How to Establish a Secure IPSec Tunnel

Step 1: Create an IPSec Policy

- 1. Click the **Start** button, select **Run**, and type **secpol.msc** in the **Open** field. The Local Security Setting screen will appear as shown in Figure C-1.
- 2. Right-click IP Security Policies on Local Computer, and click Create IP Security Policy.
- 3. Click the Next button, and then enter a name for your policy (for example, to_router). Then, click Next.
- 4. Deselect the Activate the default response rule check box, and then click the Next button.
- 5. Click the Finish button, making sure the Edit check box is checked.

Step 2: Build Filter Lists

Filter List 1: win->router

- 1. In the new policy's properties screen, verify that the Rules tab is selected, as shown in Figure C-2. Deselect the **Use Add Wizard** check box, and click the **Add** button to create a new rule.
- 2. Make sure the IP Filter List tab is selected, and click the Add button. (See Figure C-3.)





NOTE: The references in this section to "win" are references to Windows 2000 and XP.

router Properties			
lules General			
Security rule	s for communicating with	other computers	
IP Filter List	Filter Action	Authentication	Tu
	Default Besponse	Kerberos	bl

Figure C-2: Setup Tab

renerroperties		?		
Authentication Methods	Tunnel Setting	Connection Type		
IP Filter List		Filter Action		
The selected IP filter list specifies which network traffic will be secured with this rule.				
IT THEFEISTS.				
Name	Description			
Name O All ICMP Traffic	Description Matches all I	CMP packets betw		

Figure C-3: IP Filter List Tab

- 3. The IP Filter List screen should appear, as shown in Figure C-4. Enter an appropriate name, such as win->router, for the filter list, and de-select the Use **Add** Wizard check box. Then, click the **Add** button.
- 4. The Filters Properties screen will appear, as shown in Figure C-5. Select the Addressing tab. In the Source address field, select My IP Address. In the Destination address field, select A specific IP Subnet, and fill in the IP Address: 192.168.1.0 and Subnet mask: 255.255.255.0. (These are the Router's default settings. If you have changed these settings, enter your new values.)
- 5. If you want to enter a description for your filter, click the Description tab and enter the description there.
- 6. Click the **OK** button. Then, click the **OK** (for Windows XP) or **Close** (for Windows 2000) button on the IP Filter List window.
- Filter List 2: router=>win
- 7. The New Rule Properties screen will appear, as shown in Figure C-6. Select the IP Filter List tab, and make sure that **win -> router** is highlighted. Then, click the **Add** button.



Figure C-4: IP Filter List

_

Figure C-5: Filters Properties

Authentication Methods Tunnel Setting Connection Type IP Filter List Filter Action IP Filter List Filter Action	Rule Properties	?	
IP Filter List Filter Action The selected IP filter list specifies which network traffic will be secured with this rule. IP Filter Lists: Name Description All ICMP Traffic Matches al ICMP packets betw	Authentication Methods	Setting Connection Type	
The selected IP filter list specifies which network traffic will be secured with this rule. IP Filter Lists: Name Description All ICMP Traffic Matches al ICMP packets betw	IP Filter List	Filter Action	
Name Description O All ICMP Traffic Matches all ICMP packets betw	The selected IP secured with this P Filter Lists:	cifies which network traffic will be	
O All ICMP Traffic Matches all ICMP packets betw	Name	scription	
	O All ICMP Traffic	Matches all ICMP packets betw	
O All IP Traffic Matches all IP packets from this	O All IP Traffic	tches all IP packets from this	
O win->router	O win->router		

Figure C-6: New Rule Properties

- 8. The IP Filter List screen should appear, as shown in Figure C-7. Enter an appropriate name, such as router->win for the filter list, and de-select the Use **Add Wizard** check box. Click the **Add** button.
- The Filters Properties screen will appear, as shown in Figure C-8. Select the Addressing tab. In the Source address field, select A specific IP Subnet, and enter the IP Address: 192.168.1.0 and Subnet mask: 255.255.255.0. (Enter your new values if you have changed the default settings.) In the Destination address field, select My IP Address.

