VPN Firewall
User’s Manual

Contents

Administration	5
Admin	7
Setting	11
Date/Time	19
Lanugage	20
Permitted IPs	21
Logout	25
Software Update	26
Configuration	27
Interface	28
Multiple Subnet	32
Hacker Alert	43
Route Table	47
DHCP	51
DNS Proxy	53
DDNS	58
Address	**63**
Interface	64
Internal Group	68
External	72
External Group	76
DMZ	80
DMZ Group	84
Service	89
Pre-defined	90
Custom	91
Group	95

Schedule	99
Content filtering	**103**
URL Blocking	104
Script Blocking	109
Virtual Server	**111**
Mapped IP	113
Virtual Server	117
Policy	**125**
Outgoing	126
Incoming	135
External To DMZ & Internal to DMZ	141
DMZ To External & DMZ To Internal	147
VPN	153
IPSec Autokey	154
PPTP Server	231
PPTP Client	237
LOG	**243**
Traffic Log	244
Event Log	247
Connection Log	250
Log Report	253
Alarm	**257**
Traffic Alarm	258
Event Alarm	261
Statistics	**265**
WAN Statistics	266
Policy Statistics	268

Status	**271**
Interface Status	272
ARP Table	273
DHCP Clients	274
Setup Examples	275

Administration

The VPN Firewall Administration and monitoring control is set by the System Administrator. The System Administrator can add or modify System settings and monitoring mode. The sub Administrators can only read System settings but not modify them. In **Administration**, the System Administrator can:

(1) Add and change the sub Administrator's names and passwords;
(2) Back up all Firewall settings into local files;
(3) Set up alerts for Hackers invasion.

What is Administration?

"Administratoion" is the managing of settings such as the privileges of packets that pass through the firewall and monitoring controls. Administrators may manage, monitor, and configure firewall settings. All configurations are "read-only" for all users other than the Administrator; those users are not able to change any settings for the firewall.

The three sub functions under **Administrator** are **Administrator, Setting, Date/Time, Lanugage, Permitted IPs ,Logout** and **Software Update.**

Administrator: has control of user access to the firewall. He/she can add/remove users and change passwords.

Setting: The Administrator may use this function to backup firewall configurations and export (save) them to an **"Administrator"** computer or anywhere on the network; or restore a configuration file to the VPN; or restore the firewall back to default factory settings. Under **Setting**, the Administrator may enable e-mail alert notification. This will alert Administrator(s) automatically whenever the firewall has experienced unauthorized access or a network hit (hacking or flooding). Once enabled, an IP address of a SMTP(Simple Mail Transfer protocol) Server is required. Up to two e-mail addresses can be entered for the alert notifications.

Date/Time: This function enables the VPN Firewall to be synchronized either with an Internet Server time or with the client computer's clock.

Lanugage The software provides **Traditional Chinese Version**，**Simplified Chinese Version** and **English version** for you to choose.

Permitted IPs Only the authorized IP address is permitted to manage the Bandwidth Manager.

Logout Administrator logs out the VPN Firewall. This function protects your system while you are away.

Software Update: Administrators may visit distributor's web site to download the latest firmware. Administrators may update the VPN firmware to maximize its performance and stay current with the latest fixes for intruding attacks.

Firewall Administration setup

On the left hand menu, click on **Administration**, and then select **Administrator** below it. The current list of Administrator(s) shows up.

Settings of the Administration table:

Administrator Name: The username of Administrators for the firewall. The user **admin** cannot be removed.

Privilege: The privileges of Administrators (Admin or Sub Admin)
The username of the main Administrator is **Administrator** with **read/write** privilege.
Sub Admins may be created by the **Admin** by clicking **New Sub Admin.** Sub Admins have **read only** privilege.

Configure: Click **Modify** to change the "Sub Administrator's" password and click **Remove** to delete a "Sub Administrator."

Adding a new Sub Administrator:

Step 1. In the **Administration** window, click the **New Sub Admin** button to create a new **Sub Administrator.**

Step 2. In the **Add New Sub Administrator** window:

- **Sub Admin Name:** enter the username of new **Sub Admin.**
- **Password:** enter a password for the new **Sub Admin.**
- **Confirm Password:** enter the password again.

Step 3. Click **OK** to add the user or click **Cancel** to cancel the addition.

Modifying the Sub-Administrator's Password:

Step 1. In the **Administration** window, locate the **Administrator** name you want to edit, and click on **Modify** in the **Configure** field.

Step 2. The **Modify Administrator Password** window will appear. Enter in the required information:

- **Password:** enter original password.
- **New Password:** enter new password
- **Confirm Password:** enter the new password again.

Step 3. Click **OK** to confirm password change or click **Cancel** to cancel it.

Removing a Sub Administrator:

Step 1. In the Administration table, locate the Administrator name you want to edit, and click on the Remove option in the Configure field.

Step 2. The Remove confirmation pop-up box will appear.

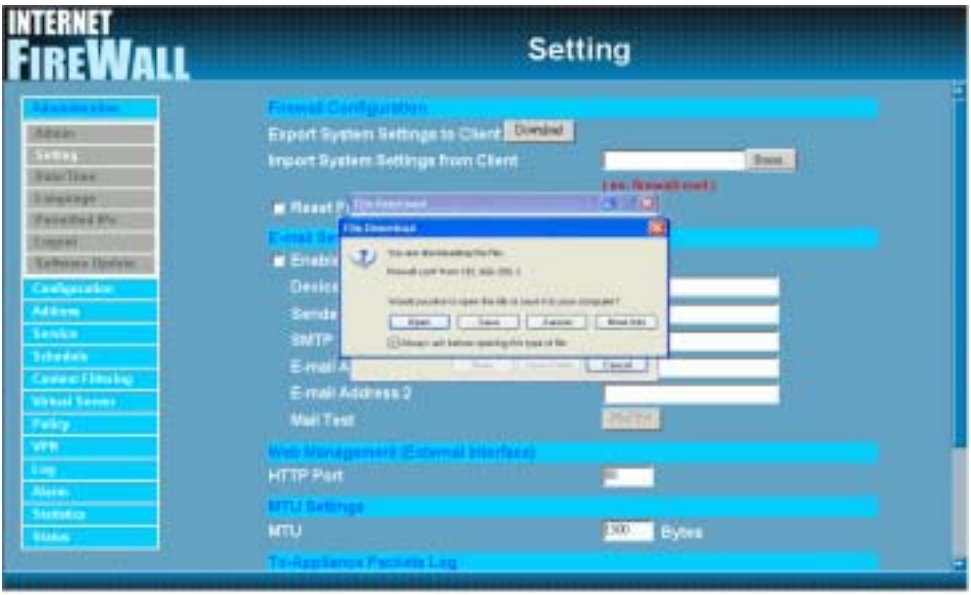
Step 3. Click **OK** to remove that Sub Admin or click **Cancel** to cancel.

Settings

The Administrator may use this function to backup firewall configurations and export (save) them to an **"Administrator"** computer or anywhere on the network; or restore a configuration file to the device; or restore the firewall back to default factory settings.

Entering the Settings window:

Click **Setting** in the **Administrator** menu to enter the **Settings** window. The **Firewall Configuration** settings will be shown on the screen.



Exporting VPN Firewall settings:

Step 1. Under **Firewall Configuration**, click on the **Download** button next to **Export System Settings to Client**.

Step 2. When the **File Download** pop-up window appears, choose the destination place in which to save the exported file. The **Administrator** may choose to rename the file if preferred.

Importing Firewall settings:

Step 1. Under **Firewall Configuration**, click on the **Browse** button next to **Import System Settings**. When the **Choose File** pop-up window appears, select the file to which contains the saved Firewall Settings, then click **OK**.

Step 2. Click **OK** to import the file into the **Firewall** or click **Cancel** to cancel importing.

Restoring Factory Default Settings:

Step 1. Select **Reset Factory Settings** under **Firewall Configuration**.
Step 2. Click **OK** at the bottom-right of the screen to restore the factory settings.

Enabling E-mail Alert Notification:

Step 1. Select **Enable E-mail Alert Notification** under **E-Mail Settings**. This function will enable the Firewall to send e-mail alerts to the System Administrator when the network is being attacked by hackers or when emergency conditions occur.

Step 2. Device Name: Enter the Device Name.

Step 3. **Sender Address (Required by some ISPs):** Enter the Sender Address.(Some ISPs need Required.)

Step 4. **SMTP Server IP:** Enter SMTP server's IP address.

Step 5. **E-Mail Address 1:** Enter the first e-mail address to receive the alarm notification.

Step 6. **E-Mail Address 2:** Enter the second e-mail address to receive the alarm notification. (Optional)

Step 7. Mail Test: The select e-mail test.

Step 8. Click **OK** on the bottom-right of the screen to enable E-mail alert notification.

Web Management (External Interface) (Remote UI management)

The administrator can change the port number used by HTTP port anytime. (Remote UI management)

Step 1. **Set Web Management (External Interface).** The administrator can change the port number used by HTTP port anytime.

MTU (set networking packet length)

The administrator can modify the networking packet length.

Step 1. **MTU Setting.** The administrator can modify the networking packet length.

To-Firewall Packets Log

Select this option to the VPN Firewall **To-Firewall Packets Log.** Once this function is enabled, every packet to this appliance will be recorded for system manager to trace.

Firewall Reboot

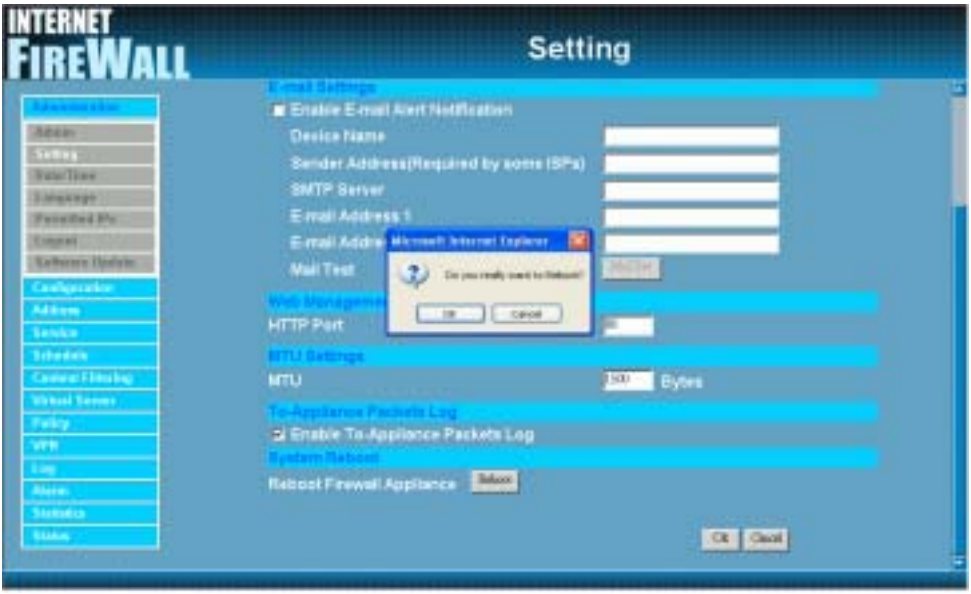
Select this option to the VPN Firewall **Firewall Reboot.** Once this function is enabled, the firewall will be reboot**.**

Step 1. Click **Setting** in the **Administration** menu to enter the settings window.

Step 2. Reboot Firewall：Click **Reboot.**

Step 3. A confirmation pop-up box will appear.

Step 4. Follow the confirmation pop-up box, click **OK** to restart firewall or click **Cancel** to discard changes.



Date/Time

Synchronizing the VPN Firewall with the System Clock

The administrator can configure the VPN Firewall.s date and time by either syncing to an Internet Network Time Server (NTP) or by syncing to your computer.s clock.

Follow these steps to sync to an Internet Time Server

Step 1. Enable synchronization by checking the box.
Step 2. Click the down arrow to select the offset time from GMT.
Step 3. Enter the Server IP Address or Server name with which you want to synchronize.
Step 4. Update system clock every 5 minutes You can set the interval time to synchronize with outside servers. If you set it to 0, it means the device will not synchronize automatically.

Follow this step to sync to your computer's clock.

Step 1. Click on the **Sync** button.

Click the **OK** button below to apply the setting or click **Cancel** to discard changes.

Lanugage

The software provides **Traditional Chinese Version**, **Simplified Chinese Version** and **English** version for you to choose.

Step 1. Click **Languag**.

Step 2. Select the language version you want（**Traditional Chinese Version**, **Simplified Chinese Version** and **English** version）.

Step 3. Click **OK** to change the language version or click **Cancel** to discard changes.

Permitted IPs

Only the authorized IP address is permitted to manage the VPN Firewall.

Add a Permitted IP Address

Step 1. Click **New Entry** button.

Step 2. In IP Address field, enter the LAN IP address or WAN IP address.

- **IP address**：Enter the LAN IP address or WAN IP address.
- **Netmask**：Enter the netmask of LAN/WAN.
- **Ping**：Select this to allow the WAN network to ping the IP Address of the Firewall.
- **WebUI**：Check this item, Web User can use HTTP to connect to the Setting window of VPN Firewall.

Step 3. Click **OK** to add Permitted IP or click **Cancel** to discard changes.

Modify a Permitted IP Address

Step 1. In the table of **Permitted IPs**, highlight the IP you want to modify, and then click **Modify**.

Step 2. In **Modify Permitted IP**, enter new IP address.

Step 3. Click **OK** to modify or click **Cancel** to discard changes.

Remove a Permitted IP addresses

Step 1. In the table of **Permitted IPs**, highlight the IP you want to remove, and then click **Remove**.

Step 2. In **Remove Permitted IP**, enter new IP address.

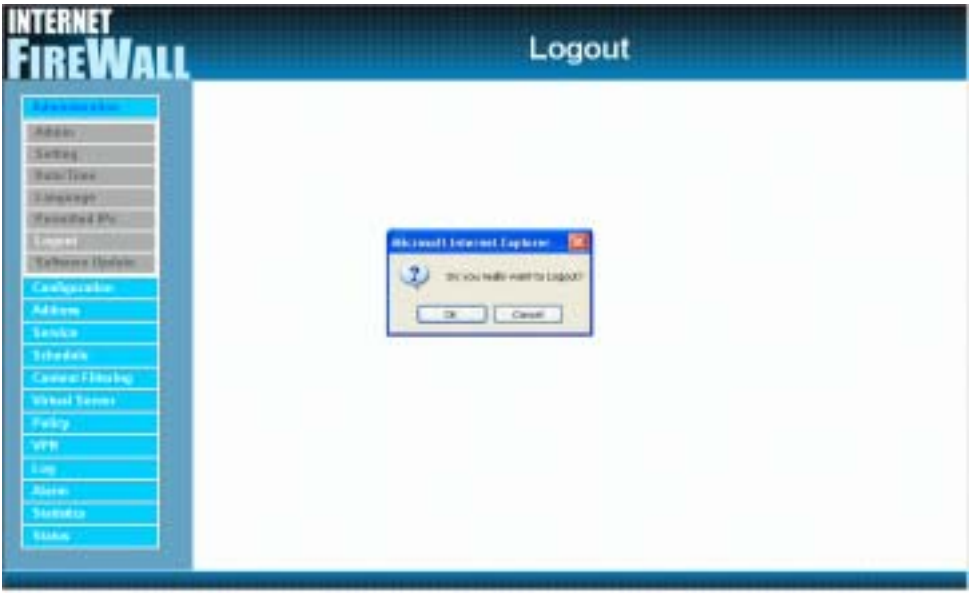
Step 3. In the confirm window, click **OK** to remove or click **Cancel** to discard changes.

Logout the firewall

Select this option to the VPN Firewall **Logout the firewall,**This function protects your sysytem while you are away

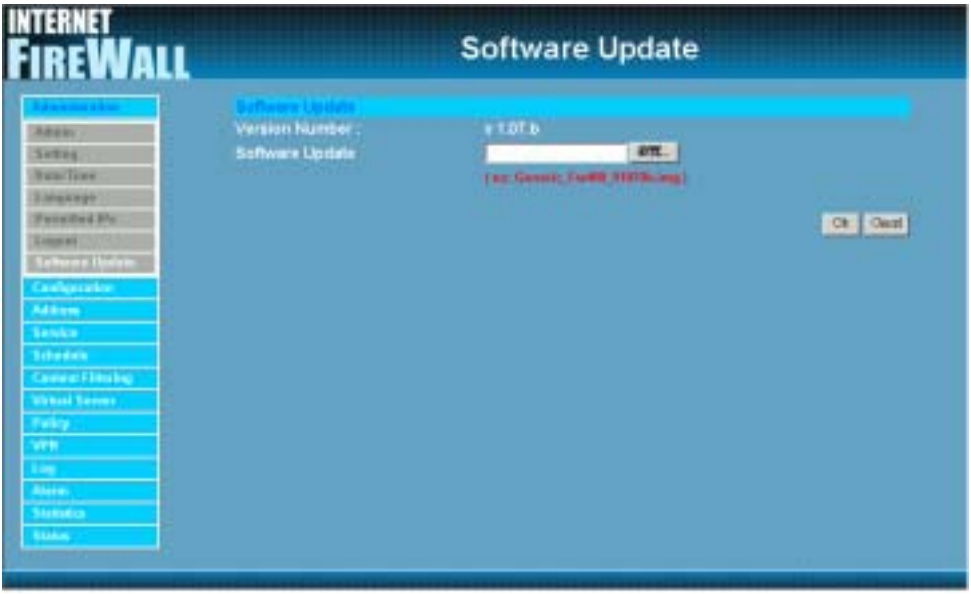
Step 1. Click Logout the firewall.

Step 2. Click OK to logout or click Cancel to discard the change.



Software Update

Under **Software Update**, the admin may update the VPN Firewall Firewall software with a newer software.



Configuration

What is System Configuration?

In this section, the Administrator can:

(1) Set up the internal, external and DMZ IP addresses
(2) Set up the Multiple Subnet
(3) Set up the Firewall detecting functions
(4) Set up a static route
(5) Set up the DHCP Server
(6) Set up DNS Proxy
(7) Set up DDNS

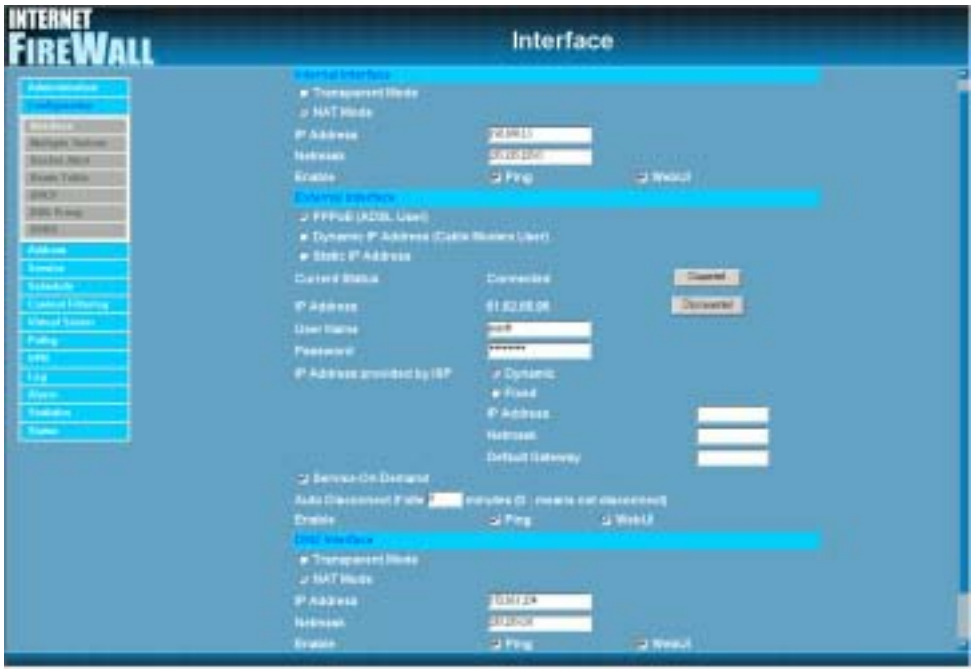
Note: *After all the settings of the Firewall configuration have been set, the Administrator can backup the System configuration into the local hard drive as shown in the* ***Administrator*** *section of this manual under the heading:* ***1-2 Settings****.*

Interface

In this section, the **Administrator** can set up the IP addresses for the office network. The Administrator may configure the IP addresses of the Internal (LAN) network, the External (WAN) network, and the DMZ network. The netmask and gateway IP addresses are also configured in this section.

Entering the Interface menu:

Click on **Configuration** in the left menu bar. Then click on **Interface** below it. The current settings of the interface addresses will appear on the screen.



Configuring the Interface Settings:

Internal Interface

Using the **Internal Interface**, the Administrator sets up the Internal (LAN) network. The Internal network will use a private IP scheme. The private IP network will not be routable on the Internet.

IP Address: The private IP address of the Firewall's internal network is the IP address of the Internal (LAN) port of the VPN Firewall. The default IP address is 192.168.1.1.

Note: The IP Address of Internal Interface and the DMZ Interface is a private IP address only.

If the new Internal IP Address is not 192.168.1.1, the **Administrator** needs to set the IP Address on the computer to be on the same subnet as the Firewall and restart the System to make the new IP address effective. For example, if the Firewall's new Internal IP Address is 172.16.0.1, then enter the new Internal IP Address 172.16.0.1 in the URL field of browser to connect to Firewall.

NetMask: This is the netmask of the internal network. *The default netmask of the VPN is 255.255.255.0.*

Ping: Select this to allow the internal network to ping the IP Address of the Firewall. *If set to enable, the VPN Firewall Firewall will respond to ping packets from the internal network.*

WebUI: Select this to allow the VPN Firewall Firewall WEBUI to be accessed from the Internal (LAN) network.

External Interface

Using the **External Interface**, the Administrator sets up the External (WAN) network. These IP Addresses are real public IP Addresses, and are routable on the Internet.

For PPPoE (ADSL User): This option is for PPPoE users who are required to enter a username and password in order to connect, such as ADSL users.

Current Status: Displays the current line status of the PPPoE connection.

IP Address: Displays the IP Address of the PPPoE connection

Username: Enter the PPPoE username provided by the ISP.

Password: Enter the PPPoE password provided by the ISP.

IP Address provided by ISP:

Dynamic: Select this if the IP address is automatically assigned by the ISP.

Fixed: Select this if you were given a static IP address. Enter the IP address that is given to you by your ISP.

Service-On-Demand:

Auto Disconnect: The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

Ping: Select this to allow the external network to ping the IP Address of the Firewall. This will allow people from the Internet to be able to ping the Firewall. *If set to enable, the* VPN Firewall Firewall *will respond to echo request packets from the external network.*

WebUI: Select this to allow the VPN Firewall Firewall WEBUI to be accessed from the External (WAN) network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the VPN Firewall Firewall always requires a username and password to enter the WebUI.

For Dynamic IP Address (Cable Modem User): This option is for users who are automatically assigned an IP address by their ISP, such as cable modem users. The following fields apply:

IP Address: The dynamic IP address obtained by the Firewall from the ISP will be displayed here. This is the IP address of the External (WAN) port of the VPN.

MAC Address: This is the MAC Address of the VPN Firewall Firewall.

Hostname: This will be the name assign to the VPN Firewall Firewall. Some cable modem ISP assign a specific hostname in order to connect to their network. Please enter the hostname here. If not required by your ISP, you do not have to enter a hostname.

Ping: Select this to allow the external network to ping the IP Address of the Firewall. This will allow people from the Internet to be able to ping the Firewall. *If set to enable, the VPN Firewall Firewall will respond to echo request packets from the external network.*

WebUI: Select this to allow the VPN Firewall Firewall WEBUI to be accessed from the External (WAN) network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the VPN Firewall Firewall always requires a username and password to enter the WebUI.

For Static IP Address: This option is for users who are assigned a static IP Address from their ISP. Your ISP will provide all the information needed for this section such as IP Address, Netmask, Gateway, and DNS. Use this option also if you have more than one public IP Address assigned to you.

IP Address: Enter the static IP address assigned to you by your ISP. This will be the public IP address of the External (WAN) port of the VPN.

Netmask: This will be the Netmask of the external (WAN) network. (i.e. 255.255.255.0)

Default Gateway: This will be the Gateway IP address.

Domain Name Server (DNS): This is the IP Address of the DNS server.

Ping: Select this to allow the external network to ping the IP Address of the Firewall. This will allow people from the Internet to be able to ping the Firewall. *If set to enable, the VPN Firewall Firewall will respond to echo request packets from the external network.*

WebUI: Select this to allow the VPN WEBUI to be accessed from the External (WAN) network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the VPN Firewall Firewall always requires a username and password to enter the WebUI.

DMZ Interface

The Administrator uses the **DMZ Interface** to set up the DMZ network. The DMZ network consists of server computers such as FTP, SMTP, and HTTP (web). These server computers are put in the DMZ network so they can be isolated from the Internal (LAN) network traffic. Broadcast messages from the Internal network will not cross over to the DMZ network to cause congestions and slow down these servers. This allows the server computers to work efficiently without any slowdowns.

IP Address: The private IP address of the Firewall's DMZ interface. This will be the IP address of the DMZ port. The IP address the Administrator chooses will be a private IP address and cannot use the same network as the External or Internal network.

NetMask: This will be the netmask of the DMZ network.

Multiple Subnet

NAT mode

Multiple Subnet allows local port to set multiple subnet works and connect with the internet through different WAN IP Addresses.

For instance：The lease line of a company applies several real IP Addresses 168.85.88.0/24, and the company is divided into R&D department, service, sales department, procurement department, accounting department, the company can distinguish each department by different subnet works for the purpose of convenient management. The settings are as the following：

1.R&D department subnet work：192.168.1.11/24(LAN) ←→ 168.85.88.253(WAN 1)

2. Service department subnet work： 192.168.2.11/24(LAN) ←→ 168.85.88.252(WAN 1)

3.Sales department subnet work： 192.168.3.11/24(LAN) ←→ 168.85.88.251(WAN 1)

4. Procurement department subnet work

192.168.4.11/24(LAN) ←→ 168.85.88.250(WAN 1)

5. Accounting department subnet work

192.168.5.11/24(LAN) ←→ 168.85.88.249(WAN 1)

The first department(R&D department) was set while setting interface IP, the other four ones have to be added in Multiple Subnet, after completing the settings, each deparm ent use the different WAN IP Address to connect to the internet. The settings of each department are as the following

Service IP Address：192.168.2.1

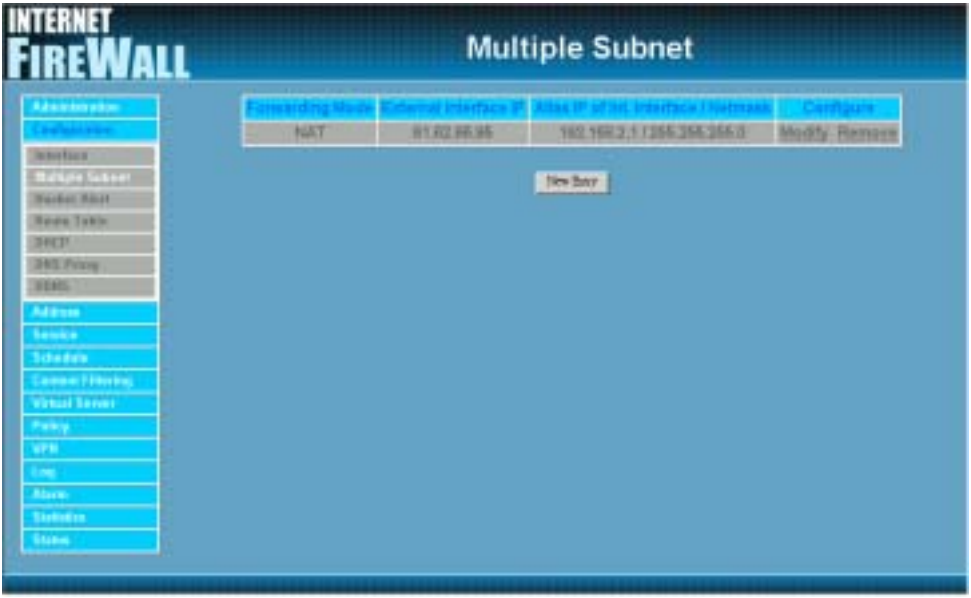
Subnet Mask：255.255.255.0

Default Gateway：192.168.2.11

The other departments are also set by groups, this is the function of Multiple Subnet.

Multiple Subnet settings

Click **Multiple Subnet** in the **System** menu to enter Multiple Subnet window.



Multiple Subnet

- **Forwarding Mode:** Display forwarding Mode. NAT mode / Routing Mode.
- **WAN Interface IP**：Display WAN Port IP Address.
- **Alias IP of Int. Interface / Netmask**： Local port IP Address and subnet Mask.
- **Modify**：Modify the settings of Multiple Subnet. Click **Modify** to modify the parameters of Multiple Subnet or click **Delete** to delete settings.

Add a Multiple Subnet NAT Mode.

Step 1. Click the **Add** button below to add Multiple Subnet.

Step 2. Enter the IP Address in the website name column of the new window.

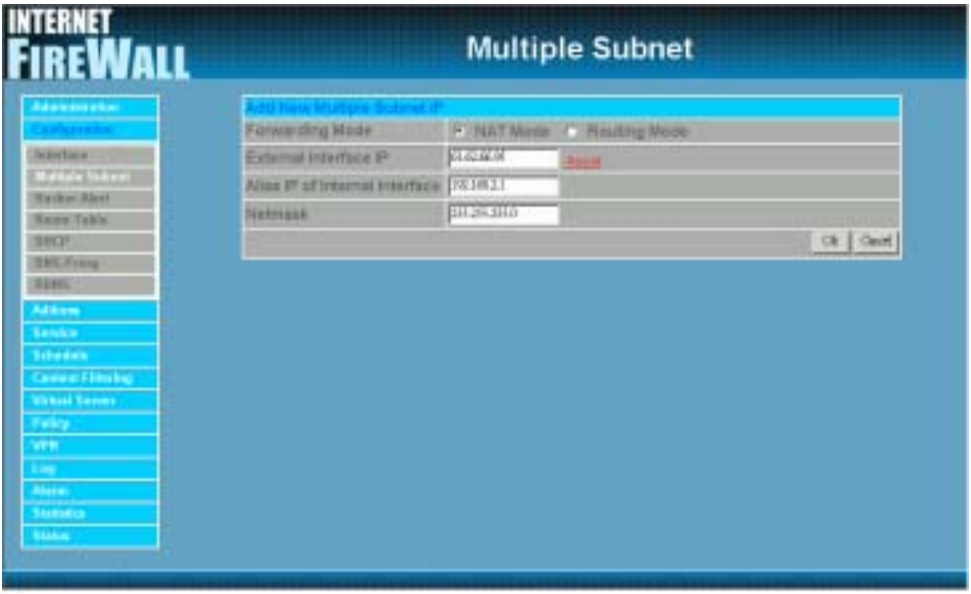
Forwarding Mode Click the NAT button below to setting.

Alias IP of LAN Interface： Enter Local port IP Address.

Netmask：Enter Local port subnet Mask.

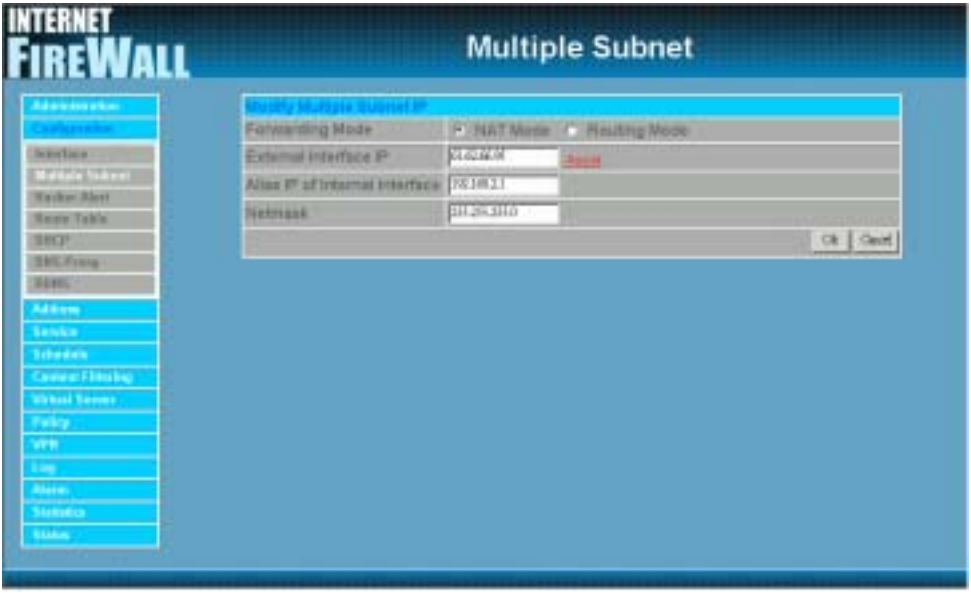
WAN Interface IP: Add WAN IP Address.

Step 3. Click **OK** to add Multiple Subnet or click **Cancel** to discard changes.



Modify a Multiple Subnet

Step 1. Find the IP Address you want to modify and click **Modify**
Step 2. Enter the new IP Address in **Modify Multiple Subnet** window.
Step 3. Click the **OK** button below to change the setting or click **Cancel** to discard changes.



Removing a Multiple Subnet

Step 1. Find the IP Address you want to delete and click **Delete**.

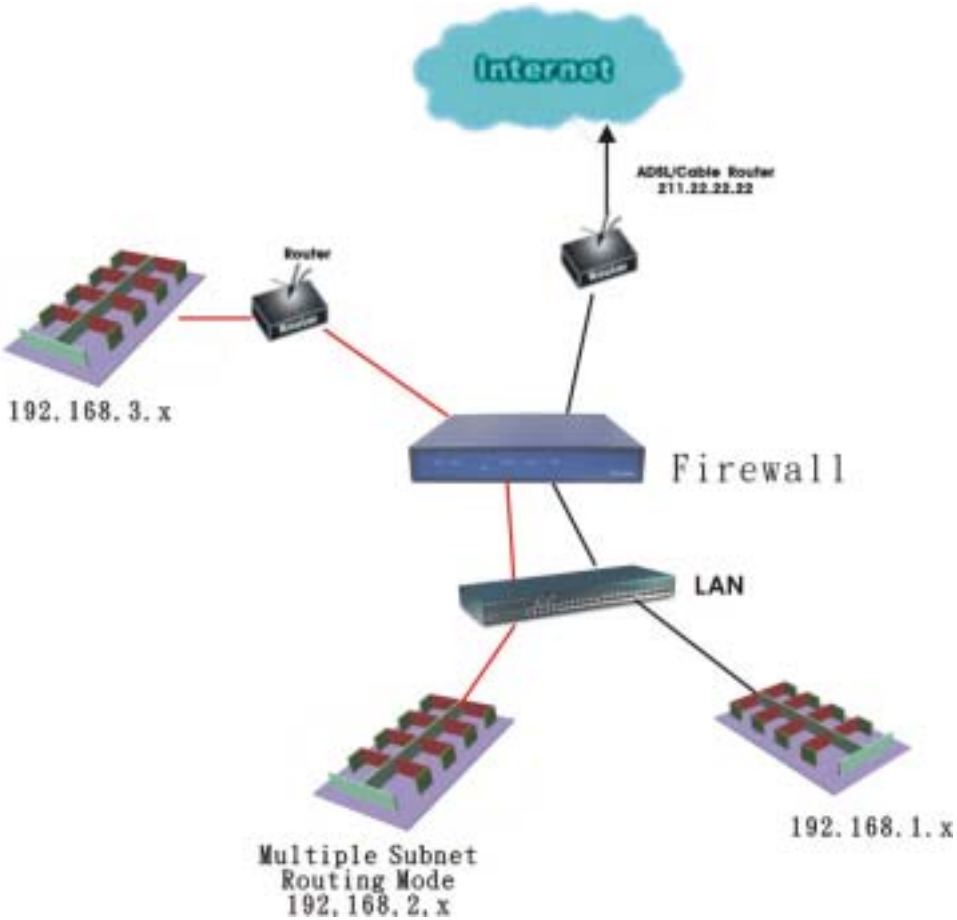
Step 2.A confirmaion pop-up box will appear, click OK to delete the setting or click Cancel to discard changes.

Routing Mode

Multiple Subnet allows local port to set Multiple Subnet Routing Mode works and connect with the internet through different WAN IP Addresses.

For example, the leased line of a company applies several real IP Addresses 192.168.2.0/24 and the company is divided into R&D, Customer Service, Sales, Procurement, and Accounting Department. The company can distinguish each department by different subnet works for the purpose of convenient management.

The settings are as the following：



Step 1. Click **System** Configuration on the left side menu bar, then click **Multiple Subnet** below it. Enter **Multiple Subnet** window.

Step 2. The definition of Multiple Subnet :

- **Forwarding Mode**：Display Forwarding Mode which is NAT Mode or Routing Mode.
- **WAN Interface IP:** Display WAN Port IP Address.
- **Alias IP of Int. Interface / Subnet Mask**： Local port IP Address and subnet Mask.
- **Modify**：Modify the settings of Multiple Subnet. Click **Modify** to modify the parameters of Multiple Subnet or click **Delete** to delete settings.

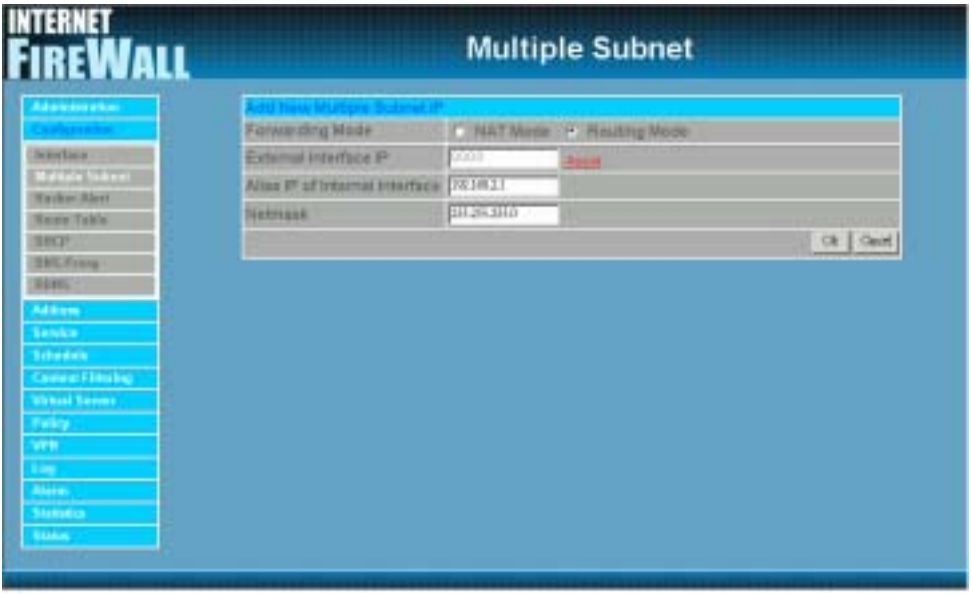
Adding a Multiple Subnet Routing Mode

Step 1. Click the **Add** button below to add Multiple Subnet.

Step 2. Enter the IP Address in **Add Multiple Subnet** window.

Forwarding Mode : Click the Routing button below to setting
WAN Interface IP : Add WAN IP.
Alias IP of LAN Interface： Enter Local port IP Address.
Netmask：Enter Local port subnet Mask.

Step 3. Click **OK** to add Multiple Subnet or click **Cancel** to discard changes.



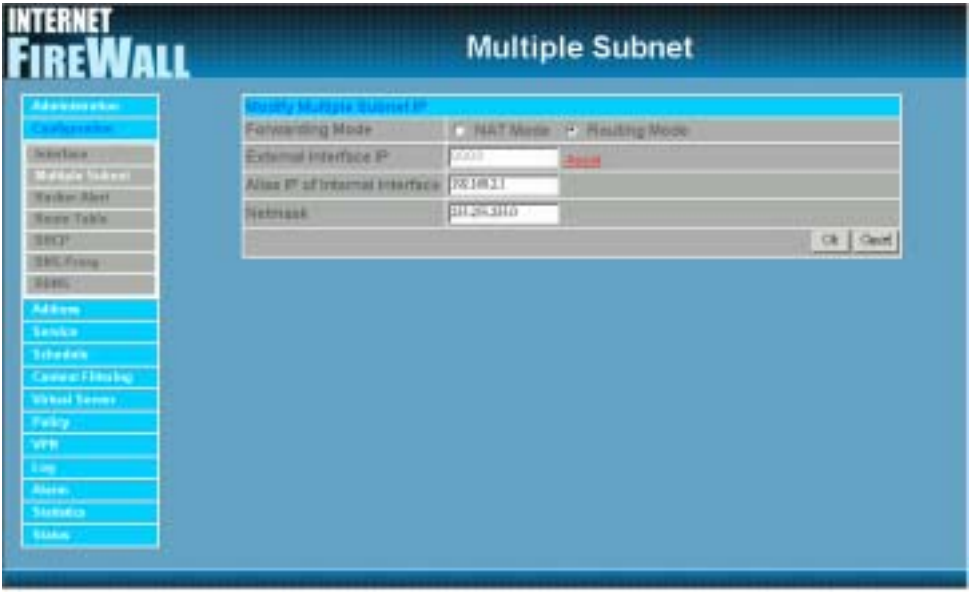
Step 4: Adding a new Incoming Policy. In the incoming window, click the **New Entry** button.

Modify a Multiple Subnet Routing Mode

Step 1. Find the IP Address you want to modify in **Multiple Subnet** menu, then click **Modify** button, on the right side of the service providers, click **OK**.

Step 2. Enter the new IP Address in **Modify Multiple Subnet** window.

Step 3. Click the **OK** button below to change the setting or click **Cancel** to discard changes.



Removing a Multiple Subnet Routing Mode

Step 1. Find the IP Address you want to delete in **Multiple Subnet** menu, then click **Delete** button, on the right side of the service providers, click **OK**.

Step 2. A confirmation pop-up box will appear, click **OK** to delete the setting or click **Cancel** to discard changes.

Hacker Alert

The Administrator can enable the VPN Firewall Firewall auto detect functions in this section. When abnormal conditions occur, the Firewall will send an e-mail alert to notify the Administrator, and also display warning messages in the **Event** window of **Alarm.**

Auto Detect functions:

- **Detect SYN Attack:** Select this option to detect TCP SYN attacks that hackers send to server computers continuously to block or cut down all the connections of the servers. These attacks will prevent valid users from connecting to the servers.

  【SYN Flood Threshold(Total) Pkts/Sec】: The System Administrator can enter the maximum number of SYN packets per second that is allow to enter the network/VPN Firewall.

  【SYN Flood Threshold(Per Source IP) Pkts/Sec】: The System Administrator can enter the maximum number of SYN packets per second from attacking source IP Address that is allow to enter the network/VPN Firewall.

