

Chapter 12

VPN

To obtain a private and secure network link, the NUS-MH2400G 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 enhance further 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.

Trunk:

In this chapter the IT administrator can apply the relevant VPN policies 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 **Trunk**. 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, Trunk and Policy** settings will be automatically created by the device. *(Figure 3,4,5,6)*

One-Step IPsec Comment	
Name	Quick_1
From Local	
Subnet / Mask	<input checked="" type="radio"/> LAN 192.168.169.0 / 255.255.255.0 <input type="radio"/> DMZ
To Remote	
Remote Gateway -- Fixed IP or Domain Name	211.22.22.22
Subnet / Mask	192.168.16.0 / 255.255.255.0
Preshared Key	123456789
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 1 One-Step IPsec Settings Window

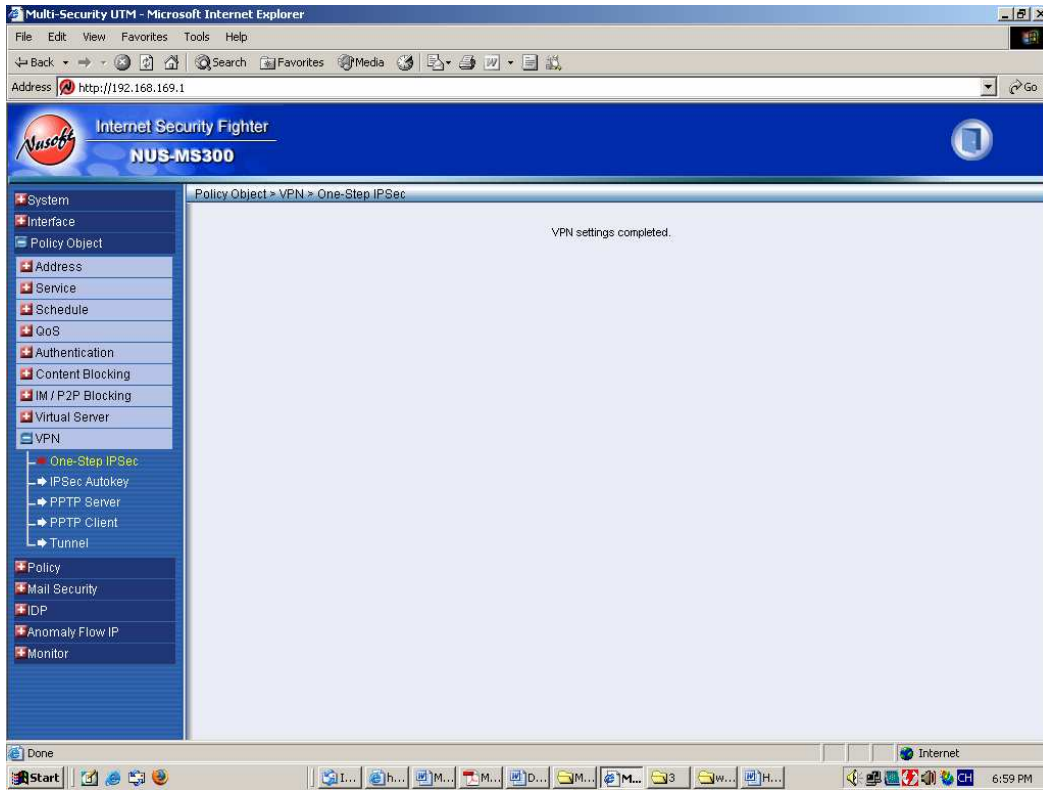


Figure 2 One-Step IPsec Settings Complete

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 > Trunk

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	To 1 <input type="button" value="v"/>
New Entry						

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

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 <input type="button" value="v"/>
<input type="button" value="New Entry"/>						

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, Trunk** 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)*

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
					

Figure 7 IPSec Autokey WebUI



NUS-MH2400G 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-MH2400G 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)*

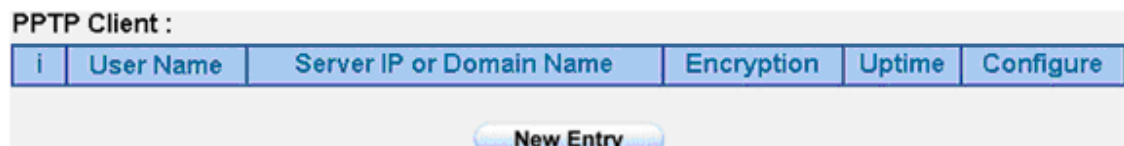


Figure 9 PPTP Client Fields





The NUS-MH2400G 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.

Trunk 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 trunk.

Local Subnet:

- Displays the local subnet address.

Remote Subnet:

- Displays the remote subnet address.

IPSec / PPTP :

- Displays all the VPN trunk (IPsec, PPTP Server, PPTP Client) in the VPN trunk.

Configure:

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

i	Name	Local Subnet	Remote Subnet	IPSec / PPTP	Configure
<input type="button" value="New Entry"/>					

Figure 10 VPN Trunk 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-MH2400G devices	
Example 2	IPSec Autokey	Setting up an IPSec VPN connection using a single NUS-MH2400G and Windows 2000	
Example 3	IPSec Autokey	Setting up an IPSec VPN connection (under Aggressive mode) between two NUS-MH2400G devices. (3DES encryption and MD5 authentication)	
Example 4	IPSec Autokey	Setting up an IPSec VPN connection between two NUS-MH2400G 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-MH2400G devices	
Example 6	PPTP	Setting up a PPTP VPN connection using a single NUS-MH2400G and Windows 2000	

Setting up an IPSec VPN Connection between Two NUS-MH2400G 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-MH2400G 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-MH2400G. Proceed with the following steps:

Step 1. From within a browser, enter Company A's NUS-MH2400G LAN IP address, 192.168.10.1. Go to **Policy Object > VPN > IPSec Autokey** then click on the **New Entry** button. *(Figure 11)*

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
<input type="button" value="New Entry"/>					

Figure 11 IPSec Autokey Field Headings

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

Necessary Item	
Name	VPN_A

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*)

To Remote	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	211.22.22.22 (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

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*)

Authentication Method	Preshare
Preshared Key	123456789 (Max. 103 characters)

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)*

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1

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)*

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

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)*

Optional Item	
Perfect Forward Secrecy	GROUP1 ▾
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

Figure 17 IPSec Autokey - Perfect Forward Secrecy Setting

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

i	Name	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	211.22.22.22	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 18 Company A IPSec Autokey – Settings Completed

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

- In the **Name** field, enter a unique name for the trunk.
- For the **From Source** setting, select **LAN**.
- In the **Source 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.
- Add **VPN_A** in the **Tunnel** field.
- Check the **Show remote Network Neighborhood** checkbox.
- Click **OK**.
- A new entry appears (Figure 20)

The screenshot shows the 'New Entry Trunk' configuration window. The 'Name' field contains 'IPSec_VPN_Trunk'. The 'From Source' is set to 'LAN'. The 'From Source Subnet / Mask' is '192.168.10.0 / 255.255.255.0'. The 'To Destination' is set to 'To Destination Subnet / Mask' with the value '192.168.20.0 / 255.255.255.0'. The 'Tunnel' section shows 'VPN_A' in the 'Selected Tunnel' list. The 'Show remote Network Neighborhood' checkbox is checked. The 'Keep alive P.' field is empty. The 'OK' and 'Cancel' buttons are visible at the bottom right.

Figure 19 New Entry Trunk Settings

ID	Name	Source Subnet	Destination Subnet	Tunnel	Configure
1	IPSec_VPN_Tr...	192.168.10.0	192.168.20.0	VPN_A	Modify Remove Pause

New Entry

Figure 20 New Entry Trunk Settings Completed

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

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

Comment:

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Schedule_1
Authentication User	All_NET
Trunk	IPSec_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	QoS_1
MAX. Concurrent Sessions	0 (0: means unlimited)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

Figure 21 VPN Trunk Outgoing Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN	  	<input type="button" value="Modify"/> <input type="button" value="Remove"/>	To <input type="text" value="1"/>

Figure 22 VPN Trunk 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.
- **Trunk:** select IPSec_VPN_Trunk.
- Click **OK**. (Figure 24)

Comment: (Max. 64 characters)

Add New Policy

Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Schedule_1
VPN Trunk	IPSec_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Concurrent Sessions	0 (Range: 1 - 99999; 0: means unlimited)
Quota Per Session	0 KBytes (Range: 0 - 999999)
Quota Per Day	0 MBytes (Range: 0 - 999999)
NAT	<input type="checkbox"/> Enable

OK Cancel

Figure 23 VPN Trunk 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 Trunk Incoming Policy Settings Completed

The LAN IP, 192.168.20.1, is the default gateway of Company B's NUS-MH2400G. 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)

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
<input type="button" value="New Entry"/>					

Figure 25 IPSec Autokey Headings

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

Necessary Item	
Name	<input type="text" value="VPN_B"/>

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)

<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="61.11.11.11"/>
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

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)

Authentication Method	<input type="text" value="Preshare"/>
Preshared Key	<input type="text" value="123456789"/> (Max. 103 characters)

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)

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1

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)

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

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)

Optional Item	
Perfect Forward Secrecy	GROUP1 ▾
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

Figure 31 IPSec Perfect Forward Secrecy Settings

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

i	Name	Gateway IP	IPSec Algorithm	Configure
--	VPN_B	61.11.11.11	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 32 Company B IPSec Autokey Settings Completed

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

- **Name:** enter a unique trunk name.
- **From Source:** 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.
- Add **VPN_B** in the **Tunnel** field.
- Check the **Show remote Network Neighborhood** checkbox.
- Click **OK**. (Figure 34)

Figure 33 New Entry Trunk Settings

	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPSec_VPN_Tr...	192.168.85.0	192.168.10.0	VPN_B	Modify Remove Pause

New Entry

Figure 34 New Entry Trunk 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**.
- **Trunk:** Select **IPSec_VPN_Trunk**.
- Click **OK**. (Figure 36)

Comment :

Add New Policy

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Schedule_1
Authentication User	All_NET
Trunk	IPSec_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	QoS_1
MAX. Concurrent Sessions	0 (0: means unlimited)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

OK Cancel

Figure 35 Setting the VPN Trunk Outgoing Policy

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

New Entry

Figure 36 VPN Trunk 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**.
- **Trunk:** Select **IPSec_VPN_Trunk**.
- Click **OK**. (Figure 38)

Comment : (Max. 64 characters)

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Schedule_1
VPN Trunk	IPSec_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
Quota Per Session	0 KBytes (Range: 0 - 999999)
Quota Per Day	0 MBytes (Range: 0 - 999999)
NAT	<input type="checkbox"/> Enable

OK Cancel

Figure 37 VPN Trunk Incoming Policy Settings

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

New Entry

Figure 38 VPN Trunk Incoming Policy Settings Completed

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

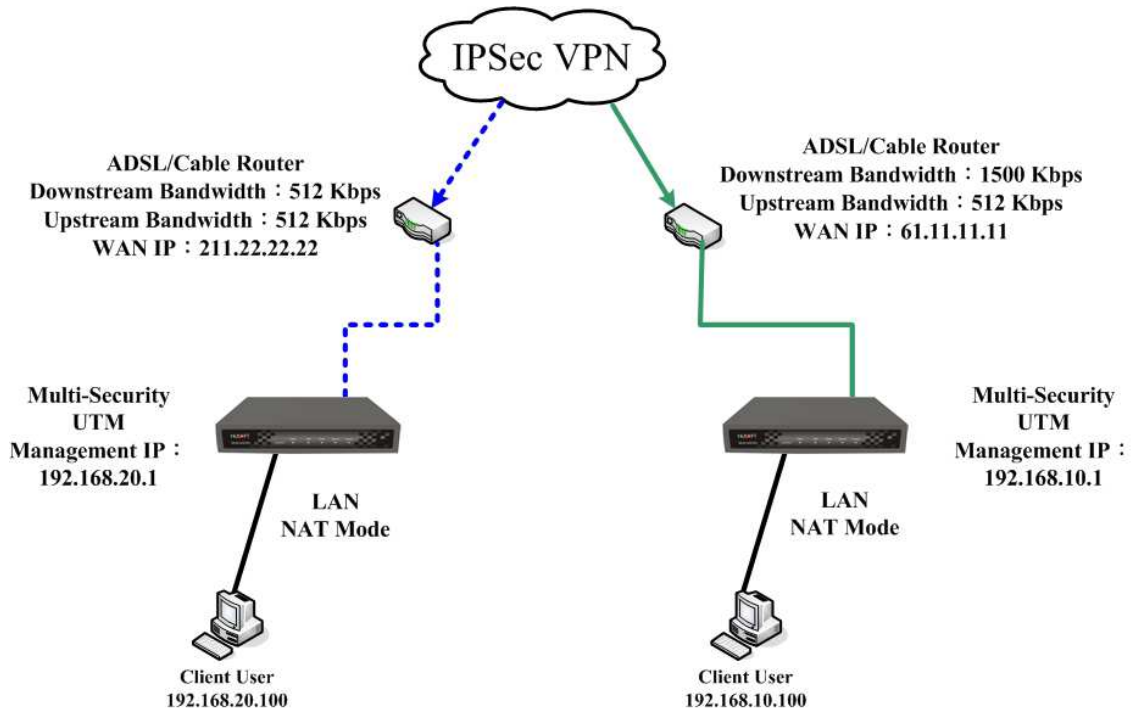


Figure 39 Completed Setup

Setting up an IPSec VPN Connection Using a Single NUS-MH2400G and Windows 2000 PC

Scenario:

Company A:

- Using a NUS-MH2400G
- 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-MH2400G 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-MH2400G. 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)

	Name	WAN	Gateway IP	IPSec Algorithm	Configure
<input type="button" value="New Entry"/>					

Figure 40 IPSec Autokey

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

Necessary Item	
Name	<input type="text" value="VPN_A"/> (Max. 12 characters)

Figure 41 The IPSec VPN Name

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

To Remote	
<input type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text"/> (Max. 99 characters)
<input checked="" type="radio"/> Remote Gateway or Client -- Dynamic IP	

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*)

Authentication Method	<input type="text" value="Preshare"/>
Preshared Key	<input type="text" value="123456789"/> (Max. 103 characters)

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)*

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
Group	GROUP 2 ▼

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)*

IPsec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
<input type="radio"/> Authentication Only	

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)

Optional Item	
Perfect Forward Secrecy	GROUP1 ▾
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

Figure 46 IPSec Autokey - Perfect Forward Secrecy Setting

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

i	Name	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	Dynamic IP	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 47 Company A IPSec Autokey – Settings Completed

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

- In the **Name** field, enter a unique name for the trunk.
- For the **From Source** setting, select **LAN**.
- In the **Local Source / Mask** field, enter 192.168.10.0 / 255.255.255.0.
- From the **To Destination** category, select **Remote Client**.
- Add **VPN_A** in the **Tunnel** field.
- Check the **Show remote Network Neighborhood** checkbox.
- Click **OK**. (Figure 49)

Figure 48 New Entry Trunk Settings

	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPSec_VPN_Tr...	192.168.10.0	Remote Client	VPN_A	Modify Remove Pause

New Entry

Figure 49 VPN Trunk 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**.
- **Trunk:** Select **IPSec_VPN_Trunk**.
- Click **OK**. (Figure 51)

Comment :

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Schedule_1
Authentication User	All_NET
Trunk	IPSec_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	QoS_1
MAX. Concurrent Sessions	0 (0: means unlimited)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

OK Cancel

Figure 50 VPN Trunk Outgoing Policy Settings




Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN	 	 <input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1

Figure 51 VPN Trunk Outgoing Policy Settings Completed

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

- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Trunk:** Select **IPSec_VPN_Trunk**.
- Click **OK**. (Figure 53)

Comment : (Max. 64 characters)

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Schedule_1
VPN Trunk	IPSec_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
Quota Per Session	0 KBytes (Range: 0 - 999999)
Quota Per Day	0 MBytes (Range: 0 - 999999)
NAT	<input type="checkbox"/> Enable

OK Cancel

Figure 52 VPN Trunk Incoming Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN	⌚	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1

New Entry

Figure 53 VPN Trunk 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)

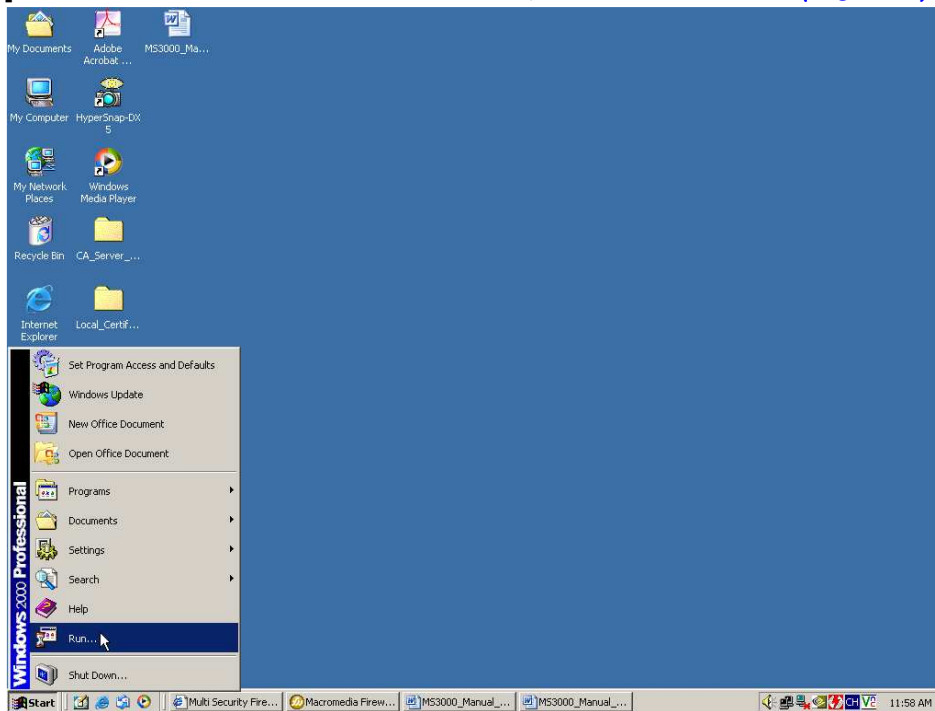


Figure 54 Start the IPSec VPN Setting in Windows 2000

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

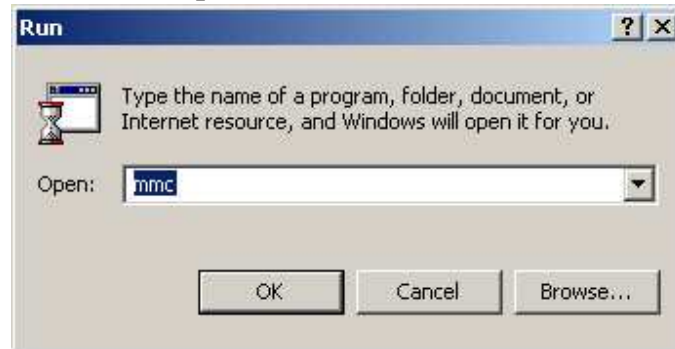


Figure 55 Starting the Windows 2000 IPsec VPN Configuration

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

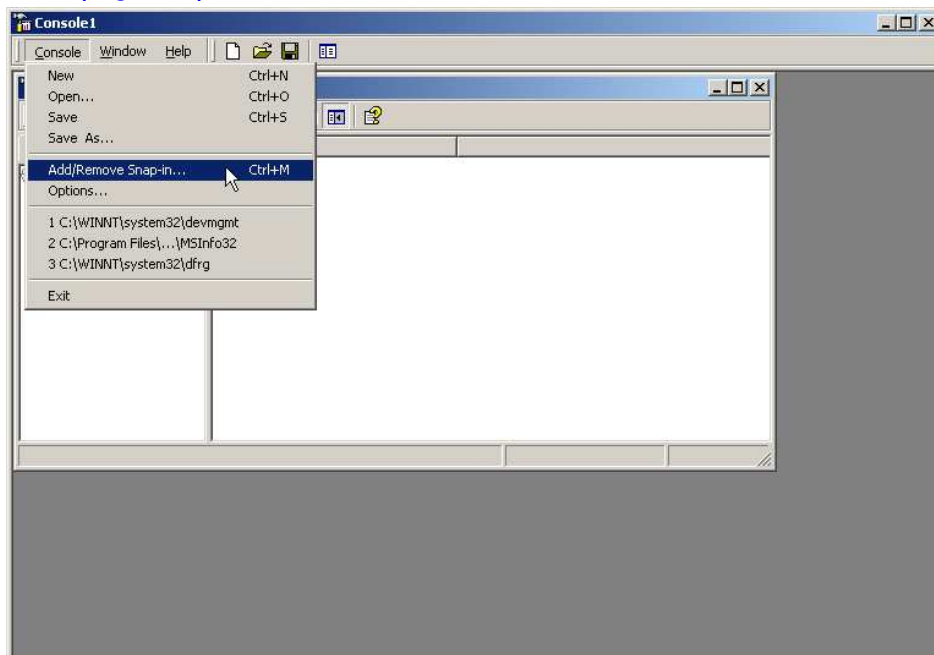


Figure 56 Add / Remove Snap-in.

