www.ovislink.com.tw

WL/IP-8000VPN

VPN Setup Guide

Version 0.6

Powered by OvisLink Corp.

Document Revision

Version	Date	Note
0.1	11/10/2005	First version with four VPN examples
0.2	11/15/2005	1. Added example 5: dynamic VPN using TheGreenBow VPN client 2. Corrected the illustration using 8000VPN icons 3. Added How To Use This Guide section
0.3	11/15/2005	Updated the cover page
0.4	11/17/2005	Minor correction for PPTP and L2TP LAN numbers
0.5	11/17/2005	Change PPTP and L2TP authentication method to CHAP
0.6	11/18/2005	Improved VPN router setup for Windows XP IPSec

Table of Content

VPN EXAMPLES

In this Guide, we will provide setup guide for 5 VPN application examples:

1. Using IPSec protocol to connect 2 remote LAN together using 2 WL/IP-8000 VPN Routers.
2. Using PPTP protocol to connect 1 remote PC with WL/IP-8000 VPN
3. Setting up IPSec protocol to connect a remote mobile PC with WL/IP-8000 VPN
4. Using L2TP protocol to connect 1 remote PC with WL/IP-8000 VPN
5. Setting up Dynamic VPN where WL/IP-8000 VPN will accept any PC worldwide from anywhere without sacrifice security

To setup a VPN connection, it involves setting up both in the router and the PC sides. 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 more clear and easier to setup.

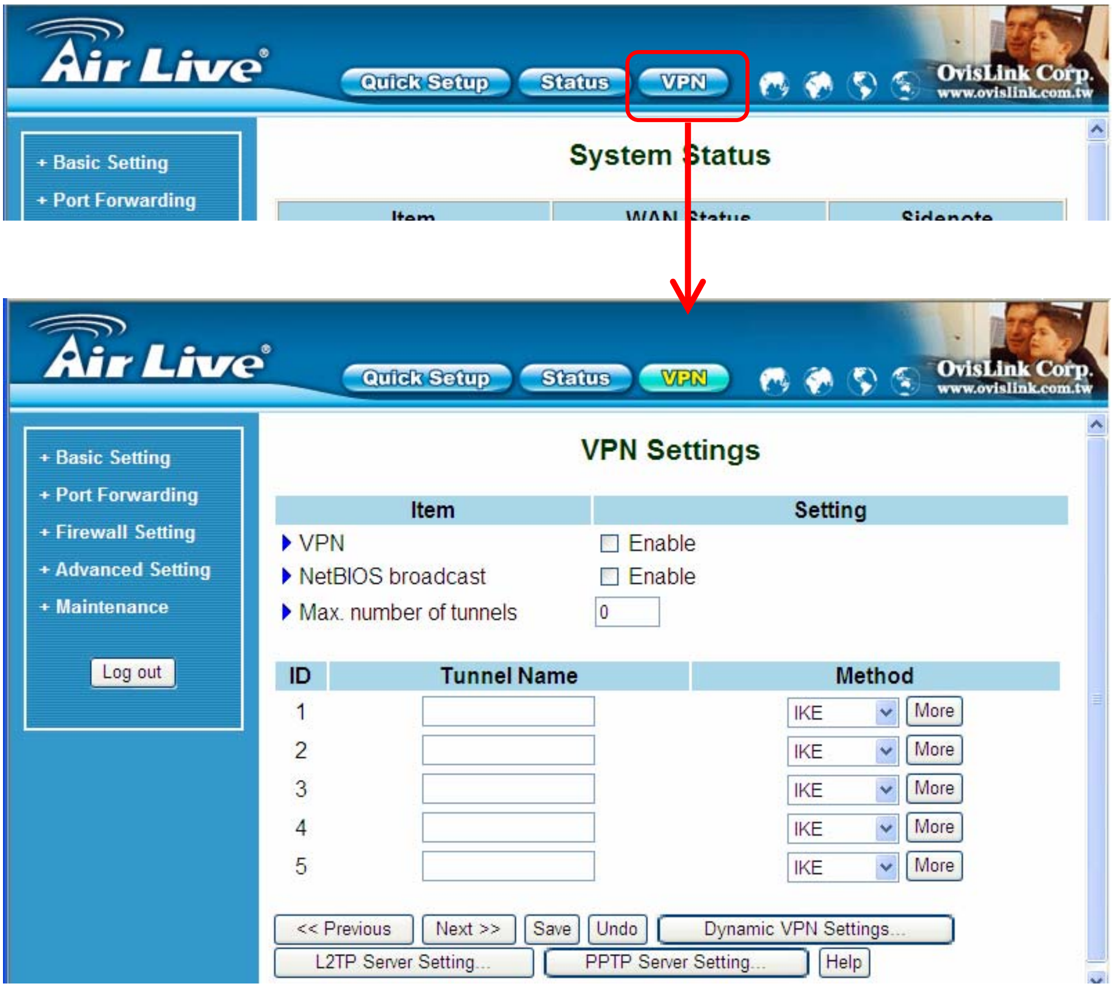
WHAT IS THIS GUIDE

The traditional VPN needs trained personnel with professional knowledge to set up. This WL/IP-8000 VPN example guide provides a step-by-step easy setup for the VPN configuration.

HOW TO USE THIS DOCUMENT

There are many options to set up secure VPN environment. Various combinations may serve for different purposes. Each example provides a way to use WL/IP-8000 VPN configuration. If you need to

- Configure the manual key IPSec VPN, please use example 1
- Configure the automatic key IPSec VPN, please use example 3
- Configure PPTP VPN, please use example 2
- Configure L2TP VPN, please use example 4
- Configure Dynamic VPN, please use example 5
- Connect 2 LAN together with secured VPN, please use example 1
- Configure central site for VPN, please use example 2 to 5
- Configure client site VPN using
  - Windows XP IPSec client, please use example 3
  - Windows XP PPTP VPN, please use example 2
  - Windows XP L2TP VPN, please use example 4
  - TheGreenBow IPSec VPN client, please use example 5

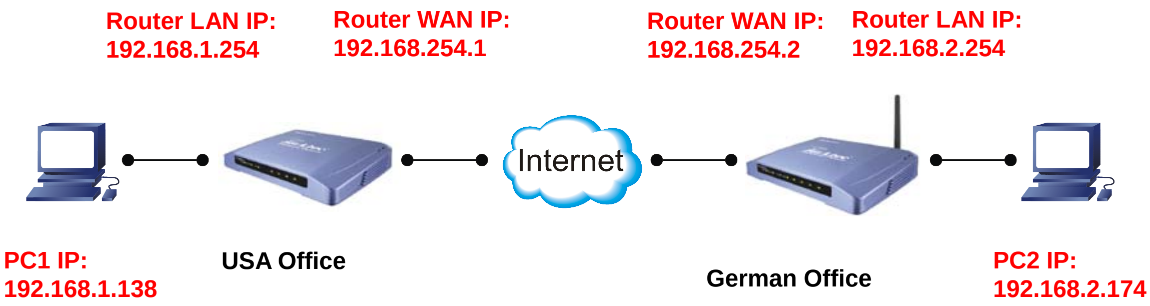


VPN Settings

Item	Setting
VPN	□ Enable
NetBIOS broadcast	□ Enable
Max. number of tunnels	0

ID	Tunnel Name	Method
1		IKE More
2		IKE More
3		IKE More
4		IKE More
5		IKE More

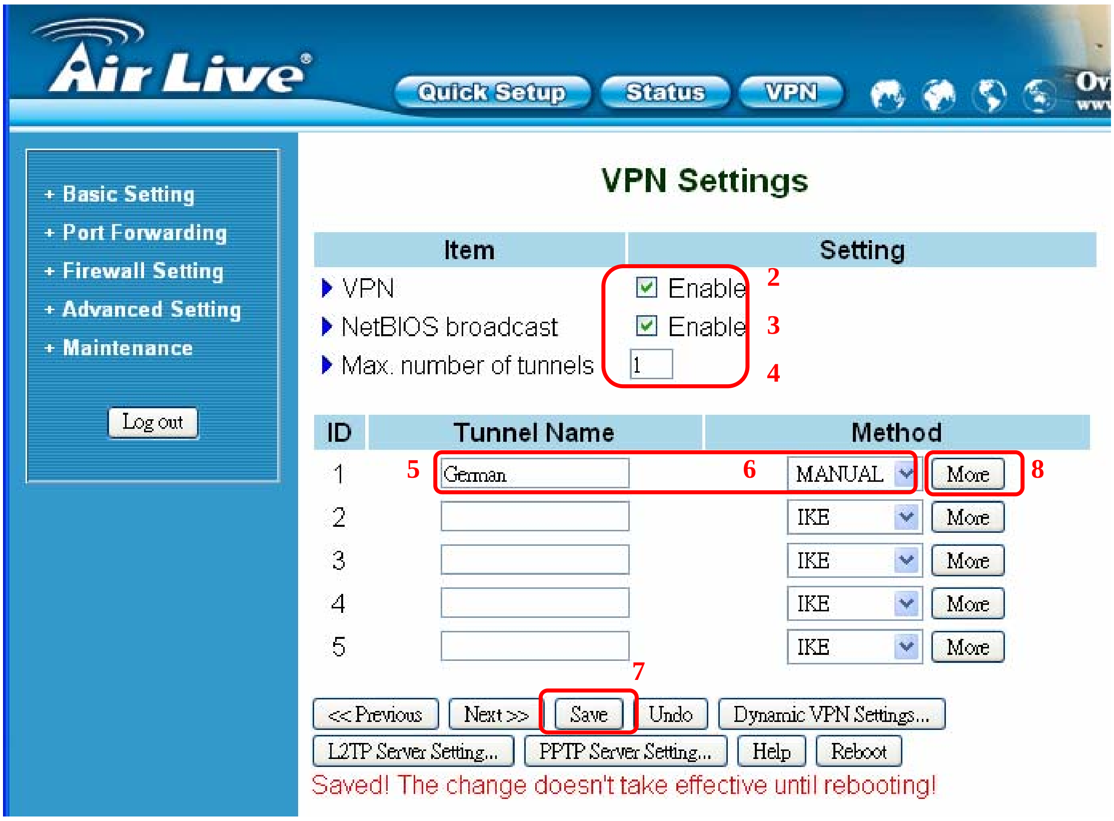
EXAMPLE 1: USING IPSEC TO CONNECT 2 LAN TOGETHER



In this example, we will connect the USA office and German office together using IPSec VPN server (WL/IP-8000VPN on both sides). The goal is to let both offices' network together and operate as if they are on the same LAN. PC1 can link to PC2 freely. 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 192.168.1.x. The German office's local IP subnet is 192.168.2.x.

USA Router Setup

1. After login to WL/IP-8000VPN, click on VPN button on top of the page.



VPN Settings

Item	Setting
VPN	☑ Enable
NetBIOS broadcast	☑ Enable
Max. number of tunnels	1

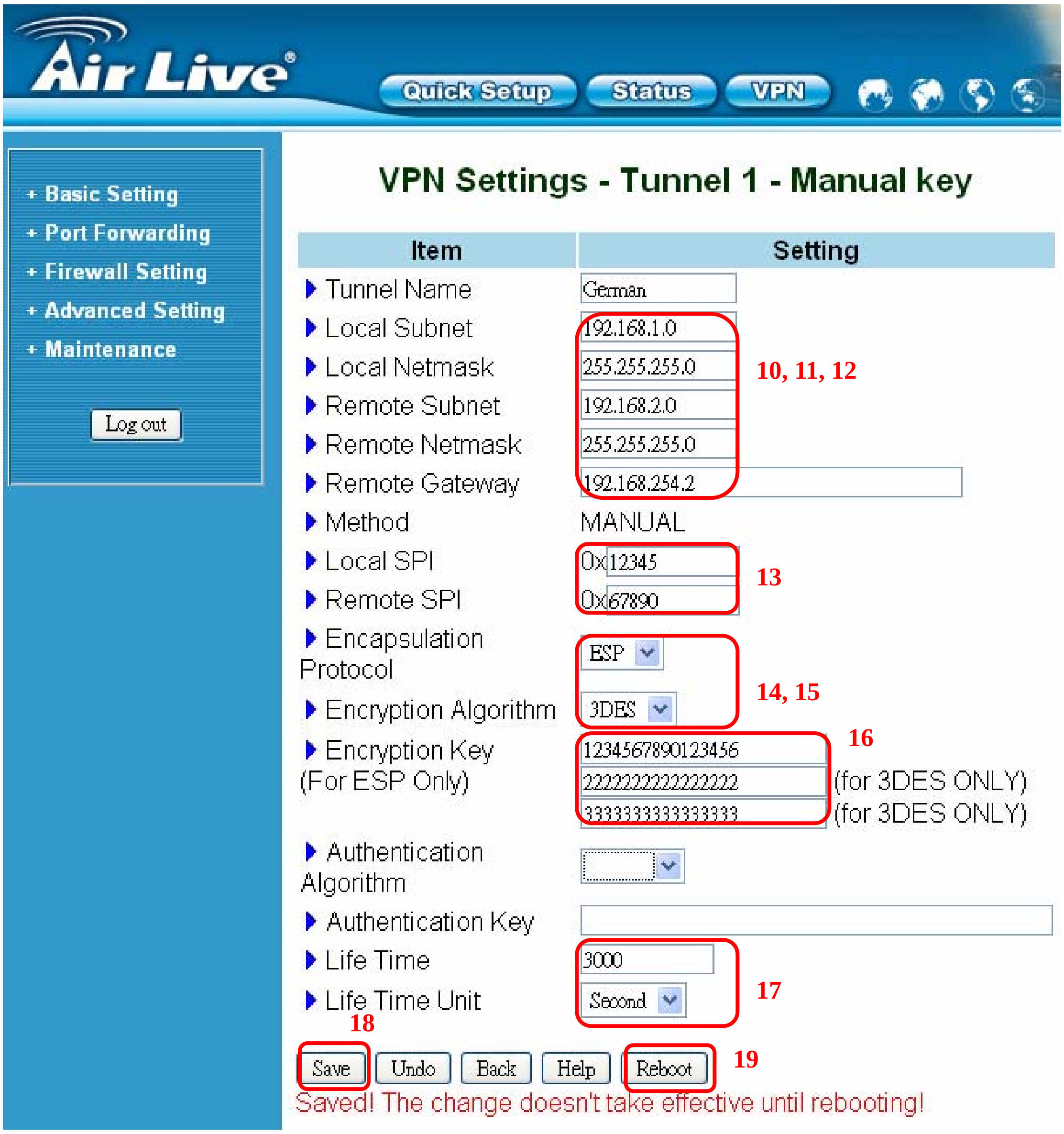
ID	Tunnel Name	Method
1	German	MANUAL
2		IKE
3		IKE
4		IKE
5		IKE

Saved! The change doesn't take effective until rebooting!

2. Check *VPN* **Enable**
3. Check *NetBIOS Broadcast* **Enable**
4. Enter *Max. number of tunnels* as **1**.
5. In tunnel *ID* 1, enter the *Tunnel Name* as **German**.
6. In tunnel *ID* 1, enter the *Method* as **Manual**.
7. Click on **Save** button at the bottom of the page. (no need to reboot now)
8. After step 7, it should jump to the next screen automatically. If not, click on **More** button at the end of tunnel *ID* 1.
9. The Tunnel Name is automatically from the last screen.
10. For the local secure group, to let the entire US office users access this VPN tunnel, enter the local subnet **192.168.1.0** and subnet mask **255.255.255.0**.
11. For the remote secure group, to let the entire German office users access this VPN tunnel, enter the remote subnet **192.168.2.0** and subnet mask **255.255.255.0**.
12. Enter the IP address of the German's WAN port. In this case, it is

192.168.254.2.

13. Enter local and remote SPI. The local SPI we set is **12345** and remote SPI **67890**.
14. *Encryption Protocol* is **ESP**.
15. *Encryption Algorithm* is **3DES**.
16. *Encryption Key*s are "**1234567890123456**", "**2222222222222222**", and "**3333333333333333**" (16 Arabic numerals per key).
17. Set the key Life Time to **3000** and the Life Time Unit to **Second**.
18. Click on **Save** button at the bottom of the page.
19. To make effect all these configuration setups, we are rebooting the router. Click on the **Reboot** button at the bottom of the page. When a dialog pop-up says "*Reboot right now*", click **OK** to reboot the router.



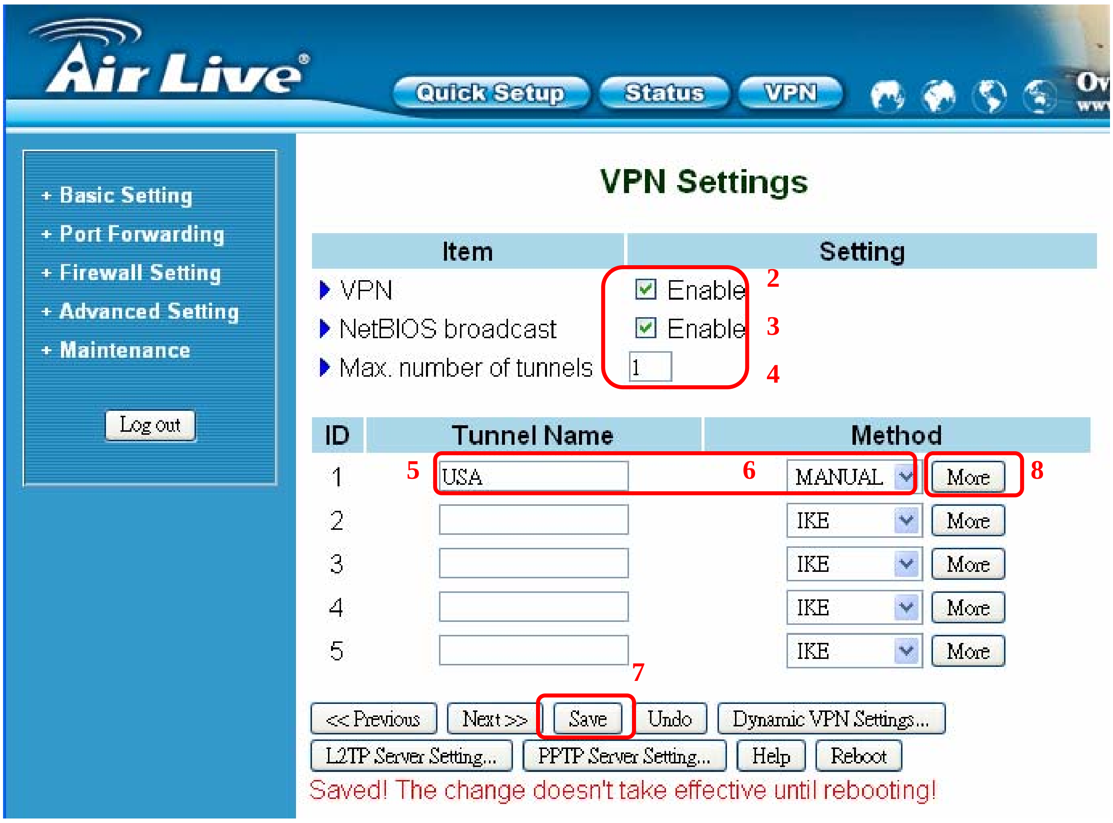
VPN Settings - Tunnel 1 - Manual key

Item	Setting
Tunnel Name	German
Local Subnet	192.168.1.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.2.0
Remote Netmask	255.255.255.0
Remote Gateway	192.168.254.2
Method	MANUAL
Local SPI	0x 12345
Remote SPI	0x 67890
Encapsulation Protocol	ESP
Encryption Algorithm	3DES
Encryption Key (For ESP Only)	1234567890123456 2222222222222222 (for 3DES ONLY) 3333333333333333 (for 3DES ONLY)
Authentication Algorithm	
Authentication Key	
Life Time	3000
Life Time Unit	Second

Saved! The change doesn't take effective until rebooting!

Germany Router Setup

1. After login to WL/IP-8000VPN, click on VPN button on top of the page.



VPN Settings

Item	Setting
VPN	☑ Enable
NetBIOS broadcast	☑ Enable
Max. number of tunnels	1

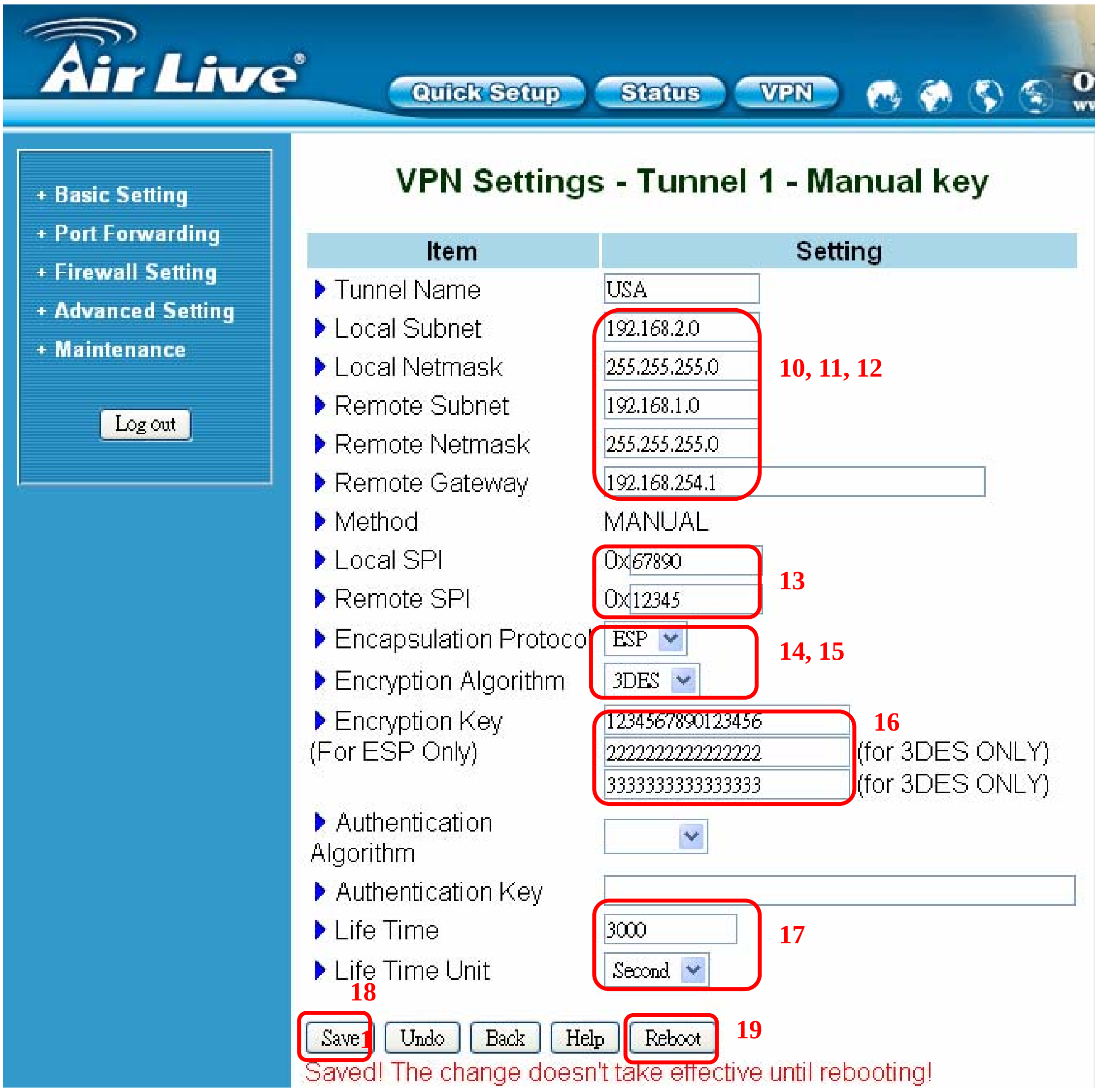
ID	Tunnel Name	Method	
1	USA	MANUAL	More
2		IKE	More
3		IKE	More
4		IKE	More
5		IKE	More

Saved! The change doesn't take effective until rebooting!

2. Check *VPN* **Enable**
3. Check *NetBIOS Broadcast* **Enable**
4. Enter *Max. number of tunnels* as **1**.
5. In tunnel *ID* 1, enter the *Tunnel Name* as **USA**.
6. In tunnel *ID* 1, enter the *Method* as **Manual**.
7. Click on **Save** button at the bottom of the page. (no need to reboot now)
8. After step 7, it should jump to the next screen automatically. If not, click on **More** button at the end of tunnel *ID* 1.
9. The Tunnel Name is automatically from the last screen.
10. For the local secure group, to let the entire US office users access this VPN tunnel, enter the local subnet **192.168.2.0** and subnet mask **255.255.255.0**.
11. For the remote secure group, to let the entire German office users access this VPN tunnel, enter the remote subnet **192.168.1.0** and subnet mask **255.255.255.0**.
12. Enter the IP address of the German's WAN port. In this case, it is

192.168.254.1.

13. Enter local and remote SPI. The local SPI we set is **67890** and remote SPI **12345**.
14. *Encryption Protocol* is **ESP**.
15. *Encryption Algorithm* is **3DES**.
16. *Encryption Key*s are “**1234567890123456**”, “**2222222222222222**”, and “**3333333333333333**” (16 Arabic numerals per key).
17. Set the key Life Time to **3000** and the Life Time Unit to **Second**.
18. Click on **Save** button at the bottom of the page.
19. To make effect all these configuration setups, we are rebooting the router. Click on the **Reboot** button at the bottom of the page. When a dialog pop-up says “*Reboot right now*”, click **OK** to reboot the router.



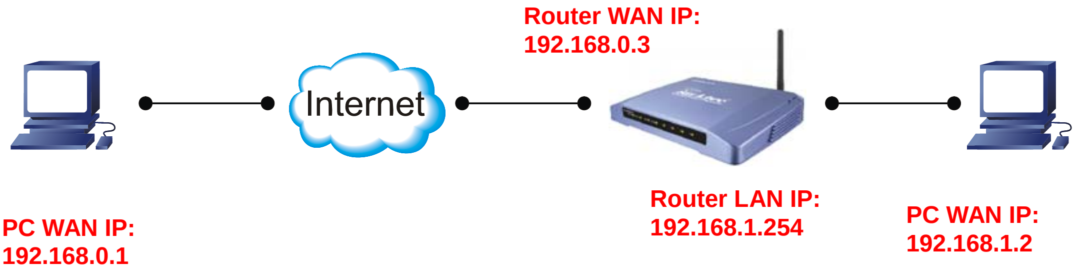
VPN Settings - Tunnel 1 - Manual key

Item	Setting
Tunnel Name	USA
Local Subnet	192.168.2.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.1.0
Remote Netmask	255.255.255.0
Remote Gateway	192.168.254.1
Method	MANUAL
Local SPI	0x 67890
Remote SPI	0x 12345
Encapsulation Protoco	ESP
Encryption Algorithm	3DES
Encryption Key (For ESP Only)	1234567890123456 2222222222222222 (for 3DES ONLY) 3333333333333333 (for 3DES ONLY)
Authentication Algorithm	
Authentication Key	
Life Time	3000
Life Time Unit	Second

Saved! The change doesn't take effective until rebooting!

After the settings are done on both sides, the routers should build a tunnel to connect the 2 sides together.

