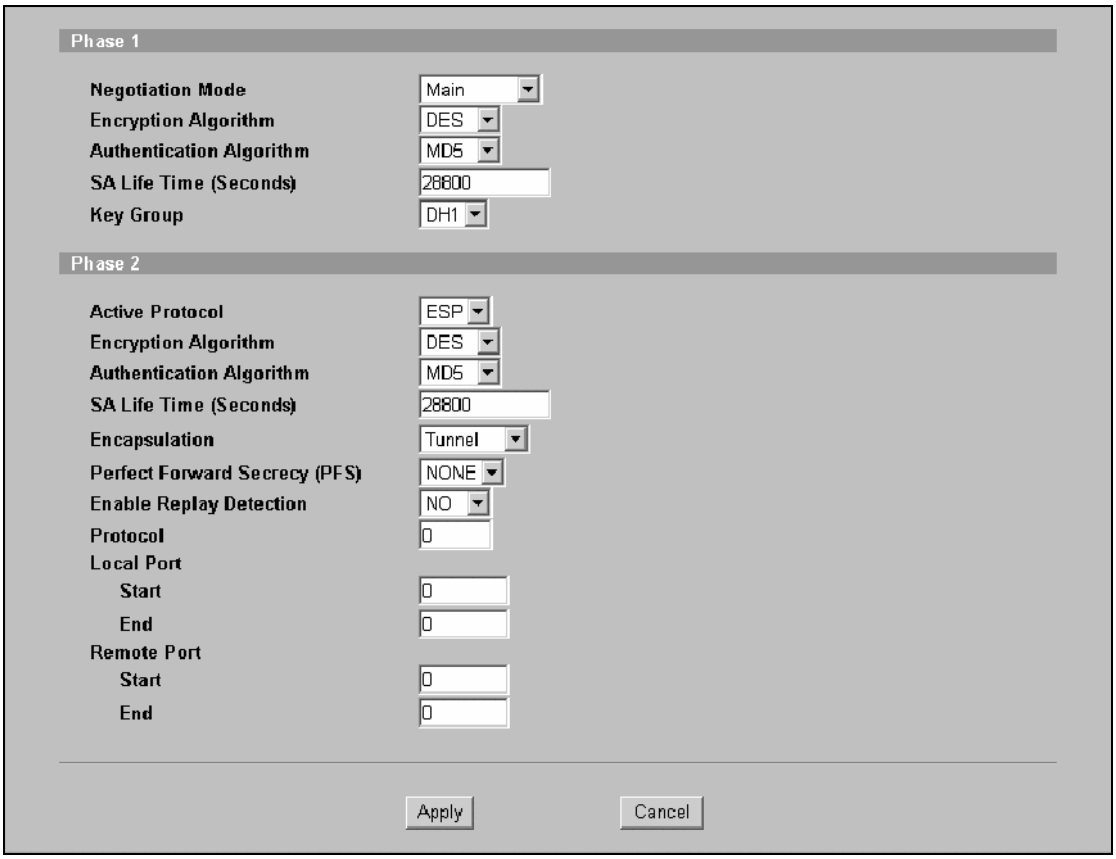


Step 6. Using Certificate in VPNon ZyWALL B

1. Activate the rule
2. Give this VPN rule a name "toZyWALL_A"
3. Select Key Management to "IKE"
4. Select Negotiation Mode to "Main"
5. Edit Local: Address Type="Subnet Address", Starting IP Address="192.168.2.0", End IP Address/Subnet Mask="255.255.255.0"
6. Edit Remote: Address Type="Subnet Address", Starting IP Address="10.1.33.0", End IP Address/Subnet Mask="255.255.255.0"
7. Authentication Key, Select Certificate, and choose certificate you enrolled for this device from drop down list.
8. Fill in My IP address= "192.168.1.36"
9. Peer ID type= "ANY".
10. Secure Gateway Address= "192.168.1.35"
11. Encapsulation Mode="Tunnel"
12. Leave other options as default.



13. You can check detailed settings by clicking Advanced button.



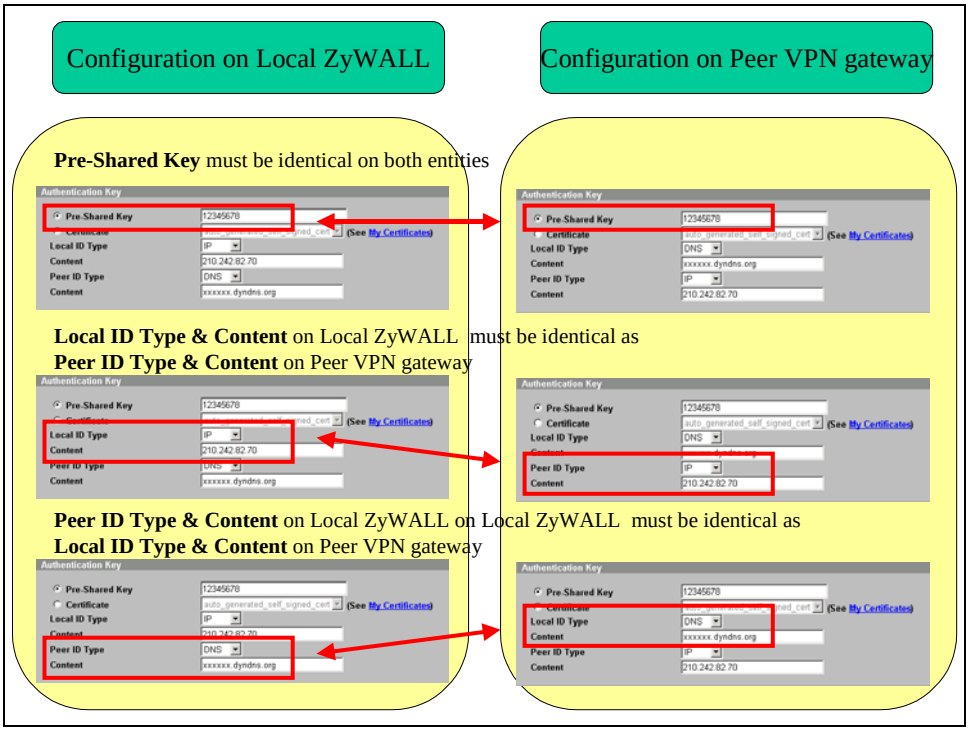
Using Pre-Shared Key for Device Authentication

The IKE protocol also provides primary authentication - verifying the identity of the remote system before negotiating the encryption algorithm and keys. Two kinds of authentication methods are supported on ZyWALL: pre-shared key & certificate.

If pre-shared key is used, a shared, symmetric key must be manually exchanged and configured on the two entities. Three types of identity are available: **IP, DNS** and **E-mail**.

Here are some rules to follow in Authentication Key:

3) Pre-shared key must be configured identically on both entities
4) The **Local ID Type** & **Content** of Local ZyWALL must be the same as that of **Peer ID Type** & **Content** of peer VPN gateway.
5) When IP is selected as ID Type, the **Content** must be in the format of X.X.X.X (e.g. 210.242.82.70)
6) When DNS/E-mail are selected as ID Type, the same string must be configured on both entities.



Note:

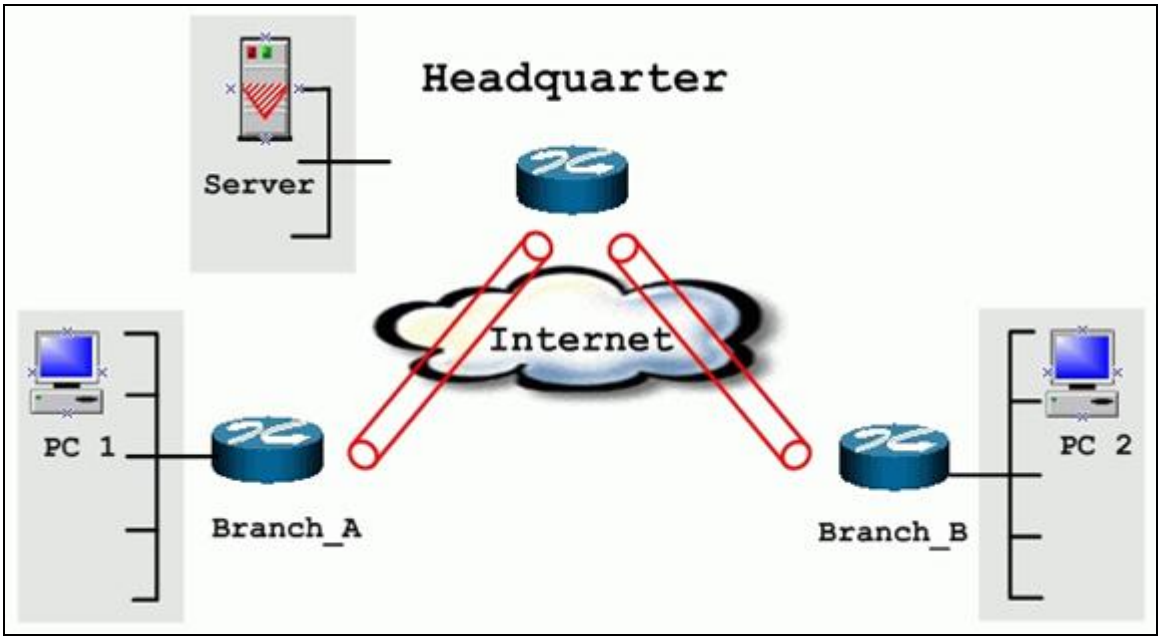
1) If "**ID Type**" is mis-configured on Local/Remote IPSec Gateway, the ZyWALL will show [NOTFY:**ERR_ID_INFO**] error message in related IKE log.
2) If "**Pre-shared Key**" or ID "**Content**" are mis-configured on Local/Remote IPSec Gateway, ZyWALL will show [NOTFY:ERR_ID_INFO] error message in related IKE log.

Using VPN routing between branches

1. Setup VPN in Branch Office A
2. Setup VPN in Branch Office B
3. Setup VPN in Headquarter

This page guides us how to setup VPN routing between branch offices through headquarter. So that whenever branch office A wants to talk to branch office B, headquarter plays as a VPN relay. Users can gain benefit from such application when the scale of branch offices is very large, because no additional VPN tunnels between branch offices are needed.In this support note, we skip the detailed configuration steps for Internet access and presume that you are familiar with basic ZyNOS VPN configuration.

As the figure shown below, each branch office have a VPN tunnel to headquarter, thus PCs in branch offices can access systems in headquarter via the tunnel. Through VPN routing, ZyWALL series now provide you a solution to let PCs in branch offices talk to each other through the existing VPN tunnels concentrated on the headquarter.



The IP addresses we use in this example are as shown below.

Branch_A	Headquarter	Branch_B
WAN:202.3.1.1 LAN:192.168.3.1	WAN:202.1.1.1 LAN:192.168.1.1	WAN:202.2.1.1 LAN:192.168.2.1
LAN of Branch_A	LAN of Headquarter	LAN of Branch_B
192.168.3.0/24	192.168.1.0/24	192.168.2.0/24

1. Setup VPN in branch office A

Because VPN routing enables branch offices to talk to each other via tunnels concentrated on headquarter. In this step, we configure an IPSec rule in ZyWALL (Branch_A) for PCs behind branch office A to access both LAN segments of headquarter and branch office B. Because the LAN segments of headquarter and branch office B are continuous, we merge them into one single rule by including these two segments in **Remote** section. If by any chance, the two segments are not continuous, we strongly recommend you to setup different rules for these segments.

1. Go to SECURITY->VPN->Press Add button

2. check **Active** check box and give a name to this policy.

3. Give this VPN rule a name, **Branch_A**.

4. Select **Key Management** to **IKE** and **Negotiation Mode** to **Main**.

5. In **Local** section, select **Address Type** to **Range Address**, set **IP Address Start** to **192.168.3.0**, and **End** to **192.168.3.255**. This section covers the LAN segment of branch office A.

6. In **Remote** section, select **Address Type** to **Range Address**, set **IP Address Start** to **192.168.1.0** and **End** to **192.168.2.255**. This section covers the LAN segment of both headquarter and branch office B.

7. **My IP Addr** is the **WAN IP of this ZyWALL**, **202.3.1.1**.

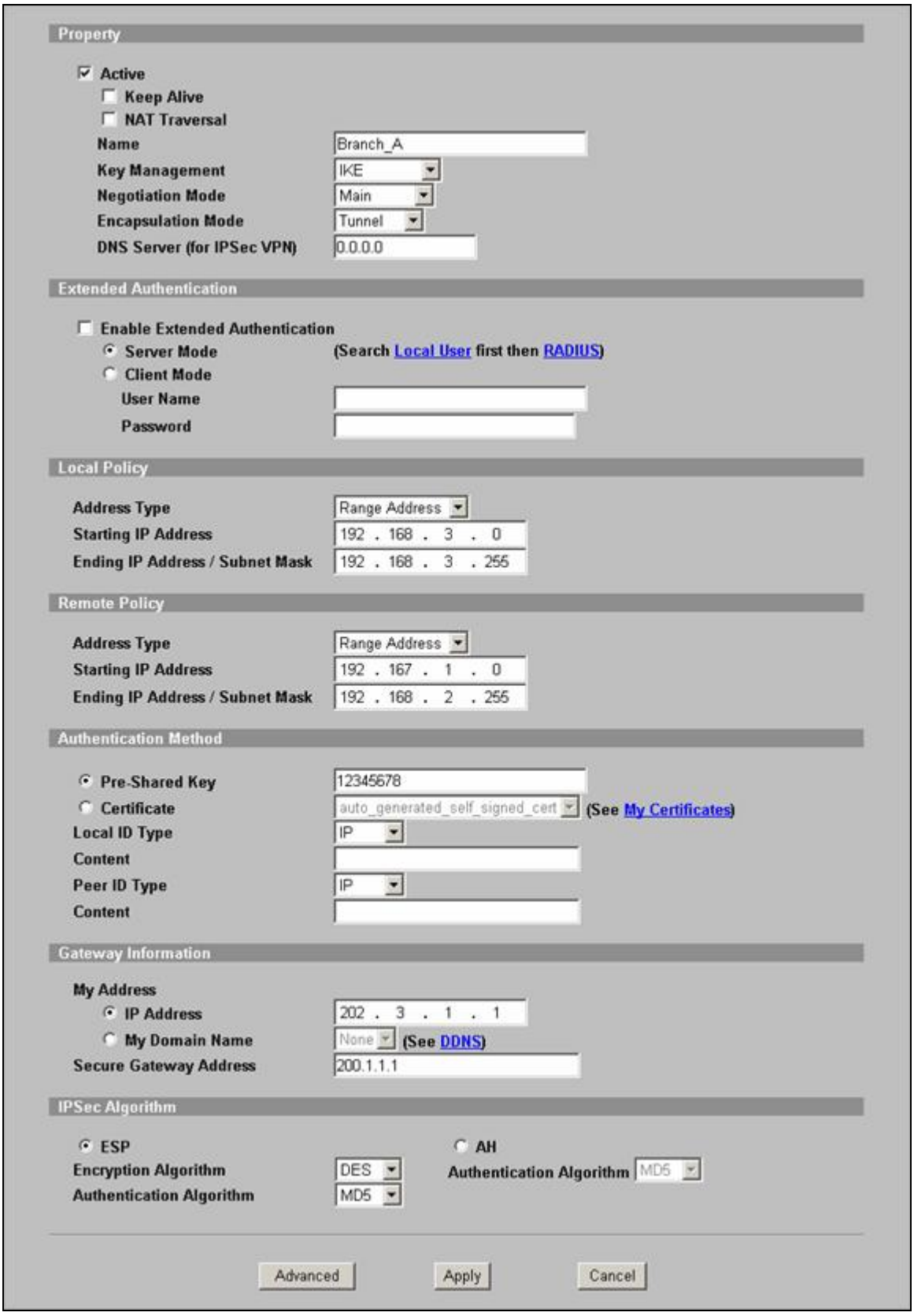
8. Set **Secure Gateway Addr** to the **IP address of Headquarter**, **202.1.1.1**.

9. Select **Encapsulation Mode** to **Tunnel**.

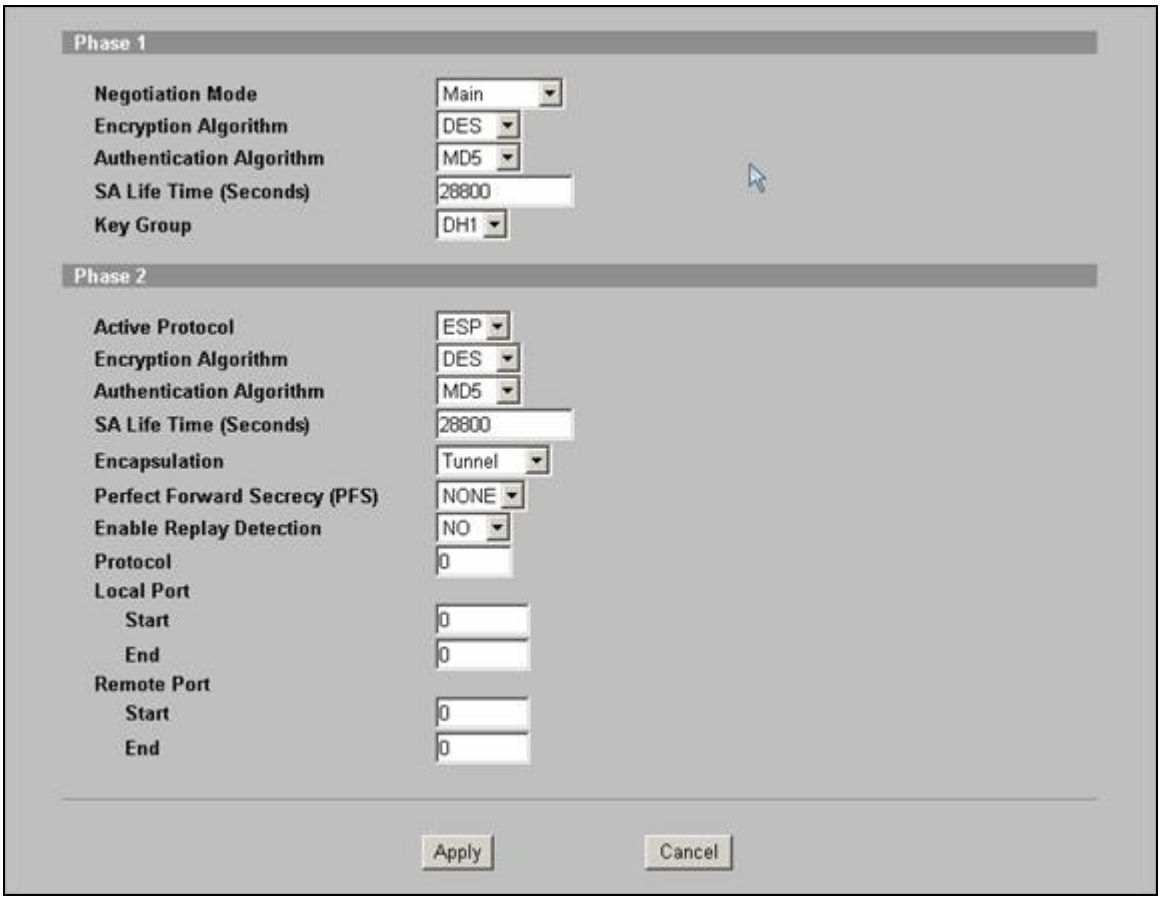
10. Check the **ESP** check box. (AH can not be used in SUA/NAT case)

11. Select **Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA-1**. These parameters are for IKE phase 2 negotiation. You can set more detailed configuration by pressing **Advanced** button.

12. Enter the key string **12345678** in the **Pre-shared Key** text box, and click **Apply**.



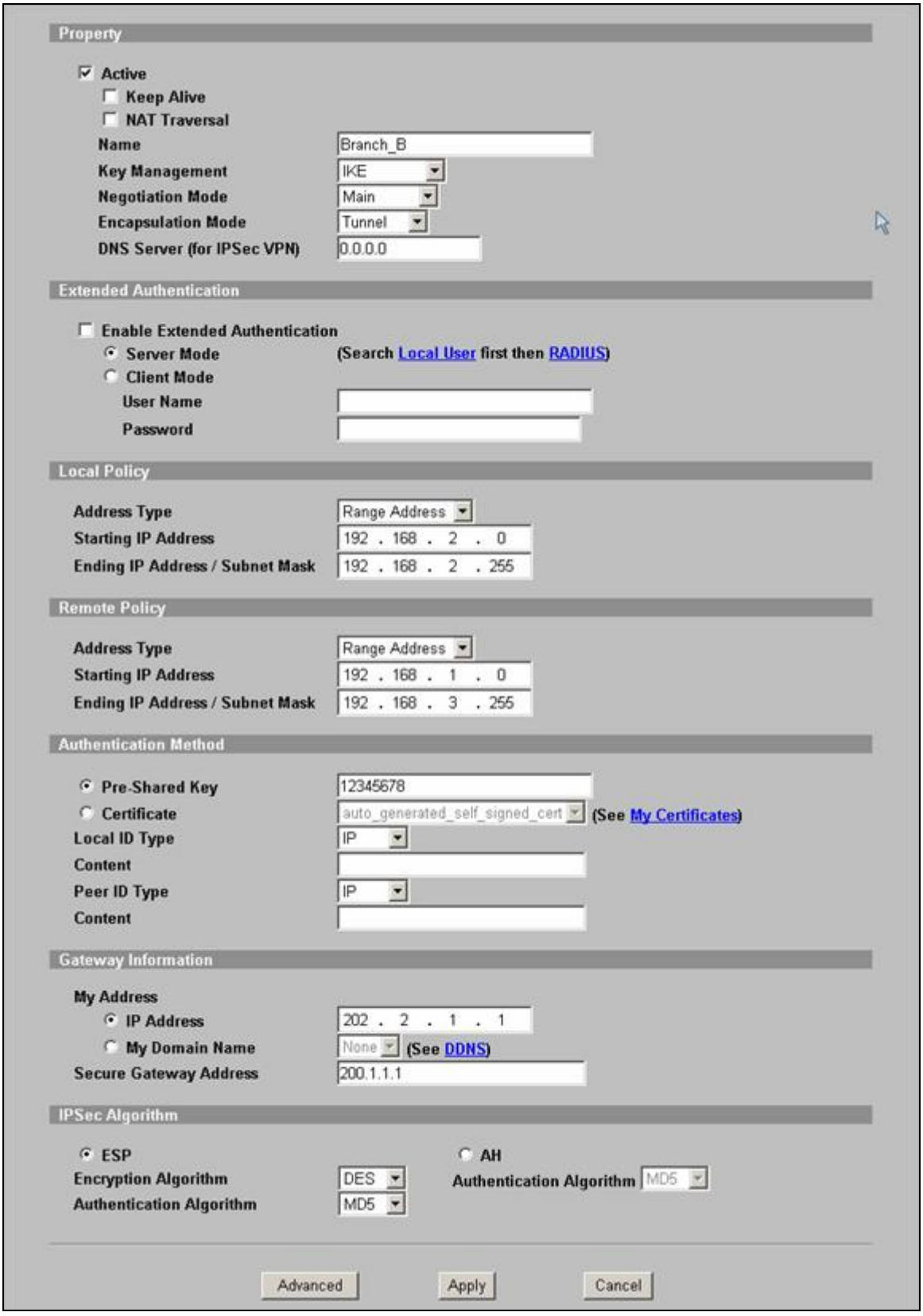
You can setup IKE phase 1 and phase 2 parameters by pressing Advanced button. Please make sure that parameters you set in this menu match with all the parameters with the correspondent VPN rule in headquarter.



2. Setup VPN in branch office B

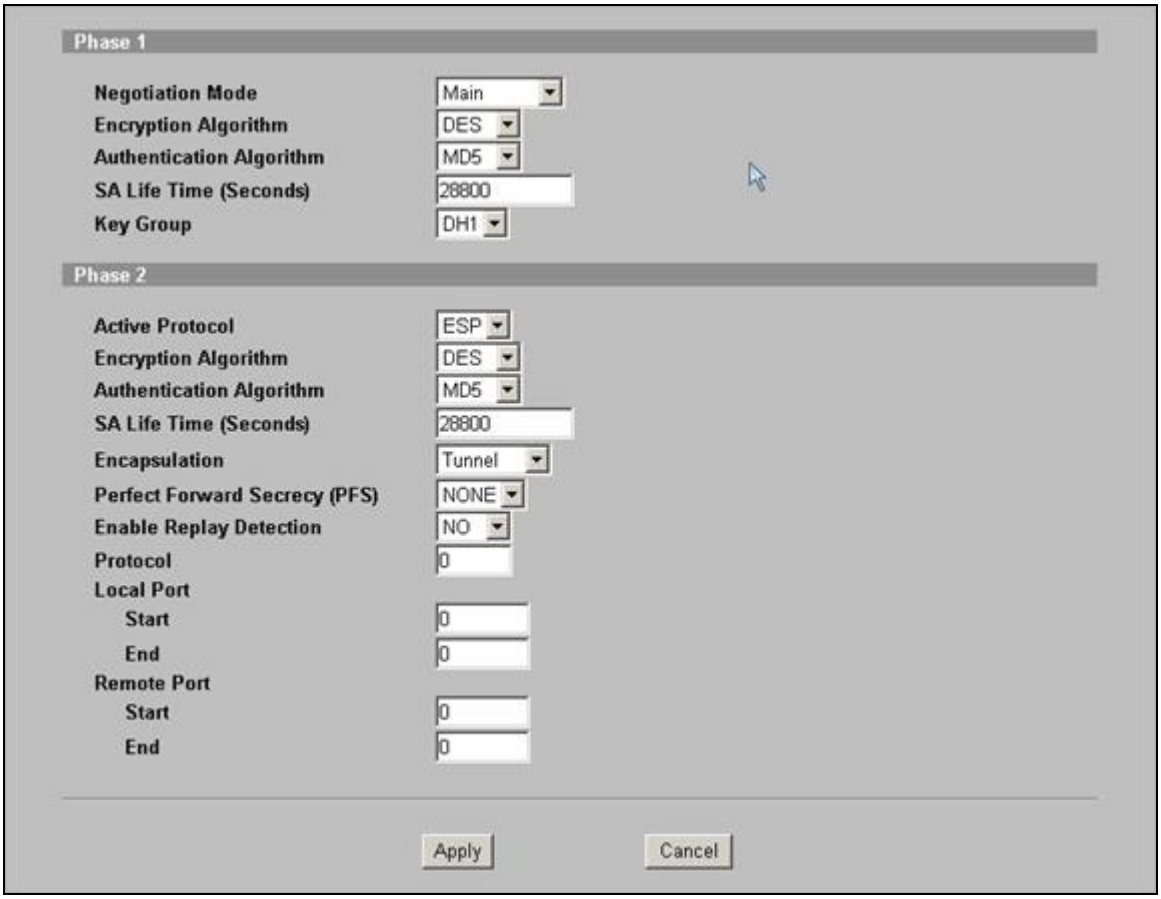
Be very careful about the remote IP address in branch office B, because for systems behind branch office B want to systems behind branch office A and headquarter, we have to specify these two segments in Remote section. However if we include these two segments in one rule, the LAN segment of branch office B will be also included in this single rule, which means intercommunication inside branch office B will run into VPN tunnel. To avoid such situation, we need two separate rules to cover the LAN segment of branch office A and headquarter.

This rule is for branch office B to access headquarter's LAN and Branch A's LAN.



Note that since Branch B's LAN is also included in remote policy, please go to ZyWALL's SMT menu 24.8 CI command mode, and issue this command, "ipsec swSkipOverlapIp on", so that local management traffic from Branch B's LAN PC to Branch B's ZyWALL would not go into VPN process.

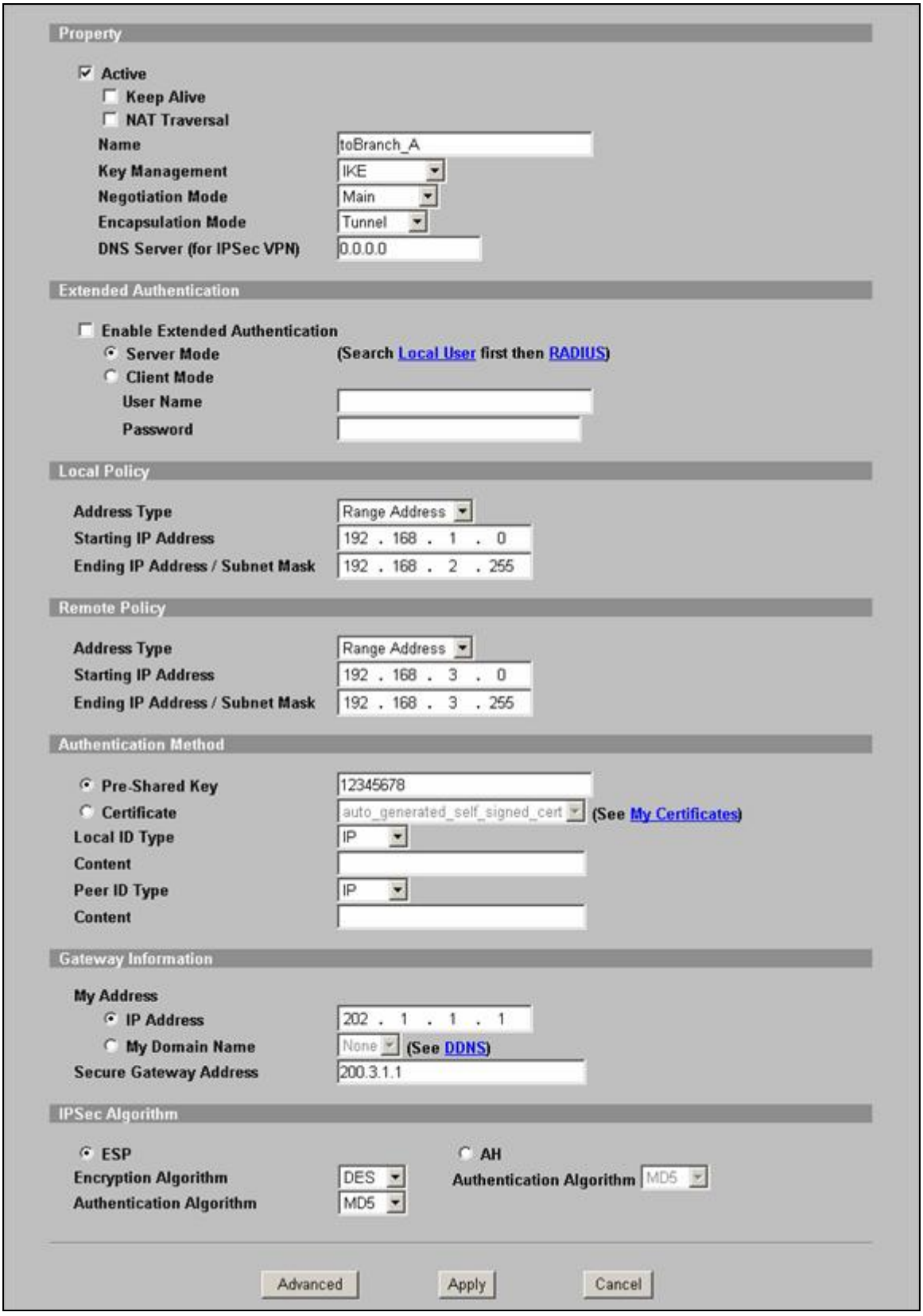
You can setup IKE phase 1 and phase 2 parameters by pressing Advanced button. Please make sure that parameters you set in this menu match with all the parameters with the correspondent VPN rule in headquarter.

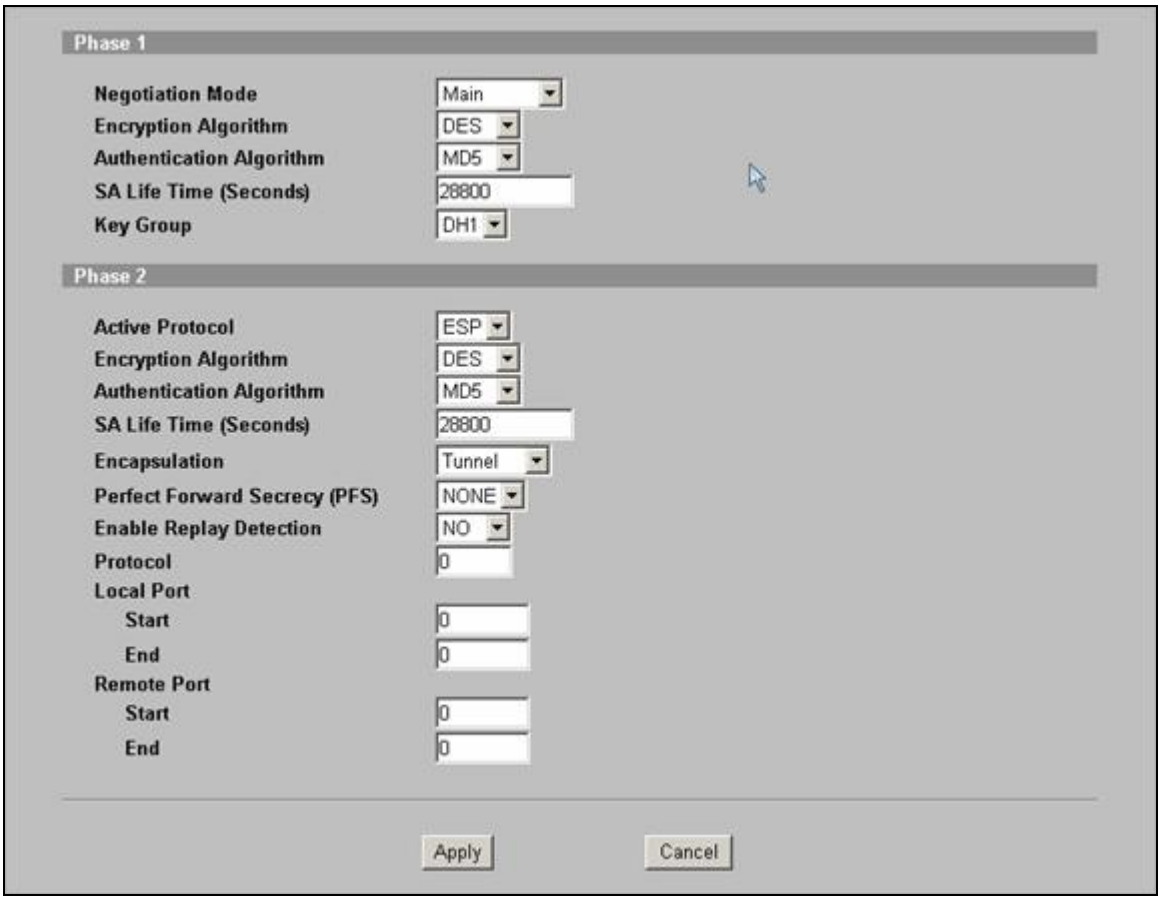


---

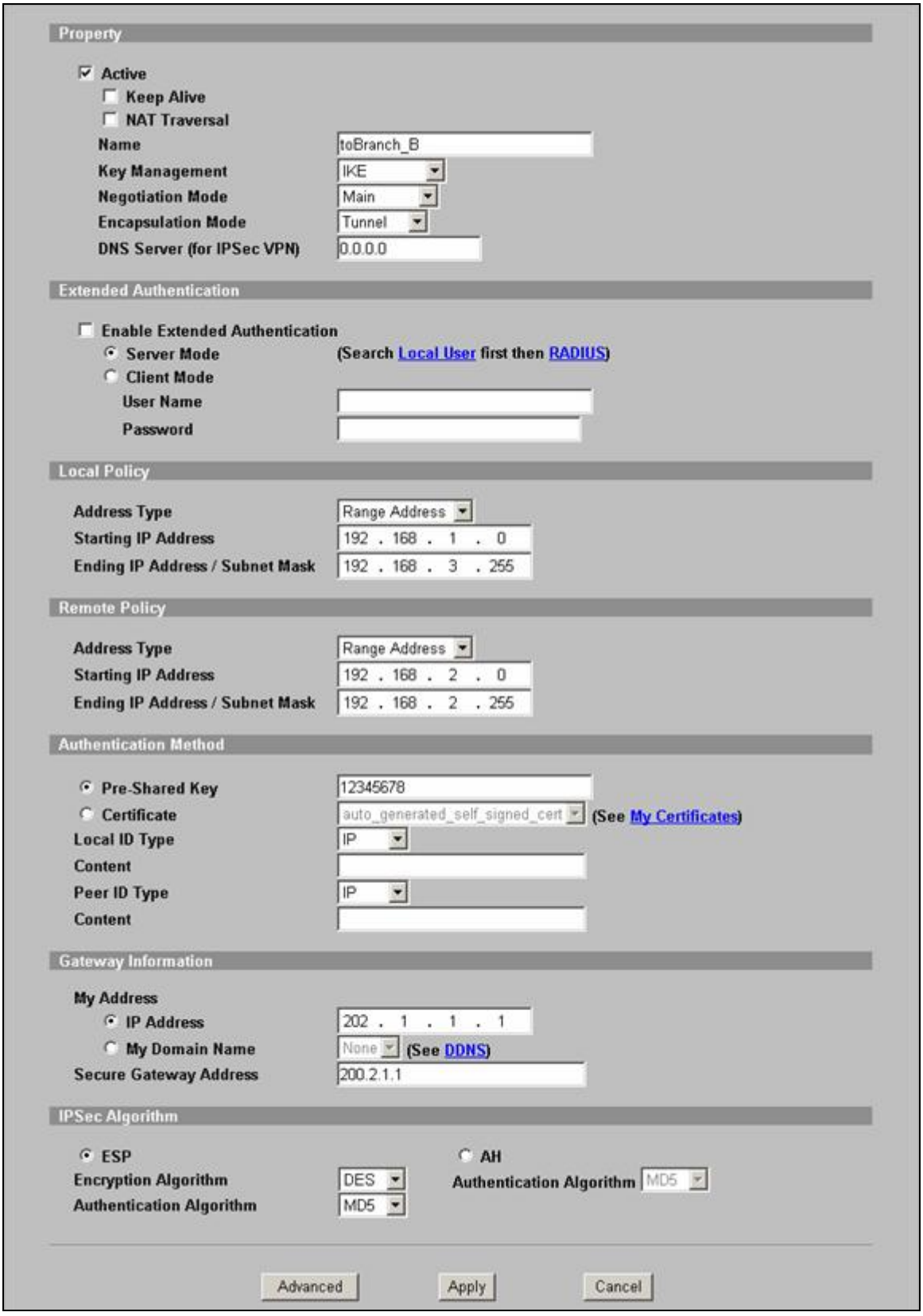
3. Setup VPN in Headquarter

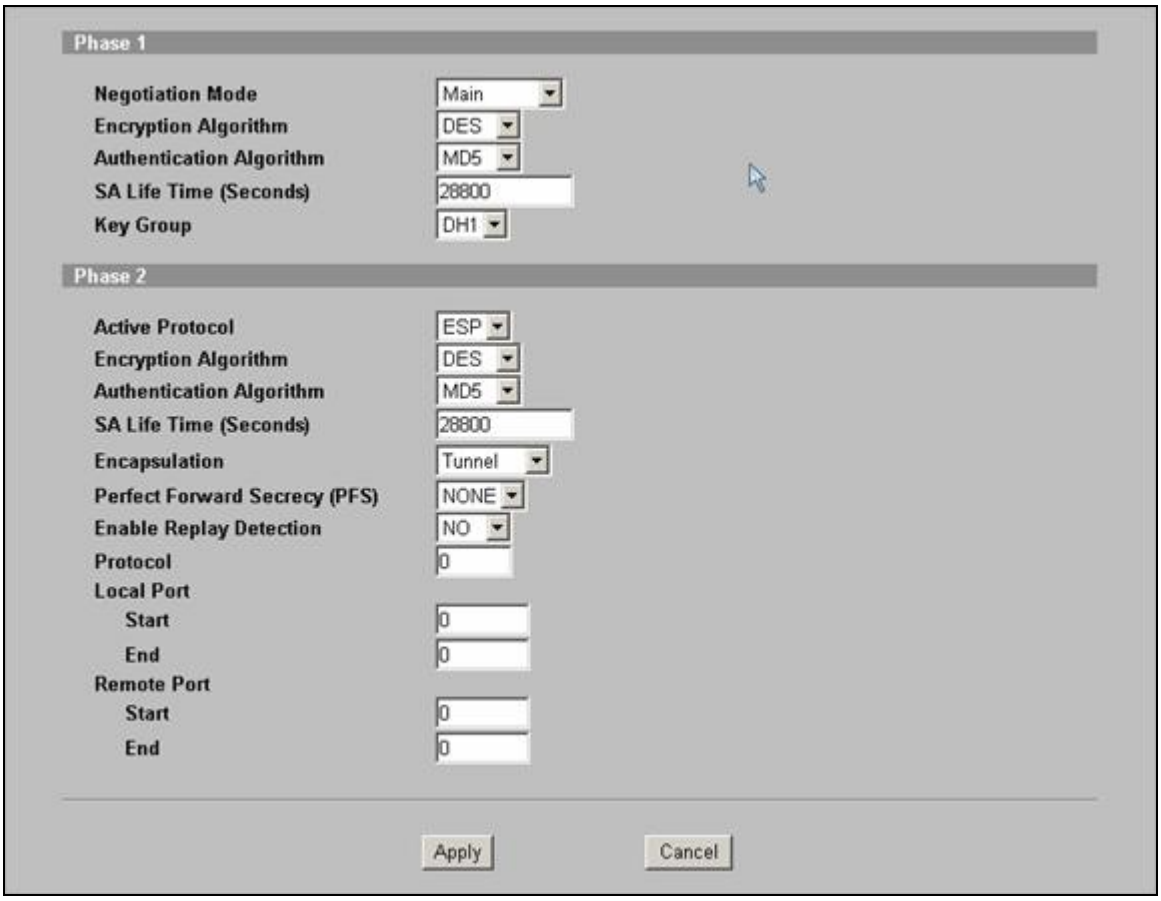
1. The correspondent rule for Branch_A in headquarter





2. The correspondent rule for Branch_B

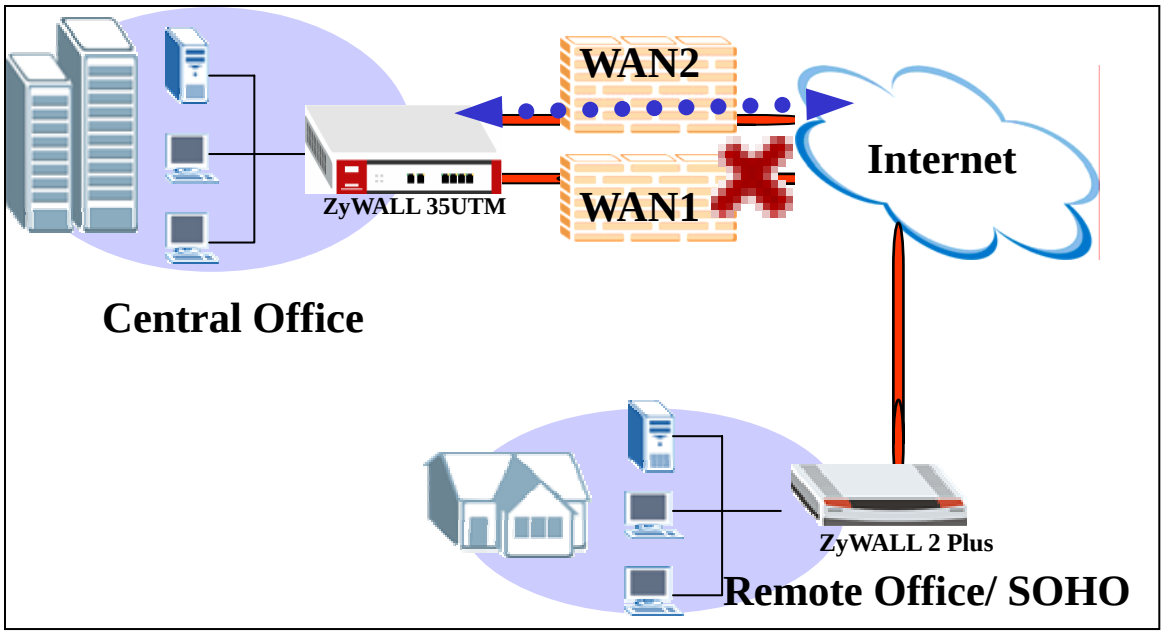




Never lost your VPN connection (IPSec High Availability)

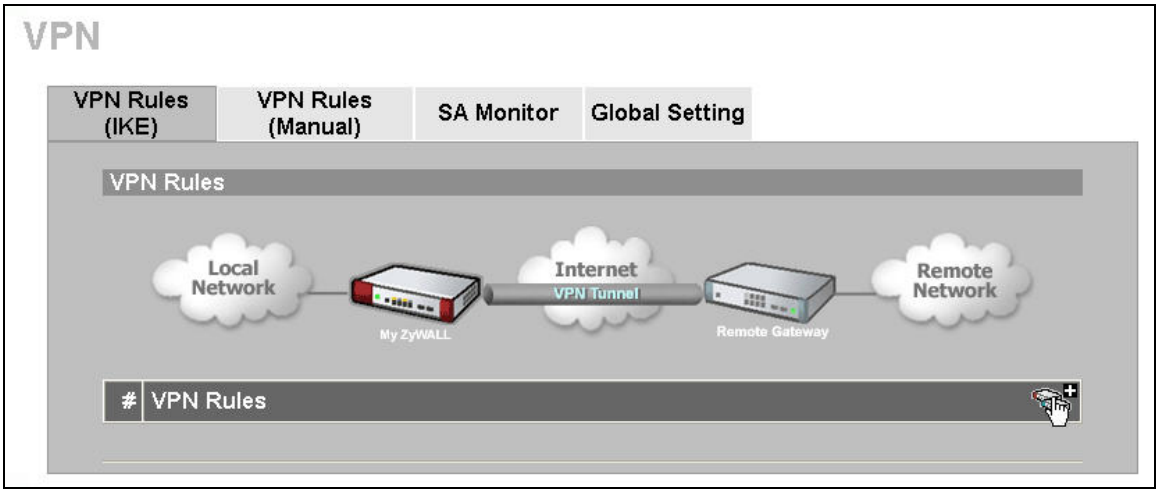
1. Setup ZyWALL VPN with high availability

The VPN high availability is design for securing VPN connection. Normally we will deploy the ZyWALL2 Plus as branch office or SOHO gateway and build up the VPN tunnel to central office. The design for IPSec HA is based on the redundant gateway option implement on the ZyWALL2 Plus. In traditional design, the VPN connection will be dropped once the remote gateway internet connection going down. ZyXEL already had Dual WAN security gateway solution to prevent the failure of internet connection but for the VPN connection transfers from primary WAN to backup WAN only support DDNS IP update before. ZyWALL2 Plus supports redundant remote gateway to continue the VPN connection once the primary WAN connection failure. The redundant gateway can be configured as IP format or Domain Name format, this provide the flexibility for administrator to configure the network setting.



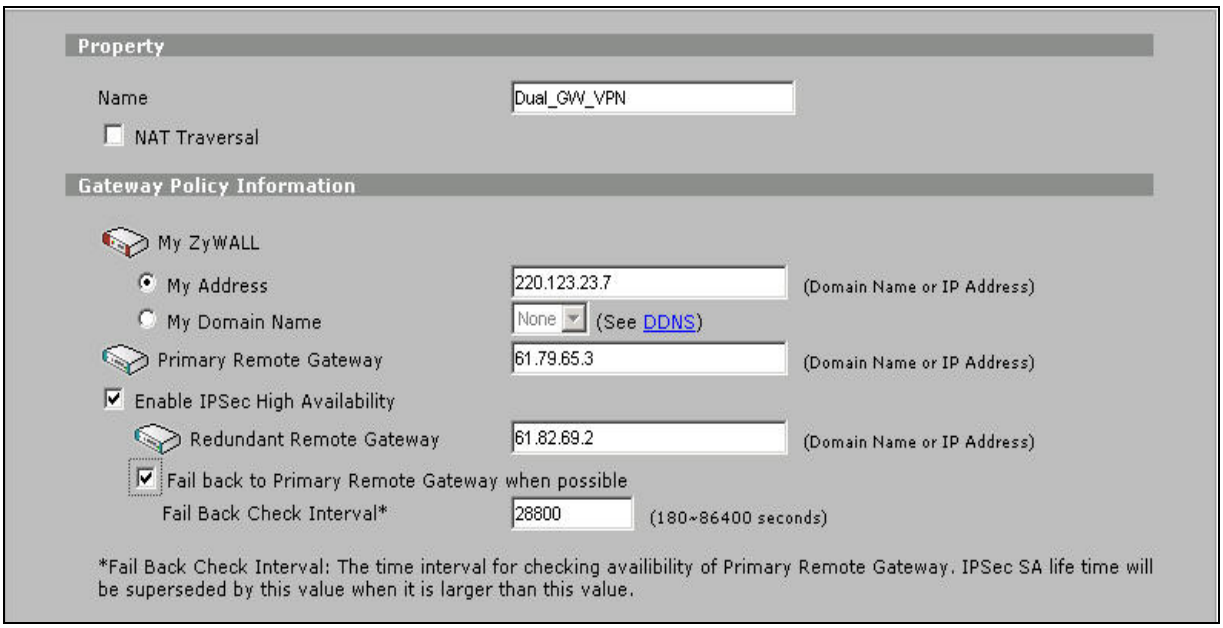
How to configure the VPN HA

1. Using a web browser, login ZyWALL by giving the LAN IP address of ZyWALL in URL field. Default LAN IP is **192.168.1.1**, default password to login web configurator is **1234**.
2. Go to SECURITY->VPN->Press **Add** button



3. Give a name for your policy, for example "**Dual_GW_VPN**"
4. **My IP Addr** is the **WAN IP of ZyWALL**. In this example, you should type 220.123.23.7 IP address on **My ZyWALL** text box.
5. **Primary Remote Gateway IP Address** is the **Central office's WAN1 IP address**. In this example, you should type 61.79.65.3 IP address on **Primary Remote Gateway** text box.

6. Check the "**Enable IPSec High Availability**" box to enable the IPSec HA and input the WAN2 IP address as the redundant gateway. In this example, you should type 61.82.69.2 IP address on **Redundant Remote Gateway** text box.
7. The "**Fail back to Primary Remote Gateway when possible**" is an option leaving to user to design if they want switching the connection back to the primary gateway when it is recovery. In this example, we decide to switch the connection back to primary gateway and the check interval is 28800 seconds.
8. The remaining VPN setting is the same as pervious steps to complete all settings.
9. Please remember to setup a corresponding VPN rule in central office's firewall for building up the VPN tunnel from WAN2 to remote office's firewall (ZyWALL2 Plus).

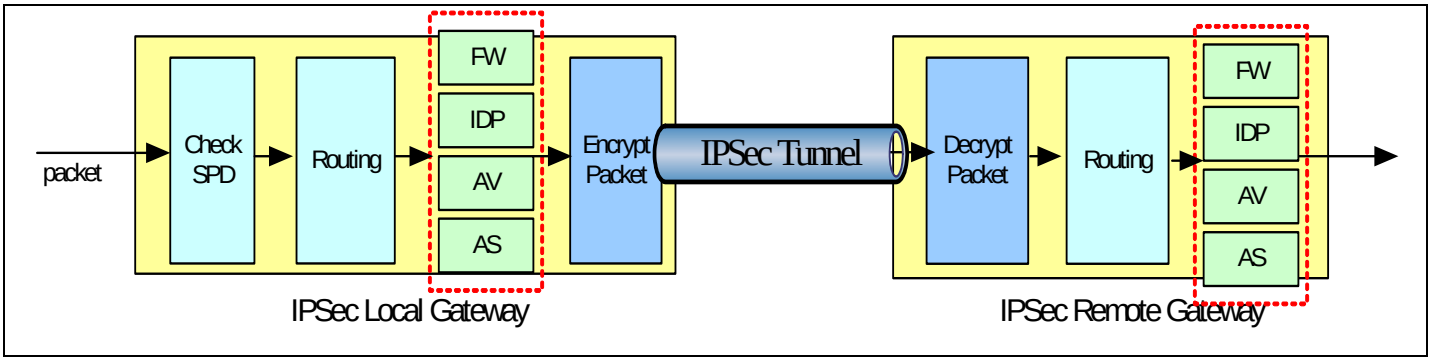


Access control and security VPN connection (Security policy enforcement IPSec)

Setup ZyWALL VPN with access control - Firewall

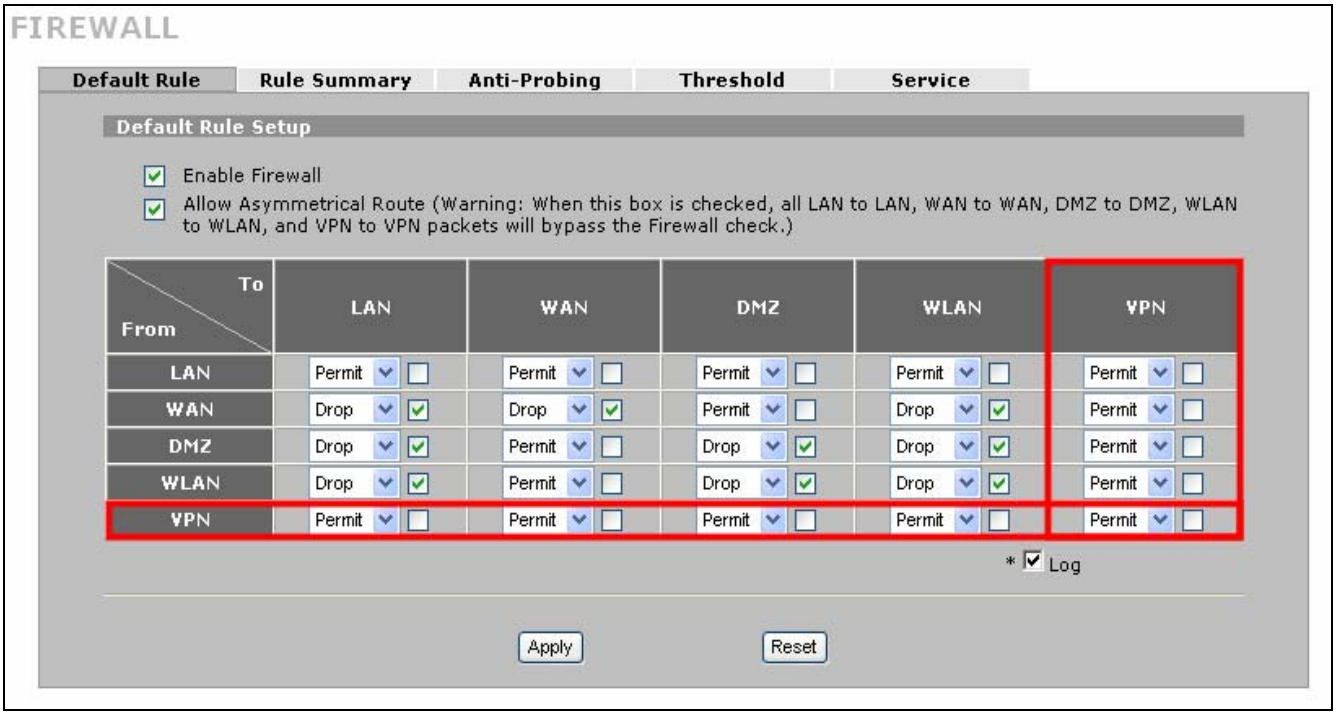
Setup ZyWALL VPN with web filtering rule – Content Filter

Normally, the traffic transmitted between VPN tunnel is treated as security connection due on multi authentication and encryption methods. Thus, the security gateway won't inspect the VPN traffic because the traffic sending with cipher text format not in plaintext. The enhanced algorithm we adopted is ZyWALL can inspect the VPN packet before encrypt or after decrypt the packet sending to or receiving from VPN tunnel.