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*)

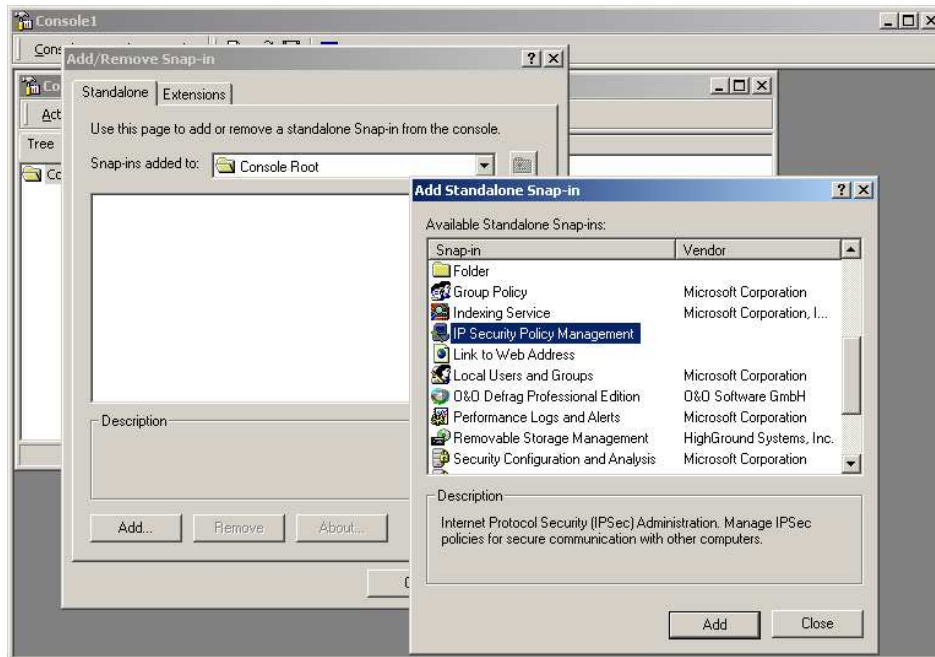
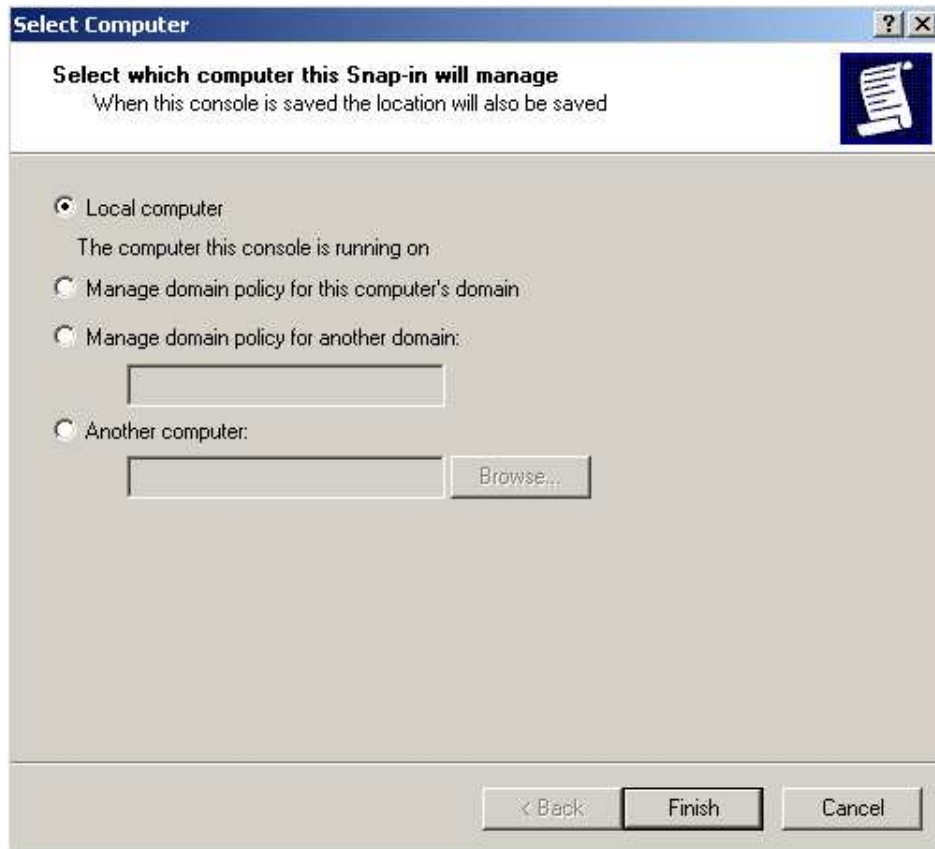
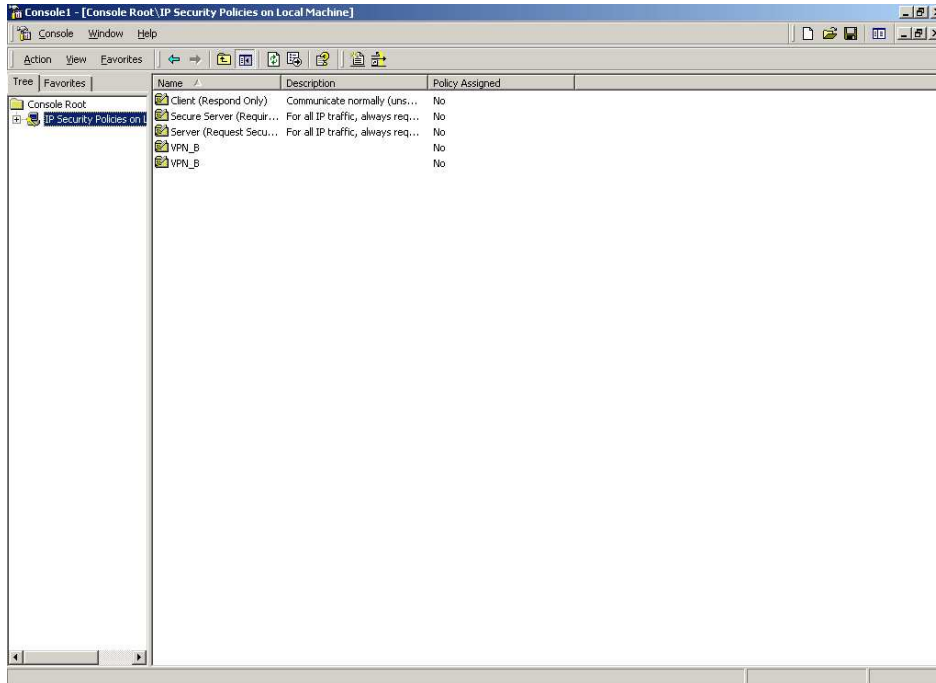


Figure 57 Adding IP Security Policy Management

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*)

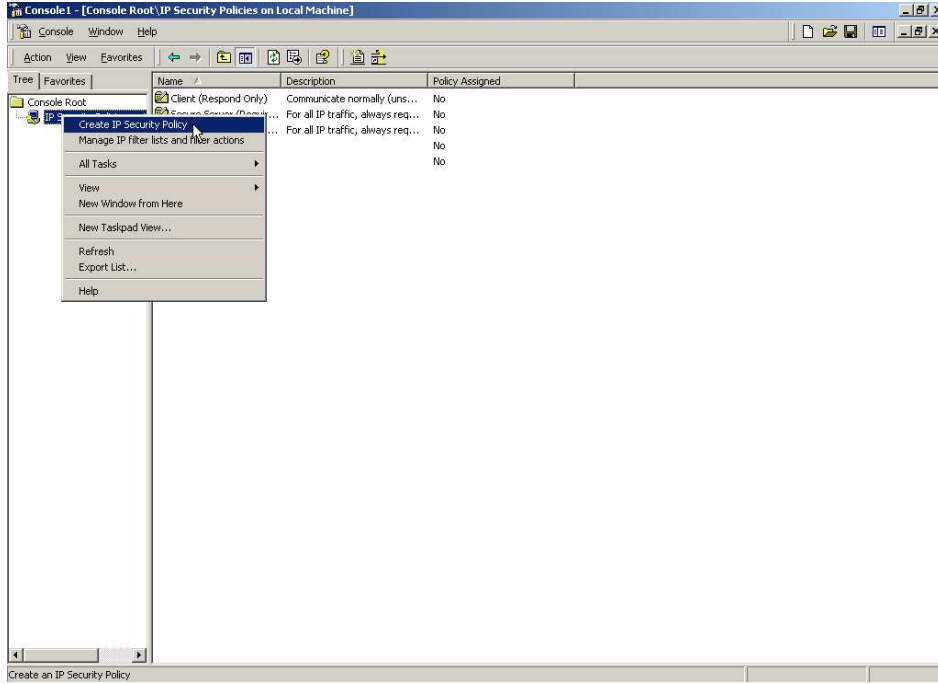
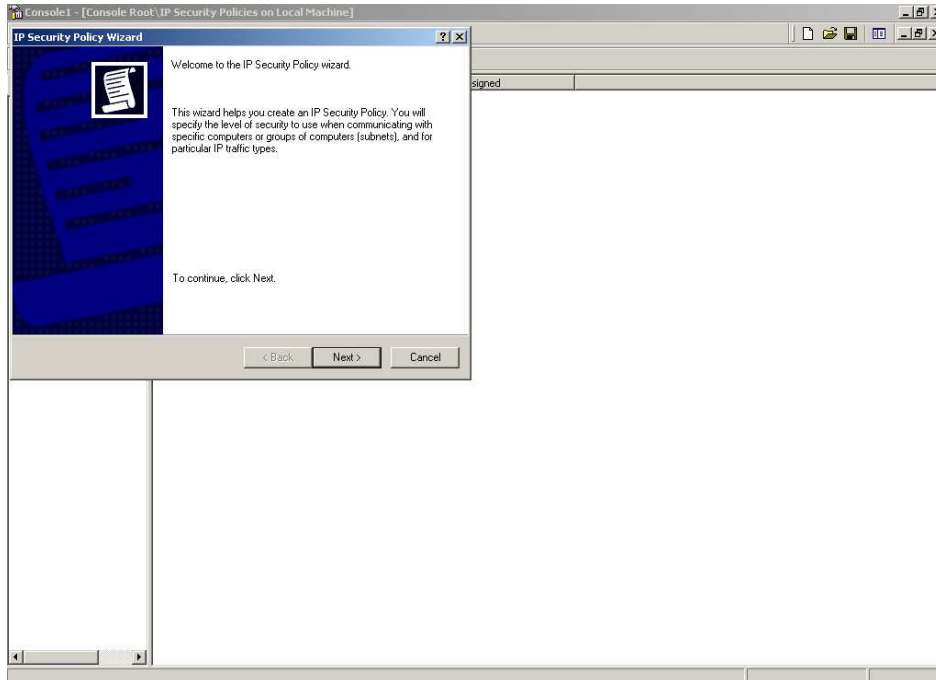
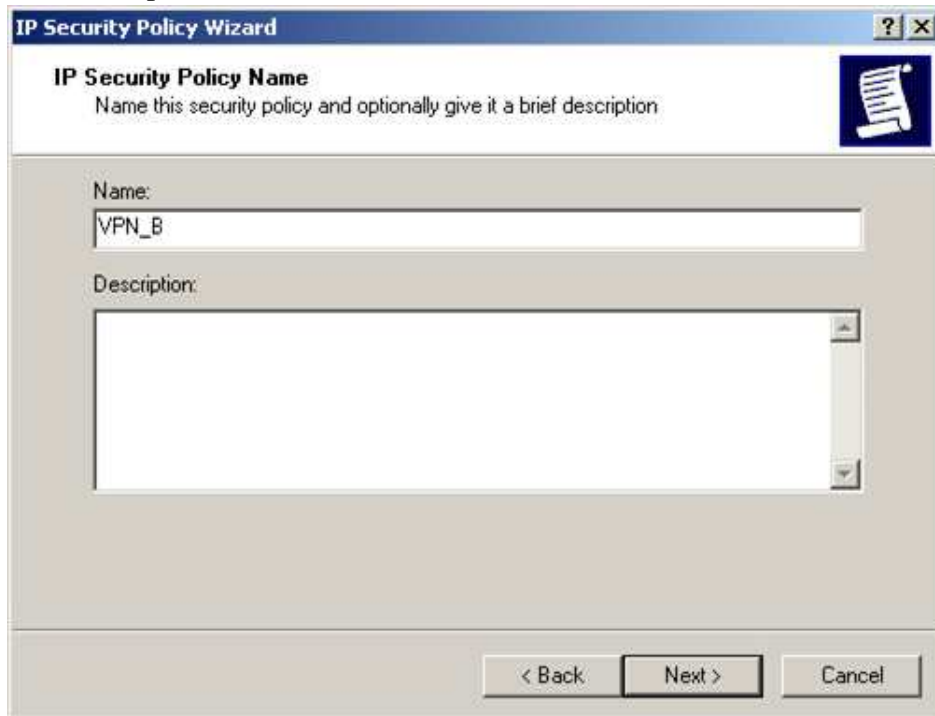


Figure 60 Create IP Security Policy

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*)



The screenshot shows a Windows-style dialog box titled "IP Security Policy Wizard". The main heading is "IP Security Policy Name" with a sub-instruction: "Name this security policy and optionally give it a brief description". There is a "Name:" label above a text input field containing "VPN_B". Below it is a "Description:" label above a large empty text area. At the bottom are three buttons: "< Back", "Next >", and "Cancel".

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*)

