Prepared by SonicWALL, Inc. 01/03/2002

Introduction

Despite its many similarities to Windows 2000, Microsoft's Windows XP is very much a different product. Microsoft designed XP with security in mind, and among the implications of this focus was a redesign of the networking subsystem. Because of these changes, VPN clients that worked with Windows 2000 do not work with Windows XP. Most VPN client vendors, SonicWALL included, do not yet have available a VPN client that works with XP, causing some difficulty for those enterprises looking to deploy Microsoft's latest OS. Both Windows XP and its predecessor Windows 2000 have VPN support built in—PPTP and L2TP—but neither of these is compatible with standard IPSec VPN's, despite the fact that the latter is a subset of the IPSec standard. This precludes the better-known VPN capabilities from natively connecting to another *true* IPSec endpoint, such as that offered by a SonicWALL.

Fortunately, Microsoft also saw fit to include true IPSec capabilities in 2K and XP, but they did not wrap them in a friendly wizard. With a few minutes of configuration via the MMC, however, it is quite simple to set up Windows XP as a VPN client to a SonicWALL VPN. This will allow current XP clients to remotely and securely access their SonicWALL protected corporate networks, and will also allow those enterprises that have been delaying XP deployment because of VPN access considerations to deploy immediately.

Configuring an IPSec VPN between Windows XP and a SonicWALL requires no changes to the SonicWALL configuration. This document assumes the SonicWALL is configured with an existing GroupVPN, and it will illustrate step-by-step how to complete the Windows XP client side configuration.





TECHnotes

(A) Conicilial Lade	ministration Missocoft Totawat Evalueur provided by MaasEvalueur				
File Edit View	Favorites Tools Help				
Address 🙆 http://1	92.168.168/management.html 💽 💽 Go 🔇 Back	- 🕥 - 🗷 🖻 🚳	🔎 Search 🛛 👷 Favorite	es 🜒 Media 🦑) 🖉 • 🗟 🖬 • 🔽
SONICWALL General	VPN Summary Configure RADIUS Certificates				🕑 Help 🚔
Log	Add/Modify IPSec Security Associations				
Filter Tools Access	Security Association IPSec Keying Mode Disable This SA	GroupVPN KE using pre-shared	secret 💌		
Advanced DHCP	Security policy	THE			
VPN	Kequre XA (only allow	s VPN clients)			
Anti-Virus	Forward packets	o remote VPNs 🔲			
High Availability	SA	Life time (secs) 2880	0		
	Encryption Method Encrypt and A	uthenticate (ESP DES I	HMAC MD5)	~	
	Shared Secret 0123M00SE3	210			
	VPN Client C	onfiguration File Exp	ort		Update Reset
Logout	STATUS: The configuration has been updated.		Exi	t	Internet

Using the Windows XP VPN Client with SonicWALL Internet Security Appliances

Figure 1. SonicWALL VPN Configuration Screen, GroupVPN.

Figure 1 shows the GroupVPN configuration screen. Any of the values on this page can be changed and the Windows XP client can be configured accordingly, but for the sake of this example, we will leave everything except the Shared Secret Key at its default value. The guide also assumes that the SonicWALL is fully configured and operational, and that VPN connectivity has been tested from a knownworking client. The information we need from the existing SonicWALL configuration is:

- The WAN IP Address (assuming 172.16.0.254)
- The LAN Subnet (assuming 192.168.168.0/24)
- The IPSec Keying Mode (assuming default IKE Using Pre-Shared Secret)
- The Encryption Method (assuming default ESP DES HMAC MD5)

The component of Windows XP that we will use to configure our Client VPN is called **secpol.msc**, a snap-in for the MMC, the Microsoft Management Console. You can launch **secpol.msc** a number of different ways, the easiest of which is to click **Preserve** then select **Run...** and type **secpol.msc** and hit **Enter**. This will launch the MMC:

SONICWALL

Decal Security Settings		- 2
File Action View Help		
Security Settings Cocount Policies Coco	Name	

Figure 2. The Secpol.msc MMC Snap-In Main Screen.

From the default view, right click on "IP Security Policies on Local Computer" and select "Create IP Security Policy..."

