P

Internet Security Appliance

RF550VPN/RF560VPN

IPSec Tunneling

Reference Guide



How To: Configuring IPSec Tunneling in Windows XP or 2000 and Connecting to an RF550VPN/RF560VPN

Copyright © 2003

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved. Multi-Tech Systems, Inc. makes no representations or warranty with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Manual Number S000261D

Revision	Date	Description
А	05/30/02	Initial release
A1	05/31/02	Added Win2K/XP screen differences
В	08/12/02	Added RF550VPN settings and static IP note.
С	04/16/03	Updated for RF550VPN software version 4.64.
D	07/07/03	Add RF560VPN.

The following configuration procedure shows how to configure IPSec tunneling on a Windows XP Professional client so that this client can access a LAN through the Internet. The LAN is located on the protected side of a RF550VPN/RF560VPN. It is assumed that the RF550VPN/RF560VPN is already configured. This configuration procedure will also work on Windows 2000 with service pack 2 installed. Comments are included for screens that differ between Win XP and 2K.

<u>Note:</u> The remote client must use a static IP address for IPSec tunneling. This configuration will not work using a dynamic IP address at the remote client.



1. At the Windows XP Professional workstation, type **mmc** in DOS command mode.



2. Left click on **File** and select **Add/Remove Snap-in**. For Win 2K, left click on **Console** and select **Add/Remove Snap-in**.



3. Click Add.

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	
	- 11
Description	_
Add Remove About	
ОК Са	ancel

4. Scroll down and highlight IP Security Policy Management and click Add.

Available Standalone Snap-ins: Snap-in Vendor Disk Defragmenter Microsoft Corp, Executi Disk Management Microsoft Corporation Disk Group Policy Microsoft Corporation Group Policy Microsoft Corporation Indexing Service Microsoft Corporation IP Security Monitor Microsoft Corporation P Security Policy Management Microsoft Corporation Disk to Web Address Microsoft Corporation Description Microsoft Corporation Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.	Add Standalone Snap-in		?×
Snap-in Vendor Image: Disk Defragmenter Microsoft Corp, Executi Image: Disk Management Microsoft Corporation Image: Disk Management Microsoft Corporation	Available Standalone Snap-ins:		
Disk Defragmenter Microsoft Corp, Executi Disk Management Microsoft and VERITAS Disk Management Microsoft Corporation Polder Microsoft Corporation Group Policy Microsoft Corporation Indexing Service Microsoft Corporation, I IP Security Monitor Microsoft Corporation IP Security Policy Management Microsoft Corporation Ink to Web Address Microsoft Corporation Local Users and Groups Microsoft Corporation Description Microsoft Corporation Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.	Snap-in	Vendor	^
Description Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.	 Disk Defragmenter Disk Management Event Viewer Folder Group Policy Indexing Service IP Security Monitor IP Security Policy Management Cink to Web Address Local Users and Groups 	Microsoft Corp, Executi. Microsoft and VERITAS Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	
Add Close	Description Internet Protocol Security (IPSec) Admini policies for secure communication with o	stration. Manage IPSec ther computers.	se

5. Choose Local computer and click Finish.

Select Computer	? ×
Select which computer this Snap-in will manage When this console is saved the location will also be saved	Ē
Local computer The computer this console is running on	
Manage domain policy for this computer's domain	
 Manage domain policy for another <u>d</u>omain: ☐ <u>A</u>nother computer: Browse 	
< Back Finish	Cancel

6. Click **Close**.

Add Standalone Sr	ap-in		?×
Available Standalone S	Snap-ins:		
Snap-in		Vendor	~
🚯 Disk Defragmente	er	Microsoft Corp, Executi	
🛛 👹 Disk Managemer	it	Microsoft and VERITAS.	
🔃 Event Viewer		Microsoft Corporation	
🔲 Folder		Microsoft Corporation	=
🚮 Group Policy		Microsoft Corporation	
🎽 🎦 Indexing Service		Microsoft Corporation, I	. 🔲
📃 🜏 IP Security Monit	or	Microsoft Corporation	
🛛 뢿 IP Security Policy	Management	Microsoft Corporation	
🛛 🧕 Link to Web Add	ress	Microsoft Corporation	
🔣 Local Users and I	Groups	Microsoft Corporation	~
Description Internet Protocol Sec policies for secure co	urity (IPSec) Admini: mmunication with ot	stration. Manage IPSec her computers.	<

