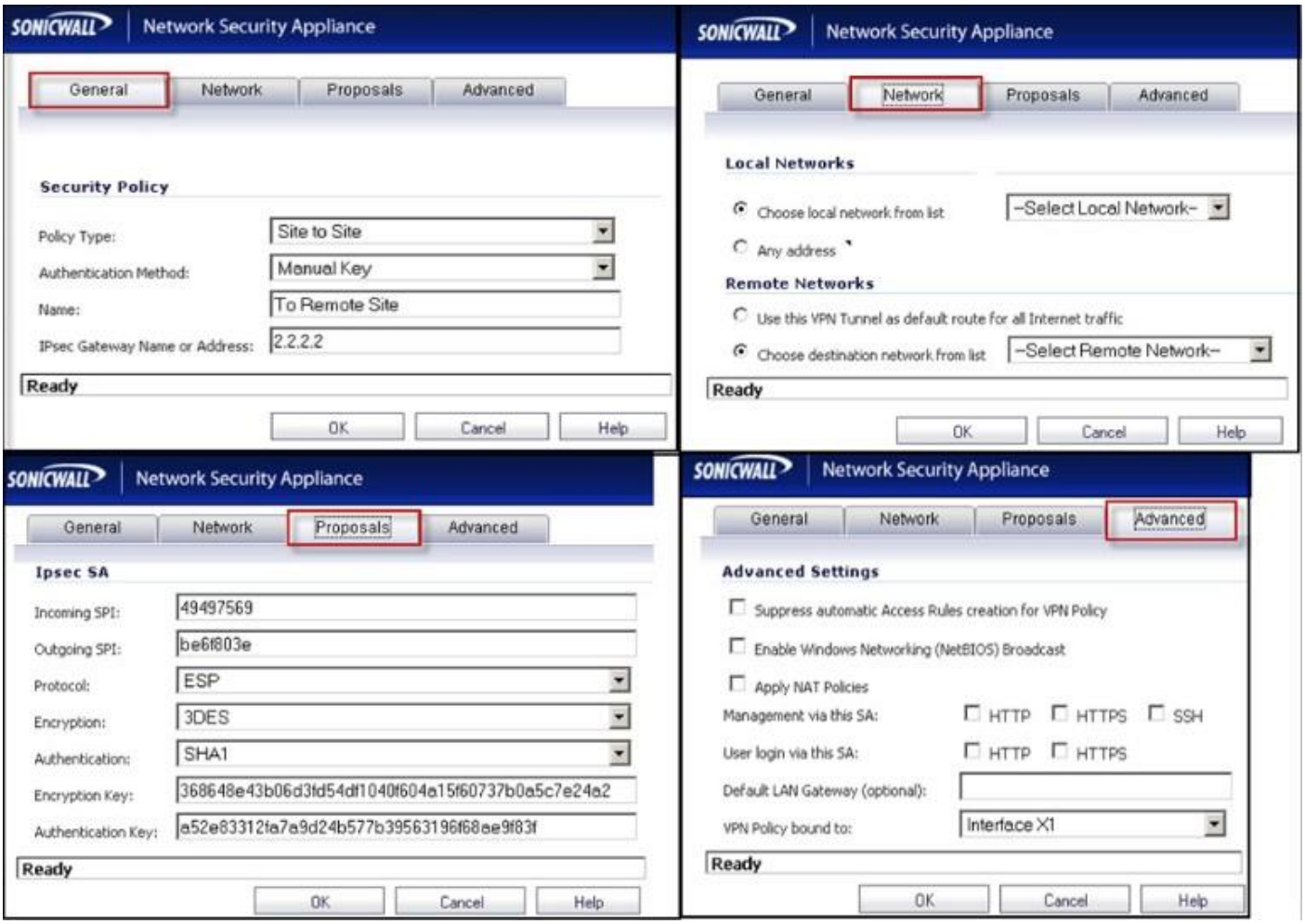
Configuring Site-to-Site VPN with Manual Key on SonicOS Enhanced

KNOWLEDGE DATABASE

SONICWALL Knowledge Database

Configuring Site-to-Site VPN with Manual Key on SonicOS Enhanced

Configuring the Local SonicWall Security Appliance:



Step 1: - Click Add on the VPN | Settings page. The VPN Policy window is displayed.
Step 2: - In the General tab of the VPN Policy window, select Manual Key from the IPsec Keying Mode menu. The VPN Policy window displays the manual key options.
Step 3: - Enter a name for the policy in the Name field.
Step 4: - Enter the host name or IP address of the remote connection in the IPsec Gateway Name or Address field.
Step 5: - Click the Network tab.
Step 6: - Select a local network from Choose local network from list if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select Any Address. Use this option is a peer has Use this VPN Tunnel as default route for all Internet traffic selected. You can only configure one SA to use this setting. Alternatively, select Choose Destination network from list, and select the address object or group.