【SYN Flood Threshold Blocking Time (Per Source IP) Seconds】: The System Administrator can enter the blocking time when the number of SYN packets per second from attacking source IP Address that is allow to enter the network/VPN Firewall exceed the maximum number (define as above). After blocking for certain seconds, the device will start to calculate the max number of SYN packets per second from attacking source IP Address, if the max number still exceed the define value, it will block the attacking IP Address continuously.

- **Detect ICMP Attack:** Select this option to detect ICMP flood attacks. When hackers continuously send PING packets to all the machines of the LAN networks or to the VPN Firewall via broadcasting, your network is experiencing an ICMP flood attack.

【ICMP Flood Threshold(Total) Pkts/Sec】: The System Administrator can enter the maximum number of ICMP packets per second that is allow to enter the network/VPN Firewall.

【ICMP Flood Threshold(Per Source IP) Pkts/Sec】: The System Administrator can enter the maximum number of ICMP packets per second from attacking source IP Address that is allow to enter the network / VPN Firewall.

【ICMP Flood Threshold Blocking Time (Per Source IP) Seconds】: The System Administrator can enter the blocking time when the number of ICMP packets per second from attacking source IP Address that is allow to enter the network / VPN Firewall exceed the maximum number (define as above). After blocking for certain seconds, the device will start to calculate the max number of ICMP packets per second from attacking source IP Address, if the max number still exceed the define value, it will block the attacking IP Address continuously.

- **Detect UDP Attack:** The same as ICMP Flood.

【UDP Flood Threshold(Total) Pkts/Sec】: The System Administrator can enter the maximum number of UDP packets per second that is allow to enter the network/VPN Firewall.

【UDP Flood Threshold(Per Source IP) Pkts/Sec】: The System Administrator can enter the maximum number of UDP packets per second from attacking source IP Address that is allow to enter the network/VPN Firewall.

【UDP Flood Threshold Blocking Time (Per Source IP) Seconds】: The System Administrator can enter the blocking time when the number of UDP packets per second from attacking source IP Address that is allow to enter the network/VPN Firewall exceed the maximum number (define as above). After blocking for certain seconds, the device will start to calculate the max number of UDP packets per second from attacking source IP Address, if the max number still exceed the define value, it will block the attacking IP Address continuously.

- **Detect Ping of Death Attack:** Select this option to detect the attacks of tremendous trash data in PING packets that hackers send to cause System malfunction This attack can cause network speed to slow down, or even make it necessary to restart the computer to get a normal operation.

- **Detect Tear Drop Attack:** Select this option to detect tear drop attacks. These are packets that are segmented to small packets with negative length. Some Systems treat the negative value as a very large number, and copy enormous data into the System to cause System damage, such as a shut down or a restart.

- **Detect IP Spoofing Attack:** Select this option to detect spoof attacks. Hackers disguise themselves as trusted users of the network in **Spoof attacks**. They use a fake identity to try to pass through the Firewall System and invade the network.

- **Filter IP Source Route Option:** Each IP packet can carry an optional field that specifies the replying address that can be different from the source address specified in packet's header. Hackers can use this address field on disguised packets to invade internal networks and send internal networks' data back to them.

- **Detect Port Scan Attack:** Select this option to detect the port scans hackers use to continuously scan networks on the Internet to detect computers and vulnerable ports that are opened by those computers.

- **Detect Land Attack:** Some Systems may shut down when receiving packets with the same source and destination addresses, the same source port and destination port, and when **SYN** on the TCP header is marked. Enable this function to detect such abnormal packets.

- **Default Packet Deny:** Denies all packets from passing the Firewall. A packet can pass only when there is a policy that allows it to pass.

After enabling the needed detect functions, click **OK** to activate the changes.

Route Table

In this section, the Administrator can add static routes for the networks.

Entering the Route Table screen:

Click **Configuration** on the left side menu bar, then click **Route Table** below it. The Route Table window appears, in which current route settings are shown.

Route Table functions:

- **Interface:** Destination network, internal or external networks.
- **Destination IP:** IP address of destination network.
- **NetMask:** Netmask of destination network.
- **Gateway:** Gateway IP address for connecting to destination network.
- **Configure:** Change settings in the route table.

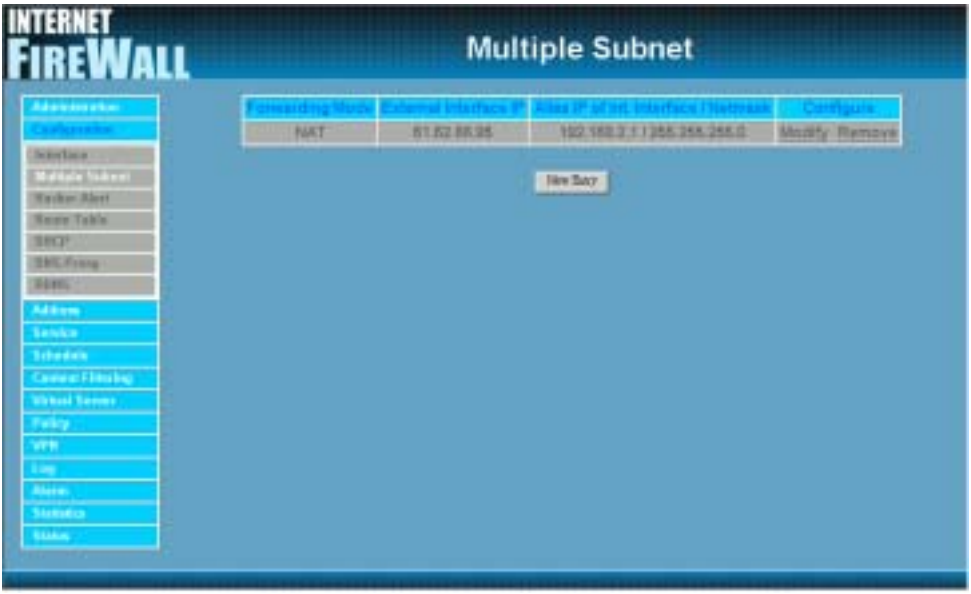
Adding a new Static Route:

Step 1. In the Route Table window, click the New Entry button.

Step 2. In the Add New Static Route window, enter new static route information.

Step 3. In the Interface field's pull-down menu, choose the network to connect (Internal, External or DMZ).

Step 4. Click **OK** to add the new static route or click **Cancel** to cancel.



Modifying a Static Route:

Step 1. In the Route Table menu, find the route to edit and click the corresponding Modify option in the Configure field.

Step 2. In the Modify Static Route window, modify the necessary routing addresses.

Step 3. Click **OK** to apply changes or click **Cancel** to cancel it.

Removing a Static Route:

Step 1. In the Route Table window, find the route to remove and click the corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to confirm removing or click **Cancel** to cancel it.

DHCP

In the section, the Administrator can configure DHCP (Dynamic Host Configuration Protocol) settings for the Internal (LAN) network.

Entering the DHCP window:

Step 1. Click **Configuration** on the left hand side menu bar, then click **DHCP** below it. The DHCP window appears in which current DHCP settings are shown on the screen.

Dynamic IP Address functions:

- **Subnet :** Internal network's subnet
- **NetMask :** Internal network's netmask
- **Gateway:** Internal network's gateway IP address
- **Broadcast:** Internal network's broadcast IP address

Enabling DHCP Support:

DHCP Address functions

Enable DHCP Support：Enable /Disable DCHP Support

- **Domain Name**：Enter the Domain Name of DHCP

Automatically Get DNS：Automatically detect DNS Server.

- **DNS Server 1** : Enter the distributed IP address of DNS Server1.
- **DNS Server 2** : Enter the distributed IP address of DNS Server2.
- **WINS Server 1** : Enter the distributed IP address of WINS Server1.
- **WINS Server 2** : Enter the distributed IP address of WINS Server2.

LAN Interface :

- **Client IP Address Range 1:** Enter the starting and the ending IP address dynamically assigning to DHCP clients.
- **Client IP Address Range 2:** Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)

DMZ Interface :

- **Client IP Address Range 1:** Enter the starting and the ending IP address dynamically assigning to DHCP clients.
- **Client IP Address Range 2:** Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)
- **Leased Time:** Enter the leased time for DHCP.

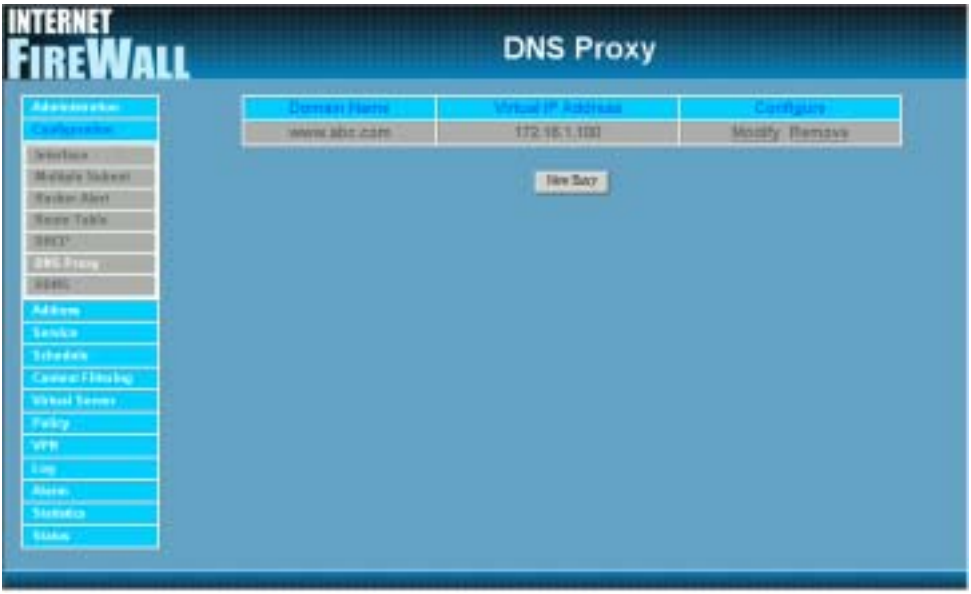
DNS-Proxy

The VPN Firewall Administrator may use the DNS Proxy function to make the VPN Firewall act as a DNS Server for the Internal and DMZ network. All DNS requests to a specific Domain Name will be routed to the firewall's IP address. For example, let's say an organization has their mail server (i.e., mail.dfl300.com) in the DMZ network (i.e. 192.168.10.10). The outside Internet world may access the mail server of the organization easily by its domain name, providing that the Administrator has set up Virtual Server or Mapped IP settings correctly. However, for the users in the Internal network, their external DNS server will assign them a public IP address for the mail server. So for the Internal network to access the mail server (mail.dfl300.com), they would have to go out to the Internet, then come back through the Firewall to access the mail server. Essentially, the internal network is accessing the mail server by a real public IP address, while the mail server serves their request by a NAT address and not a real one. This odd situation occurs when there are servers in the DMZ network and they are binded to real IP addresses. To avoid this, set up DNS Proxy so all the Internal network computers will use the VPN as a DNS server, which acts as the DNS Proxy.

If you want to use the DNS Proxy function of the VPN, the end user's main DNS server IP address should be the same IP Address as the VPN.

Entering the DNS Proxy window:

Click on **Configuration** in the menu bar, then click on **DNS Proxy** below it. The DNS Proxy window will appear.



Below is the information needed for setting up the **DNS Proxy**:

- **Domain Name:** The domain name of the server
- **Virtual IP Address:** The virtual IP address respective to DNS Proxy
- **Configure:** modify or remove each DNS Proxy policy

Adding a new DNS Proxy:

Step 1: Click on the **New Entry** button and the **Add New DNS Proxy** window will appear.

Step 2: Fill in the appropriate settings for the domain name and virtual IP address.

Step 3: Click **OK** to save the policy or **Cancel** to cancel.

Modifying a DNS Proxy:

Step 1: In the DNS Proxy window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2: Make the necessary changes needed.

Step 3: Click **OK** to save changes or click on **Cancel** to cancel modifications.

Removing a DNS Proxy:

Step 1: In the **DNS Proxy** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2: A confirmation pop-up box will appear, click **OK** to remove the DNS Proxy or click **Cancel**.

DDNS

The **DDNS** (require Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in DDNS Server will be automatically updated with the new IP address provided by ISP.

Click **DDNS** in the **Configuration** menu to enter Dynamic DNS window.

1. The nouns in Dynamic DNS window：
   - ！：Update Status【  Connecting;  Update succeed;  Update fail;  Unidentified error】
   - Domain name：Enter the password provided by ISP.
   - WAN IP Address：IP Address of the WAN port.
   - Modify：Modify dynamic DNS settings. Click **Modify** to change the DNS parameters; click Delete to delete the settings.
   -
2. How to use dynamic DNS：
   The firewall provides 3 service providers, users have to regidter first to use this function. For the usage regulations, see the providers' websites.

How to register：First, Click **DDNS** in the **Configuration** menu to enter Dynamic DNS window, then click **Add** button, on the right side of the service providers, click **Register**, the service peroviders' website will appear, please refer to the website for the way of registration.


INTERNET
FIREWALL
DDNS
External Interface IP : 210.68.147.142
Domain Name
External IP
Configure
Modify Remove

DDNS settings

Step 1: Click **DDNS** in the **Configuration** menu to enter Dynamic DNS window.

Step 2: Click **Add** button.

Step 3: Click the information in the column of the new window.

- **Service providers**：Select service providers.
- **Register**：to the service providers' website.
- **WAN IP Address**：IP Address of the WAN port.
- ☐ **automatically fill in the external IP**：Check to automatically fill in the external IP.。
- **User Name**：Enter the registered user name.
- **Password**：Enter the password provided by ISP(Internet Service Provider).
- **Domain name**：Your host domain name provided by ISP.

Step 4: Click **OK** to add dynamic DNS or click **Cancel** to discard changes.

Modify a DDNS

Step 1: Click **DDNS** in the **Configuration** menu to enter DDNS window.

Step 2: Find the item you want to change and click **Modify**.

Step 3: Enter the new information in the Modify DDNS window.

Step 4: Click **OK** to change the settings or click **Cancel** to discard changes.

Removing a DDNS

Step 1: Click **DDNS** in the **Configuration** menu to enter DDNS window.

Step 2: Find the item you want to change and click **Removing**.

Step 3: A confirmation pop-up box will appear, click OK to delete the settings or click Cancel to discard changes.

Address

The VPN VPN Firewall allows the Administrator to set Interface addresses of the Internal network, Internal network group, External network, External network group, DMZ and DMZ group.

What is the Address Table?

An IP address in the Address Table can be an address of a computer or a sub network. The Administrator can assign an easily recognized name to an IP address. Based on the network it belongs to, an IP address can be an internal IP address, external IP address or DMZ IP address. If the Administrator needs to create a control policy for packets of different IP addresses, he can first add a new group in the **Internal Network Group** or the **External Network Group** and assign those IP addresses into the newly created group. Using group addresses can greatly simplify the process of building control policies.

With easily recognized names of IP addresses and names of address groups shown in the address table, the Administrator can use these names as the source address or destination address of control policies. The address table should be built before creating control policies, so that the Administrator can pick the names of correct IP addresses from the address table when setting up control policies.

Internal

Entering the Internal window:

Step 1. Click **Internal** under the **Address** menu to enter the **Internal** window. The current setting information such as the name of the internal network, IP and Netmask addresses will show on the screen.

Adding a new Internal Address:

Step 1. In the Internal window**,** click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings of a new internal network address.

Step 3. Click **OK** to add the specified internal network or click **Cancel** to cancel the changes.

Modifying an Internal Address:

Step 1. In the Internal window, locate the name of the network to be modified. Click the **Modify** option in its corresponding **Configure** field. The **Modify Address** window appears on the screen immediately.

Step 2. In the **Modify Address** window, fill in the new addresses.

Step 3. Click **OK** to save changes or click **Cancel** to discard changes.

Removing an Internal Address:

Step 1. In the **Internal** window, locate the name of the network to be removed. Click the **Remove** option in its corresponding **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.

Internal Group

Entering the Internal Group window:
The Internal Addresses may be combined together to become a group.
Click **Internal Group** under the **Address** menu to enter the Internal Group window. The current setting information for the Internal network group appears on the screen.

Adding an Internal Group:

Step 1. In the **Internal Group** window, click the **New Entry** button to enter the **Add New Address Group** window.

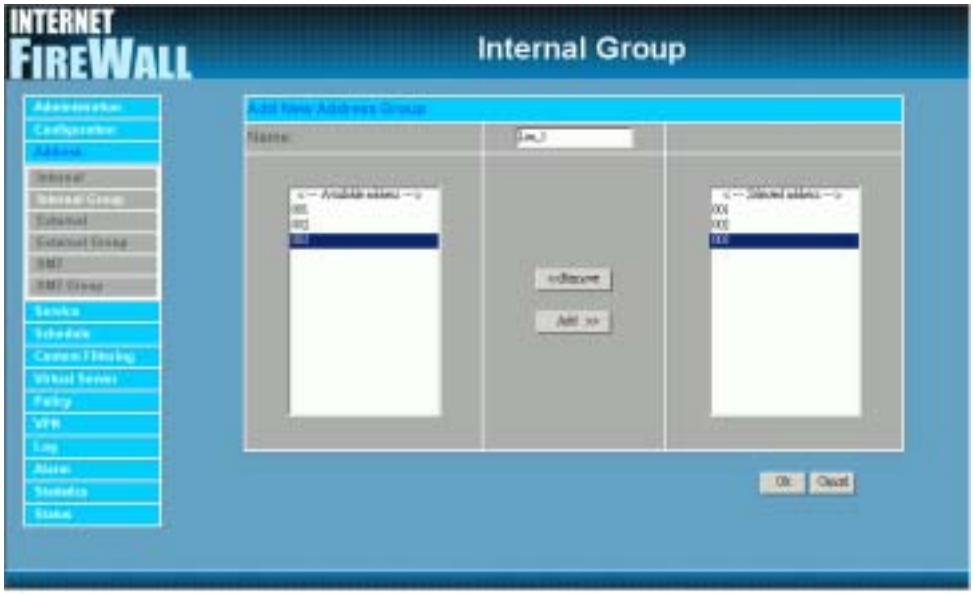
Step 2. In the **Add New Address Group** window:

- **Available Address:** list the names of all the members of the internal network.
- **Selected Address:** list the names to be assigned to the new group.
- **Name:** enter the name of the new group in the open field.

Step 3. **Add members:** Select names to be added in Available Address list, and click the **Add>>** button to add them to the Selected Address list.

Step 4. **Remove members:** Select names to be removed in the Selected Address list, and click the **<<Remove** button to remove these members from Selected Address list.

Step 5. Click **OK** to add the new group or click Cancel to discard changes.



Modifying an Internal Group:

Step 1. In the **Internal Group** window, locate the network group desired to be modified and click its corresponding **Modify** option in the **Configure** field.

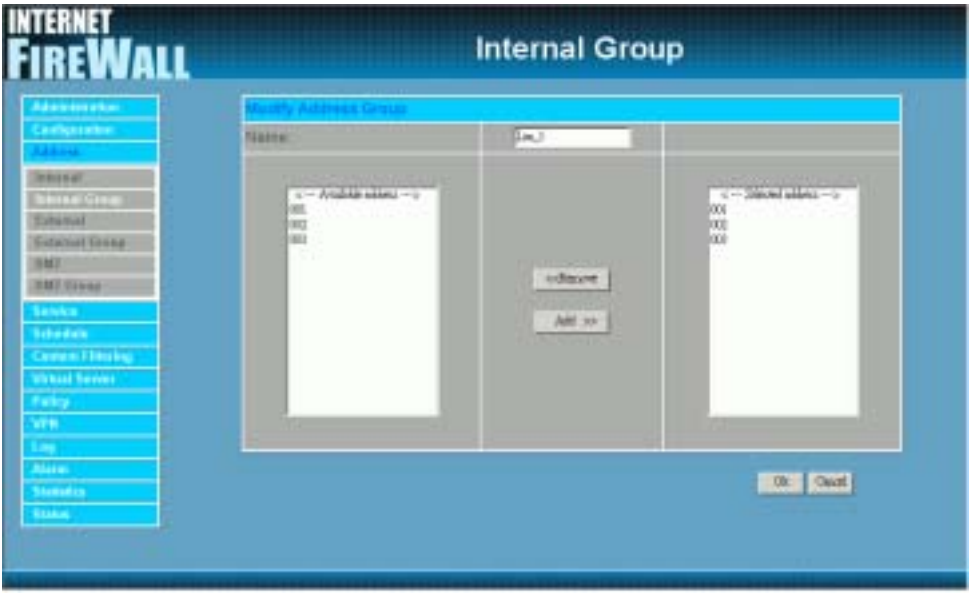
Step 2. A window displaying the information of the selected group appears:

- **Available Address:** list names of all members of the Internal network.
- **Selected Address:** list names of members which have been assigned to this group.

Step 3. **Add members:** Select names in **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 4. **Remove members:** Select names in the **Selected Address** list, and click the **<<Remove** button to remove these members from the **Selected Address** list.

Step 5. Click **OK** to save changes or click **Cancel** to discard changes.



Removing an Internal Group:

Step 1. In the **Internal Group** window, locate the group to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the group or click **Cancel** to discard changes.

External

Entering the External window:

Click **External** under the **Address** menu to enter the External window. The current setting information, such as the name of the External network, IP and Netmask addresses will show on the screen.

Adding a new External Address:

Step 1. In the External window, click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings for a new external network address.

Step 3. Click **OK** to add the specified external network or click **Cancel** to discard changes.

Modifying an External Address:

Step 1. In the External table, locate the name of the network to be modified and click the **Modify** option in its corresponding **Configure** field.

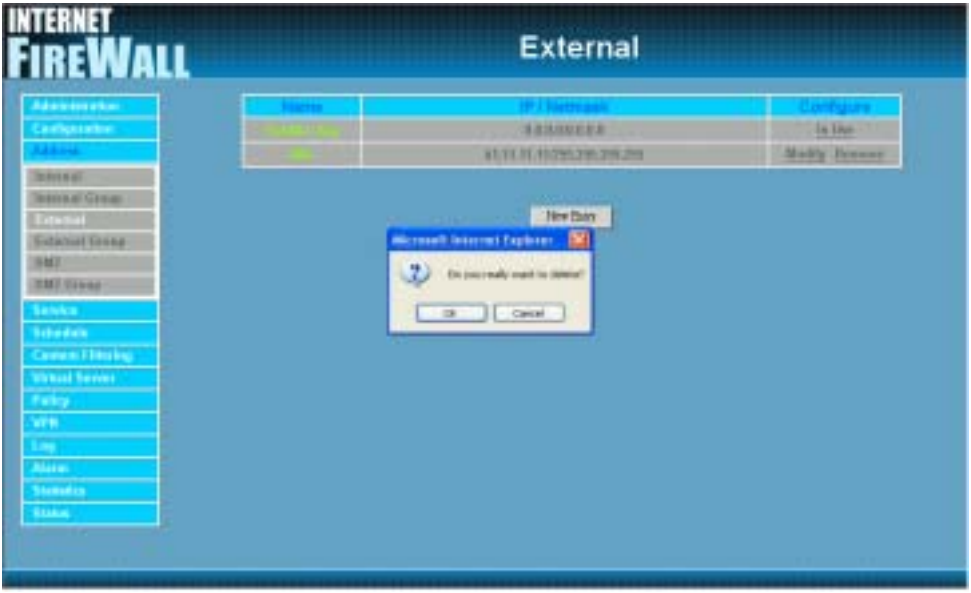
Step 2. The **Modify Address** window will appear on the screen immediately. In the **Modify Address** window, fill in new addresses.

Step 3. Click **OK** to save changes or click **Cancel** to discard changes.

Removing an External Address:

Step 1. In the **External** table, locate the name of the network to be removed and click the **Remove** option in its corresponding **Configure** field.

Step 2. In the **Remove confirmation** pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.



External Group

Entering the External Group window:
Click the **External Group** under the **Address** menu bar to enter the External window. The current settings for the external network group(s) will appear on the screen.

Adding an External Group:

Step 1. In the **External Group** window, click the **New Entry** button and the **Add New Address Group** window will appear.

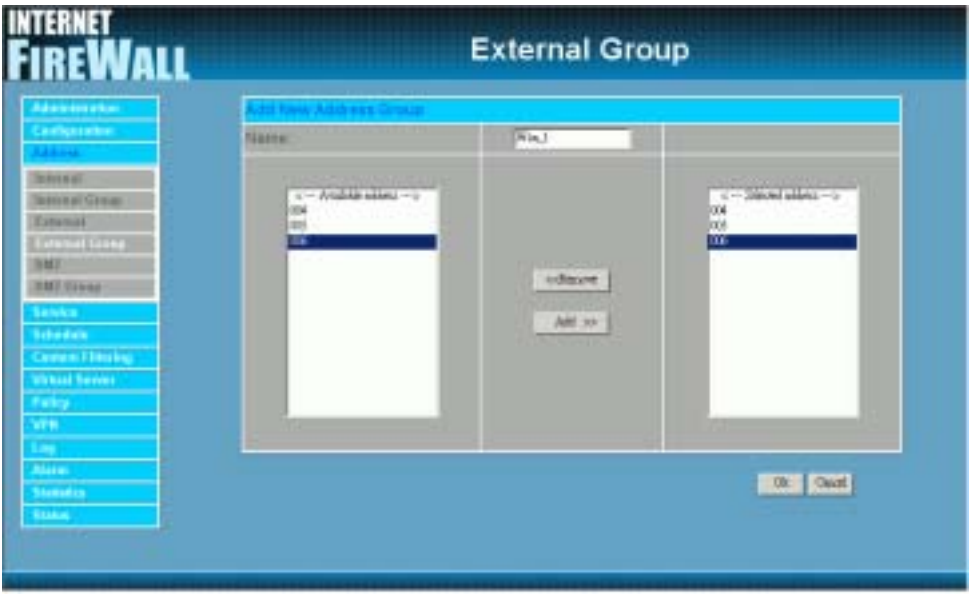
Step 2. In the **Add New Address Group** window the following fields will appear:

- **Name:** enter the name of the new group.
- **Available Address:** List the names of all the members of the external network.
- **Selected Address:** List the names to assign to the new group.

Step 3. **Add members:** Select the names to be added in the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 4. **Remove members:** Select the names to be removed in the **Selected Address** list, and click the **<<Remove** button to remove them from the **Selected Address** list.

Step 5. Click **OK** to add the new group or click **Cancel** to discard changes.



Editing an External Group:

Step 1. In the **External Group** window, locate the network group to be modified and click its corresponding **Modify** button in the **Configure** field.

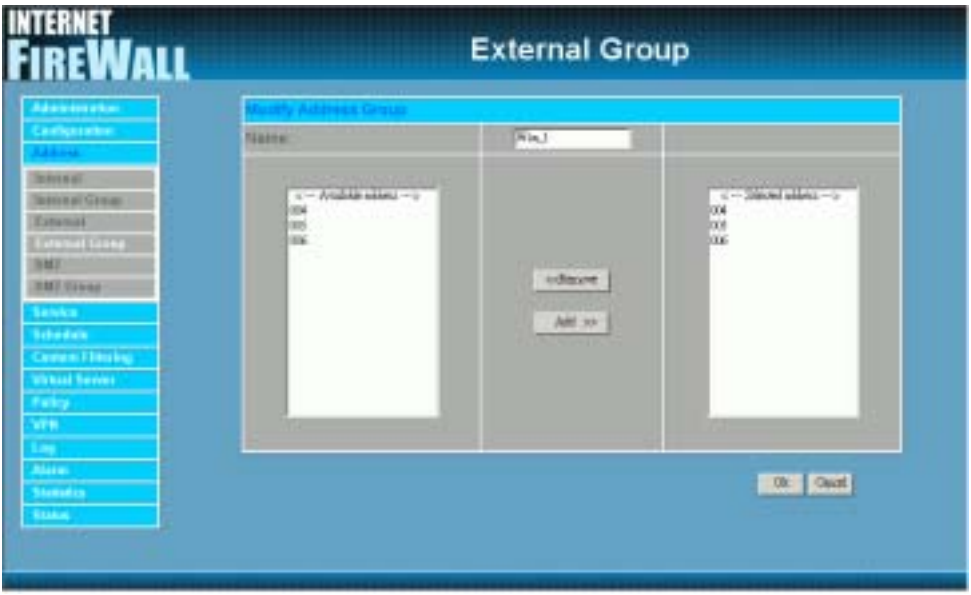
Step 2. A window displaying the information of the selected group appears:

- **Available Address:** list the names of all the members of the external network.
- **Selected Address:** list the names of the members that have been assigned to this group.

Step 3. **Add members:** Select the names to be added in the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 4. **Remove members:** Select the names to be removed in the **Selected Address** list, and click the **<<Remove** button to remove them from the **Selected Address** list.

Step 5. Click **OK** to save changes or click **Cancel** to discard changes.



Removing an External Group:

Step 1. In the **External Group** window, locate the group to be removed and click its corresponding **Modify** option in the **Configure** field.

Step 2. In the **Remove confirmation** pop-up box, click **OK** to remove the group or click **Cancel** to discard changes.

DMZ

Entering the DMZ window:

Click **DMZ** under the **Address** menu to enter the **DMZ** window. The current setting information such as the name of the internal network, IP, and Netmask addresses will show on the screen.

Adding a new DMZ Address:

Step 1. In the DMZ window, click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings for a new DMZ address.

Step 3. Click **OK** to add the specified DMZ or click **Cancel** to discard changes.

Modifying a DMZ Address:

Step 1. In the **DMZ** window, locate the name of the network to be modified and click the **Modify** option in its corresponding **Configure** field.

Step 2. In the **Modify Address** window, fill in new addresses.

Step 3. Click **OK** on save the changes or click **Cancel** to discard changes.

Removing a DMZ Address:

Step 1. In the **DMZ** window, locate the name of the network to be removed and click the **Remove** option in its corresponding **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.

DMZ Group

Entering the DMZ Group window:

Click **DMZ Group** under the **Address** menu to enter the **DMZ** window. The current settings information for the DMZ group appears on the screen.

Adding a DMZ Group:

Step 1. In the DMZ Group window, click the **New Entry** button.

Step 2. In the **Add New Address** Group window:

- **Available Address:** list names of all members of the DMZ.
- **Selected Address:** list names to assign to a new group.

Step 3. **Name:** enter a name for the new group.

Step 4. **Add members:** Select the names to be added from the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 5. **Remove members:** Select names to be removed from the **Selected Address** list, and click the **<<Remove** button to remove them from the **Selected Address** list.

Step 6. Click **OK** to add the new group or click **Cancel** to discard changes.

Modifying a DMZ Group:

Step 1. In the **DMZ** Group window, locate the **DMZ** group to be modified and click its corresponding **Modify** button in the **Configure** field.

Step 2. A window displaying information about the selected group appears:

- **Available Address:** list the names of all the members of the DMZ.
- **Selected Address:** list the names of the members that have been assigned to this group.

Step 3. **Add members:** Select names to be added from the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 4. **Remove members:** Select names to be removed from the **Selected Address** list, and click the **<<Remove** button to remove them from **Selected Address** list.

Step 5. Click **OK** to save changes or click Cancel to cancel editing.

Removing a DMZ Group:

Step 1. In the **DMZ Group** window, locate the group to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove confirmation** pop-up box, click **OK** to remove the group.

Service

In this section, network services are defined and new network services can be added. There are three sub menus under Service which are: Pre-defined, Custom, and Group. The Administrator can simply follow the instructions below to define the protocols and port numbers for network communication applications. Users then can connect to servers and other computers through these available network services.

What is Service?

TCP and UDP protocols support varieties of services, and each service consists of a TCP Port or UDP port number, such as TELNET(23), SMTP(21), POP3(110),etc. The VPN Firewall defines two services: pre-defined service and custom service. The common-use services like TCP and UDP are defined in the pre-defined service and cannot be modified or removed. In the custom menu, users can define other TCP port and UDP port numbers that are not in the pre-defined menu according to their needs. When defining custom services, the client port ranges from 1024 to 65535 and the server port ranges from 0 to 1023.

How do I use Service?

The Administrator can add new service group names in the **Group** option under **Service** menu, and assign desired services into that new group. Using service group the Administrator can simplify the processes of setting up control policies. For example, there are 10 different computers that want to access 5 different services on a server, such as HTTP, FTP, SMTP, POP3, and TELNET. Without the help of service groups, the Administrator needs to set up 50 (10x5) control policies, but by applying all 5 services to a single group name in the **service** field, it takes only one control policy to achieve the same effect as the 50 control policies.

Pre-defined

Entering a Pre-defined window:

Click **Service** on the menu bar on the left side of the window. Click **Pre-defined** under it. A window will appear with a list of services and their associated IP addresses. This list cannot be modified.

Custom

Entering the Custom window:

Click **Service** on the menu bar on the left side of the window. Click **Custom** under it. A window will appear with a table showing all services currently defined by the Administrator.

Adding a new Service:

Step 1. In the **Custom** window, click the **New Entry** button and a new service table appears.

Step 2 In the new service table:

- **New Service Name:** This will be the name referencing the new service.
- **Protocol**: Enter the network protocol type to be used, such as TCP, UDP, or Other (please enter the number for the protocol type).
- **Client Port:** enter the range of port number of new clients.
- **Server Port:** enter the range of port number of new servers.

The client port ranges from 1024 to 65535 and the server port ranges from 0 to 1023.

Step 3 Click **OK** to add new services, or click **Cancel** to cancel.

Modifying Custom Services:

Step 1. In the **Custom** table, locate the name of the service to be modified. Click its corresponding **Modify** option in the **Configure** field.

Step 2. A table showing the current settings of the selected service appears on the screen

Step 3. Enter the new values.

Step 4. Click **OK** to accept editing; or click **Cancel**.

Removing Custom Services:

Step 1. In the **Custom** window, locate the service to be removed. Click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the selected service or click **Cancel** to cancel action.

Group

Accessing the Group window:
Click **Service** in the menu bar on the left hand side of the window. Click **Group** under it. A window will appear with a table displaying current service group settings set by the Administrator.

Adding Service Groups:

Step 1. In the **Group** window, click the **New Entry** button.
In the **Add Service Group** window, the following fields will appear:

- **Available Services:** list all the available services.
- **Selected Services:** list services to be assigned to the new group.

Step 2. Enter the new group name in the group **Name** field. This will be the name referencing the created group.

Step 4. **To add new services:** Select the services desired to be added in the **Available Services** list and then click the **Add>>** button to add them to the group.

Step 5. **To remove services:** Select services desired to be removed in the **Available Services**, and then click the **<<Remove** button to remove them from the group.

Step 6. Click **OK** to add the new group.

Modifying Service Groups:

Step 1. In the **Group** window, locate the service group to be edited. Click its corresponding **Modify** option in the **Configure** field.

Step 2. In the **Mod (modify) group** window the following fields are displayed::

- **Available Services:** lists all the available services.
- **Selected Services:** list services that have been assigned to the selected group.

Step 3. **Add new services:** Select services in the **Available Services** list, and then click the **Add>>** button to add them to the group.

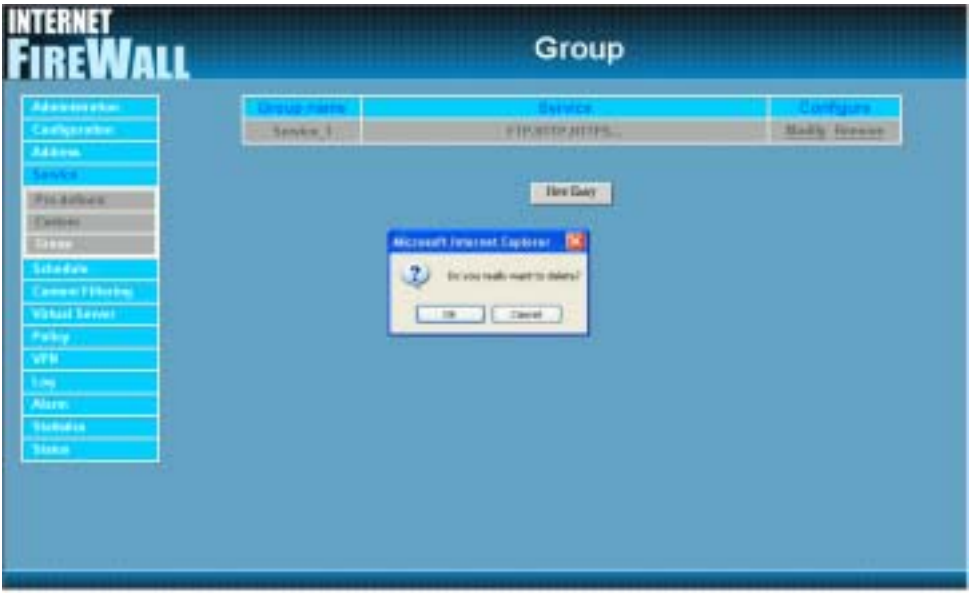
Step 4. **Remove services:** Select services to be removed in the **Selected Services** list, and then click the **<<Remove** button to remove theses services from the group.

Step 5. Click **OK** to save editing changes.

Removing Service Groups:

Step 1. In the **Group** window, locate the service group to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the selected service group or click **Cancel** to cancel removing.

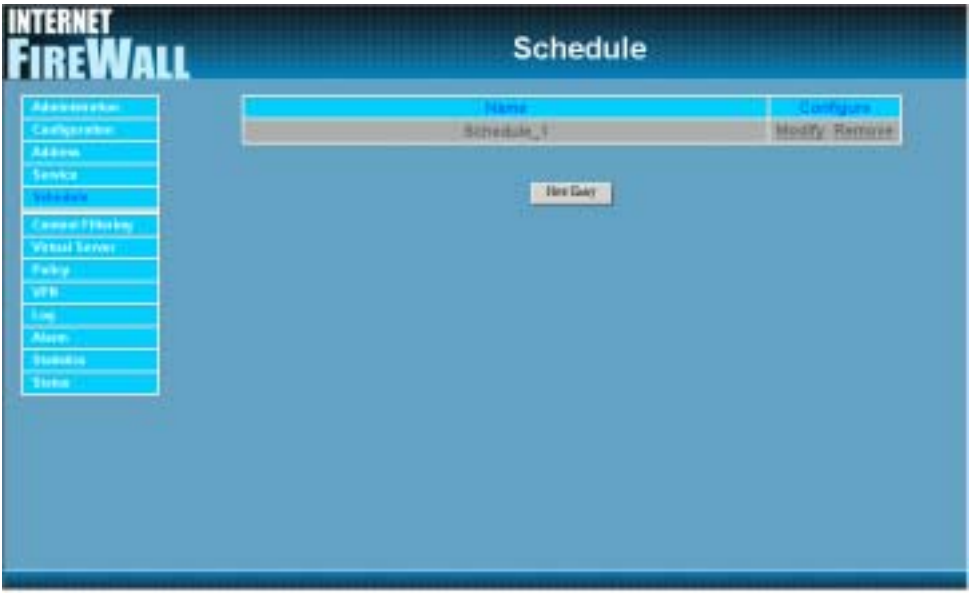


Schedule

The VPN VPN Firewall allows the Administrator to configure a schedule for policies to take affect. By creating a schedule, the Administrator is allowing the Firewall policies to be used at those designated times only. Any activities outside of the scheduled time slot will not follow the Firewall policies therefore will likely not be permitted to pass through the Firewall. The Administrator can configure the start time and stop time, as well as creating 2 different time periods in a day. For example, an organization may only want the Firewall to allow the internal network users to access the Internet during work hours. Therefore, the Administrator may create a schedule to allow the Firewall to work Monday-Friday, 8AM-5PM only. During the non-work hours, the Firewall will not allow Internet access.

Accessing the Schedule window:

Click on **Schedule** on the menu bar and the schedule window will appear displaying the active schedules.



The following items are displayed in this window:
Name: the name assigned to the schedule
Comment: a short comment describing the schedule
Configure: modify or remove

Adding a new Schedule:

Step 1: Click on the **New Entry** button and the **Add New Schedule** window will appear.

Step 2:

Schedule Name: Fill in a name for the new schedule.

Period 1: Configure the start and stop time for the days of the week that the schedule will be active.

Step 3: Click Ok to save the new schedule or click Cancel to cancel adding the new schedule.

Modifying a Schedule:

Step 1: In the **Schedule** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

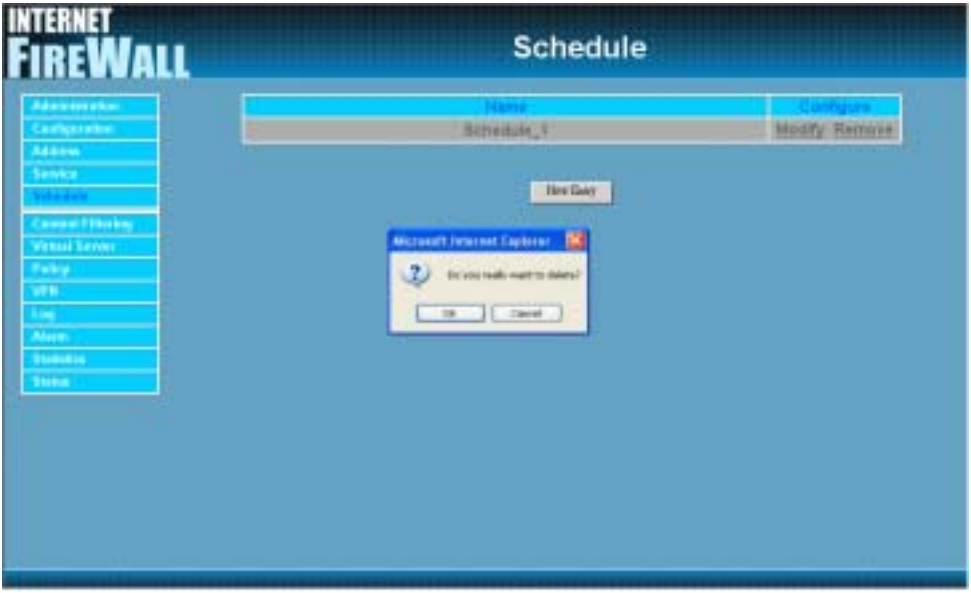
Step 2: Make needed changes.

Step 3: Click **OK** to save changes.

Removing a Schedule:

Step 1: In the **Schedule** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2: A confirmation pop-up box will appear, click on **OK** to remove the schedule.



Content filtering

Content filtering includes URL Blocking and general filtering. Content Filtering includes「**URL Blocking**」and 「**General Blocking**」。

（一）**URL Blocking**：The device manager can use a complete domain name, key word, “ ” or “*” to make rules for specific websites.

（二）**General Blocking**：To let Popup、ActiveX、Java、Cookie in or keep them out.

URL Blocking

The Administrator may setup URL Blocking to prevent Internal network users from accessing a specific website on the Internet. Any web request coming from an Internal network computer to a blocked website will receive a blocked message instead of the website.

Entering the URL blocking window:

Click on **URL Blocking** under the **Configuration** menu bar.
Click on **New Entry.**

Adding a URL Blocking policy:

Step 1: After clicking **New Entry**, the **Add New Block String** window will appear.

Step 2: Enter the URL of the website to be blocked.

Step 3: Click **OK** to add the policy. Click Cancel to discard changes.