Docal Security Setting			8
File Action View Help			
⇔ → X 🖪 😫			
Security Settings Count Policies Co	Volicies	on Policies Local Computer	
Create an IP Security policy			

Figure 3. Creating a new IP Security Policy Step 1.

A wizard will appear. Click "Next" to bring up the following screen:



IP Security Policy Wizard		2 🛛
IP Security Policy Name Name this IP Security policy and provide a brief	of description	三
Name:		
SonicWALL VPN		
Description:		
		<u> </u>
[< Ba	t > Cancel

Figure 4. Naming the IP Security Policy.

Name the IP Security Policy "SonicWALL VPN" (or whatever you wish) and optionally enter a description. Click "Next". The next screen that appears will ask if you want to enable the "Default Response Rule." DESELECT this box, we do not wish to leave this rule enabled:

IP Securit	y Policy Wizard				?
Reque Sp	sts for Secure Comm ecify how this policy respo	unication onds to requests for	secure commu	nication.	Ē
The oth sec	e default response rule re er rule applies. To commu ure communication.	sponds to remote co inicate securely, the	omputers that re computer mus	equest security, w t respond to requ	hen no ests for
	Activate the default resp	onse rule.			
			< Bac	Next >	Cancel

Figure 5. Deselecting the Default Response Rule.

After clearing the "Default Response Rule", click "Next". Leave the "Edit Properties" checkbox selected, and click "Finish".





Figure 6. Completing the Policy Wizard.

The Properties page will appear and will include a default rule. We will leave this rule deselected, and will add two rules of our own: one for traffic from our client to the SonicWALL ("SNWL Filter"), and one for return traffic ("SNWL Filter Return"):

w IP Security Polic Rules General	y Properties		?
Security ru	les for communicating with	other computers	
IP Security rules:			
IP Filter List	Filter Action	Authentication	Tu
Comparent Com	Default Response	Kerberos	No
	III		>
<u>Add</u>	Edit	Use Add <u>W</u>	<u>/</u> izard
		ОК Са	ancel

Figure 7. Adding Rules to the IP Security Policy.

Deselect the "Use Add Wizard" and click "Add" to add the first of our two Rules and Filters:



Rule Properties	2
Authentication Methods Tur IP Filter List	nnel Setting Connection Type Filter Action
The selected IP filter list	specifies which network traffic will be
P Filter Lists:	
Name	Description
O All IP Traffic	Matches all IP packets from this

Figure 8. Default Rule/Filter List Page.

Click "Add". We will define the outbound traffic Filter. Name the filter ("SNWL Filter") and enter an optional description. Clear the "Use Add Wizard" button and click "Add":

SNWL Filter			
Description:		(Add
Traffic from Client to SNWL		~	Edit
			Remove
Filters:			Use Add Wizard
Mirrored Description	Protocol	Source Port	Destinatio

Figure 9. Adding the first Filter.

The "Filter Properties" page will appear (Figure 10). Deselect the "Mirrored" box. Enter the Source and Destination addresses for this Filter. For the source address we will select "Any IP Address". This will allow for tunnel initiation from any network interface on your machine. (Note: If you only wish to allow initiation from a particular address, select "A Specific IP Address" and enter the address of the interface

Page 6 of 19



you wish to allow.) The destination address will be the LAN segment of the remote/corporate network behind the SonicWALL (192.168.168.0 255.255.255.0):

Source address: Any IP Address				J
Destination address:				
A specific IP Subnet			2	-
IP address:	192 .	168	. 168	. 1
Subnet mask:	255 .	255	. 255	. 1
Mirrored. Also match pack	ets with the e	exact o	pposite <mark>s</mark> o	urce a
destination addresses.				

Figure 10. Adding Source and Destination Addresses to "SNWL Filter".

Click "OK" and select the "SNWL Filter" button. Select the "Filter Action" tab:

Authentication Methods Tu IP Filter List	unnel Setting Connection Ty Action
The selected IP filter lis affected by this rule.	st specifies which network traffic wil
IP Filter Lists:	
Name	Description
O All ICMP Traffic O All IP Traffic	Matches all ICMP packets betw. Matches all IP packets from this
O SNWL Filter	Traffic from Client to SNWL
Add Edit	Remove

Figure 11. Selecting the Filter to Configure.



