Global Information Assurance Certification Paper

Creating a Virtual Private Network with a SonicWALL Security Appliance

Scot Lymer

GSEC Practical (v.1.4b)
October 2, 2002

Abstract

This paper will describe how to create a Virtual Private Network using a SonicWALL Security appliance. The paper will begin by introducing the concept of a VPN, uses of a VPN, and which SonicWALL appliances support VPN connections. I will then discuss some of the issues that need to be considered before establishing a VPN connection such as which authentication method is best suited for the VPN. Next I will explain the steps required to create a VPN connection between the client and the remote LAN and finish by discussing some of the tools available to test the VPN connection.

What is a Virtual Private Network?

Today, more and more companies have employees who need access to their corporate LAN for access to email, files, etc. To this end, a Virtual Private Network (VPN) is a must and can be thought of as a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. With this secure remote connection comes seamless access to network resources without the need for expensive dial-up remote access connections or toll-free phone numbers. If a user is away from work and needs access to the corporate network he or she can choose a nationwide Internet Service Provider, dial the ISP's local number to get connected to the Internet, and then connect securely to the remote local area network (LAN). If the user is telecommunicating from home or working from a remote branch office and are lucky enough to have a broadband (cable or DSL) connection through their ISP he/she can easily access the corporate network from their home or home office. The user's authentication to the corporate LAN and data access is now securely handled through the VPN's encrypted tunnel.

There are several types of VPN connections that can be configured using a VPN-enabled device. The connections types are as follows:

1. **Client to LAN**. Used by mobile workers using dial-up Internet connections. A single VPN tunnel is used for each VPN client.
2. **LAN-to-LAN**. VPN's link two LANs together using a single tunnel that handles all the secure data traffic between two locations.
3. **Intranets**. VPN's allow remote offices and users to securely access internal TCP/IP applications running on the corporate Intranet.
4. **Extranets**. VPN's enable secure access to the corporate Extranet for vendors, partners, and customers.

Which SonicWALL Appliances offer a VPN?

The following table lists the SonicWALL appliances that support VPN connections, the number of security associations, and the throughput of the VPN.

	Tele3	Tele3 TZ	Tele3 SP	SOHO3	Pro 100	Pro 200	Pro 300	GX250	GX650
VPN Included	Yes	Yes	Yes	No (Upgrade)	Yes	Yes	Yes	Yes	Yes
# of SA's	5	5	10	10	50	500	1000	5000	10000
VPN Speed	20mbps	20mbps	20mbps	20mbps	20mbps	25 mbps	45 mbps	190 mbps	285 mbps

Table 1

VPN Preinstallation

Before installing a VPN an organization's security administrator should do some planning to determine who will need access to the VPN. Is the VPN going to be providing another branch office access to the corporate LAN? Will the user's accessing the VPN connect via a dial-up or a broadband connection? Will the VPN user be responsible for maintaining personal firewall and anti-virus software? If most VPN users will be using a dial-up Internet connection, the security administrator will need to meet with management to determine the best way to secure the remote user's personal computer such as installing and configuring a personal firewall and anti-virus software.

Also, user's wishing to access the network through the VPN can be authenticated in a couple of ways. One way is by encrypting the authentication through a shared secret key that is known to both parties. A shared-secret key is nothing more than a strong password that is configured at the VPN gateway and the client VPN software and is exchanged during the authentication stage. Not only is a weak shared-secret key a risk but also, while establishing the VPN connection both parties must exchange some "unsecured" data related to the establishment of the shared secret key before establishing the secure tunnel. There is no way for both parties to simultaneously "know" the secret key without some sort of non-encrypted initial exchange. Normally, that "non-encrypted initial exchange" takes place when the individual configures the shared key on both the VPN gateway and the VPN client.

The second and most secure method of authentication is through the use of digital certificates. A digital certificate is much like a drivers license and is used to verify the identity of a user. These certificates can be obtained from a third-party Certificate Authority such as Verisign (www.Verisign.com) or Entrust (www.Entrust.com) or they can be created through a local certificate request using the SonicWALL authentication service. The certificate method is referred to as PKI or Public Key Infrastructure where both parties use a public key for encrypting data and a private key used to decrypt the data. This solution is more secure than the shared secret key method because public keys are exchanged between both sending and receiving parties. Anyone wishing to see the data would need the private key to decrypt the data that was encrypted with the public key.

Creating a SonicWALL VPN requires the administrator to configure each client machine that wishes to access the corporate network through the VPN as well as configuration of the SonicWALL firewall appliance to accept or reject remote VPN connections.