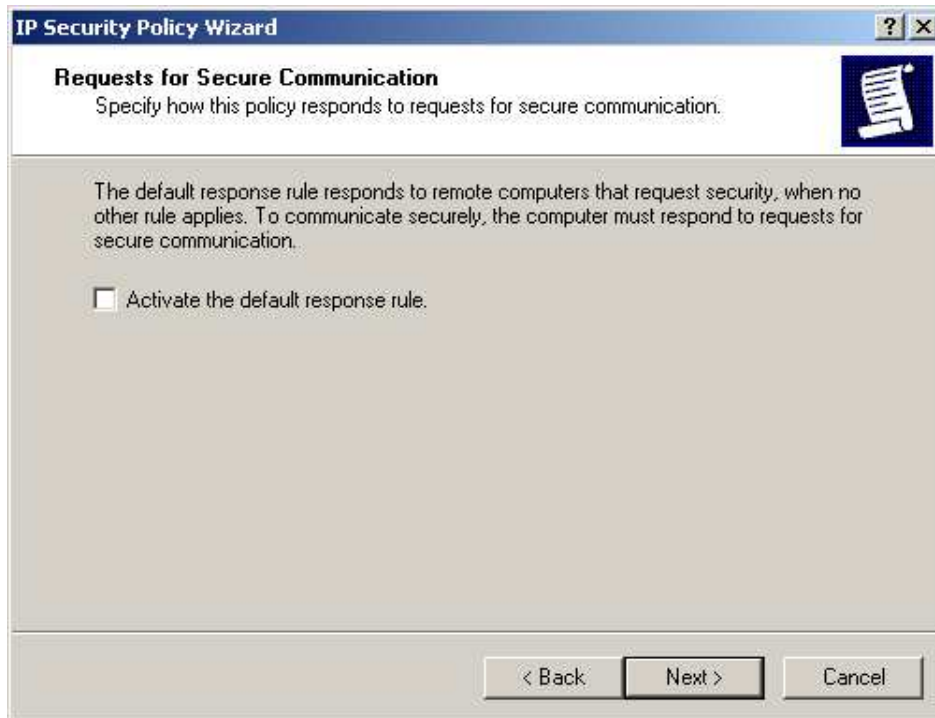


Figure 63 Leave the Box Unchecked

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

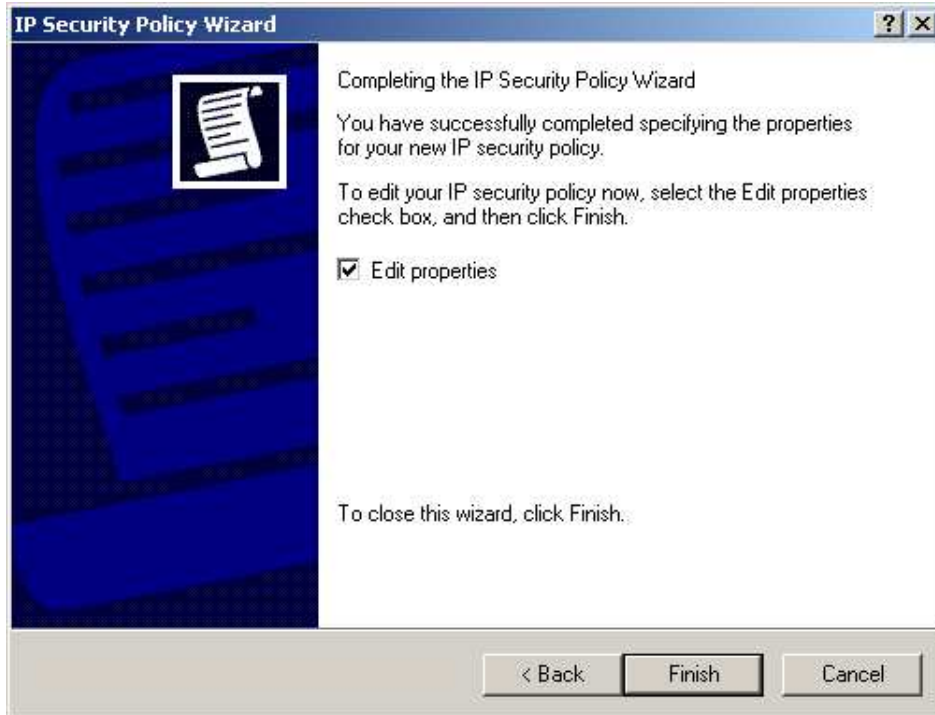


Figure 64 IP Security Policy Wizard Settings Completed

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

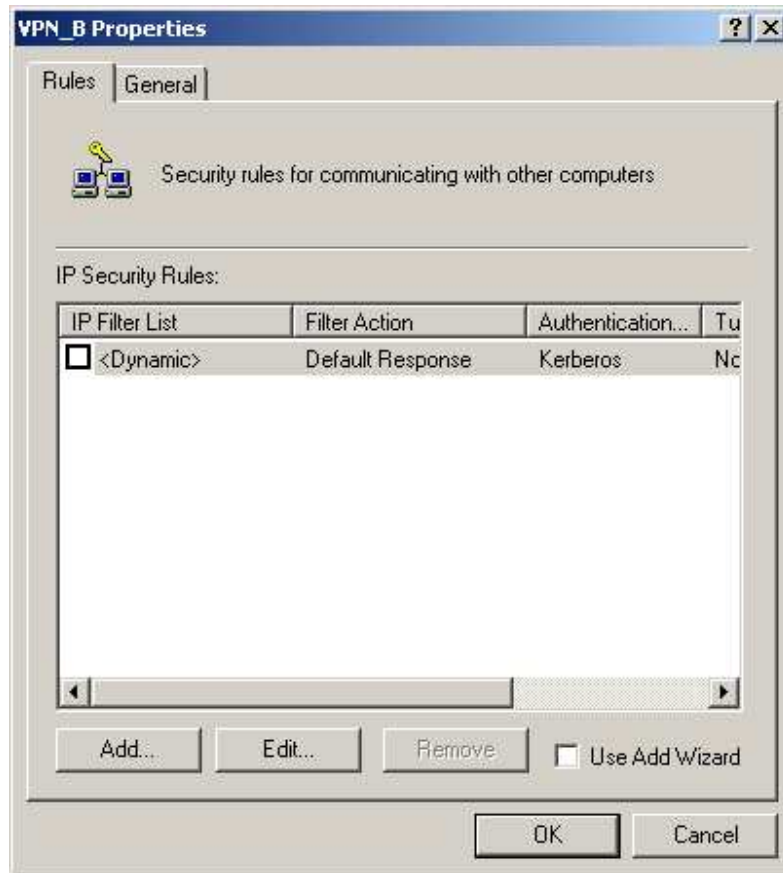


Figure 65 VPN_B Properties

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

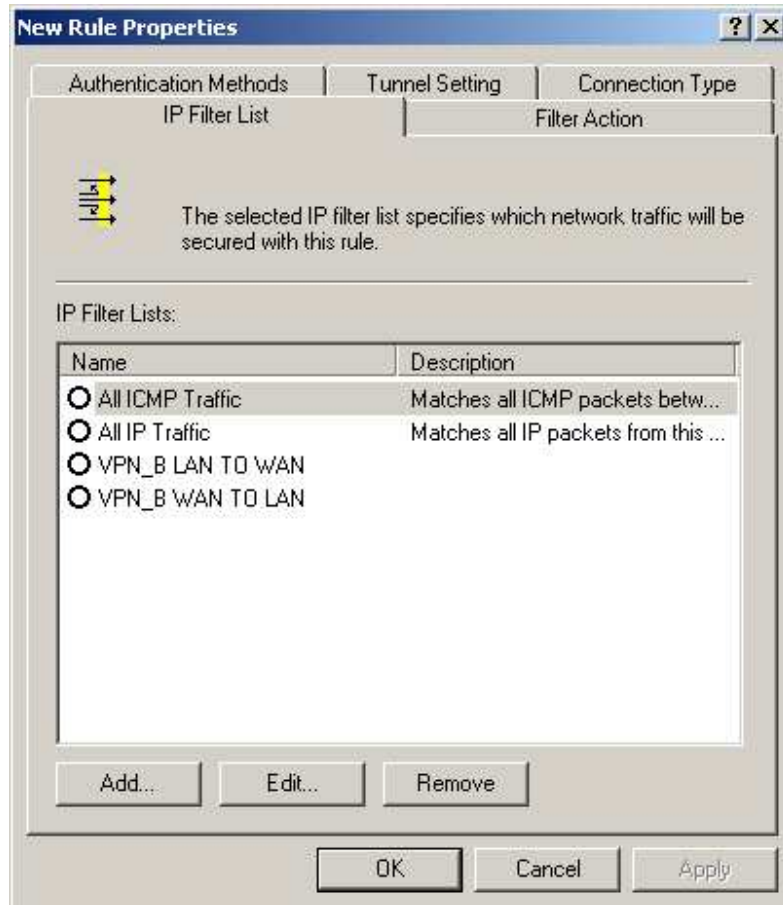


Figure 66 New Rule Properties

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)

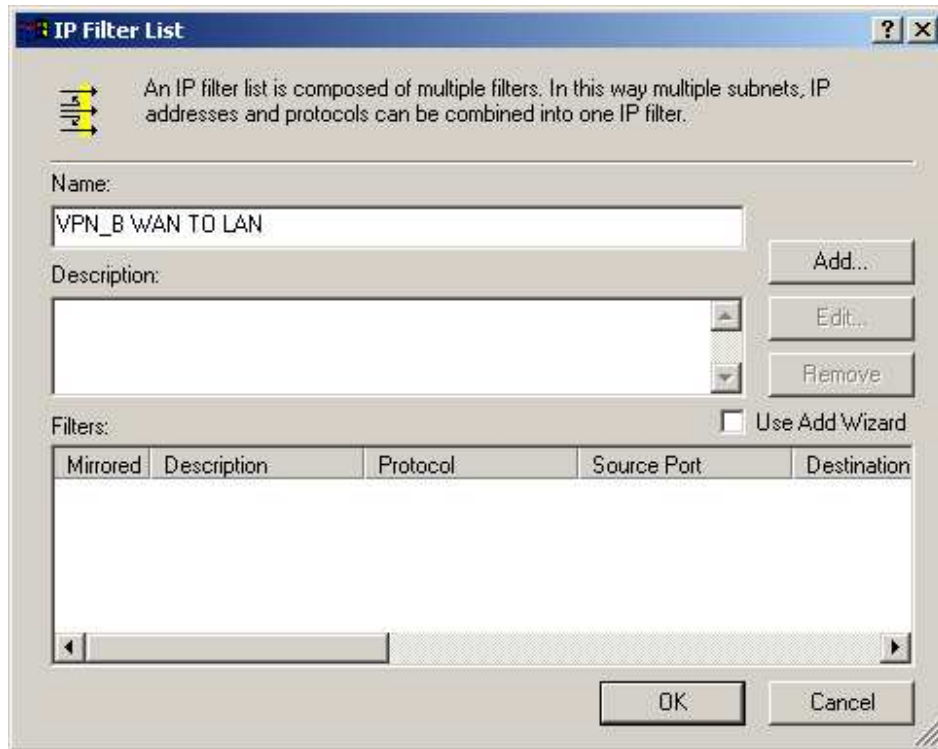
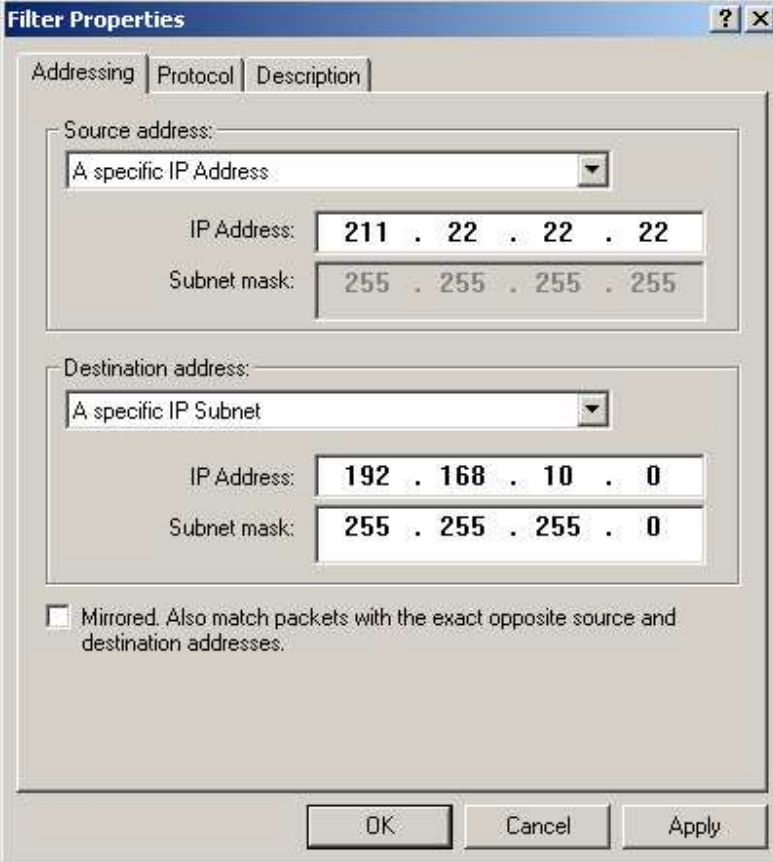


Figure 67 IP Filter List

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*)



The screenshot shows the 'Filter Properties' dialog box with three tabs: 'Addressing', 'Protocol', and 'Description'. The 'Addressing' tab is active. It contains two main sections: 'Source address' and 'Destination address'. In the 'Source address' section, a dropdown menu is set to 'A specific IP Address', with the IP Address field containing '211 . 22 . 22 . 22' and the Subnet mask field containing '255 . 255 . 255 . 255'. In the 'Destination address' section, a dropdown menu is set to 'A specific IP Subnet', with the IP Address field containing '192 . 168 . 10 . 0' and the Subnet mask field containing '255 . 255 . 255 . 0'. At the bottom, there is a checkbox labeled 'Mirrored. Also match packets with the exact opposite source and destination addresses.' which is currently unchecked. The dialog box has 'OK', 'Cancel', and 'Apply' buttons at the bottom right.

Figure 68 Filter Properties

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

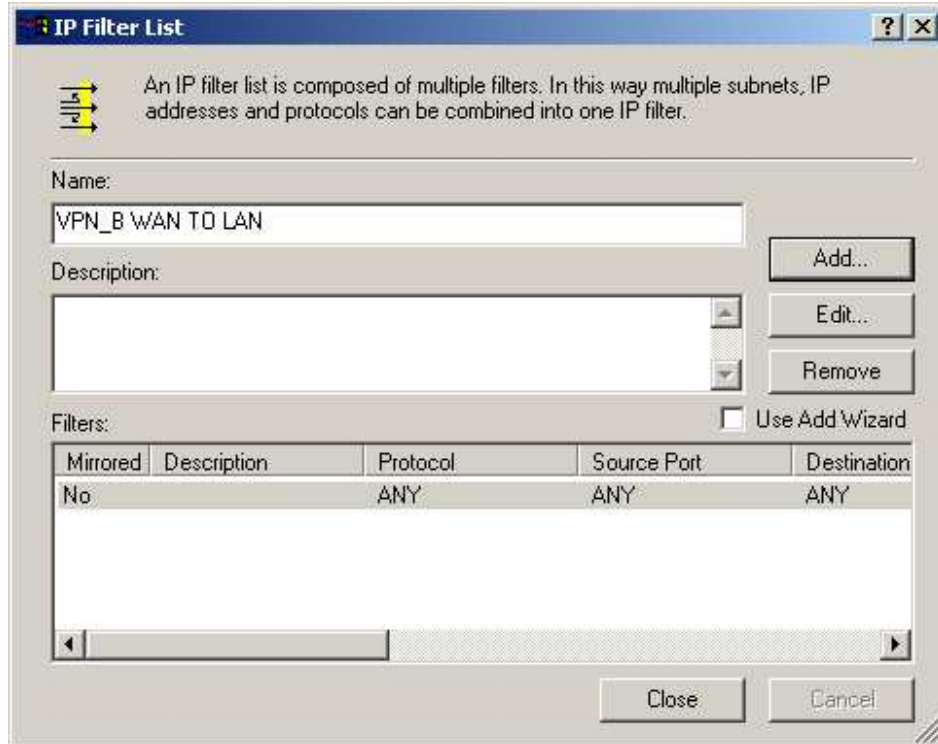


Figure 69 IP Filter List Settings Completed.

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

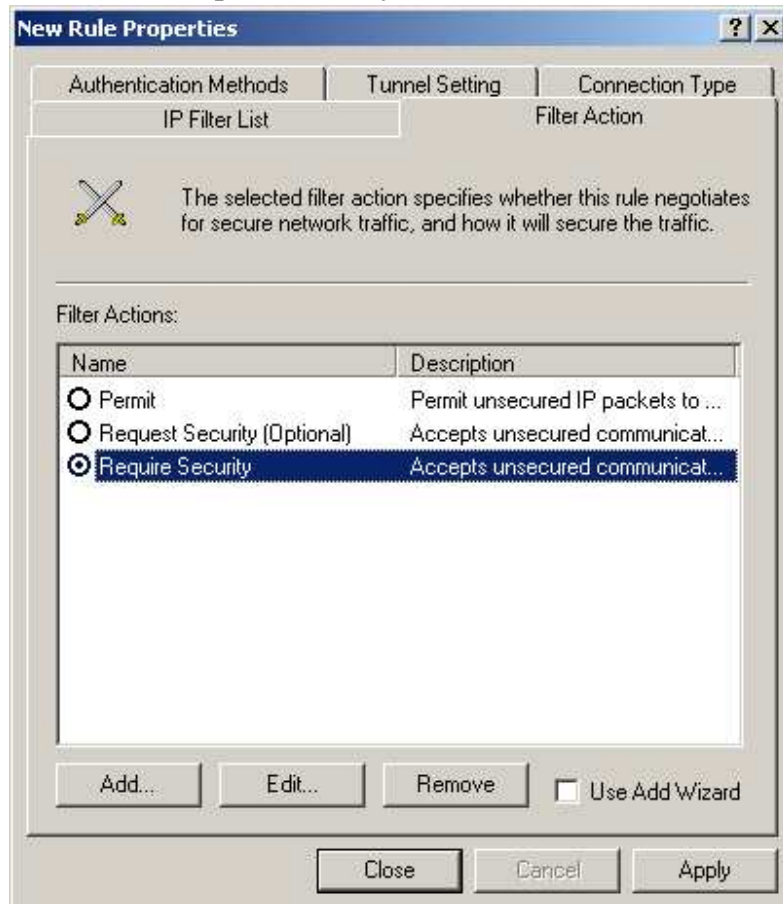


Figure 70 Filter Action Setting

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

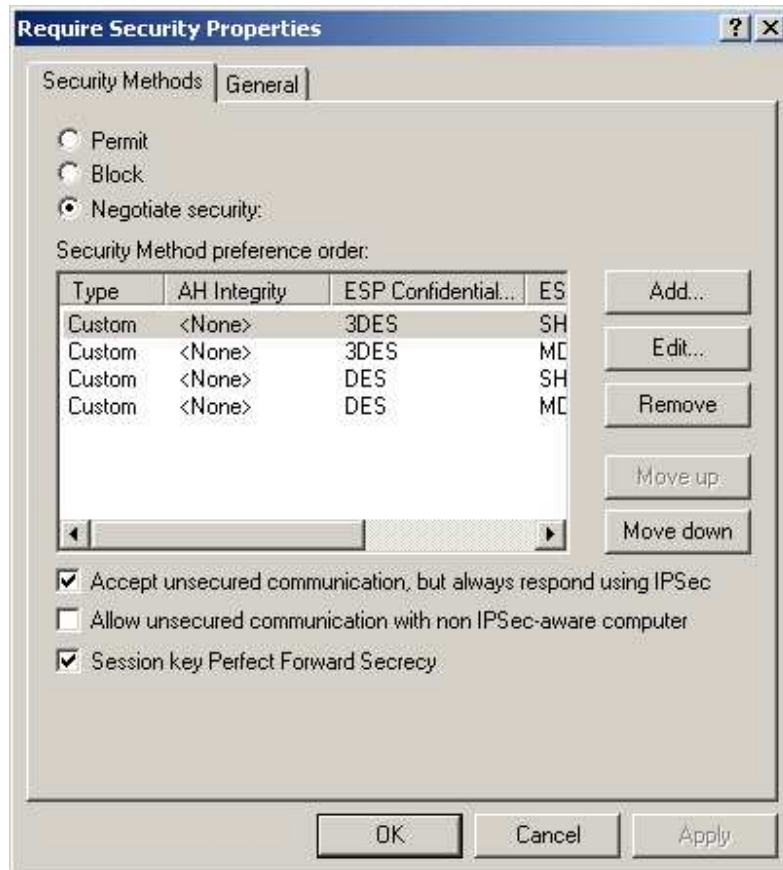


Figure 71 Select Session Key Perfect Forward Security

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

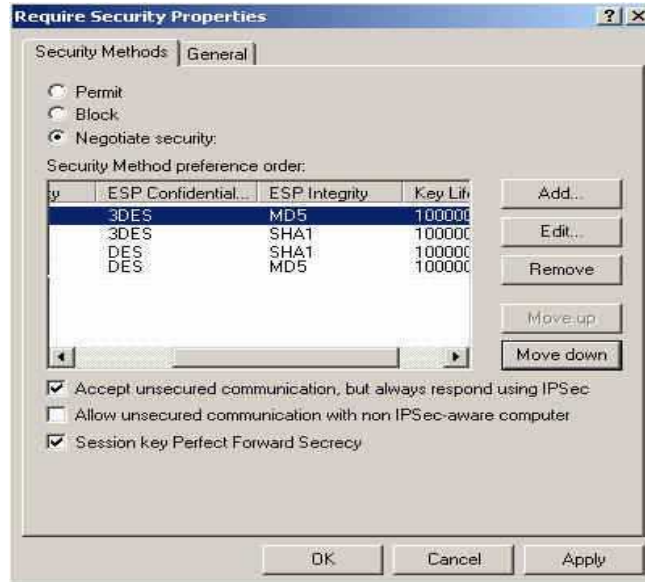


Figure 72 Editing the Security Method

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

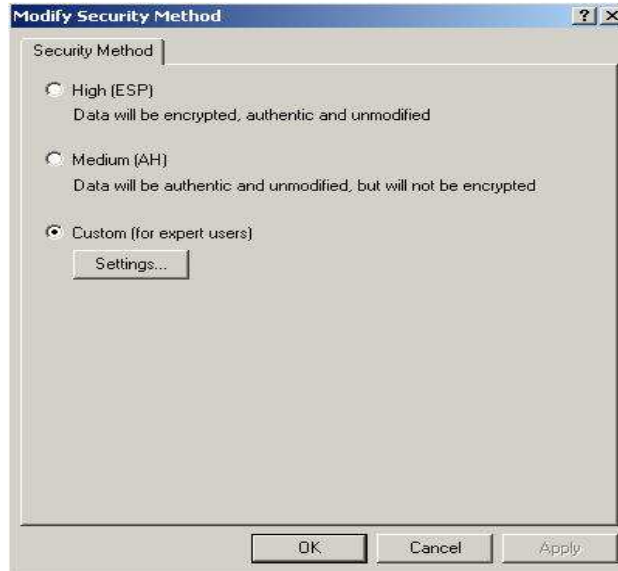


Figure 73 Custom Security Method

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*)

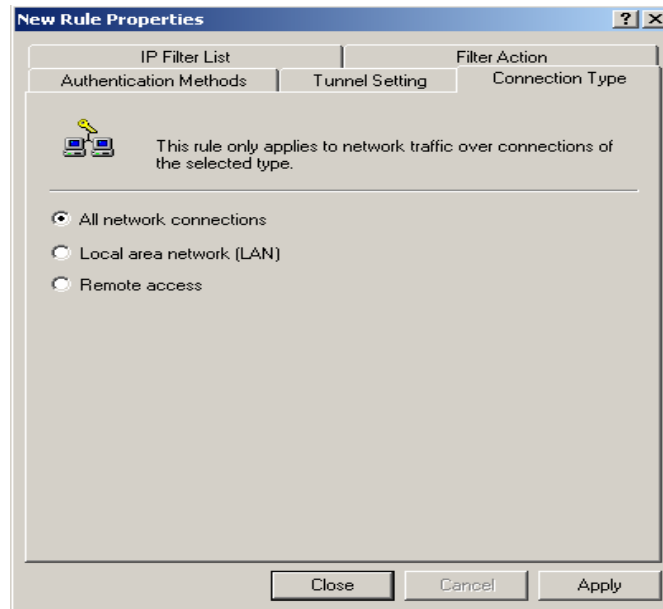


Figure 75 Connection Type Setting

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

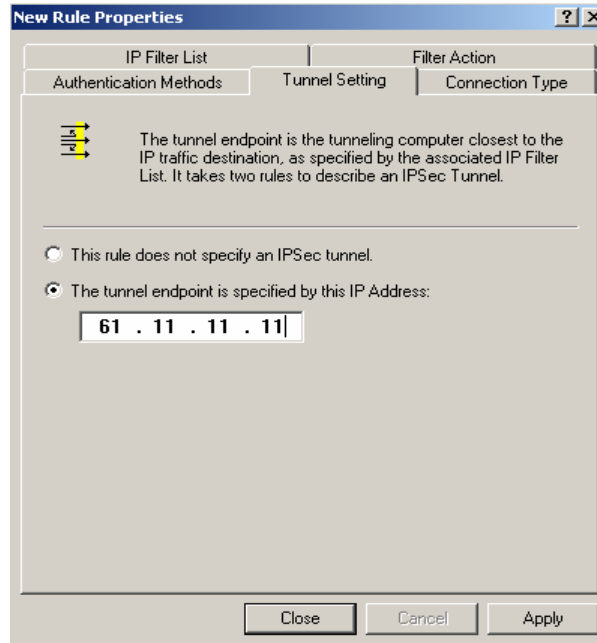


Figure 76 Trunk Setting

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)