EXAMPLE 2: USING PPTP TO CONNECT REMOTE PC TO LOCAL LAN



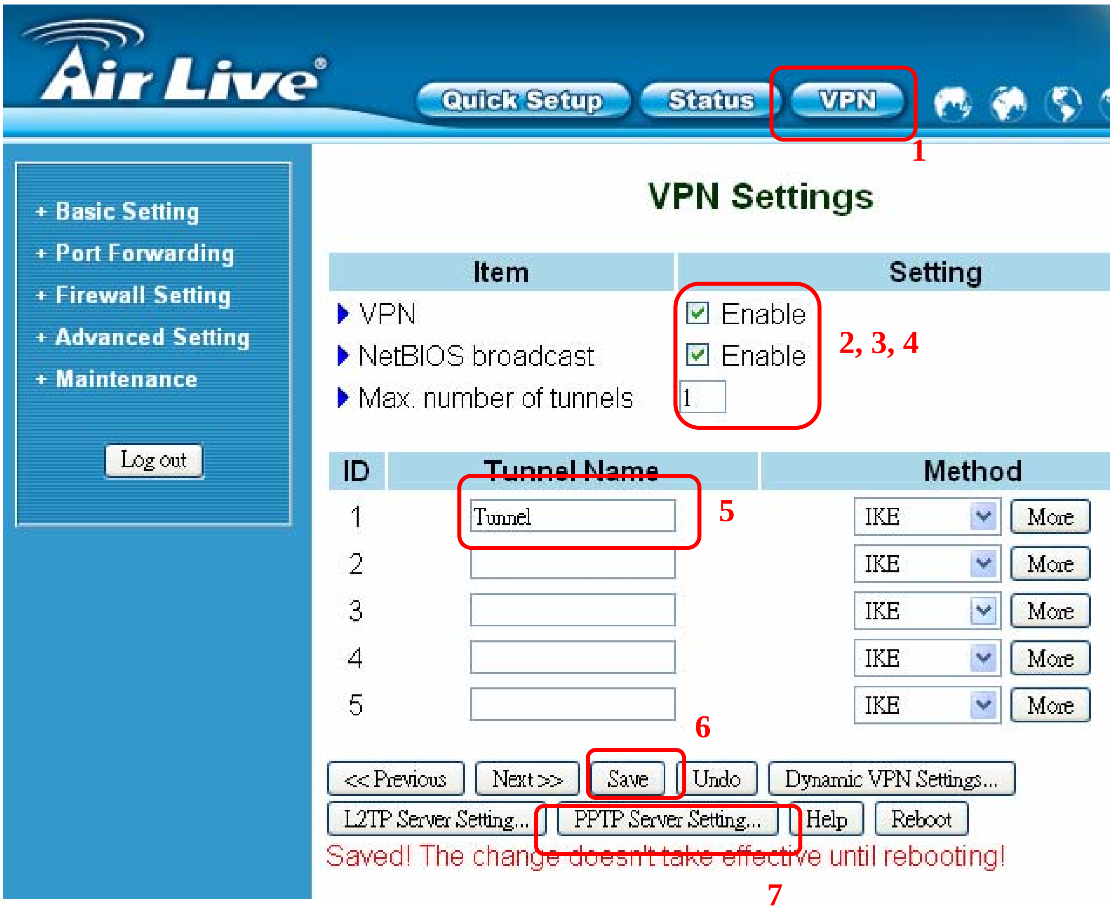
In this example, we will demonstrate how to setup a VPN connection between a remote PC and the WL/IP-8000VPN using the PPTP server function. Looking at the diagram above, the Remote PC has real IP address of 192.168.0.1. If this remote PC is connected to Internet through an IP sharing router, please make sure that router supports PPTP pass through function. In this example, the WL/IP-8000VPN's WAN IP address is 192.168.0.3. You can also register the WL/IP-8000VPN with dynamic DNS if you don't have a fixed IP address. Finally, the local LAN has IP address 192.168.1.x. Please note that if the Remote PC is behind a router, the remote PC's IP subnet must be different from the local IP subnet.

The Router's PPTP server can support 5 PPTP VPN user's accounts.

In the real world Internet connection, Remote PC would not directly connect to the router, which is WL/IP-8000 VPN here. You need to set the correct Remote Gateway both in WL/IP-8000VPN WAN port and Remote PC for your own environment.

Router's LAN, User's LAN, and PPTP virtual LAN must all have different LAN number. Router's LAN is 192.168.1.x, user's LAN is 192.168.0.y, and virtual LAN is 10.0.0.z in this case.

Router Setup



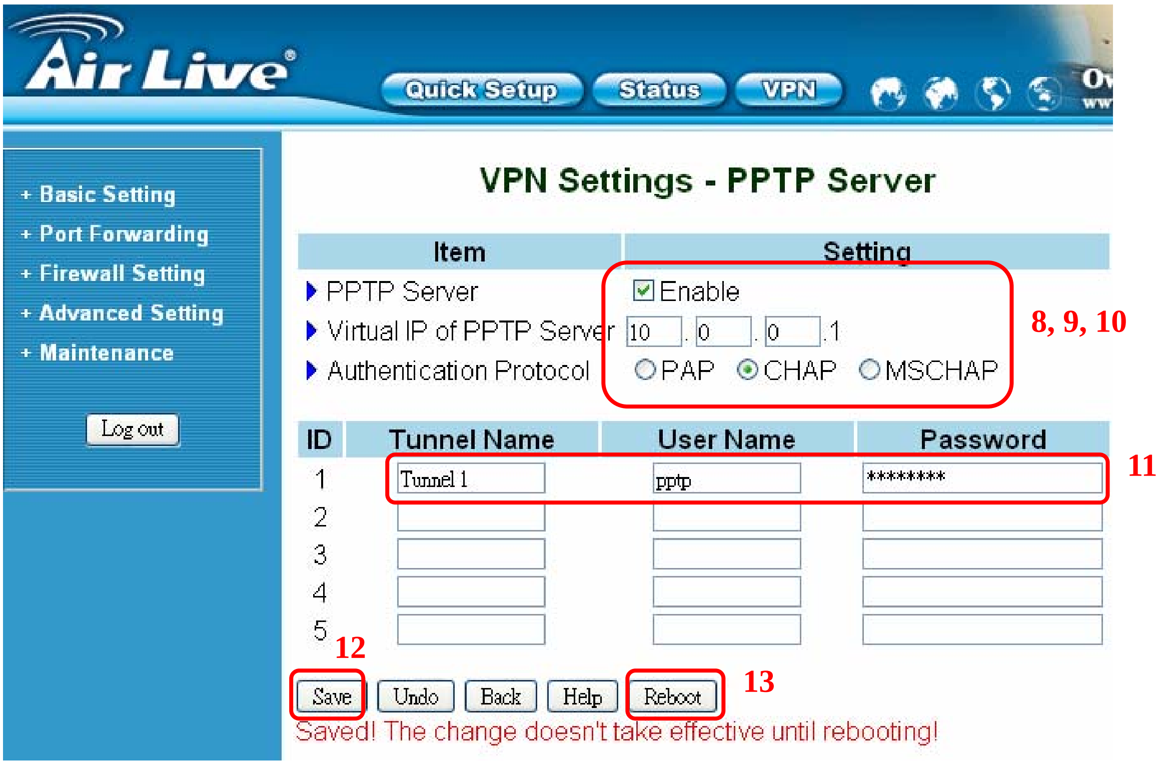
VPN Settings

Item	Setting
VPN	☑ Enable
NetBIOS broadcast	☑ Enable
Max. number of tunnels	1

ID	Tunnel Name	Method	
1	Tunnel	IKE	More
2		IKE	More
3		IKE	More
4		IKE	More
5		IKE	More

Saved! The change doesn't take effective until rebooting!

1. Click on **VPN** button on top of this page
2. Check VPN **Enable** checkbox.
3. Check NetBIOS broadcast **Enable** checkbox.
4. Enter the Max number of tunnels as **1**
5. Enter the Tunnel Name as **Tunnel**
6. Click on **Save** button at the bottom of the page (no need to reboot now)
7. Click on **PPTP Server Setting** button



VPN Settings - PPTP Server

Item	Setting
PPTP Server	☑ Enable
Virtual IP of PPTP Server	10 . 0 . 0 .1
Authentication Protocol	○ PAP ● CHAP ○ MSCHAP

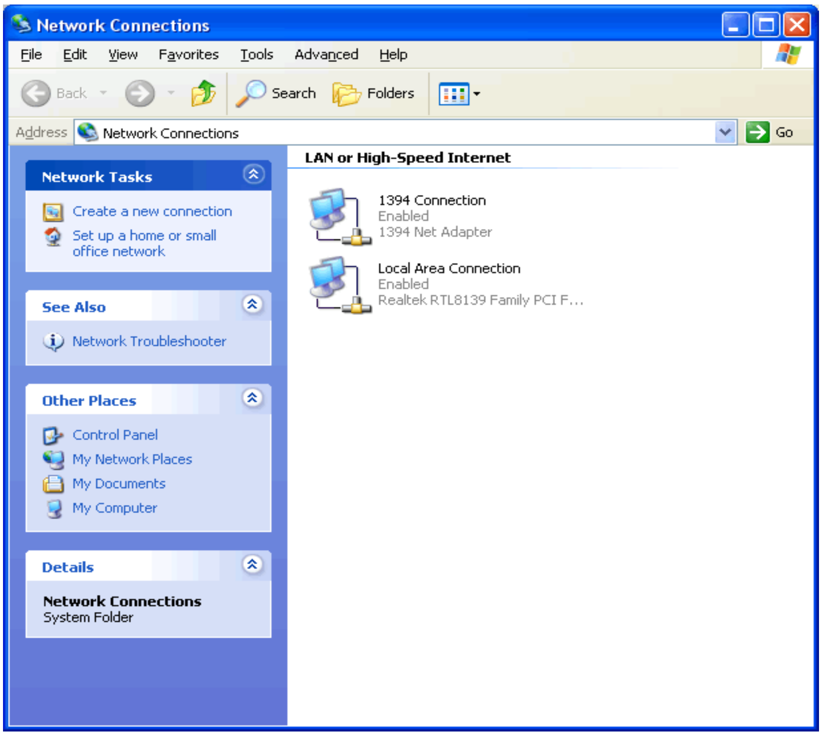
ID	Tunnel Name	User Name	Password
1	Tunnel 1	pptp	********
2			
3			
4			
5			

Saved! The change doesn't take effective until rebooting!

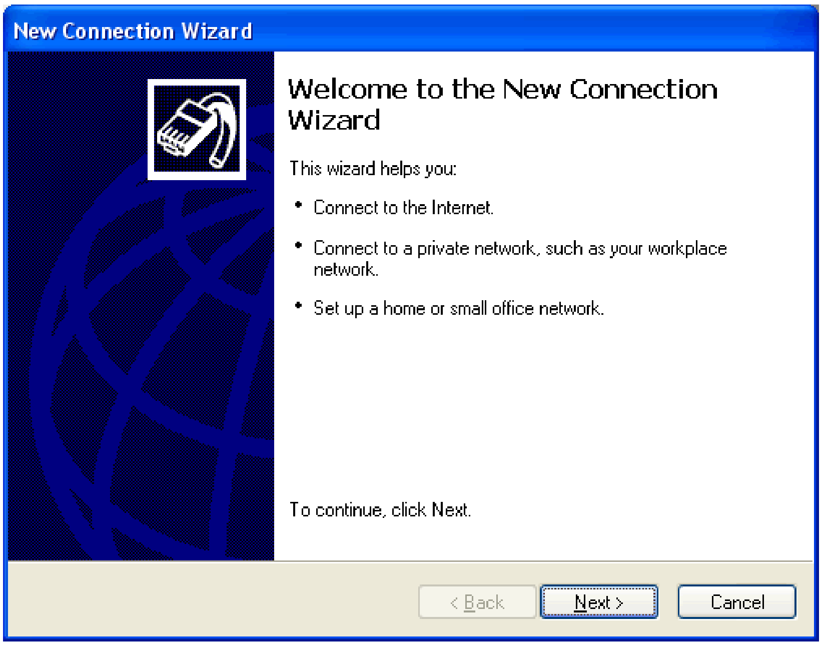
8. Check PPTP Server **Enable** checkbox.
9. Change the *Virtual IP of PPTP Server* address, if needed
10. Change the *Authentication Protocol* to **CHAP**
11. Enter the *Tunnel Name, User Name,* and *Password*.
12. Click on **Save** button
13. Click on **Reboot** button. When asked to reboot shown in a pop-up message, click **OK** to reboot and let the settings take effect.

Remote PC Setup (Using Windows XP VPN Client)

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



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



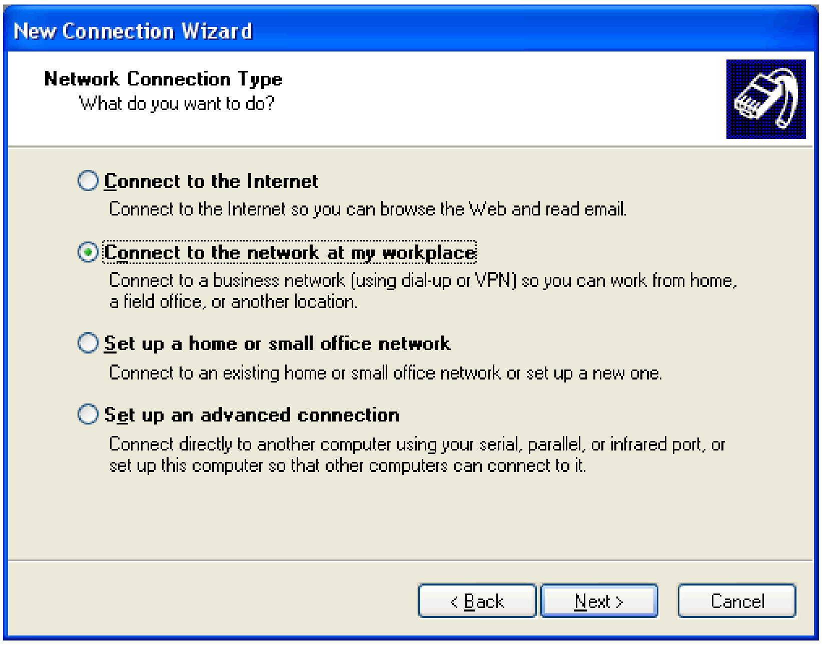
Welcome to the New Connection Wizard

This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.
- Set up a home or small office network.

To continue, click Next.

3. Click on **Next** button


New Connection Wizard

Network Connection Type
What do you want to do?

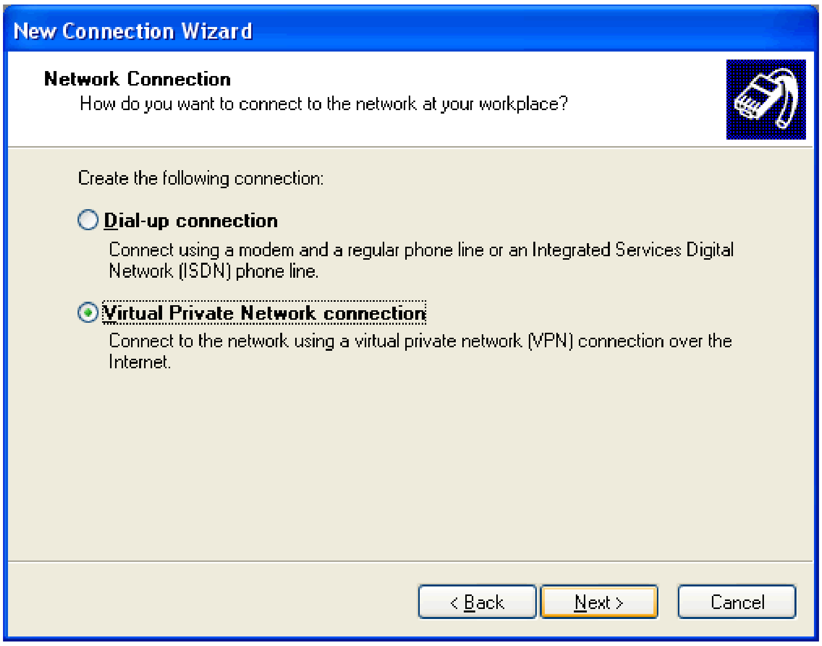
○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

● **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up a home or small office network**
Connect to an existing home or small office network or set up a new one.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

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


New Connection Wizard

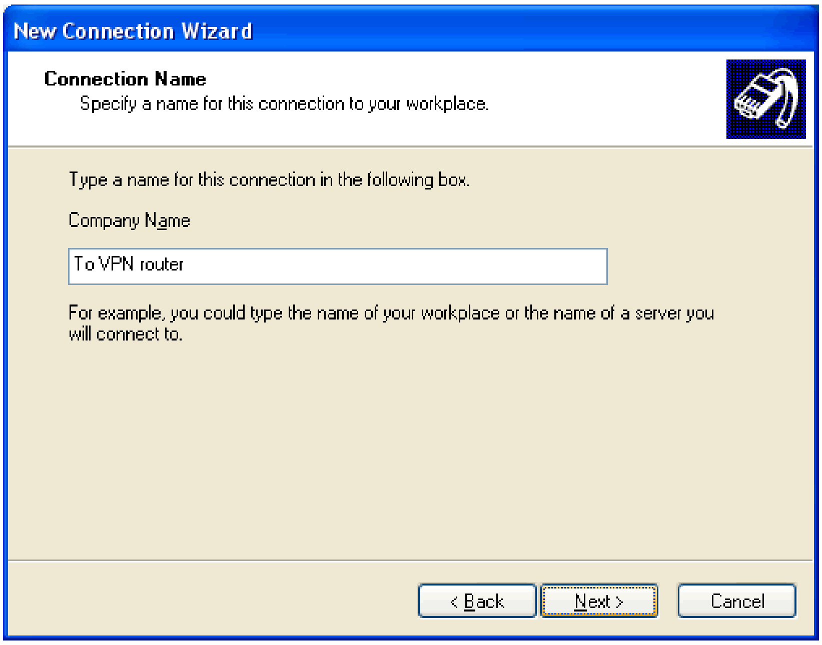
Network Connection
How do you want to connect to the network at your workplace?

Create the following connection:

○ **Dial-up connection**
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

● **Virtual Private Network connection**
Connect to the network using a virtual private network (VPN) connection over the Internet.

6. Click on Virtual Private Network connection
7. Click on **Next** button



New Connection Wizard

Connection Name

Specify a name for this connection to your workplace.

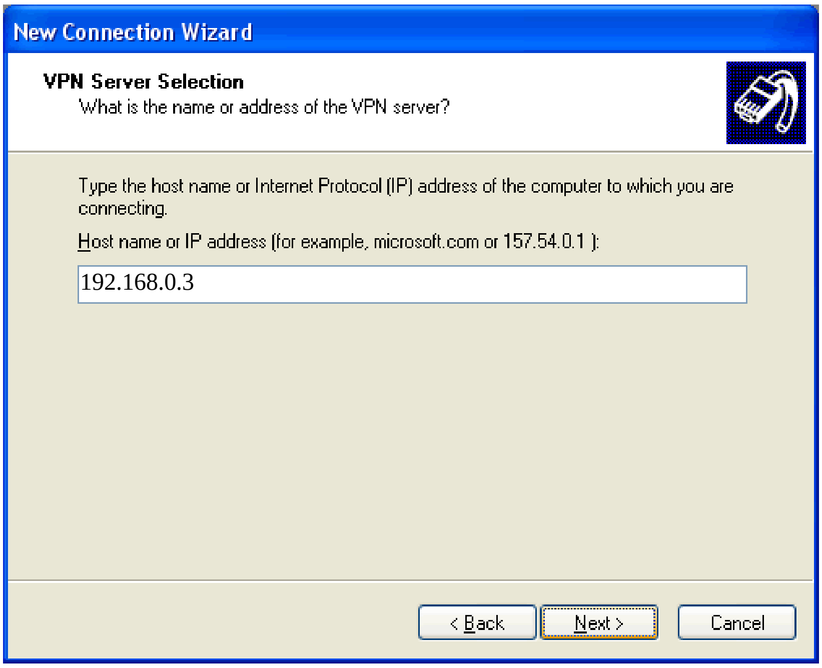
Type a name for this connection in the following box.

Company Name

To VPN router

For example, you could type the name of your workplace or the name of a server you will connect to.

8. Enter the name of this VPN connection. In this case, the name is To VPN router.
9. Click on **Next**



New Connection Wizard

VPN Server Selection

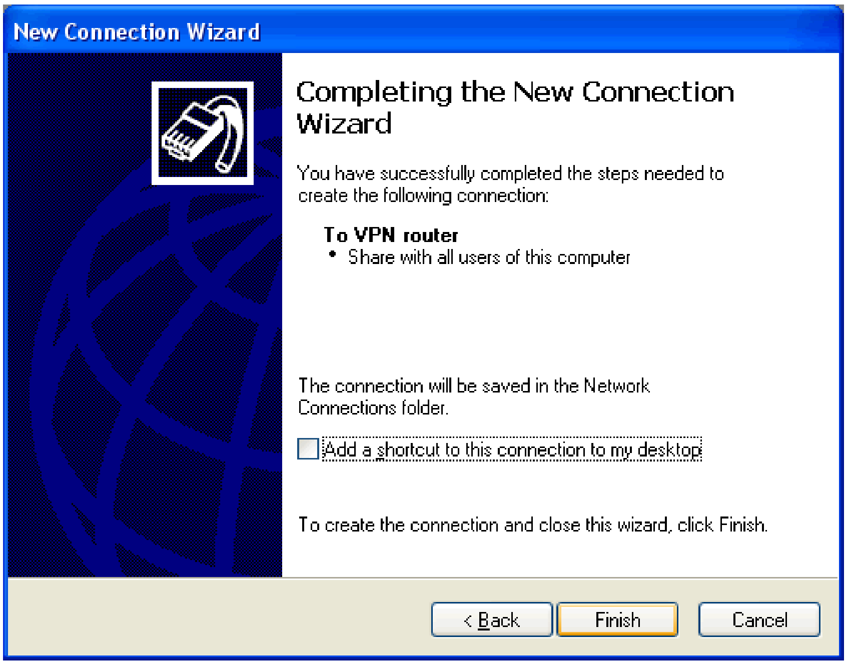
What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

192.168.0.3

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



New Connection Wizard

Completing the New Connection Wizard

You have successfully completed the steps needed to create the following connection:

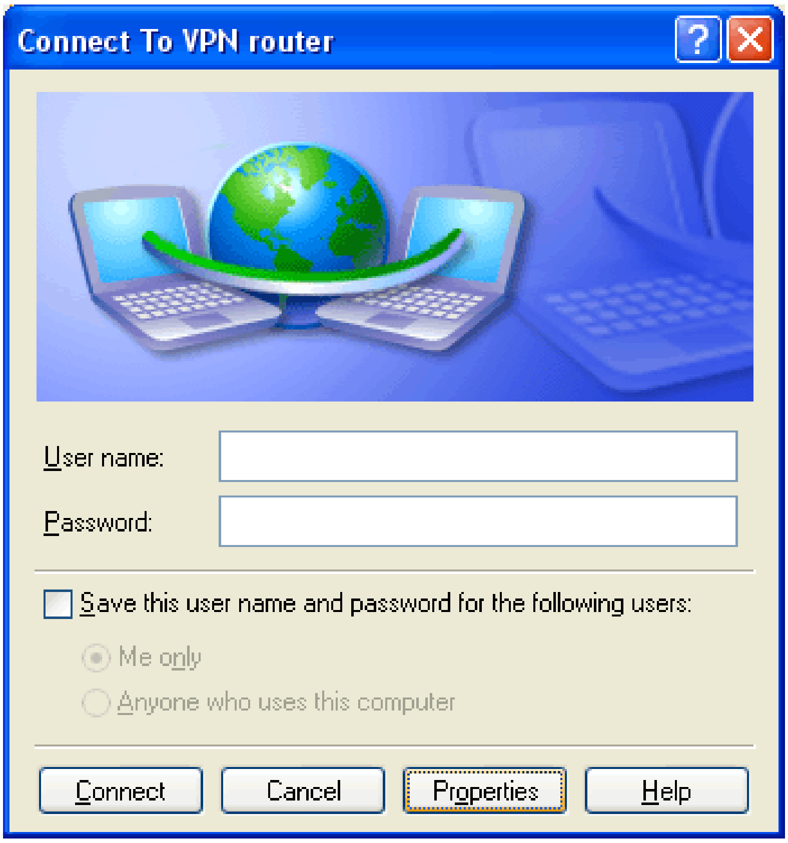
To VPN router
- Share with all users of this computer

The connection will be saved in the Network Connections folder.

□ Add a shortcut to this connection to my desktop

To create the the connection and close this wizard, click Finish.

12. If you would like this connection to 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.



Connect To VPN router

User name:

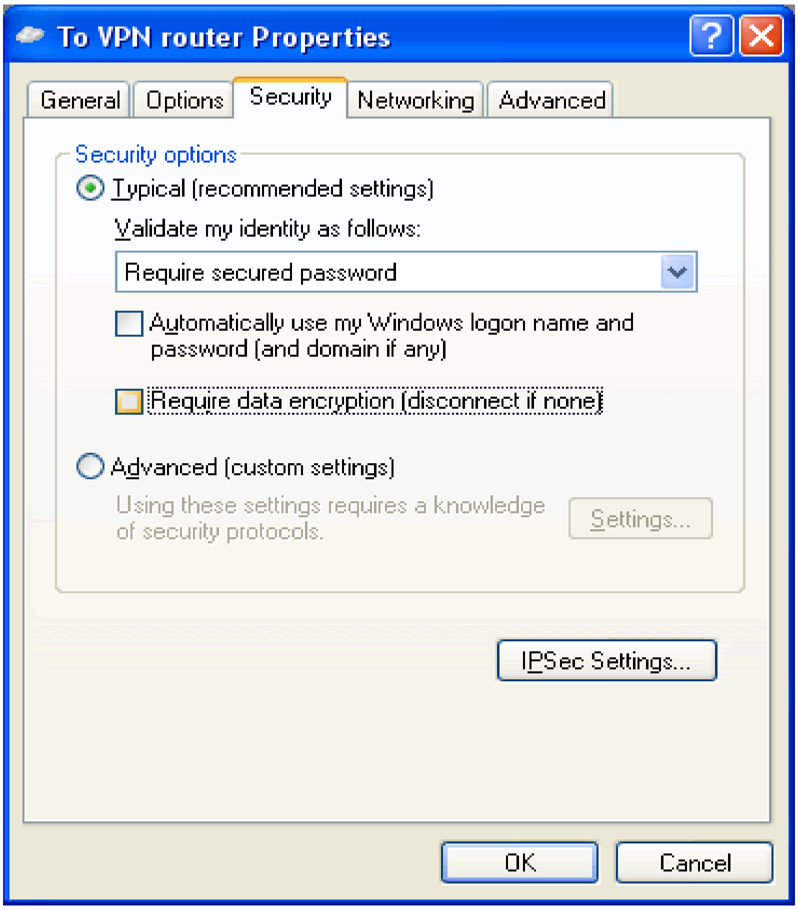
Password:

□ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

14. Click on **Properties** button



Security options

● Typical (recommended settings)

Validate my identity as follows:

Require secured password

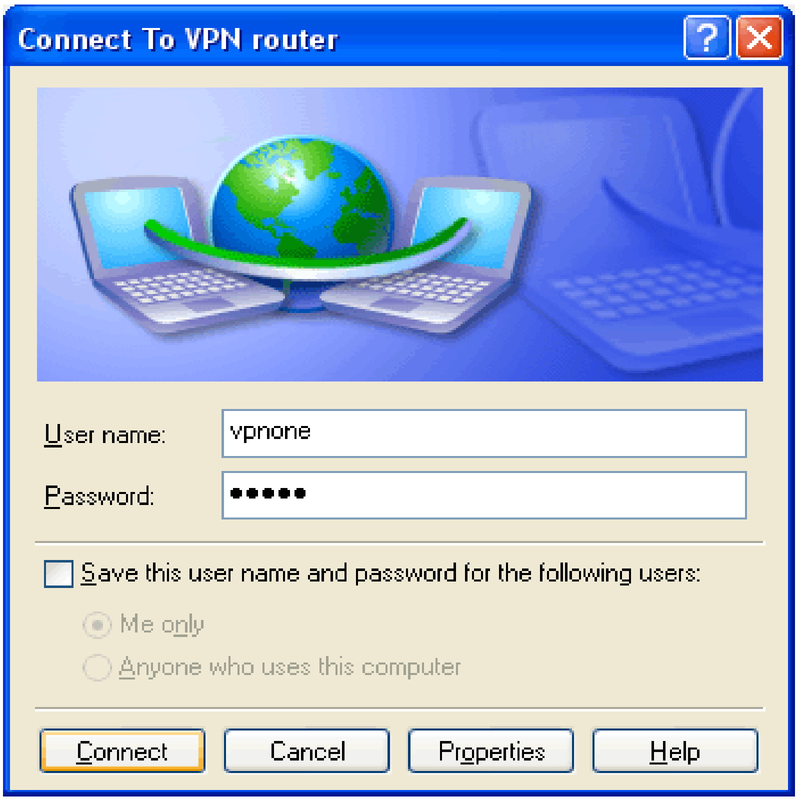
□ Automatically use my Windows logon name and password (and domain if any)

□ Require data encryption (disconnect if none)

○ Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

15. Un-tick or cancel the check box of **Require data encryption** (disconnect if none)
16. Click on **OK**



User name: vpnone

Password: ●●●●●

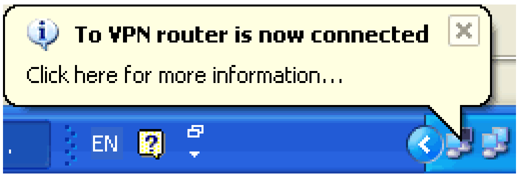
□ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

17. Enter your User name and Password
18. Click on **Connect** button.

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



To VPN router is now connected

Click here for more information...

