

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Symantec Firewall/VPN Appliances

Prepared by SonicWALL, Inc.

1/09/2003

Introduction

This technote will detail all the steps necessary to create a working IKE IPSec VPN tunnel between a SonicWALL device and a Symantec Firewall/VPN Appliance.

This technote assumes that both sides have static IP addresses for the external WAN interfaces, and that the devices have been pre-configured with unique LAN and WAN IP addresses, as well as default IP routes. SonicWALL engineering has tested and validated the settings described in this technote. Please note that all settings and screenshots contained within this technote are taken from a SonicWALL device running firmware 6.4.0.1, and a Symantec Firewall/VPN Appliance running firmware 1.5T.

Before You Begin (PLEASE READ)

SonicWALL recommends using firmware release 6.4.0.1 or newer on the SonicWALL device, and firmware release 1.5T or newer on the Symantec Firewall/VPN Appliance. Customers with new SonicWALL devices, or devices under a current support contract, can download the newest firmware from the <https://www.mysonicwall.com> customer site. Symantec customers can download the newest firmware for the Firewall/VPN Appliance from the <http://www.symantec.com/downloads> site.

SonicWALL recommends using the 'Enable Keep Alive' feature for any VPN tunnel to a Symantec Firewall/VPN Appliance. This option has proven useful in many environments where SonicWALLs have a VPN tunnel to a third-party device, and cuts down on the number of rekeying issues.

Caveats

There are a number of caveats to consider when attempting a VPN tunnel between a SonicWALL device and a Symantec Firewall/VPN Appliance. Please note the following before you begin:

- Since SonicWALL devices display its "SA Lifetime" field in seconds, be sure to calculate it to minutes on the Symantec Firewall/VPN Appliance.
- The methods of Dead Peer Detection for SonicWALL devices and Symantec Firewall/VPN Appliance are not compatible. Make sure that Dead Peer Detection is deactivated on the SonicWALL device; if it is not deactivated, it may cause problems.
- The NAT Traversal functionality in SonicWALL cannot be used with Symantec Firewall/VPN Appliance. Make sure that NAT Traversal is deactivated on the SonicWALL device, if it is not deactivated, it may cause problems.
- It is not possible to set up an Aggressive Mode VPN tunnel between the two devices when either side has a dynamically obtained WAN IP address, due to an IKE Identity incompatibility. As noted above, in order to set up a VPN tunnel between the two devices, each side must have a static WAN IP address.

SonicWALL with static WAN IP address, Symantec Firewall/VPN Appliance with static WAN IP address

This connection scenario requires that both sides have static WAN IP addresses.

SonicWALL Device Setup (6.4.0.1 firmware)

1. Log into the SonicWALL's Management GUI using a current web browser, such as Microsoft IE 5.5 or Netscape 6.2. This can be reached at 'http://x.x.x.x/management.html' (replace x.x.x.x with the LAN IP of your SonicWALL device).
2. Click on the 'VPN' button on the left side, and then click on the 'Summary' tab along the top. Uncheck the checkboxes next to 'Enable NAT Traversal' and 'Enable IKE Dead Peer Detection'.
3. Click on the 'VPN' button on the left side, and then click on the 'Configure' tab along the top.
4. From the 'Security Association' drop-down box, choose "-Add New SA-".
5. From the 'IPSec Keying Mode' drop-down box, choose "IKE using Preshared Secret".
6. In the 'Name' field, enter a unique name for your VPN tunnel to the Symantec Firewall/VPN Appliance.
7. In the 'IPSec Gateway Address' field, enter the static IP address of the WAN interface of Symantec Firewall/VPN Appliance.
8. From the 'Exchange' drop-down box, choose "Main Mode".
9. From the 'Phase 1 DH Group' drop-down box, choose "Group 1".
10. In the 'SA Life time (secs)' field, enter "28800".
11. From the 'Phase 1 Encryption/Authentication' drop-down box, choose "3DES & SHA1".
12. From the 'Phase 2 Encryption/Authentication' drop-down box, choose "Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1)".
13. In the 'Shared Secret' field, enter in the shared secret you wish to use for the VPN tunnel to the Symantec Firewall/VPN Appliance.
14. Choose the 'Specify Destination Networks Below' radio button.
15. Click on the 'Add New Network...' button.
16. In the pop-up screen that appears, enter in the subnet and mask that are behind the LAN interface of the Symantec Firewall/VPN Appliance, and click on the 'Update' button when you are done.
17. Click on the 'Advanced Settings...' button.
18. In the pop-up screen that appears, check the 'Enable Keep Alive' box and the 'Try to bring up all possible SAs' checkbox below it, and then click on the 'OK' button when you are done.
19. Click on the 'Update' button in the lower right hand of the screen to save all changes.