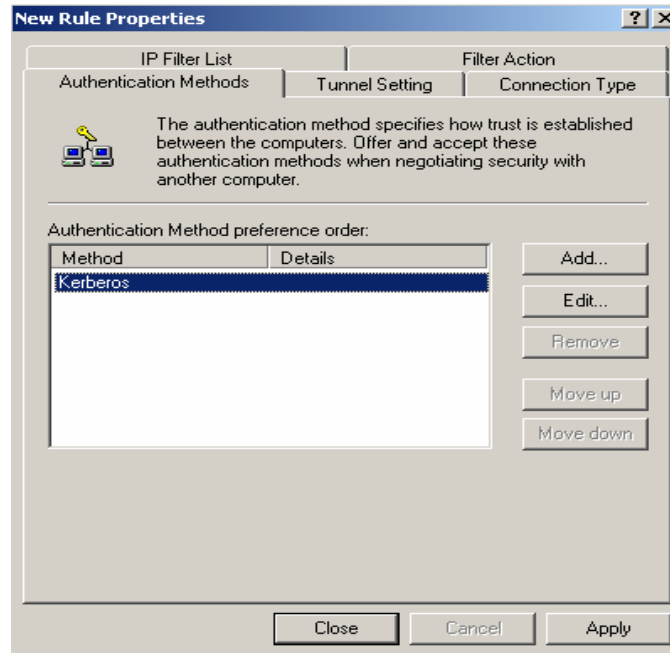


Figure 77 Authentication Methods Setting

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*)

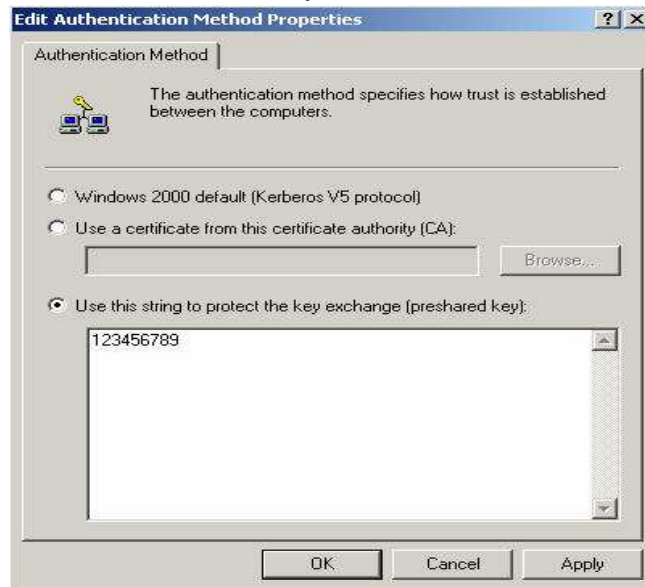


Figure 78 Setting the VPN Preshared Key

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

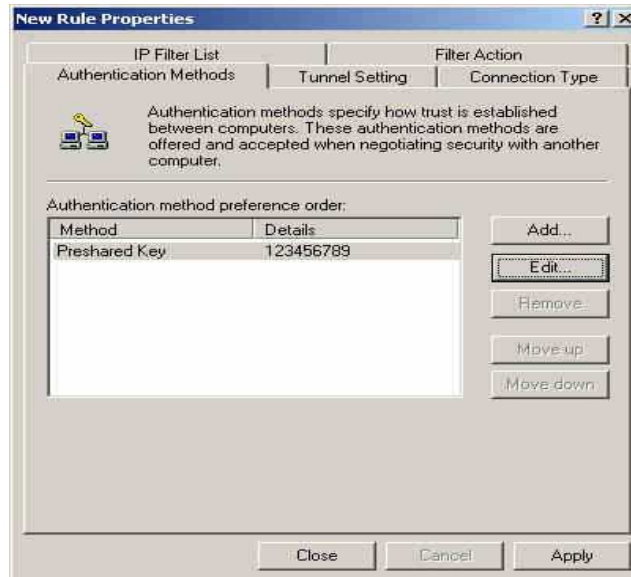


Figure 79 Complete the Authentication Methods Setting

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

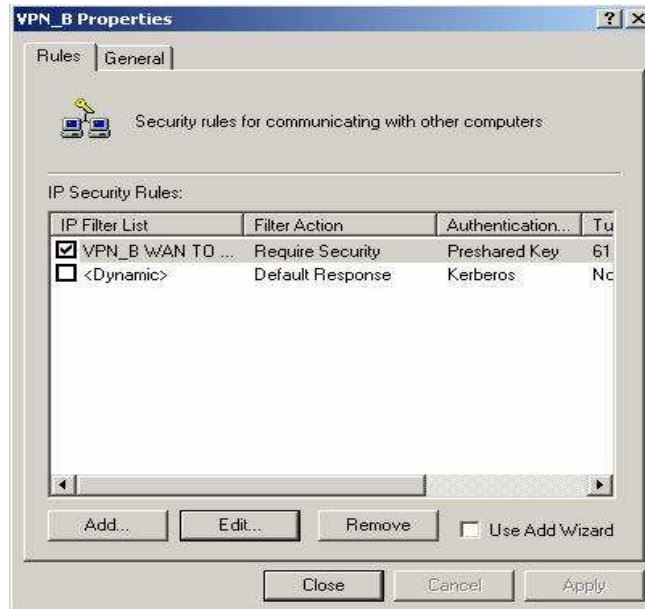


Figure 80 Complete the VPN_B WAN TO LAN Policy Setting

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*)

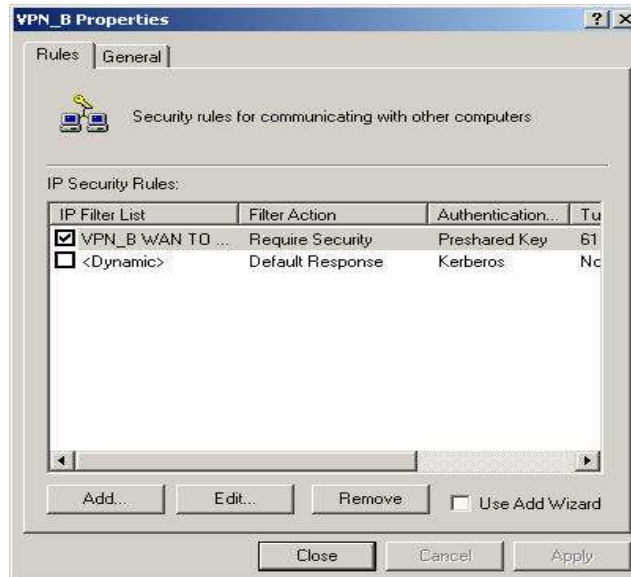


Figure 81 The **VPN_B Properties**

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

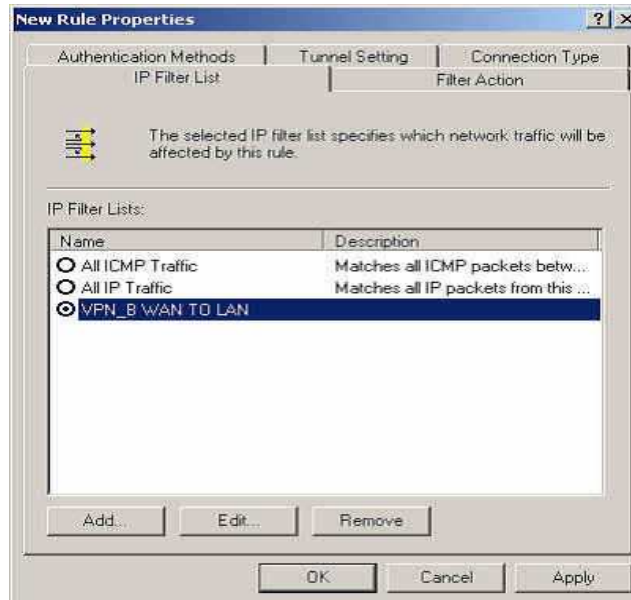


Figure 82 New Rule Properties

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)

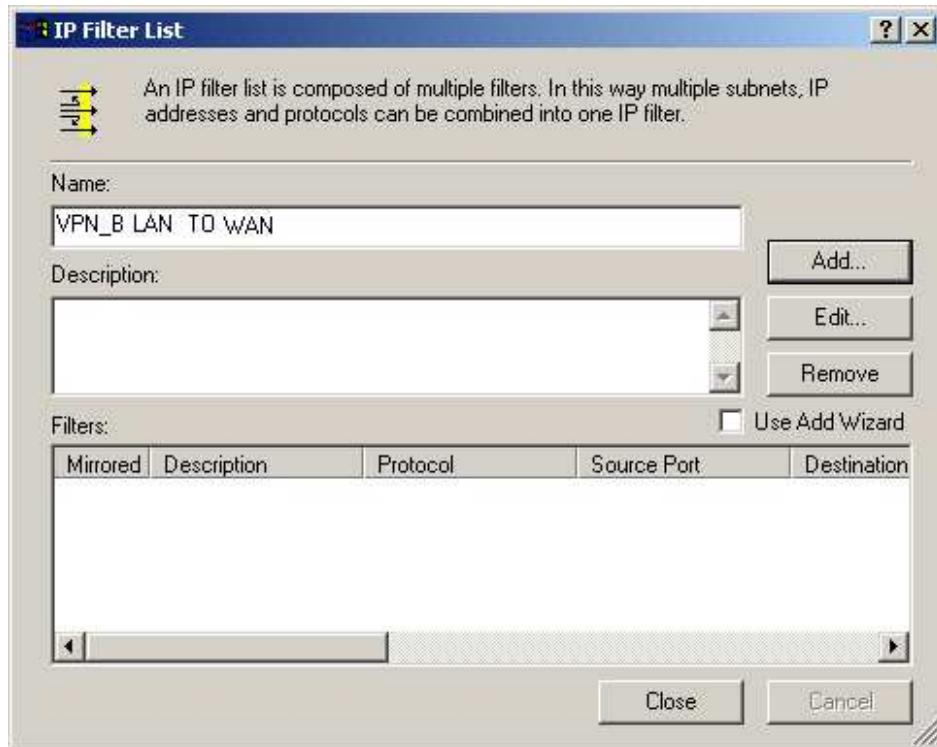
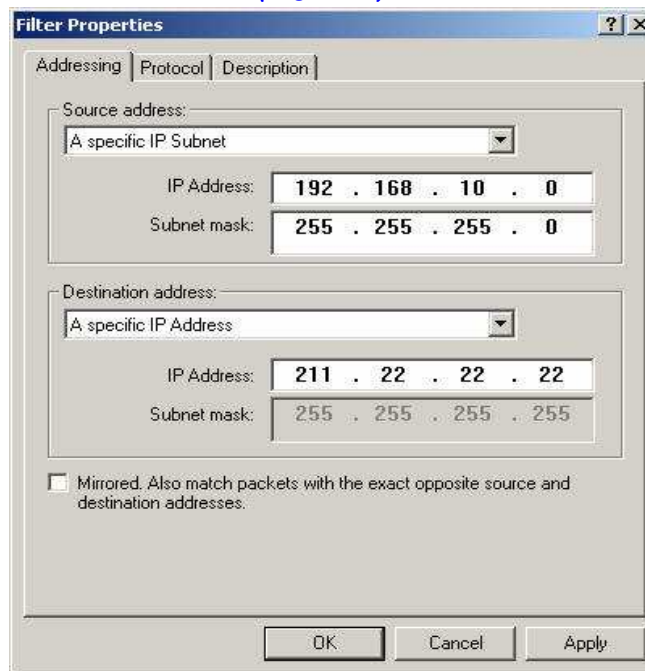


Figure 83 IP Filter List

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)



The screenshot shows the 'Filter Properties' dialog box with the 'Addressing' tab selected. The 'Source address' section has a dropdown menu set to 'A specific IP Subnet', with IP Address '192 . 168 . 10 . 0' and Subnet mask '255 . 255 . 255 . 0'. The 'Destination address' section has a dropdown menu set to 'A specific IP Address', with IP Address '211 . 22 . 22 . 22' and Subnet mask '255 . 255 . 255 . 255'. The 'Mirrored' checkbox is unchecked. The dialog has 'OK', 'Cancel', and 'Apply' buttons at the bottom.

Figure 84 Filter Properties

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

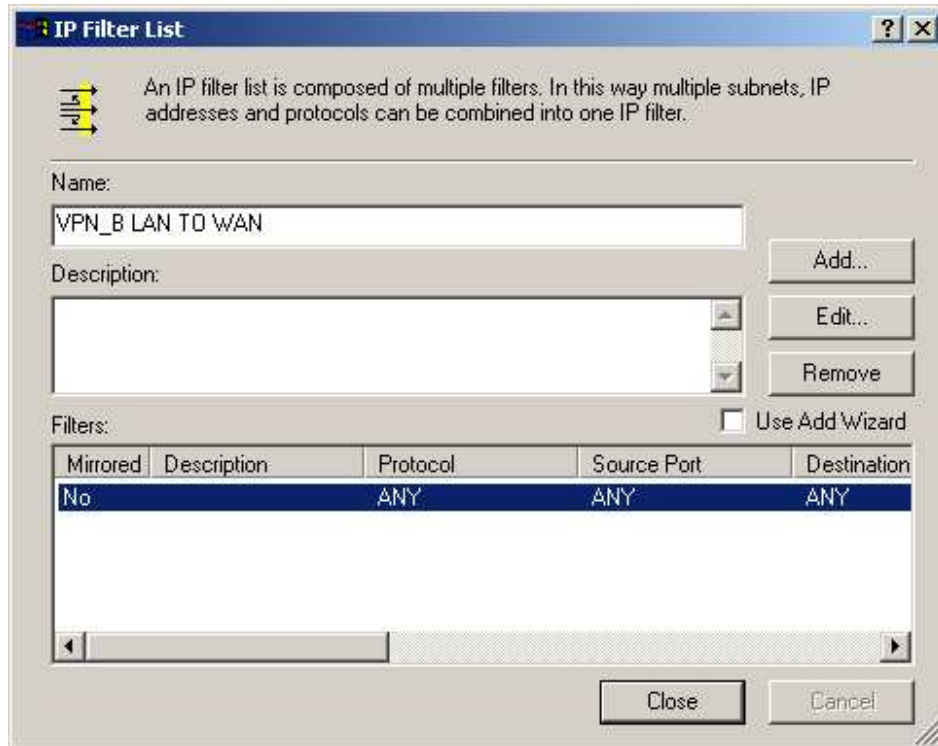


Figure 85 IP Filter List Settings Completed

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

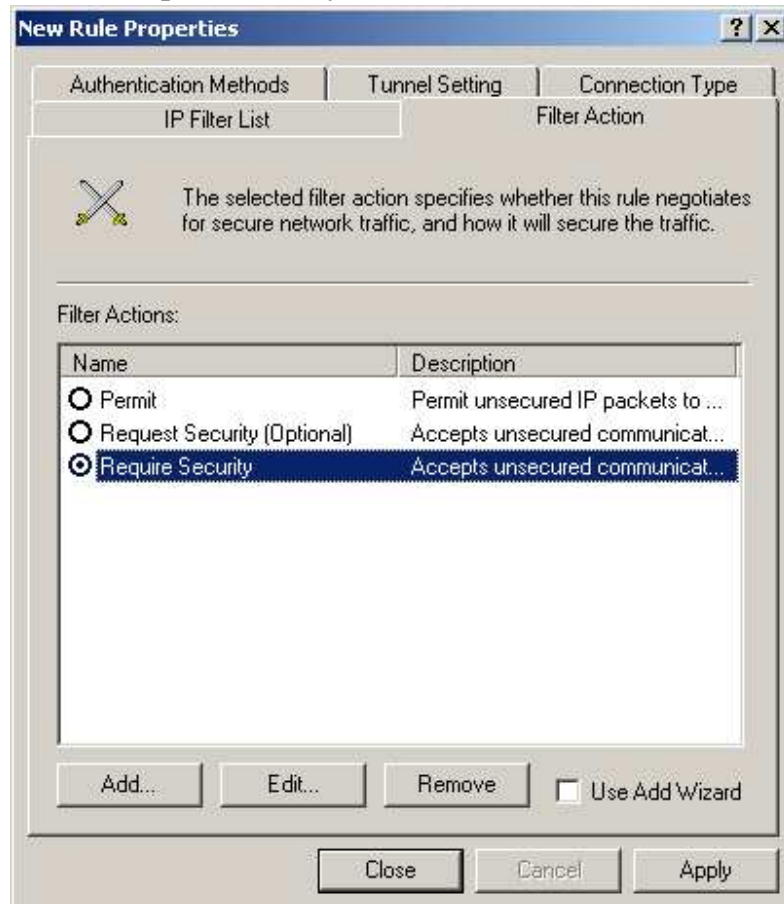


Figure 86 Filter Action

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

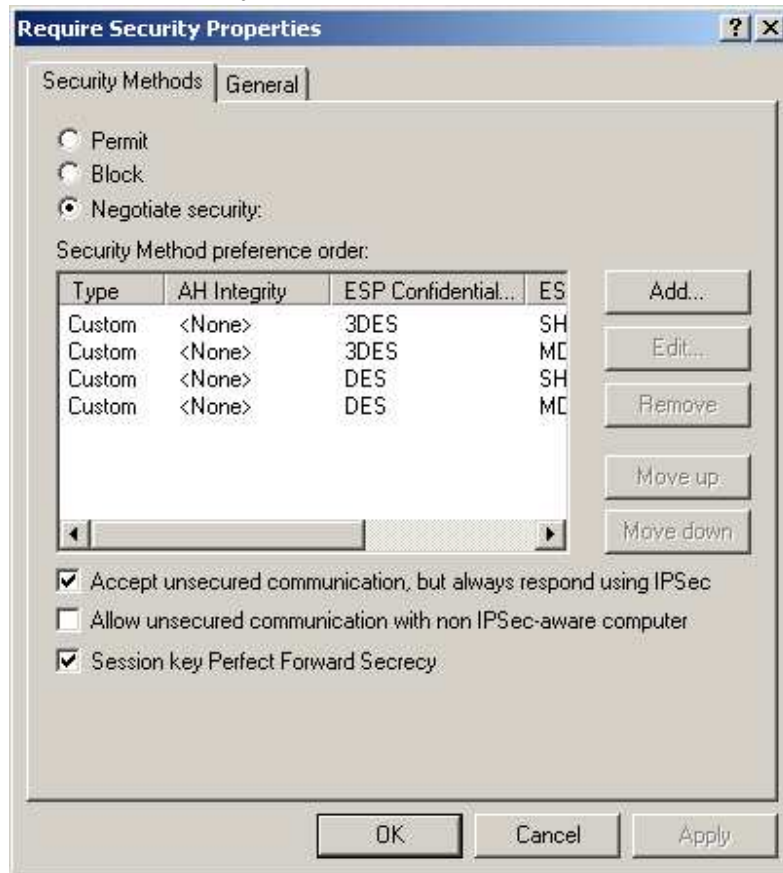


Figure 87 Select Session key Perfect Forward Security

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

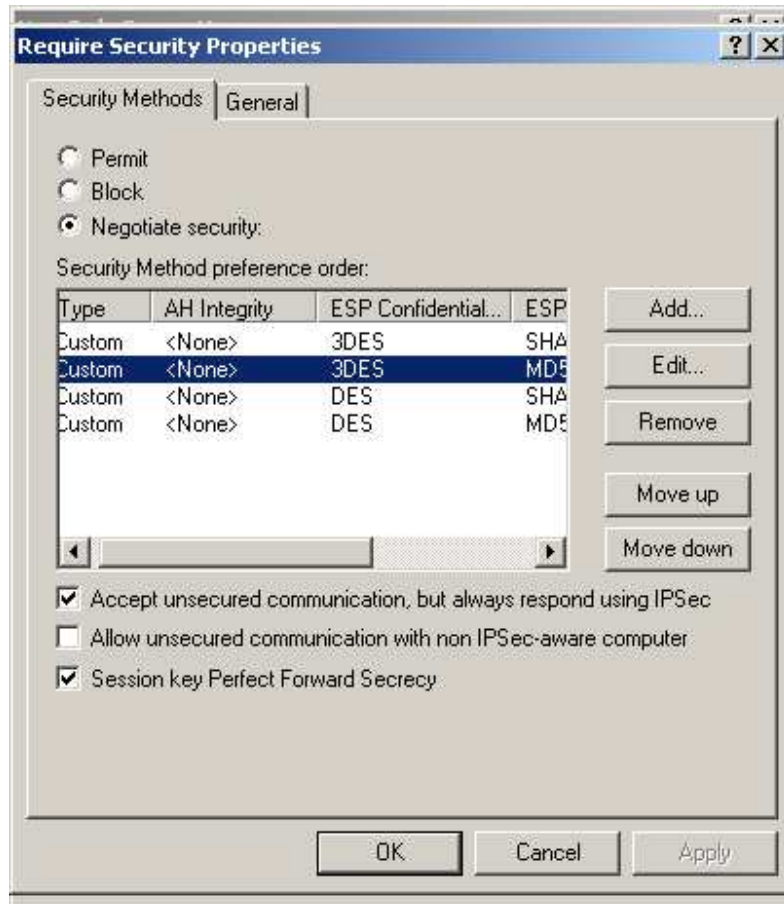


Figure 88 Set the Security Method

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*)

