

# WMU/MU9000VPN

# VPN Setup Guide

OvisLin

# **Table of Contents**

## VPN EXAMPLES

EXAMPLE 1: USING IPSEC TO CONNECT 2 LAN TOGETHER	3
USA Router Setup	4
Germany Router Setup	6
EXAMPLE 2: USING PPTP TO CONNECT REMOTE PC TO LOCAL LAN	8
Router Setup	8
Remote PC Setup (Using WinXP VPN Client)	10
EXAMPLE 3: IPSEC CONFIGURATION EXAMPLE	17
Router's IPsec Setup	18
PC's IPsec Setup (WinXP)	21

## **VPN Examples**

In this Guide, we will provided setup guide for 3 VPN applications example:

- Using IPsec protocol to connect 2 remote LAN together using 2 WMU/MU9000VPN Routers.
- 2. Using PPTP protocol to connect 1 remote PC with WMU/MU-9000VPN
- 3. Using IPsec protocol to connect a remote mobile PC with WMU/MU-9000VPN

To setup a VPN connection, it involves set up in both the router and the PC side. As you will notice, the setup for the VPN server on the router is very simple. But the setup on the client side depends on what type of VPN client software you use on the PC. Once you take time to go through the step-by-step example, it will become clear and easier to setup.

OvisLin	k video FTP Printer QoS VPN	
Quick Setup   Interface Content Filtering Advanced Mail Monitoring Mail Monitoring Restart Router Save Changes Logout	VPN Setting         Add VPN Tunnel         Show VPN Tunnel Summary         Show Pre-Shared Key Summary         Show IPSEC SPI Information	IPsec Server Functions
	PPTP Server Setting PPTP Server Function	

## Example 1: Using IPsec to connect 2 LAN together



In this example, we will connect the USA office and German office together using IPsec VPN server (WMU-9000VPN on both side). The goal is to let both office's network together and operate as if they are on the same LAN. Please note that for security purpose, IPsec require that the IP subnet on both side of the VPN tunnel must be different. Therefore, in this example, the USA office's local IP subnet is 192.168.2.x. The German office's local IP subnet is 192.168.1.x.

After firmware version .40, the router can support VPN over dynamic DNS. If the remote VPN server is using Dynamic DNS, please select "FQDN" for the Remote Secure gateway, then enter the remote server's DDNS domain name.

Please check the above diagram to get a clear idea of how the connect and IP addresses.

USA Router	Setup
OvisLin	k Video FTP Printer QoS VPN 1
Quick Setup  I Interface Content Filtering Advanced Mail Monitoring Maintenance Restart Router Save Changes	Add VPN Tunnel 2 Show VPN Tunnel Summary
Logov	Show Pre-Shared Key Summary Show IPSEC SPI Information
	PPTP Server Setting

- 1. Click on the VPN button on the top menu

2. Click on "Add VPN Tunnel"

OvisLin		→ FTP → Printer → Qc	
Quick Setup	VPN Setting		
Interface     Content Filtering     Advanced	*Tunnel Name Tunnel Status	Germany	3
<ul> <li>Mail Monitoring</li> <li>Maintenance</li> <li>Restart Router</li> </ul>	Local Secure Group IP Address/Mask	[192.168.2.0/24 <a.b.c.d m=""></a.b.c.d>	4
Save Changes	Remote Secure Group IP Address/Mask Remote Secure Gateway (	192.168.1.0/24 < <u>A.B.C.D/M&gt;</u>	5
	* ⊙ IP Address ^ ○ FQDN	10.0.0.2	6
	Encryption Authentication Encapsulation	3DES MD5 v Tunnel v	
	Key Management Key Exchange Method PFS	Auto(IKE) Enable V	7
	Key Lifetime	3600 <1200-28800>	
		8 Add Reset	

- 3. On the VPN setting page above. For the Tunnel name, please enter "Germany" for this case.
- 4. For the local secure Group. Enter the local IP subnet and the mask in this field. For USA office, the LAN IP subnet is 192.168.2.0, enter "24" for mask if you want the entire LAN to have access to the tunnel.
- 5. For the remote secure Group. Enter the remote LAN IP subnet and the mask in this field. For the remote Germany office, the LAN IP subnet is 192.168.1.0, enter "24" for mask if you want the entire remote LAN to have access to the tunnel.
- Enter the IP address of the Germany's WAN IP address. In this case, it is "10.0.0.2". If the remote VPN server is using Dynamic, please select "FQDN" and enter the remote server's DDNS address.
- 7. Please enter a Pre-Shared Key which is the key that the VPN tunnel use for data encryption. The key must set to the same on both side. In this case, we use "ovislink"
- 8. Press the Add button
- 9. Press "save changes" on the left menu bar.