7. Click OK.

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 Machine
Description
Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.
Add <u>R</u> emove <u>Ab</u> out
OK Cancel

8. Click left button on **IP Security Policies on Local Computer** under **Console Root** to display the local computer security policies under **Name**.



9. Right click on IP Security Policies on Local Computer and select Create IP Security Policy.



10. Click Next.



11. Type Name and Description for security policy, and then click **Next**.

IP Security Policy Wizard	? ×
IP Security Policy Name Name this IP Security policy and provide a brief description	Ē
Name: RF550VPN With Win_XP	
Description: RF550VPN Communication with Windows XP Professional	
	×.
< Back Next > C	ancel

12. Uncheck Activate the default response rule, then click Next.



13. Click Finish.



14. Click Add.

EA2104VPN With W2K Pro	perties		?×	
Rules General				
Security rules for communicating with other computers				
IP Security Rules:				
IP Filter List	Filter Action	Authentication	Tu	
Comparise	Default Response	Kerberos	Nc	
•			•	
	t <u>R</u> emove	Use Add <u>W</u> iz	ard	
		OK Car	icel	

15. Click Next.



16. Input IP Address into **The tunnel endpoint specified by this IP address:** and then click **Next**. (Ex: RF550VPN/RF560VPN WAN Port IP Address 204.26.122.103)

Security Rule Wizard	? ×
Tunnel Endpoint The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.	Ī
An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers. Specify the tunnel endpoint for the IP Security rule:	
 This rule does not specify a tunnel The tunnel endpoint is specified by this IP address: 	
204 . 26 . 122 . 103	
< Back Next > C	ancel

17. Choose All network connections, and then click Next.



18. Choose **Use this string to protect the key exchange (preshared key)**. Enter the key code and then click **Next**. (Ex: RF550VPN/RF560VPN preshared key 1o2t3t4f)

Security Rule Wizard	? X
Authentication Method To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.	圓
Set the initial authentication method for this security rule:	
Use a certificate from this certification authority (CA): Browse Output: Browse Output: Dise this string to protect the key exchange (preshared key):	
1o2t3t4f	~
< Back Next > 0	Cancel

19. Click Add.

Securit	y Rule Wizard		<u>? ×</u>		
IP I	F ilter List Select the IP filter list for the type o	f IP traffic to which this security rule	applies.		
	If no IP filter in the following list matches your needs, click Add to create a new one.				
	IP filter lists:				
	Name	Description	<u>A</u> dd		
	O All ICMP Traffic O All IP Traffic	Matches all ICMP packets bet Matches all IP packets from t	<u>E</u> dit		
			<u>R</u> emove		
		< <u>B</u> ack <u>N</u> ext	> Cancel		

20. Type a filter name and description then click Add.

IP Filter List			? 🗙
An IP filter list is comp addresses and protoc	osed of multiple filte ols can be combine	rs. In this way, multiple sub d into one IP filter.	nets, IP
Name:			
Win_XP to RF550VPN			
Description:		(Add
Make a filter from Win_XP to Rf	550VPN	~	E dit
		~	Remove
Filters:		V L	Jse Add Wizard
Mirrored Description	Protocol	Source Port	Destination
		ОК	Cancel

21. Click Next.



22. Select **A specific IP Address** and input Source IP address, and then click **Next**. (Ex: Windows XP Professional IP address 204.26.122.50)