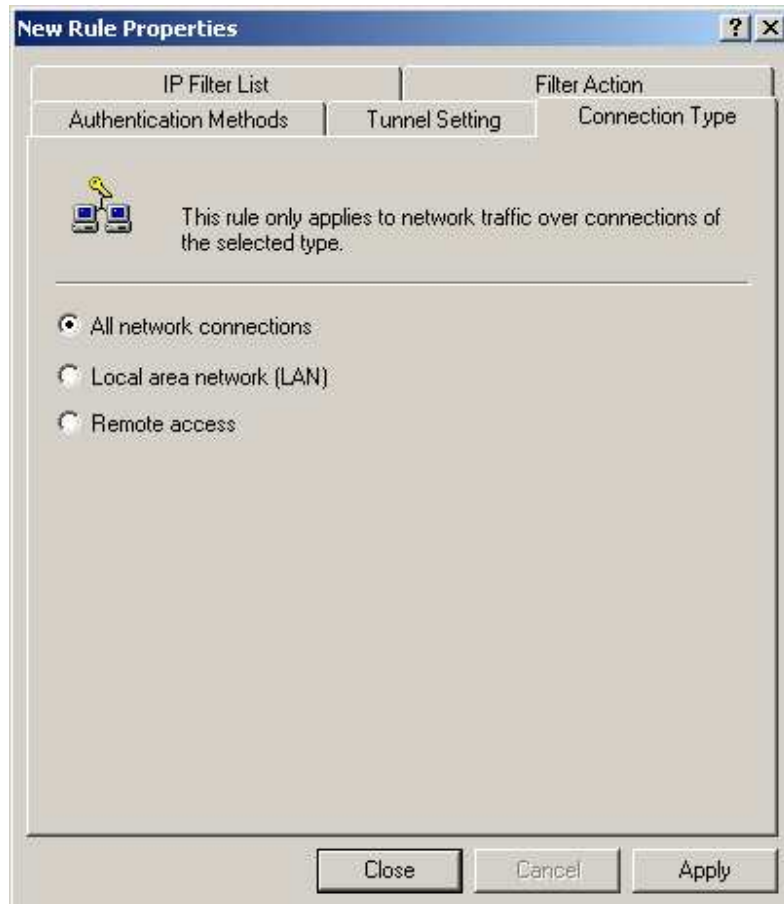


Figure 91 Connection Type Setting

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

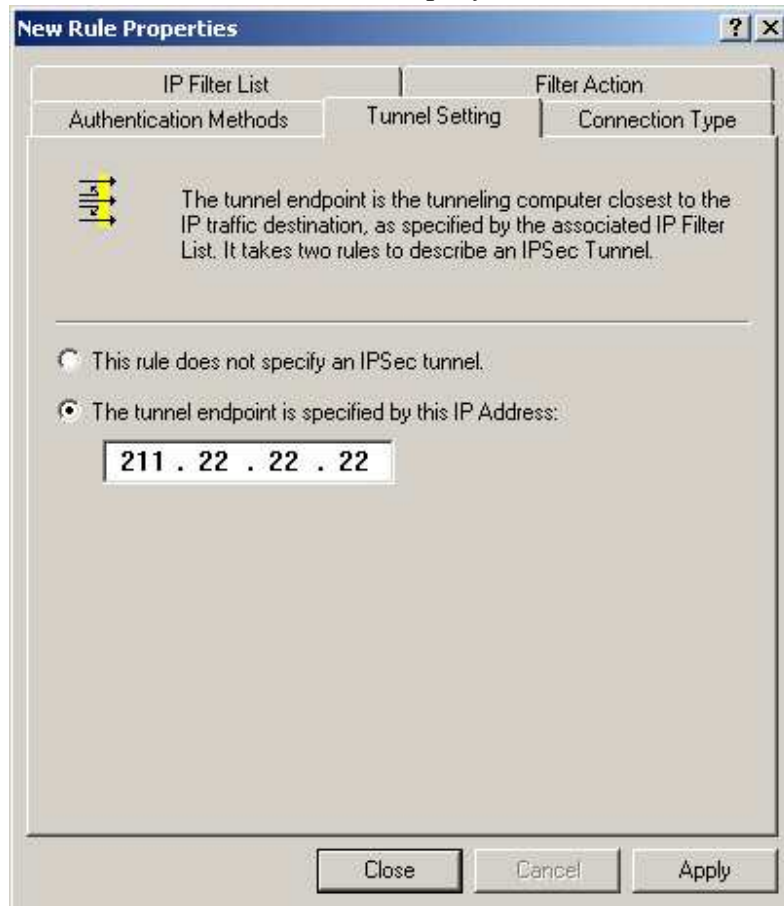


Figure 92 Trunk Setting

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)

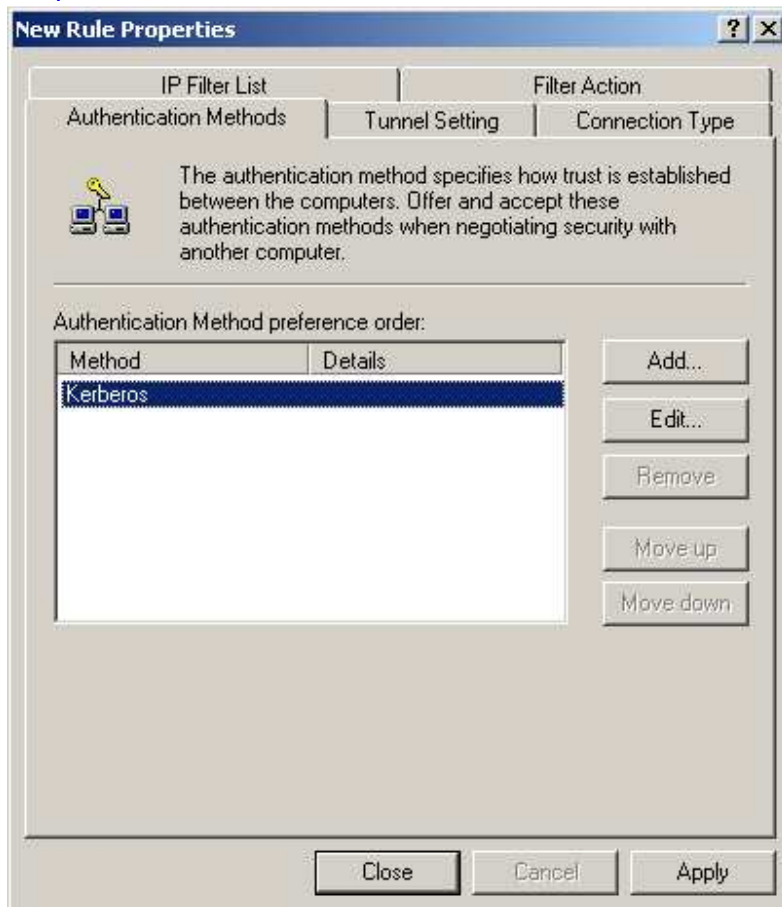


Figure 93 Authentication Methods

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*)

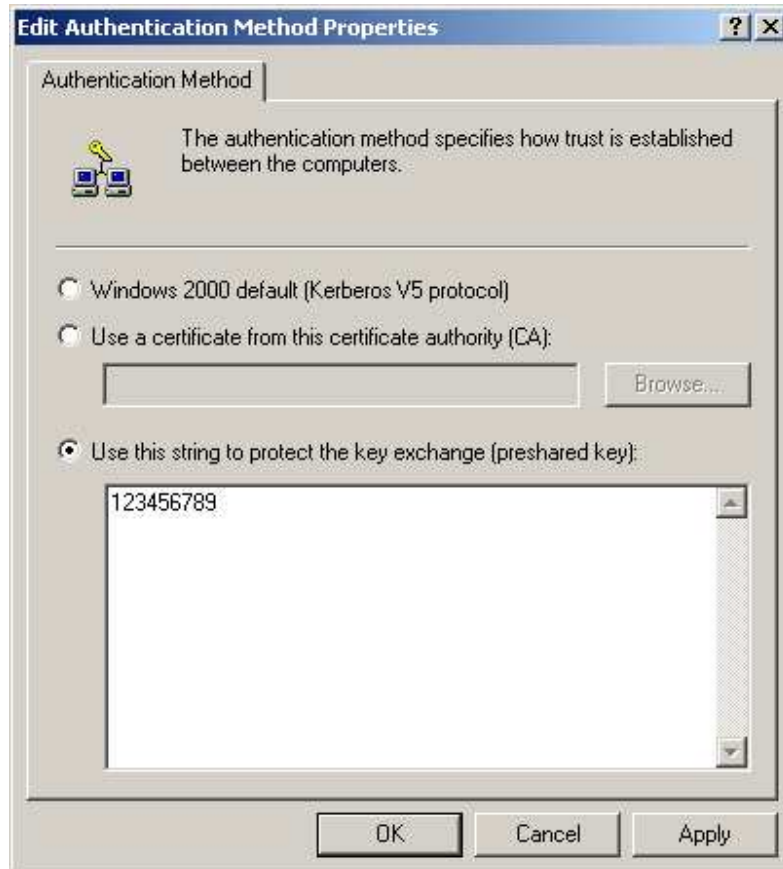


Figure 94 VPN Preshared Key Settings

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*)

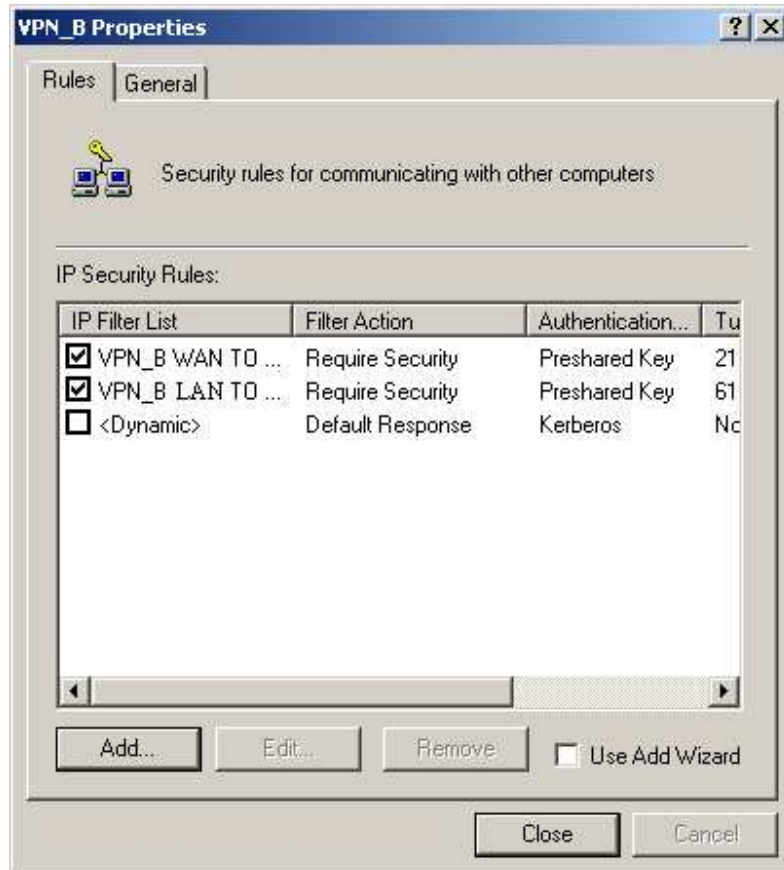


Figure 96 Complete the VPN_B LAN TO WAN Rule Settings

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

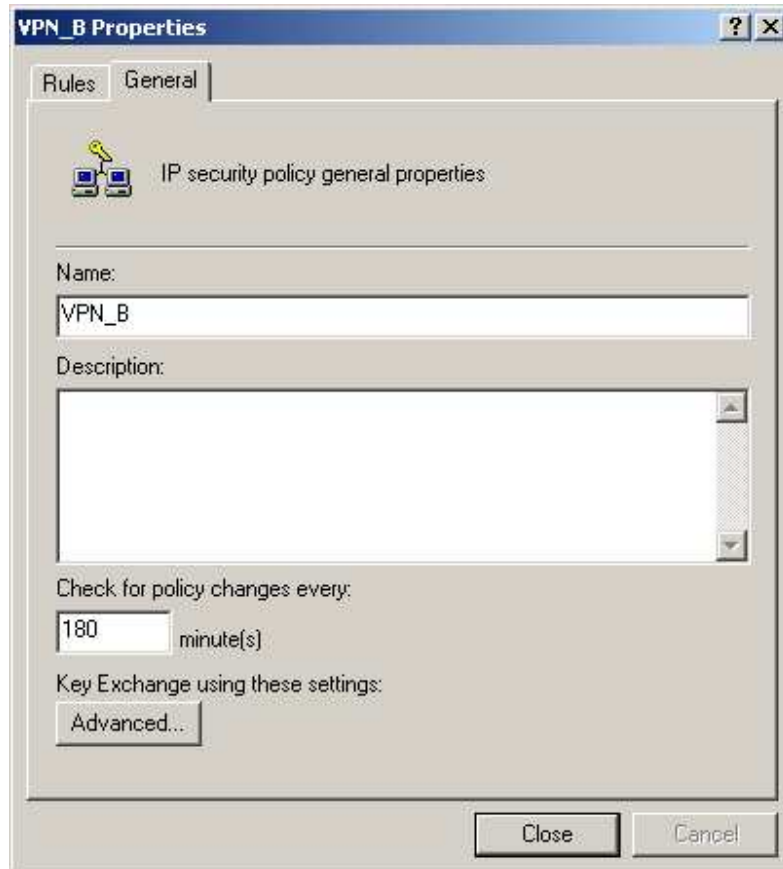


Figure 97 The VPN_B General Setting

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

(*Figure 98*)

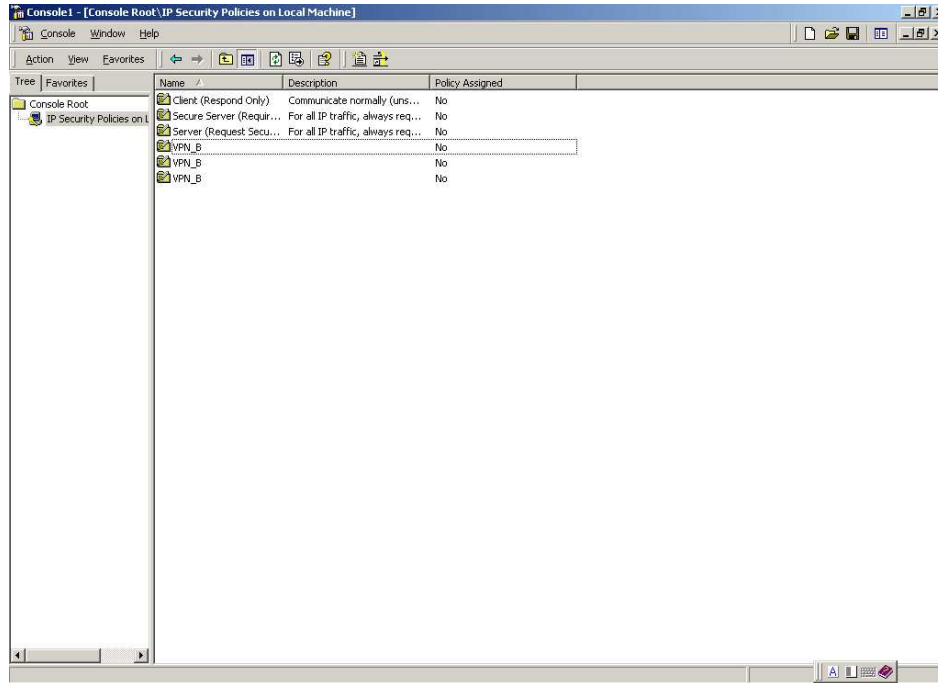


Figure 98 Key Exchange Settings

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)

