SonicWALL VPN Client Configuration

A Tech Note prepared by SonicWALL, Inc.

SonicWALL, Inc. 1160 Bordeaux Drive Sunnyvale, CA 94089-1209 1-888-557-6642 http://www.sonicwall.com

Introduction

SonicWALL VPN includes one VPN Client for Windows (95, 98 or NT) license for secure remote management of the SonicWALL Internet Security Appliance.



Quick Configuration

Setting up your SonicWALL Internet Security Appliance

1. Click the button labeled VPN on the left side of the browser window and then click the tab labeled Summary

at the top of the window. A window similar to the following will be displayed

资 SonicWALL A	Iministration - Netscape	
Eile Edit View	20 Communicator Help	
👔 🦋 Bookmark	s 🦧 Gio to: http://192.168.168.1/management.html	V N
SONICWALL	VPN Summary Configure	🕜 HELP
GENERAL	Global IPSec Settings	
LOG	Enable VPN	
FILTER	Unique Firewall Identifier 0040100C9D4C	
TOOLS		
ACCESS	Current IPSec Security Associations	
ADVANCED	Name Destination Encryption Method	
DHCP	vpn client 169.254.0.1 - 169.254.255.254 ESP DES HMAC MD5 (IKE)	
VPN		
	Upda	te Reset
	STATUS: Ready	
d* =0=	Document Done	

 Check the Enable VPN checkbox and assign an alphanumeric name for the SonicWALL in the Unique Firewall Identifier field. The Unique Firewall Identifier may range from 4 to 32 characters in length.

Click the Update button. The operation will take a few seconds to complete. Once completed, a message confirming

the update will be displayed at the bottom of the Web browser window.

资 SonicWALL Ad	ministration - Netscape	_ 🗆 ×
Eile Edit View G	λο <u>C</u> ommunicator <u>H</u> elp	
Bookmark	s 🦺 Gio to: http://192.168.168.1/management.html	V N
SONICWALL	VPN Summary Configure	🕜 HELP 🔺
GENERAL	Add/Modify IPSec Security Associations	
LOG		
FILTER	Security Association: vpn client	
TOOLS	Nome unn client	
ACCESS	Mane you extend	
ADVANCED	IPSec Keying Mode: IKE	
DHCP		
VPN	Destination Network 169.254.169.22	
	Destination Subnet Mask 255.255.0.0	
	IPSec Gateway Address 0.0.0.0	
	Encryption Method Encrypt and Authenticate (ESP DES HMAC MD5)	
	Shared Secret S*0668af\$Dhsq#!	
	Delete This SA	
	Update	Reset
	STATUS: Ready	
g* -0-	Document: Done	

3. Click the **Configure** tab at the top of your screen. A window similar to the following will be displayed.

- 4. On the **Configure** page, create a new Security Association by selecting **Add New SA** from the **Security Association** menu.
- 5. Select IKE from the IPSec Keying Mode menu.
- 6. Enter a descriptive name that identifies the VPN client in the **Name** field, such as the client's location or name.
- 7. Leave the Destination Network, Destination Subnet Mask, and IPSec Gateway Address fields blank.
- 8. Select Encrypt and Authenticate (ESP DES HMAC MD5) from the Encryption Method drop down menu.
- Define a shared secret in the Shared Secret field. The alphanumeric shared secret must match the VPN client's Shared Key and may contain up to 128 characters. Create a Shared Secret that can not be guessed by

someone else. Avoid using names of friends, family, pets or places. Instead, enter a combination of letters, numbers and symbols, such as "Aa8*^Hjj@e\$FF#," for greater security.

Once all fields are completed, click the **Update** button. The operation will take a few seconds to complete. Once completed, a message confirming the update will be displayed at the bottom of the Web browser window. Restart the SonicWALL for changes to take effect.

Installing the VPN Client Software

- 1. When the SonicWALL product is registered at http://register.sonicwall.com, a unique VPN client serial number is returned, as well as a link to download the VPN client installer.
- 2. Double-click the installer and follow the VPN client setup program's step by step instructions. Enter the VPN client's serial number when prompted.
- 3. After the VPN client setup program has finished copying files to your computer, it will prompt you to restart your computer. Select **No, I will restart my computer later** and continue with the next section.

Configuring VPCom Adapter's TCP/IP Settings

1. Open the Network Control Panel. A window similar to the following will be displayed.

Network ? 🗙					
Configuration Identification Access Control					
The following network components are installed:					
Client for Microsoft Networks					
■脚 Realtek RTL8139 PCI Fast Ethernet					
TCP/IP -> Realter BTI 9139 PCI Fast Ethernet					
¥ TCP/IP -> VPCom Adapter					
📮 File and printer sharing for Microsoft Networks 🔹 💌					
Add Remove Properties					
Primary Network Logon:					
Client for Microsoft Networks					
<u>File and Print Sharing</u>					
Description TCP/IP is the protocol you use to connect to the Internet and wide-area networks.					
OK Cancel					

2. Double click the **TCP/IP VPCom Adapter** option in the network configuration window. A window similar to the following will be displayed.

