Chapter 12

VPN

To obtain a private and secure network link, the NUS-MH300 is capable of establishing VPN connections. When used in combination with remote client authentication, it links the business' remote sites and users, conveniently provides the enterprise with an encrypted network communication method. By allowing the enterprise to utilize the Internet as a means of transferring data across the network, it forms one of the most effective and secure options for enterprises to adopt in comparison to other methods.

IPSec Autokey:

An IT administrator can create an encrypted connection between two remote sites using the Internet Key Exchange (IKE) protocol. It provides a standard method for negotiating key exchanges between two remote sites. To further enhance the security of the connection, IPSec Lifetime specifies the time before a new randomly generated session key needs to be created.

PPTP Server:

This guide will show how an IT administrator can configure the VPN-PPTP server settings.

PPTP Client:

This guide will show how an IT administrator can configure the VPN-PPTP client settings.

Tunnel:

In this chapter the IT administrator can apply the relevant VPN polices to its functions.

How is a VPN connection setup?

To establish a VPN connection, the **IPSec Autokey**, **PPTP server** or **PPTP client** connection settings need to be applied to a **Tunnel**. Policies can then be incorporated to ensure a secure connection.

Common VPN Terms:

RSA:

- Is an asymmetric cryptography system whereby a public and private key are used. Data is encrypted using a public key which is made freely available to everyone. A private key, which is kept secret, is then used to decrypt the data.

Preshared Key:

- During IPSec connections, a preshared key containing a string of Unicode characters is requested to allow the Layer Two Tunneling Protocol (L2TP) authentication processes to begin**.**

ISAKMP (Internet Security Association Key Management Protocol):

- Internet Security Association Key Management Protocol (ISAKMP) is a protocol for establishing Security Associations (SA) and cryptographic keys in an Internet environment. SA is the establishment of shared security information between two network entities to support secure communication, designating the algorithm, key length or encryption key. Note particularly that establishing an ISAKMP SA requires designating the encryption algorithm and the authentication method.

Main mode:

- The device can use either main mode or aggressive mode to establish SAs in the IKE process. Main mode, in comparison to Aggressive mode, is more time consuming due to more packets (six) being exchanged between peers during authentication, but provides a higher level of security.

Aggressive mode:

- Aggressive mode, an alternative for main mode functions, is completed using only three messages instead of the six used in main mode. By encrypting the identity with the peer's public key, it provides identity protection.

AH (Authentication Header):

- AH is intended to guarantee connectionless integrity and data origin authentication of IP datagram.

ESP (Encapsulating Security Payload):

- One of the IPSec protocols that provides encryption, authentication or both.

DES (Data Encryption Standard):

- DES, an acronym for Data Encryption Standard, is a cipher that was selected by NIST (National Institute of Standard and Technology), using a 56-bit key for encryption.

Triple-DES (3DES):

- 3DES, an acronym for Triple Data Encryption Standard, providing significantly enhanced security by executing the core DES algorithm three times in a row, is more difficult to break than DES, using a 168-bit key size.

AES (Advanced Encryption Standard):

- AES, an acronym for Advanced Encryption Standard, is more difficult to break than DES. The DES encryption key is 56 bits long; on the contrary, AES keys can be 128, 192 or 256 bits long.

NULL Algorithm:

- The NULL algorithm can be used instead of ESP encryption to provide a fast and convenient connection mode but without any security.

SHA-1 (Secure Hash Algorithm-1):

- A message-digest hash algorithm that takes a message less than 264 bits and produces a 160-bit digest.

MD5:

- MD5 is a common message digest algorithm that produces a 128-bit message digest from an arbitrary length input.

GRE

- The GRE (Generic Routing Encapsulation) only encapsulates packets and is therefore prone to attacks and monitoring. However, when combined with the encryption from IPSec, it helps form a secure connection.

One-Step IPSec Headings:

One-Step IPSec:

- All it takes is just one step to complete all the required IPSec by entering the data below:
  - Go to **VPN** > **One-Step IPSec** and enter the following data: ***(Figure 1)***
  - .In the **Name** field, enter a name for the VPN connection.
  - Next to the **Subnet / Mask** category, select **LAN.**
  - In the **Remote Gateway – Fixed IP or Domain Name** field, enter:
  - In the **Subnet / Mask** field, enter the destination's subnet and subnet mask that packets will travel across the VPN to.
  - In the **Preshared Key** field, enter the preshared key.
  - Click **OK**. ***(Figure 2)***
  - **IPSec Autokey**, **Tunnel** and **Policy** settings will be automatically created by the device. ***(Figure 3,4,5,6)***

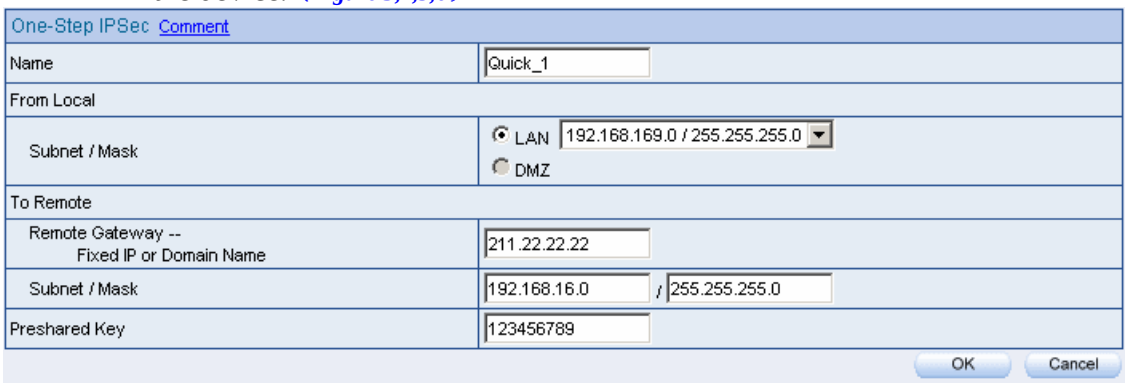

Figure 1 One-Step IPSec Settings Window

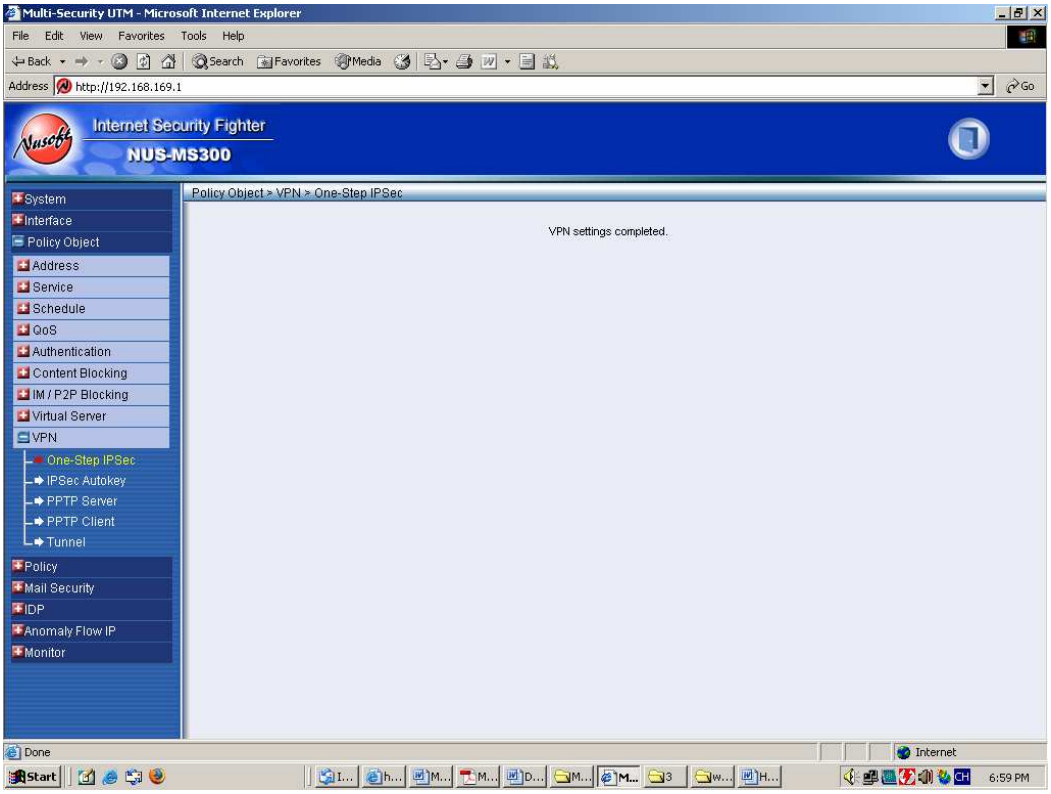

Figure 2 One-Step IPSec Settings Complete

i	Name	Gateway IP	IPSec Algorithm	Configure
	Quick_1	211.22.22.22	DES / MD5	In Use

New Entry

Figure 3 A New Entry is Automatically Created under VPN > IPSec Autokey

i	Name	Local Subnet	Remote Subnet	IPSec / PPTP	Configure
	Quick_1_T	192.168.169.0	192.166.16.0	Quick_1	In Use

New Entry

Figure 4 A New Entry is Automatically Created under VPN > Tunnel

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	To 1

New Entry

Figure 5 A New Entry is Automatically Created under Policy > Outgoing

Figure 6 A New Entry is Automatically Created under Policy > Incoming

One-Step IPSec automatically selects the following options to provide users with a quick method for establishing a VPN connection:

1) **Mode**: **Main mode**

2) **Authentication Method**: **Preshare**

3) **ISAKMP Algorithm**: **DES** + **MD5** + **Group 1**

4) **IPSec Algorithm**: **DES** + **MD5**

5) New entries for **IPSec Autokey**, **Tunnel** and **Policy** will automatically be created by the device.

IPSec Autokey Heading Meanings:

i:

- The heading name **i**, is used to represent the status of the VPN connection according to the following symbols:

Symbol	--		
Status	Not used	Disconnected	Connected

Name:

- A unique name used to identify the IPSec Autokey.

Remote Gateway – Fixed IP or Domain Name:

- The remote Gateway's WAN interface's IP address or domain name.

IPSec Algorithm :

- Indicates the VPN's current data encryption mode.

Modify/Remove:

- Click **Modify** to change the saved values of the saved IPSec Autokey; click **Remove** to delete the saved IPSec Autokey. *(Figure 7)*

Figure 7 IPSec Autokey WebUI

 NUS-MH300 will utilize its **Dead Peer Detection** mechanism by default to automatically create an IPSec VPN connection. IT administrators can operate the connection manually by checking the **Manual Connection** checkbox and entering a **Remote Gateway -- Fixed IP or Domain Name** address in the **To Remote** category.

PPTP Server Headings:

PPTP Server:

- The PPTP server can be set to either **Enable** or **Disable**.

Client IP Range:

- The range of PPTP Client IP address range can be set here.

i:

- The heading name **i**, is used to represent the status of the VPN connection according to the following symbols:

Symbol	--		
Status	Not used	Disconnected	Connected

User Name:

- This heading displays the PPTP Client's user name that will be used to connect to the PPTP Server.

Client IP:

- The client's IP address used when the PPTP client connects to the PPTP server.

Uptime:

- Displays the connection duration between the PPTP Server and Client.

Modify/Remove:

- Click **Modify** to change the saved PPTP VPN Server settings or click **Remove** to remove the saved PPTP Server settings. *(Figure 8)*

Figure 8 PPTP Server WebUI

 NUS-MH300 will utilize its **Echo-Request** mechanism by default to establish a PPTP connection. By enabling **Manual Disconnection,** IT administrators can disconnect the VPN connection to the PPTP server.

PPTP Client Heading Meanings

i:

- The heading name **i**, is used to represent the status of the VPN connection according to the following symbols:

Symbol	--		
Status	Not used	Disconnected	Connected

User Name:

- This heading displays the PPTP Client's user name that will be used to connect to the PPTP Server.

Server IP or Domain Name:

- Represents the PPTP server's IP address or domain name that the client uses to connect to the PPTP server.

Encryption:

- Displays **On** if encryption has been selected between the PPTP Client and PPTP Server.

Uptime:

- Displays the connection time between the PPTP Server and Client.

Configure:

- Click **Modify** to adjust the saved settings of the PPTP Client; click **Remove** to remove the saved settings. *(Figure 9)*

Figure 9 PPTP Client Fields

The NUS-MH300 automatically builds up VPN connections by Echo-Request. An IT administrator can also build up the PPTP VPN connection manually by checking the Manual Connect checkbox.

Tunnel Heading Meanings:

i:

- The heading name **i**, is used to represent the status of the VPN connection according to the following symbols:

Symbol	--		
Status	Not used	Disconnected	Connected

Name:

- A unique name used to identify the VPN tunnel.

Local Subnet:

- Displays the local subnet address.

Remote Subnet:

- Displays the remote subnet address.

IPSec / PPTP :

- Displays all the VPN tunnels（IPSec, PPTP Server, PPTP Client）in the VPN tunnel.

Configure:

- Click **Modify** to adjust the settings of the VPN Tunnel; click **Remove** to remove the saved settings. ***(Figure 10)***

Figure 10 VPN Tunnel Web UI

Six different VPN examples have been provided below:

No.	VPN Type	Scenario	Page
Example 1	**IPSec Autokey**	Setting up an IPSec VPN connection between two NUS-MH300 devices	
Example 2	**IPSec Autokey**	Setting up an IPSec VPN connection using a single NUS-MH300 and Windows 2000	
Example 3	**IPSec Autokey**	Setting up an IPSec VPN connection (under Aggressive mode) between two NUS-MH300 devices. (3DES encryption and MD5 authentication)	
Example 4	**IPSec Autokey**	Setting up an IPSec VPN connection between two NUS-MH300 devices. (ISAKMP 3DES encryption and MD5 authentication) (IPSec 3DES encryption and MD5 Authentication) (GRE Packet Encapsulation)	
Example 5	**PPTP**	Setting up a PPTP VPN connection between two NUS-MH300 devices	
Example 6	**PPTP**	Setting up a PPTP VPN connection using a single NUS-MH300 and Windows 2000	

VPN Example 1

Setting up an IPSec VPN Connection between Two NUS-MH300 Devices

Scenario:

Company A **WAN IP: 61.11.11.11** **LAN IP: 192.168.10.X**
Company B **WAN IP: 211.22.22.22** **LAN IP: 192.168.20.X**
Multiple Subnet: 192.168.85.X

This example is based upon the use of two NUS-MH300 devices. In this scenario, Company A's internal user, 192.168.10.100, requires to create a VPN connection with Company B's internal user, 192.168.20.100, for file sharing.

The LAN IP, 192.168.10.1, is the default gateway of Company A's NUS-MH300. Proceed with the following steps:

Step 1. From within a browser, enter Company A's NUS-MH300 LAN IP address, 192.168.10.1. Go to **Policy Object** > **VPN** > **IPSec Autokey** then click on the **New Entry** button. *(Figure 11)*

Figure 11 IPSec Autokey Field Headings

Step 2. Under the **Necessary Item** category, in the **Name** field type **VPN_A**. *(Figure 12)*

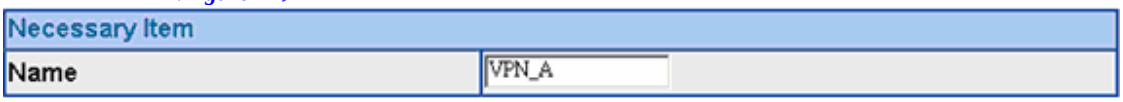

Figure 12 IPSec Autokey - Name Setting

Step 3. From within the **To Remote** category, select **Remote Gateway --Fixed IP or Domain Name**. In the field, enter the remote IP address to connect to Company B. *(Figure 13)*

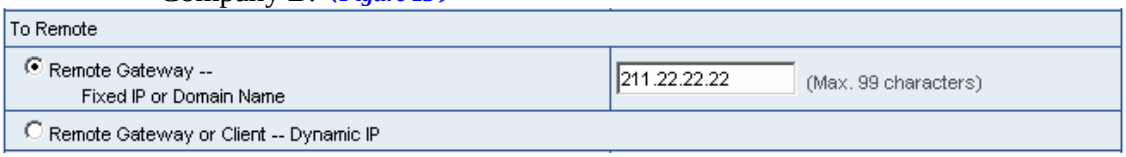

Figure 13 IPSec Autokey - To Remote Settings

Step 4. From the **Authentication Method** drop-down list, select **Preshare**. Enter the **Preshared Key** (a maximum of 103 characters). *(Figure 14)*

Figure 14 IPSec Autokey - Authentication Method Setting

Step 5. From within the **Encapsulation** category, **ISAKMP algorithms** (please refer to the Common VPN Terms section for an explanation) can be set. For the encryption algorithms, you are given choices from 3DES, DES and AES. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, you are given choices from MD5 and SHA1. Here, we have chosen **MD5** from the **Auth Algorithm** drop-down list. From the **Group** drop-down list **GROUP1.** Please note that both VPN sites have to choose the same group. *(Figure 15)*

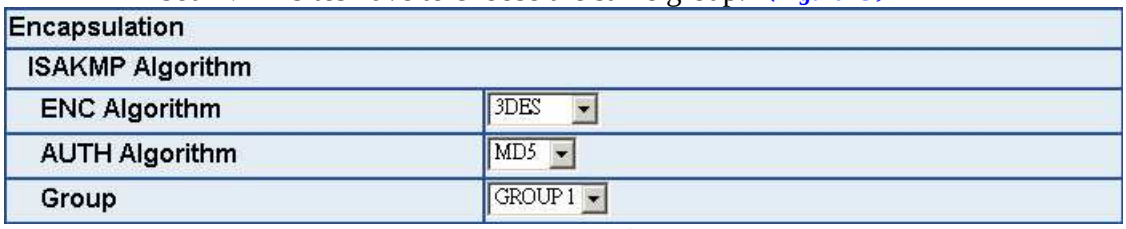

Figure 15 IPSec Encapsulation Setting

Step 6. From the **IPSec Algorithm** category**,** you can choose either **Data Encryption + Authentication** or **Authentication Only**.

Select **Data Encryption + Authentication**. For the encryption algorithms, you are given choices from 3DES, DES, AES-128, AES-192, AES-256 and NULL. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, **MD5** and **SHA1** are available. Choose **MD5** from the drop-down list. *(Figure 16)*

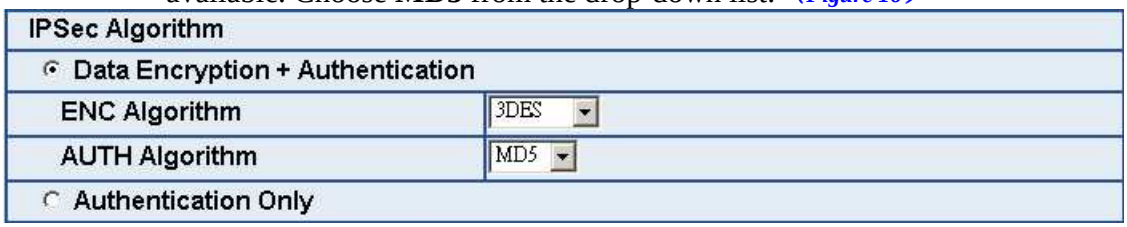

Figure 16 IPSec Algorithm Setting

Step 7. Under the **Optional Item** category, for **Perfect Forward Secrecy** select **GROUP1** from the drop-down list. For the **ISAKMP Lifetime** field, enter 3600. For the **IPSec Lifetime** field, enter 28800**.** Select the **Main mode** radio button in the **Mode** section. *(Figure 17)*

Figure 17 IPSec Autokey - Perfect Forward Secrecy Setting

Step 8. IPSec Autokey settings completed. *(Figure 18)*

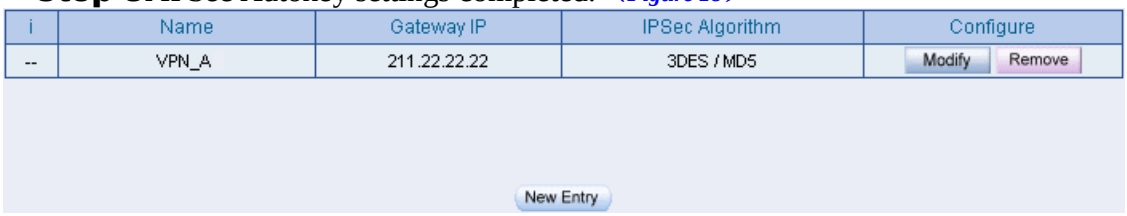

Figure 18 Company A IPSec Autokey – Settings Completed

Step 9. Go to **Policy Object** > **VPN** > **Tunnel**. Click on the **New Entry** button and then proceed with the following: *(Figure 19)*

- In the **Name** field, enter a unique name for the tunnel.
- For the **From Local** setting, select **LAN**.
- In the **Local Subnet / Mask** field, enter 192.168.10.0 / 255.255.255.0.
- From the **To Remote** category, select **To Remote Subnet / Mask** and enter 192.168.20.0 /255.255.255.0.
- From the **IPSec / PPTP Setting** drop-down list, select VPN_A.
- Check the **Show remote Network Neighborhood** checkbox.
- Click **OK**. *(Figure 20)*

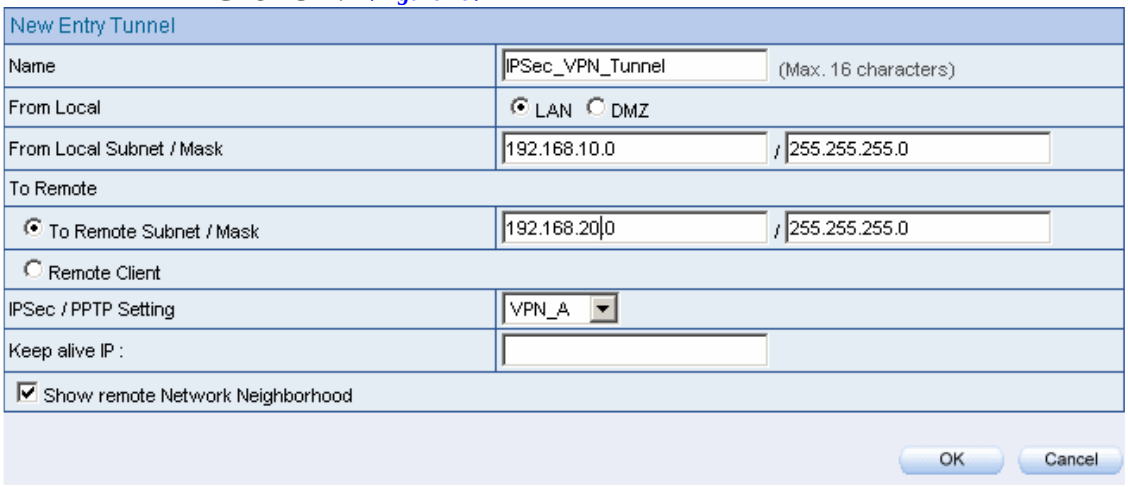

Figure 19 New Entry Tunnel Settings

Figure 20 New Entry Tunnel Settings Completed

Step 10. Go to **Policy** > **Outgoing** then click on the **New Entry** button and configure as below: *(Figure 21)*

- **Authentication User:** Select **All_NET**.
- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Tunnel:** Select **IPSec_VPN_Tunnel**.
- Click **OK**. *(Figure 22)*

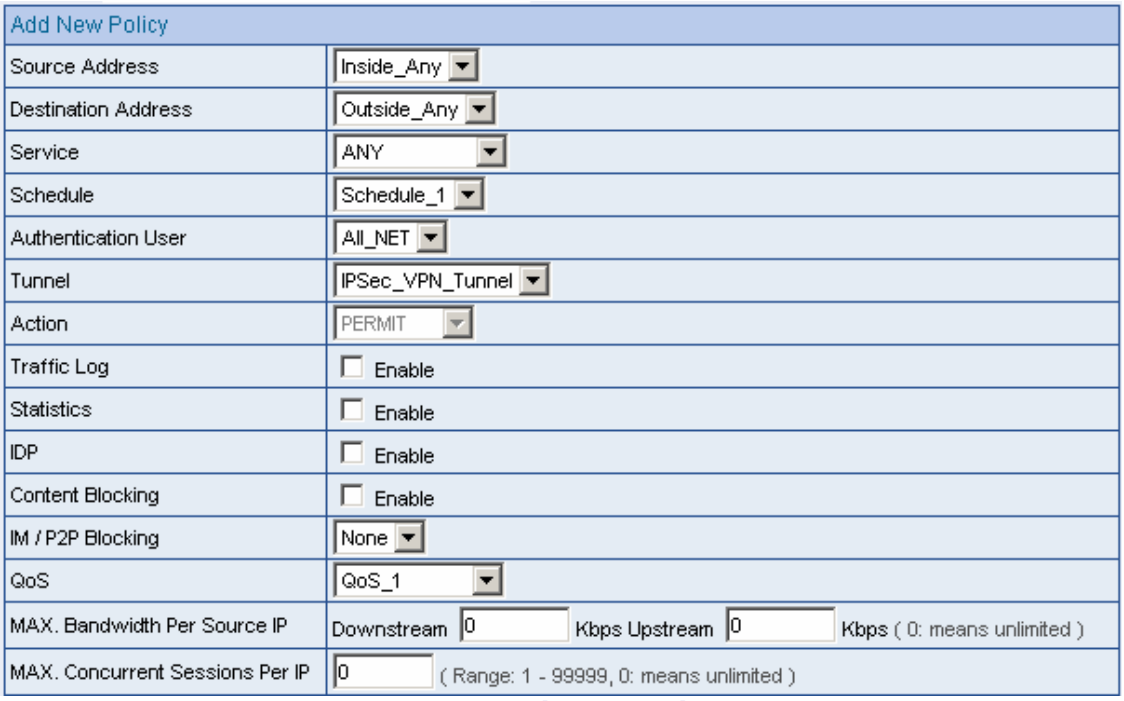

Figure 21 VPN Tunnel Outgoing Policy Settings

Figure 22 VPN Tunnel Outgoing Policy Settings Completed

Step 11. Go to **Policy** > **Incoming**, click on the **New Entry** button and enter the following settings: *(Figure 23)*

- **Schedule:** select Schedule_1.
- **QoS:** select QoS_1.
- **Tunnel:** select IPSec_VPN_Tunnel.
- Click **OK**. *(Figure 24)*

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Schedule_1
Tunnel	IPSec_VPN_Tunnel
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
NAT	Enable

Figure 23 VPN Tunnel Incoming Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove	To 1

New Entry

Figure 24 VPN Tunnel Incoming Policy Settings Completed

VPN Example 1

The LAN IP, 192.168.20.1, is the default gateway of Company B's NUS-MH300. Proceed with the following steps:

Step 1. From within a browser, enter Company B's default gateway IP address, 192.168.20.1. Go to **Policy Object** > **VPN** > **IPSec Autokey** then click on the **New Entry** button. *(Figure 25)*

Figure 25 IPSec Autokey Headings

Step 2. Under the **Necessary Item** category, in the **Name** field type VPN_B. *(Figure 26)*

Figure 26 IPSec Autokey Name Setting

Step 3. From within the **To Remote** category, select **Remote Gateway-Fixed IP or Domain Name** and enter the IP Address. *(Figure 27)*

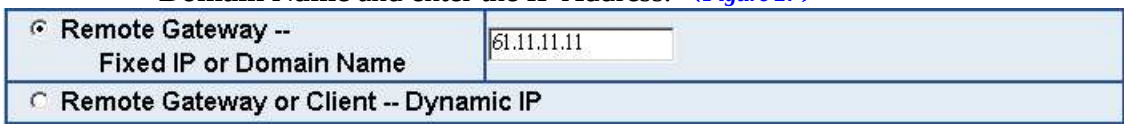

Figure 27 IPSec to Remote Settings

Step 4. From the **Authentication Method** drop-down list, select **Preshare**. Enter the **Preshared Key** (a maximum of 103 characters) *(Figure 28)*

Figure 28 IPSec Autokey - Authentication Method Setting

Step 5. From within the **Encapsulation** category, **ISAKMP algorithms** (please refer to the Common VPN Terms section for an explanation) can be set. For the encryption algorithms, you are given choices from 3DES, DES and AES. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, you are given choices from MD5 and SHA1. Here, we have chosen **MD5** from the **Auth Algorithm** drop-down list. From the **Group** drop-down list **GROUP1.** Please note that both VPN sites have to choose the same group. *(Figure 29)*

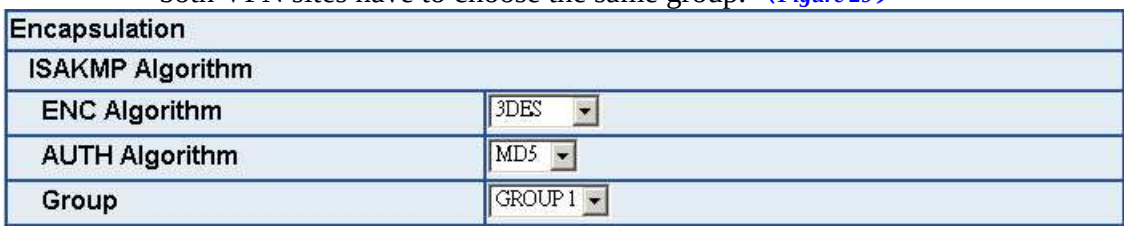

Figure 29 IPSec Encapsulation Settings

Step 6. From the **IPSec Algorithm** category, select **Data Encryption + Authentication**. From the **ENC Algorithm** drop-down list, select **3DES.** From the **AUTH Algorithm** drop-down list, select **MD5.** *(Figure 30)*

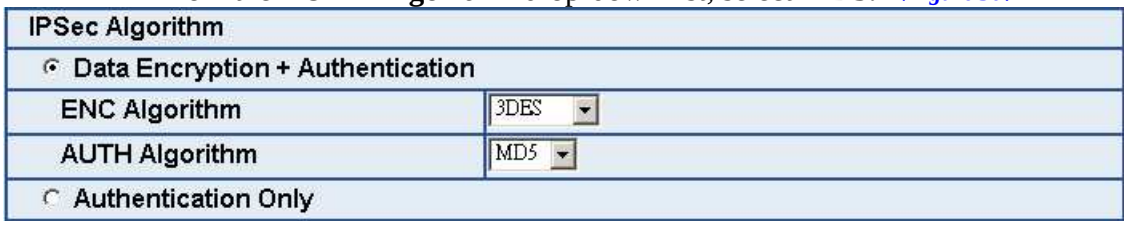

Figure 30 IPSec Algorithm Settings

Step 7. From the **Perfect Forward Secrecy** drop-down list, select **GROUP1**. In the **ISAKMP Lifetime** field, enter 3600 seconds. For the **IPSec Lifetime**, enter 28800 seconds. Select the **Main mode** radio button in the **Mode** section. *(Figure 31)*

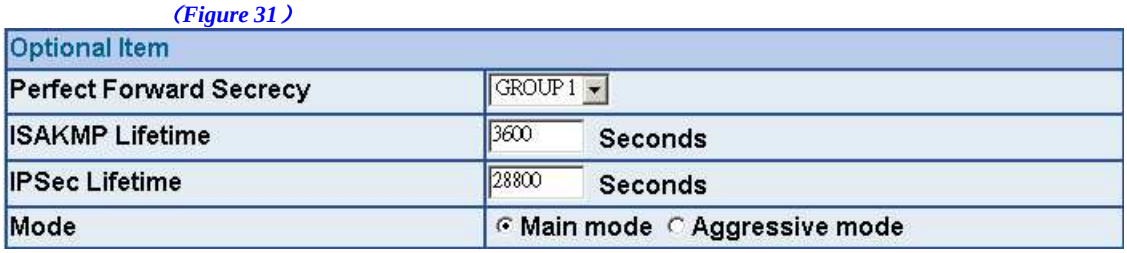

Figure 31 IPSec Perfect Forward Secrecy Settings

Step 8. IPSec Autokey settings completed. *(Figure 32)*

Figure 32 Company B IPSec Autokey Settings Completed

Step 9. Go to **Policy Object** > **VPN** > **Tunnel** and click on the **New Entry** button**.** Configure the following: *(Figure 33)*

- **Name:** enter a unique tunnel name.
- **From Local:** select **LAN**.
- **From Local Subnet / Mask:** enter 192.168.85.0 / 255.255.255.0.
- **To Remote:** select **To Remote Subnet / Mask.** Enter 192.168.10.0 /
- 255.255.255.0.
- **IPSec / PPTP Setting:** Select **VPN_B**.
- Check the **Show remote Network Neighborhood** checkbox.
- Click **OK**. *(Figure 34)*

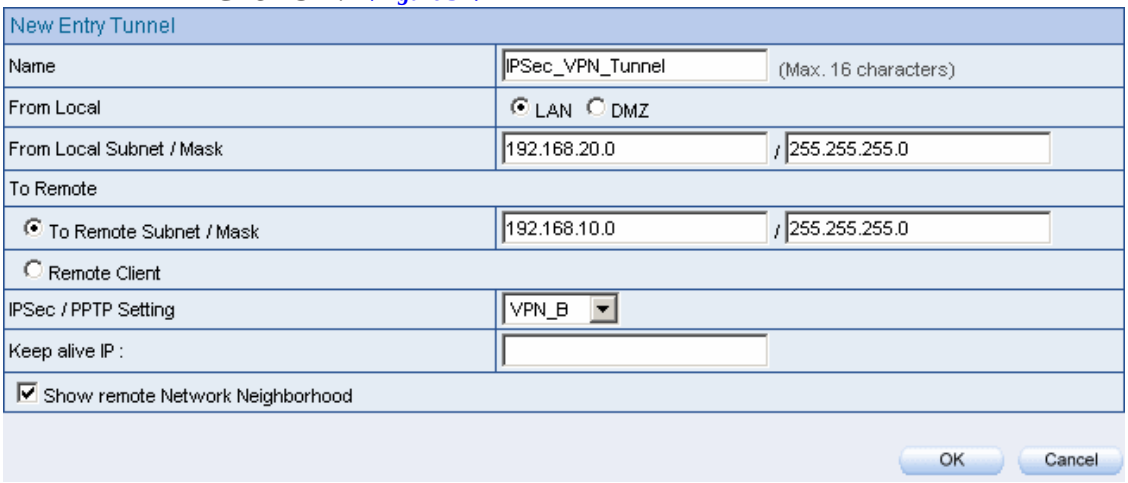

Figure 33 New Entry Tunnel Settings

Figure 34 New Entry Tunnel Settings Completed

Step 10. Go to **Policy** > **Outgoing** and click on the **New Entry** button. Enter the following settings: *(Figure 35)*

- **Authentication User:** Select **All_NET**.
- **Schedule:** Select **Schedule_1.**
- **QoS:** Select **QoS_1**.
- **Tunnel:** Select **IPSec_VPN_Tunnel**.
- Click **OK**. *(Figure 36)*