Filter Wizard	? 🗙
IP Traffic Source Specify the source address of the IP traffic.	Ħ
Source address: A specific IP Address	
IP Address: 204 . 26 . 122 . 50	
Subnet mask: 255 . 255 . 255 . 255	
< Back Next >	Cancel

23. Select **A specific IP Subnet** and input destination IP address, and then click **Next**. (Ex: RF550VPN/RF560VPN Private network (LAN) 192.168.2.0)

Filter Wizard	? ×
IP Traffic Destination Specify the destination address of the IP traffic.	Ē
Destination address:	
IP Addres 192 . 168 . 2 . 0	
Subnet mas <u>k</u> : 255 . 255 . 255 . 0	
< Back	Cancel

24. Click Next.

Filter Wizard	? ×
IP Protocol Type Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port.	Ē
Select a protocol type:	
< <u>Back</u>	Cancel

25. Click Finish.



26. Click OK. For Win 2K click on Close.

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:			
Win_XP to RF550VPN			
, Description:			Add
Make a filter from Win_XP to F	RF550VPN		Edit
		~	Remove
Filters:		ν.	Jse Add Wizard
Mirrored Description	Protocol	Source Port	Destination
Yes	ANY	ANY	ANY
<		ОК	Cancel

27. Choose Win_XP to RF550VPN/RF560VPN and then click Next.

Security Rule Wizard		? 🔀
IP Filter List Select the IP filter list for the type	of IP traffic to which this security rule	applies.
If no IP filter in the following list ma IP filter lists:	atches your needs, click Add to creal	te a new one.
Name	Description	Add
All ICMP Traffic All IP Traffic All IP Traffic Win_XP to RF550VPN	Matches all ICMP packets bet Matches all IP packets from t Make a filter from Win_XP to	Edit Remove
	< Back Next	Cancel

28. Click Add.

Security Rule Wizard	<u>? ×</u>
Filter Action Select the filter action for this secu	irity rule.
If no filter actions in the following li one. Select Use Add Wizard to cre Filter Actions:	st matches your needs, click Add to create a new eate a filter action.
Permit O Request Security (Optional) O Require Security	Permit unsecured IP packets t Accepts unsecured communi Accepts unsecured communi <u>Remove</u>
	< <u>B</u> ack <u>N</u> ext > Cancel

29. Click Next.



30. Type a filter action name and then click **Next**. (Ex: 3DES_MD5)

Filter Action Wizard	<u>? ×</u>
Filter Action Name Name this filter action and optionally give a brief description	and the second s
Name:	
3DES_MD5	
Description:	
3DES_MD5	
< <u>B</u> ack <u>N</u> ext>	Cancel

31. Choose Negotiate security and then click Next.

Filter Action	<u>? ×</u>
Filter Action General Options Set the filter action behavior.	Lease 1
Permit Block Negotiate security:	
	< <u>B</u> ack <u>N</u> ext > Cancel

32. Choose **Do not communicate with computer that do not support IPSec**, and then click **Next**.

Filter Action Wizard	? ×
Communicating with computers that do not support IPSec Communicating with computers that do not support IPSec may expose your network to security risks.	193
Do you want to allow communication with computers the do not support IPSec?	
© Do not communicate with computers that do not support IPSec.	
Fall back to <u>unsecured</u> communication.	
Use this option if there are computers that do not support IPSec on your network Communication with computers that do not support IPSec may expose your netw to security risks.	ork
< <u>B</u> ack <u>N</u> ext > C	ancel

33. Choose **Custom** and then click **Settings**.

Security Method Wizard	? ×
IP Traffic Security Specify a security method for IP traffic. To add multiple security methods edit the filter action after completing the wizard.	E.
This filter action requires at least one security method for IP traffic.	
 High (Encapsulated Secure Payload) Data will be encrypted, authenticated, and unmodified. Medium (Authenticated Header) Data will be authentic and unmodified, but will not be encrypted. 	
< <u>B</u> ack <u>N</u> ext >	Cancel

34. Check Data integrity and encryption (ESP), select Integrity algorithm (MD5) and Encryption algorithm (3DES), and then click OK.