As mentioned, clients wishing to access the VPN will connect to the Internet either through a dial-up ISP or through a broadband connection to an ISP. Both connection types require securing each client machine prior to installation of the VPN client software. A personal firewall or a hardware firewall is needed depending on the type of user's Internet connection. If a user connects by a dial-up modem a personal firewall is appropriate. A personal firewall is a piece of software that resides on the client machine and blocks unwanted traffic from entering or exiting their machine. Some popular host-based firewalls include Zone Alarm from www.Zonelabs.com and Black Ice from www.Iss.net. My personal favorite is Zone Alarm due to the ease of setup and various options such as blocking Internet servers, local servers, etc. If the user accesses the Internet from a cable modem or a DSL device a hardware firewall is recommended and a firewall such as the SonicWALL Tele3 TZ is recommended. It is crucial to the security of the VPN that the client maintain always on firewall protection of some sort to prevent rogue traffic from entering the corporate network via the internet connection.

VPN Architectures

There are 3 main types of VPN architectures. The first is a Mesh VPN where each VPN participant has a security association with all other VPN participants. For example, Chicago, Dallas, and St. Louis all have security associations defined for each other so each location can securely access the corporate LAN of each other site. The second VPN architecture is the hub and spoke VPN where each participant in the VPN has a security association with a central router that has a security association with every VPN device. The final architecture is the hybrid, which is a mixture of a mesh and a hub and spoke.

A SonicWALL VPN can be created to handle all of the above-mentioned VPN architectures and the design should be based on issues such as who needs access and to what resources and when do they need access, as well as total throughput desired, and the total number of VPN connections desired. The SonicWALL family of firewall appliances all support VPN connections to one degree or another. Refer to table 1 which describes each SonicWALL appliance and their VPN options.

VPN Firewall Installation

During installation of the VPN, the first decision the security administrator needs to make is how to organize the security associations. A security association is a group of settings related to the security requirements of a given VPN tunnel. The association can apply to a branch office or a group of users such as Sales Personnel, Field Engineers etc. These associations give the administrator the ability to create logical groupings of remote connections for users through several different VPN tunnels.

After determining the desired security associations etc. the next step is to configure the firewall for VPN connectivity. The administrator must log in to the firewall using the administrator account and password and select the VPN button and Configure. (See figure 1) Here the administrator is presented with the following screen that allows the administrator to create a new security association for the VPN clients. The administrator can select either IKE using Pre-shared Secrets or IKE using Certificates as well as name the association something descriptive such as "St. Louis Field Engineers" etc. The administrator can also disable the security association for troubleshooting purposes or if the corporate network situation changes the administrator may want to disable the VPN connection.

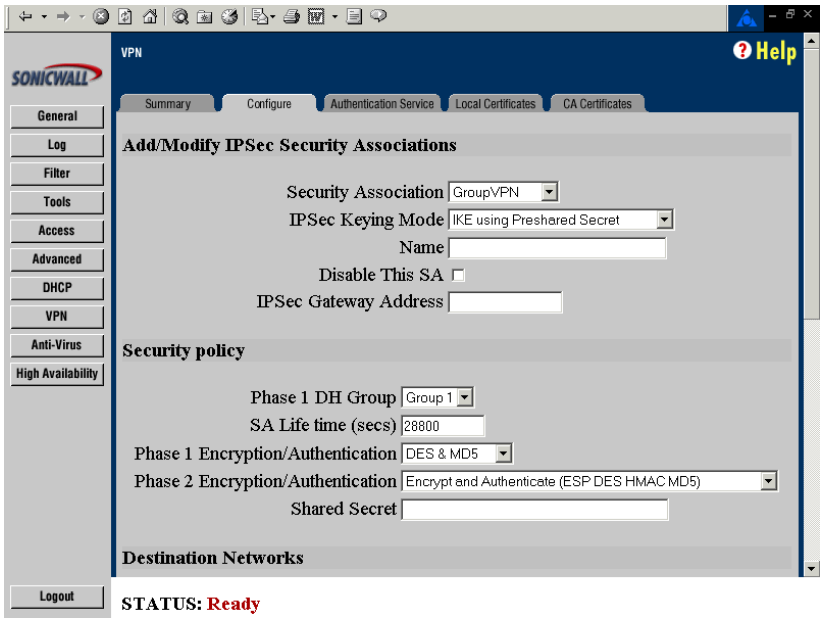


Figure 1

Under Security policy/Phase 1 DH Group the administrator can select between Group 1, 2, or 5 to determine the number of bits used for encryption. Group 1 uses 768 bits, Group 2 uses 1024 bits, and Group 5 uses 1536 bits. The bit length has a positive impact on security and a negative impact on speed and the option to set a bit-length is only available if "Enable Perfect Forward Secrecy" is selected in the advanced settings of the VPN configuration. (See figure 2) Perfect forward secrecy, in cryptography, of a key-establishment protocol, is the condition in which the compromise of a session key or long-term private key after a given session does not cause the compromise of any earlier session. Phase 1 of the VPN session deals with authentication between the client and the VPN gateway and Phase 2 handles the key exchange between the VPN client and VPN gateway. You also need to add the shared secret if not using certificates. After entering the information the administrator selects Update to save the security association settings.