## Germany Router Setup

OvisLin	k Video FTP Printer QoS VPN 1
Quick Setup	VPN Setting Add VPN Tunnel 2
Maintenance     Restart Router     Save Changes     Logout	Show VPN Tunnel Summary Show Pre-Shared Key Summary
	Show IPSEC SPI Information
	PPIP Server Setting

- 1. Click on the VPN button on the top menu
- 2. Click on "Add VPN Tunnel"

OvisLin	k video (	⇒ FTP (⇒ Printer ) (⇒ QoS	VPN
Quick Setup	VPN Setting		
Interface     Content Filtering     Advanced	*Tunnel Name Tunnel Status	USA Enable	3
Mail Monitoring     Maintenance     Restart Router	Local Secure Group IP Address/Mask Remote Secure Group	192.168.1.0/24 < <u>A.B.C.D/M</u> >	4
Logout	IP Address/Mask Remote Secure Gateway (I	192.168.2.0/24 < <u>A.B.C.D/M&gt;</u> Road Warriors Please Specify 0.0.0.0)	5
	* • IP Address * • • FQDN	10.0.0.1	6
	Encryption Authentication Encapsulation	3DES MD5 V Tunnel V	
	Key Management Key Exchange Method PFS	Auto(IKE) Enable v	
	Key Lifetime	3600 <1200-28800>	
		8 Add Reset	

- 3. On the VPN setting page above. For the Tunnel name, please enter "USA" for this case.
- 4. For the local secure Group. Enter the local IP subnet and the mask in this field. For the Germany office, the LAN IP subnet is 192.168.1.0, enter "24" for mask if you want the entire LAN to have access to the tunnel.
- For the remote secure Group. Enter the remote LAN IP subnet and the mask in this field. For the remote USA office, the LAN IP subnet is 192.168.2.0, enter "24" for mask if you want the entire remote LAN to have access to the tunnel.
- Enter the IP address of the USA's WAN IP address. In this case, it is "10.0.0.1". If the remote VPN server is using Dynamic, please select "FQDN" and enter the remote server's DDNS address.
- 7. Please enter a Pre-Shared Key which is the key that the VPN tunnel use for data encryption. The key must set to the same on both side. In this case, we use "ovislink"
- 8. Press the Add button
- 9. Press "save changes" on the left menu bar.

After the settings is done on both side, the routers should built tunnels to connect the 2 sides together.

# Example 2: Using PPTP to connect remote PC to Local LAN



In this example, we will demonstrate how to setup a VPN connection between a remote PC and the WMU-9000VPN using the PPTP server function. Looking at the diagram above, the Remote PC has real IP address of 10.0.0.1. If this remote PC is connected to Internet through an IP sharing router, please make sure that router supports PPTP pass through function. In this example, the WMU-9000VPN's WAN IP address is 10.0.0.3. You can also register the WMU-9000VPN with dynamic DNS if you don't have fixed IP address. Finally, the local LAN has IP address 192.168.1.x. Please note that if the Remote PC is under a router, the remote PC's IP subnet must be different from the local IP subnet.

The Router's PPTP server can support 10 PPTP VPN user's account.

-	
OvisLi	k Video FTP Printer Qos VPN 1
Quick Setup	VPN Setting
Interface     Content Filtering     Advanced     Mail Monitoring	Add VPN Tunnel
<ul> <li>Maintenance</li> <li>Restart Router</li> <li>Save Changes</li> <li>Logout</li> </ul>	Show VPN Tunnel Summary Show Pre-Shared Key Summary
	Show IPSEC SPI Information
	PPTP Server Setting 2

## Router Setup

3. Click on the VPN button on the top menu

## 4. Click on "PPTP Server Settings"

PTP Server			
PTP Server Status Local IP Address Remote IP Address	Enable  192.168.33.101-100 192.168.1.101-100 6 Set	Reset	<a.b.c.d[-e]> <a.b.c.d[-e]></a.b.c.d[-e]></a.b.c.d[-e]>
	Account Ma	nagemer	at
Ŭ	lser Name		Password
	Set	Reset	

- 3. Enable the PPTP Server Status
- The local IP address field is the internal IP address range used by VPN server to keep track of the IP translation. It must be on a different subnet from the local LAN. In this case, we put "192.168.33.101-110" for all 10 possible account.
- The Remote IP address field is where you put the local IP address assignment to the remote PC when they login. They must be in the same subnet as the local LAN. In this case, since the local LAN's IP subnet is 192.168.1.x. We will put "192.168.1.101-110" for the IP address assignment to the 10 accounts (from .101 to .110).
- 6. Place the "Set" button to turn on the PPTP server

TP Server		
TP Server Status cal IP Address mote IP Address	Enable   192.168.33.101-100  192.168.1.101-100  Set	<a.b.c.d[-e]> <a.b.c.d[-e]> Reset</a.b.c.d[-e]></a.b.c.d[-e]>
	Account Ma	inagement
vpnone		
	8 Set	Reset

- 7. Now Enter the User's Name and Password in the account management. In this example, please put "vpnone" for the user's name.
- 8. Press "Set" button to create VPN account.
- 9. Press "Save Changes" on the left hand menu bar.

## Remote PC Setup (Using WinXP VPN Client)

In case of WINXP, the following steps shows PPTP client setting.



- 1. Go to **Network Connection** on Control Panel
- 2. Click on **Create a new connection.**



3. Click on **Next** button



- 4. Click on **Connect** to the network at my workplace.
- 5. Click on **Next** button

6. Click on Virtual Private Network

connection

7. Click on Next

button

New Connection Wizard	8.	Enter the name of this VPN
Connection Name Specify a name for this connection to your workplace.	9	this case, the name is To VPN router. Click on <b>Next</b>
Type a name for this connection in the following box.		Check on Presk
Company N <u>a</u> me		
To VPN router		
For example, you could type the name of your workplace or the name of a server you will connect to.		
Cancel		

Then, enter Matrix's domain IP address. If you're using static IP and already applied for a domain name, or if you are using dynamic IP with DDNS domain name applied and activated built-in DDNS function in this router. Then you can enter the domain name in this section.

