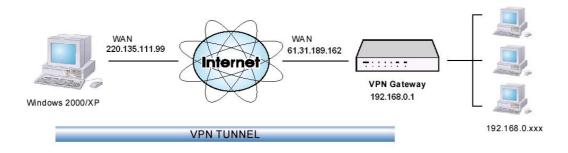


WBR-3460 IPSec VPN vs. Win XP IPSec VPN

Windows 2000/XP client with public IP connects to WBR-3460 Broadband VPN Gateway and gains access to the local LAN.



Windows 2000/XP Client to Broadband VPN Gateway

Windows 2000/XP IPSec client configuration can be a little bit confusing for the first time. Basically you will need to create an IP Sec security policy in Windows and set both "way to the router" and "back from the router". Below is a step by step guidance.

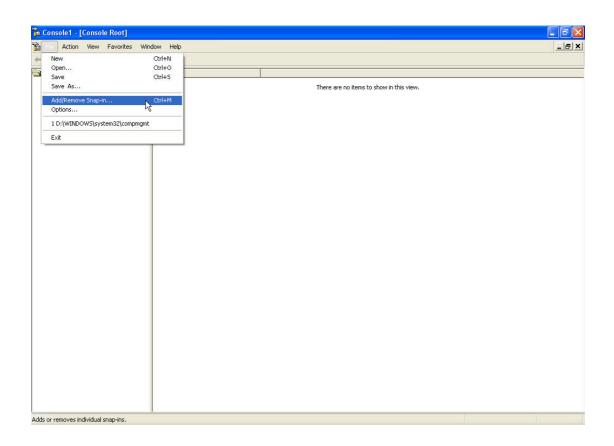
1. Start \rightarrow Run \rightarrow <mmc>



2. You should see the console screen.

🚡 Console1 - [Console Root]					
File Action View Favorites Winder ← → ■ □ □ □ □	dow Help				<u>_8×</u>
Console Root	Name				
		-	There are no items to show in this view	ı.	

3. Under file, select "Add/Remove Snap-in".



4. Click on "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	
Description	
Add Remove 🔓 About	
ОК Са	ancel

5. Select "IP Security Policy Management".

Snap-in	Vendor	1
🕄 Group Policy Object Editor	Microsoft Corporation	1
😫 Indexing Service	Microsoft Corporation, I	
晃 IP Security Monitor	Microsoft Corporation	
晃 IP Security Policy Management .	Microsoft Corporation	
Link to Web Address	Microsoft Corporation ら	
🕵 Local Users and Groups	Microsoft Corporation	
🕎 Performance Logs and Alerts	Microsoft Corporation	
PRemovable Storage Management	Microsoft Corporation	-
🕄 Resultant Set of Policy	Microsoft Corporation	
🞐 Security Configuration and Analysis	Microsoft Corporation	1
Description nternet Protocol Security (IPSec) Adminis policies for secure communication with ot		

6. Select "Local Computer" then finish.

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 if a member Another Active Directory domain (Use the DNS name, e.g. "example.microsoft.com"): Another computer: Browse
K Back Finish Cancel

7. Click on "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 🗸 🗸	
IP Security Policies on Local Computer	
Description	
Description Internet Protocol Security (IPSec) Administration. Manage IPSec policie	is 🔼
for secure communication with other computers.	
	<u> </u>
Add Remove About	
ок са	ancel

8. You will see the console screen with security policy added.

File Action					Policies on Local Comp				
	•••••				, solo				
		±⊛	<u> </u>		-	1	1	1	
Console Root	· Policies	oploca	Com	uter	Name /	Description	Policy Assigned		
C IF Security	POILLES	ULLUCA	ii Cuint	uter		Communicate normally (uns For all IP traffic, always req			
					Secure Server (Requir.	 For all IP traffic, always req For all IP traffic, always req 	. No		
					Derver (Kequest Detu.	Tor airte trainc, aways req	. 140		
					↔				

 Right click on IP Security Policy on Local Computer → Create IP Security Policy.

