

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Netgear FVS318 Devices

Prepared by SonicWALL, Inc.

12/05/2002

Introduction

This technote will detail all the steps necessary to create a working IKE IPSec VPN tunnel between a SonicWALL device and Netgear FVS318 Firewall/VPN device.

Please note that both the SonicWALL and the Netgear FVS318 device must have static WAN IP addresses in order to set up a VPN tunnel between the two. 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 6.4.0.0, and a Netgear FVS318 device running firmware 1.2.

Before You Begin (PLEASE READ)

SonicWALL recommends using firmware release 6.4.0.0 or newer on the SonicWALL device, and firmware release 1.2 on the Netgear FVS318 device. 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. Netscreen customers can download the newest firmware for the FVS318 device from the <http://www.netgear.com> site.

SonicWALL recommends using the 'Enable Keep Alive' feature for any VPN tunnel to a Netgear FVS318 device. 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 Netgear FVS318 device. Please note the following before you begin:

- Since SonicWALL devices use its "SA Lifetime" field for both phase one and phase two negotiations, you must take care use the same time for both the ISAKMP and IPSEC fields in the Netgear FVS318 device.
- The methods of Dead Peer Detection for SonicWALL devices and Netgear FVS318 devices 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 Netgear FVS318 devices. Make sure that NAT Traversal is deactivated on the SonicWALL device, if it is not deactivated, it may cause problems.
- The Netgear FVS318 device allows the admin to define the IKE Identity it sends, and the IKE Identity it expects from the peer device. If these are not set correctly, the VPN tunnel will not establish.
- The Netgear FVS318 does not allow the user to select the hashing mechanism – it automatically sends both MD5 and SHA-1 for all IKE/IPSec negotiations.
- The Netgear FVS318 does not allow the user to select the DH Group when doing a Main Mode negotiation – it automatically uses DH Group 2.
- The Netgear FVS318 does not allow the user to specify different encryption protocols for phase one and phase two – a single drop-down box is used for both.
- If the Netgear FVS318 has a dynamically obtained WAN IP address, it will not be possible to set up a VPN tunnel to the SonicWALL device, due to the way the Netgear FVS318 calculates the initialization vector for phase two. This is a Netgear issue and cannot be addressed by SonicWALL.

Scenario One: SonicWALL with static WAN IP address, Netgear FVS318 with static WAN IP address

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

SonicWALL Device Setup (6.4.0.0 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 Netgear FVS318 device.
7. In the 'IPSec Gateway Address' field, enter the static IP address of the WAN interface of the Netgear FVS318 device.
8. From the 'Exchange' drop-down box, choose "Main Mode".
9. From the 'Phase 1 DH Group' drop-down box, choose "Group 2".
10. In the 'SA Life time (secs)' field, enter "28800"
11. From the 'Phase 1 Encryption/Authentication' drop-down box, choose "3DES & MD5".
12. From the 'Phase 2 Encryption/Authentication' drop-down box, choose "Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)".
13. In the 'Shared Secret' field, enter in the shared secret you wish to use for the VPN tunnel to the Netgear FVS318 device
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 Netgear FVS318 device, 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.