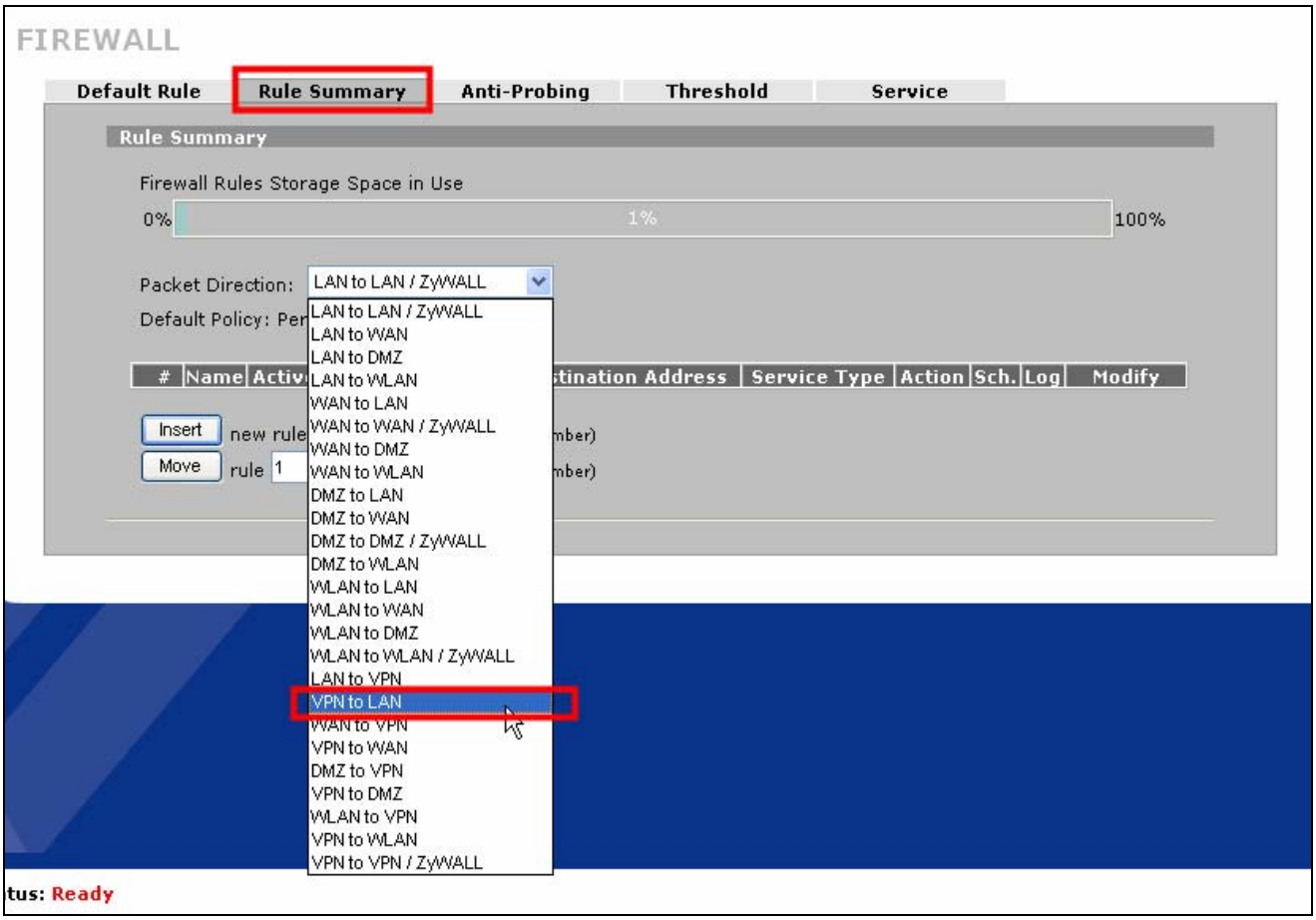


How to configure access control rule over VPN

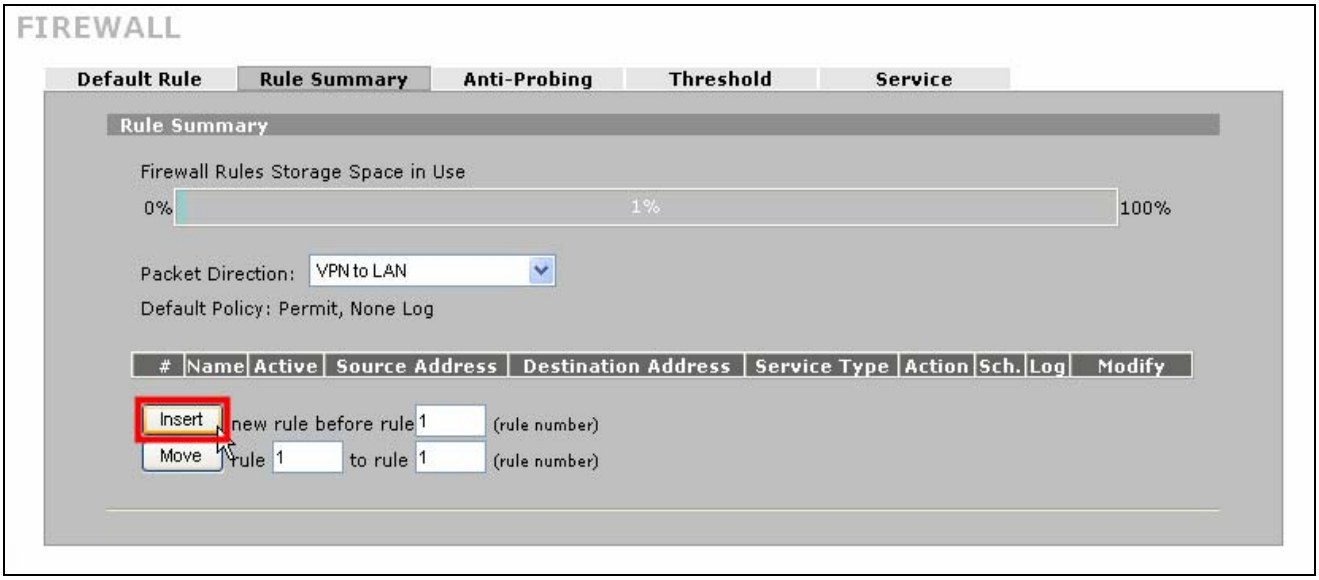
1. Log into the web configurator on the ZyWALL. In a web browser, enter the IP address (the default is **192.168.1.1**) of your ZyWALL in the Address field. A screen displays, enter the administrative login password (**1234** is the default).
2. Access control in VPN tunnel application can be enforced via Firewall feature. Switch to Security>Firewall menu to configure the traffic from VPN or to VPN access control rule.



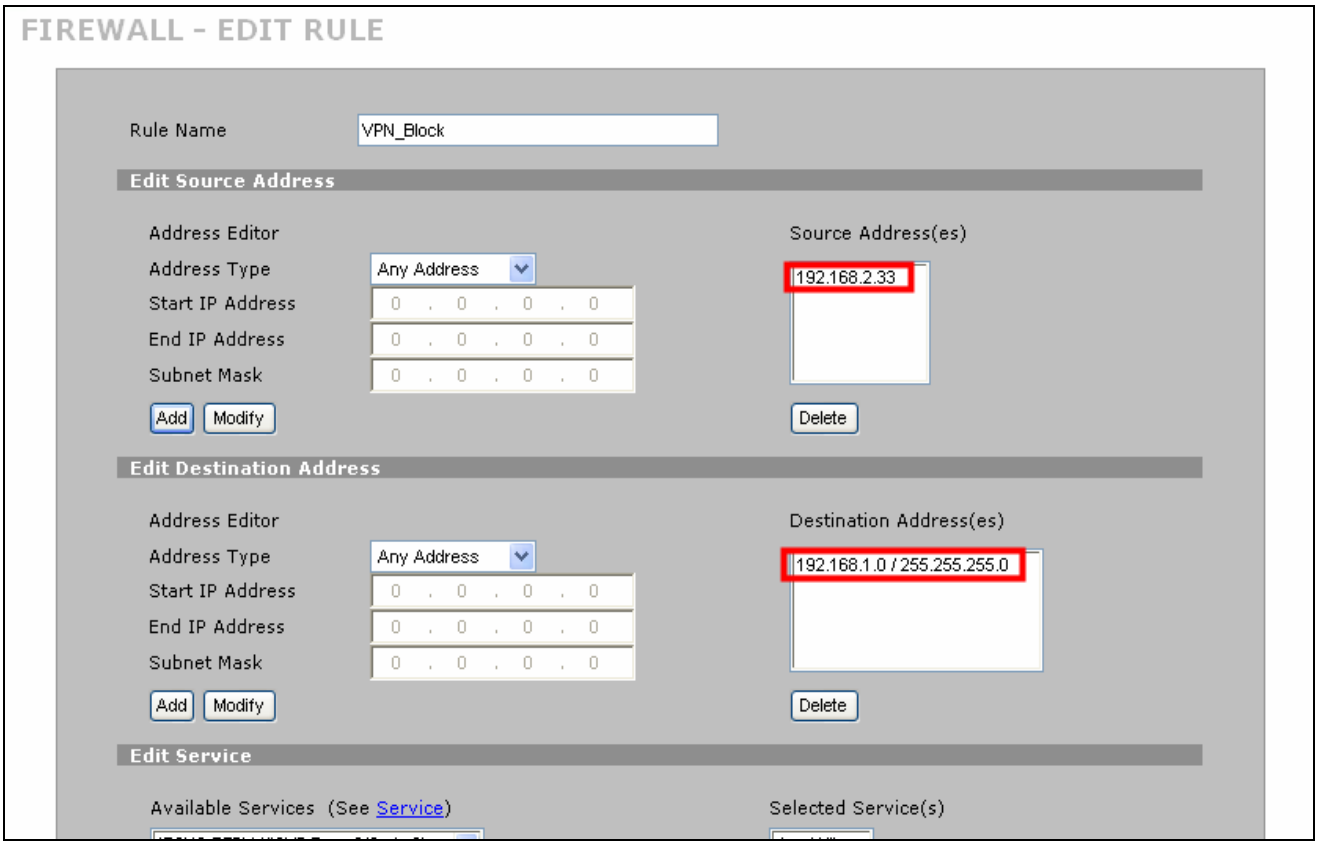
3. For example, the remote VPN policy is 192.168.2.0/24 and we want to block the traffic from 192.168.2.33 to access local LAN subnet 192.168.1.0/24. The default VPN to LAN traffic is permit and we have to change the VPN to LAN access control rule in rule summary sub menu.



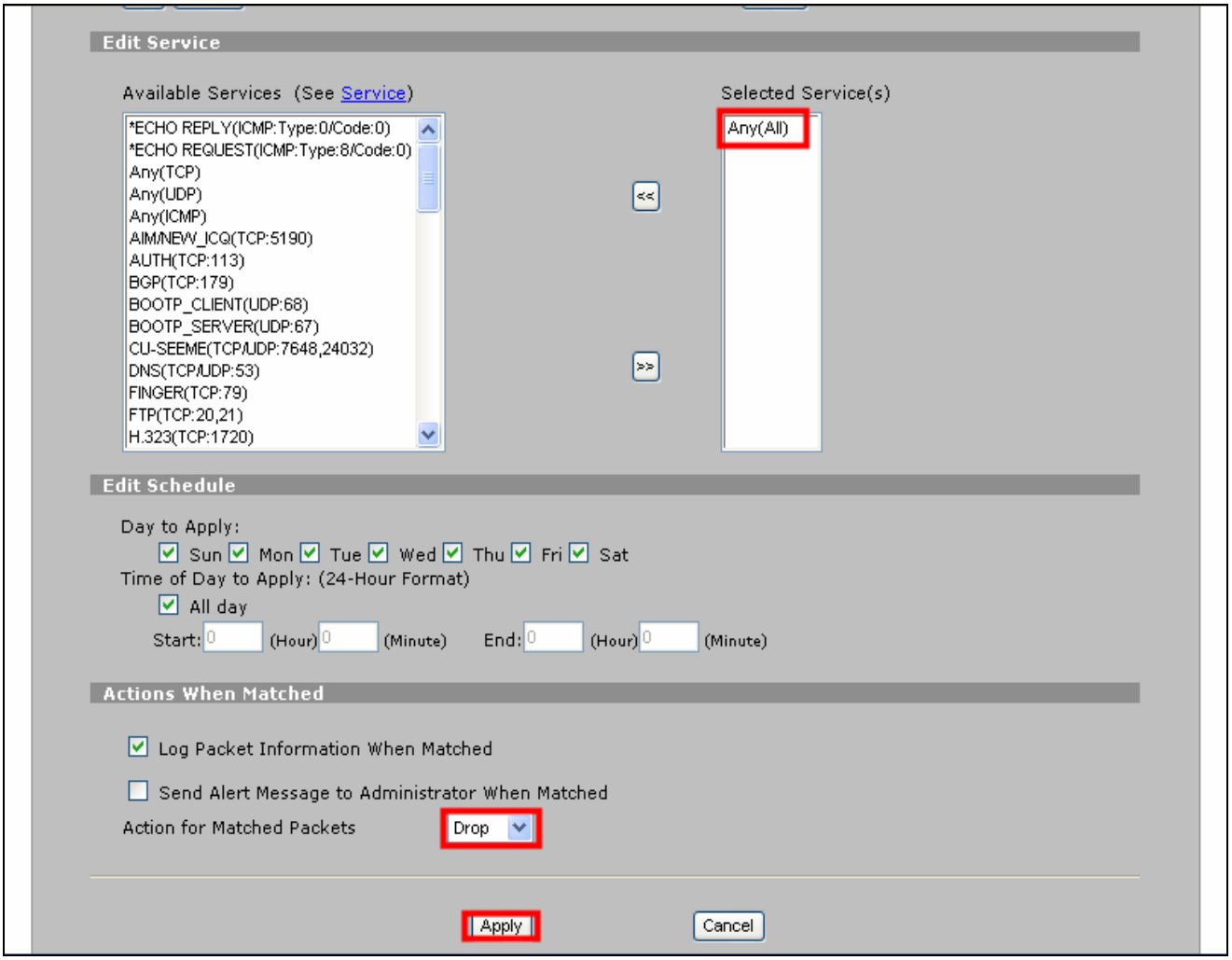
4. Click the Insert button to insert a new rule.



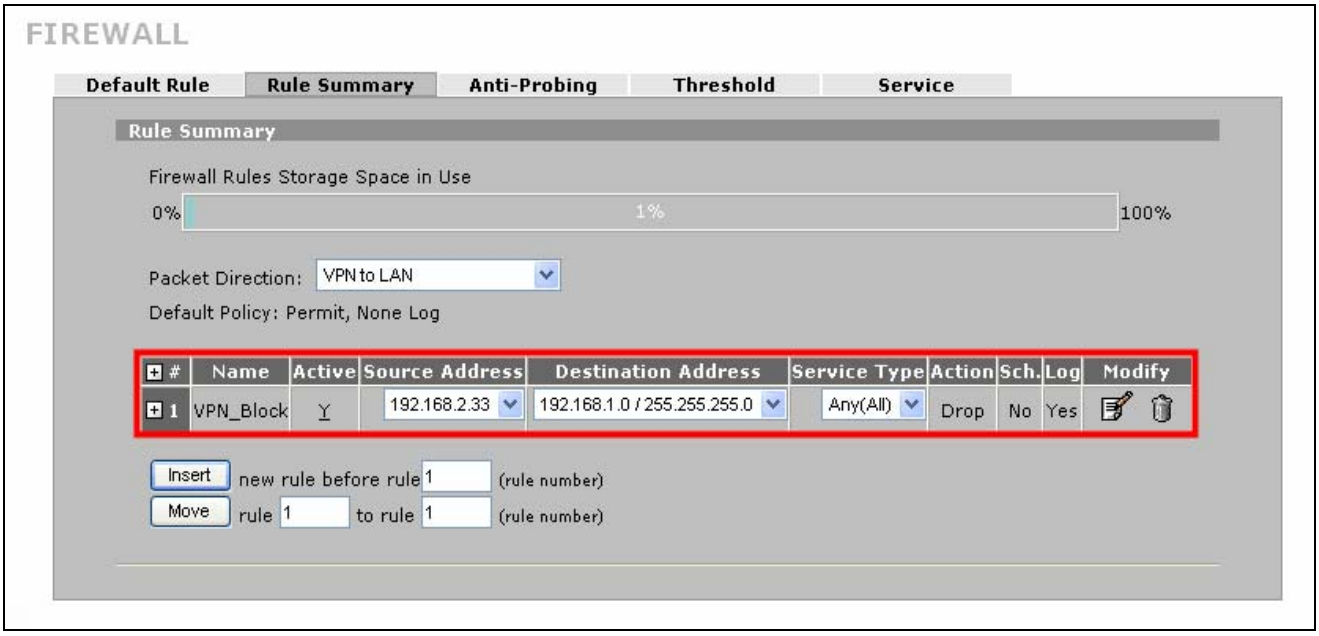
5. Edit the source and destination address as 192.168.2.33 and 192.168.1.0/255.255.255.0



6. The service type is **Any** to block all kind of traffic from 192.168.2.33 to access LAN subnet and **Action for Matched Packets** is **Drop** and then click apply to save and activate the configuration.

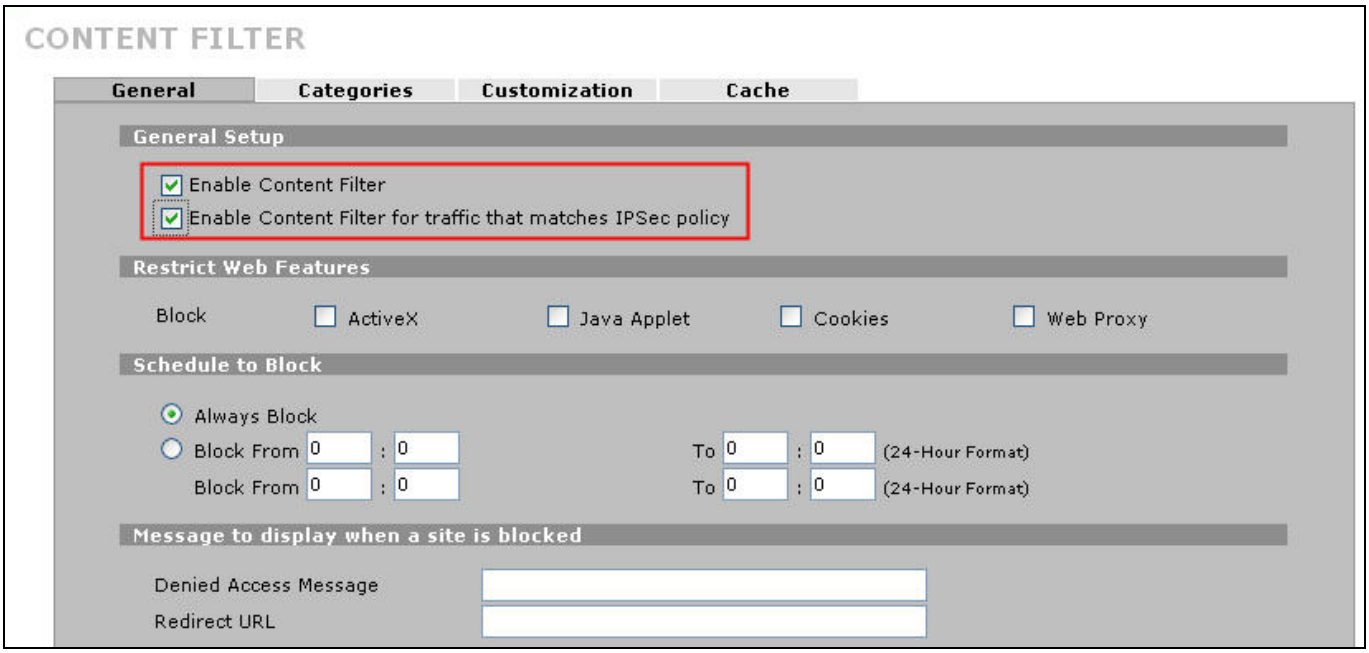


7. We can see a new rule had been configured and showed in the rule summary page. This will achieve our goal to block all traffic from VPN remote host 192.168.2.33 to access the LAN subnet.



How to configure Web filtering rule over VPN – Content Filter

1. The switch to enable the content filtering over VPN traffic is available in Content Filter general configuration page. The content filtering over VPN can only be enabled after the content filter global switch enabled otherwise the enable content filter for VPN traffic option will be gray out.



2. The traffic decrypted from VPN tunnel and send to internet can be applied the web filtering rule after enable the content filter for traffic that matches IPSec policy.

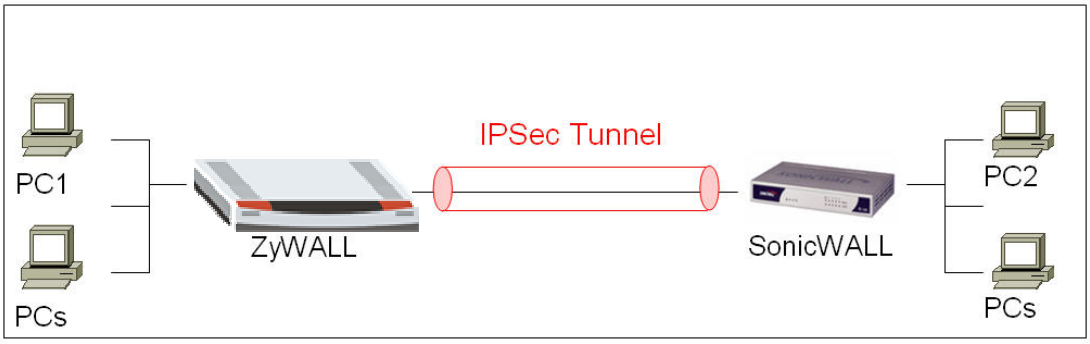
ZyWALL vs 3rd Party VPN Gateway

SonicWALL with ZyWALL VPN Tunneling

1. Setup ZyWALL VPN
2. Setup SonicWALL VPN

This page guides us to setup a VPN connection between the ZyWALL and SonicWALL router.

As the figure shown below, the tunnel between PC1 and PC2 ensures the packet flows between them are secure. Because the packets go through the IPSec tunnel are encrypted. To setup this VPN tunnel, the required settings for ZyWALL and SonicWALL are explained in the following sections. As the red pipe shown in the following figure, **the tunneling endpoints are ZyWALL router and SonicWALL router.**



The IP addresses we use in this example are as shown below.

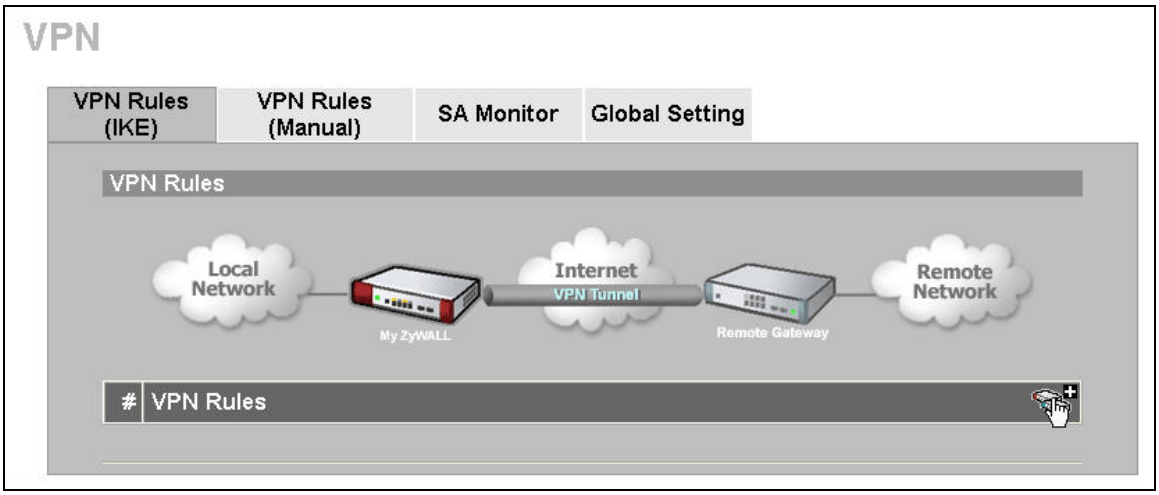
PC 1	ZyWALL	SonicWALL	PC2
192.168.1.33	WAN: 172.22.3.89 LAN: 192.168.1.1	WAN: 172.22.1.251 LAN: 192.168.168.618	192.168.168.6

---

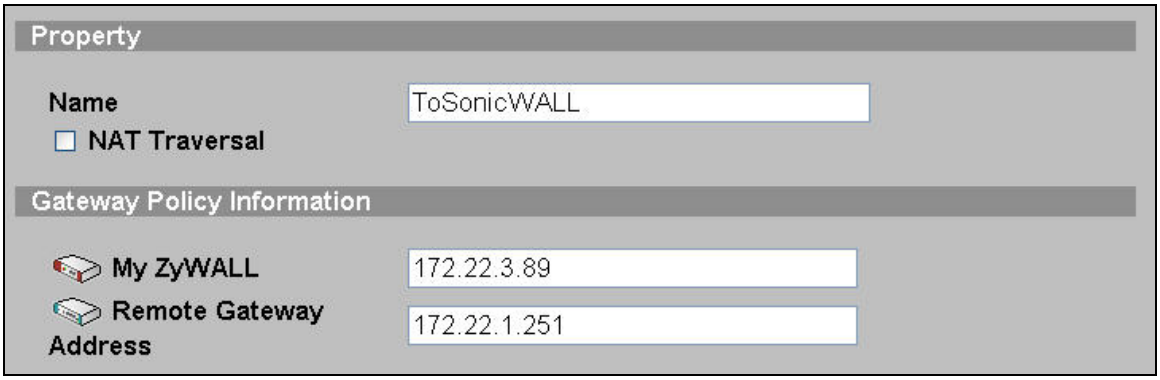
1. Setup ZyWALL VPN

10. Using a web browser, login ZyWALL by giving the LAN IP address of ZyWALL in URL field. Default LAN IP is **192.168.1.1**, default password to login web configurator is **1234**.

11. Go to SECURITY->VPN->Press **Add** button

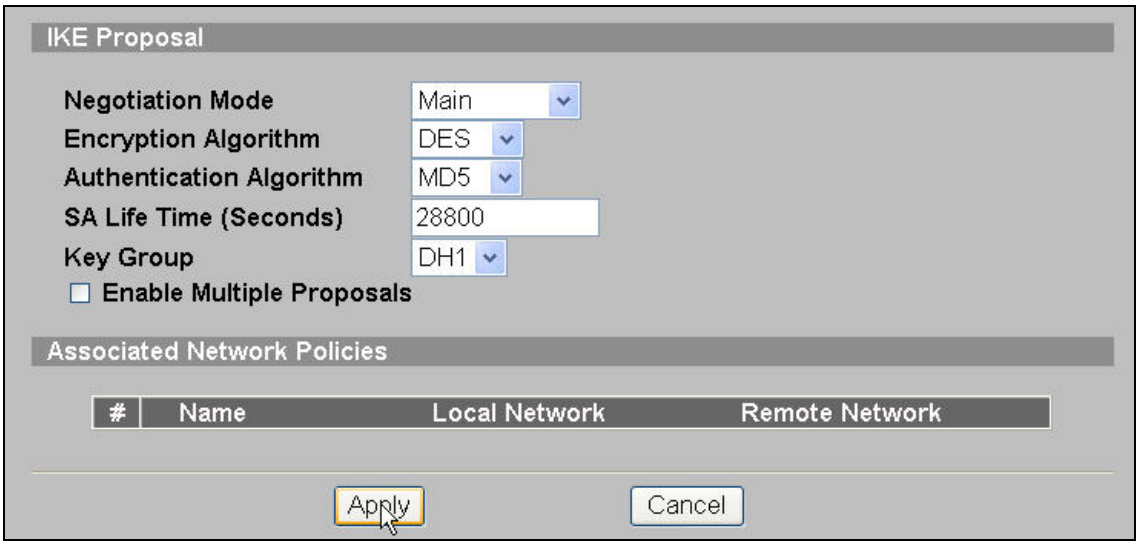


12. Give a name for your policy, for example "**ToSonicWALL**"
13. **My IP Addr** is the **WAN IP of ZyWALL**. In this example, you should type 172.22.3.89 IP address on **My ZyWALL** text box.
14. **Secure Gateway IP Addr** is the **SonicWALL's WAN IP address**. In this example, you should type 172.22.1.251 IP address on **Remote Gateway** text box.

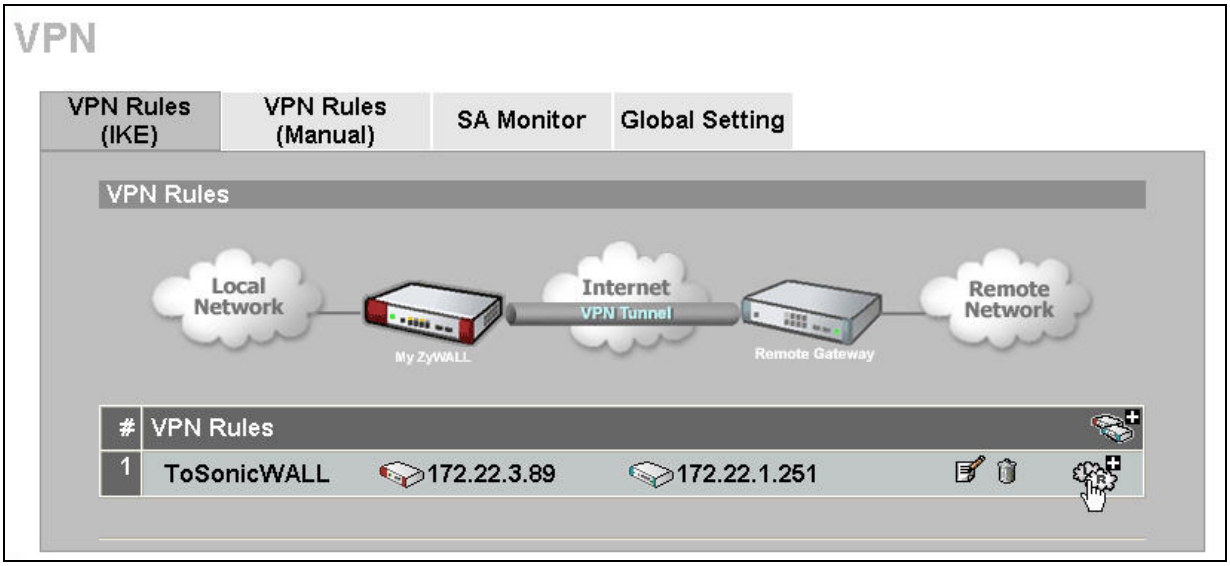


15. In **Authentication Key**, enter the key string **12345678** in the **Pre-Shared Key** text box.

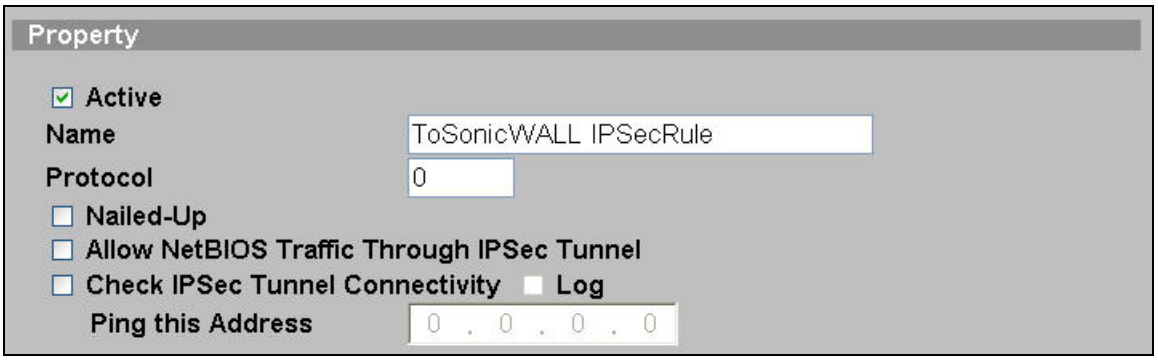
16. Select **Negotiation Mode** to **Main mode**, **Encryption Algorithm** to **DES**, **Authentication Algorithm** to **MD5**, **Key Group** to **DH1**, and then press **Apply** button on this page.



17. You will see an IKE rule on your VPN page, press L/R button to edit your IPSec rule.

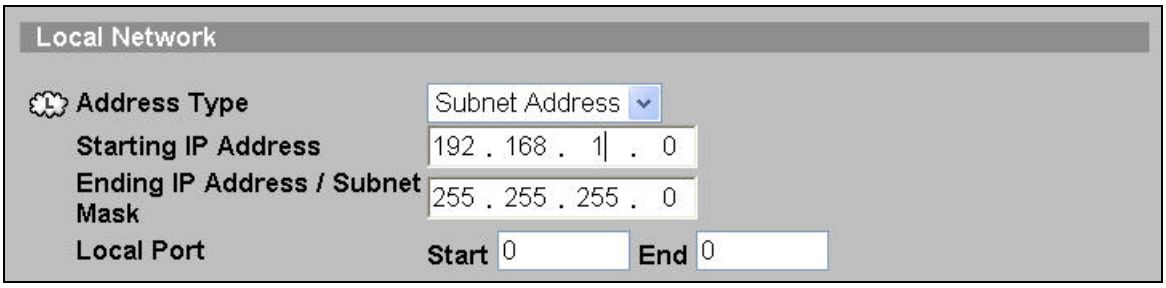


18. Check **Active** check box and give a name to this policy.

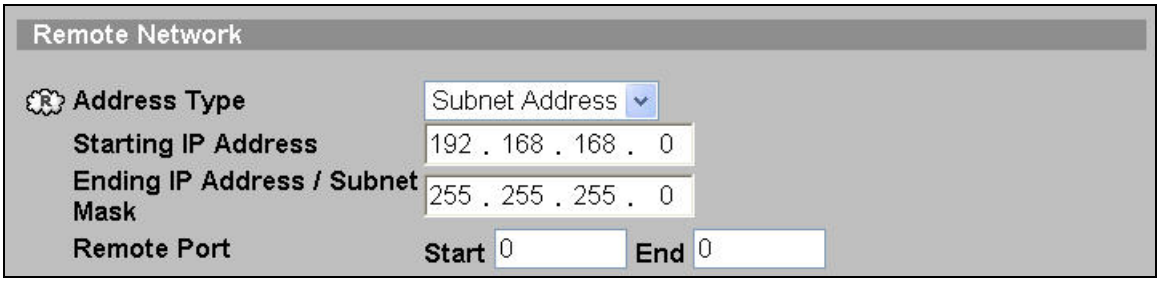


19. On Gateway Policy Information, you should choose **ToSonicWALL** IKE policy for your IPSec rule.

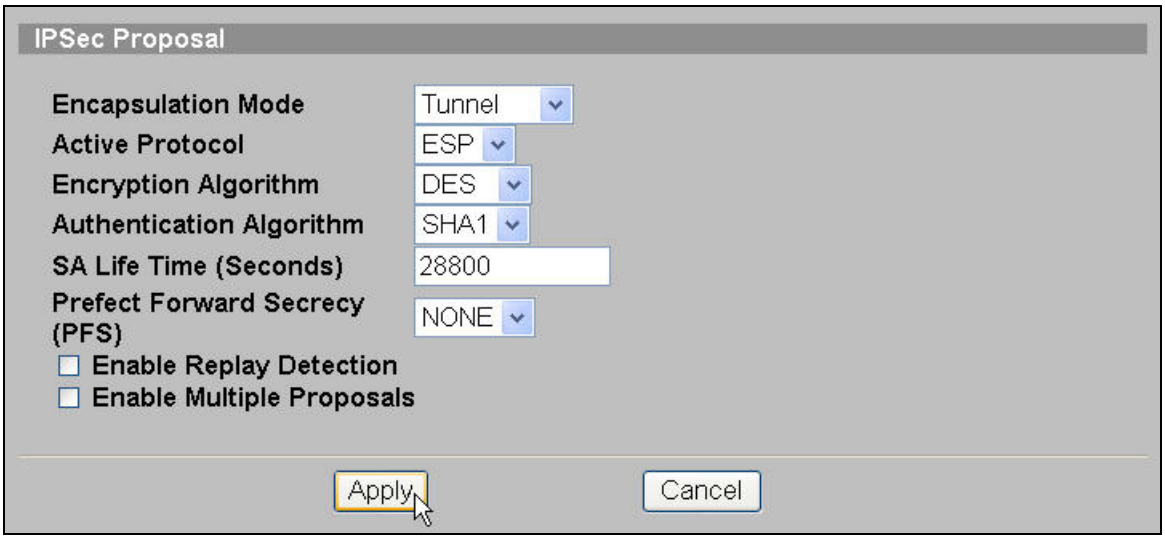
20. On **Local Network,** choose **Subnet Address** for your **Address Type. Starting IP Address** and **Ending IP Address/Subnet** are your local site LAN IP addresses. In this example, you should type 192.168.1.0 on **Starting IP Address** field and then type 255.255.255.0 on **Ending IP Address/Subnet** field.



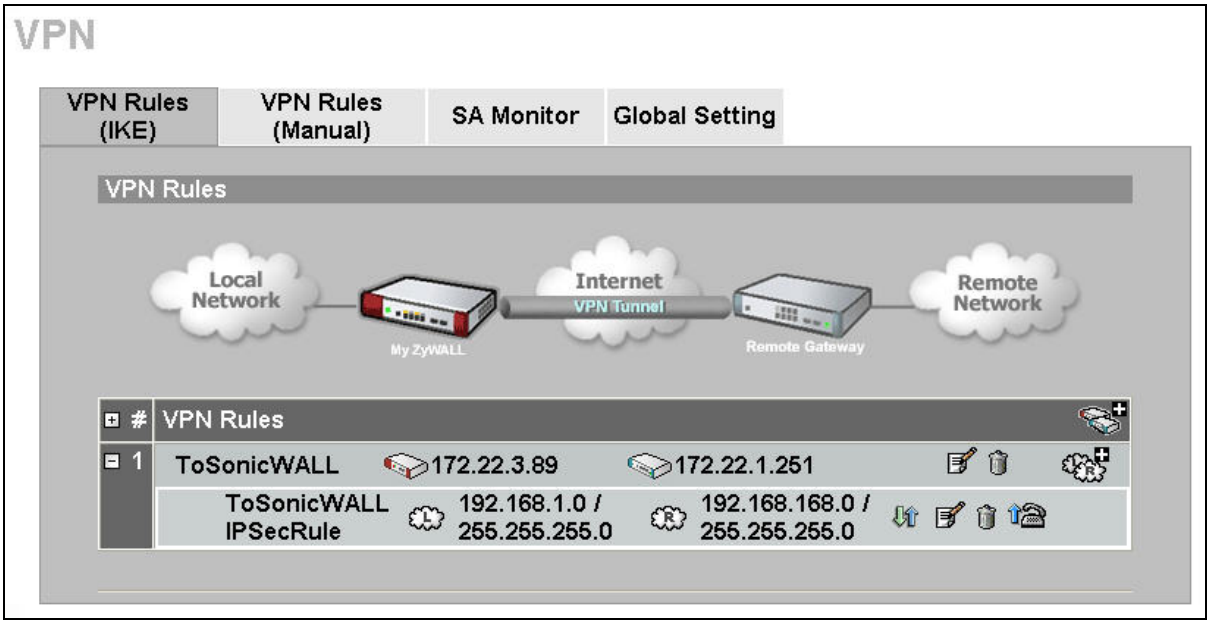
21. On **Remote Network,** choose **Subnet Address** for your **Address Type. Starting IP Address** and **Ending IP Address/Subnet** are your remote site LAN IP addresses. In this example, you should type 192.168.168.0 on **Starting IP Address** field and then type 255.255.255.0 on **Ending IP Address/Subnet** field.



22. On **IPSec Proposal,** select **Encapsulation Mode** to **Tunnel, Active Protocol** to **ESP, Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA1**, and then press Apply button on this page.



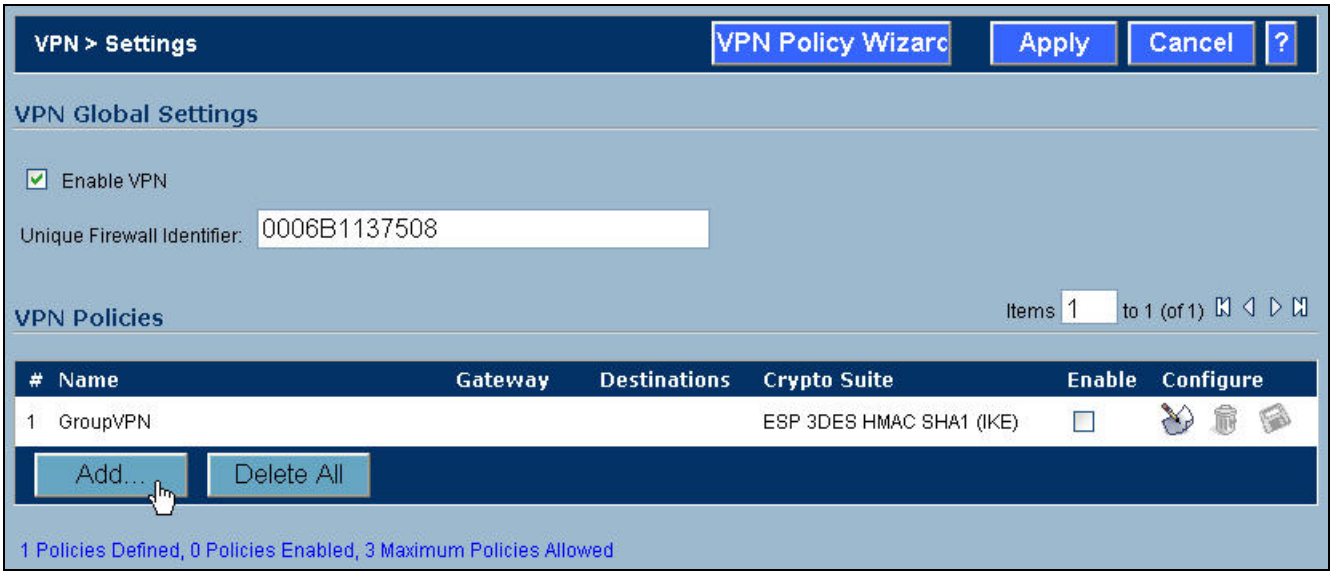
23. When you finished doing your settings, you will see the following page.



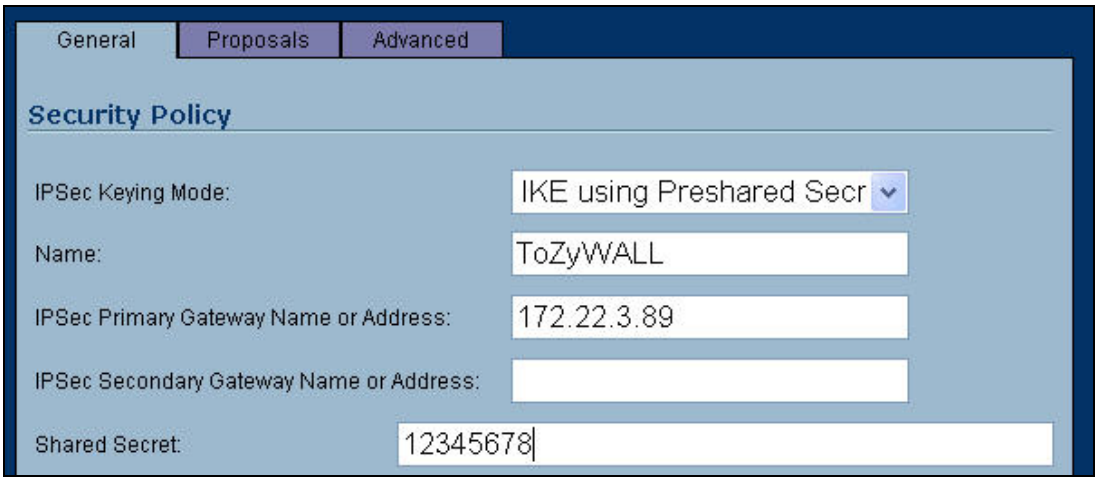
2. Setup SonicWALL VPN (We choose SonicWALL TZ150 device in this example.)

1. Using a web browser, login SonicWALL by giving the LAN IP address of SonicWALL in URL field.

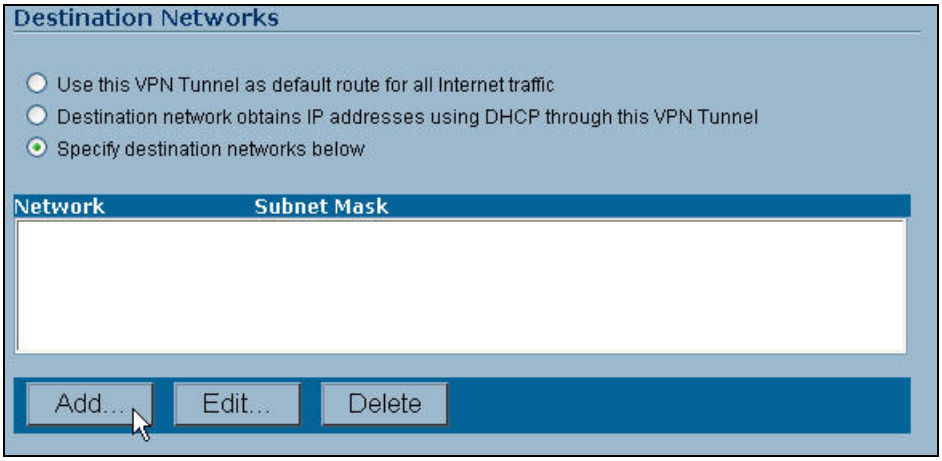
Go to VPN page, check **Enable VPN** check box, and then press **Add** button, it will bring up a page which you could do your VPN settings. (Note: You could use **VPN Policy Wizard** to set up your VPN rules as well.)



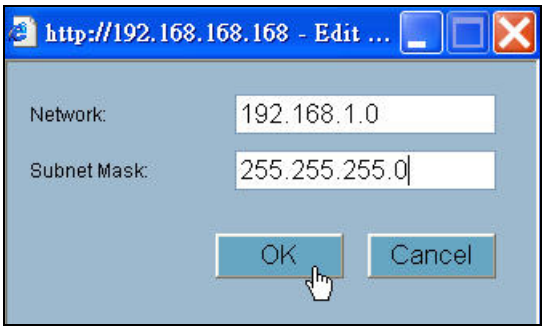
2. Click **General** tab, on Security Policy settings, give a name to this policy. In this example, type **ToZyWALL** on **Name** text box. **IPSec Primary Gateway Name or Address** is the **ZyWALL's WAN IP Address** (remote gateway IP address). In this example, you should type 172.22.3.89 on **IPSec Primary Gateway Name or Address** text box. Then, enter the key string **12345678** on **Shared Secret** text box.



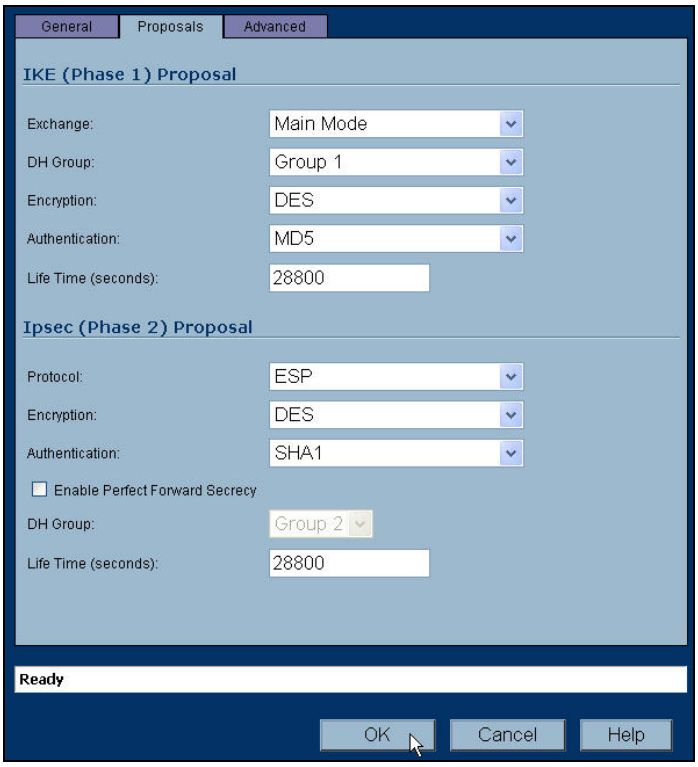
3. On **Destination Networks**, select **Specify destination networks below** option, and then press **Add** button.



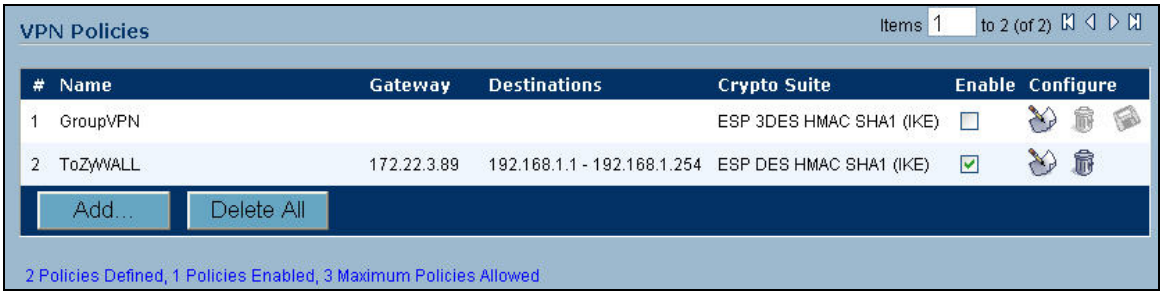
4. **Network IP Address** and **Subnet Mask** are your remote site LAN IP addresses. In this example, you should type 192.168.1.0 on **Network** text box and then type 255.255.255.0 on **Subnet Mask** text box, and then press **OK** button.



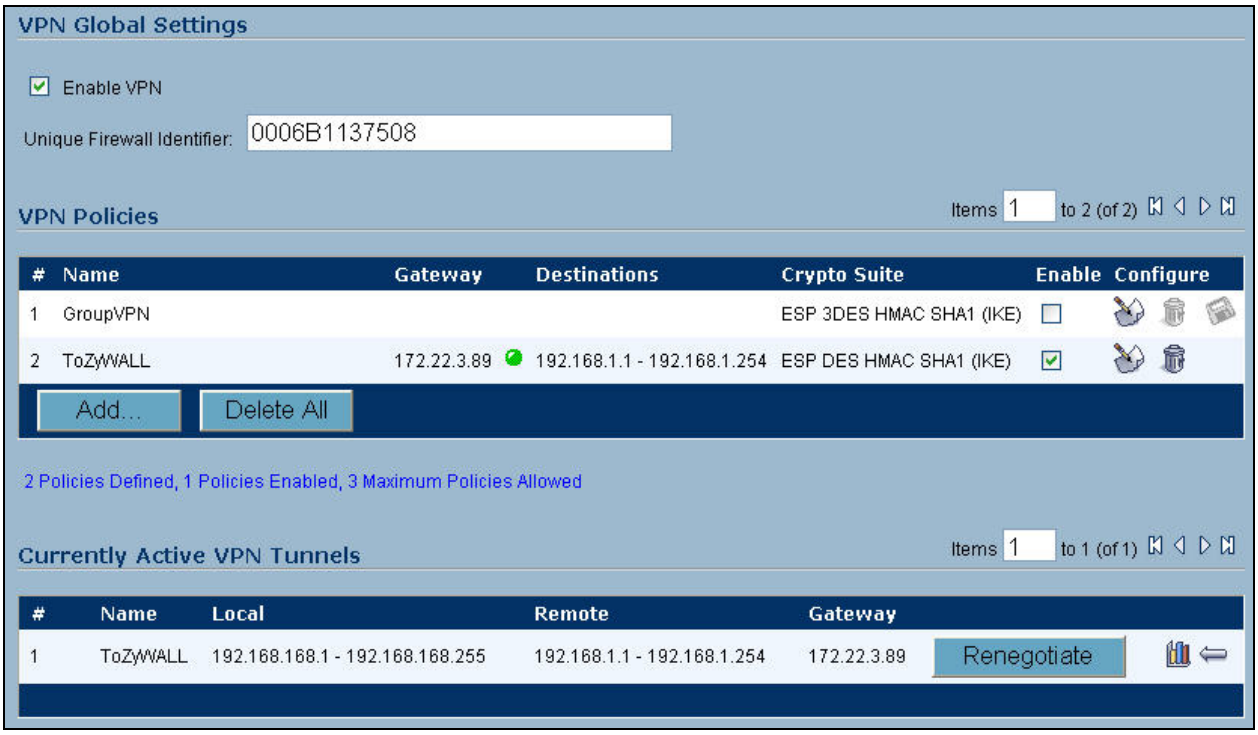
5. Click **Proposals** tab, on IKE(Phase1) proposal settings, select **Main mode**, **DH Group** to **Group1**, **Encryption** to **DES** and **Authentication** to **MD5**. On IPsec(Phase2) proposal settings, select **ESP Protocol**, **Encryption** to **DES** and **Authentication** to **SHA1**. Then, press **OK** button on this page.