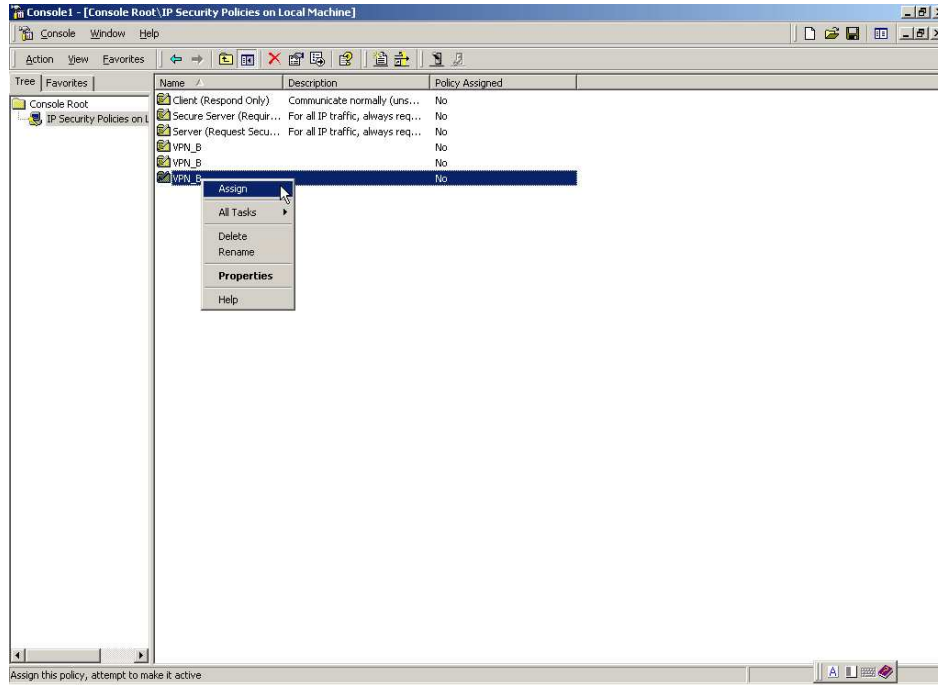


Figure 101 Assigning the VPN_B Security Rules

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

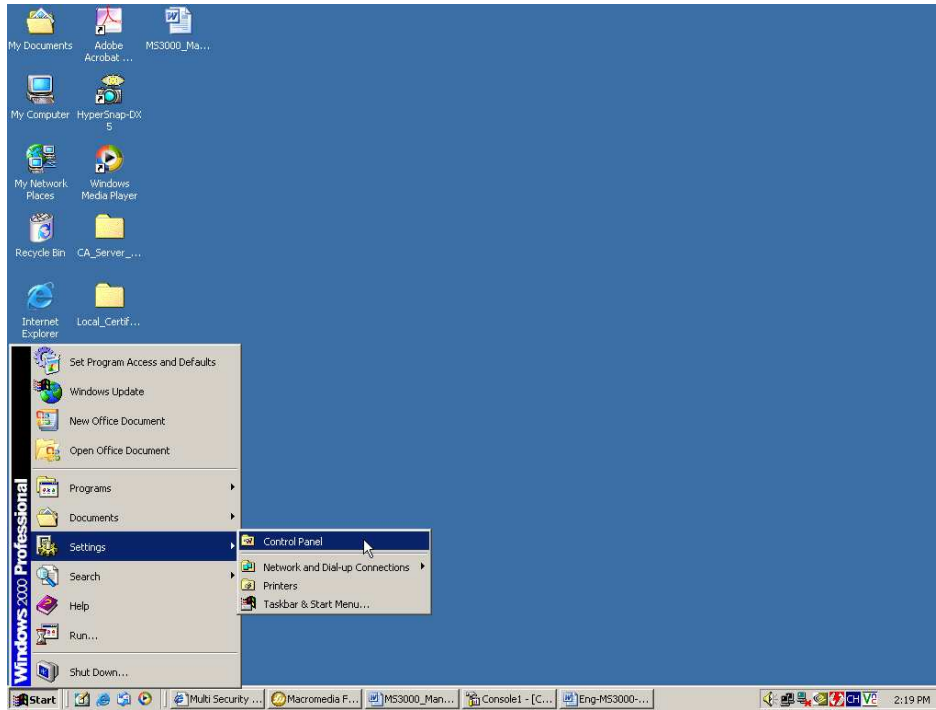


Figure 102 Enter the Control Panel

Step 50. In the Control Panel window, double-click on **Administrative Tools**.
(Figure 103)

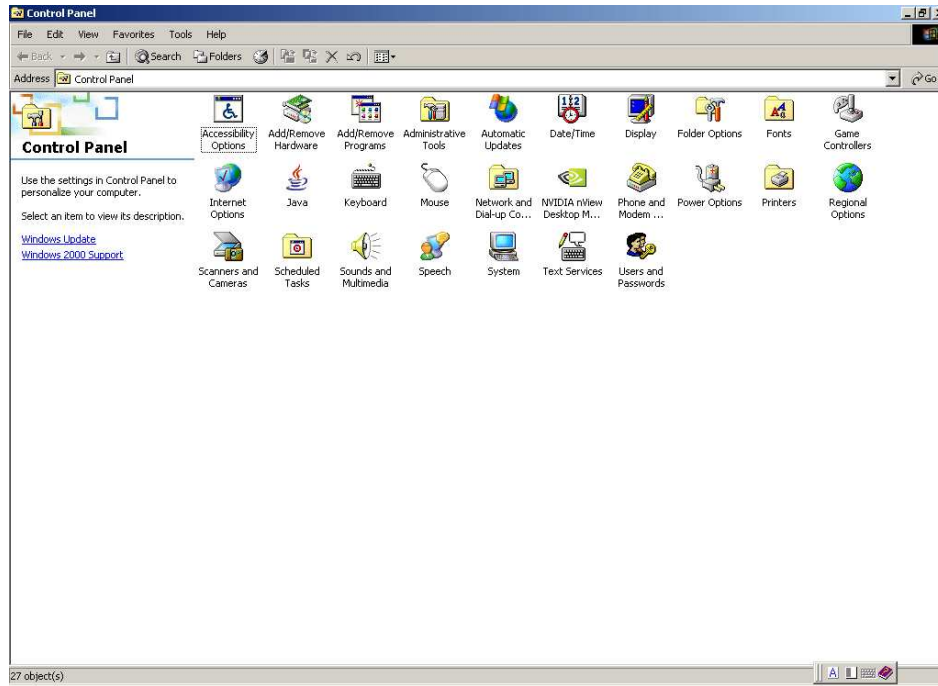


Figure 103 Enter the Administrative Tools

Step 51. In the **Administrative Tools** window, double-click on **Services**.

(Figure 104)

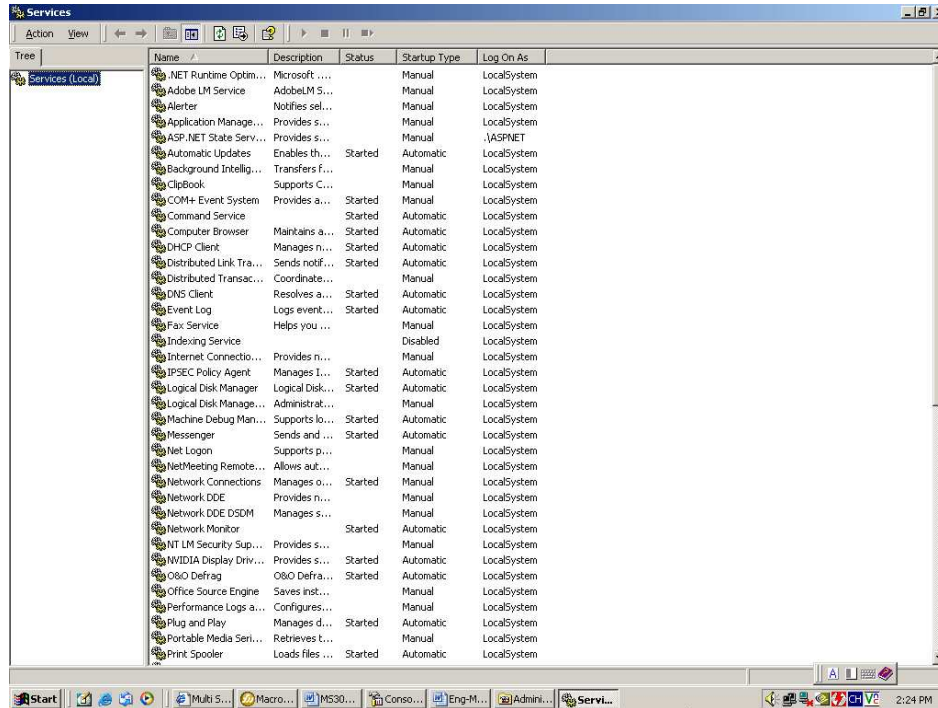


Figure 104 Enter the Services

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

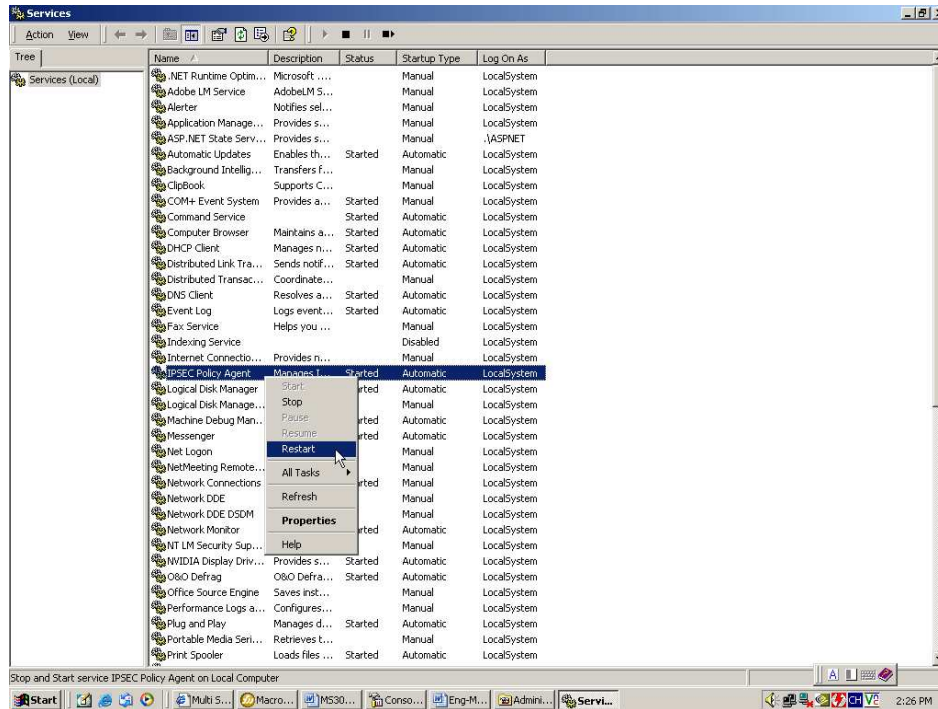


Figure 105 Restart IPsec Policy Agents

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

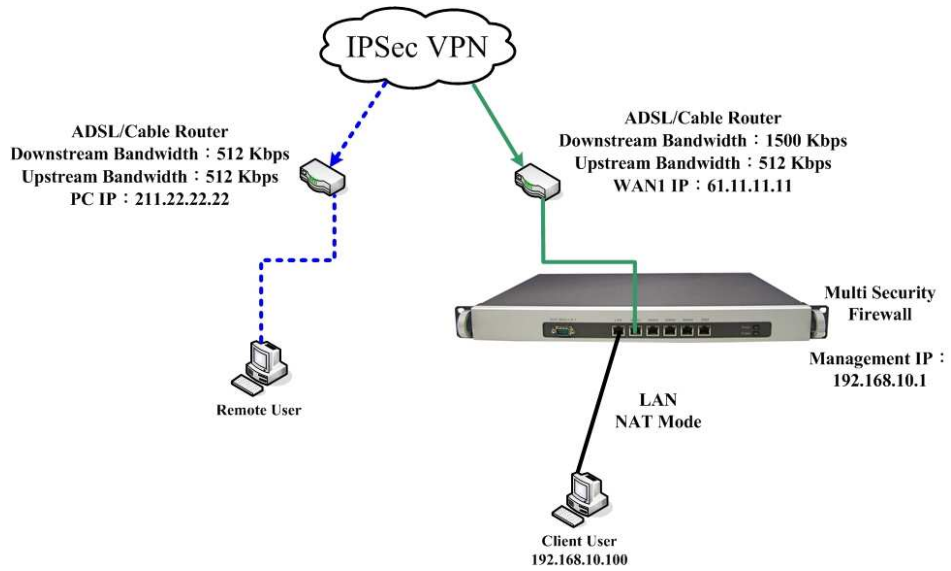


Figure 106 The NUS-MH2400G and Windows 2000 IPSec VPN Deployment

Setting up an IPSec VPN Connection (Aggressive Mode) between Two NUS-MH2400G 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-MH2400G 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-MH2400G. 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)



	Name	WAN	Gateway IP	IPSec Algorithm	Configure
New Entry					

Figure 107 IPSec Autokey

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

Necessary Item	
Name	VPN_A

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)*

To Remote	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	211.22.22.22 (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

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)*

Authentication Method	Preshare
Preshared Key	123456789 (Max. 103 characters)

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*)

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES ▼
AUTH Algorithm	SHA1 ▼
Group	GROUP 2 ▼

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*)

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼

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)

Optional Item	
Perfect Forward Secrecy	GROUP1
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

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)

Mode	<input type="radio"/> Main mode <input checked="" type="radio"/> Aggressive mode
My ID	11.11.11.11 (Max. 39 characters)
Peer ID	@abc123 (Max. 39 characters)

Figure 114 The IPSec Aggressive Mode Setting

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

i	Name	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	211.22.22.22	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 115 Company A IPSec Autokey – Settings Completed

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

- In the **Name** field, enter a unique name for the trunk.
- For the **From Source** setting, select **LAN**.
- In the **Source Subnet / Mask** field, enter 192.168.10.0 / 255.255.255.0.
- From the **To Destination** category, select **To Destination Subnet / Mask** and enter 192.168.20.0 / 255.255.255.0.
- Add **VPN_A** in the Tunnel field.
- Check the **Show remote Network Neighborhood** checkbox.
- Click **OK**. (Figure 117)

Modify IPsec_VPN_Trunk.Trunk

Name: IPSec_VPN_Trunk

From Source: LAN DMZ

From Source Subnet / Mask: 192.168.10.0 / 255.255.255.0

To Destination:

To Destination Subnet / Mask: 192.168.20.0 / 255.255.255.0

Remote Client

Tunnel:

Available Tunnel: VPN_A

Selected Tunnel: VPN_A

Buttons: Remove, Add

Keep alive IP: []

Show remote Network Neighborhood

OK Cancel

Figure 116 New Entry Trunk Settings

I	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPSec_VPN_Tr...	192.168.10.0	192.168.20.0	VPN_A	Modify Remove Pause

New Entry

Figure 117 New Entry Trunk 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.
- **Trunk:** Select IPSec_VPN_Trunk.
- Click **OK**. (Figure 119)

Comment :

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	Schedule_1 ▾
Authentication User	All_NET ▾
Trunk	IPSec_VPN_Trunk ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	QoS_1 ▾
MAX: Concurrent Sessions	<input type="text" value="0"/> (0: means unlimited)
Quota Per Session	<input type="text" value="0"/> KBytes
Quota Per Day	<input type="text" value="0"/> MBytes

OK Cancel

Figure 118 VPN Trunk 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 Trunk 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**.
- **Trunk:** select **IPSec_VPN_Trunk**.
- Click **OK**. (Figure 121)

Comment : (Max. 64 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	Schedule_1 ▾
VPN Trunk	IPSec_VPN_Trunk ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	QoS_1 ▾
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
Quota Per Session	0 KBytes (Range: 0 - 999999)
Quota Per Day	0 MBytes (Range: 0 - 999999)
NAT	<input type="checkbox"/> Enable

OK Cancel

Figure 120 VPN Trunk Incoming Policy Settings

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

New Entry

Figure 121 VPN Trunk Incoming Policy Settings Completed

The LAN IP, 192.168.20.1, is the default gateway of Company B's NUS-MH2400G. 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)

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
<input type="button" value="New Entry"/>					

Figure 122 IPSec Autokey Headings

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

Necessary Item	
Name	<input type="text" value="VPN_B"/> (Max. 12 characters)

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)

To Remote	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="61.11.11.11"/> (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

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)

Authentication Method	Preshare ▾
Preshared Key	<input type="text" value="123456789"/> (Max. 103 characters)

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)*

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	SHA1
Group	GROUP 2

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)*

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

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)

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds

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)

Mode	<input type="radio"/> Main mode <input checked="" type="radio"/> Aggressive mode
My ID	@abc123 (Max. 39 characters)
Peer ID	11.11.11.11 (Max. 39 characters)

Figure 129 The IPSec Aggressive Mode Setting

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

i	Name	Gateway IP	IPSec Algorithm	Configure
--	VPN_B	61.11.11.11	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 130 IPSec Autokey – Settings Completed

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

- **Name:** Enter a specific Trunk name.
- **From Source:** Select **LAN**.
- **From Source Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **To Destination:** Select **To Destination Subnet / Mask** and enter 192.168.10.0 / 255.255.255.0 in the field.
- Add **VPN_B** in the **Tunnel** field.
- Check **Show remote Network Neighborhood**.
- Click **OK**. (Figure 132)

Figure 131 New Entry Trunk Settings

	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPSec_VPN_Tr...	192.168.20.0	192.168.10.0	VPN_B	Modify Remove Pause

New Entry

Figure 132 New Entry Trunk 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_Trunk** from the **Trunk** drop-down list.
- Click **OK**. (Figure 134)

Comment :

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Schedule_1
Authentication User	All_NET
Trunk	IPSec_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	QoS_1
MAX. Concurrent Sessions	0 (0: means unlimited)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

OK Cancel

Figure 133 VPN Trunk 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 Trunk 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**.
- **Trunk:** select **IPsec_VPN_Trunk**.
- Click **OK**. (Figure 136)

Comment : (Max. 64 characters)

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Schedule_1
VPN Trunk	IPSec_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
Quota Per Session	0 KBytes (Range: 0 - 999999)
Quota Per Day	0 MBytes (Range: 0 - 999999)
NAT	<input type="checkbox"/> Enable

OK Cancel

Figure 135 VPN Trunk Incoming Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Modify Remove	To 1

New Entry

Figure 136 VPN Trunk Incoming Policy Settings Completed

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

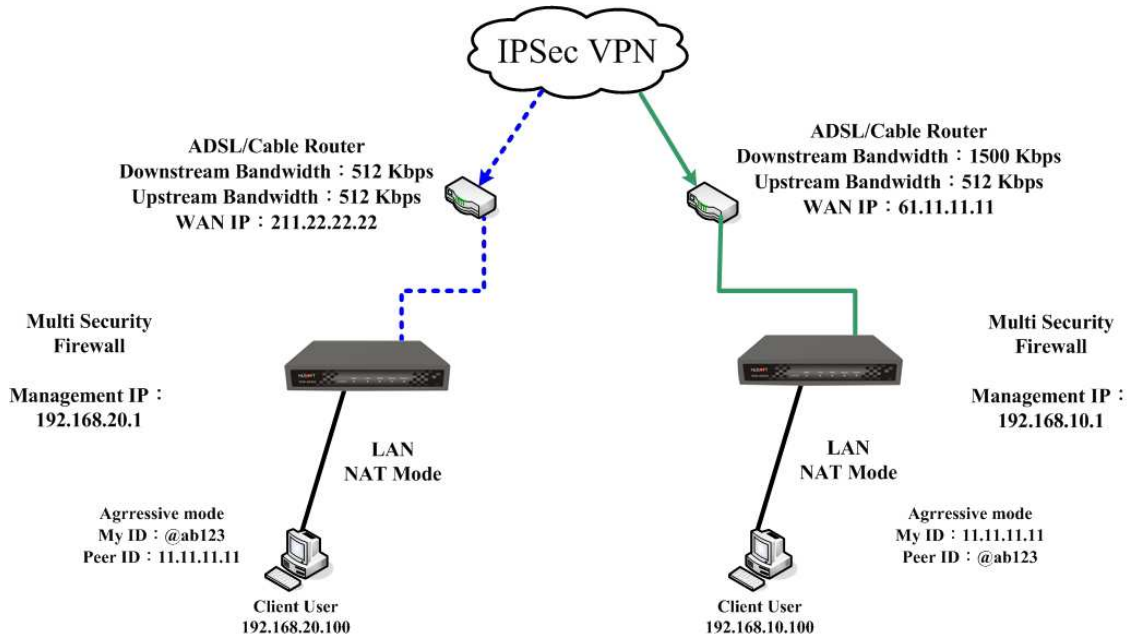


Figure 137 Completed Setup

Setting up an IPSec VPN Connection between Two NUS-MH2400G 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-MH2400G 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-MH2400G. 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)*

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
<input type="button" value="New Entry"/>					

Figure 138 IPSec Autokey Headings

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

Necessary Item	
Name	VPN_A

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)

To Remote	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	211.22.22.22 (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

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)

Authentication Method	Preshare
Preshared Key	123456789 (Max. 103 characters)

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)

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP1

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)

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

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)

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

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)

GRE/IPSec	
GRE Local IP	192.168.50.100
GRE Remote IP	192.168.50.200

Figure 145 GRE/IPSec Settings

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

i	Name	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	211.22.22.22	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 146 Company A IPSec Autokey – Settings Completed