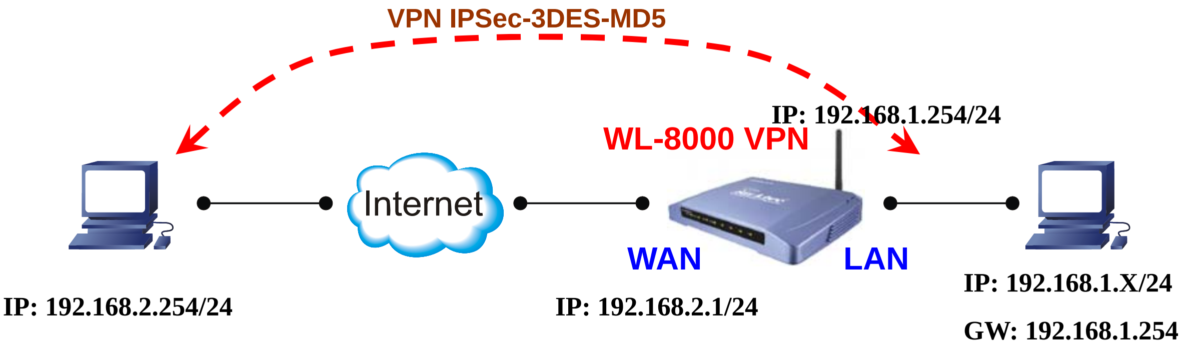
You can also access to your web-based management page from your router and go to PPTP server setting page. From the bottom of the page, you will see the current PPTP VPN connection status from Client Management section.

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 provides 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.

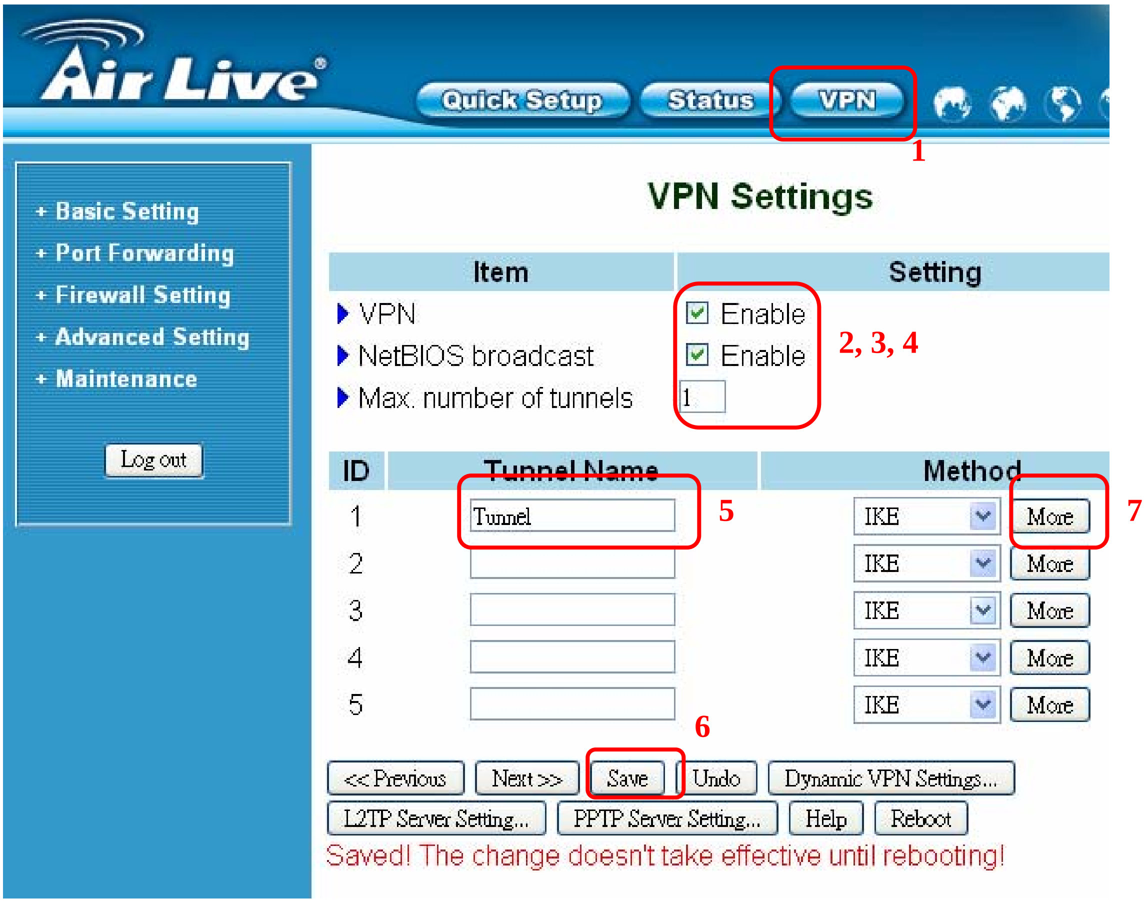


The above diagram provides simple illustration of how to connect two end points via your router by VPN technique. In this case, a PC with IP address of 192.168.2.254/24 is trying to connect with another PC with its IP address of 192.168.1.x/24 via your VPN router with its IP address of 192.168.1.254/24.

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

In the real world Internet connection, Remote PC would not directly connect to the router, which is WL/IP-8000 VPN here. You need to set the correct Remote Gateway both in WL/IP-8000VPN WAN port and Remote PC for your own environment.

Router's IPSec Setup



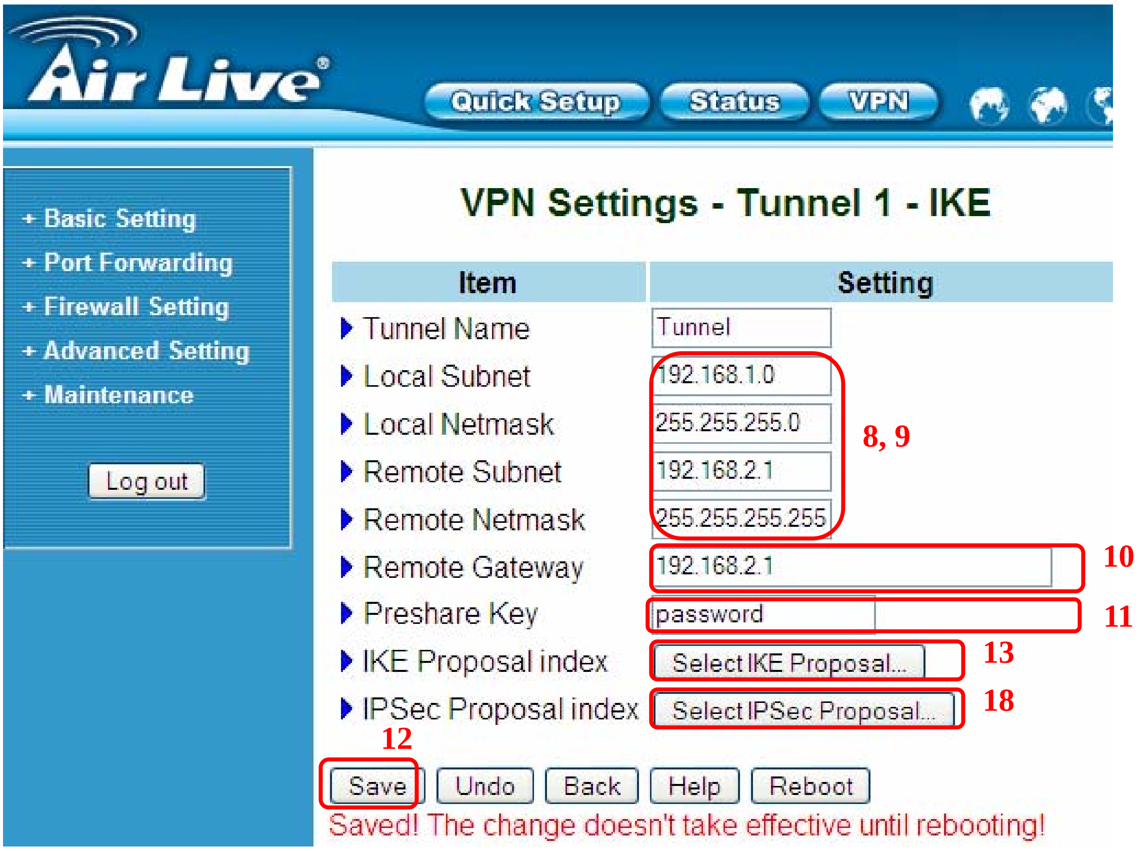
VPN Settings

Item	Setting
VPN	☑ Enable
NetBIOS broadcast	☑ Enable
Max. number of tunnels	1

ID	Tunnel Name	Method	
1	Tunnel	IKE	More
2		IKE	More
3		IKE	More
4		IKE	More
5		IKE	More

Saved! The change doesn't take effective until rebooting!

1. Click on **VPN** button on top of this page
2. Check VPN **Enable** checkbox.
3. Check NetBIOS broadcast **Enable** checkbox.
4. Enter the Max number of tunnels as **1**
5. Enter the Tunnel Name as **Tunnel**
6. Click on **Save** button at the bottom of the page (no need to reboot now)
7. Click on **More** button at the end of *ID 1*.



VPN Settings - Tunnel 1 - IKE

Item	Setting
Tunnel Name	Tunnel
Local Subnet	192.168.1.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.2.1
Remote Netmask	255.255.255.255
Remote Gateway	192.168.2.1
Preshare Key	password
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Saved! The change doesn't take effective until rebooting!

8. Enter the local subnet **192.168.1.0** and subnet mask **255.255.255.0**.
9. Enter the remote subnet **192.168.2.1** and subnet mask **255.255.255.255**.
10. Enter the IP address of the router's WAN port. In this case, it is **192.168.2.1**.
11. Enter the *Preshared Key*
12. Click on **Save** button (no need to reboot for now)
13. Click on **Select IKE Proposal** button

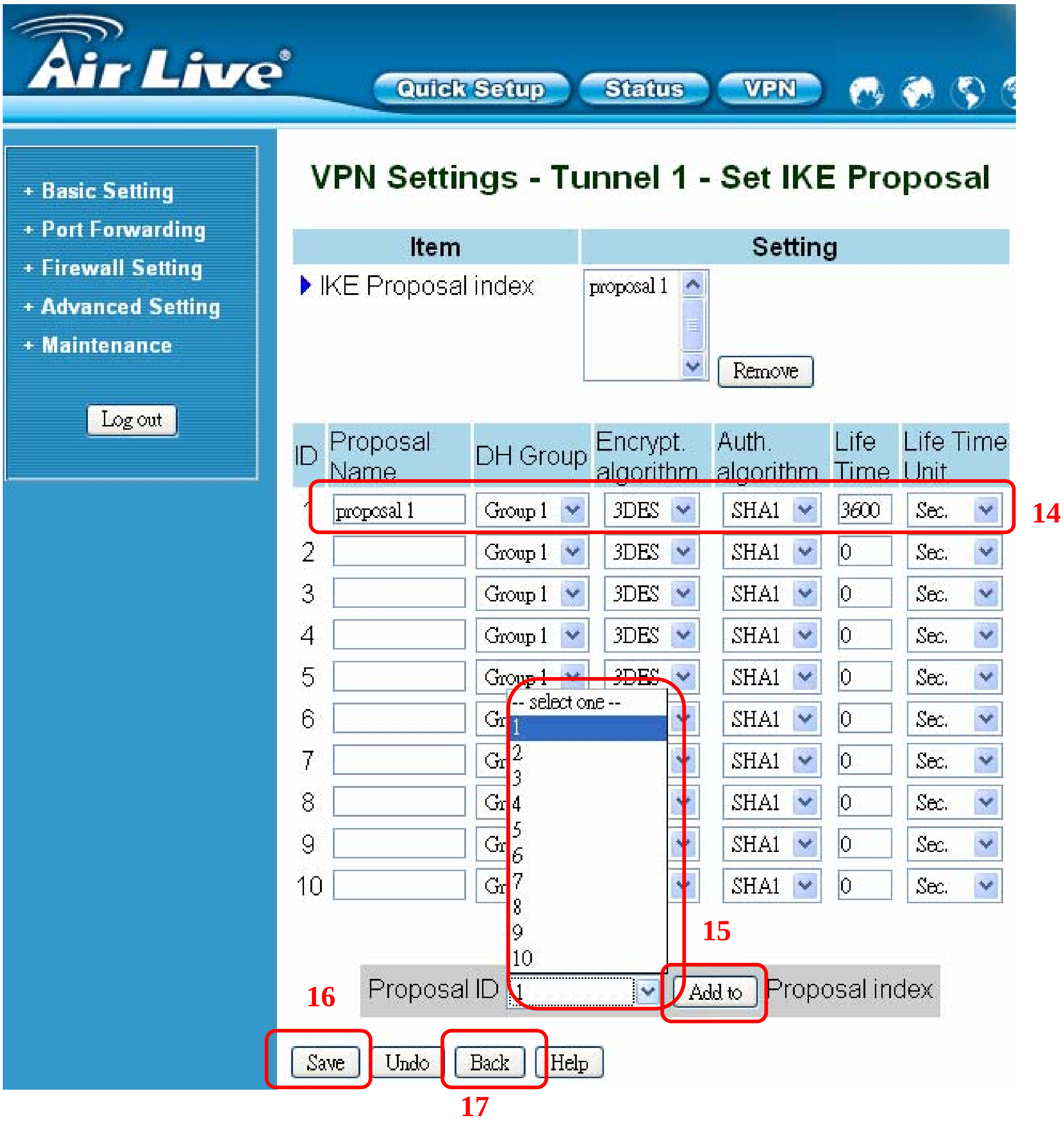
14.Enter *Proposal Name,* key *Life Time*, and change any other settings, if needed, for proposal *ID 1*. (Note that you must use **Group 2** with **3DES**, or **Group 1** with **DES** for default Windows XP IPSec)

15.Select *Proposal ID **1*** and click button **Add to** *Proposal index*. You can add maximal 4 proposals in total from the IKE proposal index.

16.Click on **Save** button (no need to reboot now)

17.Click on **Back** button (go back to the screen on this page above)

18.Click on **Select IPSec Proposal** button (in **Dynamic VPN Settings** page)



VPN Settings - Tunnel 1 - Set IKE Proposal

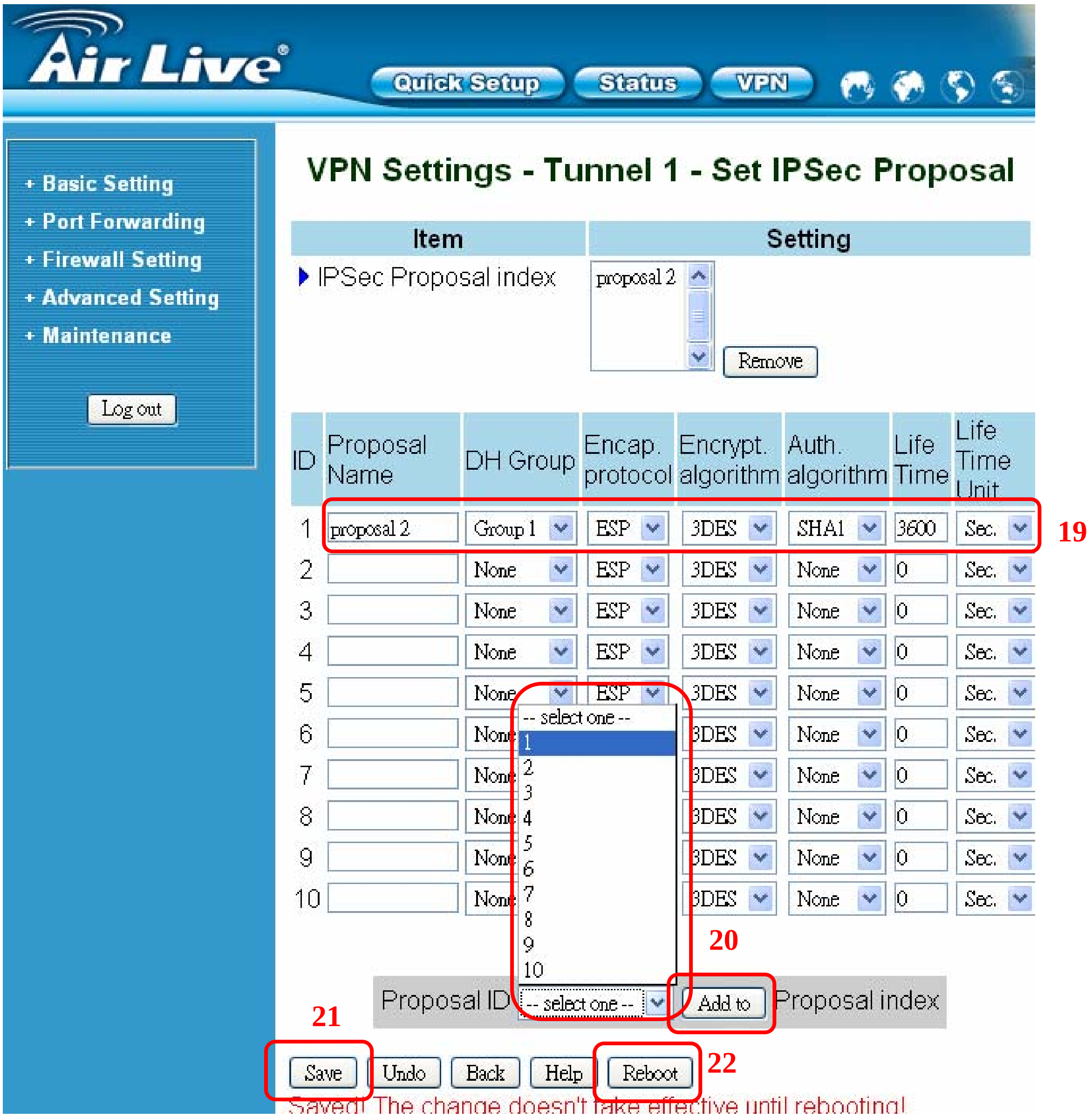
Item	Setting
IKE Proposal index	proposal 1

ID	Proposal Name	DH Group	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	proposal 1	Group 1	3DES	SHA1	3600	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Gr		SHA1	0	Sec.
7		Gr		SHA1	0	Sec.
8		Gr		SHA1	0	Sec.
9		Gr		SHA1	0	Sec.
10		Gr		SHA1	0	Sec.

-- select one --
1
2
3
4
5
6
7
8
9
10

Proposal ID 1 Add to Proposal index

19. Enter IPSec *Proposal Name*, key *Life Time*, select *DH Group*, *Auth algorithm*, and change any other settings, if needed, for IPSec proposal *ID 1*. (Note that you must use **Group 2** with **3DES**, or **Group 1** with **DES** for default Windows XP IPSec)
20. Select *Proposal ID* ***1*** and click button **Add to** *Proposal index*. You can add maximal 4 proposals in total from the IKE proposal index.
21. Click on **Save** button
22. Click on **Reboot** button. When asked to reboot shown in a pop-up message, click **OK** to reboot and let the settings take effect.



VPN Settings - Tunnel 1 - Set IPSec Proposal

Item	Setting
IPSec Proposal index	proposal 2 Remove

ID	Proposal Name	DH Group	Encap. protocol	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	proposal 2	Group 1	ESP	3DES	SHA1	3600	Sec.
2		None	ESP	3DES	None	0	Sec.
3		None	ESP	3DES	None	0	Sec.
4		None	ESP	3DES	None	0	Sec.
5		None	ESP	3DES	None	0	Sec.
6		None		3DES	None	0	Sec.
7		None		3DES	None	0	Sec.
8		None		3DES	None	0	Sec.
9		None		3DES	None	0	Sec.
10		None		3DES	None	0	Sec.

Proposal ID -- select one -- (-- select one --, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10) Add to Proposal index

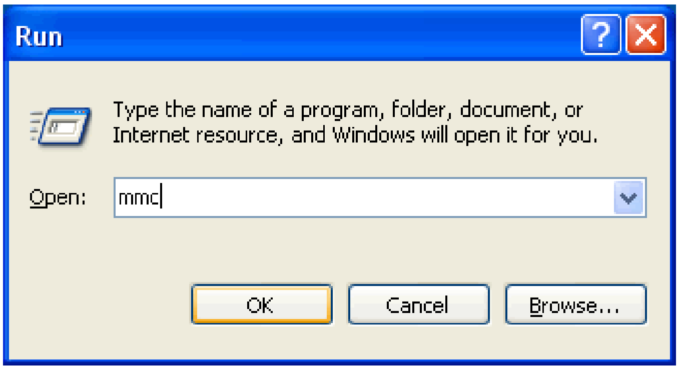
Save Undo Back Help Reboot

Saved! The change doesn't take effective until rebooting!

PC's IPSec Setup (Windows XP)

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

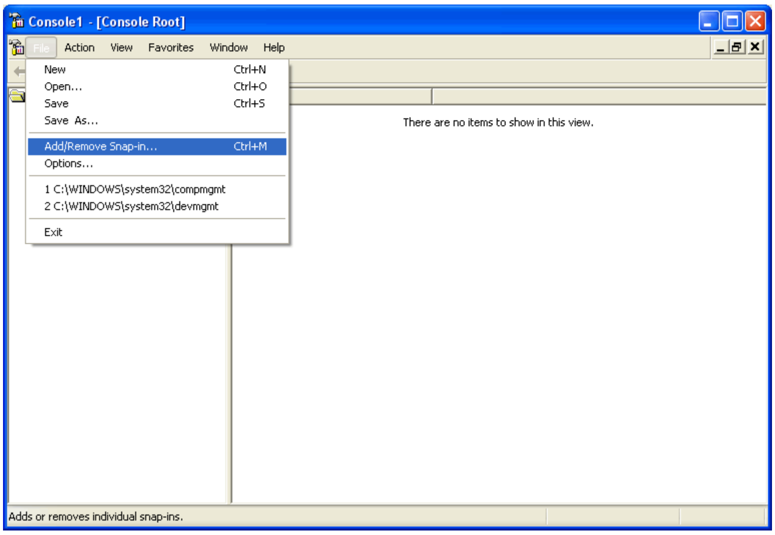
Before you start to configure Windows XP IPSec environment, make sure you don't have other 3rd party IPSec clients installed in your system. Otherwise, Windows XP IPSec will refuse to work.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

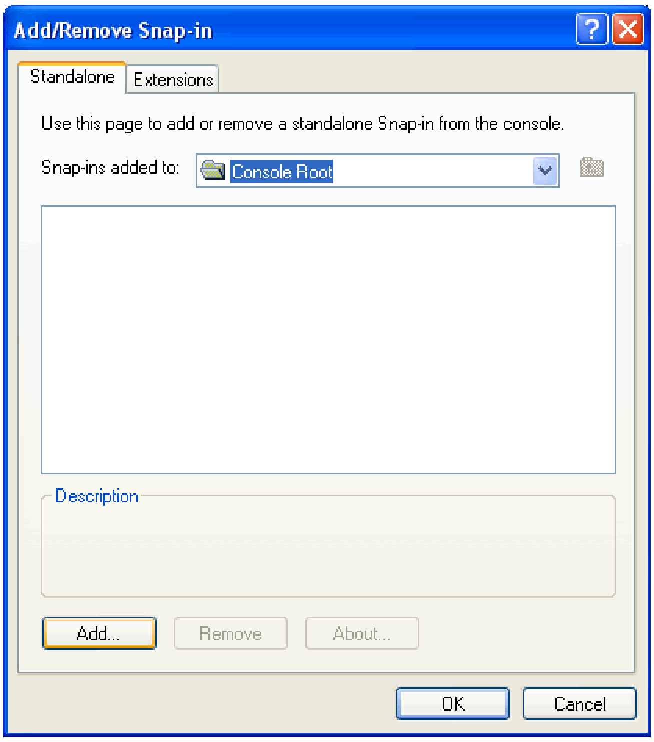
1. Go to **Start** button and select **Run**
2. Type *mmc* in open field
3. Click **OK**.


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\WINDOWS\system32\compmgmt
2 C:\WINDOWS\system32\devmgmt
Exit

There are no items to show in this view.

Adds or removes individual snap-ins.

