Manual Key Configuration for Two SonicWALLs

VPN between two SonicWALLs allows users to securely access files and applications at remote locations. The first step to set up a VPN between two SonicWALLs is creating corresponding Security Associations (SAs). The instructions below describe how to create an SA using Manual Key configuration. These instructions are followed by an example illustrating a VPN tunnel between two SonicWALLs.

VPN Advanced Settings

All of the Advanced Settings for VPN connections are accessed by clicking Advanced Settings located on the Configure tab. The following settings are available in the Edit Advanced Settings window:

- Enable Windows Networking (NetBIOS) broadcast
- Apply NAT and firewall rules
- Forward packets to remote VPNs
- Route all internet traffic through this SA
- Default LAN Gateway

Enable Windows Networking (NetBIOS) broadcast

Computers running Microsoft Windows® communicate with one another through NetBIOS broadcast packets. Select the Enable Windows Networking (NetBIOS) broadcast check box to access remote network resources by browsing the Windows® Network Neighborhood.

Apply NAT and firewall rules

This feature allows the remote site’s LAN subnet to be hidden from the corporate site, and is most useful when a remote office’s network traffic is initiated to the corporate office. The IPSec tunnel is located between the SonicWALL WAN interface and the LAN segment of the corporation. To protect the traffic, NAT (Network Address Translation) is performed on the outbound packet before it is sent through the tunnel, and in turn, NAT is performed on inbound packets when they are received. By using NAT for a VPN connection, computers...
on the remote LAN are viewed as one address (the SonicWALL public address) from the corporate LAN.

If the SonicWALL uses the **Standard** network configuration, using this check box applies the firewall access rules and checks for attacks, but not NAT.

**Note:** You cannot use this feature if you have **Route all internet traffic through this SA** enabled.

**Note:** Offices can have overlapping LAN IP ranges if this feature is selected.

**Forward Packets to Remote VPNs**

Selecting the **Forward Packets to Remote VPNs** check box for a **Security Association** allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can now be forwarded to a remote site via another VPN tunnel. Normally, inbound traffic is decrypted and only forwarded to the SonicWALL LAN or a specific route on the LAN specified on the **Routes** tab located under the **Advanced** section.

Enabling this feature allows a network administrator to create a “hub and spoke” network configuration by forwarding inbound traffic to a remote site via a VPN security association. To create a “hub and spoke” network, enable the **Forward Packets to Remote VPNs** check box for each Security Association in your SonicWALL. Traffic can travel from a branch office to a branch office via the corporate office.

**Route all internet traffic through this SA**

Selecting this box allows a network administrator to force all WAN-destined traffic to go through a VPN tunnel to a central site. Outgoing packets are checked against the remote network definitions for all Security Associations (SA). If a match is detected, the packet is then routed to the appropriate destination. If no match is detected, the SonicWALL checks for the presence of a SA using this configuration. If an SA is detected, the packet is sent using that SA. If there is no SA with this option enabled, and if the destination does not match any other SA, the packet goes unencrypted to the WAN.

**Note:** Only one SA can have this check box enabled.

**Default LAN Gateway**

A **Default LAN Gateway** is used at a central site in conjunction with a remote site using the **Route all internet traffic through this SA** check box. 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.

Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a **Default LAN Gateway**. If a **Default LAN Gateway** is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
**Manual Key between Two SonicWALLs**

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

1. Select **Manual Key** from the **IPSec Keying Mode** menu.
2. Select **-Add New SA-** from the **Security Association** menu.

![Configuration Screen](image)

3. Enter a descriptive name for the **Security Association**, such as “Chicago Office” or “Remote Management”, in the **Name** field.

4. Enter the IP address of the remote VPN gateway, such as another SonicWALL VPN gateway, in the **IPSec Gateway Address** field. This must be a valid IP address and is the remote VPN gateway NAT Public Address if NAT is enabled. Enter “0.0.0.0” if the remote VPN gateway has a dynamic IP address.

5. Define an **SPI** (Security Parameter Index) that the remote SonicWALL uses to identify the **Security Association** in the **Incoming SPI** field.

6. Define an **SPI** that the local SonicWALL uses to identify the **Security Association** in the **Outgoing SPI** field.

**Note:** SPIs should range from 3 to 8 characters in length and include only hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). If you enter an invalid **SPI**, an error message will
be displayed at the bottom of the browser window. An example of a valid SPI is 1234abcd.

**Note:** Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.

7. Select an encryption algorithm from the **Encryption Method** menu. The SonicWALL supports the following encryption algorithms:

   - **Tunnel Only (ESP NULL)** does not provide encryption or authentication. This option offers access to computers at private addresses behind NAT and allows unsupported services through the SonicWALL.
   - **Encrypt (ESP DES)** uses 56-bit DES to encrypt data. DES is an extremely secure encryption method, supporting over 72 quadrillion possible encryption keys that can be used to encrypt data.
   - **Fast Encrypt (ESP ARCFour)** uses 56-bit ARCFour to encrypt data. ARCFour is a secure encryption method and has little impact on the throughput of the SonicWALL.
   - **Strong Encrypt (ESP 3DES)** uses 168-bit 3DES (Triple DES) to encrypt data. 3DES is considered an almost “unbreakable” encryption method, applying three DES keys in succession, but it significantly impacts the data throughput of the SonicWALL.
   - **Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)** uses 168 bit 3DES encryption and HMAC MD5 authentication. 3DES is an extremely secure encryption method, and HMAC MD5 authentication is used to verify integrity. This method significantly impacts the data throughput of the SonicWALL.
   - **Encrypt for Check Point (ESP DES rfc1829)** is interoperable with Check Point Firewall-1. In **Manual Keying** mode, Encrypt for Check Point uses 56-bit DES as specified in RFC 1829 as the encryption method.
   - **Encrypt and Authenticate (ESP DES HMAC MD5)** uses 56-bit DES encryption and HMAC MD5 authentication. This method impacts the data throughput of VPN communications. SonicWALL VPN client software supports this method.
   - **Authenticate (AH MD5)** uses AH to authenticate VPN communications but it does not encrypt data.

8. Enter a 16-character hexadecimal key in the **Encryption Key** field if you are using DES or ARCFour encryption. Enter a 48-character hexadecimal key if you are using Triple DES encryption. This encryption key must match the remote SonicWALL’s encryption key.

   **Note:** Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.

When a new SA is created, a 48-character key is automatically generated in the **Encryption Key** field. This can be used as a valid key for Triple DES. If this key is used, it must also be entered in the Encryption Key field in the remote SonicWALL.
Tunnel Only (ESP NULL) or Authenticate (AH MD5) is used, the Encryption Key field is ignored.

9. Enter a 32-character, hexadecimal key in the Authentication Key field.

**Note:** Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef1234567890abcdef is an example of a valid authentication key. If you enter an incorrect authentication key, an error message is displayed at the bottom of the browser window.

When a new SA is created, a 32-character key is automatically generated in the Authentication Key field. This key can be used as a valid key. If this key is used, it must also be entered in the Authentication Key field in the remote SonicWALL. If authentication is not used, this field is ignored.

10. Click Add New Network... to enter the destination network addresses. Clicking Add New Network... automatically updates the VPN configuration and opens the VPN Destination Network window.

11. Enter the beginning IP address of the remote network address range in the Range Start field. If NAT is enabled on the remote SonicWALL, enter a private LAN IP address. Enter "0.0.0.0" to accept all remote SonicWALLs with matching encryption and authentication keys.

12. Enter the ending IP address of the remote network's address range in the Range End field. If NAT is enabled on the remote SonicWALL, enter a private LAN IP address. Enter "0.0.0.0" to accept all remote SonicWALLs with matching encryption and authentication keys.

13. Enter the remote network subnet mask in the Destination Subnet Mask for NetBIOS broadcast field if Enable Windows Networking (NetBIOS) Broadcast is selected. Otherwise, enter "0.0.0.0" in the field.

14. Click Update to add the remote network and close the VPN Destination Network window. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

15. Click Advanced Settings and check the boxes that apply to your SA:

   • Enable Windows Networking (NetBIOS) broadcast - if the remote clients use Windows Network Neighborhood to browse remote networks.
   • 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 configuration
   • Route all internet traffic through this SA - if forcing internet traffic from the WAN to use this SA to access a remote site.

SonicWALL VPN using Manual Key Configuration Page 5
• **Default LAN Gateway** if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the **Route all internet traffic through this SA** check box.

16. Click **OK** to close the **Advanced Settings** window. Then click **Update** to update the SonicWALL.

**Configuring the Second SonicWALL Appliance**

To configure the second SonicWALL appliance, follow the same configuration steps as the first SonicWALL. You must enter the same SPIs and Encryption keys as the first SonicWALL appliance into the settings of the second SonicWALL appliance.

**Example of Manual Key Configuration between Two SonicWALLs**

Widgit, Inc. wants to connect their main office with a branch office on the East Coast. Using a SonicWALL PRO-VX and a TELE2, they can configure a secure VPN tunnel between the two sites. The main office has the following network settings:

- SonicWALL LAN IP address - 192.168.11.1
- LAN subnet mask - 255.255.255.0
- WAN router address - 209.33.22.1
- SonicWALL WAN IP address - 209.33.22.2
- WAN subnet mask - 255.255.255.224

The remote office has the following network settings:

- SonicWALL LAN IP address - 192.168.22.222
- LAN subnet mask - 255.255.255.0
- WAN router address - 207.66.55.129
- SonicWALL WAN IP address - 207.66.55.130
- WAN subnet mask - 255.255.255.248
To configure the main office PRO-VX, use the following steps:

1. Configure the network settings for the firewall using the **Network** tab located in the **General** section.
2. Click **Update** and restart the SonicWALL if necessary.
3. Click **VPN**, then the **Configure** tab.
4. Create a name for the main office SA, for example, **Main Office**.
5. Type in the branch office WAN IP address for the **IPSec Gateway Address**.
6. Create an **Incoming SPI** using alphanumeric characters.
7. Create an **Outgoing SPI** using alphanumeric characters.
8. Select **Strong Encrypt (ESP 3DES)** as the **Encryption Method**.
9. Write the **Encryption Key** down or use cut and paste to copy it to a Notepad window.
10. Click **Add New Network**. Type the IP address, “192.168.22.1” in the **Range Start** field. Type the IP address, “192.168.22.255” in the **Range End** field. This **Range End** value is appropriate even if NetBIOS broadcast support is enabled. Leave the subnet mask field blank. Click **Update**.
11. Click **Advanced Settings** and select the features that apply to the SA.
   - **Enable Windows Networking (NetBIOS) broadcast** - if the remote clients use Windows Network Neighborhood to browse remote networks.
   - **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 configuration
   - **Route all internet traffic through this SA** - if forcing internet traffic from the WAN to use this SA to access a remote site.
   - **Default LAN Gateway** if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the **Route all internet traffic through this SA** check box.
12. Click **OK**, and then click **Update**.

**Configuring the Remote SonicWALL**

To configure the remote SonicWALL, use the following steps:

1. Configure the network settings for the firewall using the **Network** tab located in the **General** section.
2. Click **Update** and restart the SonicWALL if necessary.
3. Click **VPN**, then the **Configure** tab.
4. Create a name for the remote office SA, for example, **Remote Office**.
5. Type in the main office WAN IP address for the **IPSec Gateway Address**.
6. Create an **Incoming SPI** using alphanumeric characters.
7. Create an **Outgoing SPI** using alphanumeric characters.
8. Select **Strong Encrypt (ESP 3DES)** as the **Encryption Method**.
9. Enter the **Encryption Key** from the Main Office configuration.
10. Click **Add New Network**. Type the IP address, “192.168.11.1” in the **Range Start** field. Type the IP address, “192.168.11.255” in the **Range End** field. This **Range End** value is appropriate even if NetBIOS broadcast support is enabled. Leave the subnet mask field blank. Click **Update**.
11. Click **Advanced Settings** and select the features that apply to the SA.
   - **Enable Windows Networking (NetBIOS) broadcast** - if the remote clients use Windows Network Neighborhood to browse remote networks.
   - **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 configuration
   - **Route all internet traffic through this SA** - if forcing internet traffic from the WAN to use this SA to access a remote site.
   - **Default LAN Gateway** if specifying the IP address of the default LAN route for incoming IPSec packets for this SA. This is used in conjunction with the **Route all internet traffic through this SA** check box.
12. Click **OK**, and then click **Update**.