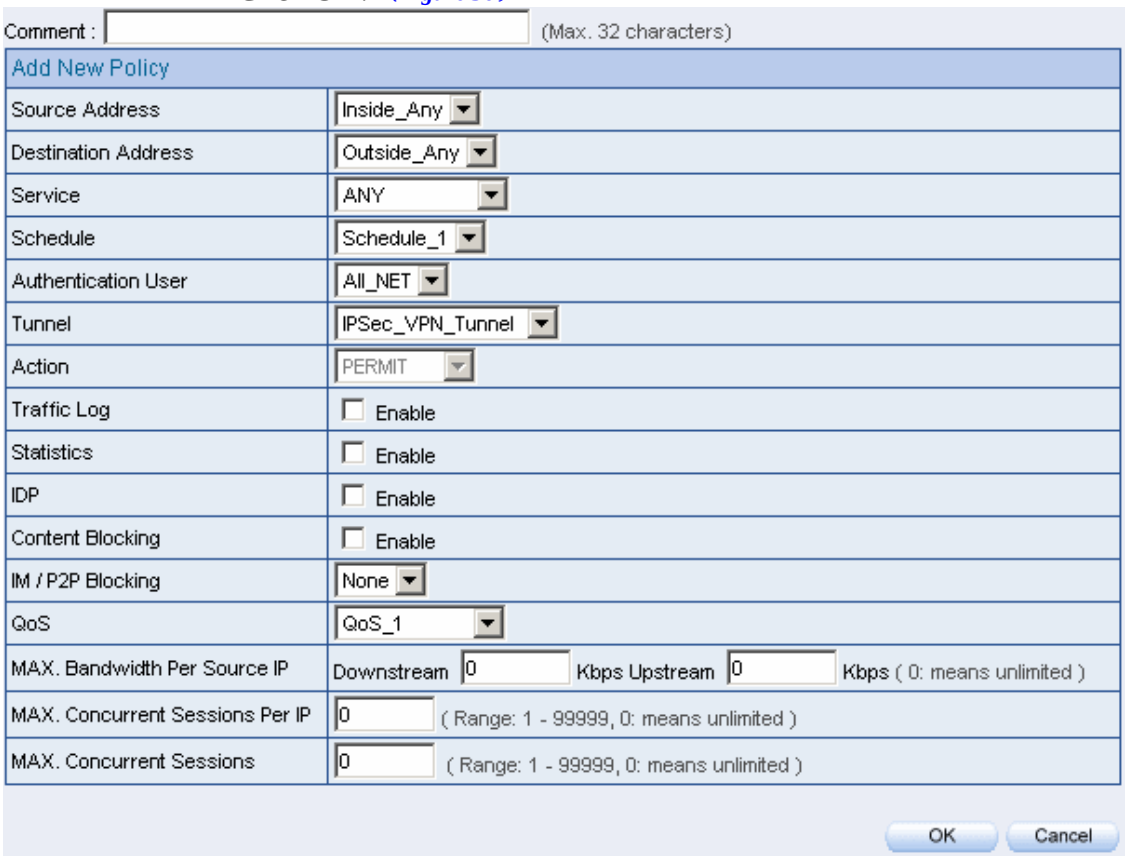

Figure 35 Setting the VPN Tunnel Outgoing Policy

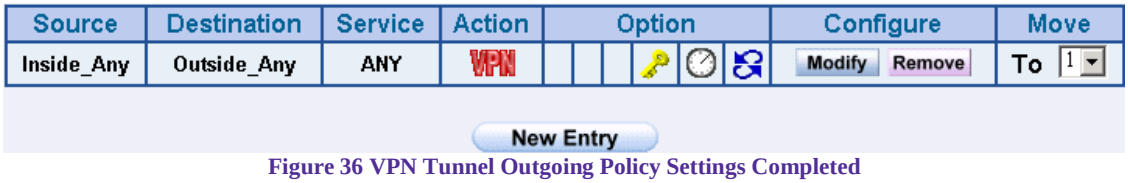

Figure 36 VPN Tunnel Outgoing Policy Settings Completed

Step 11. Go to **Policy** > **Incoming**, and click on the **New Entry** button. Configure the following: *(Figure 37)*

- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Tunnel:** Select **IPSec_VPN_Tunnel**.
- Click **OK**. *(Figure 38)*

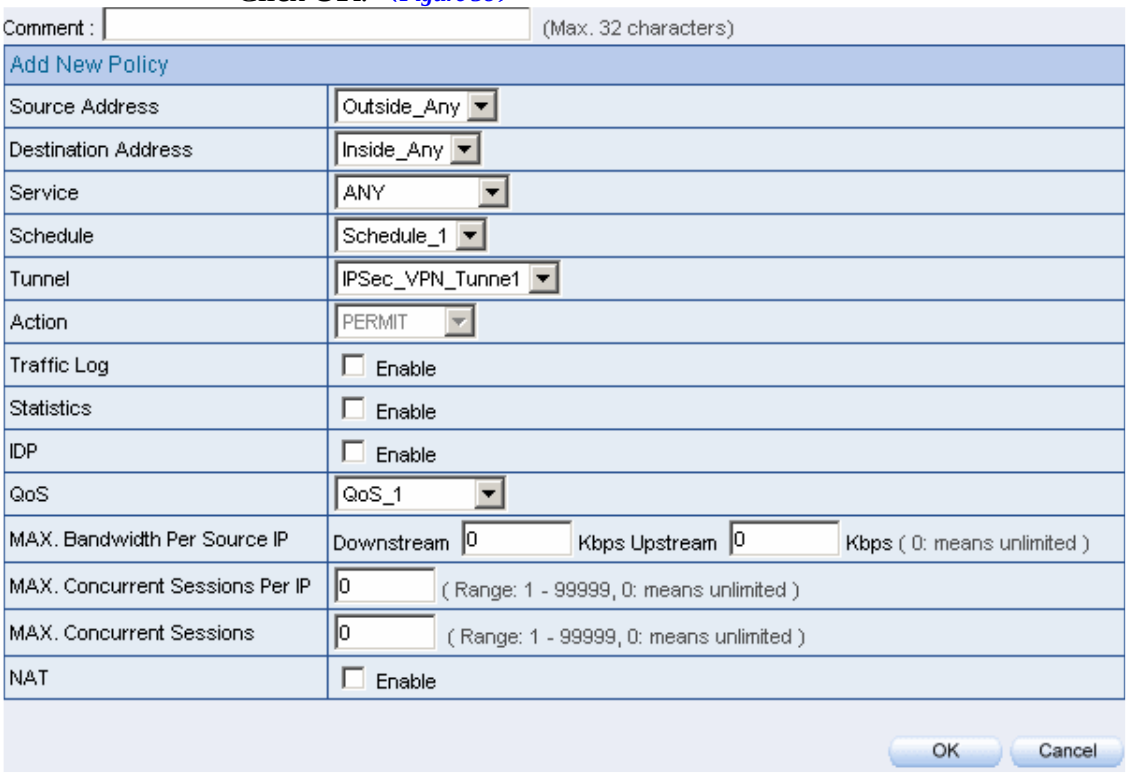

Figure 37 VPN Tunnel Incoming Policy Settings

Figure 38 VPN Tunnel Incoming Policy Settings Completed

Step 12. The completed IPSec VPN connection setup. *(Figure 39)*

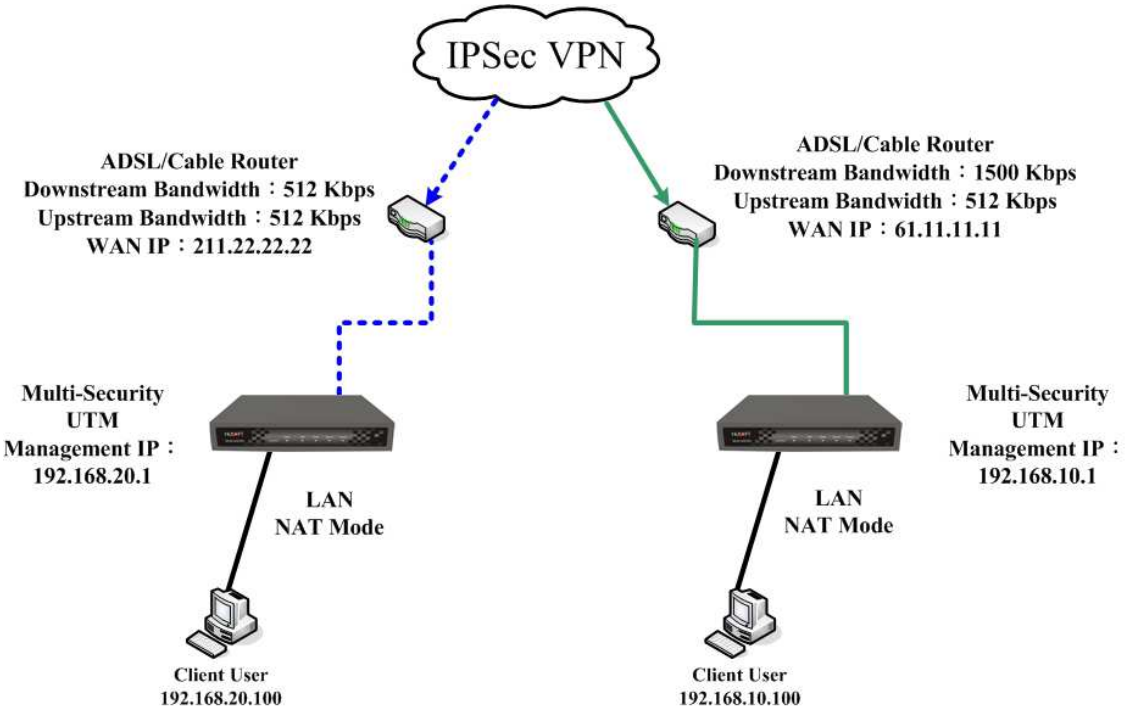

Figure 39 Completed Setup

Setting up an IPSec VPN Connection Using a Single NUS-MH300 and Windows 2000 PC

Scenario:

Company A:

- Using a NUS-MH300
- WAN IP: 61.11.11.11
- LAN IP: 192.168.10.X

Company B

- Using a Windows 2000 PC
- WAN IP: 211.22.22.22

In this example, the VPN-IPSec connection settings are for a single NUS-MH300 and a Windows 2000 PC. Supposing a user from company B, 211.22.22.22, wishes to establish a VPN connection with company A, 192.168.10.100, for accessing files.

The LAN IP, 192.168.10.1, is the default gateway of Company A's NUS-MH300. Proceed with the following steps:

Step 1. From within a browser, enter Company A's default gateway IP address, 192.168.10.1. Go to **Policy Object** > **VPN** > **IPSec Autokey** then click on the **New Entry** button. *(Figure 40)*

Figure 40 IPSec Autokey

Step 2. In the **Name** field, enter VPN_A. *(Figure 41)*

Figure 41 The IPSec VPN Name

Step 3. From within the **To Remote** category, select **Remote Gateway or Client --- Dynamic IP**. *(Figure 42)*

Figure 42 The IPSec To Remote Setting

Step 4. From within the **Authentication Method** drop-down list, select **Preshare** and enter the **Preshared Key** (The maximum **Preshared Key** length is 103 characters). *(Figure 43)*

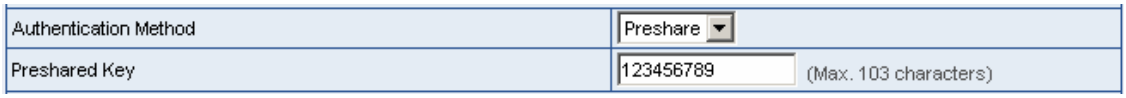

Figure 43 IPSec Authentication Method Settings

Step 5. From within the **Encapsulation** category, **ISAKMP algorithms** (please refer to the Common VPN Terms section for an explanation) can be set. For the encryption algorithms, you are given choices from 3DES, DES and AES. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, you are given choices from MD5 and SHA1. Here, we have chosen **MD5** from the **Auth Algorithm** drop-down list. From the **Group** drop-down list **GROUP_2.** Please note that both VPN sites have to choose the same group. *(Figure 44)*

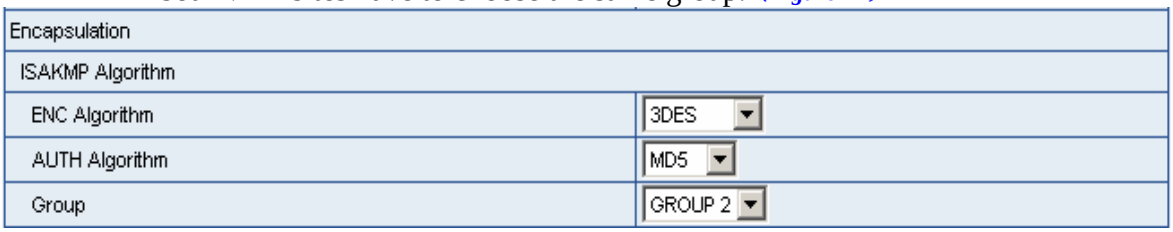

Figure 44 The IPSec Encapsulation Settings

Step 6. From the **IPSec Algorithm** category**,** you can choose either **Data Encryption + Authentication** or **Authentication Only**.

Select the **Data Encryption + Authentication** option. For the encryption algorithms, you are given choices from 3DES, DES, AES-128, AES-192, AES-256 and NULL. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, **MD5** and **SHA1** are available. Choose **MD5** from the drop-down list. *(Figure 45)*

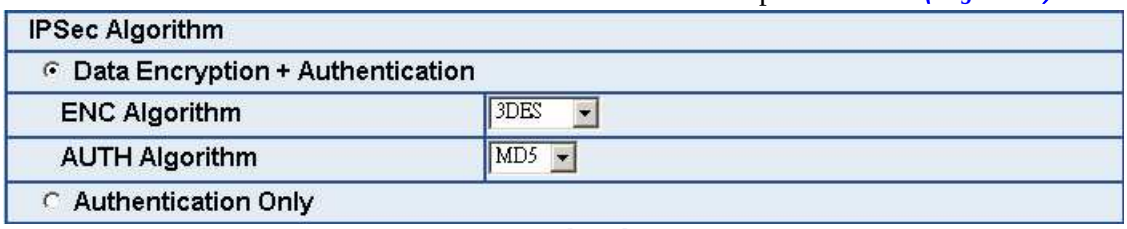

Figure 45 IPSec Algorithm Settings

Step 7. Under the **Optional Item** category, for **Perfect Forward Secrecy** select **GROUP1** from the drop-down list. For the **ISAKMP Lifetime** field, enter 3600. For the **IPSec Lifetime** field enter 28800**.** Select the **Main mode** radio button in the **Mode** section. *(Figure 46)*

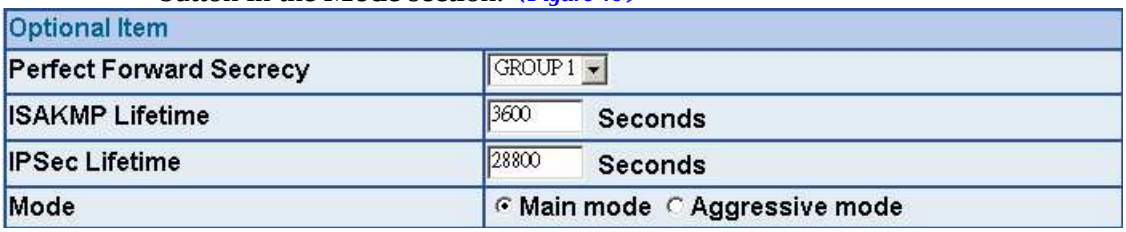

Figure 46 IPSec Autokey - Perfect Forward Secrecy Setting

Step 8. IPSec Autokey settings completed. *(Figure 47)*

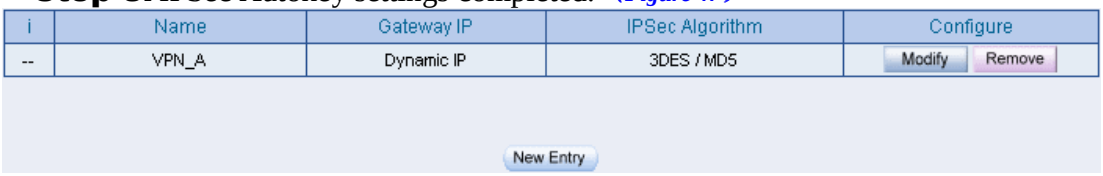

Figure 47 Company A IPSec Autokey – Settings Completed

Step 9. Go to **Policy Object > VPN > Tunnel**. Click on the **New Entry** button and then proceed with the following: *(Figure 48)*

- In the **Name** field, enter a unique name for the tunnel.
- For the **From Local** setting, select **LAN**.
- In the **Local Subnet / Mask** field, enter 192.168.10.0 / 255.255.255.0.
- From the **To Remote** category, select the **Remote Client**.
- From the **IPSec / PPTP Setting** drop-down list, select VPN_A.
- Check the **Show remote Network Neighborhood** checkbox.
- Click **OK**. *(Figure 49)*

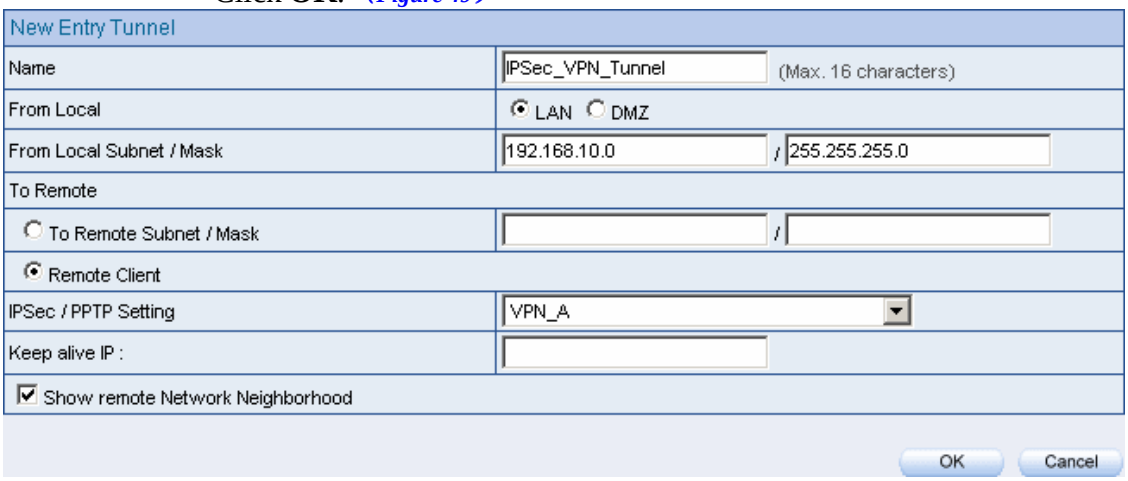

Figure 48 New Entry Tunnel Settings

Figure 49 VPN Tunnel Settings Completed

Step 10. Go to **Policy > Outgoing.** Click on the **New Entry** button and enter the following settings: *(Figure 50)*

- **Authentication User:** Select **All_NET**.
- **Schedule:** Select **Schedule_1**.
- QoS: Select QoS_1.
- **Tunnel:** Select **IPSec_VPN_Tunnel**..
- Click **OK**. *(Figure 51)*

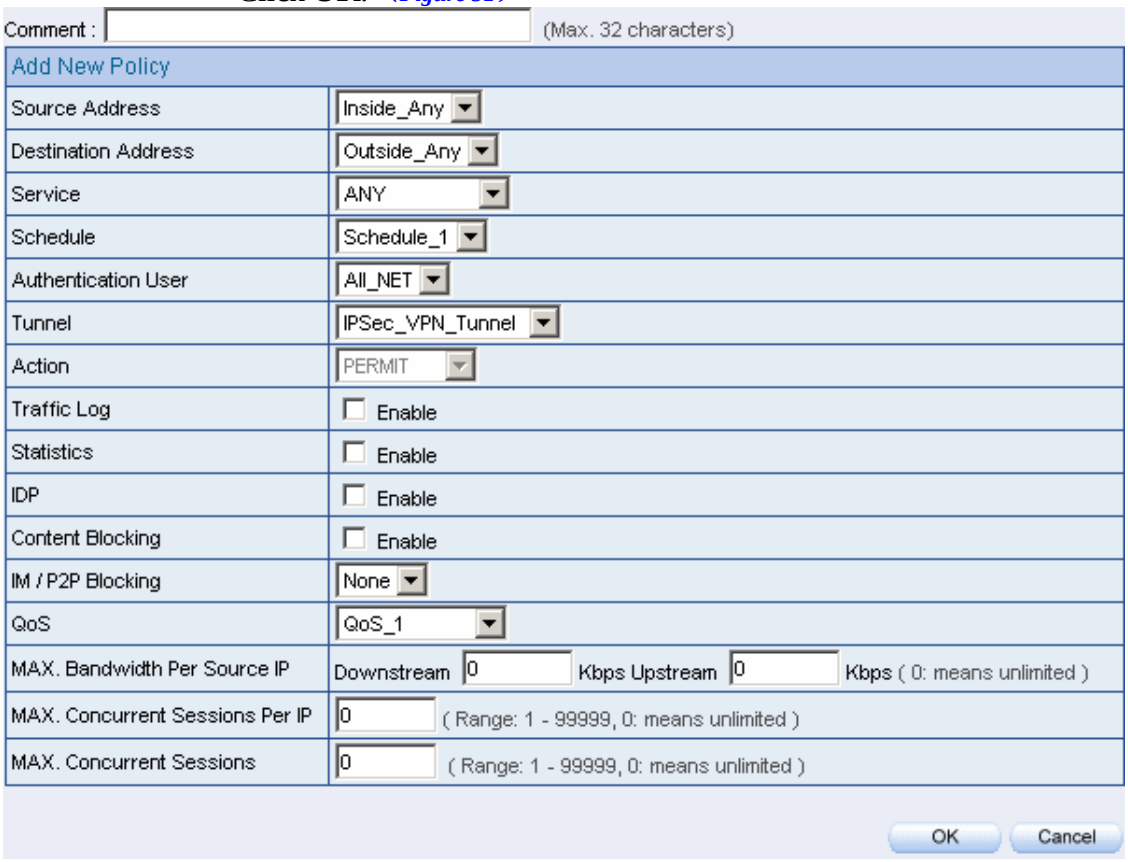

Figure 50 VPN Tunnel Outgoing Policy Settings

Figure 51 VPN Tunnel Outgoing Policy Settings Completed

Step 11. Go to **Policy > Incoming.** Click on the **New Entry** button and enter the following settings: *(Figure 52)*

- **Authentication User:** Select **All_NET**.
- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Tunnel:** Select **IPSec_VPN_Tunnel**.
- Click **OK**. *(Figure 53)*

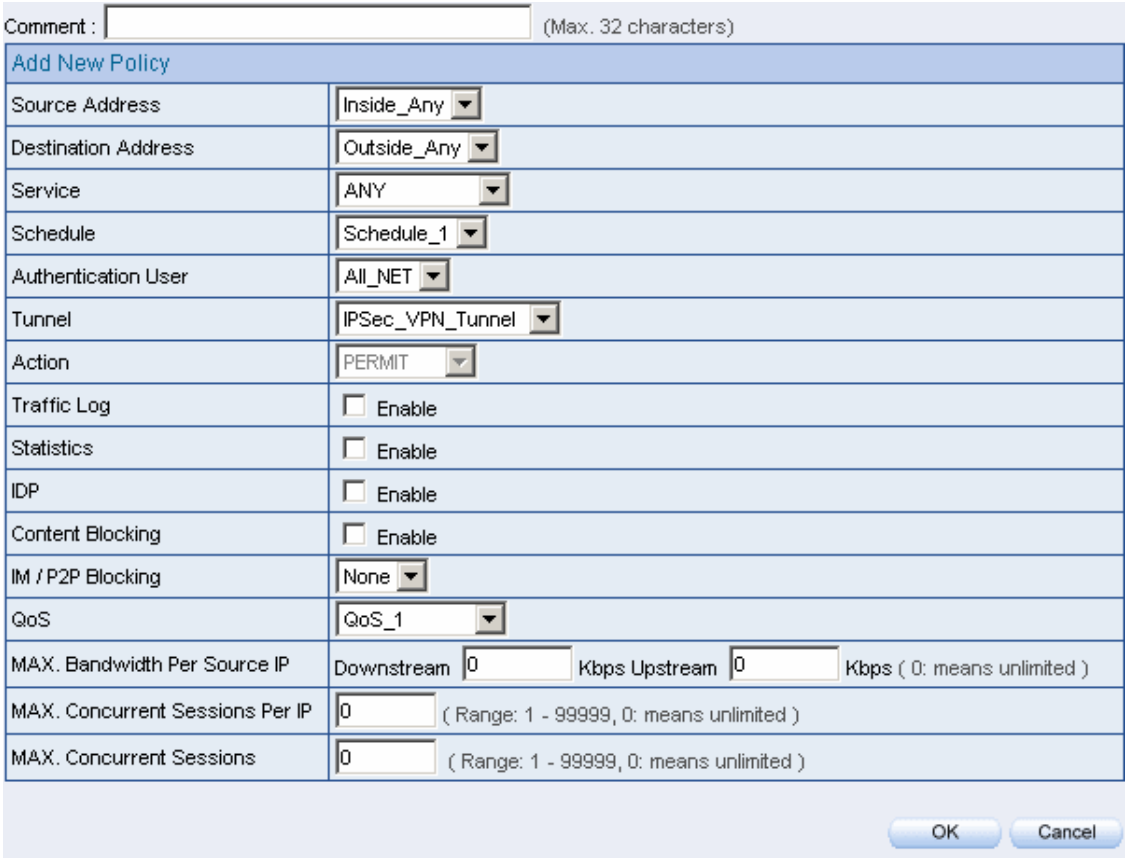

Figure 52 VPN Tunnel Incoming Policy Settings

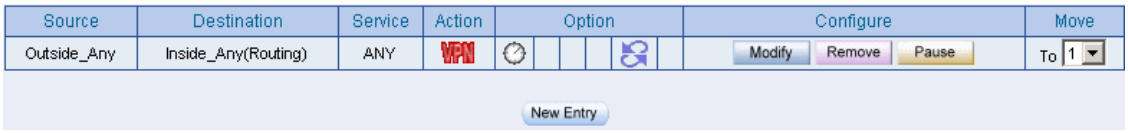

Figure 53 VPN Tunnel Incoming Policy Settings Completed

Company B's PC has the real IP address 211.22.22.22. Proceed with the following steps:

Step 1. From the Windows 2000 start menu, click **Start** > **Run.** *(Figure 54)*

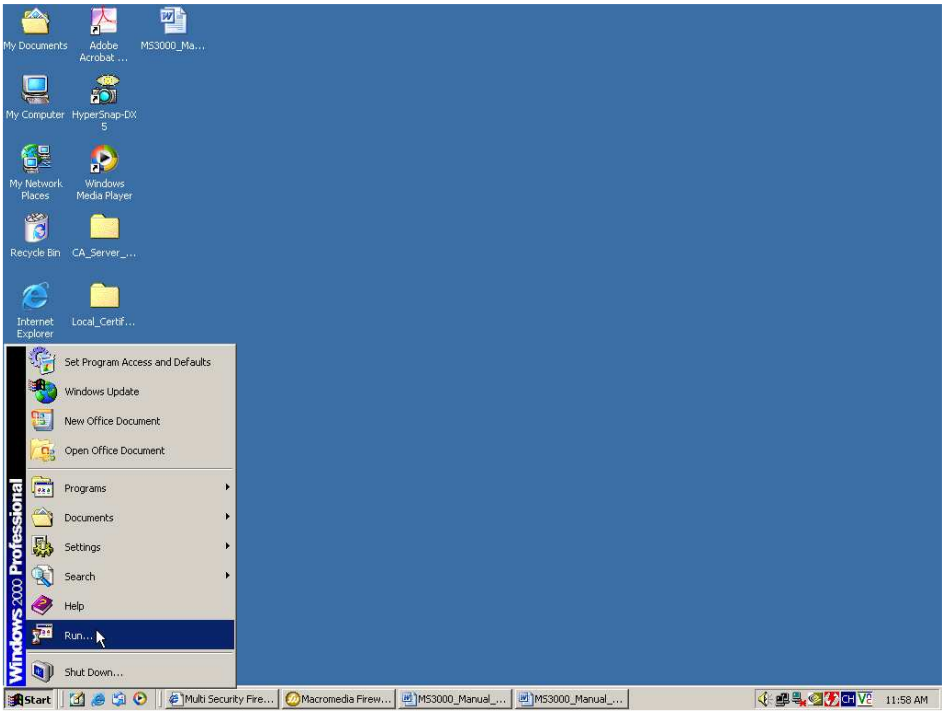

Figure 54 Start the IPSec VPN Setting in Windows 2000

Step 2. Enter **mmc** in the **Open** field and click **OK**. *(Figure 55)*

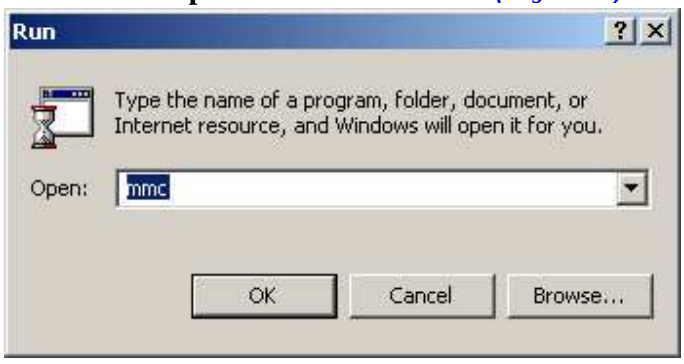

Figure 55 Starting the Windows 2000 IPSec VPN Configuration

Step 3. From the main drop-down menu, go to **Console**> **Add/Remove Snap-in**. *(Figure 56)*

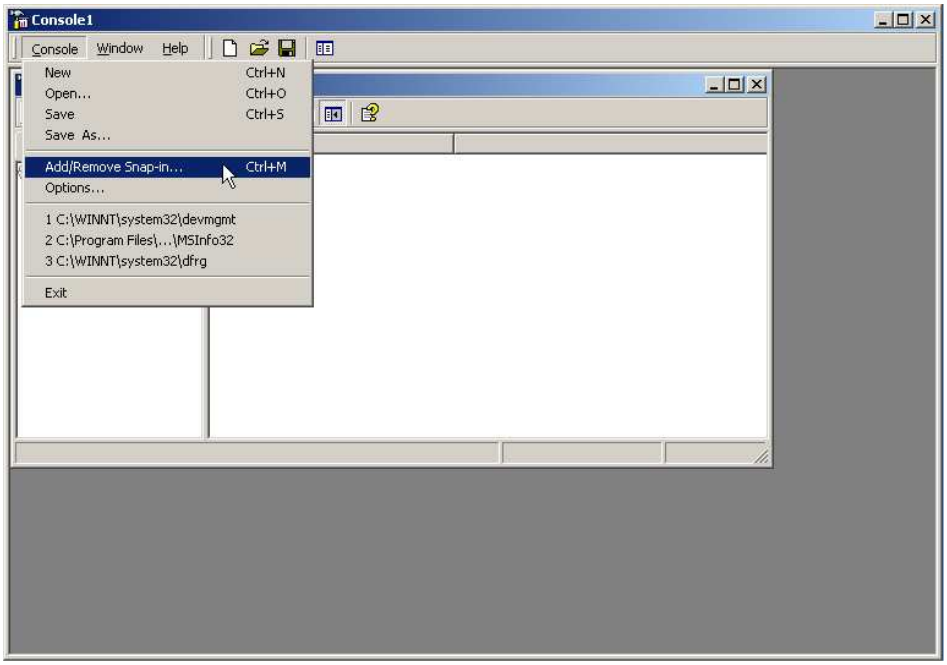

Figure 56 Add / Remove Snap-in.

Step 4. In the **Add / Remove Snap-in** window, click **Add**. Then, in the **Add Standalone Snap-in** window, select **IP Security Policy Management** then click **Add**. *(Figure 57)*

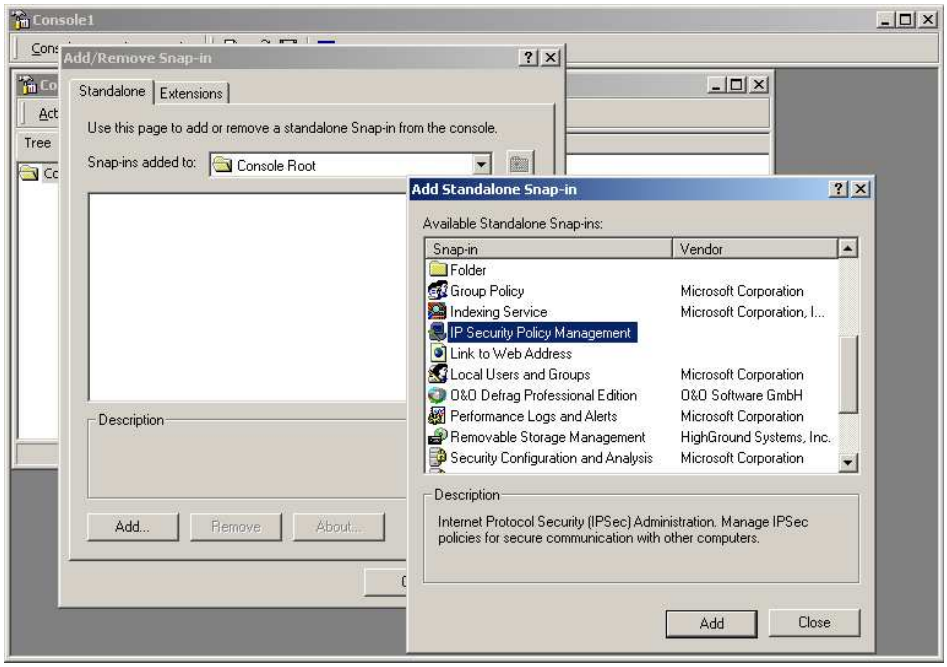

Figure 57 Adding IP Security Policy Management

Step 5. Select **Local Computer**, click **finish**. *(Figure 58)*

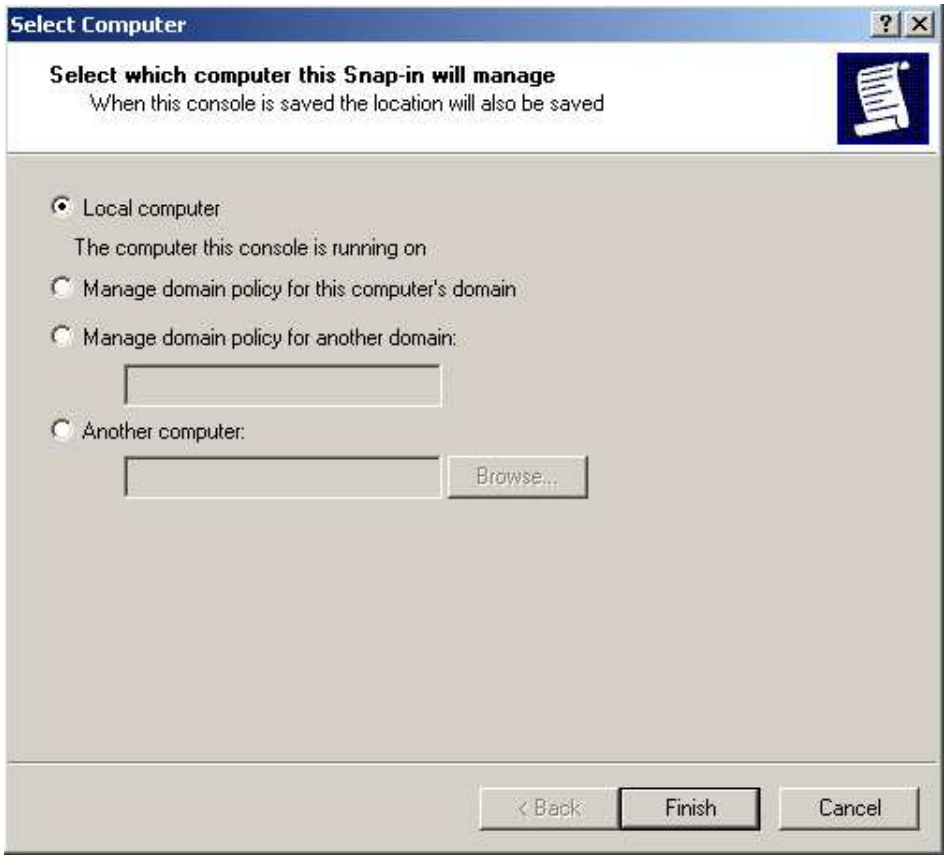

Figure 58 IP Security Policy Management Selection

Step 6. IP Security Policy Management Ready for Configuration. *(Figure 59)*

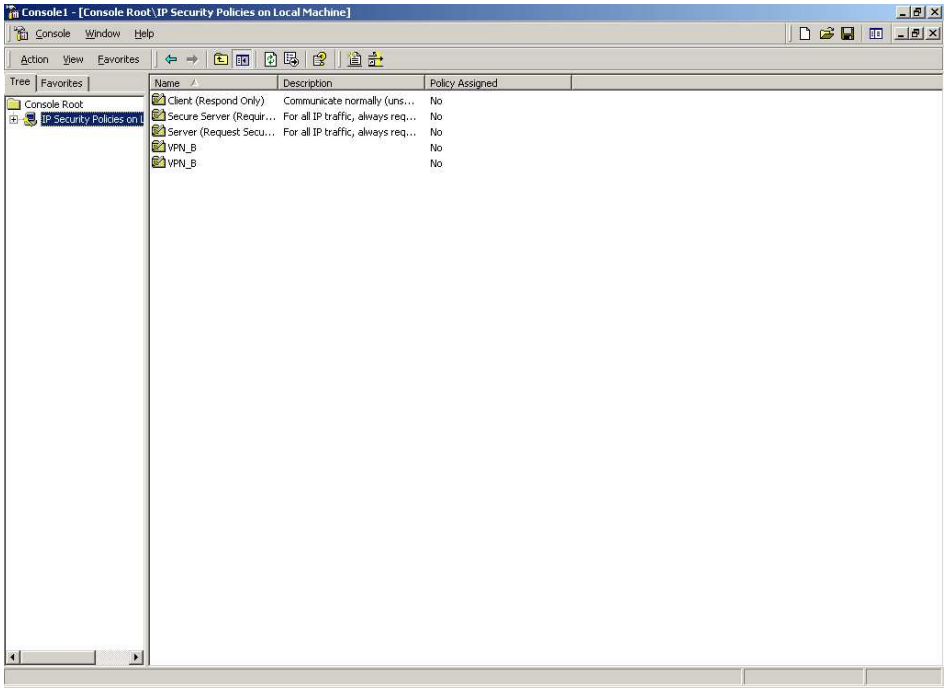

Figure 59 IP Security Policy Management Ready for Configuration

Step 7. Right-click on the **IP Security Policies on Local Machine**, and select **Create IP Security Policy**. *(Figure 60)*