Step 7: - Click on the Proposals tab.
Step 8: - Define an Incoming SPI and an Outgoing SPI. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.
Caution: - 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.
Step 9: - The default values for Protocol, Phase 2 Encryption, and Phase 2 Authentication are acceptable for most VPN SA configurations.
Note: - The values for Protocol, Phase 2 Encryption, and Phase 2 Authentication must match the values on the remote SonicWall.
Step 10: - Enter a 16 character hexadecimal encryption key in the Encryption Key field or use the default value. This encryption key is used to configure the remote SonicWall encryption key, therefore, write it down to use when configuring the SonicWall.
Step 11: - Enter a 32 character hexadecimal authentication key in the Authentication Key field or use the default value. Write down the key to use while configuring the SonicWall settings.
Tip: - 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.
Step 12: - Click the Advanced tab and select any of the following optional settings you want to apply to your VPN policy.

- The Suppress automatic Access Rules creation for VPN Policy setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select Enable Windows Networking (NetBIOS) broadcast to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select Apply NAT Policies if your want the SonicWall to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the Translated Local Network drop-down box. To translate the Remote Network, select or create an Address Object in the Translated Remote Network drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. Apply NAT Policies is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- To manage the local SonicWall through the VPN tunnel, select HTTP, HTTPS, or both from Management via this SA.
- Select HTTP, HTTPS, or both in the User login via this SA to allow users to login using the SA.
- If you have an IP address for a gateway, enter it into the Default LAN Gateway (optional) field.
- Select an interface from the VPN Policy bound to menu.

Step 13: - Click OK.
Step 14: - Click Apply on the VPN | Settings page to update the VPN Policies.
Configuring the Remote SonicWall Security Appliance
Step 1: - Click **Add** on the **VPN | Settings** page. The **VPN Policy** window is displayed.
Step 2: - In the **General** tab, select **Manual Key** from the **IPsec Keying Mode** menu.
Step 3: - Enter a name for the SA in the **Name** field.
Step 4: - Enter the host name or IP address of the local connection in the **IPsec Gateway Name or Address field**.
Step 5: - Click the **Network** tab.
Step 6: - Select a local network from **Choose local network** from list if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Select **Use this VPN Tunnel** as default route for all Internet traffic if traffic from any local user cannot leave the SonicWall security appliance unless it is encrypted. You can only configure one SA to use this setting. Alternatively, select Choose Destination network from list, and select the address object or group.

Calle 140 #11-45. Bogotá D.C. Colombia
+57 1 3680290 / +57 318 4914652
sales@itclatam.com / tss@itclatam.com

Step 7: - Click the **Proposals** tab.
Step 8: - Define an Incoming SPI and an Outgoing SPI. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.
Warning: - 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.
Step 9: - The default values for Protocol, Phase 2 Encryption, and Phase 2 Authentication are acceptable for most VPN SA configurations.
Note: - The values for Protocol, Phase 2 Encryption, and Phase 2 Authentication must match the values on the remote SonicWall.
Step 10: - Enter a 16 character hexadecimal encryption key in the Encryption Key field or use the default value. This encryption key is used to configure the remote SonicWall encryption key, therefore, write it down to use when configuring the remote SonicWall.
Step 11: - Enter a 32 character hexadecimal authentication key in the Authentication Key field or use the default value. Write down the key to use while configuring the remote SonicWall settings.
Tip: - 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.
Step 12: - Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy:

- The Suppress automatic Access Rules creation for VPN Policy setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select Enable Windows Networking (NetBIOS) broadcast to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select Apply NAT Policies if you want the SonicWall to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the Translated Local Network drop-down box. To translate the Remote Network, select or create an Address Object in the Translated Remote Network drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. Apply NAT Policies is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
  WarningYou cannot use this feature if you have selected Use this VPN Tunnel as the default route for all Internet traffic on the Network tab.
- To manage the remote SonicWall through the VPN tunnel, select HTTP, HTTPS, or both from Management via this SA.
- Select HTTP, HTTPS, or both in the User login via this SA to allow users to login using the SA.
- If you have an IP address for a gateway, enter it into the Default LAN Gateway (optional) field.
- Select an interface from the VPN Policy bound to menu.

Step 13: - Click **OK**.
Step 14: - Click **Apply** on the **VPN | Settings** page to update the VPN Policies.
Tip: - Since Window Networking (NetBIOS) has been enabled, users can view remote computers in their Windows Network Neighborhood. Users can also access resources on the remote LAN by entering servers' or workstations' remote IP addresses.