Modifying a URL Blocking policy:

Step 1: In the **URL Blocking** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2: Make the necessary changes needed.

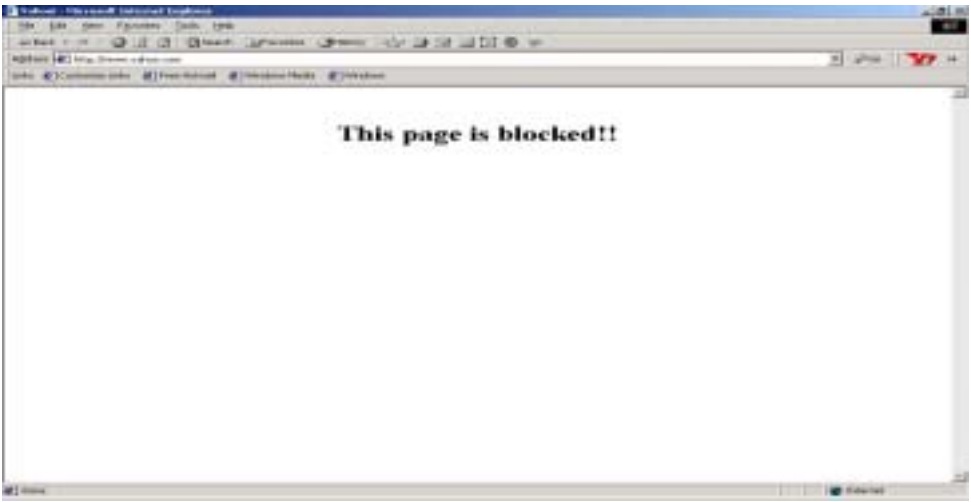
Step 3: Click on **OK** to save changes or click on Cancel to cancel modifications.

Removing a URL Blocking policy:

Step 1: In the **URL Blocking** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2: A confirmation pop-up box will appear, click on **OK** to remove the policy or click on Cancel to discard changes.

Blocked URL site:
When a user from the Internal network tries to access a blocked URL, the error below will appear.



Script Blocking

To let Popup、ActiveX、Java、Cookie in or keep them out.

Step 1: Click **Content Filtering** in the menu.

Step 2: 【**Script Blocking**】detective functions.

- Popup filtering：Prevent the pop-up boxes appearing.
- ActiveX filtering：Prevent ActiveX packets.
- Java filtering：Prevent Java packets.
- Cookie filtering：Prevent Cookie packets.

Step 3: After selecting each function, click the **OK** button below.

When the system detects the setting, the firewall will spontaneously work.

Virtual Server

The VPN VPN Firewall separates an enterprise's Intranet and Internet into internal networks and external networks respectively. Generally speaking, in order to allocate enough IP addresses for all computers, an enterprise assigns each computer a private IP address, and converts it into a real IP address through Firewall's NAT (Network Address Translation) function. If a server which provides service to the external networks, is located in the internal networks, outside users can't directly connect to the server by using the server's private IP address.

The VPN Firewall's Virtual Server can solve this problem. A virtual server has set the real IP address of the Firewall's external network interface to be the Virtual Server IP. Through the virtual server feature, the Firewall translates the virtual server's IP address into the private IP address of physical server in the Internal (LAN) network. When outside users on the Internet request connections to the virtual server, the request will be forwarded to the private internal server.

Virtual Server owns another feature know as one-to-many mapping. This is when one virtual server IP address on the external interface can be mapped into 4 internal network server private IP addresses. This option is useful for Load Balancing, which causes the virtual server to distribute data packets to each private IP addresses (which are the real servers). By sending all data packets to all similar servers, this increases the server's efficiency, reduces risks of server crashes, and enhances servers' stability.

How to use Virtual Server and mapped IP

Virtual Server and Mapped IP are part of the IP mapping scheme. By applying the incoming policies, Virtual Server and IP mapping work similarly. They map real IP addresses to the physical servers' private IP addresses (which is opposite to NAT), but there still exists some differences:

- Virtual Server can map one real IP to several internal physical servers while Mapped IP can only map one real IP to one internal physical server (1-to-1 Mapping). The Virtual Servers' load balance feature can map a specific service request to different physical servers running the same services.
- Virtual Server can only map one real IP to one service/port of the internal physical servers while Mapped IP maps one real IP to all the services offered by the physical server.

IP mapping and Virtual Server work by binding the IP address of the external virtual server to the private internal IP address of the physical server that supports the services. Therefore users from the external network can access servers of the internal network by requesting the service from the IP address provided by Virtual Server.

Mapped IP

Internal private IP addresses are translated through NAT (Network Address Translation). If a server is located in the internal network, it has a private IP address, and outside users cannot connect directly to internal servers' private IP address. To connect to a internal network server, outside users have to first connect to a real IP address of the external network, and the real IP is translated to a private IP of the internal network. Mapped IP and Virtual Server are the two methods to translate the real IP into private IP. Mapped IP maps IP in one-to-one fashion; that means, all services of one real external IP address is mapped to one private internal IP address.

Entering the Mapped IP window:

Click **Mapped IP** under the **Virtual Server** menu bar and the Mapped IP configuration window will appear.

Adding a new IP Mapping:

Step 1. In the **Mapped IP** window, click the New Entry button the Add New Mapped IP window will appear.

- External IP: select the external public IP address to be mapped.
- Internal IP: enter the internal private IP address or DMZ IP address which will be mapped 1-to-1 to the external IP address.

Step 2. Click **OK** to add new IP Mapping or click **Cancel** to cancel adding.

Modifying a Mapped IP:

Step 1. In the **Mapped IP** table, locate the Mapped IP desired to be modified and click its corresponding Modify option in the Configure field.

Step 2. Enter settings in the Modify Mapped IP window.

Step 3. Click **OK** to save change or click **Cancel** to cancel.

Note: *A Mapped IP cannot be modified if it has been assigned/used as a destination address of any Incoming policies.*

Removing a Mapped IP:

Step 1. In the Mapped IP table, locate the Mapped IP desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up window, click **Ok** to remove the Mapped IP or click **Cancel** to cancel.

Virtual Server

Virtual server is a one-to-many mapping technique, which maps a real IP address from the external interface to private IP addresses of the internal network. This is done to provide services or applications defined in the Service menu to enter into the internal network. Unlike a mapped IP which binds an external IP to an Internal/DMZ IP, virtual server binds external IP ports to Internal IP ports.

Adding a Virtual Server:

Step 1. Click an available virtual server from **Virtual Server** in the **Virtual Server** menu bar to enter the virtual server configuration window. In the following, Virtual Server is assumed to be the chosen option:

Step 2. Click the **click here to configure** button and the Add new Virtual Server IP window appears and asks for an IP address from the external network.

Step 3. Select an IP address from the drop-down list of available external network IP addresses.

Note: *If the drop-down list contains only (Disable), there is no available IP addresses of external network of the System and no Virtual Server can be added.*

Step 4. Click **OK** to add new Virtual Server or click **Cancel** to cancel adding.

Modifying a Virtual Server IP Address:

Step 1. Click the virtual server to be modified Virtual Server under the **Virtual Server** menu bar. A new window appears displaying the IP address and service of the specified virtual server.

Step 2. Click on the Virtual Server's IP Address button at the top of the screen.

Step 3. Choose a new IP address from the drop-down list.

Step 4. Click **OK** to save new IP address or click **Cancel** to cancel modification.

Removing a Virtual Server:

Step 1. Click the virtual server to be removed in the corresponding Virtual Server option under the **Virtual Server** menu bar. A new window displaying the virtual server's IP address and service appears on the screen.

Step 2. Click the Virtual Server's IP Address button at the top of the screen.

Step 3. Select Disable in the drop-down list in.

Step 4. Click **OK** to remove the virtual server.

Setting the Virtual Server's services:

Step 1. For the Virtual Server which has already been set up with an IP address, click the New Service button in the table.

Step 2. In the Virtual Server Configurations window:

- **Virtual Server IP:** displays the external IP address assigned to the Virtual Server
- **External Service Port:** select the port number that the virtual server will use. Changing the Service will change the port number to match the service.
- **Service:** select the service from the pull down list that will be provided by the Virtual Server.

Note: *The services in the drop-down list are all defined in the Pre-defined and Custom section of the* ***Service*** *menu.*

Step 3. Enter the IP address of the internal network server(s), to which the virtual server will be mapped. Up to four IP addresses can be assigned at most.

Step 4. Click **OK** to save the settings of the Virtual Server.

Modifying the Virtual Server configurations:

Step 1. In the Virtual Server window's service table, locate the name of the service desired to be modified and click its corresponding Modify option in the Configure field.

Step 2. In the Virtual Server Configuration window, enter the new settings.

Step 3. Click **OK** to save modifications or click **Cancel** to cancel modification.

Note: *A virtual server cannot be modified or removed if it has been assigned to the destination address of any Incoming policies.*

Removing the Virtual Server service:

Step 1. In the Virtual Server window's service table, locate the name of the service desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up box, click **Ok** to remove the service or click **Cancel** to cancel removing.

Policy

This section provides the Administrator with facilities to sent control policies for packets with different source IP addresses, source ports, destination IP addresses, and destination ports. Control policies decide whether packets from different network objects, network services, and applications are able to pass through the Firewall.

What is Policy?

The VPN uses policies to filter packets. The policy settings are: source address, destination address, services, permission, packet log, packet statistics, and flow alarm. Based on its source addresses, a packet can be categorized into:

(1). Outgoing: a client is in the internal networks while a server is in the external networks.

(2) Incoming, a client is in the external networks, while a server is in the internal networks.

(3) To DMZ: a client is either in the internal networks or in the external networks while, server is in DMZ.

(4) From DMZ, a client is in DMZ while server is either in the internal networks or in the external networks.

How do I use Policy?

The policy settings are source addresses, destination addresses, services, permission, log, statistics, and flow alarm. Among them, source addresses, destination addresses and IP mapping addresses have to be defined in the **Address** menu in advance. Services can be used directly in setting up policies, if they are in the Pre-defined Service menu. Custom services need to be defined in the C**ustom** menu before they can be used in the policy settings.

If the destination address of an incoming policy is a Mapped IP address or a Virtual Server address, then the address has to be defined in the **Virtual Server** section instead of the **Address** section.

Policy Directions:

Step 1.	In **Address**, set names and addresses of source networks and destination networks.
Step 2.	In **Service**, set services.
Step 3.	In **Virtual Server**, set names and addresses of mapped IP or virtual server (only applied to **Incoming policies**).
Step 4.	Set control policies in **Policy**

Outgoing

This section describes steps to create policies for packets and services from the Internal (LAN) network to the External (WAN) network.

Entering the Outgoing window:

Click **Policy** on the left hand side menu bar, then click **Outgoing** under it. A window will appear with a table displaying currently defined Outgoing policies.

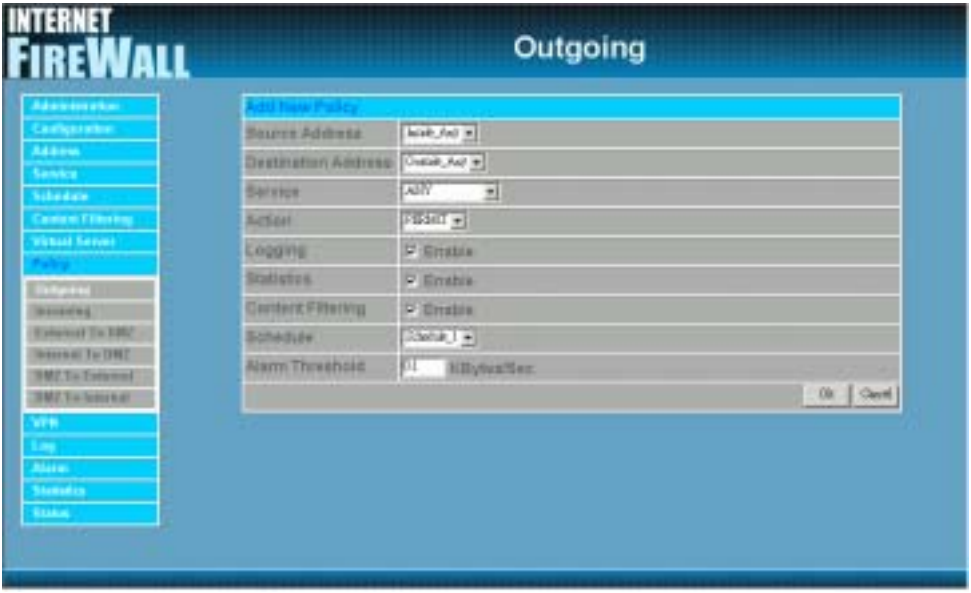
The fields in the Outgoing window are:

- **Source:** source network addresses that are specified in the **Internal** section of **Address** menu, or all the Internal (LAN) network addresses.
- **Destination:** destination network addresses that are specified in the **External** section of the **Address** menu, or all the External (WAN) network addresses.
- **Service:** specify services provided by external network servers.
- **Action:** control actions to permit or deny packets from internal networks to external network travelling through the Firewall.
- **Option:** specify the monitoring functions on packets from internal networks to external networks travelling through the Firewall.

- **Configure:** modify settings.
- **Move:** this sets the priority of the policies, number 1 being the highest priority.

Adding a new Outgoing Policy:

Step 1: Click on the New Entry button and the Add New Policy window will appear.



Step 2:

Source Address: Select the name of the Internal (LAN) network from the drop down list. The drop down list contains the names of all internal networks defined in the **Internal** section of the **Address** menu. To create a new source address, please go to the **Internal** section under the **Address** menu.

Destination Address: Select the name of the External (WAN) network from the drop down list. The drop down list contains the names of all external networks defined in the **External** section of the **Address** window. To create a new destination address, please go to the **External** section under the **Address** menu.

Service: Specified services provided by external network servers. These are services/application that are allowed to pass from the Internal network to the External network. Choose ANY for all services.

Action: Select Permit or Deny from the drop down list to allow or reject the packets travelling between the source network and the destination network.

Logging: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

Content Filtering: Select Enable to enable Content Filtering.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: set a maximum flow rate (in Kbytes/Sec). An alarm will be sent if flow rates are higher than the specified value.

Step 3: Click **OK** to add a new outgoing policy; or click **Cancel** to cancel adding a new outgoing policy.

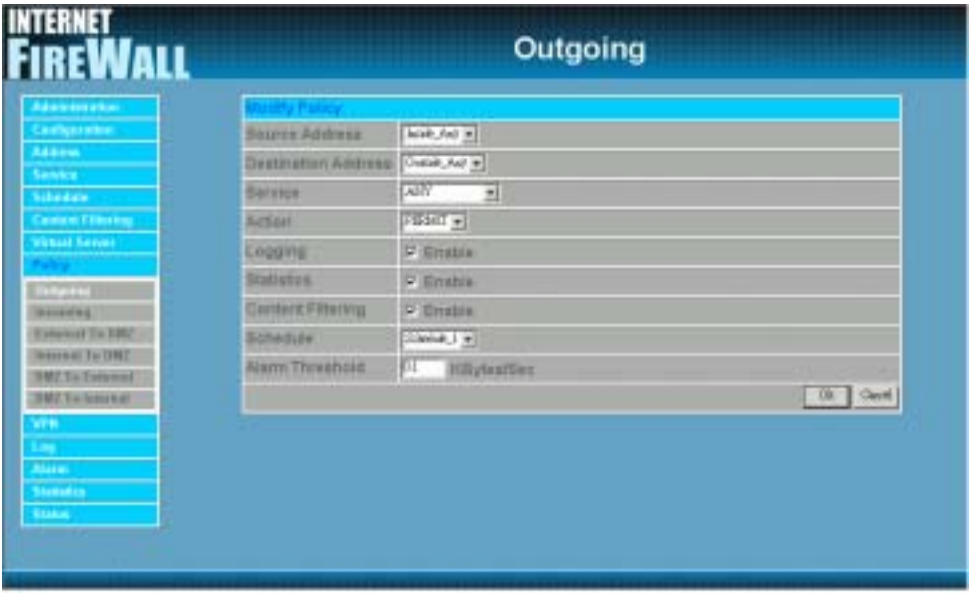
Modifying an Outgoing policy:

Step 1: In the **Outgoing** policy section, locate the name of the policy desired to be modified and click its corresponding Modify option under the Configure field.

Step 2: In the **Modify Policy** window, fill in new settings.

Note: To change or add selections in the drop-down list for source or destination address, go to the section where the selections are setup. (Source Address→ Internal of **Address** menu; Destination Address → External of **Address** menu; Service→[Pre-defined],[Custom] or Group under **Service**).

Step 3: Click **OK** to do confirm modification or click **Cancel** to cancel it.



Removing the Outgoing Policy:

Step 1. In the **Outgoing** policy section, locate the name of the policy desired to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation dialogue box, click **OK** to remove the policy or click **Cancel** to cancel removing.

Enabled Monitoring function:

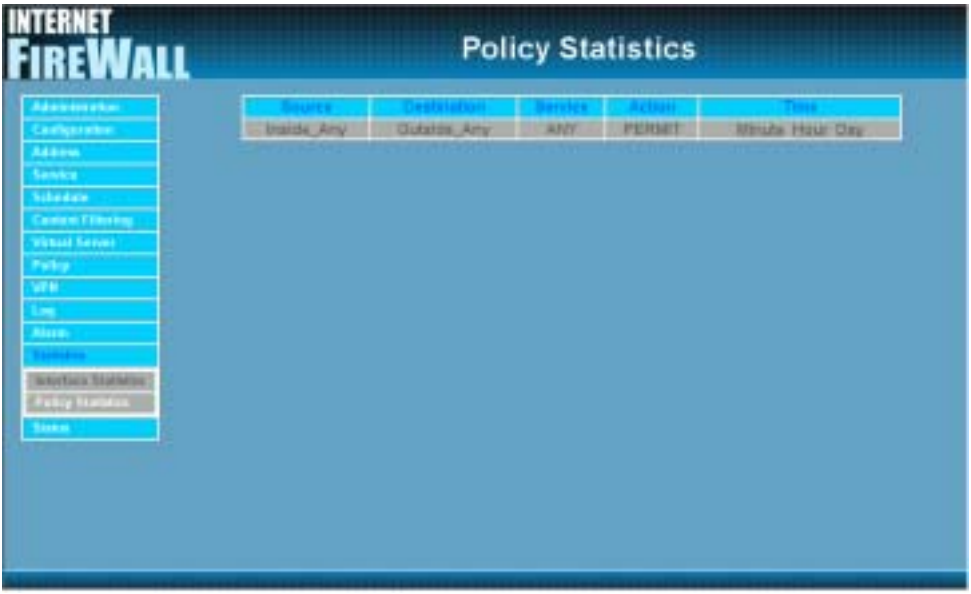
Log: If Logging is enabled in the outgoing policy, the VPN will log the traffic and event passing through the Firewall. The Administrator can click **Log** on the left menu bar to get the flow and event logs of the specified policy.

Note: *System Administrator can back up and clear logs in this window. Check* ***the chapter entitled "Log"*** *to get details about the log and ways to back up and clear logs.*

Alarm: If Logging is enabled in the outgoing policy, the VPN Firewall will log the traffic alarms and event alarms passing through the Firewall. The Administrator can click **Alarm** on the left menu to get the logs of flow and event alarms of the specified policy.

Note: *The Administrator can also get information on alarm logs from the Alarm window. Please refer to the section entitled "**Alarm"** for more information.*

Statistics: If Statistics is enabled in the outgoing policy, the VPN will display the flow statistics passing through the Firewall.



Note: *The Administrator can also get flow statistics in* ***Statistics****. Please refer to* ***Statistics*** *in Chapter 11 for more details.*

Incoming

This chapter describes steps to create policies for packets and services from the External (WAN) network to the Internal (LAN) network including Mapped IP and Virtual Server.

Enter Incoming window:

Step 1: Click **Incoming** under the **Policy** menu to enter the Incoming window. The Incoming table will display current defined policies from the External (WAN) network to assigned Mapped IP or Virtual Server.

Step 2: The fields of the **Incoming** window are:

- **Source:** source networks which are specified in the **External** section of the **Address** menu, or all the external network addresses.
- **Destination:** destination networks, which are IP Mapping addresses or Virtual server network addresses created in **Virtual Server** menu.
- **Service:** services supported by Virtual Servers (or Mapped IP).
- **Action:** control actions to permit or deny packets from external networks to Virtual Server/Mapped IP travelling through the VPN.

- **Option:** specify the monitoring functions on packets from external networks to Virtual Server/Mapped IP travelling through the Firewall.
- **Configure:** modify settings or remove incoming policy.
- **Move:** this sets the priority of the policies, number 1 being the highest priority.

Adding an Incoming Policy:

Step 1: Under **Incoming** of the **Policy** menu, click the New Entry button.

Step 2:

Source Address: Select names of the external networks from the drop down list. The drop down list contains the names of all external networks defined in the **External** section of the **Address** menu. To create a new source address, please go to the **Internal** section under the **Address** menu.

Destination Address: Select names of the internal networks from the drop down list. The drop down list contains the names of IP mapping addresses specified in the **Mapped IP** or the **Virtual Server** sections of **Virtual Server** menu. To create a new destination address, please go to the **Virtual Server** menu. (Please refer to Chapter 8 for Virtual Server for details)

Service: Specified services provided by internal network servers. These are services/application that are allowed to pass from the External network to the Internal network. Choose ANY for all services.

Action: Select Permit or Deny from the drop down list to allow or reject the packets travelling between the specified external network and Virtual Server/Mapped IP.

Logging: select Enable to enable flow monitoring.

Statistics: select Enable to enable flow statistics.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: set a maximum flow rate (in Kbytes/Sec). An alarm will be sent if flow rates are higher than the specified value.

Step 3: Click **OK** to add new policy or click **Cancel** to cancel adding new incoming policy.

Modifying Incoming Policy:

Step 1: In the **Incoming** window, locate the name of policy desired to be modified and click its corresponding Modify option in the Configure field.

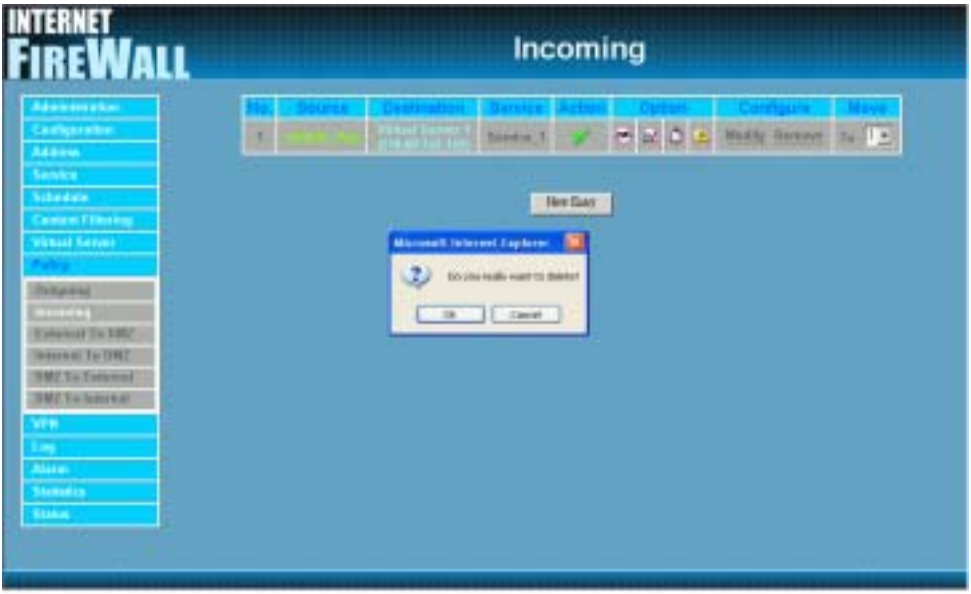
Step 2: In the Modify Policy window, fill in new settings.

Step 3: Click **OK** to save modifications or click **Cancel** to cancel modifications.

Removing an Incoming Policy:

Step 1: In the **Incoming** window, locate the name of policy desired to be removed and click its corresponding [Remove] in the Configure field.

Step 2: In the Remove confirmation window, click **Ok** to remove the policy or click **Cancel** to cancel removing.

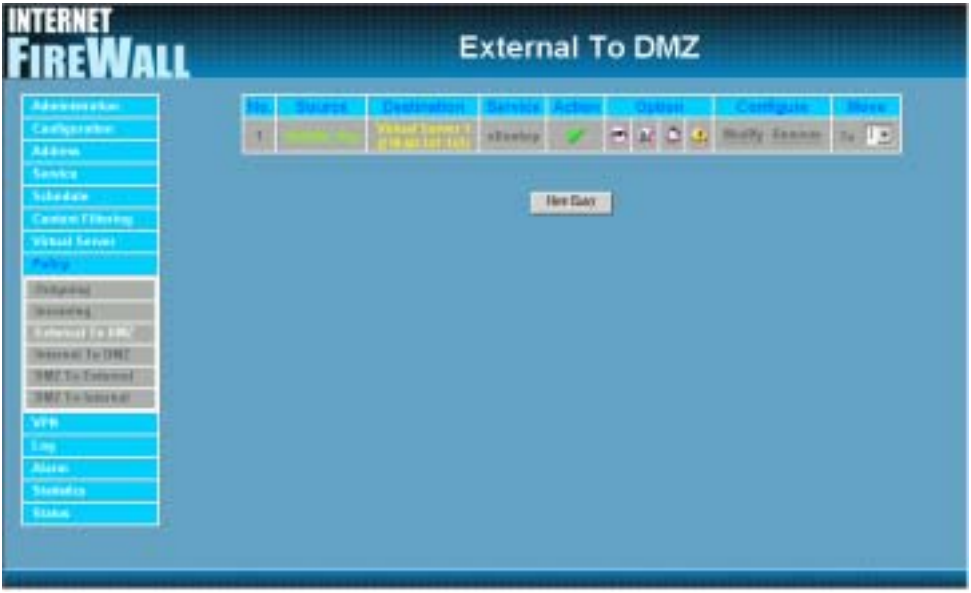


External To DMZ & Internal to DMZ

This section describes steps to create policies for packets and services from the External (WAN) networks to the DMZ networks. Please follow the same procedures for Internal (LAN) networks to DMZ networks.

Enter [External To DMZ] (or [Internal To DMZ]) window:

Click **External To DMZ** under **Policy** menu to enter the **External To DMZ** window. The External To DMZ table will show up displaying currently defined policies.



The fields in External To DMZ window:

- **Source:** source networks, which are addresses specified in the **External** section of the **Address** menu, or all the external network addresses.
- **Destination:** destination networks, which are addresses specified in **DMZ** section of the **Address** menu and **Mapped IP** addresses of the **Virtual Server** menu.
- **Service:** services supported by servers in DMZ network.

- **Action:** control actions, to permit or deny packets from external networks to DMZ travelling through the VPN.
- **Option:** specify the monitoring functions of packets from external network to DMZ network travelling through Firewall.
- **Configure:** modify settings or remove policies.

Adding a new External To DMZ Policy:

Step 1: Click the New Entry button and the Add New Policy window will appear.

Step 2:
Source Address: Select names of the external networks from the drop down list. The drop down list contains the names of all external networks defined in the **External** section of the **Address** menu. To create a new source address, please go to the **Internal** section under the **Address** menu.

Destination Address: Select the name of the DMZ network from the drop down list. The drop down list contains the names of the DMZ network created in the **Address** menu. It will also contain Mapped IP addresses from the **Virtual Server** menu that were created for the DMZ network. To create a new destination address, please go to the **Virtual Server** menu. (Please refer to the sections entitled **Address** and **Virtual Server** for details)

Service: Select a service from drop down list. The drop down list will contain services defined in the **Custom** or **Group** section under the **Service** menu. These are services/application that are allowed to pass from the External network to the DMZ network. Choose ANY for all services. To add or modify these services, please go to the **Service** menu. (Please refer to the section entitled **Services** for details)

Action: Select Permit or Deny from the drop down list to allow or reject the packets travelling from the specified external network to the DMZ network.

Logging: select Enable to enable flow monitoring.

Statistics: select Enable to enable flow statistics.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: set a maximum flow rate (in Kbytes/Sec). An alarm will be send if a flow rate exceeds the specified value.

Step 3: Click **OK**.

Modifying an External to DMZ policy:

Step 1: In the **External To DMZ** window, locate the name of policy desired to be modified and click its corresponding **Modify** option in the **Configure** field.

Step 2: In the **Modify Policy** window, fill in new settings.

Step 3: Click **OK** to do save modifications.

Removing an External To DMZ Policy:

Step 1: In the **External To DMZ** window, locate the name of policy desired to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2: In the **Remove** confirmation pop-up box, click **OK** to remove the policy.

DMZ To External & DMZ To Internal

This section describes steps to create policies for packets and services from DMZ networks to External (WAN) networks. Please follow the same procedures for DMZ networks to Internal (LAN) networks.

Entering the DMZ To External window:

Click **DMZ To External** under **Policy** menu and the **DMZ To External** table appears displaying currently defined **DMZ To External** policies.

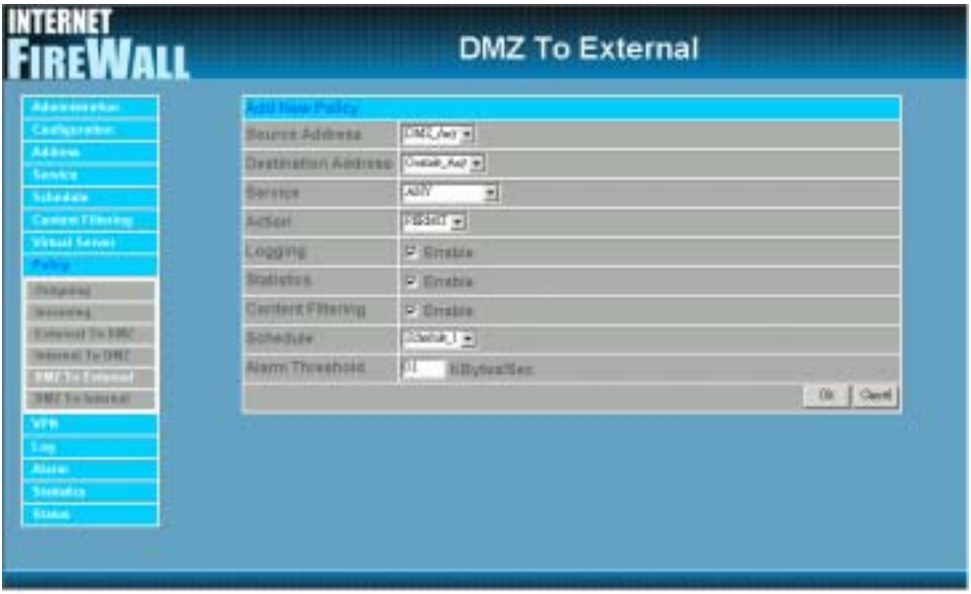
The fields in the DMZ To External window are:

- **Source:** source network addresses which are specified in the **DMZ** section of the **Address** window.
- **Destination:** destination networks, which is the external network address
- **Service:** services supported by Servers of external networks.
- **Action:** control actions, to permit or deny packets from the DMZ network to external networks travelling through the VPN.

- **Option:** specify the monitoring functions on packets from the DMZ network to external networks travelling through the Firewall.
- **Configure:** modify settings or remove policies
- **Move:** this sets the priority of the policies, number 1 being the highest priority.

Adding a DMZ To External Policy:

Step 1: Click the New Entry button and the Add New Policy window will appear.



Step 2:

Source Address: Select the name of the DMZ network from the drop down list. The drop down list will contain names of DMZ networks defined in **DMZ** section of the **Address** menu. To add a new source address, please go to the **DMZ** section under the **Address** menu.

Destination Address: Select the name of the external network from the drop down list. The drop down list lists names of addresses defined in **External** section of the **Address** menu. To add a new destination address, please go to **External** section of the **Address** menu.

Service: Select a service from drop down list. The drop down list will contain services defined in the **Custom** or **Group** section under the **Service** menu. These are services/application that are allowed to pass from the DMZl network to the External network. Choose ANY for all services. To add or modify these services, please go to the **Service** menu.

Action: Select Permit or Deny from the drop down list to allow or reject the packets travelling from the specified DMZ network to the external network.

Logging: select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

Content Filtering: Select Enable to enable Content Filtering.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: set a maximum flow rate (in Kbytes/Sec). An alarm will be sent if flow rates are higher than the specified value.

Step 3: Click **OK** to add new policy or click **Cancel** to cancel adding.

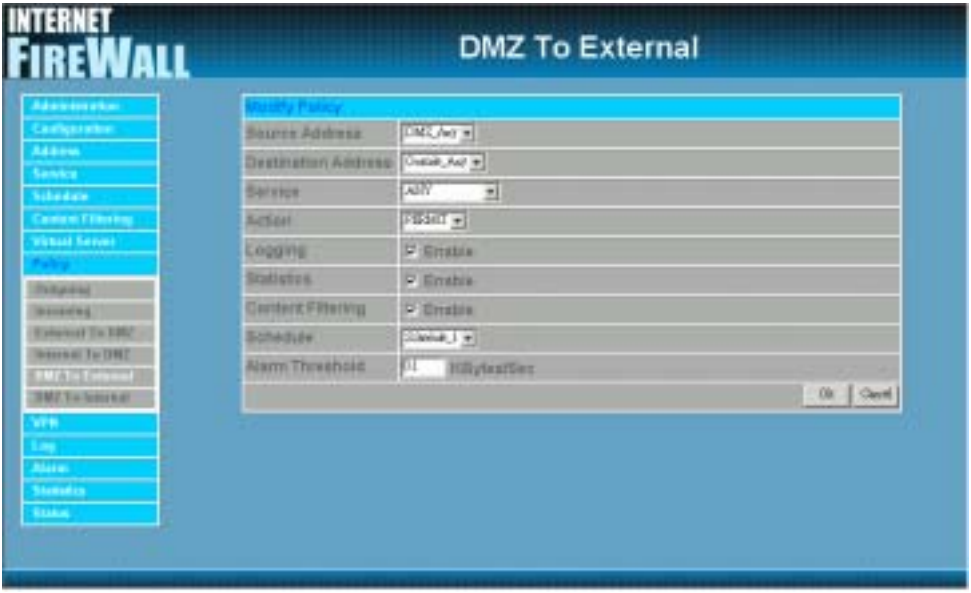
Modifying a DMZ To External policy:

Step 1: In the DMZ to External window, locate the name of policy desired to be modified and click its corresponding Modify option in the Configure field.

Step 2: In the Modify Policy window, fill in new settings.

Note: To change or add selections in the drop-down list, go to the section where the selections are setup. (Source Address→DMZ of Address; Destination Address→External, Service→Pre-defined Service, Custom or Group under Service.)

Step 3: Click OK to save modifications or click Cancel to cancel modifications.



Removing a DMZ To External Policy:

Step 1. In the **DMZ To External** window, locate the name of policy desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the **Remove confirmation** dialogue box, click **OK.**

VPN

The VPN Firewall's VPN (Virtual Private Network) is set by the System Administrator. The System Administrator can add, modify or remove VPN settings.

What is VPN?

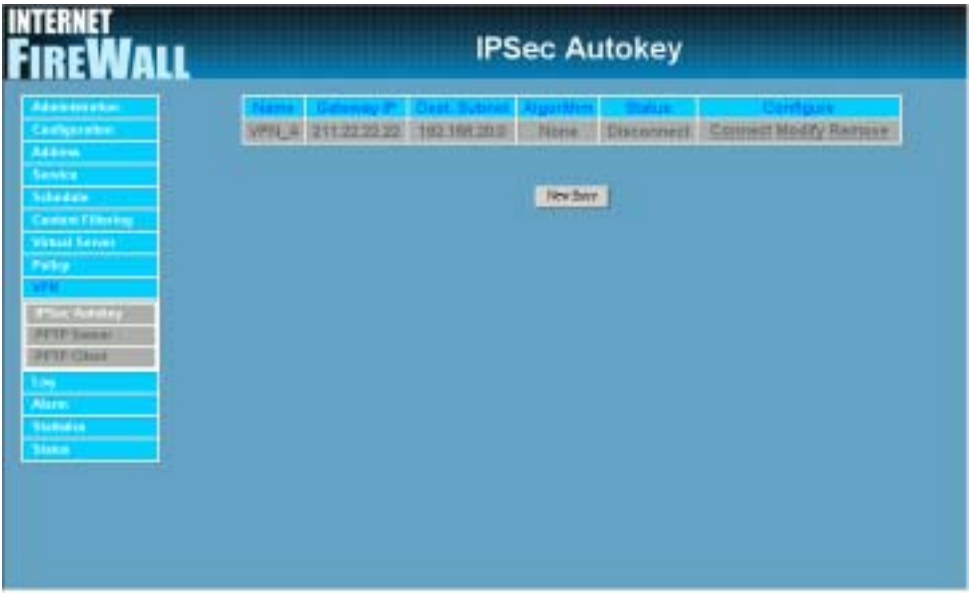
To set up a **Virtual Private Network** (VPN), you *don't need* to configure an Access Policy to enable encryption. Just fill in the following settings: VPN Name, Source Subnet, Destination Gateway, Destination Subnet, Authentication Method, Preshare key, Encapsulation and IPSec lifetime. The VPN Firewalls on both ends must use the same **Preshare** key and **IPSec** lifetime to make a **VPN** connection.

PPTP Server: The administrator could enter the relate setting of VPN-PPTP Server.

PPTP Client: The administrator could enter the relate setting of VPN-PPTP Client.

The fields in the IPSec window are:

- **Name:** The VPN name to identify the VPN tunnel definition. The name must be different for the two sites creating the tunnel.
- **Gateway IP:** The WAN interface IP address of the remote VPN Firewall.
- **Destination Subnet:** Destination network subnet.
- **Algorithm:** The display the Algorithm way.
- **Status:** Connect/Disconnect or Connecting/Disconnecting.
- **Configure:** Connect, Disconnect, Modify and Delete.



There are 4 examples of VPN setting.

Example 1. Create a VPN connection between two VPN Firewall.

Example 2. Create a VPN connection between the VPN Firewall and Windows 2000 VPN Client.

Example 3. Create a VPN connection between two VPN Firewall using Aggressive mode Algorithm (3 DES and MD5), and data encryption for IPSec Algorithm (3DES and MD5)

Example 4. Create a VPN connection between two VPN Firewall using ISAKMP Algorithm (3DES and MD5), data encryption for IPSec Algorithm (3DES and MD5) and GRE.

The definition of VPN:

IPSec Algorithm: The administrator could fill in the following further settings to setup VPN; IPSec Lifetime and Perfect Forward Secrecy to enable the VPN Firewall select or update randomly the unrecognized AutoKey.

- **Preshare Key:** The IKE VPN must be defined with a Preshared Key. The Key may be up to 128 bytes long.

ISAKMP Algorithm

- **Encryption Algorithm:** The device selects 56 bit DES-CBC or 168-bit Triple DES-CBC encryption algorithm. The default algorithm 56 bit DES-CBC.
- **ESP-Authentication Method:** The device -selects MD5 or SHA-1 authentication algorithm. The default algorithm is MD5.

IPSec Algorithm: The device Select Data Encryption + Authentication or Authentication Only.

Data Encryption + Authentication

Encryption Algorithm: The device selects 56 bit DES-CBC or 168-bit Triple DES-CBC or AES or NULL encryption algorithm. The default algorithm is 56 bit DES-CBC.

- **ESP-Authentication Method:** The device -selects MD5 or SHA-1 authentication algorithm. The default algorithm is MD5.
- **IPSec Lifetime:** New keys will be generated whenever the lifetime of the old keys is exceeded. The Administrator may enable this feature if needed and enter the lifetime in seconds to re-key. The default is 28800 seconds (eight hours). Selection of small values could lead to frequent re-keying, which could affect performance.

Keep alive IP : Check to allow Remote Client computer IP Address connected to keep alive.

Aggressive mode: The device Select Aggressive mode Algorithm.

GRE/IPSec: The device Select GRE/IPSec (Generic Routing Encapsulation) packet seal technology.

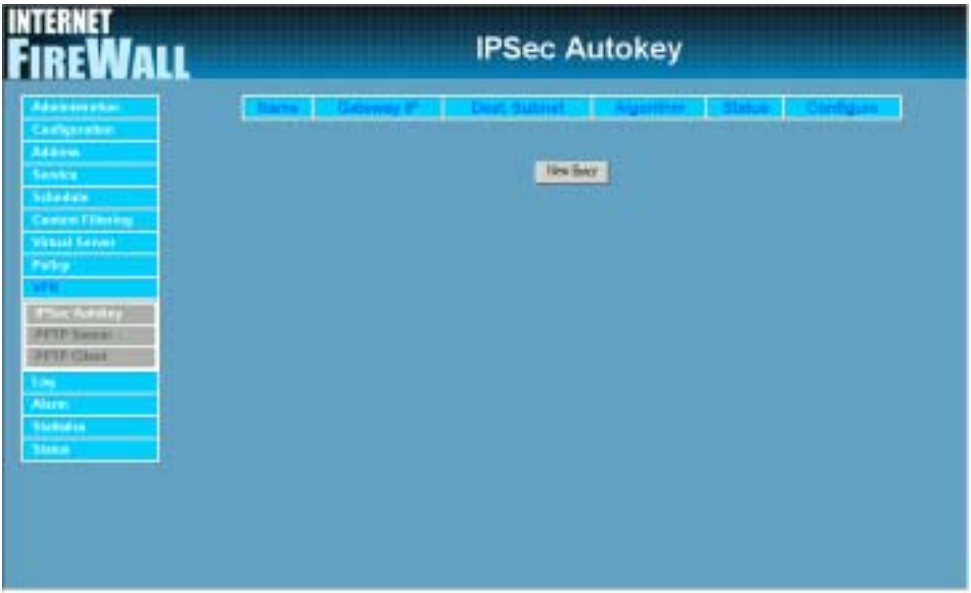

INTERNET
FIREWALL
IPSec Autokey

Example 1. Create a VPN connection between two VPN Firewalls.

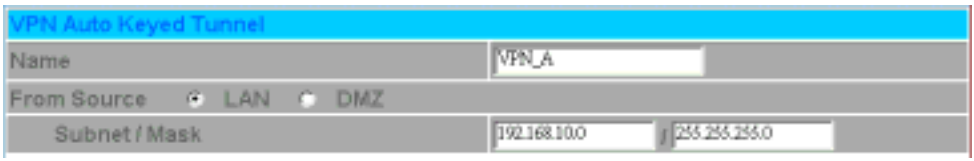
Preparation Task:
Company A External IP is 61.11.11.11
Internal IP is 192.168.10.X
Company B External IP is 211.22.22.22
Internal IP is 192.168.20.X
To suppose Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's VPN Firewall, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

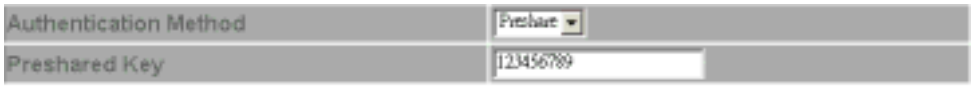


Step 2. Enter the VPN name, VPN_A in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.10.0 and subnet mask, 255.255.255.0.