Custom Security Method Settings	? ×
Specify the settings for this custom security method.	
Data and address integrity without encryption (AH) : [ntegrity algorithm:	
MD5	
Data integrity and encryption (ESP): Integrity algorithm: MD5	
Encryption algorithm:	
Session Key Settings:	
Generate a new key every: Generate a new key every: 1000000 Kbytes	very
OK Can	cel

35. Click Next.

Security Method Wizard	? ×
IP Traffic Security Specify a security method for IP traffic. To add multiple security methods edit the filter action after completing the wizard.	Real Provide P
This filter action requires at least one security method for IP traffic.	
 High (Encapsulated Secure Payload) Data will be encrypted, authenticated, and unmodified. Medium (Authenticated Header) Data will be authentic and unmodified, but will not be encrypted. 	
<u>Custom</u> <u>Settings</u>	
< <u>B</u> ack <u>N</u> ext >	Cancel

36. Click Finish.



37. Select **3DES_MD5** and then click **Edit**.

Security Rule Wizard	?×
Filter Action Select the filter action for this secu	rity rule.
If no filter actions in the following lis one. Select Use Add Wizard to cre	t matches your needs, click Add to create a new ate a filter action.
Filter A <u>c</u> tions:	🔽 Use Add <u>W</u> izard
Name	Description <u>A</u> dd
OBDES_MD5	3DES_MD5
O Permit	Permit unsecured IP packets t
O Request Security (Optional)	Accepts unsecured communi Remove
O Require Security	Accepts unsecured communi
	< <u>B</u> ack <u>N</u> ext > Cancel

38. Check Accept unsecured communications and Session key Perfect Forward Secrecy, and then click OK.

3DE5_MD5 Properties	? ×
Security Methods General	
 Permit Block Negotiate security: Security Method preference order: 	
Type AH Integrity ESP Confidential ES	A <u>d</u> d
Custom <none> 3DES ME</none>	<u>E</u> dit
	<u>R</u> emove
	Move <u>up</u>
	Move d <u>o</u> wn
Accept unsecured communication, but always respond	using IPSec
Allow unsecured communication with non IPSec-aware	computer
Session key Perfect Forward Secrecy	
OK Cancel	Apply

39. Click Next.



40. Uncheck Edit properties and click Finish.



41. Click Add.

RF550VPN With Win_X	(P Properties		?×
Rules General			
Security rules I	for communicating with o	ther computers	
IP Security rules:			
IP Filter List	Filter Action	Authentication	Tu
Win XP to RF550	3DES MD5	Preshared Key	20
Oynamic>	_ Default Response	Kerberos	Nc
<	ш)	4	>
Add Edi	t Remove	🛛 🔽 Use Add W	izard
		Close Ca	ncel

42. Click Next.



43. Input IP Address into **The tunnel endpoint specified by this IP address:** and then click **Next**. (Ex: Windows XP Professional IP Address 204.26.122.50)

Security Rule Wizard	? ×
Tunnel Endpoint The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.	Ē
An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers. Specify the tunnel endpoint for the IP Security rule: This rule does not specify a tunnel The tunnel endpoint is specified by this IP address: 204 . 26 . 122 . 50	
< Back Next > Ca	ncel

44. Choose All network connections, and then click Next.

Security Rule Wizard	<u>?</u> ×
Network Type The security rule must be applied to a network type.	Ī
Select the network type: All network connections Local area network (LAN) Emote access	
< <u>B</u> ack <u>N</u> ext >	Cancel

45. Choose **Use this string to protect the key exchange (preshared key)**. Enter the key code, and then click **Next**. (Ex: RF550VPN/RF560VPN preshared key 1o2t3t4f)