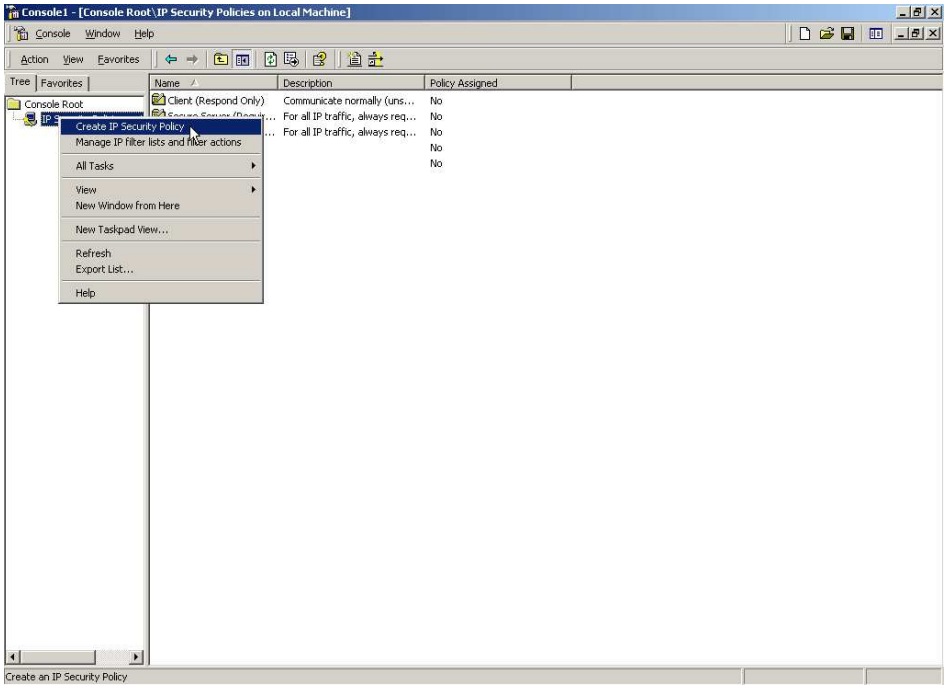

Figure 60 Create IP Security Policy

Step 8. Click **Next**. ***(Figure 61)***

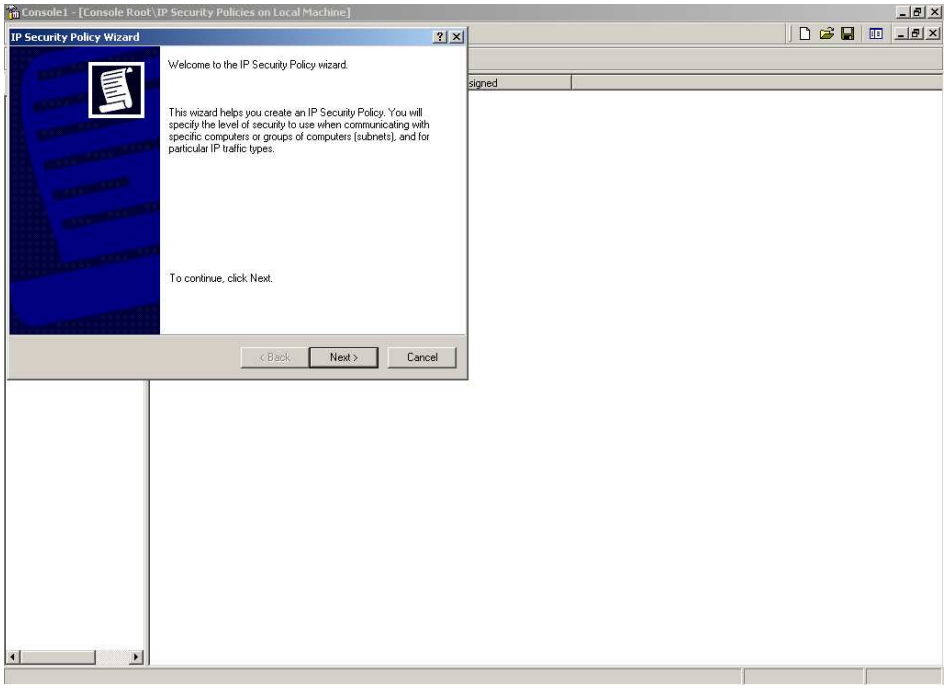

Figure 61 Starting the IP Security Policy Wizard

Step 9. In the **Name** field, enter the VPN name. In the **Description** field, enter a description if desired. *(Figure 62)*

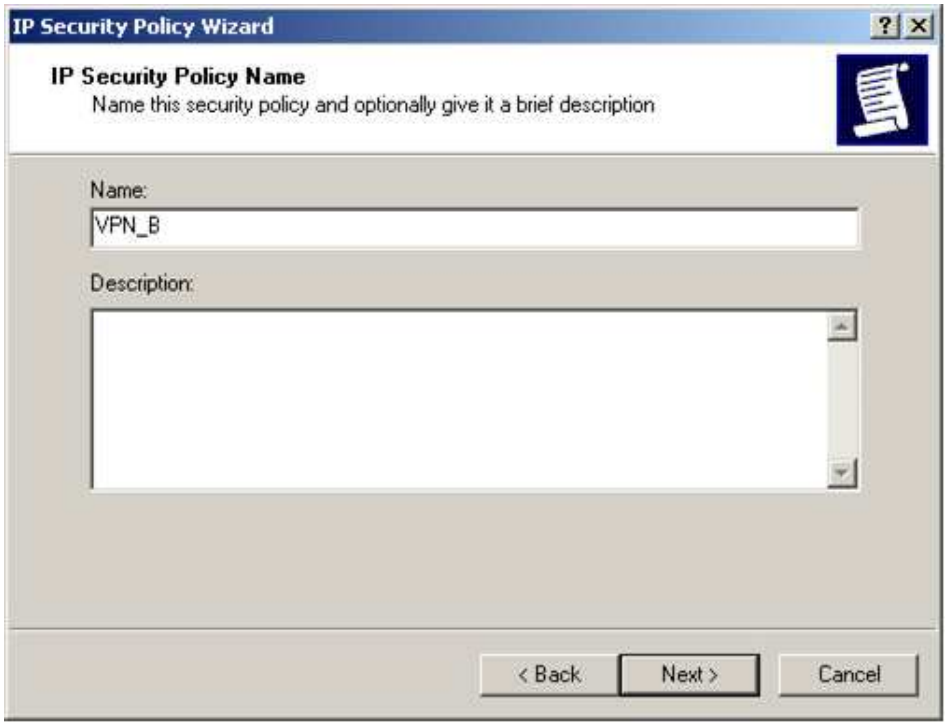

Figure 62 Designating a VPN name and description

Step 10. Ensure that the **Activate the default response rule** checkbox is not checked, and click **Next**. *(Figure 63)*

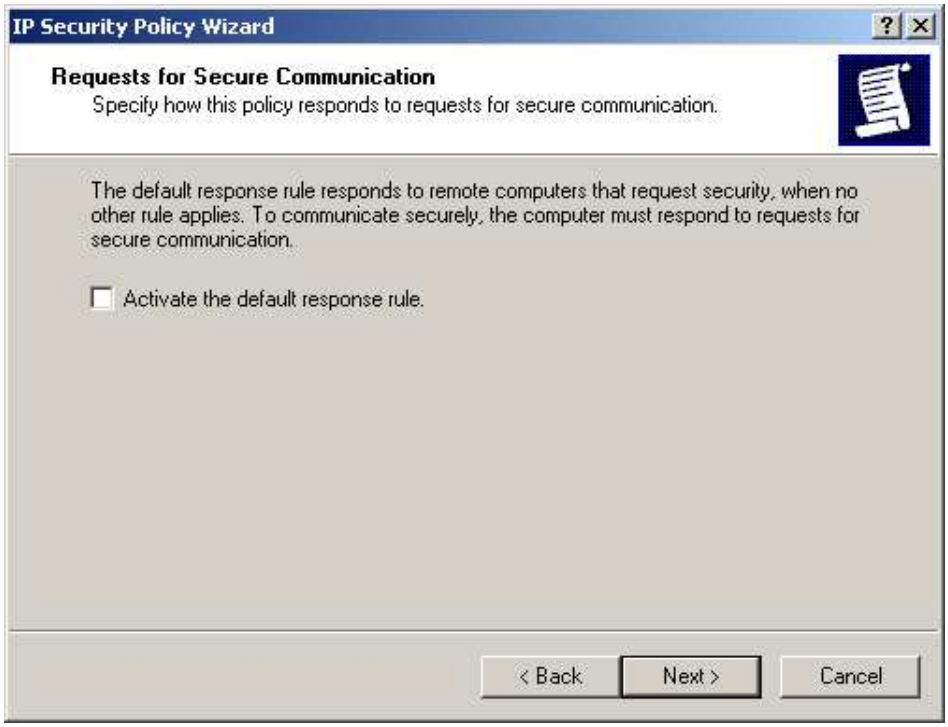

Figure 63 Leave the Box Unchecked

Step 11. In the **IP Security Policy Wizard** window**,** check **Edit properties** and click **Finish**. *(Figure 64)*

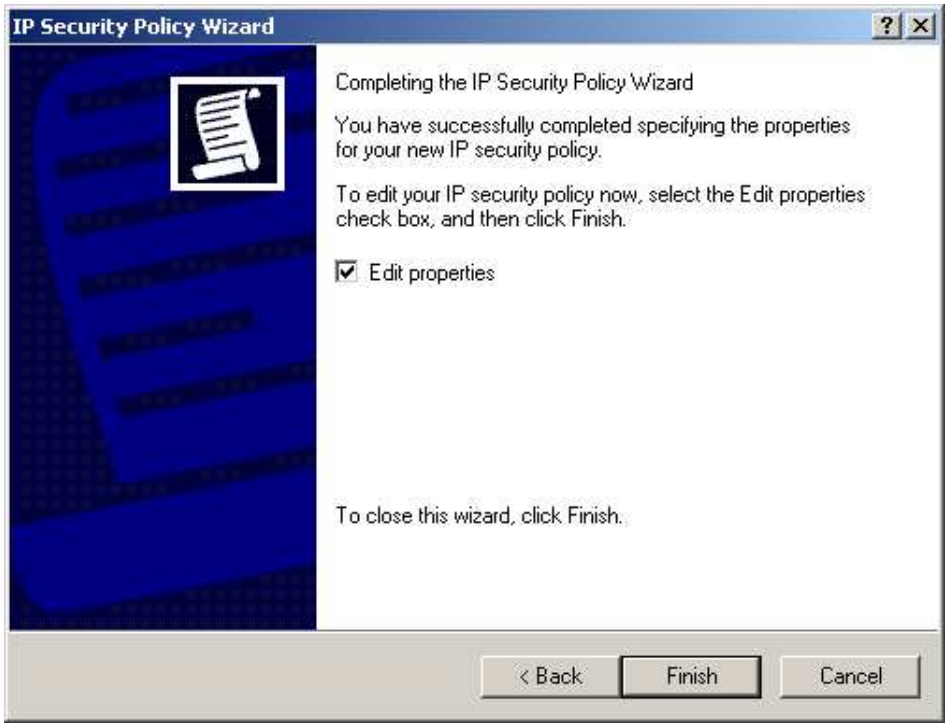

Figure 64 IP Security Policy Wizard Settings Completed

Step 12. In the **VPN_B Properties** window, leave the **Use Add Wizard** checkbox unchecked, and click **Add**. *(Figure 65)*

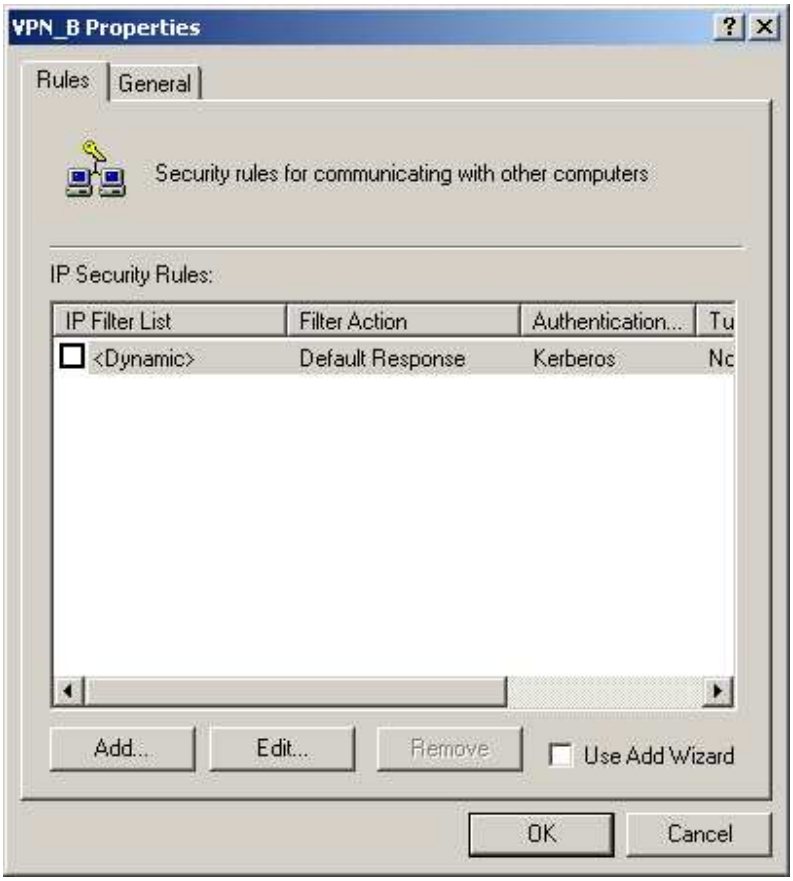

Figure 65 VPN_B Properties

Step 13. In the **New Rule Properties** window, click **Add**. *(Figure 66)*

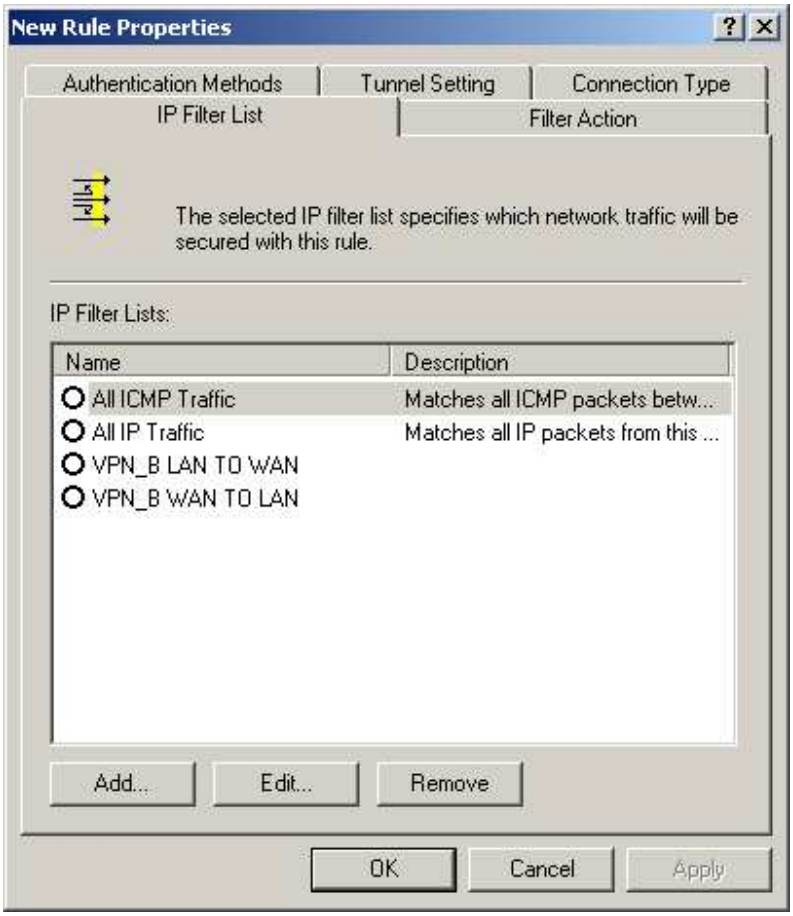

Figure 66 New Rule Properties

Step 14. In the **IP Filter List** window, do not check the **Use Add Wizard** checkbox. Modify the **Name** into VPN_B WAN TO LAN and then click **Add.** *(Figure 67)*

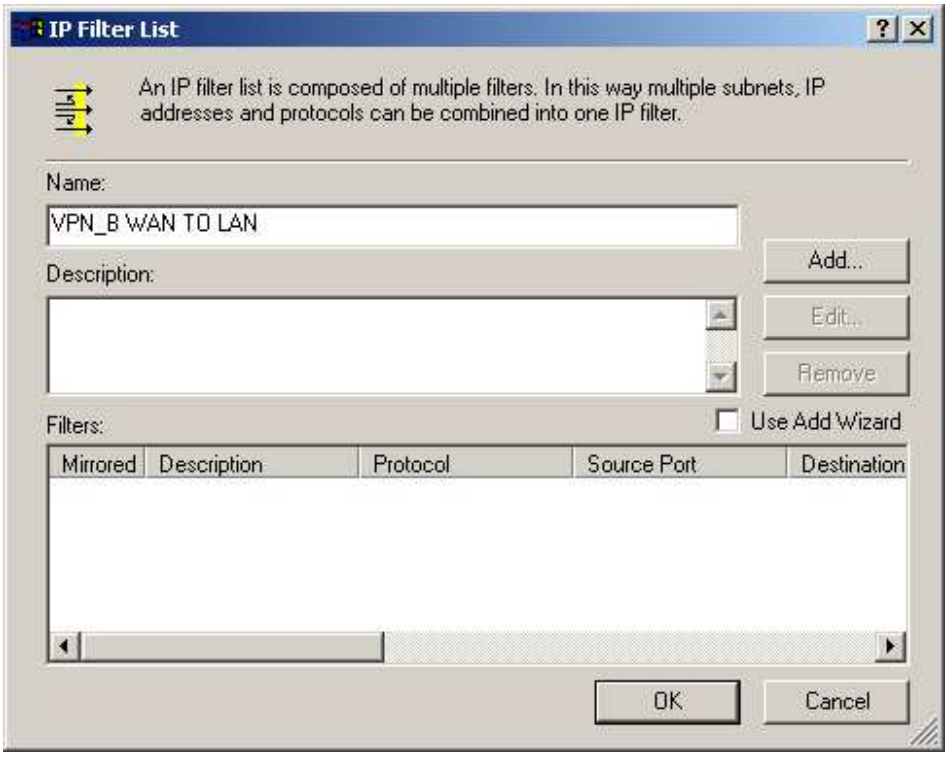

Figure 67 IP Filter List

Step 15. In the **Filter Properties** window, beneath **Source address** select **A specific IP Address** from the drop-down menu, then type in Company B's WAN IP address 211.22.22.22 and subnet mask 255.255.255.255 into the fields. After that, from the drop-down menu beneath **Destination address,** select **A specific IP Subnet**, then enter 192.168.10.0 as Company A's LAN IP address, and 255.255.255.0 as subnet mask. Do not check the **Mirrored. Also match packets with the exact opposite source and destination addresses** checkbox. *(Figure 68)*

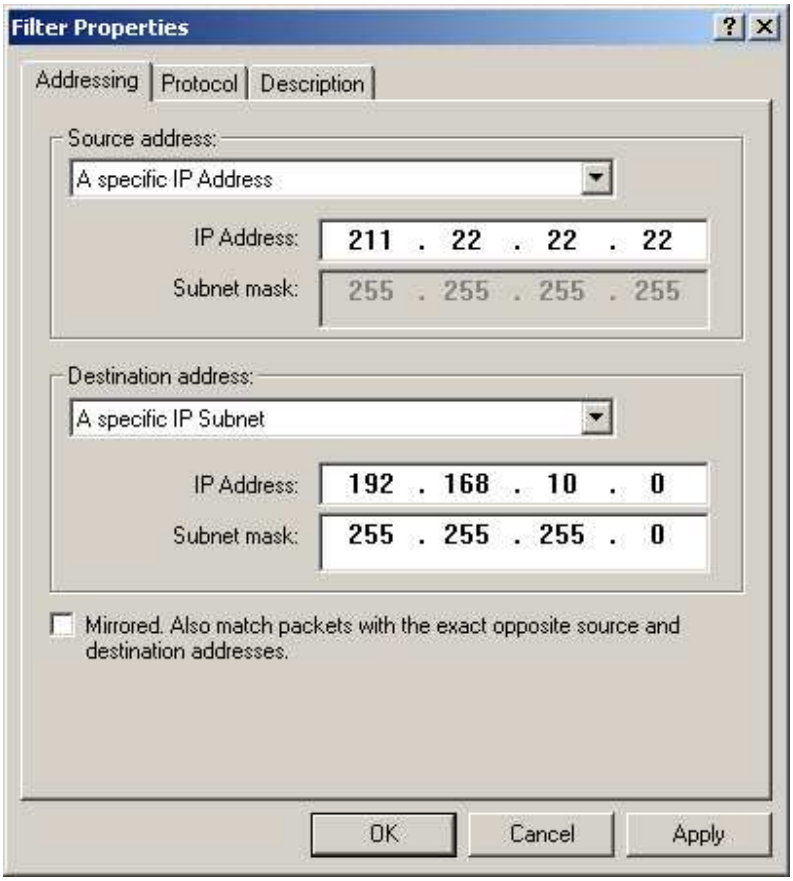

Figure 68 Filter Properties

Step 16. The settings are now complete. Close the **IP Filter List**. *(Figure 69)*

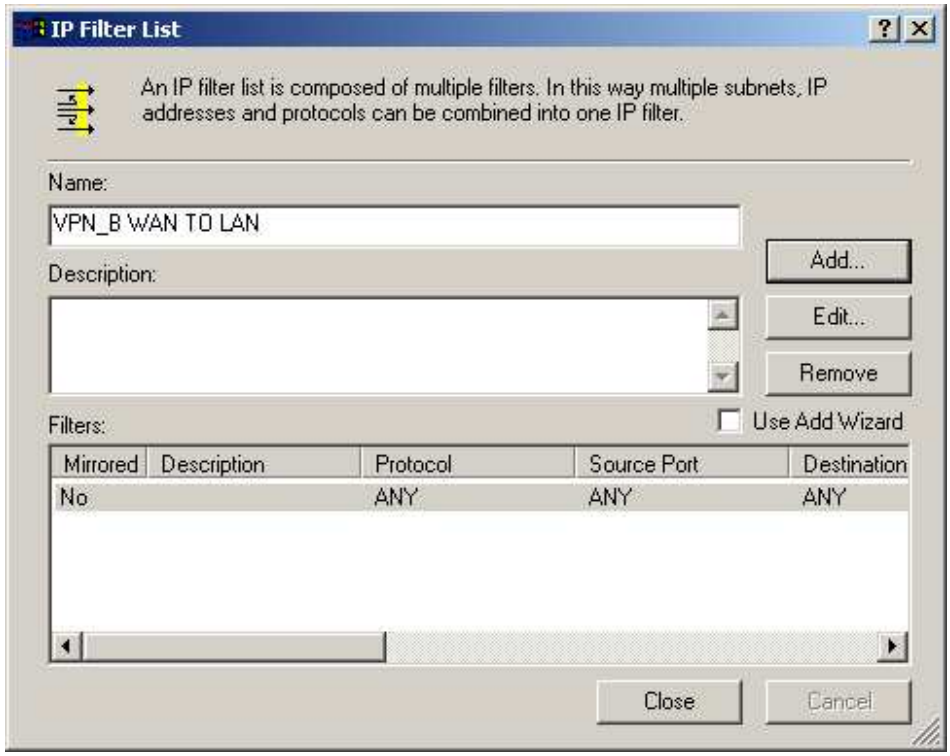

Figure 69 IP Filter List Settings Completed.

Step 17. In the **New Rule Properties** window, click on the **Filter Action** tab and then check **Require Security**. Next, click **Edit.** *(Figure 70)*

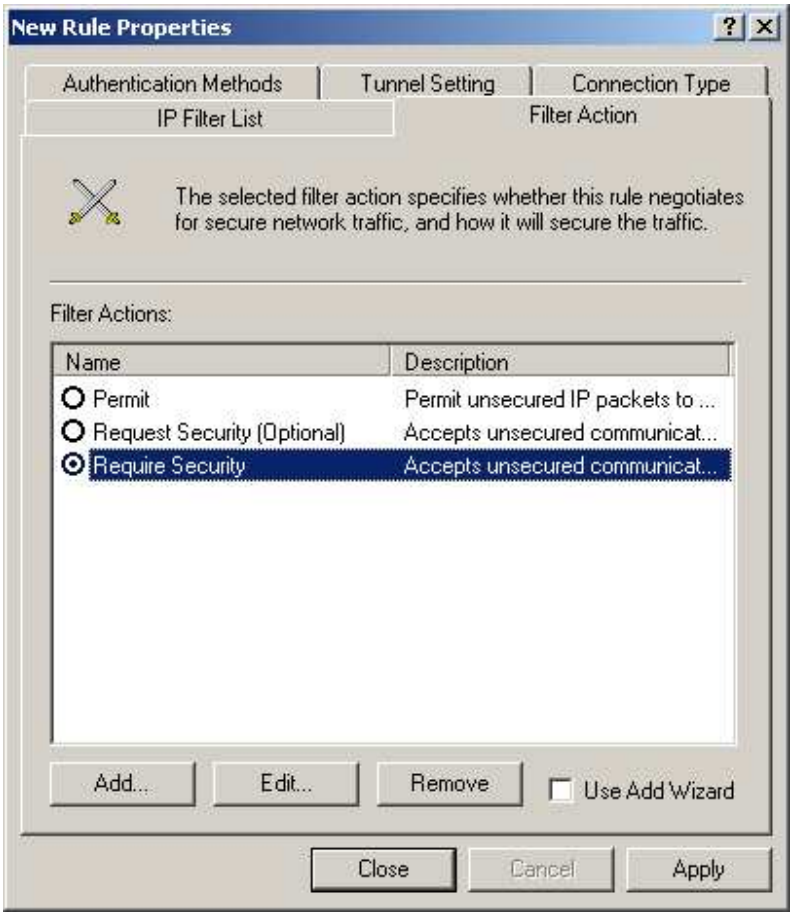

Figure 70 Filter Action Setting

Step 18. In the **Require Security Properties** window, select **Negotiate security** and check **Session Key Perfect Forward Secrecy** on the bottom. *(Figure 71)*

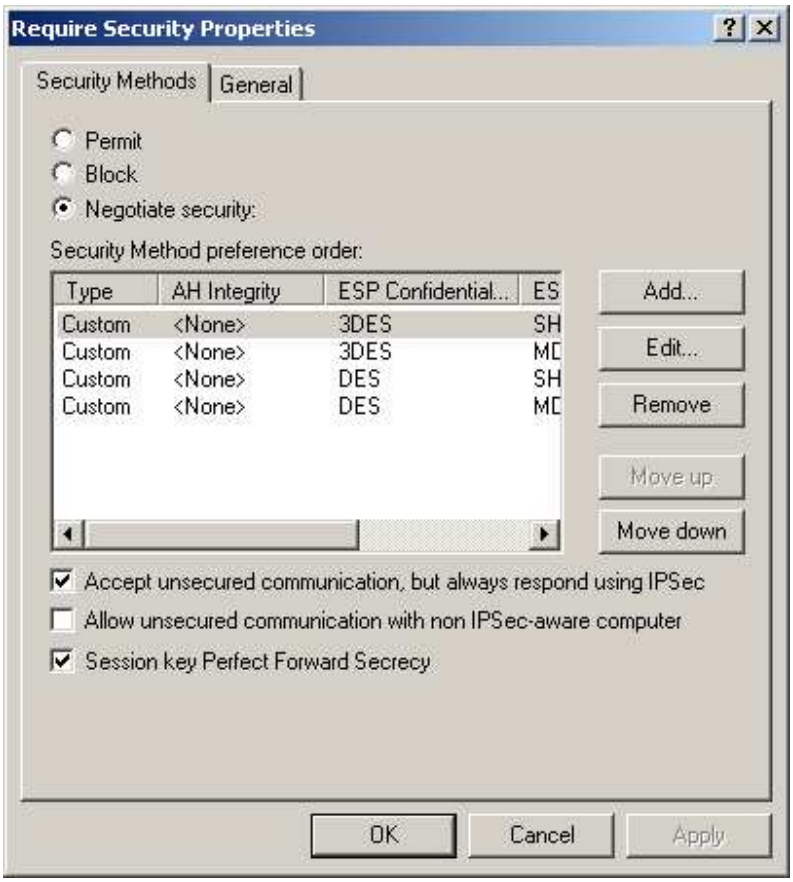

Figure 71 Select Session Key Perfect Forward Secrecy

Step 19. From within the **Security Method preference order** list, select the security method (**Custom / None / 3DES / MD5**), click **Edit**. *(Figure 72)*

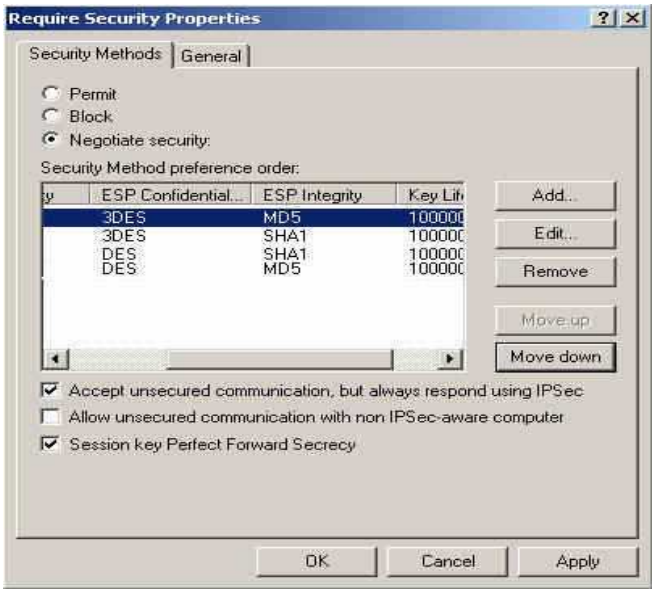

Figure 72 Editing the Security Method

Step 20. Select **Custom (for expert users),** and click **Settings**. *(Figure 73)*

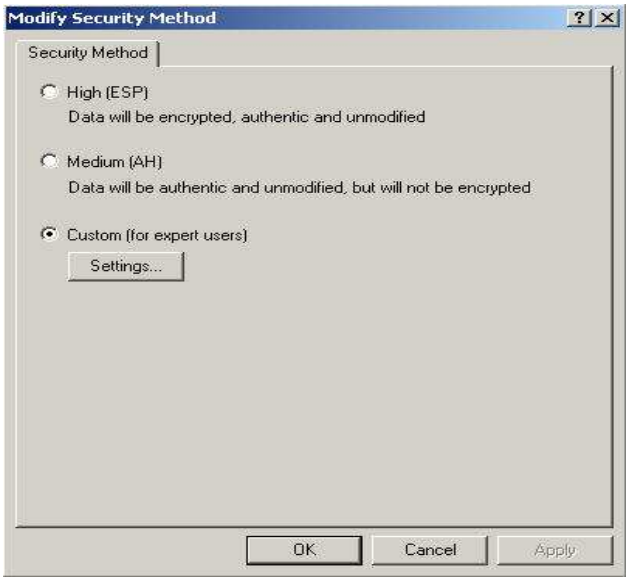

Figure 73 Custom Security Method

Step 21. Check **Data Integrity and encryption (ESP)**, and select **MD5** for **Integrity algorithm** and **3DES** for **Encryption algorithm** from the drop-down menu. Check **Generate a new key every**, and enter 28800 in the **seconds** field, then click **OK** to return to **New Rule Properties** window.