This will bring up the "Filter Action" screen with the three default actions. Leave these deselected. We will create a new action by clearing the "Use Add Wizard" and clicking the "Add" button, as illustrated in figure 12:

w Rule Properties	
Authentication Methods	Tunnel Setting Connection Type Filter Action
The selected filter a for secure network t	ction specifies whether this rule negotiate raffic, and how it will secure the traffic.
Filter Actions:	Description
O Permit O Request Security (Optional) O Require Security	Permit unsecured IP packets to Accepts unsecured communicat Accepts unsecured communicat
	Close Cancel Apply

Figure 12. Adding a Filter Action for "SNWL Filter".

On the Filter Action Properties screen (figure 13) clear the "...unsecured communication..." boxes toward the bottom, select "Negotiate Security" at the top, and click "Add":





Туре	AH Integrity	ESP Confidential ES	Add
			Edit
			Remove
			Move up
<	100	>	Move dowr

Figure 13. Defining Filter Action Properties

Under "Security Method" select "Custom" and then "Settings" (figure 14):

	New Security Method	2 🛛
	Security Method	
	C 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	
	ttings	
	OK Can	

Figure 14. Selecting Custom Security Method.

We will now select a security method to match the configuration of our SonicWALL GroupVPN (ESP DES HMAC MD5). You can leave the Session Key settings at default (never timeout) or change them as you wish:

Page 9 of 19



Data ani	d address inte	grity without	encryption (Al	H) :
Integrity	algorithm:			
MD5		Ŧ		
Data inte Integrity	egrity and enci algorithm:	ryption (ESP):	
MD5		-		
Encrypti	on algorithm:			
DES		•		
Session ke	ey settings: — rate a new ke Kbytes	y every:	Gener	ate a new key every

Figure 15. Defining a Custom Security Method.

Click "OK" a few times to return to the "New Rule Properties" screen. Select the filter action ("SNWL Filter") you just created:

Authentication Metho ng Connection Trendstring IP Filter List Filter Action IP Filter List Filter Action Image: Secure network traffic, and how it will secure the traffic Filter Actions: Name Description Permit Permit unsecured IP packets to Accepts unsecured communicat Accepts unsecured communicat SNWL Filter Action Security Setting for SonicWALL	w Rule Properties		
IP Filter List Filter Action Image: Secure Relation Specifies whether this rule negot for secure network traffic, and how it will secure the traffic Filter Actions: Name Description Permit Permit unsecured IP packets to Accepts unsecured communicat Accepts unsecured communicat SNWL Filter Action SNWL Filter Action Security Setting for Sonic/WALL	Authentication Metho	ing Connection Typ	
Add Edit Femore Use Add Wit	IP Filter List	Filter Action	
Name Description Pemit Permit unsecured IP packets to Request Security (Optional) Accepts unsecured communicat SNWL Filter Action Security Setting for Sonic/WALL Add Edit	The selected filter acti for secure network tra	on specifies whether this rule negotia ffic, and how it will secure the traffic.	
Name Description Permit Permit unsecured IP packets to Accepts unsecured communicat Accepts unsecured communicat SNWL Filter Action SNWL Filter Action Security Setting for SonicWALL	Filter Actions:		
Permit Permit unsecured IP packets to Accepts unsecured communicat Accepts unsecured communicat Accepts unsecured communicat SNWL Filter Action Security Setting for SonicWALL Add Edit Bemove Use Add Wi	Name	Description	
Accepts unsecured communicat Accepts unsecured communicat Accepts unsecured communicat SNWL Filter Action Add Edit Femove Use Add Wi	O Permit	Permit unsecured IP packets to	
Require Security Accepts unsecured communicat SNWL Filter Action Security Setting for SonicWALL	O Request Security (Optional)	Accepts unsecured communicat.	
SNWL Filter Action Security Setting for SonicWALL	O Require Security	Accepts unsecured communicat	
Add Edit Bemove T Use Add Wi	O SNWL Filter Action	Security Setting for SonicWALL.	

Figure 16. Selecting the Defined Filter Action.