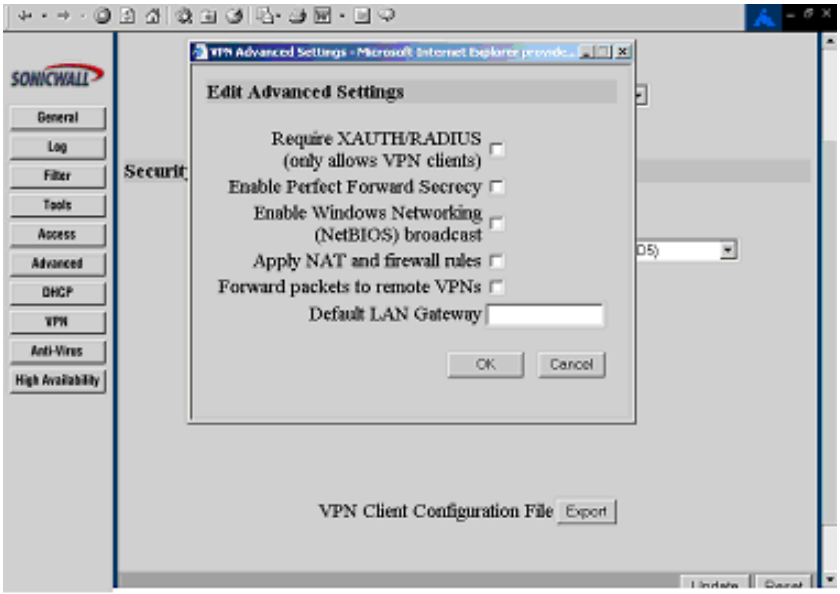


Figure 2

After configuring the group VPN settings such as Pre-shared Secret or Certificate and Phase 1 Diffie-Hellman settings select Advanced to configure additional settings including:

- Require authentication of VPN clients via Xauth- Authentication using a RADIUS Server. (A RADIUS server is a server maintaining a centralized database of users)
- Enable Packet Forward Secrecy- Adds an added layer of security to prevent compromise of prior session keys when long-term private key value is determined.
- Phase 2 DH Group- Generates an additional key exchange between client and VPN gateway for increased security
- Apply NAT and firewall rules- Apply rules created at the firewall.
- Forward packets to remote VPN's- Only used in hub and spoke configurations and sends IPSec packets to all VPN devices.
- Default LAN Gateway- enables specification of the default LAN to forward inbound IPSec traffic.

VPN Authentication and Encryption

There are some questions to consider when determining which VPN encryption method to use. Should data be encrypted and nothing else? Should there be assurances that the data has not been altered? Several methods exist to provide security of the Authentication Header of an IPSec packet and the actual data payload. Below is a table

explaining the options available and the benefits of each.

	DES	3DES	MD5	SHA-1
Uses	Used to encrypt and authenticate data	Used to encrypt and authenticate data	Used to ensure data has not been altered	Used to ensure data has not been altered
Key Length	56-bit key length	168-bit key length	128-bit value	160-bit value
Strengths	Resistant to most cryptanalysis attacks	Has not been cracked	Faster than SHA-1	Maximum Security
Weaknesses	Subject to brute-force attacks	Slower than DES	Minimum Security	Slower than MD5

Table 2

Note: Additional authentication and encryption options are available to connect other VPN devices such as a Checkpoint VPN Gateway, etc. to the SonicWALL VPN.

After completing the required settings for the security association and selecting Update the administrator can view the current security association settings, edit the current group VPN, and configure VPN bandwidth management. (See figure 3 and 4) VPN Bandwidth Management gives the administrator the ability to determine how much VPN guaranteed bandwidth and VPN maximum bandwidth to allocate to outbound VPN traffic.