(Figure 74)

Figure 74 Custom Security Method Settings

Step 22. In the **New Rule Properties** window, click on the **Connection Type** tab and select **All network connections**. *(Figure 75)*

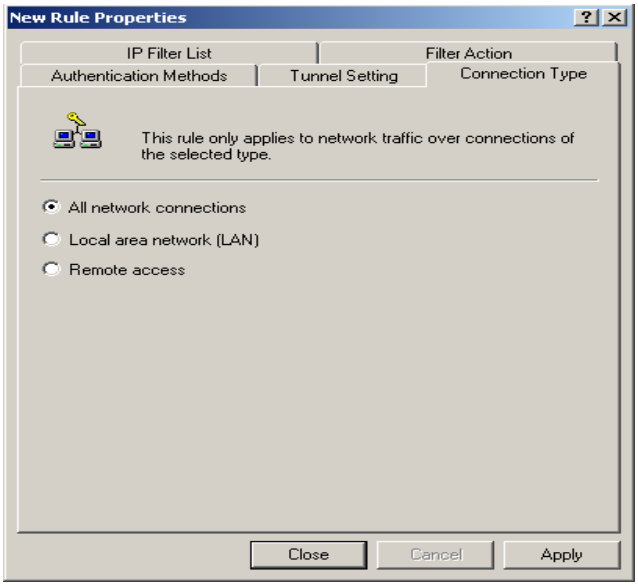

Figure 75 Connection Type Setting

Step 23. In the **New Rule Properties** window, click on **Tunnel Setting** tab. After that, check **The tunnel endpoint is specified by this IP Address**, then enter 61.11.11.11 as Company A's WAN IP address. *(Figure 76)*

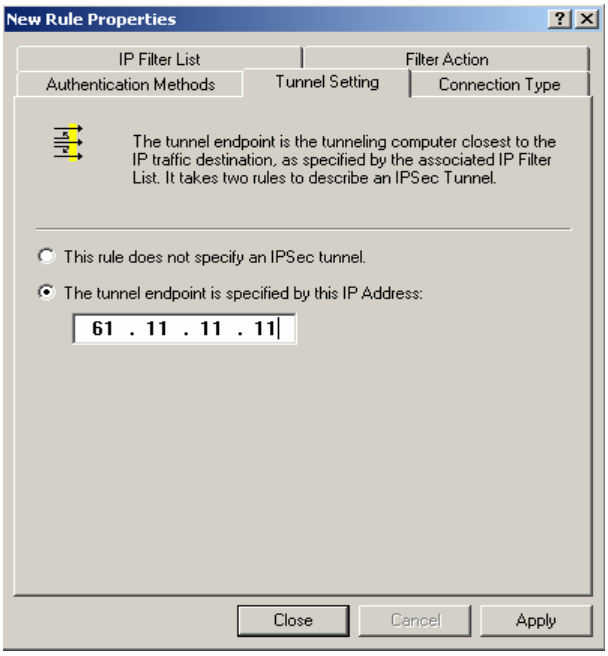

Figure 76 Tunnel Setting

Step 24. In the **New Rule Properties** window**,** click on the **Authentication Methods** tab. Next, select a method and click **Edit** on the right. *(Figure 77)*

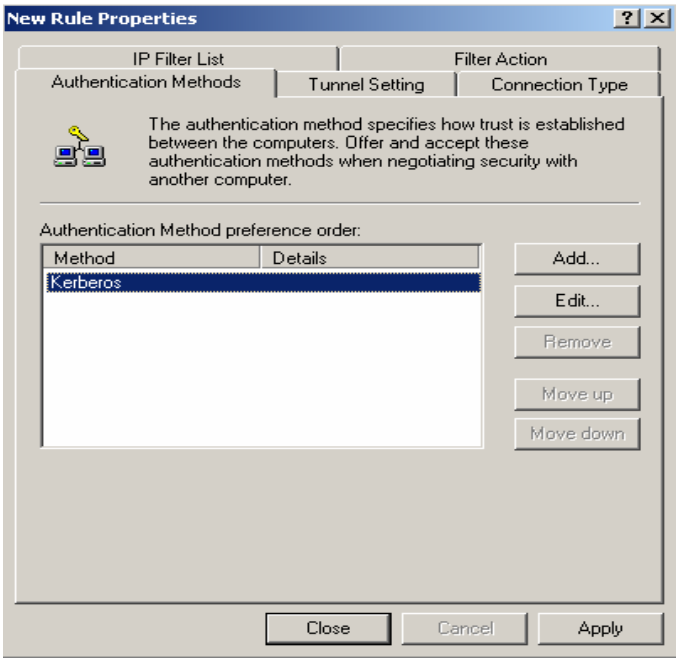

Figure 77 Authentication Methods Setting

Step 25. Select **Use this string to protect the key exchange (preshared key)**, and then enter the Preshared Key, 123456789, into the field. *(Figure 78)*

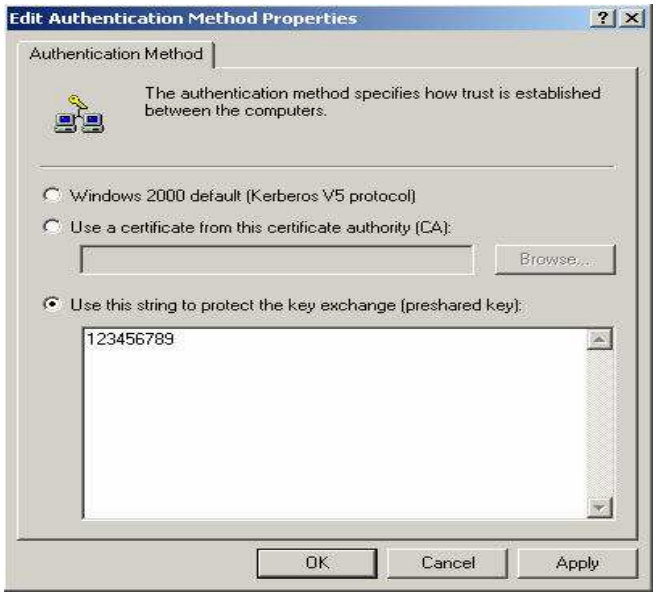

Figure 78 Setting the VPN Preshared Key

Step 26. Click **Apply**, and then click **Close** to close the window. *(Figure 79)*

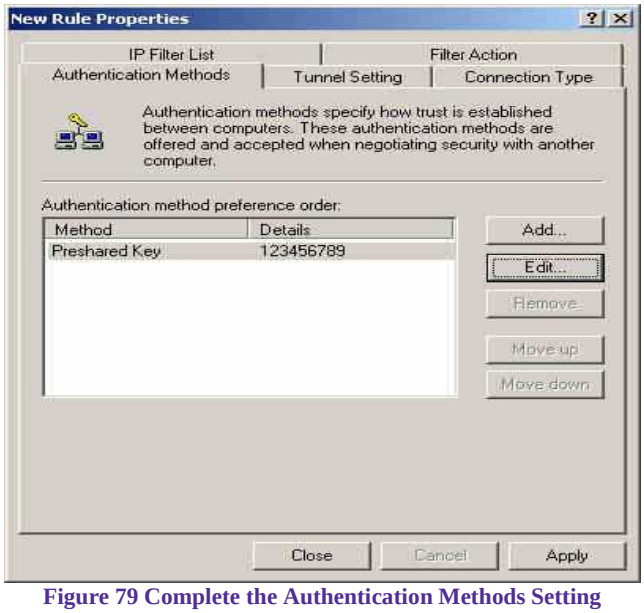

Figure 79 Complete the Authentication Methods Setting

Step 27. Complete the VPN_B WAN TO LAN settings. *(Figure 80)*

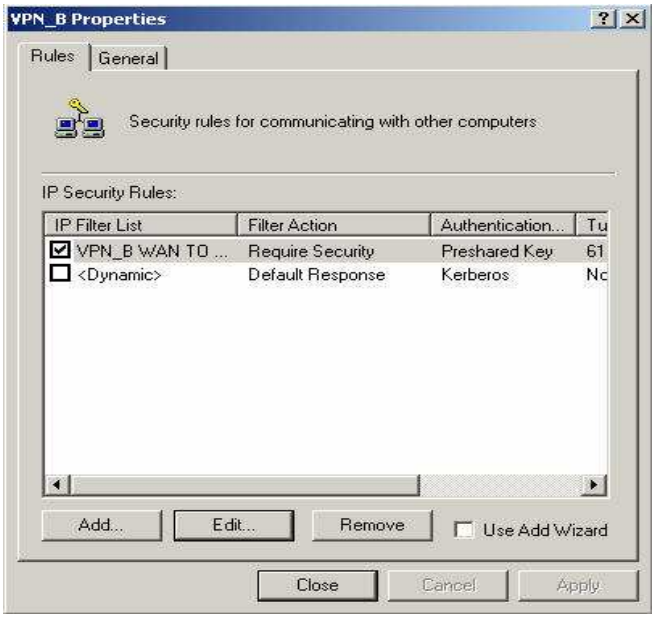

Figure 80 Complete the VPN_B WAN TO LAN Policy Setting

Step 28. In the **VPN_B Properties** window, do not check **Use Add Wizard**; Click **Add** to create the second IP security rule. *(Figure 81)*

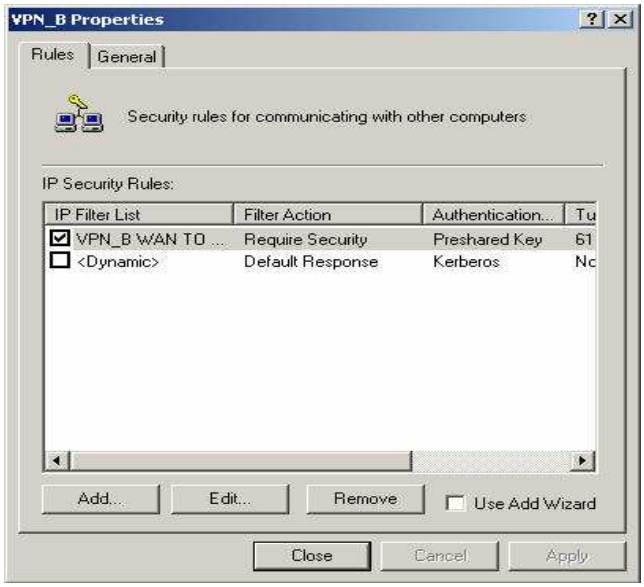

Figure 81 The VPN_B Properties

Step 29. In the **New Rule Properties** window, click **Add**. *(Figure 82)*

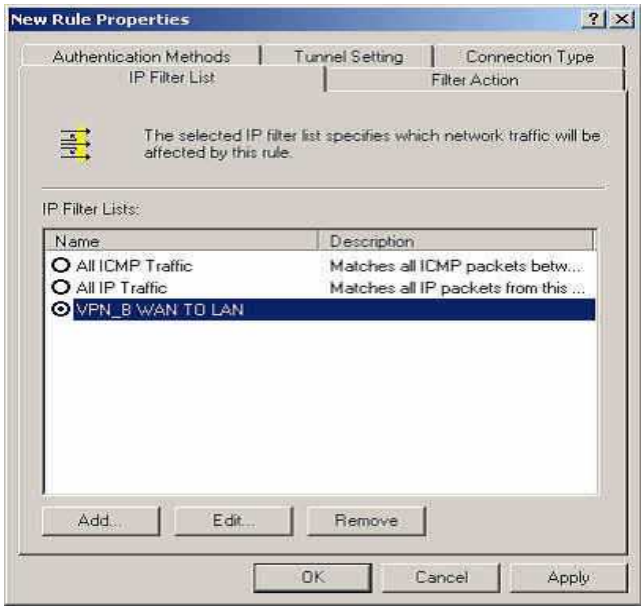

Figure 82 New Rule Properties

Step 30. In the **IP Filter List** window, do not check **Use Add Wizard**; Modify the **Name** into VPN_B LAN TO WAN, then click **Add**. *(Figure 83)*

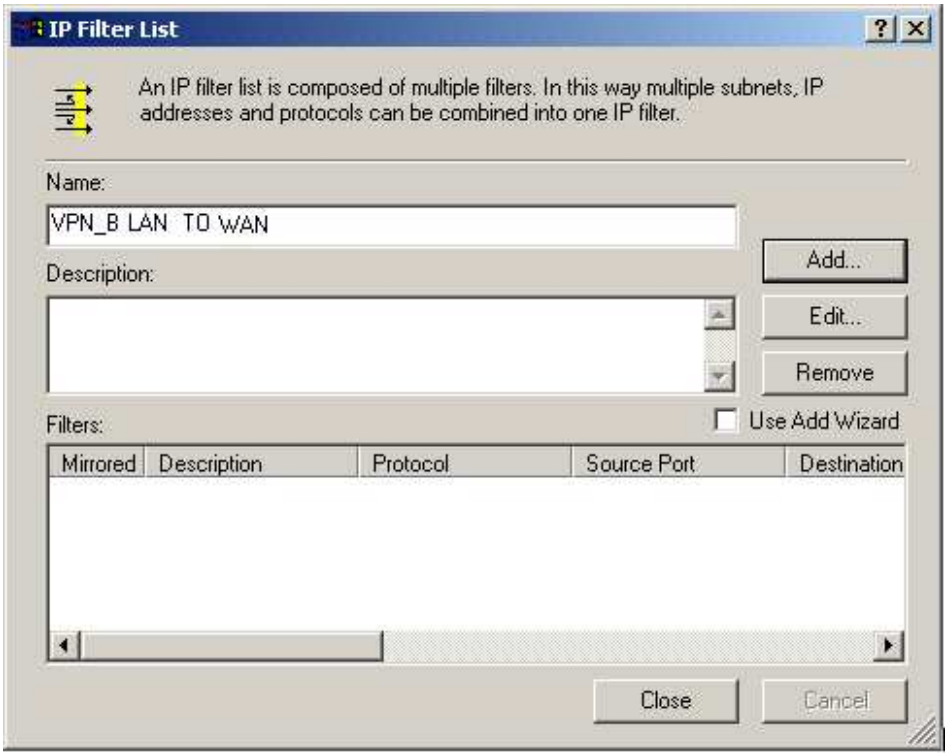

Figure 83 IP Filter List

Step 31. In the **Filter Properties** window, beneath **Source address** select **A specific IP Address** from the drop-down menu, then enter 192.168.10.0 as Company A's LAN IP address and 255.255.255.0 for the **Subnet mask**. After that, select **A specific IP Address** from the pull-down menu beneath **Destination address**, then enter 211.22.22.22 as Company's WAN IP Address and 255.255.255.255 for the **Subnet mask**. Note, do not enable **Mirrored. Also match packets with the exact opposite source and destination addresses**. *(Figure 84)*

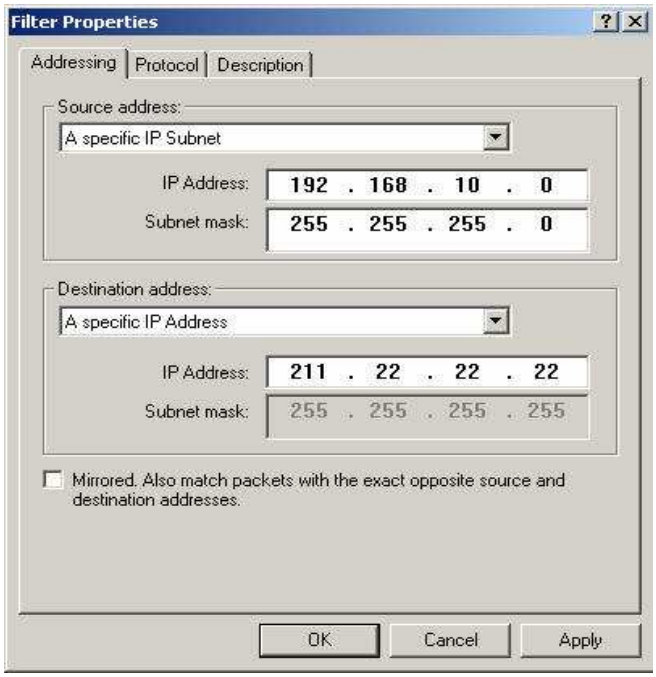

Figure 84 Filter Properties

Step 32. Settings completed, close the **IP Filter List**. *(Figure 85)*

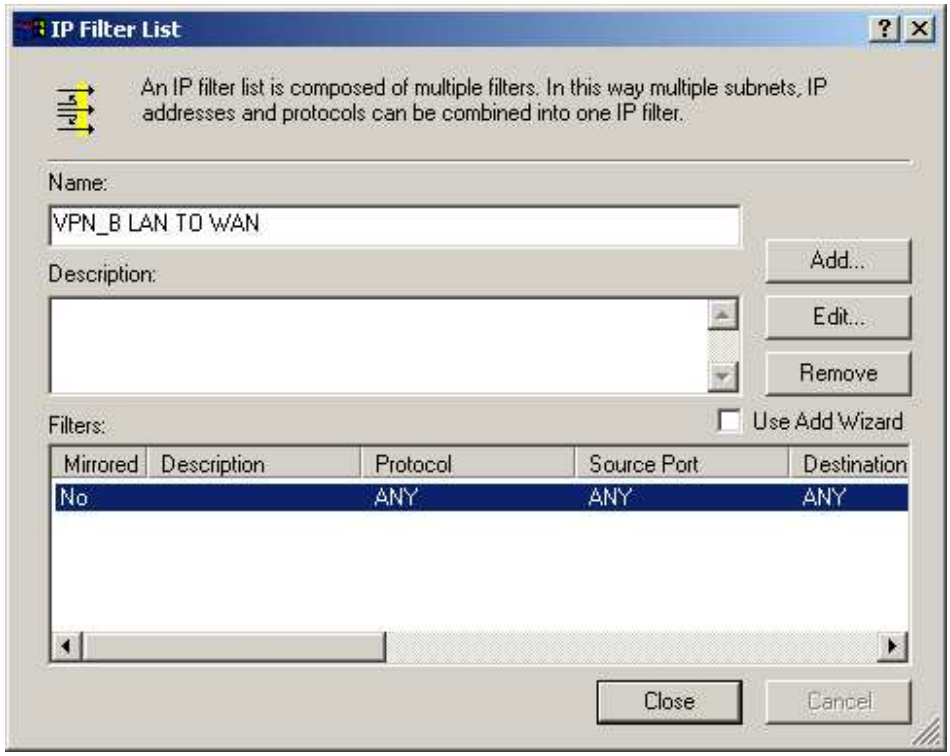

Figure 85 IP Filter List Settings Completed

Step 33. In the **New Rule Properties** window, click on the **Filter Action** tab; Check **Require Security** and then click **Edit**. *(Figure 86)*

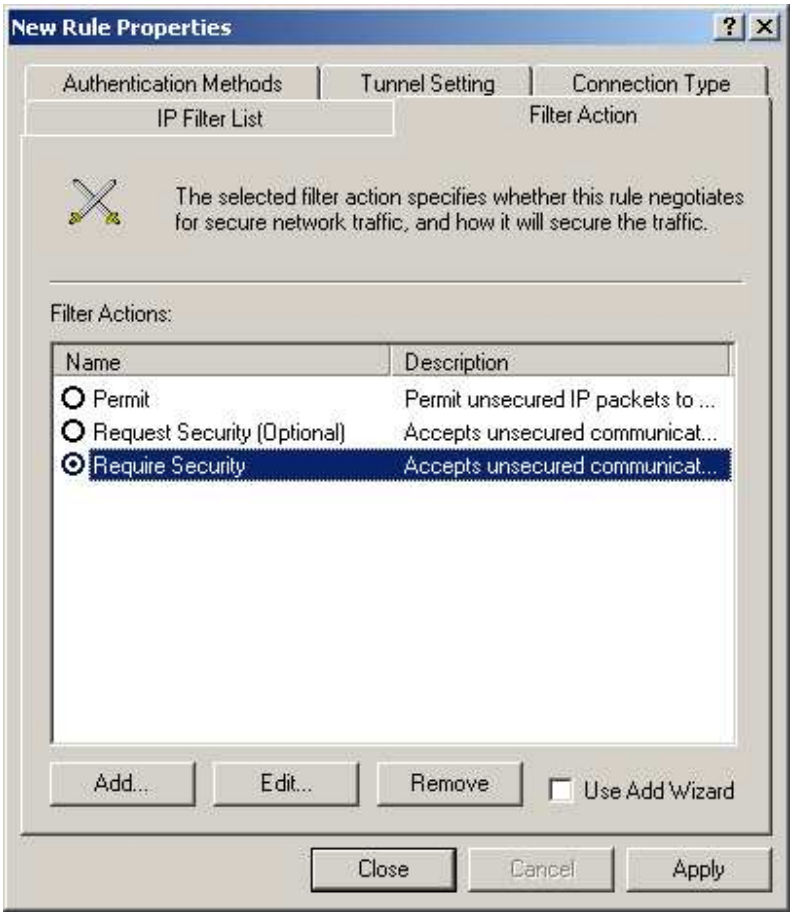

Figure 86 Filter Action

Step 34. In the **Require Security Properties** window, check **Session key Perfect Forward Secrecy**. *(Figure 87)*

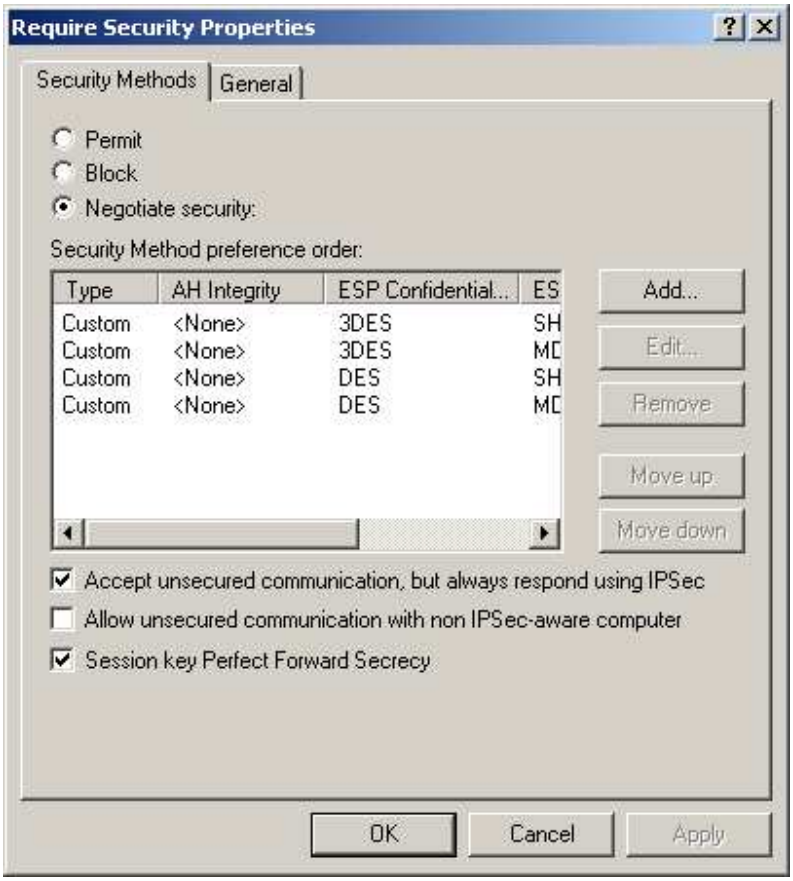

Figure 87 Select Session key Perfect Forward Secrecy

Step 35. From the **Security Method preference order** list, select the security method: (**Custom / None / 3DES / MD5**), click **Edit**. *(Figure 88)*

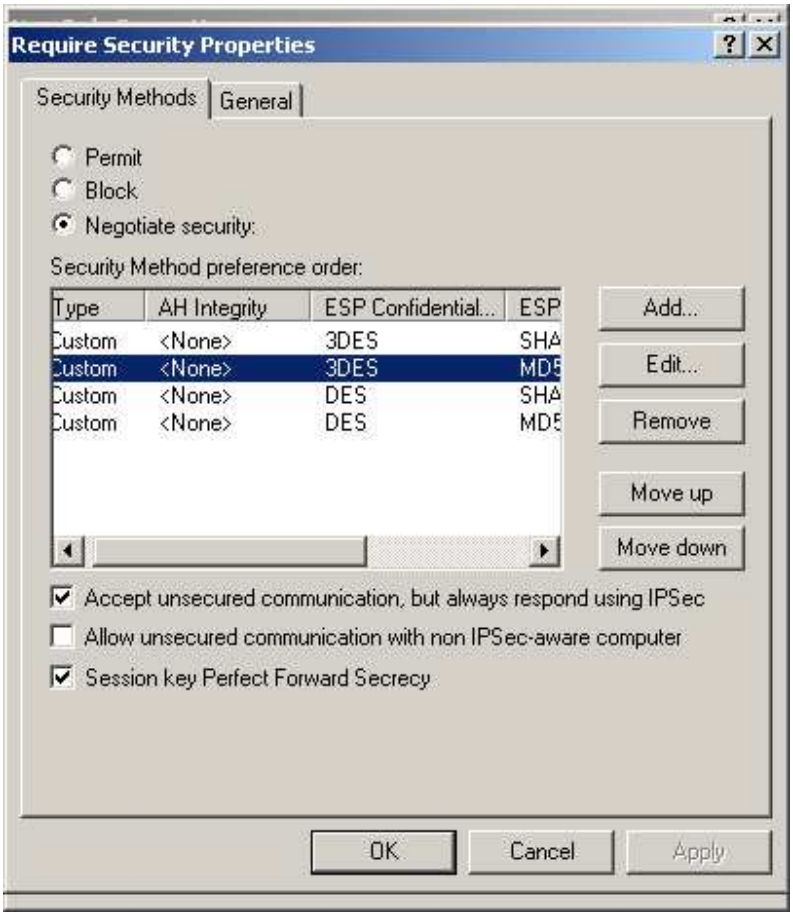

Figure 88 Set the Security Method

Step 36. Select **Custom (for expert users**), and click **Settings**. *(Figure 89)*

Figure 89 Custom Security Method Settings

Step 37. Check **Data integrity and encryption**. From the drop-down menus, for **Integrity algorithm** select **MD5** and for **Encryption algorithm** select **3DES**. Check **Generate a new key every**, and enter 28800 in the **seconds** field, then click **OK** to return to **New Rule Properties** window. *(Figure 90)*

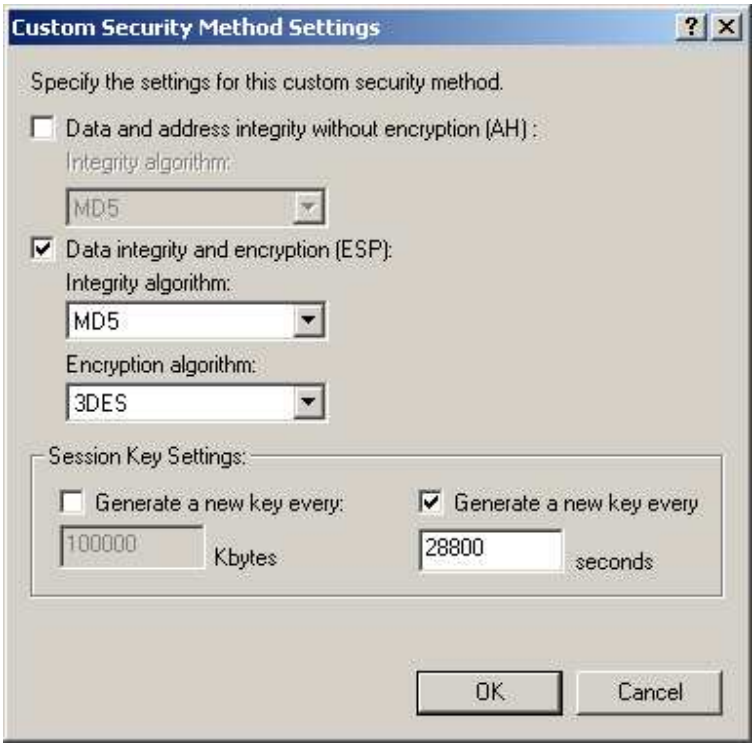

Figure 90 Custom Security Methods Settings

Step 38. In the **New Rule Properties** window, click on the **Connection Type** tab and select **All network connections**. *(Figure 91)*

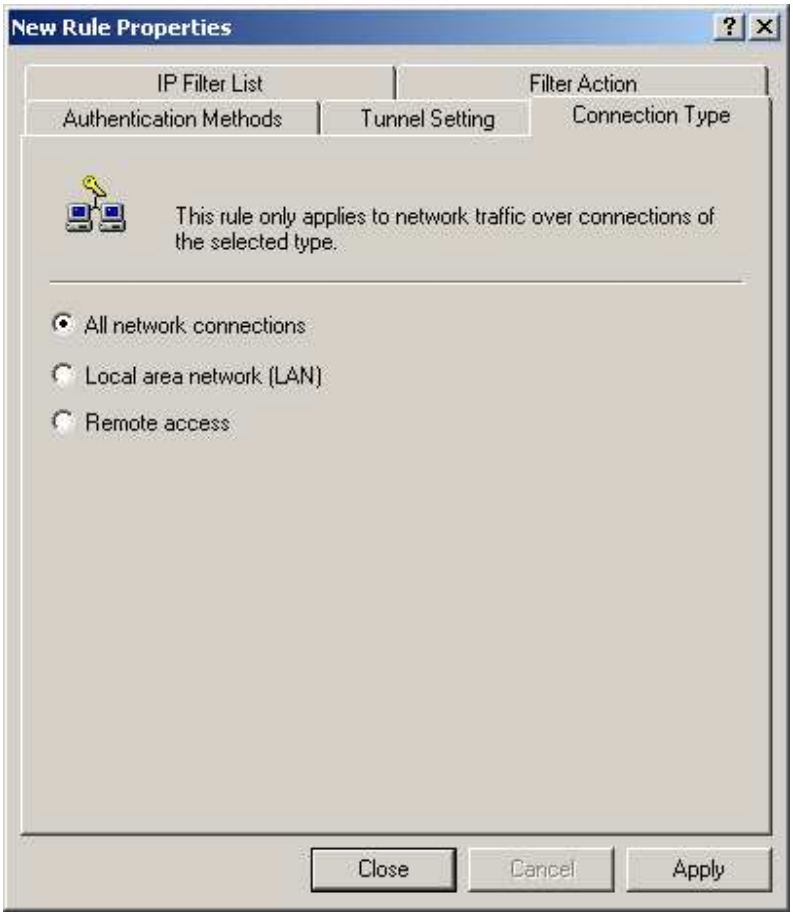

Figure 91 Connection Type Setting

Step 39. In the **New Rule Properties** window, click on the **Tunnel Setting** tab. After that, select **The tunnel endpoint is specified by this IP Address**, then enter 211.22.22.22 as Company B's WAN IP address. *(Figure 92)*

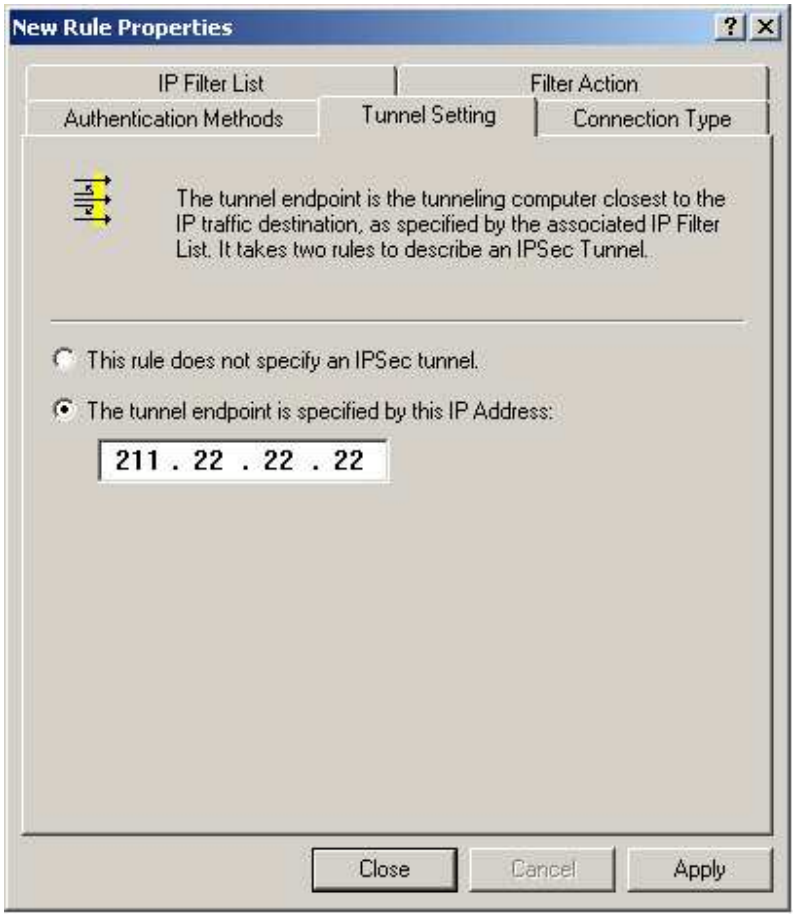

Figure 92 Tunnel Setting

Step 40. In the **New Rule Properties** window**,** click on the **Authentication Methods** tab. Next, select a method and click **Edit** on the right. *(Figure 93)*

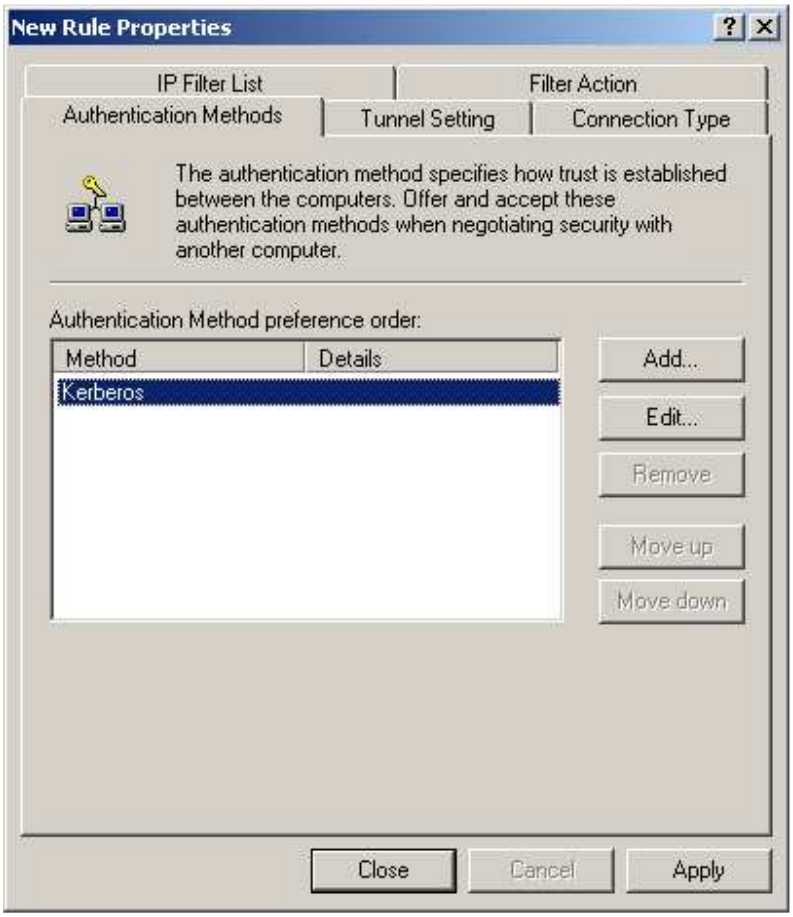

Figure 93 Authentication Methods

Step 41. Select **Use this string to protect the key exchange (preshared key)**, and then enter the Preshared Key, 123456789, in the field. *(Figure 94)*

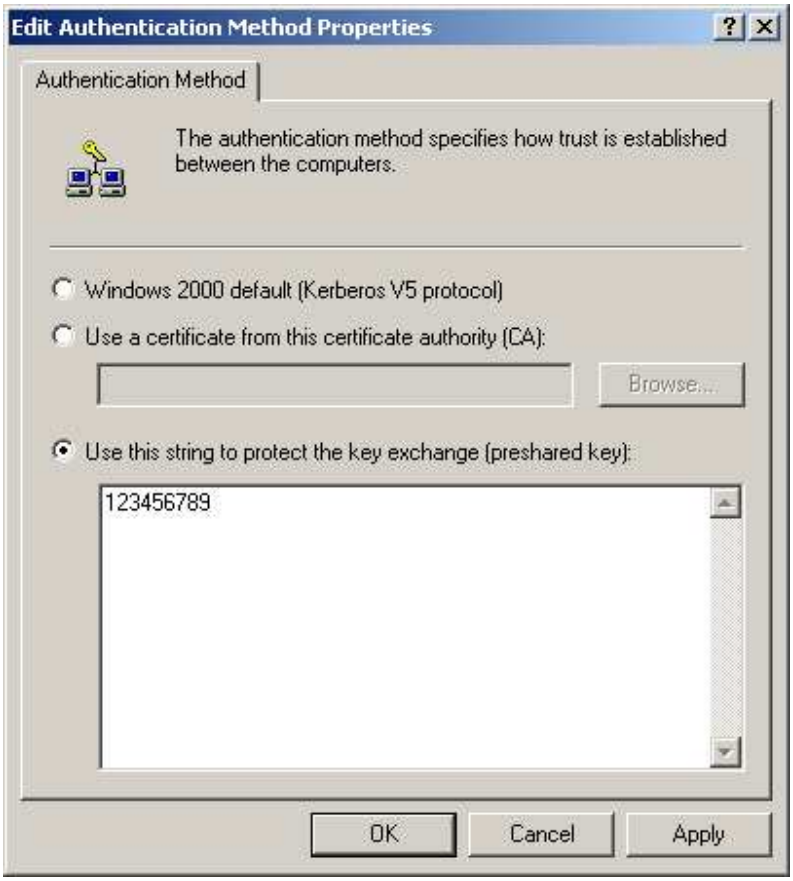

Figure 94 VPN Preshared Key Settings

Step 42. Click **Apply**, then click **Close** to close the window. *(Figure 95)*