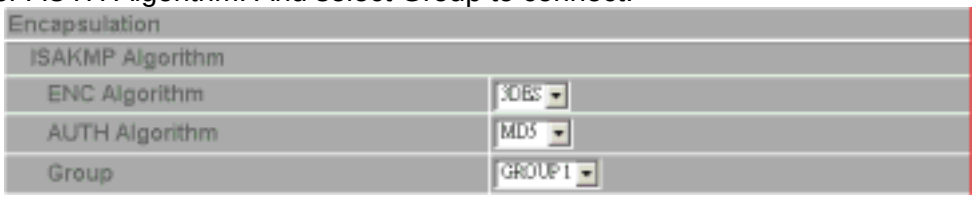


Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company B's subnet IP and mask.

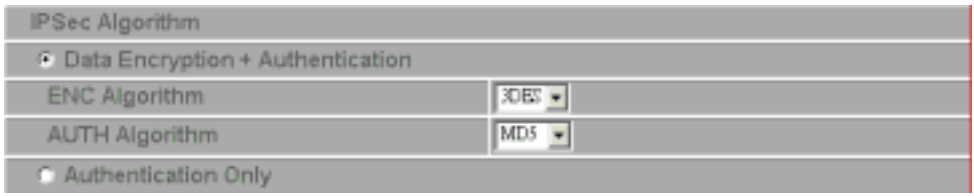
Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)



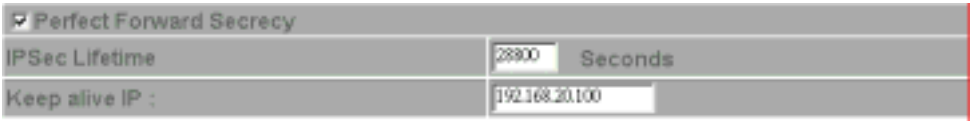
Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group to connect.



Step 6. In IPSec Algorithm Table , choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



Step 7. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

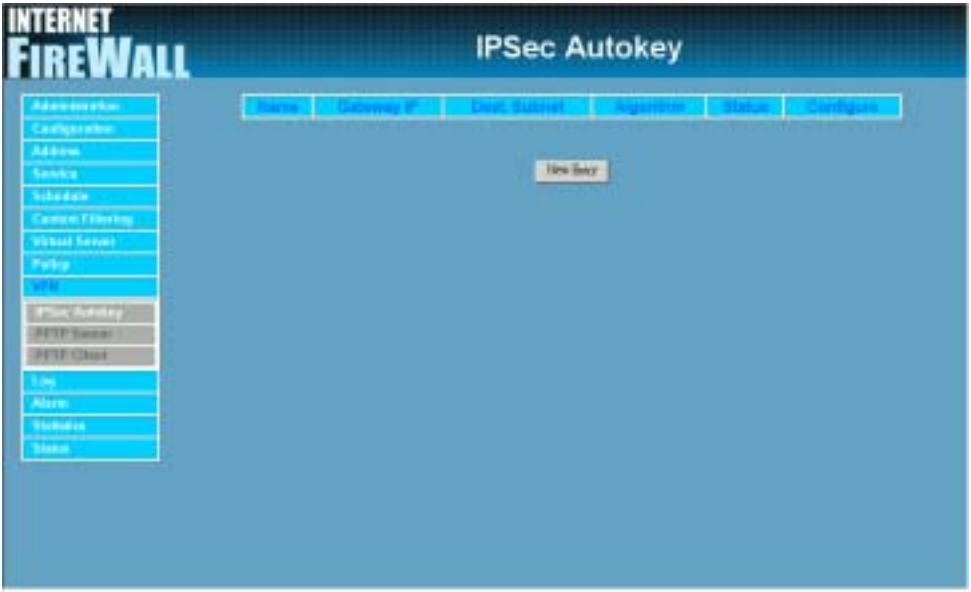


Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Step 9. Click OK to finish the setting of Company A.

The Gateway of Company B is 192.168.20.1. The settings of company B are as the following.

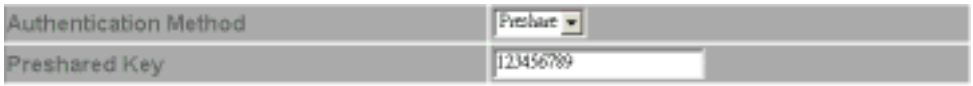
Step 1. Enter the default IP of Company B's VPN Firewall, 192.168.20.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.



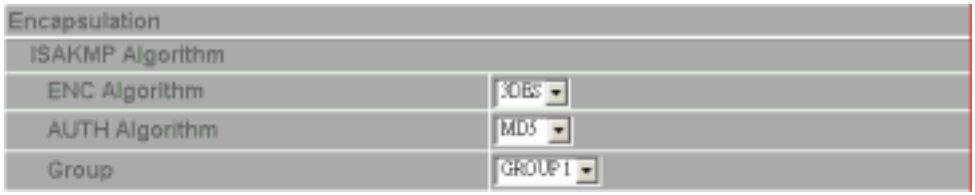
Step 2. Enter the VPN name, VPN_B in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.20.0 and subnet mask, 255.255.255.0.

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.

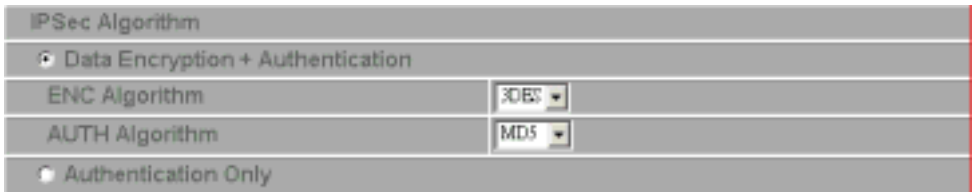
Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)



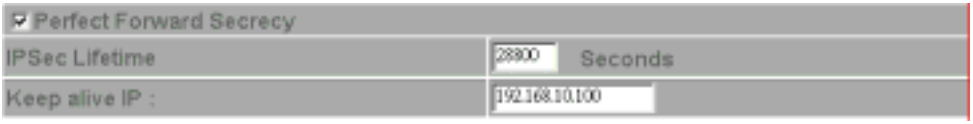
Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group to connect.



Step 6. In IPSec Algorithm Table , choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



Step 7. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.



Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule . Refer to the corresponding section for details.

Step 9. Click OK to finish the setting of Company B.

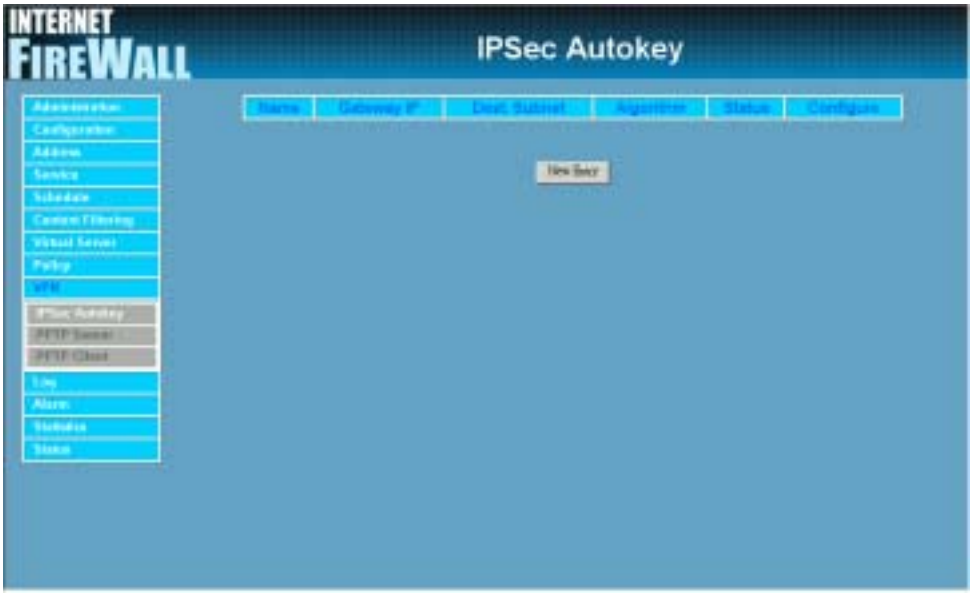
Example 2. Create a VPN connection between the VPN Firewall and Windows 2000 VPN Client.

Preparation Task:
Company A External IP is 61.11.11.11
Internal IP is 192.168.10.X
Company B External IP is 211.22.22.22
Internal IP is 192.168.20.X

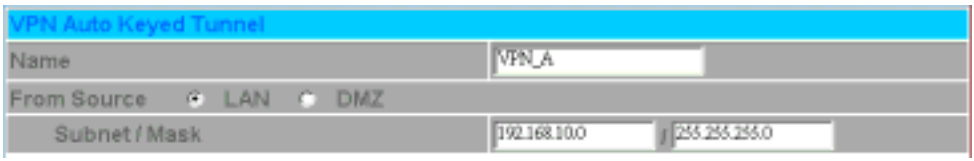
To suppose Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's VPN Firewall, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

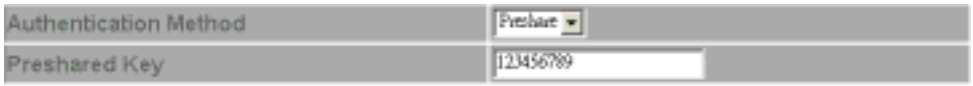


Step 2. Enter the VPN name, VPN_A in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.10.0 and subnet mask, 255.255.255.0.

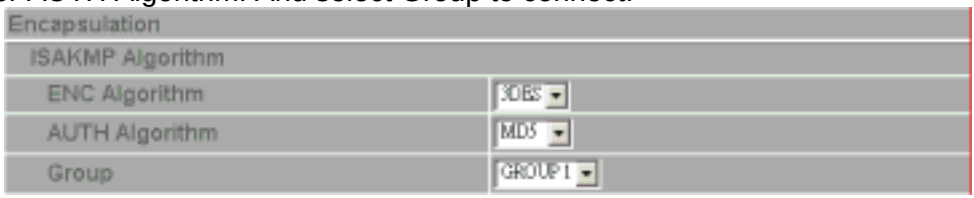


Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company B's subnet IP and mask.

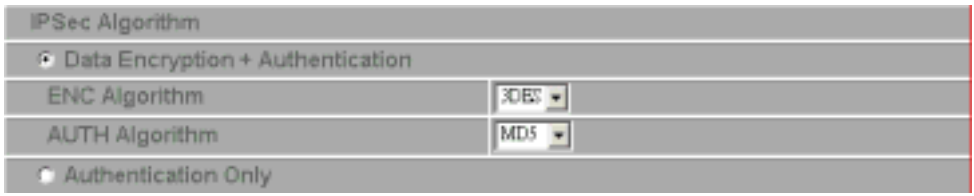
Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)



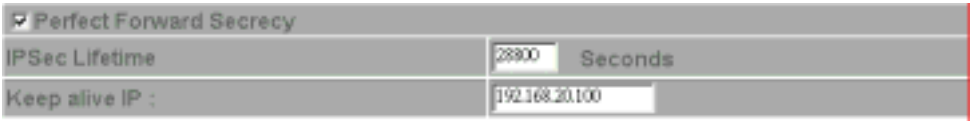
Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group to connect.



Step 6. In IPSec Algorithm Table , choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



Step 7. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

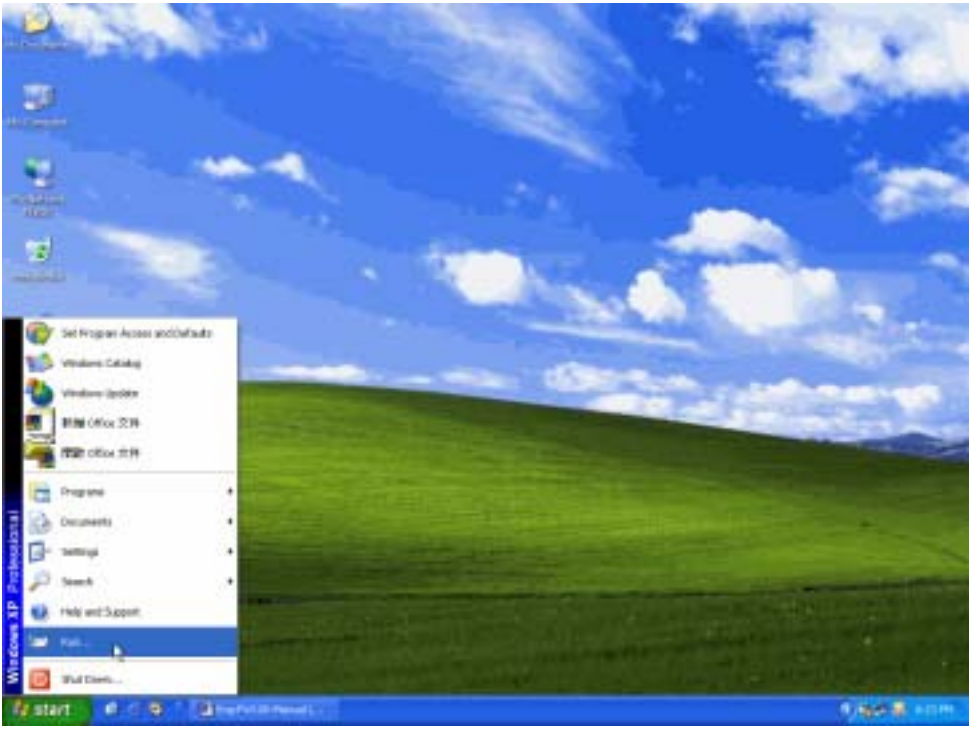


Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Step 9. Click OK to finish the setting of Company A.

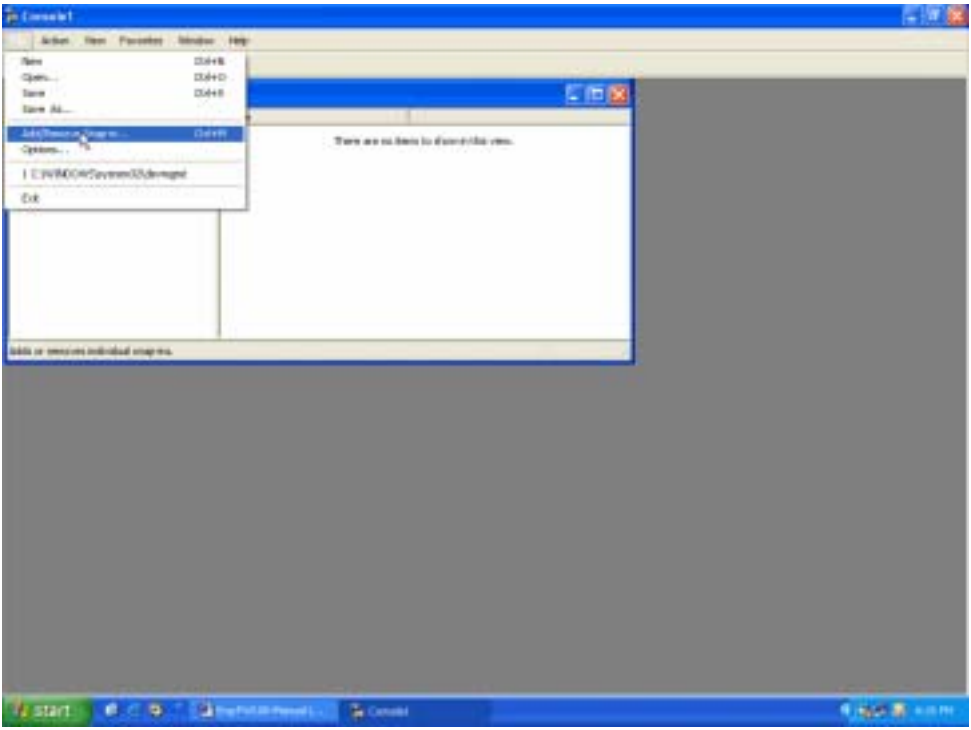
The Gateway of Company B is 192.168.20.100. The settings of company B are as the following.

Step 1. Enter Windows XP, click Start and click Execute function.

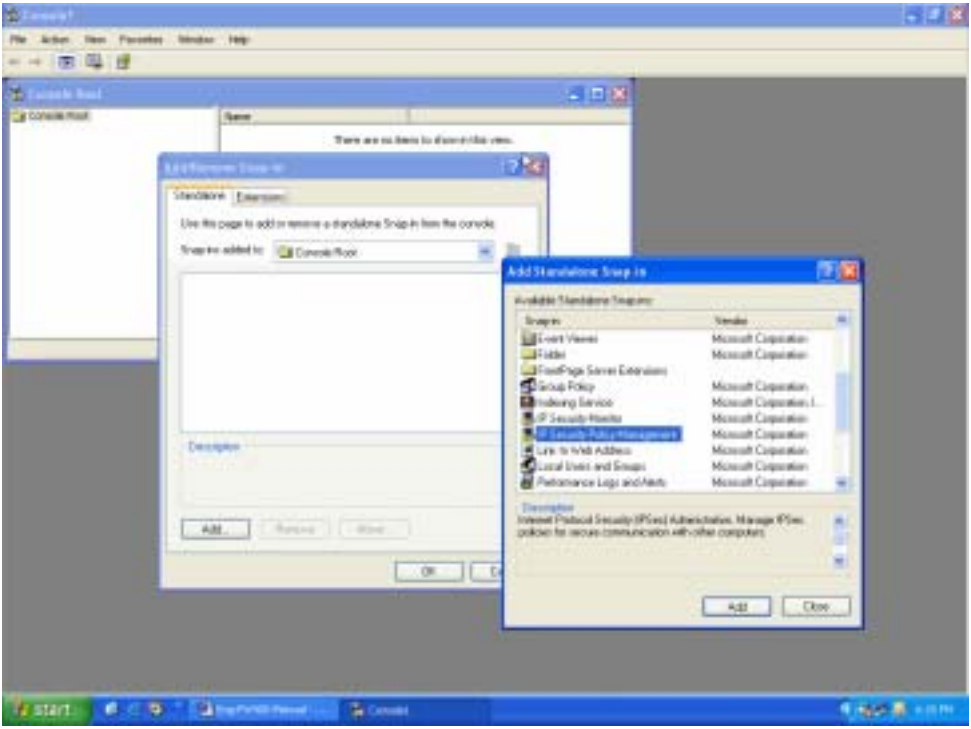


Step 2. In the Execute window, enter the command, MMC in Open.

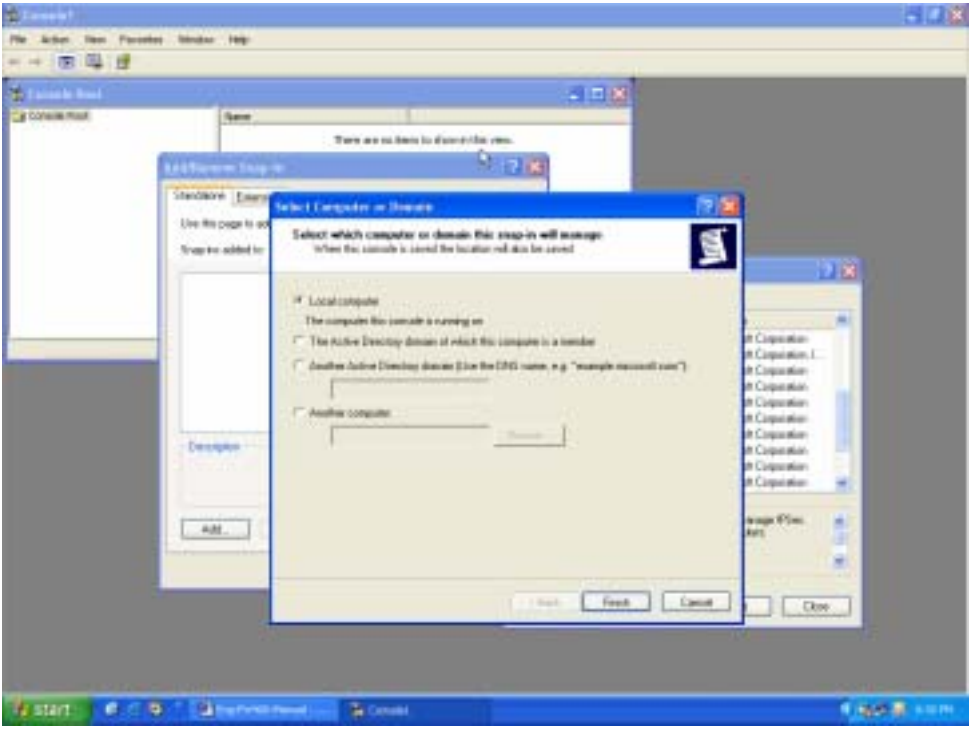
Step 3. Enter the Console window, click Console(C) option and click Add/Remove Embedded Management Option.



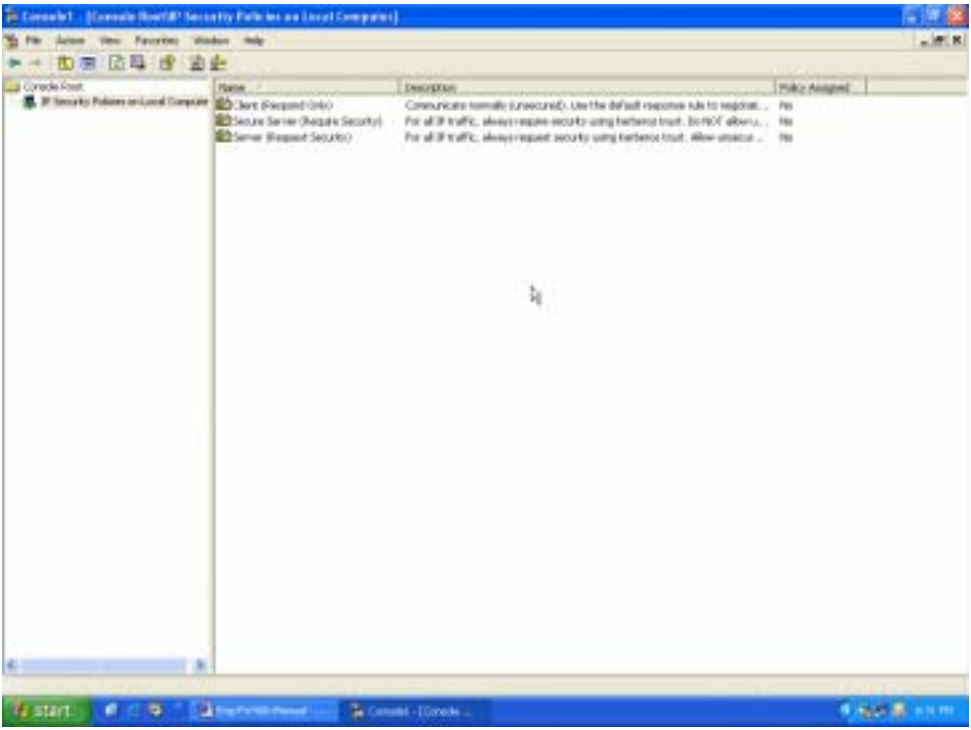
Step 4. Enter Add/Remove Embedded Management Option window and click Add. In Add/ Remove Embedded Management Option window, click Add to add Create IP Security Policy.



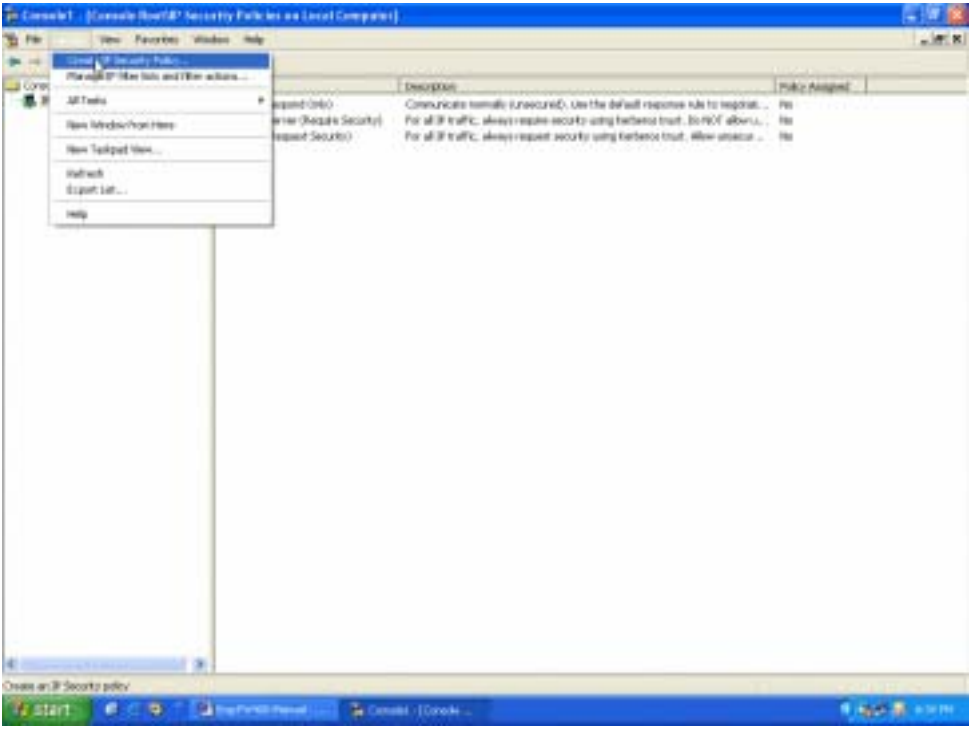
Step 5. Choose Local Machine (L) for finishing the setting of Add.



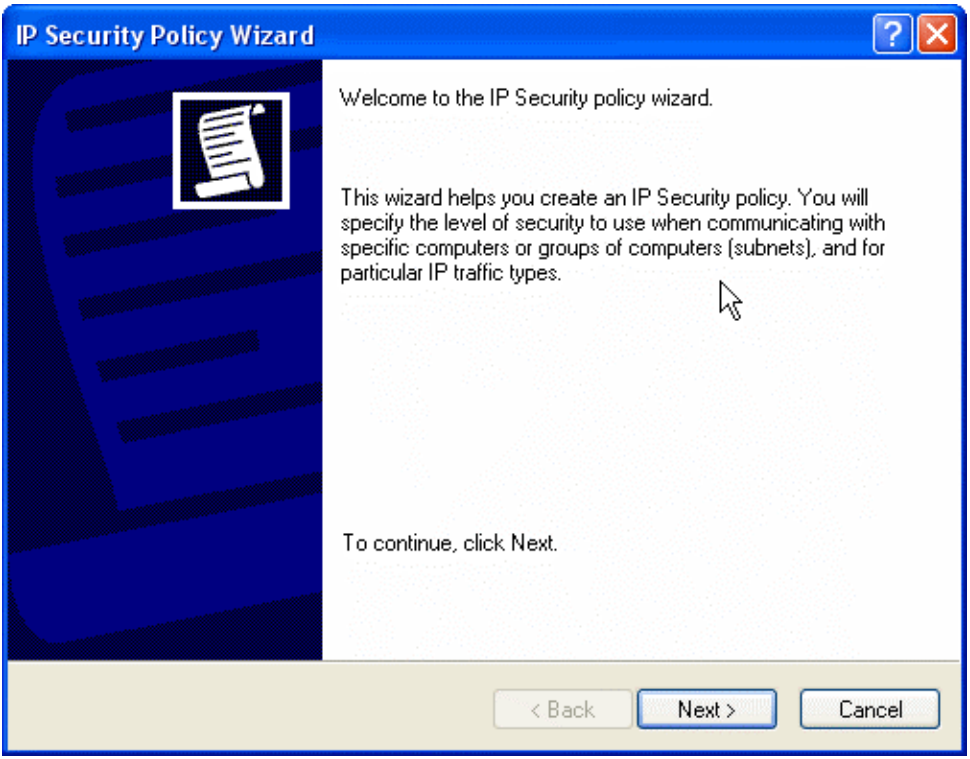
Step 6. Finish the setting of Add.



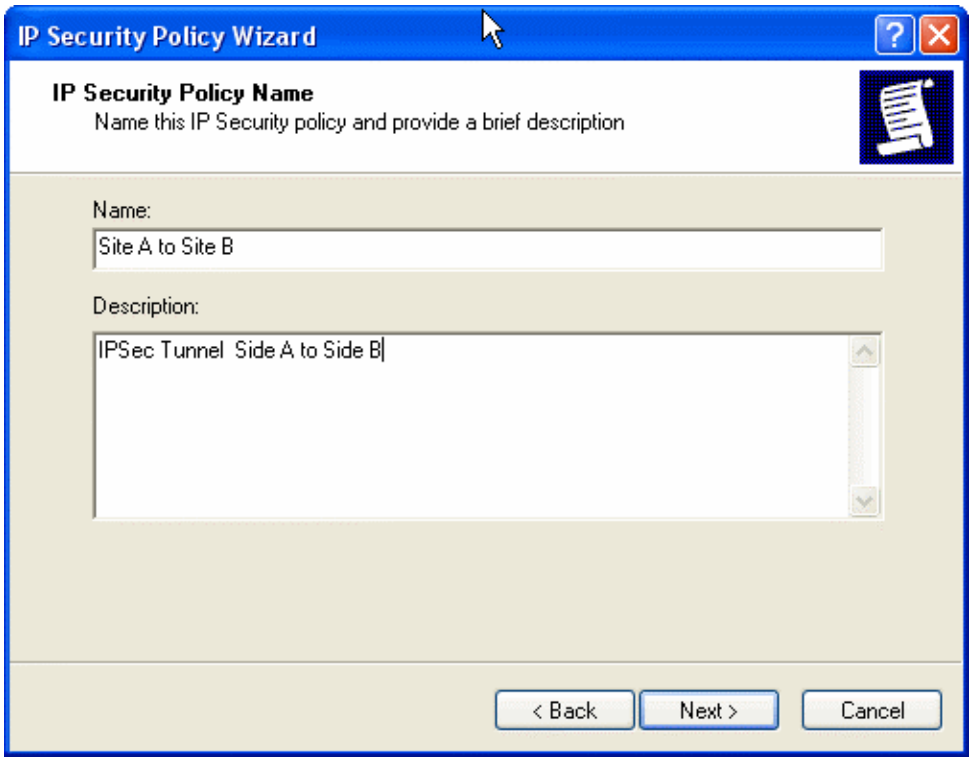
Step 7. Click the right button of mouse in IP Security Policies on Local Machine and choose Create IP Security Policy(C) option.



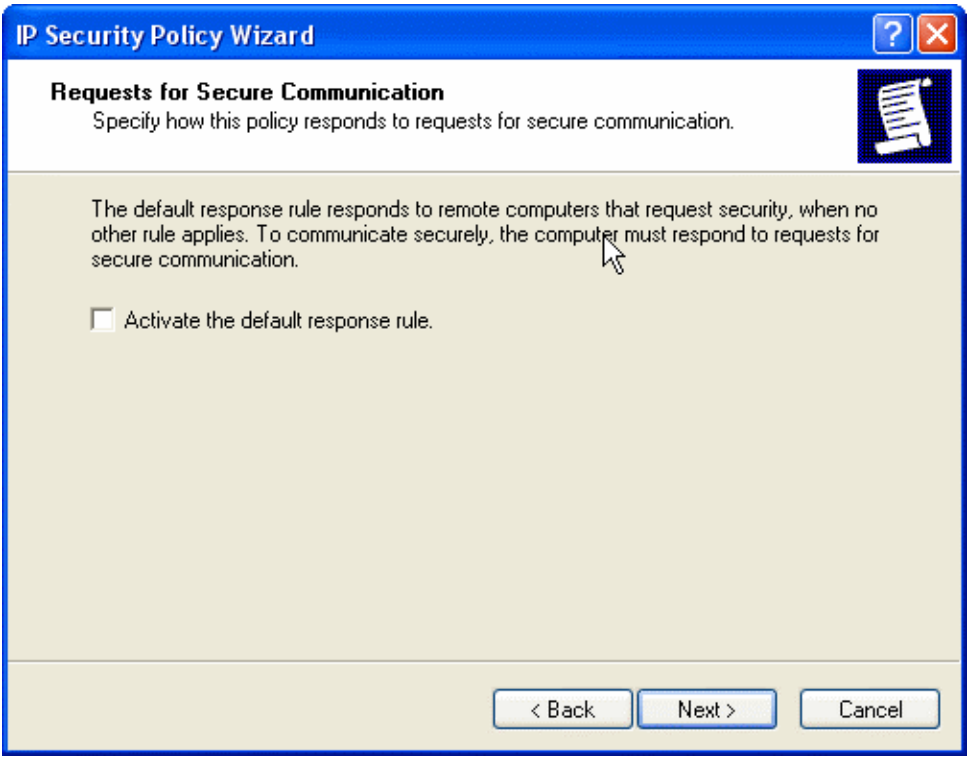
Step 8. Click Next.



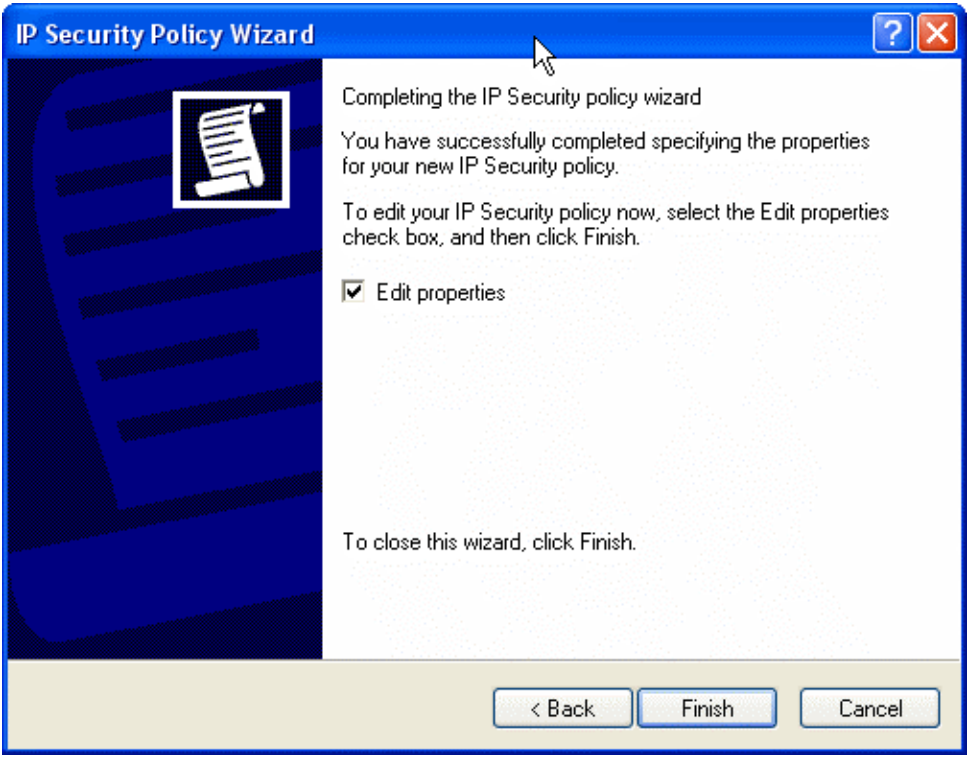
Step 9. Enter the Name of this VPN and optionally give it a brief description.



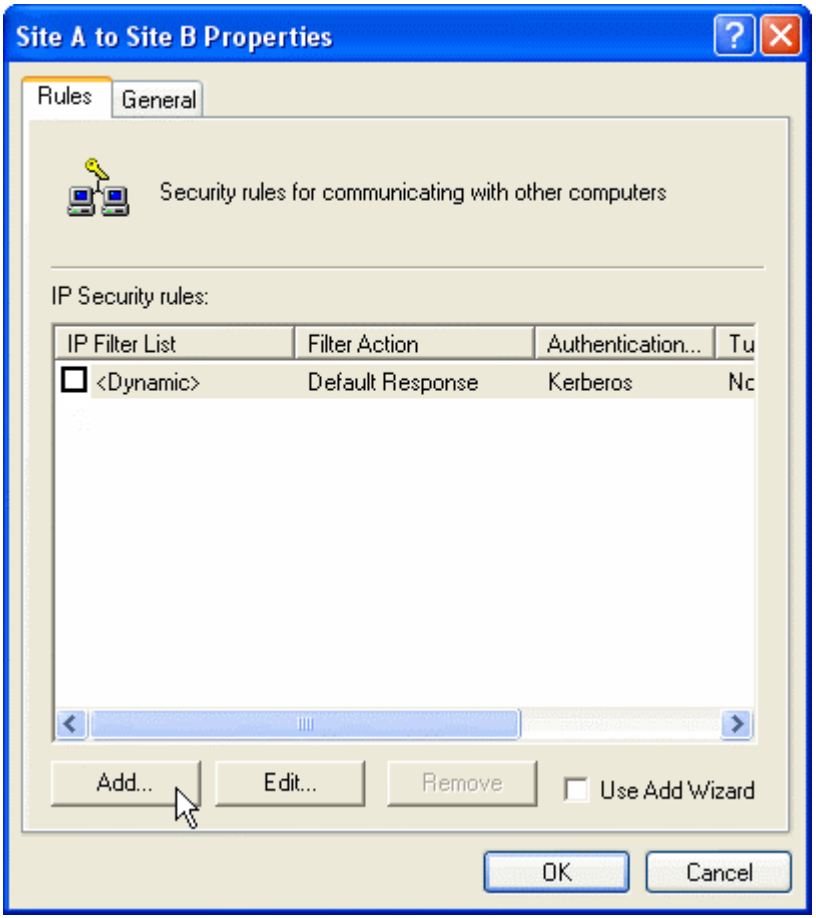
Step 10. Disable Activate the default response rule. And click Next.



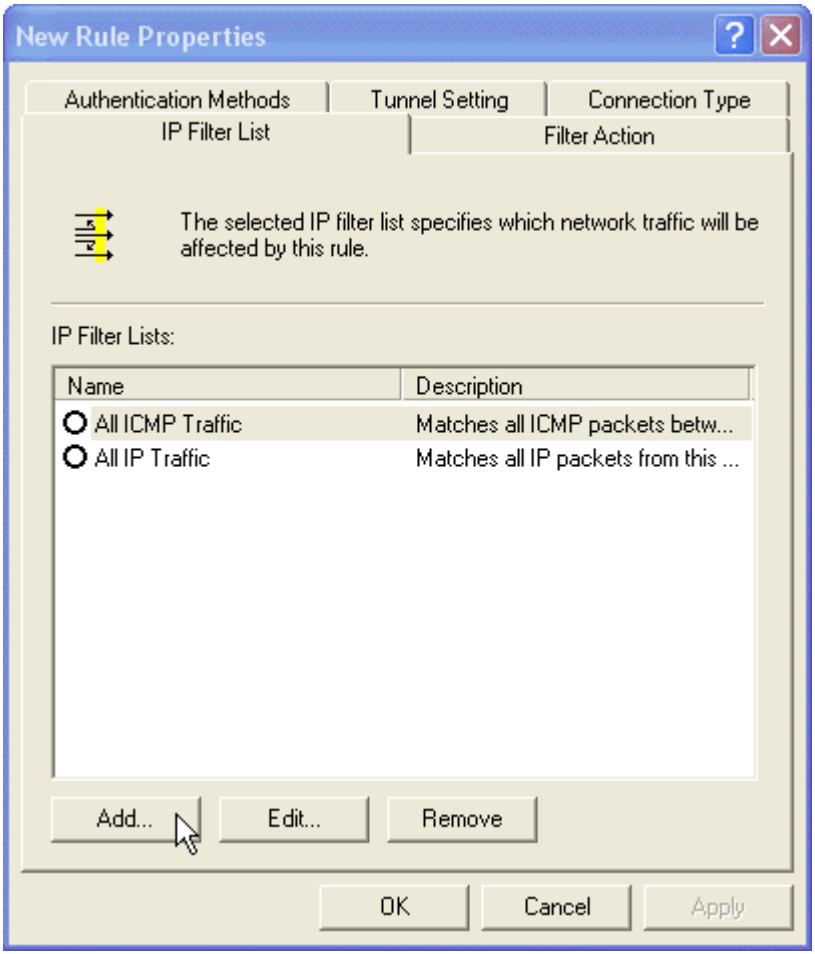
Step 11. Completing the IP Security Policy setting and click Finish. Enable Edit properties.



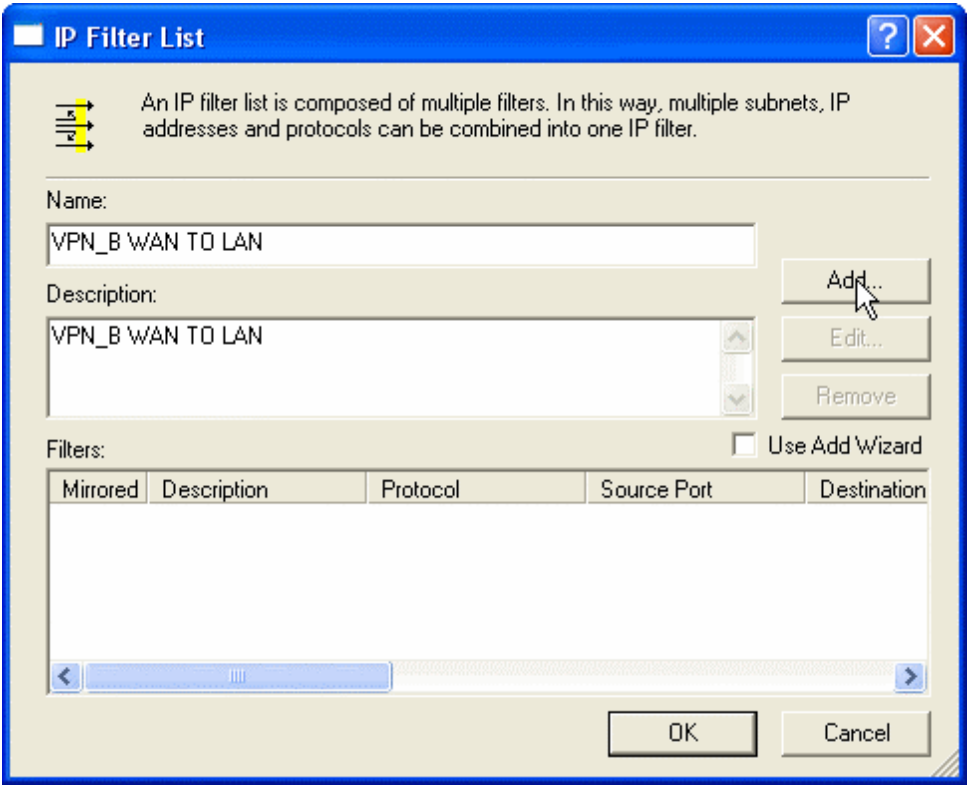
Step 12. In VPN_B window, click Add and please don't click Use Add Wizard.