Network			? ×	(
Configurati	on Identification Acc	ess Control						
The follo	wing <u>n</u> etwork componer	nts are installed:						
Client for Microsoft Networks								
🗐 Rea	🐨 Realtek RTL8139 PCI Fast Ethernet							
■ ØVPC	■⊉ VPCom Adapter							
TCP	VIP -> Realtek RTL8139	8 PCI Fast Ethernet	_					
e TUP	7IP -> VPLom Adapter							
Rep rile	TCP/IP Properties			? ×				
	Bindings	Advanced	NetBl	os)				
	DNS Configuration	Gateway WINS Cont	iguration IP	Address				
Primary	· · · ·							
Client f	An IP address can	be automatically assigned	ed to this comp	uter.				
	your network admir	histrator for an address, a	and then type i	tin				
<u>File</u>	the space below.							
Desci								
TCP/ wide-	C <u>O</u> btain an IP	address automatically						
mae .	- Specify an IP	address:						
	<u>o</u> provij uni							
	IP Address:	169.254.169	9.22					
	S <u>u</u> bnet Masł	< 255.255. O	. 0					
				ancel				

- Assign the VPCom adapter a private IP address. The IP address must be different from the SonicWALL's LAN subnet. Examples of private IP addresses are 10.0.0.0--10.255.255.255, 172.16.0.0--172.31.255.255, 169.254.0.0--169.254.255.255, and 192.168.0.0--192.168.255.255.
- 4. Assign the VPCom Adapter a subnet mask in the Subnet Mask field.
- 5. Click OK in both the TCP/IP Properties and Network windows and then restart the computer.

Configuring the VPN Client

To launch the VPCom Security Agent, select the program from the Windows Start menu, or double-click the VPCom Security Agent icon in the Windows Task Bar. A window similar to the following will be displayed.

VPCom Secu	irity Agent		1		×
	ent Policy	IPSec Auditin	g 🔩 ISAKN	4P Auditing 동탄	[
Gateway	Remote Host	Port Entry	Negotiate	IKE Setup	
- Security I	Policy Database	rity Policy Cor	figuration		
VPCON	1		ОК	Cancel	<u>A</u> pply

1. In the **VPCom Security Agent** window, highlight the **Security Policy Configuration** and click the **Gateway** button. A **Remote Security Gateway** window, similar to the following, will be displayed.

Remote Se	curity Gateway	×
	Description :	Main Office Security Policy
- Informatio	on	
í 🗟 😹	Server ID :	
V	IP Address :	209 . 100 . 100 . 100
	Domain Name :	
- Preshared	d Key	
	Shared Key :	RS%#7*5)0tft
OK		Cancel Policy

- 2. Assign a name for this Security Policy, such as "Main Office Security Policy," in the Description field.
- 3. Leave the **Server ID** field blank.
- 4. Type the IP address of the SonicWALL in the **IP Address** field. If Network Address Translation has been enabled on SonicWALL, then enter the **NAT Public Address**.
- 5. You may leave the **Domain Name** field blank.

- 6. Enter the SonicWALL's Shared Secret in the Shared Key field. Click OK.
- Highlight the newly created Security Policy (in this case "Main Office Security Policy") below the Security Policy Configuration and click the Remote Host button. A Remote Host window, similar to the following, will be displayed.

Remote Ho	st m Description :	Main Office LAN
- Informatio	n	
	Host Name :	
inni	IP Address :	192 . 168 . 168 . 1
	Subnet Mask :	255 . 255 . 255 . 0
	Domain Name :	
	OK	Cancel

- 8. Enter any descriptive name in the **Description** field.
- 9. You may skip the Host Name entry field.
- 10. Enter the SonicWALL's LAN IP Address in the **IP Address** field.
- 11. Type the SonicWALL's LAN Subnet Mask in the Subnet Mask field.
- 12. You may skip the **Domain Name** entry field. Click **OK**.

Negotiating a VPN Session Between VPN Client and the SonicWALL

Restart your computer. The VPN client will automatically establish a VPN tunnel if your computer has an active Internet connection when it is restarted. If it does not, you can manually negotiate a VPN tunnel by following the steps listed below:

 To complete the first phase of VPN negotiation, highlight the Security Policy (in our example " Main Office Security Policy") below the Security Policy Configuration and click the Negotiate button. This operation will take a few seconds to complete

 To complete the second phase of VPN negotiation, expand everything below the Security Policy Configuration by clicking the + symbols preceding each entry. A window similar to the following will be displayed.

VPCom Securi	ty Agent				×		
😻 VPN Clien	t Policy 🔄	IPSec Auditin	g 🛛 🗟 ISAKM	P Auditing			
		S					
Security Po	Security Policy Database						
	E-Secu E-M	nty Policy Con lain Office Se Main Office Sel Wildca	inguration curity Policy a LAN rd Connections				
VPCOM			пк	Cancel 1	Annlu		
01-00111					1177 T		

 Highlight Wildcard Connections and click the Negotiate button. This operation will take a few seconds to complete.

After successfully negotiating the VPN session, the administrator will be able to securely manage the remote SonicWALL by entering its LAN IP address in a browser on the computer running the VPN client software.