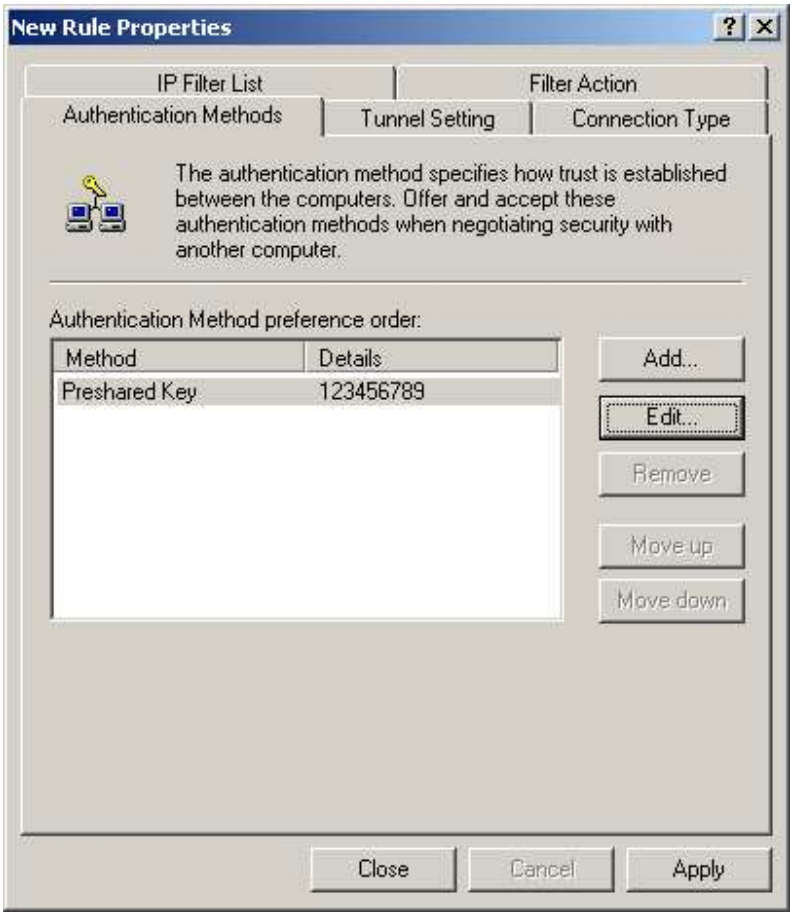

Figure 95 New Rule Settings Completed

Step 43. Configure the VPN_B LAN TO WAN settings. *(Figure 96)*

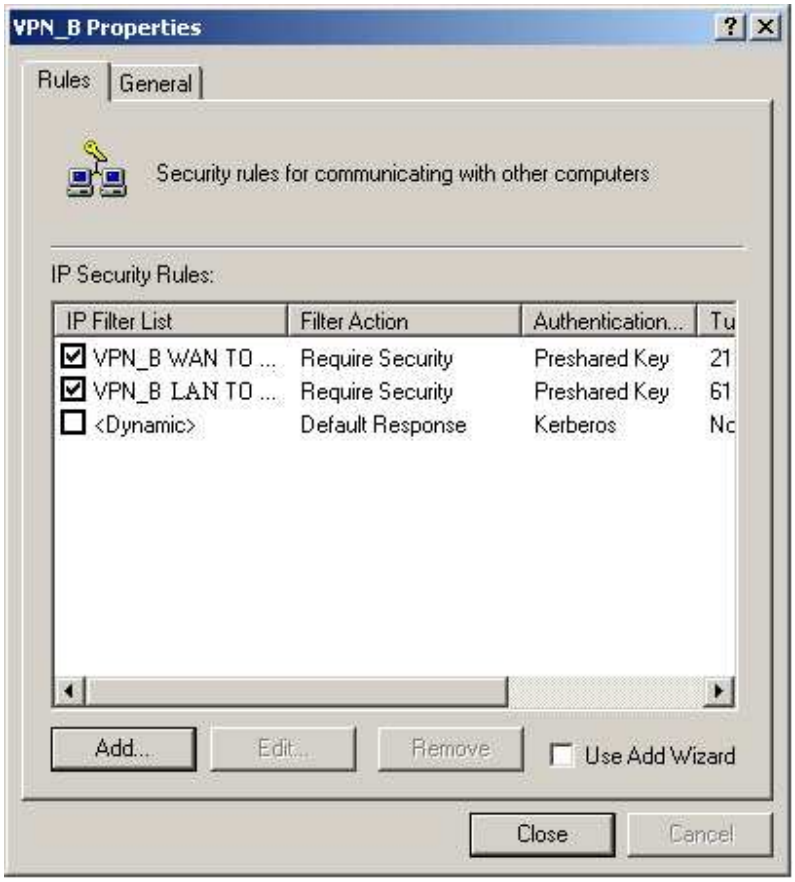

Figure 96 Complete the VPN_B LAN TO WAN Rule Settings

Step 44. In the **VPN_B Properties** window, click on the **General** tab and click on **Advanced.** *(Figure 97)*

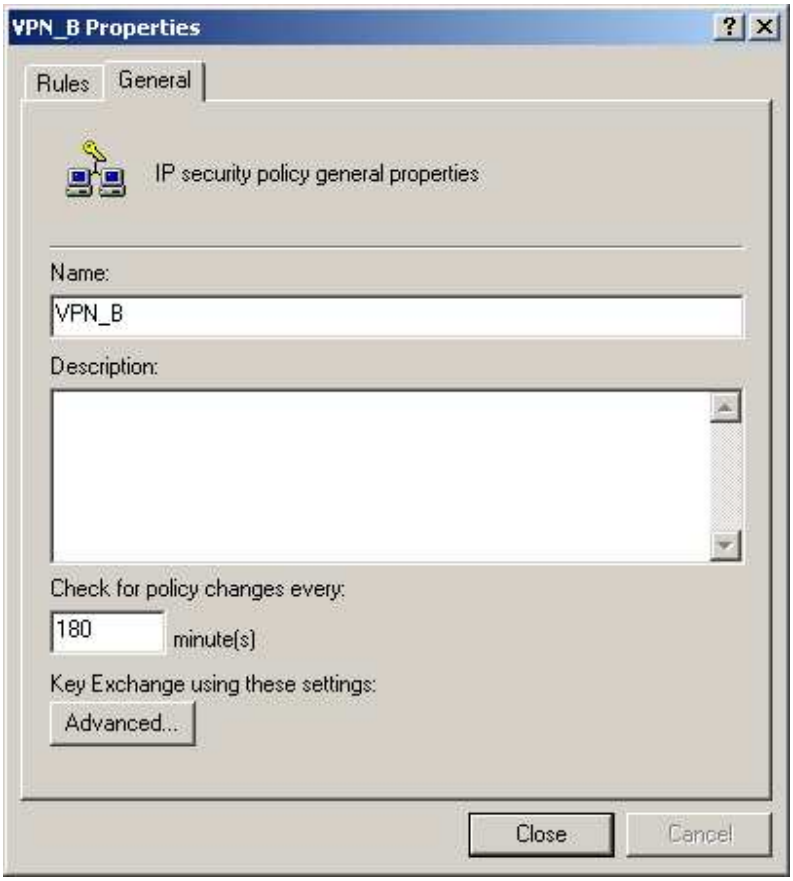

Figure 97 The VPN_B General Setting

Step 45. Check **Master Key Perfect Forward Secrecy** and then click **Methods**.

(Figure 98)

Figure 98 Key Exchange Settings

Step 46. Click **Move up** or **Move down** to arrange the order of the selected item, and click **OK**. *(Figure 99)*

Figure 99 Arranging the Security Methods

Step 47. Completion of all the Windows 2000 VPN settings. *(Figure 100)*

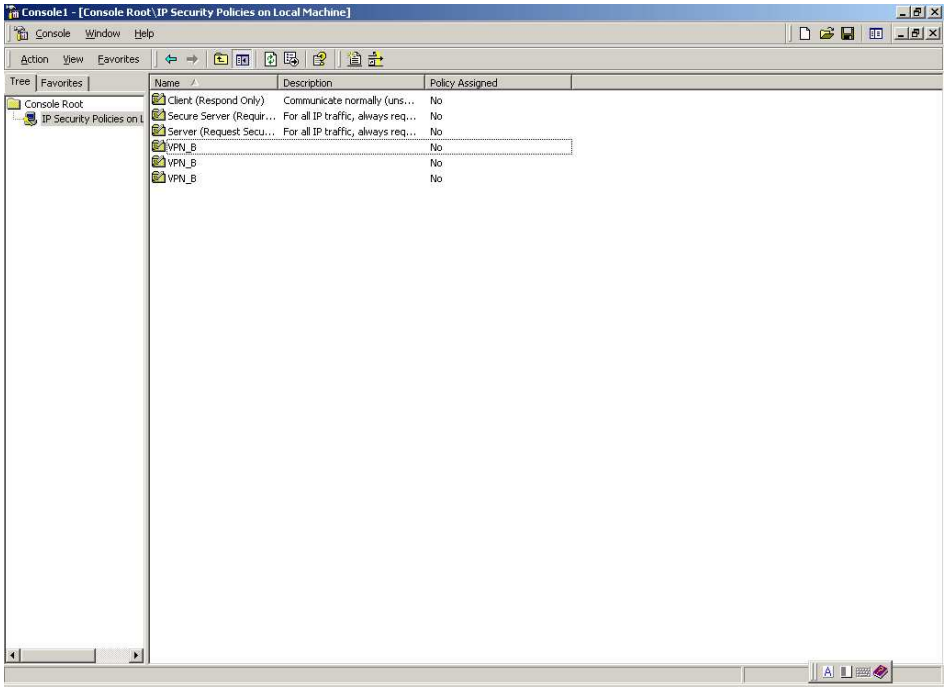

Figure 100 Windows 2000 IP Sec VPN Settings Completed

Step 48. Right-click on VPN_B and click on **Assign**. *(Figure 101)*

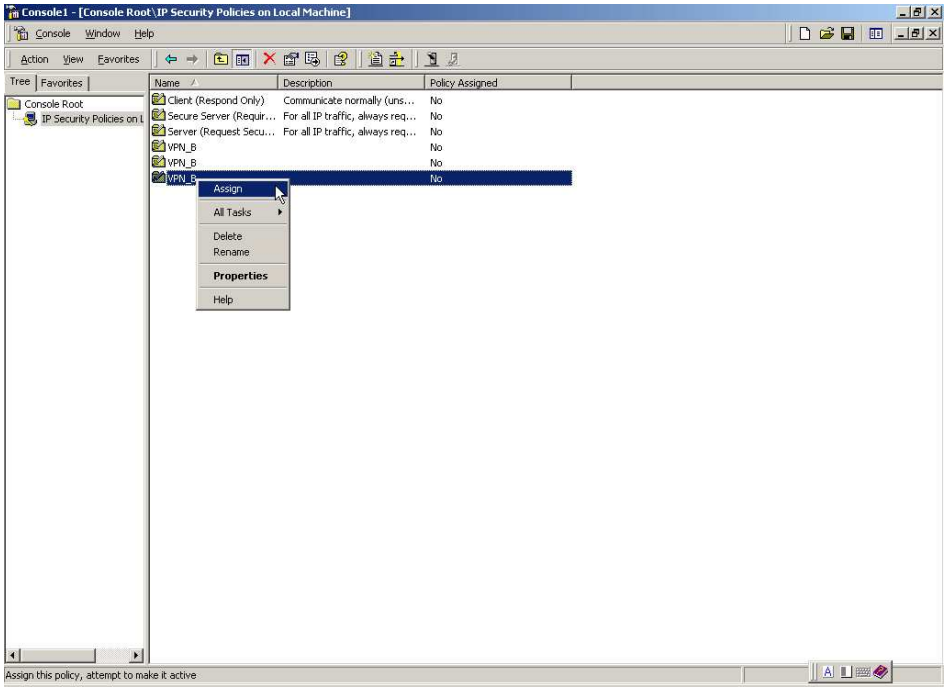

Figure 101 Assigning the VPN_B Security Rules

Step 49. The IPSec Service needs to be restarted in order for the settings to take effect. Click **Start > Setting > Control Panel**. *(Figure 102)*

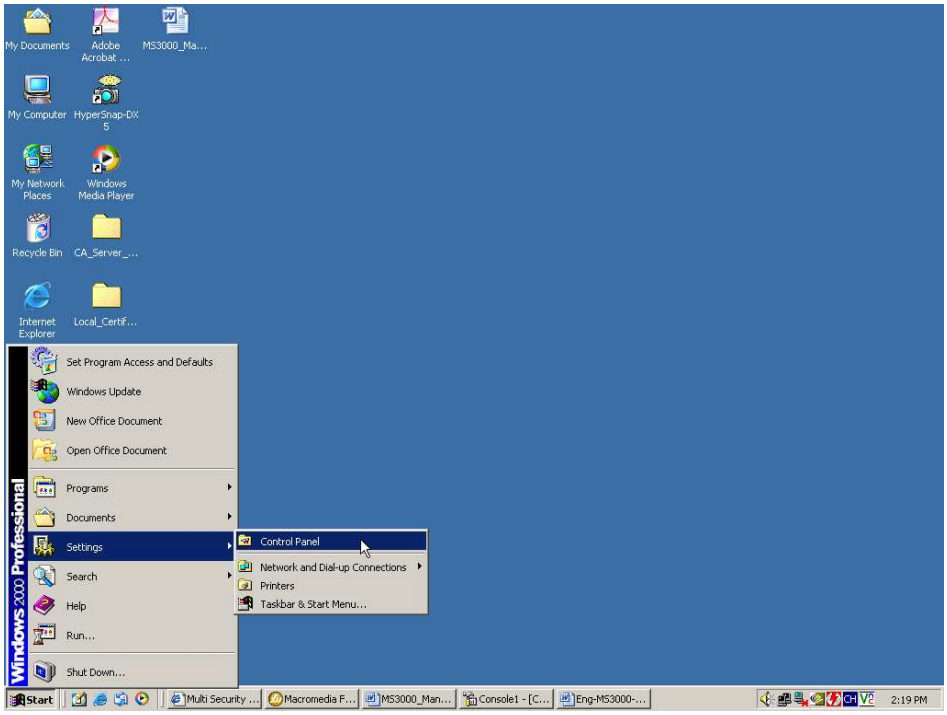

Figure 102 Enter the Control Panel

Step 50. In the **Control Panel** window, double-click on **Administrative Tools**.

(Figure 103)

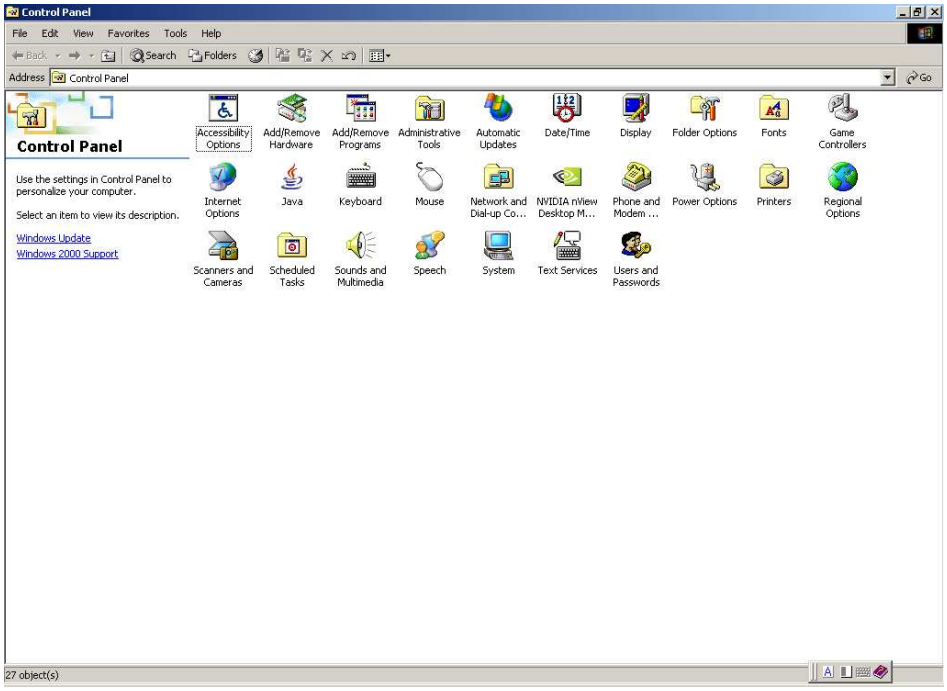

Figure 103 Enter the Administrative Tools

Step 51. In the **Administrative** Tools window, double-click on **Services**. *(Figure 104)*

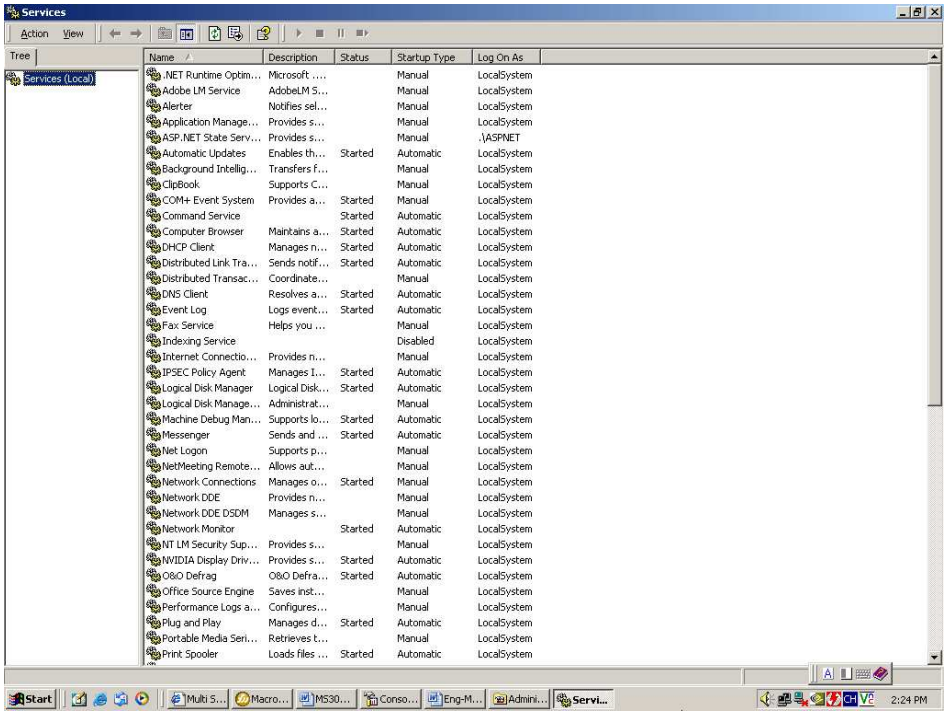

Figure 104 Enter the Services

Step 52. In the **Services** window, right-click on **IPSec Policy Agent** and click on **Restart**. *(Figure 105)*

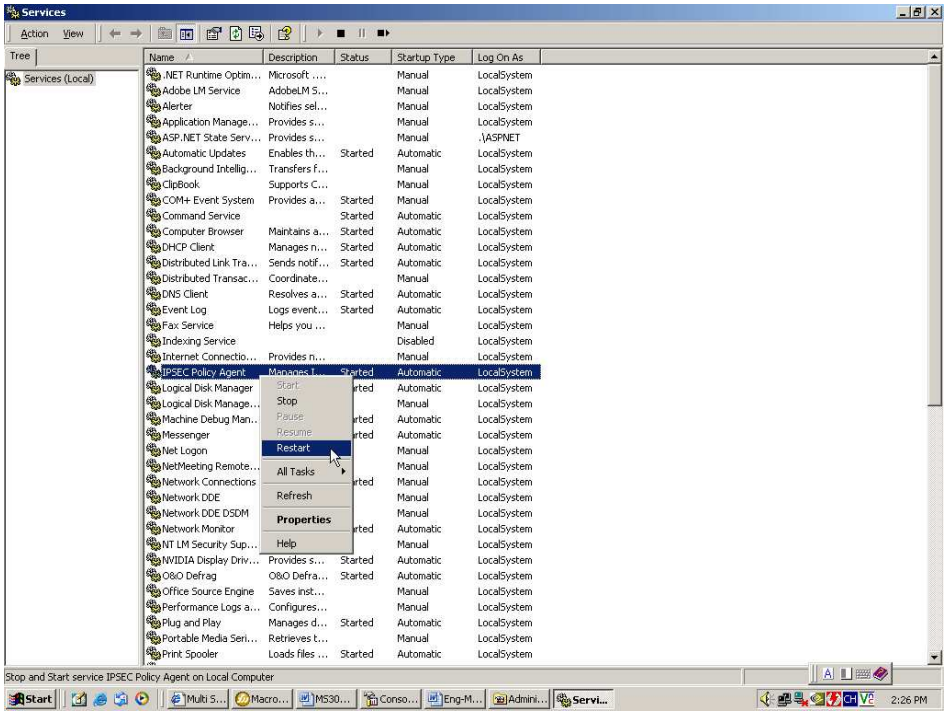

Figure 105 Restart IPSec Policy Agents

Step 53. The completed setup. *(Figure 106)*

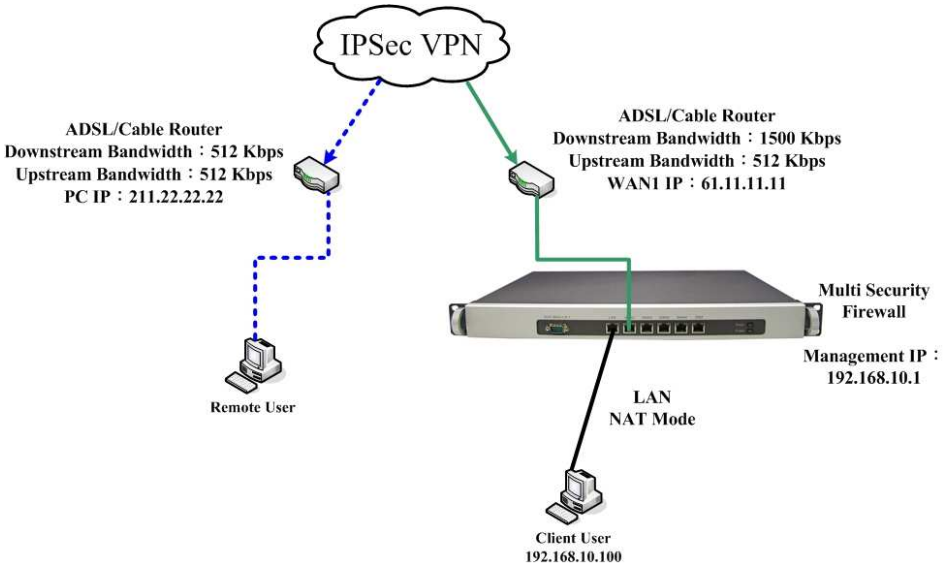

Figure 106 The NUS-MH300 and Windows 2000 IPSec VPN Deployment

Setting up an IPSec VPN Connection (Aggressive Mode) between Two NUS-MH300 Devices

Scenario:

Company A **WAN IP : 61.11.11.11** **LAN IP is 192.168.10.X**
Company B **WAN IP :211.22.22.22** **LAN IP is 192.168.20.X**

This example is based upon the use of two NUS-MH300 devices. In this scenario, Company A's internal user, 192.168.10.100, requires to create a VPN connection with Company B's internal user, 192.168.20.100, for file sharing.

The LAN IP, 192.168.10.1, is the default gateway of Company A's NUS-MH300. Proceed with the following steps:

Step 1. From within a browser, enter Company A's LAN IP address, 192.168.10.1. Go to **Policy Object** > **VPN** > **IPSec Autokey,** then click on the **New Entry** button. ***(Figure 107)***

Figure 107 IPSec Autokey

Step 2. Under the **Necessary Item** category, type **VPN_A** in the **Name** field. *(Figure 108)*

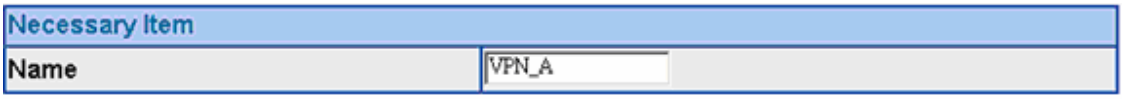

Figure 108 IPSec Autokey - Name Setting

Step 3. From within the **To Remote** category, select **Remote Gateway --Fixed IP or Domain Name**. In the field, enter the remote IP address to connect to Company B. *(Figure 109)*

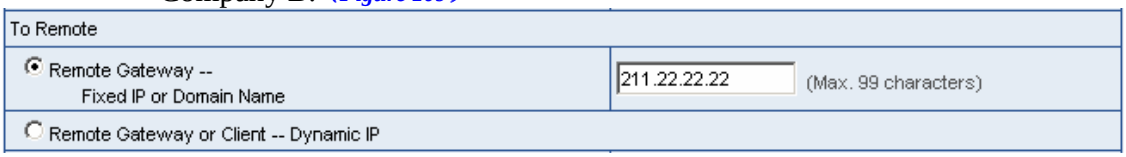

Figure 109 IPSec Autokey - To Remote Settings

Step 4. From the **Authentication Method** drop-down list, select **Preshare**. Enter the **Preshared Key** (a maximum of 103 characters). *(Figure 110)*

Figure 110 IPSec Autokey - Authentication Method Setting

Step 5. From within the **Encapsulation** category, **ISAKMP algorithms** (please refer to the Common VPN Terms section for an explanation) can be set. For the encryption algorithms, you are given choices from 3DES, DES and AES. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, you are given choices from MD5 and SHA1. Here, we have chosen **SHA1** from the **Auth Algorithm** drop-down list. From the **Group** drop-down list **GROUP2.** Please note that both VPN sites have to choose the same group. *(Figure 111)*

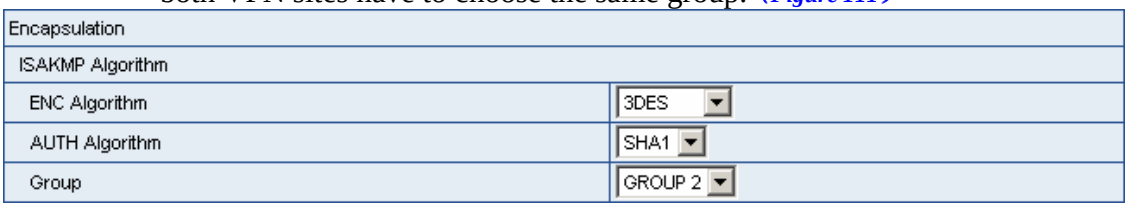

Figure 111 IPSec Encapsulation Setting

Step 6. From the **IPSec Algorithm** category**,** you can choose either **Data Encryption + Authentication** or **Authentication Only**.
Select the **Data Encryption + Authentication** option. For the encryption algorithms, you are given choices from 3DES, DES, AES-128, AES-192, AES-256 and NULL. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, **MD5** and **SHA1** are available. Choose **MD5** from the drop-down list. *(Figure 112)*

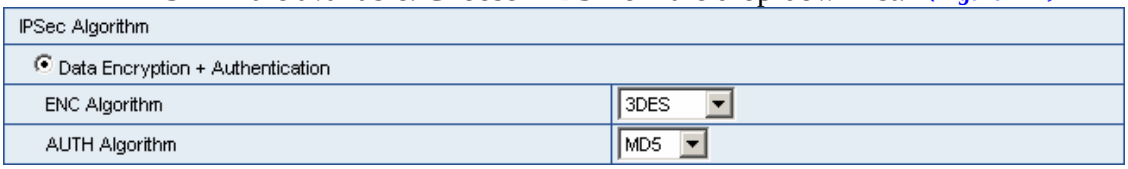

Figure 112 IPSec Algorithm Setting

Step 7. Under the **Optional Item** category, for **Perfect Forward Secrecy**, select **GROUP1** from the drop-down list. For the **ISAKMP Lifetime** field, enter 3600. For the **IPSec Lifetime** field, enter 28800. *(Figure 113)*

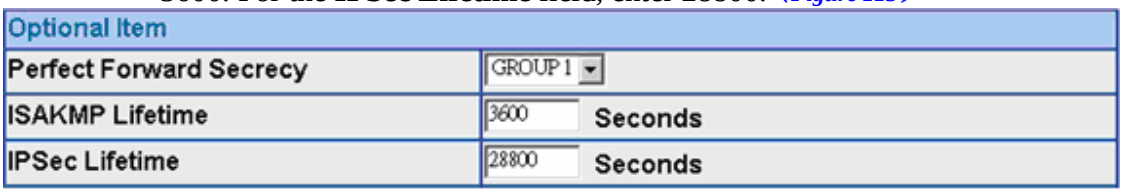

Figure 113 IPSec Autokey - Perfect Forward Secrecy Setting

Step 8. For the **Mode** option, select **Aggressive mode** (refer to the Common VPN Terms section for an explanation).
The **My ID** and **Peer ID** fields are optional.

If used, both sites will need to enter in different IP addresses, for example 11.11.11.11 and 22.22.22.22 respectively. If alphabet letters or numbers are used as ID's then they need to be preceded by the '@' character, for example, "@123a" or "@abcd1". *(Figure 114)*

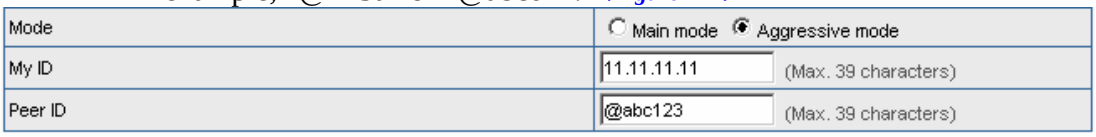

Figure 114 The IPSec Aggressive Mode Setting

Step 9. IPSec Autokey settings completed. *(Figure 115)*

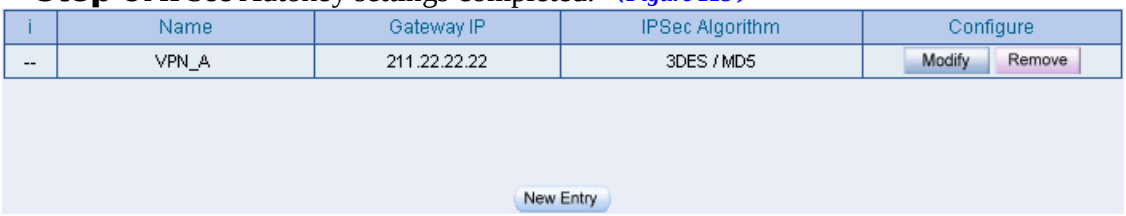

Figure 115 Company A IPSec Autokey – Settings Completed

Step 10. Go to **Policy Object > VPN > Tunnel**. Click on the **New Entry** button and then proceed with the following: *(Figure 116)*

- In the **Name** field, enter a unique name for the tunnel.
- For the **From Local** setting, select **LAN**.
- In the **Local Subnet / Mask** field, enter 192.168.10.0 / 255.255.255.0.
- From the **To Remote** category, select **To Remote Subnet / Mask** and enter 192.168.20.0 /255.255.255.0.
- From the **IPSec / PPTP Setting** drop-down list, select VPN_A.
- Check the **Show remote Network Neighborhood** checkbox.
- Click **OK**. *(Figure 117)*

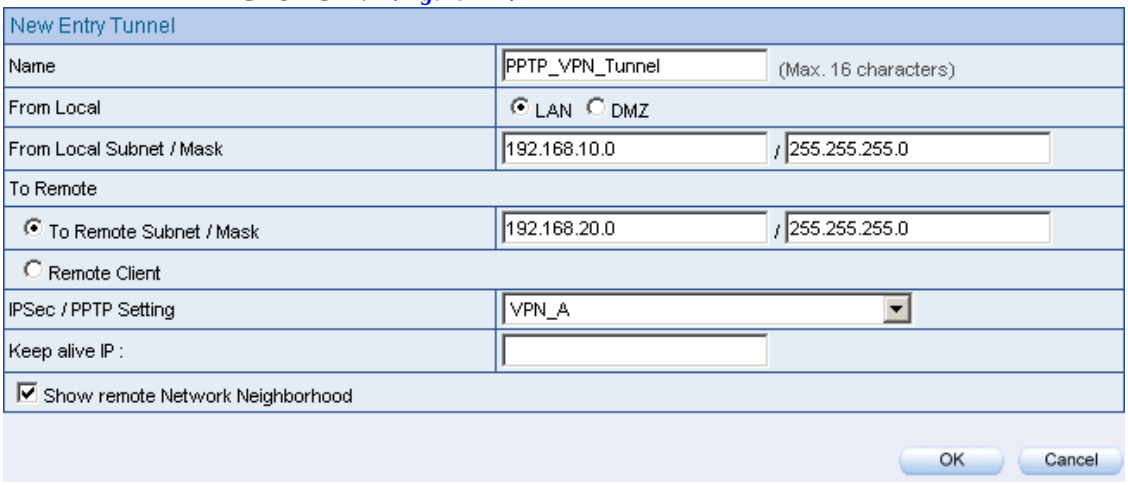

Figure 116 New Entry Tunnel Settings

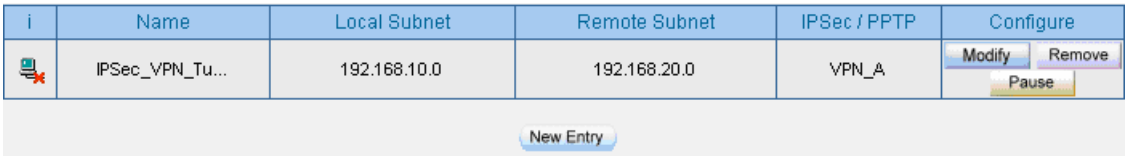

Figure 117 New Entry Tunnel Settings Completed

Step 11. Go to **Policy** > **Outgoing** then click on the **New Entry** button and configure as below: *(Figure 118)*

- **Authentication User:** Select All_NET.
- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Tunnel:** Select IPSec_VPN_Tunnel.
- Click **OK**. *(Figure 119)*

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Schedule_1
Authentication User	All_NET
Tunnel	IPSec_VPN_Tunnel
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
IM / P2P Blocking	None
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)

Figure 118 VPN Tunnel Outgoing Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove	To 1

New Entry

Figure 119 VPN Tunnel Outgoing Policy Settings Completed

Step 12. Go to **Policy** > **Incoming**, click on the **New Entry** button and enter the following settings: *(Figure 120)*

- **Schedule:** select **Schedule_1**.
- **QoS:** select **QoS_1**.
- **Tunnel:** select **IPSec_VPN_Tunnel**.
- Click **OK**. *(Figure 121)*

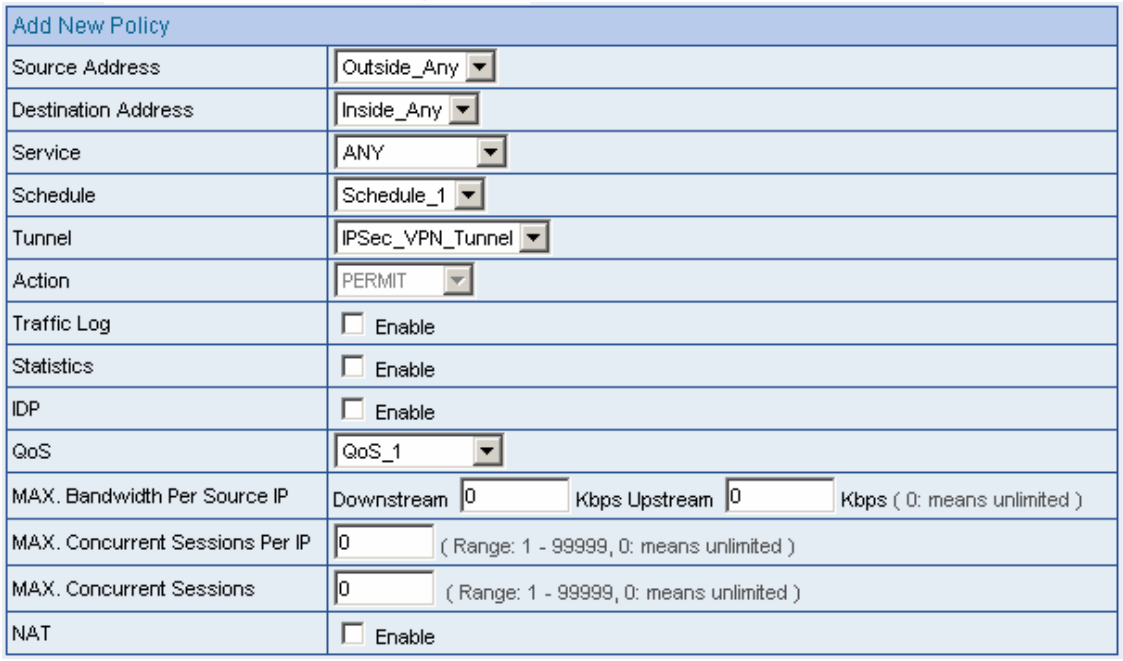

Figure 120 VPN Tunnel Incoming Policy Settings

Figure 121 VPN Tunnel Incoming Policy Settings Completed

VPN Example 3

The LAN IP, 192.168.20.1, is the default gateway of Company B's NUS-MH300. Proceed with the following steps:

Step 1. From within a browser, enter Company B's LAN IP address, 192.168.20.1. Go to **Policy Object** > **VPN** > **IPSec Autokey**, then click on the **New Entry** button. *(Figure 122)*

Figure 122 IPSec Autokey Headings

Step 2. Under the **Necessary Item** category, type **VPN_B** in the **Name** field. *(Figure 123)*

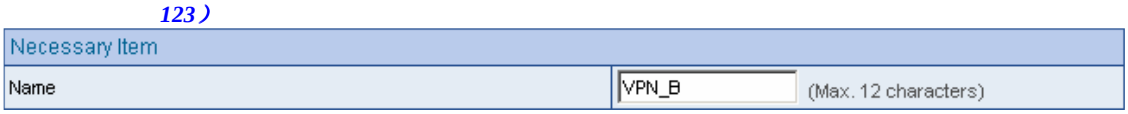

Figure 123 IPSec Autokey - Name Setting

Step 3. From within the **To Remote** category, select **Remote Gateway --Fixed IP or Domain Name**. In the field, enter the remote IP address to connect to Company A. *(Figure 124)*

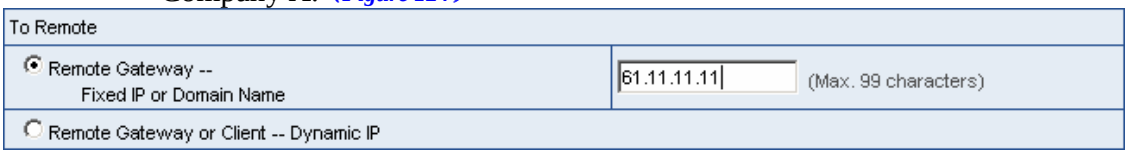

Figure 124 IPSec Autokey - To Remote Settings

Step 4. From the **Authentication Method** drop-down list, select **Preshare**. Enter the **Preshared Key** (a maximum of 103 characters). *(Figure 125)*

Figure 125 IPSec Autokey - Authentication Method Setting

Step 5. From within the **Encapsulation** category, **ISAKMP algorithms** (please refer to the Common VPN Terms section for an explanation) can be set. For the encryption algorithms, you are given choices from 3DES, DES and AES. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, you are given choices from MD5 and SHA1. Here, we have chosen **SHA1** from the **Auth Algorithm** drop-down list. From the **Group** drop-down list **GROUP2.** Please note that both VPN sites have to choose the same group. *(Figure 126)*

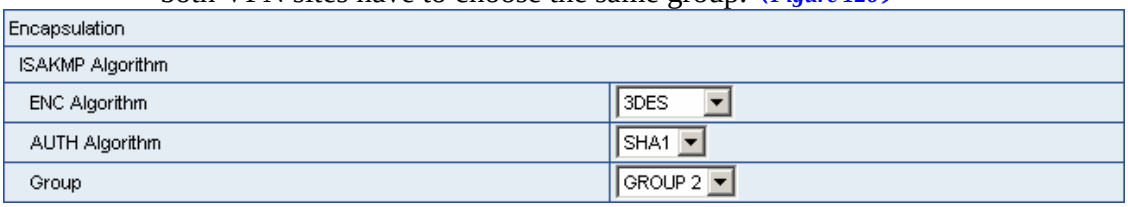

Figure 126 IPSec Encapsulation Setting

Step 6. From the **IPSec Algorithm** category**,** you can choose either **Data Encryption + Authentication** or **Authentication Only**.
Select the **Data Encryption + Authentication** option. For the encryption algorithms, you are given choices from 3DES, DES, AES-128, AES-192, AES-256 and NULL. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, **MD5** and **SHA1** are available. Choose **MD5** from the drop-down list. *(Figure 127)*

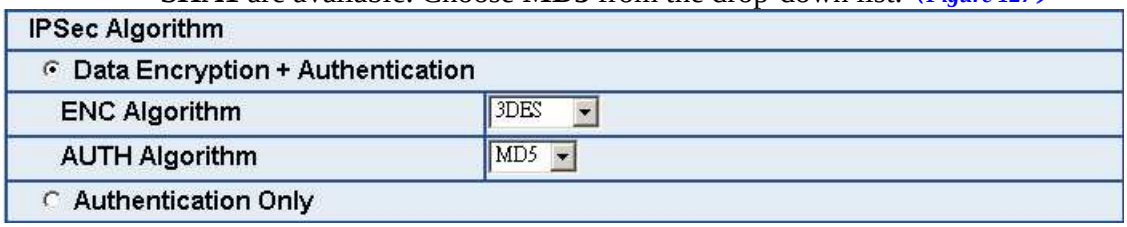

Figure 127 IPSec Algorithm Setting

Step 7. Under the **Optional Item** category, for **Perfect Forward Secrecy,** select **GROUP1** from the drop-down list. For the **ISAKMP Lifetime** field, enter 3600. For the **IPSec Lifetime** field enter 28800**.** *(Figure 128)*

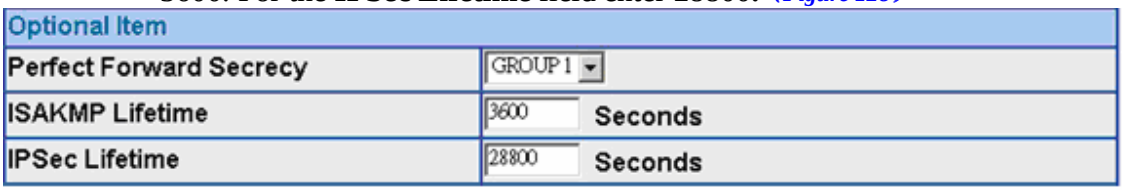

Figure 128 IPSec Autokey - Perfect Forward Secrecy Setting

Step 8. For the **Mode** option select **Aggressive mode** (refer to the Common VPN Terms section for an explanation).
The **My ID** and **Peer ID** fields are optional. If used, both sites will need to enter in different IP addresses, for example 11.11.11.11 and 22.22.22.22 respectively. If alphabet letters or numbers are used as ID's then they need to be preceded by the '@' character, for example, "@123a" or "@abcd1". *(Figure 129)*

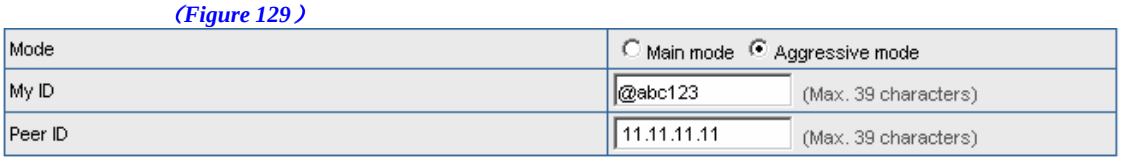

Figure 129 The IPSec Aggressive Mode Setting

Step 9. IPSec Autokey settings completed. *(Figure 130)*

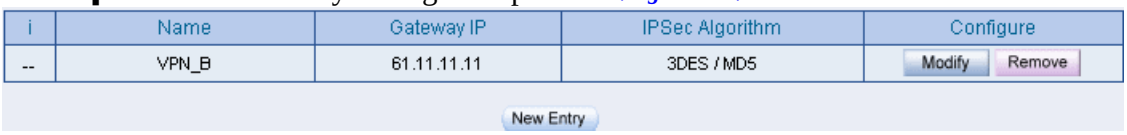

Figure 130 IPSec Autokey – Settings Completed

Step 10. Go to **VPN** > **Tunnel**. Click on the **New Entry** button and enter the following settings: *(Figure 131)*

- **Name:** Enter a specific Tunnel name.
- **From Local:** Select **LAN**.
- **From Local Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **To Remote:** Select **To Remote Subnet / Mask**.
- **To Remote Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select PPTP_Client_PPTP_Connection.
- Check **Show remote Network Neighborhood**.
- Click **OK**. *(Figure 132)*

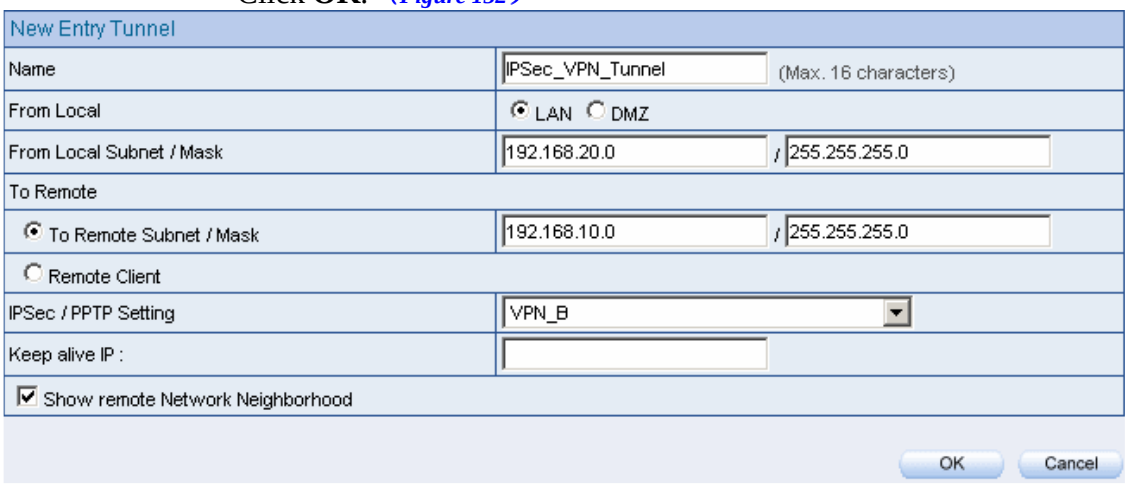

Figure 131 New Entry Tunnel Settings

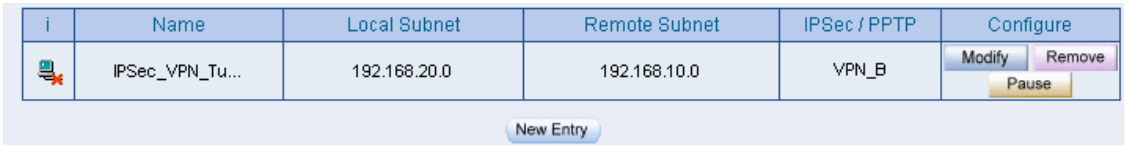

Figure 132 New Entry Tunnel Setting Completed

Step 11. Go to **Policy** > **Outgoing** then click on the **New Entry** button and configure as below: *(Figure 133)*

- **Authentication User:** Select **All_NET**.
- **Schedule:** Select **Schedule_1**.
- **QoS:** Select QoS_1.
- Select **IPSec_VPN_Tunnel** from the **Tunnel** drop-down list.
- Click **OK**. *(Figure 134)*

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Schedule_1
Authentication User	All_NET
Tunnel	IPSec_VPN_Tunnel
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
IM / P2P Blocking	None
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)

Figure 133 VPN Tunnel Outgoing Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove	To 1

New Entry

Figure 134 VPN Tunnel Outgoing Policy Settings Completed

Step 12. Go to **Policy** > **Incoming**, click on the **New Entry** button and enter the following settings: *(Figure 135)*

- **Schedule:** select **Schedule_1**.
- **QoS:** select **QoS_1**.
- **Tunnel:** select **IPsec_VPN_Tunnel**.
- Click **OK**. *(Figure 136)*

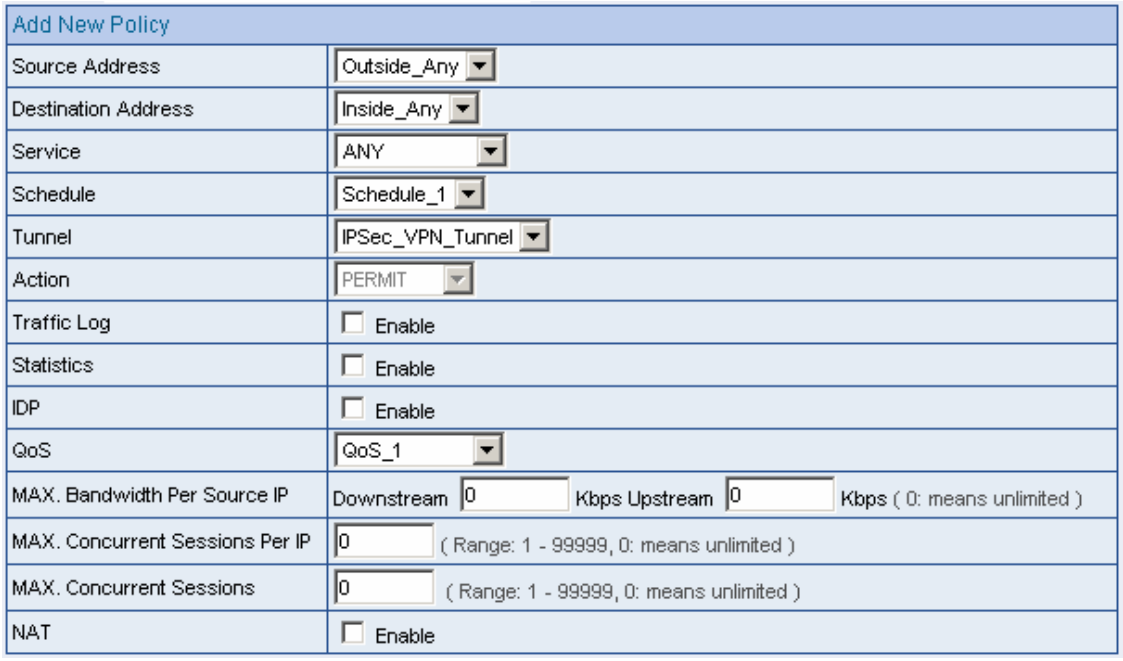

Figure 135 VPN Tunnel Incoming Policy Settings

Figure 136 VPN Tunnel Incoming Policy Settings Completed

Step 13. The completed IPSec VPN aggressive mode connection setup *(Figure 137)*

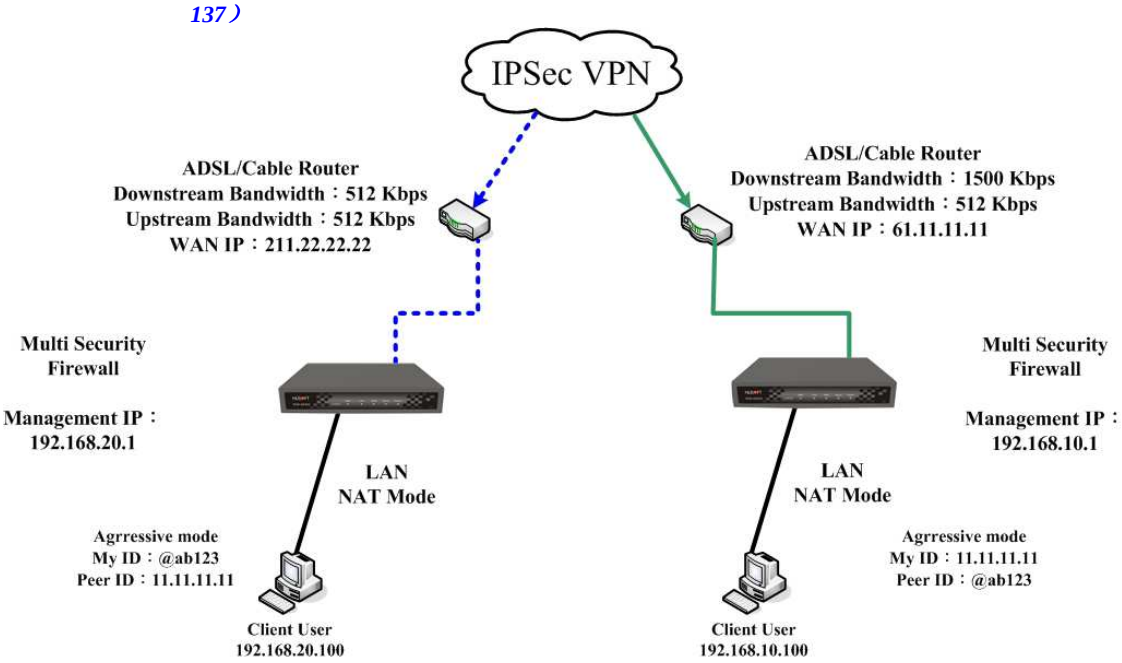

Figure 137 Completed Setup

VPN | Example 4

Setting up an IPSec VPN Connection between Two NUS-MH300 Devices

(Using GRE/IPSec Packet Encapsulation Algorithm)

Scenario:

Company A	**WAN IP: 61.11.11.11**	**LAN IP: 192.168.10.X**
Company B	**WAN IP: 211.22.22.22**	**LAN IP: 192.168.20.X**

This example is based upon the use of two NUS-MH300 devices. In this scenario, Company A's internal user, 192.168.10.100, requires to create a VPN connection with Company B's internal user, 192.168.20.100, for file sharing (Using **GRE/IPSec packet encapsulation algorithm** for the connection).

The LAN IP, 192.168.10.1, is the default gateway of Company A's NUS-MH300. Proceed with the following steps:

Step 1. From within a browser, enter Company A's LAN IP address, 192.168.10.1. Go to **Policy Object** > **VPN** > **IPSec Autokey** then click on the **New Entry** button. *(Figure 138)*

Figure 138 IPSec Autokey Headings

Step 2. Under the **Necessary Item** category, type **VPN_A** in the **Name** field. *(Figure 139)*

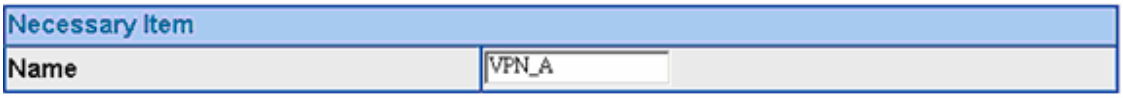

Figure 139 IPSec Autokey - Name Setting

Step 3. From within the **To Remote** category, select **Remote Gateway --Fixed IP or Domain Name**. In the field, enter the remote IP address to connect to Company B. *(Figure 140)*

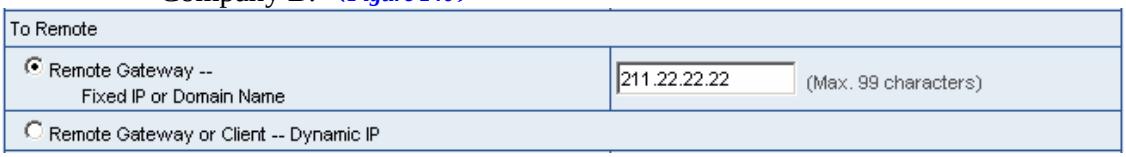

Figure 140 IPSec Autokey - To Remote Settings

Step 4. From the **Authentication Method** drop-down list, select **Preshare**. Enter the **Preshared Key** (a maximum of 103 characters). *(Figure 141)*

Figure 141 IPSec Autokey - Authentication Method Setting

Step 5. From within the **Encapsulation** category, **ISAKMP algorithms** (please refer to the Common VPN Terms section for an explanation) can be set. For the encryption algorithms, you are given choices from 3DES, DES and AES. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, you are given choices from MD5 and SHA1. Here, we have chosen **MD5** from the **Auth Algorithm** drop-down list. From the **Group** drop-down list **GROUP1.** Please note that both VPN sites have to choose the same group. *(Figure 142)*

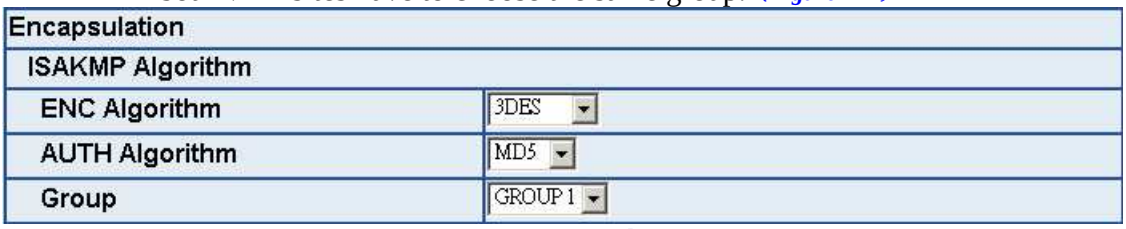

Figure 142 IPSec Encapsulation Setting

Step 6. From the **IPSec Algorithm** category**,** you can choose either **Data Encryption + Authentication** or **Authentication Only**.

Select the **Data Encryption + Authentication** option. For the encryption algorithms, you are given choices from 3DES, DES, AES-128, AES-192, AES-256 and NULL. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, **MD5** and **SHA1** are available. Choose **MD5** from the drop-down list. *(Figure 143)*

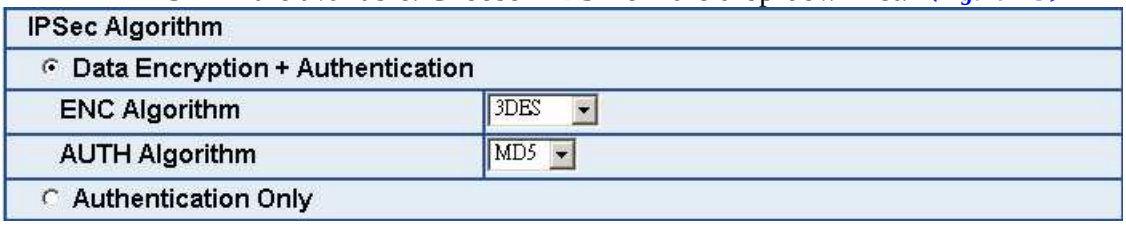

Figure 143 IPSec Algorithm Setting

Step 7. Under the **Optional Item** category, for **Perfect Forward Secrecy** select **GROUP1** from the drop-down list. For the **ISAKMP Lifetime** field, enter 3600. For the **IPSec Lifetime** field, enter 28800**.** Select the **Main mode** radio button from the **Mode** section. *(Figure 144)*

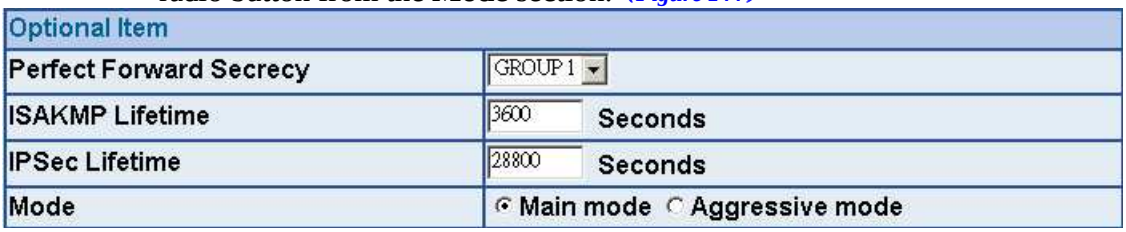

Figure 144 IPSec Autokey - Perfect Forward Secrecy Setting

Step 8. Enter 192.168.50.100 in the **GRE Local IP** field. Enter 192.168.50.200 in the **GRE Remote IP**. *(Figure 145)*

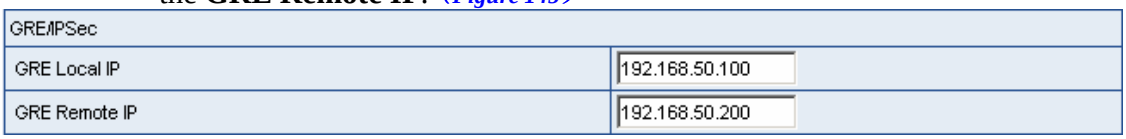

Figure 145 GRE/IPSec Settings

Step 9. IPSec Autokey settings completed. *(Figure 146)*

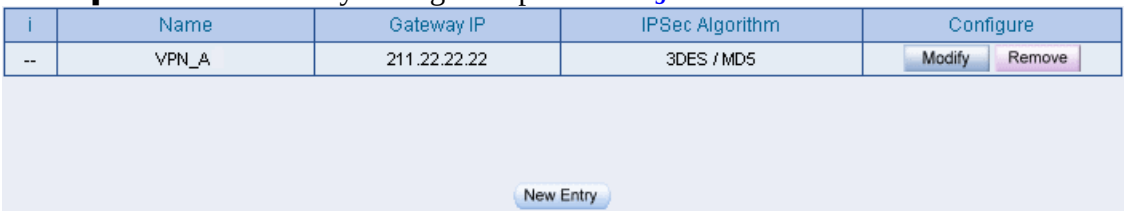

Figure 146 Company A IPSec Autokey – Settings Completed

Step 10. Go to **Policy Object > VPN > Tunnel**. Click on the **New Entry** button and then proceed with the following: *(Figure 147)*

- In the **Name** field, enter a unique name for the tunnel.
- For the **From Local** setting, select **LAN.**
- In the **Local Subnet / Mask** field, enter 192.168.10.0 / 255.255.255.0.
- From the **To Remote** category, select **To Remote Subnet / Mask** and enter 192.168.20.0 /255.255.255.0.
- From the **IPSec / PPTP Setting** drop-down list, select VPN_A.
- Check the **Show remote Network Neighborhood** checkbox.
- Click **OK**. *(Figure 148)*

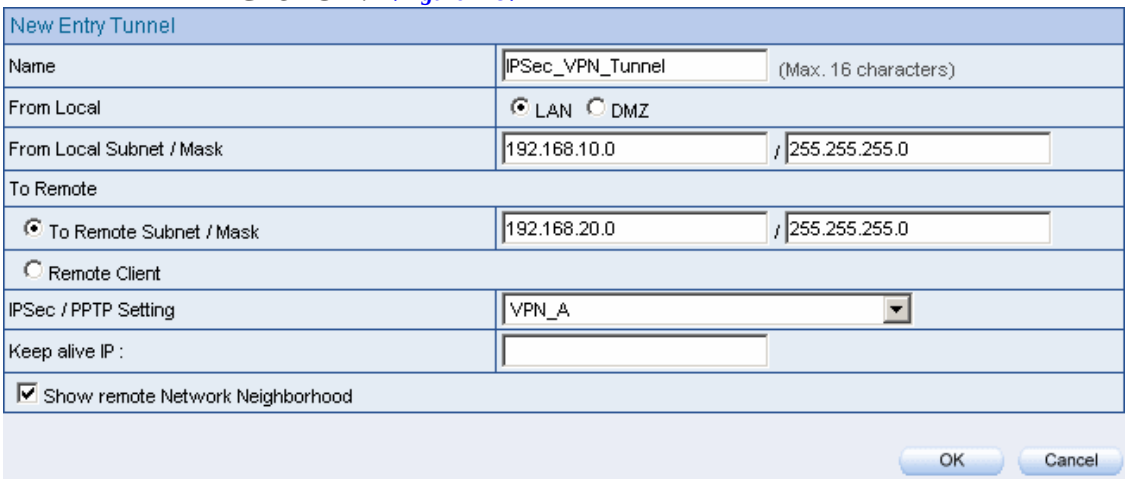

Figure 147 New Entry Tunnel Settings

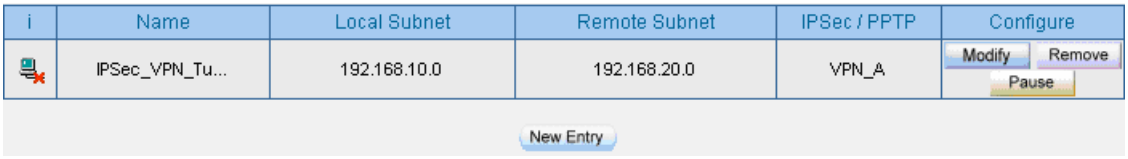

Figure 148 New Entry Tunnel Settings Completed

Step 11. Go to **Policy** > **Outgoing** then click on the **New Entry** button and configure as below: *(Figure 149)*

- **Authentication User:** Select All_NET.
- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Tunnel:** Select IPSec_VPN_Tunnel.
- Click **OK**. *(Figure 150)*

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Schedule_1
Authentication User	All_NET
Tunnel	IPSec_VPN_Tunnel
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
IM / P2P Blocking	None
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)

Figure 149 VPN Tunnel Outgoing Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove	To 1

New Entry

Figure 150 VPN Tunnel Outgoing Policy Settings Completed

Step 12. Go to **Policy** > **Incoming**, click on the **New Entry** button and enter the following settings: *(Figure 151)*

- **Schedule:** select **Schedule_1**.
- **QoS:** select **QoS_1**.
- **Tunnel:** select **IPSec_VPN_Tunnel**.
- Click **OK**. *(Figure 152)*

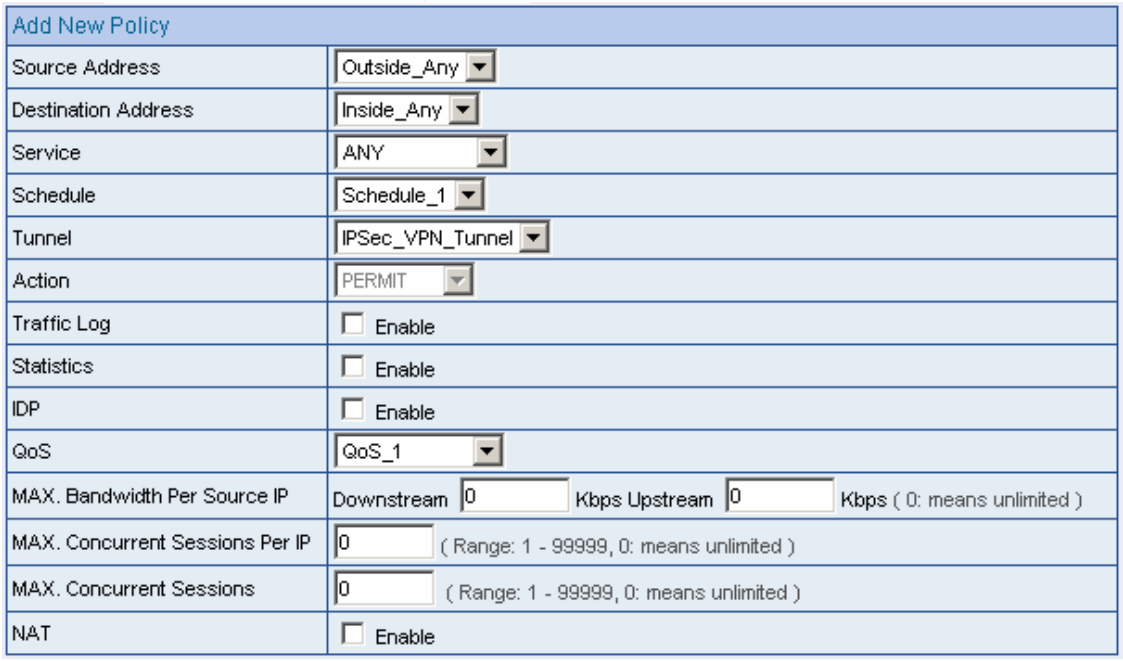

Figure 151 VPN Tunnel Incoming Policy Settings

Figure 152 VPN Tunnel Incoming Policy Settings Completed

VPN Example 4

The LAN IP, 192.168.20.1, is the default gateway of Company B's NUS-MH300. Proceed with the following steps:

Step 1. From within a browser, enter Company B's LAN IP address, 192.168.20.1. Go to **Policy Object** > **VPN** > **IPSec Autokey** then click on the **New Entry** button. *(Figure 153)*

Figure 153 IPSec Autokey Headings

Step 2. Under the **Necessary Item** category, enter **VPN_B** in the **Name** field. *(Figure 154)*

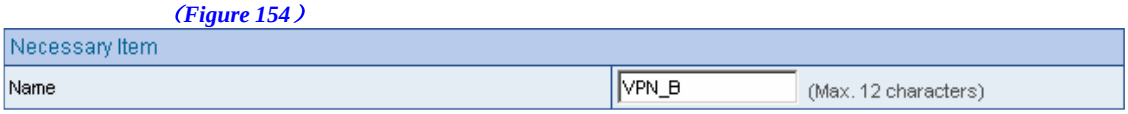

Figure 154 IPSec Autokey - Name Setting

Step 3. From within the **To Remote** category, select **Remote Gateway --Fixed IP or Domain Name**. In the field, enter the remote IP address to connect to Company A. *(Figure 155)*

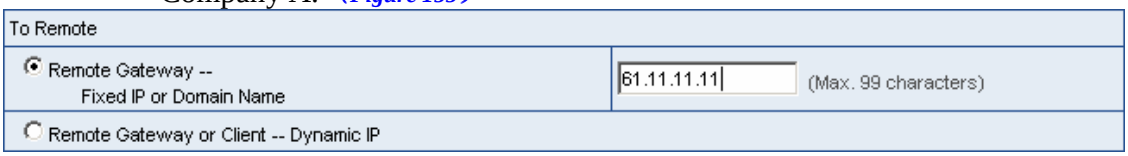

Figure 155 IPSec Autokey - To Remote Settings

Step 4. From the **Authentication Method** drop-down list, select **Preshare**. Enter the **Preshared Key** (a maximum of 103 characters) *(Figure 156)*

Figure 156 IPSec Autokey - Authentication Method Setting

Step 5. From within the **Encapsulation** category, **ISAKMP algorithms** (please refer to the Common VPN Terms section for an explanation) can be set. For the encryption algorithms, you are given choices from 3DES, DES and AES. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, you are given choices from MD5 and SHA1. Here, we have chosen **MD5** from the **Auth Algorithm** drop-down list. From the **Group** drop-down list **GROUP1.** Please note that both VPN sites have to choose the same group. *(Figure 157)*

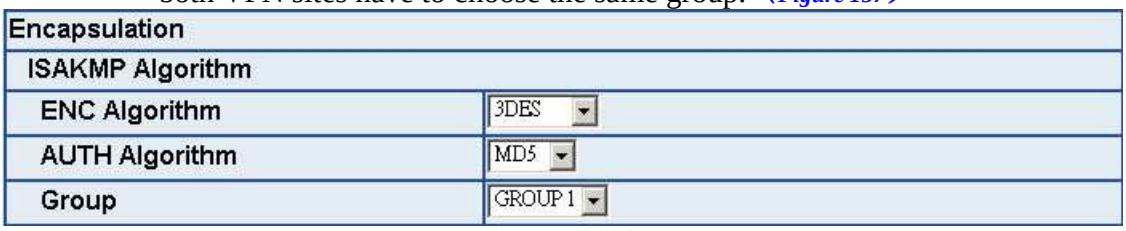

Figure 157 IPSec Encapsulation Setting

Step 6. From the **IPSec Algorithm** category**,** you can choose either **Data Encryption + Authentication** or **Authentication Only**. Select the **Data Encryption + Authentication** option. For the encryption algorithms, you are given choices from 3DES, DES, AES-128, AES-192, AES-256 and NULL. In this example, we have chosen **3DES** from the **ENC Algorithm** drop-down list. For the authentication algorithms, **MD5** and **SHA1** are available. Choose **MD5** from the drop-down list. *(Figure 158)*

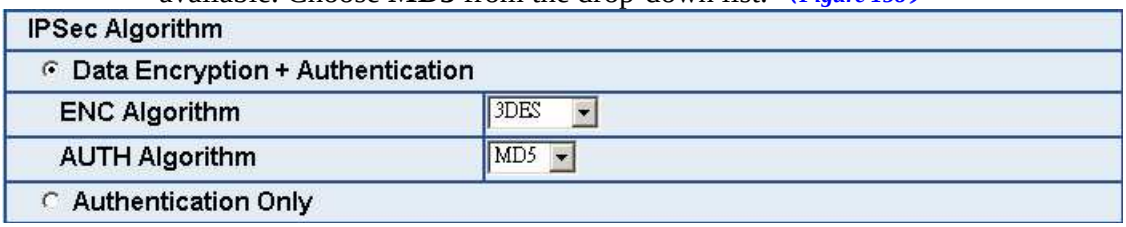

Figure 158 IPSec Algorithm Setting

Step 7. From the **Perfect Forward Secrecy** drop-down list, select **GROUP1**. In the **ISAKMP Lifetime** field, enter 3600 seconds. For the **IPSec Lifetime**, enter 28800 seconds. In the **Mode** option, select **Main mode**. *(Figure 159)*