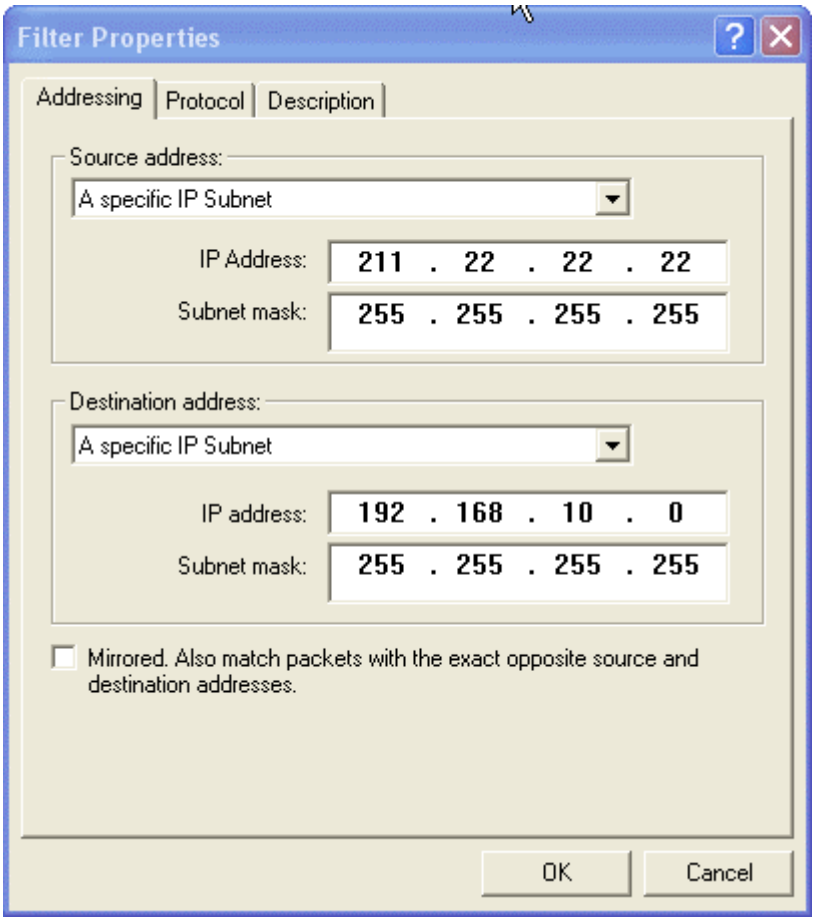
Step 13. In IP Filter List tab, click Add.



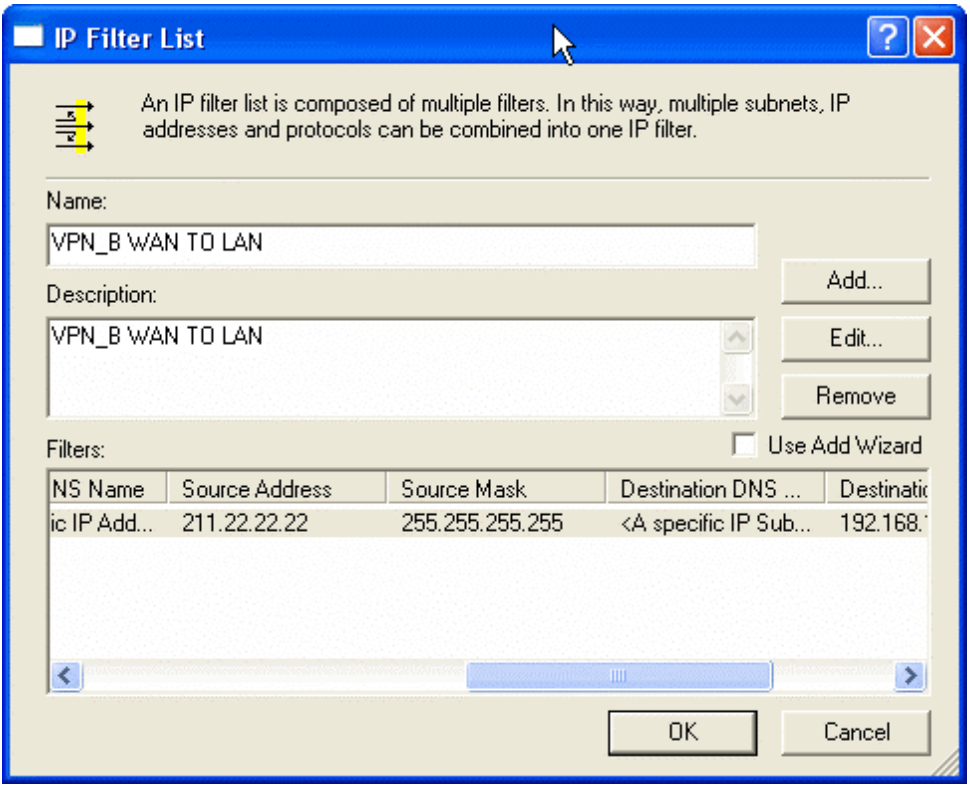
Step 14. In IP Filter List window, please don't choose Use Add Wizard and change Name to VPN_B WAN TO LAN. Click Add.



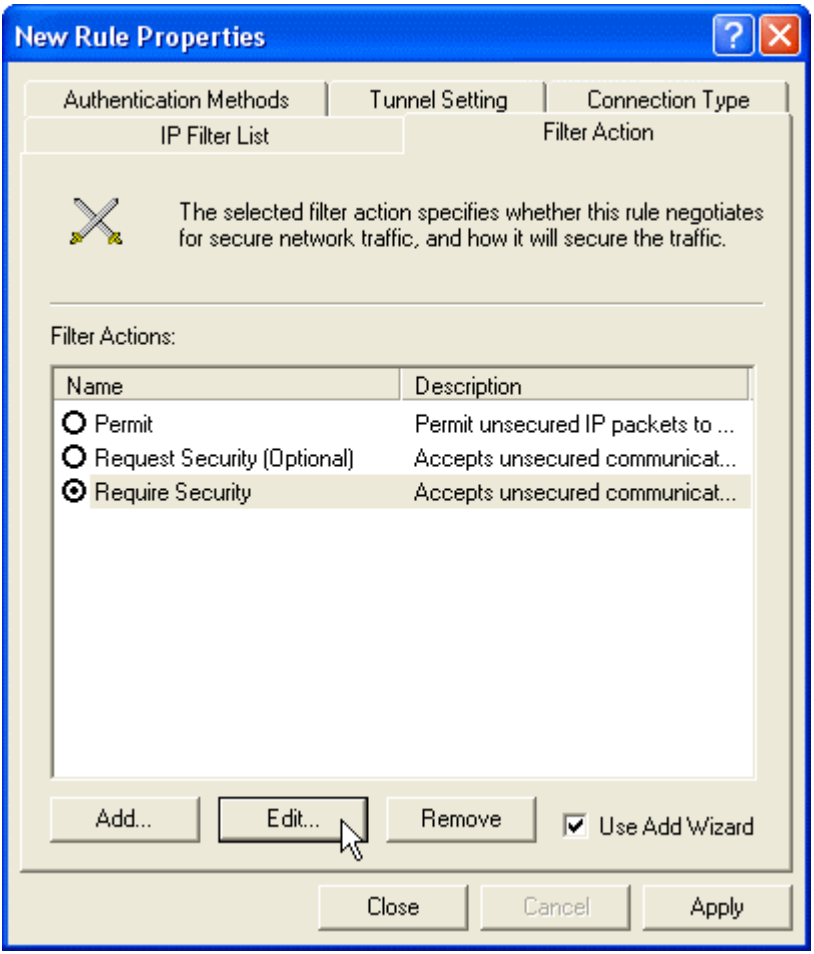
Step 15. In Filter Properties window, in Source address, click down the arrow to select the specific IP Subnet and fill Company B's IP Address, 211.22.22.22 and Subnet mask, 255.255.255.255. In Destination address, click down the arrow to select the specific IP Subnet and fill Company A's IP Address, 192.168.10.0 and Subnet mask 255.255.255.0. Please disable Mirrored. Also match packets with the exact opposite source and destination addresses.



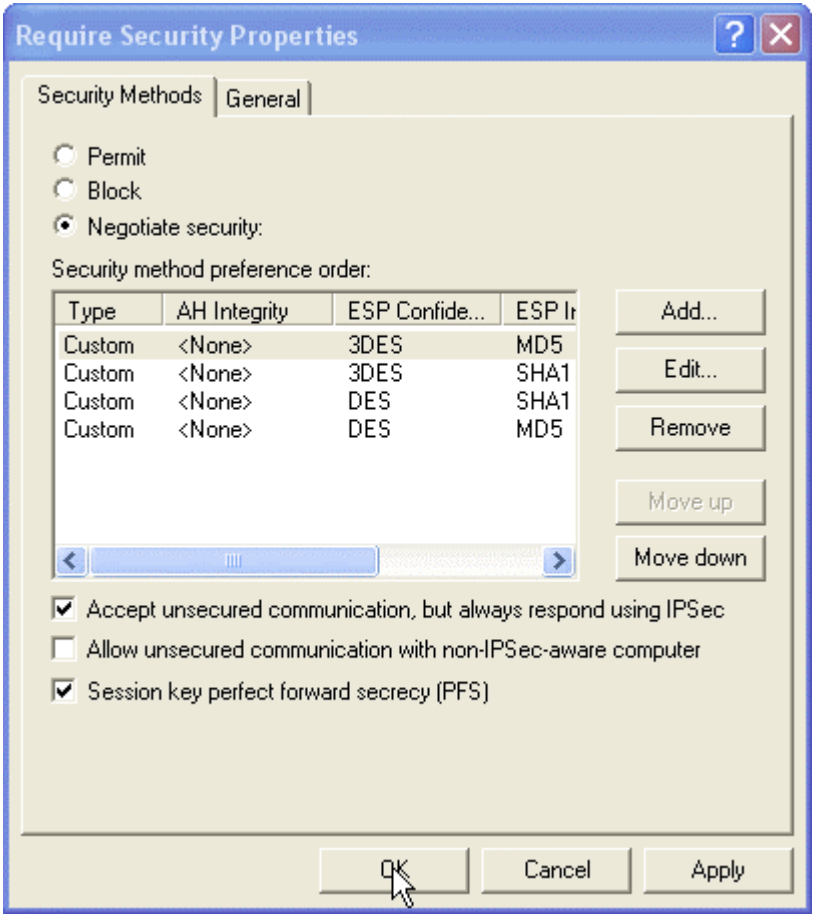
Step 16. Finish the setting and close IP Filter List window.



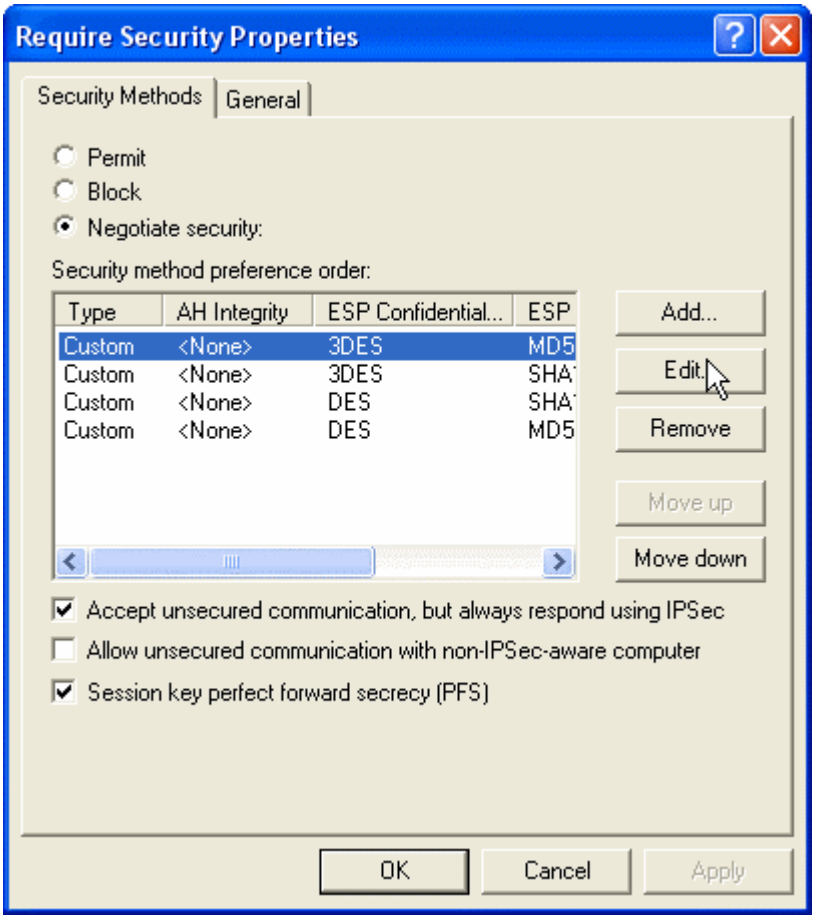
Step 17. Click Filter Action tab and choose Require Security. Click Edit.



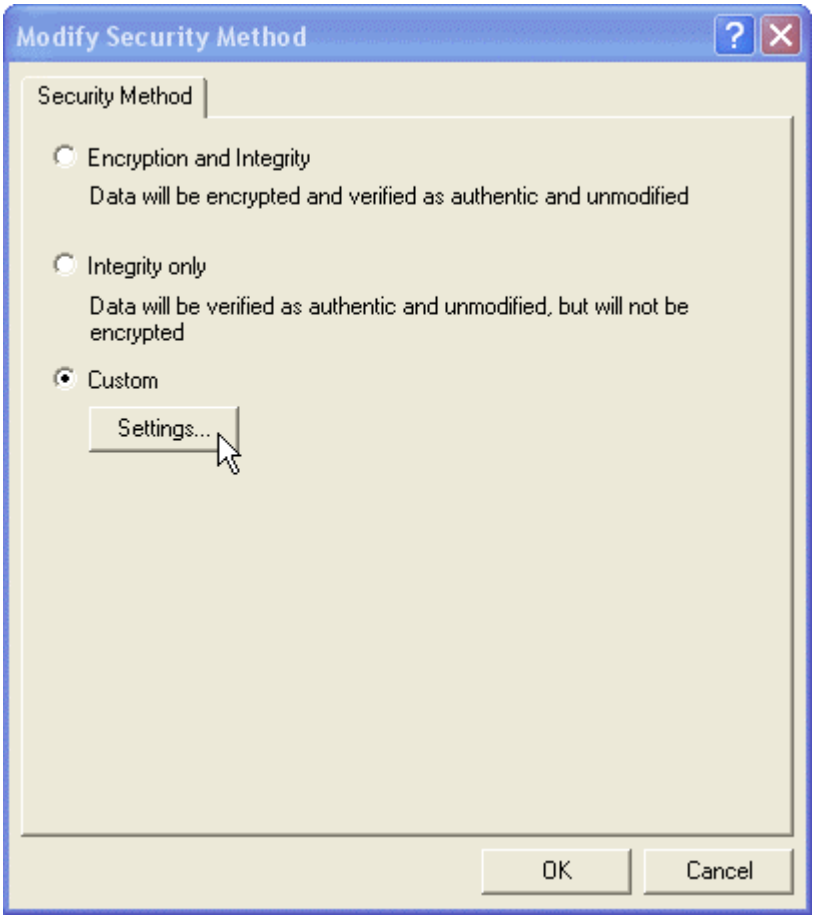
Step 18. In Security Methods tab, choose accept unsecured communication, but always respond using IPSec.



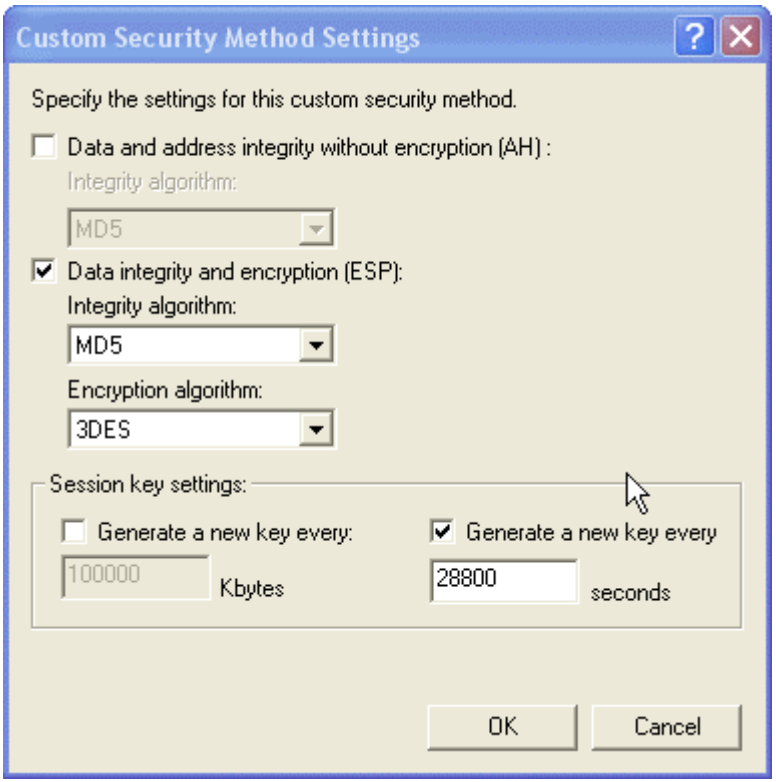
Step 19. Click Edit in Custom/ None/ 3DES/ MD5.



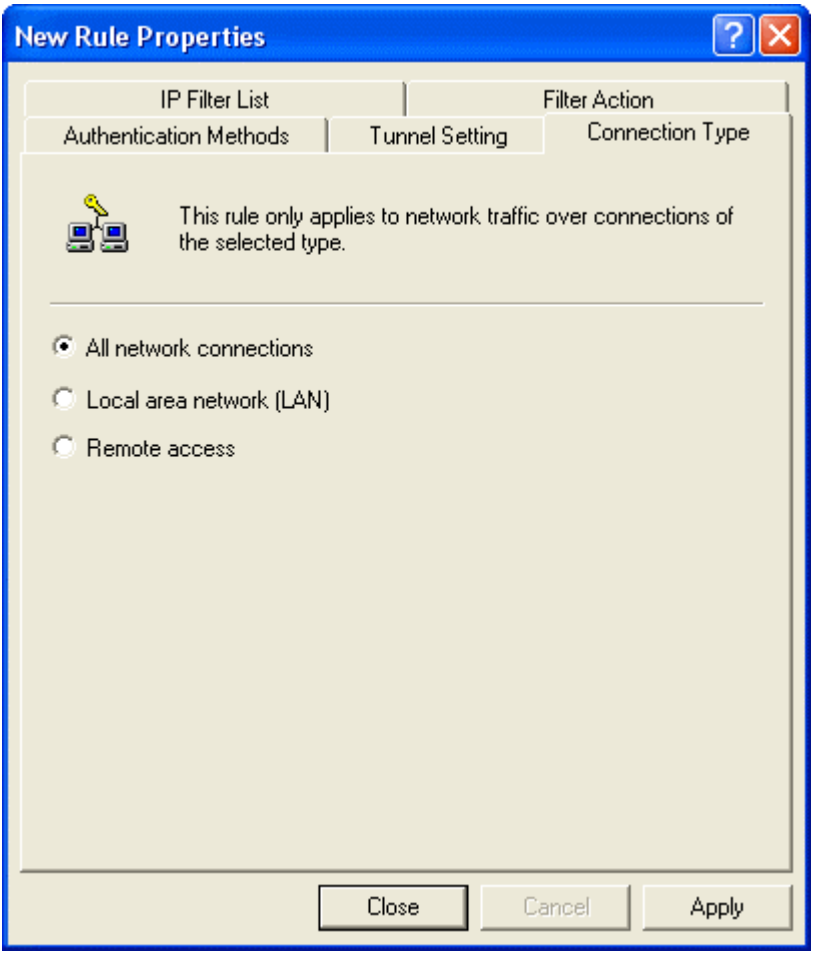
Step 20. Click Custom(For professional user) and click Edit.



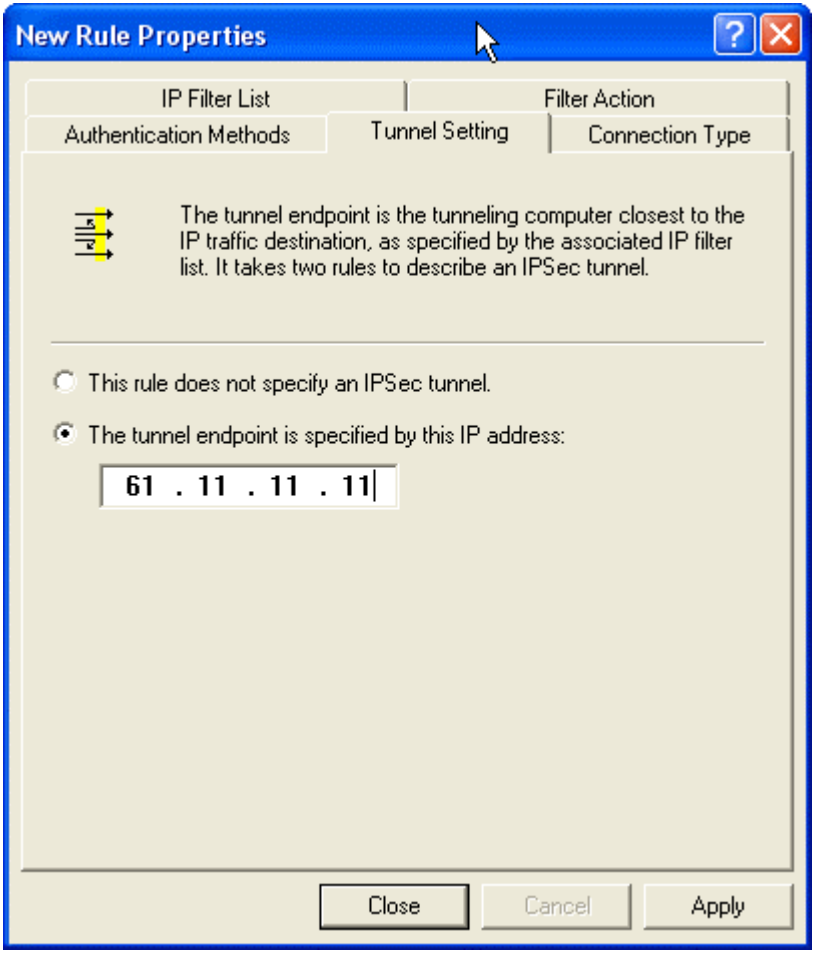
Step 21. Click Data Integrity and Encapsulation and choose MD5 and 3DES. Click Generate a New key after every 28800 seconds. And click 3 times OK to return.



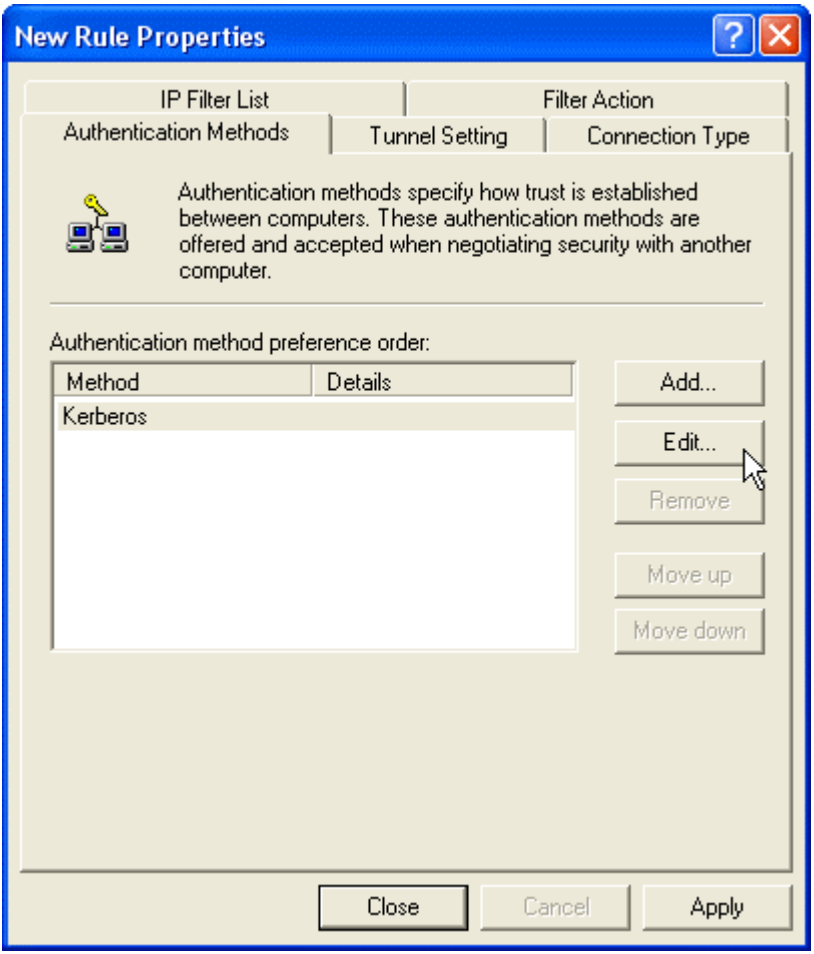
Step 22. Click Connection Type tab and click all network connections.



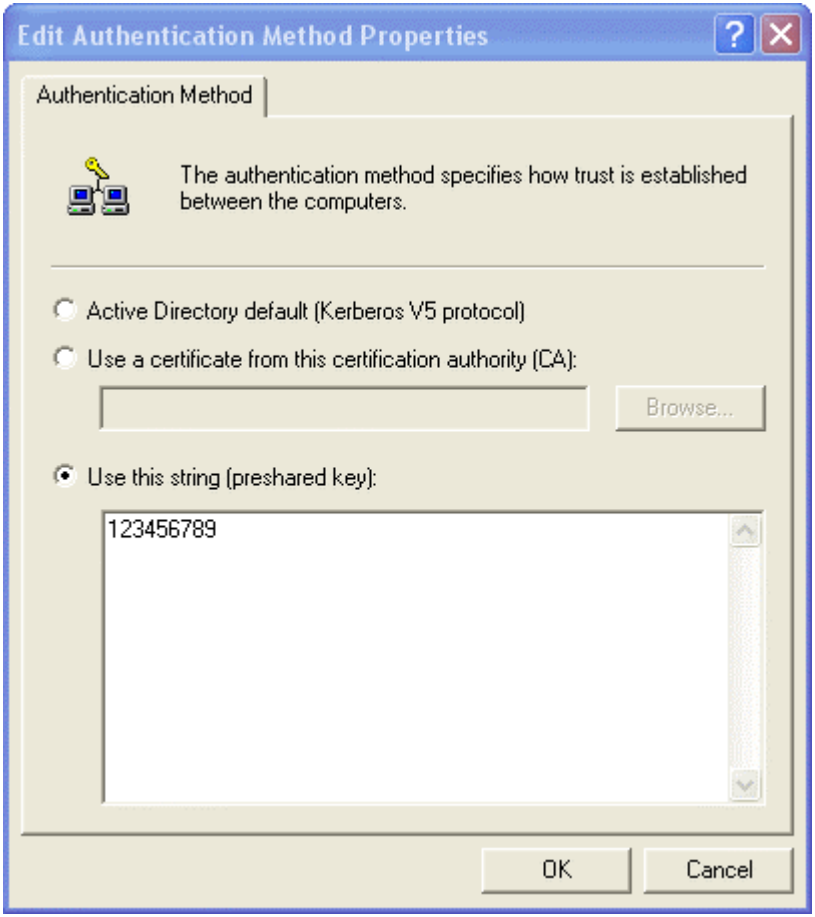
Step 23. Click Tunnel Setting tab, and click The tunnel endpoint is specified by the IP Address. Enter the WAN IP of Company A, 61.11.11.11.



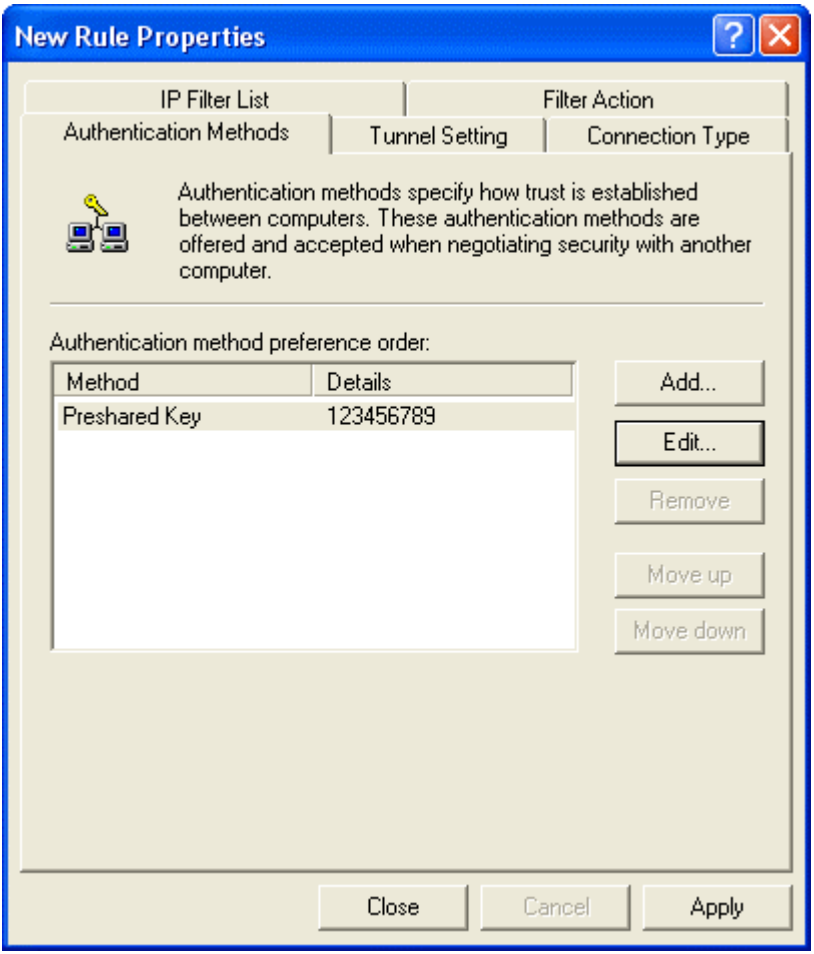
Step 24. Click Authentication Methods and click Edit.



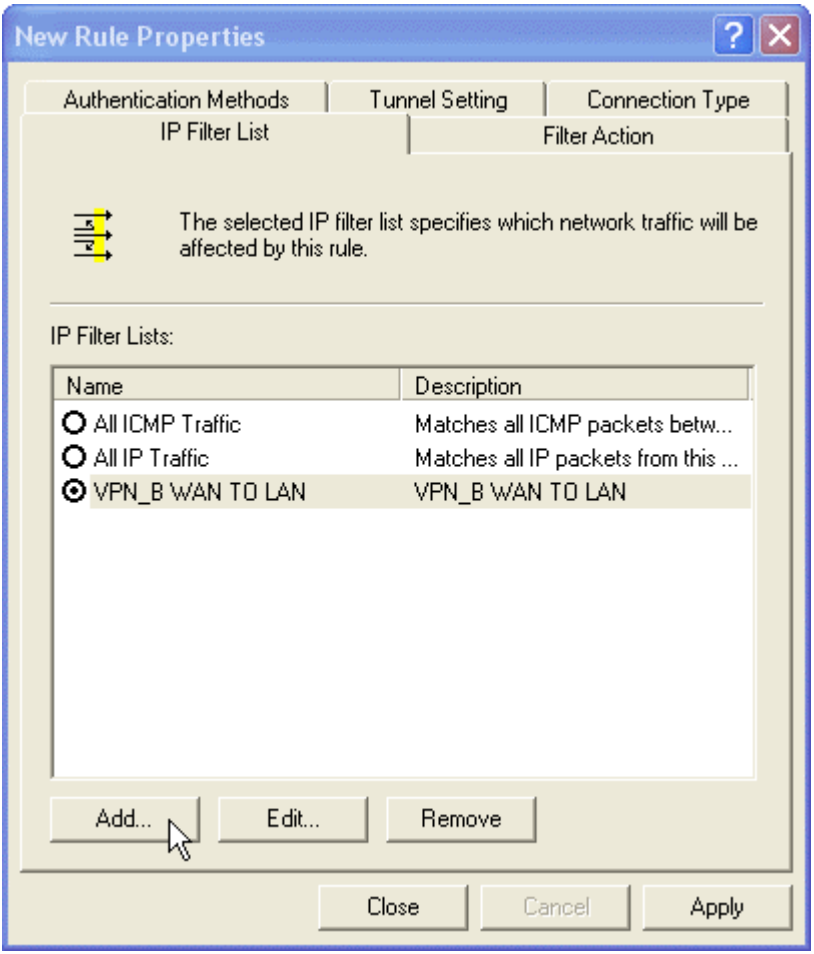
Step 25. Choose Use this string to protect the key exchange (Preshared Key). And enter the key, 123456789.



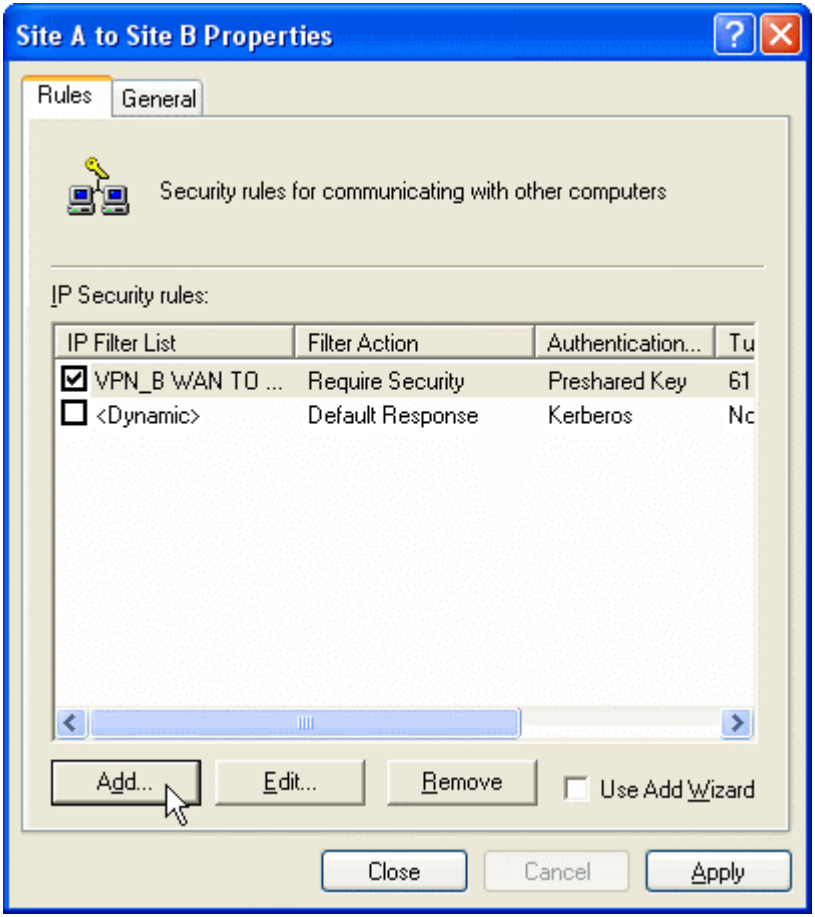
Step 26. Finish the setting, and close the window.



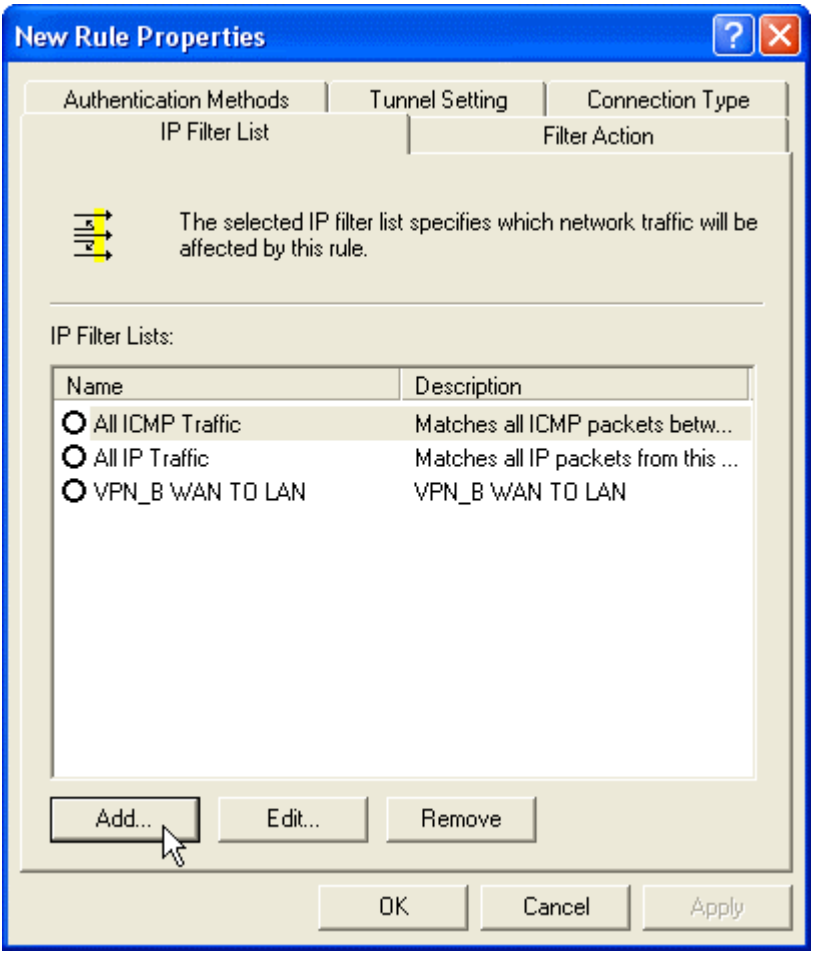
Step 27. Finish the Policy setting of VPN_B WAN TO LAN.



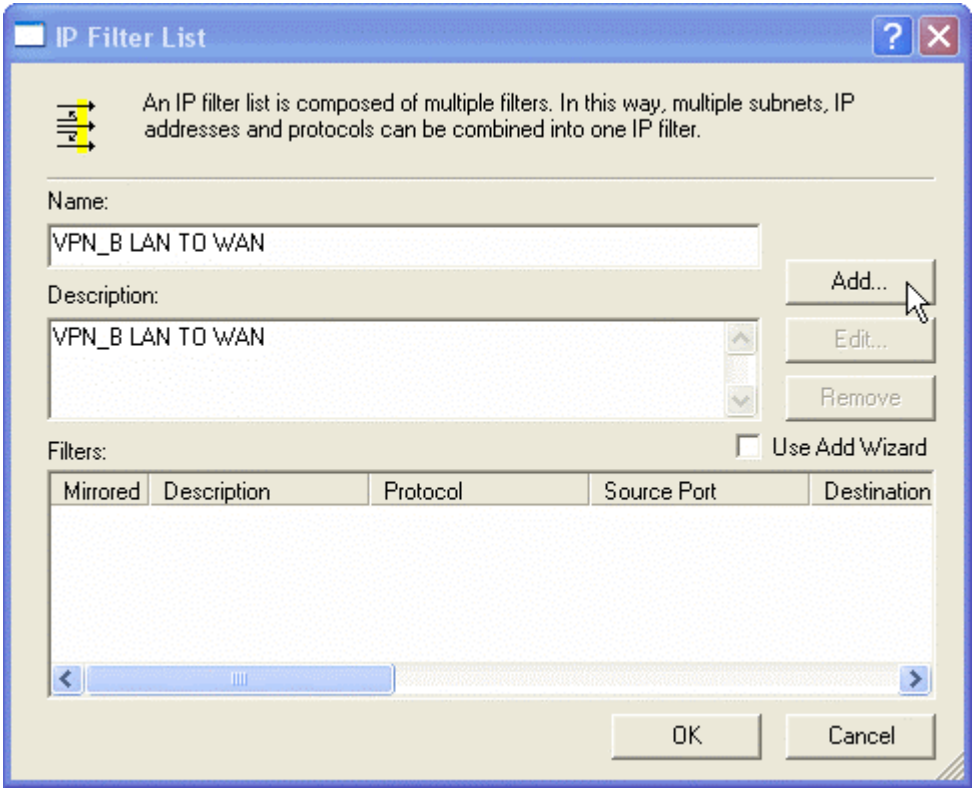
Step 28. Enter VPN_B window again and click Add to add second IP Security Policy. Please don't enable Use Add Wizard.



Step 29. In New Rule Properties, click Add.

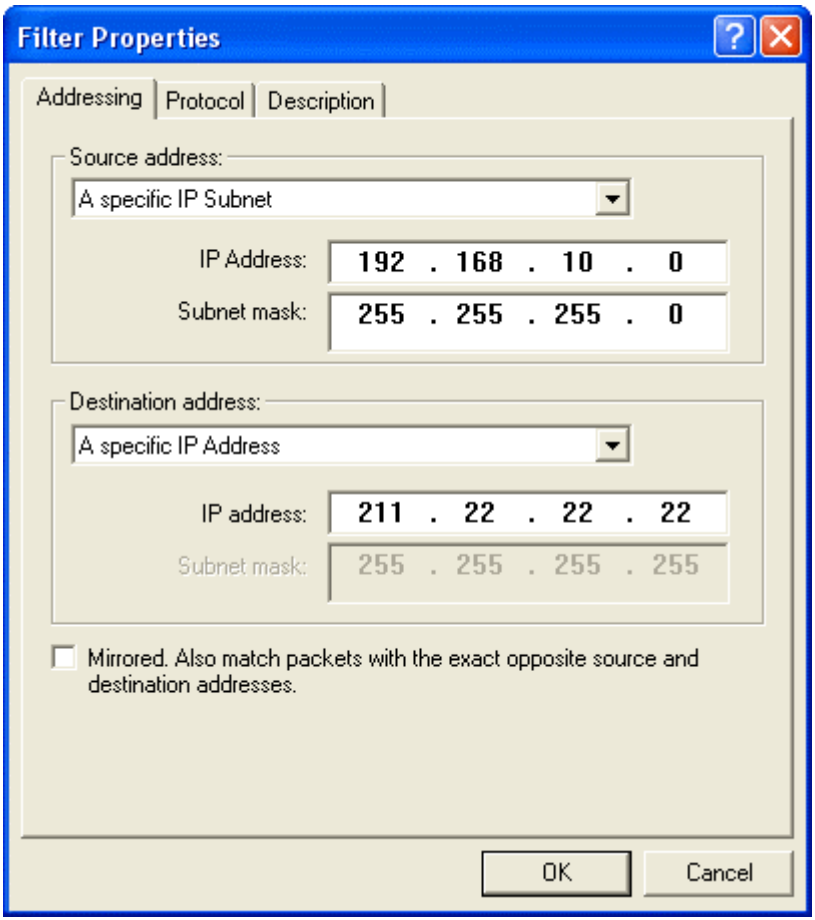


Step 30. In IP Filter List window, please disable Use Add Wizard, and change Name to VPN_B LAN TO WAN. Click Add.