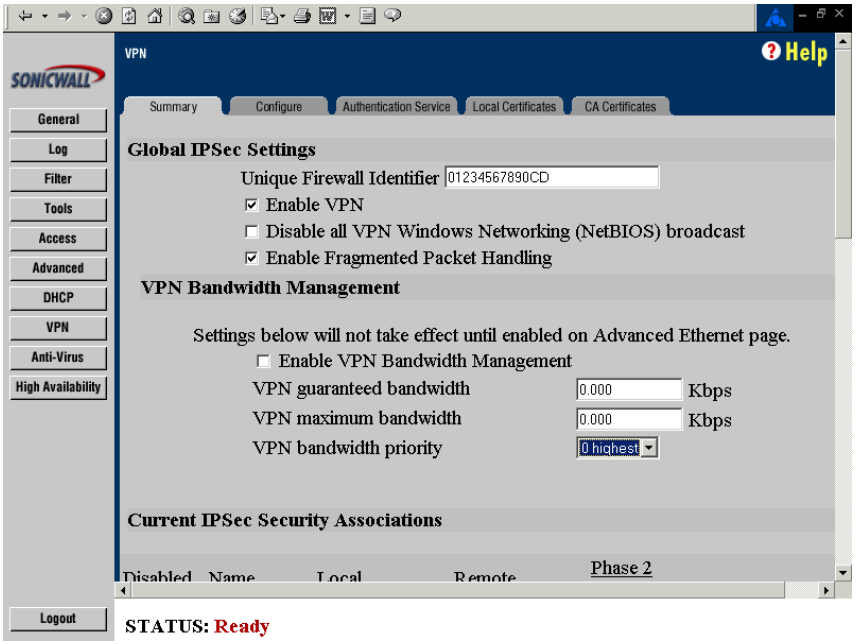


Figure 3

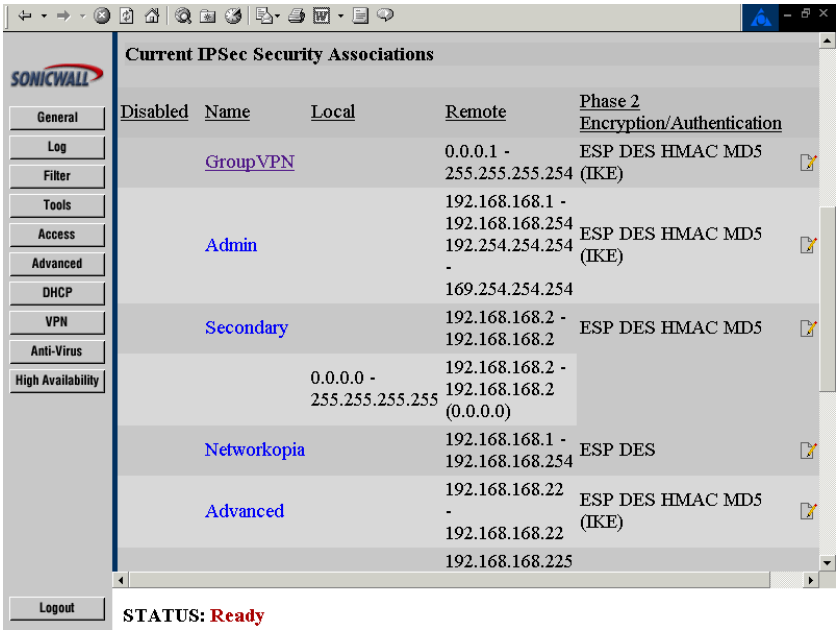


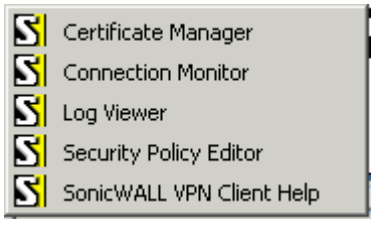
Figure 3

VPN Client Installation

The administrator is now ready to configure the client machine to access the newly created VPN. System requirements for the SonicWALL VPN client are as follows:

- IBM compatible computer with an Intel Pentium (or equivalent) processor
- Microsoft Windows 95, 98, Me, NT 4.0, 2000, XP
- 32 MB hard disk space
- 16 MB RAM for Windows 95, 98, Me, 32 MB RAM for Windows NT and 64 MB RAM for Windows 2000, XP
- Ethernet network interface card with NDIS compliant driver and/or dialup adapter (internal or external modem, ISDN adapter) or Wireless LAN.

After the VPN client is installed a new program group is created which includes several programs related to the SonicWALL VPN client.



These programs assist in the VPN tunnel establishment, monitoring, etc. and include:

1. **Security Policy Editor-** To create, import, or manage connections and their

associated proposals that make up a user's security policy.

2. **Certificate Manager-** Where users request, import, and store the certificates they receive from certificate authorities (CAs)

3. **SonicWALL VPN client help-** The help file for the SonicWALL VPN client.

4. **Log Viewer-** Contains the communications log, which lists the IKE negotiations that occur during Phase 1 Authentication

5. **Connection Monitor-** Shows statistical and diagnostic information for each active connection in the security policy

To configure the client PC for access to the SonicWALL VPN simply open the Security Policy Editor as seen below in Table 3. Here you can add a new VPN connection and specify settings from the VPN gateway configuration. The clients settings determine how you will connect to the remote VPN and whether you will connect via an IP address, IP Subnet, or IP range. You also need to select the Connect Using box to specify connecting to the VPN using a Secure Gateway Tunnel.