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

- In the **Name** field, enter a unique name for the trunk.
- For the **From Source** setting, select **LAN**.
- In the **Source Subnet / Mask** field, enter 192.168.10.0 / 255.255.255.0.
- From the **To Destination** category, select **To Destination Subnet / Mask** and enter 192.168.20.0 / 255.255.255.0.
- Add **VPN_01** and **VPN_02** in the **Tunnel** field.
- Check the **Show remote Network Neighborhood** checkbox.
- Click **OK**. (Figure 148)

Figure 147 New Entry Trunk Settings

	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPSec_VPN_Tr...	192.168.10.0	192.168.20.0	VPN_01, ...	Modify Remove Pause

New Entry

Figure 148 New Entry Trunk 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.
- **Trunk:** Select IPSec_VPN_Trunk.
- Click **OK**. (Figure 150)

Comment:

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Schedule_1
Authentication User	All_NET
Trunk	IPSec_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	QoS_1
MAX. Concurrent Sessions	0 (0: means unlimited)
Quota Per Session	0 kBytes
Quota Per Day	0 MBytes

OK Cancel

Figure 149 VPN Trunk 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 Trunk 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**.
- **Trunk:** select **IPSec_VPN_Trunk**.
- Click **OK**. (Figure 152)

Comment : (Max. 64 characters)

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Schedule_1
VPN Trunk	IPSec_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
Quota Per Session	0 KBytes (Range: 0 - 999999)
Quota Per Day	0 MBytes (Range: 0 - 999999)
NAT	<input type="checkbox"/> Enable

OK Cancel

Figure 151 VPN Trunk Incoming Policy Settings

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

New Entry

Figure 152 VPN Trunk Incoming Policy Settings Completed

The LAN IP, 192.168.20.1, is the default gateway of Company B's NUS-MH2400G. 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)

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
<input type="button" value="New Entry"/>					

Figure 153 IPSec Autokey Headings

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

Necessary Item	
Name	<input type="text" value="VPN_B"/> (Max. 12 characters)

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)

To Remote	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="61.11.11.11"/> (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

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)

Authentication Method	<input type="text" value="Preshare"/>
Preshared Key	<input type="text" value="123456789"/> (Max. 103 characters)

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)

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1

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)

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

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)

Optional Item	
Perfect Forward Secrecy	GROUP1
ISAKMP Lifetime	3600 Seconds
IPSec Lifetime	28800 Seconds
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

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)

GRE/IPSec	
GRE Local IP	192.168.50.200
GRE Remote IP	192.168.50.100

Figure 160 GRE/IPSec Settings

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

i	Name	Gateway IP	IPSec Algorithm	Configure
--	VPN_B	61.11.11.11	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
<input type="button" value="New Entry"/>				

Figure 161 Company B IPSec Autokey Settings Completed

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

- **Name:** Enter a specific Trunk name.
- **From Source:** Select **LAN**.
- **From Source Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **To Destination:** Select **To Destination Subnet / Mask** and enter 192.168.10.0 / 255.255.255.0.
- Add **VPN_01** and **VPN_02** in the **Tunnel** field.
- Check **Show remote Network Neighborhood**.
- Click **OK**. (Figure 163)

Figure 162 New Entry Trunk Settings

I	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPSec_VPN_Tr...	192.168.20.0	192.168.10.0	VPN_01, ...	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

Figure 163 New Entry Trunk 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**.
- **Trunk:** Select **IPSec_VPN_Trunk**.
- Click **OK**. (Figure 165)

Comment :

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Schedule_1
Authentication User	All_NET
Trunk	IPSec_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	QoS_1
MAX. Concurrent Sessions	0 (0: means unlimited)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

OK Cancel

Figure 164 VPN Trunk 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 Trunk 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**.
- **Trunk:** select **IPSec_VPN_Trunk**.
- Click **OK**. (Figure 167)

Comment : (Max: 64 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	Schedule_1 ▾
VPN Trunk	IPSec_VPN_Trunk ▾
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	QoS_1 ▾
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
Quota Per Session	0 KBytes (Range: 0 - 999999)
Quota Per Day	0 MBytes (Range: 0 - 999999)
NAT	<input type="checkbox"/> Enable

OK Cancel

Figure 166 VPN Trunk Incoming Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN	<input type="checkbox"/> <input type="checkbox"/>	Modify Remove	To 1 ▾

New Entry

Figure 167 VPN Trunk Incoming Policy Settings Completed

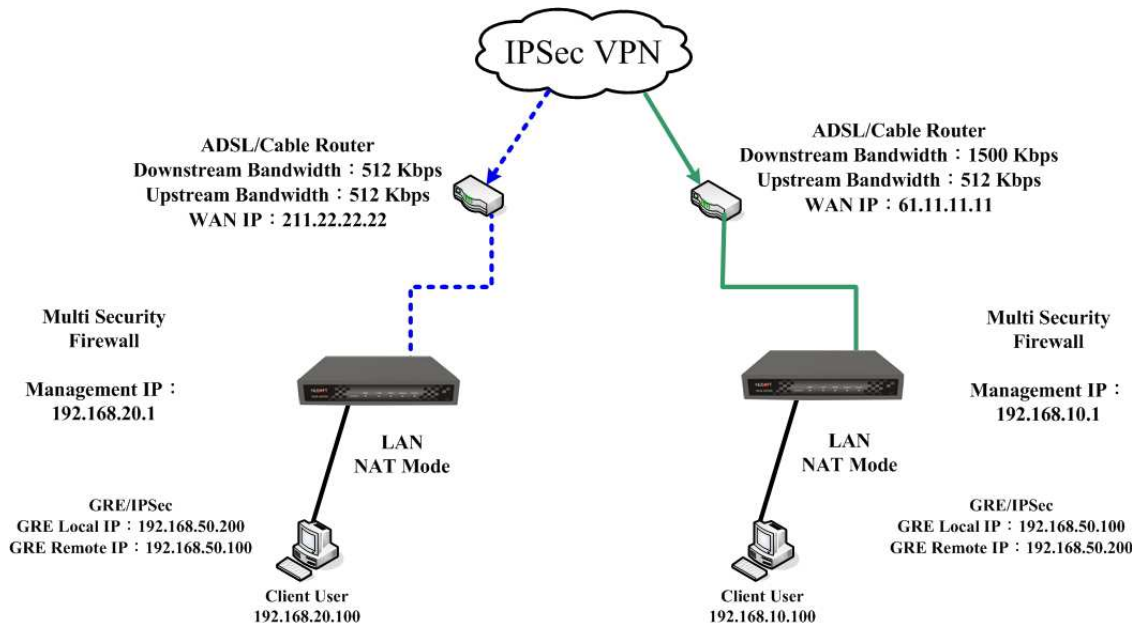
Step 13. The Completed IPsec VPN GRE/IPsec Connection Setup (Figure 168)

Figure 168 Completed Setup

Setting up a PPTP VPN Connection between Two NUS-MH2400G Devices

Scenario:

Company A **WAN 1 IP: 61.11.11.11**
 WAN 2 IP: 61.22.22.22
 LAN IP: 192.168.10.X

Company B **WAN 1 IP: 211.22.22.22**
 WAN 2 IP: 211.33.33.33
 LAN IP: 192.168.20.X

To build the IPSec VPN between Company A WAN1 (Server) and Company B WAN1 (Client).

To build the IPSec VPN between Company A WAN2 (Server) and Company B WAN2 (Client).

This example is based upon two NUS-MH2400G 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-MH2400G. Proceed with the following steps:

Step 1. Using Company A's NUS-MH2400G, 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)

Modify Server Design	
<input type="radio"/>	Disable PPTP
<input checked="" type="radio"/>	Enable PPTP
<input checked="" type="checkbox"/>	Encryption
Client IP Range :	192.44.75.1 -- 254
<input checked="" type="checkbox"/>	Allow remote client to connect to Internet.
<input checked="" type="checkbox"/>	WAN1
<input checked="" type="checkbox"/>	WAN2
<input checked="" type="checkbox"/>	WAN3
<input checked="" type="checkbox"/>	WAN4
Auto-Disconnect if idle	0 minutes (Range: 0 - 999999, 0: means always connected)
Echo-Request	Retry 3 times Timeout 15 Second (Retry Range: 0 - 9, 0: means disable; Timeout Range: 1 - 30)
<input type="checkbox"/>	Enable RADIUS Server Authentication
(IP or Domain Name)	
RADIUS Server Port	1812 (Range: 1 - 65535)
Shared Secret	(Max. 40 characters)
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 169 Enable PPTP VPN Server Settings



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



RADIUS Server Authentication can be done under Authentication > RADIUS. In this case, the IT administrator should add a **username** as **[*]** and a **password** as **[@radius]** for the client user to authenticate and connect to the PPTP VPN server.

Step 2. Using Company A's NUS-MH2400G, go to **Policy Object > VPN > PPTP Server**. Click on the **New Entry** button and configure the following:

- Click **New Entry**.
- **User Name:** Enter **PPTP_01**. (Figure 170)
- **Password:** Enter 123456789.
- From the **Client IP assigned by** category, select **IP Range**.
- Click **OK**.
- Click **New Entry**. (Figure 171)
- **User Name:** Enter **PPTP_02**. (Figure 172)
- **Password:** Enter 987654321.
- From the **Client IP assigned by** category, select **IP Range**.
- Click **OK**. (Figure 173)

Figure 170 PPTP VPN Server Settings

I	User Name	Client IP	Uptime	Configure
--	PPTP_01	0.0.0.0	---	Modify Remove

Figure 171 PPTP VPN Server Settings Completed

Add New PPTP Server

User Name :	<input type="text" value="PPTP_02"/>	(Max. 16 characters)
Password :	<input type="password" value="*****"/>	(Max. 19 characters)
Client IP assigned by		
<input checked="" type="radio"/> IP Range		
<input type="radio"/> Fixed IP :	<input type="text"/>	
<input type="checkbox"/> Manual Disconnect		

Figure 172 PPTP VPN Server Settings

PPTP Server (Enable, Encryption: ON):

Client IP Range : 192.44.75.1-254

i	User Name	Client IP	Uptime	Configure
--	PPTP_01	0.0.0.0	---	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
--	PPTP_02	0.0.0.0	---	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 173 PPTP VPN Settings Completed

Step 3. Go to **Policy Object > VPN > Trunk**. Click on the **New Entry** button and enter the following settings: *(Figure 174)*

- **Name:** Enter a unique name for the Trunk.
- **From Local:** Select **LAN**.
- **From Source Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet/ Mask and enter 192.168.20.0/ 255.255.255.0.
- Add **PPTP_Server_PPTP_01** and **PPTP_Server_PPTP_02** in the **Tunnel** field.
- Check **Show remote Network Neighborhood**.
- Click **OK**. *(Figure 175)*

Figure 174 New Entry Trunk Setting

I	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	IPSec_VPN_Tr...	192.168.10.0	192.168.20.0	PPTP_Ser...	Modify Remove Pause

New Entry

Figure 175 VPN Trunk Settings Completed

Step 4. Go to **Policy > Outgoing** and click on the **New Entry** button and enter the following settings: (Figure 176)

- **Authentication User:** Select **All_NET**.
- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Trunk:** Select **PPTP_VPN_Trunk**.
- Click **OK**. (Figure 177)

Comment:

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Schedule_1
Authentication User	All_NET
Trunk	PPTP_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	QoS_1
MAX. Concurrent Sessions	0 (0 means unlimited.)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

OK Cancel

Figure 176 VPN Trunk Outgoing Policy Settings

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

New Entry

Figure 177 VPN Trunk Outgoing Policy Settings Completed

Step 5. Go to **Policy > Incoming**. Click on the **New Entry** button and enter the following settings: (Figure 178)

- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Trunk:** Select **PPTP_VPN_Trunk**.
- Click **OK**. (Figure 179)

Comment : (Max. 64 characters)

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Schedule_1
VPN-Trunk	PPTP_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
Quota Per Session	0 KBytes (Range: 0 - 999999)
Quota Per Day	0 MBytes (Range: 0 - 999999)
NAT	<input type="checkbox"/> Enable

OK Cancel

Figure 178 VPN Trunk Incoming Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Modify Remove	To 1

New Entry

Figure 179 VPN Trunk Incoming Policy Settings Completed

The LAN IP, 192.168.20.1, is the default gateway of Company B's NUS-MH2400G. Proceed with the following steps:

- Step 1.** Using company B's NUS-MH2400G. Go to **Policy Object > VPN > PPTP Client**. Click on the **New Entry** button and enter the following settings:
- **User Name:** Enter PPTP_01. *(Figure 180)*
 - **Password:** Enter 123456789.
 - **Server IP or Domain Name:** Enter Company A's WAN IP address.
 - Check **Encryption**.
 - **WAN interface:** Select **WAN 1**
 - Click **OK**.
 - Click **New Entry**. *(Figure 181)*
 - **User Name:** Enter PPTP_02. *(Figure 182)*
 - **Password:** Enter 987654321.
 - **Server IP or Domain Name:** Enter Company B's WAN 2 IP address.
 - Check **Encryption**.
 - **WAN interface:** Select **WAN 2**.
 - Click **OK**. *(Figure 183)*

Figure 180 PPTP VPN Client Settings

PPTP Client :

i	User Name	Server IP or Domain Name	Encryption	Uptime	Configure
--	PPTP_01	61.11.11.11	ON	---	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 181 PPTP VPN Client Settings Completed

Add New PPTP Client

User Name :	<input type="text" value="PPTP_02"/>	(Max. 16 characters)
Password :	<input type="password" value="*****"/>	(Max. 19 characters)
Server IP or Domain Name :	<input type="text" value="61.22.22.22"/>	(Max. 39 characters) <input checked="" type="checkbox"/> Encryption
WAN interface :	<input type="radio"/> WAN 1 <input checked="" type="radio"/> WAN 2 <input type="radio"/> WAN 3 <input type="radio"/> WAN 4	
<input type="checkbox"/> NAT (Connect to Windows PPTP Server)		
<input type="checkbox"/> Manual Connect		
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

Figure 182 PPTP VPN Client Settings

PPTP Client :

I	User Name	Server IP or Domain Name	Encryption	Uptime	Configure
--	PPTP_01	61.11.11.11	ON	---	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
--	PPTP_02	61.22.22.22	ON	---	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 183 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-MH2400G) and the PPTP Server (Windows).

Step 2. Go to **VPN > Trunk**. Click on the **New Entry** button and enter the following settings: (Figure 184)

- **Name:** Enter a specific Trunk name.
- **From Source:** Select **LAN**.
- **From Source Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **To Remote:** Select **To Remote Subnet / Mask** and enter 192.168.10.0 / 255.255.255.0.
- Add **PPTP_Client_PPTP_01(61.11.11.11)** and **PPTP_Client_PPTP_02(61.22.22.22)** in the **Tunnel** field.
- Check **Show remote Network Neighborhood**.
- Click **OK**. (Figure 185)

Figure 184 New Entry Trunk Settings

	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	PPTP_VPN_Tru...	192.168.20.0	192.168.10.0	PPTP_Cli...	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

New Entry

Figure 185 New Entry Trunk Setting Completed

Step 3. Go to **Policy > Outgoing**. Click on the **New Entry** button and enter the following settings: (Figure 186)

- **Authentication User:** Select **All_NET**.
- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Trunk:** Select **PPTP_VPN_Trunk**.
- Click **OK**. (Figure 187)

Comment :

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	Schedule_1
Authentication User	All_NET
Trunk	PPTP_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS	QoS_1
MAX. Concurrent Sessions	0 (0: means unlimited)
Quota Per Session	0 KBytes
Quota Per Day	0 MBytes

Figure 186 VPN Trunk Outgoing Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1

Figure 187 VPN Trunk Outgoing Policy Setting Completed

Step 4. Go to **Policy > Incoming**. Click on the **New Entry** button and enter the following settings: *(Figure 188)*

- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Trunk:** Select **PPTP_VPN_Trunk**.
- Click **OK**. *(Figure 189)*

Comment: (Max. 64 characters)

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	Schedule_1
VPN Trunk	PPTP_VPN_Trunk
Action, WAN Port	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	QoS_1
MAX. Concurrent Sessions	0 (Range: 1 - 99999; 0: means unlimited)
Quota Per Session	0 KBytes (Range: 0 - 999999)
Quota Per Day	0 MBytes (Range: 0 - 999999)
NAT	<input type="checkbox"/> Enable

OK Cancel

Figure 188VPN Trunk Incoming Policy Settings

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

New Entry

Figure 189VPN Trunk Incoming Policy Setting Completed

Step 5. The completed PPTP VPN connection setup (Figure 190)

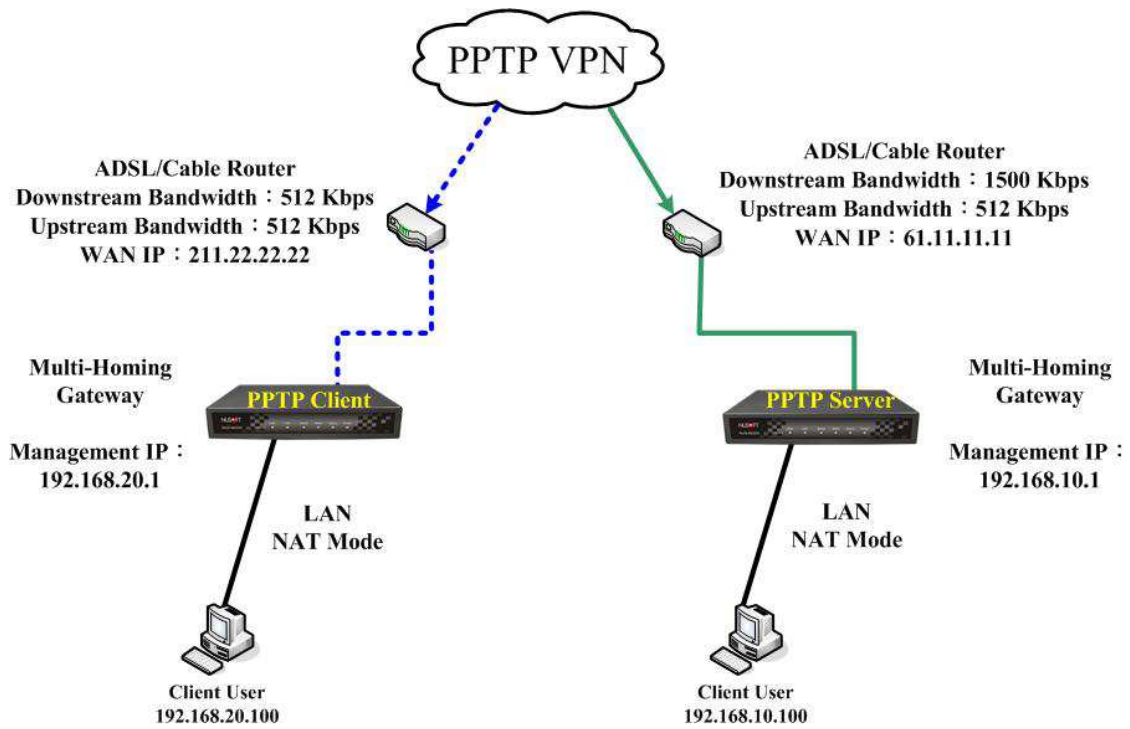


Figure 190 PPTP VPN Connection Deployment

Setting up a PPTP VPN Connection Using a Single NUS-MH2400G and a Windows 2000 PC

Scenario:

Company A:

- Using a NUS-MH2400G
- 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-MH2400G 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-MH2400G. Proceed with the following steps:

Step 1. Using Company A's NUS-MH2400G, 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 191)

Modify Server Design	
<input type="radio"/>	Disable PPTP
<input checked="" type="radio"/>	Enable PPTP
<input checked="" type="checkbox"/>	Encryption
Client IP Range :	192.44.75.1 -- 254
<input checked="" type="checkbox"/>	Allow remote client to connect to Internet.
<input checked="" type="checkbox"/>	WAN1
<input checked="" type="checkbox"/>	WAN2
<input checked="" type="checkbox"/>	WAN3
<input checked="" type="checkbox"/>	WAN4
Auto-Disconnect if idle	0 minutes (Range: 0 - 999999, 0: means always connected)
Echo-Request Retry	3 times Timeout 15 Second (Retry Range: 0 - 9, 0: means disable; Timeout Range: 1 - 30)
<input type="checkbox"/>	Enable RADIUS Server Authentication
(IP or Domain Name)	
RADIUS Server Port	1812 (Range: 1 - 65535)
Shared Secret	(Max. 40 characters)
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 191 Enable PPTP VPN Server Settings



RADIUS Server Authentication can be done under Authentication > RADIUS. In this case, the IT administrator should add a [username] as [*] and a [password] as [@radius] for the client user to authenticate and connect to the PPTP VPN server.