6. When you finished doing your settings, you will see the following page.



7. When your VPN tunnel is up, you will see the following page.

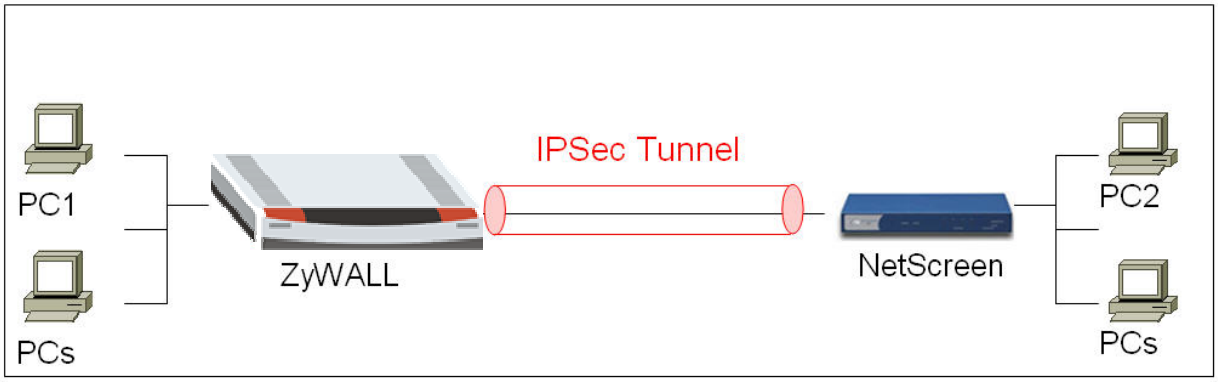


NetScreen with ZyWALL VPN Tunneling

1. Setup ZyWALL VPN
2. Setup NetScreen VPN

This page guides us to setup a VPN connection between the ZyWALL and NetScreen router.

As the figure shown below, the tunnel between PC1 and PC2 ensures the packet flows between them are secure. Because the packets go through the IPSec tunnel are encrypted. To setup this VPN tunnel, the required settings for ZyWALL and NetScreen are explained in the following sections. As the red pipe shown in the following figure, **the tunneling endpoints are ZyWALL router and NetScreen router.**



The IP addresses we use in this example are as shown below.

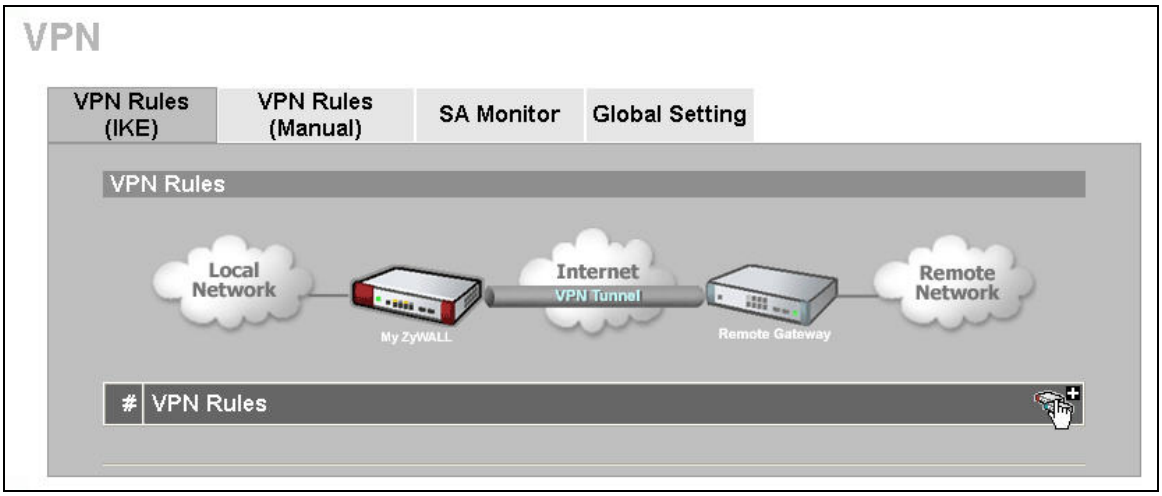
PC 1	ZyWALL	Netscreen	PC2
192.168.2.33	WAN: 172.22.3.89 LAN: 192.168.2.1	WAN: 172.22.1.251 LAN: 192.168.1.1	192.168.1.36

---

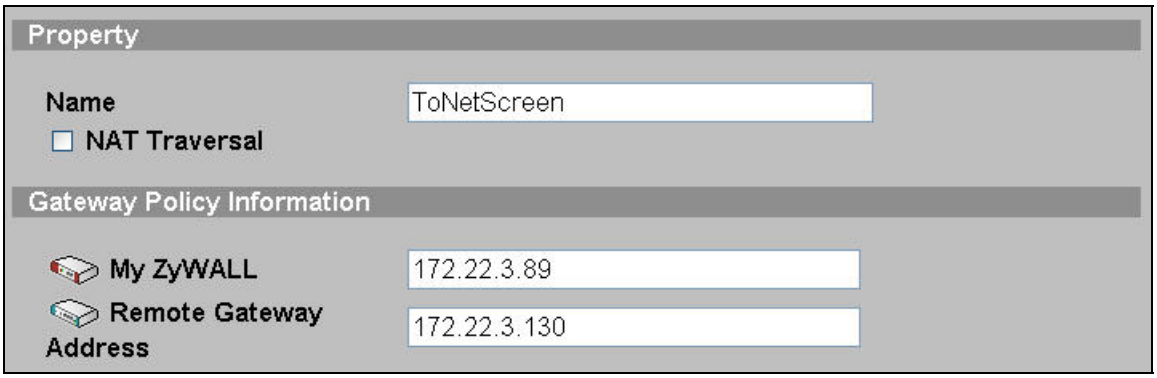
1. Setup ZyWALL VPN

24. Using a web browser, login ZyWALL by giving the LAN IP address of ZyWALL in URL field.

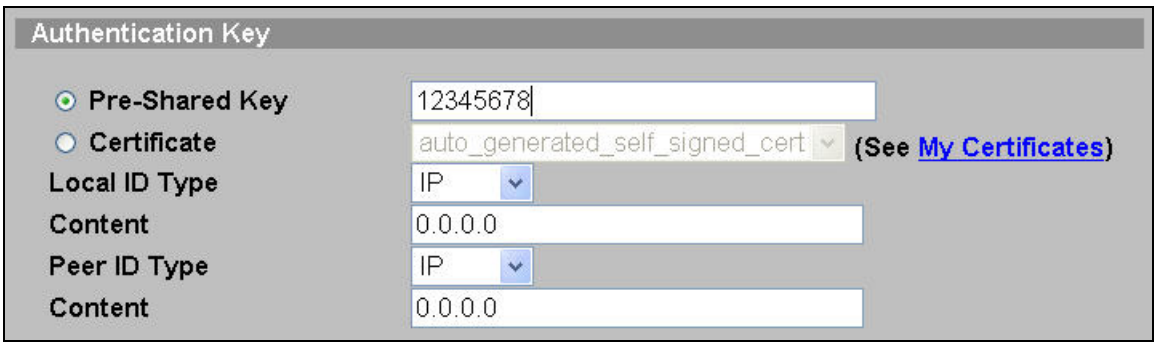
2. Go to SECURITY->VPN->Press **Add** button



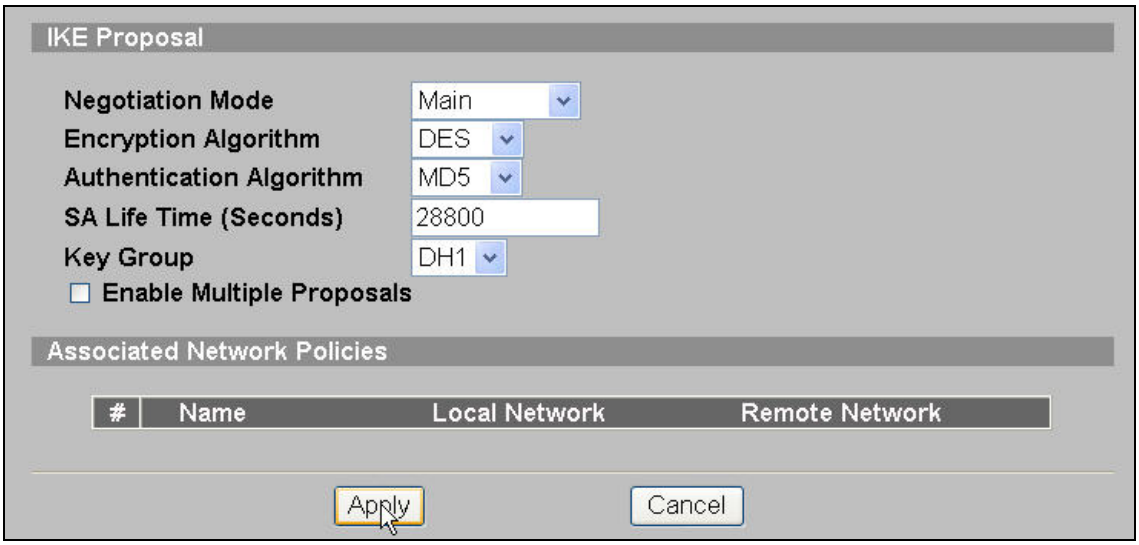
3. Give a name for your policy, for example "**ToNetScreen**"
4. **My IP Addr** is the **WAN IP of ZyWALL**. In this example, you should type 172.22.3.89 IP address on **My ZyWALL** text box.
5. **Secure Gateway IP Addr** is the **NetScreen's WAN IP address**. In this example, you should type 172.22.3.130 IP address on **Remote Gateway** text box.



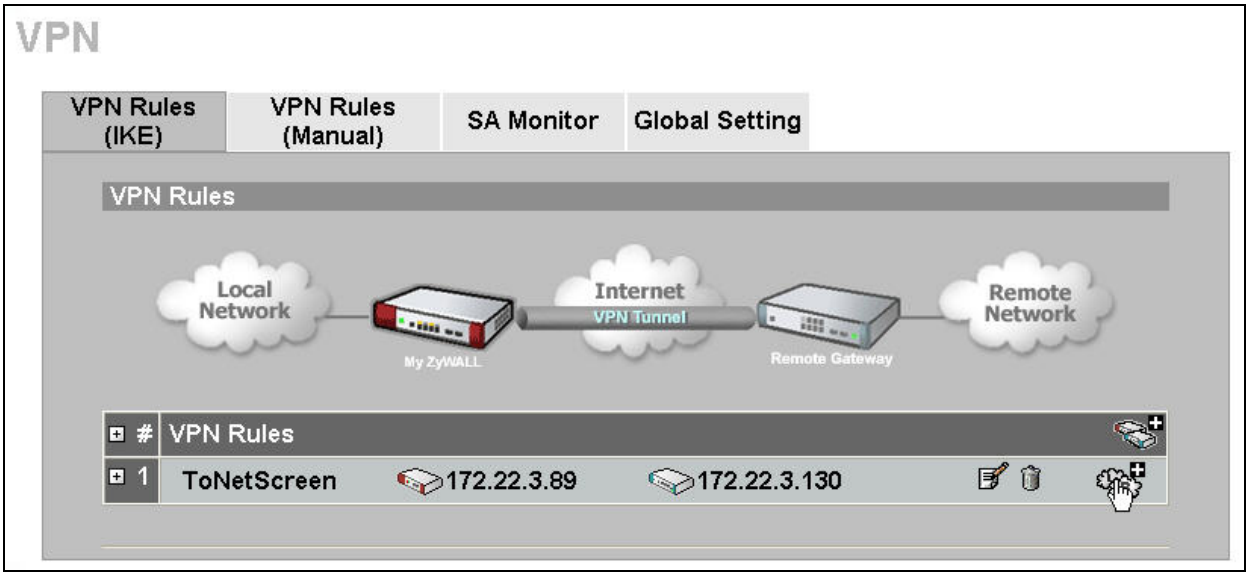
6. In **Authentication Key**, enter the key string **12345678** in the **Pre-Shared Key** text box.



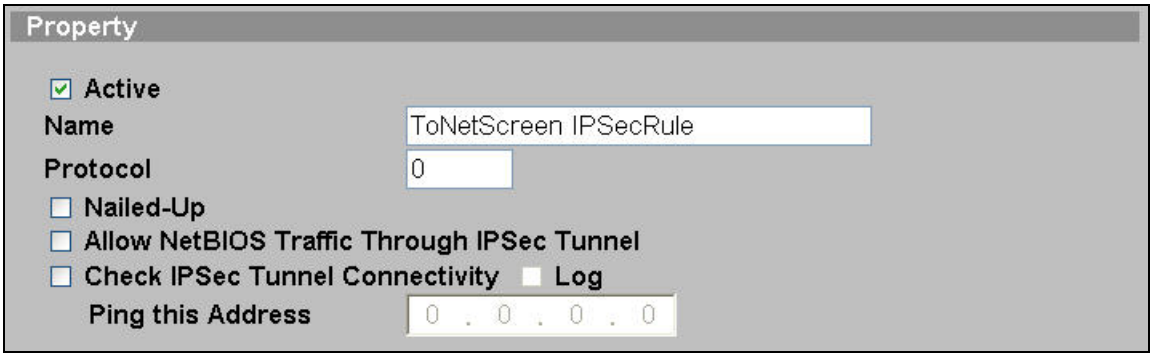
7. Select **Negotiation Mode** to **Main mode**, **Encryption Algorithm** to **DES**, **Authentication Algorithm** to **MD5**, **Key Group** to **DH1,** and then click **Apply** button on this page.



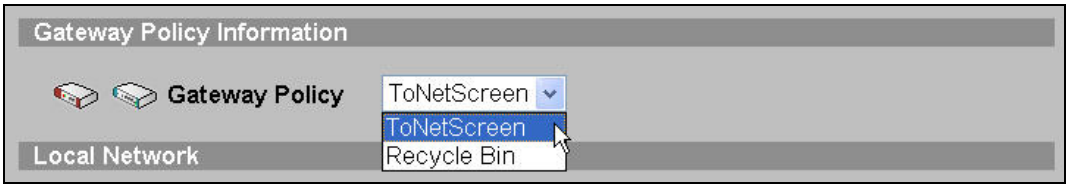
8. You will see an IKE rule on your VPN page, click L/R button to edit your IPSec rule.



9. Check **Active** check box and give a name to this policy.

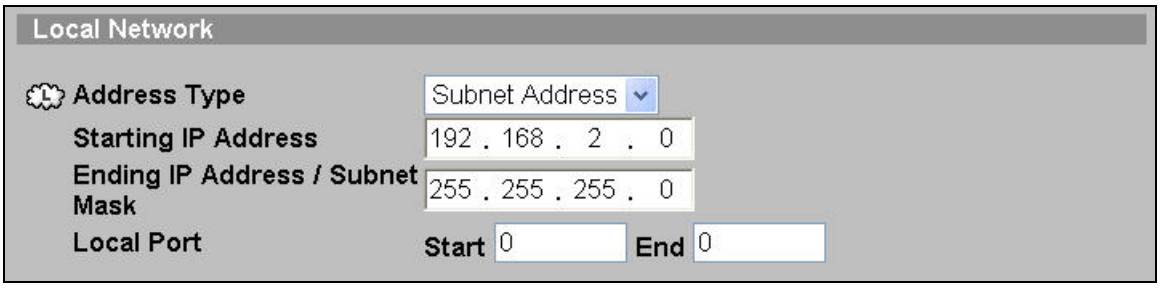


10. On Gateway Policy Information, you should choose **ToNetScreen** IKE policy for your IPSec rule.

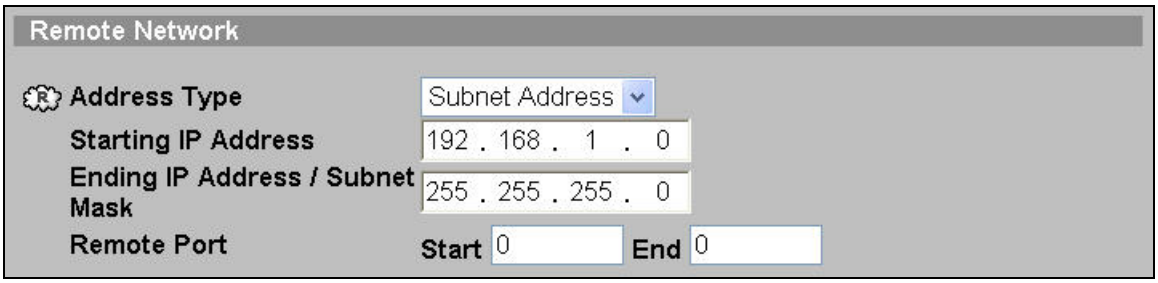


11. On **Local Network,** choose **Subnet Address** for your **Address Type. Starting IP Address** and **Ending IP Address/Subnet** are your local site LAN IP addresses. In this example, you should

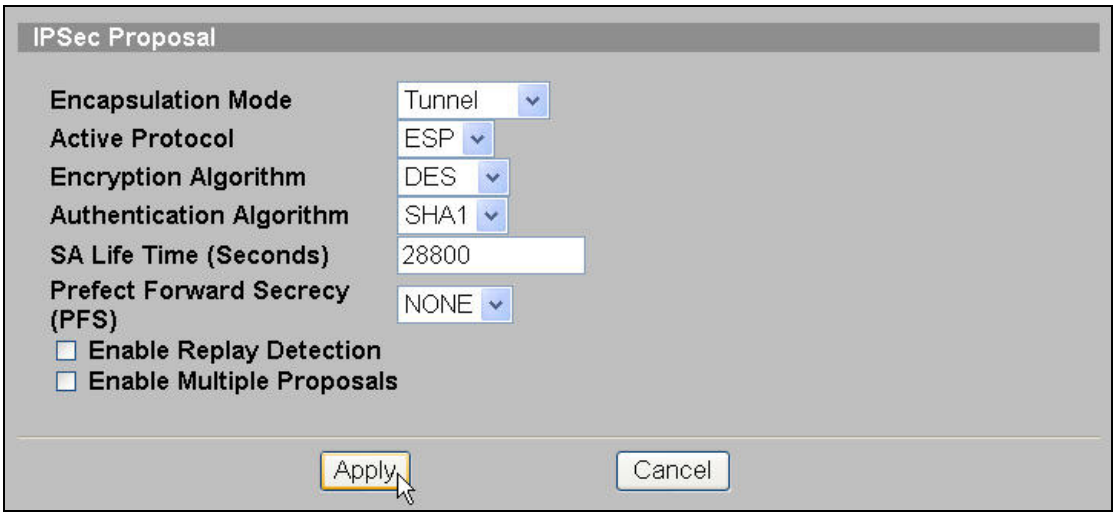
type 192.168.2.0 on **Starting IP Address** field and then type 255.255.255.0 on **Ending IP Address/Subnet** field.



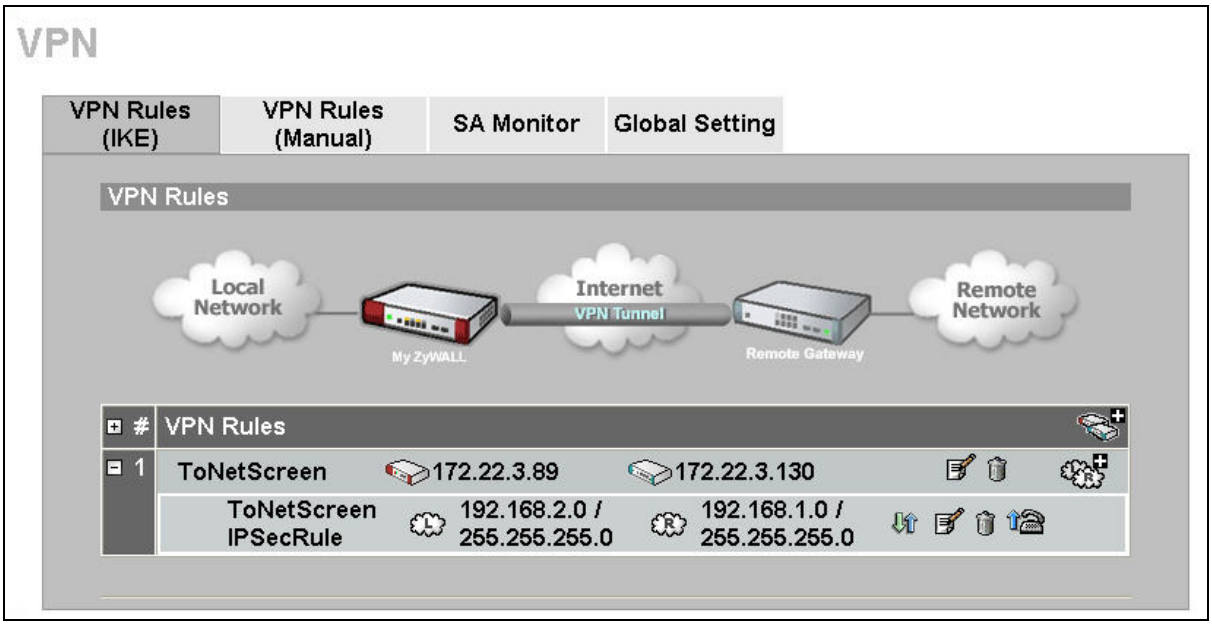
12. On **Remote Network,** choose **Subnet Address** for your **Address Type. Starting IP Address** and **Ending IP Address/Subnet** are your remote site LAN IP addresses. In this example, you should type 192.168.1.0 on **Starting IP Address** field and then type 255.255.255.0 on **Ending IP Address/Subnet** field.



13. On **IPSec Proposal,** select **Encapsulation Mode** to **Tunnel, Active Protocol** to **ESP, Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA1**, and then press Apply button on this page.



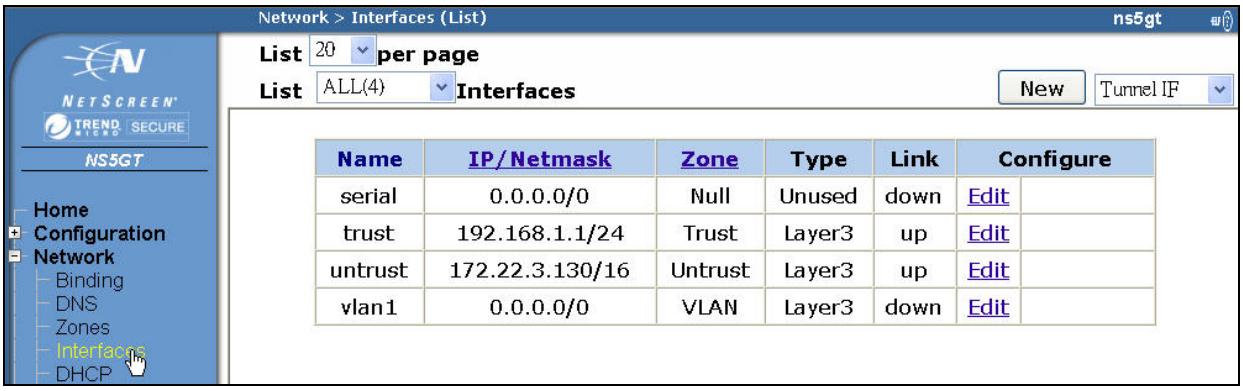
14. When you finished doing your settings, you will see the following page.



2. Setup NetScreen VPN (We choose NetScreen-5GT device in this example.)

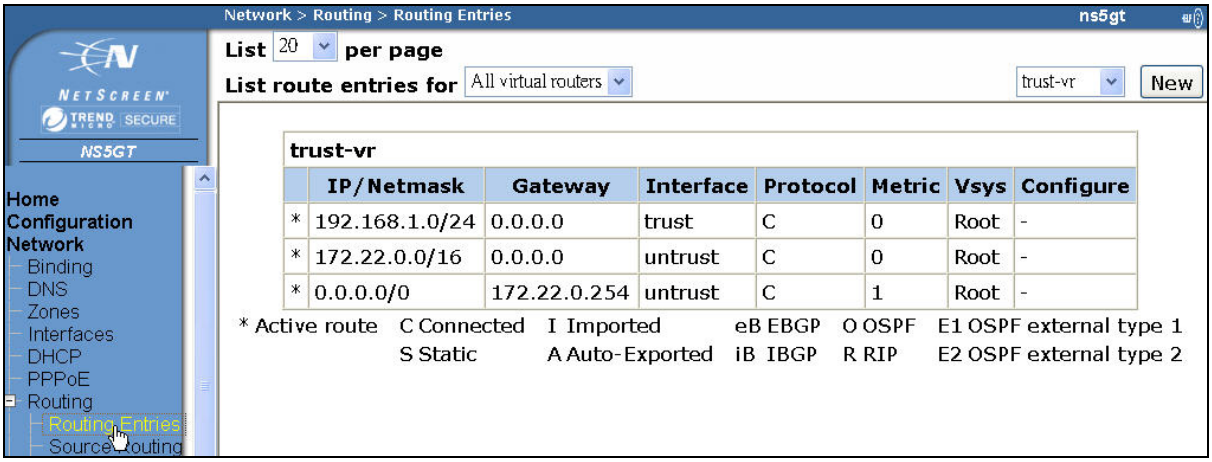
3. Using a web browser, login NetScreen by giving the LAN IP address of NetScreen in URL field.
4. **Check your WAN/LAN IP address**

Click **Network** -> **Interfaces**, the **trust IP/Netmask** used for **LAN**, the **untrust IP/Netmask** used for **WAN**.



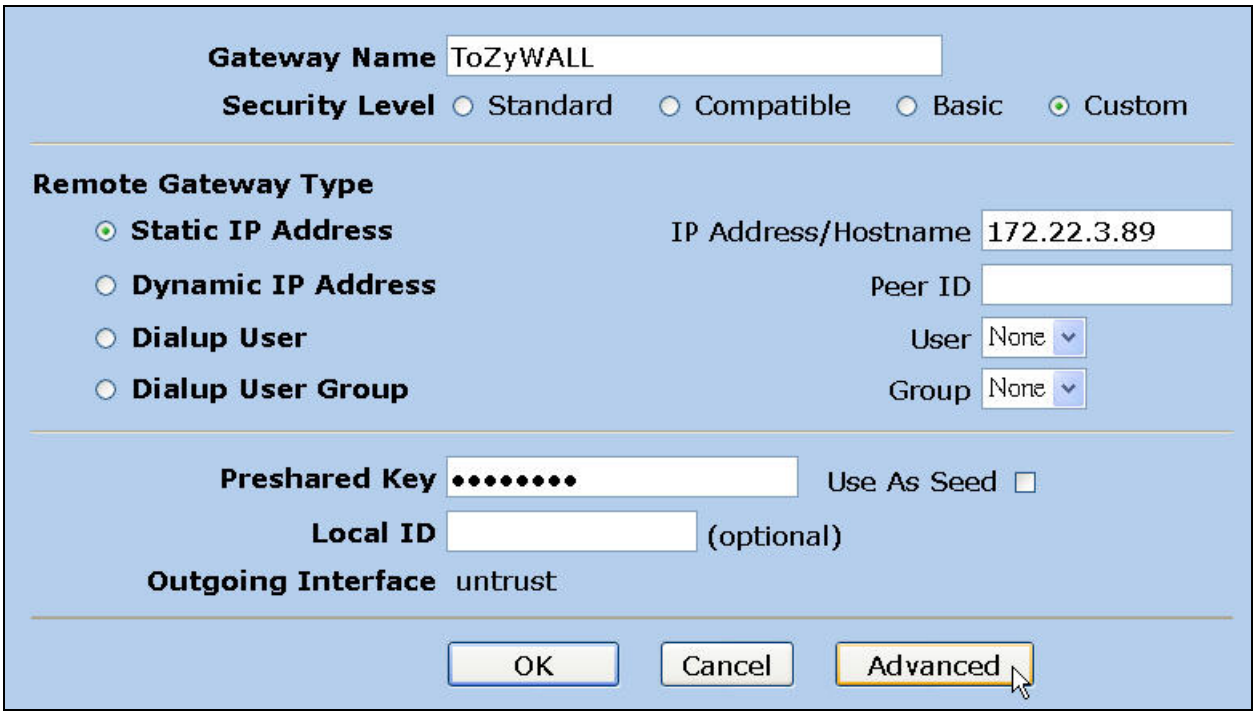
Note: About the settings, you could reference to NetScreen user guide to get the detail info.

5. If you set a static IP address for your WAN port, you should click Network -> Routing -> Routing Entries to edit your Gateway IP address. In this example, my Gateway IP address is 172.22.0.254.

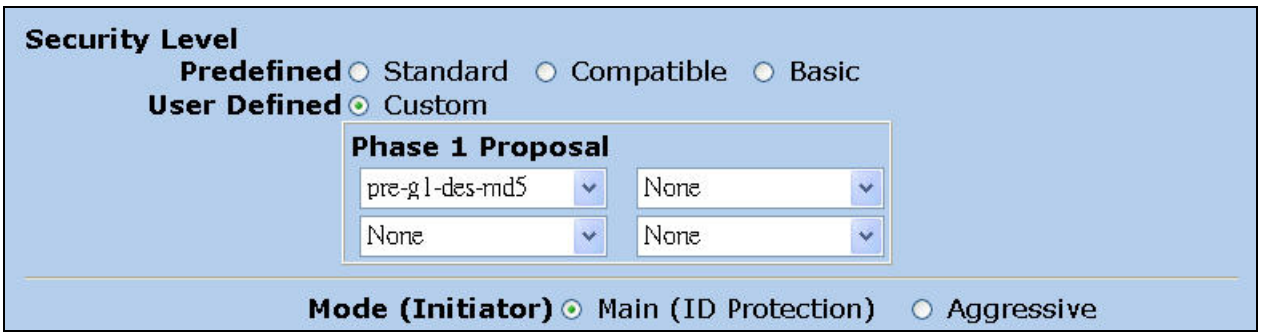


6. To edit your IPSec rule, click **VPNs** -> **AutoKey Advanced** -> **Gateway**, and then press **New** button to edit your IKE rules.

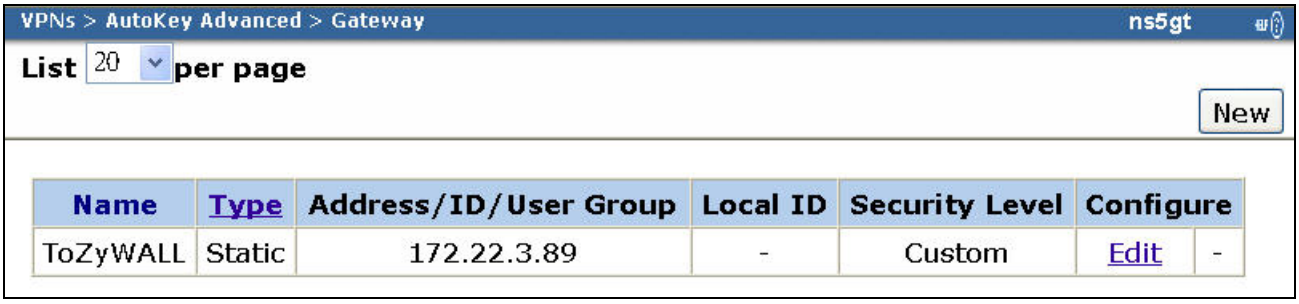
7. Give a name for your policy, for example "**ToZyWALL**". **Remote Gateway IP Addr** is the **ZyWALL's WAN IP address.** In this example, select **Static IP Address** option and set **172.22.3.89** on the text box. Enter the key string **12345678** on **Preshared Key** text box, and then press **Advanced** button to edit the advanced settings.



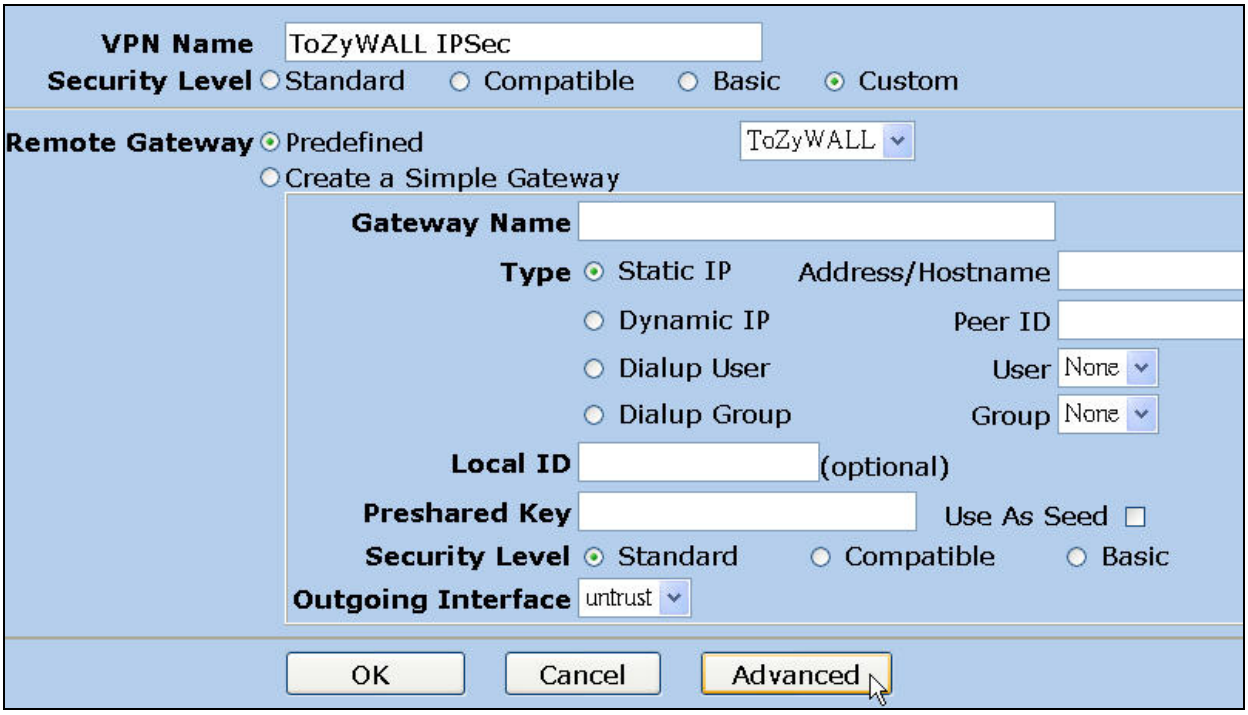
6. On Security Level settings, you could set up phase 1 IKE rules. In this example, select User Defined, and choose pre-g1-des-md5 rule. The pre-g1-des-md5 means `Pre-Share Key`, `group1`, **DES** for **Encryption Algorithm** and **MD5** for **Authentication Algorithm**. Select Main (ID Protection) option for Mode (Initiator). Then, press Return button, and press OK button on next page to save your settings.



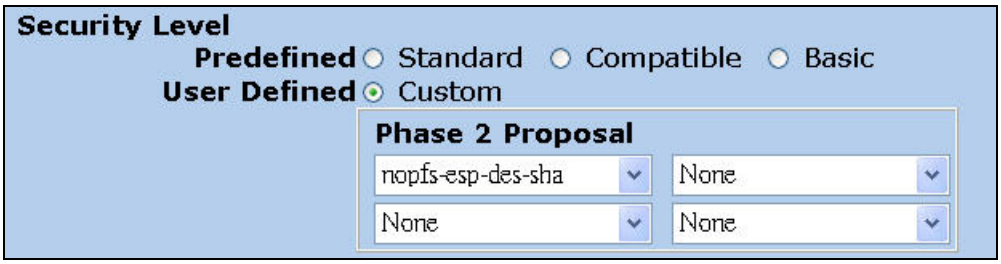
7. When you finished doing the settings, you will see an IKE rule on the page.



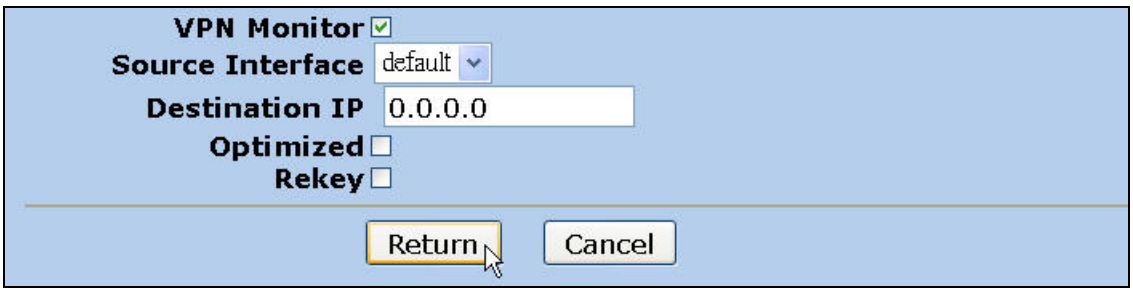
8. To edit your IPSec rule, click **VPNs** -> **AutoKey IKE**, and then press **New** button to edit your IPSec rules.
9. Give a name for your VPN, for example "**ToZyWALL IPSec**". On Remote Gateway, choose Predefined option and select ToZyWALL rule. Then, press **Advanced** button to edit the advanced settings.



10. On **Security Level** settings, choose **User Defined** option, and choose **nopfs-esp-des-sha** rule on **Phase 2 Proposal**. The **nopfs-esp-des-sha** means no PFS, **ESP Protocol, Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA1**.

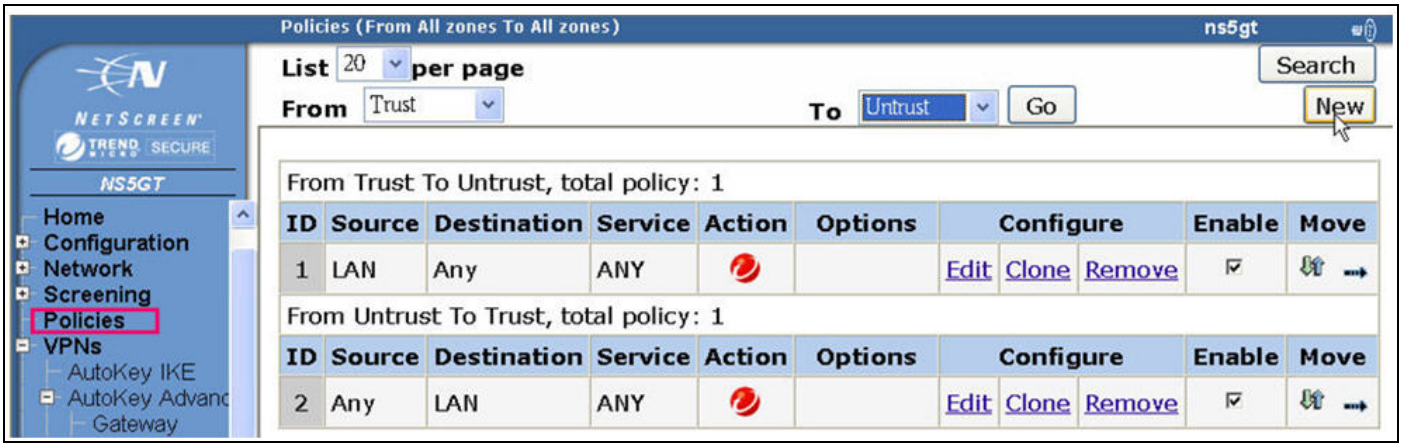


11. Check **VPN Monitor** check box, thus you can monitor your VPN tunnels. Then, press Return button, and press OK button on next page to save your settings.



12. When you finished doing the settings, you will see an IPSec rule on the page.

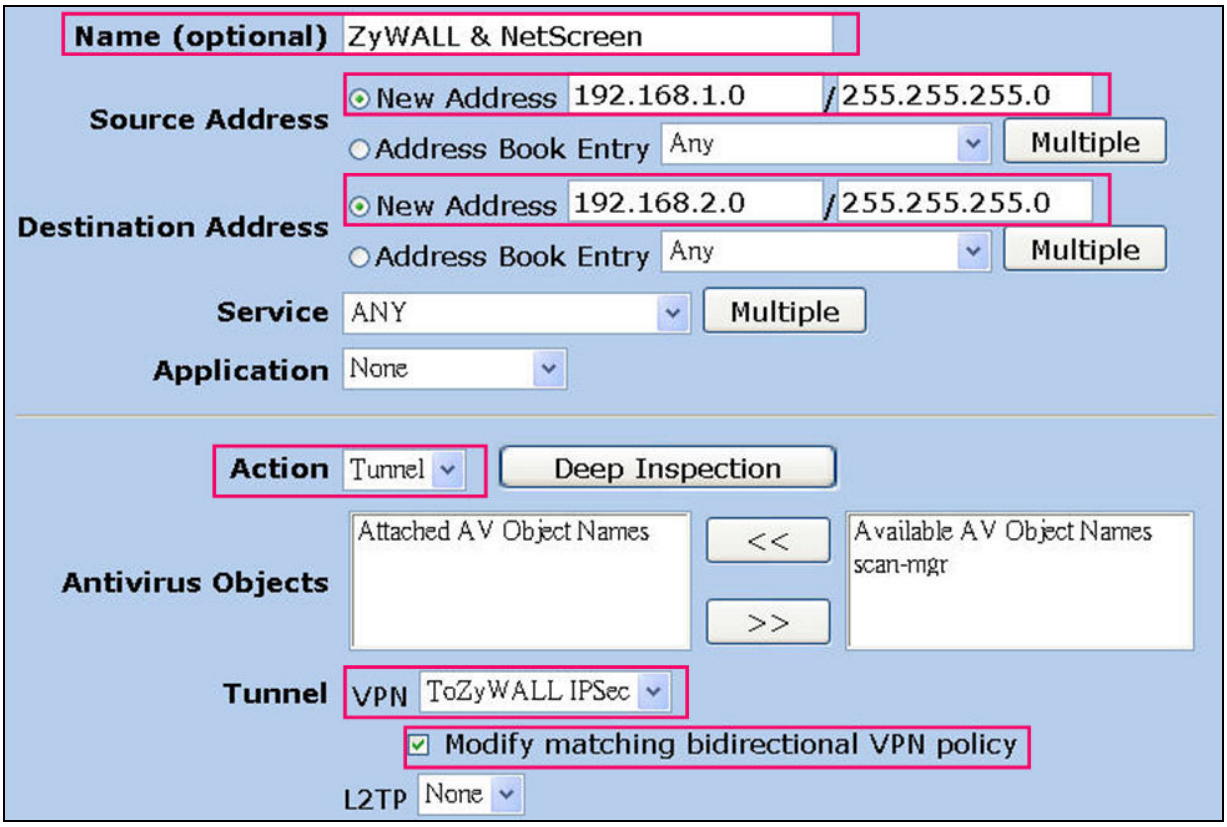
13. On your main page, click **Policies** to set up your policy rules. To choose **From** to **Trust**, and **To** to **Untrust** (it means from LAN to WAN), and then press **New** button to edit your policy rules.



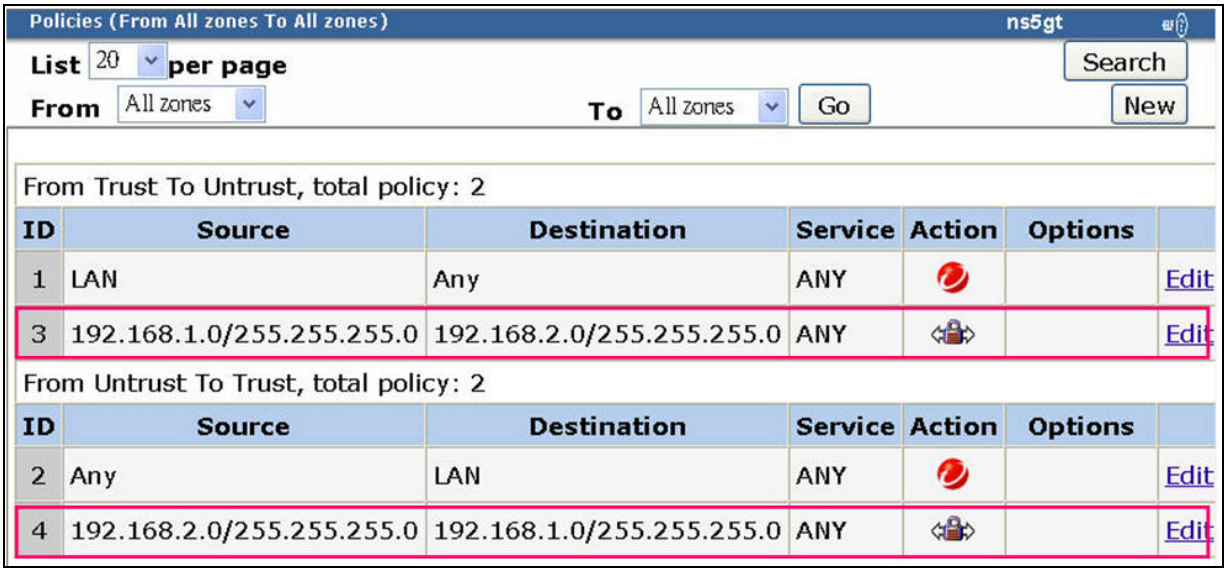
14. Give a name for your policy, for example "**ZyWALL & NetScreen**".

15. On **Source Address**, you should set up Local LAN IP addresses. In this example, select **New Address** option, and type **192.168.1.0 / 255.255.255.0** on the text box. On **Destination Address**, you should set up remote IP addresses. In this example, select **New Address** option, and type **192.168.2.0 / 255.255.255.0** on the text box.

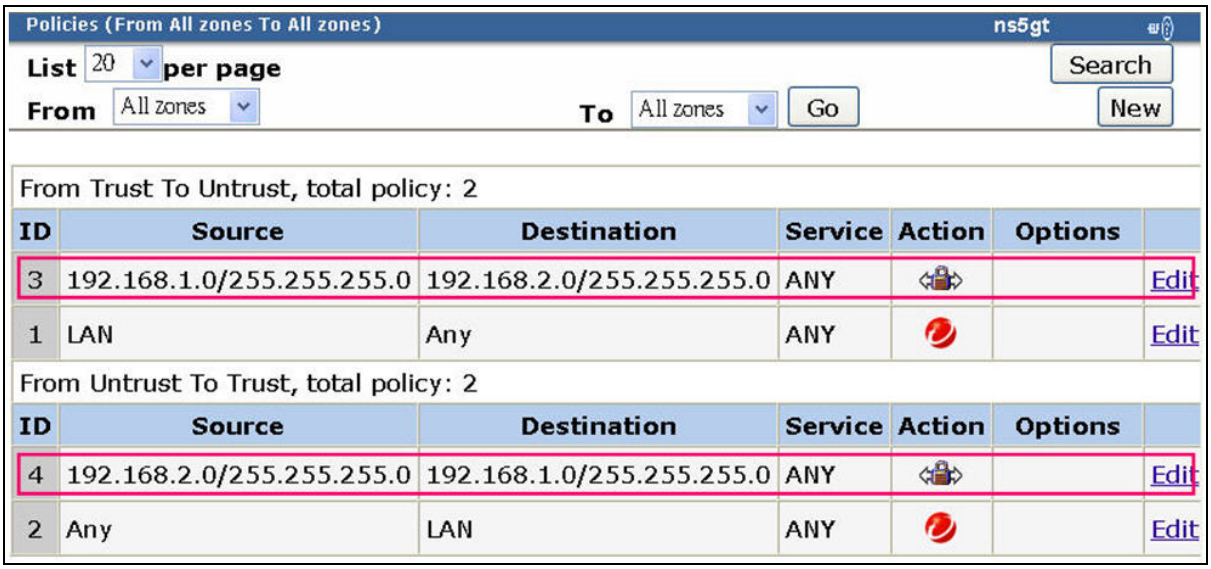
16. Select **Action** to **Tunnel**, and select **ToZyWALLIPSec**VPN rule. Check **Modify matching bidirectional VPN policy** check box, it means that you can create/modify the VPN policy for the opposite direction. Then, press **OK** button to save your settings.



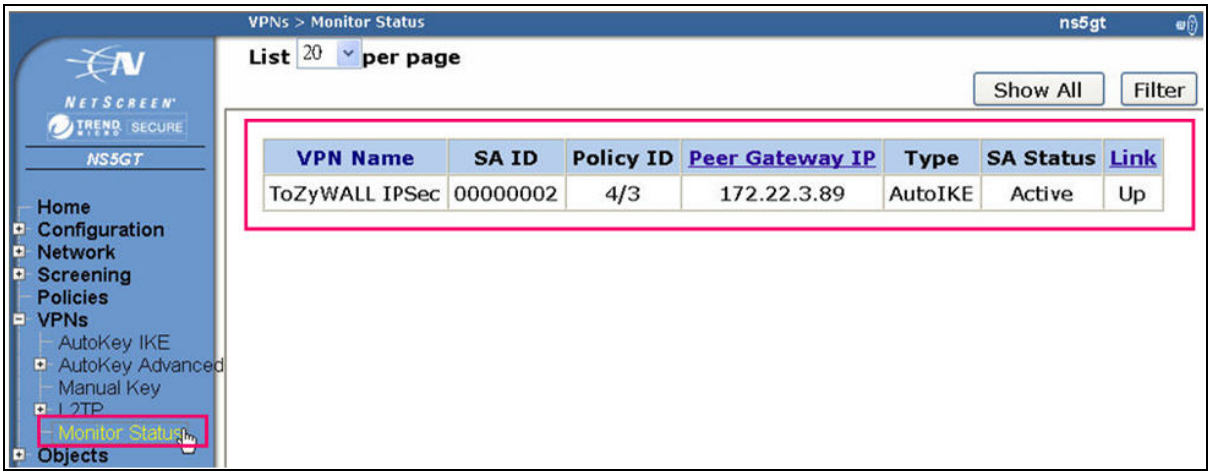
17. When you finished doing the settings, you will see the policy rules on the page.



18. Move your policy rules to top, thus your device will check the rule at first.



19. Click VPNs -> Monitor Status, this page displays a table that lists all the VPN groups configured on the NetScreen device. You could check the link states to know your VPN tunnel is up or down.

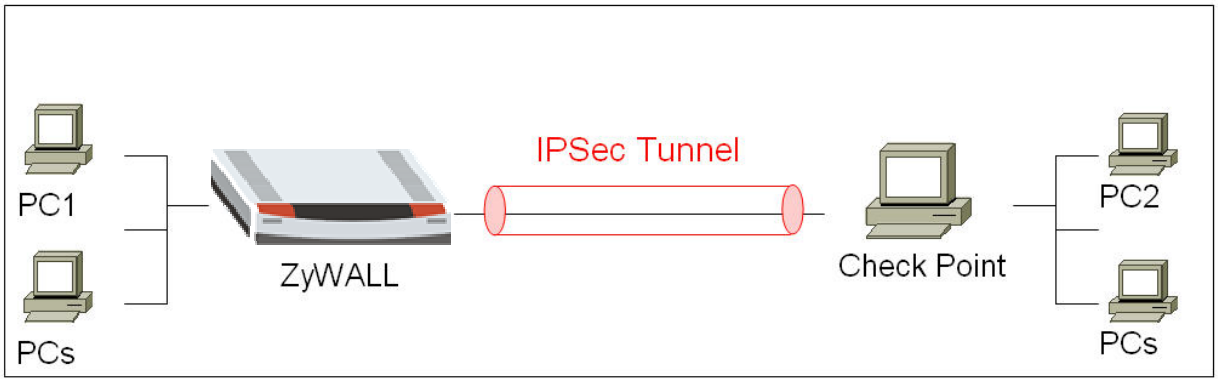


Check Point with ZyWALL VPN Tunneling

1. Setup ZyWALL VPN
2. Setup Check Point VPN

This page guides us to setup a VPN connection between the ZyWALL and a PC which uses Check Point software.

As the figure shown below, the tunnel between PC1 and PC2 ensures the packet flows between them are secure. Because the packets go through the IPSec tunnel are encrypted. To setup this VPN tunnel, the required settings for ZyWALL and Check Point are explained in the following sections. As the red pipe shown in the following figure, **the tunneling endpoints are ZyWALL router and a PC which uses Check Point software.**

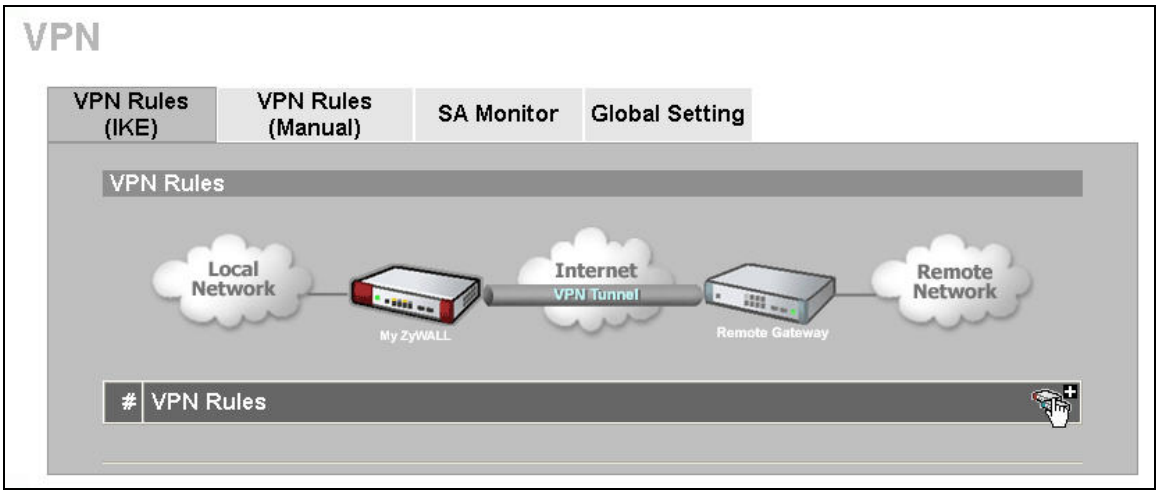


The IP addresses we use in this example are as shown below.