🖀 Console1 - [Console Root\l	⁹ Security	Policies on Local Compu	ter]			- 7 🛛
📸 File Action View Favorites	: Window	Help				_ 8 ×
← → 🗈 🖬 🚯 😫	1 🗎 📩					
Console Root	Create IP Manage IF All Tasks View	ow from Here ad View	Description promunicate normally (uns y all IP traffic, always req n all IP traffic, always req	No		
Create an IP Security policy		*				

10. Please name the policy.

Security P	olicy Wizard				?
	Policy Name	and provide a briel	f description		
Name:					
XP to 3	460				
Descript	ion:				
					<u>^</u>
					~
					<u>×</u>
		C	< Back	Next>	Cancel

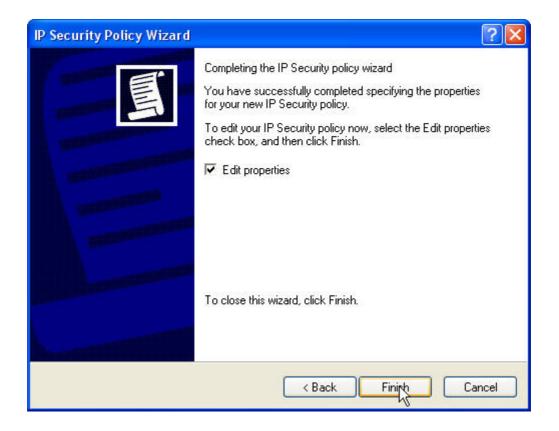
11. Next.

IP Security Policy Wizard
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.
< Back Nerty Cancel

12. Use the Preshared Key, in this example we use "12345678".

이상에 가지 않는 것 같은 것 같은 것 같아요. 가슴에 가지 않는 것 같이 많이 많이 많이 없다.	ation methods, edit the default respo	nse rule after
Set the initial authentication	on method for this security rule:	
C Active Directory defau	ult (Kerberos V5 protocol)	
C Use a certificate from	this certification authority (CA):	
		Browse
Use this string to prote	ect the key exchange (preshared key	y):
Use this string to prote 12345678	ect the key exchange (preshared key	ı): A
	ect the key exchange (preshared key	ı):
	ect the key exchange (preshared key	ı):
	ect the key exchange (preshared key	ı):

13. Click on Finish.



14. In this screen, please disable "use add wizard" and "dynamic". Then click on add button.

XP to 3460 Properti	es	? 🛛
Rules General		
Security ru	les for communicating with	other computers
IP Security rules:		
IP Filter List	Filter Action	Authentication Tu
Oynamic>	Default Response	Preshared Key Nc
Add	Edit Remove	Use Add Wizard
		Close Cancel

From this step, the snapshots show the finished setting. Please follow the same configuration as shown. You will need to create XP to 3460 and 3460 to XP 2 policies.

XP to 3460 Proper	ties	?
Rules General		
	ules for communicating with	other computers
IP Security rules:	Filter Action	Authentication Tu
☑ XP to 3460	Require Security	Preshared Key 61.
☑ 3460 to XP □ <dynamic></dynamic>	Require Security Default Response	Preshared Key 22(Preshared Key No
Add	Edit Remove	Use Add Wizard
	ОК	Cancel Apply

16. We can start with XP to 3460 first. Please configure as shown below.

Edit Rule Properties	? 🛛
IP Filter List	unnel Setting Connection Type Filter Action
The selected IP filter I affected by this rule.	list specifies which network traffic will be
O 3460 to XP	Description
O All ICMP Traffic O All IP Traffic O All IP Traffic O XP to 34	Matches all ICMP packets betw Matches all IP packets from this
Add Edit	Remove
	OK Cancel Apply