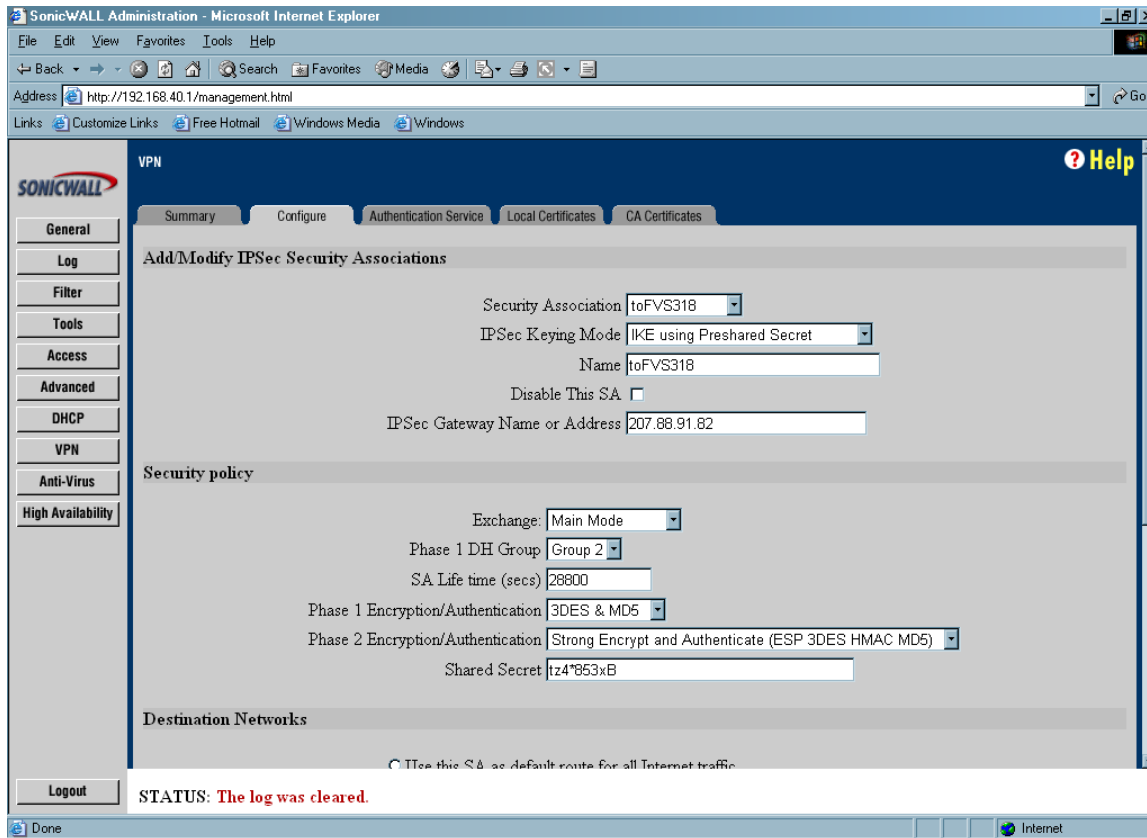
Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Netgear FVS318 Devices

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://192.168.40.1/management.html`. The interface features a navigation menu on the left with options like General, Log, Filter, Tools, Access, Advanced, DHCP, VPN, Anti-Virus, and High Availability. The main content area is titled 'VPN' and includes a 'Summary' tab. Under 'Global VPN Settings', the Unique Firewall Identifier is '0040100FCD42'. The 'Enable VPN' checkbox is checked, while 'Disable all VPN Windows Networking (NetBIOS) broadcast', 'Enable NAT Traversal', and 'Enable IKE Dead Peer Detection' are unchecked. The 'Keep Alive interval (seconds)' is set to 240, 'Dead Peer Detection Interval (seconds)' is 60, and 'Failure Trigger Level (missed heartbeats)' is 3. The 'VPN Bandwidth Management' section is currently disabled, with a note stating 'Settings below will not take effect until enabled on Advanced Ethernet page.' The bandwidth management options include 'Enable VPN Bandwidth Management' (unchecked), 'VPN guaranteed bandwidth' (0.000 Kbps), 'VPN maximum bandwidth' (0.000 Kbps), and 'VPN bandwidth priority' (highest). A status message at the bottom reads 'STATUS: The log was cleared.' The browser's status bar at the bottom shows 'Done' and 'Internet'.