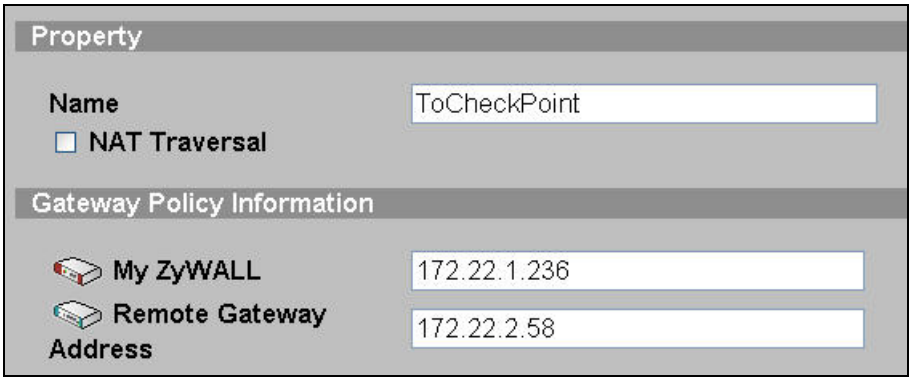
ZyWALL	Check Point
WAN: 172.22.1.236 LAN: 192.168.1.0/24	WAN: 172.22.2.58 LAN: 192.168.2.0/24

1. Setup ZyWALL VPN

1. Using a web browser, login ZyWALL by giving the LAN IP address of ZyWALL in URL field. Default LAN IP is **192.168.1.1**, default password to login web configurator is **1234**.
2. Go to SECURITY->VPN->Press **Add** button

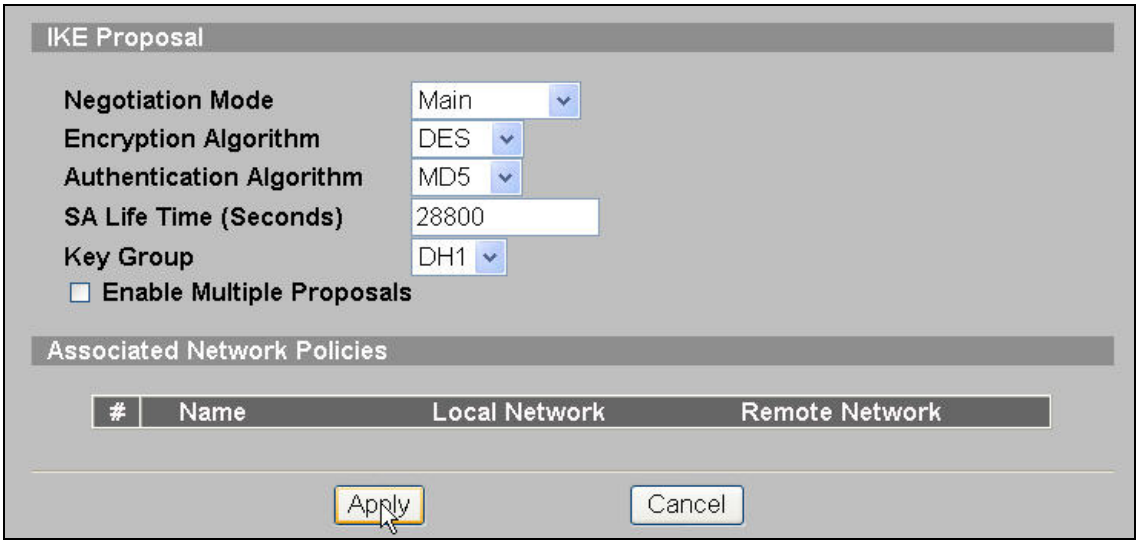


3. Give a name for your policy, for example "**ToCheckPoint**"
4. **My IP Addr** is the **WAN IP of ZyWALL**. In this example, you should type 172.22.1.236 IP address on **My ZyWALL** text box.
5. **Secure Gateway IP Addr** is the **remote PC's IP address**. In this example, you should type 172.22.2.58 IP address on **Remote Gateway** text box.



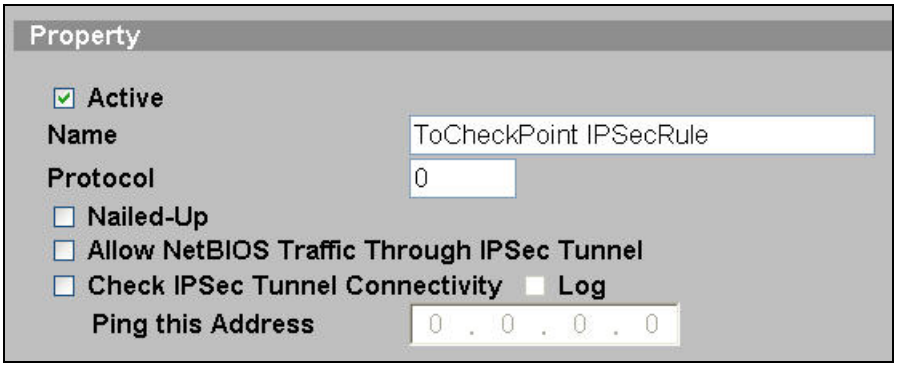
6. In **Authentication Key**, enter the key string **12345678** in the **Pre-Shared Key** text box.

7. Select **Negotiation Mode** to **Main mode**, **Encryption Algorithm** to **DES**, **Authentication Algorithm** to **MD5**, **Key Group** to **DH1**, and then press **Apply** button on this page.

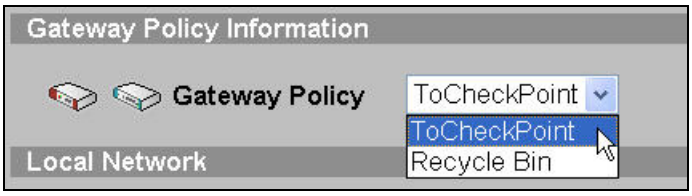


8. After you press the **Apply** button, you will see an IKE rule on this page, press L/R button to edit your

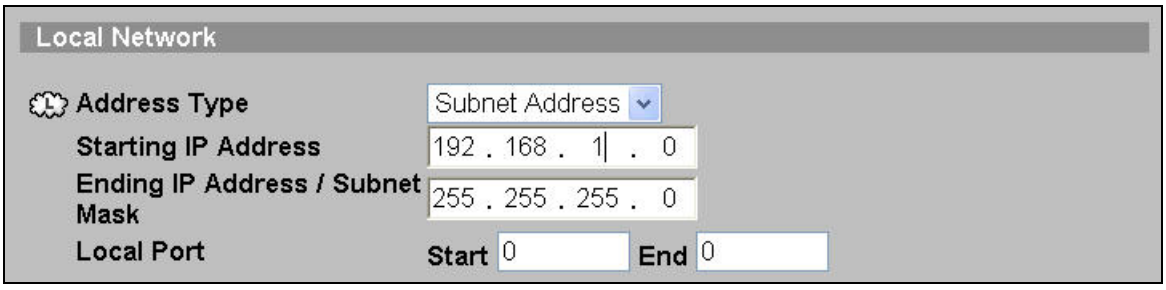
9. Check **Active** check box and give a name to this policy.



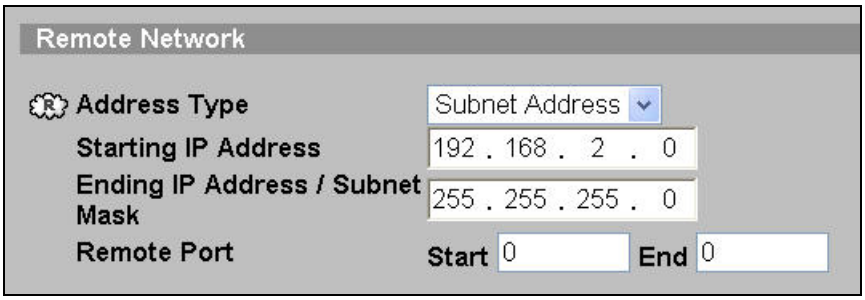
10. On Gateway Policy Information, you should choose **ToCheckPoint** IKE policy for your IPSec rule.



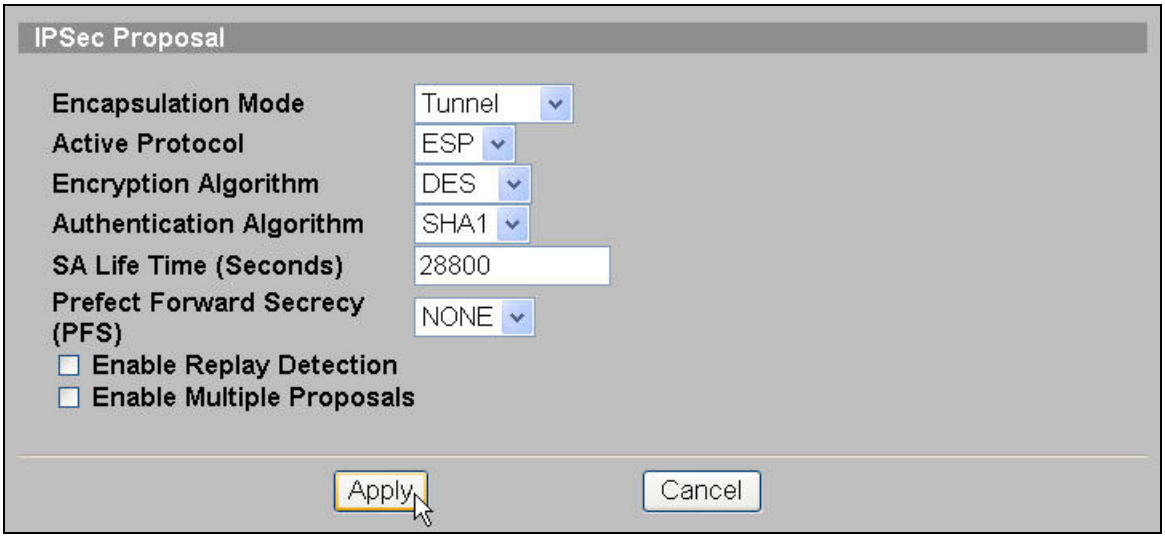
11. On **Local Network,** choose **Subnet Address** for your **Address Type. Starting IP Address** and **Ending IP Address/Subnet** are your local site LAN IP addresses. In this example, you should type 192.168.1.0 on **Starting IP Address** field and then type 255.255.255.0 on **Ending IP Address/Subnet** field.



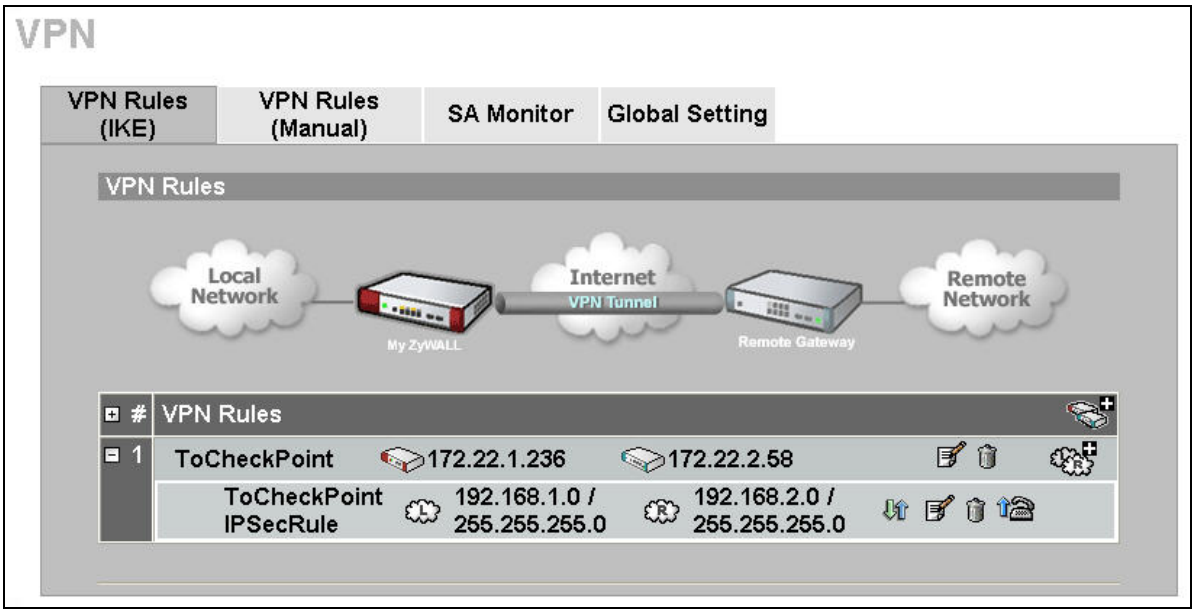
12. On **Remote Network,** choose **Subnet Address** for your **Address Type. Starting IP Address** and **Ending IP Address/Subnet** are your remote site LAN IP addresses. In this example, you should type 192.168.2.0 on **Starting IP Address** field and then type 255.255.255.0 on **Ending IP Address/Subnet** field.



13. On **IPSec Proposal,** select **Encapsulation Mode** to **Tunnel, Active Protocol** to **ESP, Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA1**, and then press Apply button on this page.

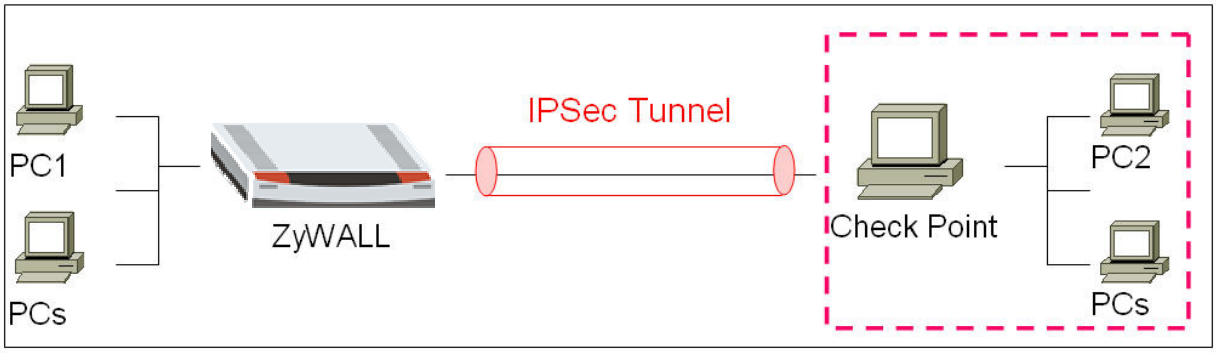


14. After you press the **Apply** button, you will see the following page.



2. Setup CheckPoint VPN

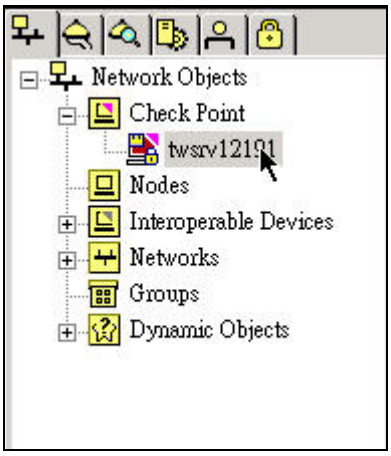
I. Setup Network Objects



1. on your PC, clicking Start->Programmer->Check Point SmartConsole R60 -> SmartDashboard

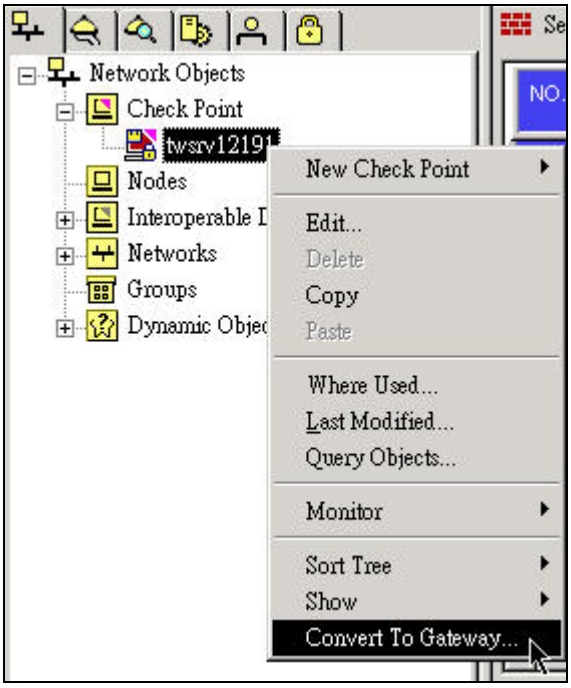
2. Enter your user name and password, then press OK button to use your Check Point.

3. On Network Objects, you must see a default check point object here. For this example, my default check point object is **twsrv12191**, double click the object to check its settings.

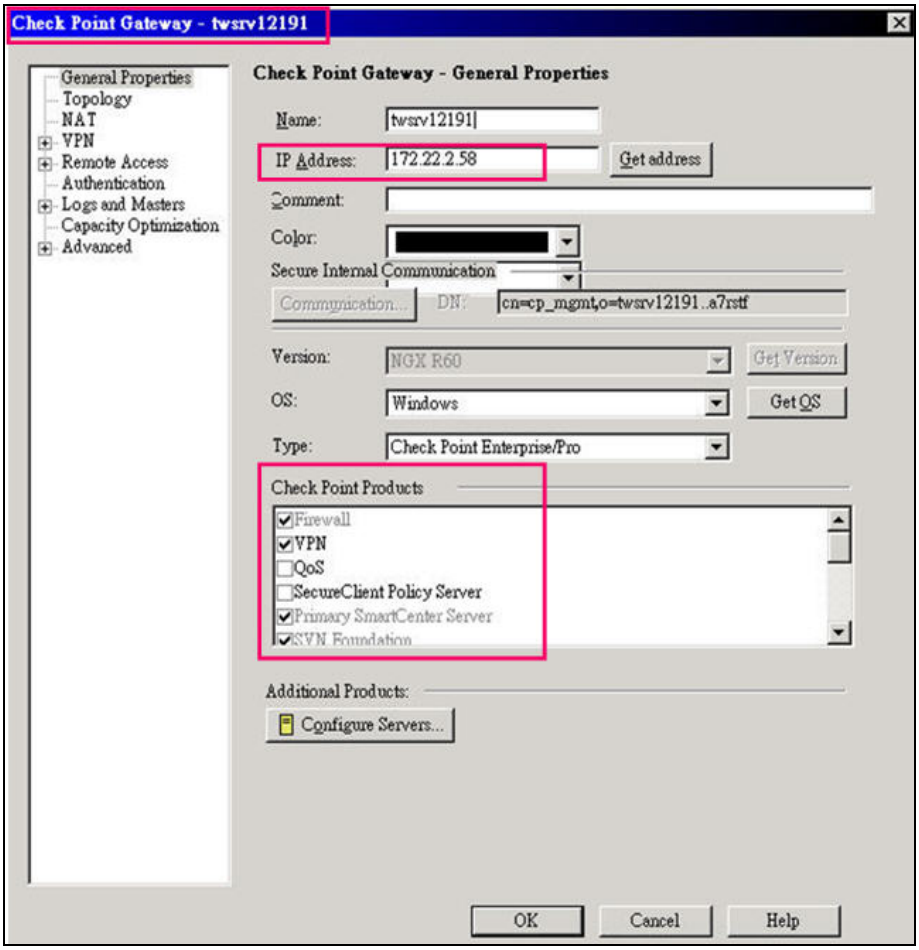


4. Before you did the settings, you should make sure that your object is a **Check Point Gateway**.(not a Check Point Host)

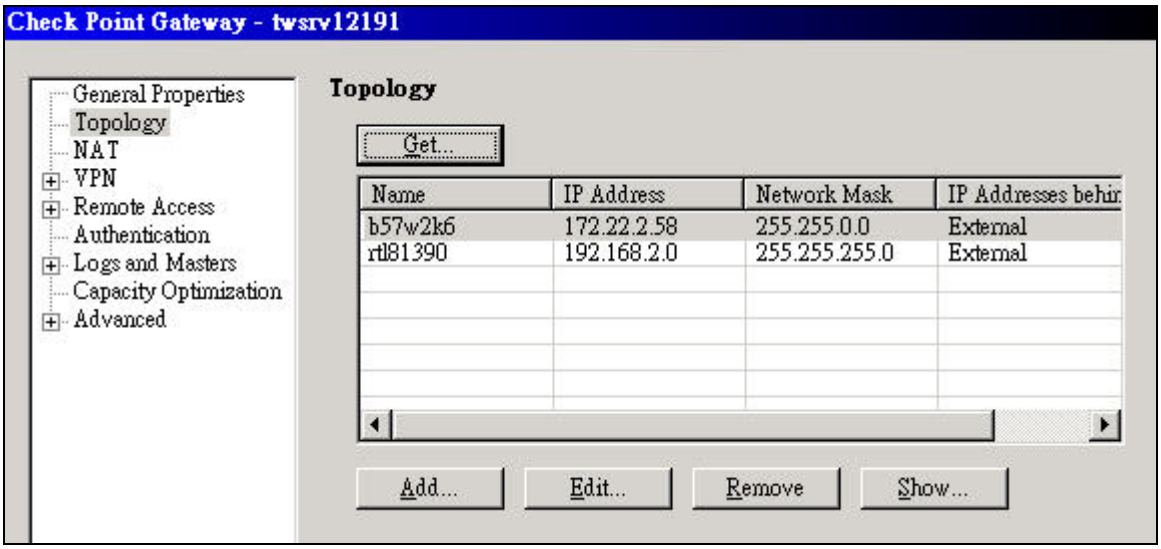
5. If your check point object is a Check Point Host, select your object and click the right button on your mouse, then choose **Convert To Gateway** to change its settings.



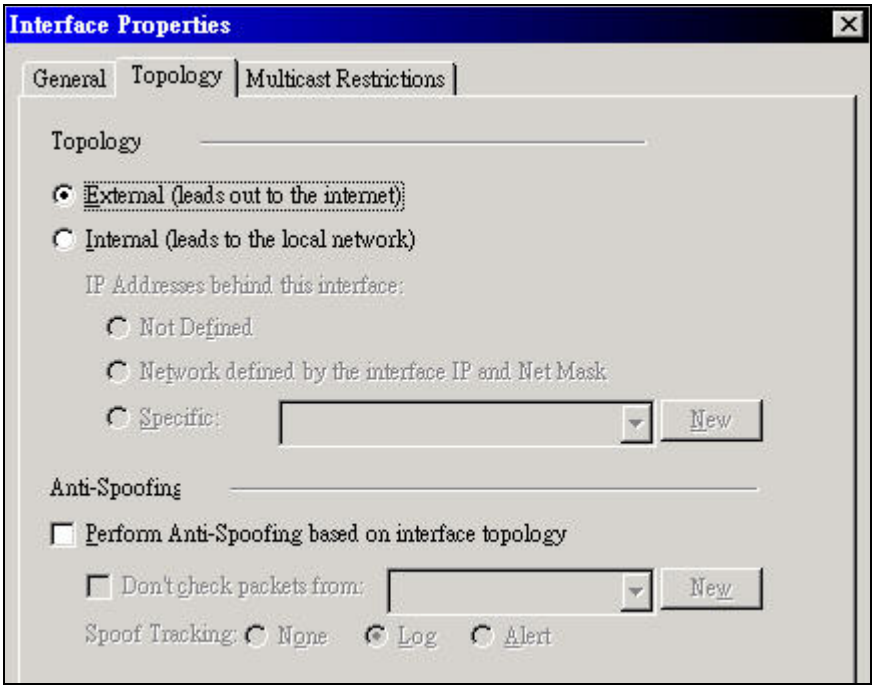
6. On **General Properties**, the **IP Addrrss** field is the **WAN IP of your PC**. In this example, you should type **172.22.2.58** IP address on the text box. On **Check Point Products** settings, check **VPN** check box here.



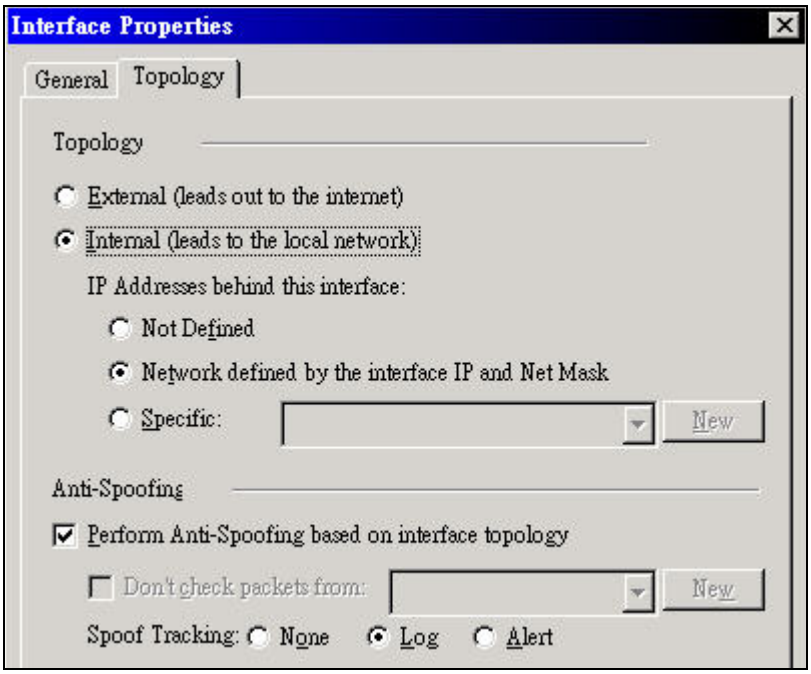
7. On **Topology** settings, you should see two interfaces of IP settings here if your PC has two network cards.



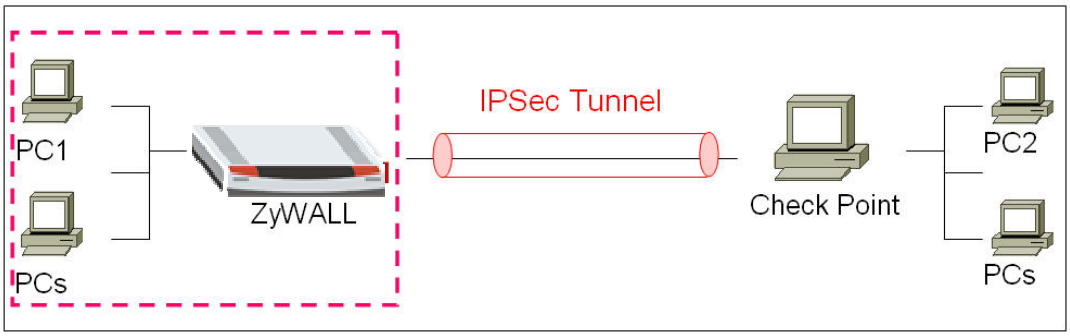
8. Selecting **172.22.2.58 interface**, and press **Edit** button to check its settings. Clicking **Topology** screen, choose **External (leads out to the internet)** for the interface. Then, press OK button to save the settings.



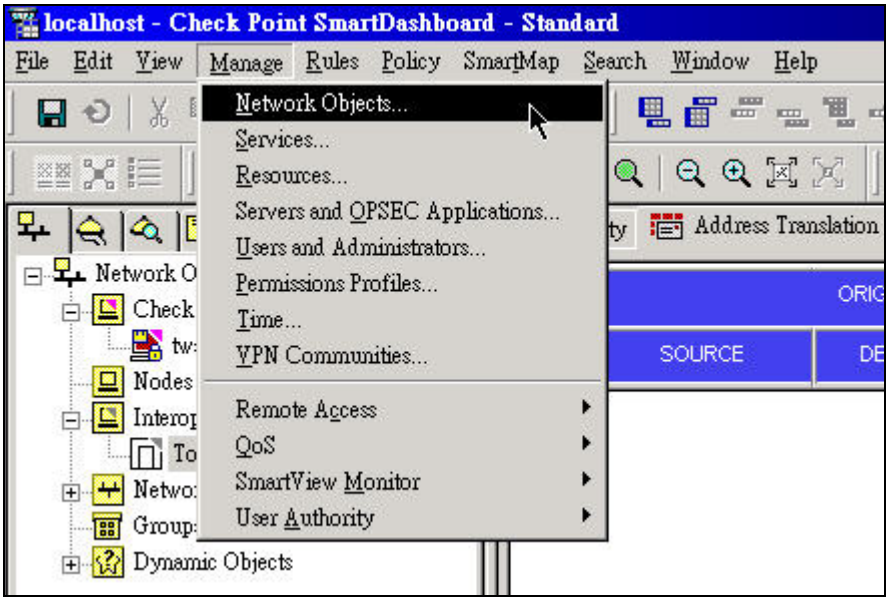
9. Selecting **192.168.2.0 interface**, and press **Edit** button to check its settings. Clicking **Topology** screen, choose **Internal (leads to the local network)** and **Network defined by the interface IP and Net Mask** for the interface, then press **OK** button to save the settings.



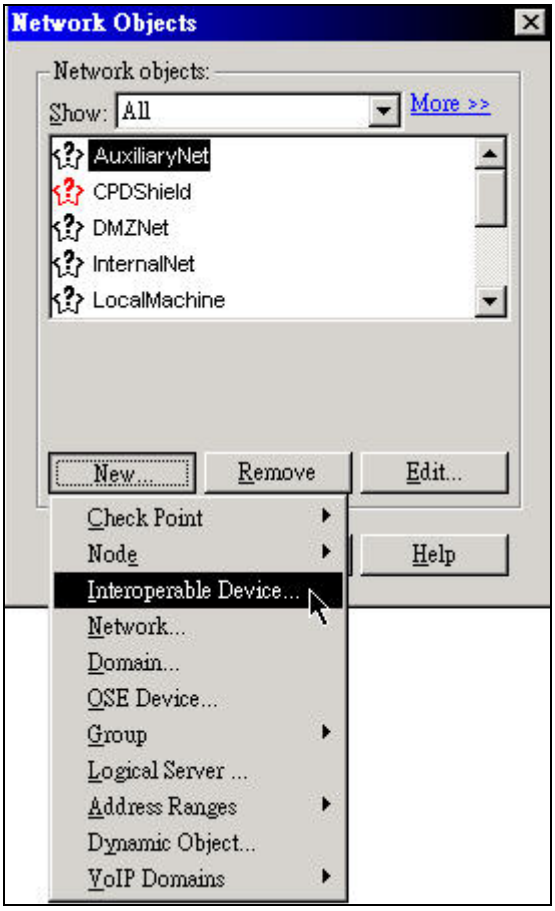
II. Setup Interoperable Device



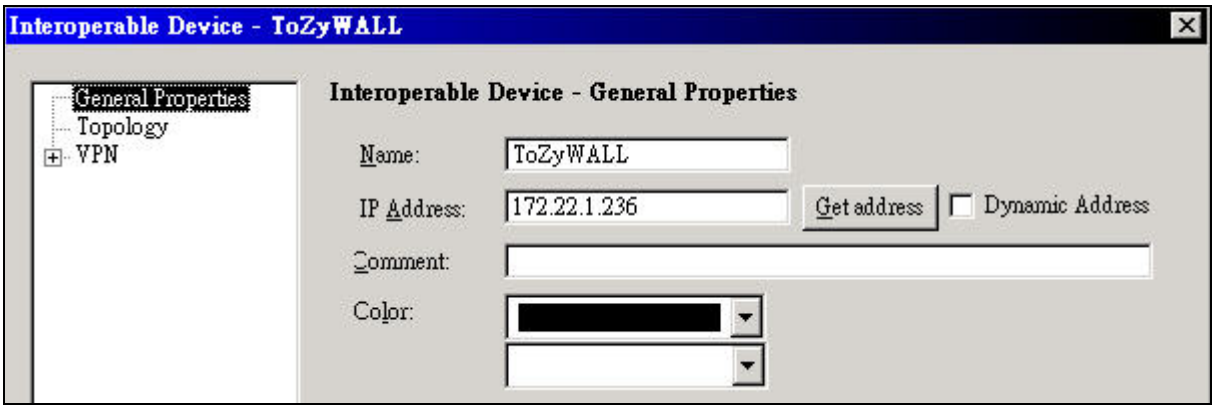
10. On the main menu, click **Manage** -> **Network Objects**.



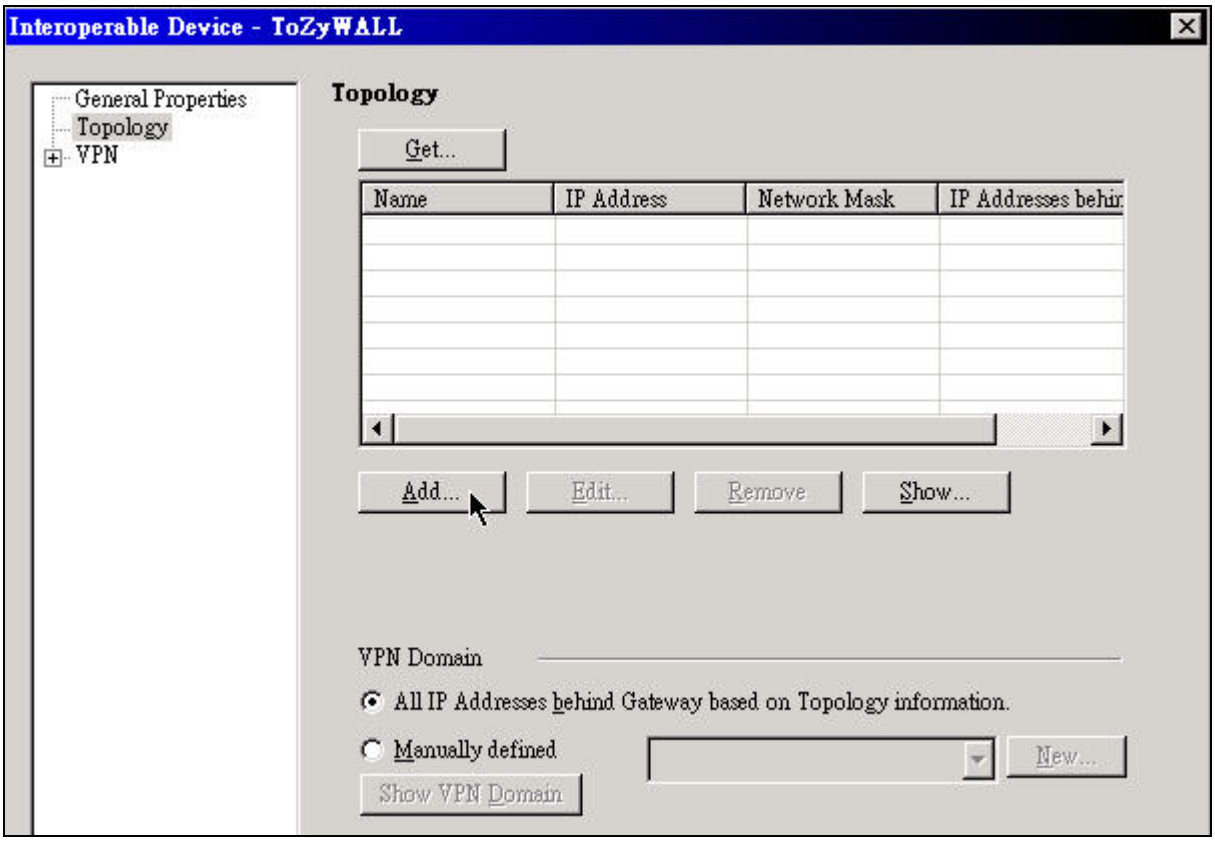
11. You will see the network objects window, press **new** button and select **Interoperable Device**.



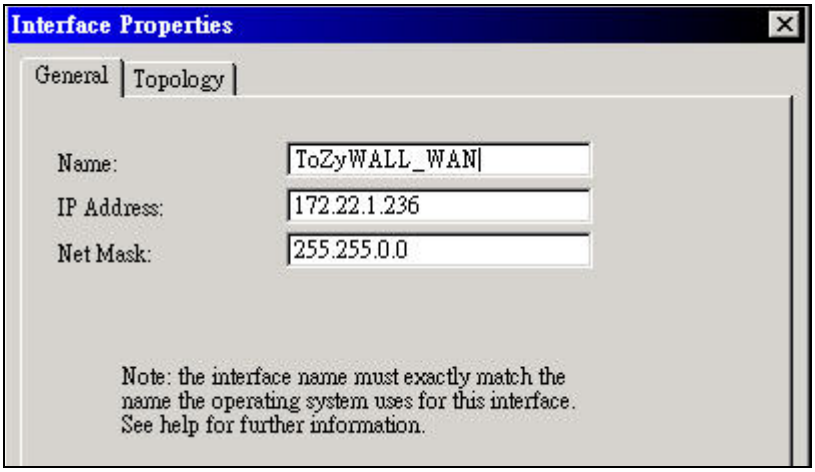
12. On **General Properties** settings, give a name and an IP address for the Interoperable Device. In this example, the IP address is ZyWALL's WAN IP address.



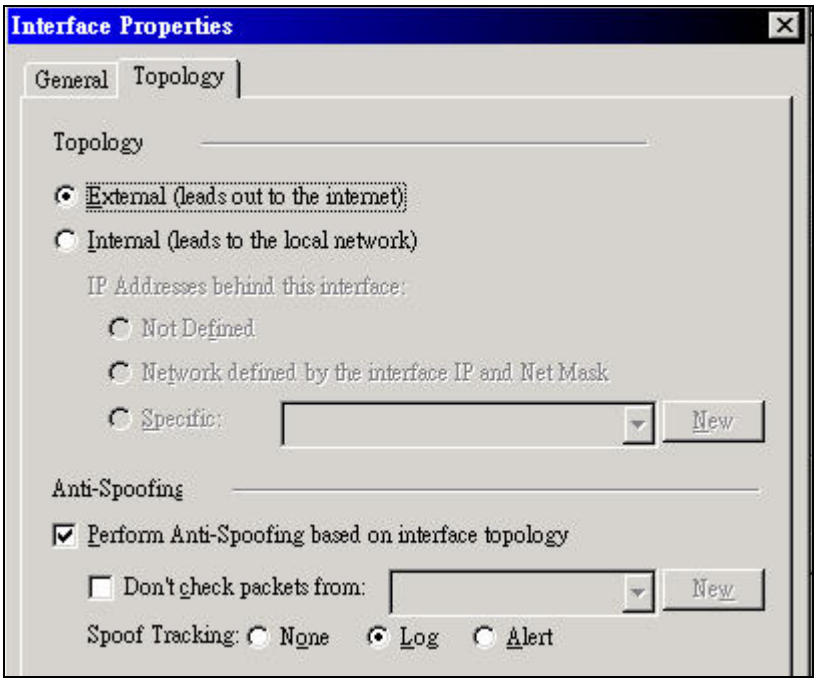
13. On **Topology** settings, pressing **Add** button to add a new interface.



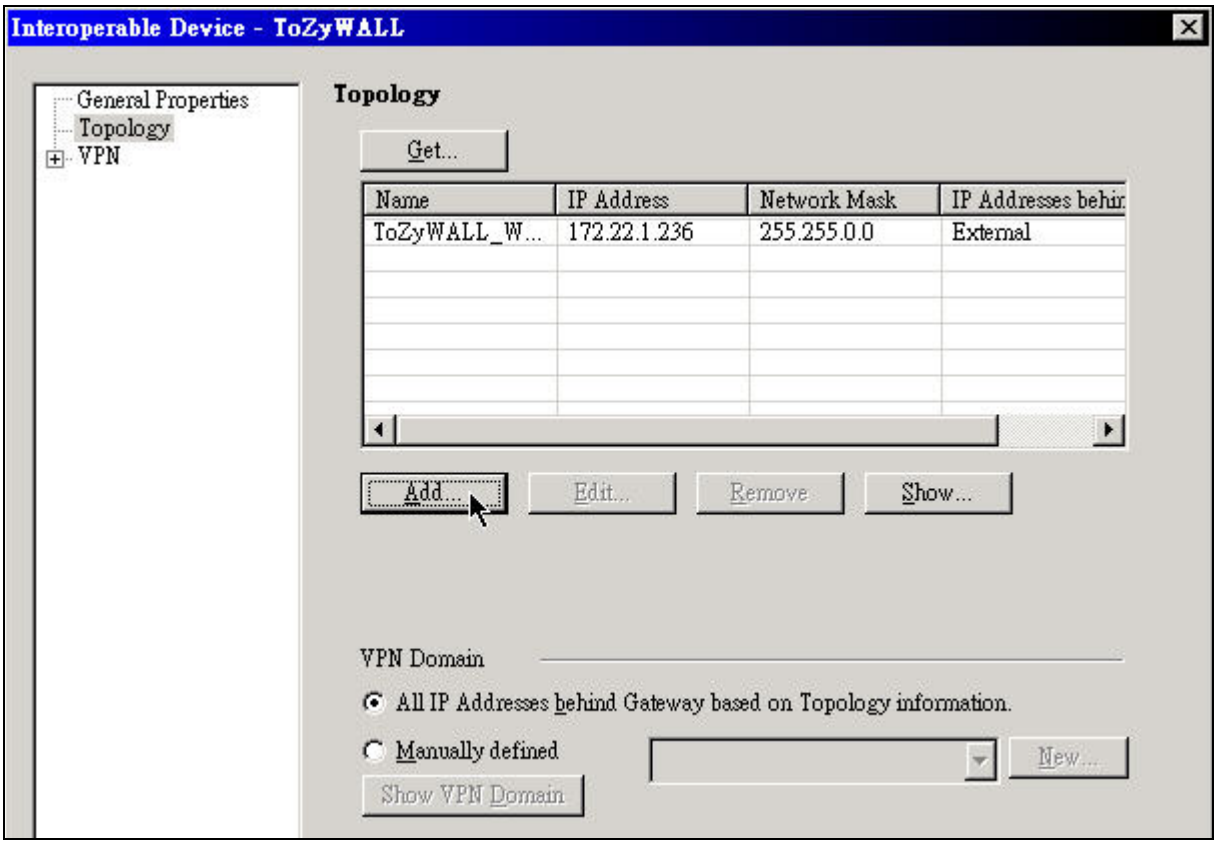
14. Giving a name for the interface, and assign the IP address/ subnet mask for the interface. In this example, you should assign ZyWALL's WAN port settings.



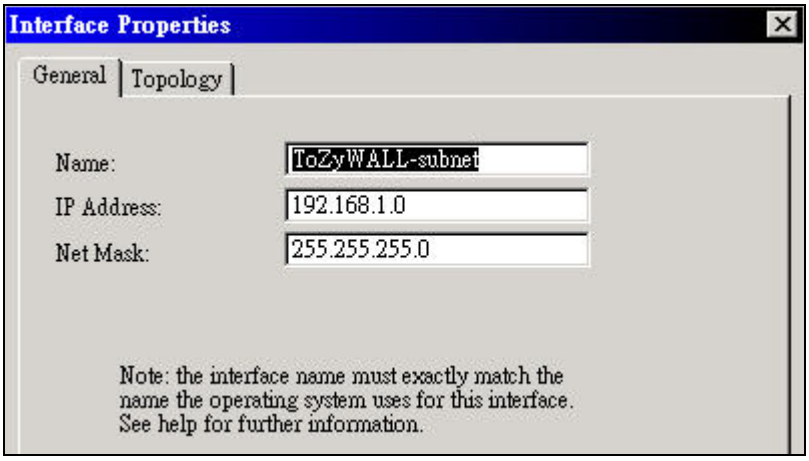
15. Clicking **Topology** screen, and choose **External (leads out to the internet)** for the interface. Then, press OK button to save the settings.



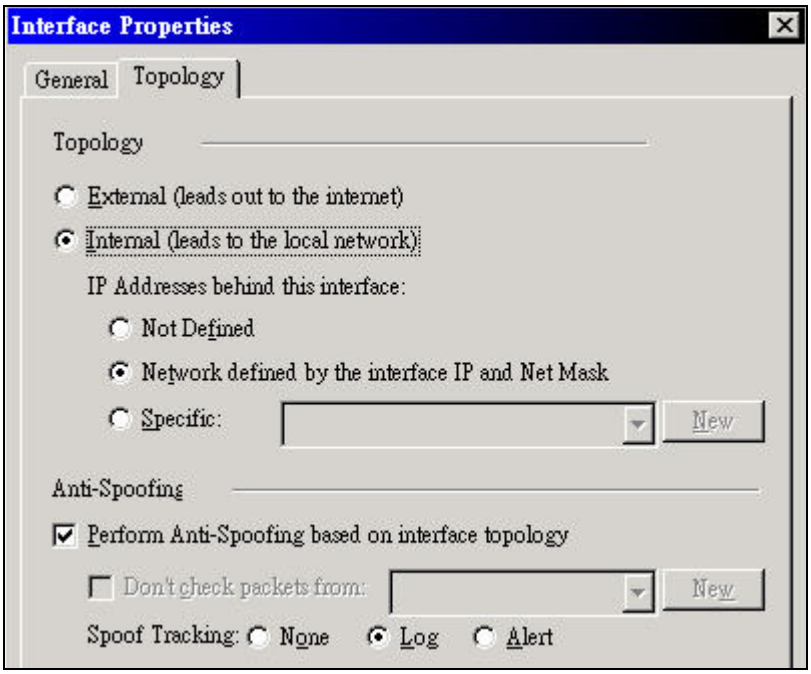
16. Pressing **Add** button to add another interface.



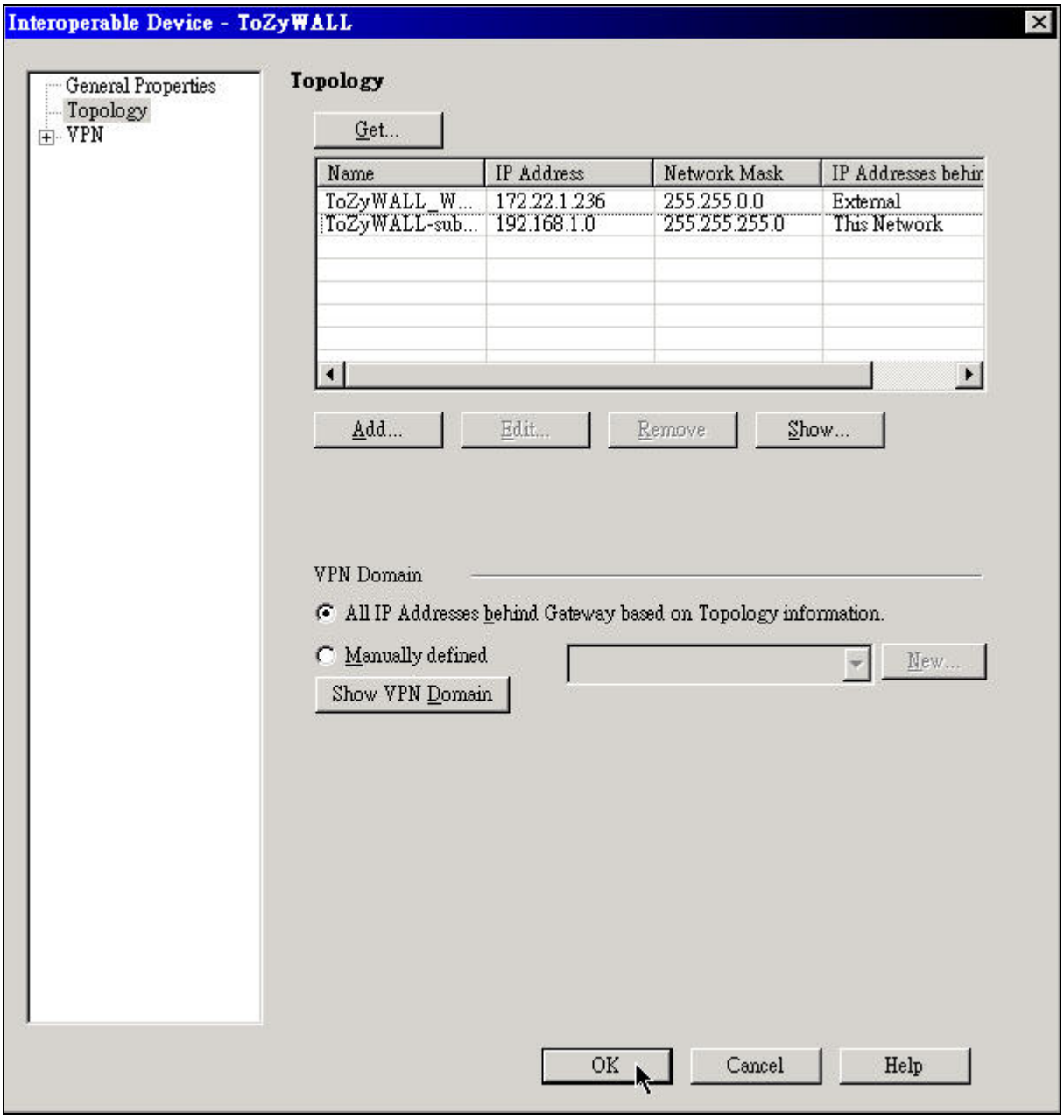
17. Giving a name for the interface, and assign the IP address/ subnet mask for the interface. In this example, you should assign ZyWALL's LAN port settings.



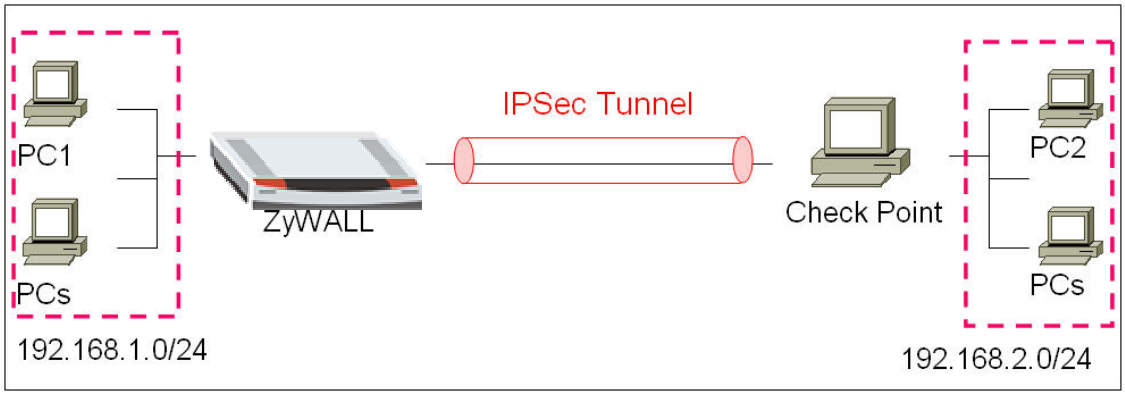
18. Clicking **Topology** screen, choose **Internal (leads to the local network)** and **Network defined by the interface IP and Net Mask** for the interface, then press **OK** button to save the settings.



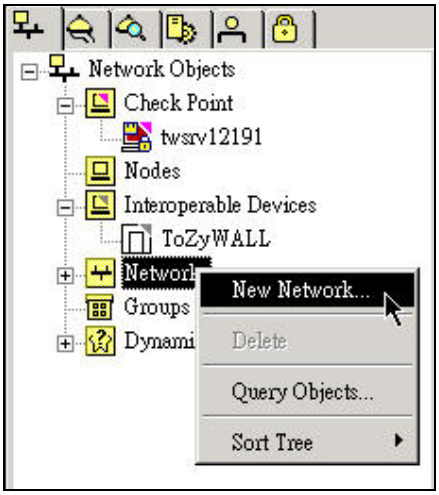
19. Pressing OK button to save the settings.



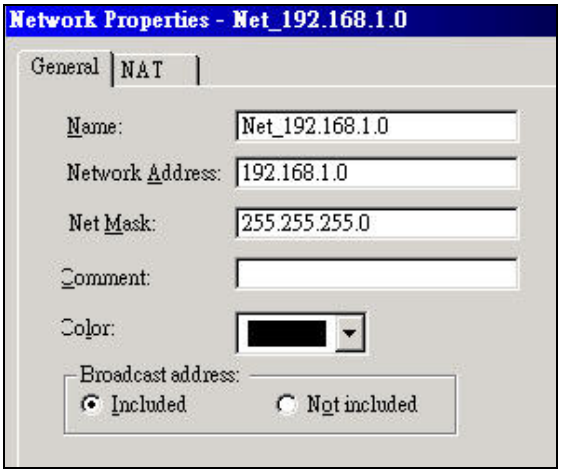
III. Setup Networks



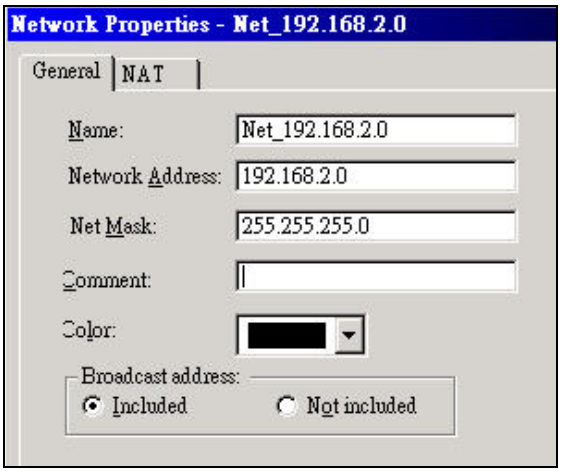
20. Selecting **Networks** object and click the right button of your mouse, and choose **New Network**.



21. Give a name for your network policy, and set the network IP address to **192.168.1.0/24**. Then, press **OK** button to save the settings.



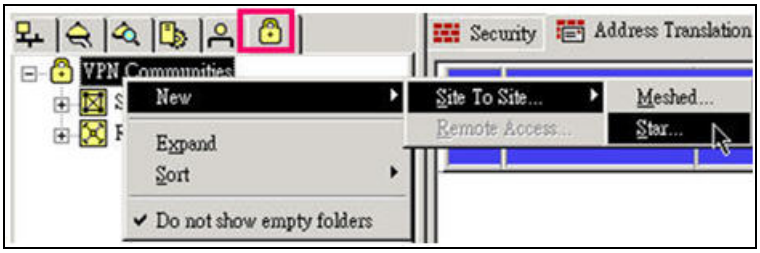
22. To add another network policy, and set the network IP address **192.168.2.0/24**. Then, press **OK** button to save the settings.