Name: XP to 3460			
Description:			Add
	L	<u>A</u>	Edit
		~	Remove
Filters:		Γι	Jse Add Wizard
Mirrored Description	Protocol	Source Port	Destination
No	ANY	ANY	ANY

Filter Properties	? 🛛
Addressing Protocol Descrip Source address: My IP Address	ption
A specific IP Subnet	
IP address: Subnet mask:	192 . 168 . 0 . 0 255 . 255 . 255 . 0
Mirrored. Also match pack destination addresses.	kets with the exact opposite source and

t Rule Properties	?
Authentication Methods	Tunnel Setting Connection Type Filter Action
The selected filter a for secure network	action specifies whether this rule negotiate traffic, and how it will secure the traffic.
Filter Actions: Name	Description
O Permit	Permit unsecured IP packets to
 O Request Security (Optional) O Require Security 	Accepts unsecured communicat Accepts unsecured communicat
Add Edit	Remove Use Add Wizard

equire Security	y Properties		?
Security Methods Permit Block Negotiate sec Security method p			
AH Integrity	ESP Confidential	ESP Integrity	Add
<none> <none></none></none>	3DES 3DES	MD5 MD5	Edit
<none> <none></none></none>	DES DES	SHA1 MD5	Remove
			Move up
<		>	Move down
	cured communication, b red communication with perfect forward secrecy	non-IPSec-aware	a contra de la contr
	OK	Cancel	Apply

Modify Security Method	? 🗙
Security Method	
 Encryption and Integrity Data will be encrypted and verified as authentic and unmodified 	
C Integrity only	
Data will be verified as authentic and unmodified, but will not be encrypted	
Custom	
Settings	
OKCar	ncel

Custom Security Method Setting	gs 🛛 🕐 🔀
Specify the settings for this custom sec Data and address integrity without a Integrity algorithm:	
MD5 Data integrity and encryption (ESP) Integrity algorithm: MD5	
Encryption algorithm: 3DES Session key settings:	
Generate a new key every:	Generate a new key every
	OK Cancel

17. The end point is the WAN IP address of WBR-3460.

Edit Rule I	Properties		? 🛛
Authent	IP Filter List ication Methods The tunnel endpo	 Tunnel Setting pint is the tunneling	Filter Action Connection Type computer closest to the the associated IP filter
The tilde	list. It takes two m ule does not specify a unnel endpoint is spec 1 . 31 . 189 . 1	cified by this IP add	
		Close	Cancel Apply

t Rule Properties		?
IP Filter List	e., 1	Filter Action
Authentication Metho	ds Tunnel Setting	g Connection Type
between offered a computer		
Authentication method Method	preference order: Details	Add
Preshared Key	12345678	Edit
		Remove
		Move up
		Move down
	Close	Cancel Apply

Edit Authentication Method Properties	? 🛛
Authentication Method	
The authentication method specifies how trust et al. between the computers.	t is established
Active Directory default (Kerberos V5 protocol)	
C Use a certificate from this certification authority (CA):	
	Browse
Use this string (preshared key):	
12345678	~
ОК	Cancel

18. Finish XP to 3460.

P Security rules:		
IP Filter List	Filter Action	Authentication
🗹 XP to 3460	Require Security	Preshared Key 61
🗹 3460 to XP	Require Security	Preshared Key 22
Cynamic>	Default Response	Preshared Key N
	10	>

19. Configure 3460 to XP.

Edit Rule Properties	? 🛛
IP Filter List	nnel Setting Connection Type Filter Action specifies which network traffic will be
IP Filter Lists:	Description
 3460 to XP All ICMP Traffic All IP Traffic XP to 3460 	Matches all ICMP packets betw Matches all IP packets from this
Add Edit	Remove
40	Cancel Apply

Name: 3460 to XP			
Description:			Add
		~	Edit
		~	Remove
Filters:		Γ	Use Add Wizard
Mirrored Description	Protocol	Source Port	Destination
No	ANY	ANY	ANY