Security Rule Wizard		? ×
Authentication Method To add multiple authentication methods, edit the security rule after com IP Security rule wizard.	pleting the	Ī
Set the initial authentication method for this security rule:		
 Active Directory default (Kerberos V5 protocol) 		
O Use a certificate from this certification authority (CA):		
	Browse	1
Use this string to protect the key exchange (preshared key):		-
1o2t3t4f	^	J
	~	
< Back Next >	Car	ncel

46. Click **Add**.

Security Rule Wizard		? 🗙
IP Filter List Select the IP filter list for the type	e of IP traffic to which this security rule	e applies.
If no IP filter in the following list m	natches your needs, click Add to crea	ite a new one.
Name All ICMP Traffic All IP Traffic Win_XP to RF550VPN	Description Matches all ICMP packets bet Matches all IP packets from t Make a filter from Win_XP to	Add Edit Remove
	< Back Nex	Cancel

47. Type a filter name and description and then click **Add**.

🗖 IP Filte	r List			? 🗙
	An IP filter list is con addresses and prote	nposed of multiple filte ocols can be combine	rs. In this way, multiple sul d into one IP filter.	onets, IP
Name.				
RE550VP	N to Win_XP			
Description	n:			Add
Make a fil	ter from RF550VPN	to Win_XP	~	E dit
			~	Remove
Filters:				Use Add Wizard
Mirrored	Description	Protocol	Source Port	Destination
<				>
			ОК	Cancel

48. Click Next.



49. Select "A specific IP Subnet" and input Source address and then click "Next." (Ex: RF550VPN/RF560VPN Private network(LAN) 192.168.2.0)

Filter Wizard	? X
IP Traffic Source Specify the source address of the IP traffic.	Ē
Source address:	
A specific IP Subnet	
IP Addres 192 . 168 . 2 . 0	
Subnet <u>m</u> ask: 255 . 255 . 255 . 0	
< <u>B</u> ack <u>N</u> ext > Ca	ancel

50. Select A specific IP Address and input destination IP address and then click Next.

(Ex: Windows XP Professional IP address 204.26.122.50)

Filter Wizard						? 🗙
IP Traffic Destination Specify the destination addr	ess of the	IP traffic.				Ē
Destination address:				_		
A specific IP Address			•]		
IP address.	204	. 26	. 122	. 50	>	
Subnet mask:	255	. 255	. 255	. 255]	
			< Back	Nex	t>	Cancel

51. Click Next.

Filter Wizard	<u>?</u> ×
IP Protocol Type Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port.	Ē
Select a protocol type:	
< <u>B</u> ack <u>N</u> ext>	Cancel

52. Click Finish.



53. Click OK. For Win 2K click on Close.

Name:				
RF550VP	N to Win_XP			
Description	n:			Add
Make a fil	ter from RF550VPN	I to Win_XP	~	E dit
			~	Remove
Filters:				Remove Use Add Wizard
Filters: Mirrored	Description	Protocol	Source Port	Remove Use Add Wizard Destination
Filters: Mirrored Yes	Description	Protocol	Source Port	Remove Use Add Wizar Destinatio ANY
filters: Mirrored Yes	Description	Protocol ANY	Source Port ANY	Remove Use Add Wiza Destinatio ANY
Filters: Mirrored Yes	Description	Protocol ANY	Source Port ANY	Remove Use Add Wizan Destinatio ANY

54. Select **RF550VPN/RF560VPN to Win_XP**, and then click **Next**.

Security Rule Wizard		? 🗙					
IP Filter List Select the IP filter list for the typ	IP Filter List Select the IP filter list for the type of IP traffic to which this security rule applies.						
If no IP filter in the following list i IP filter lists:	matches your needs, click Add to creat	e a new one.					
Name	Description	Add					
All ICMP Traffic	Matches all ICMP packets bet Matches all IP packets from t	Edit					
Win_XP to RF550VPN	Make a filter from RF550VPN Make a filter from Win_XP to	Remove					
	< Back Next:	Cancel					