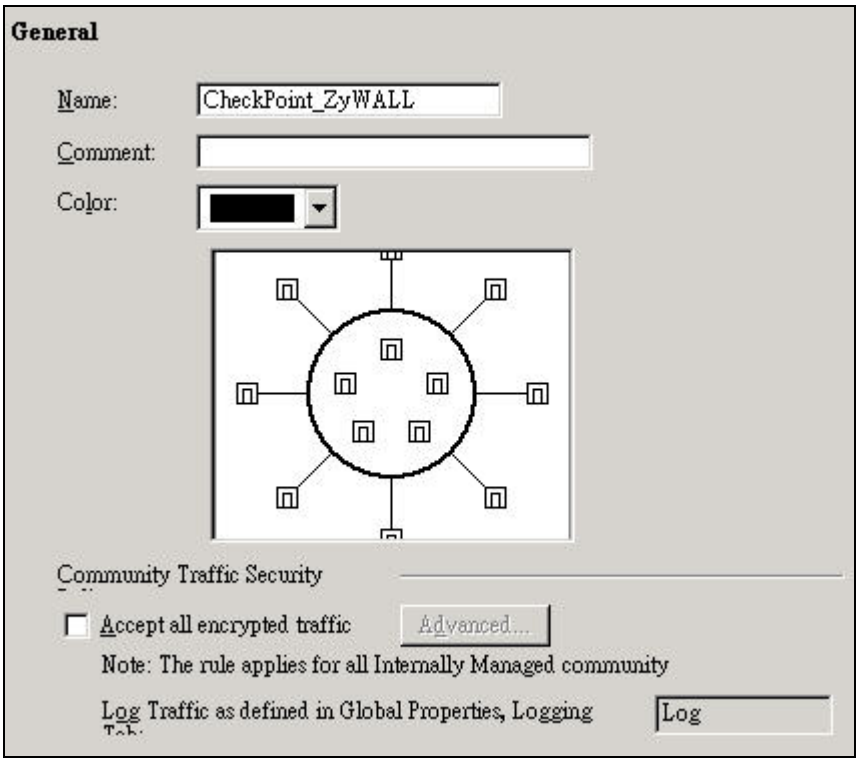
IV. Setup VPN Communities

23. Click VPN communities tab to do the settings.

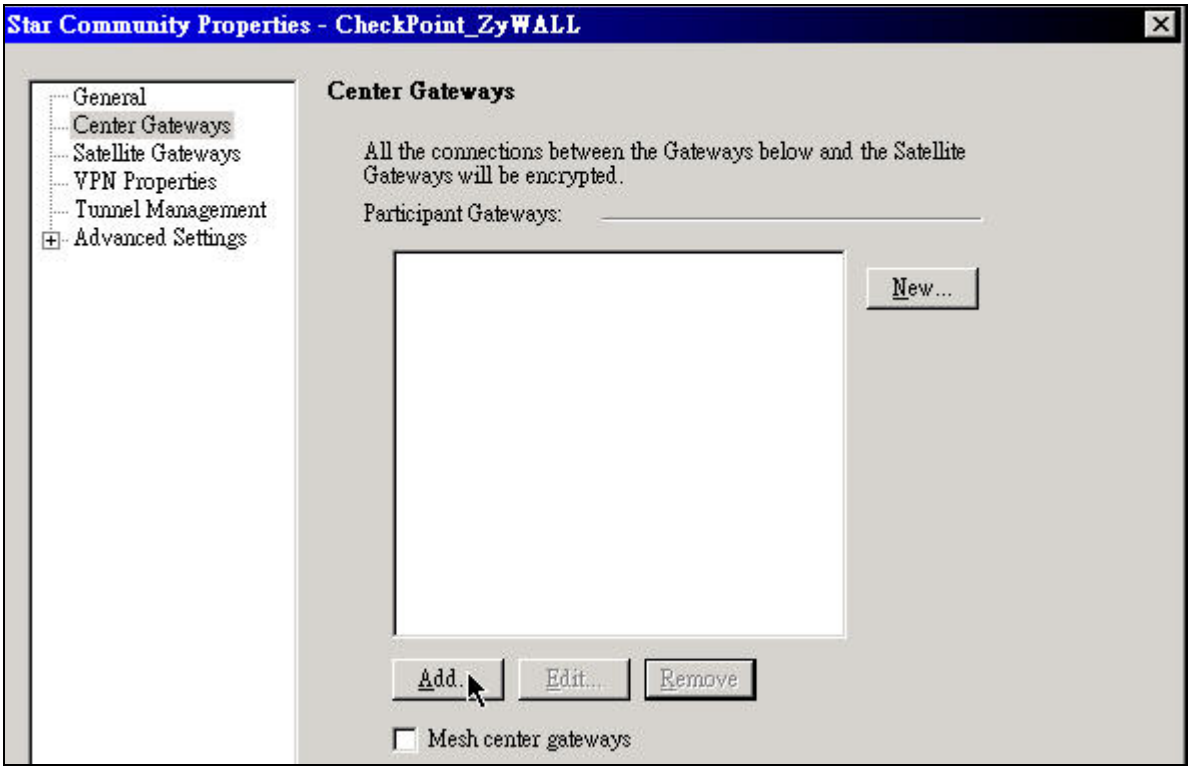
24. On VPN communities, click **New** -> **Site To Site** -> **Star**



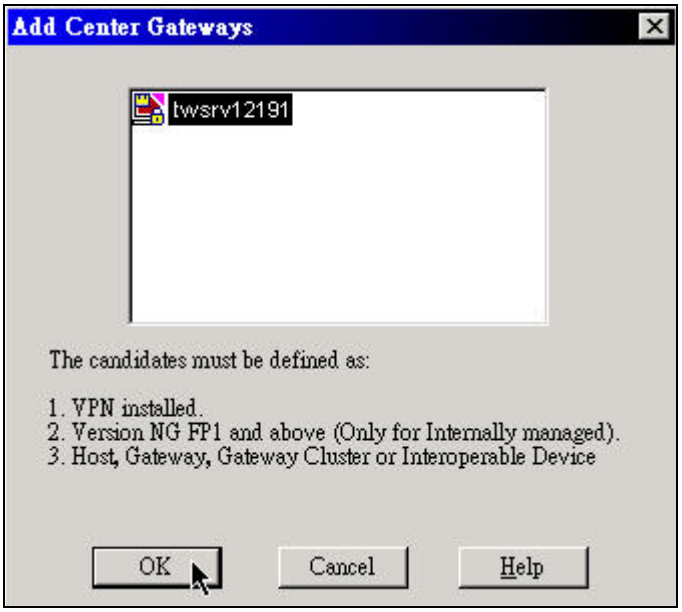
25. On General settings, giving a name for your VPN communities. For example, **CheckPoint_ZyWALL**.



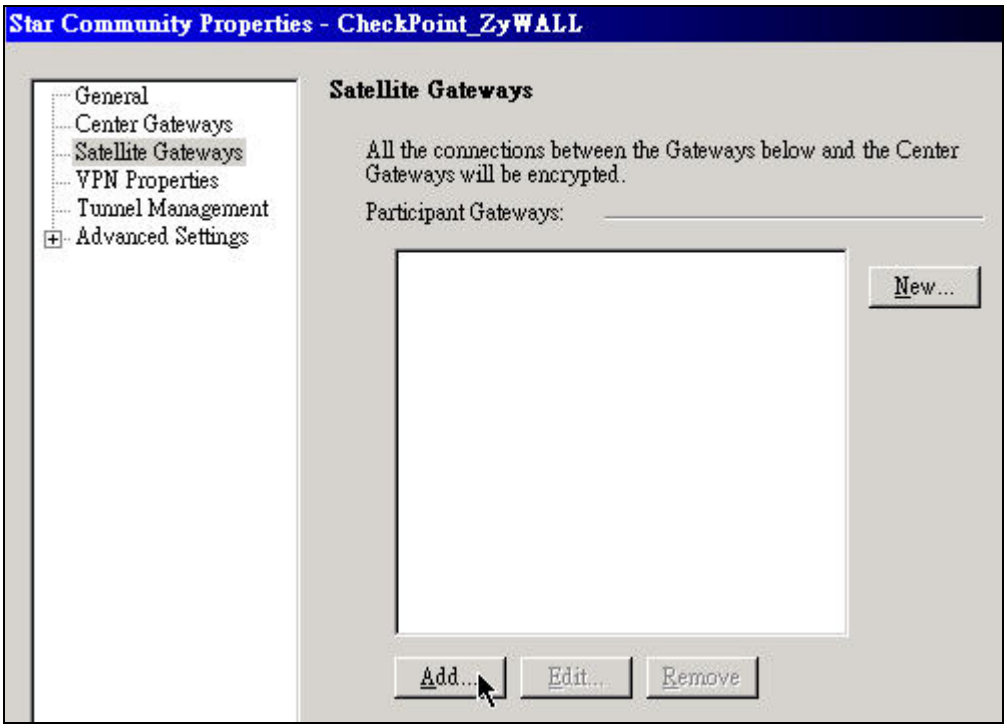
26. On **Center Gateways** settings, press **Add** button to add a center gateway.



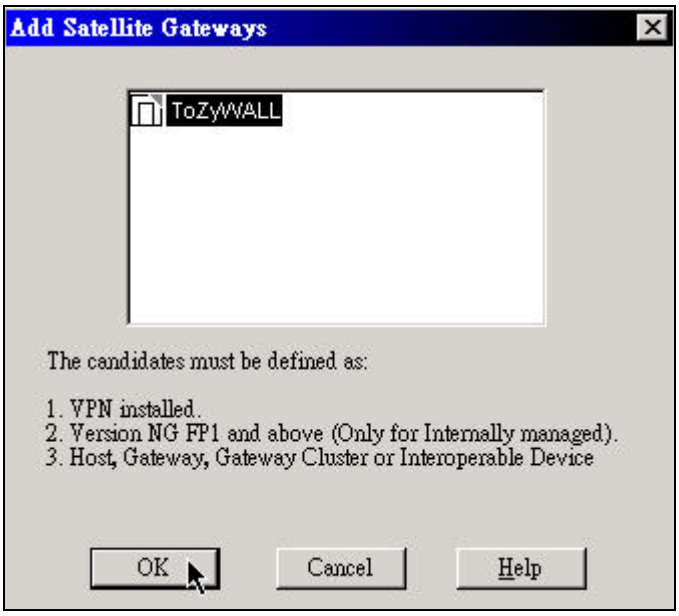
27. If you have already done the previous settings, you should see a central gateway here. Select the gateway, and then press **OK** button.



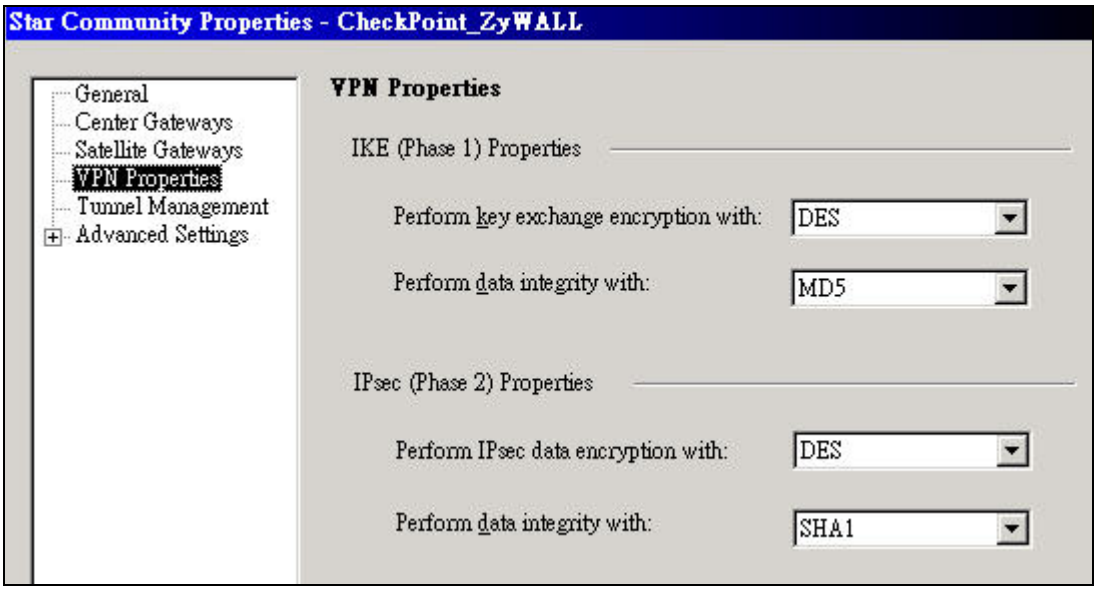
28. On **Satellite Gateways** settings, press **Add** button to add a remote gateway.



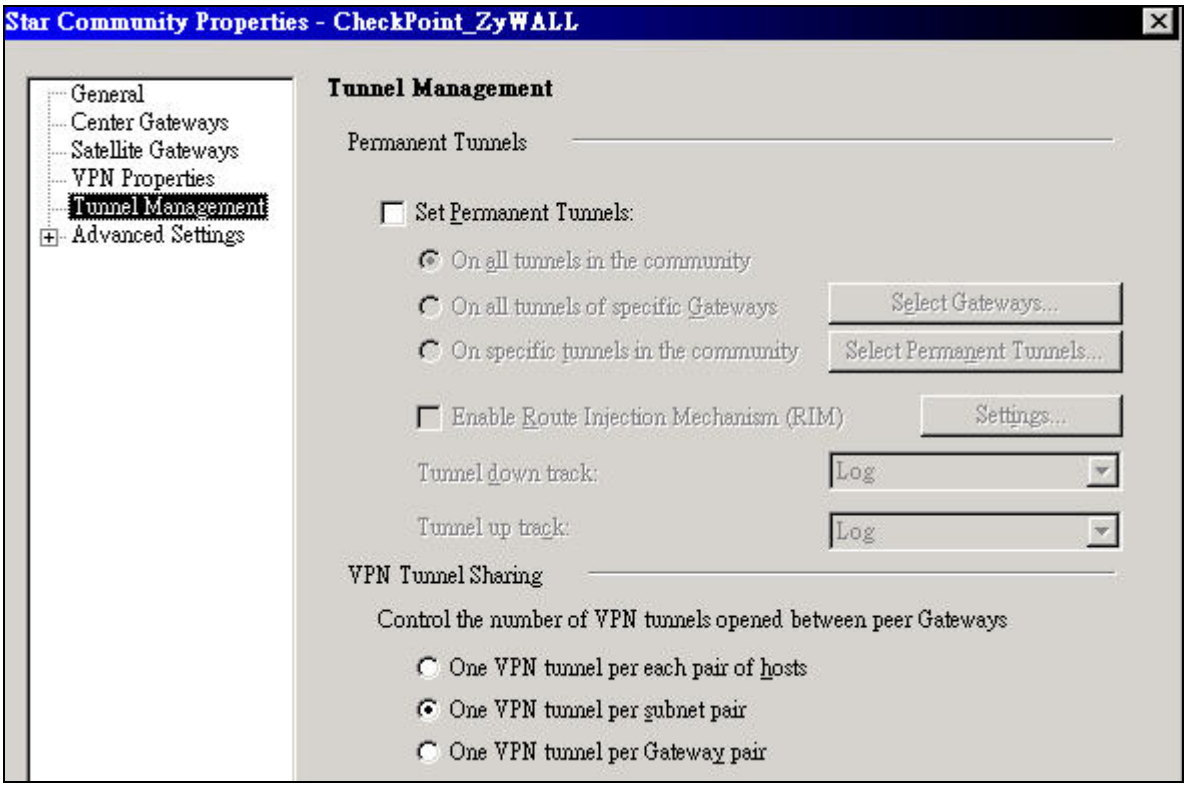
29. If you have already done the previous settings, you should see a remote gateway here. Select the gateway, and then press **OK** button.



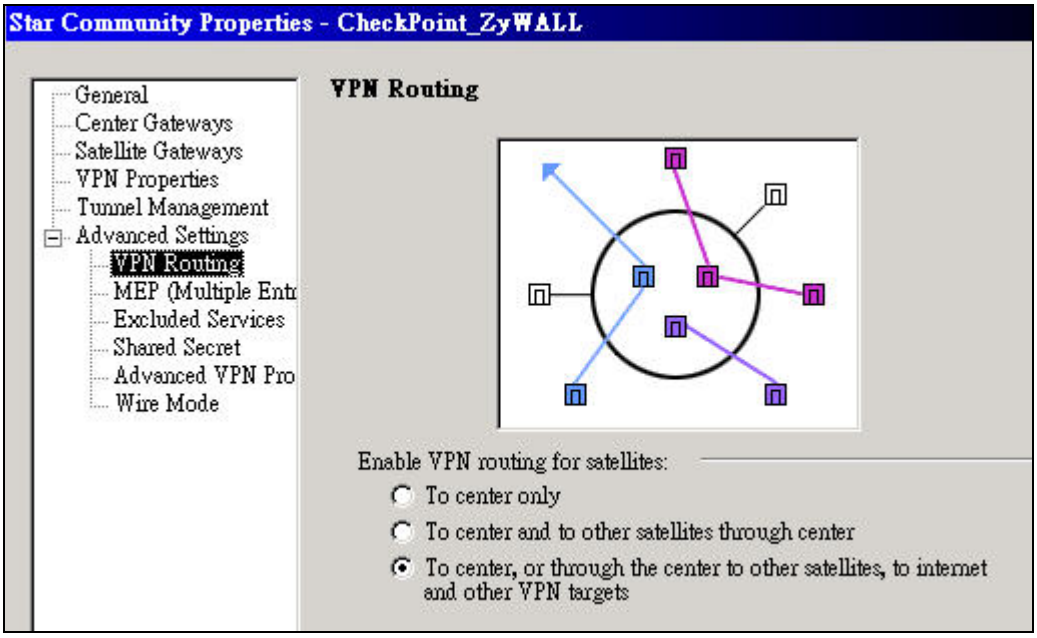
30. On **VPN Properties** settings**,** select **Encryption Algorithm** to **DES**, **Authentication Algorithm** to **MD5** on phase 1, and also select **Encryption Algorithm** to **DES**, **Authentication Algorithm** to **SHA1** on phase 2.



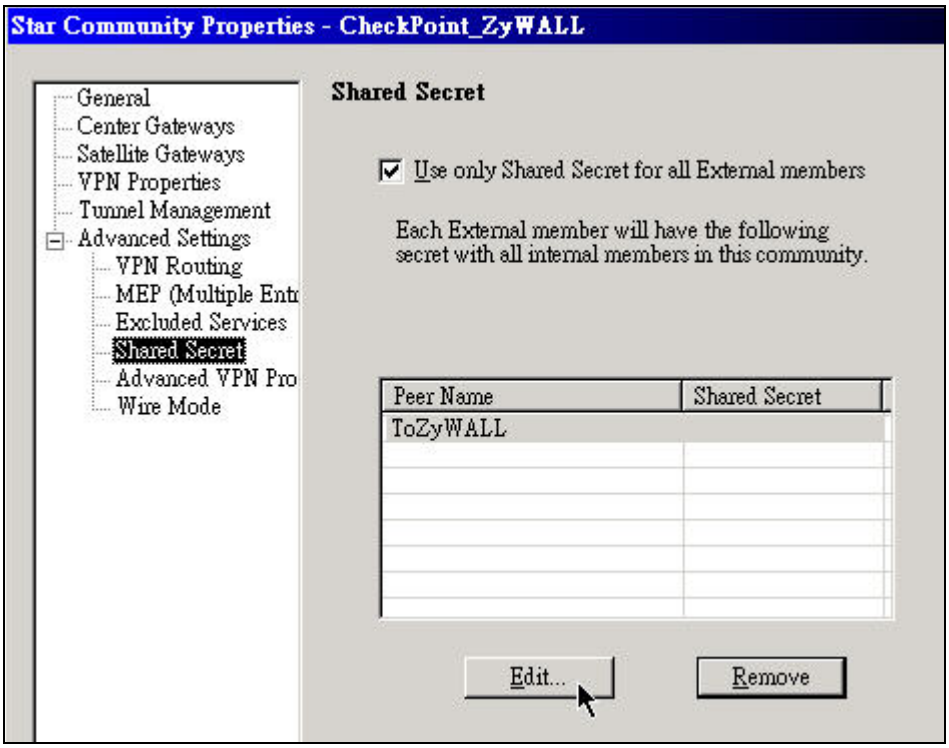
31. On **Tunnel Management**, leave the settings to default settings.



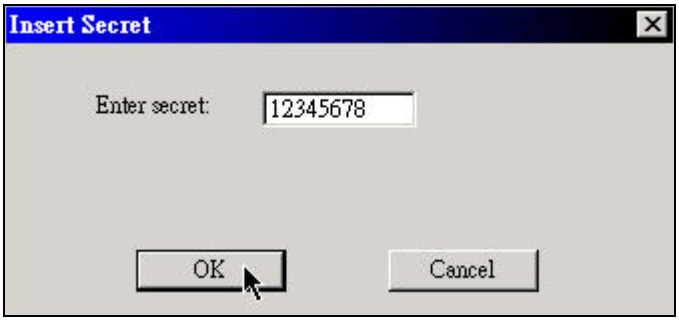
32. On VPN routing settings, choose **To center, or through the center to other satellites, to internet and other VPN targets** option.



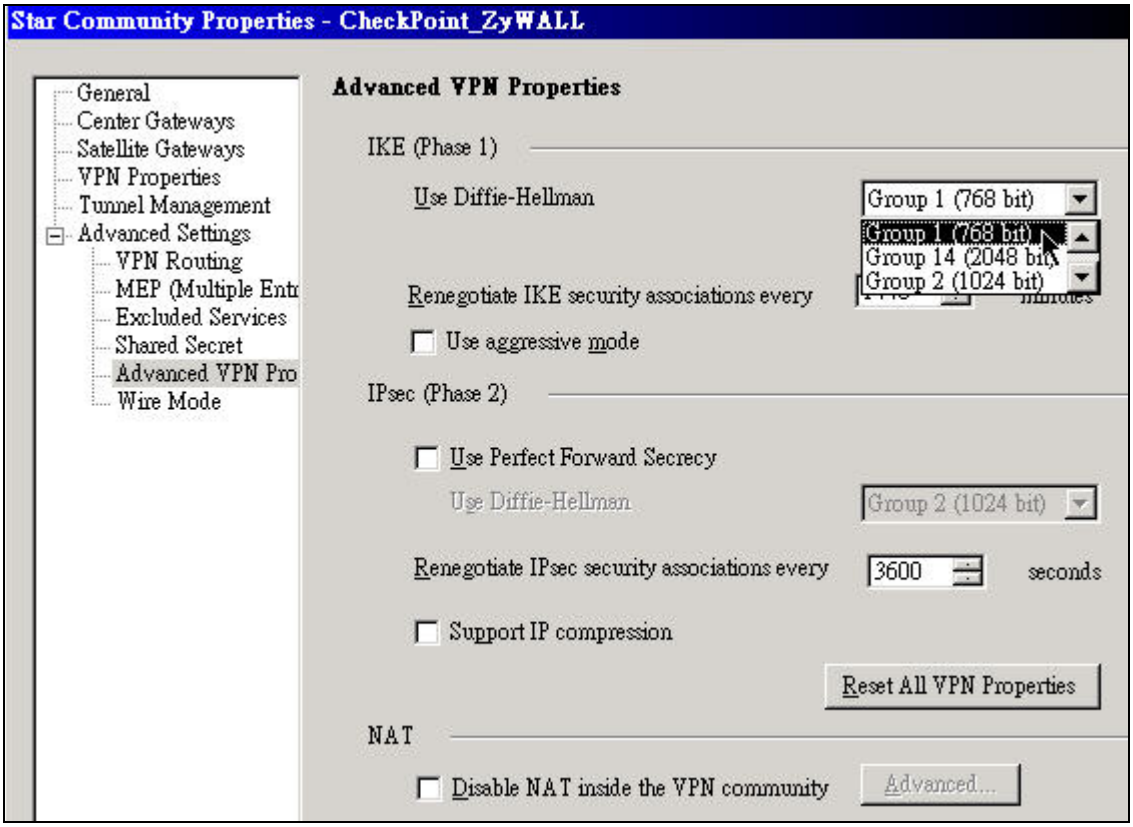
33. On Shared Secret settings, choose ToZyWALL option, and press Edit button



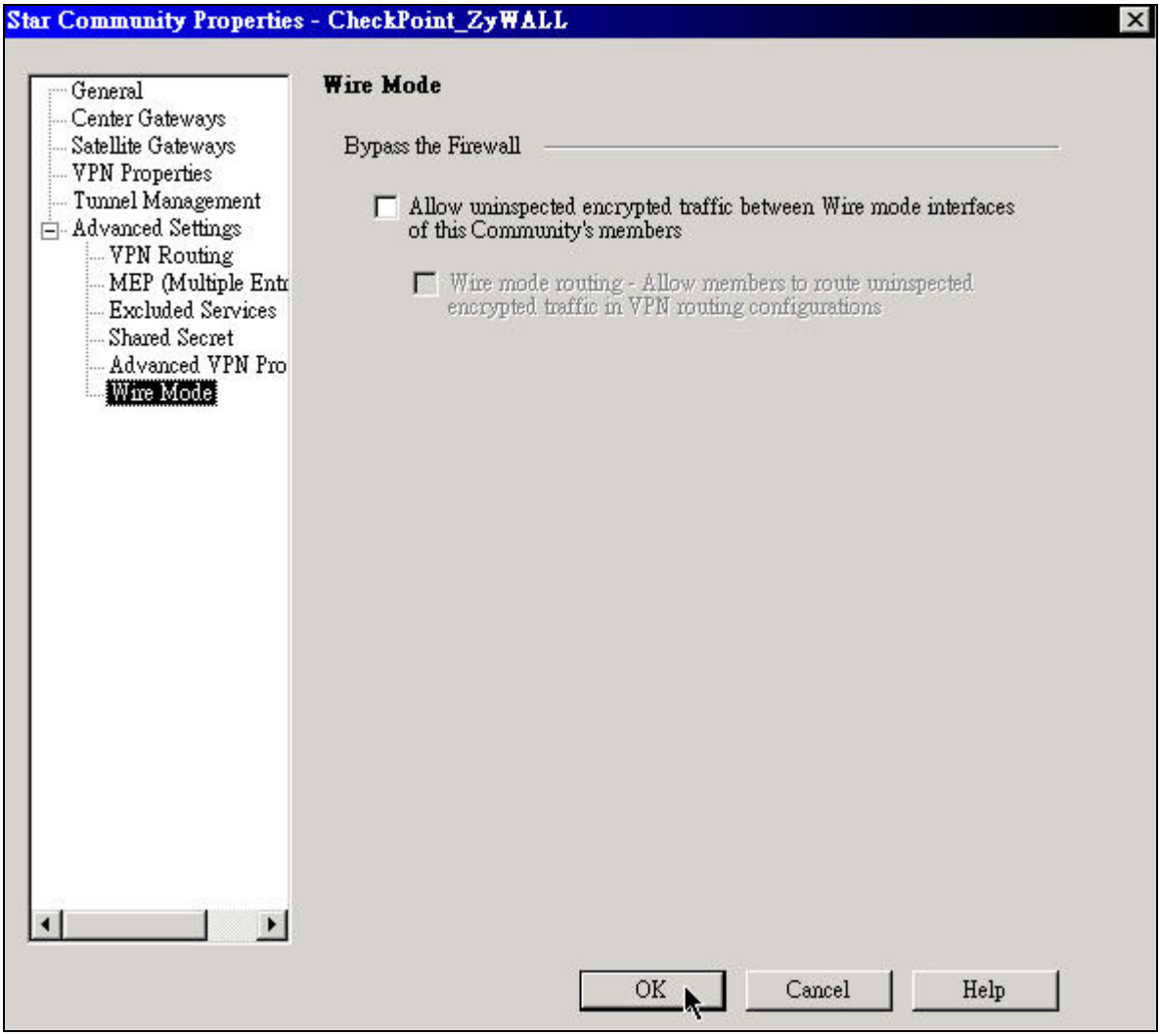
34. Enter the secret key in the text box, and then press **OK** button.



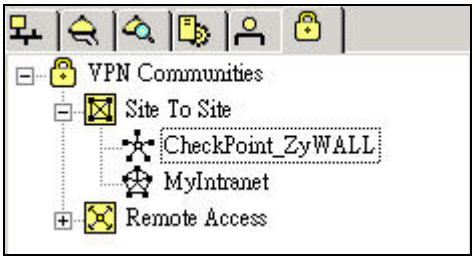
35. On Advanced VPN Properties settings, choose **Group 1** for Diffie-Hellman settings.



36. Press **OK** button to save your settings.



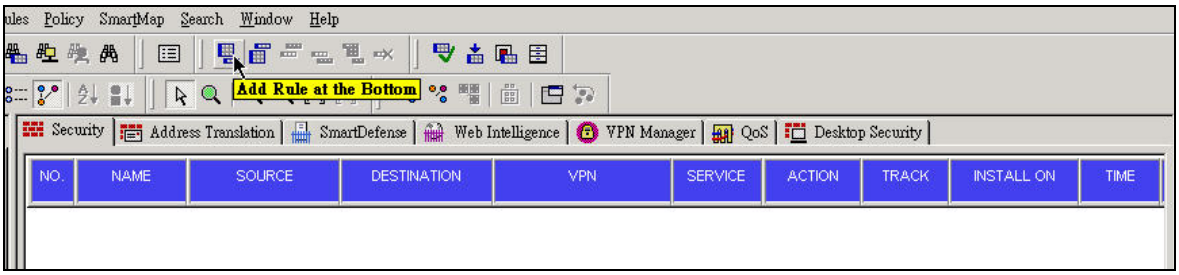
37. After you press OK button, you should see a new object here.



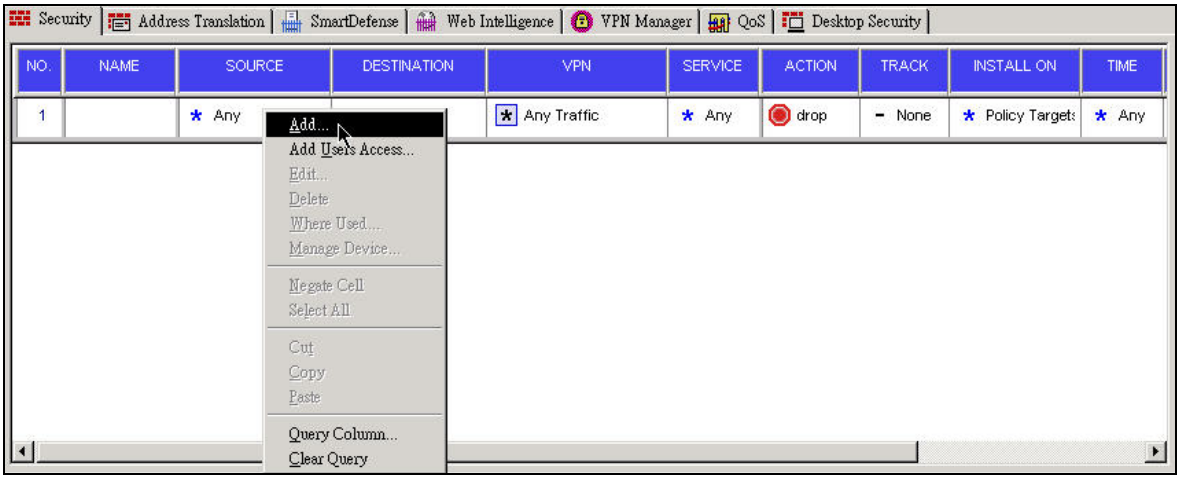
IV. Setup Security

38. Click **Security** tab on the right side to do the security settings.

39. Press Add button to add a rule.

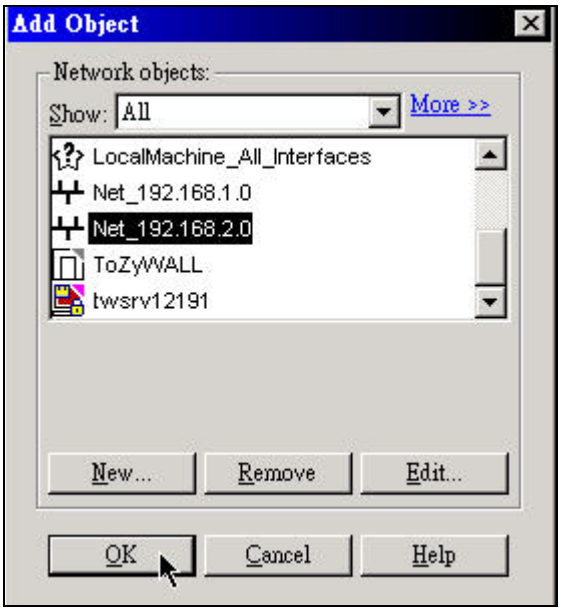


40. On the default rule, select the source field, and click right button of your mouse, and then choose **Add…** option to add your network objects.



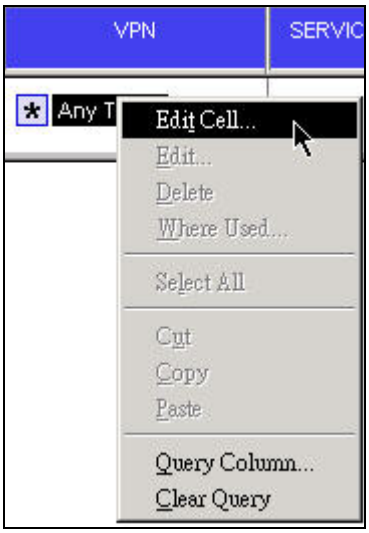
41. Choosing **Net_192.168.1.0** network object, and press **OK** button to save your settings.

42. To use the same way to add another network object (**Net_192.168.2.0**) on the source field.

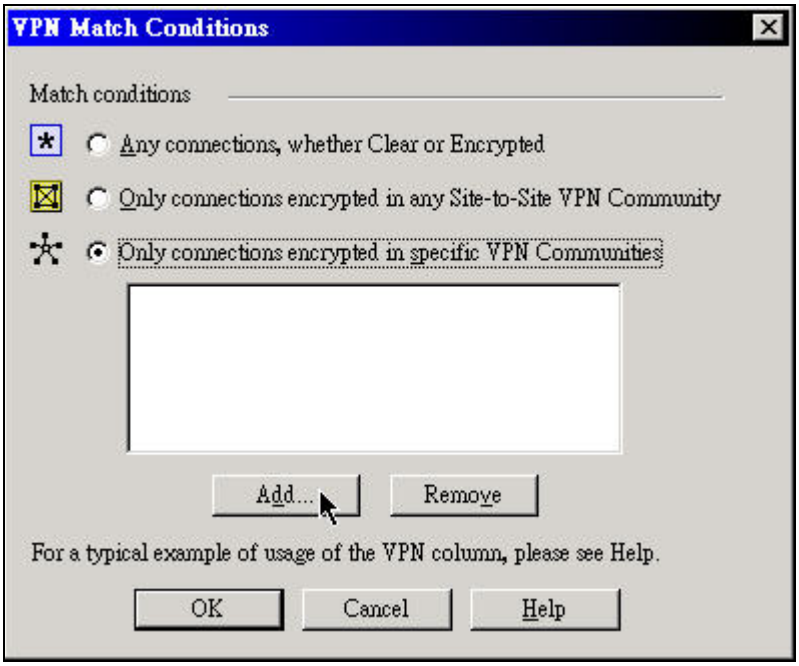


43. On the destination field, please use the same way to add your network objects: **Net_192.168.1.0** and **Net_192.168.2.0**.

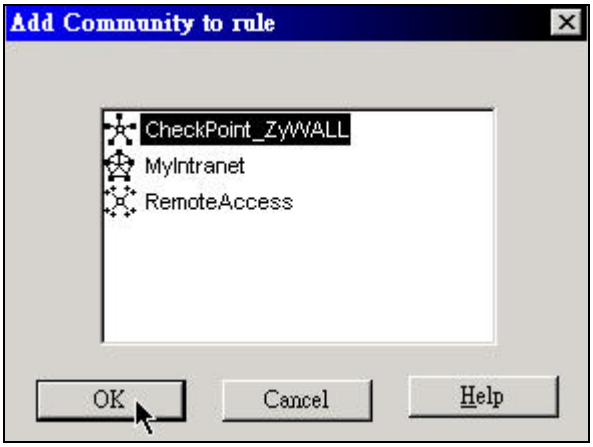
44. On the VPN field, click right button of your mouse, and choose **Edit Cell…** option to add your VPN communities.



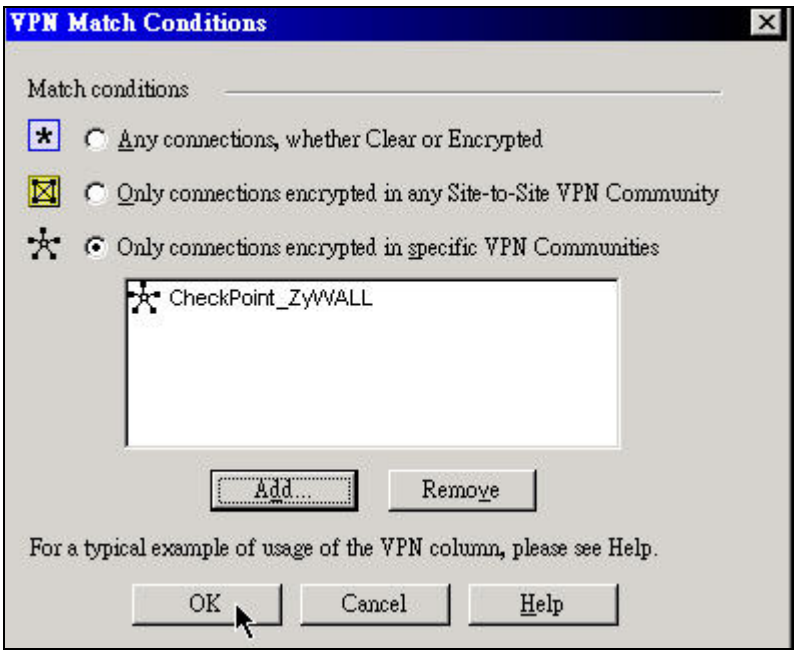
45. On VPN Match Conditions, choose **Only connections encrypted in specific VPN Communities** option, and press **Add** button to add community to your rule.



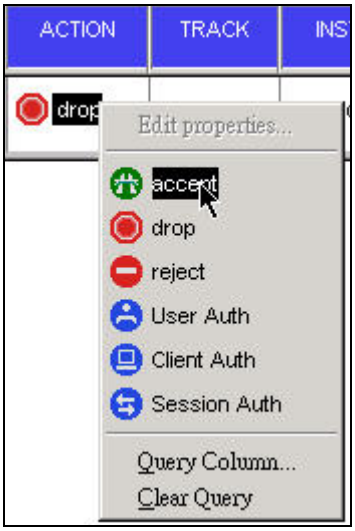
46. Choosing **CheckPoint_ZyWALL** object for your rule, and press **OK** button.



47. Clicking **OK** button to save your settings.



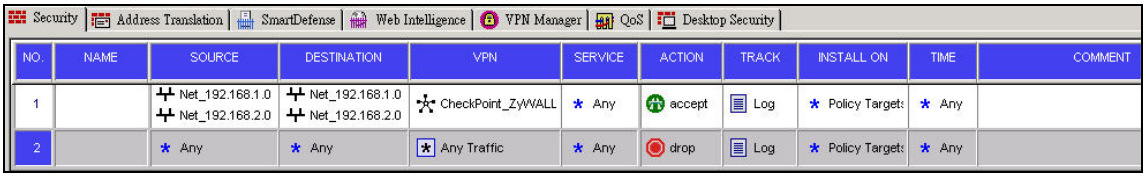
48. On action field, click right button of your mouse, and choose **accept** option for your rule.



49. On the track field, click right button of your mouse, and choose **Log** option for your rule.

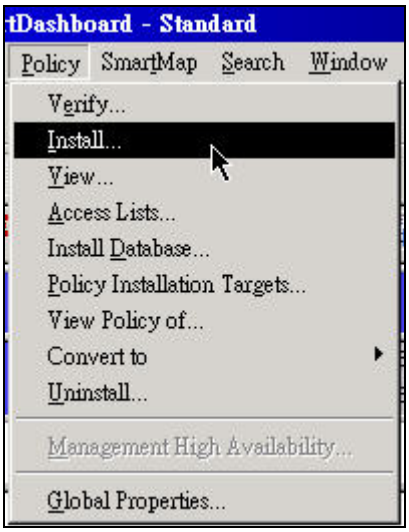
50. If you finished the settings, you should see a rule as below.

51. Pressing add button to add another rule which could drop packets if it doesn't match your VPN rule.

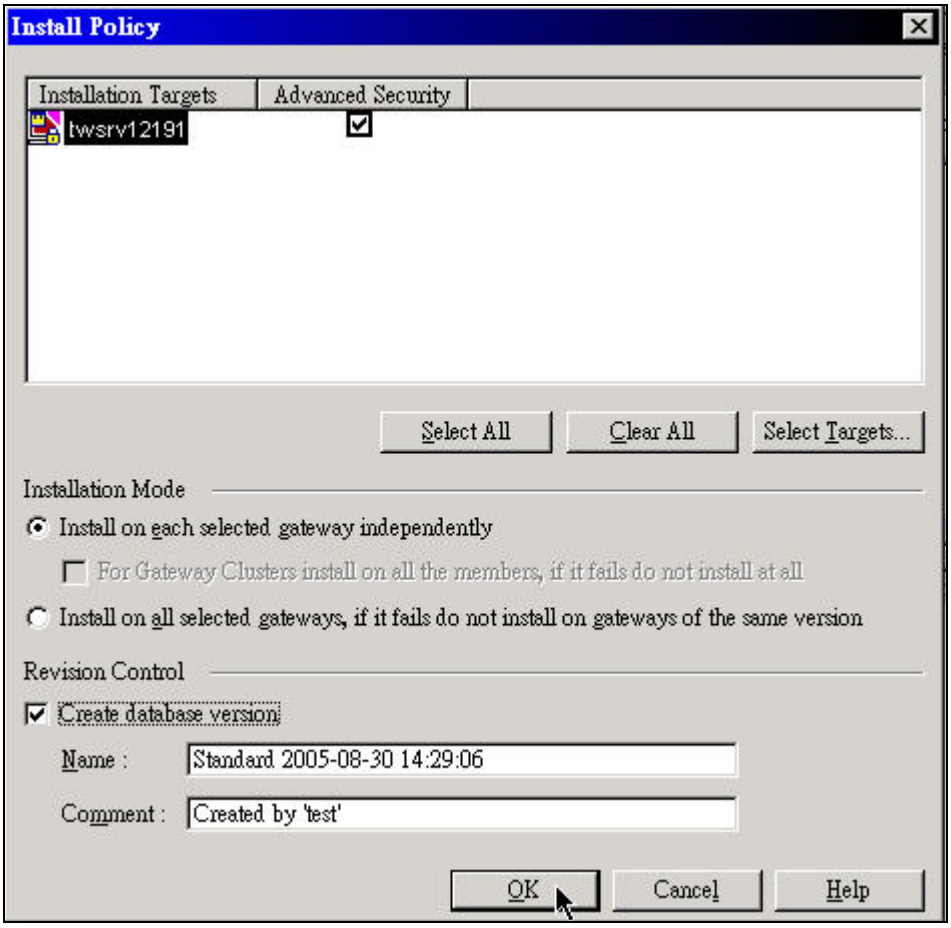


V. Install Policy

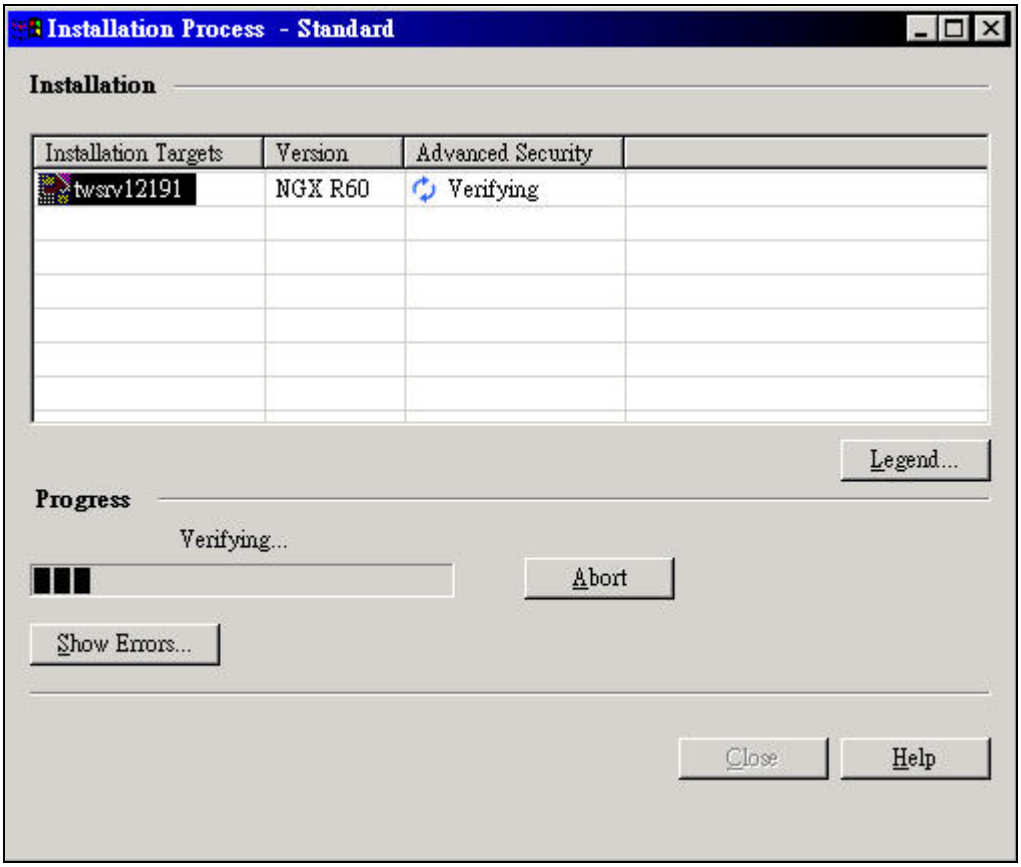
52. On your main menu, click Policy -> Install.. option to Install your policy.



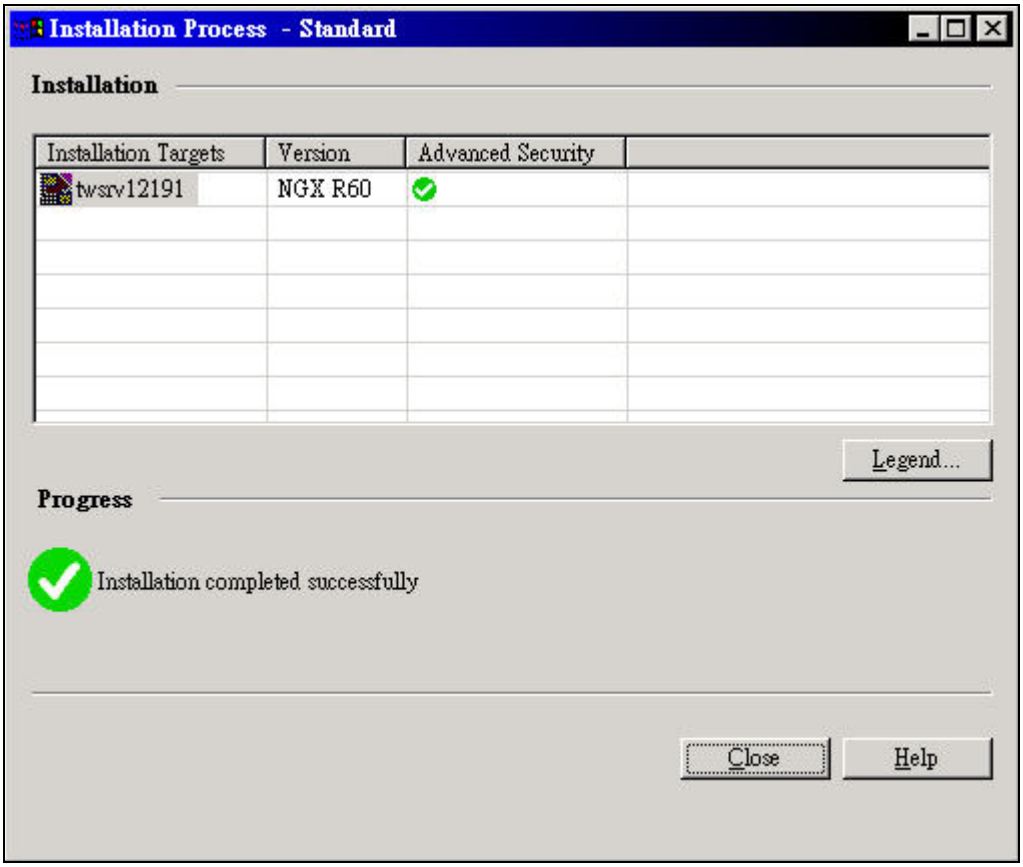
53. Selecting your policy rule, and press **OK** button to install the policy.



54. Waiting few seconds for the installation.



55. If you install the policy successfully, your VPN tunnel should work normally with your ZyWALL.

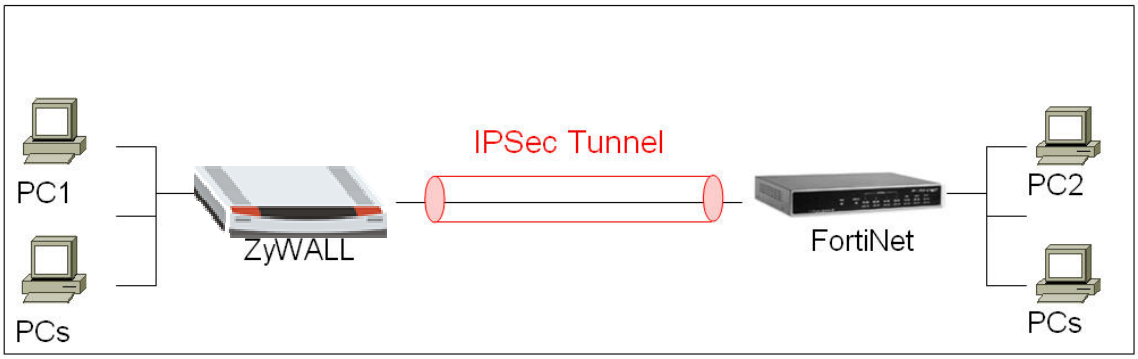


FortiNet with ZyWALL VPN Tunneling

1. Setup ZyWALL VPN
2. Setup FortiNet VPN

This page guides us to setup a VPN connection between the ZyWALL and FortiNet router.

As the figure shown below, the tunnel between PC1 and PC2 ensures the packet flows between them are secure. Because the packets go through the IPSec tunnel are encrypted. To setup this VPN tunnel, the required settings for ZyWALL and FortiNet are explained in the following sections. As the red pipe shown in the following figure, **the tunneling endpoints are ZyWALL router and FortiNet router.**



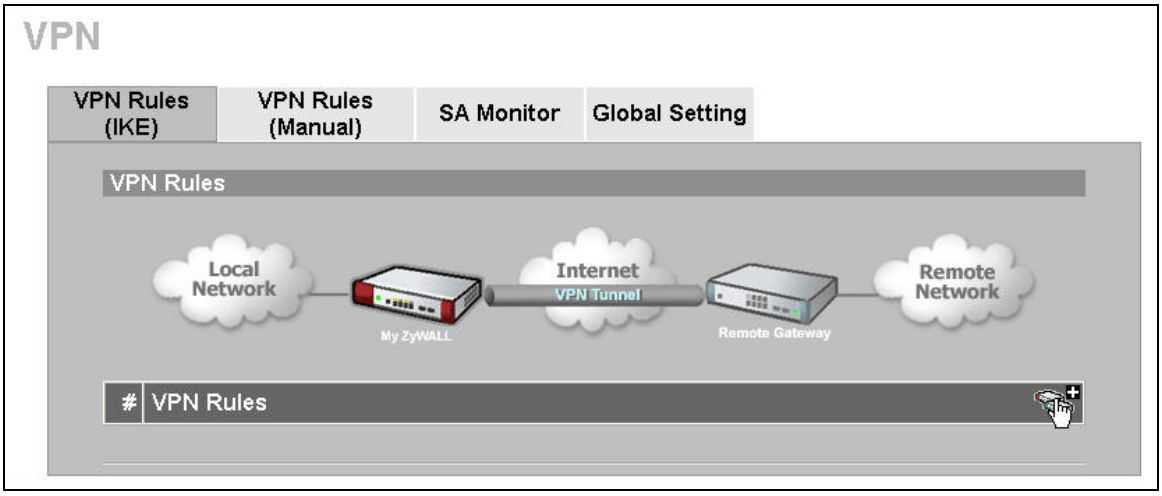
The IP addresses we use in this example are as shown below.

