Enabling Group VPN on the SonicWALL

Click **VPN** on the left side of the SonicWALL browser window, and then click the **Configure** tab at the top of the window.

SonicWALI	_ Administr	ation - Micro	soft I	nternet Explorer			_	
Eile Edit ⊻ie	rw F <u>a</u> vorites	Tools Help						霰
4⇒Back ▼ ⇒	- 🕲 🖸 🖓	QSearch 🗟 Fi	avorites	: 🕲 History 🖓 🕶 🖼 💌 🖻 🤤	272			
Address 🔊 ht	tp://192.168.16	8.1/management.i	ntml				•	∂G0
SONICWALL	VPN Summary	Configure		RADIUS Certificates			@ H @	lp
	Global TPSe	c Settings						
Ciller		Uni	me Fir	ewall Identifier 0040100F1566				
Taala		V	Enable	VPN				
10015			Disable	e all VPN Windows Networking (N	etBIOS) broadcast			
Access		Г	Enable	Fragmented Packet Handling				
Advanced	Current TPS	las Saemite Ass	ocioti	220				
UNCP	Curencin	et betuny Ass	otrati	511.5				
VPN	<u>Disabled</u>	Name	Local	Remote	Encryption Method			
Anti-Virus		<u>GroupVPN</u>		0.0.0.1 - 255.255.255.254	ESP DES HMAC MD	5 (IKE)	¥ 0	
High Availability	•	Boston Office		192.168.168.1 - 192.168.168.254	ESP DES HMAC SH.	A1 (IKE)	ă D	
		Main Office		192.168.22.1 - 192.168.22.254	ESP 3DES	L	ă O	
		SAs enabled 2		SAs defined 3	SAs allowed 1001			
						Update	Res	et
Logout	STATUS, D	aadu						
 ຢ່າ	STATUS: N	eauy				Internet		

The SonicWALL **VPN** tab defaults to a **Group VPN** setting. This feature facilitates the set up and deployment of multiple VPN clients by the administrator of the SonicWALL appliance. Security settings can now be exported to the remote client and imported into the remote VPN client settings. **Group VPN** allows for easy deployment of multiple VPN clients as it eliminates the need to individually configure remote VPN clients. **Group VPN** is only available for VPN clients and it is recommended to use Authentication Service or XAUTH/RADIUS in conjunction with the Group VPN for added security.

To enable **Group VPN**, follow the instructions below:

- 1. Click **VPN** on the left side of the management station interface.
- 2. Click on Group VPN. The Security Association default setting is Group VPN.
- Configure the Group VPN to use either IKE using Preshared Secrets or IKE using Certificates. To use certificates, an Authentication Service upgrade must be purchased.
- 4. Select Group 2 from the Phase 1 DH Group menu.
- 5. Enter the **SA Life Time** value in minutes. A value of 28800 seconds (8 hours) is recommended.
- 6. Select **DES & SHA1** from the **Phase 1 Encryption/Authentication** menu.

- 7. Select Encrypt and Authenticate (ESP DES HMAC MD5) from the Phase 2 Encryption/Authentication menu.
- 8. Type the **Shared Secret** in the **Shared Secret** text box or use the **Shared Secret** automatically generated by the SonicWALL. The **Shared Secret** should consist of a combination of letters and numbers rather than the name of a family member, pet, etc. It is also case-sensitive.
- 9. Click **Advanced Settings** to open the window. Check any of the following boxes that apply to your SA:
 - Require XAUTH/RADIUS (Only allows VPN clients) if using a RADIUS server.
 - Enable Windows Networking (NetBIOS) broadcast if remote clients use Windows Network Neighborhood to browse remote resources.
 - **Apply NAT and firewall rules** to apply NAT and firewall rules to the SA or just firewall rules if in Standard mode.
 - Forward packets to remote VPNs if creating a "hub and spoke" network
 - Enable Perfect Forward Secrecy creates additional security by generating an additional Phase 2 DH key exchange.
 - Phase 2 DH Group generates a additional key exchange.
 - **Default LAN Gateway** The **Default LAN Gateway** field allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA
- 10. Click **Update** to enable the changes.