Select the "Tunnel Settings" tab, and specify the WAN address of your SonicWALL:



1

IP	Filter List	_ 1	Filter Acti	on
Authenticatio	on Methods	Tunnel Setting	Conr	nection Typ
	The tunnel endp IP traffic destina ist. It takes two	point is the tunneling tion, as specified by rules to describe an	computer c the associa IPSec tunn	losest to th ted IP <mark>filt</mark> er el.
C This rule of	lose not ensoitu	an IPSac tunnal		
 Inis rule d 	ives not specify	an ir sec tunnel.		
The tunne	endpoint is spe	ecified by this IP add	ress:	
The tunne	el endpoint is species of the second se	ecified by this IP add	ress:	
The tunne	el endpoint is special de la special de l 16.0.1	ecified by this IP add	ress:	
The tunne	el endpoint is specific de la specif	ecified by this IP add 254	ress:	
The tunne 172	el endpoint is spe	ecified by this IP add	ress:	
The tunne The tun	el endpoint is spo	ecified by this IP add	ress:	
	el endpoint is spo	ecified by this IP add	ress:	
€ The tunne	el endpoint is spo	ecified by this IP add	ress:	

Figure 17. Set the Client to SonicWALL tunnel endpoint.

Select the "Authentication Methods" tab, highlight the default "Kerberos" method, and click edit, as illustrated in figure 18:

	100	
IP Filter List		Filter Action
Authentication Methods	Tunnel Setting	Connection Typ
Authenticatio between con offered and a computer.	n methods specify ho iputers. These auther accepted when negoti	w trust is established ntication methods are iating security with anothe
Authentication method pre Method	ference order: Details	Add
Kerberos		Edit
		Remove
		Move up
		Move down

Figure 18. Editing the Authentication Method.

Selecting "Edit" will allow us to specify our shared-secret key (0123MOOSE3210) that we retrieved from the SonicWALL GroupVPN configuration:

Page 11 of 19



(
Authenticati	on Method	
	The authentication method specifies how trust is between the computers.	established
C Active	Directory default (Kerberos V5 protocol)	
		Browse
I	<u> </u>	0101100
Use the set of the	is string (preshared key):	
	10	1
		2
		2

Figure 19. Entering the Preshared Secret Key.

Clicking "OK" will take you back to the "New Rules Property" page. We are now done with the first half of the configuration. The second half is considerably quicker, since most of our components are already defined. We will now build the Rule and Filters for traffic from the SonicWALL back to our Client.

Select the "IP Filter List" tab again, and click "Add", as illustrated in figure 20:

w Rule Properties	2	
The selected IP filter li affected by this rule.	unnel Setting Connection Type Filter Action	
IP Filter Lists:	Description	
O All ICMP Traffic	Matches all ICMP packets betw	
O All IP Traffic	Matches all IP packets from this	
O SNWL Filter	Traffic from Client to SNWL	
Add	Remove	

Figure 20. Adding a filter for return traffic.





This will bring up the now familiar "IP Filter List" screen. Name the filter list ("SNWL Filter Return"), enter an optional description, deselect "Use Add Wizard" and click "Add". This will bring up the Filter Properties screen:

IP Address:	
Subnet mask:	255 . 255 . 255 .
Mirrored. Also match pack	kets with the exact opposite source a
destination addresses	

Figure 21. Setting the Return Filter properties

Just as we did before, we will define the properties of this IP Security filter, only this time, we will reverse the flow. The Source Address will become the remote/corporate subnet (192.168.168.0 255.255.255.0), and the Destination Address will be "Any Address" (or whatever option you wish to select, as described earlier). Be sure to again clear the "Mirrored" box, and click "OK" twice. You will return to the "IP Filter List" screen, and it should now look as follows:



Page 13 of 19



Figure 22. The IP Filter List with both filters defined.

Click "Close" to return to the "SonicWALL VPN Properties - Rules" page. It should look as follows:

P Security rules:			
IP Filter List	Filter Action	Authentication	Tu
CDynamic>	Default Response	Kerberos	No
		1	

Figure 23. The "SonicWALL VPN Properties" Rules page.