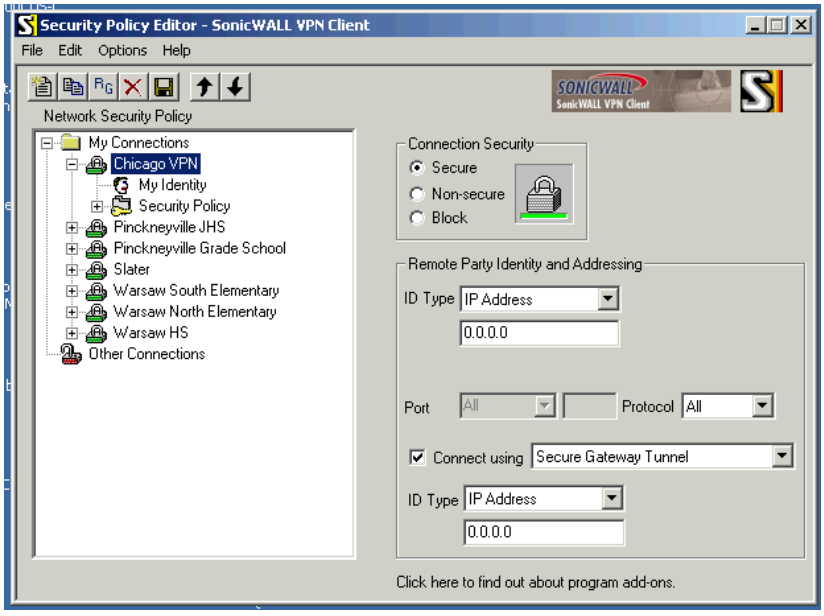


Table 3

Next, you need to provide details of your identity by selecting My Identity under the newly created VPN connection (See Table 4) Items such as certificate type, (i.e. Administrator EFS Certificate if using SonicWALL's Authentication Services, Select automatically during IKE negotiation, or None if using a Pre-Shared Secret Key) can be configured here. If, during the firewall VPN installation, you selected Pre-Shared key you can enter the 8-character Pre-Shared Key information in the space provided. (See Table 5) As mentioned earlier, a Pre-Shared Key is nothing more than a password and should meet certain conditions to be considered secure. These conditions include

Uppercase/Lowercase letters, letters and numbers, and special characters. For example, 53AsrTi&%. You can also indicate which network interface in which to establish the VPN.