55. Choose **3DES_MD5** and then click **Next**.

Security Rule Wizard		<u>? ×</u>
Filter Action Select the filter action for this secu	rity rule.	
If no filter actions in the following lis one. Select Use Add Wizard to cre	st matches your needs, click Add to eate a filter action.	create a new
Filter Actions:	V	Use Add <u>W</u> izard
Name	Description	<u>A</u> dd
 DES_MD5 Permit Request Security (Optional) Require Security 	3DES_MD5 Permit unsecured IP packets t Accepts unsecured communi Accepts unsecured communi	<u>E</u> dit <u>R</u> emove
	< <u>B</u> ack <u>N</u> ext	Cancel

56. Click Finish.



57. Highlight Win_XP to RF550VPN/RF560VPN and then click Edit.

RF550VPN With Win_X	(P Properties		? ×
Rules General			
Security rules	for communicating with o	her computers	
IP Security rules:			
IP Filter List	Filter Action	Authentieation	Tu
Win_XP to RF550	3DES_MD5	Preshared Key	20
RF550VPN to Win	3DES_MD5	Preshared Key	20
Oynamic>	Default Response	Kerberos	Nc
< <u> </u>			
Add Ed	it Remove	🛛 🔽 Use Add W	ïzard
		Close Ca	incel

58. Select Win_XP to RF550VPN/RF560VPN and then click Edit.

Edit Rule Properties	? 🛛
Authentication Methods Tur IP Filter List	nel Setting Connection Type Filter Action
The selected IP filter list	specifies which network traffic will be
IP Filter Lists:	
Name	Description
O AILICMP Traffic	Matches all ICMP packets betw
O AILIP Traffic	Matches all IP packets from this
Q RF550VPN to Win_XP	Make a filter from RF550VPN to
Win_XP to RF550VPN	Make a filter from Win_XP to RF
Add Edit	Remove
OK	Cancel Apply

59. Click Edit.

IP Filter	List			? 🗙
	an IP filter list is co addresses and prot	mposed of multiple filte cocols can be combine	rs. In this way, multiple su d into one IP filter.	bnets, IP
Name:				
Win_XP to	RF550VPN			
, Description				Add
Make a filt	er from Win_XP to	RF550VPN		Edit
				Bemove
			<u> </u>	
Filters:	Description	Protocol	Courses Port	Destination
Yes	Description	ANY	ANY	ANY
<				>

60. Uncheck **Mirrored. Also match packets with exact opposite source and destination address** and then click **OK**.

Filt	er Properties								?×
A	ddressing Protocol Descri	ption							
	Source address:								
	A specific IP Address						•		
	IP Address:	204		26		122		50	-
	Subnet mask:	255		255		255		255	
	Destination address:								
	A specific IP Subnet						•		
	IP address:	192	•	168	•	2	•	0	
	Subnet mask:	255	•	255	•	255	•	0	-
	Myrrored. Also match pack destination addresses.	ets with t	he	exact o	pp	osite sc	ourc	e and	
				\langle		OK		Ca	ncel

61. Click **OK**. For Win 2K click on **Close**.

IP Filter List			? 🛛
An IP filter list is compo addresses and protoco	sed of multiple filter Is can be combined	s. In this way, multiple sub Linto one IP filter.	onets, IP
Name:			
Win_XP to RF550VPN			
Description:			Add
Make a filter from Win_XP to RF	550VPN	<u>^</u>	Edit
		~	Remove
Filters:		▼ 1	Jse Add Wizard
Mirrored Description	Protocol	Source Port	Destination
No	ANY	ANY	ANY
<			

62. Choose RF550VPN/RF560VPN to Win_XP and then click Edit.

Edit Rule Properties	? 🗙
Authentication Methods Tur IP Filter List	nel Setting Connection Type
The selected IP filter list	specifies which network traffic will be
IP Filter Lists:	
Name	Description
O AILICMP Traffic	Matches all ICMP packets betw
All IP Traffic	Matches all IP packets from this
(⊙ PF550VPN to Win_XP	Make a filter from RF550VPN to
Win_XP to RF550VPN	Make a filter from Win_XP to RF
Add Edit	Remove
Clos	e Cancel Apply