NOTE: Values can and will be different depending upon your networking environment. The above steps use example data – you will need to substitute your network values where necessary.

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Symantec Firewall/VPN Appliances

SonicWALL Device Screenshot, VPN Summary Tab:

The screenshot displays the SonicWALL Administration web interface in Microsoft Internet Explorer. The browser's address bar shows the URL `http://192.168.60.1/management.html`. The interface features a navigation menu on the left with categories like General, Log, Filter, Tools, Access, Advanced, DHCP, VPN, Anti-Virus, and High Availability. The main content area is titled 'VPN' and includes tabs for Summary, Configure, Authentication Service, Local Certificates, and CA Certificates. The 'Summary' tab is active, showing 'Global VPN Settings' with the following configuration:

- Unique Firewall Identifier: 0040100F15F8
- Enable VPN
- Disable all VPN Windows Networking (NetBIOS) broadcast
- Enable Fragmented Packet Handling
- Enable NAT Traversal
- Keep Alive interval (seconds): 240
- Enable IKE Dead Peer Detection
- Dead Peer Detection Interval (seconds): 60
- Failure Trigger Level (missed heartbeats): 3

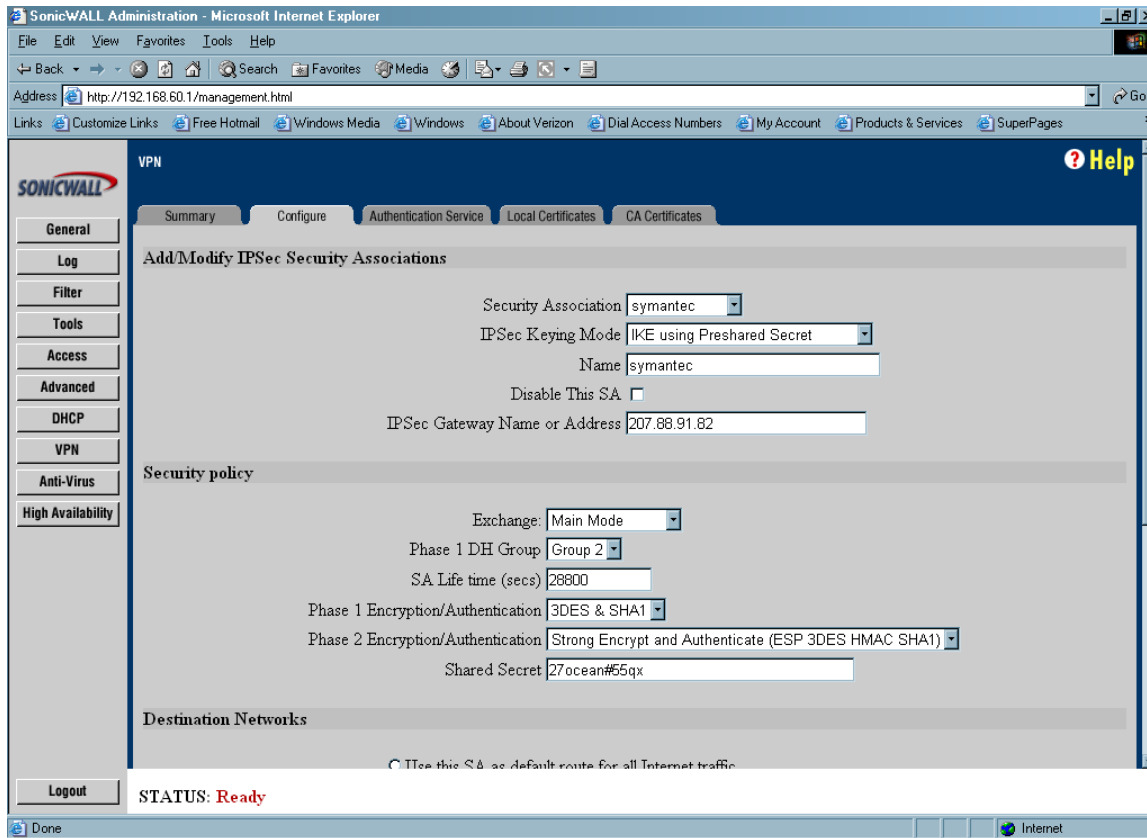
Below this is the 'VPN Bandwidth Management' section, which includes a note: 'Settings below will not take effect until enabled on Advanced Ethernet page.' The configuration for this section is:

- Enable VPN Bandwidth Management
- VPN guaranteed bandwidth: 0.000 Kbps
- VPN maximum bandwidth: 0.000 Kbps
- VPN bandwidth priority: 0 highest

At the bottom of the interface, a 'Logout' button is visible, and the status is indicated as 'STATUS: Ready'. The system tray at the bottom right shows an 'Internet' connection icon.

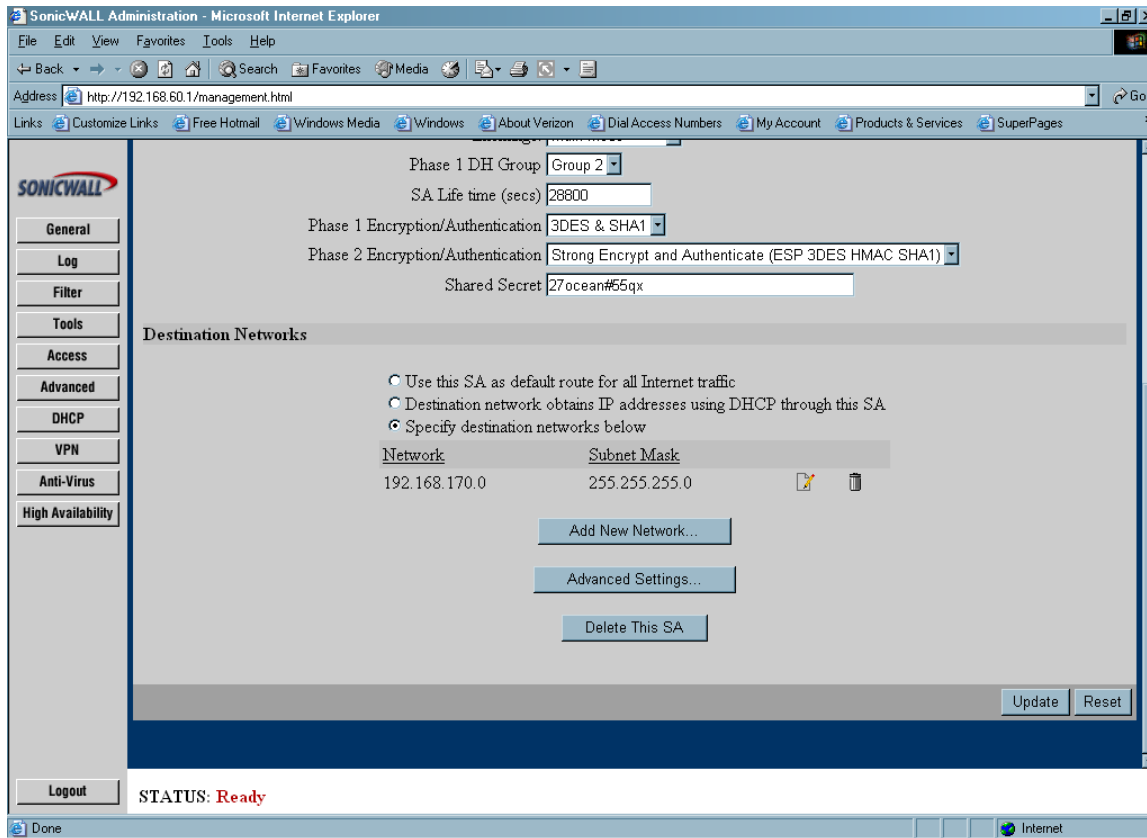
Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Symantec Firewall/VPN Appliances