New Connection Wizard
VPN Server Selection What is the name or address of the VPN server?
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting. <u>H</u> ost name or IP address (for example, microsoft.com or 157.54.0.1 ):
10.0.0.3
< <u>B</u> ack Next> Cancel

10. Enter the WAN IP address or DDNS domain name of your VPN router. 11. Click on Next

New Connection Wizard		12. If you would like this connection to
	Completing the New Connection Wizard You have successfully completed the steps needed to create the following connection: To VPN router • Share with all users of this computer	appear on your desktop. Please do so by ticking the check box of Add a shortcut to the connection to my desktop. 13. Click on Finish button.
	The connection will be saved in the Network Connections folder. Add a <u>shortcut to this connection to my desktop</u>	
	To create the connection and close this wizard, click Finish.	
	< <u>B</u> ack Finish Cancel	
Connect To VPN ro	14. Click on <b>Properties</b> button	
<u>U</u> ser name:		
Password:		
Save this user name	e and password for the following users: es this computer	
<u>C</u> onnect C	ancel Properties <u>H</u> elp	

🗢 To VPN router Properties 🛛 🔹 💽	15. Un-tick or cancel the check box of
General Options Security Networking Advanced	Require data encryption
	(disconnect if
	none) 16. Click on <b>OK</b>
Validate my identity as follows:	
Require secured password	
Automatically use my Windows logon name and password (and domain if any)	
Require data encryption (disconnect if none)	
Agvanced (custom settings)	
of security protocols.	
I <u>P</u> Sec Settings	
OK Cancel	
	17 Enter your Hoon
Connect To VPN router	name and
	Password
	button.
User name: Vpriorie	
Password:	
<u>ave this user name and password for the following users:</u>	
Me only     Annound a second sec	
Anyone who uses this computer	
Connect Cancel Properties Hale	

15

Once the successful connection is made, your WINXP connection logo will appear on the bottom of your Window to confirm the successful connection.



You can also access to your web-based management page from your router and go to PPTP server setting page. From the bottom of the page, you will see the current PPTP VPN connection status from Client Management section.

On Client Management section, if Disconnect check box is ticked and click on Set, it will allow PPTP disconnection. If the Reset button is clicked, PPTP disconnection will be cancelled and the PPTP will be reconnected again.

Now the remote PC can access the Local LAN. It should be able to ping the PC at 192.168.1.2 directly.

## **Example 3: IPSEC Configuration Example**

IPSec provide tunneling, authentication, and encryption technique so it ensure your data is safely transmitted on Internet without been attack by hackers. In order to create a secure VPN tunnel or channel between two endpoints by IPSEC, please take the following steps.



The above diagram provides simple illustration of how to connect two end points via your router by VPN technique. In this case, a PC with IP address of 192.168.2.254/24 is trying to connect with another PC with its IP address of 192.168.1.x/24 via your VPN router with it's IP address of 192.168.1.254/24.

The above diagram is the basis for the configuration environment of our VPN router.

## Router's IPsec Setup

OvisLin	k Video FTP Printer Qos VPN 1
Quick Setup	VPN Setting Add VPN Tunnel 2
Maintenance     Restart Router     Save Changes     Logout	Show VPN Tunnel Summary Show Pre-Shared Key Summary
	Show IPSEC SPI Information PPTP Server Setting

- 1. Click on **VPN** button on top manual bar of your web page.
- 2. Click on Add VPN Tunnel.

VPN Setting				
*Tunnel Name	ForWinXP		3	
Tunnel Status	Enable 🔻		4	
Local Secure Group				
IP Address/Mask	192.168.1.0/24	<a.b.c.d m=""></a.b.c.d>		
Remote Secure Grou	þ			
IP Address/Mask		<a.b.c.d m=""></a.b.c.d>		
Remote Secure Gates	way (Road Warriors	s Please Specify 0.0	0.0.0)	
* © IP Address * O FQDN	0.0.0.0			
Encryption Authentication	3DES MD5			
Encapsulation	Tunnel 💌			
Key Management				
Key Exchange Metho	d Auto(IKE)			
PFS	Enable 💌			
*Pre-Shared Key	vpntest			
Key Lifetime	3600 <1200-2	28800>		
	Add Res	et		