4. From **File** pull-down window, select **Add/Remove Snap-in**

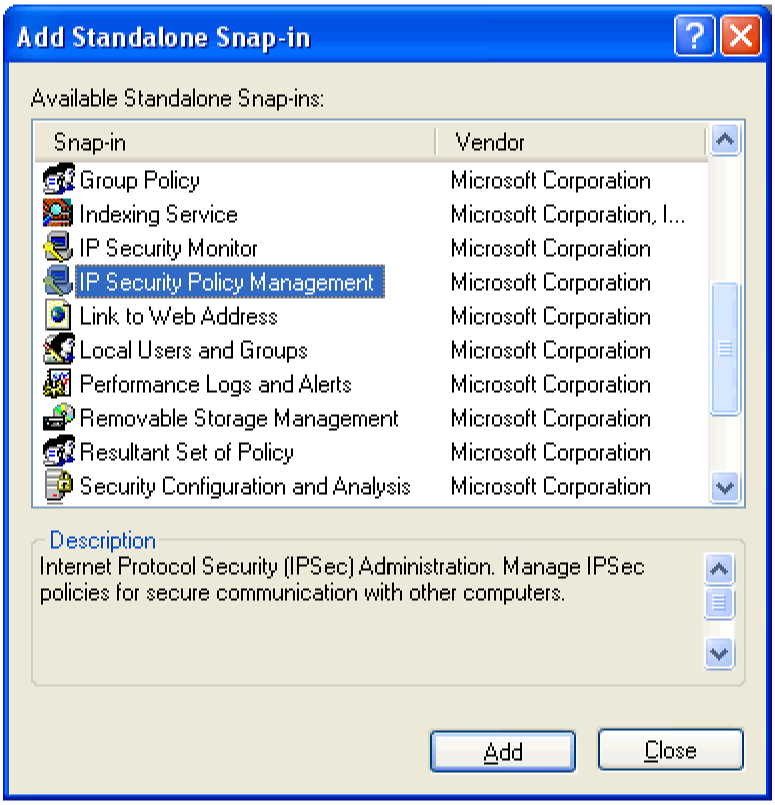


Add/Remove Snap-in

Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

5. Click on **Add** button



Add Standalone Snap-in

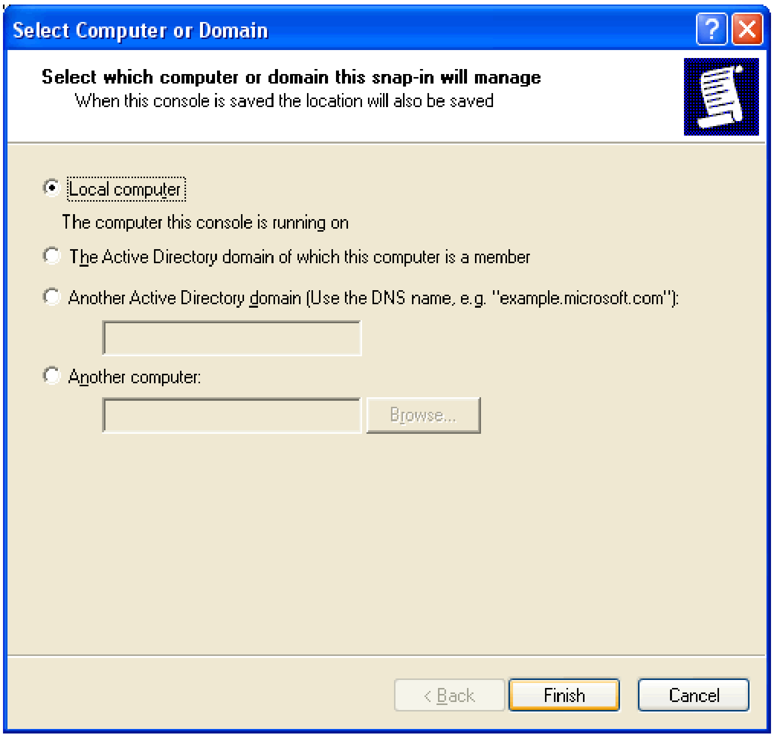
Available Standalone Snap-ins:

Snap-in	Vendor
Group Policy	Microsoft Corporation
Indexing Service	Microsoft Corporation, I...
IP 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
Removable 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.

6. Click on IP Security policy management
7. Click on **Add** button

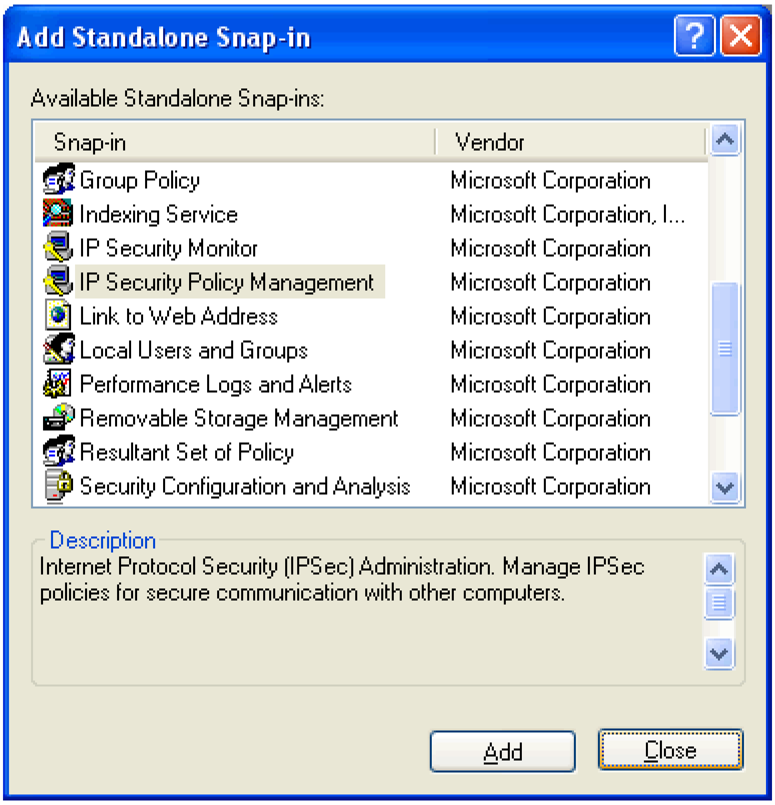


Select Computer or Domain

Select which computer or domain this snap-in will manage
When this console is saved the location will also be saved

● Local computer
The computer this console is running on
○ The Active Directory domain of which this computer is a member
○ Another Active Directory domain (Use the DNS name, e.g. "example.microsoft.com"):
○ Another computer:

8. Select Local Computer
9. Click on **Finish** button



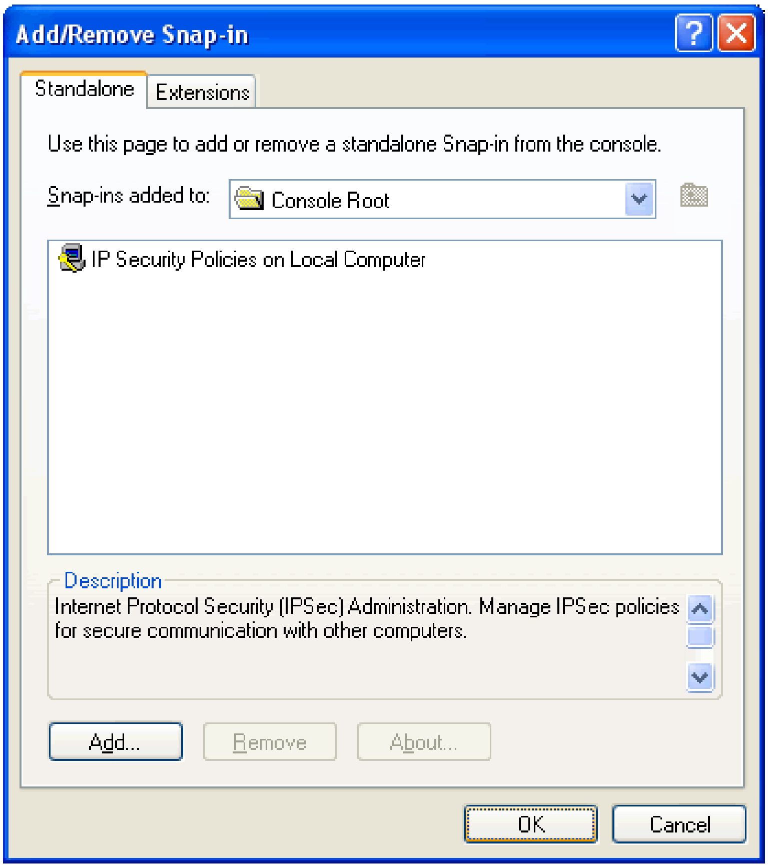
Add Standalone Snap-in

Available Standalone Snap-ins:

Snap-in	Vendor
Group Policy	Microsoft Corporation
Indexing Service	Microsoft Corporation, I...
IP 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
Removable 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.

10. Click on **Close** button



Add/Remove Snap-in

Standalone | Extensions

Use this page to add or remove a standalone Snap-in from the console.

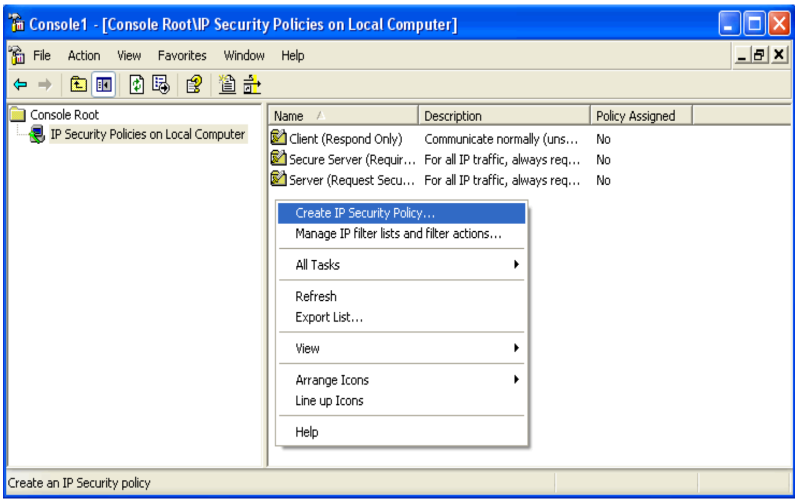
Snap-ins added to: Console Root

IP Security Policies on Local Computer

Description

Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.

11. Click on **OK** button



Console1 - [Console Root\IP Security Policies on Local Computer]

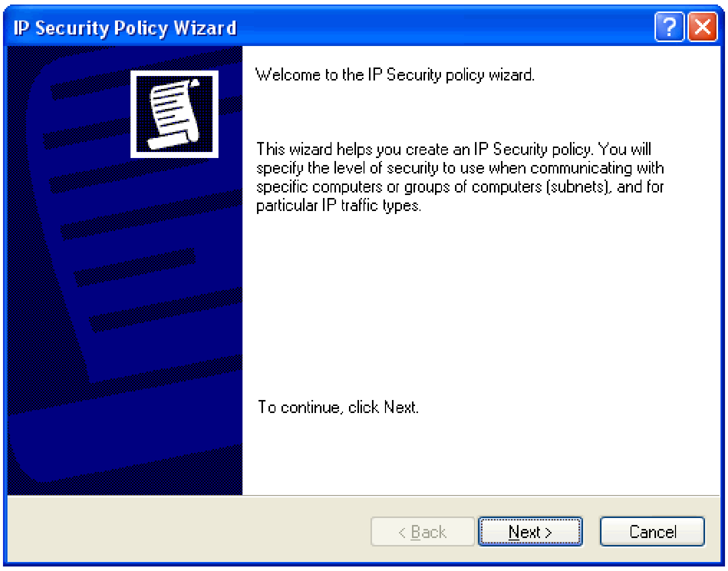
File
Action
View
Favorites
Window
Help
Console Root
IP Security Policies on Local Computer

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
Line up Icons
Help

Create an IP Security policy

12. Click on IP Security Policies on Local Computer on the left screen
13. On the right screen, move your mouse cursor to the blank area and hit a single click on the right hand button of your mouse.
14. Select **Create IP Security Policy** from the pull-down window.

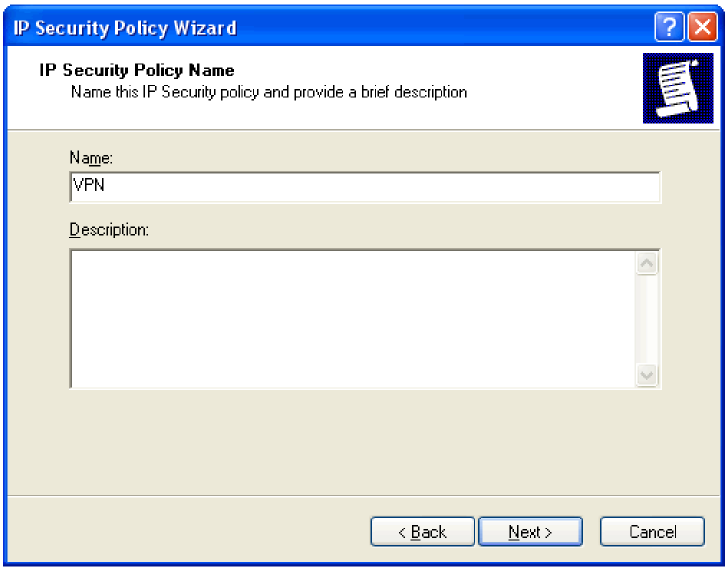


Welcome to the IP Security policy wizard.

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.

15. Click on **Next** button



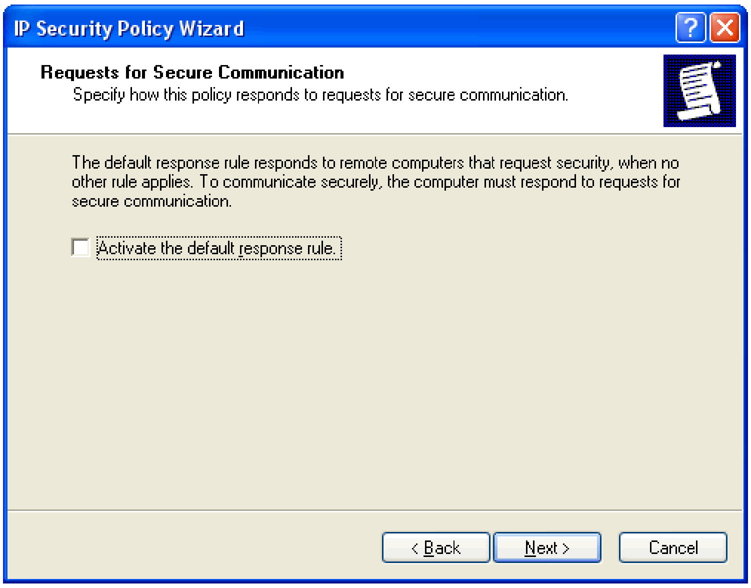
IP Security Policy Name

Name this IP Security policy and provide a brief description

Name: VPN

Description:

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



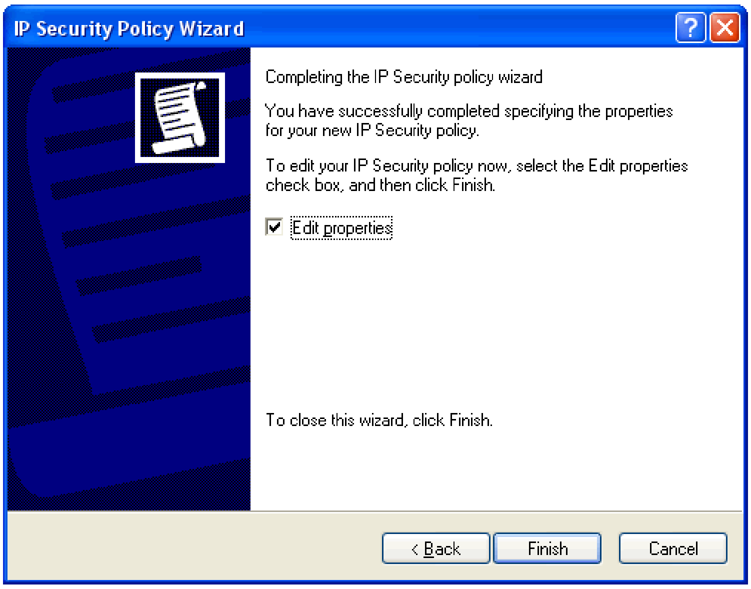
Requests for Secure Communication

Specify how this policy responds to requests for secure communication.

The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.

□ Activate the default response rule.

17. Un-check or cancel the square box next to **Activate the default response rule**.
18. Click on **Next** button



IP Security Policy Wizard

Completing the IP Security policy wizard

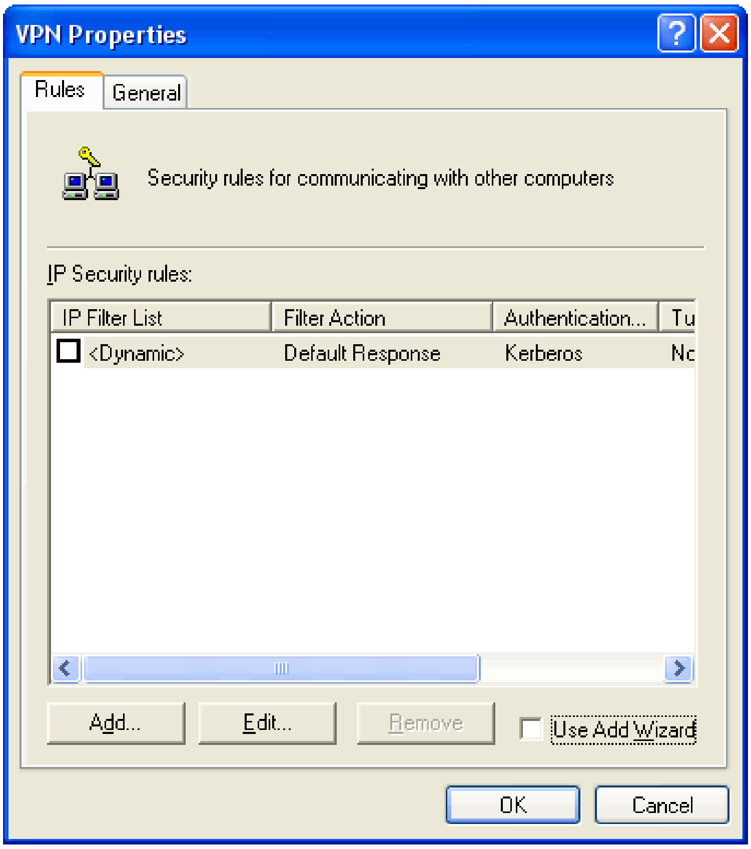
You have successfully completed specifying the properties for your new IP Security policy.

To edit your IP Security policy now, select the Edit properties check box, and then click Finish.

☑ Edit properties

To close this wizard, click Finish.

19. Tick on the square box next to **Edit** properties
20. Click on **Finish** button



VPN Properties

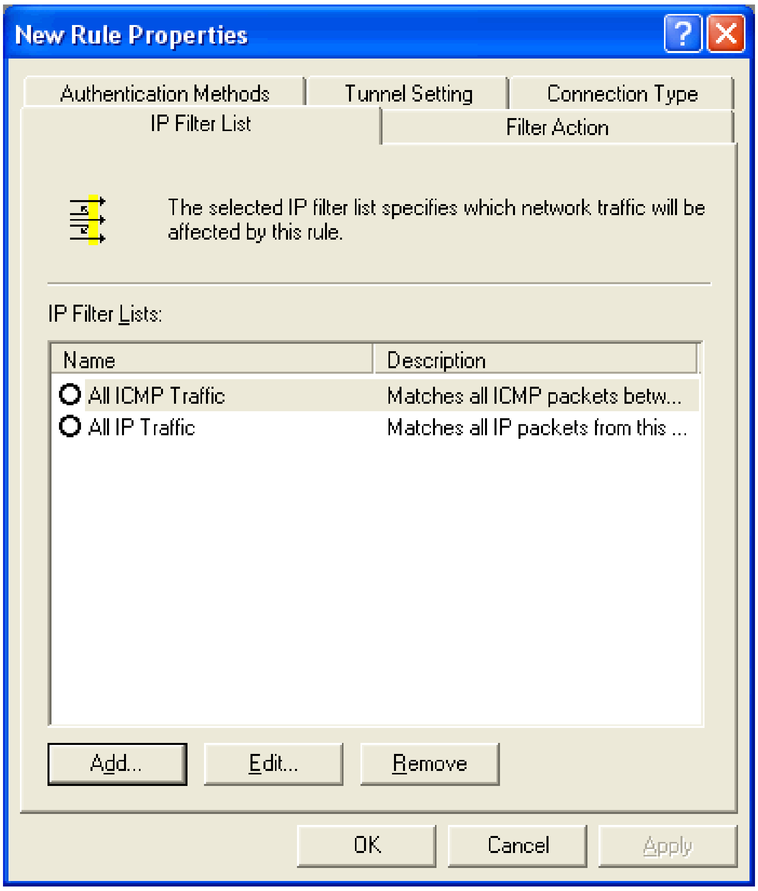
Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
□ <Dynamic>	Default Response	Kerberos	Nc

□ Use Add Wizard

21. Un-tick or cancel **Use Add Wizard**
22. Click on **Add** button

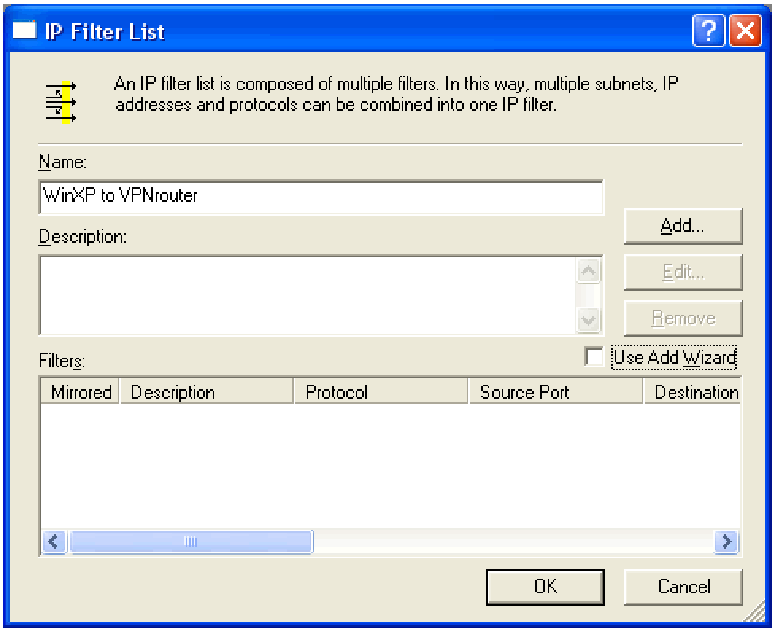


The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...

23. Click on **Add** button



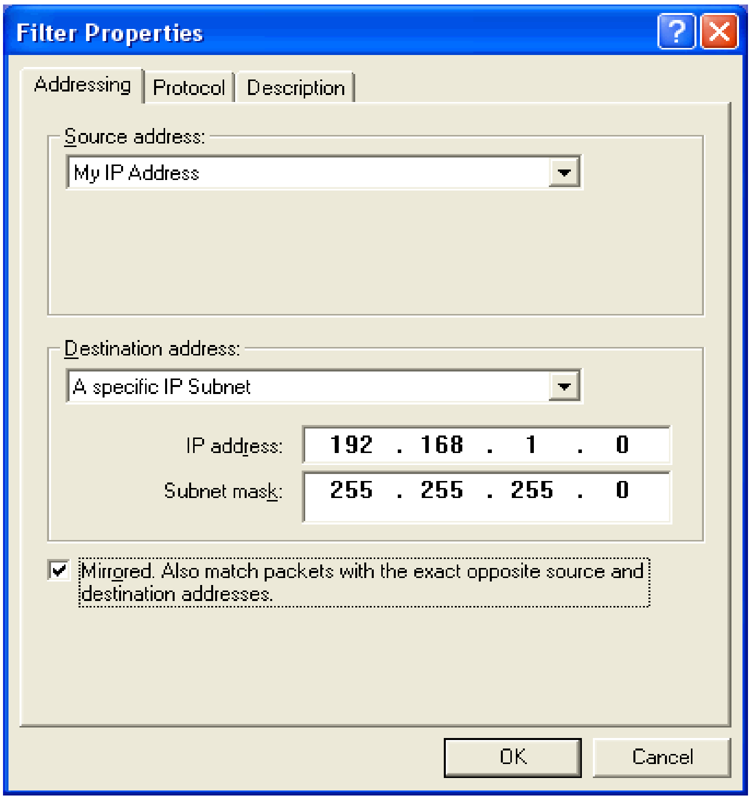
An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: WinXP to VPNrouter

Description:

Filters: □ Use Add Wizard

24. Enter the name of the IP Filter List. (In this case, the name is WinXP to VPN router)
25. Uncheck Use Add Wizard.
26. Click **OK**.



Source address: My IP Address

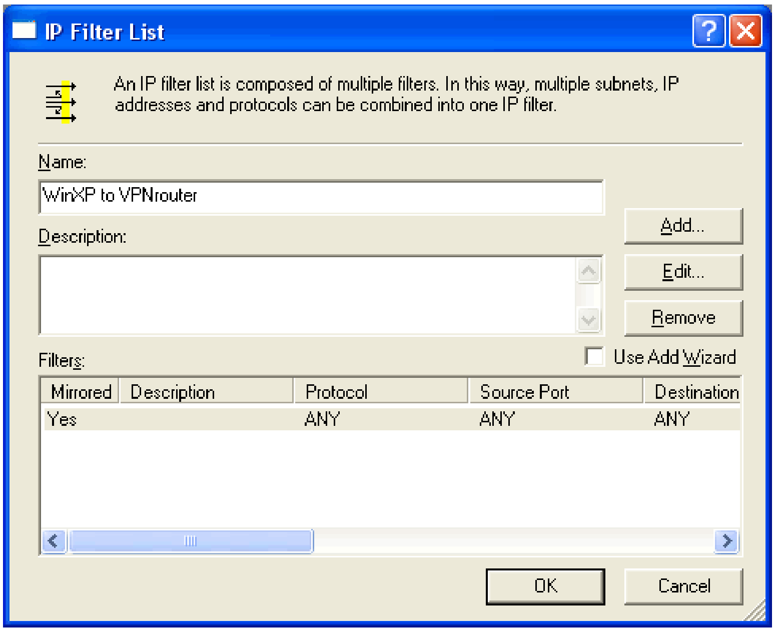
Destination address: A specific IP Subnet

IP address: 192 . 168 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

☑ Mirrored. Also match packets with the exact opposite source and destination addresses.