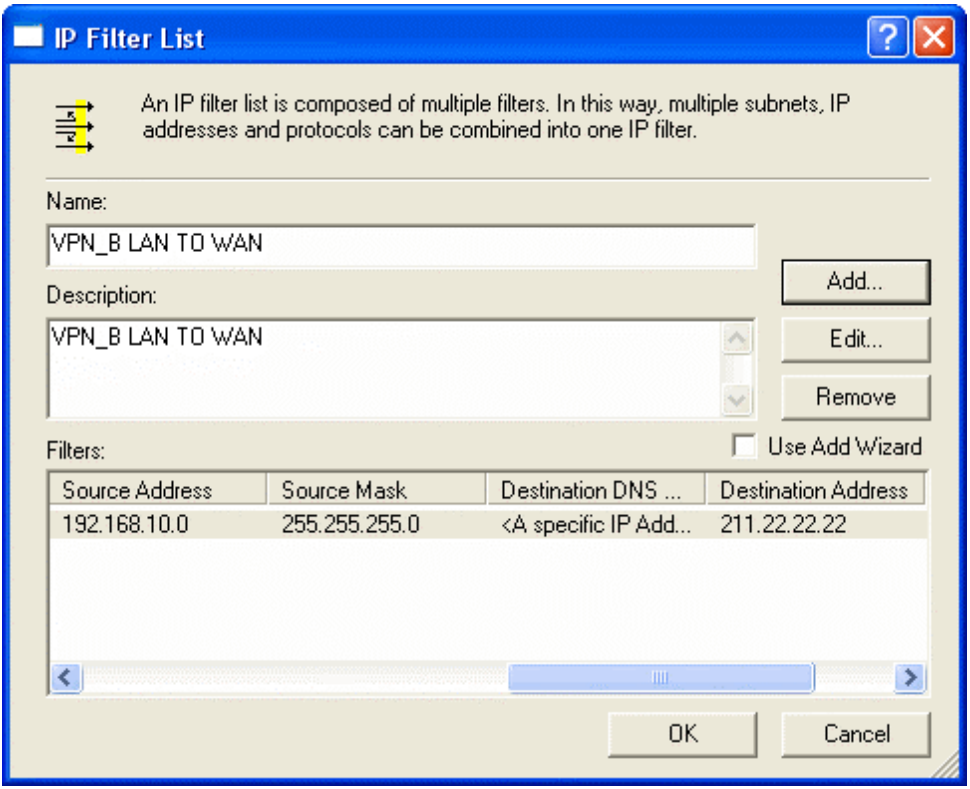


Step 31. In Filter Properties window,
in Source address, click down the arrow to select the specific IP Subnet and fill Company A's IP Address, 192.168.10.0 and Subnet mask 255.255.255.0.

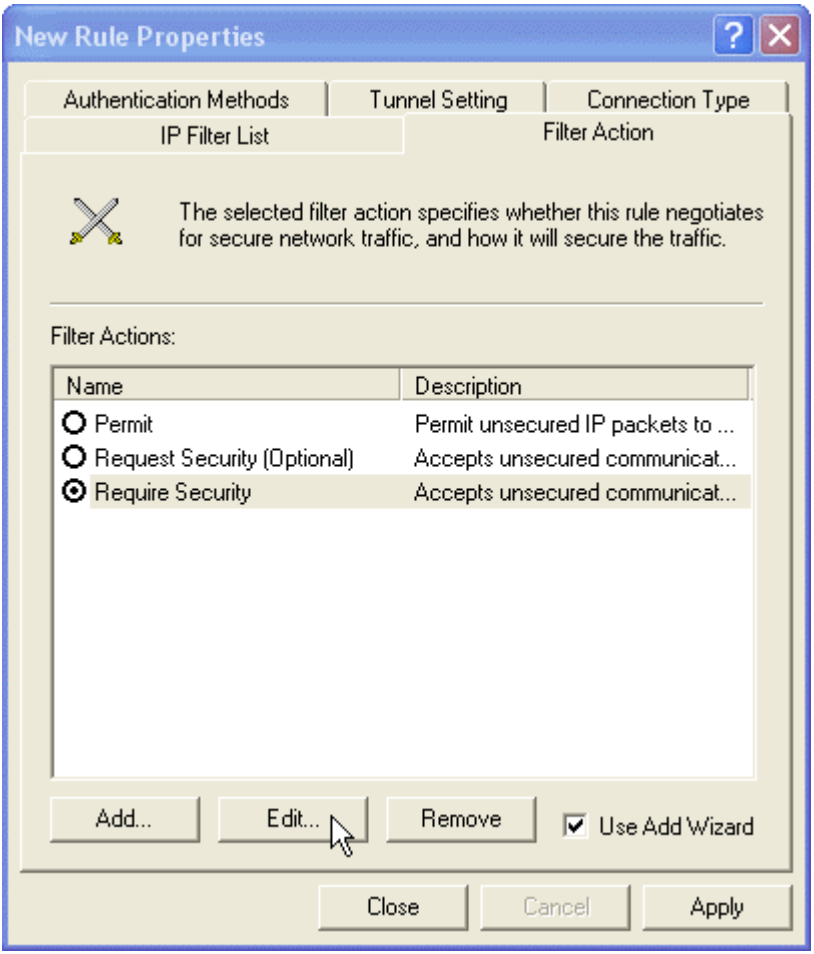
In Destination address click down the arrow to select the specific IP Subnet and fill Company B's IP Address, 211.22.22.22 and Subnet mask, 255.255.255.255., Please disable Mirrored. Also match packets with the exact opposite source and destination addresses.



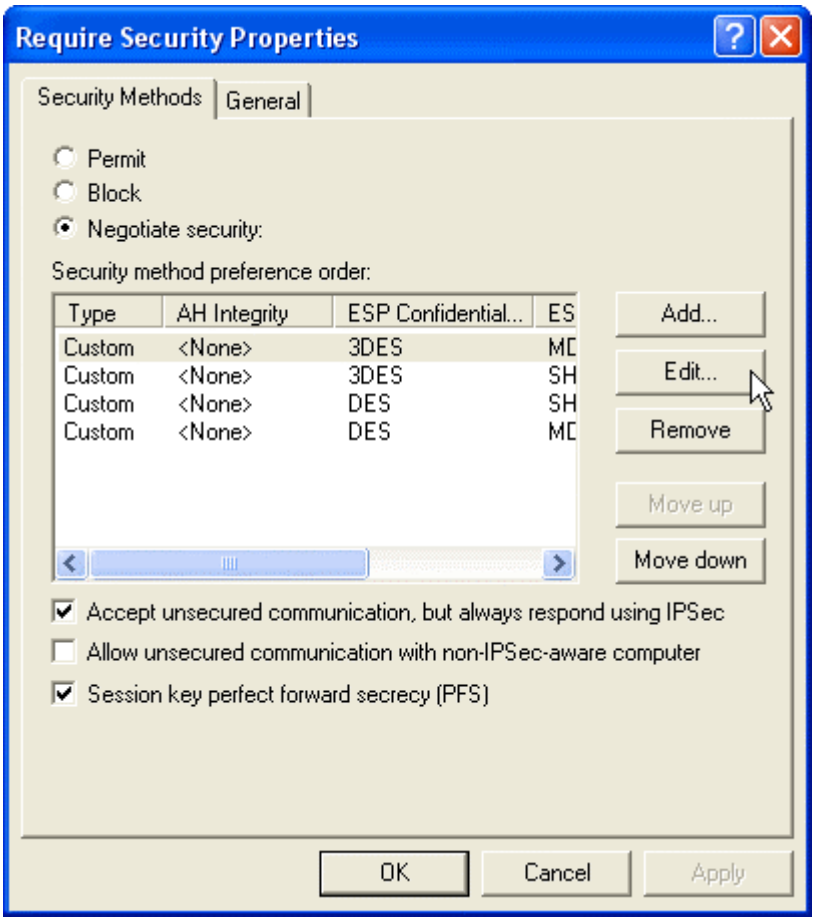
Step 32. Finish the setting and close IP Filter List window.



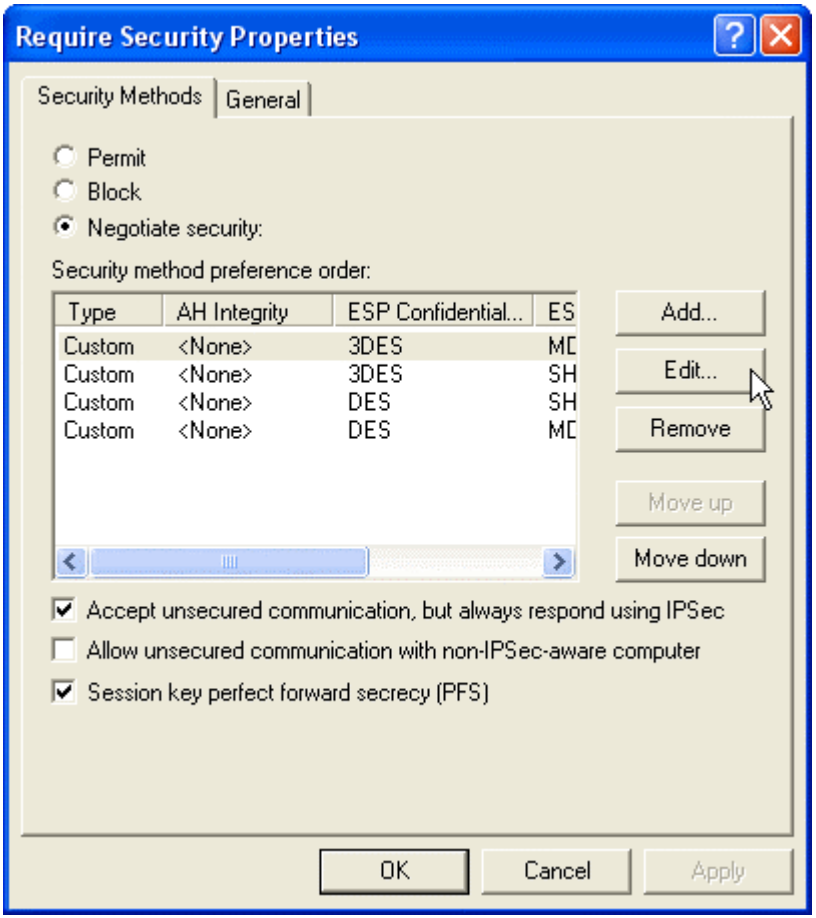
Step 33. Click Filter Action tab and choose Require Security. Click Edit.



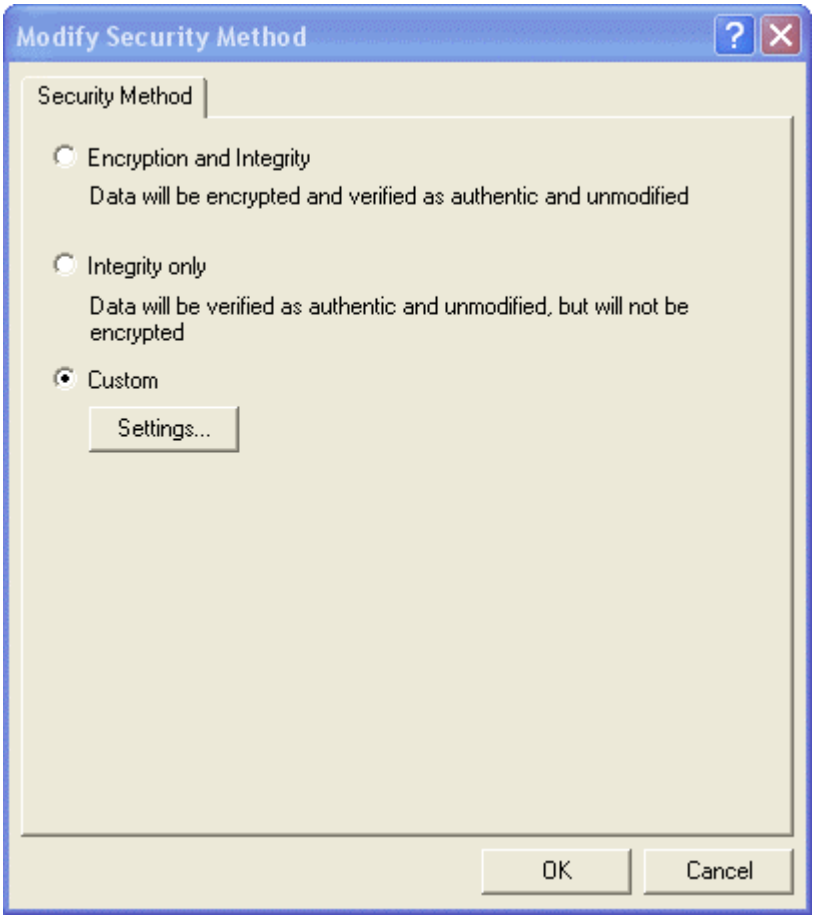
Step 34. In Security Methods tab, choose accept unsecured communication, but always respond using IPSec.



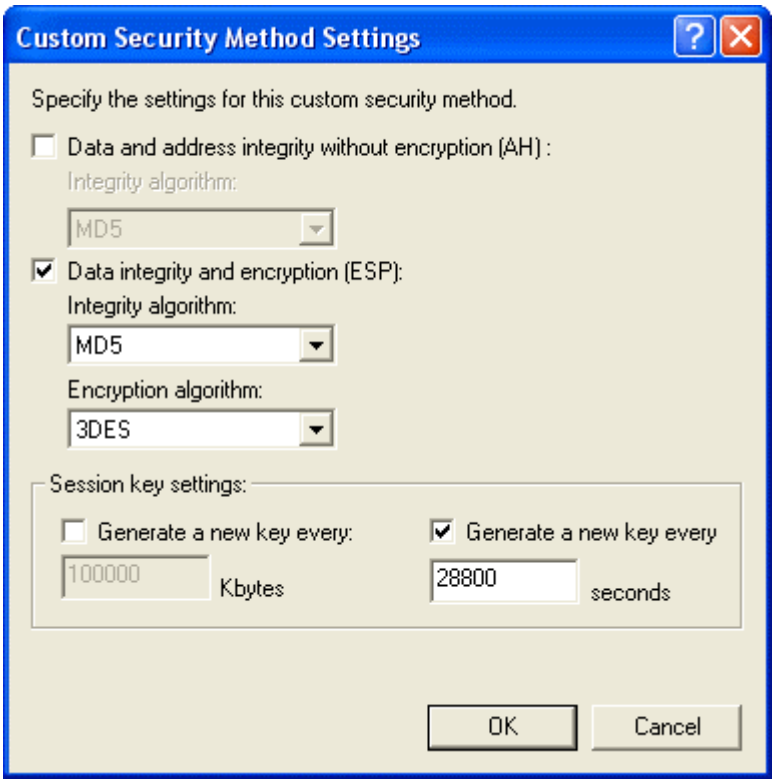
Step 35. Click Edit in Custom/ None/ 3DES/ MD5.



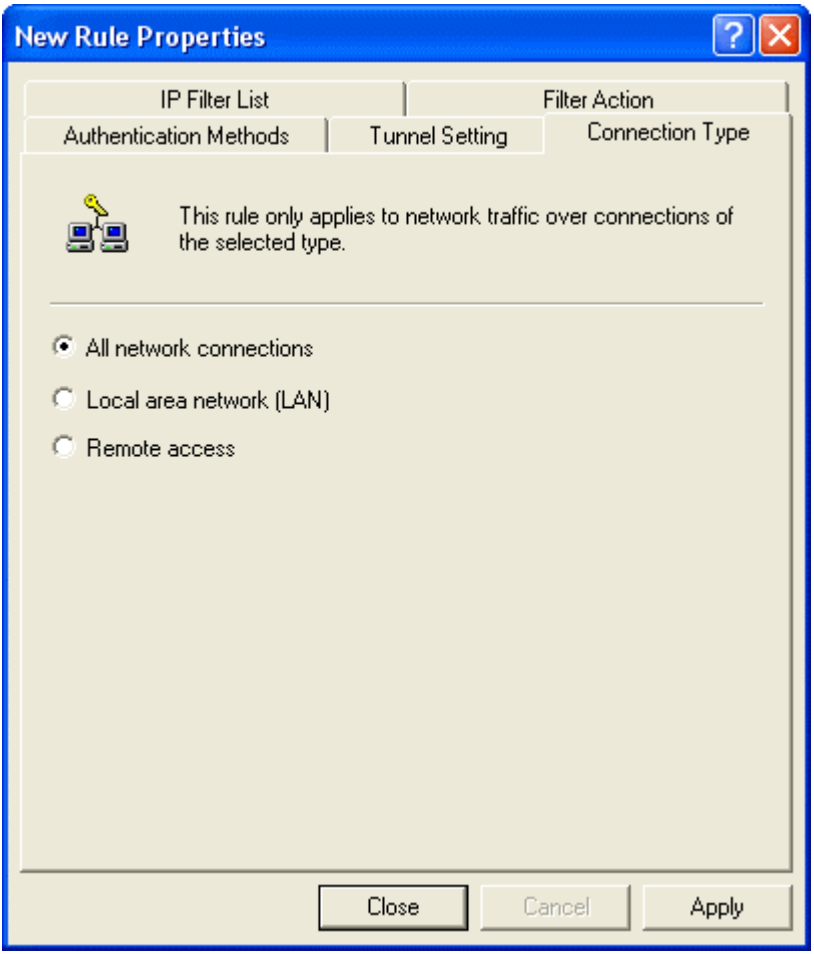
Step 36. Click Custom(For professional user) and click Edit.



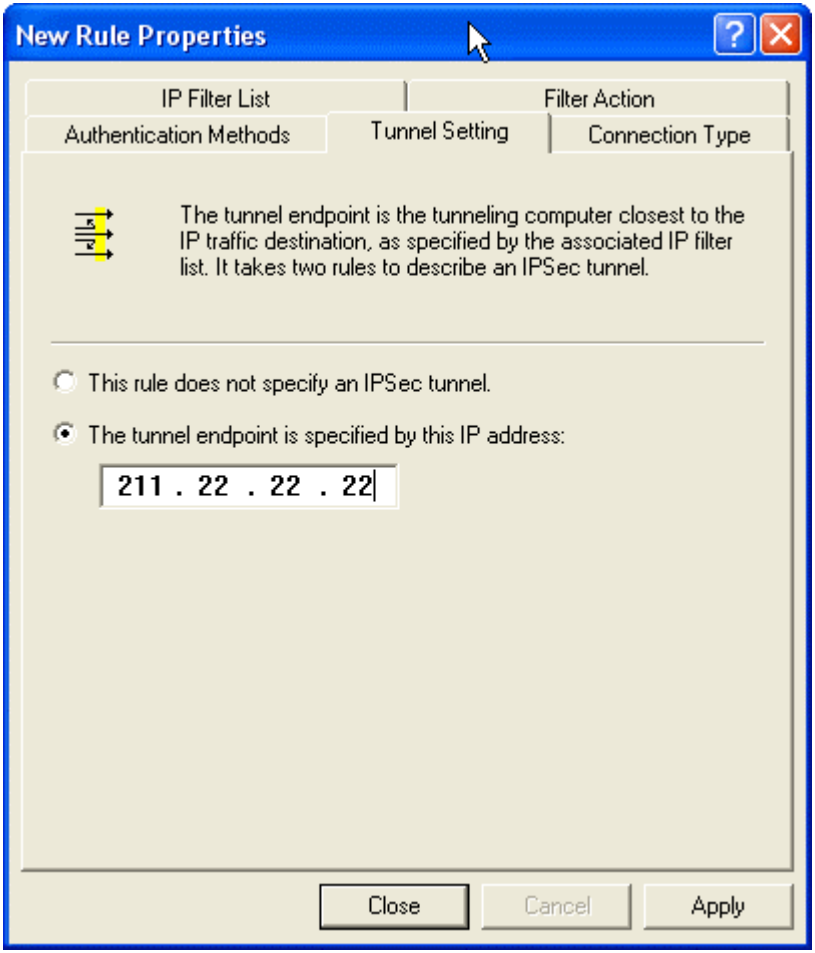
Step 37. Click Data Integrity and Encapsulation and choose MD5 and 3DES. Click Generate a New key after every 28800 seconds. And click 3 times OK to return.



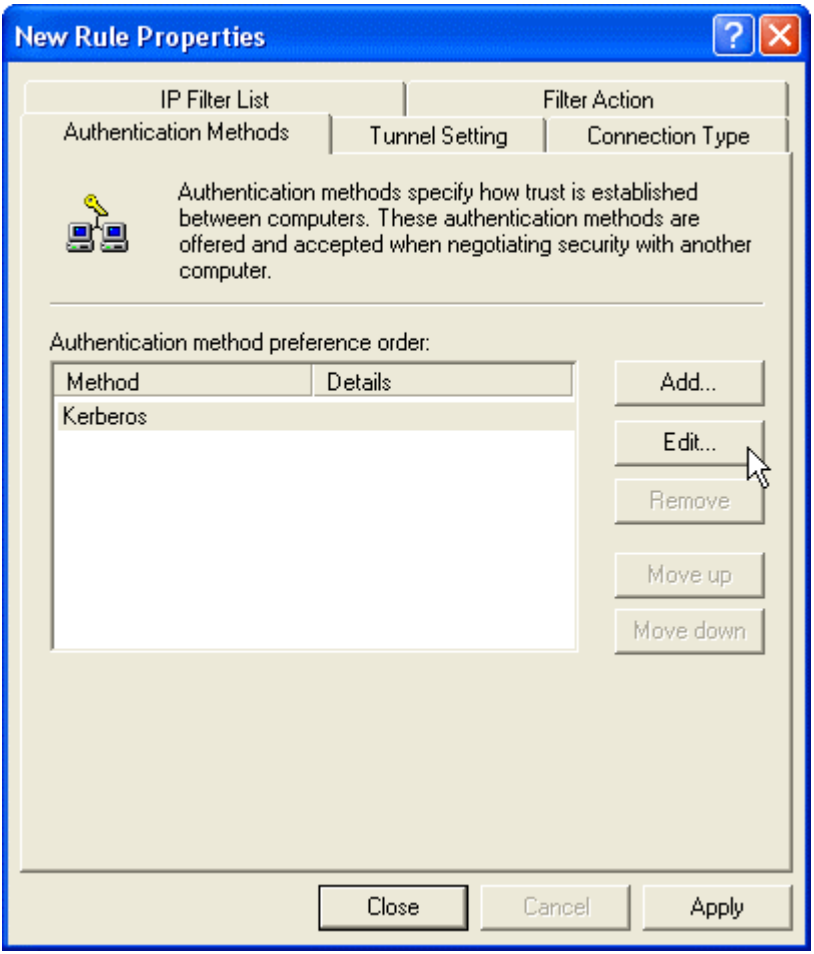
Step 38. Click Connection Type tab and click all network connections.



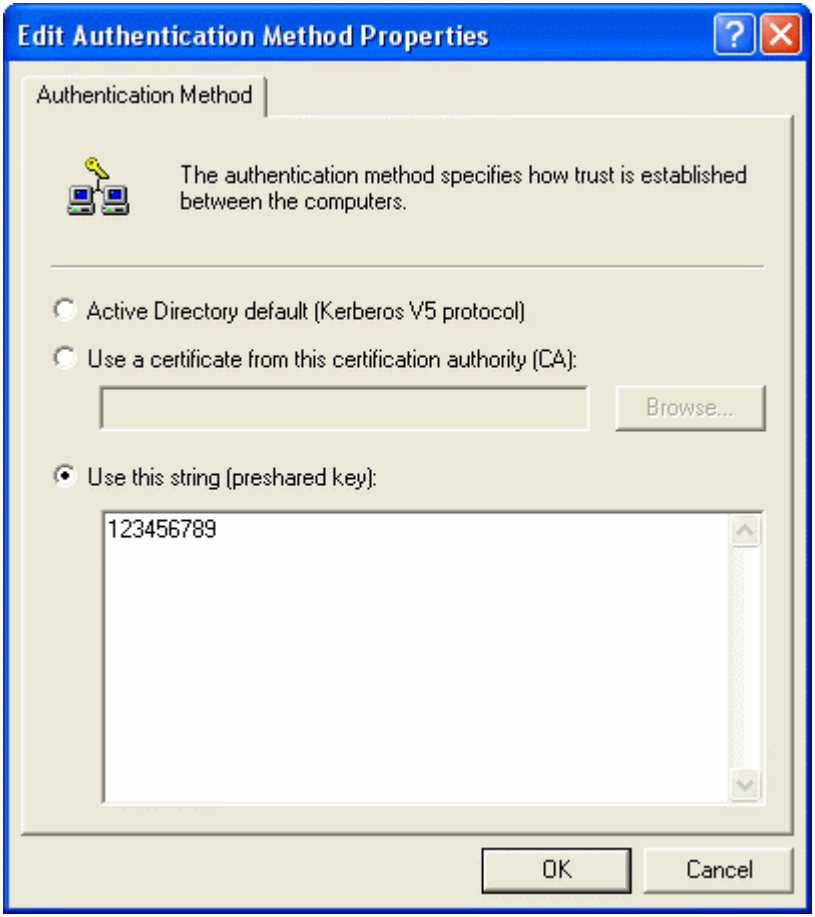
Step 39. Click Tunnel Setting tab, and click The tunnel endpoint is specified by the IP Address. Enter the WAN IP of Company B, 211.22.22.22.



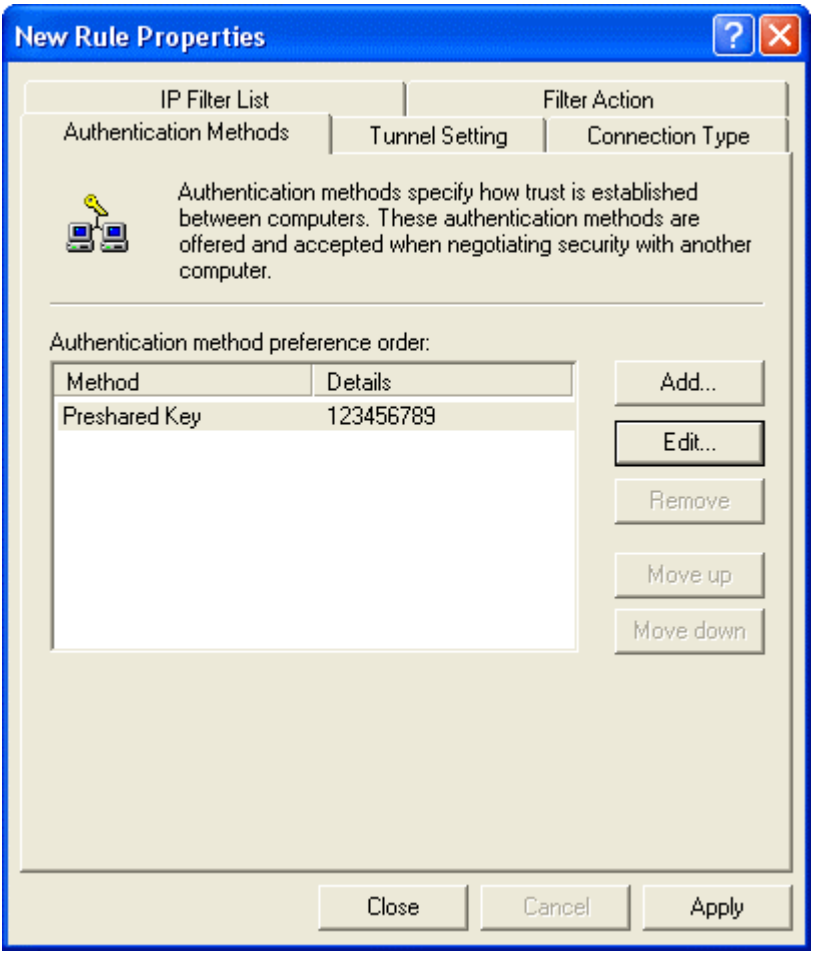
Step 40. Click Authentication Methods and click Edit.



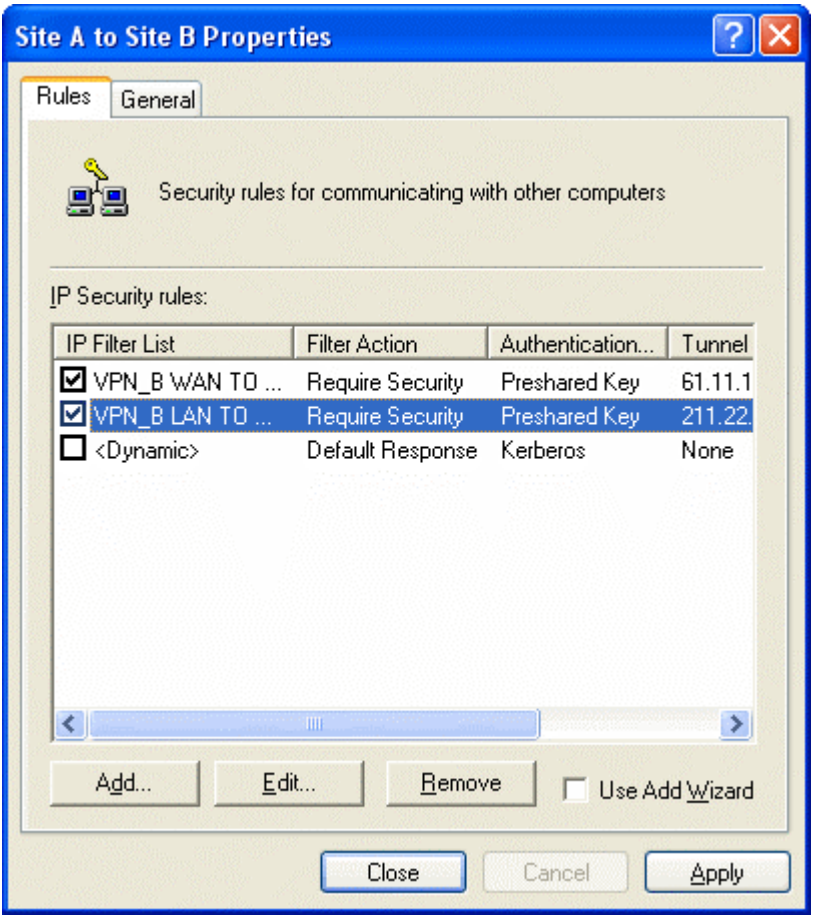
Step 41. Choose Use this string to protect the key exchange (Preshared Key). And enter the key, 123456789.



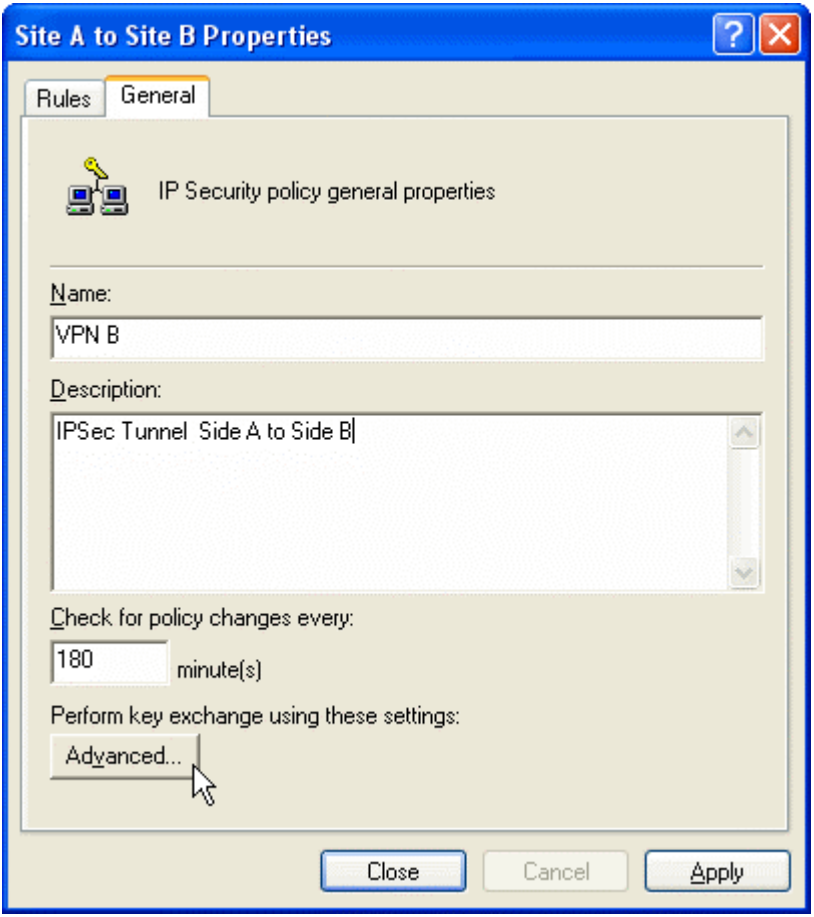
Step 42. Finish the setting, and close the window.



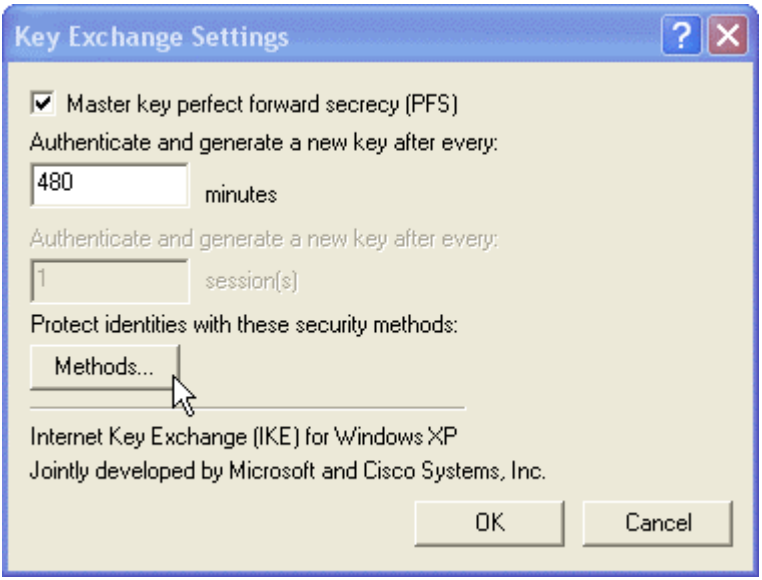
Step 43. Finish the Policy setting of VPN_B LAN TO WAN.



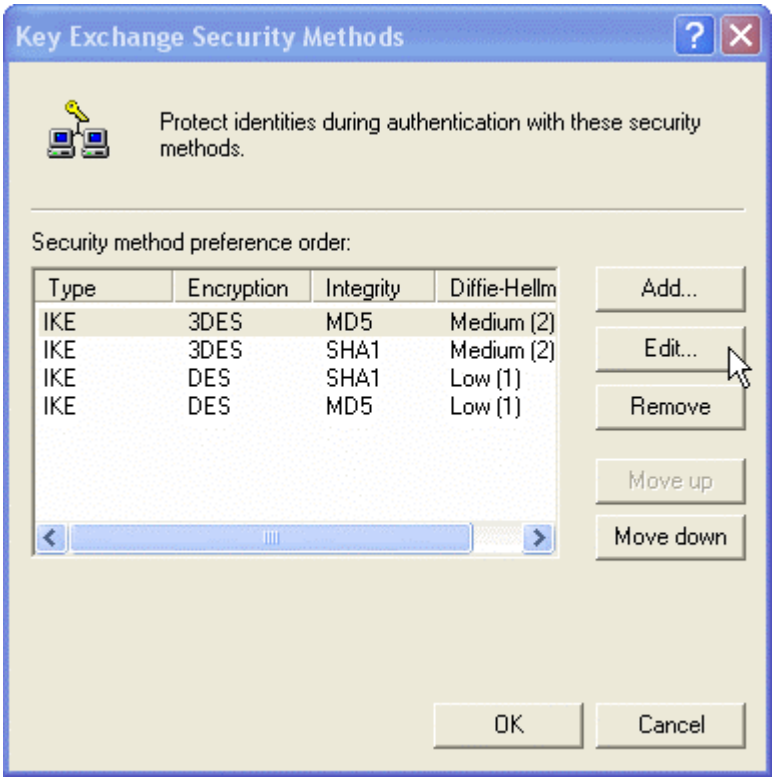
Step 44. In VPN_B window, click General tab. And click Advanced for Key Exchange using these settings.



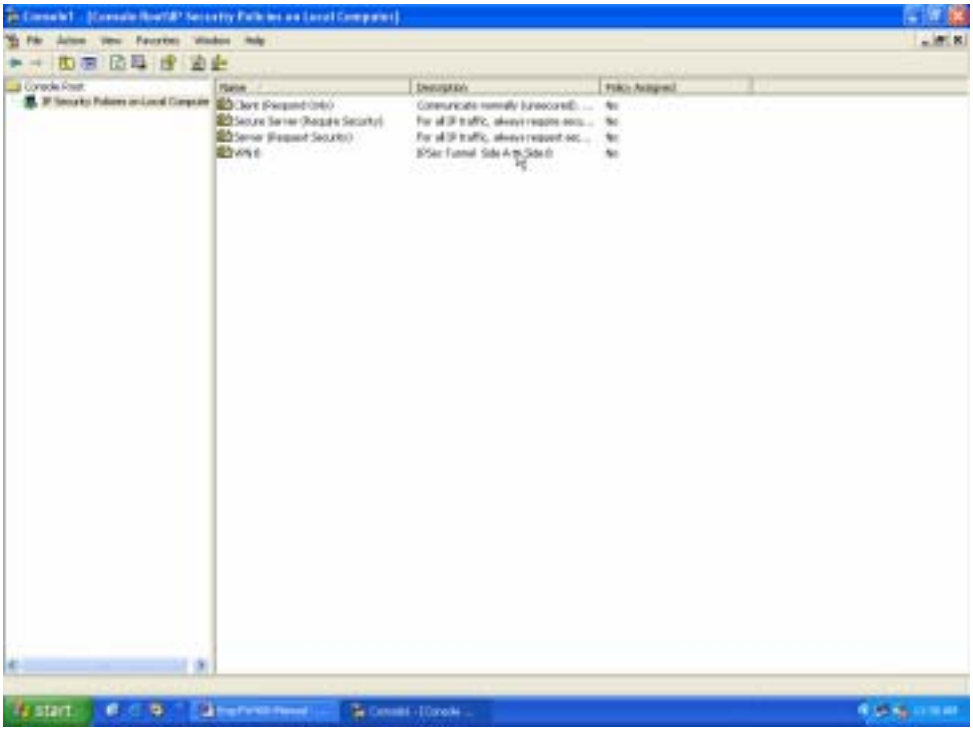
Step 45. Click Master key Perfect Forward Secrecy.



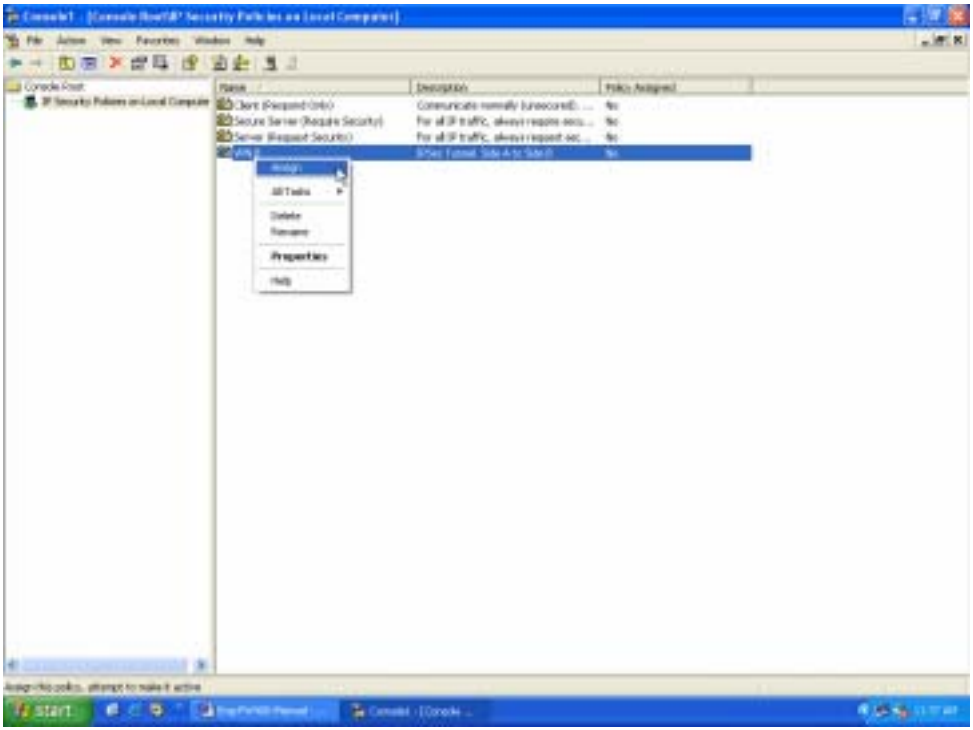
Step 46. Move IKE/ 3DES/ MD5/ up to the highest order. Finish all settings.



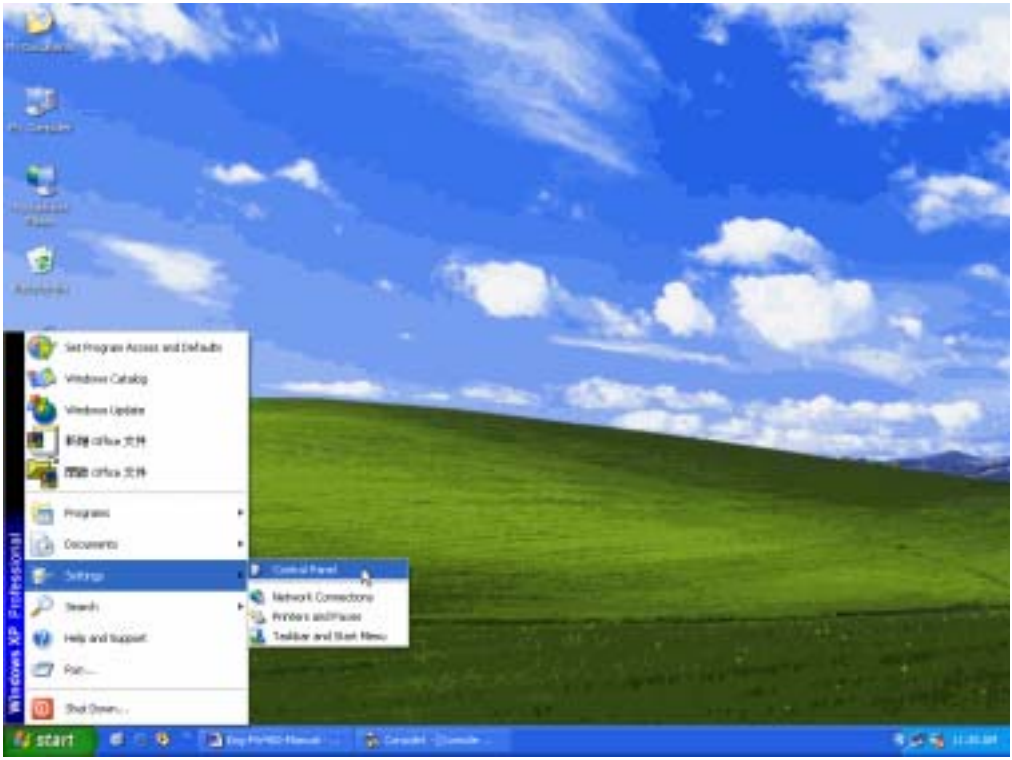
Step 47. Finish the settings of Company B’s Windows 2000 VPN.