- Enter the name of the tunnel in the **Tunnel name** field. It allows you to identify multiple tunnels from your tunnel group. It does not have to match the name used at the other end of the tunnel. For this example, please enter "ForWinXP"
- 4. Select Enable from Tunnel Status field to activate the tunnel.
- The Local Secure Group is the computer (s) on your LAN that can access the tunnel. Enter the IP address and subnet mask of your local VPN router in the field. For this example, enter "192.168.1.0/24"
- 6. The **Remote Secure group** is the computer (s) on the remote end of the tunnel that can access the tunnel. Enter the IP address and subnet mask of the computer at the other end of the tunnel in this field. Since in this example, we leave the option open for any PC with correct authentication key. Therefore, we leave the option blank.
- 7. The Remote Security Gateway is the VPN device, such as a second VPN router on the remote end of the VPN tunnel. Enter the IP address of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN router, a VPN server, or a computer with VPN client software that supports IPSec. The IP address may either be static or dynamic, depending on the settings of the remote VPN device. Make sure that you have entered the IP address correctly, or the connection cannot be made. In this example, since the connection is for any remote PC with correct authentication key, we leave it at "0.0.0.0".
- Currently you have only one option to select one type of Encryption as 3DES.
   This is the most secure type of encryption and it is set as the default value.
- 9. From **Authentication**, you have option to select either **MD5** or **SHA1**. It is recommended to select SHA1 as it is more secure than MD5.
- 10. From Key Management section, select Auto (IKE) as default value and select PFS (Perfect Forward Secrecy) and enter a series of numbers or letters in the Pre-Shared Key field. Based on this word, which must be entered at both ends of the tunnel. You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you like the key to be useful. The default value if Key Lifetime is 3600 seconds. In this example, we use "vpntest"
- 11. Click on **add** to confirm your VPN tunnel settings.

After the VPN tunnel has been established, you should see the name of VPN tunnel and status from the first page as following:

VPN Setting			
VPN Tunnel			
Tunnel Name	Status		
ForWinXP	Enable		
Add VPN Tunnel			
Show VPN Tunnel Summary			
Show Pre-Shared Key Summary			
Show IPSEC SPI Information			
PPTP Server Setting			

## Show VPN Tunnel Summary

To view IPSec VPN tunnel setting values, please click on **Show VPN Tunnel Summary** button to access the information.

```
VPN Tunnel Summary
```

```
Interface wan crypto map detail:
Crypto map "ForWinXP" ipsec-isakmp
Match address 192.168.1.0/24
Current peer: 0.0.0.0
Transform-set=(ForWinXP)
Security association lifetime: 28800 seconds
PFS (Y/N): Y
ISAKMP authentication : Pre-share
ISAKMP Security association lifetime: 3600 seconds
Passive mode(Y/N) : N
```

## Show Pre-Shared Key Summary

To view all Pre-shared Key configuration information, please click on Show

Pre-Shared Key Summary button.



Since the VPN has not yet established, therefore if you click on "Show IPSec SPI Information" then it will show no values.

## PC's IPsec Setup (WinXP)

The following section will explain the configuration steps on how to connection VPN tunnels between your PC (WinXP) with your VPN router.

Run       ? >         Image: Second secon	<ul> <li>19. Go to Start button and select Run</li> <li>20. Type mmc in open field</li> <li>21. Click Ok.</li> </ul>
Image: Console 1 - [Console Root]         Image: Action View Favorites Window Help         New       Ctrl+0         Save       Ctrl+3         Save As         Add/Remove Snap*in         Ctrl+M         Options         1 C:\WINDOWS\system32\compage         Exit	22. From File pull-down window, select Add/Remove Snap-in

Add/Remove Snap-in		23.
Standalone Extensions		
Use this page to add or remove a standalone Snap	o-in from the console.	
Snap-ins added to: 🔄 Console Root		
Description		
Add Remove About	]	
L		
		24.
Add Standalone Snap-in	2	24.
Add Standalone Snap-in Available Standalone Snap-ins:	? 🔀	24. 25.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in	Vendor	24. 25.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Group Policy	Vendor Microsoft Corporation	24. 25.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Group Policy Indexing Service	Vendor Microsoft Corporation Microsoft Corporation, I	24. 25.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Group Policy Indexing Service IP Security Monitor	Vendor Microsoft Corporation Microsoft Corporation, I Microsoft Corporation Microsoft Corporation	24.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Group Policy Indexing Service IP Security Monitor Link to Web Address	Vendor Microsoft Corporation Microsoft Corporation, I Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	24. 25.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Group Policy Indexing Service IP Security Monitor IP Security Monitor Link to Web Address Local Users and Groups	Vendor Microsoft Corporation Microsoft Corporation, I Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	24.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Group Policy Indexing Service IP Security Monitor IP Security Policy Management Link to Web Address Local Users and Groups Performance Logs and Alerts	Vendor Microsoft Corporation Microsoft Corporation, I Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	24. 25.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Group Policy Indexing Service IP Security Monitor IP Security Policy Management Link to Web Address Local Users and Groups Performance Logs and Alerts Performance Logs and Alerts Removable Storage Management Besultant Set of Policy	Vendor Microsoft Corporation Microsoft Corporation, I Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	24.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Group Policy Indexing Service IP Security Monitor Link to Web Address Local Users and Groups Performance Logs and Alerts Removable Storage Management Resultant Set of Policy Security Configuration and Analysis	Vendor Microsoft Corporation Microsoft Corporation, I Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	24.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Control Policy Control Policy Indexing Service IP Security Monitor Performance Vice Management Control Users and Groups Performance Logs and Alerts Performance Logs and Alerts Performance Logs and Alerts Removable Storage Management Resultant Set of Policy Security Configuration and Analysis	Vendor Microsoft Corporation Microsoft Corporation, I Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	24.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Group Policy Indexing Service IP Security Monitor IP Security Monitor Link to Web Address Local Users and Groups Performance Logs and Alerts Performance Logs and Alerts Removable Storage Management Resultant Set of Policy Security Configuration and Analysis Description Internet Protocol Security (IPSec) Admin	Vendor Microsoft Corporation Microsoft Corporation, I Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	24.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Control Policy Control Policy Prescurity Policy Management Prescurity Policy Management Control Veb Address Cocal Users and Groups Performance Logs and Alerts Performance Logs and Alerts Perfo	Vendor Microsoft Corporation Microsoft Corporation, I Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	24.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Control Policy Indexing Service IP Security Monitor IP Security Policy Management IP Security Policy Management Ink to Web Address Cocal Users and Groups Incal Users and Groups Performance Logs and Alerts Performance Logs and Alerts Performance Logs and Alerts Resultant Set of Policy Security Configuration and Analysis Description Internet Protocol Security (IPSec) Admir policies for secure communication with o	Vendor Microsoft Corporation Microsoft Corporation, I Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	24.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Group Policy Indexing Service IP Security Monitor IP Security Policy Management Ink to Web Address Link to Web Address Local Users and Groups Performance Logs and Alerts Performance Logs and Alerts Resultant Set of Policy Security Configuration and Analysis Description Internet Protocol Security (IPSec) Admir policies for secure communication with o	Vendor Microsoft Corporation Microsoft Corporation	24.
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Group Policy Indexing Service IP Security Monitor F Security Policy Management Link to Web Address Cocal Users and Groups Ferformance Logs and Alerts Performance Logs and Alerts Removable Storage Management Resultant Set of Policy Security Configuration and Analysis Description Internet Protocol Security (IPSec) Admir policies for secure communication with o	Vendor Microsoft Corporation Microsoft Corporation, I Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	24.