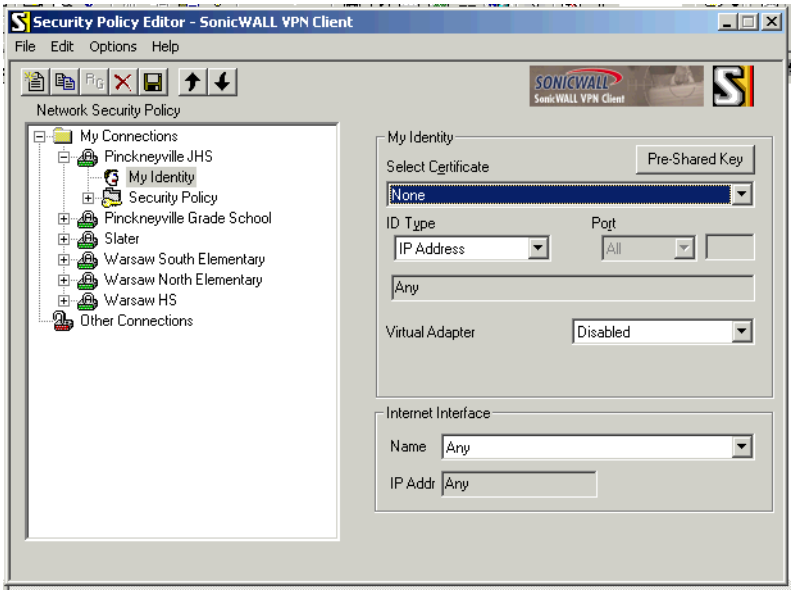


Table 4

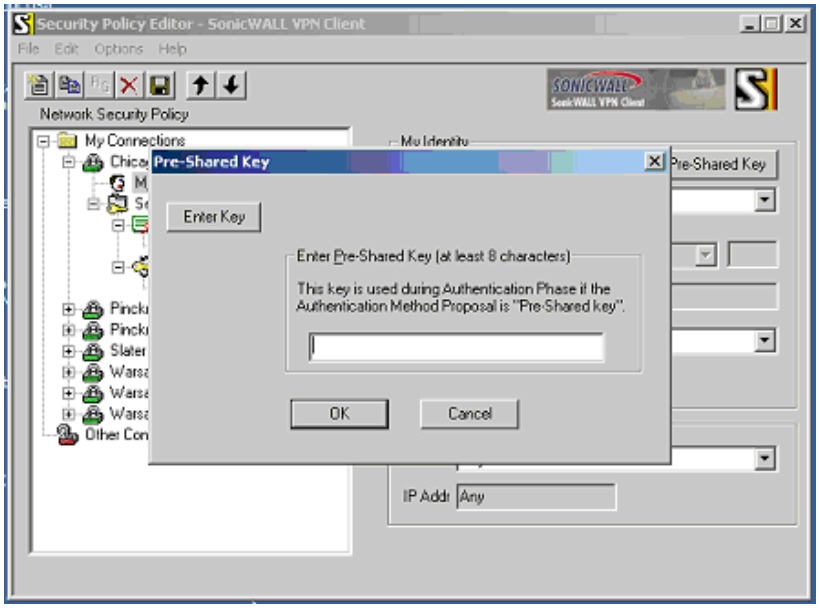


Table 5

Next select Security Policy under the VPN connection and configure the Phase 1 Negotiation Mode, which is the VPN authentication mode. (See Table 6) Available options include:
:

1. Main Mode- Ensures the highest level of security when the communicating parties are negotiating authentication (Phase 1).
2. Aggressive Mode- Quicker than Main Mode because it eliminates several steps when the communicating parties are negotiating authentication (Phase 1). Should be used when the SonicWALL VPN device is located behind a Network Address Translation device.
3. Use Manual Keys- Requires no negotiations; available for troubleshooting only.

You can also specify Enable Perfect Forward Secrecy, Perfect Forward Secrecy Key Group, and Enable Replay Detection. Enable Replay Detection sets a counter that determines whether or not a packet is unique to prevent data from being falsified.

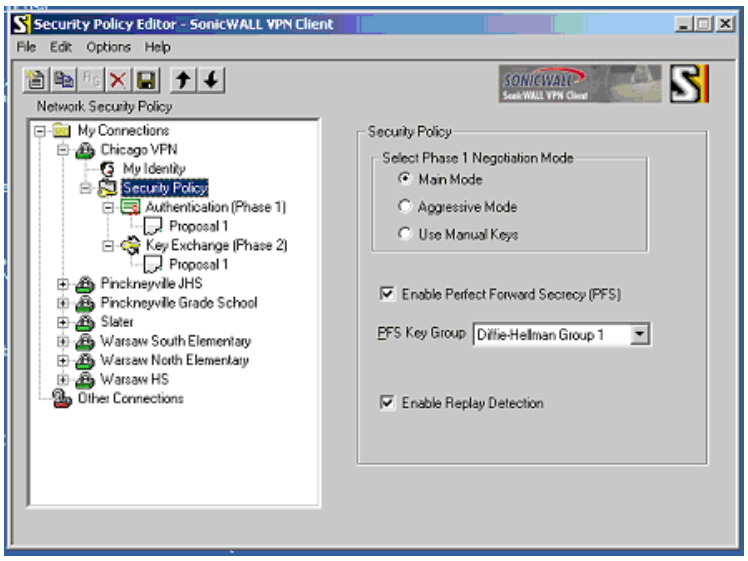


Table 6

Next configure the Authentication phase (Phase 1) to specify the authentication method, encrypting algorithm, and hashing algorithm along with the SA Life and Key Group. Again, these settings must match the VPN gateway settings of the SonicWALL security appliance. Encryption refers to taking a plaintext message, apply a mathematical algorithm to that text, which results in scrambled-text known as cipher text. A hashing algorithm is a function that takes a variable-length string, a message, and compresses and transforms it into a fixed-length value referred to as a hash-vale. SA Life is used to determine how often IKE encryption and authentication keys will be renegotiated and Key Group relates to the authentication settings the security administrator entered in the security policy configuration of the SonicWALL VPN device. As mentioned earlier, Group 1 provides a pre-shared key length of 768. Group 2 provides a pre-shared key length of 1024 and Group 5 provides a pre-shared key length of 1536.