63. Click Edit.

IP Filter	List			?
	n IP filter list is co ddresses and prot	mposed of multiple filte ocols can be combine	rs. In this way, multiple su d into one IP filter.	bnets, IP
Name:				
RF550VPN	to Win_XP			
Description:				Add
Make a filte	r from RF550VPN	I to Win_XP	~	Edit
				Bemove
1			<u> </u>	
Filters:	Description	Protocol	Source Port	Destination
Yes	Description	ANY	ANY	ANY
<				>
			ОК	Cancel

64. Uncheck **Mirrored. Also match packets with exact opposite source and destination address** and then click **OK**.

Fil	ter Properties	?	×
A	ddressing Protocol Description		
	r Source address:		,
	A specific IP Subnet		
	IP Address: 192 . 168 . 2 . 0	_	
	Subnet mask: 255 . 255 . 255 . 0	_	
	Destination address:		
	A specific IP Address		
	IP address: 204 . 26 . 122 . 50	_	
	Subnet mask: 255 . 255 . 255 . 255	_	
$\left(\right)$	Mirrored. Also match packets with the exact opposite source and destination addresses.		
	ОКС	ancel	

65. Click **OK**. For Win 2K click on **Close**.

DEEEM/E	N ta trên MD			-2
Descriptio	n:			Add
Make a fi	Iter from RF550VPN	I to Win_XP	~	Edit
			~	Remove
Filters:			I∎	Use Add Wizard
Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

66. Highlight **Win_XP to RF550VPN/RF560VPN** and make sure a dot is in the circle for this selection, and then click **Close**.

Edit Rule Properties	<u>?</u> ×
Authentication Methods Tur IP Filter List	nel Setting Connection Type Filter Action
The selected IP filter list	specifies which network traffic will be
IP Filter Lists:	
Name	Description
O AILICMP Traffic	Matches all ICMP packets betw
O All IP Traffic	Matches all IP packets from this
Q RF550VPN to Win_XP	Make a filter from RF550VPN to
Win_XP to RF550VPN	Make a filter from Win_XP to RF
Add Edit	Remove
Clos	Cancel Apply

67. Click Close.

RF550VPN With Win_X	(P Properties		?×	
Rules General				
Security rules for communicating with other computers				
IP Security rules:				
IP Filter List	Filter Action	Authentication	Tu	
☑ Win_XP to RF550	3DES_MD5	Preshared Key	20	
RF550VPN to Win	3DES_MD5	Preshared Key	20	
Oynamic>	Default Response	Kerberos	Nc	
<			>	
Add Ed	t Remove	🛛 🔽 Use Add W	'izard	
Close Cancel				

68. Click right button on **RF550VPN/RF560VPN with Win_XP** and click **Assign**. The **Policy Assigned** column will change from **No** to **Yes** for this item.

🚡 Console1 - [Console Root\IP Security Policies on Local Com 🔳 🗖	X
🚡 File Action View Favorites Window Help	×
← → 🖻 📧 🗙 🖙 🖳 😫 🎦 🏦 📩 🧕	
Console Root Name A Description	Polic
IP Security Policies (Client (Respond Only) Communicate normally (uns	No
RF550VPN With Win_XP RF550VPN Communication w	Yes
Secure Server (Requir For all IP traffic, always req	No
Server (Request Secu For all IP traffic, always req	No
	2

69. Now you want to verify that IPSec Services have been started. To do this, left click **Start** in the lower left corner of the screen; then click **Administrative Tools**; then **Services**, and then **IPSEC Services**. Start **IPSEC Services**.



70. Ping Remote private network (192.168.2.100) on Dos Command Mode. After several failures, you should see successful replies. If this fails, check your cabling, RF550VPN/RF560VPN configuration and Win XP IPSec configuration.