24. Click on IP Security policy management
25. Click on Add button

Click on Add button

Select Computer or Domain			
Select which computer or domain this snap-in will manage When this console is saved the location will also be saved			
<ul> <li>Local computer</li> <li>The computer this console is running on</li> <li>The Active Directory domain of which this computer is a member</li> <li>Another Active Directory domain (Use the DNS name, e.g. "example.microsoft.com"):</li> </ul>			
C Another computer:			
< <u>Back</u> Finish Cancel			

A	dd Standalone Snap-in		2 🗙
	Available Standalone Snap-ins:		
	Snap-in	Vendor	~
	🕵 Group Policy	Microsoft Corporation	
	🞥 Indexing Service	Microsoft Corporation, I	
	lP Security Monitor	Microsoft Corporation	
	IP Security Policy Management	Microsoft Corporation	
	🗕 Link to Web Address	Microsoft Corporation	
	🔝 Local Users and Groups	Microsoft Corporation	=
	👹 Performance Logs and Alerts	Microsoft Corporation	
	Pernovable Storage Management	Microsoft Corporation	
	🕵 Resultant Set of Policy	Microsoft Corporation	
	📴 Security Configuration and Analysis	Microsoft Corporation	~
Description Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.			<
	(	Add Close	

26. Select Local Computer27. Click on Finish button

28. Click on **Close** button

Add/Remove Snap-in 🔹 💽 🗙
Standalone Extensions
Use this page to add or remove a standalone Snap-in from the console.
Snap-ins added to: 🔄 Console Root 💌 🛍
Recurity Policies on Local Computer
Description Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.
Add <u>R</u> emove <u>About</u>
OK Cancel

🚡 Console1 - [Console Root\IP Security	y Policies on Local Computer]	
📸 File Action View Favorites Window	Help	_ 8 ×
← → 🗈 🖬 🛊 🖧 🟦 🏦		
Console Root	Name         Description         Policy Assigned           Client (Respond Only)         Communicate normally (uns         No           Secure Server (Requir         For all IP traffic, always req         No           Server (Request Secu         For all IP traffic, always req         No           Create IP Security Policy         Manage IP filter lists and filter actions         All Tasks           Refresh         Export List         View         Arrange Icons           View         Help         Help         Help	
Create an IP Security policy	1	

30. Click on **IP** Security Policies on Local Computer on the left screen

29. Click on **OK** button

- 31. On the right screen, move you mouse cursor to the blank area and hit a single click on the right hand button of your mouse.
- 32. Select **Create IP Security Policy** from the pull-down window.

IP Security Policy Wizard	
	Welcome to the IP Security policy wizard.
	This wizard helps you create an IP Security policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.
	To continue, click Next.
	< Back Next > Cancel
IP Security Policy Wizard	
IP Security Policy Wizard IP Security Policy Name Name this IP Security pol	cy and provide a brief description
IP Security Policy Wizard IP Security Policy Name Name this IP Security pol	cy and provide a brief description
IP Security Policy Wizard IP Security Policy Name Name this IP Security pol Name: VPN	cy and provide a brief description
IP Security Policy Wizard IP Security Policy Name Name this IP Security pol Name: VPN Description:	cy and provide a brief description
IP Security Policy Wizard IP Security Policy Name Name this IP Security pol Name: VPN Description:	Cy and provide a brief description
IP Security Policy Wizard IP Security Policy Name Name this IP Security pol Name: VPN Description:	cy and provide a brief description

33. Click on Next button

34. From the **Name** field, enter the name of VPN tunnel. (in this case, the name is called VPN)

- IP Security Policy Wizard
   Image: Communication

   Specify how this policy responds to requests for secure communication.
   Image: Communication computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.