SonicWALL Device Screenshot, VPN Configure Tab, Top:



Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Symantec Firewall/VPN Appliances

SonicWALL Device Screenshot, VPN Configure Tab, Bottom:



SonicWALL Device Screenshot, VPN Configure Tab, 'Add New Network' Button:

VPN Destination Network - Microsoft Internet Explorer

Edit VPN Destination Network

Network

Subnet mask

SonicWALL Device Screenshot, VPN Configure Tab, 'Advanced Settings' button:

VPN Advanced Settings - Microsoft Internet Explorer

Edit Advanced Settings

Enable Keep Alive

Try to bring up all possible SAs

Require authentication of local users

Require authentication of remote users

Remote users behind VPN gateway

Remote VPN clients with XAUTH

Enable Windows Networking (NetBIOS) broadcast

Apply NAT and firewall rules

Forward packets to remote VPNs

Enable Perfect Forward Secrecy

Phase 2 DH Group

Default LAN Gateway

VPN Terminated at LAN DMZ LAN/DMZ

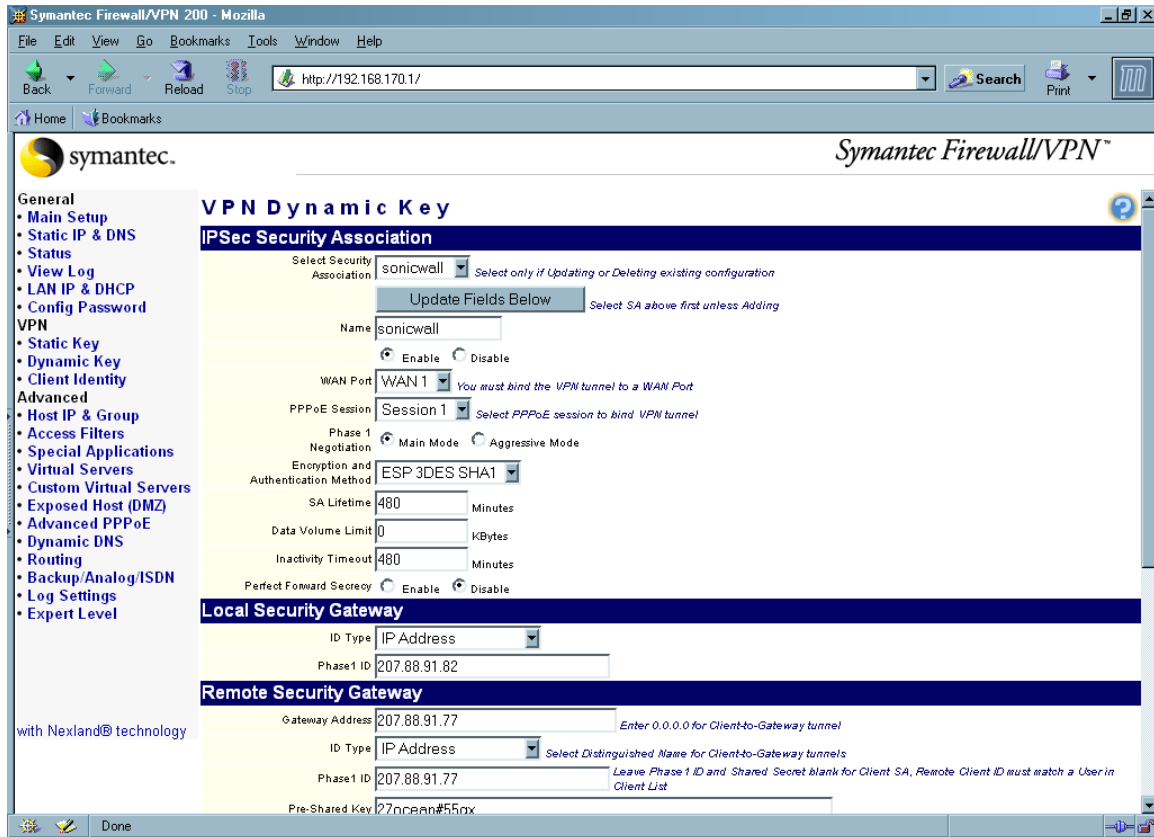
Note that after clicking OK you must click Update on the main page to save changes made here.