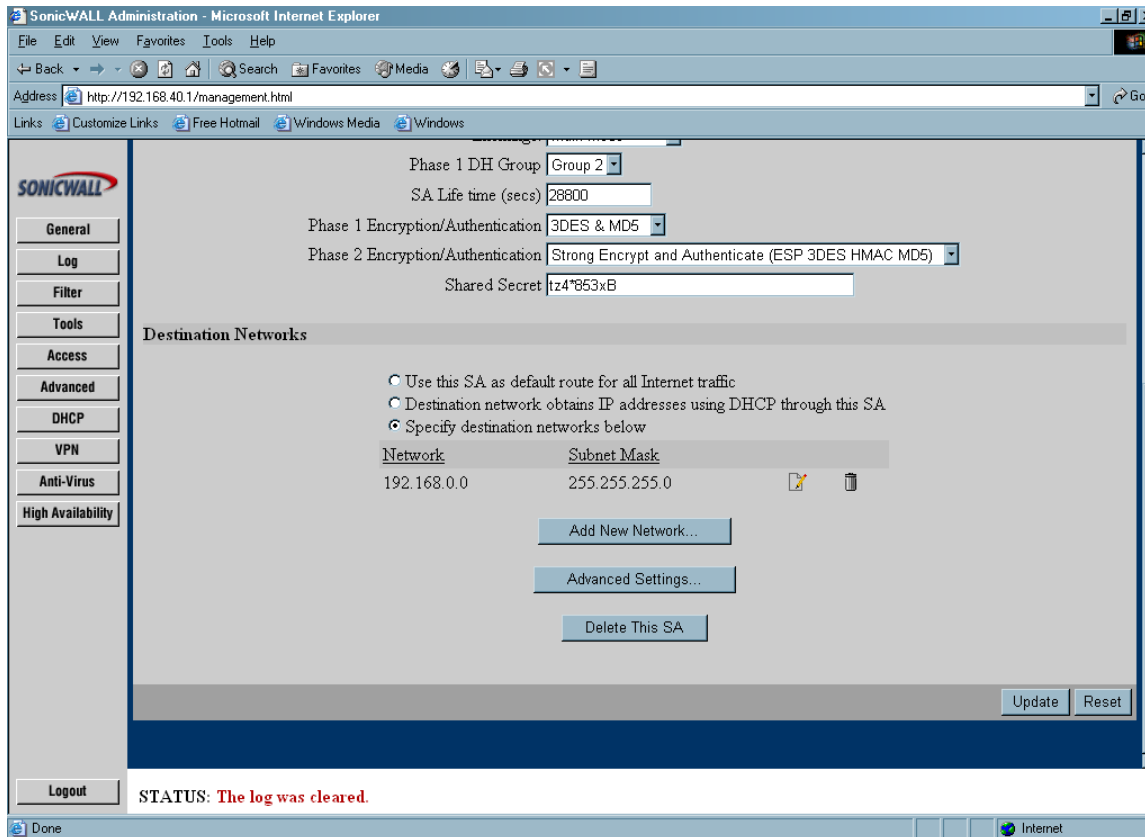
Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Netgear FVS318 Devices

SonicWALL Device Screenshot, VPN Configure Tab, Top:

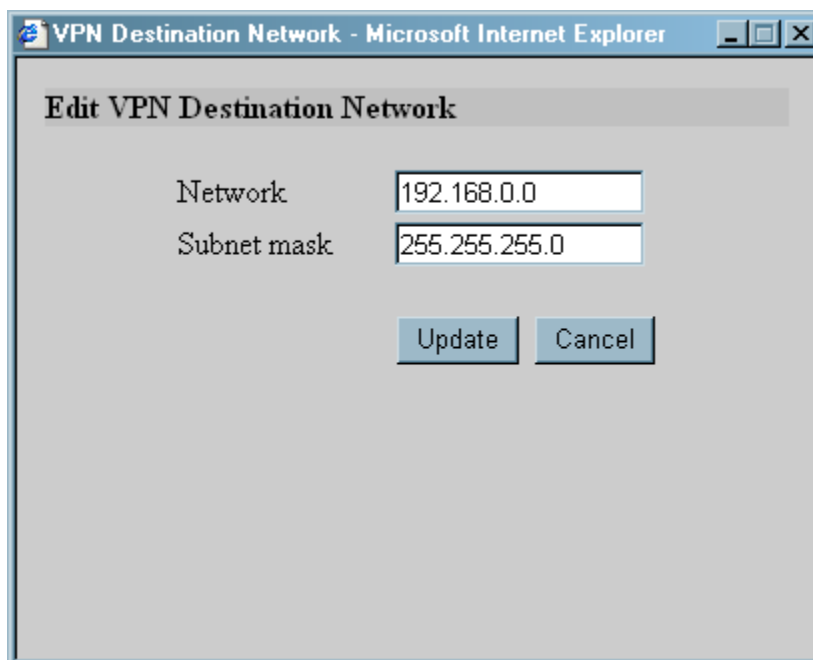


Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Netgear FVS318 Devices

SonicWALL Device Screenshot, VPN Configure Tab, Bottom:

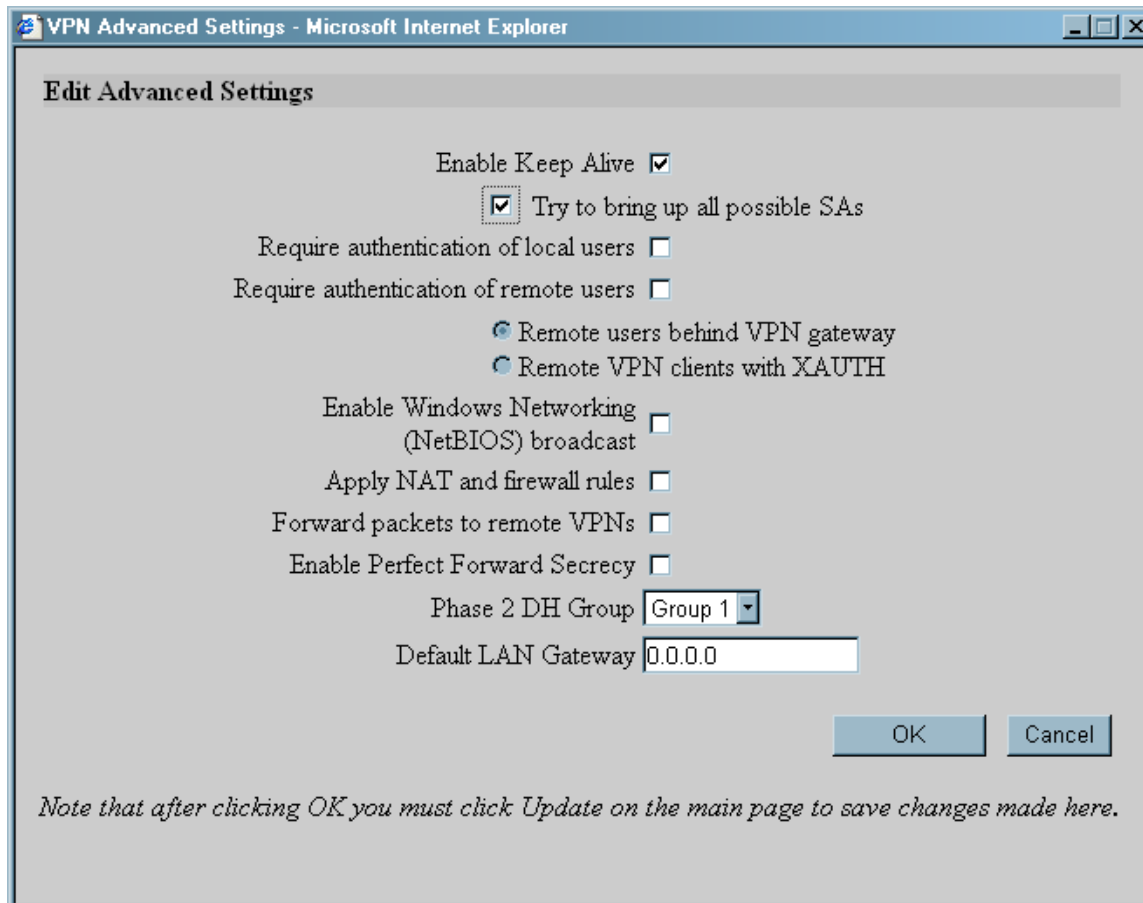


SonicWALL Device Screenshot, VPN Configure Tab, 'Add New Network' Button:



Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Netgear FVS318 Devices

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

OK Cancel

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

Netgear FVS318 Device Setup

1. Log into the Netgear FVS318'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' (replace x.x.x.x with the LAN IP of your Netgear FVS318 device).
2. Click on the 'VPN Settings' link on the left side, select an empty radio button, and then click on the 'Edit' button below it. This will open a new screen titled 'VPN Settings – Main Mode'.
3. In the 'Connection Name' box, enter in a unique name for the VPN tunnel to the SonicWALL device.
4. In the 'Local IPSec Identifier' box, enter in the FVS318's WAN IP address.
5. In the 'Remote IPSec Identifier' box, enter in the SonicWALL's WAN IP address.
6. In the 'Remote LAN IP Address', enter in the subnet of the remote SonicWALL's LAN interface (example: 192.168.40.0).
7. In the 'Remote LAN Subnet Mask', enter in the subnet mask of the remote SonicWALL's LAN interface (example: 255.255.255.0).
8. From the 'Secure Association' drop-down box, select "Main Mode".
9. Next to 'Perfect Forward Secrecy', select the "Disabled" radio button.
10. From the 'Encryption Protocol' drop-down box, select "3DES".
11. In the 'PreShared Key' box, enter in the same preshared key you set up on the remote SonicWALL device for this VPN tunnel.
12. In the 'Key Life' box, enter in "28800" seconds.
13. In the 'IKE Life Time', enter in "28800" seconds.
14. Click on the 'Apply' button in the lower center of the screen to save all changes. When it returns to the 'VPN Settings' screen, make sure the checkbox next to 'Enable' is checked.
15. Reboot the Netgear FVS318

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 Netgear FVS318 Devices

Netgear FVS318 Device Screenshot, 'VPN Settings' Screen:

The screenshot shows the 'VPN Settings' page for a Netgear FVS318 ProSafe VPN Firewall. The browser window title is 'NETGEAR Router - Microsoft Internet Explorer' and the address bar shows 'http://192.168.0.1'. The page has a purple header with the Netgear logo and 'settings' text. A left sidebar contains navigation menus for 'Basic Settings', 'VPN Settings', 'Security', 'Maintenance', 'Advanced', and 'Logout'. The main content area is titled 'VPN Settings' and contains a table with the following data:

#	Enable	Connection Name	Local IPSec ID	Remote IPSec ID
1	<input checked="" type="checkbox"/>	toSNWL	207.88.91.82	207.88.91.89
2	<input type="checkbox"/>	-	-	-
3	<input type="checkbox"/>	-	-	-
4	<input type="checkbox"/>	-	-	-
5	<input type="checkbox"/>	-	-	-
6	<input type="checkbox"/>	-	-	-
7	<input type="checkbox"/>	-	-	-
8	<input type="checkbox"/>	-	-	-

Below the table are 'Edit', 'Delete', and 'Cancel' buttons. To the right is a 'VPN Settings Help' section with the following text:

A Virtual Private Network (VPN) allows two hosts or networks to connect securely over the public Internet. For each secure connection, you must create and configure a Security Association (SA), which is a set of policies and keys for authentication and encryption between the two sides.

To set up a VPN Security Association (SA):

1. Click the button next to a number on the table.
2. Click **Edit** to open the editing menu.
3. Type a name for this Security Association in the **Connection Name** box.
(This is for identification purposes only.)
4. Enter a **Local IPSec Identifier** name for this router. This name must be entered in the other endpoint as Remote IPSec Identifier.
5. Enter a **Remote IPSec Identifier** name for the remote router or host. This name must be entered in the other endpoint as Local IPSec Identifier.
6. Define the remote network by entering its **Remote LAN IP Address** and **Subnet Mask**. If the destination is a single host, type 255.255.255.255 as the Subnet Mask.
7. Type the **Remote WAN IP Address**, which will be the public IP address of the remote router or host.

Note: The Local and Remote IPSec Identifiers must not be used by any other Security Association defined in this network.

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Netgear FVS318 Devices

Netgear FVS318 Device Screenshot, 'VPN Settings – Main Mode' Screen:

