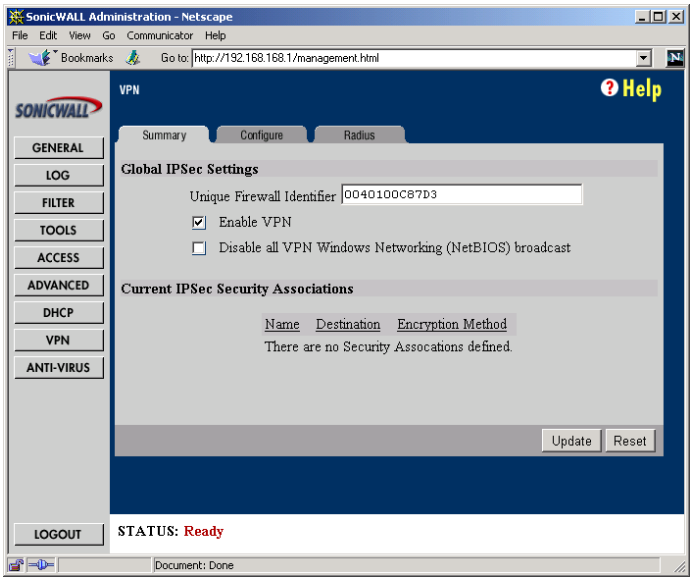
VPN Client Advanced Configuration

Advanced Configuration uses Internet Key Exchange (IKE) to automatically negotiate encryption and authentication keys. Advanced Configuration is similar to Simple Configuration, but it requires a more complex set-up and is not recommended for most SonicWALL administrators. Only one VPN client can connect to each Advanced Configuration SA.

The following instructions describe the configuration of the SonicWALL, the installation and setup of the SonicWALL VPN Client, and the procedure to access the SonicWALL remotely after the VPN tunnel has been established.

1. First, configure the SonicWALL. 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.



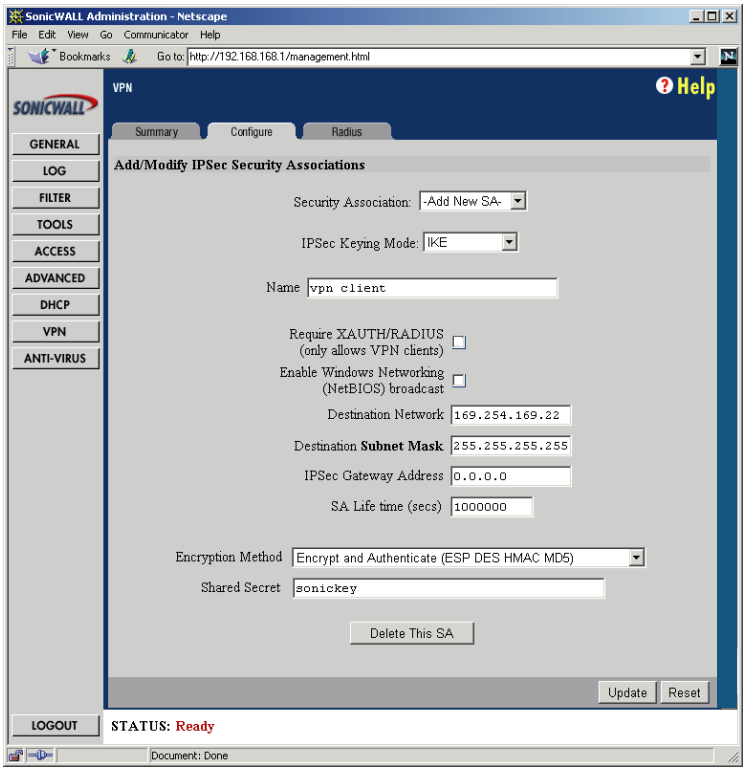
2. Check the **Enable VPN** checkbox and assign an alphanumeric name for the SonicWALL in the **Unique Firewall Identifier** field. The **Unique Firewall Identifier** may range from 4 to 32 characters in length. Make note of the **Unique Firewall Identifier**, as it will be needed for the SonicWALL VPN Client.

3. Leave the **Disable all Windows Networking (NetBIOS) broadcast** checkbox unchecked to allow Windows Networking (NetBIOS) broadcasts to pass across some or all VPN SAs. *Windows Networking (NetBIOS) broadcasts may be transmitted between two VPN gateways but are not passed to the SonicWALL VPN Client.*

4. 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.

5. Click the **Configure** tab at the top of the browser. A window similar to the following will be displayed.

6. On the **Configure** page, create a new **Security Association** by selecting **Add New SA** from the **Security Association** menu.



7. Select **IKE** from the **IPSec Keying Mode** menu.

8. Enter a name that identifies the VPN client in the **Name** field, such as the VPN client's location or name. This name will also be entered in the SonicWALL VPN Client.

9. Leave the **Require XAUTH/RADIUS (only allows VPN clients)** checkbox unchecked, unless a RADIUS server is present on the LAN and the SonicWALL's RADIUS settings have been configured.

10. Leave the **Enable Windows Networking (NetBIOS) broadcast** checkbox unchecked because the SonicWALL VPN Client will not transmit Windows Networking (NetBIOS) traffic.

11. Enter the internal IP address of the SonicWALL VPN Client in the **Destination Network Address** field. This is an arbitrary address that will be assigned to the VPN

client, and should be a private address, such as "10.0.0.1" or "192.168.168.1". This address must be in a different subnet than the SonicWALL's LAN.

12. Enter the internal subnet mask of the VPN client in the **Destination Subnet Mask** field. The subnet mask "255.255.255.255" is recommended.

13. Define the length of time before the encryption and authentication keys are updated in the **SA Life Time (secs)** field. The SA Life Time may range from 120 to 2,500,000 seconds. 86,400 seconds (1day) is recommended.

14. Leave the **IPSec Gateway Address** field blank.

15. Select **Encrypt and Authenticate (ESP DES HMAC MD5)** from the **Encryption Method** drop down menu.

16. Define a shared secret in the **Shared Secret** field. The alphanumeric shared secret must match the VPN client's **Shared Key** and may range from 8 to 128 characters in length. 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. Once the SonicWALL has been updated, a message confirming the update will be displayed at the bottom of the Web browser window. Restart the SonicWALL for changes to take effect.

Install the VPN Client Software

1. When SonicWALL PRO, SonicWALL PRO-VX or the VPN Upgrade is registered at <http://register.sonicwall.com>, a unique VPN client serial number is returned, as well as a link to download the SonicWALL VPN Client zip file.

2. Unzip the SonicWALL VPN Client zip file.

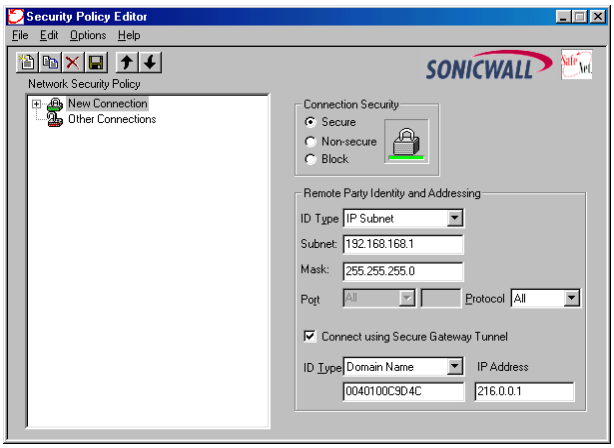
3. Double-click **setup.exe** and follow the VPN client setup program's step by step instructions. Enter the VPN client's serial number when prompted.

4. Restart your computer after the VPN client setup program has finished installing.

Launch the SonicWALL VPN Client

To launch the VPN client, select SonicWALL VPN Client **Security Policy Editor** from the Windows **Start** menu, or double-click the  icon in the Windows Task Bar.

Select **Add > New Connection** in the **Edit** menu at the top of the **Security Policy Editor** window. A window similar to the following will be displayed.



Note: *The security policy may be renamed by highlighting* ***New Connection*** *in the Network Security Policy box and typing the desired security policy name.*

Configure Connection Security and Remote Identity

1. Select **Secure** in the Connection Security box.

2. Select **IP Subnet** in the **ID Type** menu.

3. Type the **SonicWALL LAN IP Address** in the **Subnet** field.

4. Type the **LAN Subnet Mask** in the **Mask** field.

5. Select **All** in the **Protocol** menu to permit all IP traffic through the VPN tunnel.

6. Check the **Connect using Secure Gateway Tunnel** checkbox.

7. Select **Domain Name** in the **ID Type** menu at the bottom of the Security Policy Editor window.

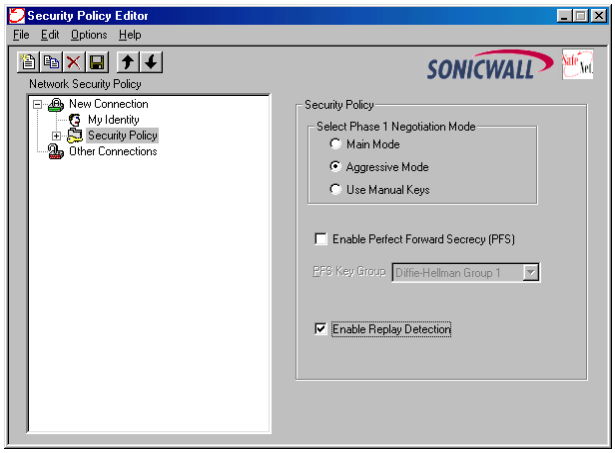
8. Enter the SonicWALL's **Unique Firewall Identifier** in the field directly below the **ID Type** menu. Note that this field is case sensitive.

9. Enter the SonicWALL's **WAN IP Address** in the **IP Address** field. Enter the NAT Public Address if NAT is enabled.

Configure the VPN Client Security Policy

1. Double click **New Connection** in the Network Security Policy box on the left side of the Security Policy Editor window. **My Identity** and **Security Policy** should appear below **New Connection.**

2. Click **Security Policy** in the Network Security Policy box. A window similar to the following will be displayed.



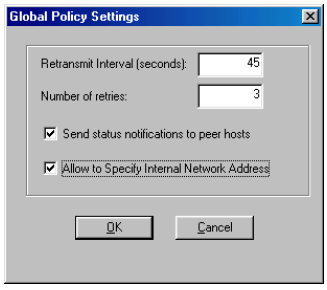
3. Select **Aggressive Mode** in the **Select Phase 1 Negotiation Mode** box.

4. Leave the **Enable Perfect Forward Secrecy (PFS)** checkbox unchecked.

5. Check the **Enable Replay Detection** to redisplay auditing messages.

Configure Global Policy Settings

Select **Global Policy Settings** in the **Options** menu at the top of the Security Policy Editor window. A window similar to the following will be displayed.

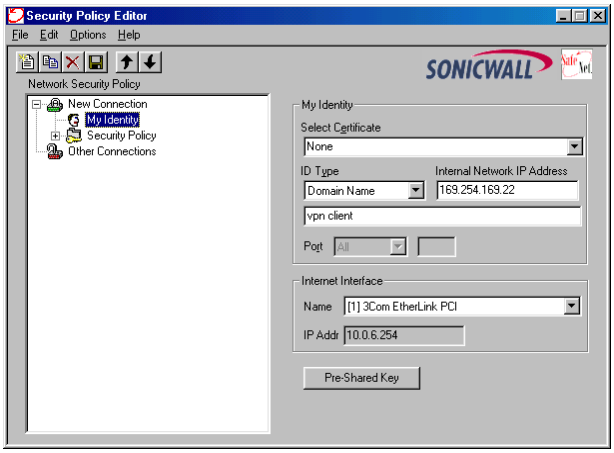


1. Increase the **Retransmit Interval (seconds):** period to **45**.

2. Check the **Allow to specify Internal Network Address** checkbox and click **OK**.

Configure VPN Client Identity

1. Click **My Identity** in the Network Security box on the left side of the Security Policy Editor window. A window similar to the following will be displayed.



2. Choose **None** in the **Select Certificate** menu.

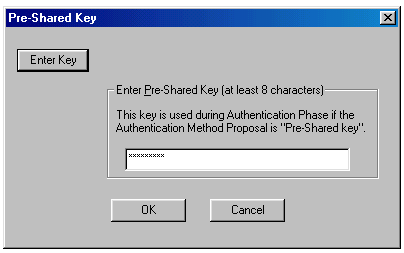
3. Select **Domain Name** in the **ID Type** menu.

4. Enter the SonicWALL's VPN **Destination Network Address** in the **Internal Network IP Address** field. This address must be in a different subnet than the SonicWALL's LAN.