10. If you want to enter a description for your filter, click the Description tab and enter the description there.

11. Click the **OK** button and the New Rule Properties screen should appear with the IP Filer List tab selected, as shown in Figure C-9. There should now be a listing for "router -> win" and "win -> router". Click the **OK** (for WinXP) or **Close** (for Win2000) button on the IP Filter List window.



Figure C-7: IP Filter List

Filter Properties		? ×
Addressing Protocol Descri	iption	
Source address:	_	
IP Address: Subnet mask:	192 168 1 0 255 255 255 0	
Destination address:		
My IP Address	<u> </u>	
Mirrored. Also match pack	kets with the exact opposite source and	
destination addresses.		

Figure C-8: Filters Properties

w Rule Properties		?
Authentication Methods	Tunnel Setting	Connection Type
IP Filter List		Filter Action
The selected IP filter list specifies which network traffic will secured with this rule.		
Name	Description	
O All ICMP Traffic	Matches all I	CMP packets betw
O All IP Traffic	Matches all I	P packets from this
O router->win		
O win->router		

Figure C-9: New Rule Properties

Step 3: Configure Individual Tunnel Rules

Tunnel 1: win->router

- 1. From the IP Filter List tab, shown in Figure C-10, click the filter list win->router.
- 2. Click the **Filter Action** tab (as in Figure C-11), and click the filter action Require Security radio button. Then, click the Edit button.
- 3. From the Security Methods tab, shown in Figure C-12, verify that the Negotiate security option is enabled, and deselect the **Accept unsecured communication**, but always respond using IPSec check box. Select **Session key Perfect Forward Secrecy**, and click the **OK** button.

Rule Properties		?	
Authentication Methods	Tunnel Setting	Connection Type	
IP Filter List		Filter Action	
The selected IP secured with this	filter list specifies whic s rule.	h network traffic will be	
IP Filter Lists:			
IP Filter Lists:	Description		
IP Filter Lists: Name O All ICMP Traffic	Description Matches all IC	CMP packets betw	
IP Filter Lists: Name O All ICMP Traffic O All IP Traffic	Description Matches all IC Matches all IF	CMP packets betw P packets from this	
IP Filter Lists: Name All ICMP Traffic All IP Traffic O router->win	Description Matches all IC Matches all IF	CMP packets betw P packets from this	

Figure C-10: IP Filter List Tab

Rule Properties		?
Authentication Methods	Tunnel Setting	Connection Type
IP Filter List		Filter Action
The selected filter	action specifies wh	ether this rule negotiates
Filter Actions:	traffic, and how it v	vill secure the traffic.
For secure network	traffic, and how it v	vill secure the traffic.
For secure network Eilter Actions: Name O Permit	traffic, and how it v	vill secure the traffic.
for secure network for secure network Eilter Actions: Name Permit Request Security (Optional)	traffic, and how it v Description Permit unsec Accepts uns	vill secure the traffic. ured IP packets to ecured communicat

Figure C-11: Filter Action Tab

Red	juire Secu	rity Properties			<u>? ×</u>
S	ecurity Meth	nods General			
	 Permit Block Negotia Security Me 	te security: thod preference o	rder:		
	Туре	AH Integrity	ESP Confidential	ES	Add
	Custom Custom	<none> <none></none></none>	3DES 3DES	SH	Edit
	Custom	<none></none>	DES	ME	Remove
					Move up
	•			F	Move down
	Accept unsecured communication, but always respond using IPSec Allow unsecured communication with non IPSec-aware computer Session key Perfect Forward Secrecy				

Figure C-12: Security Methods Tab

- 4. Select the Authentication Methods tab, shown in Figure C-13, and click the Edit button.
- 5. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, as shown in Figure C-14, and enter the preshared key string, such as XYZ12345. Click the **OK** button.
- 6. This new Preshared key will be displayed in Figure C-15. Click the OK or Close button to continue.