Filter Properties
Addressing Protocol Description Source address:
Destination address: My IP Address
Mirrored. Also match packets with the exact opposite source and destination addresses.
OK Cancel

t Rule Properties	?
Authentication Methods	Tunnel Setting Connection Type Filter Action
The selected filter a for secure network	action specifies whether this rule negotiate traffic, and how it will secure the traffic.
Filter Actions: Name	Description
O Permit	Permit unsecured IP packets to
 O Request Security (Optional) O Require Security 	Accepts unsecured communicat Accepts unsecured communicat
Add Edit	Remove Use Add Wizard

equire Security Pro	operties		?
Security Methods Gen Permit Block Negotiate security: Security method prefer	eral		
ESP Confidential	ESP Integrity	Key Lifetime	Add
3DES 3DES	MD5 MD5	0 / 3600 100000 / 90	Edit
DES DES	SHA1 MD5	100000 / 90 100000 / 90	Remove
			Моче ир
<	.100		Move down
 Accept unsecured Allow unsecured or Session key perfection 	ommunication with	n non-IPSec-aware	
	ОК	Cancel	Apply

Modify Security Method	? 🔀
Security Method	
 Encryption and Integrity Data will be encrypted and verified as authentic and unmodified 	
C Integrity only	
Data will be verified as authentic and unmodified, but will not be encrypted	
Custom	
Settings	
OK Ca	ancel

Custom Security Method Settin	gs 🛛 💽 🔀
Specify the settings for this custom sec Data and address integrity without Integrity algorithm	
MD5 Data integrity and encryption (ESP) Integrity algorithm:	:
MD5 💌	
Encryption algorithm:	
3DES 💌	
Session key settings: Generate a new key every: 100000 Kbytes	Generate a new key every
	OK Cancel

20. The end point is the WAN IP address of Windows 2000/XP.

Edit Rule Properties		? 🛛
IP Filter List Authentication Methods	 Tunnel Setting	Filter Action
IP traffic destinat		computer closest to the the associated IP filter IPSec tunnel.
 This rule does not specify The tunnel endpoint is spe 		ress:
220.135.111.	99	
	Close	Cancel Apply

t Rule Properties		?
IP Filter List	e., 1	Filter Action
Authentication Metho	ds Tunnel Setting	g Connection Type
between offered a computer		
Authentication method Method	preference order: Details	Add
Preshared Key	12345678	Edit
		Remove
		Move up
		Move down
	Close	Cancel Apply

Edit Authentication Method Properties	
Authentication Method	
The authentication method specifies how trust is established between the computers.	Ъ
Active Directory default (Kerberos V5 protocol)	
C Use a certificate from this certification authority (CA):	
Browse	
Use this string (preshared key):	
12345678	~
OK Canc	el

^o Security rules:		
IP Filter List	Filter Action	Authentication
🗹 XP to 3460	Require Security	Preshared Key 61
☑ 3460 to XP	Require Security	Preshared Key 22
Clynamic>	Default Response	Preshared Key N
<		3

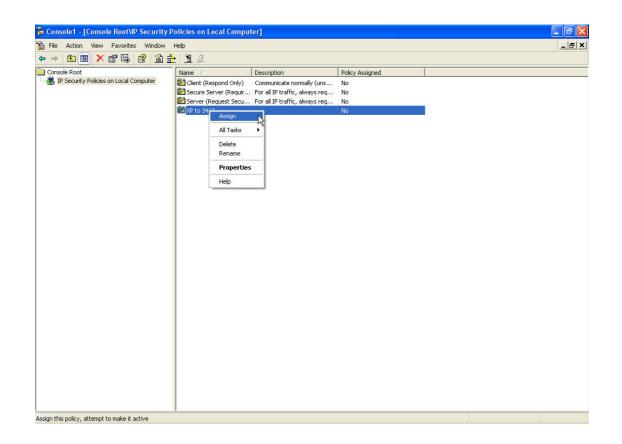
21. Click on General Tab. Configure as below.