To export the **Group VPN** settings to remote VPN clients, click on **Export** next to **VPN Client Configuration File**. The security file can be saved to a floppy disk or e-mailed to a remote VPN client. The **Shared Secret**, however, is not exported, and must be entered manually by the remote VPN client.

Note: You must use the **Group VPN Security Association** even if you have only one VPN client to deploy. The **Group VPN Security Association** defaults to the **Simple Configuration** previously available in firmware version 5.1.1. If you have only one client to deploy, you may want to consider **Manual Key Configuration** for your appliance and client.

Installing the VPN Client Software

- 1. When you register your SonicWALL or SonicWALL VPN Upgrade at <http:// www.mysonicwall.sonicwall.com>, a unique VPN client serial number and link to download the SonicWALL VPN Client zip file is displayed.
- 2. Unzip the SonicWALL VPN Client zip file.
- 3. Double-click **setup.exe** and follow the VPN client setup program step-by-step instructions. Enter the VPN client's serial number when prompted.
- 4. Restart your computer after you have installed the VPN client software.

For detailed instructions on installing the client software, download the **Client Installation Guide** available at http:// www.sonicwall.com/documentation.html.

Group VPN Client Configuration

To import the Group VPN security policy into the Client, use the following steps:

1. Open the VPN Client. Click File, and then Import Security Policy.



2. A file location box appears which allows searching for the location of the saved security file. Select the file, and click **Open**.

Open			? ×
Look jn: 🖾	Downloads	• • •	▼≣ *
Group VPM	1_0040100C8D6E.spd		
File <u>n</u> ame:	GroupVPN_0040100C8D6E		<u>O</u> pen
Files of <u>type</u> :	Security Policy Database File (*.spo) 🔽	Cancel

 A dialogue box asking to import the security file appears. Click Yes, and another box appears confirming the file is successfully imported into the client. The client application now has an imported Group VPN policy. 4. Click the + sign next to Group VPN to reveal two sections: My Identity and Security Policy. Select My Identity to view the settings.

Security Policy Editor - SonicWALL VI <u>F</u> ile <u>E</u> dit <u>O</u> ptions <u>H</u> elp	PN Client	_ 🗆 X
	SON My Identity Select Certificate None ID Type Pott All V Internet Interface Name Arry IP Addr Arry	Pre Shared Key

5. Click **Pre-Shared Key** to enter the **Pre-Shared Secret** created in the **Group VPN** settings in the SonicWALL appliance. Click **OK**.

Pre-Shared Ke	у	×
Enter Key		
	Enter <u>P</u> re-Shared Key (at least 8 characters) This Key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".	
	OK Cancel	

 Select None in the Select Certificate menu, and select Domain Name in the ID Type menu. Enter any word or phrase in the field below the ID Type menu. Do not leave this field blank. 7. In the Internet Interface box, select the adapter used to access the Internet. Select PPP Adapter in the Name menu if you have a dial-up Internet account. Select your Ethernet adapter if you have a dedicated Cable, ISDN, or DSL line.

à®is×₽ †↓	SONICWALL
Department D	My Identity Selec Cystone Per Shared Kay Pore I D Type Port Are Port Ar

8. Click File, then Save Changes to save the settings to the security policy.

SONICWALL
Security Polog Security Pology Aggressive Mode C Use Manual Keys C Use Manual Keys Security Pology Security Pology Security Pology Employ Reyck Onter Helman Group 1 × Employ Reycky Detection

There is no need to configure the **Security Policy** as it is imported directly into the **Client** application. Exporting the security association to a file facilitates configuration of a large number of VPN clients and eliminates the need to configure each client individually.

Group VPN may also be configured using digital certificates in the **Security Association** settings. For more information on **Group VPN** configuration using digital certificates, refer to the **Authentication Service User's Guide** on the SonicWALL website: http://www.sonicwall.com/vpn-center/vpn-setup.html.