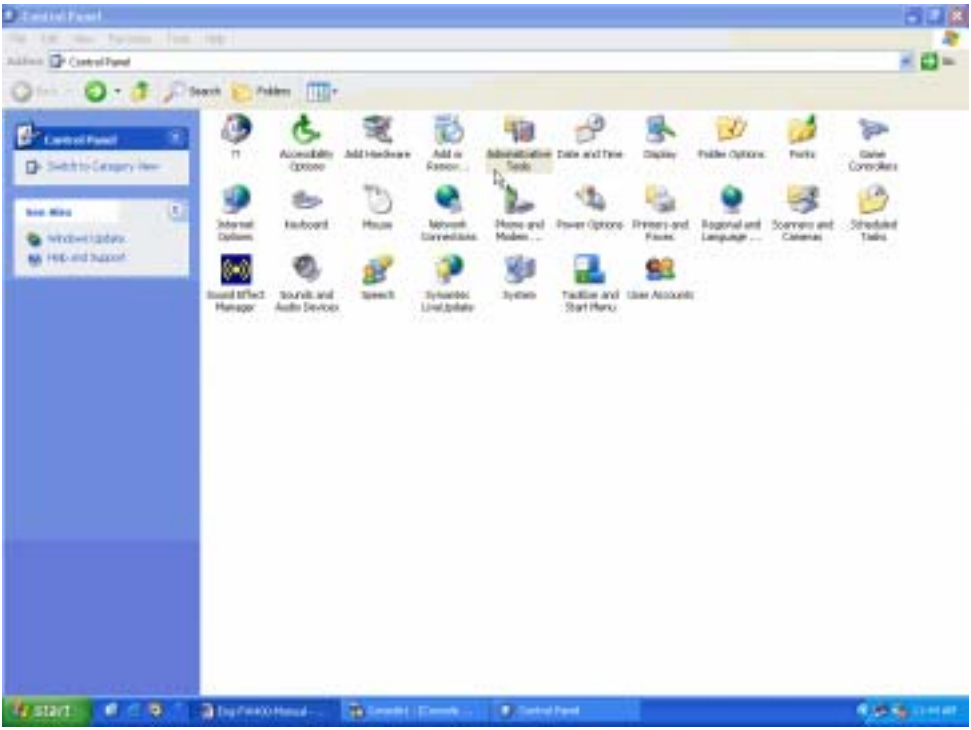
Step 48. Click the right button of mouse in VPN_B and enable Assign.



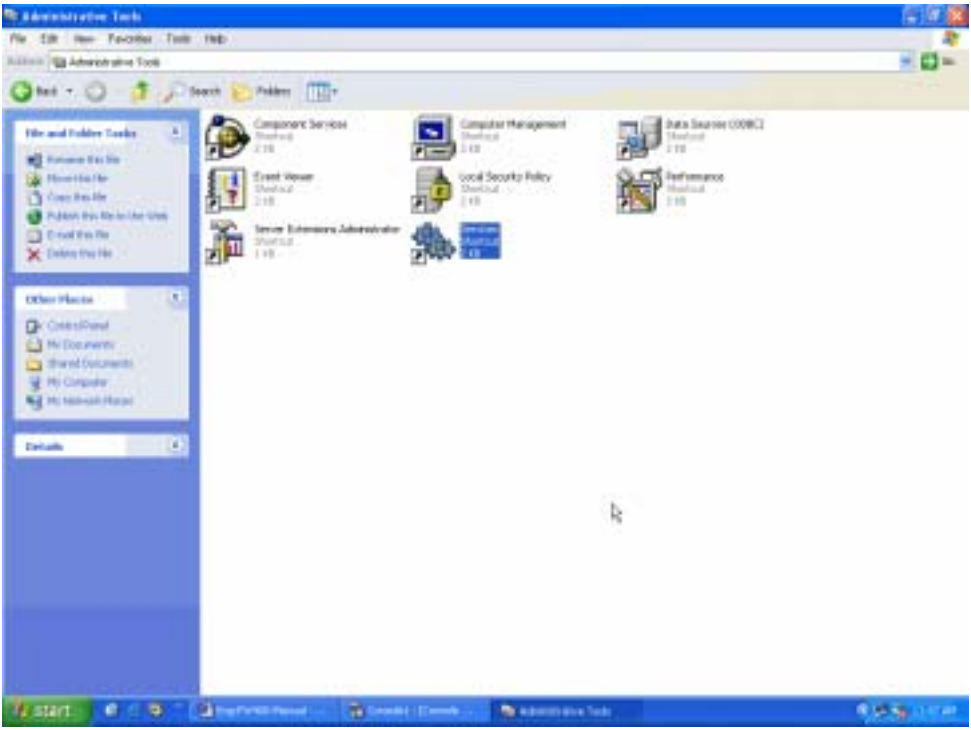
Step 49. To restart IPSec by Start→Settings→Control Panel



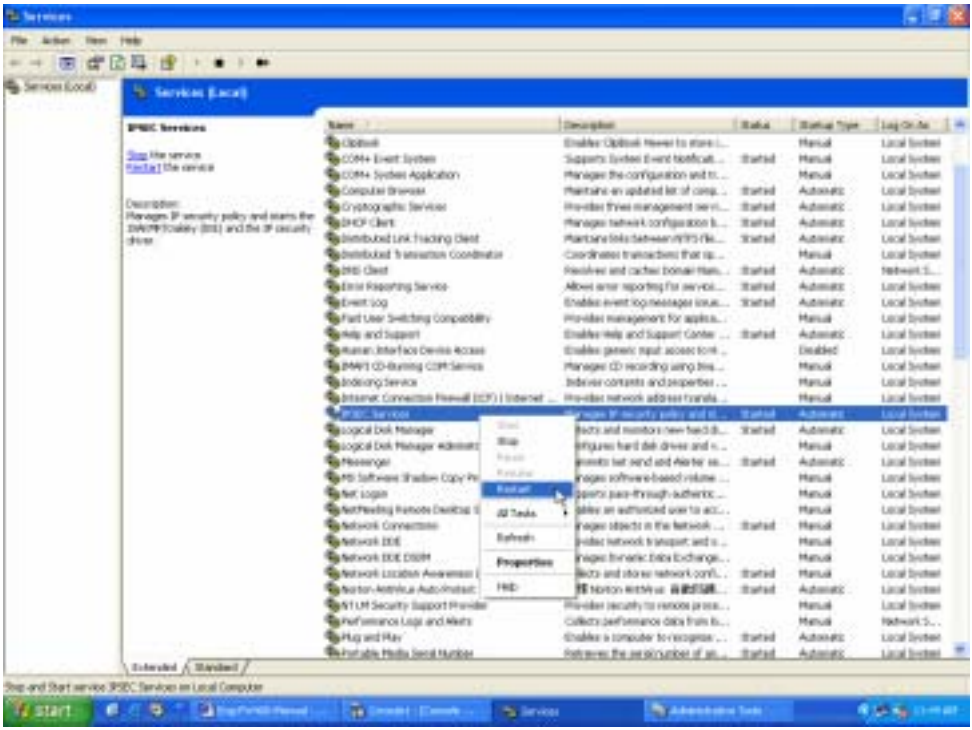
Step 50. Enter Control Panel and click Administrative Tools.



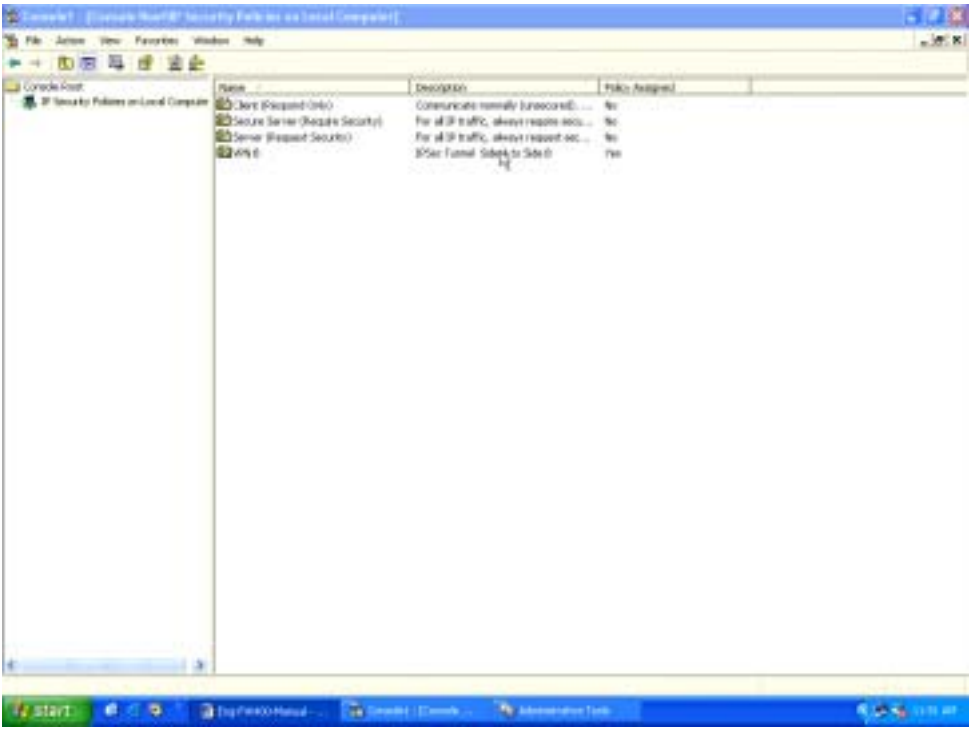
Step 51. After entering Administrative Tools, click Services.



Step 52. After entering Service, click IPSec Services, Restart the Service.



Step 53. Finish all settings.



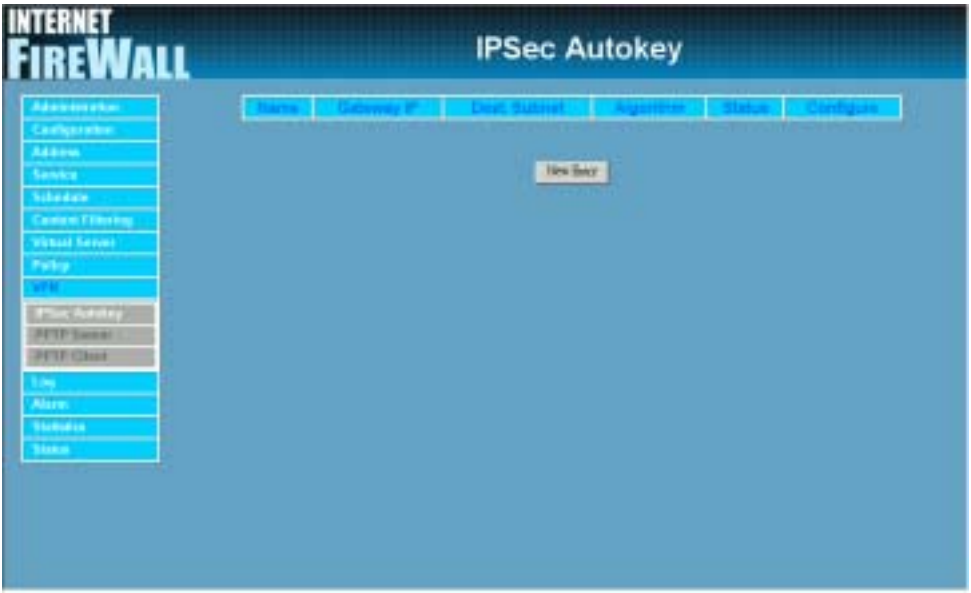
Example 3. Create a VPN connection between two VPN Firewall using Aggressive mode Algorithm (3 DES and MD5), and data encryption for IPSec Algorithm (3DES and MD5)

Preparation Task:
Company A External IP is 61.11.11.11
Internal IP is 192.168.10.X
Company B External IP is 211.22.22.22
Internal IP is 192.168.20.X

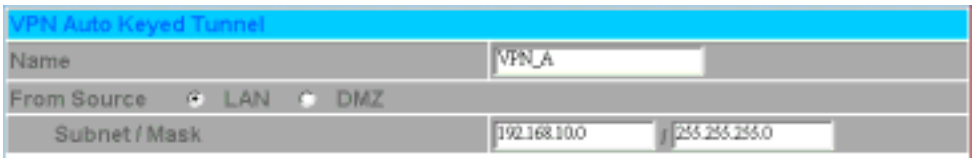
To suppose Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file by Aggressive mode Algorithm.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's VPN Firewall, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

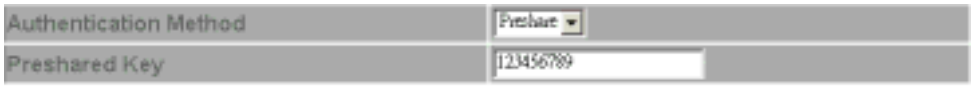


Step 2. Enter the VPN name, VPN_A in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.10.0 and subnet mask, 255.255.255.0.

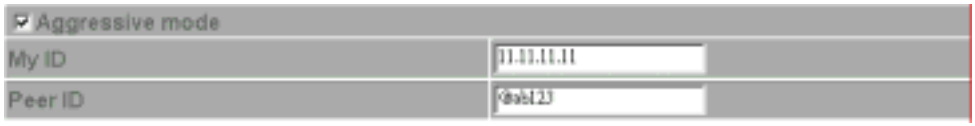


Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company B's subnet IP and mask.

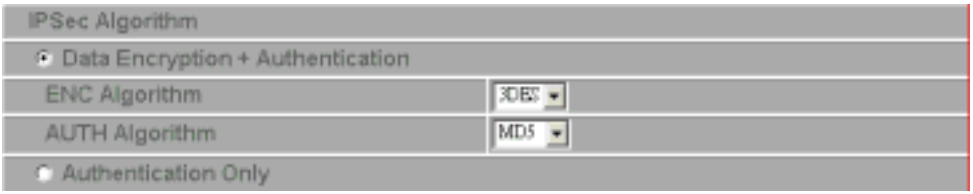
Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)



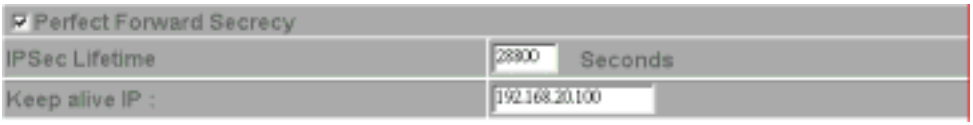
Step 5. In Encapsulation or Authentication table, choose Aggressive mode Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 2 to connect.
Enter Local ID/ Remote ID optionally. If we choose to enter Local ID/ Remote ID, they couldn't be equal. For instance, Local ID is 11.11.11.11 and Remote ID is 22.22.22.22. Add @ before number or text, for instance, @123A and @Abcd1.



Step 6. In IPSec Algorithm Table , choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



Step 7. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

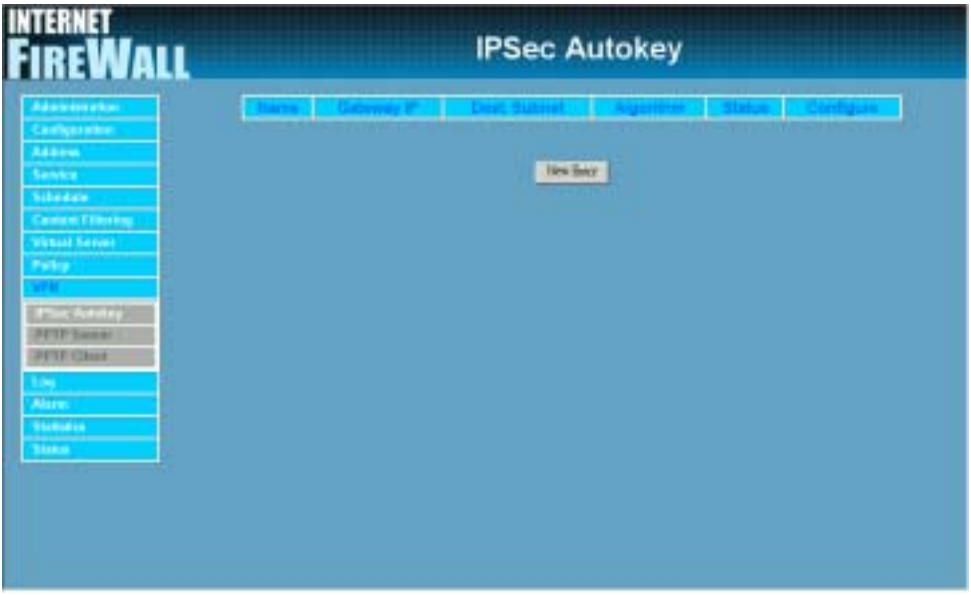


Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

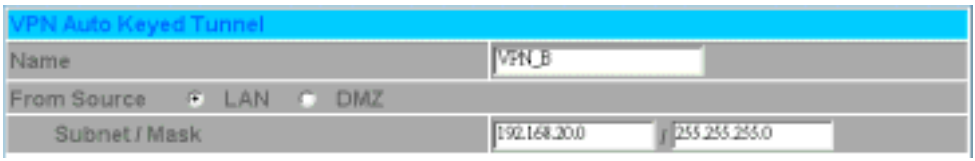
Step 9. Click OK to finish the setting of Company A.

The Gateway of Company B is 192.168.20.1. The settings of company B are as the following.

Step 1. Enter the default IP of Company B's VPN Firewall, 192.168.20.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

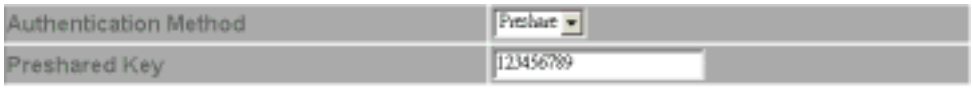


Step 2. Enter the VPN name, VPN_B in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.20.0 and subnet mask, 255.255.255.0.

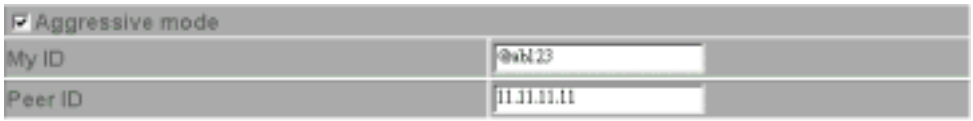


Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.

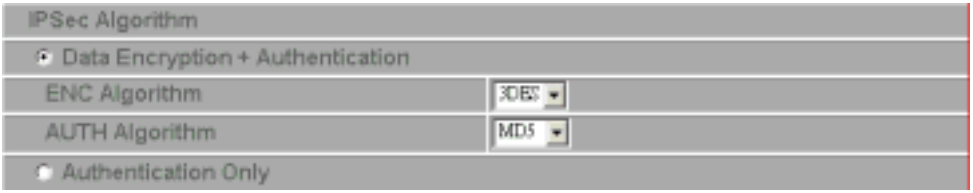
Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)



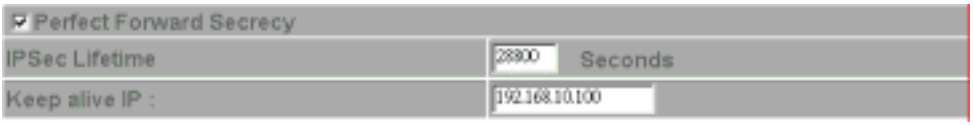
Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 2 to connect.
Enter Local ID/ Remote ID optionally. If we choose to enter Local ID/ Remote ID, they couldn't be equal. For instance, Local ID is 11.11.11.11 and Remote ID is 22.22.22.22. Add @ before number or text, for instance, @123A and @Abcd1.



Step 6. In IPSec Algorithm Table , choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



Step 7. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.



Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Step 9. Click OK to finish the setting of Company B.

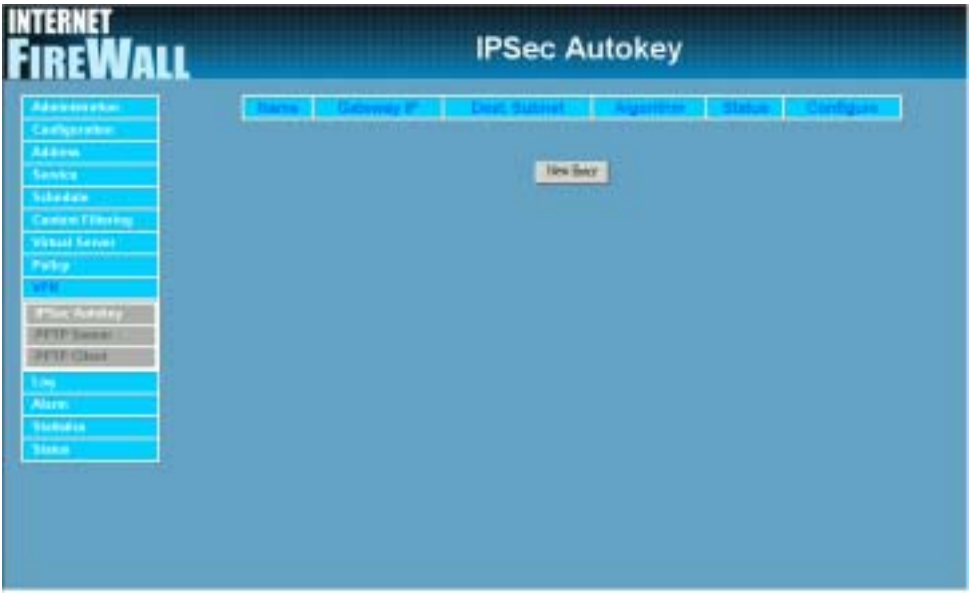
Example 4. Create a VPN connection between two VPN Firewall using ISAKMP Algorithm (3DES and MD5), data encryption for IPSec Algorithm (3DES and MD5) and GRE.

Preparation Task:
Company A External IP is 61.11.11.11
Internal IP is 192.168.10.X
Company B External IP is 211.22.22.22
Internal IP is 192.168.20.X

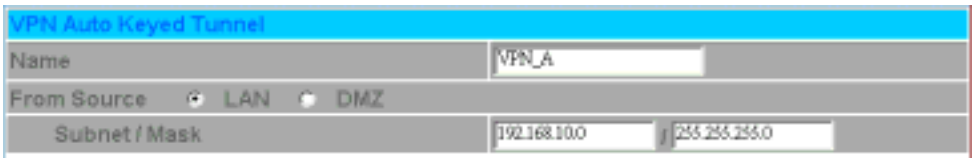
To suppose Company A, 192.168.10.100 create a VPN connection with company B, 192.168.20.100 for downloading the sharing file by GRE/ IPSec Algorithm.

The Gateway of Company A is 192.168.10.1. The settings of company A are as the following.

Step 1. Enter the default IP of Company A's VPN Firewall, 192.168.10.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.

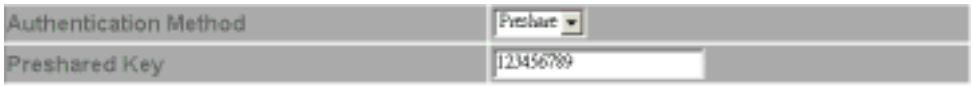


Step 2. Enter the VPN name, VPN_A in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.10.0 and subnet mask, 255.255.255.0.

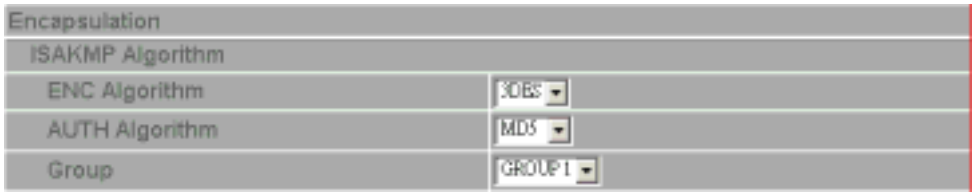


Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company B's subnet IP and mask.

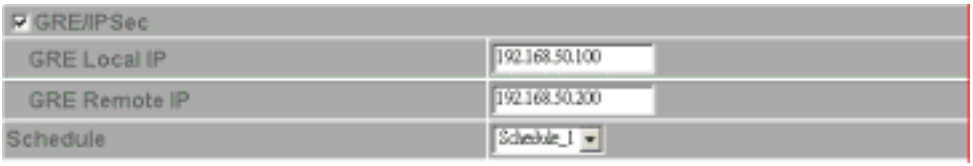
Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)



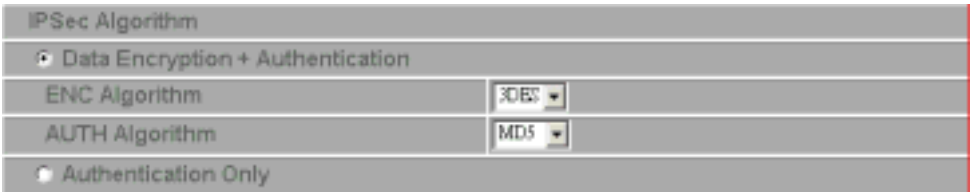
Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group to connect.



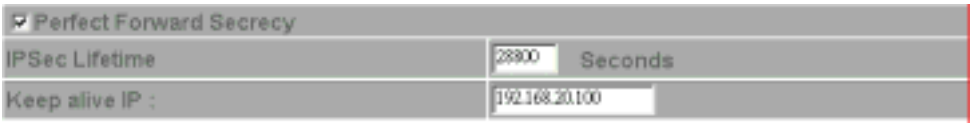
Step 6. Choose GRE/ IPSec and enter GRE Source IP, 192.168.50.100 and GRE Remote IP, 192.168.50.200.
Note. The Source IP and Remote IP should be in the same C Class and modified by Administrator.



Step 7. In IPSec Algorithm Table , choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



Step 8. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.

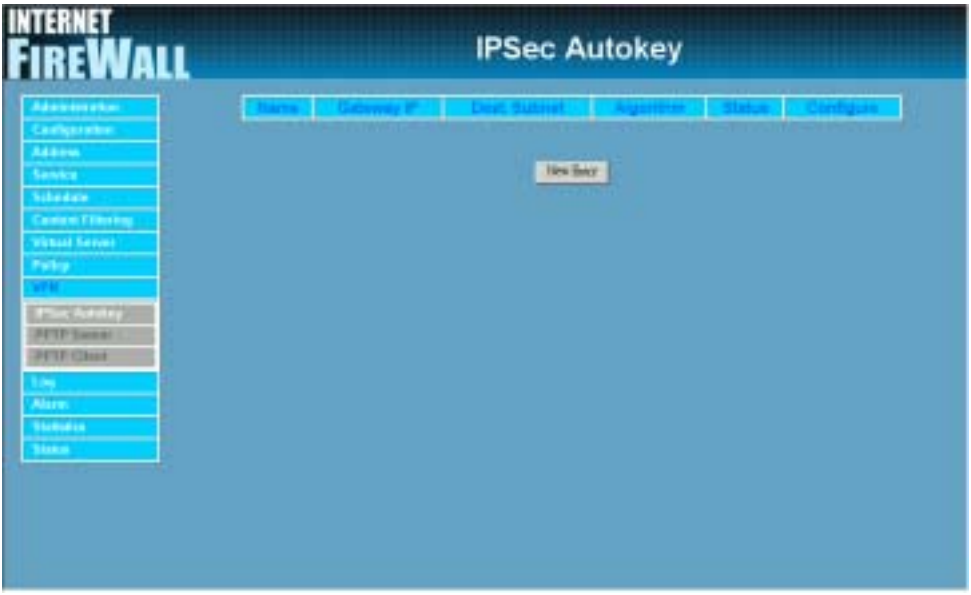


Step 9. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Step 10. Click OK to finish the setting of Company A.

The Gateway of Company B is 192.168.20.1. The settings of company B are as the following.

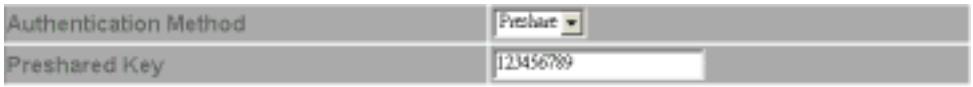
Step 1. Enter the default IP of Company B's VPN Firewall, 192.168.20.1. Click VPN in the menu bar on the left hand side, and then select the sub-select IPSec Autokey. Click Add.



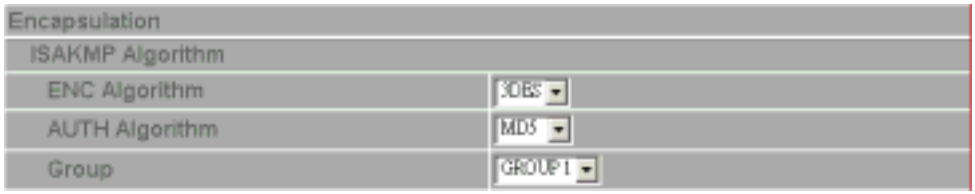
Step 2. Enter the VPN name, VPN_B in IPSec Autokey window, and choose From Source to be Internal. Fill the subnet IP, 192.168.20.0 and subnet mask, 255.255.255.0.

Step 3. In To Destination table, choose Remote Gateway-Fixed IP, enter the IP desired to be connected, company A's subnet IP and mask, 192.168.10.0 and 255.255.255.0 respectively.

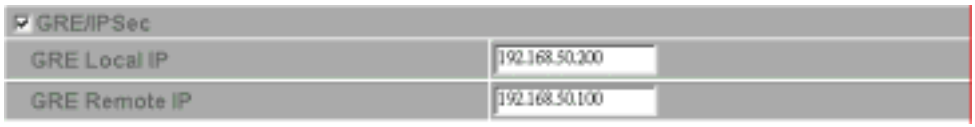
Step 4. In Authentication Method Table, choose Preshare and enter the Preshared Key. (The max length is 100 bits.)



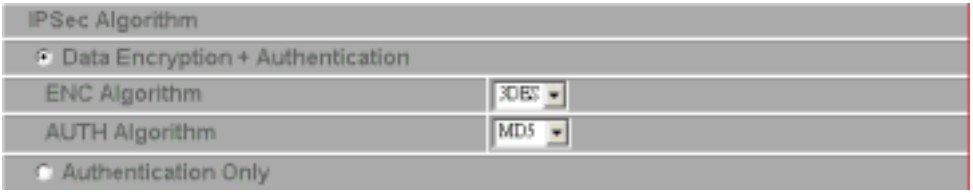
Step 5. In Encapsulation or Authentication table, choose ISAKMP Algorithm. For communication via VPN, we choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm. And select Group 1 to connect.



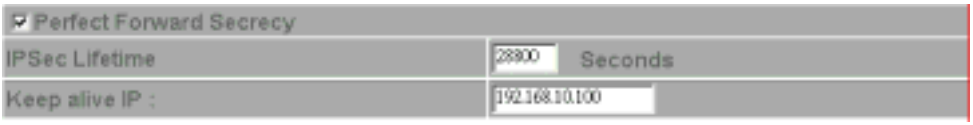
Step 6. Choose GRE/ IPSec and enter GRE Source IP, 192.168.50.200 and GRE Remote IP, 192.168.50.100.
Note. The Source IP and Remote IP should be in the same C Class and modified by Administrator.



Step 6. In IPSec Algorithm Table , choose Data Encryption + Authentication. We choose 3DES for ENC Algorithm and MD5 for AUTH Algorithm.



Step 7. Choose Perfect Forward Secrecy, and enter 28800 seconds in IPSec Lifetime and Keep alive IP to keep connecting.



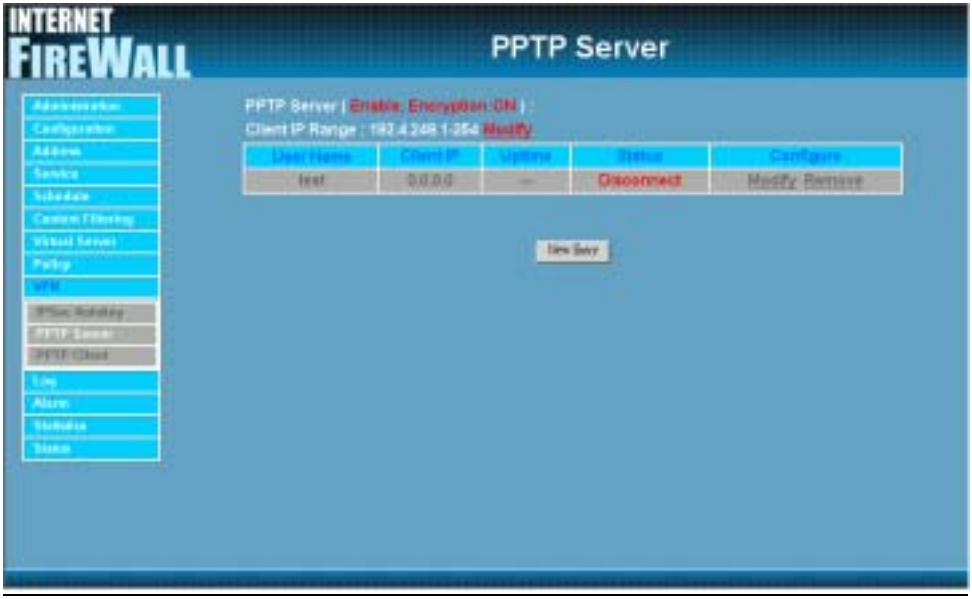
Step 8. Click the down arrow to select the policy of schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Step 9. Click OK to finish the setting of Company B.

PPTP Server

Entering the PPTP Server window

Step 1. Select **VPN→PPTP Server**.



- **PPTP Server**：Click **Modify** to select Enable or Disable.
- **Client IP Range**: **192.26.145.1-254**：Display the IP addresses range for PPTP Client connection.
- **User Name**：Displays the PPTP Client user's name for authentication.
- **Client IP**：Displays the PPTP Client's IP address for authentication.。
- **Uptime**：Displays the connection time between PPTP Server and Client.
- **Status**：Displays current connection status between PPTP Server and PPTP client.
- **Configure**：Click 【**Modify**】to modify the PPTP Client settings or click 【**Remove**】to remove the item.

Modifying PPTP Server Design

Step 1. Select **VPN→PPTP Server**.

Step 2. Click【**Modify**】after the Client IP Range.

Step 3. In the【Modify Server Design 】Window, enter appropriate settings.

- ☐**Disable PPTP**：Check to disable PPTP Server.
- ☐ **Enable PPTP**：Check to enable PPTPServer.

  1.Encyption: the default is set to disabled.

  2.Client IP Range：Enter the IP range allocated for PPTP Client to connect to the PPTP server.
- **Auto-Disconnect if idle □ minutes**: Configure this device to disconnect to the PPTP Server when there is no activity for a predetermined period of time. To keep the line always connected, set the number to 0.
- **Schedule**：Click the down arrow to select the schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications

Adding PPTP Server

Step 1. Select **VPN→PPTP Server**. Click **NewEntry.**

Step 2. Enter appropriate settings in the following window.

- **User name:** Specify the PPTP client. This should be unique.
- **Password:** Specify the PPTP client password.
- **Remote Client：**

  ☐Single Machine**:** Check to connect to single computer.
  ☐Multi-Machine: Check to allow multiple computers connected to the PPTP server.
  IP Address：Enter the PPTP Client IP address.
  Netmask: Enter the PPTP Client Sub net mask.

- Client IP assigned by：
  1. IP Range: check to enable auto-allocating IP for PPTP client to connect.
  2. Fixed IP: check and enter a fixed IP for PPTP client to connect.

Step 3. Click **OK** to save modifications or click **Cancel** to cancel modifications

Modifying PPTP Server

Step 1. Select **VPN→PPTP Server**.

Step 2. In the【PPTP Server】window, find the PPTP server that you want to modify. Click 【Configure】and click 【Modify】.

Step 3. Enter appropriate settings.

Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications

Removing PPTP Server

Step 1. Select **VPN→PPTP Server**.

Step 2. In the【**PPTP Server**】window, find the PPTP server that you want to modify. Click 【**Configure**】and click 【remove】.

Step 3. Click **OK** to remove the PPTP server or click **Cancel** to exit without rmoval.

PPTP Client

Entering the PPTP Client window

Step 1. Select **VPN→PPTP Client**.

- **User Name**：Displays the PPTP Client user's name for authentication.
- **Server Address**：Displays the PPTP Server Address IP address。
- **Encryption**：Displays the Encryption ON/OFF。
- **Uptime**：Displays the connection time between PPTP Server and Client.
- **Status**：Displays current connection status between PPTP Server and PPTP client.
- **Configure**：

  Click 【**Connect**】to connect the PPTP Server settings .

  Click 【**Modify**】to modify the PPTP Client settings .

  Click 【**Remove**】to remove the item.

Adding a PPTP Client

Step 1. Select **VPN→PPTP Client**.

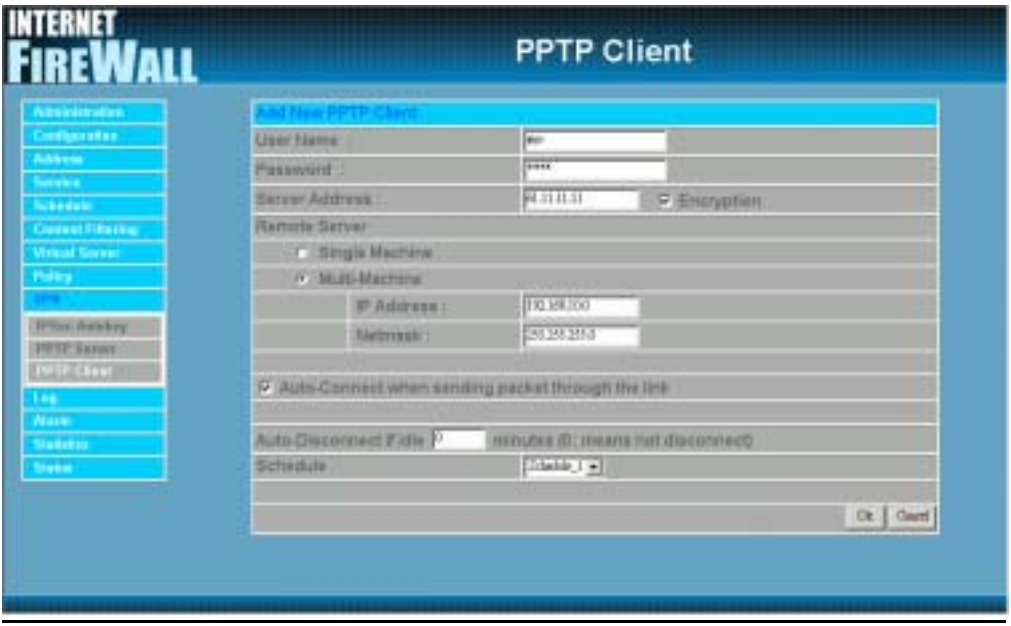
- User name: Specify the PPTP client. This should be unique.
- Password: Specify the PPTP client password.
- Server Address: Enter the PPTP Server's IP address.
- Remote Client：

☐**Single Machine:** Check to connect to single computer.

☐**Multi-Machine:** Check to allow multiple computers connected to the PPTP server.

IP Address：Enter the PPTP Client IP address.

Netmask: Enter the PPTP Client Sub net mask.



- **□Auto-Connect when sending packet through the link**: Check to enable the auto-connection whenever there's packet to transmit over the connection.
- **Auto-Disconnect if idle □ minutes**: Configure this device to disconnect to the PPTP Server when there is no activity for a predetermined period of time. To keep the line always connected, set the number to 0.
- **Schedule**：Click the down arrow to select the schedule, which was pre-determined in Schedule. Refer to the corresponding section for details.

Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications.

Modifying PPTP Client

Step 1. Select **VPN→PPTP Client**.

Step 2. In the【PPTP Client】window, find the PPTP server that you want to modify. Click 【Configure】and click 【Modify】.

Step 3. Enter appropriate settings.

Step 4. Click **OK** to save modifications or click **Cancel** to cancel modifications

Removing PPTP Client

Step 1. Select **VPN→PPTP Client**.

Step 2. In the【**PPTP Client**】window, find the PPTP client that you want to modify. Click 【**Configure**】and click 【remove】.

Step 3. Click **OK** to remove the PPTP client or click **Cancel** to exit without removal.

Log

The VPN VPN Firewall supports traffic logging and event logging to monitor and record services, connection times, and the source and destination network address. The Administrator may also download the log files for backup purposes. The Administrator mainly uses the Log menu to monitor the traffic passing through the VPN Firewall.

What is Log?

Log records all connections that pass through the Firewall's control policies. Traffic log's parameters are setup when setting up control policies. Traffic logs record the details of packets such as the start and stop time of connection, the duration of connection, the source address, the destination address and services requested, for each control policy. Event logs record the contents of System Configuration changes made by the Administrator such as the time of change, settings that change, the IP address used to log on, etc.

How to use the Log

The Administrator can use the log data to monitor and manage the VPN and the networks. The Administrator can view the logged data to evaluate and troubleshoot the network, such as pinpointing the source of traffic congestions.

Traffic Log

The Administrator queries the Firewall for information, such as source address, destination address, start time, and Protocol port, of all connections.

Entering the Traffic Log window:

Click the **Traffic Log** option under **Log** menu to enter the Traffic Log window.

Traffic Log:

The table in the Traffic Log window displays current System statuses:

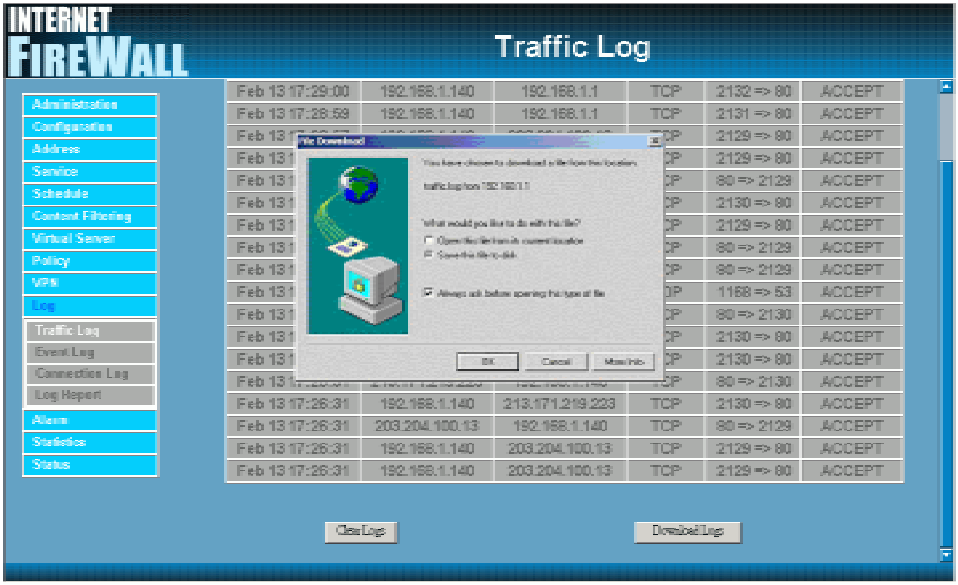
- **Time**: The start time of the connection.
- **Source:** IP address of the source network of the specific connection.
- **Destination:** IP address of the destination network of the specific connection.
- **Protocol & Port:** Protocol type and Port number of the specific connection.
- **Disposition:** Accept or Deny.