(P to 3460 Properties	? 🛛
Rules General	
IP Security policy general properties	
Name:	
XP to 3460	
Description:	
	~
	<u>×</u>
Check for policy changes every:	
ninuce(s)	
Perform key exchange using these settings:	
Advanced	
OK Cancel	Apply
	and a second

curity method p	preference order:		
Encryption	Integrity	Diffie-Hellman	Add
3DES	MD5	Low (1)	7
3DES	MD5	Medium (2)	Edit
DES DES	SHA1 MD5	Low (1) Low (1)	Remove
200	,	1	Move up
		>	Move dowr

IKE Security Algorithms	? 🗙
Integrity algorithm:	
MD5	
Encryption algorithm:	Ν
3DES 💌	45
Diffie-Hellman group:	
Low (1)	
ОК	Cancel

22. Once complete, return to the console screen, right click on the policy and select "assign" to activate.



Below is the sample configuration for WBR-3460 VPN server

23. Please do not forget to enable the VPN tunnel.

ile Edit View Favorites Tools He		
3 Back - 🜔 - 💽 🛃 🐔	🔎 Search 👷 Favorites 🚱 🔗 - 🌺 🔜	
dress 🗃 http://192.168.0.1/vpn_list.htm		🔽 🄁 Go 🛛 Links
	VPN Policies	
Ē	# Enable Name Endpoint Type Local LAN Remote LAN ESP • 1 1 test2 n/a Auto 192.168.0.1 / 255.255.255.0 3DES	
	Add Auto Policy Add Manual Policy VPN Status Help	
	X	

24. Sample configuration of WBR-3460 VPN.

General	Policy Name: test2
	Remote VPN Endpoint
	Address Type: Dynamic IP address 🛛 🔽
	Address Data: <mark>n/a.</mark>
	NetBIOS Enable
Local LAN	IP Address Subnet address 👻
	IP address: 192 168 0 1
	Subnet Mask: 255 255 0
Remote LAN	
Remote LAN	IP Address Single PC-no Subnet 💌
	IP address: ^^ Subnet Mask
IKE	Direction Responder only
	Exchange Mode Main Mode 🗹
	Diffie-Hellman (DH) Group Auto
	Local Identity Type WAN IP Address 🗸
	Data n/a.
	Remote Identity Type IP Address
	Data n/a
	n Baid
SA Parameters	Encryption: 3DES 💌
	Authentication: Auto 🖂
	Pre-shared Key. 12345678
	SA Life Time: 28800 (Seconds)
	Enable PFS (Perfect Forward Security)

25. Ping from Windows 2000/XP VPN Client to WBR-3460 via VPN tunnel.

es D:\	WINDO	WS\system32\cm	nd.exe - pin	g 192.168.0.1		- 🗆 ×
		192.168.0.1:				
		192.168.0.1:				
		192.168.0.1:				
		192.168.0.1:				
		192.168.0.1:				
		192.168.0.1:				
		192.168.0.1:				
		192.168.0.1:				
		192.168.0.1:				
		192.168.0.1:				
		192.168.0.1:				
		192.168.0.1:				
		192.168.0.1:				
		192.168.0.1:				1
Reply	from	192.168.0.1:	bytes=32	time=109ms	TTL=255	
		192.168.0.1:				
		192.168.0.1:				
Reply	from	192.168.0.1:	bytes=32	time=250ms	TTL=255	
Reply	from	192.168.0.1:	bytes=32	time=203ms	TTL=255	
Reply	from	192.168.0.1:	bytes=32	time=187ms	TTL=255	
Reply	from	192.168.0.1:	bytes=32	time=156ms	TTL=255	
		192.168.0.1:				
Reply	from	192.168.0.1:	bytes=32	time=187ms	TTL=255	
Reply	from	192.168.0.1:	bytes=32	time=125ms	TTL=255	