Figure C-13: Authentication Methods

Edit Authentic	ation Method Properties	? ×
Authentication	n Method	
	The authentication method specifies how trust is establish between the computers.	hed
C Window: C Use a ce	s 2000 default (Kerberos V5 protocol) etificate from this certificate authority (CA):	
Use this	string to protect the key exchange (preshared key):	
XYZ12	2345	<u> </u>

Figure C-14: Preshared Key

New Rule Properties		<u>? ×</u>	
IP Filter List		Filter Action	
Authentication Methods	Tunnel Setting	Connection Type	
Authentication Method pre	The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.		
Method	Details	Add	
Preshared Key	XYZ12345		
		<u>E</u> ai	
		<u>R</u> emove	

Figure C-15: New Preshared Key

Appendix C: Configuring IPSec between a Windows 2000 PC and the Router How to Establish a Secure IPSec Tunnel

- 7. Select the **Tunnel Setting** tab, shown in Figure C-16, and click **The tunnel endpoint is specified by this IP Address** radio button. Then, enter the Router's WAN IP Address.
- 8. Select the **Connection Type** tab, as shown in Figure C-17, and click **All network connections**. Then, click the **OK** or **Close** button to finish this rule.

Tunnel 2: router->win

9. In the new policy's properties screen, shown in Figure C-18, make sure that "win -> router" is selected and deselect the **Use Add Wizard** check box. Then, click the **Add** button to create the second IP filter.

New Rule Properties		<u>? ×</u>		
IP Filter List	1	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.				
This rule does not specify an IPSec tunnel. The tunnel endpoint is specified by this IP Address:				
140.111.1.	1			

Figure C-16: Tunnel Setting Tab

_Router Properties			?
Rules General			
Security ru	les for communicating with	other computers	
IP Filter List	Filter Action	Authentication	Tu
IP Filter List	Filter Action Require Security	Authentication Preshared Key	Tu 14

Figure C-17: Connectin Type Tab

Authentication Methods	Tunnel Setting Connection	Tune
IP Filter List	Filter Action	
The selected filter a	ction specifies whether this rule ne	gotiate
ilter Actions:	ranic, and now it will secure the tra	
ilter Actions:	Description	
ilter Actions: Name O Permit	Tarric, and now it will secure the tra	to
ilter Actions: Name O Permit O Request Security (Optional)	Description Permit unsecured IP packets Accepts unsecured communi	to pat

Figure C-18: Properties Screen

- 10. Go to the **IP Filter List** tab, and click **the filter list router->win**, as shown in Figure C-19.
- 11. Click the **Filter Action** tab, and select the filter action **Require Security**, as shown in Figure C-20. Then, click the **Edit** button.
- 12. Click the **Authentication Methods** tab, and verify that the authentication method Kerberos is selected, as shown in Figure C-21. Then, click the **Edit** button.

ew Rule Properties		<u>? ×</u>			
Authentication Methods	Tunnel Setting	Connection Type			
IP Filter List		Filter Action			
The selected IP filter list specifies which network traffic will be secured with this rule.					
Name	Description				
O All ICMP Traffic	Matches all I	CMP packets betw			
O All IP Traffic Matches all IP packets from this					
O router->win	⊙ router->win				
O win->router					

Figure C-19: IP Filter List Tab

Authentication Methods	Tunnel Setting	Connection Typ
IP Filter List		Filter Action
The selected filte	r action specifies wh	ether this rule negotia
For secure networ ilter Actions:	k traffic, and how it	will secure the traffic.
for secure networ ilter Actions: Name	K traffic, and how it	will secure the traffic.
ilter Actions: Name O Permit	k traffic, and how it	will secure the traffic.
iter Actions: Name O Permit O Request Security (Optiona	k traffic, and how it Description Permit unsed	will secure the traffic. cured IP packets to ecured communicat

Figure C-20: Filter Action Tab

Rule Properties			?	
IP Filter List		Fi	ilter Action	
Authentication Methods	Tunnel S	Tunnel Setting Connection Type		
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.				
Authentication Method pr	ererence order:			
Authentication Method pr Method	Details		Add	
Authentication Method pr Method Kerberos	Details		Add	
Authentication Method pr Method Kerberos	Details		Add	

Figure C-21: Authentication Methods Tab

- 13. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, and enter the preshared key string, such as XYZ12345, as shown in Figure C-22. (This is a sample key string. Yours should be a key that is unique but easy to remember.) Then click the **OK** button.
- 14. This new Preshared key will be displayed in Figure C-23. Click the **OK** button to continue.
- 15. From the Tunnel Setting tab, shown in Figure C-24, click the radio button for **The tunnel endpoint is specified by this IP Address,** and enter the Windows 2000/XP computer's IP Address.