ZyWALL	FortiNet
WAN: 172.22.1.147 LAN: 192.168.2.0/24	WAN: 172.22.2.138 LAN: 192.168.1.0/24

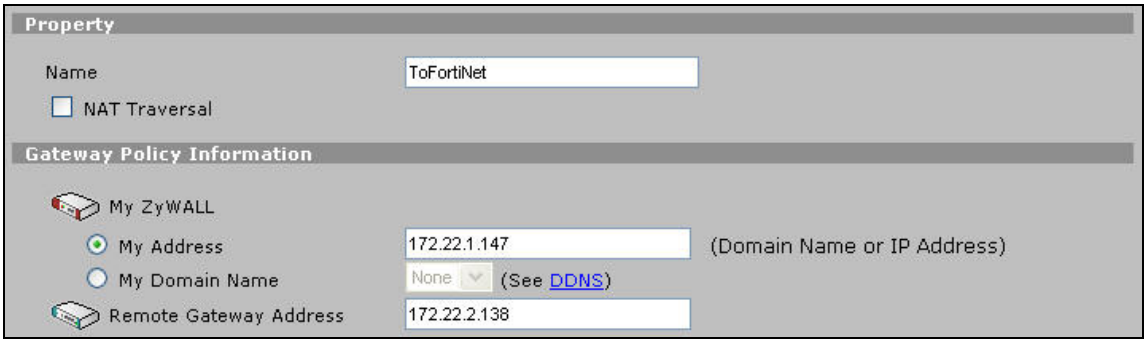
---

1. Setup ZyWALL VPN

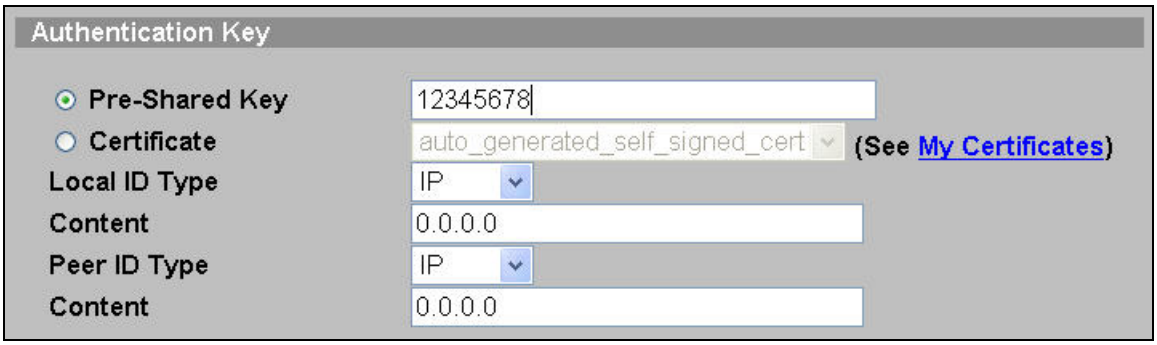
1. Using a web browser, login ZyWALL by giving the LAN IP address of ZyWALL in URL field.
2. Go to SECURITY->VPN->Press **Add** button



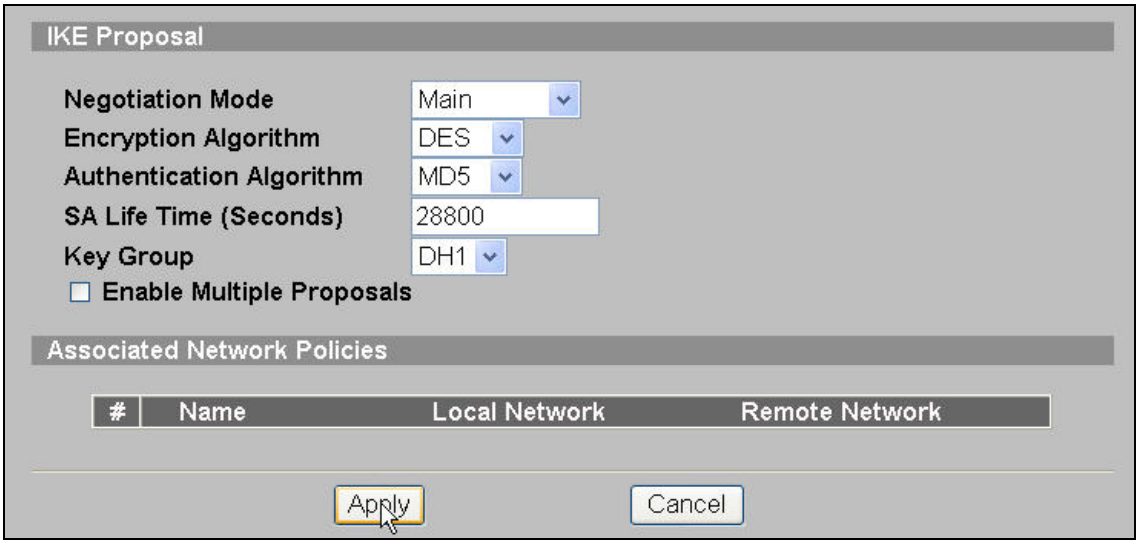
3. Give a name for your policy, for example "**ToFortiNet**"
4. **My IP Addr** is the **WAN IP of ZyWALL**. In this example, you should type 172.22.1.147 IP address on **My ZyWALL** text box.
5. **Secure Gateway IP Addr** is the **FortiNet's WAN IP address**. In this example, you should type 172.22.2.138 IP address on **Remote Gateway** text box.



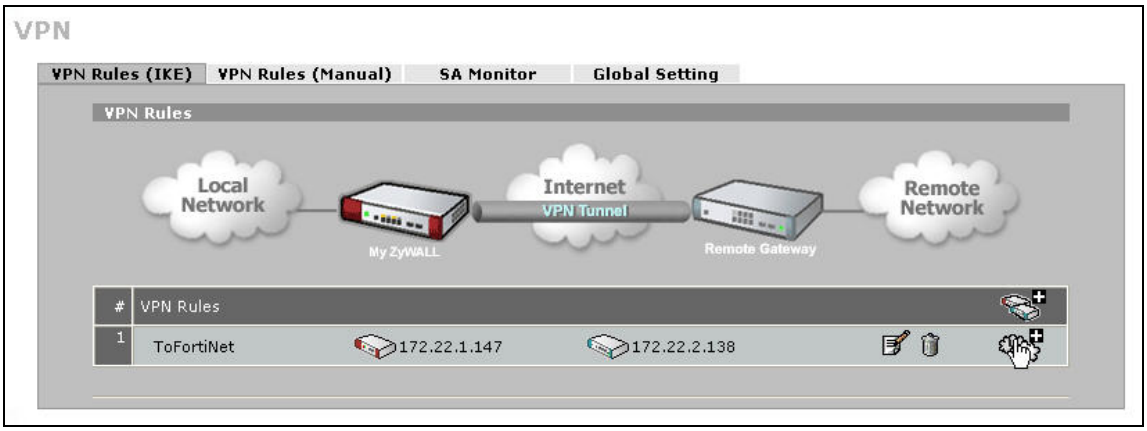
6. In **Authentication Key**, enter the key string **12345678** in the **Pre-Shared Key** text box.



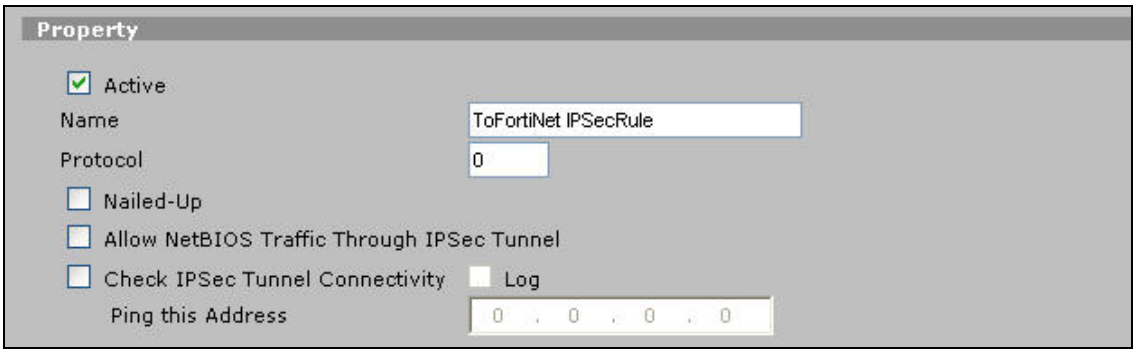
7. Select **Negotiation Mode** to **Main mode**, **Encryption Algorithm** to **DES**, **Authentication Algorithm** to **MD5**, **Key Group** to **DH1,** and then click **Apply** button on this page.



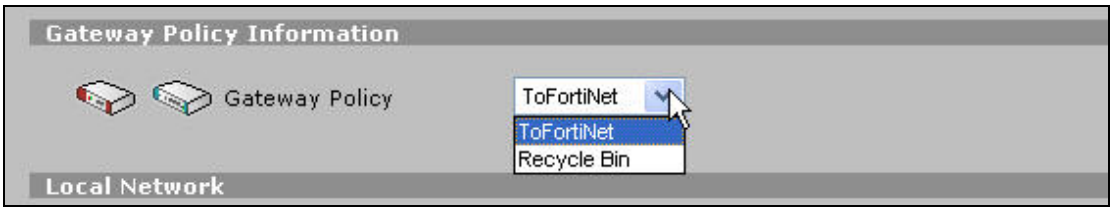
8. After you press the **Apply** button, you will see an IKE rule on this page, click L/R button to edit your IPSec rule.



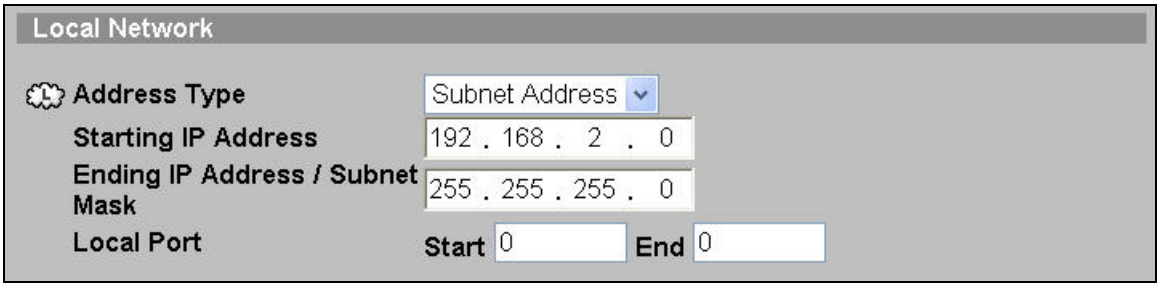
9. Check **Active** check box and give a name to this policy.



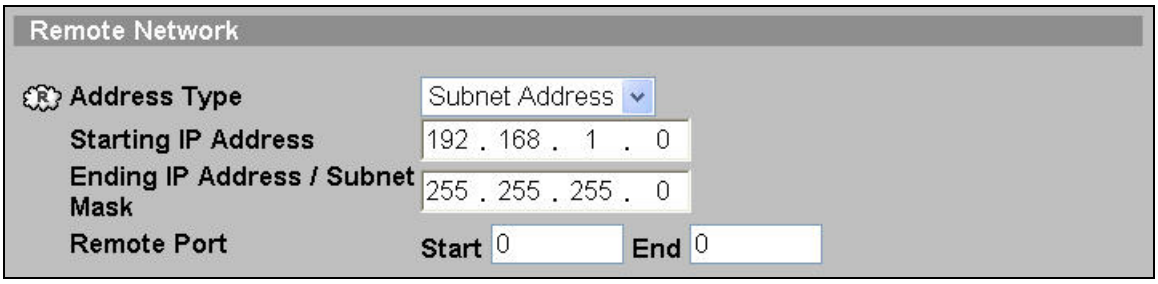
10. On Gateway Policy Information, you should choose **ToFortiNEt** IKE policy for your IPSec rule.



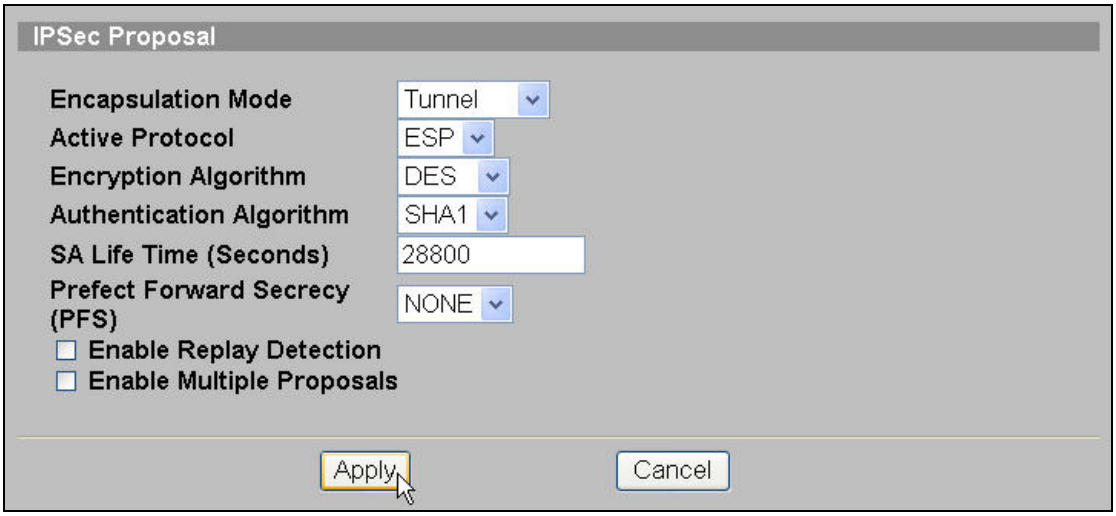
11. On **Local Network,** choose **Subnet Address** for your **Address Type. Starting IP Address** and **Ending IP Address/Subnet** are your local site LAN IP addresses. In this example, you should type 192.168.2.0 on **Starting IP Address** field and then type 255.255.255.0 on **Ending IP Address/Subnet** field.



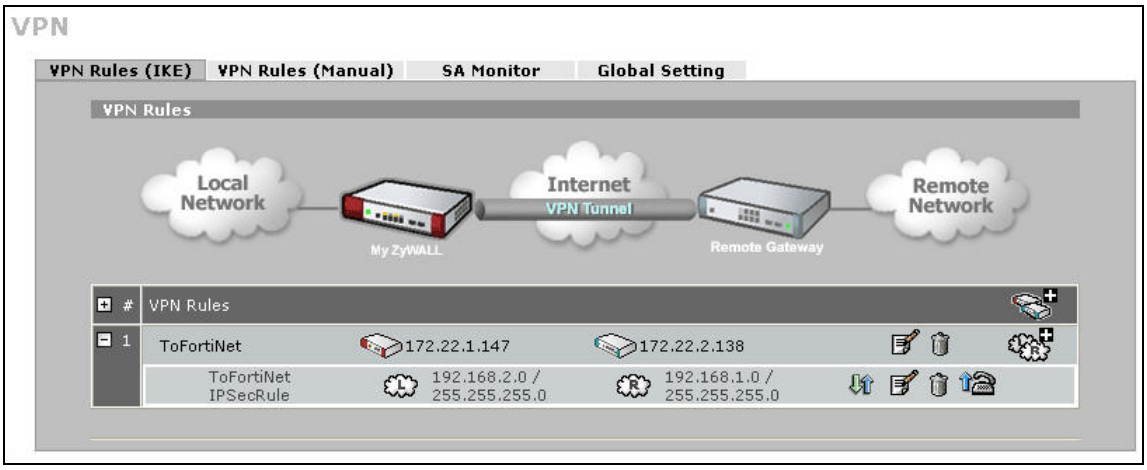
12. On **Remote Network,** choose **Subnet Address** for your **Address Type. Starting IP Address** and **Ending IP Address/Subnet** are your remote site LAN IP addresses. In this example, you should type 192.168.1.0 on **Starting IP Address** field and then type 255.255.255.0 on **Ending IP Address/Subnet** field.



13. On **IPSec Proposal,** select **Encapsulation Mode** to **Tunnel, Active Protocol** to **ESP, Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA1**, and then press Apply button on this page.



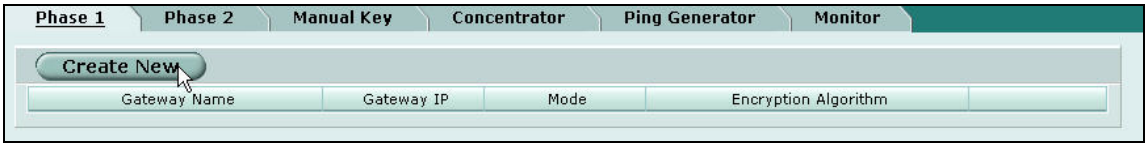
14. After you press the **Apply** button, you will see the following page.



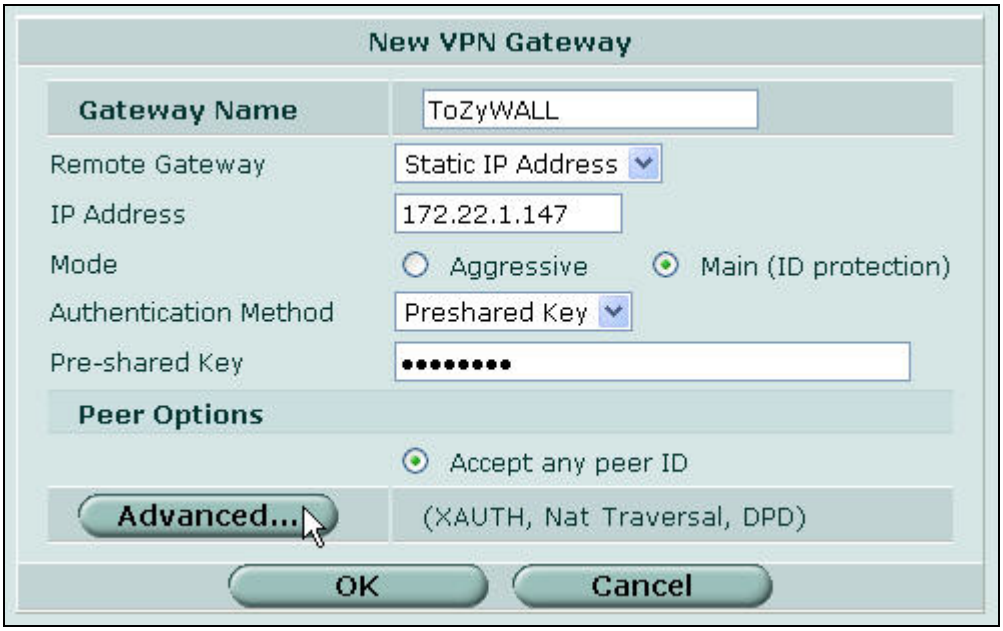
---

2. Setup FortiNet VPN (We choose FortiGate-60 device in this example.)

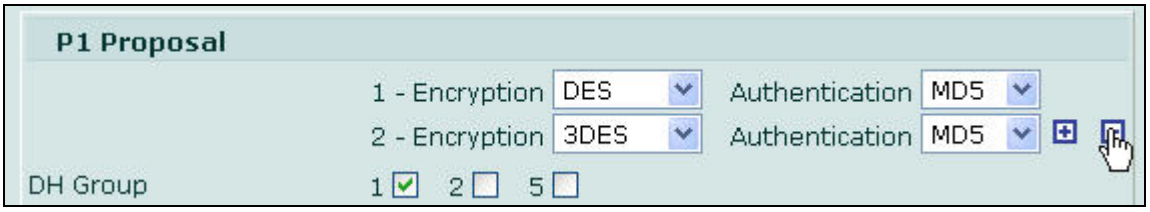
1. Using a web browser, login FortiNet by giving the LAN IP address of FortiNet in URL field.
2. To edit your IPSec rule, click **VPN** -> **IPSec** -> **Phase 1**, and then press **Create New** button to edit your IKE rules.



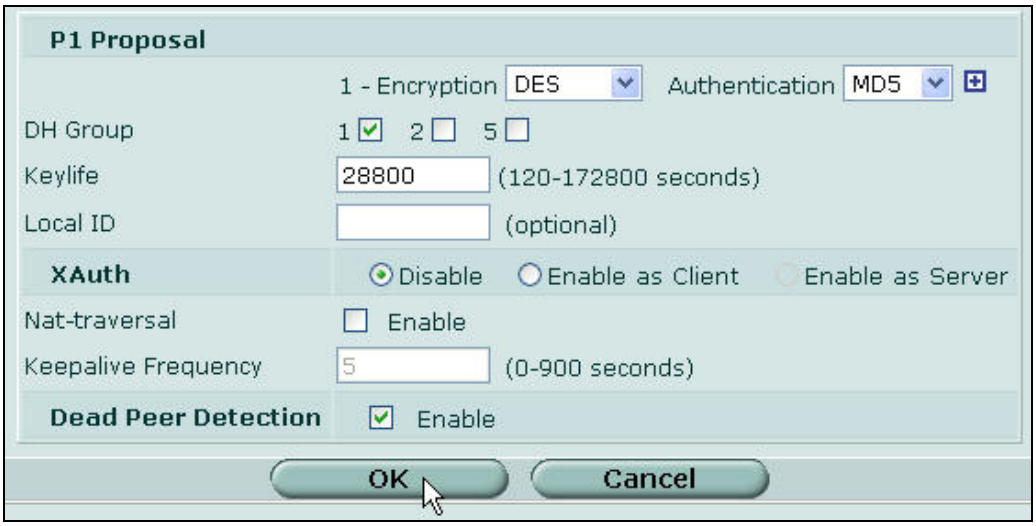
3. Give a name for your policy, for example "**ToZyWALL**". **Remote Gateway IP Addr** is the **ZyWALL's WAN IP address.** In this example, select **Static IP Address** option and set **172.22.1.147** on the text box. Choosing **Main** mode, and also enter the key string **12345678** on **Preshared Key** text box. Then, press **Advanced** button to edit the advanced settings.



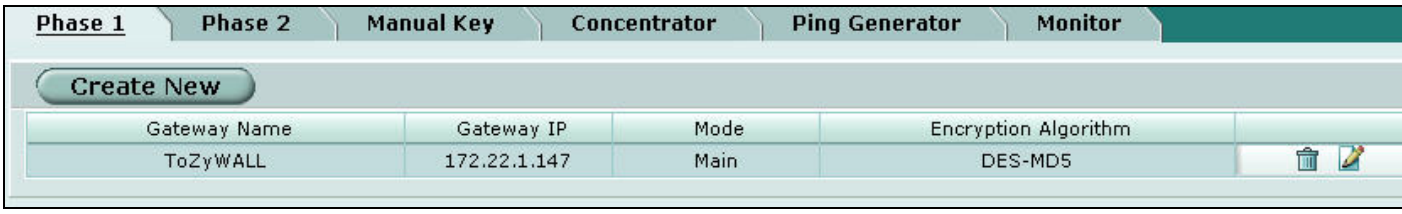
4. On P1 proposal settings, select **Encryption** to **DES**, **Authentication** to **MD5, and DH Group** to **Group1**. Then, press "-" button to delete the second P1 proposal rules.



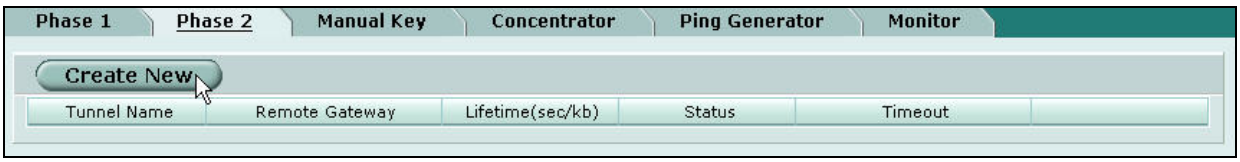
5. To uncheck the **Nat-traversal** check box. And then press **OK** button to save the settings.



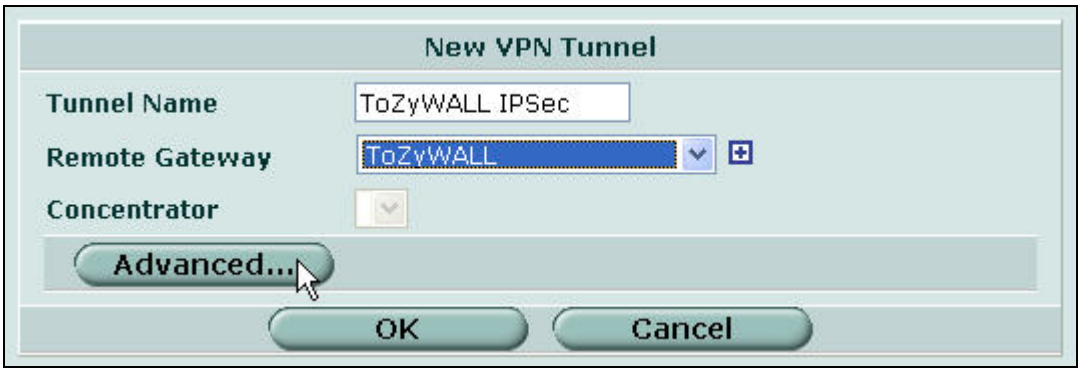
6. After you press the **OK** button, you will see a Phase 1 rule on this page.



7. To edit your IPSec rule(phase 2), click **VPN** -> **IPSec** -> **Phase 2**, and then press **Create New** button to edit your IPSec rules.

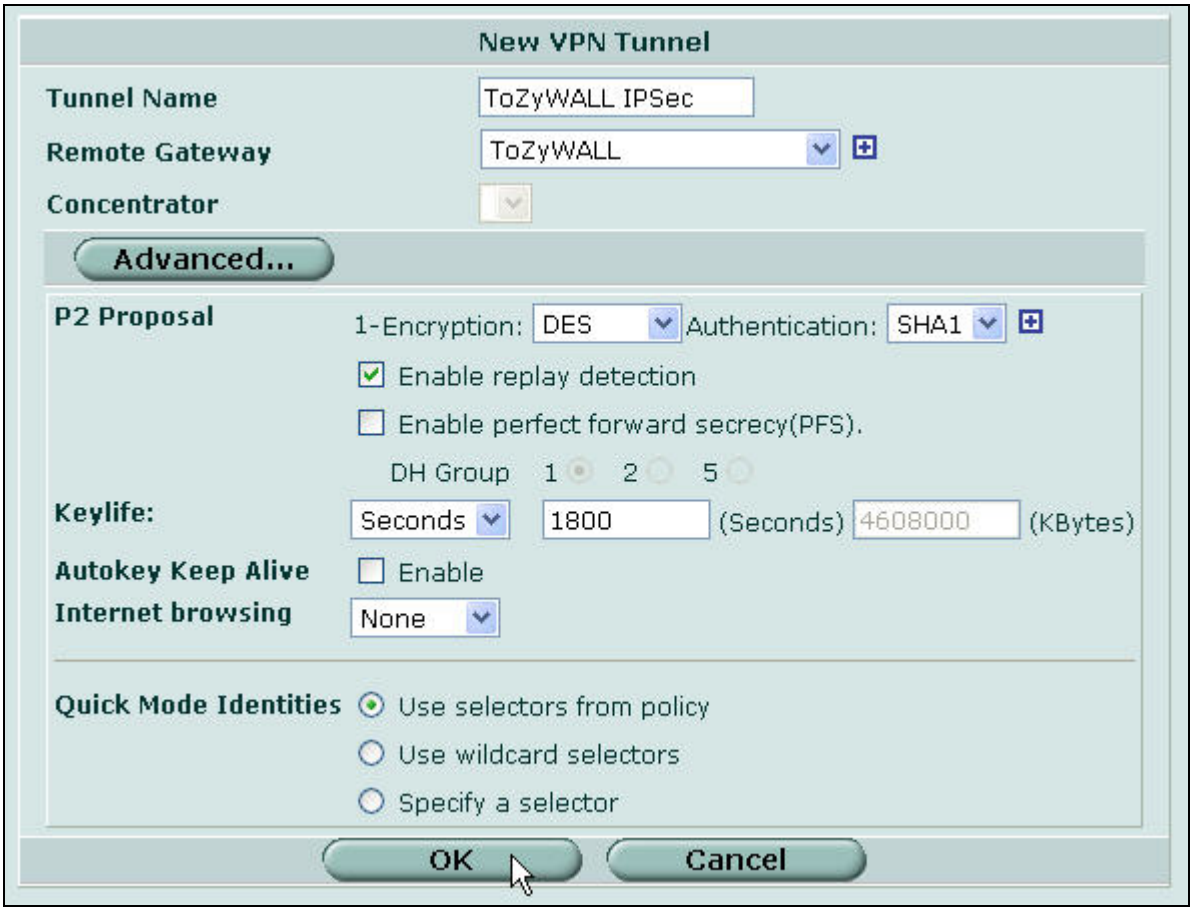


8. Give a name for your VPN, for example "**ToZyWALL IPSec**", and choose **ToZyWALL** policy rule for your Remote Gateway. Then, press **Advanced** button to edit the advanced settings.

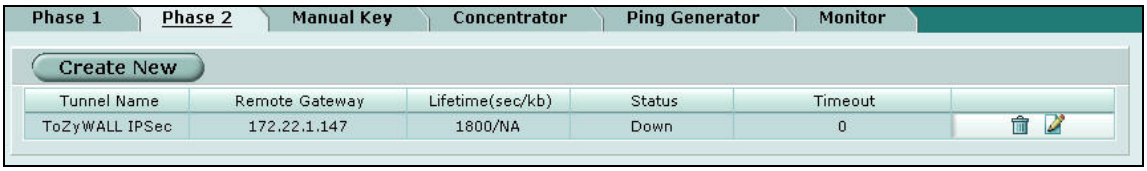


9. On **P2 Proposal** settings, select **Encryption** to **DES**, and **Authentication** to **SHA1**, and also press "-" button to delete the second P2 proposal rules.

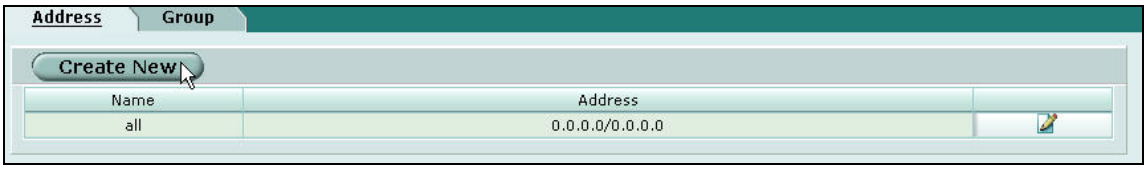
10. To uncheck the **Enable perfect forward secrecy(PFS)** check box. And then, press **OK** button to save the settings.



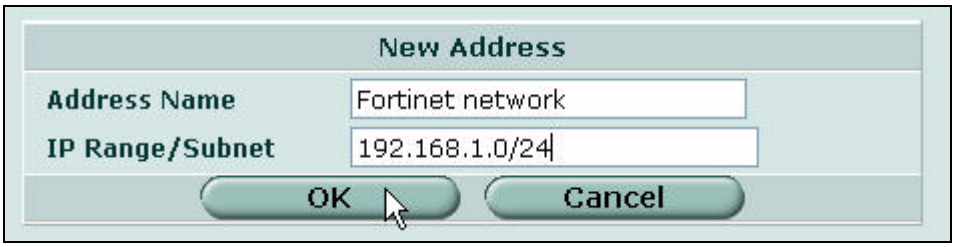
11. After you press the OK button, you will see your IPSec rule(Phase2) on this page.



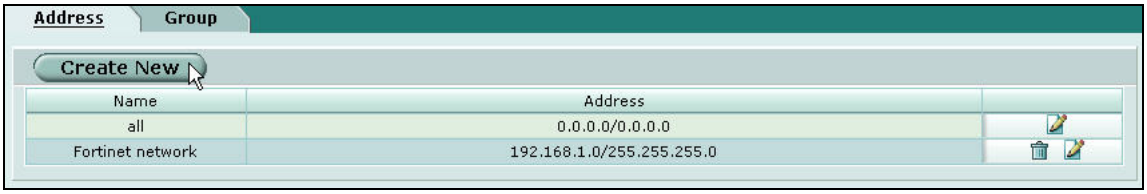
12. On the main page, click **Firewall -> Address**, and then press **Create New** button to edit your address rules.



13. To define the IP source address of the Network behind FortiNet. Giving a name for your address rule, for example "**Fortinet network**", and enter the IP Range/Subnet in the text box. In this example, you should enter **192.168.1.0/24** IP Range/Subnet for the FortiNet network. Then, press **OK** button to save your settings.

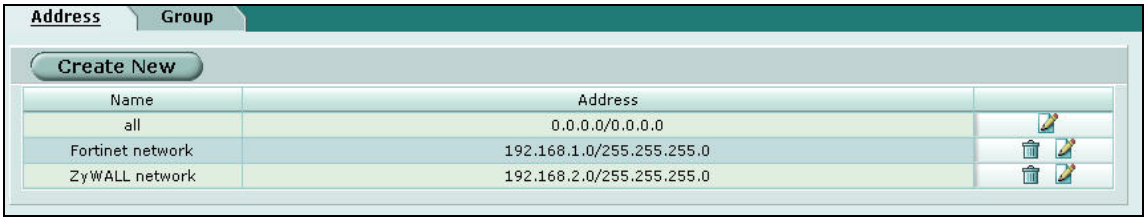


14. Press **Create New** button to edit another address rules.



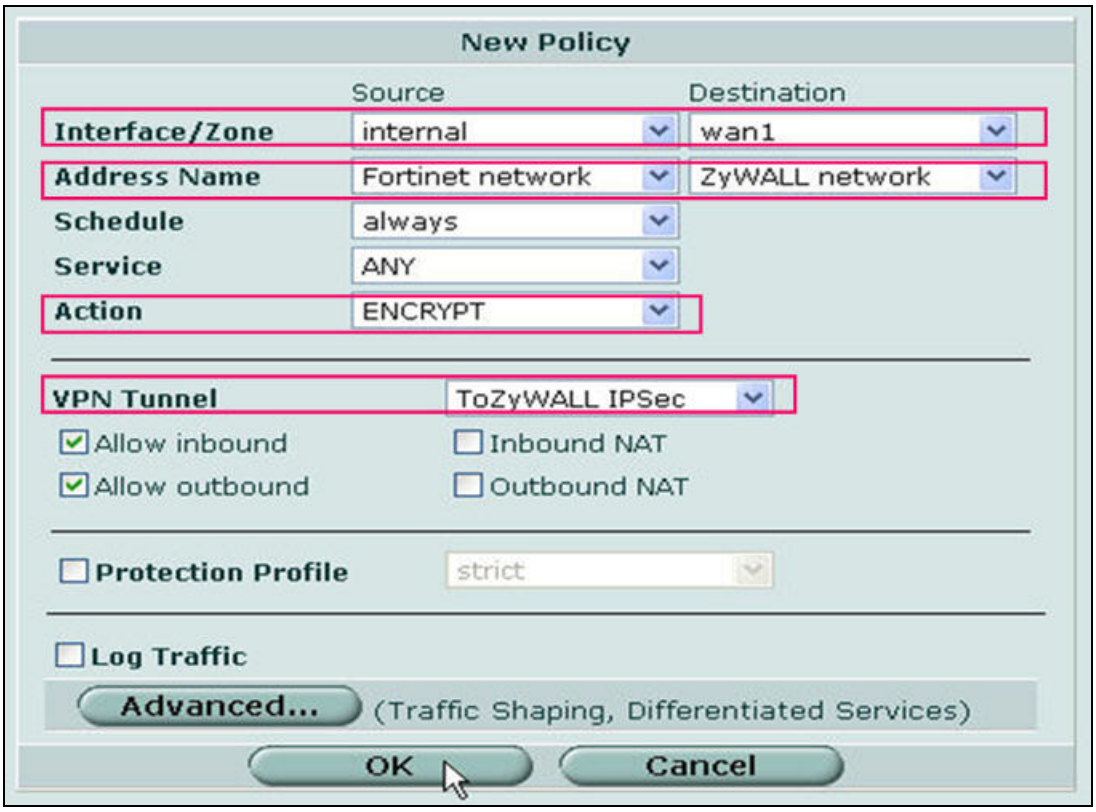
14. 15. To define the IP source address of the Network behind ZyWALL. Giving a name for your address rule, for example "**ZyWALL network**", and enter the IP Range/Subnet in the text box. In this example, you should enter **192.168.2.0/24** IP Range/Subnet for the ZyWALL network. Then, press **OK** button to save your settings.

16. After you finished the settings, you should see two address rules on this page.

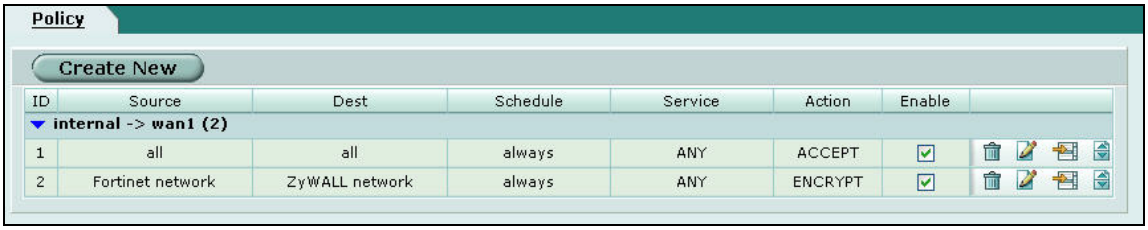


17. On the main page, click **Firewall -> Policy**, and then press **Create New** button to edit your policy rules.

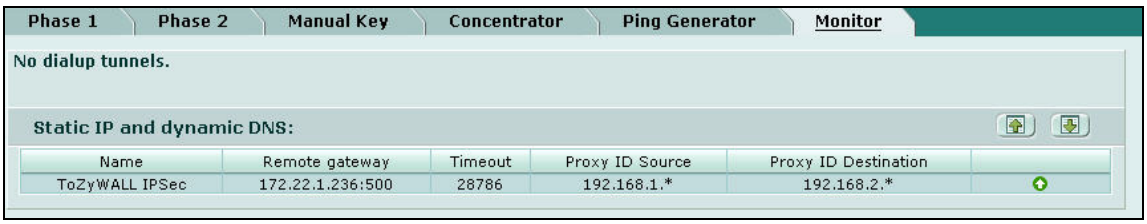
18. On **Interface/Zone** settings, select the interface to internal (private) network, and select the interface to external (public) network. In this example, choose **internal** option for your source Interface/zone, and choose **wan1** option for your destination Interface/Zone.
19. On **Address Name** settings, choose **Fortinet network** rule for your source address rules, and choose **ZyWALL network** rule for your destination address rules.
20. On **Action** settings, choose **ENCRYPT** option, and choose **ToZyWALL IPSec** rule for your VPN Tunnel. Then, press **OK** button to save your settings.



21. After you press the **OK** button, you will the policy rule on this page.



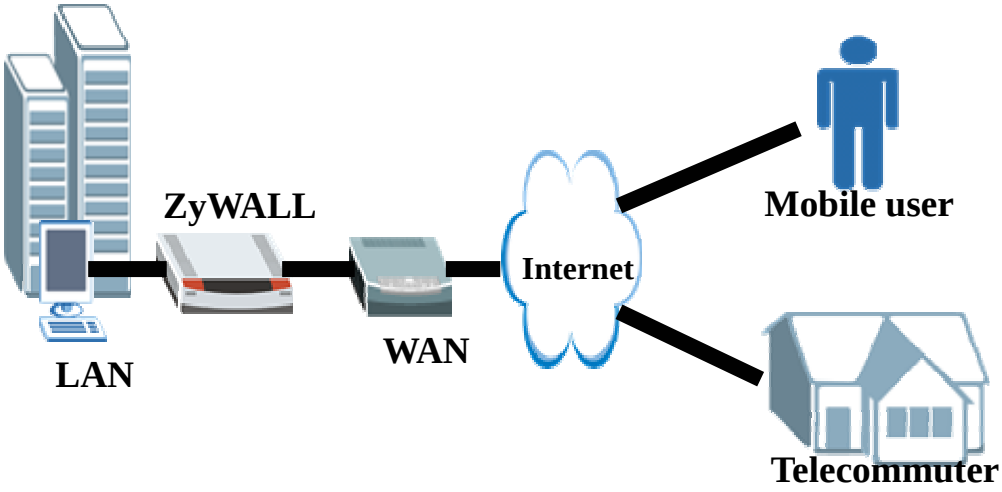
22. Click **VPN** -> **IPSec** -> **Monitor**, this page displays a table that lists all the VPN rules configured on the FortiNet device. You could check the link states here to know your VPN tunnel is up or down.



Remote Access VPN Scenario

The remote access VPN scenario is to provide a remote users secure connections to access corporate network over a public networking infrastructure.

VPN has become the logical solution for remote access connectivity. The remote access VPN scenario is to provide a remote users secure connections to access corporate network over a public networking infrastructure. Deploying a remote access VPN enables corporations to reduce communications expenses by leveraging the infrastructures of Internet service providers. At the same time, VPN allows remote to take advantage of broadband connectivity. Remote users (e.g. mobile users, telecommuters) may use dial-up, ISDN, digital subscriber line (DSL) or cable technologies to gain Internet access



Because IP address is dynamically assigned by service providers, the **Remote Gateway Address** of gateway way policy must be configured with **0.0.0.0** or **domain name**. If "**0.0.0.0**" is used as **Remote Gateway Address**, ZyWALL accepts all attempts from any IP address and authenticate the remote VPN device with pre-shared key or certificate. If the remote entity passes authentication, ZyWALL and remote entity will then generate dynamic shared keys for the IKE SAs and IPSec/QM SAs.

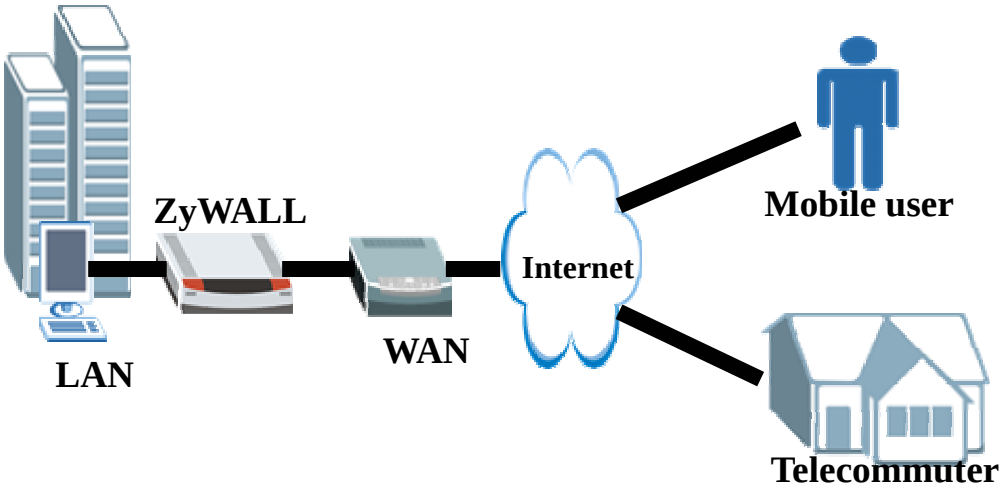
Using xAuth for User Authentication

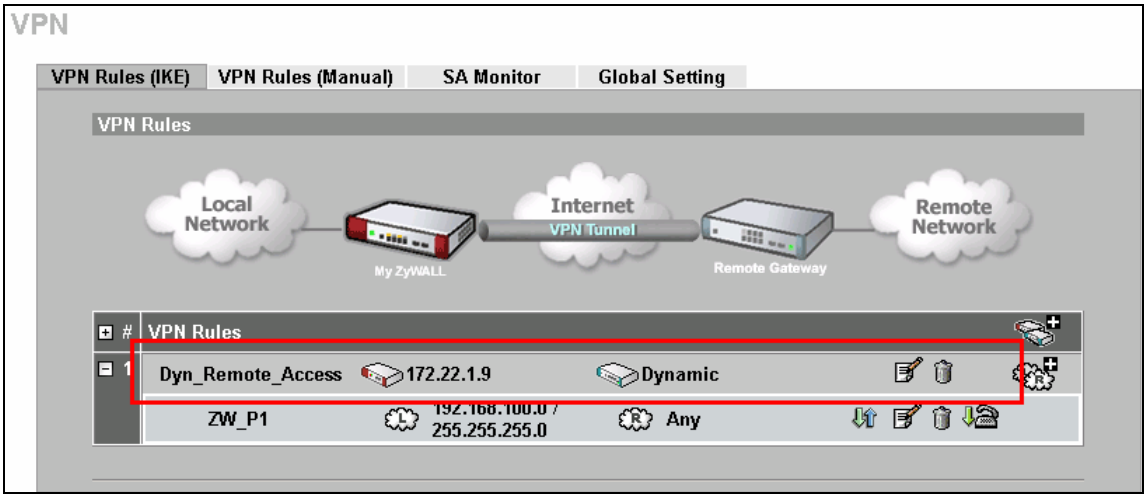
IKE Extended Authentication (Xauth) is a draft RFC developed by the Internet Engineering Task Force (IETF) based on the Internet Key Exchange (IKE) protocol. The Xauth feature is an enhance to the

existing Internet Key Exchange (IKE) Protocol feature. Xauth allows authentication methods to perform user authentication in a separate phase after the IKE authentication phase 1 exchange. The Xauth feature is an extension to the IKE feature, and does not replace IKE authentication.

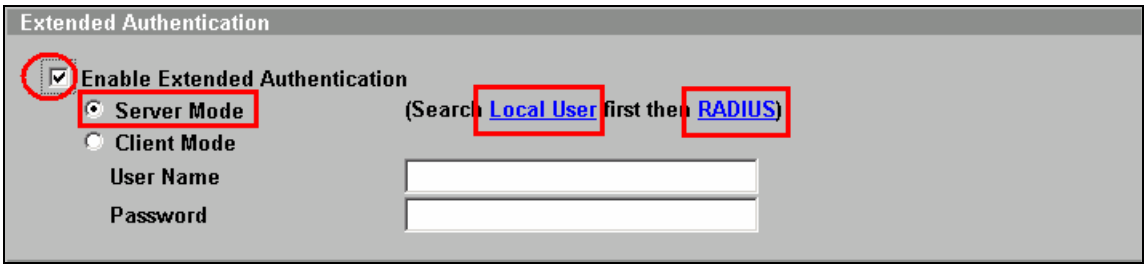
Before Xauth, IKE only supported authentication of the device, not authentication of the user using the device. With Xauth, IKE can now authenticate the user using the device after the device has been authenticated during normal IKE authentication.

Since remote users may use the same pre-shared key for device authentication, it may have some problem once the key is compromised. Otherwise, an extra authentication would be more.

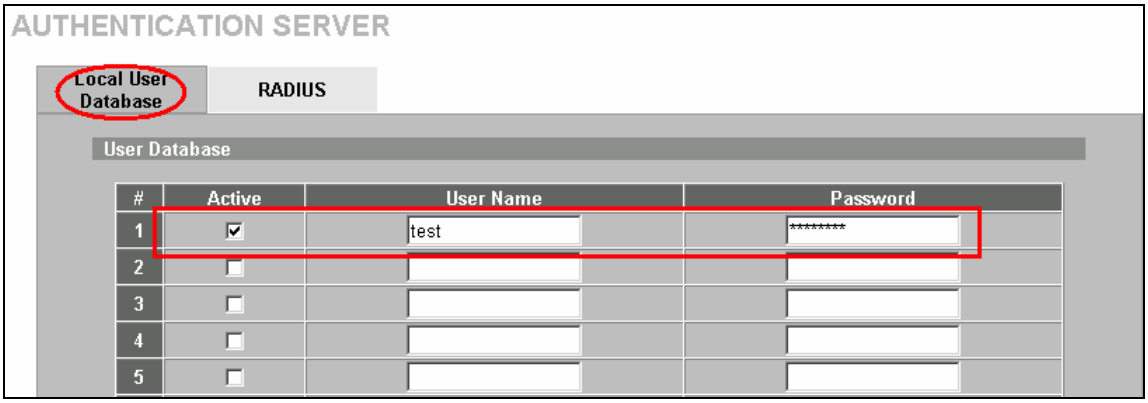




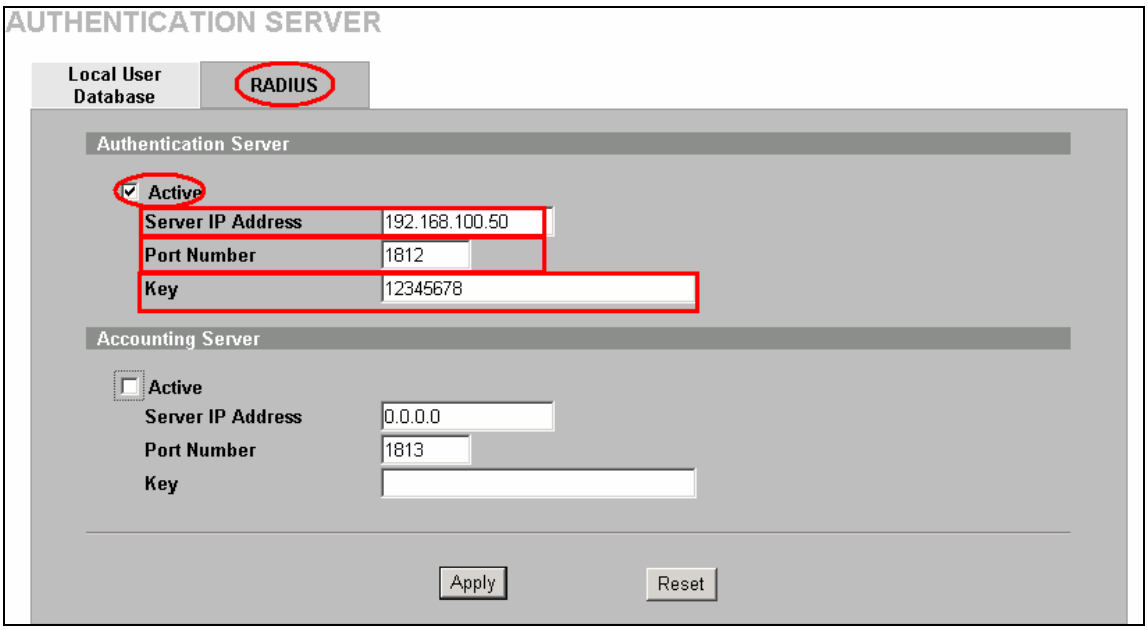
To Use “xAuth” for authentication, enable “Extended Authentication” while configuring “VPN Gateway Policy”. Select “Server Mode” on the VPN concentrator. There are two kinds of user_identification (username/password) database can be used for authentication: Local_User & RADIUS. (Note that Local_User first then RADIUS if both exist).



Local User



RADIUS



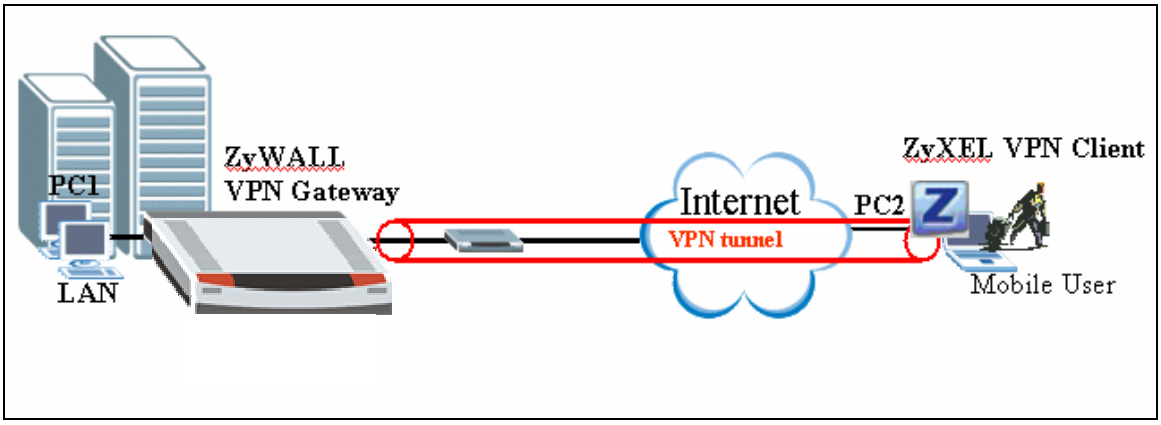
When external “RADIUS” is selected, please input the Service IP address of the external RADIUS server and the shared Key which must be configured on the RADIUS. The default (UDP) port number for RADIUS is 1812. If RADIUS server uses a different port number, please configure it correctly.

ZyXEL VPN Client to ZyWALL Tunneling

1. Setup ZyWALL VPN Client
2. Setup ZyWALL

This page guides us to setup a VPN connection between the VPN software and ZyWALL router. There will be several devices we need to setup for this case. They are VPN software and ZyWALL router.

As the figure shown below, the tunnel between PC 2 and ZyWALL ensures the packets flow between them is secure. Because the packets go through the IPSec tunnel are encrypted. To setup this VPN tunnel, the required settings for the software and ZyWALL are explained in the following sections.



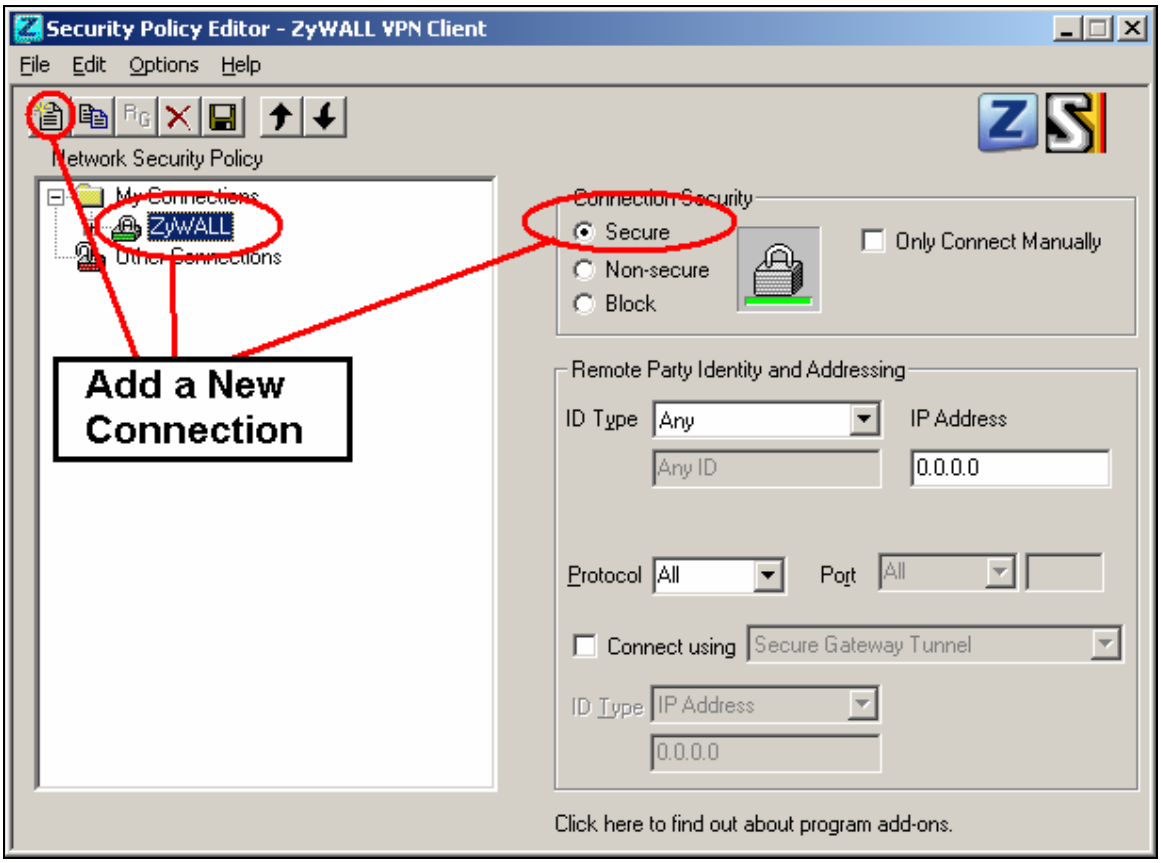
The IP addresses we use in this example are as shown below.