Downloading the Traffic Logs:

The Administrator can backup the traffic logs regularly by downloading it to the computer.

Step 1. In the Traffic Log window, click the Download Logs button at the bottom of the screen.

Step 2. Follow the File Download pop-up window to save the traffic logs into a specified directory on the hard drive.



Clearing the Traffic Logs:

The Administrator may clear on-line logs to keep just the most updated logs on the screen.

Step 1. In the Traffic Log window, click the Clear Logs button at the bottom of the screen.

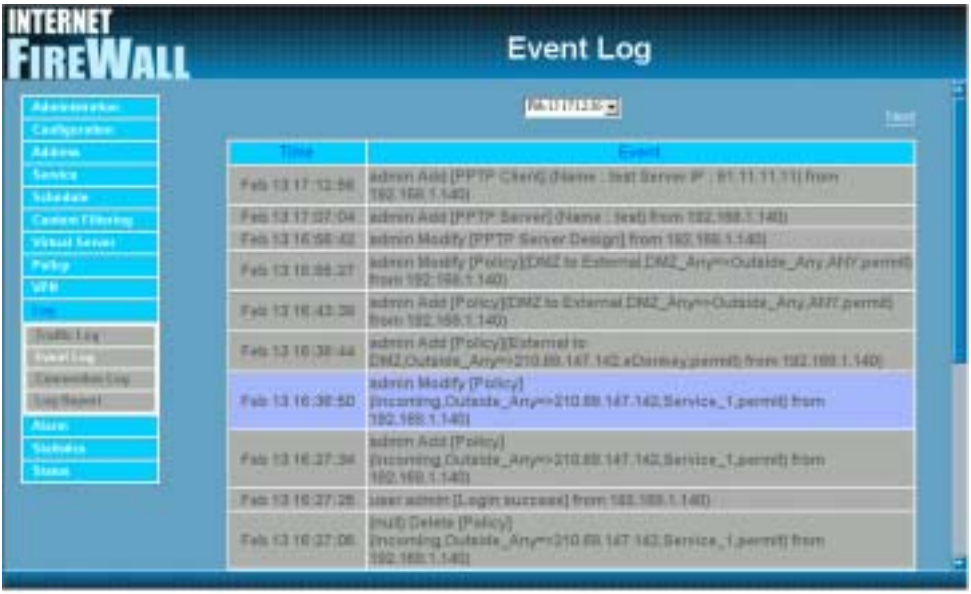
Step 2. In the Clear Logs pop-up box, click **Ok** to clear the logs or click **Cancel** to cancel it.

Event Log

When the VPN Firewall detects events, the Administrator can get the details, such as time and description of the events from the Event Logs.

Entering the Event Log window:

Click the **Event Log** option under the **Log** menu and the Event Log window will appear.



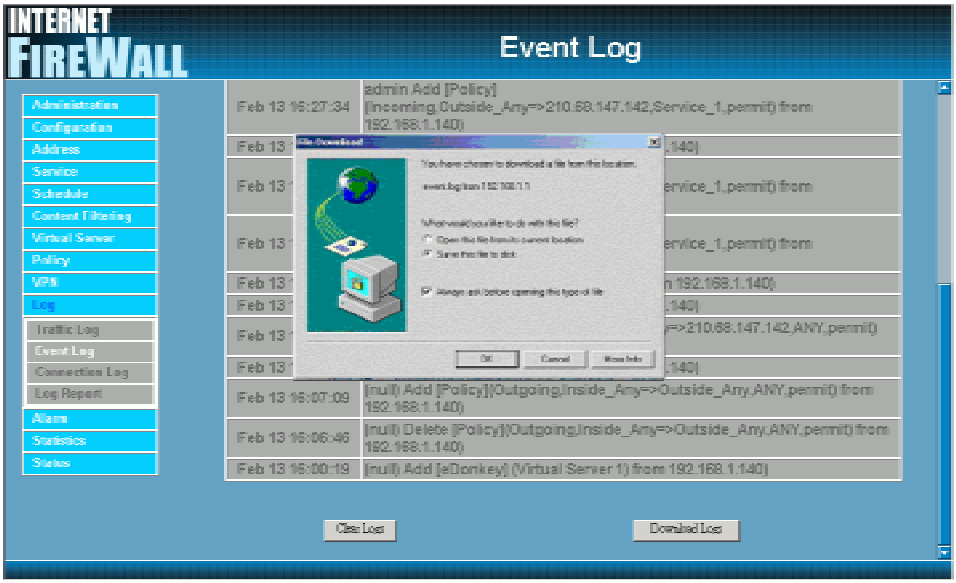
The table in the Event Log window displays the time and description of the events.

- **Time:** time when the event occurred.
- **Event:** description of the event.

Downloading the Event Logs:

Step 1. In the Event Log window, click the Download Logs button at the bottom of the screen.

Step 2. Follow the File Download pop-up window to save the event logs into a specific directory on the hard drive.

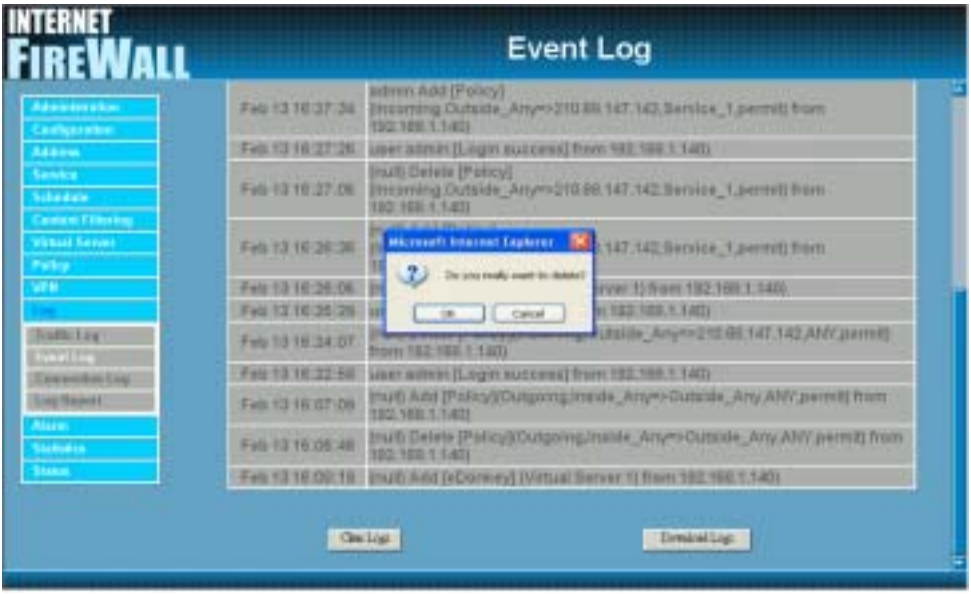


Clearing the Event Logs:

The Administrator may clear on-line event logs to keep just the most updated logs on the screen.

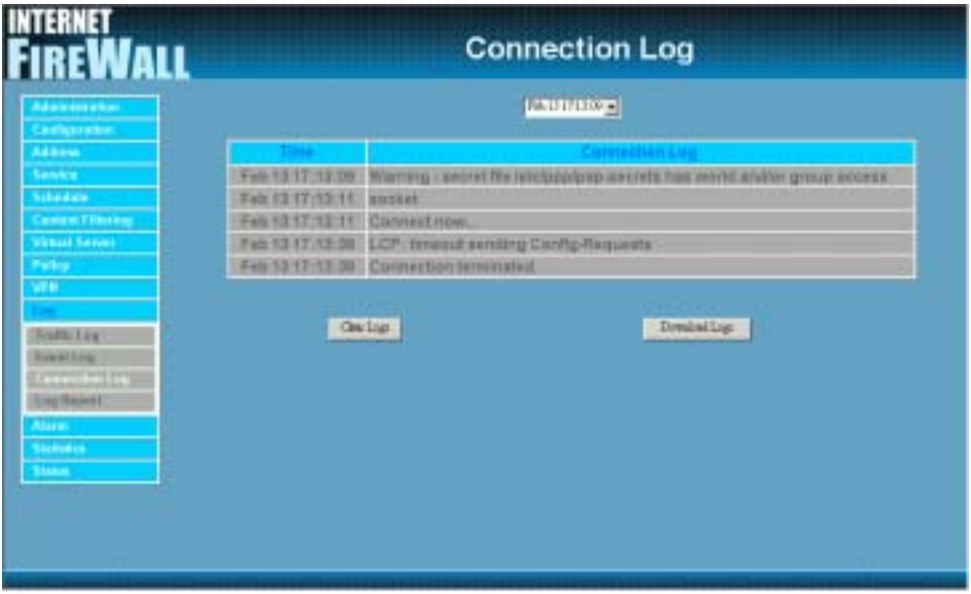
Step 1. In the Event Log window, click the Clear Logs button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **OK** to clear the logs or click **Cancel** to cancel it.



Connection Log

Click Log in the menu bar on the left hand side, and then select the sub-selection Connection Log.



Definition:

Time：The start and end time of connection.

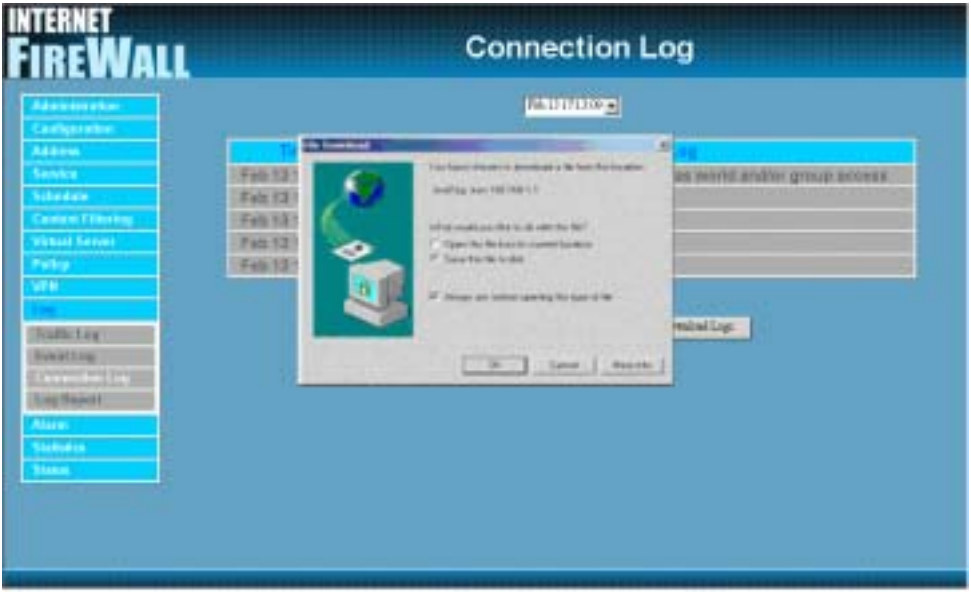
Connection Log：Event description during connection.

Download Logs

Step 1. Click **Log** in the menu bar on the left hand side and then select the sub-selection **Connection Log**.

Step 2. In Connection Log window, click the **Download Logs** button.

Step 3. In the Download Logs window, save the logs to the specified location.

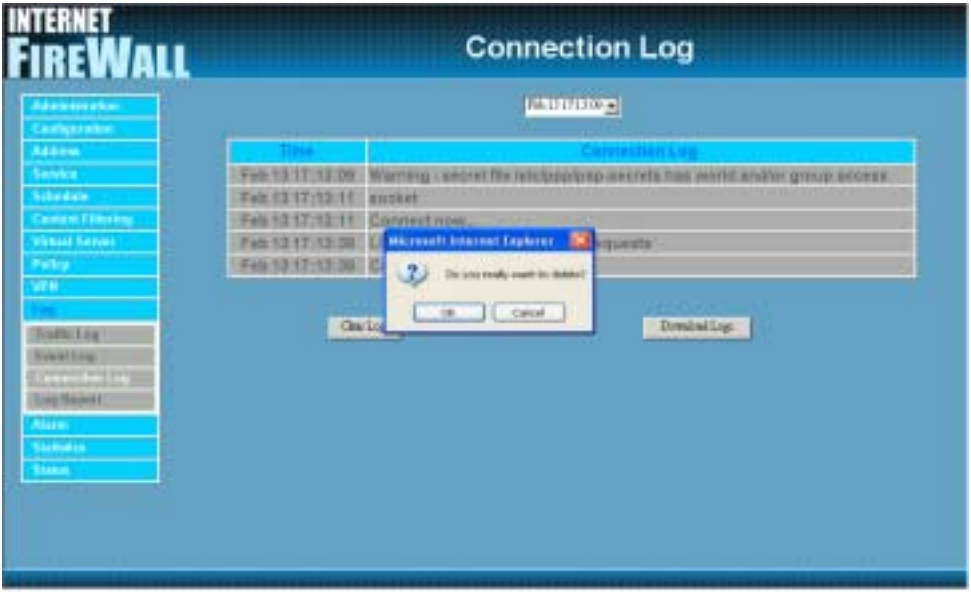


Clear Logs

Step 1. Click **Log** in the menu bar on the left hand side, and then select the sub-selection **Connection Logs**.

Step 2. In Connection Log window, click the **Clear Logs** button.

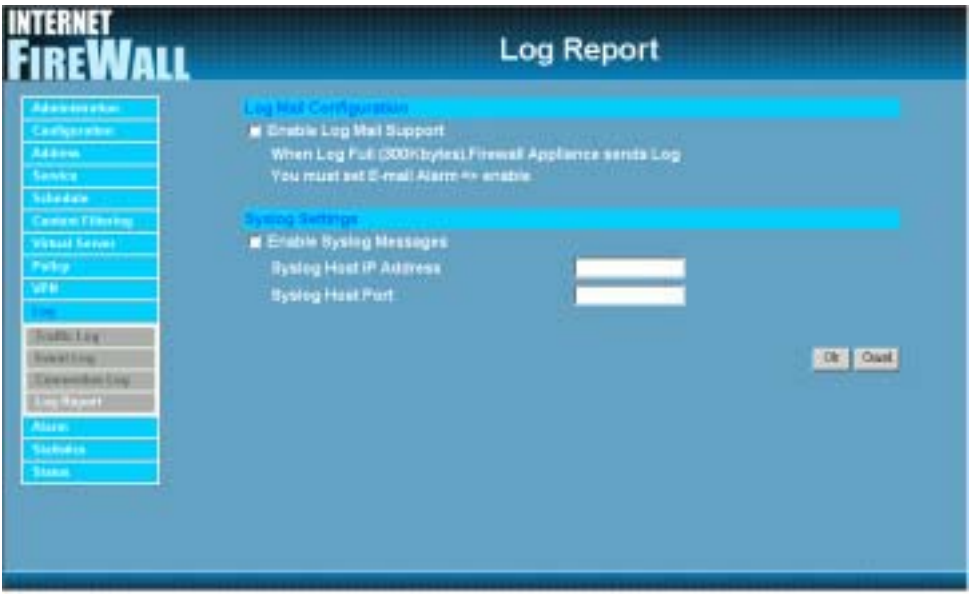
Step 3. In Clear Logs window, click **OK** to clear the logs or click **Cancel** to discard changes.



Log Report

The Log Report

Step 1. Click **Log →Log Report**.



Step 2. Log Mail Configuration：When the Log Mail files accumulated up to 300Kbytes, router will notify administrator by email with the traffic log and event log.。

***Note**: Before enabling this function, you have to enable E-mail Alarm in Administrator.*

Syslog Settings：If you enable this function, system will transmit the Traffic Log and the Event Log simultaneously to the server which supports Syslog function.

Enable Log Mail Support & Syslog Message

Log Mail Configuration /Enable Log Mail Support

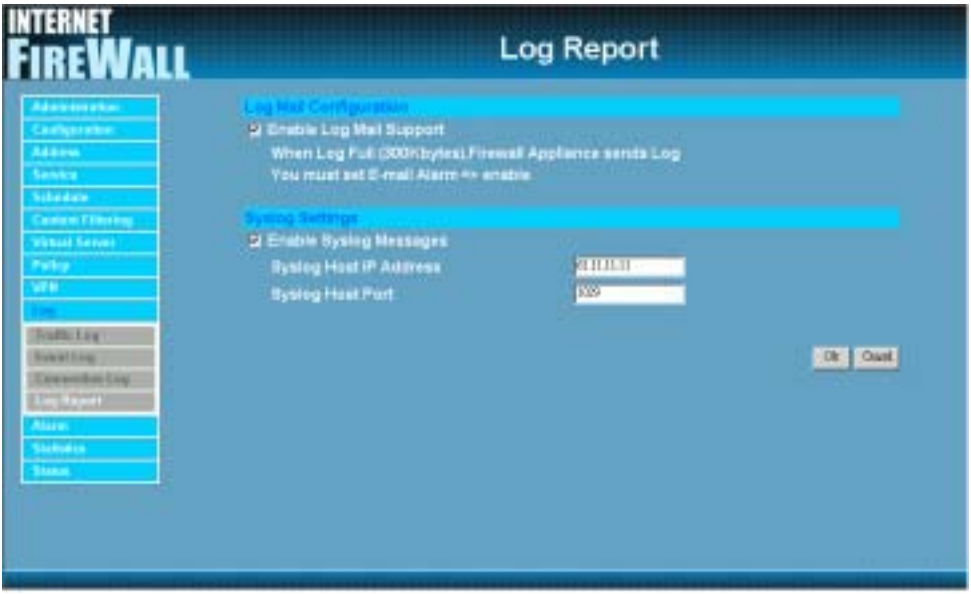
Step 1. Firstly, go to **Admin** –Select **Enable E-mail Alert Notification** under **E-Mail Settings**. Enter the e-mail address to receive the alarm notification. Click **OK**.

Step 2. Go to **LOG →Log Report.** Check to enable **Log Mail Support.** Click **OK.**

System Settings/Enable Syslog Message

Step 3. Check to enable Syslog Message. Enter the Host IP Address and Host Port number to receive the Syslog message.

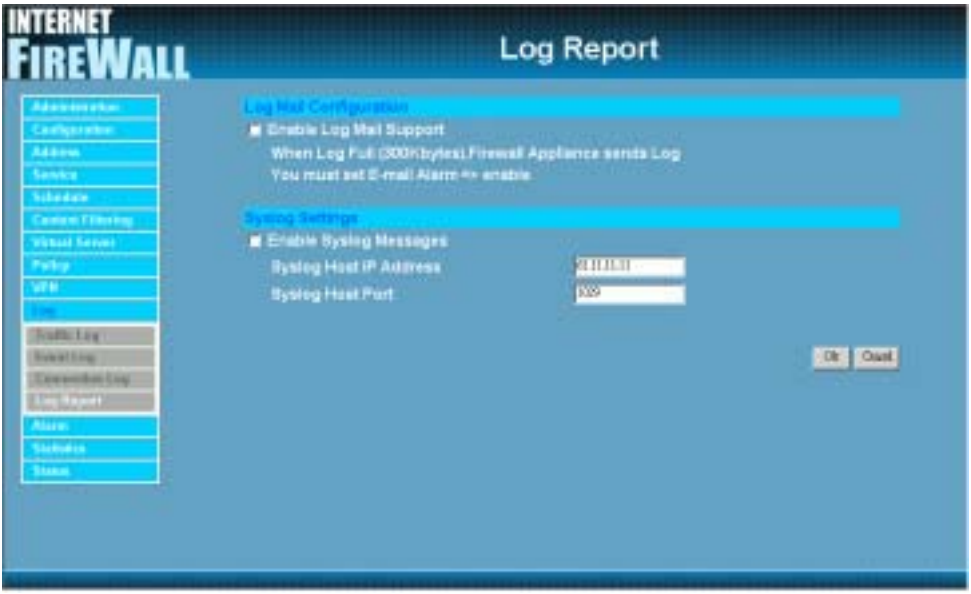
Step 4. Click **OK**.



Disable Log Mail Support & Syslog Message

Step 1. Go to **LOG →Log Report.** Uncheck to disable **Log Mail Support.** Click **OK.**

Step 2. Go to **LOG →Log Report.** Uncheck to disable **Settings Message.** Click **OK.**



Alarm

In this chapter, the Administrator can view traffic alarms and event alarms that occur and the firewall has logged.
Firewall has two alarms: **Traffic Alarm** and **Event Alarm**.

Traffic alarm:

In control policies, the Administrator set the threshold value for traffic alarm. The System regularly checks whether the traffic for a policy exceeds its threshold value and adds a record to the traffic alarm file if it does.

Event alarm:

When Firewall detects attacks from hackers, it writes attacking data in the event alarm file and sends an e-mail alert to the Administrator to take emergency steps.

Traffic Alarm

Entering the Traffic Alarm window:

Click the **Traffic Alarm** option below **Alarm** menu to enter the Traffic Alarm window.

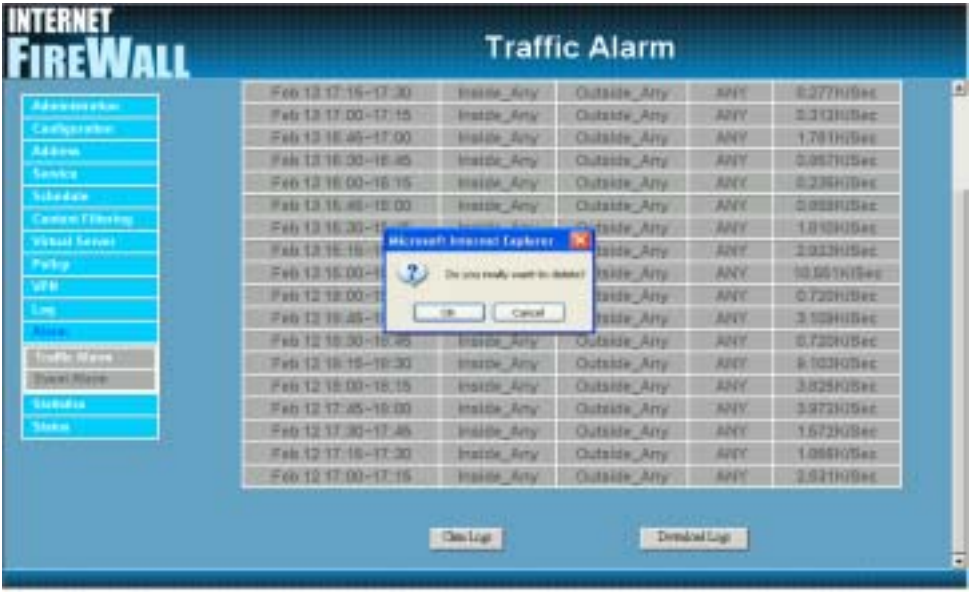
The table in the Traffic Alarm window displays the current traffic alarm logs for connections.

- **Time:** The start and stop time of the specific connection.
- **Source:** Name of the source network of the specific connection.
- **Destination:** Name of the destination network of the specific connection.
- **Service:** Service of the specific connection.
- **Traffic:** Traffic (in Kbytes/Sec) of the specific connection.

Clearing the Traffic Alarm Logs:

Step 1. In the Traffic Alarm window, click the Clear Logs button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **Ok** to clear the logs or click **Cancel** to cancel.

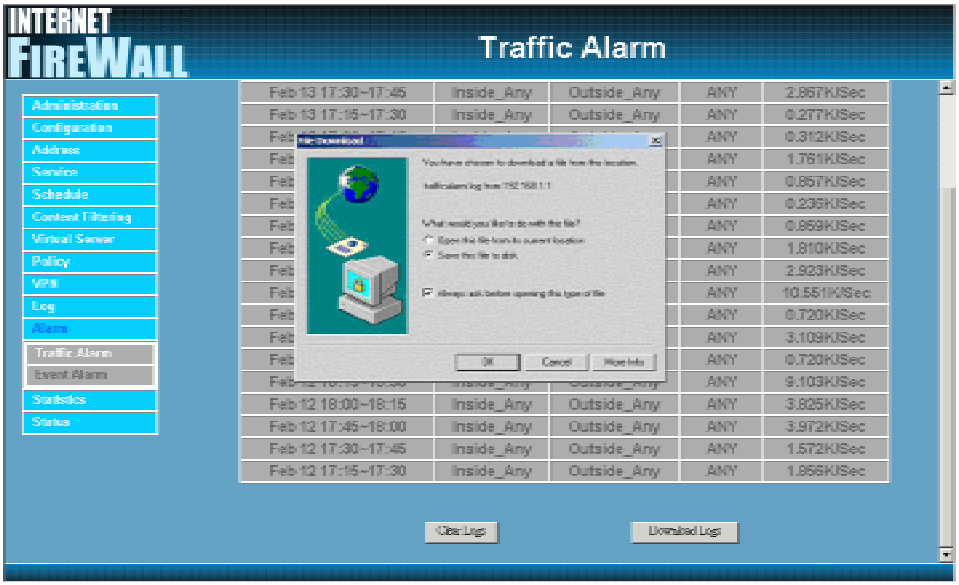


Downloading the Traffic Alarm Logs:

The Administrator can back up traffic alarm logs regularly and download it to a file on the computer.

Step 1. In the Traffic Alarm window, click the Download Logs button on the bottom of the screen.

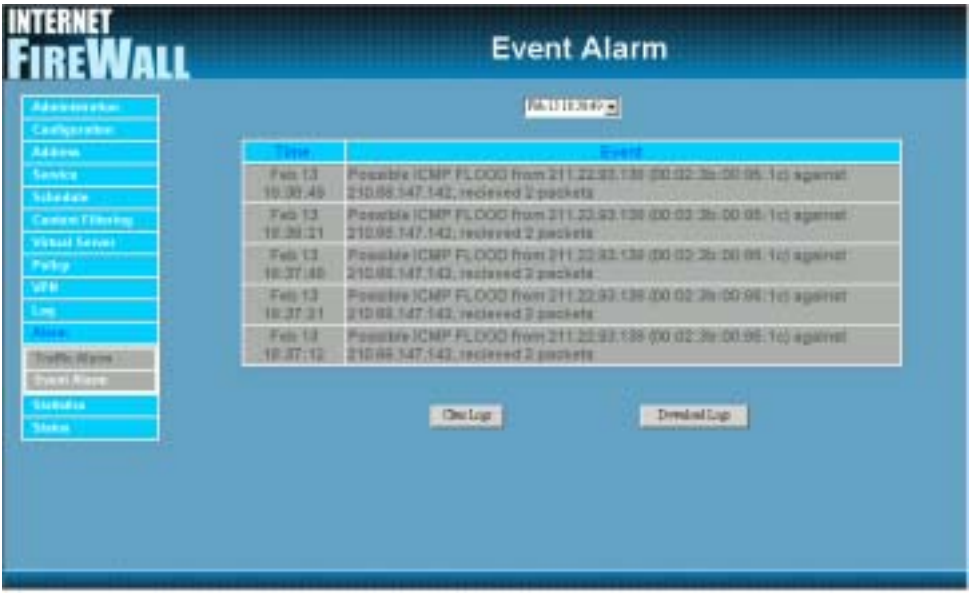
Step 2. Follow the File Download pop-up box to save the traffic alarm logs into specific directory on the hard drive.



Event Alarm

Entering the Event Alarm window:

Click the **Event Alarm** option below the **Alarm** menu to enter the Event Alarm window.



The table in Event Alarm window displays current traffic alarm logs for connections.

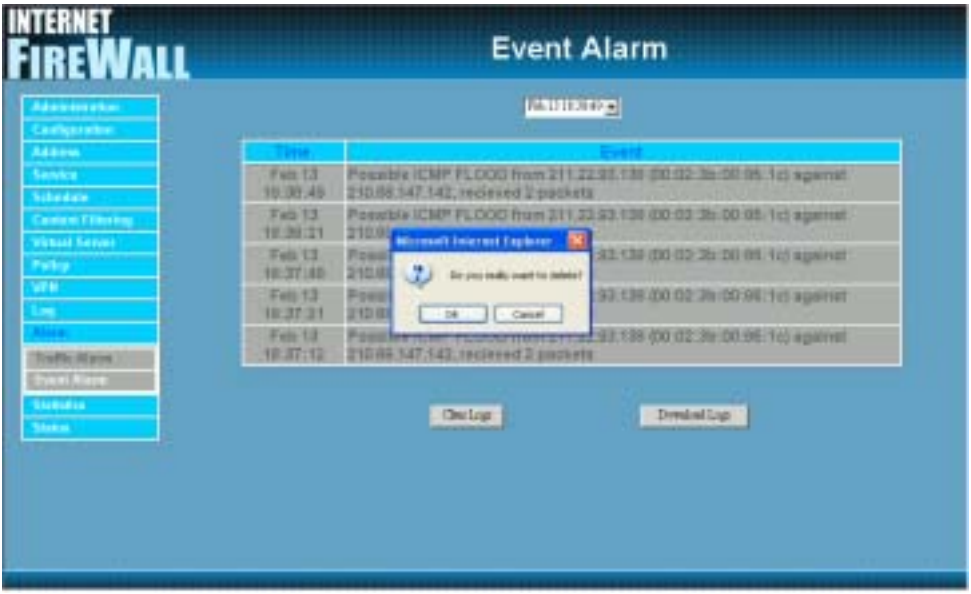
- **Time:** log time.
- **Event:** event descriptions.

Clearing Event Alarm Logs:

The Administrator may clear on-line logs to keep the most updated logs on the screen.

Step 1. In the Event Alarm window, click the Clear Logs button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **OK**.

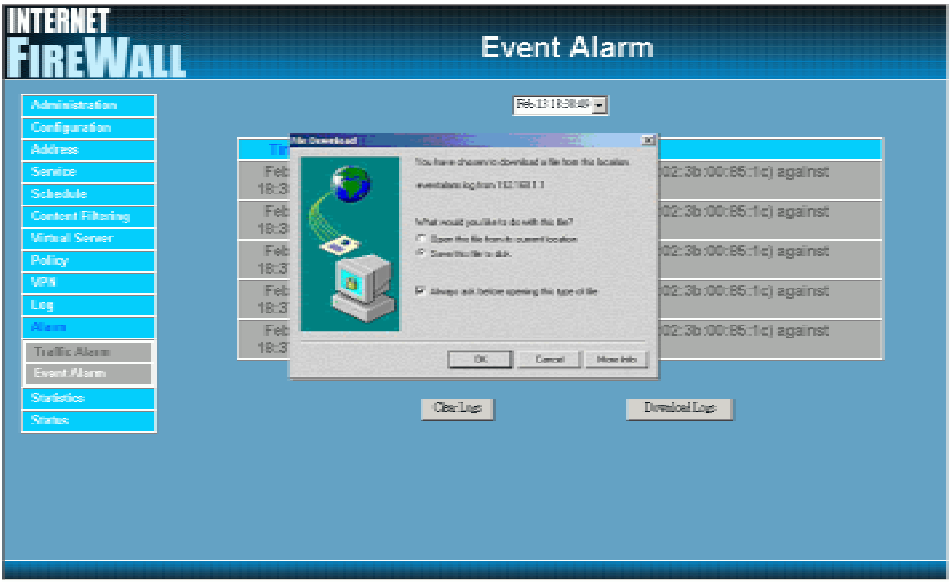


Downloading the Event Alarm Logs:

The Administrator can back up event alarm logs regularly by downloading it to a file on the computer.

Step 1. In the Event Alarm window, click the Download Logs button at the bottom of the screen.

Step 2. Follow the File Download pop-up box to save the event alarm logs into specific directory on the hard drive.



Statistics

In this chapter, the Administrator queries the VPN Firewall for statistics of packets and data which passes across the VPN Firewall. The statistics provides the Administrator with information about network traffics and network loads.

What is Statistics

Statistics are the statistics of packets that pass through the VPN Firewall by control policies setup by the Administrator.

How to use Statistics

The Administrator can get the current network condition from statistics, and use the information provided by statistics as a basis to mange networks.

WAN Statistics

Step 1. Click Statistics in the menu bar on the left hand side, and then select WAN Statistics.

Step 2. The WAN Statistics will be displayed.

Entering the Statistics window by Time

The Statistics window displays the statistics of network connections (downstream and upstream as well) by minute, hour, or day.

WAN Interface : Displays statistics of WAN network connections (downstream and upstream as well) in a total amount by minute, hour or day.

Step 1. Click **Statistics** in the menu bar on the left hand side, and then select **WAN Statistics**.

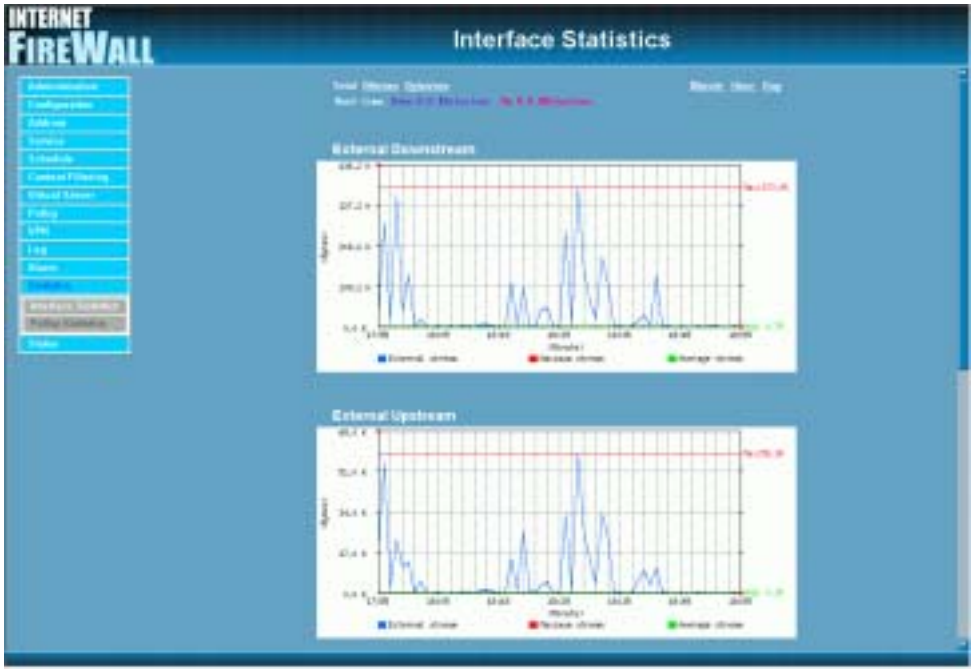
Step 2. In Statistics window, find the domain name you want to view.

Step 3. In the Statistics window, find the network you want to view and click Minute on the right hand side, and then you will be able to view the Statistics figure every minute; click Hour to view the Statistics figure every hour; click Day to view the Statistics figure every day.

Real-Time: Real display Download speed (KBytes/Sec) and Upload speed (KBytes/Sec)

Y-Coordinate：Network Traffic（Kbytes/Sec）.

X-Coordinate：Time（Hour/Minute/Day）.



Policy Statistics

Entering the Statistics window

Step 1. The Statistics window displays the statistics of current network connections.

- **Source:** the name of source address.
- **Destination:** the name of destination address.
- **Service:** the service requested.
- **Action:** permit or deny
- **Time:** viewable by minutes, hours, or days

Entering the Policy Satistics

Step 1. Click **Statistics** in the menu bar on the left hand side, and then select **WAN Statistics**.

Step 2. In Statistics window, find the domain name you want to view

Step 3. In the Statistics window, find the network you want to view and click Minute on the right hand side, and then you will be able to view the Statistics figure every minute; click Hour to view the Statistics figure every hour; click Day to view the Statistics figure every day.

Real-Time: Real display Download speed (KBytes/Sec) and Upload speed (KBytes/Sec)
Y-Coordinate：Network Traffic（Kbytes/Sec）.
X-Coordinate：Time（Hour/Minute/Day）.

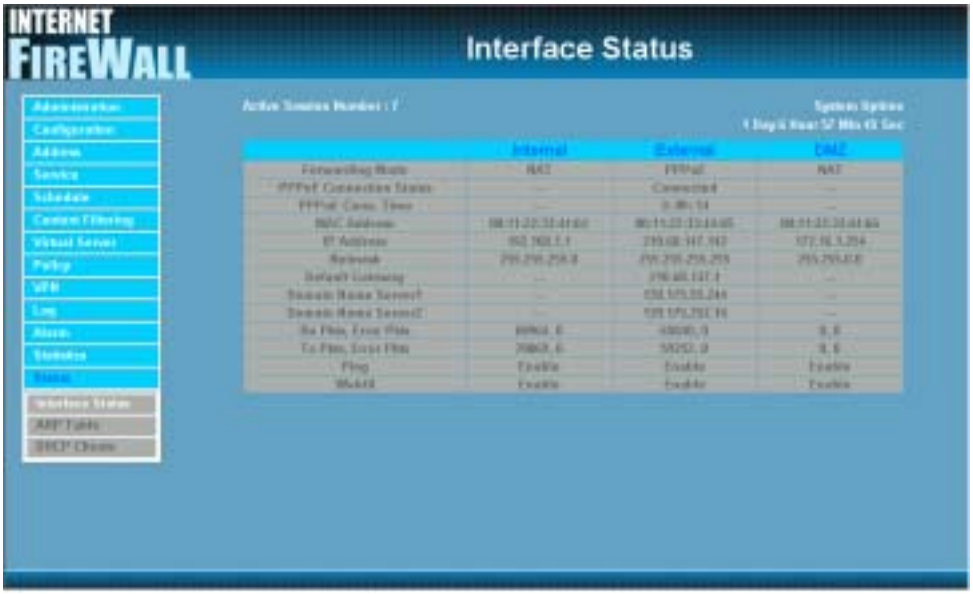
Status

In this section, the VPN Firewall displays the status information about the Firewall. Status will display the network information from the Configuration menu. The Administrator may also use Status to check the DHCP lease time and MAC addresses for computers connected to the Firewall.

Interface Status

Entering the Interface Status window:

Click on **Status** in the menu bar, then click **Interface Status** below it. A window will appear providing information from the **Configuration** menu. **Interface Status** will list the settings for **Internal Interface, External Interface, and the DMZ Interface.**



ARP Table

Entering the ARP Table window:

Click on **Status** in the menu bar, then click **ARP Table** below it. A window will appear displaying a table with IP addresses and their corresponding MAC addresses. For each computer on the Internal, External, and DMZ network that replies to an ARP packet, the VPN Firewall will list them in this ARP table.

IP Address: The IP address of the host computer
MAC Address: The MAC address of that host computer
Interface: The port that the host computer is connected to (Internal, External, DMZ)

DHCP Clients

Entering the DHCP Clients window:

Click on **Status** in the menu bar, then click on **DHCP Clients** below it. A window will appear displaying the table of DHCP clients that are connected to the VPN. The table will list host computers on the Internal network that obtain its IP address from the Firewall's DHCP server function.

IP Address: the IP address of the internal host computer
MAC Address: MAC address of the internal host computer
Leased Time: The Start and End time of the DHCP lease for the internal host computer.

Setup Examples

Example 1: Allow the Internal network to be able to access the Internet

Example 2: The Internal network can only access Yahoo.com website

Example 3: Outside users can access the internal FTP server through Virtual Servers

Example 4: Install a server inside the Internal network and have the Internet (External) users access the server through IP Mapping ----------

Please see the explanation of the examples below:

Example 1: Allow the Internal network to be able to access the Internet

Step 1 Enter the Outgoing window under the Policy menu.

Step 2 Click the New Entry button on the bottom of the screen.

Step 3 In the Add New Policy window, enter each parameter, then click OK.

Step 4 When the following screen appears, the setup is completed.

Example 2: The Internal network can only access 61.11.11.11 website.

Step 1. Enter the External window under the Address menu.

Step 2. Click the New Entry button.

Step 3. In the Add New Address window, enter relating parameters.

Step 4. Click **OK** to end the address table setup.

Step 5. Go to the Outgoing window under the Policy menu.

Step 6. Click the New Entry button.

Step 7. In the Add New Policy window, enter corresponding parameters. Click **OK**.

Step 8. When the following screen appears, the setup is completed.

Example 3: Outside users can access the internal FTP server through Virtual Servers

Step 1. Enter Virtual Server under the Virtual Server menu.

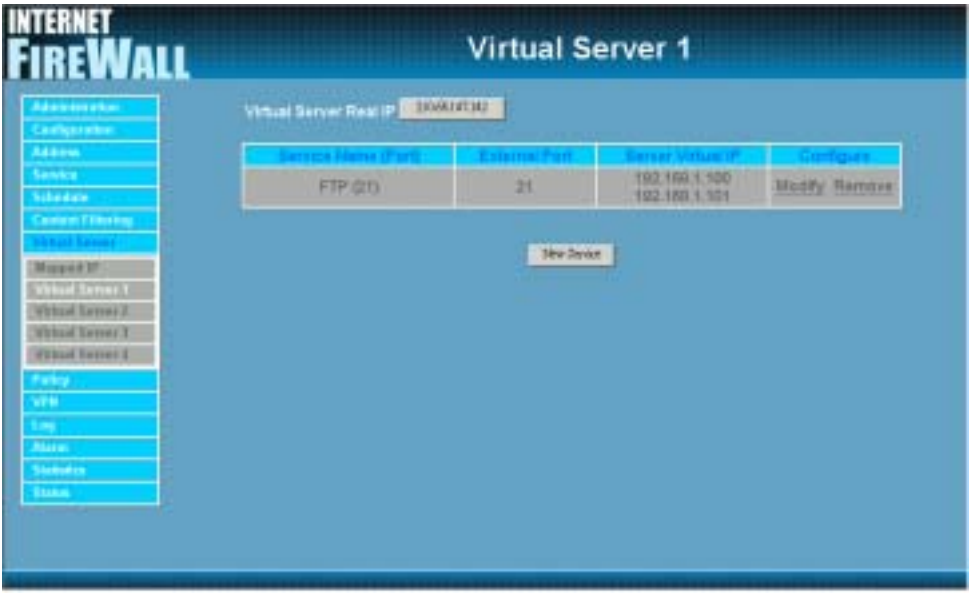
Step 2. Click the click here to configure button.

Step 3. Select an External IP address, then click OK.

Step 4. Click the New Service button on the bottom of the screen.

Step 5. Add the FTP service pointing to the internal server IP address. Click OK.

Step 6. A new Virtual Service should appear.



Step 7. Go to the Incoming window under the Policy menu, then click on the New Entry button.

Step 8. In the Add New Policy window, set each parameter, then click OK.

Step 9. An Incoming FTP policy should now be created.

Example 4: Install a server inside the Internal network and have the Internet (External) users access the server through IP Mapping

Step 1. Enter the Mapped IP window under the Virtual Server menu.

Step 2. Click the New Entry button.

Step 3. In the Add New IP Mapping window, enter each parameter, and then click OK.

Step 4. When the following screen appears, the IP Mapping setup is completed.

Step 5. Go to the Incoming window under the Policy menu.

Step 6. Click the New Entry button.

Step 7. In the Add New Policy window, set each parameter, then click OK.

Step 8. Open all the services. (ANY)

Step 9. The setup is completed.