Symantec Firewall/VPN Appliance Setup (1.5T firmware)

1. From the 'VPN' menu on the left, select 'Dynamic Key'.
2. In the 'Name' field, enter in the unique name for this tunnel (example: "tosnw").
3. Select the radio button next to 'Enable'.
4. From the 'WAN Port' drop-down box, select the WAN Port this VPN tunnel will bind to.
5. From the 'PPPoE Session' drop-down box, select the PPPoE session this VPN tunnel will bind to.
6. Select the radio button next to 'Main Mode'.
7. From the 'Encryption and Authentication' drop-down box, select 'ESP 3DES SHA1'.
8. In the 'SA Lifetime' field, enter "480".
9. In the 'Data Volume Limit' field, leave it at "0".
10. In the 'Inactivity Timeout' field, enter "480".
11. Select the radio button next to Perfect Forward Secrecy 'Disable'.
12. From the Local Security Gateway 'ID Type' drop-down box, select "IP Address".
13. In the Local Security Gateway 'Phase 1 ID' field, enter in the WAN IP address of the Symantec Firewall/VPN Appliance.
14. In the Remote Security Gateway 'Gateway Address' field, enter in the WAN IP address of the SonicWALL device.
15. From the Remote Security Gateway 'ID Type' drop-down box, select "IP Address".
16. In the Remote Security Gateway 'Phase 1 ID' field, enter in the WAN IP address of the SonicWALL device.
17. In the Remote Security Gateway 'Pre-Shared Key' field, enter in the preshared key you wish to use for the VPN tunnel to the SonicWALL device.
18. Select the radio button next to NetBIOS Broadcast 'Disable'.
19. Select the radio button next to Global Tunnel 'Disable'.
20. In the Remote Subnet 'IP' and 'Mask' fields, enter in the IP subnet(s) and mask(s) behind the SonicWALL device.
21. Click on the 'Add' button.

NOTE: Values can and will be different depending upon your networking environment. The above steps use example data – you will need to substitute your network values where necessary.

Symantec Firewall/VPN Appliance, VPN Dynamic Key Screen, Top:



Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Symantec Firewall/VPN Appliances

Symantec Firewall/VPN Appliance, VPN Dynamic Key Screen, Bottom:

The screenshot shows the Symantec Firewall/VPN 200 web interface in a Mozilla browser window. The interface is divided into several sections for configuring VPN tunnels:

- Local Security Gateway:** ID Type is set to IP Address, and Phase 1 ID is 207.88.91.82.
- Remote Security Gateway:** Gateway Address is 207.88.91.77. ID Type is IP Address, and Phase 1 ID is 207.88.91.77. A Pre-Shared Key of 27ocean#55qx is entered.
- For Gateway-to-Gateway Tunnels...:** Includes options for NetBIOS Broadcast (Disable), Global Tunnel (Disable), and five Remote Subnet entries with their respective IP addresses and masks.
- Security Association List:** A table showing the status of the VPN connection.

Status	Name	Security Gateway	Remote Subnet	Encryption Method
Connected	sonicwall	207.88.91.77	192.168.60.0 - 255.255.255.0 192.168.65.0 - 255.255.255.0	ESP 3DES SHA1