PC 1	ZyWALL	PC2
202.132.171.33	LAN: 202.132.171.1 WAN: 202.132.170.1	202.132.155.33

---

1. Setup ZyWALL VPN Client

1. Open ZyWALL VPN Client Security Policy Editor
2. Add a new connection named 'ZyWALL' as shown below.
3. Select Connection Security to Secure

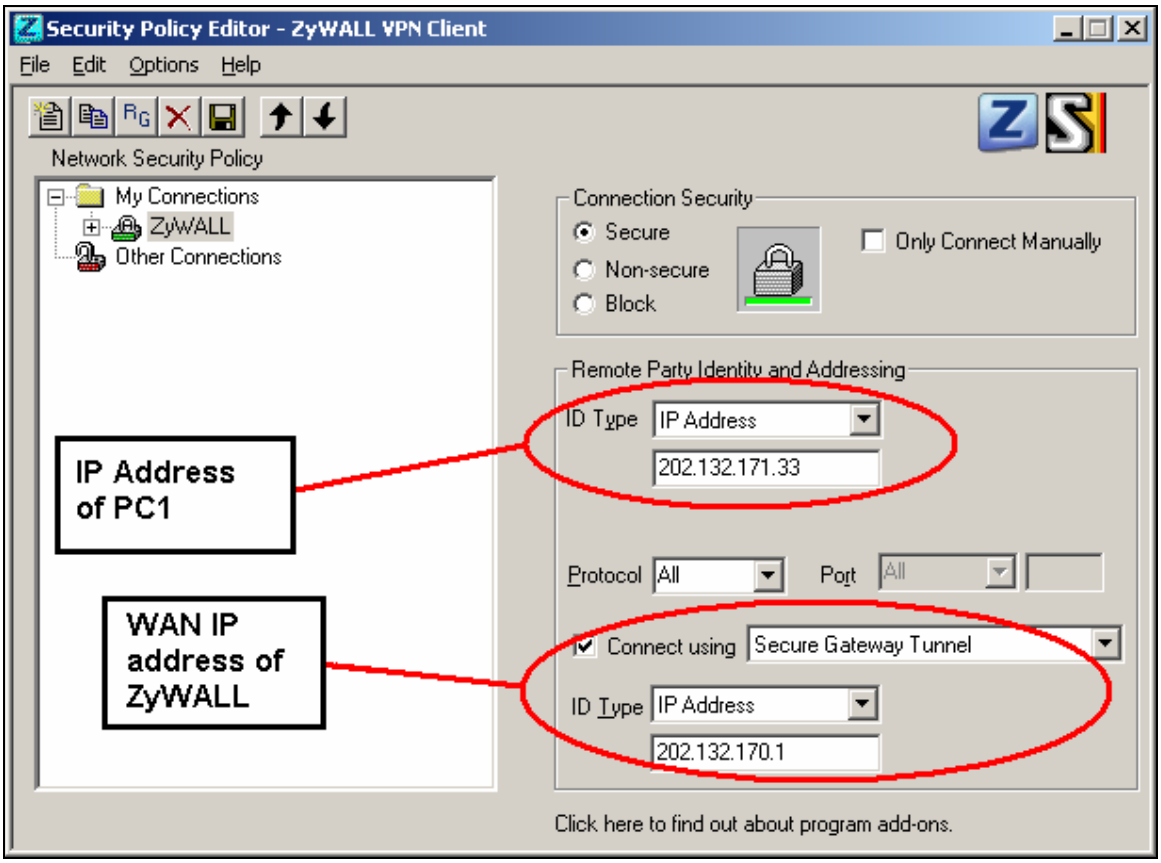


Remote Party Identity and Addressing settings:

4. In **ID Type** option, please choose **IP Address** option, and enter the IP address of the remote PC (PC 2 in this case).

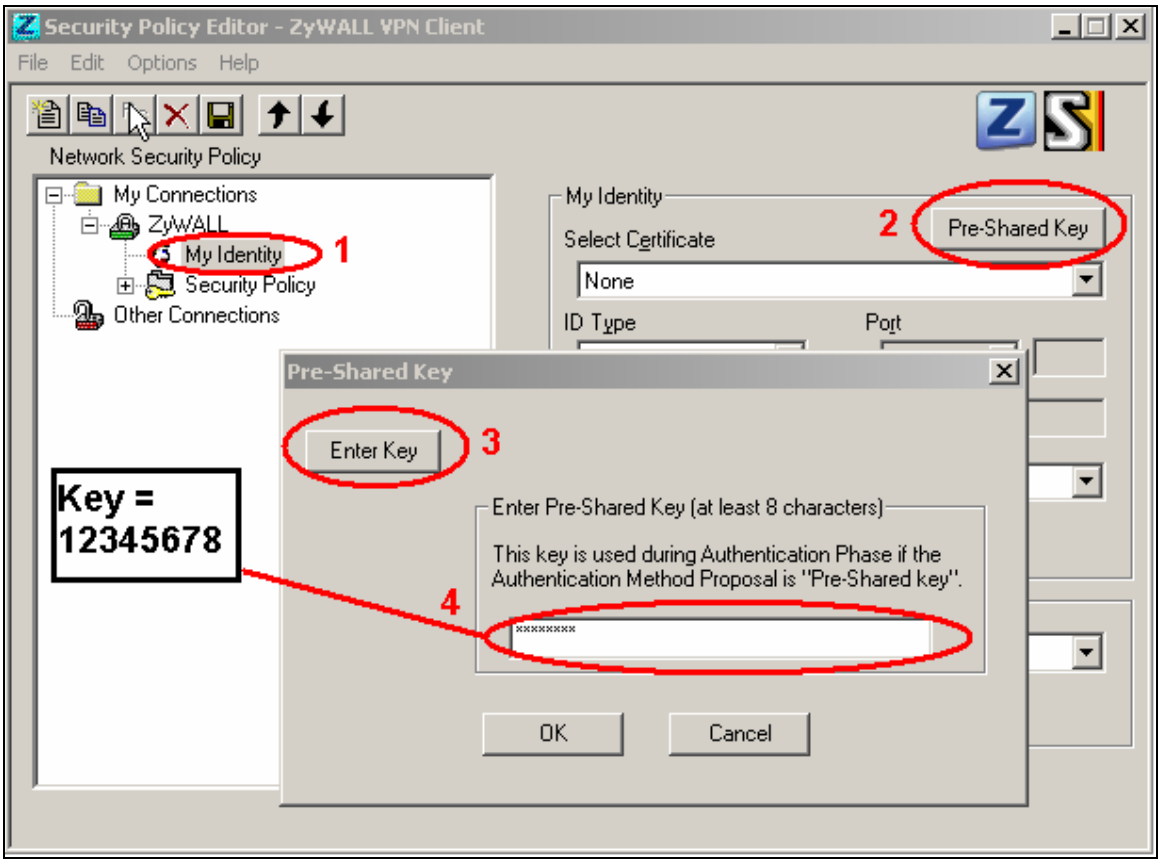
5. Check **Connect using Secure Gateway Tunnel**, please also select **IP Address** as ID Type, and enter ZyWALL's WAN
IP address in the following field.

The detailed configuration is shown in the following figure.



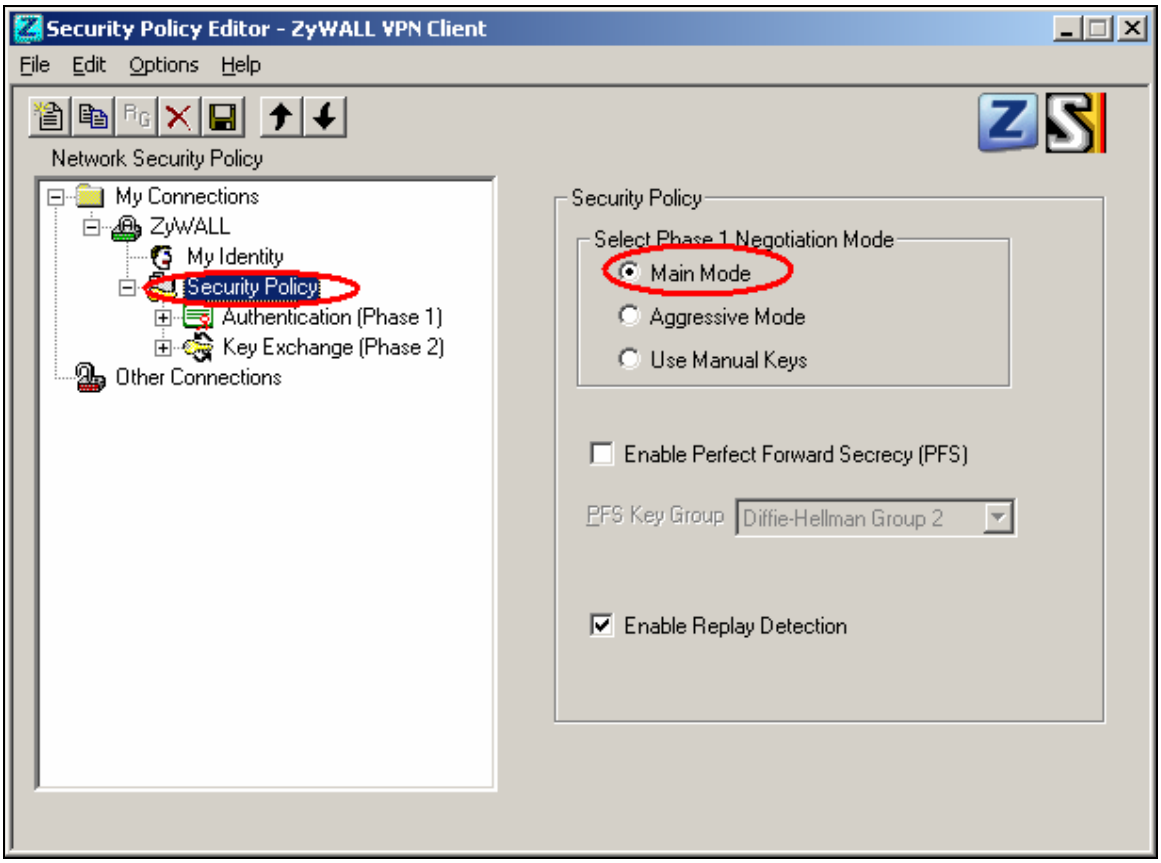
Pre-Share Key Settings:

6. Extend ZyWALL icon, you may see My Identity.
7. Click My Identity; click the Pre-Shared Key icon in the right side of the window.
8. Enter a key you that later you will also need to configure in ZyWALL in the pop out windows. In this example, we enter
12345678. See below.

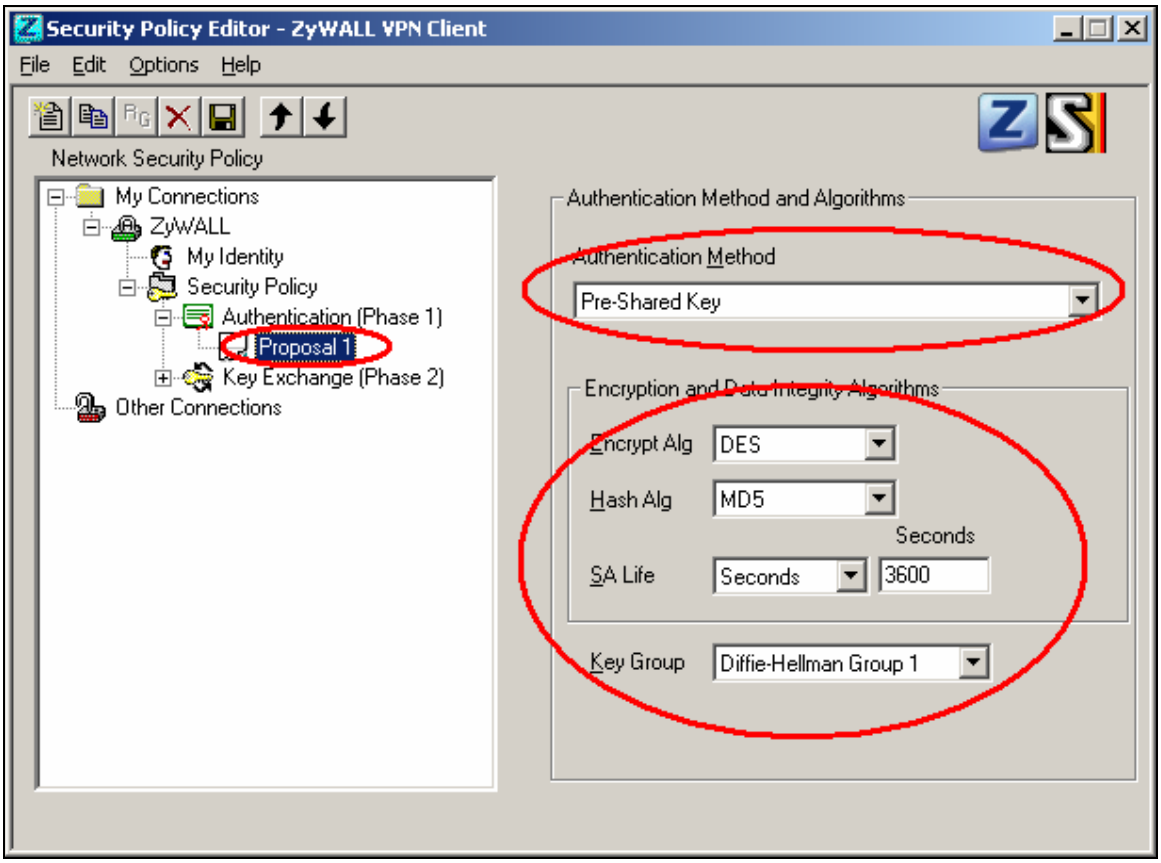


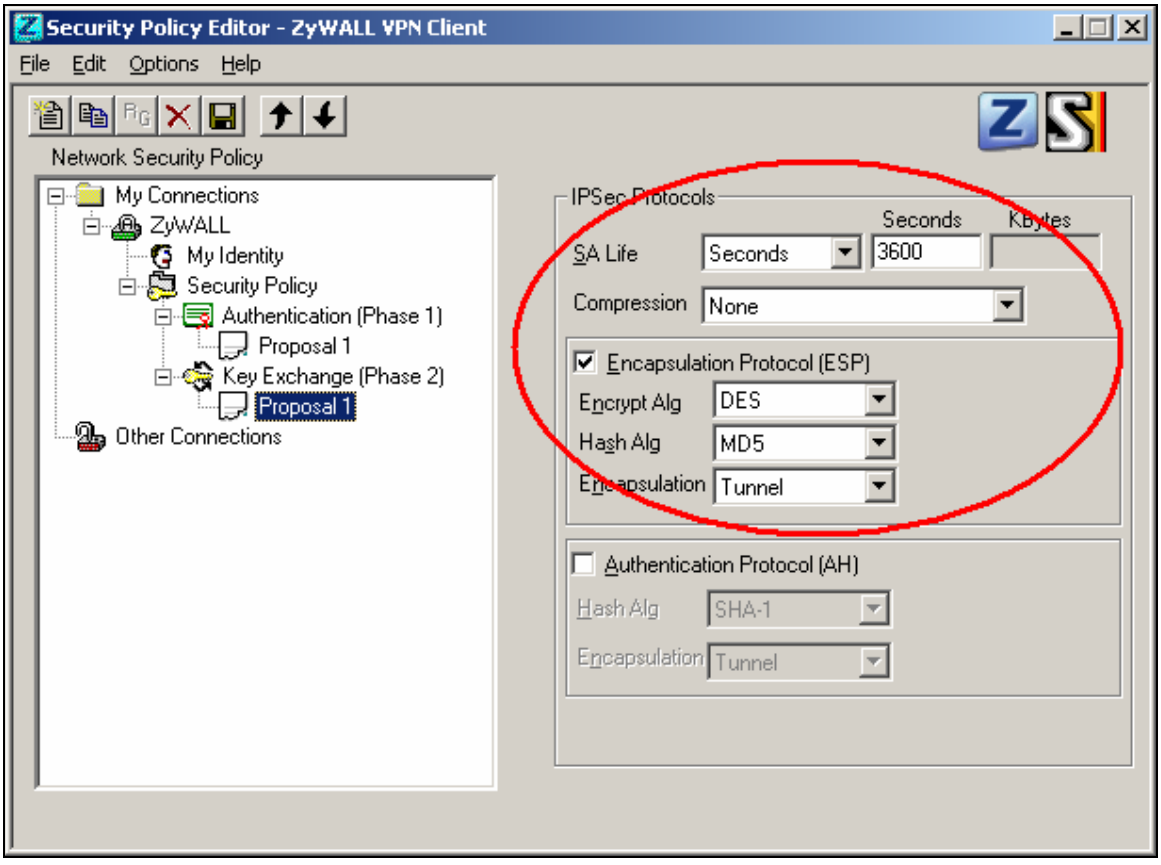
Security Policy Settings:

9. Click **Security Policy** option to choose **Main Mode** as Phase 1 Negotiation Mode



10. Extend **Security Policy** icon, you will see two icons, **Authentication (Phase 1)** and **Key Exchange (Phase 2)**.
11. The settings shown in the following two figures for both Phases are our examples. You can choose any, but they should match whatever you enter in ZyWALL.

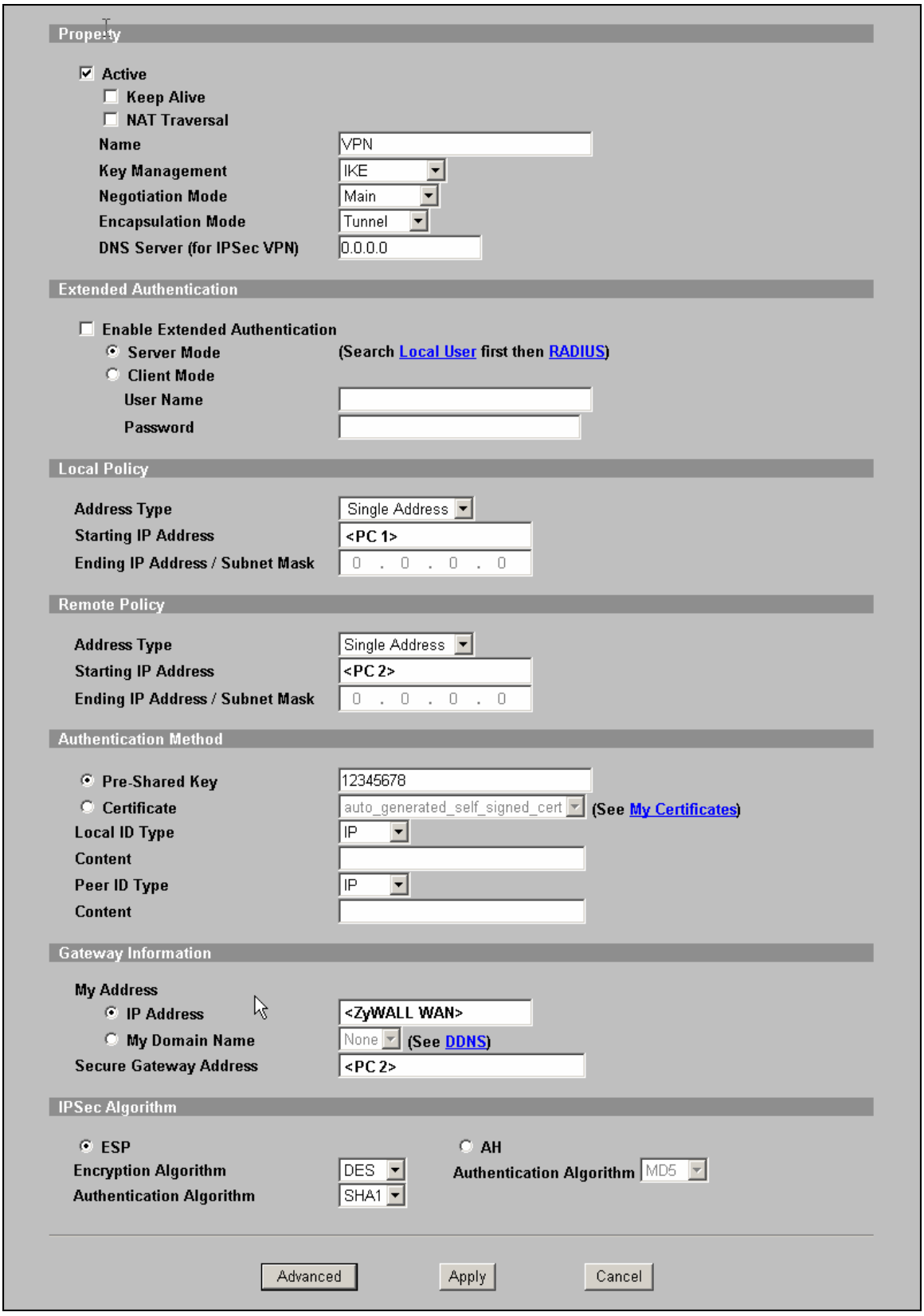




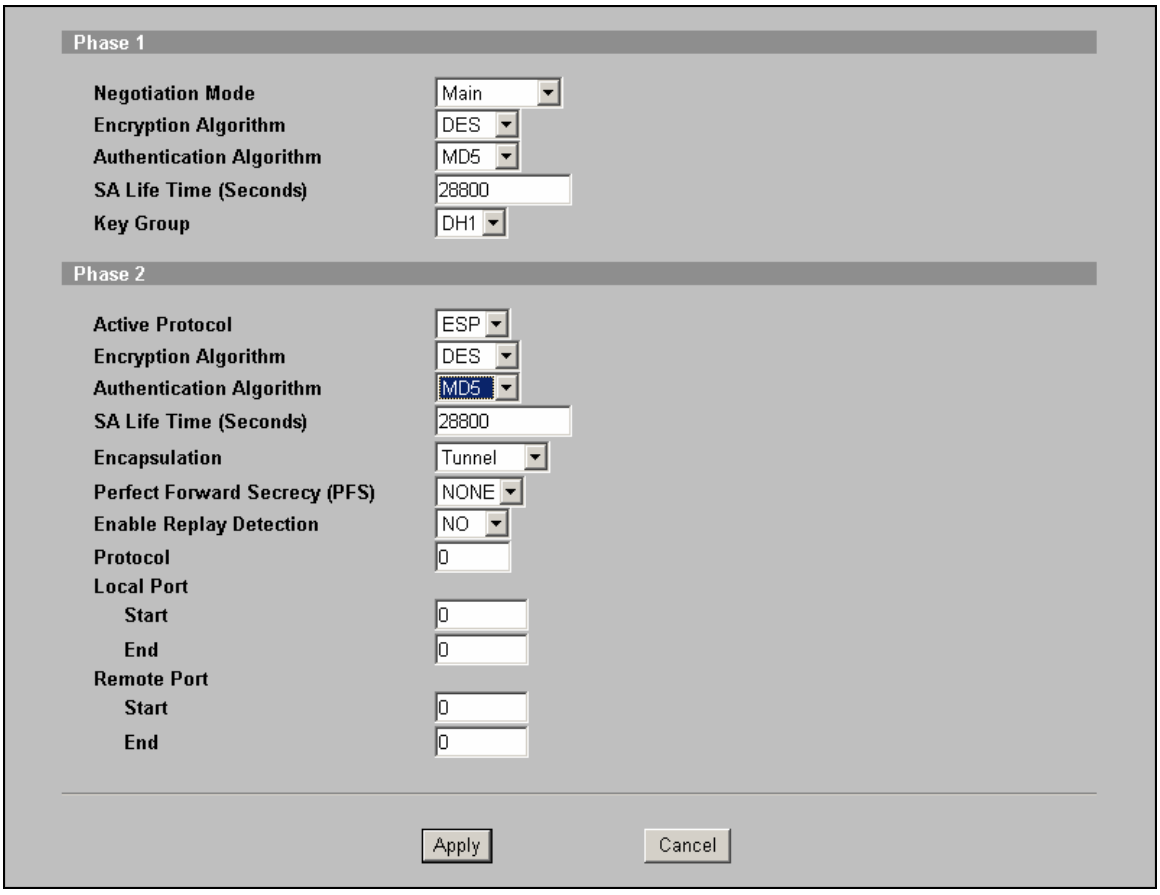
2. Setup ZyWALL VPN

1. Using a web browser, login ZyWALL by giving the LAN IP address of ZyWALL in URL field. Default LAN IP is **192.168.1.1**, default password to login web configurator is **1234**.
2. Go to SECURITY->VPN->Press Add button
3. check **Active** check box and give a name to this policy.
4. Select **IPSec Keying Mode** to **IKE** and **Negotiation Mode** to **Main**, as we configured in ZyWALL VPN Client.
5. **Source IP Address Start** and **Source IP Address End** are **PC 2** IP in this example. (the secure host behind ZyWALL)
6. **Destination IP Address Start** and **Destination IP Address End** are **PC 1** in this example. (the secure remote host) Note: You may assign a range of Source/Destination IP addresses for multiple VPN sessions.
7. **My IP Addr** is the **WAN IP of ZyWALL.**
8. **Secure Gateway IP Addr** is the remote secure gateway IP, which is **PC 1** in this example.
9. Select **Encapsulation Mode** to **Tunnel**.
10. Check the **ESP** check box. (AH can not be used in SUA/NAT case)
11. Select **Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA1**, as we configured in ZyWALL VPN Client.
12. Enter the key string **12345678** in the **Pre-shared Key** text box, and click **Apply**.

See the VPN rule screen shot



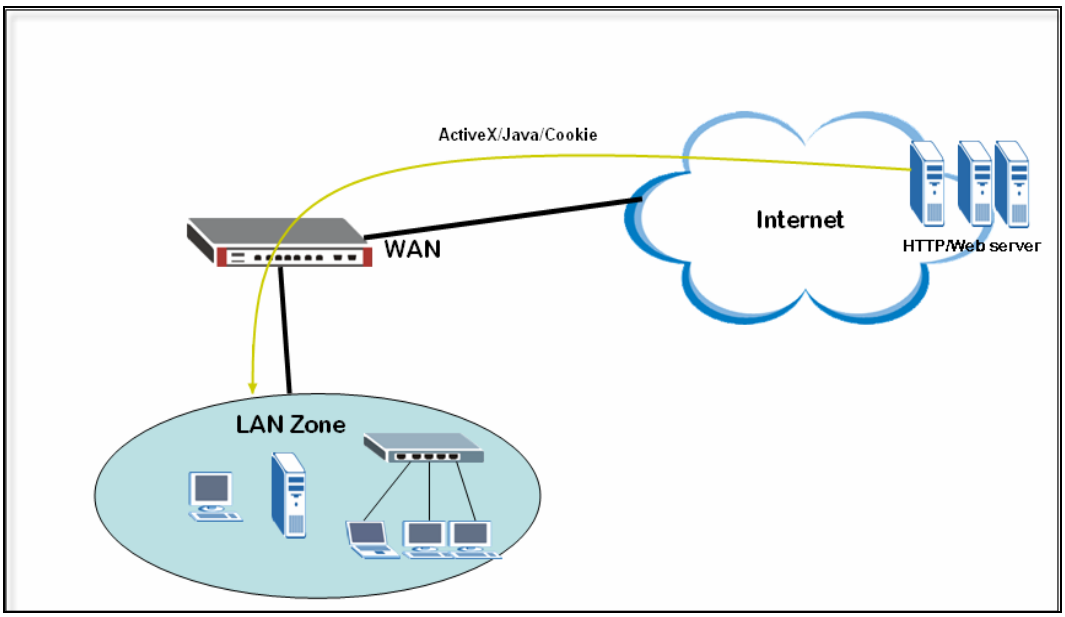
You can further adjust IKE Phase 1/Phase 2 parameters by pressing Advanced button.



Content Filter Application

To filter non-work related and unproductive web surfing to mitigate spyware and phishing threats

Web browsing is one of the most common activity people do on daily bases. However there are lots of threats and traps that are available on the WWW too. Web browsing should be sanctioned as the figure listed below so that the impact of hazardous web content (malicious java and ActiveX), spyware, and phishing attack can be minimized. These attacks are known to be found in websites that provides pirate software, pornography, and other illegitimate websites. Also, the non-business web surfing such as the sports, financial and gambling web sites should be prevented to increase company productivity. With ZyWALL 2 Plus Content Filter service, network administrator can effectively allow/prevent network users from viewing different categories of web sites.

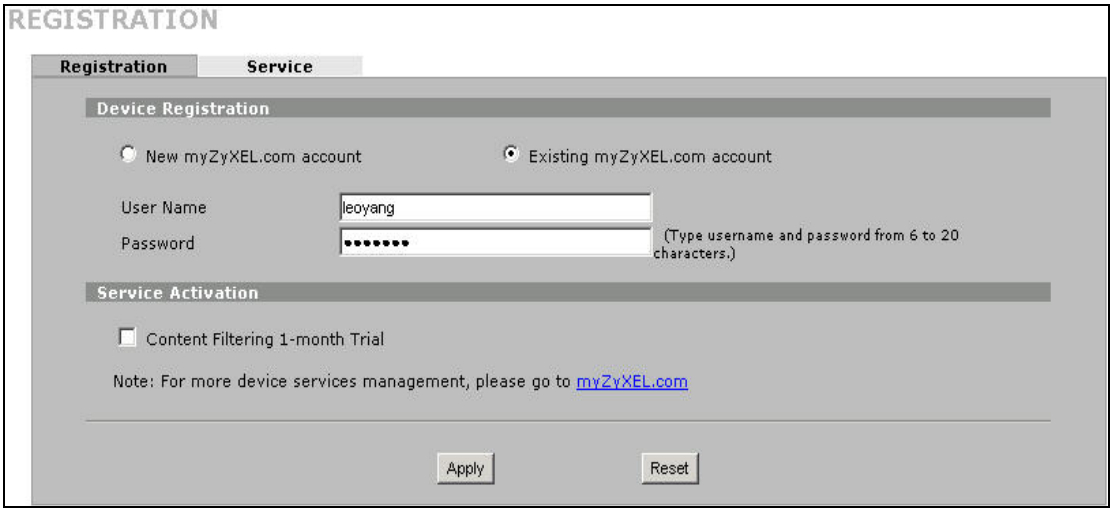


1. Minimize Spyware Attack

As mentioned earlier, pornography websites are known to contain Spyware and Trojans, thus it is recommended to use ZyWALL 2 Plus to prevent users from access these types of websites. Below is an example to illustrate how to configure ZyWALL to fulfill this purpose

1.1 CF License Activation

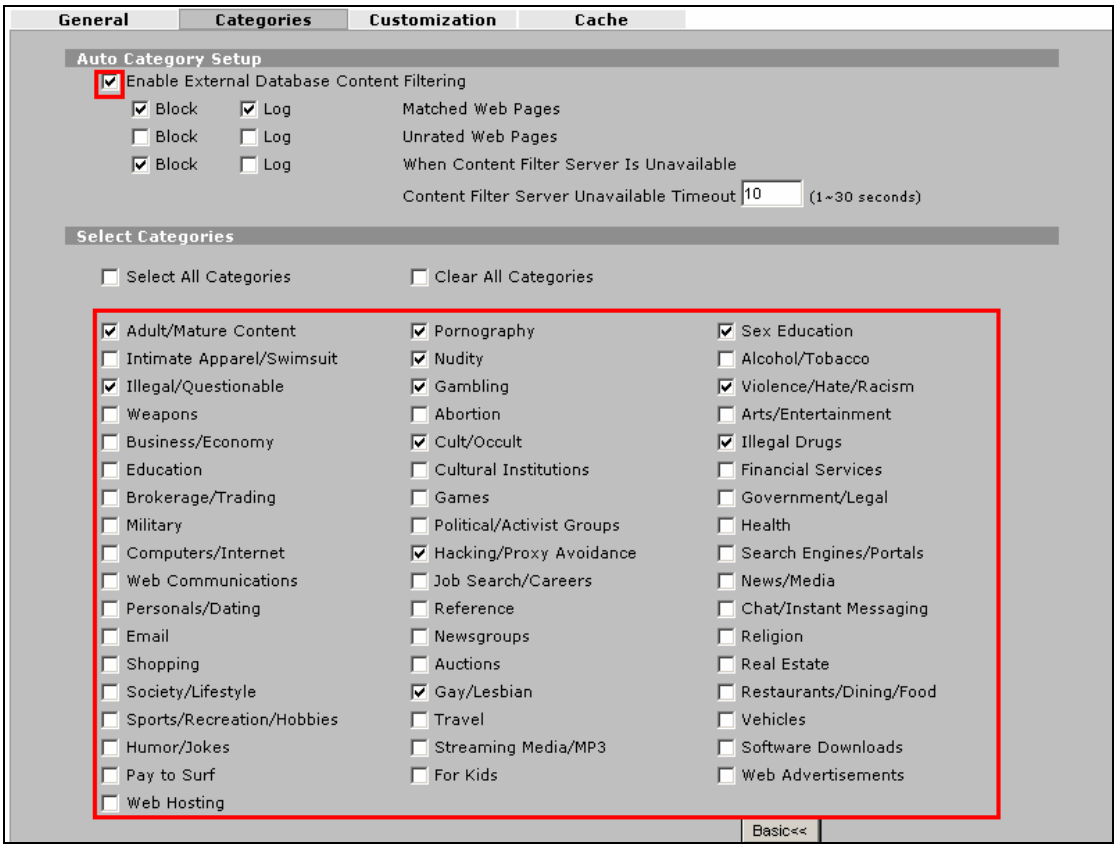
In **Registration** page, if you already have an account exist in myZyXEL.com, then all you have to do is, first select "**Existing myZyXEL.com account**" and enter your username password, and select Content Filter 1 month trial version to activate



1.2 Using external database content filtering to achieve best result

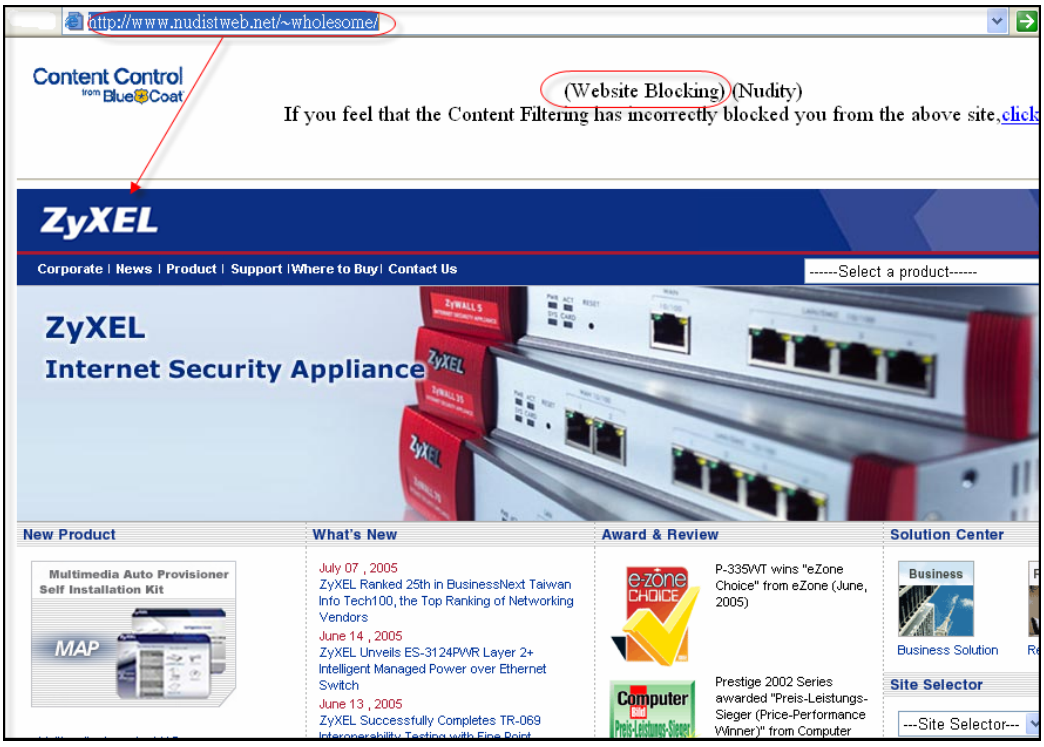
Enable external database content filtering in the **CONTENT FILTER -> Categories**, with selecting the "**Adult/Mature Content**", "**Sex Education**", "**Pornography**", "**Nudity**", "**Hacking/Proxy Avoidance**",

"**Violence/Hate/Racism**", "**Gay/Lesbian**", "**Gambling**", "**Illegal/Questionable**", "**Illegal Drugs**", and "**Cult/Occult**" categories(*most spyware comes from such kind of websites*) to be filtered while accessing a website which contains these specified categories of contents.



1.3 Demonstrate Content Filtering by an example:

Using a browser to browse the nudity website, for example, *www.nudistweb.net*, it will be blocked and redirected to *www.zyxel.com* with "**(Website Blocking)**" message displayed at the moment.



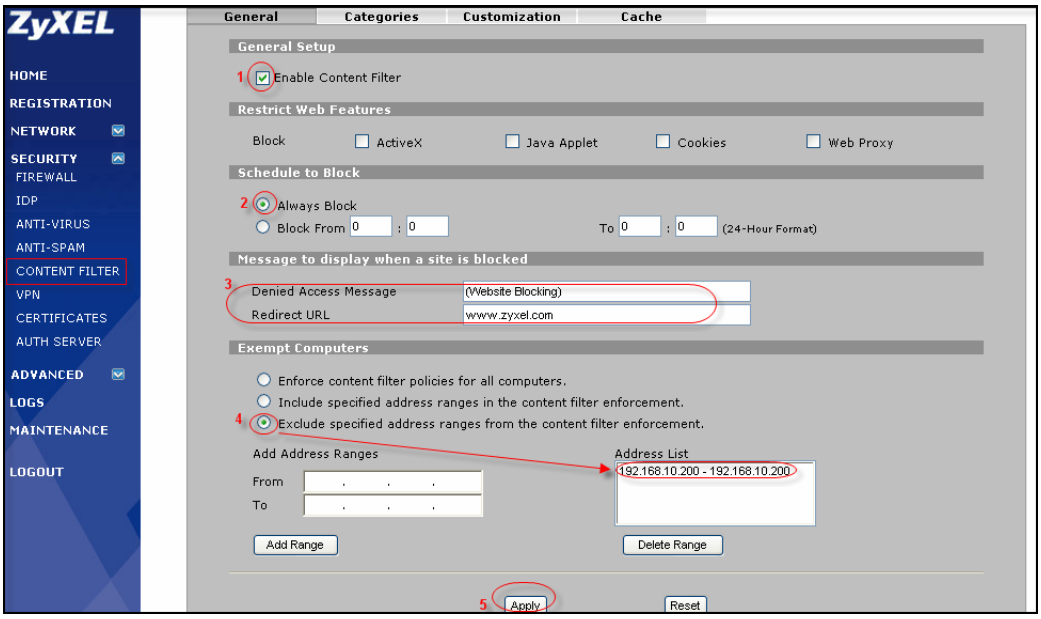
2. Proactively Prevent Phishing

Phishing – The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. With the CF feature provided by ZyWALL 2 Plus, network administrator can dramatically lower the chance of company network to prevent users accessing the known phishing websites.

2.1 ☐ Setup the ZyWALL 2PLUS CF service to block the known phishing web sites

2.1.1 The General settings:

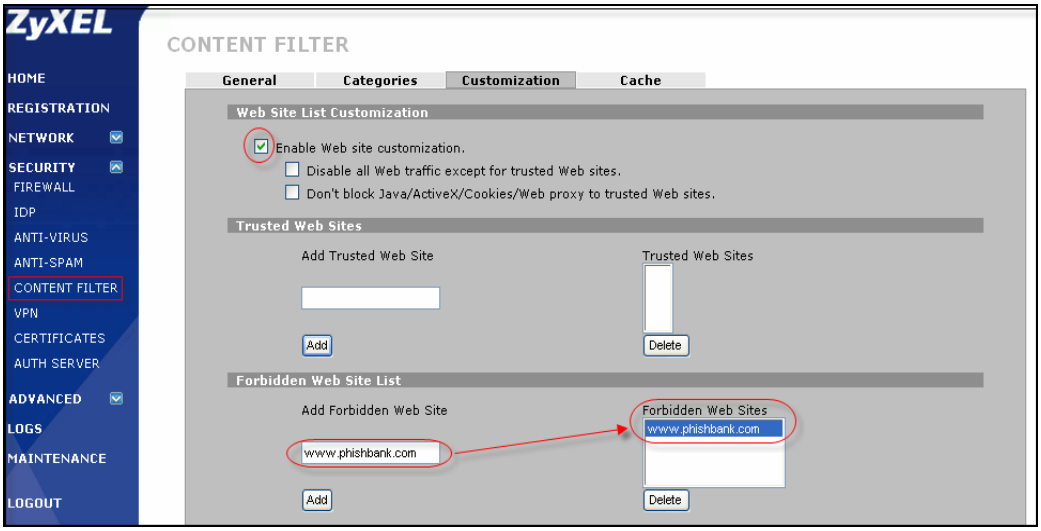
1. In **CONTETN FILTER ->General**, check the **Enable Content Filter** check box to enable CF function.
2. In **Schedule to Block**, select the **Always Block** to let CF engine to do blocking the web sites.
3. In **Message to display when a site is blocked**, you can input the text, say "**(Website Blocking)**", to remind the users that the website he is trying to access is blocked. And you can input the URL in the **Redirect URL** field, for example, "www.zyxel.com" to redirect the original URL to this redirect- URL.
4. In **Exempt Computers** item, we can select **Exclude specified address ranges from the content filter enforcement** to NOT apply content filter policies to the specified IP address ranges, for example, if the CEO's computer which is assigned an IP address: 192.168.10.200 needed NOT to be applied by CF engine, the IT staff can add this IP address 192.168.10.200 to the list to meet this exclusion requirement.
5. Click on the **Apply** button to save the settings.



2.1.2 ☐ Customize the Forbidden web sites which are known phishing web sites

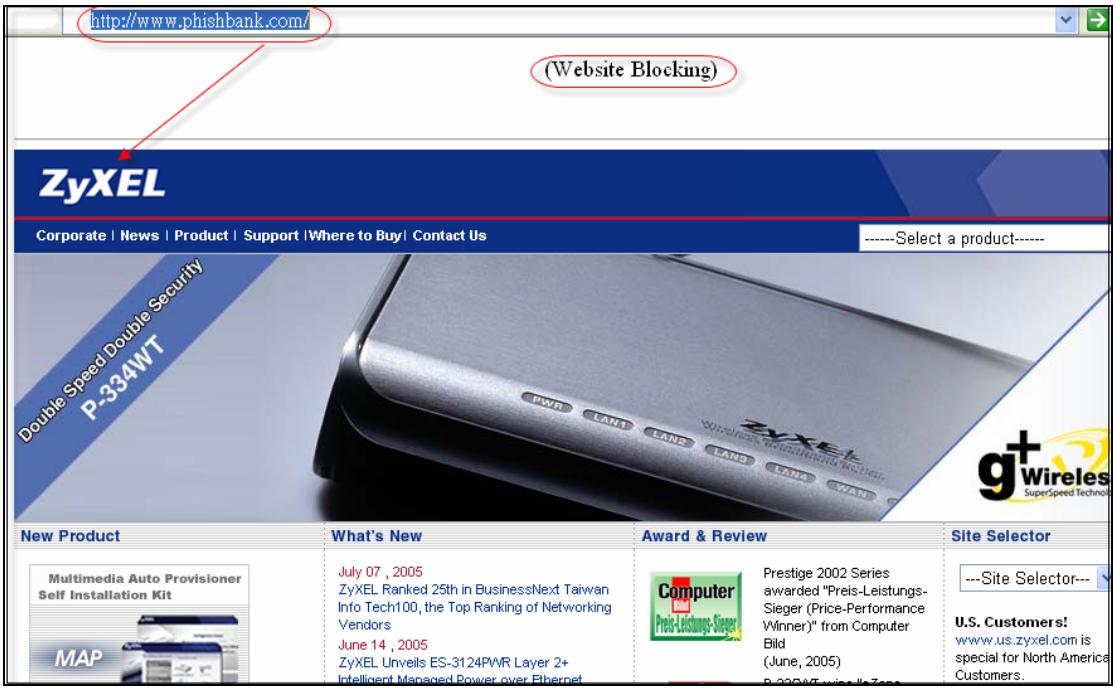
In addition to use external content filter server to do filtering policies, we can customize the filter policies as our own. Just as the settings in the **CONTETN FILTER->Customization**: Check **Enable Web site customization** check box. Enter the distrusted web site in the **Forbidden Web Site** list.

(The forbidden list is similar to the black list.)



2.1.3 ☐ Demonstrate "*Customization*" Content filtering by an example:

Using a browser to browse "*www.phishbank.com*", the attempt will be blocked (because "*www.phishbank.com*" is added in the forbidden list) and will be redirected to "*www.zyxel.com*" with "**(Website Blocking)**" message displayed at the moment.



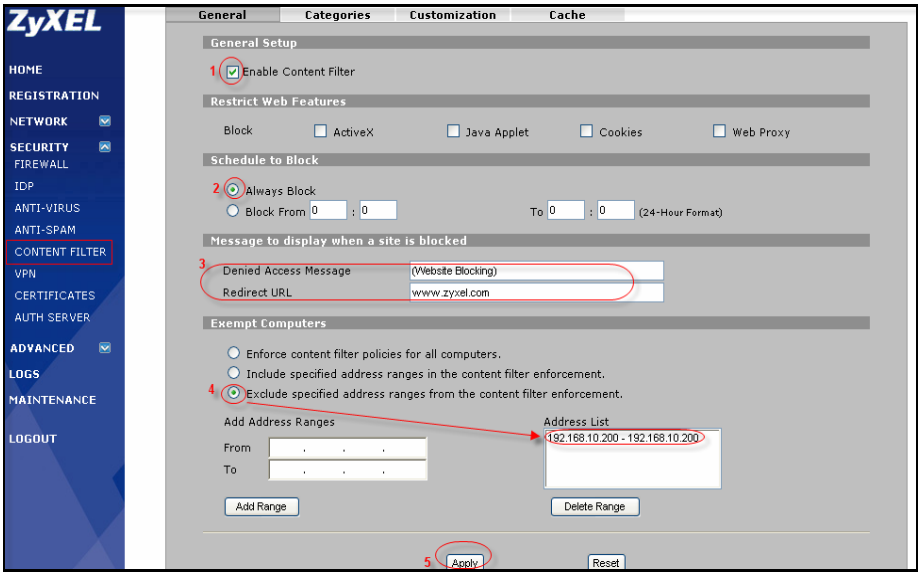
3. Prevent non-business web surfing

Below is an example that demonstrates how to configure the ZyWALL 2 Plus CF service to prevent employee from surfing websites that are not related to work.

Setting up the ZyWALL 2 Plus CF service to block the non-business web surfing.

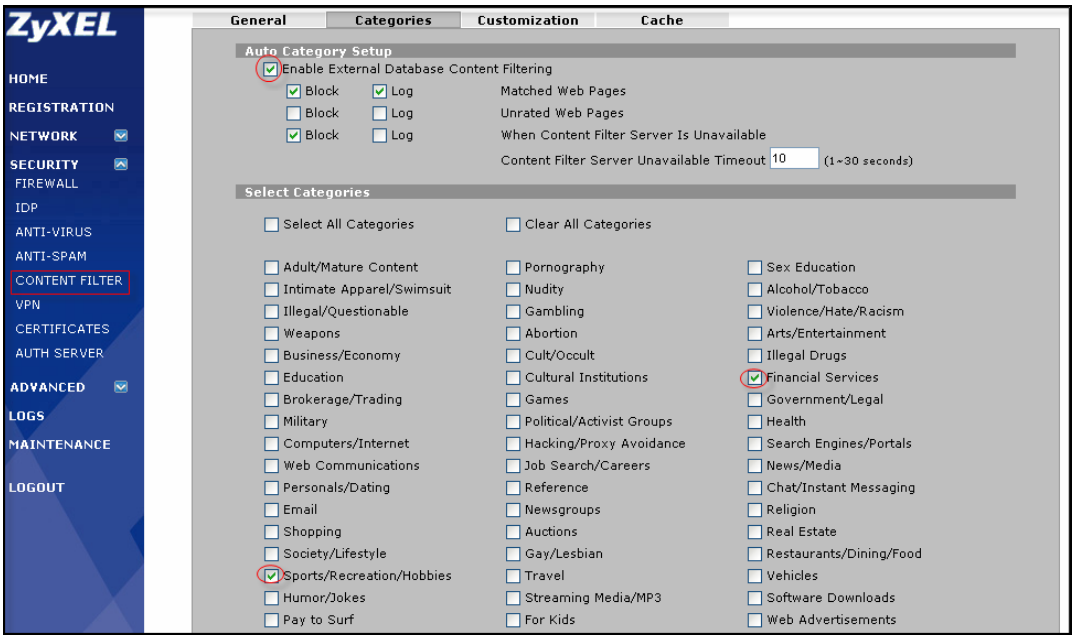
3.1 The General settings:

1. In **CONTETN FILTER ->General**, check the **Enable Content Filter** check box to enable CF function.
2. In **Schedule to Block**, select the **Always Block** to let CF engine to do blocking the websites all the time.
3. In **Message to display when a site is blocked**, you can input the text, say "**(Website Blocking)**", to remind the users that the website he is trying to access is blocked. And you can input the URL in the **Redirect URL** field, for example, "www.zyxel.com" to redirect the original URL to this redirect-URL.
4. In **Exempt Computers**, we can select **Exclude specified address ranges from the content filter enforcement** to NOT apply content filter policies to the specified IP address ranges, for example, if the CEO's computer which is assigned an IP address: 192.168.10.200 needed NOT to be applied by CF engine, the IT staff can add this IP address 192.168.10.200 to the list to meet this exclusion requirement.
5. Click on the **Apply** button to save the settings.



3.2 Using external database content filtering

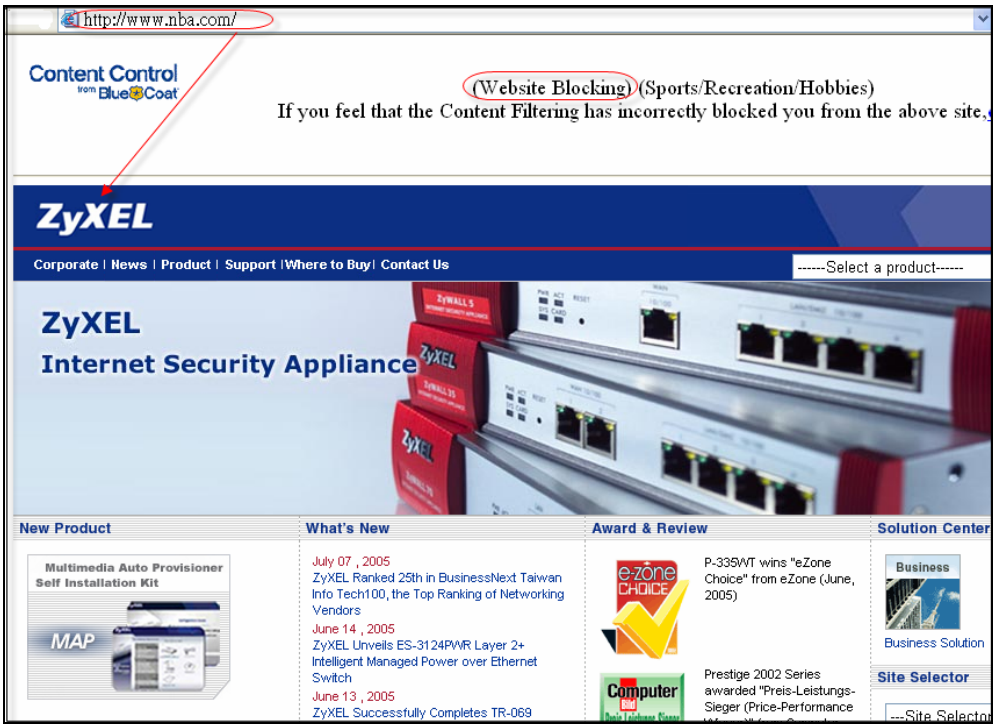
If you have registered the CF service, you can enable external database content filtering in the **CONTENT FILTER -> Categories** page, with selecting the categories check boxes to specify the types of contents to be filtered while accessing a website which contains these specified categories of contents. As the figure listed below, "**Sports/Recreation/Hobbies**" and "**Financial Services**" are selected.



3.3 Demonstrate Content Filtering by an example:

Using a browser to browse the sports website, for example, *www.nba.com*, it will be blocked and redirected

to *www.zyxel.com* with "**(Website Blocking)**" message displayed at the moment.