   Image: Communication communication other rule applies. To communicate securely, the computer must respond to requests for secure communication.

   Image: Communication communication other rule applies. To communicate securely, the computer must respond to requests for secure communication.

   Image: Communication communication other rule applies. To communicate securely, the computer must respond to requests for secure communication.

   Image: Communication communication communication.

   Image: Communication communication communication communication communication communication.

   Image: Communication communication communication communication communication communication communication.

   Image: Communication communica
- 35. Un-check or cancel the square box next to Activate the default response rule.
- 36. Click on Next button



VPN Properties	NERSEA AND AND AND AND AND AND AND AND AND AN		<b>?</b> ×		
Rules General					
Security rules for communicating with other computers					
IP Security rules:					
IP Filter List	Filter Action	Authentication	Tu		
Oynamic>	Default Response	Kerberos	Nc		
<			>		
<u>Add E</u> d	it <u>R</u> emove	🗆 🗆 Use Add <u>W</u>	izard		
		ОК Са	ancel		

37. Tick on the square box next to Edit properties
38. Click on Finish button

39. Un-tick or cancel
Use Add Wizard
40. Click on Add
button

New Rule Properties	200
Authentication Methods Tu IP Filter List	nnel Setting Connection Type   Filter Action
The selected IP filter lis affected by this rule.	st specifies which network traffic will be
IP Filter <u>L</u> ists:	
Name	Description
O AILICMP Traffic	Matches all ICMP packets betw
O All IP Traffic	Matches all IP packets from this
A <u>d</u> d <u>E</u> dit	<u>R</u> emove
0	K Cancel Apply
🔲 IP Filter List	? 🔀
An IP filter list is composed of mult addresses and protocols can be c <u>N</u> ame: WirXP to VPNrouter	iple filters. In this way, multiple subnets, IP ombined into one IP filter.
Description:	<u>A</u> dd
	Edit.
[	
Mirrored Description Protocol	Source Port Destination
< III	
	OK Cancel

41. Click on **Add** button

42. Enter the **name** of the **IP Filter List**. (In this case, the name is WinXP to VPNrouter)

Filter Properties 🔹 🤶 🔀
Addressing Protocol Description
Source address:
My IP Address
A specific IP Subnet
IP address: 192 . 168 . 1 . 0
Subnet mask: 255 . 255 . 255 . 0
Mirrored. Also match packets with the exact opposite source and destination addresses.
OK Cancel

IP Filter List 🔹 🥐 🔀				
An IP filter list is com addresses and proto	posed of multiple filte cols can be combine	rs. In this way, multiple sul d into one IP filter.	bnets, IP	
<u>N</u> ame:				
WinXP to VPNrouter				
<u>D</u> escription:			<u>A</u> dd	
		<u>_</u>	<u>E</u> dit	
		~	<u>R</u> emove	
Filter <u>s</u> :		Γ	Use Add <u>W</u> izard	
Mirrored Description	Protocol	Source Port	Destination	
Yes	ANY	ANY	ANY	
<			>	
		OK	Cancel	

- 43. From **Source** address pull-down window, select My **IP Address** 44. From **Destination** address pull-down window, select  $\boldsymbol{A}$ specific IP Subnet. Enter destination IP address and its subnet mask. (in this case, the destination IP is 192.168.1.0/255.25 5.255.0) • 45. Check the box of Mirrored. Also match packets
- with the exact opposite source and destination addresses. 46. Click on OK

47. Click on **OK** button

button

New Rule Properties	
Authentication Methods   Tu IP Filter List	nnel Setting Connection Type
The selected IP filter lis affected by this rule.	t specifies which network traffic will be
IP Filter <u>L</u> ists:	
Name	Description
O AILICMP Traffic	Matches all ICMP packets betw
O All IP Traffic	Matches all IP packets from this
WinXP to VPNrouter	
Add <u>E</u> dit	<u>R</u> emove
Clo	se Cancel <u>Apply</u>

- 48. Click on IP Filter name of your previous setting. (in this case, it's WinXP to VPNrouter)
  49. Click on Filter
  - Action tab from the top.

New Rule Properties	? 🔀
Authentication Methods Tur IP Filter List	nnel Setting Connection Type   Filter Action
The selected filter actio for secure network traffi	n specifies whether this rule negotiates c, and how it will secure the traffic.
Filter Actions:	
Name	Description
O Permit	Permit unsecured IP packets to
O Request Security (Optional)	Accepts unsecured communicat
Require Security	Accepts unsecured communicat
	Personal
	se Cancel Apply

Re	quire Se	curity Prop	perties			?	K
S	ecurity Me	ethods Gener	ral				
	<ul> <li>○ Permil</li> <li>○ Block</li> <li>○ Negol</li> </ul>	t tiate security:					
	Security n	nethod preferer	nce order:				
	Туре	AH Integrity	ESP Conf	identiality	ESP Inti	A <u>d</u> d	
	Custom Custom Custom	<none> <none> <none></none></none></none>	3DES 3DES DES		SHA1 MD5 SHA1	<u>E</u> dit	
	Custom	<none></none>	DES		MD5	<u>R</u> emove	
						Move <u>u</u> p	
	<				>	Move d <u>o</u> wn	
	☐ Accep ☐ Allow ✔ Sessio	ot unsecured c unsecured cor on key <u>p</u> erfect	ommunication nmunication forward sec	on, but alw n <u>w</u> ith non-l rrecy (PFS)	ays respon PSec-awa	nd using <u>I</u> PSec are computer	
			0	ж	Cancel		