27. From Source address pull-down window, select **My IP Address**
28. From Destination address pull-down window, select **A specific IP Subnet**. Enter destination IP address and its subnet mask. (in this case, the destination IP is 192.168.1.0/255.255.255.0)
29. Check the box of Mirrored. Also match packets with the exact opposite source and destination addresses.
30. Click on **OK** button



An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

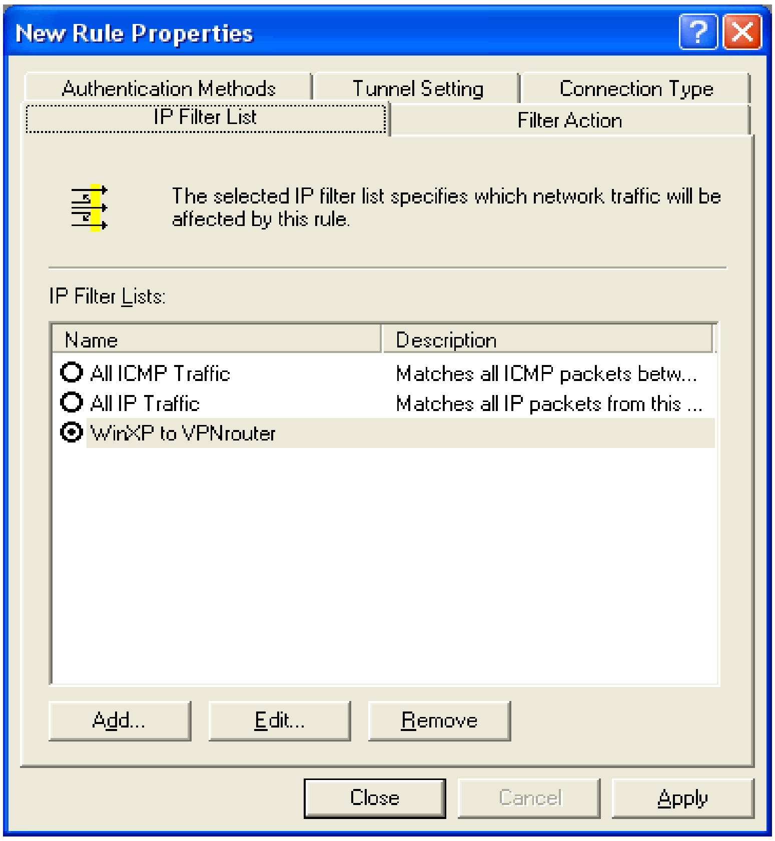
Name: WinXP to VPNrouter

Description:

Filters: □ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY

31. Click on **OK** button



New Rule Properties

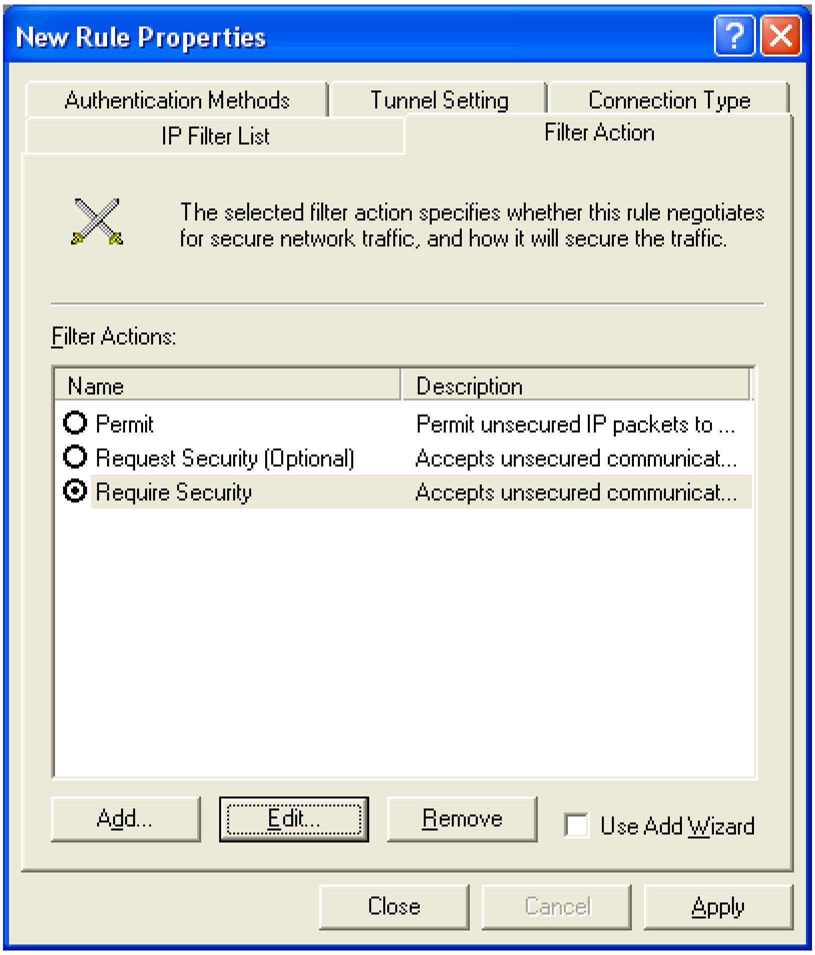
Authentication Methods | Tunnel Setting | Connection Type | IP Filter List | Filter Action

The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
● WinXP to VPNrouter	

32. Click on IP Filter name of your previous setting. (in this case, it’s WinXP to VPNrouter)



New Rule Properties

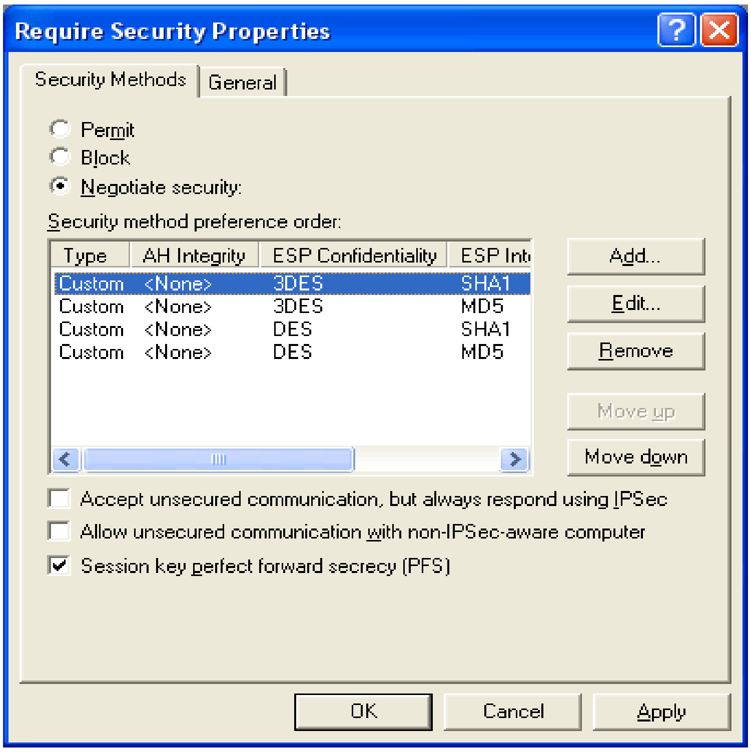
Authentication Methods | Tunnel Setting | Connection Type | IP Filter List | Filter Action

The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

Name	Description
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
● Require Security	Accepts unsecured communicat...

33. Click on Require Security
34. Click on **Edit** button



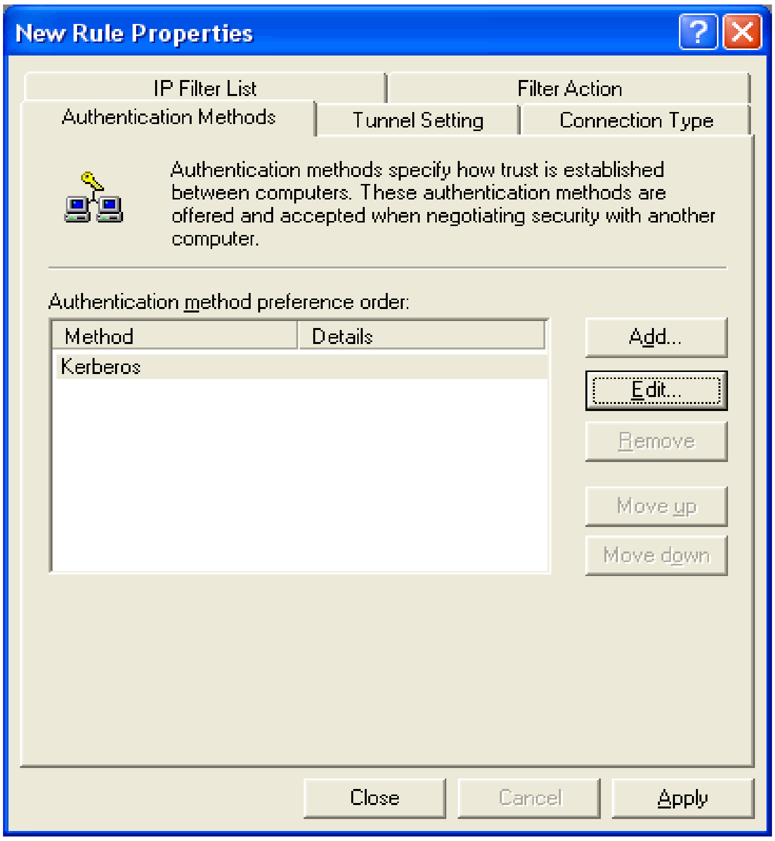
○ Permit
○ Block
● Negotiate security:

Security method preference order:

Type	AH Integrity	ESP Confidentiality	ESP Int
Custom	<None>	3DES	SHA1
Custom	<None>	3DES	MD5
Custom	<None>	DES	SHA1
Custom	<None>	DES	MD5

☐ Accept unsecured communication, but always respond using IPSec
☐ Allow unsecured communication with non-IPSec-aware computer
☑ Session key perfect forward secrecy (PFS)

35. Click on Negotiate security
36. Cancel the check box of Accept unsecured communication, but always respond using IPSec
37. Tick the box of session key **perfect forward secrecy (PFS)**.
38. Click on **OK** button

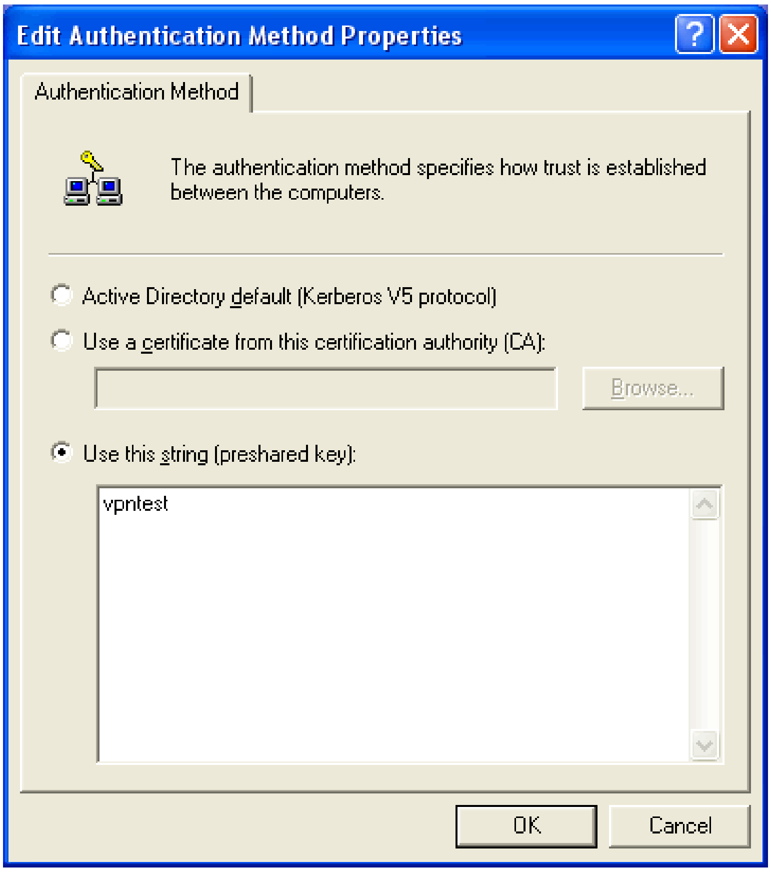


Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Kerberos	

39. Click on **Edit** button



The authentication method specifies how trust is established between the computers.

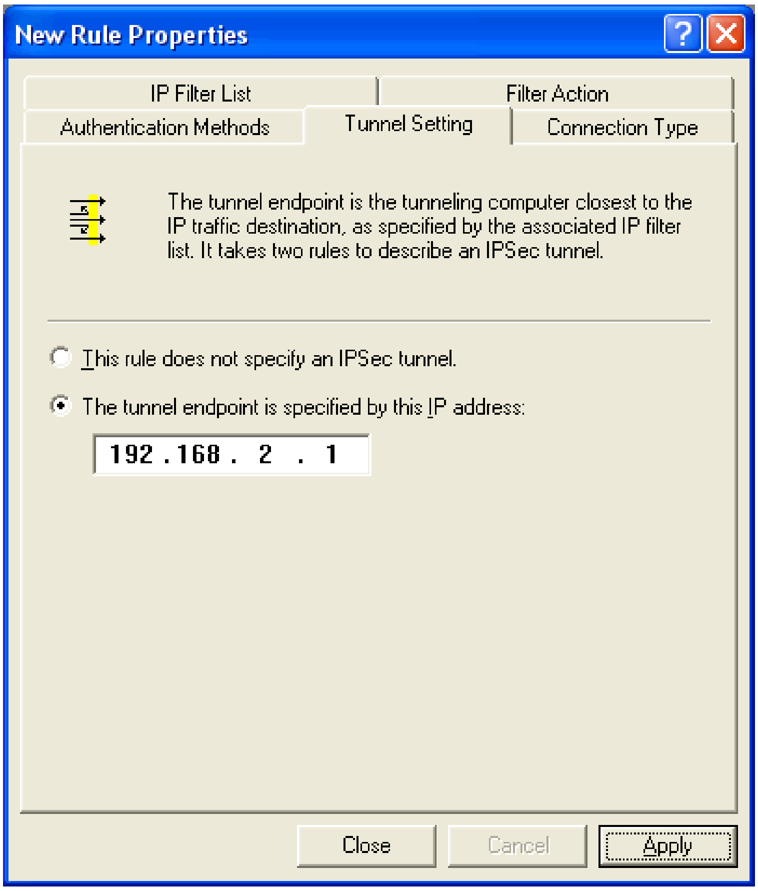
○ Active Directory default (Kerberos V5 protocol)

○ Use a certificate from this certification authority (CA):

● Use this string (preshared key):

vpntest

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



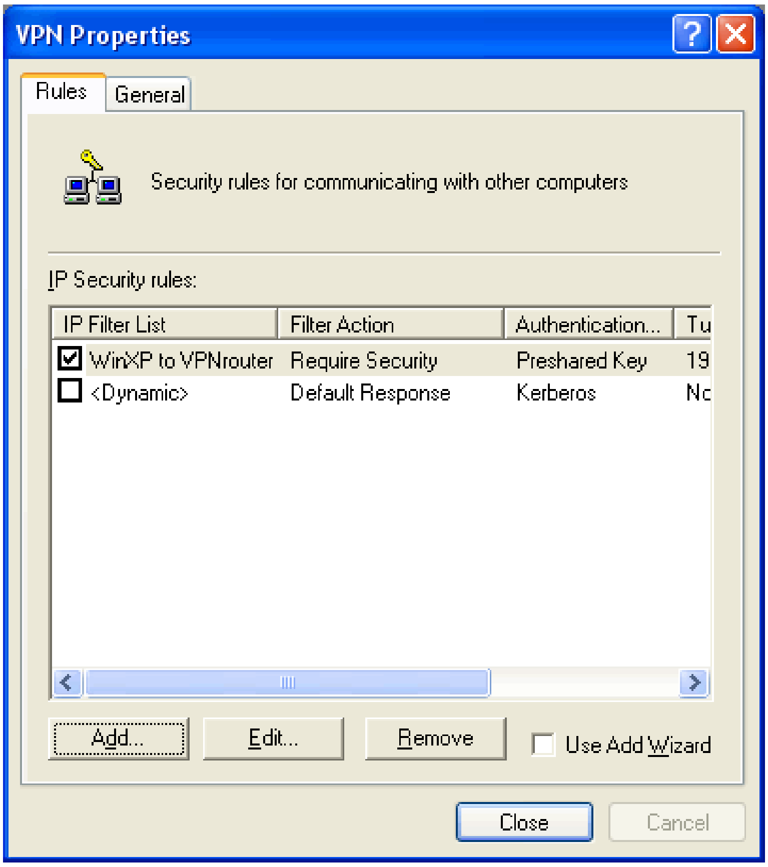
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP address:

192 . 168 . 2 . 1

43. Click on The tunnel endpoint is specified by this IP address
44. Enter the WAN IP address of destination endpoint of VPN tunnel. (in this case, it's 192.168.2.1)
45. Click on **Apply** and then **OK** buttons



VPN Properties

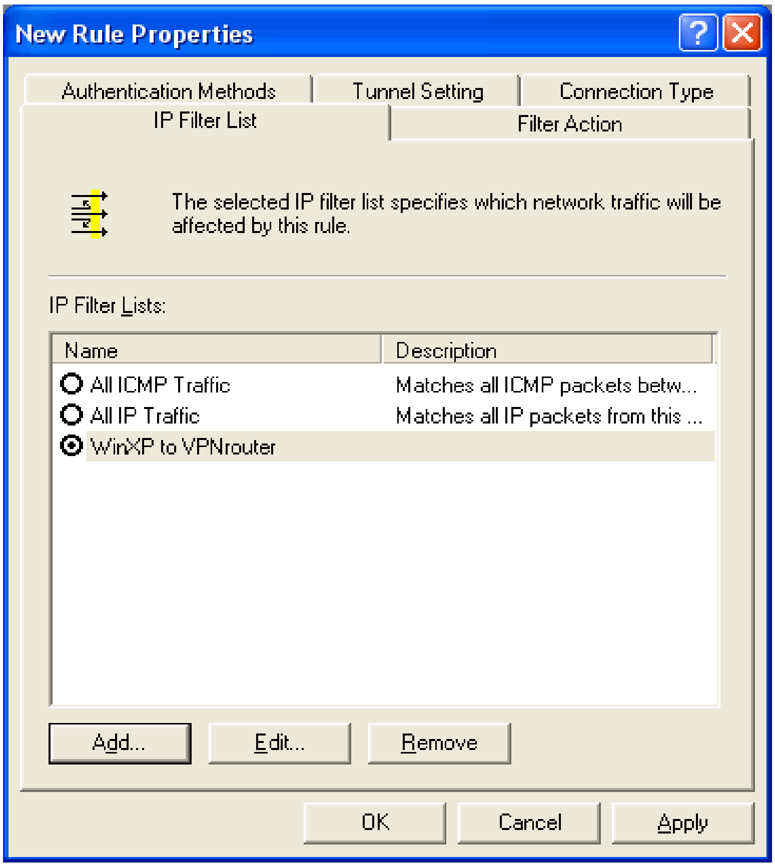
Rules | General

Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ WinXP to VPNrouter	Require Security	Preshared Key	19
□ <Dynamic>	Default Response	Kerberos	Nc

46. Click on pre-defined IP Security rules. (in this case it's WinXP to VPNtunnel)
47. Click on **Add** button



New Rule Properties

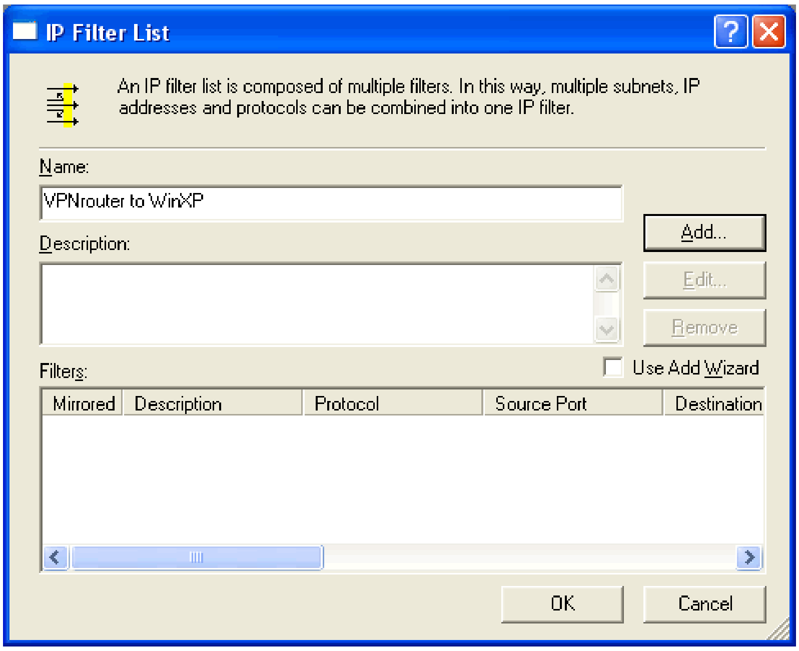
Authentication Methods | Tunnel Setting | Connection Type | IP Filter List | Filter Action

The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
● WinXP to VPNrouter	

48. Click on **Add** button



IP Filter List

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: VPNrouter to WinXP

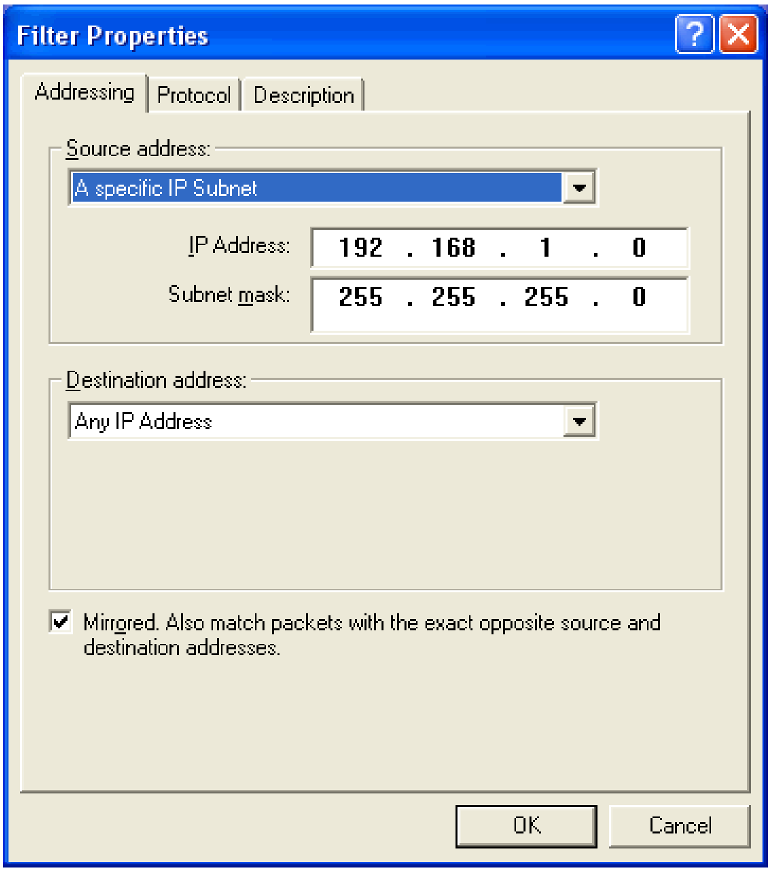
Description:

□ Use Add Wizard

Filters:

Mirrored	Description	Protocol	Source Port	Destination

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



Filter Properties

Source address: A specific IP Subnet

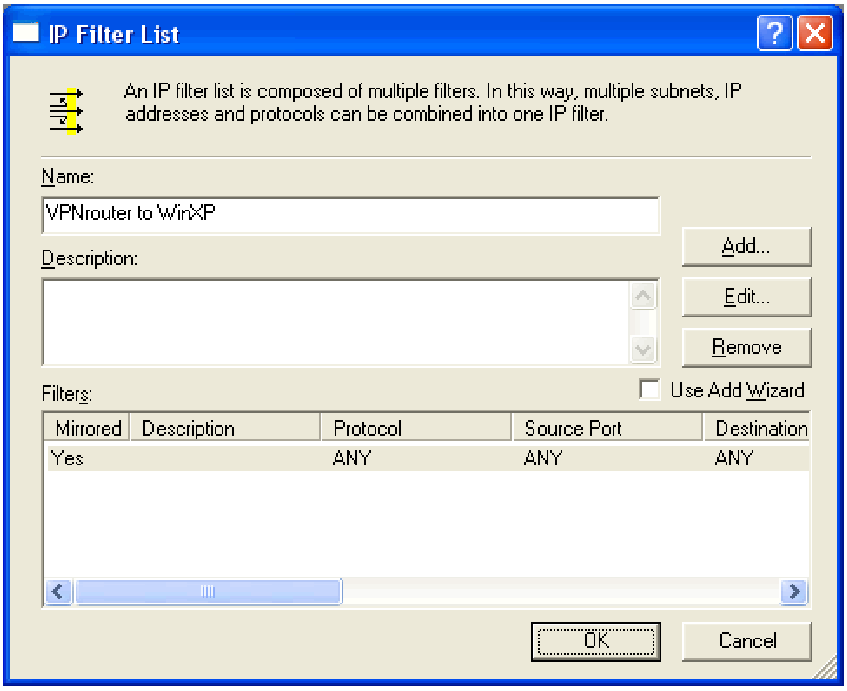
IP Address: 192 . 168 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

Destination address: Any IP Address

☑ Mirrored. Also match packets with the exact opposite source and destination addresses.

51. From Source address pull-down window, select **A specific IP Subnet**
52. Enter destination IP address and its subnet mask. (in this case, the destination IP is 192.168.1.0/255.255. 255.0) 。
53. From Destination address pull-down window, select **Any IP Address**.
54. Check the box of Mirrored. Also match packets with the exact opposite source and destination addresses.
55. Click on **OK** button



IP Filter List

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

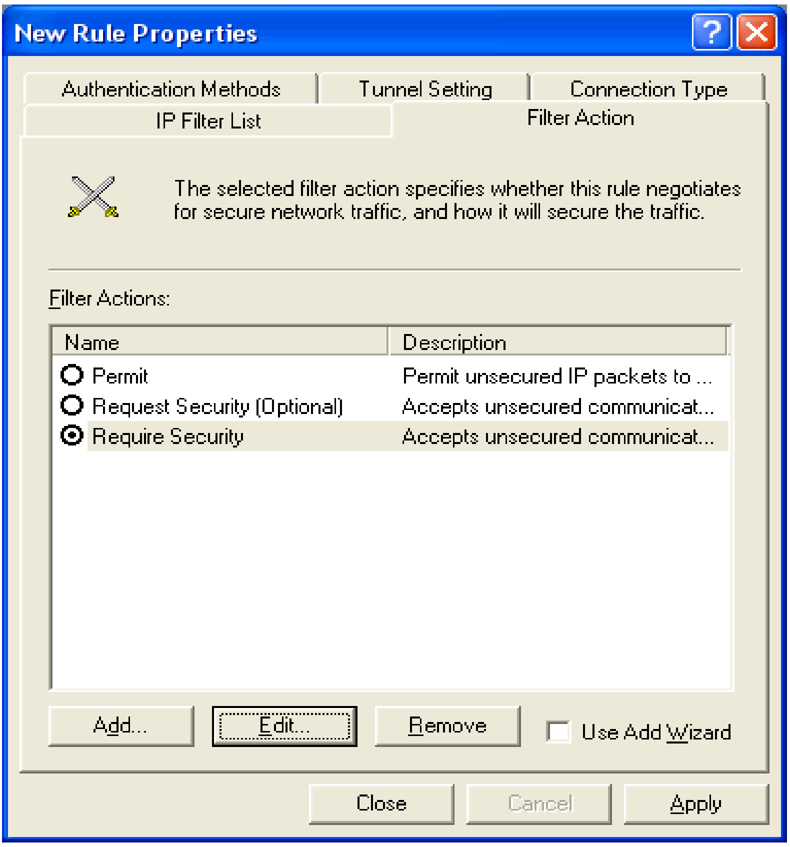
Name: VPNrouter to WinXP

Description:

Filters:

Mirrored	Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY

56. Click on **OK** button



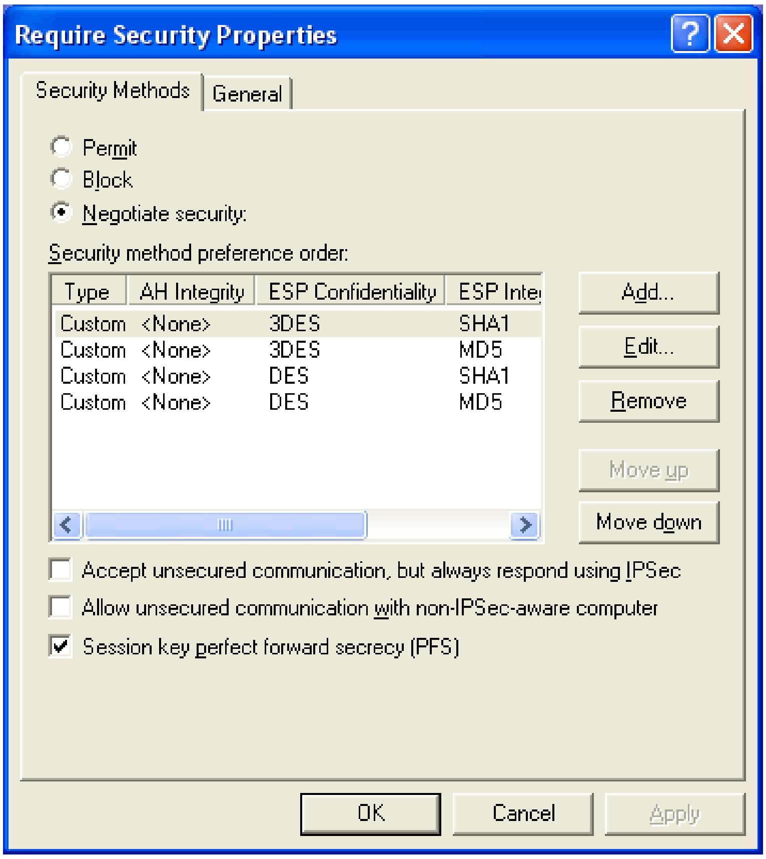
New Rule Properties

The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

Name	Description
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
● Require Security	Accepts unsecured communicat...