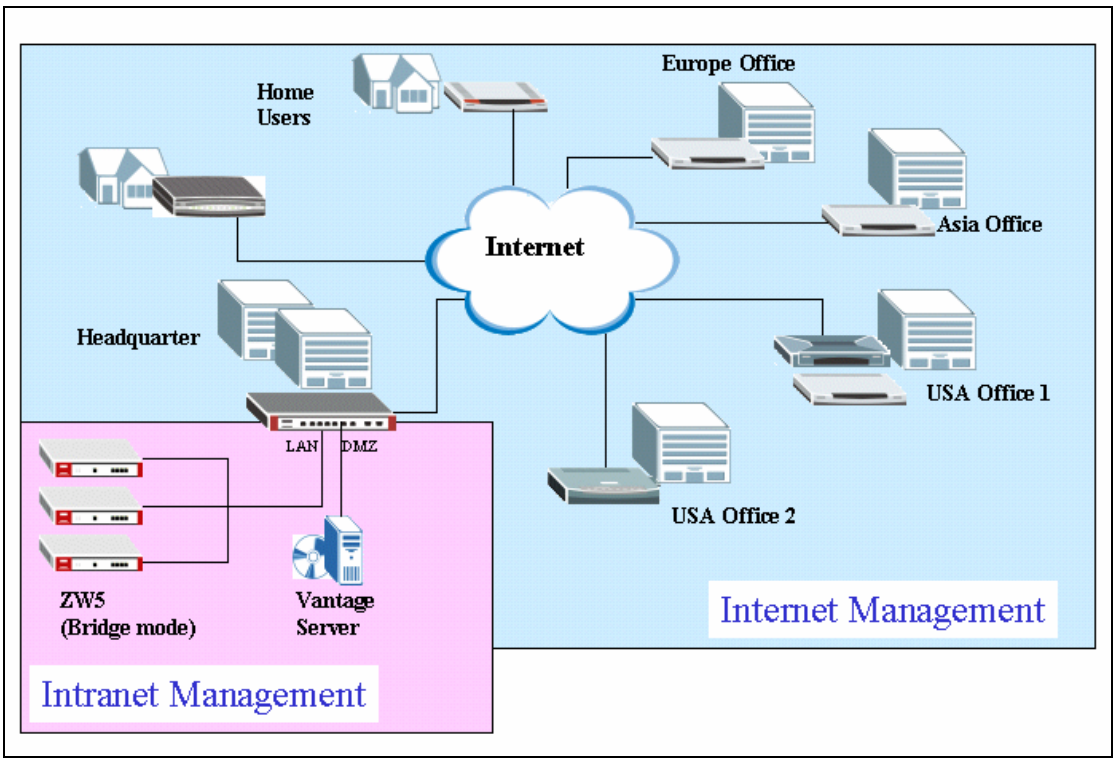
Centralized Management

Using Vantage CNM for Management

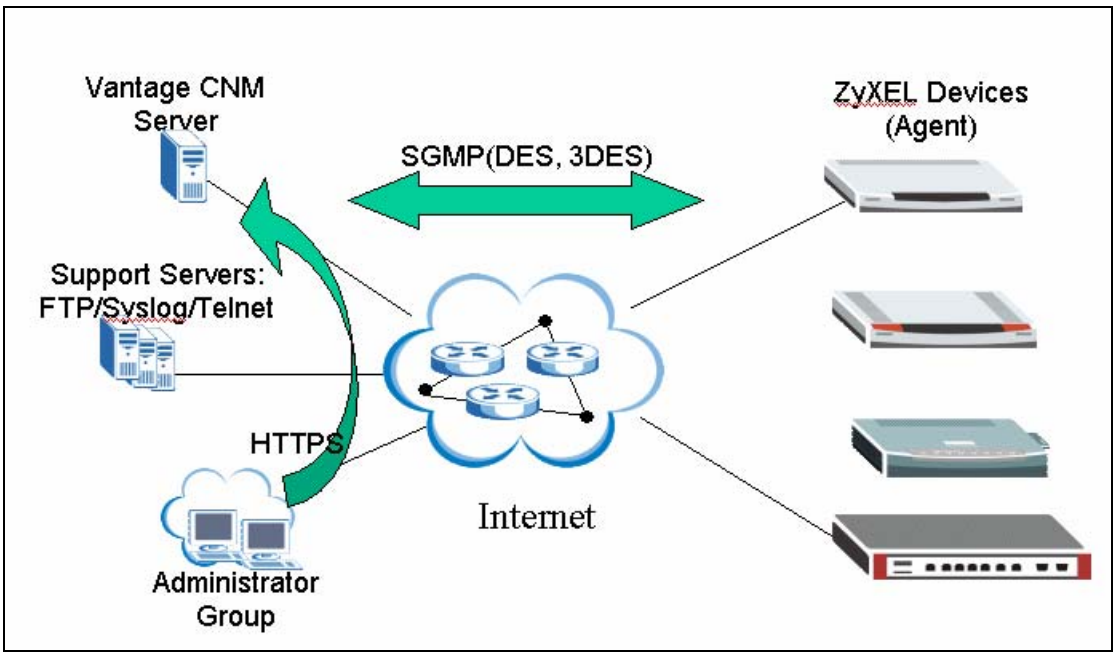
Vantage CNM is a centralized network management solution that allows users to easily configure, manage and monitor ZyWALL devices from any location.

Vantage CNM provides some key features like Centralized Firewall Management, Firmware Upgrade and Management, Intuitive Device and Account Monitoring, Logs and Alarms, One-click VPN and Multiple Administrator, Multiple Domain Management.

The following diagram depicts an example of the network environment for using Vantage CNM.



To manage your ZyWALLs through Vantage CNM, user needs to prepare Vantage CNM server and 3rd party FTP/Syslog/Telnet servers. For the detailed installation & registration process (to myZyXEL.com), please refer to **Vantage CNM Support Note**.



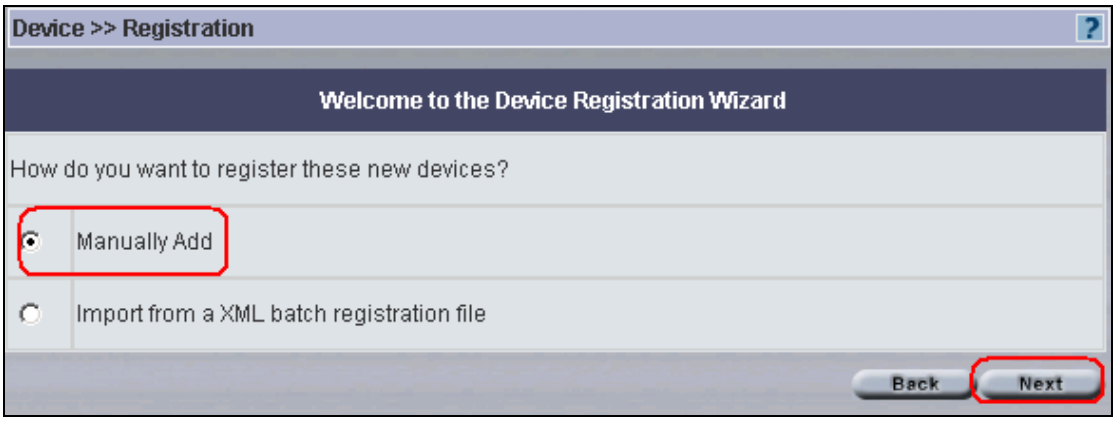
In the following section, we will explain how to add your ZyWALL to Vantage CNM server manually. Note that ZyWALL must be registered on Vantage CNM before it can be managed via Vantage CNM. In

the following section, we will explain how to register device manually. Devices can be also added (imported) to Vantage CNM through XML files. For detailed operation, please refer to **Vantage CNM Support Note**. Please check **CNM Reference Guide for XML description files.pdf** for detailed description.

Add device manually

Step 1. Left click on the folder (e.g. AAA) and go to **Device**>>**Registration**.

Step 2. Select **Manual Add**, and press **Next**. Select No, for not to associate the device to the device owner now, then press Next.

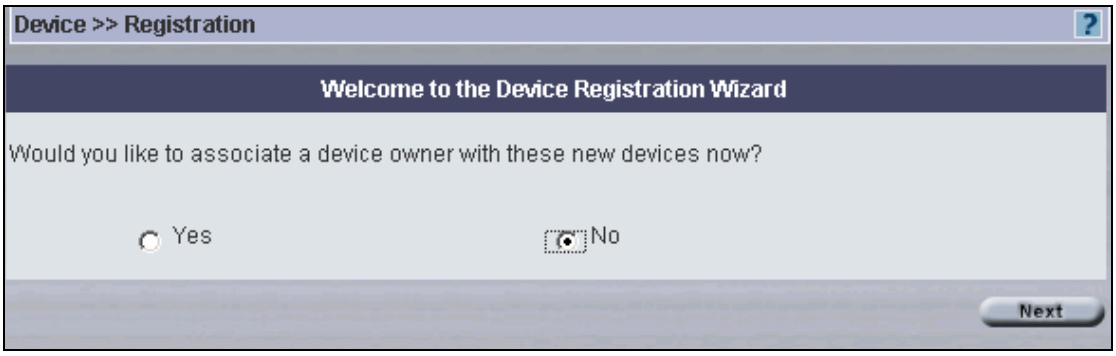


You can register (add) as many devices as you wish at one time via importing XML file to Vantage. In the XML file, you need to define

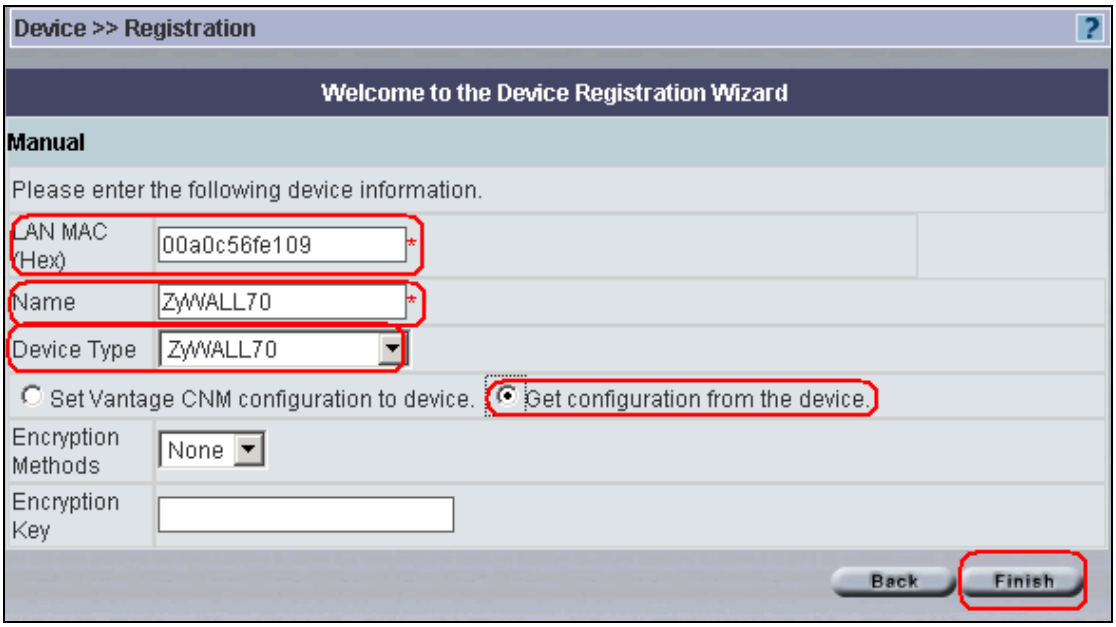
1. device type
2. device name
3. device's LAN MAC address

The XML file can be used for mass deployment.

User can assign a device owner or leave it to the owner of folder AAA.

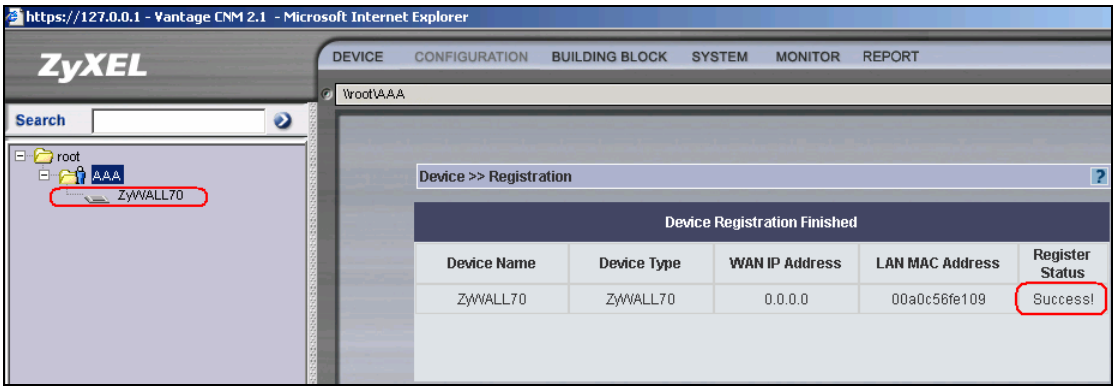


Step 3. Input the MAC address of LAN interface of the device. Give this device a name. Select the corresponding Device Type, press **Finish**.

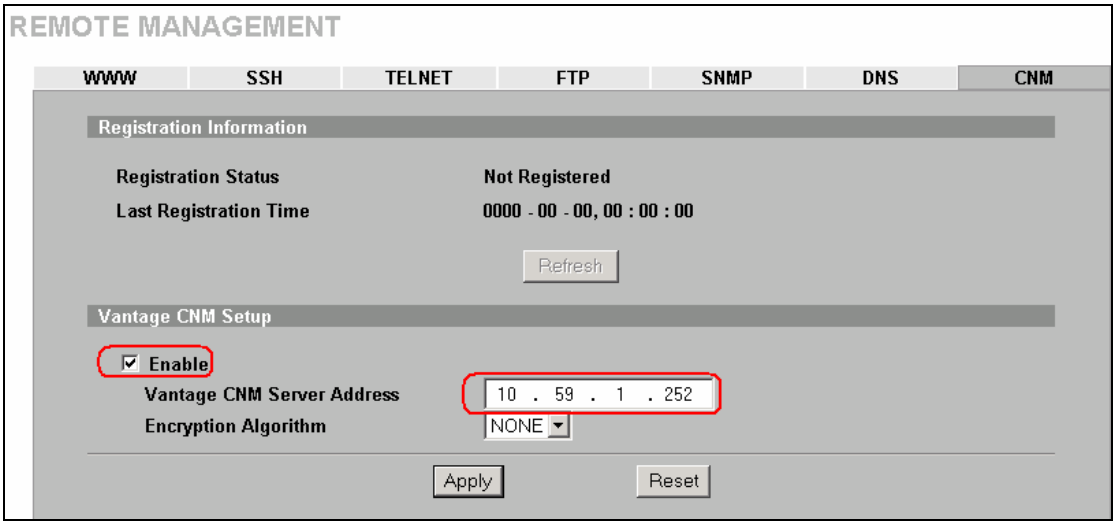


Note that if the ZyWALL has been deployed (configured) and you want to retrieve the configuration from device. You can select the option “Get configuration from the device”. Otherwise, you can use “Set Vantage CNM configuration to device” to overwrite existing configuration on device as soon as it registers to Vantage CNM.

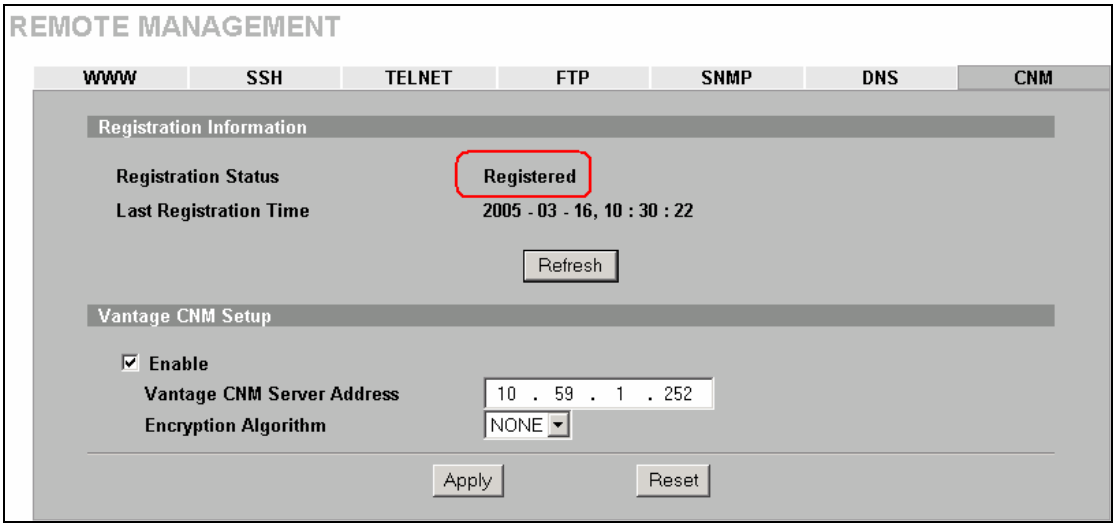
After finishing the configuration on Vantage CNM, click on “Finish” to finish the registration of device on CNM and following screen will show up and ZyWALL is added to CNM under folder AAA.



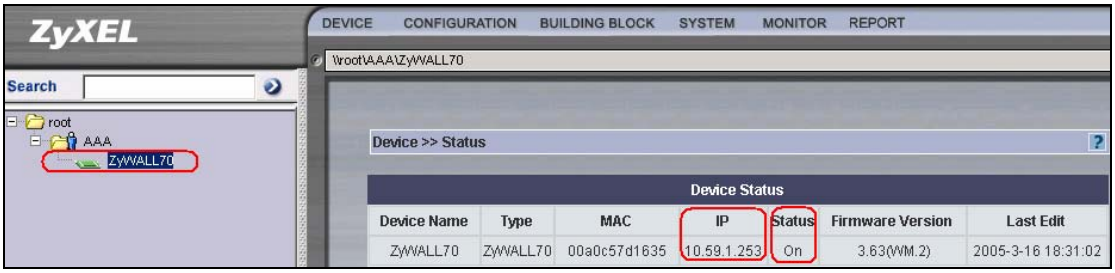
Step 4. On the device, go to **ADVANCED->REMOTE MGMT->CNM**, enable Vantage CNM and configure Vantage CNM Server Address in the filed. If Encryption Algorithm is enabled, you must select the same algorithm and secret key on both device and Vantage CNM. In the following case, the Encryption Algorithm is disabled.



Step 5. After configuring CNM remote management on device, ZyWALL will start to register itself to configured Vantage CNM server. After exchanging the configuration between ZyWALL and Vantage CNM, the Registration Status will change to “Registered”. At this moment, the configuration is synchronized on both device and Vantage CNM.



On Vantage CNM, the device icon will turn green and the device status will change to “On” and the WAN IP of the device will be shown on the content screen.



FAQ

A. Product FAQ

A01. 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.

A02. 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.

A03. 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.

A04. 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.

A05. Does the ZyWALL support PPPoE?

Yes. The ZyWALL supports PPPoE since ZyNOS 2.50.

A06. 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.

A07. 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.

A08. How can I configure the ZyWALL?

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

A09. 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.

A10. Does ZyWALL support dynamic IP addressing?

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

A11. 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.

A12. 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.

A13. 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.

A14. 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.

A15. 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.

A16. 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.

A17. 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.

A18. 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.

A19. 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.

A20. 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).

A21. 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. WinXP/2000 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.

A22. 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.

A23. 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.

A24. 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.

A25. 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.

A26. 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.

A27. 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.

A28. 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.

A29. What is STP (Spanning Tree Protocol) /RSTP (Rapid STP)?

When the ZyWALL is set to bridge mode, (R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP-compliant bridges in your network to ensure that only one path exists between any two stations on the network. The configuration is especially for the advanced user who knows the protocol well.

A30. What is the flow ZyWALL handles inbound and outgoing traffic?

(1) For a ZyWALL with **router** mode, following are the inspection flow for inbound and outgoing traffic.

Traffic from WAN: -> NAT -> Firewall-> Policy Route -> Load Balance -> Static Route -> IDP -> AV -> AS -> CF -> BWM

Traffic to WAN: -> Firewall -> Policy Route -> Load Balance -> Static Route -> IDP -> AV -> AS -> CF -> BMW -> NAT

B. Firewall FAQ

B01. 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.

B02. 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.

B03. 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.

B04. 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.

B05. 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.

B06. 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

B07. 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.

B08. 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.

B09. 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.

B10. 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.

B11. What is Brute-force attack?

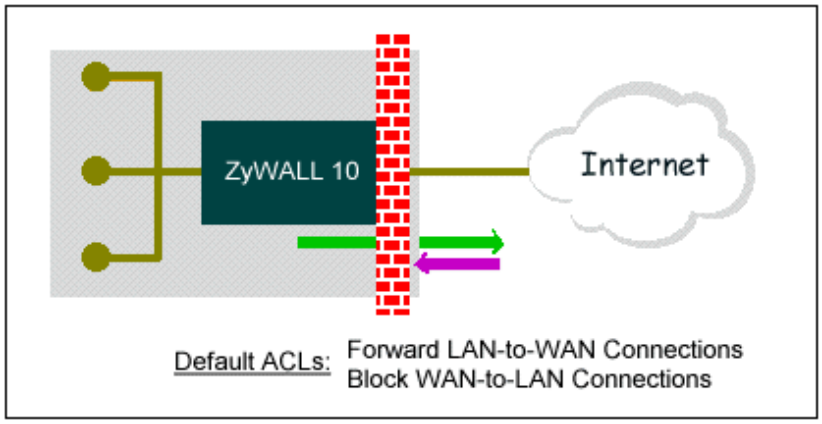
A Brute-force attack, such as 'Smurf' attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker flood a destination IP address of each packet is the broadcast address of the network; the router will 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.

B12. 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.

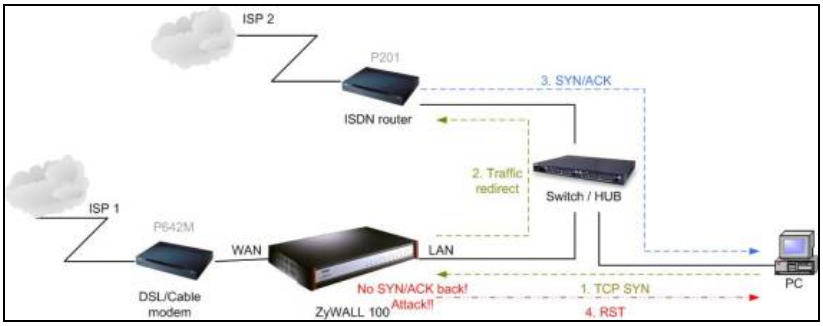
B13. What are the default ACL firewall rules in ZyWALL?

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.



B14. Why does 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. 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.

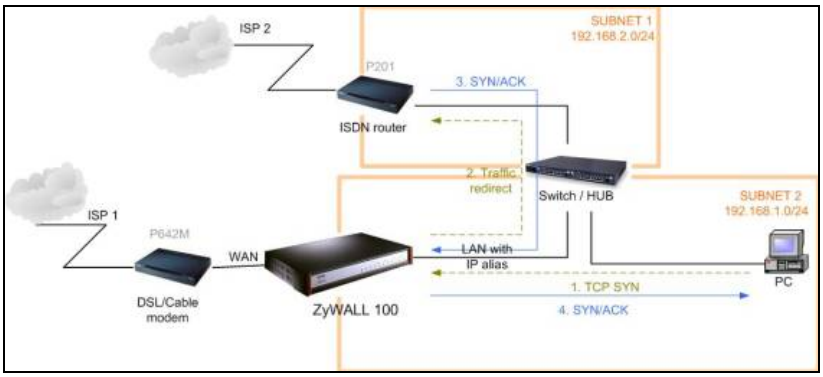
Step 2. And because of **Static route/Traffic Redirect/Policy Routing**, ZyWALL forwards the traffic to another gateway (ISDN/Router) which is in **the same segment** as ZyWALL's LAN.

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.

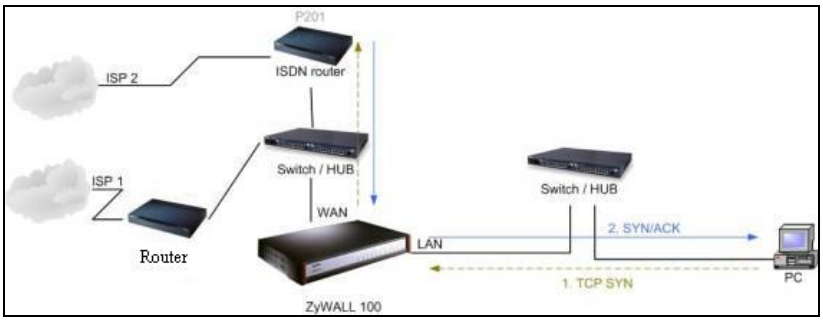
When firewall is turned on, ZyWALL will check the outgoing traffic by ACL and create dynamic sessions to allow return traffic to go back. To achieve Anti-DoS, ZyWALL will send RST packets to the PC and the peer since it never receives the TCP SYN/ACK packet. Thus the connection will always be reset by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

B15. 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.

C. Security Service licenses FAQ

C01. What is iCard?

iCard is used for delivering security service license of ZyXEL products, including ZyWALL product family. ZyWALL security service is enabled by purchasing an iCard to obtain a user license.

C02. Where can I buy the iCard and how much does it cost?

You can buy the iCard from the local dealer or distributor, please contact them for the price. Please check http://www.zyxel.com for ZyXEL global contact information.

C03. How many kinds of iCard does ZyXEL provide?

Choices are ranging from **Platinum**, **Silver** and **Gold**, depending on the model of the device. For the models supported by each type, please check the print on the cards.

C04. Is each type of iCard device specific?

Yes. Different model of ZyXEL product may uses different type of iCard for registration. Users need to check the supported model names before purchasing.

C05. What are the available security service licenses which require additional purchase and license activation in ZyNOS v4.00?

V4.00 is a major new release of ZyNOS and it includes the following security services which require license purchase and activation:

1. Anti-Virus + IDP security service
2. Anti-Spam security service
3. Content Filtering security service

C06. What kind of iCard should I buy?

It depends on the ZyWALL model you have, the security service you desire and the license period you need. See the following table for those mappings. (Here we highlight ZyWALL 5/35/70 since they especially provide AV+IDP, AS features.

	AV+IDP		AS		CF	
	1 Year	2 Year	1 Year	2 Year	1 Year	2 Year
ZyWALL 2	N/A	N/A	N/A	N/A	1-year, Silver	N/A
ZyWALL 2Plus	N/A	N/A	N/A	N/A	1-year, Silver	N/A
ZyWALL 5	1-year,Silver	2-year, Silver	1-year, Silver	2-year, Silver	1-year, Silver	N/A
ZyWALL 35	1-year, Gold	2-year, Gold	1-year, Gold	2-year, Gold	1-year, Gold	N/A
ZyWALL 70	1-year, Gold	2-year, Gold	1-year, Gold	2-year, Gold	1-year, Gold	N/A

C07. If I violate the mappings described above, for example, using a silver iCard for ZyWALL 35 or ZyWALL 70, what will happen?

The activation will fail.

C08. Can I try the Content Filtering service for free? How long is the free trial period of Content Filtering service?

Yes, you can try the Content Filtering service for free.

The free trial period is 30 days and is available to ZyWALL 2, ZyWALL 2Plus, ZyWALL 5, ZyWALL 35, ZyWALL 70, ZyWALL 5 UTM, ZyWALL 35 UTM and ZyWALL 70 UTM owners.

D. Security Service Activation and UpdateFAQ

D01. Why do I have to register?

1. If you wanted to use the free trial service of ZyWALL, your have to activate it from within myZyXEL.com.
2. If you purchased iCard for a security service, you must activate the security service from within myZyXEL.com. The security services in ZyNOS v4.00 includes: AV+IDP, Anti-Spam and Content Filtering service.

D02. In addition to registration, what can I do with myZyXEL.com?

1. Access firmware and security service updates.
2. Get ZyWALL alerts on services, firmware, and products.
3. Manage (activate, change or delete) your ZyWALL security services online.

In summary, myZyXEL.com delivers a convenient, centralized way to register all your ZyWALL security appliances and security services. It eliminates the hassle of registering individual ZyWALL appliances and upgrades to streamline the management of all your ZyWALL security services.
Instead of registering each ZyWALL product individually, using myZyXEL.com you have a single user profile where you can manage all your product registration and service activation.

D03. Is there anything changed on myZyXEL.com because of the launch of ZyNOS v4.00? Which ZyWALL models can be registered via myZyXEL.com?

Yes. Because the launch of ZyNOS v4.00, we are proudly to introduce the new registration flow on myZyXEL.com. However, you can still register devices running older firmware. Please refer to the following table for model mappings.

Model Mappings for Registration on myZyXEL.com

	Device Registration	AV+IDP Service Activation	Anti-Spam Service Activation	Content Filtering Service Activation
New Registration Flow	ZW2plus (v4.00) ZW5 (v4.00) ZW35 (v4.00) ZW70 (v4.00)	ZW5 (v4.00) ZW35 (v4.00) ZW70 (v4.00)	ZW5 (v4.00) ZW35 (v4.00) ZW70 (v4.00)	ZW2plus (v4.00) ZW5 (v4.00) ZW35 (v4.00) ZW70 (v4.00)
Previous Registration Flow	ZW2 (v3.62) ZW5 (v3.64/v3.62) ZW35 (v3.64 or below) ZW70 (v3.65 or below)	N/A	N/A	ZW2 (v3.62) ZW5 (v3.64/v3.62) ZW35 (v3.64 or below) ZW70 (v3.65 or below)
Note	Devices running ZyNOS v4.00 dose NOT support the Previous Registration Flow.			

D04. What's the difference between new registration flow and previous registration? What's the advantage of new registration flow over the previous registration flow?

1. In new registration flow, the registration is processed within device's WebGUI. In previous registration flow, the registration is processed through hyperlink to myZyXEL.com in a separate browser window.

2. The new registration flow is easier to use for both experienced customers and new customers.
In the new registration flow, it's no longer necessary to open another web browser window to register your device. Instead, the registration flow is embedded in device's WebGUI.
Furthermore, customer is no longer required to manually input the MAC of the device because the MAC will be automatically sent to myZyXEL.com during the registration flow.

D05. If I were new to myZyXEL.com, what are the required fields when I register my ZyWALL device on myZyXEL.com?

The required fields include: user name, password, valid email address and country.

D06. When using the new registration flow of myZyXEL.com for ZyNOS v4.0, do I have to create a new account if I were already a registered user on myZyXEL.com?

No, you don't have to re-create a user account on myZyXEL.com if you were a registered user. Your user profile is already stored on myZyXEL.com.

D07. What is mySecurityZone?

1. mySecurityZone is a free service portal. It's open to the public.
2. For public users, you can browse the latest security news and updates from ZSRT, access free resources and subscribe to our free newsletter.
3. For those ZyWALL product owners who have already registered on myZyXEL.com, you can additionally use the same username/password to login to mySecurityZone to view detail description for all policies of AV+IDP service and make queries. Furthermore, you automatically receive our advisories carrying latest security updates and valuable information.

Summary
In mySecurityZone you can:
1. Display, share ZyWALL security information, including AV/IDP policy, advisory, and resource
2. Search ZyWALL detailed product information, including AV/IDP policy, advisory, and resource
3. Receive ZyWALL advisory news by email

D08. What is Update Server?

Update Server is designed to serve the AV+IDP security service subscribers to assure their device is update so that is capable to handle latest threats from Internet.
When a ZyWALL device is scheduled to download the AV+IDP signature pack, the download request is pointed to the Update Server.
Update Server is hosted by ZyXEL and the capacity of Update Server is precisely calculated. After taking the following factors into consideration: bandwidth consumption, availability, geographically distribution of subscribers, we have decided to build the Update Server in IDCs in a globally distributed architecture plus 24x7 monitoring mechanism. This will fully assure the maximum quality of service for all security service subscribers.

D09. Who maintains mySecurityZone & Update Server?

It's maintained by ZyXEL Security Response Team (ZSRT) who manages backend support from the beginning of outbreak happen to attack sample collection, analyze it and output it as policy, and finally make solution of advisory. ZSRT is formed as a group of security experts.

D10. What's the URL for these service portals?

myZyXEL.com
http://www.myzyxel.com/myzyxel/

mySecurityZone
https://mysecurity.zyxel.com/mysecurity/

For Update Server, there is no interactive login screen available since it communicates with ZyWALL devices only.

E. Content Filter FAQ

E01. What's the operation between ZyXEL appliance and BlueCoat data center?

Whenever a PC behind ZyXEL appliance issues HTTP requests to some public WEB server. ZyXEL appliance will forward the request to the targeted WEB server, but also issue an categorization query to BlueCoat data center. When the HTTP response is back to ZyXEL appliance, the appliance will hold the response for a while, and wait for the query result from the BlueCoat data center. If the query is not back within 10 seconds (by default setting), ZyXEL appliance will block (by default setting) the HTTP response to the PC. If the query is back, ZyXEL appliance will drop or forward the request according to the Content Filtering policy set in the appliance. The result of categorization query will be cached in ZyXEL appliance. Later on, HTTP requests to the same WEB server will be inspected by local cache.

E02. How many entries can the cache of Web Site Auto Categorization keep at most?

ZyXEL appliance can keep 1024 entries in the cache at most. Entries that are used less frequently will be overwritten first when the cache is full. Contents inside the cache will be cleared out after rebooting.

E03. Can I specify the time out value of the query response from BlueCoat data center?

Yes, you can change it on ZyXEL appliance. The default value of the time out is 10 seconds.

E04. Can I decide whether to forward or drop the HTTP response if the query to BlueCoat data center is timed out?

Yes, you can set the policy, drop or forward, when query is timed out. The default policy is block.

E05. How to register for BlueCoat service?

Either for free trial purpose or if you get PIN code by purchasing iCard, you need to initiate registration process from ZyXEL appliance by clicking **Registration and Reports** button from content Filter-> Categories page.

E06. Why can't I make registration successfully?

Since the Registration job is between ZyXEL appliance and Http://myZyXEL.com server. Please make sure your Internet connection from ZyXEL appliance is ok first, and keep the connection between them online during the registration process. Since once the registration is granted on the Http://myZyXEL.com server, Http://myZyXEL.com needs to feedback the result (either Successful or Fail) to ZyXEL appliance.

E07. What services can I get with Trial Registration?

With Trial Registration, you can get Web Site Auto Categorization, and Content Filtering Report services.

E08. What types of content filter does ZyWALL provide?

ZyWALL supports three types of content filtering.

- Restrict Web Data including ActiveX, Java Applet, Cookie, Web proxy
- URL keywords blocking
- BlueCoat filter list

E09. What are the primary features of ZyXEL Content Filtering?

- Blocking or Forwarding Policy Management (ZyXEL appliance)
- Monitoring (BlueCoat)
- Real-time URL Rating (BlueCoat)
- Real-Time Reporting (BlueCoat)

E10. Who needs ZyXEL Content Filtering? Is ZyXEL Content Filtering for small companies or for large corporations?

All businesses can benefit from using the ZyXEL Content Filtering solution
ZyXEL Content Filtering helps organizations manage, monitor, and report on users' Internet activity regardless of their location within the organization. Almost any organization — business, government, or school — can benefit from BlueCoat's centrally managed, web-based filtering service. Consider the following:

- 30 to 40% of Internet surfing during work hours is not business related.
- In some companies as much as 70% of bandwidth is consumed by non-productive pursuits.
- 68% of all Internet porn traffic occurs during the 9 to 5 workday.
- 53% of teens have encountered offensive Web sites that include pornography, hate, or violence. Of these, 91% unintentionally found the offensive sites while searching the Web.

ZyXEL Content Filtering is helpful to improve productivity, minimize legal liability, and conserve costly Internet bandwidth within the organization. BlueCoat provides the most complete and accurate Internet filtering solution of any Internet management provider and enables companies to better manage, secure and protect their Internet investment.

E11. Can I have different policies in effect for different times of the day or week?

Yes, but only one blocking period of time is supported currently on ZyXEL appliance.

E12. How many policies can I create?

Two. One is for all users, the other is exempting zone. With exempting zone, you can define a specific range of IP exempting from the policy for all users.

E13. Can I create my own categories?

No, you can't create your own policies other than the 52 categories BlueCoat provides.

E14. Can I override (block or allow) certain URLs regardless of the rating?

Yes, you can use key word blocking to override ratings in the BlueCoat database.

E15. How many URL keywords does ZyWALL support?

64 keywords are supported.

E16. How do I keep database of Content Filtering service updated?

From the current design, there is no local Content Filtering signature database stored on the ZyWALL devices.
As a result, you don't have to worry about the signature update of ZyWALL devices since it's not required.
The transactions and queries between CF-enabled ZyWALL devices and our dynamic database server are taking place dynamically and automatically in the background.
However, you may want to maintain your own URL/keyword list on device to maximize the effectiveness of the Content Filtering service.

E17. What is BlueCoat Filter list?

BlueCoat (http://www.cerberian.com) provides Internet content filtering service through an outsourced model to original equipment manufacturers (OEMs) and service providers. With the BlueCoat Integration Kit, ZyXEL integrates the BlueCoat content filtering service into ZyXEL appliances, such as ZyWALL, Prestige, ZyAir series.

E18. How many ratings does the BlueCoat database contain?

BlueCoat database contains 4.3 million ratings. The BlueCoat database contains about 4.3 million ratings. Because BlueCoat rates sites at the domain or directory level, the database actually covers hundreds of millions of unique web pages.

E19. How often does BlueCoat update the database?

BlueCoat continuously updates the ratings database, but BlueCoat's outsourced model does not require customers to update a local database.
Unlike other Internet content filtering solutions, BlueCoat's outsourced solution does not require clients to receive large database updates daily or weekly. Instead, BlueCoat customers all access the same ratings database. When a user requests a URL not contained in the database, the BlueCoat solution uses Dynamic Real-time Rating to assign a rating to that page. All unrated URLs are further analyzed by background technologies and human raters.

E20. How do I locate sites to block?

BlueCoat provides category ratings for Web sites. Based on the category rating from BlueCoat, users of ZyXEL appliances then define blocking/forwarding policy in WEB GUI.
Do humans review the web sites?

BlueCoat uses expert Web content raters to train the ratings technology.
Initially, category experts create a list of URLs that represent good content for each category. The ratings technology then uses this initial set of pages to recognize content similar to those initial pages. Through BlueCoat's internal processes, the ratings technology learns to better categorize pages as it rates more and more user requests. The BlueCoat staff also continually adds new pages to all categories and evaluates any pages that the rating process could not recognize. Users can request BlueCoat staff to rate specific new pages or review automatic ratings assigned by the technology. Through this process, the ratings technology becomes more accurate at categorizing future user requests.

E21. Do humans review the ratings?

BlueCoat's Web content raters periodically review each content area. They also examine pages based on categorization requests from end-users.
BlueCoat periodically reviews certain content areas to fine tune the ability of the ratings technology to recognize specific types of content. Also, when users believe a page has received an incorrect rating, BlueCoat rating experts will review the categories assigned and make changes as necessary. BlueCoat also uses the human-rated sites to further train and improve the content analysis system.

E22. How can I do if I find a WEB site is mis-categorized?

When you find a web site is not categorized as you expect, you can report to either support@zyxel.com.tw or BlueCoat Site Submissions.

E23. How many and what categories do you provide?

ZyXEL Content Filtering provides 52 categories.

We currently recognizes the following 52 categories:
Potential Liable & Objectionable Content Categories
· Adult/Mature Content
· Alcohol/Tobacco
· Gambling
· Hacking/Proxy Avoidance Systems
· Illegal Drugs
· Illegal/Questionable
· Intimate Apparel/Swimsuit
· Nudity
· Pornography

· Sex Education
· Violence/Hate/Racism
· Weapons

Potential Non-Productive Categories
· Abortion
· Arts/Entertainment
· Auctions
· Brokerage/Trading
· Business & Economy
· Chat/Instant Messaging
· Computers/Internet
· Cult/Occult
· Cultural Institutions
· Education
· Email
· Financial Services
· For Kids
· Games
· Gay & Lesbian
· Government/Legal
· Health
· Humor/Jokes
· Job Search/Careers
· Military
· News & Media
· Newsgroups
· Pay to surf sites
· Personals & Dating
· Political/Activist Groups
· Real Estate
· Reference
· Religion
· Restaurants/Dining/Food
· Search Engines and Portals
· Shopping
· Society & Lifestyle
· Software Downloads

· Sports/Recreation/Hobbies
· Streaming Media/MP3
· Travel
· Vehicles
· Web Advertisements
· Web Communications
· Web Hosting

E24. How does the ZyXEL content filtering handle dynamically generated sites?

We use BlueCoat's Dynamic Real-Time Rating service to accurately categorize dynamic content. Because BlueCoat provides Dynamic Real-Time Rating technology, most dynamic sites receive the correct rating. BlueCoat's database continually reviews the ratings of stored URLs to ensure that the content has not changed.

E25. Does BlueCoat have more than one data center? Is the BlueCoat Web Filter geographically load balanced?

Yes, BlueCoat provides several, geographically distributed data centers to meet the demand of users around the world.

E26. Who can generate and view reports on BlueCoat WEB site?

Anyone with the administration username and password can view and generate reports.

E27. How can I get Content Filtering report?

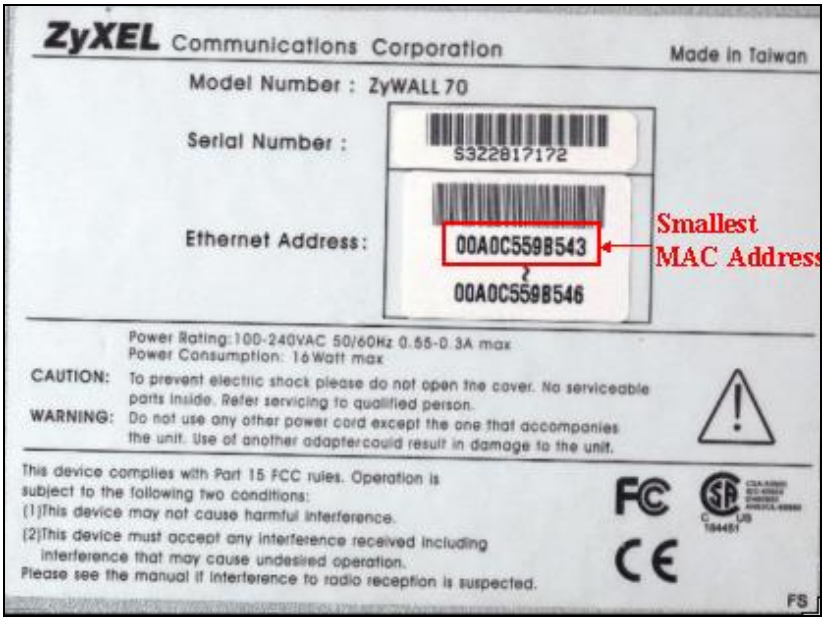
You can get report for content filtering by clicking **Register** button from ZyXEL appliance's WEB GUI, and then you will be redirected to http://myZyXEL.com web server. By clicking **Content Filtering Report**, the WEB interface of BlueCoat reporting system will pop out. By entering the MAC address you registered to Http://myZyXEL.com web server, which you can check from **Registration Status** of Http://myZyXEL.com server, and password you specified when doing registration, you can log into BlueCoat reporting system.

E28. Can I change the password for BlueCoat service?

Yes, you can click **Register** button from ZyXEL appliance's WEB GUI, then Http://myZyXEL.com web page would popped out. You can change password in user profile.

E29. Which User Name & Password should I input for Content Filtering report?

The User Name is the smallest Ethernet MAC address of your device. To identify check the sticker in the bottom of the device as below,



password is the password to login Http://myZyXEL.com.

E30. My device can't get connected to Http://myZyXEL.com, so I can't get into Registration page. What should I check?

1. Please check the Internet Access is ok via launching Internet Browser and connect to a public WEB site.
2. If your ZyWALL is using Static (or Fixed) WAN IP address, please make sure that you have configured DNS server's IP address for the device in "System->General->System DNS Servers" or "Maintenance->General->System DNS Server".

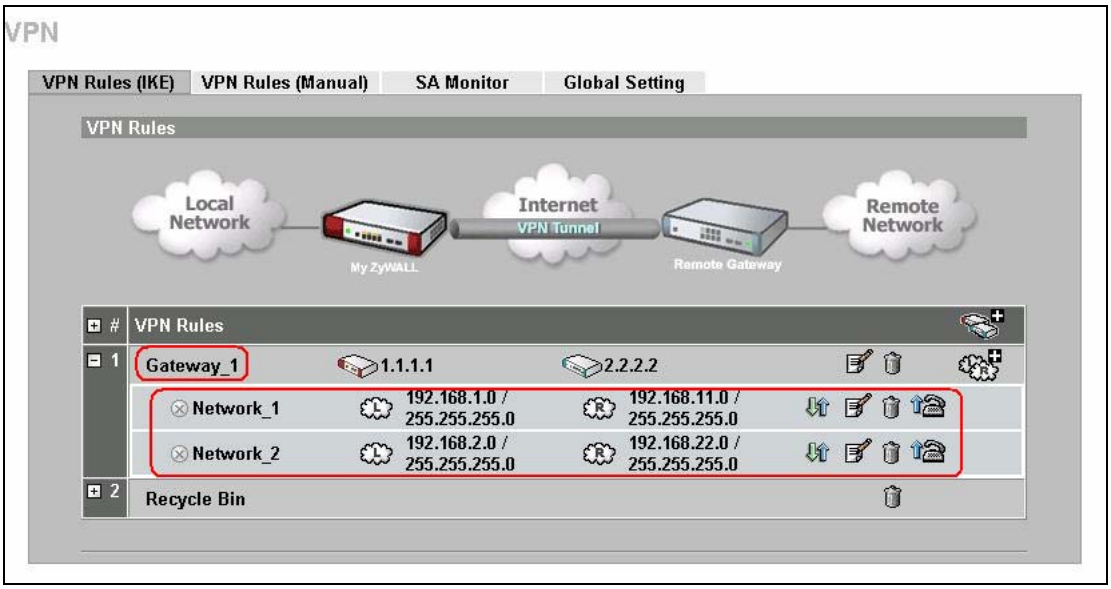
F. IPSec FAQ

F01. How to count my VPN tunnels on ZyWALL?

On 3.64, multiple Network Policies (IKE Phase 2) can be mapped to same Gateway policy (IKE Phase 1). ZyWALL counts the Network policies as VPN tunnels.

In following example, two network policies, Netowrk_1 & Network_2 are mapped to same gateway

policy, Gateway_1. In this case, this will be counted as two VPN tunnels.



F02. 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.

F03. 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.

F04. 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).

F05. 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.

F06. 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.

F07. 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.

F08. 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.

F09. 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.

F10. 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.

F11. 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.

F12. 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.

F13. How do I configure ZyWALL VPN?

You can configure ZyWALL for VPN via web GUI. ZyWALL 1 supports Web only.

F14. What VPN protocols are supported by ZyWALL?

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

F15. What types of encryption does ZyWALL VPN support?

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

F16. 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.

F17. 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 frond 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.

F18. 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.

F19. 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

F20. 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

F21. Will ZyXEL support Secure Remote Management?

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

F22. Does ZyWALL VPN support NetBIOS broadcast?

Yes, the ZyWALL does support NetBIOS broadcast over VPN.

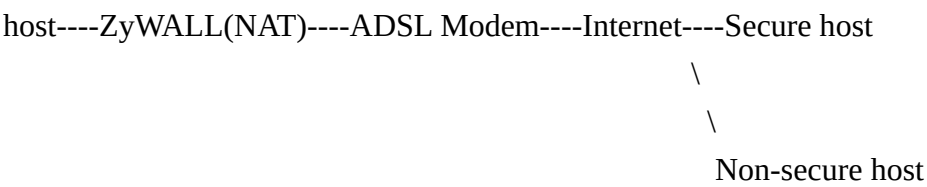
F23. Is the host behind NAT allowed to use IPSec?

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.

F24. 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:



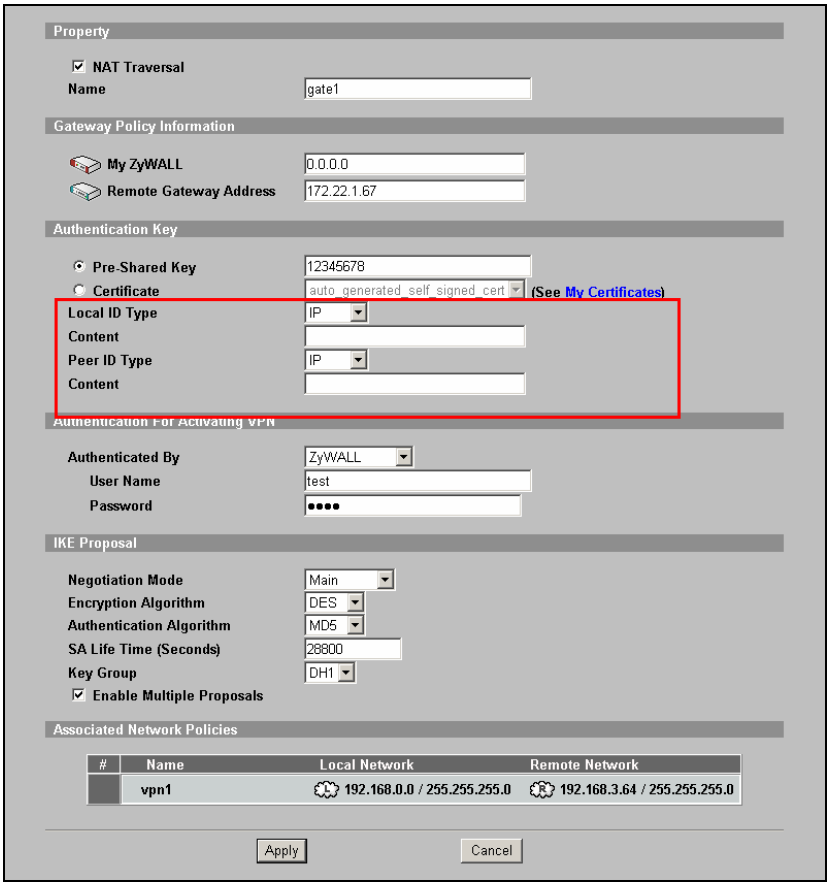
F25. I am planning my ZyWALL behind a NAT router. What do I need to know?

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

F26. Where can I configure Phase 1 ID in ZyWALL?

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



F27. 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.

F28. Single, Range, Subnet, which types of IP address does ZyWALL support in VPN/IPSec?

All ZyWALL series support single, range, and subnet configuration for VPN IPSec. 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.

F29. 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).

F30. 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**".

G. PKI FAQ

G01. 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).

G02. 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.

G03. 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.

G04. 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.

G05. 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.)

G06. 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.

G07. 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.

G08. What are Certificate Policies (CPs)?

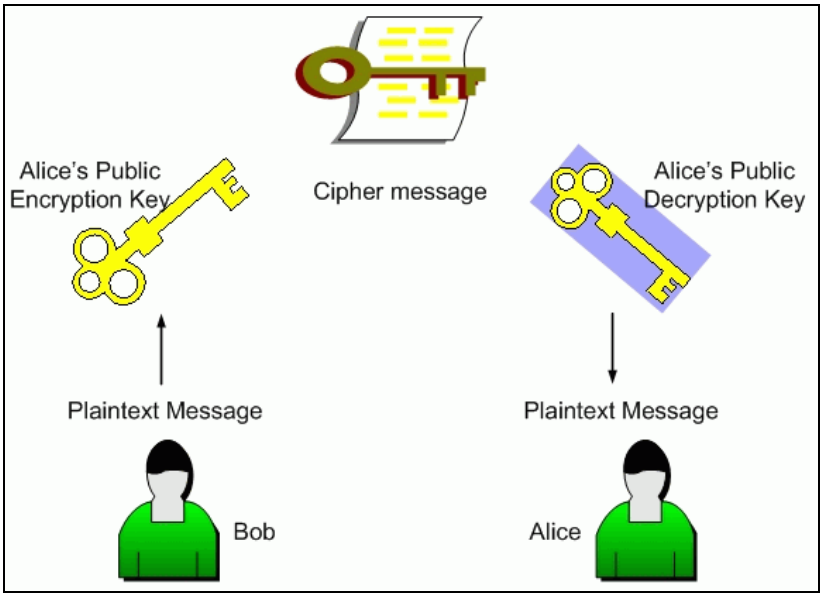
Certification Authorities issue digital certificates that are appropriate to specific purposes or applications. For example, in the Government of Canada Public Key Infrastructure, digital certificates for data confidentiality are different from those used for digital signatures. Certificate Policies

describe the rules governing the different uses of these certificates.

G09. 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.



G10. What is a digital signature?

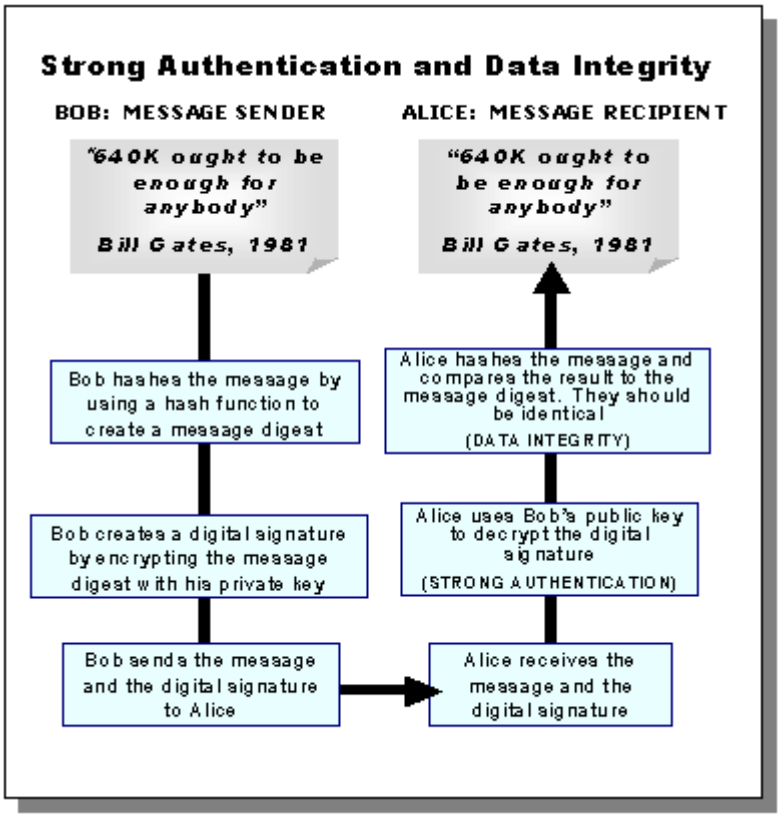
Not to be confused with a digitized signature (a scan of a hand-written signature), a digital signature can be used with either encrypted or unencrypted messages to confirm the sender's identity and ensure the recipient that the message content has not been changed in transmission. Digital signatures 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.

G11. 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.



G12. 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.

G13. 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.

G14. 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.

G15. 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.

G16. 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.

G17. 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.

G18. 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.

G19. 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.