Click "Add" and we will define the rule for return traffic. Figure 24 depicts the "New Rule Properties" view:

A alcontraction Medicade	Turnel Collins 1 Coursesting T	
IP Filter List	Tunner Setting Connection 1	
The selected IP fill	er list specifies which network traffic wi e.	
P Filter Lists:		
Name	Description	
O All ICMP Traffic	Matches all ICMP packets betw	
O All IP Traffic	Matches all IP packets from this	
O SNWL Filter	Traffic from Client to SNWL	
SNWL Filter Return	Traffic from SNWL to Client	
Add Edit.	Remove	

Figure 24. New Rule Properties.

Select the "SNWL Filter Return" button. Click on the "Filter Action" tab, and select the previously defined "SNWL Filter Action":

Page 14 of 19



Authentication Methods	Funnel Setting Connection Ty				
IP Filter List	Hiter Action				
The selected filter action specifies whether this rule negotiate for secure network traffic, and how it will secure the traffic.					
Filter Actions:					
Name					
O Fermit	Accents unsecured IP packets to				
C Request Security (Ontional)	Accente uneacurad communicat				
O Request Security (Optional) O Require Security	Accepts unsecured communicat. Accepts unsecured communicat.				
Request Security (Optional) Require Security SNWL Filter Action	Accepts unsecured communicat. Accepts unsecured communicat.				
Request Security (Optional) Require Security SNWL Filter Action	Accepts unsecured communicat. Accepts unsecured communicat.				
Request Security (Optional) Require Security SNWL Filter Action	Accepts unsecured communicat. Accepts unsecured communicat.				
Request Security (Optional) Require Security SNWL Riter Action	Accepts unsecured communicat. Accepts unsecured communicat.				
Request Security (Optional) Require Security SNWL Filter Action	Accepts unsecured communicat. Accepts unsecured communicat.				
Request Security (Optional) Require Security SNWL Filter Action	Accepts unsecured communicat. Accepts unsecured communicat.				
Require Security (Optional) Require Security SNWL Filter Action	Accepts unsecured communicat. Accepts unsecured communicat.				

Figure 25. Selecting the "SNWL Filter Action".

Next, select the "Tunnel Setting" tab, and enter the Client's IP address (assume 64.65.66.67). This is the only parameter that must be unique to the client's configuration:

Edit Rule Properties		(
IP Filter List	1	Filter Action
Authentication Methods	Tunnel Setting	Connection Type
IP traffic destinat list. It takes two r	oint is the tunneling o tion, as specified by t rules to describe an I	computer closest to the he associated IP filter PSec tunnel.
C This rule does not specify	an <mark>I</mark> PSec tunnel.	
The tunnel endpoint is spe	cified by this IP addr	ess:
1 04 . 05 . 00 .	07	
	OK	

Figure 26. Setting the return tunnel endpoint.

Select the "Authentication Methods" tab, once again, highlight the default "Kerberos" method, and click edit, as illustrated in figure 27:

Page 15 of 19



IP Filter List	1	Filter Action
Authentication Methods	Tunnel Setting	Connection Type
Authenticati between co offered and computer.	on methods specify how tr mputers. These authentica accepted when negotiatin	ust is established ation methods are g security with anothe
uthentication method pre	eference order:	Add
Kerberos	Details	Aud
		Edit
		Remove
		Move up
		Move dowr

Figure 27. Editing the Authentication Method.

Selecting "Edit" will allow us to specify our shared-secret key (0123MOOSE3210) that we retrieved from the SonicWALL GroupVPN configuration:

Authenticatio	n Method	6
	The authentication method specifies how trust is es between the computers.	tablished
C Active C Use a c	Directory default (Kerberos V5 protocol) certificate from this certification authority (CA):	rowse
© Use thi	s string (preshared key):	~
		2
	ОК	Cancel

Figure 28. Entering the Preshared Secret Key.

Clicking "OK" will return you to the "SonicWALL VPN Properties" page. It should now look as follows:





P Security rules:	for communicating with	other computers	
IP Filter List	Filter Action	Authentication	Tu
SNWL Filter	SNWL Rule 1	Preshared Key	17
SNWL Filter Return	SNWL Rule 1	Preshared Key	19
CDynamic>	Default Response	Kerberos	No
<	101]	>

Figure 29. The completed Rules page.