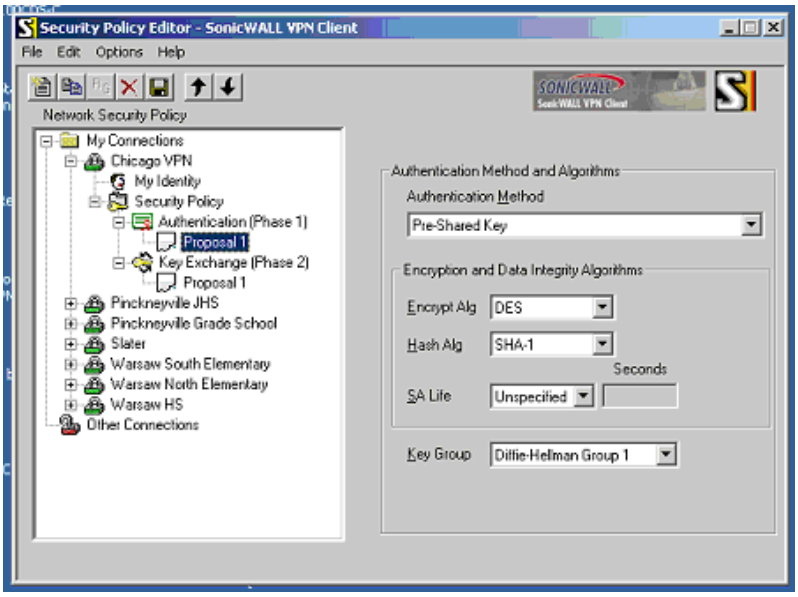


Table 7

You then need to configure the Key Exchange Phase (See Table 8) to specify the IPSec portion of the VPN. Parameters such as length of SA Life and compression are configured here. Compression is highly recommended to increase the throughput rates of the VPN. You need to configure the encapsulation mode, which is either transport-mode or tunnel-mode. Transport mode acts the same as regular IP but with authenticated headers and encrypted contents whereas tunnel mode encrypts the entire packet, header and all. Transport mode is typically used for client to VPN gateway communications and Tunnel mode is used for router-to-router or other endpoint communication links.

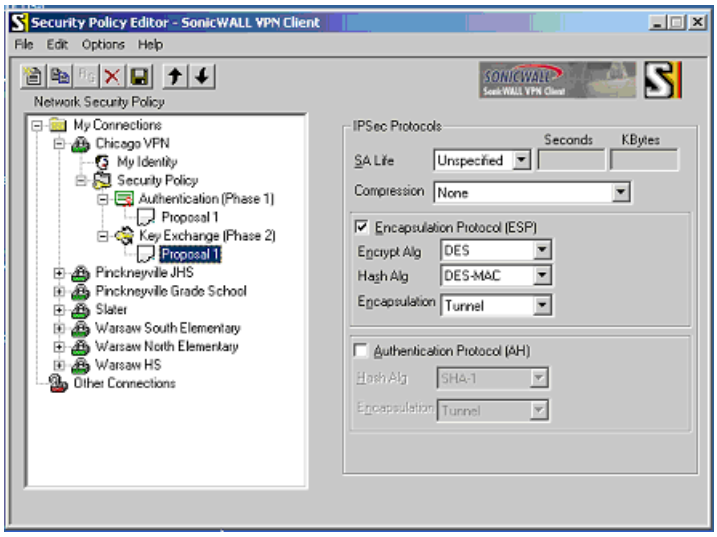


Table 8

Once you have completed the above parameters and saved the policy you are ready to test the VPN connection.

Testing the VPN

The first step in testing the VPN connection is to determine if your VPN session is actually active. You can check the status of your VPN connection by looking at the SonicWALL VPN Client system tray icon.

Several variations of the icon may appear and table 9 describes the various appearances of the SonicWALL VPN Client icon.

	IREIKE service did not start or the security policy is deactivated. Reload the security policy or you may need to restart your PC or reinstall the SonicWALL VPN client software
	PC is ready to establish and transmit data over the VPN.
	PC has established no secure connections and is transmitting unsecured data.
	PC has established a secure connection but is not transmitting any data
	PC has established a secured connection but is transmitting unsecured data
	PC has established a secured connection and is transmitting secured data
	PC has established a secured connection and is transmitting both secured and unsecured data

Table 9

Whether your connection is active or not, you can use the Connection Monitor to view statistical and diagnostic information for any active connection you have created using the Security Policy Editor. Here you can view secured and non-secured packets, packets dropped, etc.