5. Enter the **Name** of the SonicWALL Security Association in the field below the **ID Type** menu. Note that this field is case sensitive.

6. In the Internet Interface box, select the adapter you use 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 dedicated Cable, ISDN or DSL line.

7. Then click the **Pre-Shared Key** button. A dialog box similar to the following will appear. Note that this field is case sensitive.

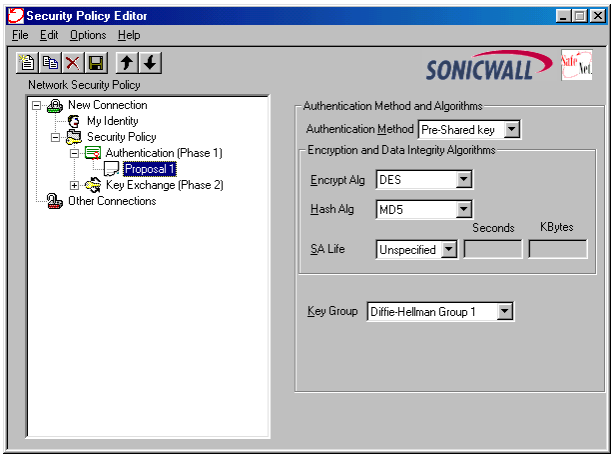


8. Click the **Enter Key** button in the Pre-Shared Key dialog box. Then enter the SonicWALL's **Shared Secret** in the **Pre-Shared Key** field and click **OK.**

Configure VPN Client Authentication Proposal

1. Double click **Security Policy** in the Network Security Policy box to display **Authentication** and **Key Exchange**.

2. Double click **Authentication**. Then select **Proposal 1** below **Authentication**. A window similar to the following will be displayed.



3. Select **Pre-Shared key** in the **Authentication Method** menu.

4. Select **DES** in the **Encrypt Alg** menu.

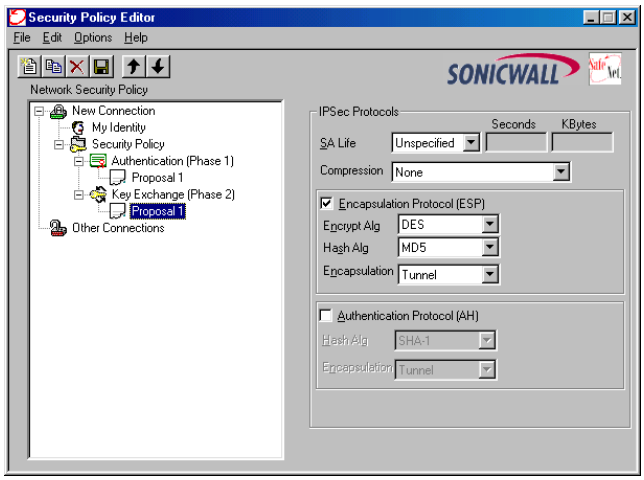
5. Select **MD5** in the **Hash Alg** menu.

6. Select **Unspecified** in the **SA Life** menu

7. Select **Diffie-Hellman Group 1** in the **Key Group** menu.

Configure VPN Client Key Exchange Proposal

1. Double click **Key Exchange** in the Network Security Policy box. Then select **Proposal 1** below **Key Exchange**. A window similar to the following will be displayed.



2. Select **Unspecified** in the **SA Life** menu.

3. Select **None** in the **Compression** menu.

4. Check the **Encapsulation Protocol (ESP)** checkbox.

5. Select **DES** in the **Encrypt Alg** menu.

6. Select **MD5** in the **Hash Alg** menu.

7. Select **Tunnel** in the **Encapsulation** menu.

8. Leave the **Authentication Protocol (AH)** checkbox unchecked.

Save SonicWALL VPN Client Settings

1. Select **Save Changes** in the **File** menu in the top left corner of the Security Policy Editor window.

After completing the VPN client configuration, the administrator may securely manage the remote SonicWALL by entering the **SonicWALL LAN IP Address** in a browser on the computer running the VPN client software.

The SonicWALL VPN Client may also access remote resources by locating servers or workstations by their remote IP addresses. To find out more about accessing remote resources over a Virtual Private Network, visit <http://www.sonicwall.com/firewall/vpnremotehostswp.html>.