Click "Apply" and "Close" to return to the "Local Security Settings" master page:

⊢→ Ē ፼ ಔ ĝ 😫 📩			
Security Settings	Name 🔺	Description	Policy Assigned
Account Policies Local Policies Delicies Delicies Delicies Delicies Delicies Delicies Delicies IP Security Policies on Local Computer	Client (Respond Only)	Communicate normally (uns	No
	New IP Security Policy		No
	New IP Security Policy (1)		No
	Secure Server (Require Security)	For all IP traffic, always req	No
	Server (Request Security)	For all IP traffic, always req	No
	SonicWALL VPN	WinXP to SNWL GroupVPN	Yes
	1000 C		

Figure 30. Completed Local Security Settings page.

Right Click on the "SonicWALL VPN" Security Policy, and select "Assign". The policy is now active, and you should be able to bring up the VPN by initiating traffic to the 192.168.168.0 network; a ping should do. The first packet or few packets will initiate the VPN connection, and will display "Negotiating IP Security." Depending on the speed of your connection, the tunnel should come up after 1 to 10 ping packets:

Page 17 of 19



TECHnotes

Using the Windows XP VPN Client with SonicWALL Internet Security Appliances

ex Command Prompt	
C:\Documents and Settings\jlevy.MOOSELAND>ping 192.168.168.168	A
Pinging 192.168.168.168 with 32 bytes of data:	
Negotiating IP Security. Reply from 192.168.168.168: bytes=32 time=1ms TTL=64 Reply from 192.168.168.168: bytes=32 time=1ms TTL=64 Reply from 192.168.168.168: bytes=32 time=1ms TTL=64	
Ping statistics for 192.168.168.168: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 1ms Auximum = 1ms Auerage = 1ms	
minimum stus, nazimam stus, nyci ago stus	-

Figure 31. Negotiating the VPN with ICMP traffic.

You should now have VPN connectivity between you Windows XP client, and your SonicWALL VPN.





Supplement: Exporting and Importing the Windows XP Client VPN Settings

NOTE: Only use this option if there are no existing IP Security Policies defined on the export or import machines. Using this export/import method with other IP Security Policies present will yield unpredictable results. This method also assumes that Source and Destination addresses pertaining to the Client have been defined as "My IP Address" or "Any IP Address" and do not specifically define Client IP addresses.

This section is offered to speed the deployment of Windows XP to SonicWALL VPN configurations. It allows an administrator to configure the settings described above one time on a single Windows XP client, and to export the registry values containing that configuration for easy import by clients. The information contained within the exported registry data contains all defined network information and your shared-secret key and should be considered VERY SENSITIVE information. Treat it with care.

secpol.msc has its own built in import and export facility. Using the integrated facility is no more secure than the method presented below, but it does require a bit more user intervention. With ease in mind, it has been excluded. You can use it, if you wish, but it requires that the client launch secpol.msc, import the policy, change a setting, and then activate it. The method presented below requires double clicking a .reg file and modifying a single setting.

After you have successfully configured a Windows XP client for VPN access to your SonicWALL, you can export the associated registry information with the following command:

C:\> regedit /e C:\VPN.reg "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Micros oft\Windows\IPSec\Policy\Local"

This will export the settings to the file VPN.reg (about 160KB) in the root of your C:\ drive. Carefully distribute this file to clients, and remind them to treat the file with similar care. They can import these settings onto their workstation by double-clicking on the VPN.reg file and selecting "Yes" at the "Are you sure you want to add..." prompt. This will import and activate the policy. Now all the client must do is change the "SNWL Filter Return: Tunnel Setting: IP Address" value.

[Start], [Run] and type *cmd* and hit *Enter.* Type *ipconfig* and hit *Enter.* This will offer a basic view of interfaces and addresses. Note the address through which you want the VPN to be established. Type *secpol.msc* and hit *Enter*. This will launch the MMC. Double click the "SonicWALL VPN" Security Policy. Double click the "SNWL Filter Return" rule. Select the "Tunnel Setting" tab, and enter the correct IP address.

The client should then be able to bring the tunnel up by initiating traffic to the remote/corporate subnet.

Page 19 of 19