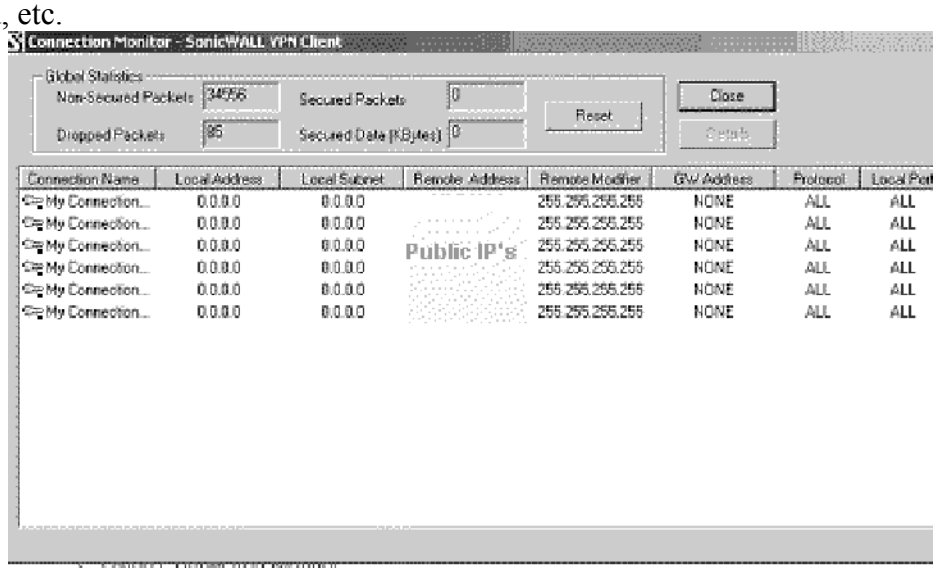


Table 10

Another tool to use when testing the VPN connection is the Log Viewer. Here you can view the IKE negotiations occurring during authentication (Phase 1) along with ongoing negotiations based on the Security Association Life configured on the SonicWALL security appliance.

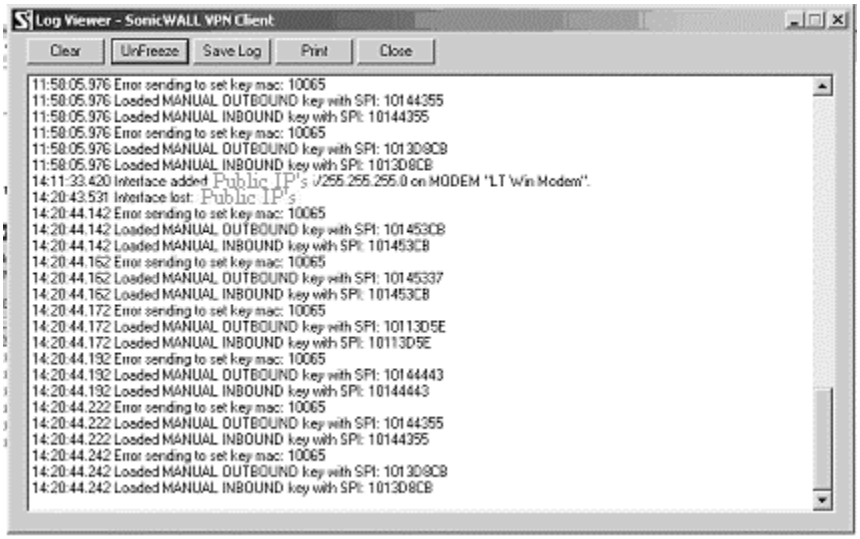


Table 11

Conclusion

In conclusion, the SonicWALL family of firewall appliances provides networks of any size the ability to create secure remote connections in a quick and easy manner. Many administrators fear the task of creating a VPN connection due to the many configuration options available from a multitude of vendors but I hope you are now able to see just how easy a VPN can be installed using the SonicWALL firewall appliance.

With this ease of installation comes secured remote connections to the corporate network established using the strongest encryption level (3DES) as well as offering the administrator the ability to balance security with speed.

Once the VPN is established, several tools are available to allow users of the VPN the ability to troubleshoot and view any VPN connection.

References

Virtual Private Network- "A SearchNetworking.Com Definition"
URL http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213324_top1,00.html

[2] "What is a VPN? – Virtual Private Networks and Data Security on the Internet
URL http://www.sonicwall.com/vpn-center/what-is-vpn.html - vpn-types

[3] Matthew Strebe and Charles Perkins. Firewalls- 24/7 Second Edition.

Sybex Press 2002

[4] Matthew Strebe and Charles Perkins. Firewalls- 24/7 Second Edition.
Sybex Press 2002

[5] Sarah Carter "What is forward secrecy"?
URL http://www.itsecurity.com/asktecs/may201.htm

[6] Security Complete. Sybex Press. 2001

[7] SonicWALL VPN FAQ
Url http://www.sonicwall.com/products/documentation/vpnclient_qa.html

[8] Help File "What's included in the SonicWALL VPN Client"? - SonicWALL VPN Client Version 8.0.0 (Build 10)

[9] Help File "SonicWALL VPN Client"? - SonicWALL VPN Client Version 8.0.0 (Build 10)

[10] Configuring a Pre-Shared Key.
URL
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnsg/icrwpsk.htm - 1064995