57. Select **Filter Action** tab on top
58. Click on Require Security
59. Click on **Edit** button



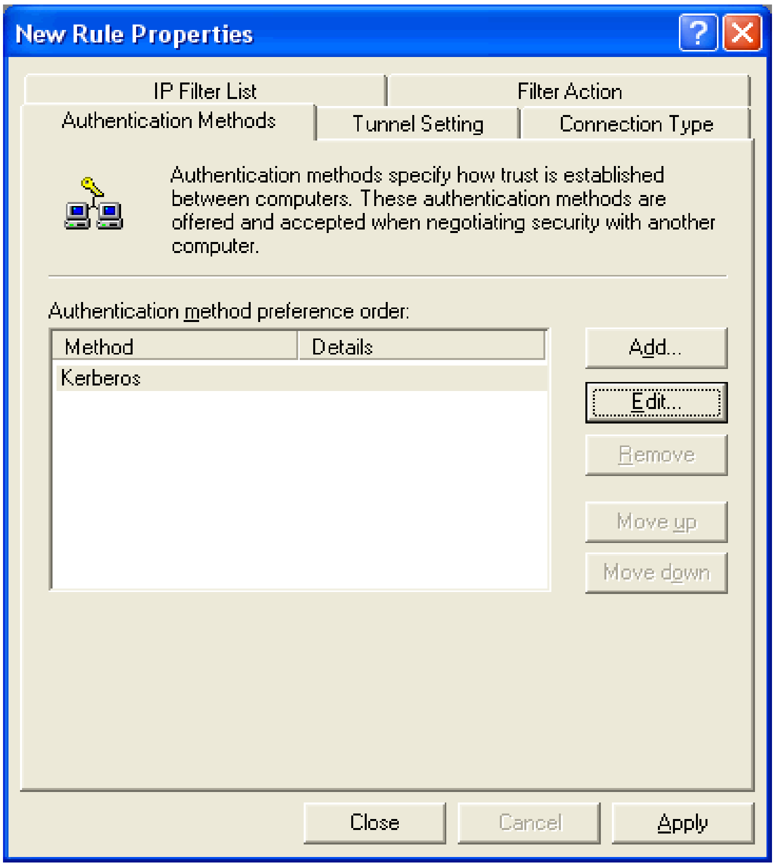
○ Permit
○ Block
● Negotiate security:

Security method preference order:

Type	AH Integrity	ESP Confidentiality	ESP Inte
Custom	<None>	3DES	SHA1
Custom	<None>	3DES	MD5
Custom	<None>	DES	SHA1
Custom	<None>	DES	MD5

□ Accept unsecured communication, but always respond using IPSec
□ Allow unsecured communication with non-IPSec-aware computer
☑ Session key perfect forward secrecy (PFS)

60. Click on Negotiate security
61. Cancel the check box of Accept unsecured communication, but always respond using IPSec
62. Tick the box of session key **perfect forward secrecy (PFS)**.
63. Click on **OK** button

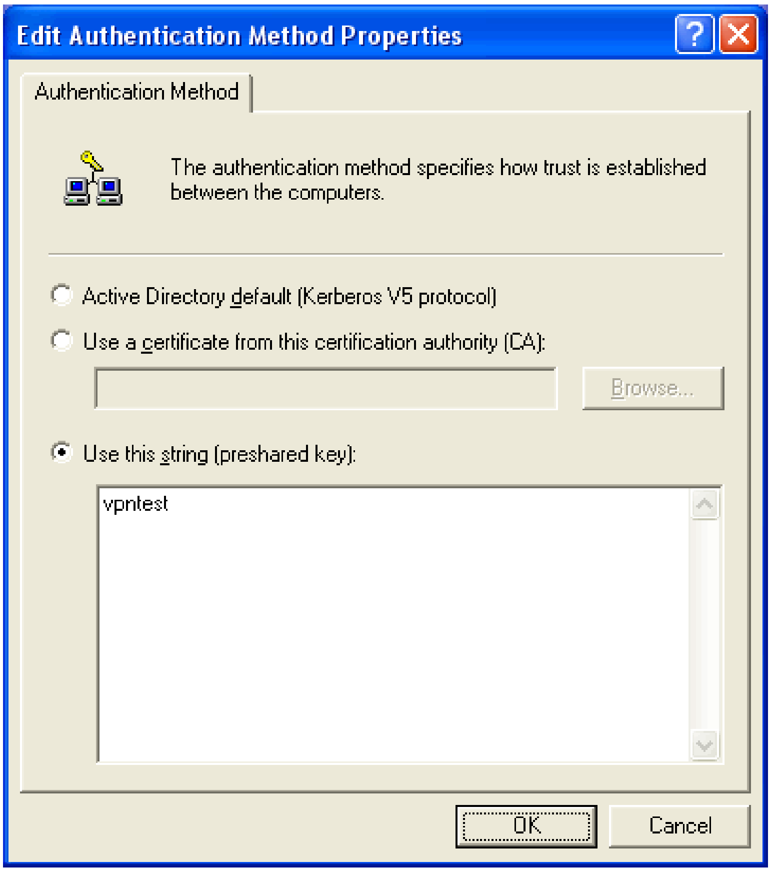


Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Kerberos	

64. Click on **Edit** button



Edit Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

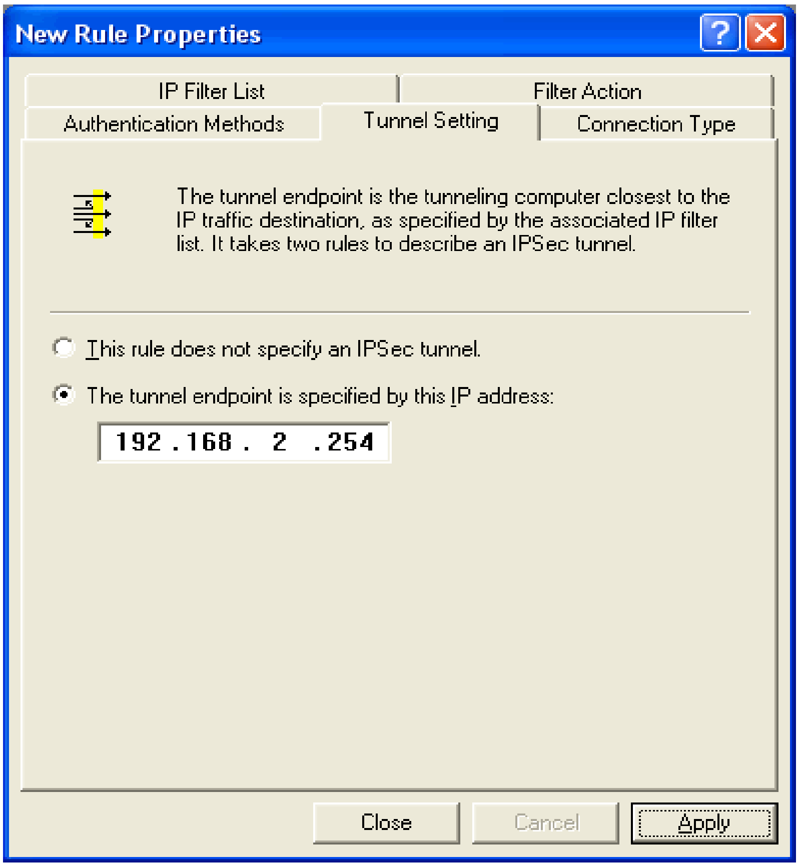
○ Active Directory default (Kerberos V5 protocol)

○ Use a certificate from this certification authority (CA):

● Use this string (preshared key):

vpntest

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



New Rule Properties

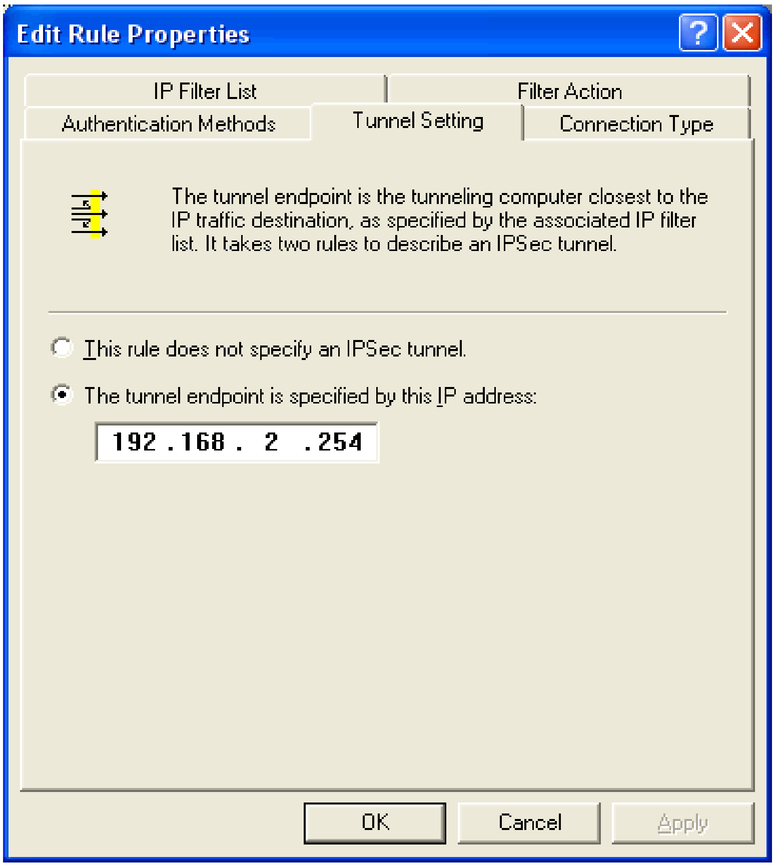
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP address:

192 . 168 . 2 . 254

68. Click on The tunnel endpoint is specified by this IP address
69. Enter the WAN IP address of your Windows XP PC (in this case, it's 192.168.2.254)
70. Click on **Apply** and then **Close** buttons



Edit Rule Properties

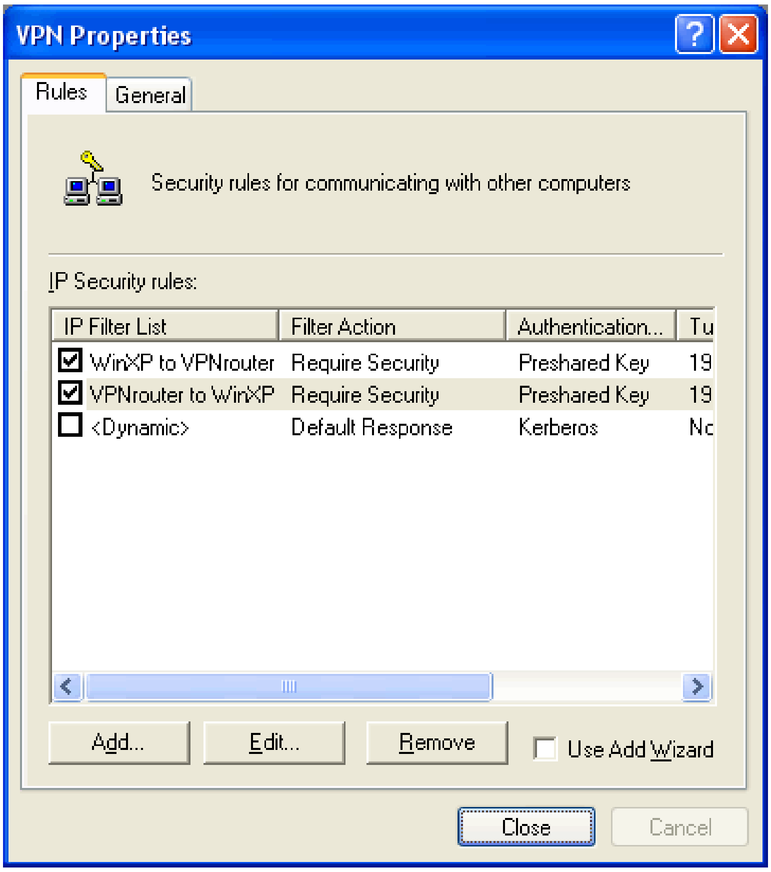
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP address:

192 .168 . 2 .254

71. Click on **OK** button



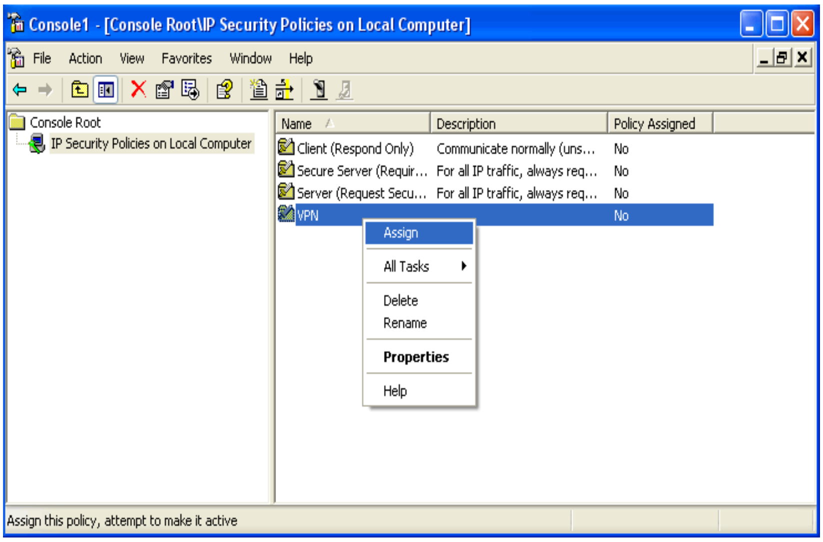
VPN Properties

Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ WinXP to VPNrouter	Require Security	Preshared Key	19
☑ VPNrouter to WinXP	Require Security	Preshared Key	19
□ <Dynamic>	Default Response	Kerberos	Nc

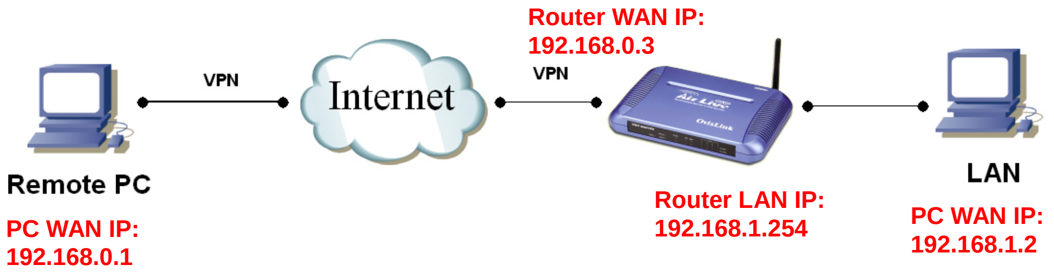
72. Make sure you have checked the box of both IP Security rules you configured in previous section. In this case, they are WinXP to VPNrouter and VPNrouter to WinXP.
73. Click on **Close** button


Console1 - [Console Root\IP Security Policies on Local Computer]
File Action View Favorites Window Help
Console Root
IP Security Policies on Local Computer
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
VPN
No
Assign
All Tasks
Delete
Rename
Properties
Help
Assign this policy, attempt to make it active

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

After successfully configure the Windows XP, you should be able to ping the network device at remote side. However, if the remote device is a Windows XP, the ping will get timeout due to Windows XP firewall setup. You can use *Control Panel* to turn off firewall temporary to enable the ping echo back. Remember to turn the firewall back on after the VPN successfully built up.

EXAMPLE 4: USING L2TP TO CONNECT REMOTE PC TO LOCAL LAN



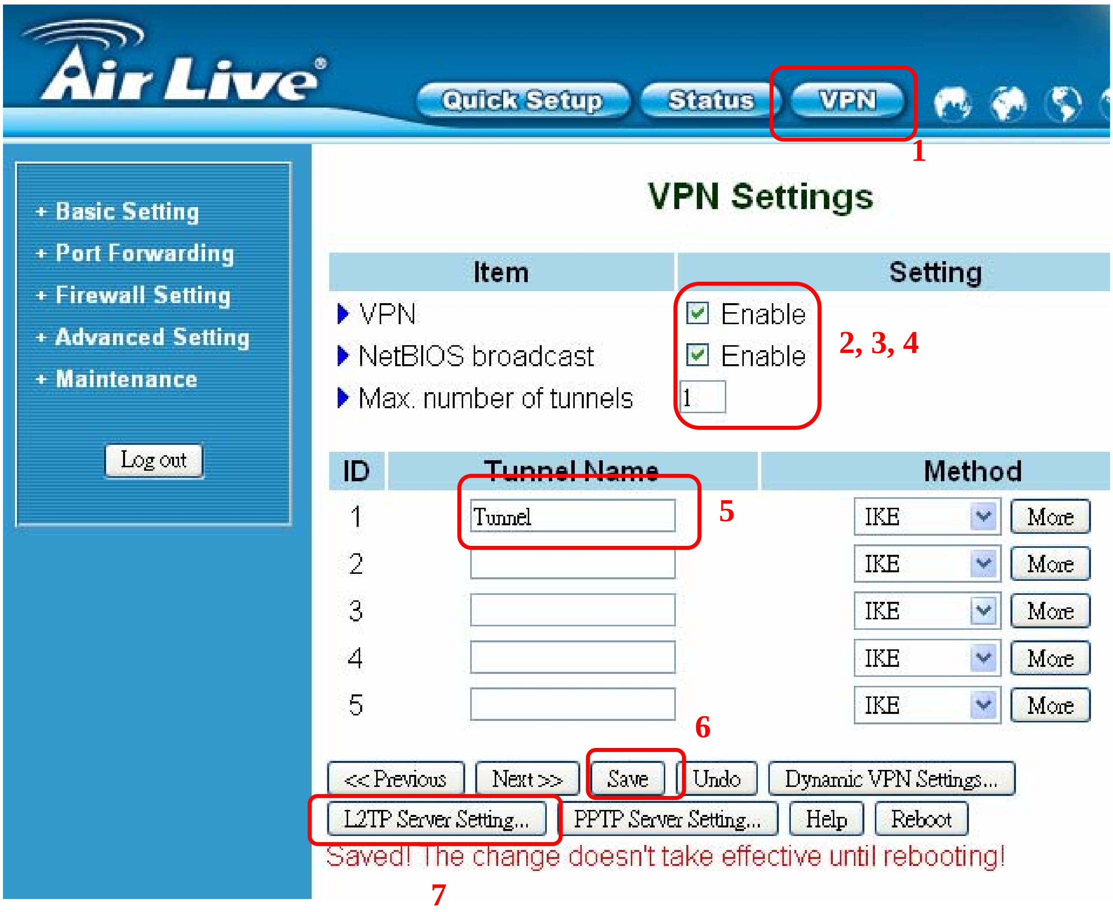
In this example, we will demonstrate how to setup a VPN connection between a remote PC and the WL/IP-8000VPN using the L2TP server function. Looking at the diagram above, the Remote PC has real IP address of 192.168.0.1. If this remote PC is connected to Internet through an IP sharing router, please make sure that router supports L2TP pass through function. In this example, the WL/IP-8000VPN's WAN IP address is 192.168.0.3. You can also register the WL/IP-8000VPN with dynamic DNS if you don't have a fixed IP address. Finally, the local LAN has IP address 192.168.1.x. Please note that if the Remote PC is behind a router, the remote PC's IP subnet must be different from the local IP subnet.

The Router's L2TP server can support 5 L2TP VPN user's accounts.

In the real world Internet connection, Remote PC would not directly connect to the router, which is WL/IP-8000 VPN here. You need to set the correct Remote Gateway both in WL/IP-8000VPN WAN port and Remote PC for your own environment.

Router's LAN, User's LAN, and PPTP virtual LAN must all have different LAN number. Router's LAN is 192.168.1.x, user's LAN is 192.168.0.y, and virtual LAN is 10.0.1.z in this case.

Router Setup



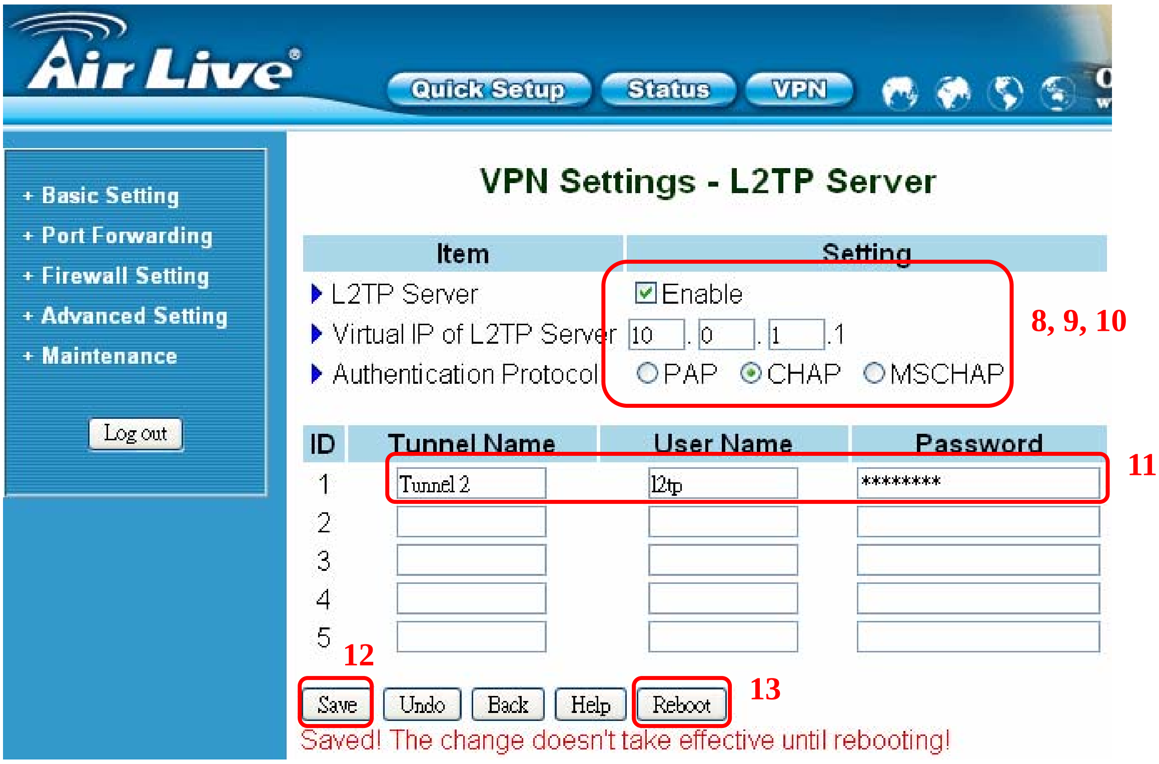
VPN Settings

Item	Setting
VPN	☑ Enable
NetBIOS broadcast	☑ Enable
Max. number of tunnels	1

ID	Tunnel Name	Method	
1	Tunnel	IKE	More
2		IKE	More
3		IKE	More
4		IKE	More
5		IKE	More

Saved! The change doesn't take effective until rebooting!

1. Click on **VPN** button on top of this page
2. Check VPN **Enable** checkbox.
3. Check NetBIOS broadcast **Enable** checkbox.
4. Enter the Max number of tunnels as **1**
5. Enter the Tunnel Name as **Tunnel**
6. Click on **Save** button at the bottom of the page (no need to reboot now)
7. Click on **L2TP Server Setting** button



VPN Settings - L2TP Server

Item	Setting
L2TP Server	☑ Enable
Virtual IP of L2TP Server	10 . 0 . 1 .1
Authentication Protocol	○ PAP ● CHAP ○ MSCHAP

ID	Tunnel Name	User Name	Password
1	Tunnel 2	l2tp	********
2			
3			
4			
5			

Saved! The change doesn't take effective until rebooting!

8. Check L2TP Server **Enable** checkbox.
9. Change the *Virtual IP of L2TP Server* address, if needed
10. Change the *Authentication Protocol* to **CHAP**
11. Enter the *Tunnel Name, User Name,* and *Password*.
12. Click on **Save** button
13. Click on **Reboot** button. When asked to reboot shown in a pop-up message, click **OK** to reboot and let the settings take effect.

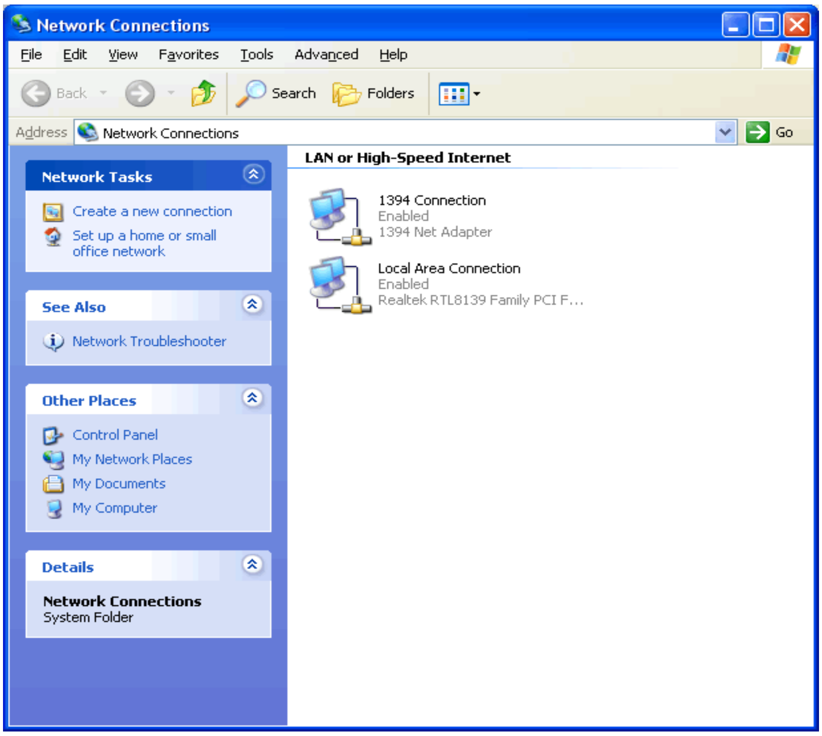
Remote PC Setup (Using Windows XP VPN Client)

In case of Windows XP, the following steps shows L2TP client setting.