50. Click on Require Security51. Click on Edit button

- 52. Click on Negotiate security
- 53. Cancel the check box of Accept unsecured communication, but always respond using IPSec
- 54. Tick the box of session key perfect forward secrecy (PFS).
- 55. Click on **OK** button

New Rule Properties		? 🔀
IP Filter List Authentication Methods Authenticatior between com offered and ac computer.	Filte Tunnel Setting methods specify how trust is puters. These authentication ccepted when negotiating se	r Action Connection Type s established methods are curity with another
Authentication <u>m</u> ethod prefe Method Kerberos	erence order: Details	Add Edit Remove Move up Move down
-	Close	

Edit Authentication Method Properties	? 🗙
Authentication Method	
The authentication method specifies how trust is establish Label Computers.	ied
C Active Directory default (Kerberos V5 protocol)	
C Use a certificate from this certification authority (CA):	
Browse	
Use this string (preshared key):	
vpntest	X
OK Car	ncel

56. Click on Edit button

- 57. Click on Use this string (preshared key)
- 58. From the bottom blank area, enter the name of preshared key defined in web-based management from previous setting. 59. Click on **OK** buton

New Rule Properties
IP Filter List Filter Action Authentication Methods Tunnel Setting Connection Type
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.
<ul> <li><u>I</u>his rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this <u>I</u>P address:</li> <li><u>192.168.2.1</u></li> </ul>
Close Carool

- 60. Click on The tunnel endpoint is specified by this IP address
  61. Enter the WAN IP
- address of destination endpoint of VPN tunnel. (in this case, it's 192.168.2.1)
  62. Click on Apply
- button

- **?**× **VPN Properties** Rules General Security rules for communicating with other computers IP Security rules: IP Filter List Filter Action Authentication... Tu WinXP to VPN router Require Security Preshared Key 19 Comparise Default Response Kerberos No < > Edit... Add.. <u>R</u>emove Use Add <u>W</u>izard Г Close Cancel
- 63. Click on pre-defined IP Security rules. (in this case it's WinXP to VPNtunnel)
  64. Click on Add button

New Rule Properties	2
Authentication Methods Tur IP Filter List	nnel Setting Connection Type   Filter Action
The selected IP filter list affected by this rule.	specifies which network traffic will be
IP Filter <u>L</u> ists:	
Name	Description
O All ICMP Traffic O All IP Traffic	Matches all ICMP packets betw Matches all IP packets from this
WinXP to VPNrouter	
Add Edit	Remove
	Tourses
	Cancel Apply

65. Click on Add
button

🗆 IP Filter List 📀 🔀				
t∎ T	An IP filter list is compo- addresses and protocol	sed of multiple filte s can be combine	rs. In this way, multiple sub d into one IP filter.	nets, IP
<u>N</u> ame:				
VPNrou	ter to WinXP			
<u>D</u> escripti	ion:			<u>A</u> dd
			<u> </u>	<u>E</u> dit
			~	Remove
Filter <u>s</u> :			Πι	Jse Add <u>W</u> izard
Mirrore	d Description	Protocol	Source Port	Destination
1				
	III		ОК	Cancel

66. Enter the name of IP filter list in opposite direction. In this case, it's VPNrouter to WinXP.
67. Click on Add button

Filter Properties
Addressing Protocol Description
Source address:
A specific IP Subnet
IP Address: 192 . 168 . 1 . 0
Subnet <u>mask:</u> 255 . 255 . 255 . 0
Destination address:
Any IP Address
Mirrored. Also match packets with the exact opposite source and destination addresses.
OK Cancel

- 68. From **Source** address pull-down window, select **A** specific IP Subnet
- 69. Enter destination IP address and its subnet mask. (in this case, the destination IP is 192.168.1.0/255.25 5. 255.0) ∘
- 70. From **Destination** address pull-down window, select **Any IP Address**.
- 71. Check the box of Mirrored. Also match packets with the exact opposite source and destination addresses.
- 72. Click on **OK** button

IP Filter	List			? 🗙
	an IP filter list is compo addresses and protoco	sed of multiple filte Is can be combine	rs. In this way, multiple sub d into one IP filter.	nets, IP
<u>N</u> ame:				
VPNrouter	to WinXP			
Description	c			<u>A</u> dd
			<u>^</u>	<u>E</u> dit
			× 1	<u>R</u> emove
Filter <u>s</u> :			Γι	Jse Add <u>W</u> izard
Mirrored	Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY
<			<u>ОК</u>	Cancel

73. Click on **OK** button

New Rule Properties	
Authentication Methods Tur IP Filter List	nnel Setting Connection Type   Filter Action
The selected filter actio for secure network traffi	n specifies whether this rule negotiates ic, and how it will secure the traffic.
Eilter Actions:	
Name	Description
O Permit	Permit unsecured IP packets to
O Request Security (Optional)	Accepts unsecured communicat
A <u>d</u> d	Bemove Use Add Wizard
Clo:	se Cancel <u>Apply</u>