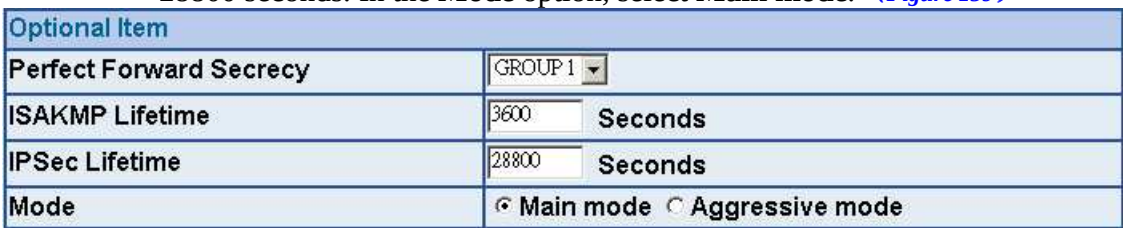

Figure 159 IPSec Perfect Forward Secrecy Settings

Step 8. Under the **GRE/IPSec** category and inside the **GRE Local IP** field, enter 192.168.50.200. For the **GRE Remote IP** field, enter 192.168.50.100. *(Figure 160)*

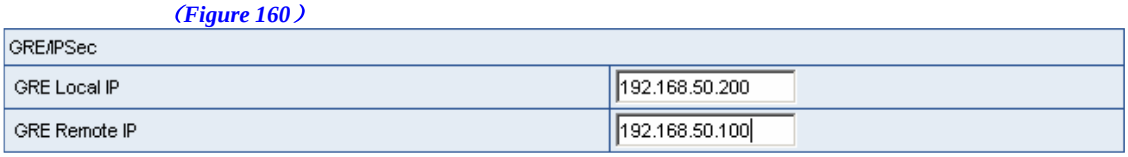

Figure 160 GRE/IPSec Settings

Step 9. IPSec Autokey settings completed. *(Figure 161)*

Figure 161 Company B IPSec Autokey Settings Completed

Step 10. Go to **VPN** > **Tunnel**. Click on the **New Entry** button and enter the following settings: *(Figure 162)*

- **Name:** Enter a specific Tunnel name.
- **From Local:** Select **LAN**.
- **From Local Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **To Remote:** Select **To Remote Subnet / Mask**.
- **To Remote Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select **PPTP_Client_PPTP_Connection**.
- Check **Show remote Network Neighborhood**.
- Click **OK**. *(Figure 163)*

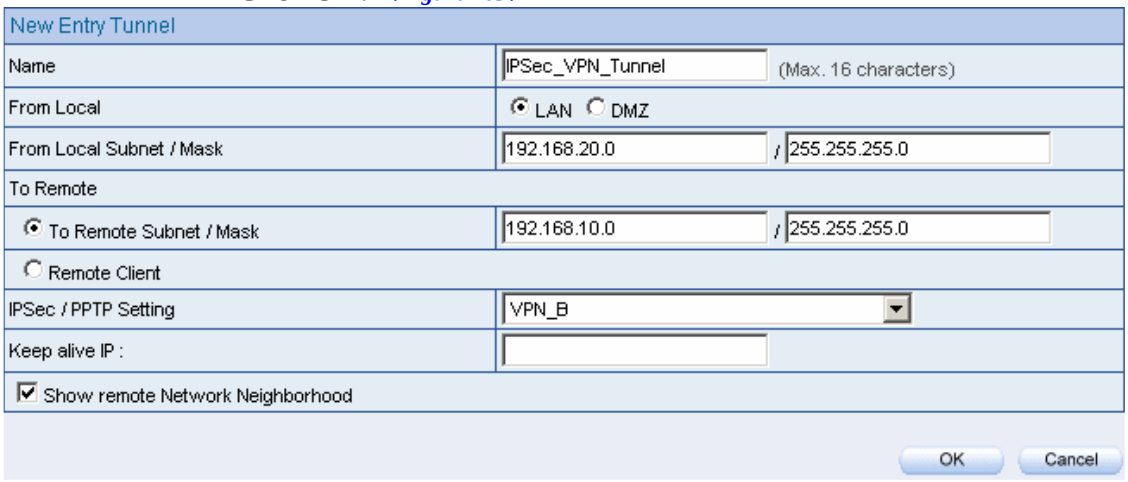

Figure 162 New Entry Tunnel Settings

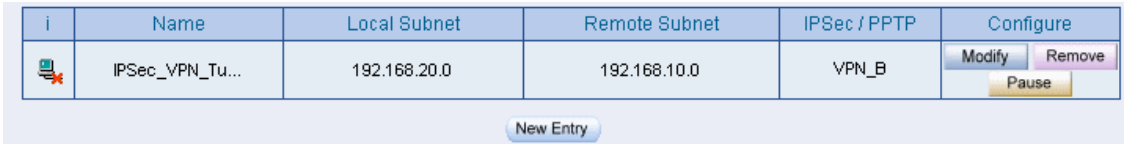

Figure 163 New Entry Tunnel Settings Completed

Step 11. Go to **Policy** > **Outgoing** then click on the **New Entry** button and configure as below: *(Figure 164)*

- **Authentication User:** Select **All_NET**.
- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Tunnel:** Select.
- Click **OK**. *(Figure 165)*

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Schedule_1
Authentication User	All_NET
Tunnel	IPSec_VPN_Tunnel
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
Content Blocking	Enable
IM / P2P Blocking	None
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)

Figure 164 VPN Tunnel Outgoing Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove	To 1

New Entry

Figure 165 VPN Tunnel Outgoing Policy Settings Completed

Step 12. Go to **Policy** > **Incoming**, click on the **New Entry** button and enter the following settings: *(Figure 166)*

- **Schedule:** select **Schedule_1**.
- **QoS:** select **QoS_1.**
- **Tunnel:** select **IPSec_VPN_Tunnel.**
- Click **OK**. *(Figure 167)*

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Schedule_1
Tunnel	IPSec_VPN_Tunnel
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
IDP	Enable
QoS	QoS_1
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
NAT	Enable

Figure 166 VPN Tunnel Incoming Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove	To 1

New Entry

Figure 167 VPN Tunnel Incoming Policy Settings Completed

Step 13. The Completed IPSec VPN GRE/IPSec Connection Setup *(Figure 168)*

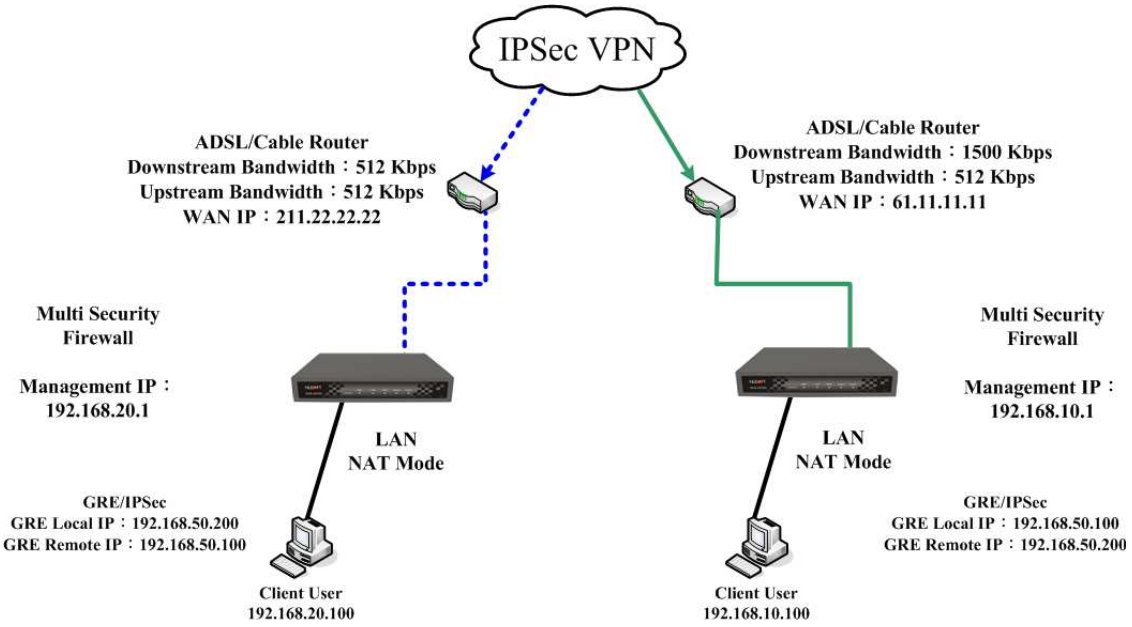

Figure 168 Completed Setup

VPN Example 5

Setting Up a PPTP VPN Connection between Two NUS-MH300 Devices

Scenario:

Company A	**WAN IP: 61.11.11.11**
	LAN IP: 192.168.10.X
Company B	**WAN IP: 211.22.22.22**
	LAN IP: 192.168.20.X

This example is based upon two NUS-MH300 devices. In this scenario, Company B's internal user, 192.168.20.100, requires a VPN connection with Company A's internal user, 192.168.10.100, so that he/she can download a file.

The LAN IP, 192.168.10.1, is the default gateway of Company A's NUS-MH300. Proceed with the following steps:

Step 1. Using Company A's NUS-MH300, go to **Policy Object** > **VPN** > **PPTP Server**. Click on the **Modify** button and configure the following:

- Select **Enable PPTP**.
- Check **Encryption**.
- **Client IP Range:** enter 192.44.75.1-254.
- **Auto-Disconnect if idle:** enter 0. *(Figure 169)*

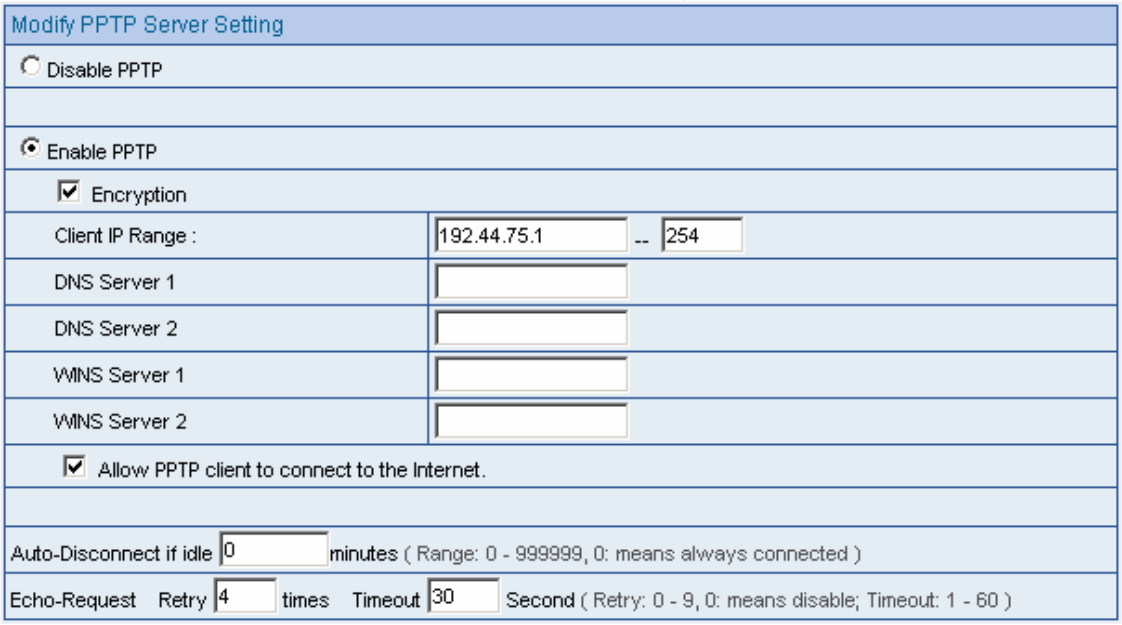

Figure 169 Enable PPTP VPN Server Settings

When a VPN connection is made between external users and the PPTP server of the NUS-MH300, IT administrators can decide whether to permit or block their access.

Idle Time: This nominates the time (in minutes) that the VPN connection will remain active after no activity has taken place.

Step 2. Using Company A's NUS-MH300, go to **Policy Object** > **VPN** > **PPTP Server.** Click on the **New Entry** button and configure the following: *(Figure 170)*

- **User Name**: Enter **PPTP_Connection**.
- **Password**: Enter 123456789.
- From the **Client IP assigned by** category select **IP Range**.
- Click **OK**. *(Figure 171)*

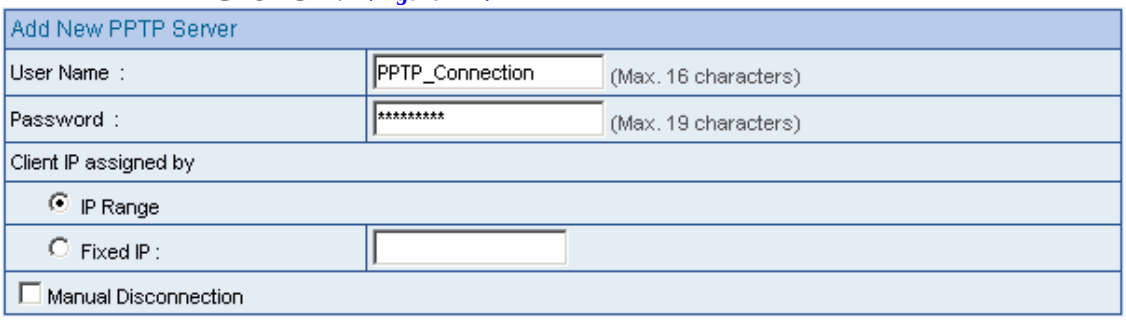

Figure 170 PPTP VPN Server Settings

Figure 171 PPTP VPN Server Settings Completed

Step 3. Go to **Policy Object** > **VPN** > **Tunnel.** Click on the **New Entry** button and enter the following settings: *(Figure 172)*

- **Name**: Enter a unique name for the Tunnel.
- **From Local:** Select **LAN**.
- **From Local Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **To Remote:** Select **Remote Client**.
- **IPSec / PPTP Setting:** Select **PPTP_Server_PPTP_Connection**.
- Check **Show remote Network Neighborhood**.
- Click **OK**. *(Figure 173)*

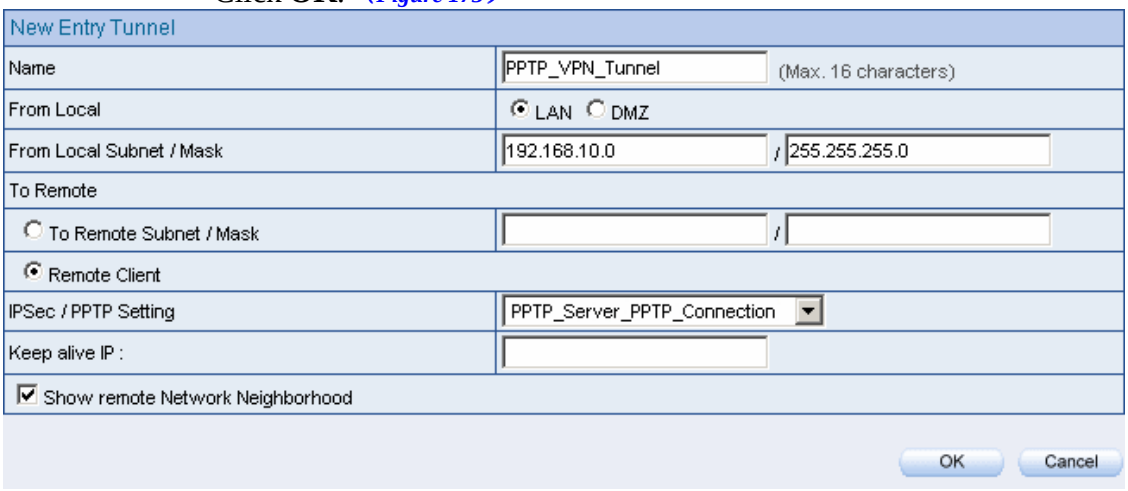

Figure 172 New Entry Tunnel Setting

Figure 173 VPN Tunnel Settings Completed

Step 4. Go to **Policy** > **Outgoing** and click on the **New Entry** button and enter the following settings: *(Figure 174)*

- **Authentication User:** Select **All_NET**.
- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Tunnel:** Select **PPTP_VPN_Tunnel**.
- Click **OK**. *(Figure 175)*

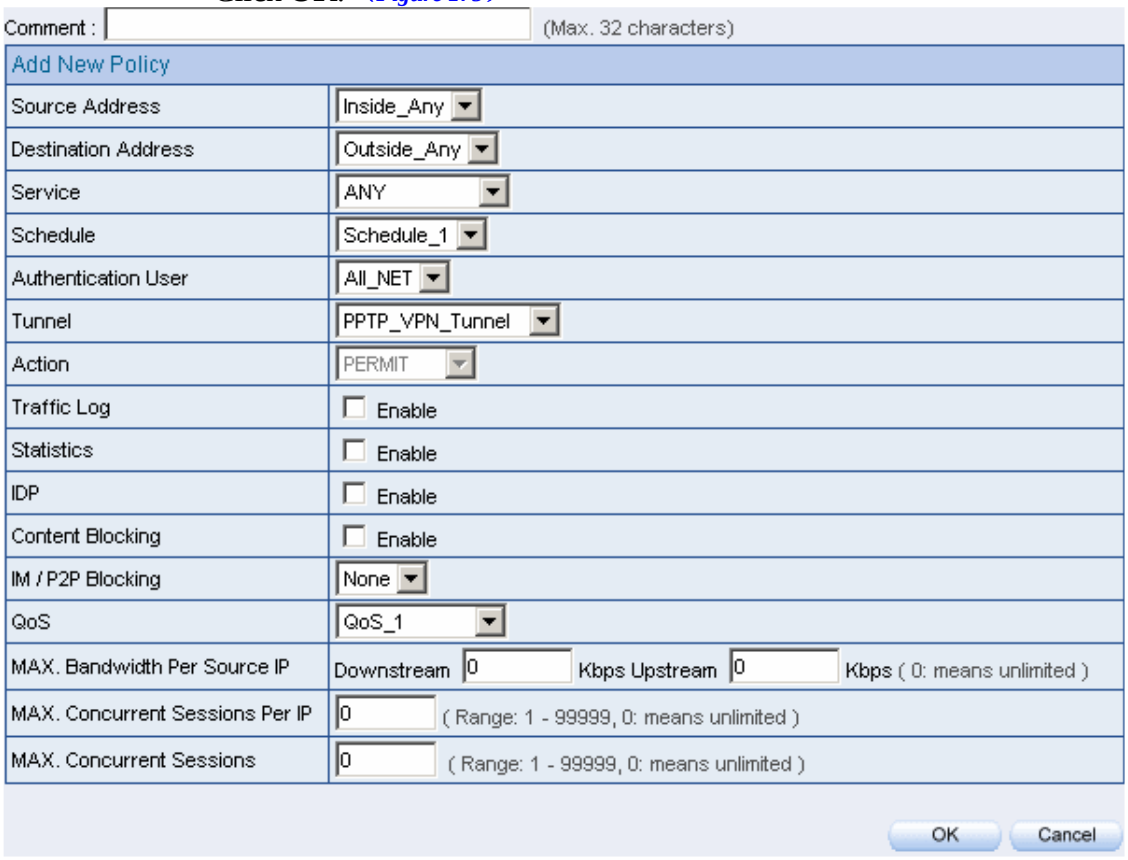

Figure 174 VPN Tunnel Outgoing Policy Settings

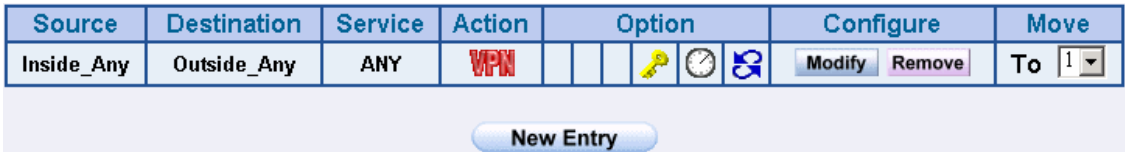

Figure 175 VPN Tunnel Outgoing Policy Settings Completed

Step 5. Go to **Policy** > **Incoming.** Click on the **New Entry** button and enter the following settings: *(Figure 176)*

- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Tunnel:** Select **PPTP_VPN_Tunnel**.
- Click **OK**. *(Figure 177)*

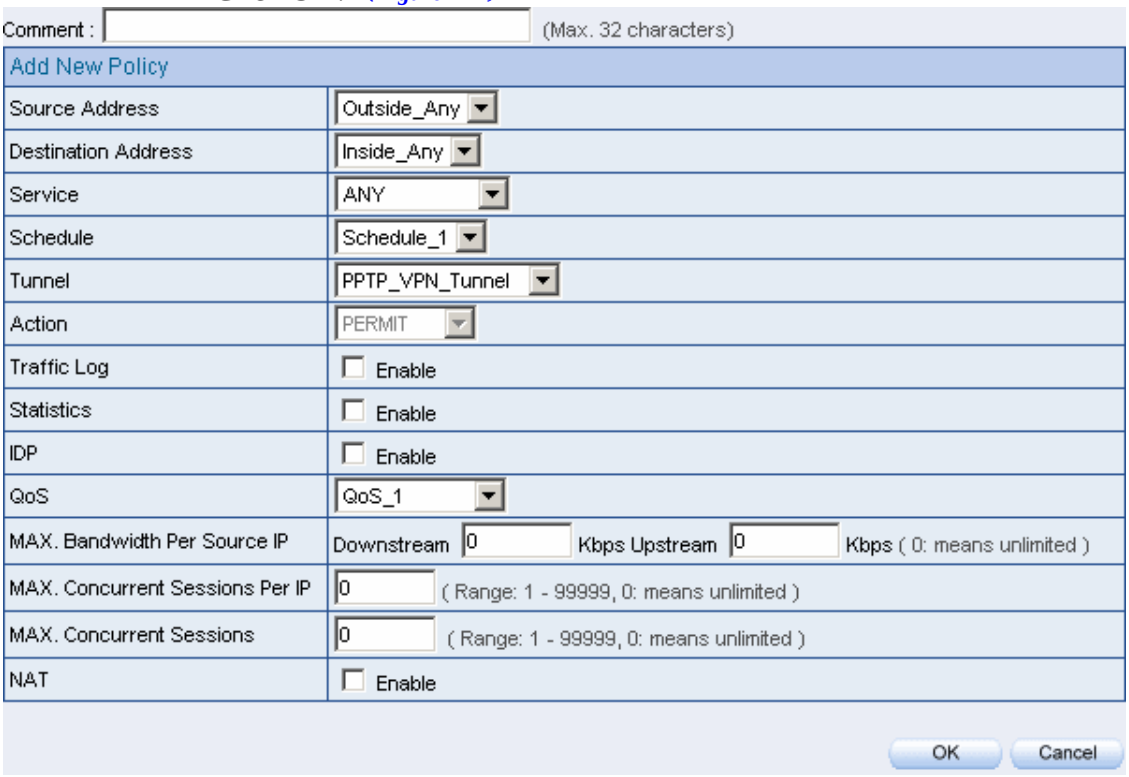

Figure 176 VPN Tunnel Incoming Policy Settings

Figure 177 VPN Tunnel Incoming Policy Settings Completed

The LAN IP, 192.168.20.1, is the default gateway of Company B's NUS-MH300. Proceed with the following steps:

Step 1. Using company B's NUS-MH300. Go to **Policy Object** > **VPN** > **PPTP Client**. Click on the **New Entry** button and enter the following settings: *(Figure 178)*

- **User Name**: Enter PPTP_Connection.
- **Password**: Enter123456789.
- **Server IP or Domain Name**: Enter Company A's WAN IP address.
- Check **Encryption**.
- Click **OK**. *(Figure 179)*

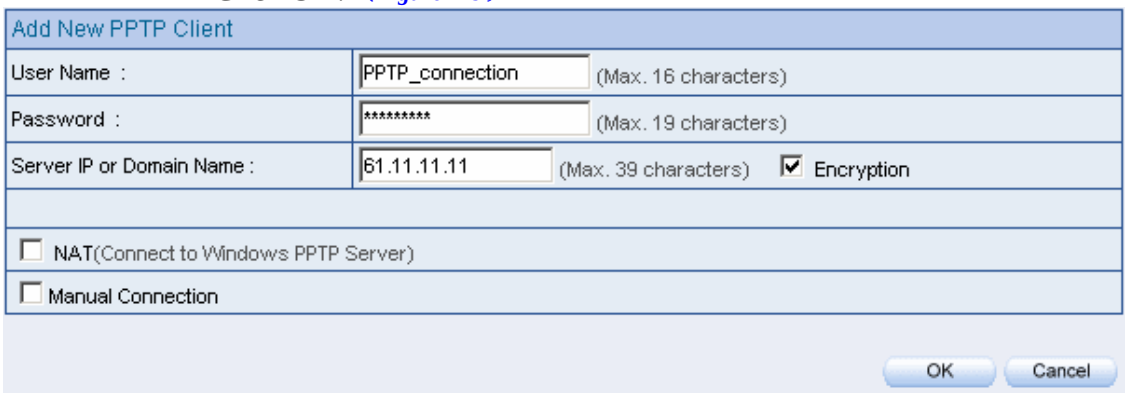

Figure 178 PPTP VPN Client Settings

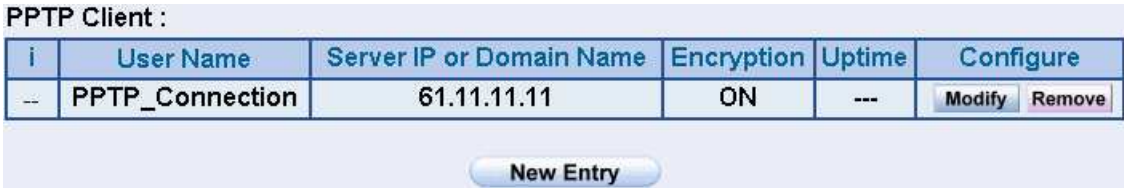

Figure 179 PPTP VPN Client Settings Completed

 In order to enable all local users connected to the device to access all the Windows-based resources, the checkbox **NAT (Connect to Windows PPTP Server)** must be checked before creating a VPN session between the PPTP Client (NUS-MH300) and the PPTP Server (Windows).

Step 2. Go to **VPN** > **Tunnel**. Click on the **New Entry** button and enter the following settings: *(Figure 180)*

- **Name:** Enter a specific Tunnel name.
- **From Local:** Select **LAN**.
- **From Local Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **To Remote:** Select **To Remote Subnet / Mask**.
- **To Remote Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select **PPTP_Client_PPTP_Connection(61.11.11.11).**
- Check **Show remote Network Neighborhood**.
- Click **OK**. *(Figure 181)*

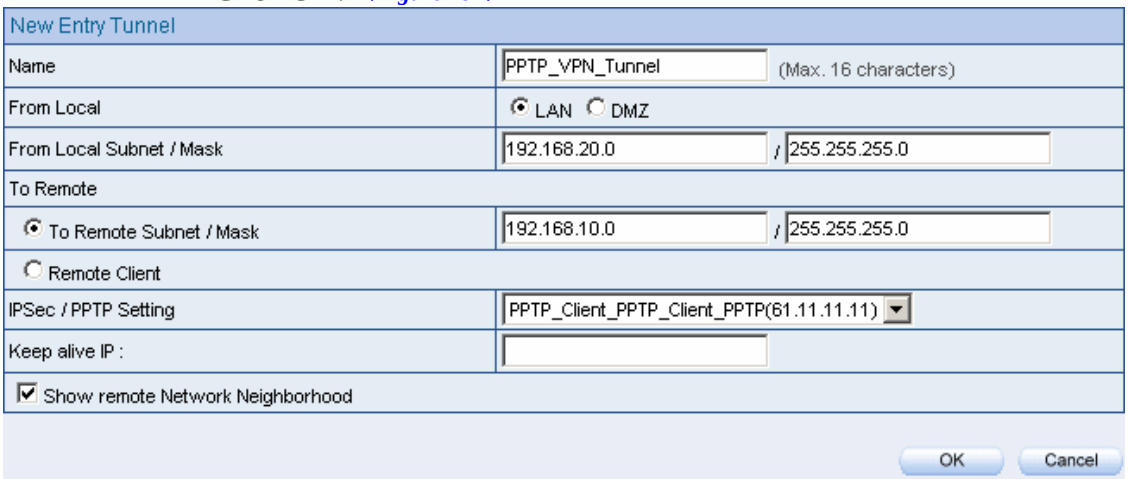

Figure 180 New Entry Tunnel Settings

Figure 181 New Entry Tunnel Setting Completed

Step 3. Go to **Policy** > **Outgoing.** Click on the **New Entry** button and enter the following settings: *(Figure 182)*

- **Authentication User:** Select **All_NET**.
- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1.**
- **Tunnel:** Select **PPTP_VPN_Tunnel**.
- Click **OK**. *(Figure 183)*

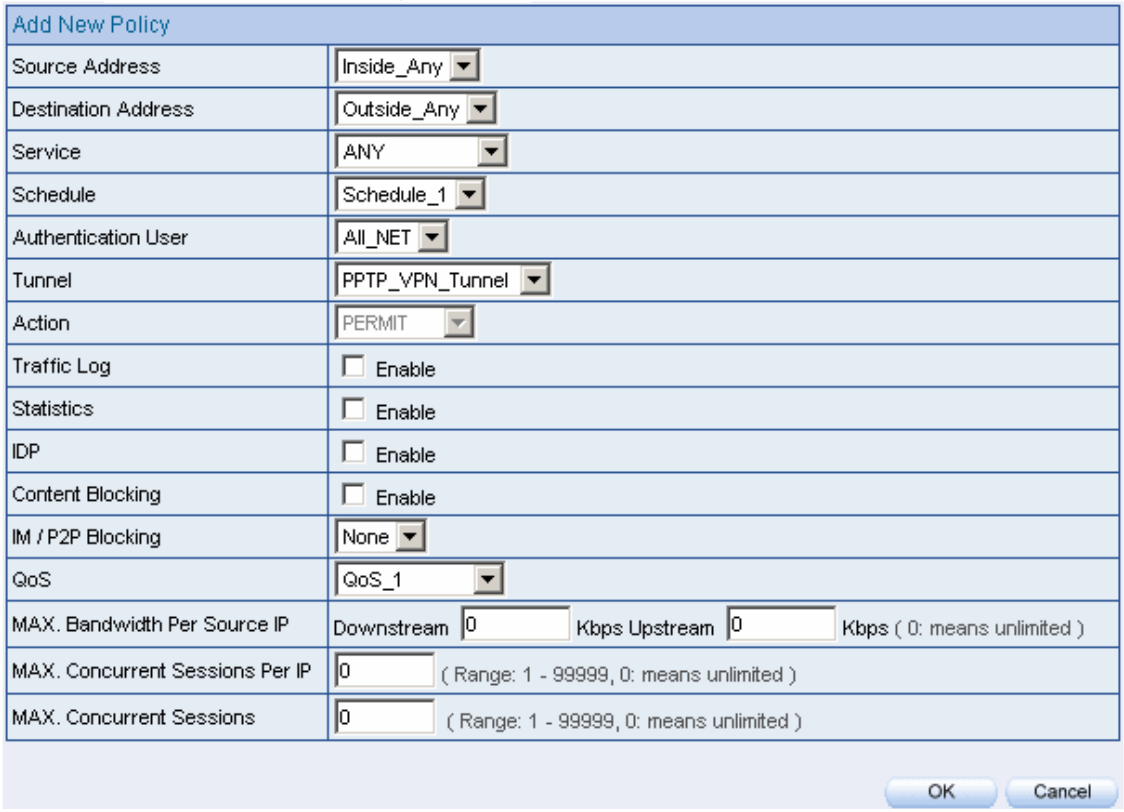

Figure 182 VPN Tunnel Outgoing Policy Settings

Figure 183 VPN Tunnel Outgoing Policy Setting Completed

Step 4. Go to **Policy** > **Incoming.** Click on the **New Entry** button and enter the following settings: *(Figure 184)*

- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Tunnel:** Select **PPTP_VPN_Tunnel**.
- Click **OK**. *(Figure 185)*

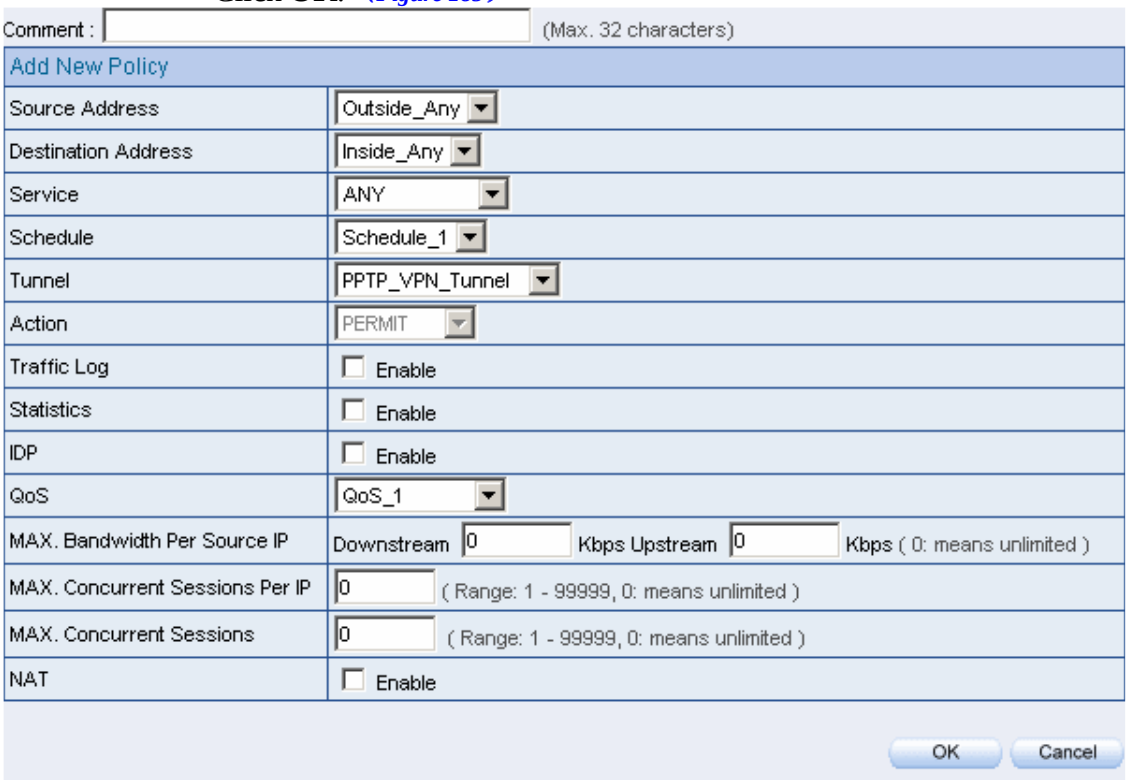

Figure 184 VPN Tunnel Incoming Policy Settings

Figure 185 VPN Tunnel Incoming Policy Setting Completed

VPN Example 5

Step 5. The completed PPTP VPN connection setup *(Figure 186)*

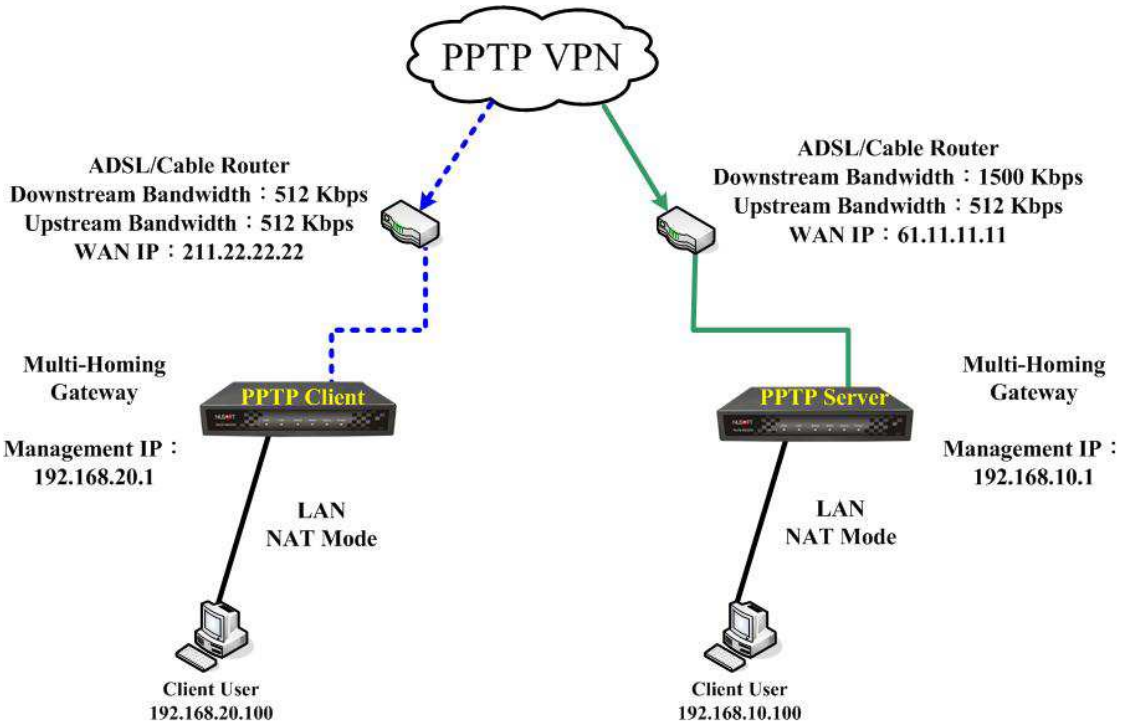

Figure 186 PPTP VPN Connection Deployment

VPN Example 6

Setting up a PPTP VPN Connection Using a Single NUS-MH300 and a Windows 2000 PC

Scenario:

Company A:

- Using a NUS-MH300
- WAN IP: **61.11.11.11**
- LAN IP: **192.168.10.X**

Company B

- Using a Windows 2000 PC
- WAN IP: **211.22.22.22**

In this example, the VPN IPSec connection settings are for a single NUS-MH300 and a Windows 2000 PC. Supposing a user from company B, 211.22.22.22, wishes to establish a VPN connection with company A, 192.168.10.100, for accessing files.