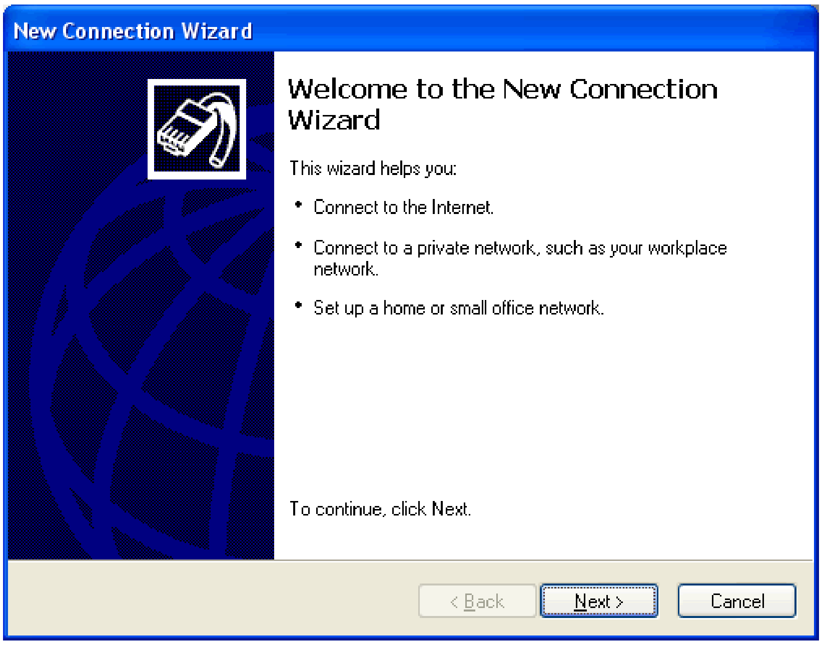
Due to the limitation of L2TP protocol definition, we will need to disable IPSec in Windows remote access client. Please download file **disableipsec.zip** from Internet. Go to the link below:

http://support.iglou.com/fom-serve/cache/473.html

Unzip it and double click on the file **DisableIPSEC.reg**. Click on **Yes** button, when the pop-up message asked if you really want to add the registry item.



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



New Connection Wizard

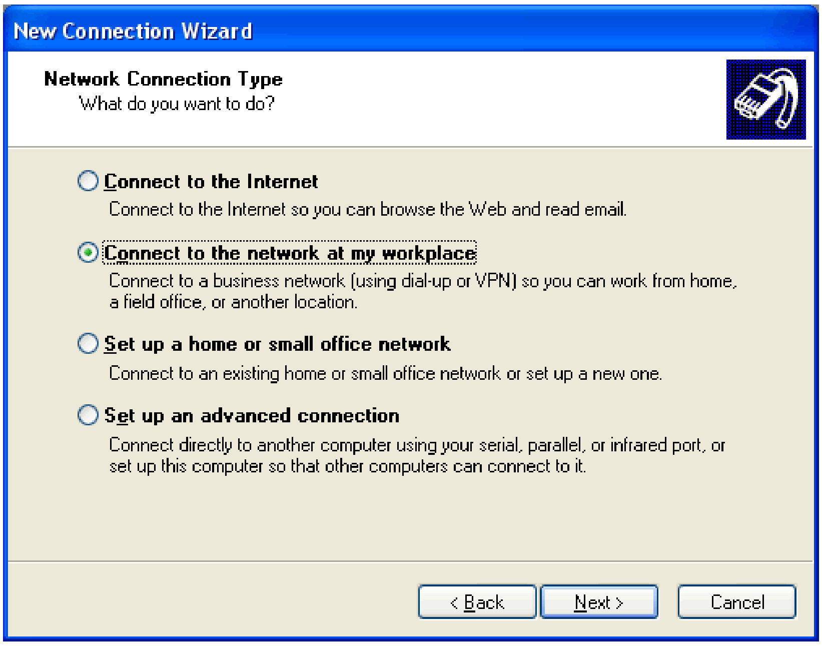
Welcome to the New Connection Wizard

This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.
- Set up a home or small office network.

To continue, click Next.

3. Click on **Next** button



New Connection Wizard

Network Connection Type
What do you want to do?

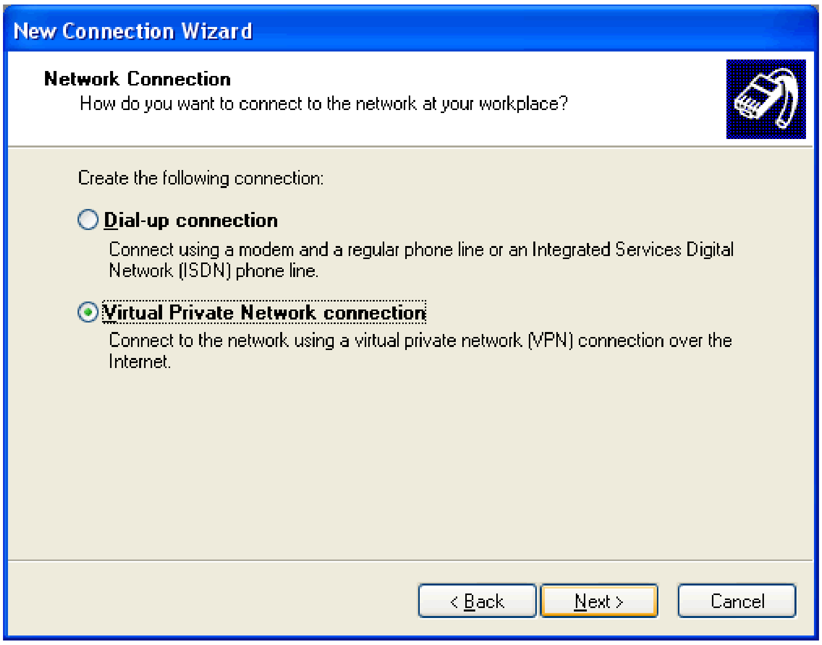
○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

● **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up a home or small office network**
Connect to an existing home or small office network or set up a new one.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

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



Network Connection

How do you want to connect to the network at your workplace?

Create the following connection:

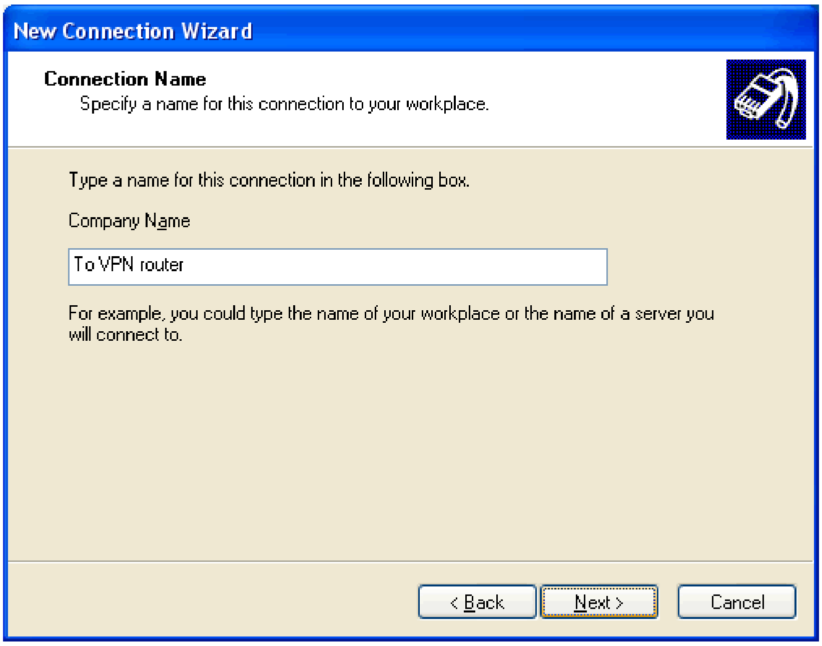
○ **Dial-up connection**

Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

● **Virtual Private Network connection**

Connect to the network using a virtual private network (VPN) connection over the Internet.

6. Click on Virtual Private Network connection
7. Click on **Next** button



Connection Name

Specify a name for this connection to your workplace.

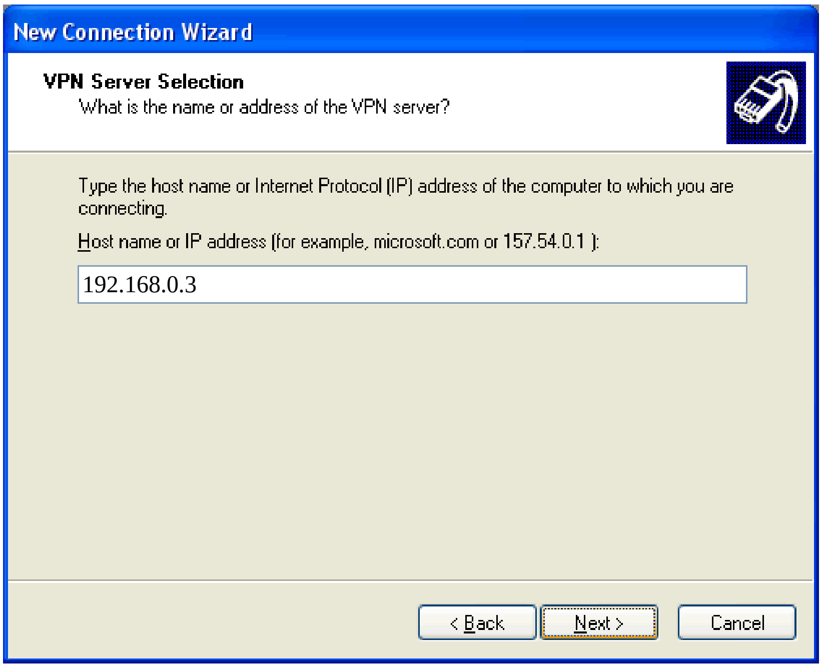
Type a name for this connection in the following box.

Company Name

To VPN router

For example, you could type the name of your workplace or the name of a server you will connect to.

8. Enter the name of this VPN connection. In this case, the name is To VPN router.
9. Click on **Next**



New Connection Wizard

VPN Server Selection

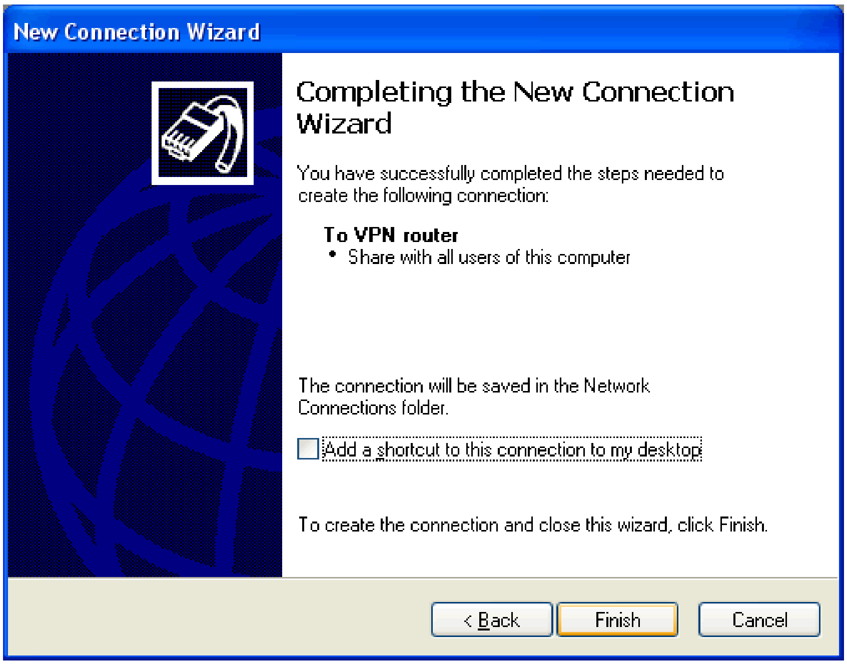
What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

192.168.0.3

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



New Connection Wizard

Completing the New Connection Wizard

You have successfully completed the steps needed to create the following connection:

To VPN router

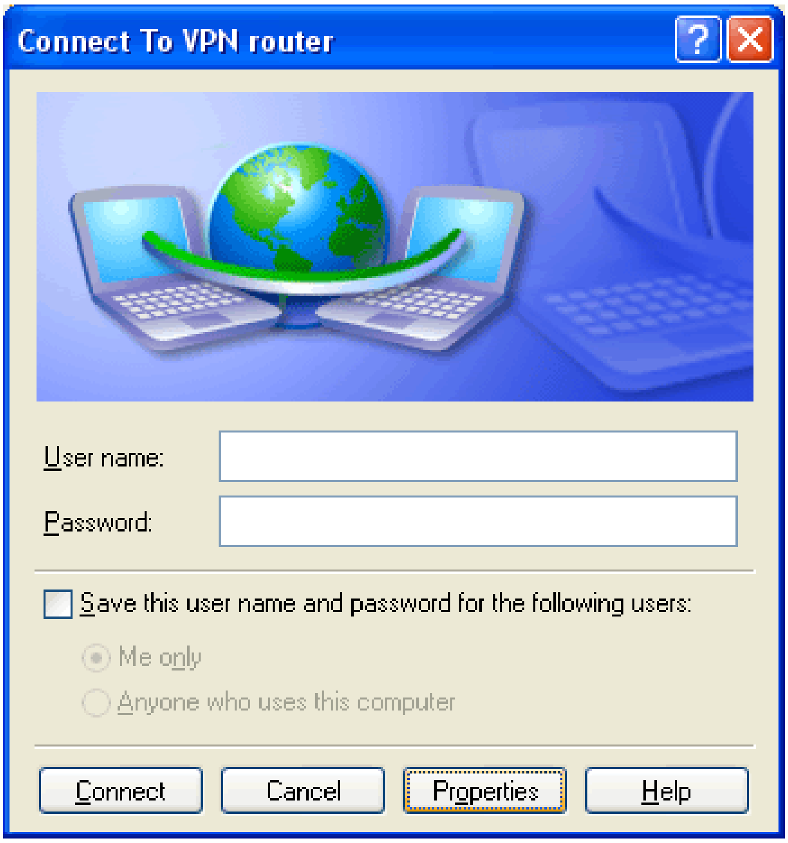
- Share with all users of this computer

The connection will be saved in the Network Connections folder.

□ Add a shortcut to this connection to my desktop

To create the connection and close this wizard, click Finish.

12. If you would like this connection to 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.



Connect To VPN router

User name:

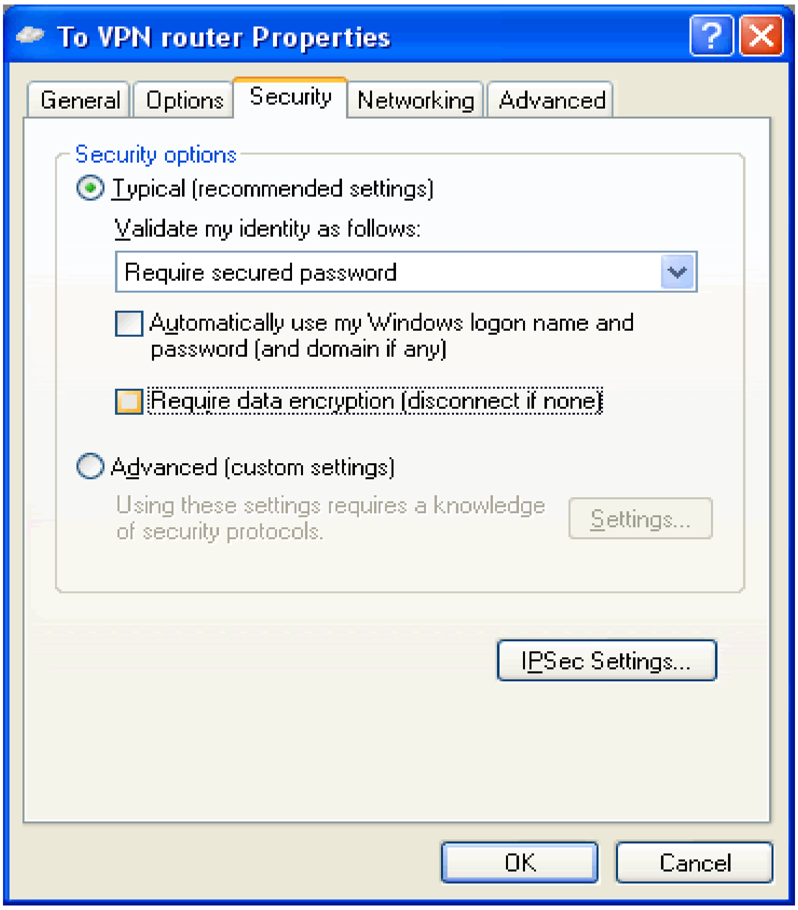
Password:

□ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

14. Click on **Properties** button



To VPN router Properties

Security options

● Typical (recommended settings)

Validate my identity as follows:

Require secured password

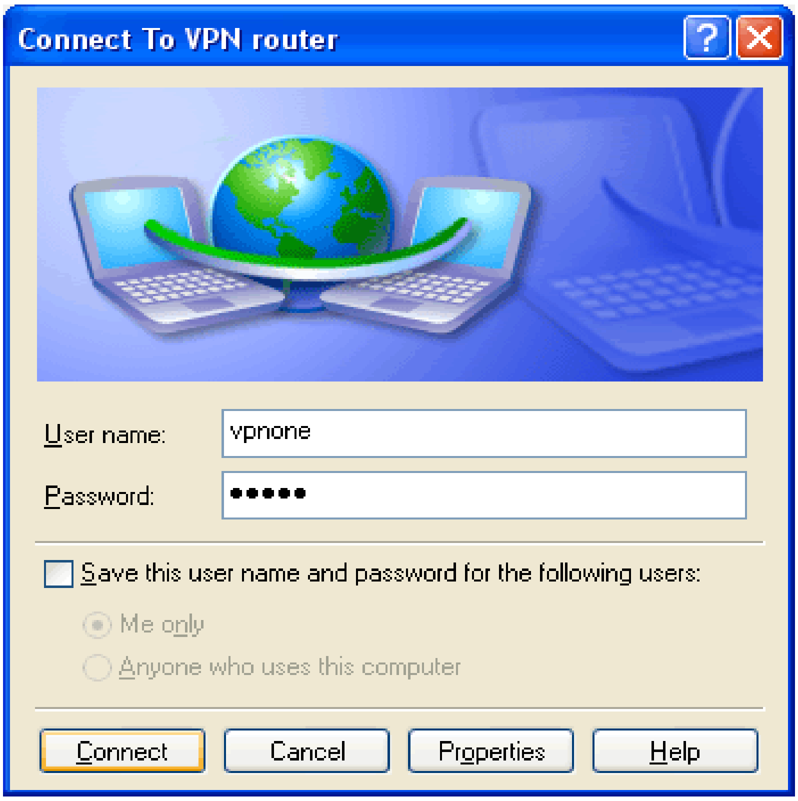
□ Automatically use my Windows logon name and password (and domain if any)

□ Require data encryption (disconnect if none)

○ Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

15. Un-tick or cancel the check box of **Require data encryption** (disconnect if none)
16. Click on **OK**



Connect To VPN router

User name: vpnone

Password: •••••

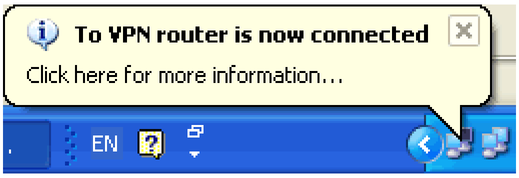
□ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

17. Enter your User name and Password
18. Click on **Connect** button.

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



To VPN router is now connected

Click here for more information...

You can also access to your web-based management page from your router and go to L2TP server setting page. From the bottom of the page, you will see the current L2TP VPN connection status from Client Management section.

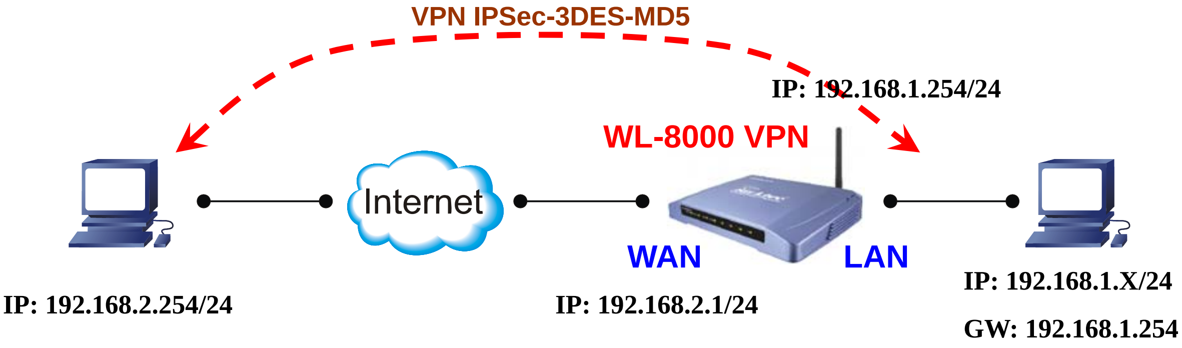
On Client Management section, if Disconnect check box is ticked and click on Set, it will allow L2TP disconnection. If the Reset button is clicked, L2TP disconnection will be cancelled and the L2TP will be reconnected again.

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

EXAMPLE 5: DYNAMIC VPN APPLICATION EXAMPLE

This example demonstrates the configuration for Dynamic VPN.
The previous four VPN configurations are based on an assumption that we will configure both ends of the VPN. In the real world, it is almost impossible asking MIS people to set up VPN connections for every individual in the central site. To let central site VPN accepts any VPN connection request from worldwide, a Dynamic VPN setup is needed.

We will use the similar environment in example 3.

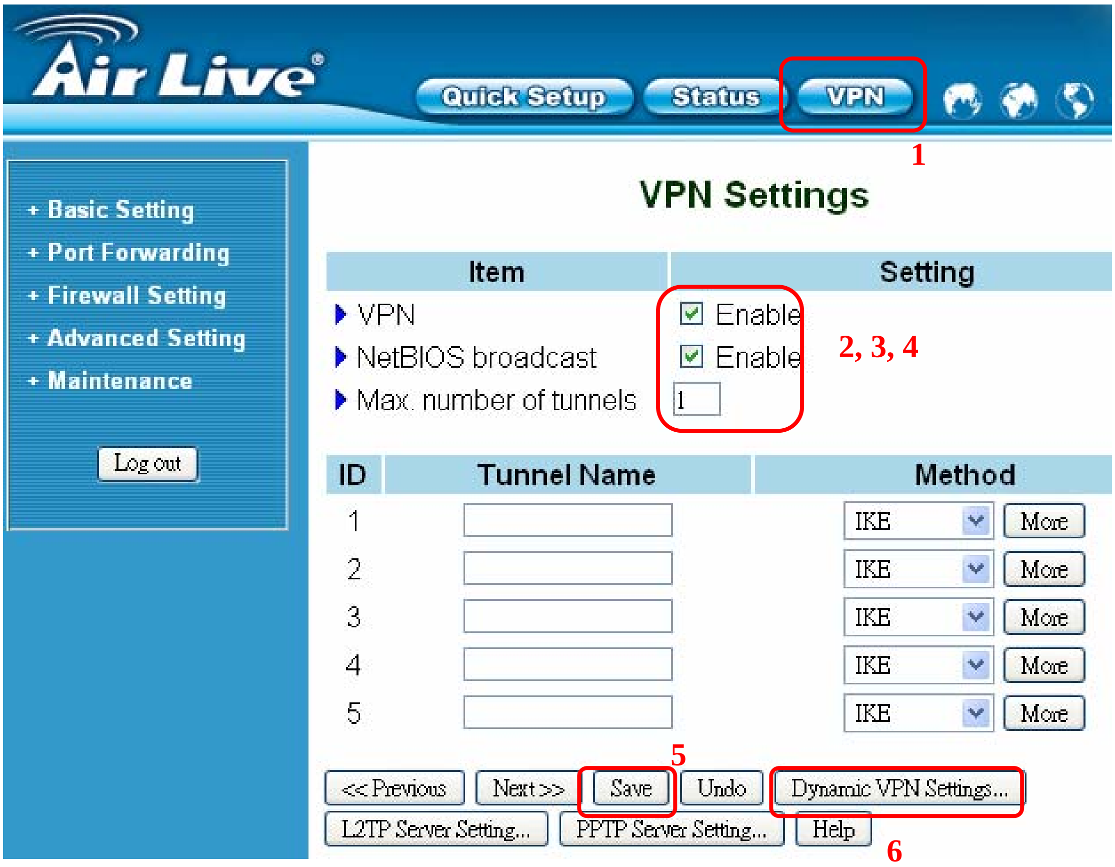


The only difference is: in this case, we will not care about the remote site IP address and subnet mask. Central site does not need remote site IP address information.

We will use TheGreenBow VPN client for this case.

In the real world Internet connection, Remote PC would not directly connect to the router, which is WL/IP-8000 VPN here. You need to set the correct Remote Gateway both in WL/IP-8000VPN WAN port and Remote PC for your own environment.