Require Sec	urity Pro	perties		? 🔀
Security Meth	ods Gene	ral		
<ul> <li>Permit</li> <li>Block</li> <li>Negotial</li> <li>Security met</li> </ul>	te security: thod prefere	nce order:		
Type A	H Integrity	ESP Confidentiality	ESP Inte	Add
Custom <1 Custom <1	None> None> None>	3DES 3DES DES	SHA1 MD5 SHA1	<u>E</u> dit
Custom <1	None>	DES	MD5	<u>R</u> emove
				Move <u>u</u> p
<			>	Move d <u>o</u> wn
Accept ( Allow un Session	unsecured o isecured co key <u>p</u> erfect	communication, but al mmunication <u>w</u> ith non forward secrecy (PFS	ways respond HPSec-aware	using <u>I</u> PSec computer
		OK	Cancel	Apply

74. Click on Require Security75. Click on Edit button

- 76. Click on Negotiate security
- 77. Cancel the check box of Accept unsecured communication, but always respond using IPSec
- 78. Tick the box of session key perfect forward secrecy (PFS).
  79. Click on OK
- 79. Click on **OK** button

New Rule Properties		? 🔀
IP Filter List Authentication Methods Authentication between comp offered and ac computer.	Tunnel Setting Tunnel Setting methods specify how trust is puters. These authentication scepted when negotiating sec	Action Connection Type established methods are curity with another
Authentication <u>m</u> ethod prefe Method Kerberos	Prence order:	Add Edit Remove Move up Move down
	<b>Close</b> Cance	

Edit Authentication Method Properties	? 🔀
Authentication Method	
The authentication method specifies how trust between the computers.	t is established
C Active Directory default (Kerberos V5 protocol)	
O Use a certificate from this certification authority (CA):	
	<u>B</u> rowse
Use this string (preshared key):	
vpntest	<
OK	Cancel

80. Click on **Edit** button

- 81. Click on **Use this** string (preshared key)
- 82. From the bottom blank area, enter the name of preshared key defined in web-based management from previous setting.
  83. Click on **OK** buton

New Rule Properties			? 🗙
IP Filter List Authentication Methods	   Tunnel Se	Filter Action	ction Type
The tunnel end IP traffic destin list. It takes two	dpoint is the tunr lation, as specifi o rules to describ	neling computer clos ed by the associate be an IPSec tunnel.	est to the d IP filter
<ul> <li><u>I</u>his rule does not specif</li> <li>The tunnel endpoint is specif</li> <li>192.168.2</li> </ul>	y an IPSec tunn pecified by this <u>I</u> I • <b>254</b>	el. P address:	
,			
	Class	L const L	
	Liose	Lancel	<u>Apply</u>

- 84. Click on The tunnel endpoint is specified by this IP address
  85. Entropole WAN ID
- 85. Enter the **WAN IP** address of your WINXP PC (in this case, it's 192.168.2.254)
- 86. Click on **Apply** button

Edit Rule Properties		? 🔀
IP Filter List	1	Filter Action
Authentication Methods	Tunnel Setting	Connection Type
The tunnel endpoir IP traffic destination list. It takes two rule	nt is the tunneling c n, as specified by th as to describe an IF	omputer closest to the le associated IP filter Sec tunnel.
Ihis rule does not specify an	IPSec tunnel.	
The tunnel endpoint is specification	ied by this <u>I</u> P addre	ss:
192.168.2.25	i4	
	ок с	ancel <u>Apply</u>

87. Click on **OK** button

VPN Properties			? 🗙
Rules General			
Security rules	for communicating with ot	her computers	
IP Security rules:			-
	Filter Action	Authentication	
WinXP to VPNrouter	Require Security	Preshared Key	19
VPNrouter to WinXP	Require Security	Preshared Key	19
L <dynamic></dynamic>	Default Response	Kerberos	Nc
<	III )		>
<u>Add E</u> d	t <u>R</u> emove	Use Add <u>w</u>	(izard
nally is in which is shirted		<b>Close</b> Ca	ancel

- 88. Make sure you have checked the box of both IP Security rules you configured in previous section. In this case, they are WinXP to VPNrouter and VPNrouter to WinXP.
- 89. Click on **Close** button

File Action View Favorites Window	v Help					_8
• > 🖻 📧 🗙 🗗 😼 🔮 🎽	i 🖹 🖉					
Console Root	Name 🛆		Descrip	tion	Policy Assigned	e generale non ensemble de
IP Security Policies on Local Computer	🖄 Client (Resp	ond Only)	Commu	nicate normally (uns	No	
	Secure Serv	er (Requir	For all 1	P traffic, always req	No	
	🖄 Server (Rec	uest Secu	For all 1	P traffic, always req	No	
	🗱 VPN				No	
		Assign				
		All Tasks	•			
		Delete				
		Rename				
		Proper	ies			
		Help				

- 90. From IP Security Policy, click on the name of your VPN tunnel setting and click on the right hand button of your mouse.
  91. Click on Assign
- from pull-down window.

Now, you have successfully established the VPN tunnel. In Web-Based management page of your router, go to **VPN** > **Show IPSEC SPI information**. The information page will appear and show all relevant information regards to your VPN connection.