New Rule Properties				<u>? ×</u>	
IP Filter I	_ist	Filter Action			
Authentication Mel	Authentication Methods Tunne		Connection Type		
The au betwee auther anothe Authentication <u>M</u> eth	The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.				
Method	Details		Add.		
Preshared Key XYZ12345					
			Bema	VP	

Figure C-23: New Preshared Key



Figure C-24: Tunnel Seting Tab

- 16. Click the **Connection Type** tab, shown in Figure C-25, and select **All network connections**. Then click the **OK** (for Windows XP) or **Close** (for Windows 2000) button to finish.
- 17. From the Rules tab, shown in Figure C-26, click the **OK** button to return to the secool screen.

Step 4: Assign New IPSec Policy

In the IP Security Policies on Local Computer window, shown in Figure C-27, right-click the policy named to_router, and click **Assign**. A green arrow appears in the folder icon.



Figure C-25: Connection Type

Router Properties			?
lules General			
Security ru	les for communicating with	other computers	
IP Security Rules: IP Filter List	Filter Action	Authentication	Tu
-			
✓ win->router	Require Security	Preshared Key	14
vin->router	Require Security Require Security	Preshared Key Preshared Key	14 14
✓ win->router ✓ router->win ✓ router->win ✓ Cynamic>	Require Security Require Security Default Response	Preshared Key Preshared Key Kerberos	14 14 Nc

Figure C-26: Rules



Figure C-27: Local Computer

Appendix C: Configuring IPSec between a Windows 2000 PC and the Router How to Establish a Secure IPSec Tunnel

Step 5: Create a Tunnel Through the Web-Based Utility

- 1. Open your web browser, and enter 192.168.1.1 in the Address field. Press the Enter key.
- 2. When the User name and Password field appears, enter the default the user name and password **admin**. Press the **Enter** key.
- 3. From the Setup tab, click the **VPN** tab.
- 4. From the VPN tab, shown in Figure C-28, select the tunnel you wish to create in the Select Tunnel Entry dropdown box. Then click **Enabled**. Enter the name of the tunnel in the Tunnel Name field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.
- 5. Enter the IP Address and Subnet Mask of the local VPN Router in the Local Secure Group fields. To allow access to the entire IP subnet, enter 0 for the last set of IP Addresses. (e.g. 192.168.1.0).
- 6. Enter the IP Address and Subnet Mask of the VPN device at the other end of the tunnel (the remote VPN Router or device with which you wish to communicate) in the Remote Security Gateway fields.
- 7. Select fromtwo different types of encryption: DES or 3DES (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting Disable.
- 8. Select from two types of authentication: MD5 and SHA (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to Disable authentication.
- 9. Select the Key Management. Select Auto (IKE) and enter a series of numbers or letters in the Pre-shared Key field. Check the box next to PFS (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure. 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'd like the key to be useful, or leave it blank for the key to last indefinitely.

10. Click the Save Settings button to save these changes.

Your tunnel should now be established.

Security	Setup Wireless	Security Access Applications	& Administration Status
	Firewall VPN	802.1x Setup	
VPN Passthrough	IPSec Passthrough: PPTP Passthrough: L2TP Passthrough:	Enabled C Disabled Enabled C Disabled Enabled C Disabled Enabled C Disabled	More
VPN Tunnel	Select Tunnel Entry: VPN Tunnel: Tunnel Name :	Tunnel 1 () 💌 C Enabled © Disabled	
Local Secure Group Remote Secure Group	IP Address : Mask :	0 . 0 . 0 . 0 0 . 0 . 0 . 0	
Remote Secure Gateway	IP Address : Mask : IP Address :	0 . 0 . 0 . 0 0 . 0 . 0 . 0 0 . 0 . 0	
	Encryption : Authentication :	DES 💌 MD5 💌	
Key Management	Key Exchange Method PFS :	Auto(IKE) = C Enabled © Disabled [Please enter shared secret] Please enter RSA 3500	
Status	Advanced VPN	Tunnel Setup	Cisco Systems
		Save Settings Cancel Change	en iliteration

Figure C-28: VPN Tab