Router's Dynamic VPN with IPSec Setup

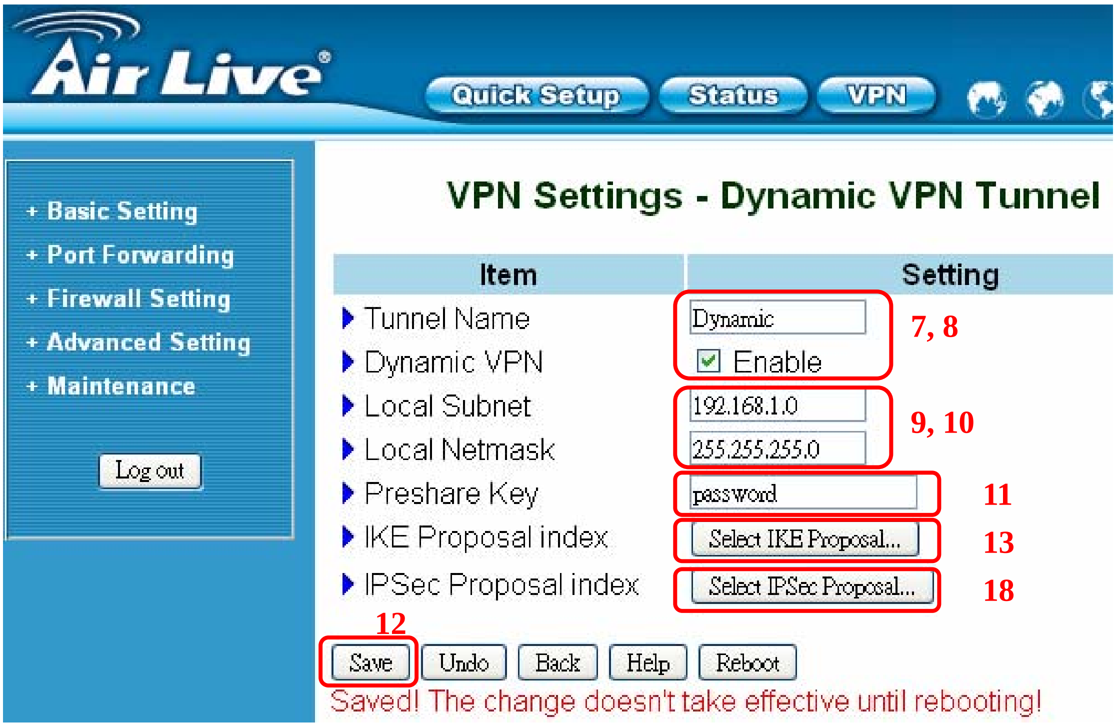


VPN Settings

Item	Setting
VPN	☑ Enable
NetBIOS broadcast	☑ Enable
Max. number of tunnels	1

ID	Tunnel Name	Method	
1		IKE	More
2		IKE	More
3		IKE	More
4		IKE	More
5		IKE	More

1. Click on **VPN** button on top of this page
2. Check VPN **Enable** checkbox.
3. Check NetBIOS broadcast **Enable** checkbox.
4. Enter the Max number of tunnels as **1**
5. Click on **Save** button at the bottom of the page (no need to reboot now)
6. Click on **Dynamic VPN Settings** button

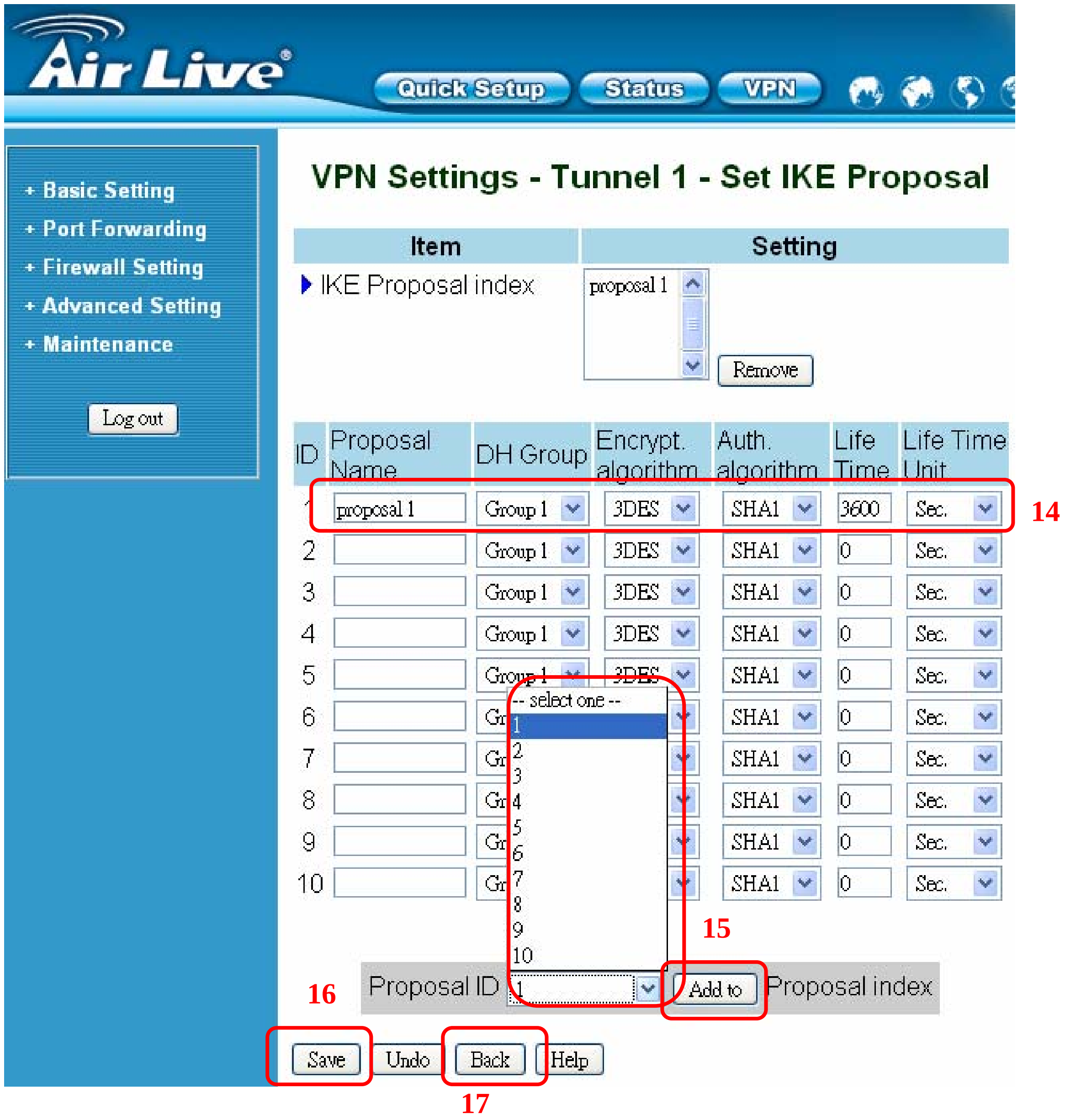


VPN Settings - Dynamic VPN Tunnel

Item	Setting
Tunnel Name	Dynamic
Dynamic VPN	☑ Enable
Local Subnet	192.168.1.0
Local Netmask	255.255.255.0
Preshare Key	password
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Saved! The change doesn't take effective until rebooting!

7. Enter *Tunnel Name*
8. **Enable** *Dynamic VPN* by clicking on the check box
9. Enter *Local subnet*
10. Enter *Local Netmask*
11. Enter *Pre-share Key* (Note: the same key will be used in the VPN client)
12. Click on **Save** button (no need to reboot for now)
13. Click on **Select IKE Proposal** button



VPN Settings - Tunnel 1 - Set IKE Proposal

Item	Setting
IKE Proposal index	proposal 1 Remove

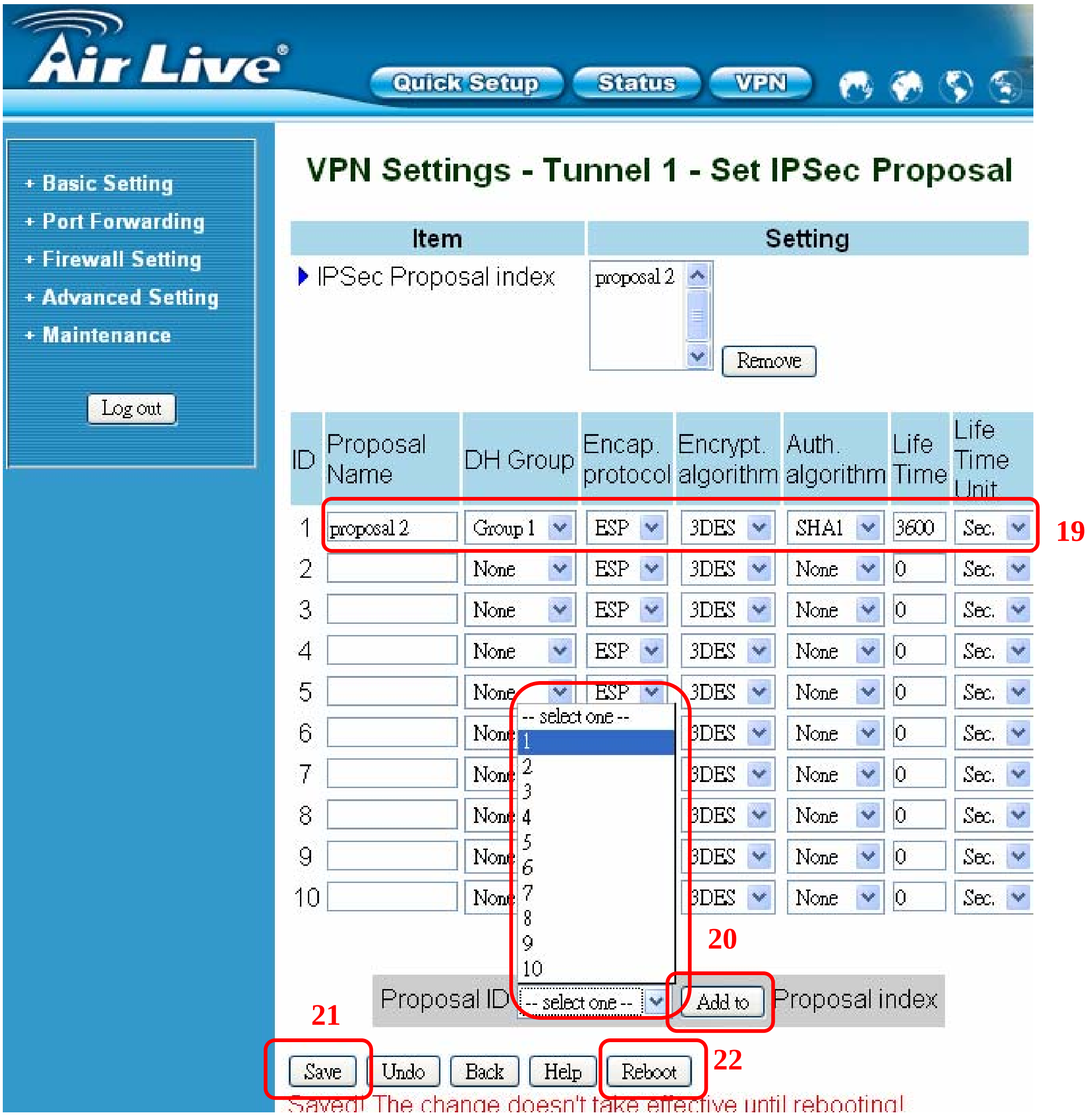
ID	Proposal Name	DH Group	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	proposal 1	Group 1	3DES	SHA1	3600	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Gr		SHA1	0	Sec.
7		Gr		SHA1	0	Sec.
8		Gr		SHA1	0	Sec.
9		Gr		SHA1	0	Sec.
10		Gr		SHA1	0	Sec.

-- select one --
1
2
3
4
5
6
7
8
9
10

Proposal ID 1 Add to Proposal index

Save Undo Back Help

14. Enter *Proposal Name,* key *Life Time*, and change any other settings, if needed, for proposal *ID 1*. (Note that you must use **Group 2** with **3DES**, or **Group 1** with **DES** if you use default Windows XP IPSec client)
15. Select *Proposal ID* ***1*** and click button **Add to** *Proposal index*. You can add maximal 4 proposals in total from the IKE proposal index.
16. Click on **Save** button (no need to reboot now)
17. Click on **Back** button (go back to the screen on this page above)
18. Click on **Select IPSec Proposal** button (in **Dynamic VPN Settings** page)



VPN Settings - Tunnel 1 - Set IPSec Proposal

Item	Setting
IPSec Proposal index	proposal 2

ID	Proposal Name	DH Group	Encap. protocol	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	proposal 2	Group 1	ESP	3DES	SHA1	3600	Sec.
2		None	ESP	3DES	None	0	Sec.
3		None	ESP	3DES	None	0	Sec.
4		None	ESP	3DES	None	0	Sec.
5		None	ESP	3DES	None	0	Sec.
6		None		3DES	None	0	Sec.
7		None		3DES	None	0	Sec.
8		None		3DES	None	0	Sec.
9		None		3DES	None	0	Sec.
10		None		3DES	None	0	Sec.

-- select one --
1
2
3
4
5
6
7
8
9
10

Proposal ID -- select one -- Add to Proposal index

Saved! The change doesn't take effective until rebooting!

19. Enter IPSec *Proposal Name*, key *Life Time*, select *DH Group*, *Auth algorithm*, and change any other settings, if needed, for IPSec proposal *ID 1*. (Note that you must use **Group 2** with **3DES**, or **Group 1** with **DES** if you use default Windows XP IPSec client)
20. Select *Proposal ID **1*** and click button **Add to** *Proposal index*. You can add maximal 4 proposals in total from the IKE proposal index.
21. Click on **Save** button
22. Click on **Reboot** button. When asked to reboot shown in a pop-up message, click **OK** to reboot and let the settings take effect.

Set up TheGreenBow VPN client

Before start to set up the VPN client, it is assumed that

(1) your computer is able to connect to Internet,
(2) the Internet connection allows IPSec pass through, and
(3) you have TheGreenBow VPN client installed in your PC.

You can get TheGreenBow VPN client from the following link.

http://www.theTheGreenBow.com/vpn_down.html

You should be able to use the latest TheGreenBow VPN client.

The tested TheGreenBow VPN client is 3.00.010.
Note: after install TheGreenBow VPN client, Windows XP IPSec is disabled. If you need to use Windows XP IPSec, you need to uninstall TheGreenBow VPN client.

No matter the VPN is dynamic or not, the client side always needs to have some detail information including

central site gateway,
central site LAN subnet, and
central site LAN net mask.

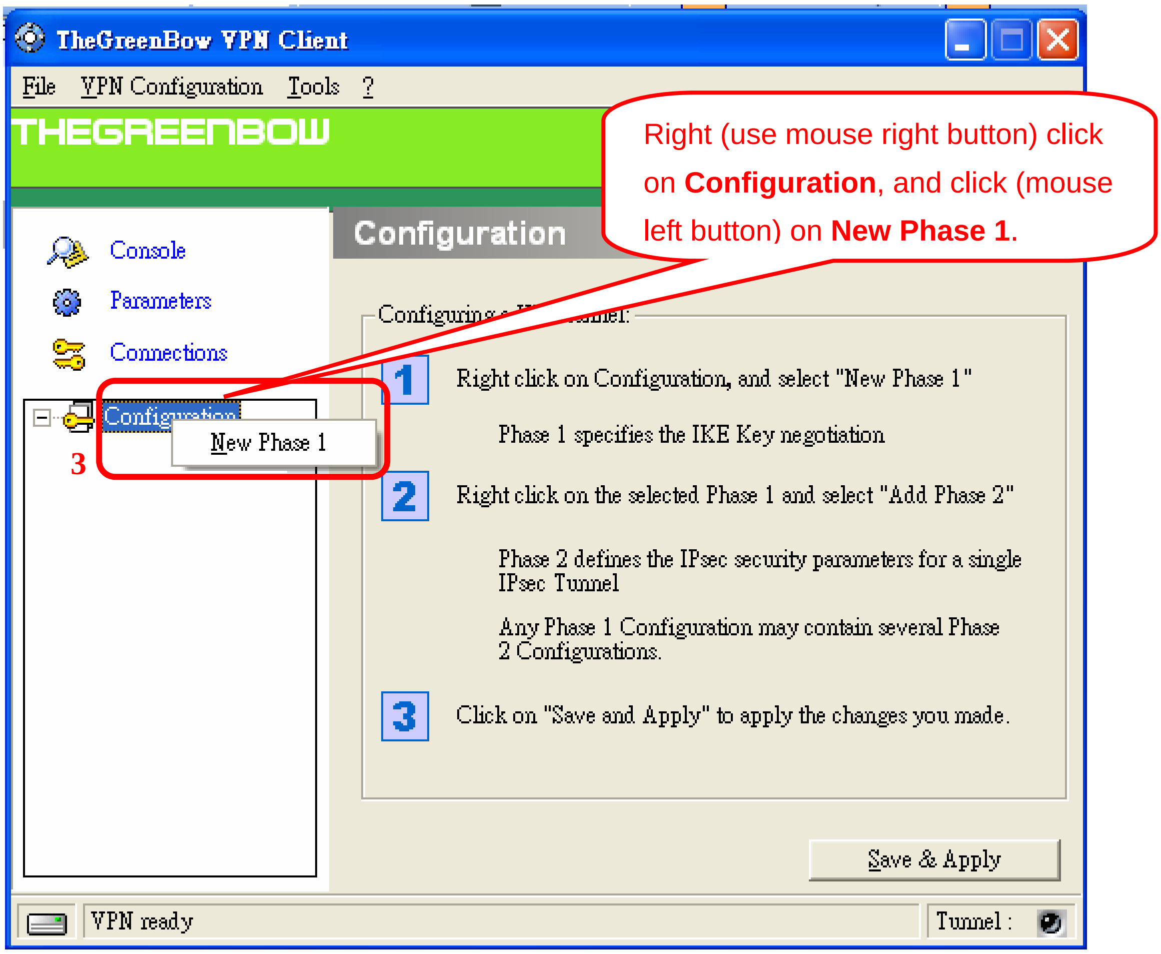
The example below has

central site gateway: **192.168.122.195**
central site LAN subnet: **192.168.122.0**
central site LAN net mask: **255.255.255.0**.

Please use the following steps to set up your TheGreenBow VPN client.

1. Install TheGreenBow VPN client in your PC.
2. Launch TheGreenBow VPN client.
3. Use mouse right button to click on **Configuration**, and add a **New Phase 1** VPN connection.

Note: in TheGreenBow VPN client examples, we have changed IPSec client address from 192.168.2.254 to 192.168.122.x (x means doesn't matter in this configuration) and IPSec router from 192.168.2.1 to 192.168.122.195. The remote LAN are also changed from 192.168.1.x to 192.168.21.x.



Right (use mouse right button) click on **Configuration**, and click (mouse left button) on **New Phase 1**.

Configuring a VPN Tunnel:

1 Right click on Configuration, and select "New Phase 1"

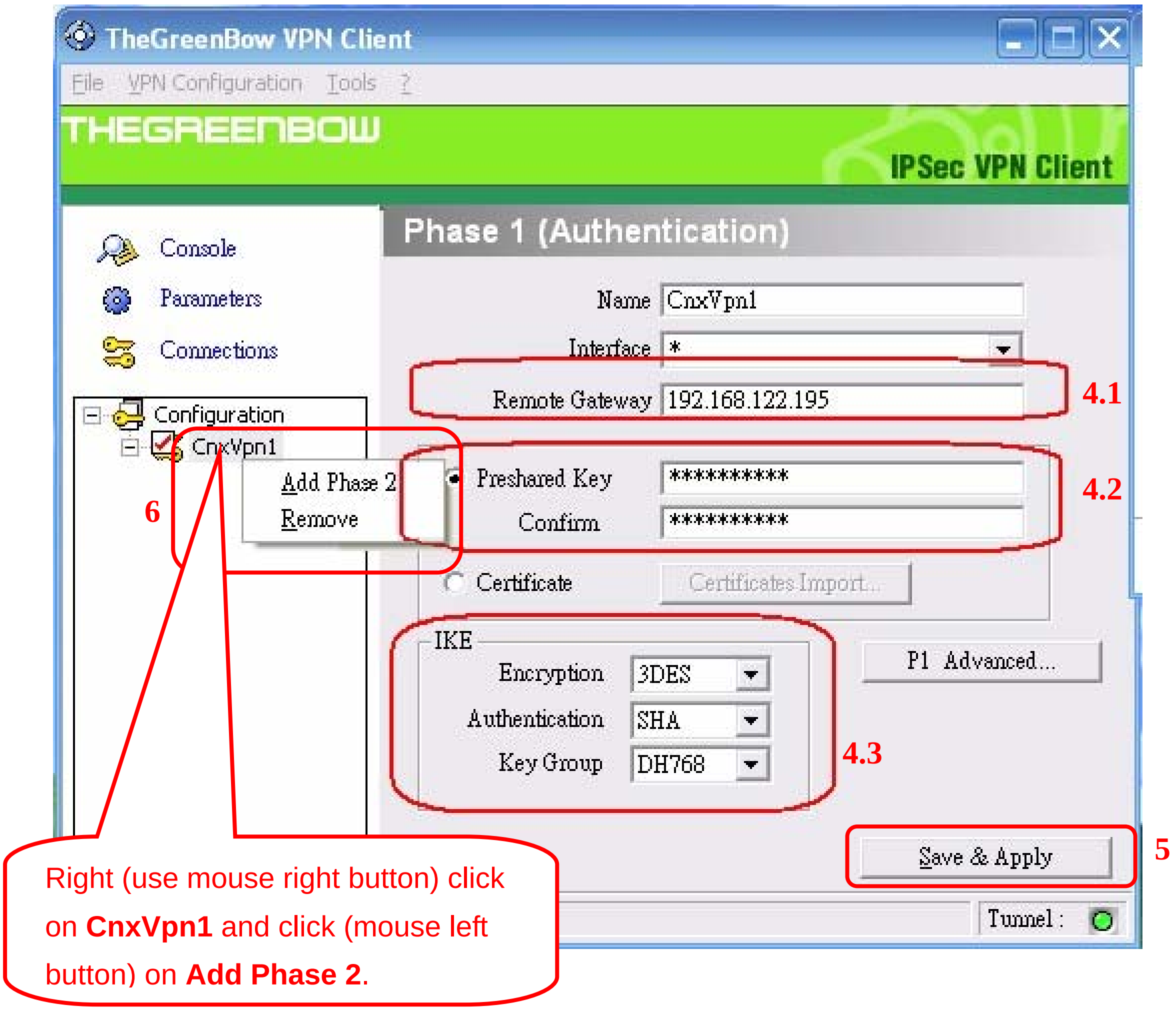
Phase 1 specifies the IKE Key negotiation

2 Right click on the selected Phase 1 and select "Add Phase 2"

Phase 2 defines the IPsec security parameters for a single IPsec Tunnel

Any Phase 1 Configuration may contain several Phase 2 Configurations.

3 Click on "Save and Apply" to apply the changes you made.



Name: CnxVpn1
Interface: *
Remote Gateway: 192.168.122.195
● Preshared Key: **********
Confirm: **********
○ Certificate
IKE
Encryption: 3DES
Authentication: SHA
Key Group: DH768

Right (use mouse right button) click on **CnxVpn1** and click (mouse left button) on **Add Phase 2**.

4. Click on **CnxVpn1**. Add the following information for phase 1.

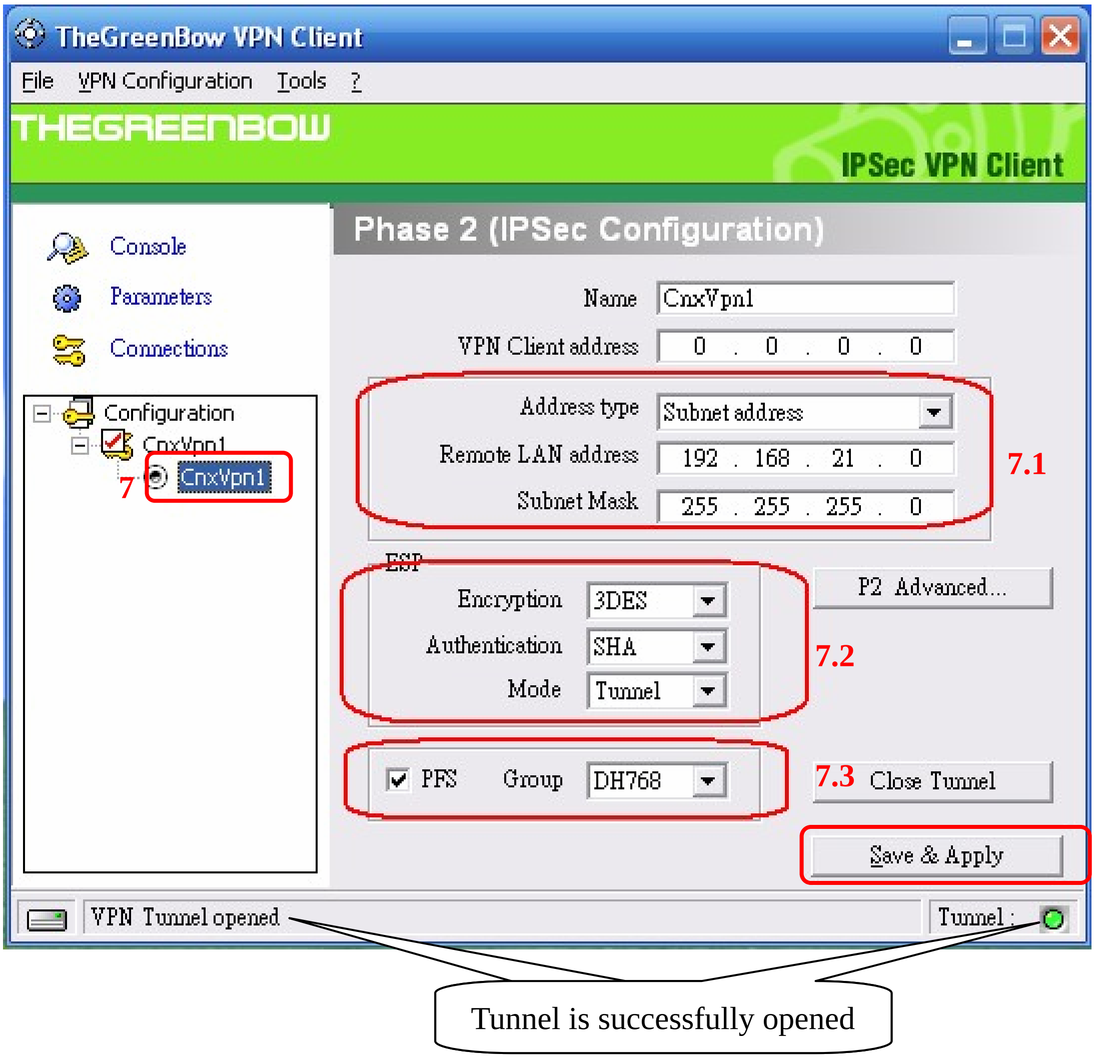
   4.1 Remote Gateway

   4.2 Preshared Key twice (the second one in **Confirm field**)

   4.3 IKE information: select Key Group **DH768** (If you use **DH 1024** in WL/IP-8000 VPN, then you will need to use the right one).

5. Click on **Save & Apply** button to store phase 1 information.

6. Use mouse right button to click on **CnxVpn1**, and add a New Phase 2 VPN connection by clicking (left mouse button) on **Add Phase 2**.



Phase 2 (IPSec Configuration)

Name: CnxVpn1
VPN Client address: 0 . 0 . 0 . 0
Address type: Subnet address
Remote LAN address: 192 . 168 . 21 . 0
Subnet Mask: 255 . 255 . 255 . 0

ESP
Encryption: 3DES
Authentication: SHA
Mode: Tunnel

☑ PFS Group: DH768

VPN Tunnel opened
Tunnel : ●

Tunnel is successfully opened

7. Click on the second **CnxVpn1**. Add the following phase 2 information.
   7.1 Select Address type as **Subnet address**, Remote LAN address, and Subnet Mask
   7.2 The ESP information: **3DES**, **SHA**, and **Tunnel** mode
   7.3 Check mark **PFS** and select Group **DH768**. (If you use **DH 1024** in WL/IP-8000 VPN, then you will need to use the right one).
8. Click on **Save & Apply** button to store phase 2 information.
9. Click on **Open Tunnel** button.

If everything you have set is right, you would see the status shows VPN Tunnel Opened. You now have a secured IPSec VPN tunnel.

Click on **Close Tunnel** to end the VPN tunnel, if you don't need to use the

VPN any more.

The following link provides more information for TheGreenBow VPN client.

http://www.thegreenbow.com/vpn_doc.html