VPN Example 6

The LAN IP, 192.168.10.1, is the default gateway of Company A's NUS-MH300. Proceed with the following steps:

Step 1. Using Company A's NUS-MH300, go to **Policy Object** > **VPN** > **PPTP Server**. Click on the **Modify** button and configure the following:

- Select **Enable PPTP**.
- Check **Encryption**.
- **Client IP Range:** enter 192.44.75.1-254.
- Check the **Allow PPTP Client to connect to the Internet** checkbox.
- **Auto-Disconnect if idle:** enter 0. *(Figure 187)*

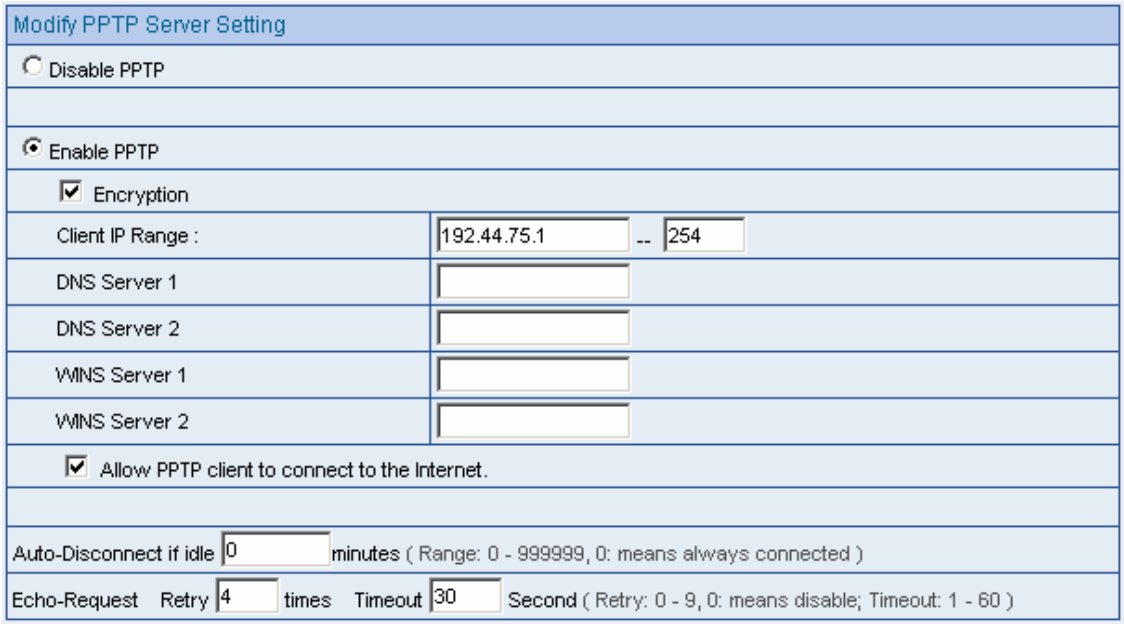

Figure 187 Enable PPTP VPN Server Settings

When a VPN connection is made between external users and the PPTP server of the NUS-MH300, IT administrators can decide whether to permit or block their access.

Idle Time: This nominates the time (in minutes) that the VPN connection will remain active after no activity has taken place.

Step 2. Using Company A's NUS-MH300, go to **Policy Object** > **VPN** > **PPTP Server.** Click on the **New Entry** button and configure the following: *(Figure 188)*

- **User Name**: Enter PPTP_Connection.
- **Password**: Enter 123456789.
- From the **Client IP assigned by** category select **IP Range**.
- Click **OK**. *(Figure 189)*

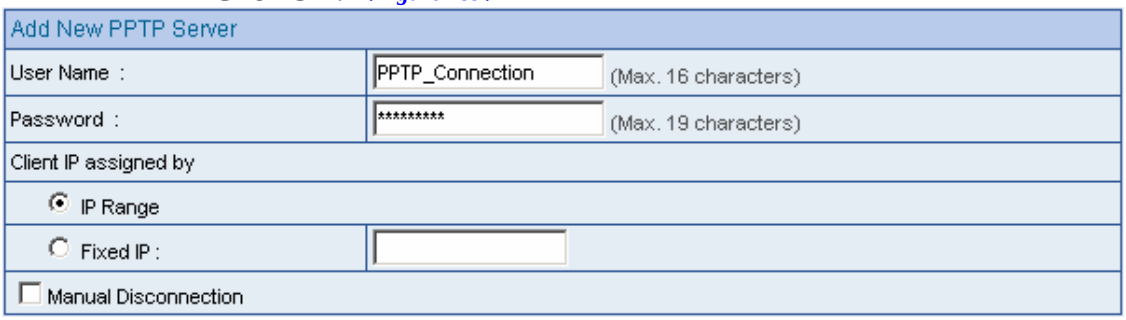

Figure 188 PPTP VPN Server Settings

Figure 189 PPTP VPN Server Settings Completed

Step 3. Go to **Policy Object** > **VPN** > **Tunnel.** Click on the **New Entry** button and enter the following settings: *(Figure 190)*

- **Name**: Enter a unique name for the Tunnel.
- **From Local:** Select LAN.
- **From Local Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **To Remote:** Select **To Remote Client**.
- **IPSec / PPTP Setting:** Select **PPTP_Server_PPTP_Connection**.
- Check **Show remote Network Neighborhood**.
- Click **OK**. *(Figure 191)*

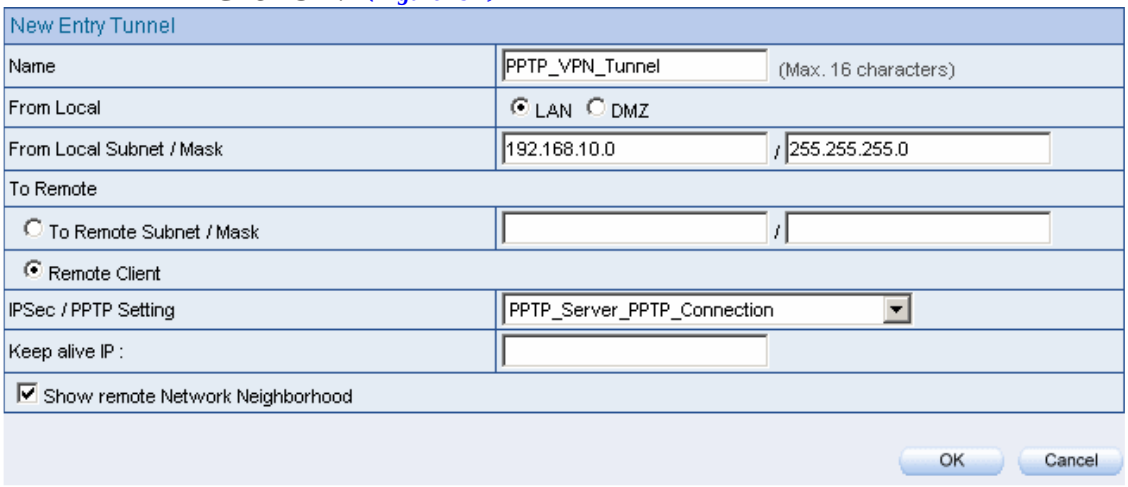

Figure 190 New Entry Tunnel Setting

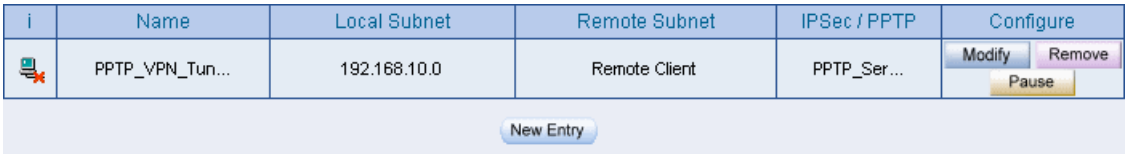

Figure 191 VPN Tunnel Settings Completed

Step 4. Go to **Policy** > **Outgoing** and click on the **New Entry** button and enter the following settings: *(Figure 192)*

- **Authentication User:** Select **All_NET**.
- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Tunnel:** Select **PPTP_VPN_Tunnel**.
- Click **OK**. *(Figure 193)*

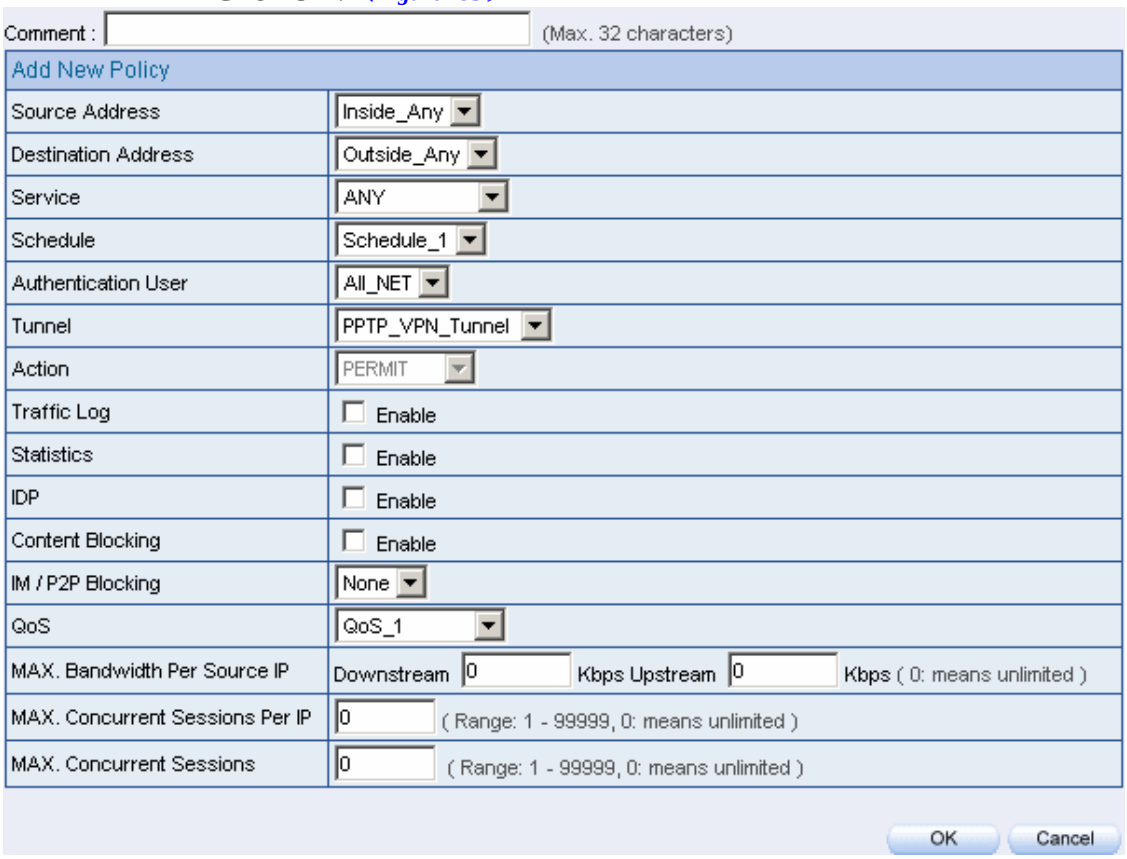

Figure 192 VPN Tunnel Outgoing Policy Settings

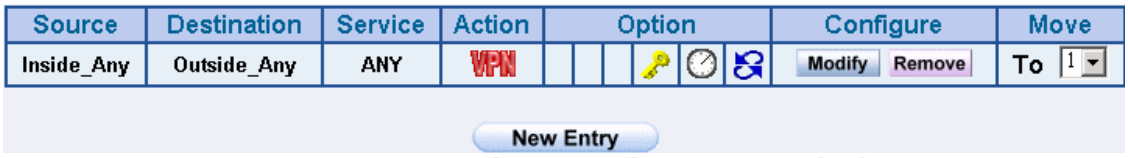

Figure 193 VPN Tunnel Outgoing Policy Settings Completed

Step 5. Go to **Policy** > **Incoming.** Click on the **New Entry** button and enter the following settings: *(Figure 194)*

- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Tunnel:** Select **PPTP_VPN_Tunnel**.
- Click **OK**. *(Figure 195)*

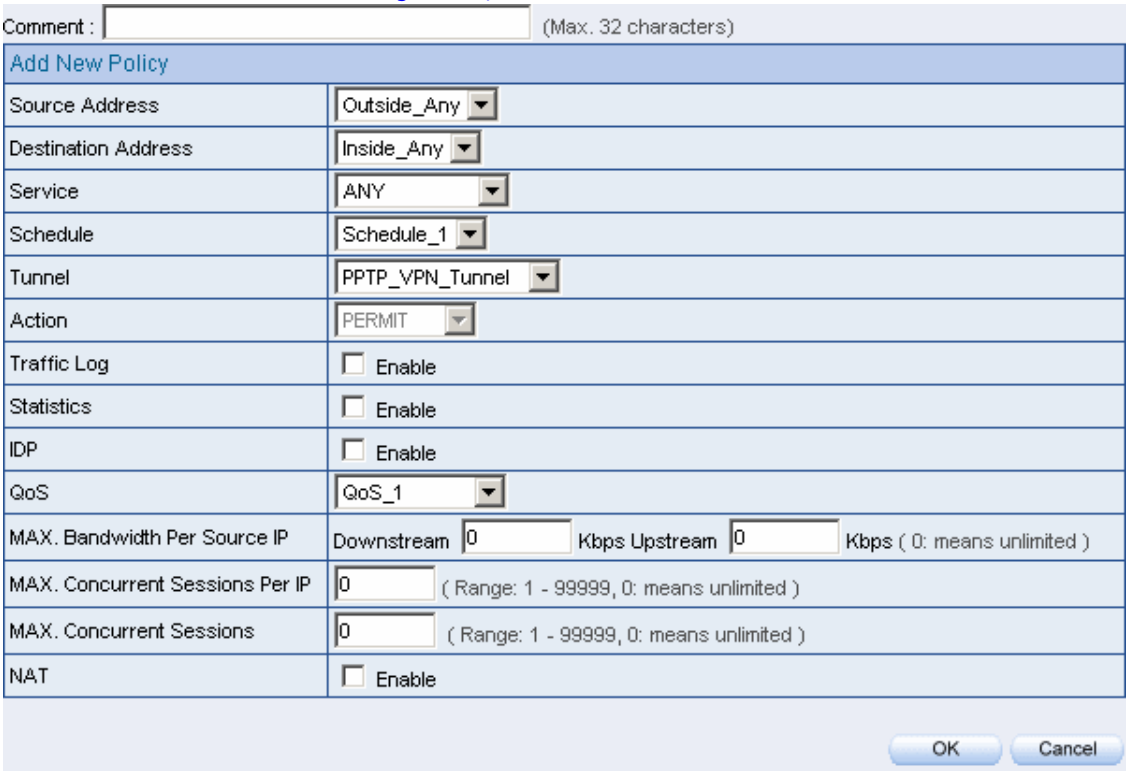

Figure 194 VPN Tunnel Incoming Policy Settings

Figure 195 VPN Tunnel Incoming Policy Settings Completed

VPN Example 6

A user from Company B is using the real IP address 211.22.22.22. Proceed with the following steps:

Step 1. Right-click on **My Network Places**, then click on **Properties**. *(Figure 196)*

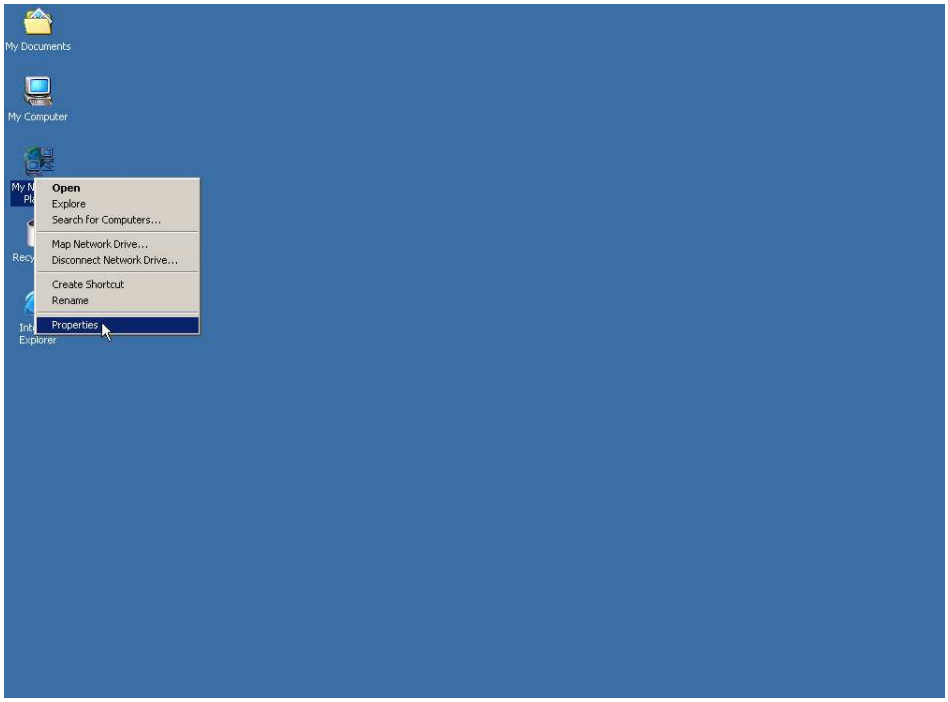

Figure 196 Starting the Windows 2000 PPTP VPN Settings

Step 2. In the **Network and Dial-up Connections** window, double click on **Make New Connection**. *(Figure 197)*

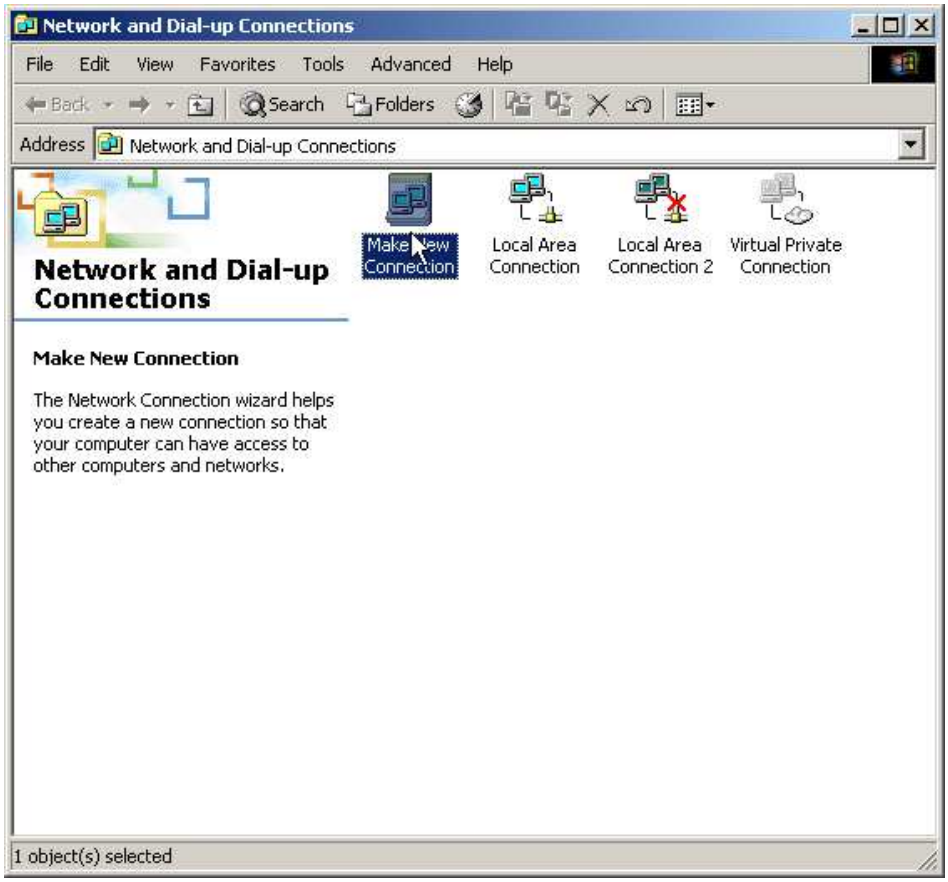

Figure 197 Network and Dial-up Connections

Step 3. In the **Location Information** window, set the **Country / Region, Area code** and the **phone system** according to your location, then click **OK**. *(Figure 198)*

Figure 198 The Local Information Settings

Step 4. In the **Phone And Modem Options** window, click **OK**. *(Figure 199)*

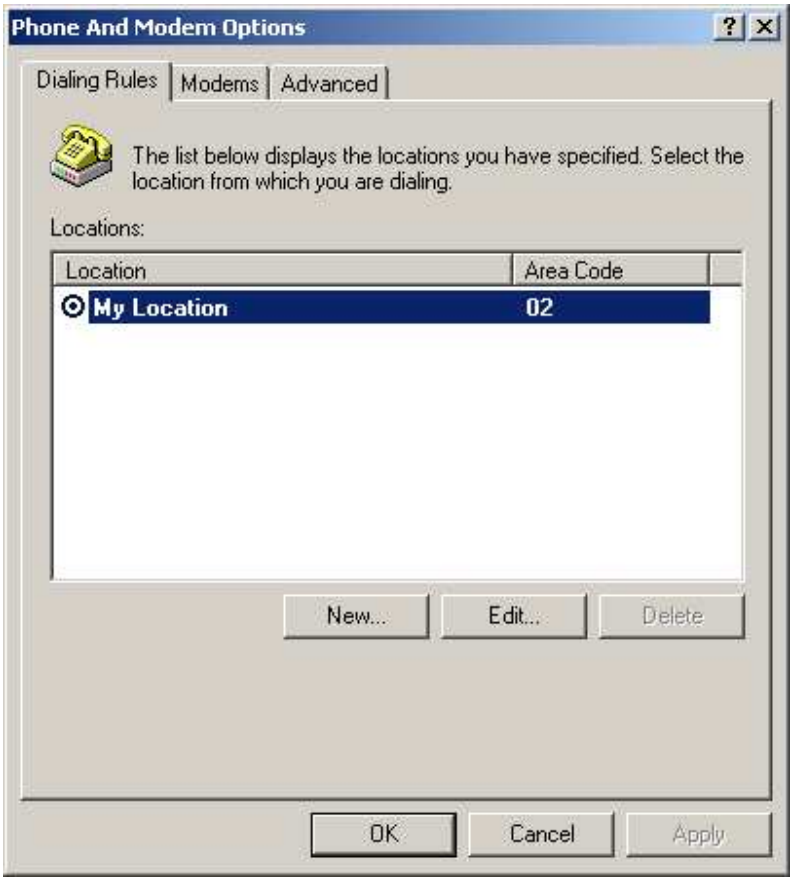

Figure 199 Phone And Modem Options

Step 5. In the **Network Connection Wizard** window, click **Next.** *(Figure 200)*

Figure 200 Network Connection Wizard

Step 6. In the **Network Connection Type** window, select **Connect to a private network through the Network** and then click **Next**. *(Figure 201)*

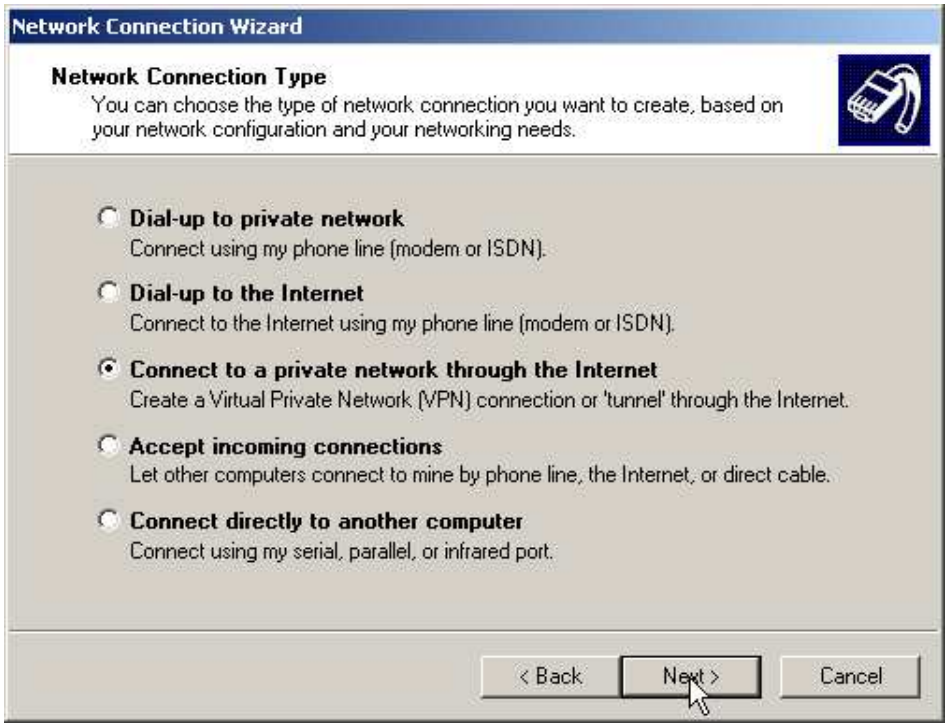

Figure 201 To Connect to a Private Network through the Internet

Step 7. In the **VPN Server Selection** window, enter the VPN IP address and click **Next.** *(Figure 202)*

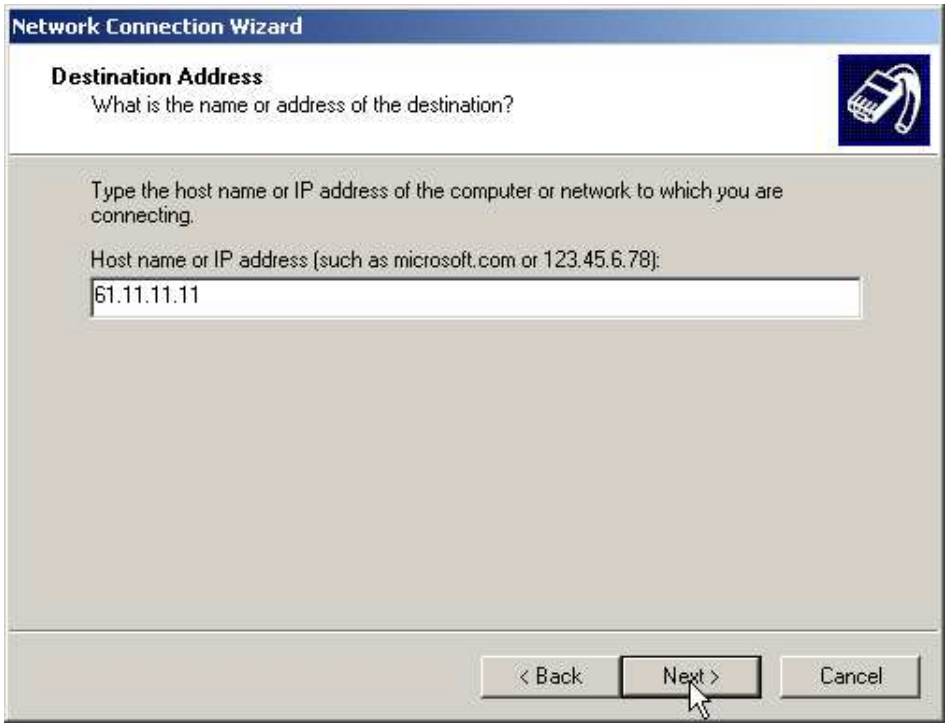

Figure 202 Setup the Host Name or IP Address

Step 8. In the **Connection Availability** window, select **For all users** and click **Next**.

(Figure 203)

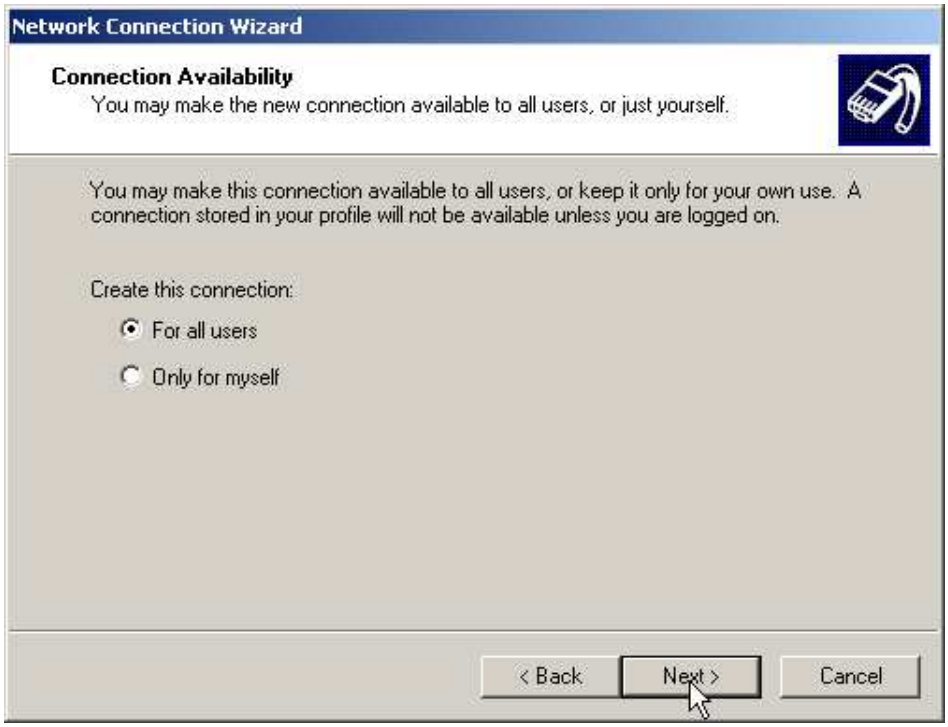

Figure 203 Setup the Connection Availability

Step 9. In the **Completing the New Connection Wizard** window, enter a **Connection Name** and then click **Finish**. *(Figure 204)*

Figure 204 New Connection Wizard Settings Complete

Step 10. In the **Connect Virtual Private Connection** window, set as below: *(Figure 205)*

- **User Name**, enter PPTP_Connection.
- Enter 123456789 in the **Password** field.
- Check the **Save Password** checkbox.
- Click **Connect**.
- Now the **Connecting to Virtual Private Connection** window will be displayed. *(Figure 206)*
- Finally, the **Connection Complete** window will be displayed. *(Figure 207)*

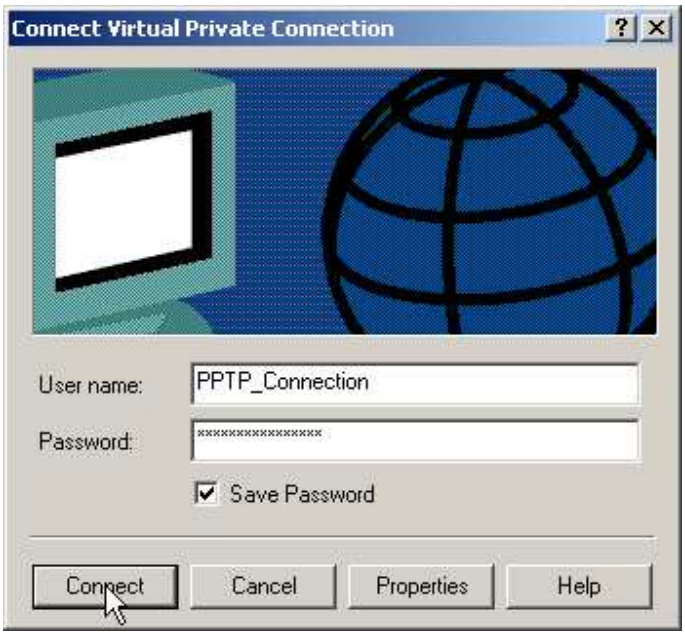

Figure 205 Connect Virtual Private Connection Window

Figure 206 Establishing the PPTP VPN Session

Figure 207 PPTP VPN Connections Complete

Step 11. Complete PPTP VPN setup. *(Figure 208)*

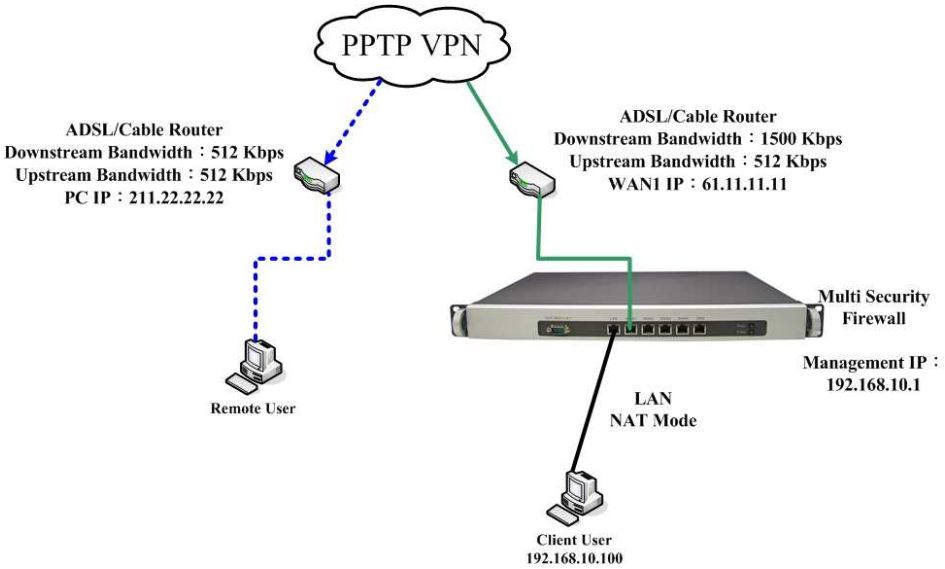

Figure 208 The Completed PPTP VPN Deployment