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-MH2400G, go to **Policy Object > VPN > PPTP Server**. Click on the **New Entry** button and configure the following: (Figure 192)

- **User Name:** Enter PPTP_Connection.
- **Password:** Enter 123456789.
- From the **Client IP assigned by** category select **IP Range**.
- Click **OK**. (Figure 193)

Add New PPTP Server	
User Name :	<input type="text" value="PPTP_Connection"/> (Max. 16 characters)
Password :	<input type="password" value="*****"/> (Max. 19 characters)
Client IP assigned by	
<input checked="" type="radio"/>	IP Range
<input type="radio"/>	Fixed IP : <input type="text"/>
<input type="checkbox"/>	Manual Disconnection

Figure 192 PPTP VPN Server Settings

PPTP Server (Enable, Encryption:ON) :

Client IP Range : 192.44.75.1-254

	User Name	Client IP	Uptime	Configure
--	PPTP_Connection	0.0.0.0	---	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 193 PPTP VPN Server Settings Completed

Step 3. Go to **Policy Object > VPN > Trunk**. Click on the **New Entry** button and enter the following settings: (Figure 194)

- **Name:** Enter a unique name for the Trunk.
- **From Source :** Select LAN.
- **From Source Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **To Destination :** Select **Remote Client**.
- Add **PPTP_Server_PPTP_Connection** in the **Tunnel** field.
- Check **Show remote Network Neighborhood**.
- Click **OK**. (Figure 195)

Figure 194 New Entry Trunk Setting

	Name	Source Subnet	Destination Subnet	Tunnel	Configure
	PPTP_VPN_Tru...	192.168.10.0	Remote Client	PPTP_Ser...	Modify Remove Pause

New Entry

Figure 195 VPN Trunk Settings Completed

Step 4. Go to **Policy > Outgoing** and click on the **New Entry** button and enter the following settings: (Figure 196)

- **Authentication User:** Select **All_NET**.
- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Trunk:** Select **PPTP_VPN_Trunk**.
- Click **OK**. (Figure 197)

Comment :

Add New Policy

Source Address :	Inside_Any ▾
Destination Address :	Outside_Any ▾
Service :	ANY ▾
Schedule :	Schedule_1 ▾
Authentication User :	All_NET ▾
Trunk :	PPTP_VPN_Trunk ▾
Action, WAN Port :	<input checked="" type="checkbox"/> PERMIT ALL <input type="checkbox"/> DENY ALL <input type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4
Traffic Log :	<input type="checkbox"/> Enable
Statistics :	<input type="checkbox"/> Enable
Content Blocking :	<input type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> P2P <input type="checkbox"/> IM <input type="checkbox"/> Download <input type="checkbox"/> Upload
QoS :	QoS_1 ▾
MAX. Concurrent Sessions :	<input type="text" value="0"/> (0: means unlimited)
Quota Per Session :	<input type="text" value="0"/> KBytes
Quota Per Day :	<input type="text" value="0"/> MBytes

Figure 196 VPN Trunk Outgoing Policy Settings

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN	  	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To <input type="text" value="1"/> ▾

Figure 197 VPN Trunk Outgoing Policy Settings Completed

Step 5. Go to **Policy > Incoming**. Click on the **New Entry** button and enter the following settings: (Figure 198)

- **Schedule:** Select **Schedule_1**.
- **QoS:** Select **QoS_1**.
- **Trunk:** Select **PPTP_VPN_Trunk**.
- Click **OK**. (Figure 199)

Comment : (Max. 64 characters)

Add New Policy	
Source Address:	Outside_Any
Destination Address:	Inside_Any
Service:	ANY
Schedule:	Schedule_1
VPN Trunk:	PPTP_VPN_Trunk
Action, WAN Port:	<input checked="" type="checkbox"/> PERMIT <input type="checkbox"/> DENY
Traffic Log:	<input type="checkbox"/> Enable
Statistics:	<input type="checkbox"/> Enable
QoS:	QoS_1
MAX. Concurrent Sessions:	0 (Range: 1 - 99999, 0: means unlimited)
Quota Per Session:	0 KBytes (Range: 0 - 999999)
Quota Per Day:	0 MBytes (Range: 0 - 999999)
NAT:	<input type="checkbox"/> Enable

OK Cancel

Figure 198 VPN Trunk Incoming Policy Settings

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

New Entry

Figure 199 VPN Trunk Incoming Policy Settings Completed

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 200*)

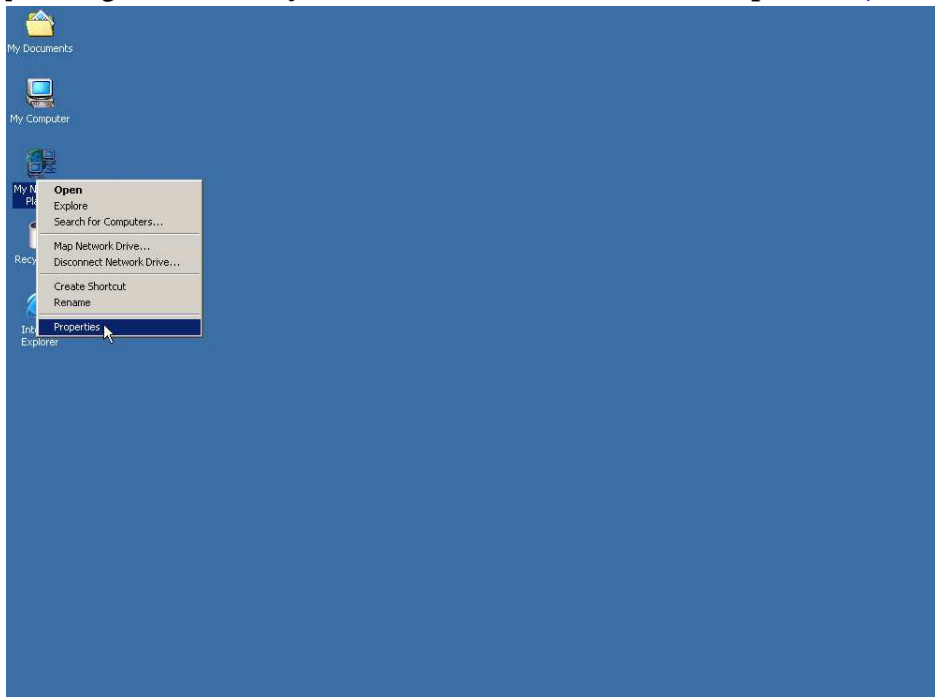


Figure 200 Starting the Windows 2000 PPTP VPN Settings

Step 2. In the Network and Dial-up Connections window, double click on Make New Connection. (Figure 201)

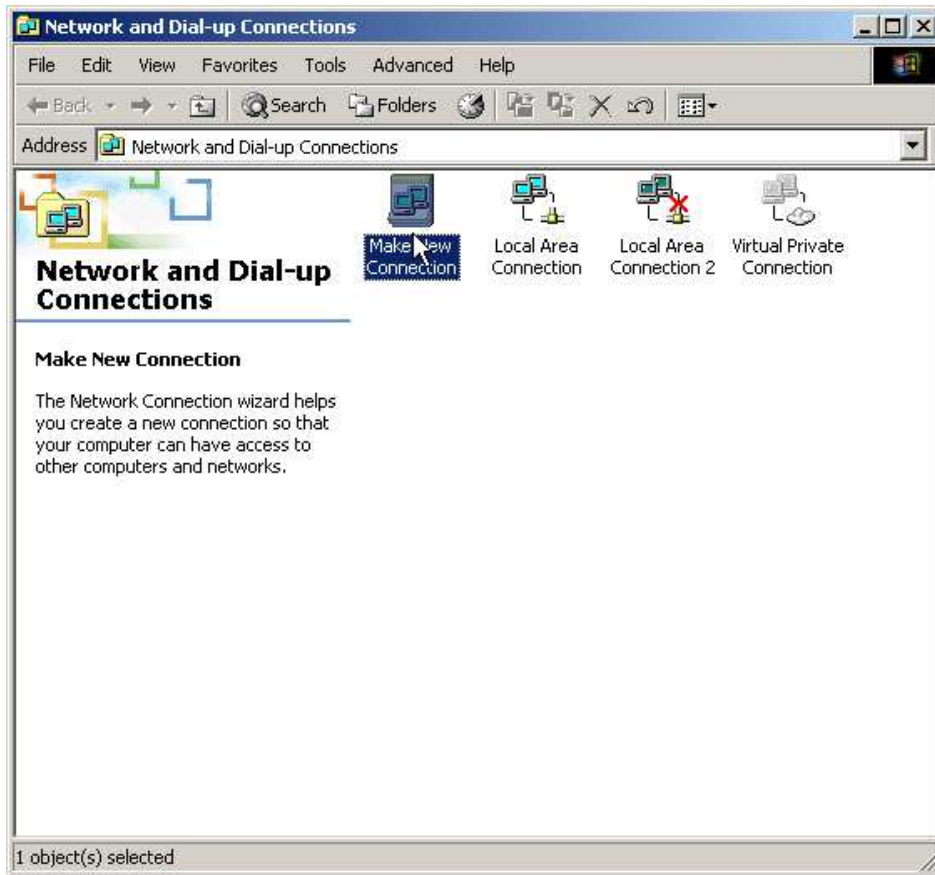


Figure 201 Network and Dial-up Connections

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 202)



Figure 202 The Local Information Settings

Step 4. In the **Phone And Modem Options** window, click **OK**. (*Figure 203*)

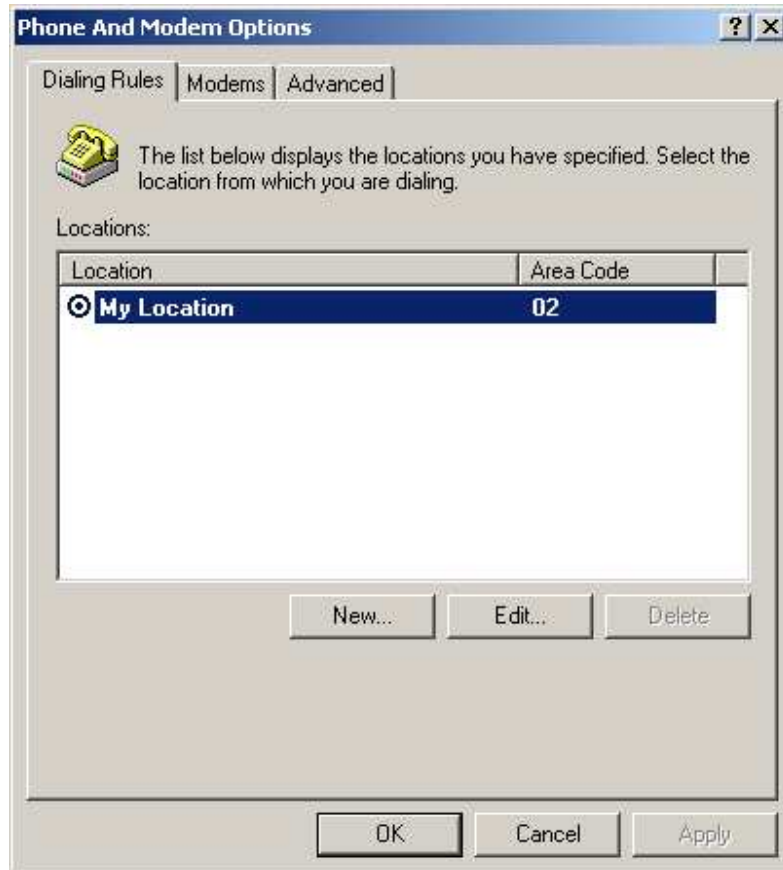


Figure 203 Phone And Modem Options

Step 5. In the **Network Connection Wizard** window, click **Next**. (*Figure 204*)



Figure 204 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 205)

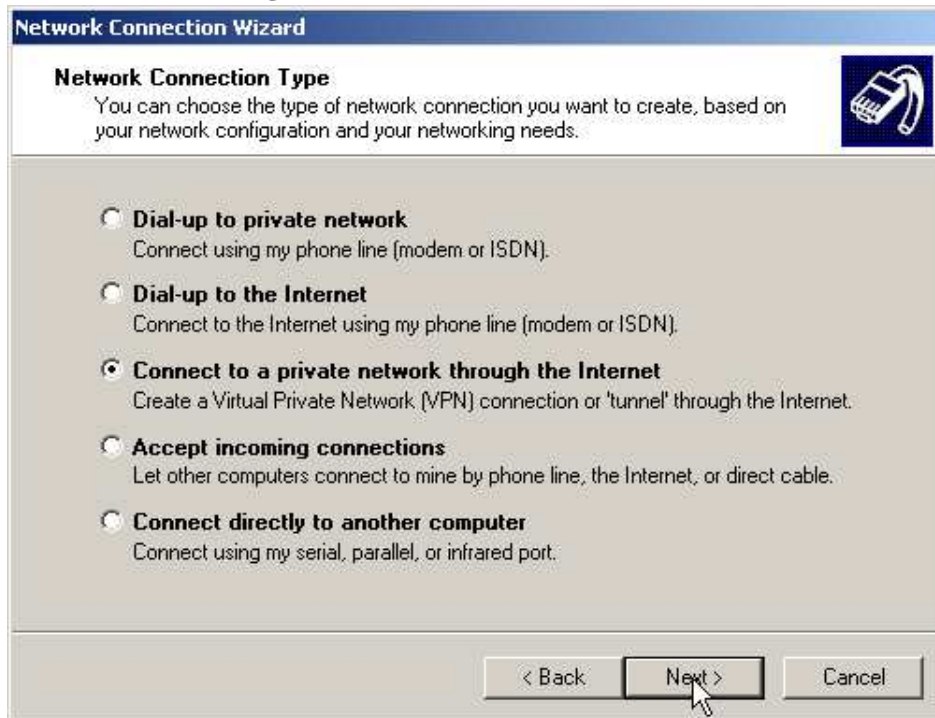
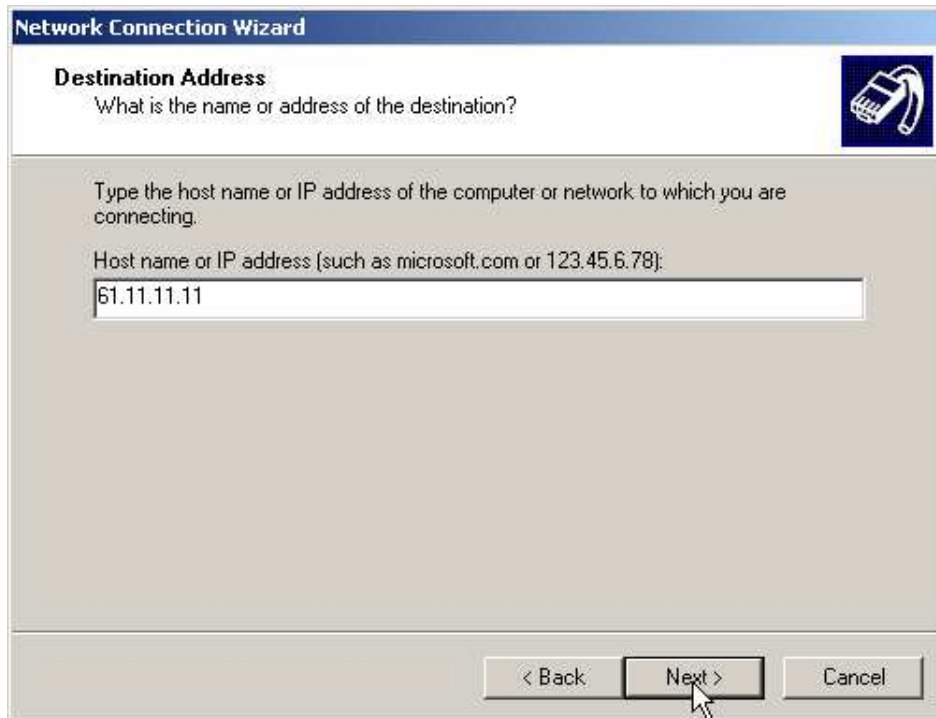


Figure 205 To Connect to a Private Network through the Internet

Step 7. In the **VPN Server Selection** window, enter the VPN IP address and click **Next**. (*Figure 206*)



The screenshot shows a window titled "Network Connection Wizard" with a sub-header "Destination Address". Below the sub-header is the question "What is the name or address of the destination?". A small icon of a mobile phone is visible in the top right corner. The main area contains the instruction "Type the host name or IP address of the computer or network to which you are connecting." followed by a text box labeled "Host name or IP address (such as microsoft.com or 123.45.6.78):" containing the IP address "61.11.11.11". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". A mouse cursor is pointing at the "Next >" button.

Figure 206 Setup the Host Name or IP Address

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

(Figure 207)



Figure 207 Setup the Connection Availability

Step 9. In the **Completing the New Connection Wizard** window, enter a **Connection Name** and then click **Finish**. (*Figure 208*)



Figure 208 New Connection Wizard Settings Complete

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

(*Figure 209*)

- **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 210*)
- Finally, the **Connection Complete** window will be displayed. (*Figure 211*)



Figure 209 Connect Virtual Private Connection Window



Figure 210 Establishing the PPTP VPN Session



Figure 211 PPTP VPN Connections Complete

Step 11. Complete PPTP VPN setup. (*Figure 212*)

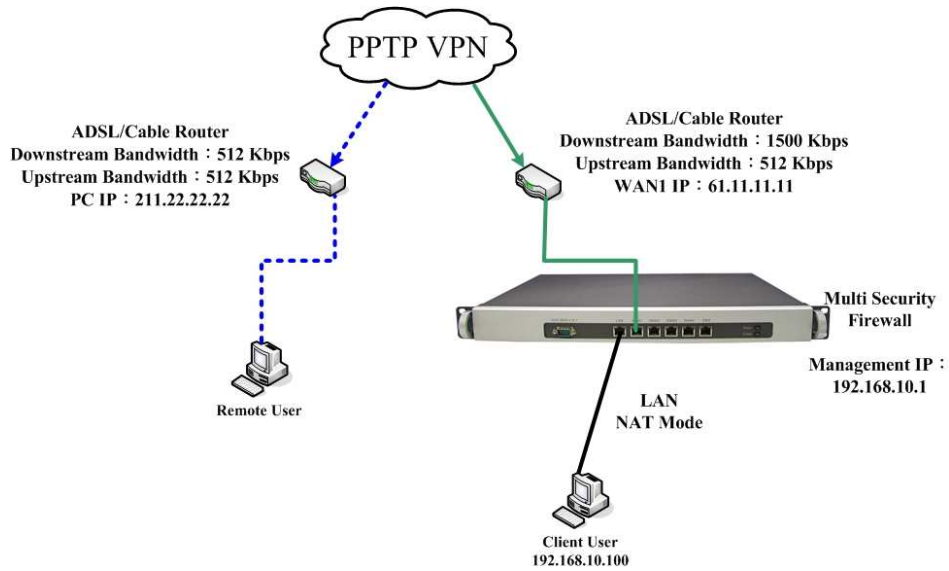


Figure 212 The Completed PPTP VPN Deployment