

Topics

[Home](#)

[Apple](#) (31/0)

[Mac OS X](#) (11/0)

[Grrr!](#) (2/0)

[Windows](#) (3/0)

[All About Me](#) (14/0)

[WTF?](#) (14/0)

[Cool stuff](#) (11/0)

[Product Reviews](#) (3/0)

[Reader mail](#) (1/0)

[General News](#) (11/0)

[Rescued!](#) (1/0)

User Functions

Username:

Password:

Don't have an account yet?

Sign up as a [New User](#)

Events

There are no upcoming events

Older Stories

Wednesday 05-Jan

- [Yo...](#) (0)

Thursday 30-Dec

- [An elaboration on my inexpensive Mac comments to Red Herring IT journal](#) (4)

Wednesday 29-Dec

- [A question for Windows users: Would you buy a \\$500 Mac?](#) (0)
- [Jerry Orbach from Law & Order dies](#) (0)

Establishing a VPN with IPSecuritas and the Netgear FVS318

Monday, December 20 2004 @ 01:57 PM EST

Contributed by: [Aaron](#)

Views: 73



The Google search term that brings more people to this page than any other is "free VPN client". I've written about [IPSecuritas before](#), and I'm assuming that's the article to which the Google search links. At the same time, during my surfing, I've seen a number of users with questions about how to connect to the [Netgear FVS318](#) with a VPN client, sometimes IPSecuritas specifically.

There don't seem to be any good directions on the web for IPSecuritas and the FVS318, so I decided to post some here. Read more for illustrations and complete instructions.

I prefer to set up the FVS318 first. As wonderful as Safari is, for some reason it doesn't cooperate very well with Netgear's built-in web-based management pages. Instead of Safari, I use [Firefox](#) — you're obviously free to use whatever browser works for you.

After logging into the FVS318, click on "VPN Settings" in the left frame. You'll get a list of VPN connections like this one:

VPN Settings

| | # | Enable | Connection Name | Local IPsec ID | Remote IPsec ID |
|-----------------------|---|-------------------------------------|-----------------|----------------|-----------------|
| <input type="radio"/> | 1 | <input checked="" type="checkbox"/> | | | |
| <input type="radio"/> | 2 | <input checked="" type="checkbox"/> | | | |
| <input type="radio"/> | 3 | - | - | - | - |
| <input type="radio"/> | 4 | - | - | - | - |
| <input type="radio"/> | 5 | - | - | - | - |
| <input type="radio"/> | 6 | - | - | - | - |
| <input type="radio"/> | 7 | - | - | - | - |
| <input type="radio"/> | 8 | - | - | - | - |

I've blurred out the information from my FVS318 for privacy reasons. Click the radio button next to one of the connection numbers and then click the "Edit" button below. You'll be presented with the "VPN Settings - Main Mode" page.

| | |
|-----------------------------|--|
| Connection Name | Remote Access |
| Local IPsec Identifier | |
| Remote IPsec Identifier | |
| Tunnel can be accessed from | <input type="text" value="a subnet of local address"/> |
| Local LAN start IP Address | |

Monday 27-Dec

- [The iPod halo effect](#) (0)

Sunday 26-Dec

- [An idea for an improvement to iPhoto](#) (0)

Friday 24-Dec

- [Insert entirely neutral and inoffensive generic holiday greeting, if any, here](#) (0)
- [The Blizzard of 2004](#) (0)

Wednesday 22-Dec

- [New forums are now open for your participation](#) (0)

Tuesday 21-Dec

- [iPod Battery Replacement](#) (0)

The screenshot shows a configuration window for a VPN connection. The settings are as follows:

- Local LAN finish IP Address: 0.0.0.0
- Local LAN IP Subnetmask: 255.255.255.0
- Tunnel can access: a single remote address (dropdown)
- Remote LAN start IP Address: 192.168.1.0
- Remote LAN finish IP Address: 192.168.1.0
- Remote LAN IP Subnetmask: 255.255.255.0
- Remote WAN IP or FQDN: 0.0.0.0
- Secure Association: Aggressive Mode (dropdown)
- Perfect Forward Secrecy: Enabled (radio button selected)
- Encryption Protocol: AES - 256 (dropdown)
- Key Group: Diffie-Hellman Group1 (dropdown)
- PreShared Key: *****
- Key Life: 28800 Seconds
- IKE Life Time: 86400 Seconds
- NETBIOS Enable

Buttons for 'Apply' and 'Cancel' are visible at the bottom.

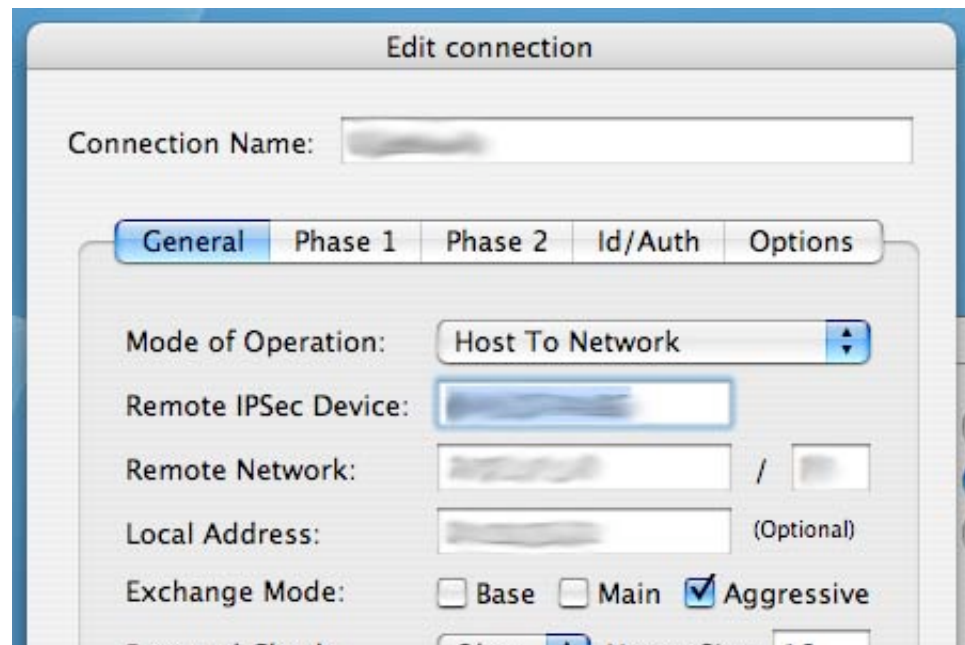
Now let's fill in the boxes:

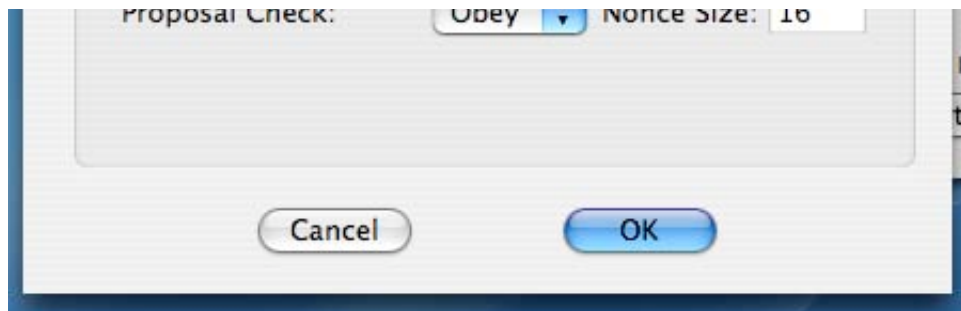
- **Connection name:** This is a name you give the connection so that you can identify it later. This name can be anything and only serves to remind you what the connection is for.
- **Local IPSec Identifier:** This is a name you're giving to the firewall to identify it in the VPN connection. Remember this name because it will be needed later when we set up the client. For instance, you could enter "Firewall" in this box to identify the FVS318 as your firewall.
- **Remote IPSec Identifier:** This name identifies the device connecting to the FVS318 to create the VPN, in this case, your Mac. To keep things simple, you can enter "Mac" into this box. Remember this name for later too.
- **Tunnel can be accessed from:** This drop-down determines what devices can access the VPN tunnel from behind the firewall. In our particular case, we're going to select "a subnet of local addresses". This will allow devices from a specific subnet connected to the firewall to communicate over the VPN. This setting can be changed to meet specific needs. For instance, if you want only one device behind the firewall to communicate over the VPN, you can select "a single local IP address".
- **Local LAN start IP Address:** Since we selected to allow a subnet to access the tunnel, this value needs to be the IP address that designates the subnet we want to allow. Most users are probably using a class C subnet of some kind, so that's the example I'll use here. In the case of a class C subnet, the IP address to enter into these boxes is 192.168.1.0.
- **Local LAN finish IP Address:** This section is unnecessary in the example setup. It would be useful if you selected "a range of local addresses" from the drop-down a couple of steps ago.
- **Local LAN IP Subnetmask:** This is the subnet mask of the LAN behind the firewall which we allowed to access the VPN tunnel. For the class C IP address given earlier, the subnet mask is 255.255.255.0.
- **Tunnel can access:** This setting specifies which remote devices can be accessed by devices communicating over the VPN from behind the firewall. In our example, we're going to select "a single remote address" because we're connecting a single remote Mac to the firewall.

- **Remote LAN start IP address:** This is an address that is going to be assigned to the virtual interface that will be created on the Mac for the VPN connection. The firewall will have to route traffic to this address, so it cannot be in the same subnet as the devices behind the firewall. Since devices behind the firewall are assigned 192.168.1.x, it would be acceptable to assign the IP address 10.1.2.3 to the remote Mac we're connecting from.
- **Remote LAN finish IP Address:** For this example, we leave this setting blank.
- **Remote LAN IP Subnetmask:** For this example, we leave this setting blank.
- **Remote WAN IP or FQDN:** This should be set to 0.0.0.0.
- **Secure association:** Set this drop-down to "Aggressive Mode".
- **Prefect Forward Secrecy:** Click the "Enabled" button.
- **Encryption Protocol:** This specifies what kind of encryption will be used to secure data as it travels across the tunnel. Different protocols have their positives and negatives. I personally like AES-256 because it's secure and efficient. You may choose whatever encryption protocol you like, but be sure to adjust these instructions so that you're using the same protocol at the firewall and at the VPN client. After all, your Mac and the firewall can't talk to each other if they're speaking a different encrypted language.
- **Key Group:** Select "Diffie-Hellman Group 1" from the drop-down.
- **PreShared Key:** This is a sort of password that both your Mac's VPN client and the FVS318 both know so they can verify they're supposed to communicate with each other. Enter a secure word or phrase here, using the same rules you would use to create a secure password.
- **Key Life:** Set this value to 28800 seconds.
- **IKE Life Time:** Set his value to 86400 seconds.
- **NETBIOS Enable:** NetBIOS is protocol that communicates via broadcasts. Since broadcasts are non-routable, any NetBIOS traffic that a VPN client would want to send or receive will not make it to an intended destination on the other end of the VPN tunnel. I assume this check box uses some technical trickery to forward those broadcasts over the tunnel. Macs do not use NetBIOS, so there is no reason to check this box.
- Click the "Apply" button.

Your FVS318 firewall should now be set up to accept a VPN connection from your Mac. Now we need to set up the VPN client, in this case, IPSecuritas, on the Mac.

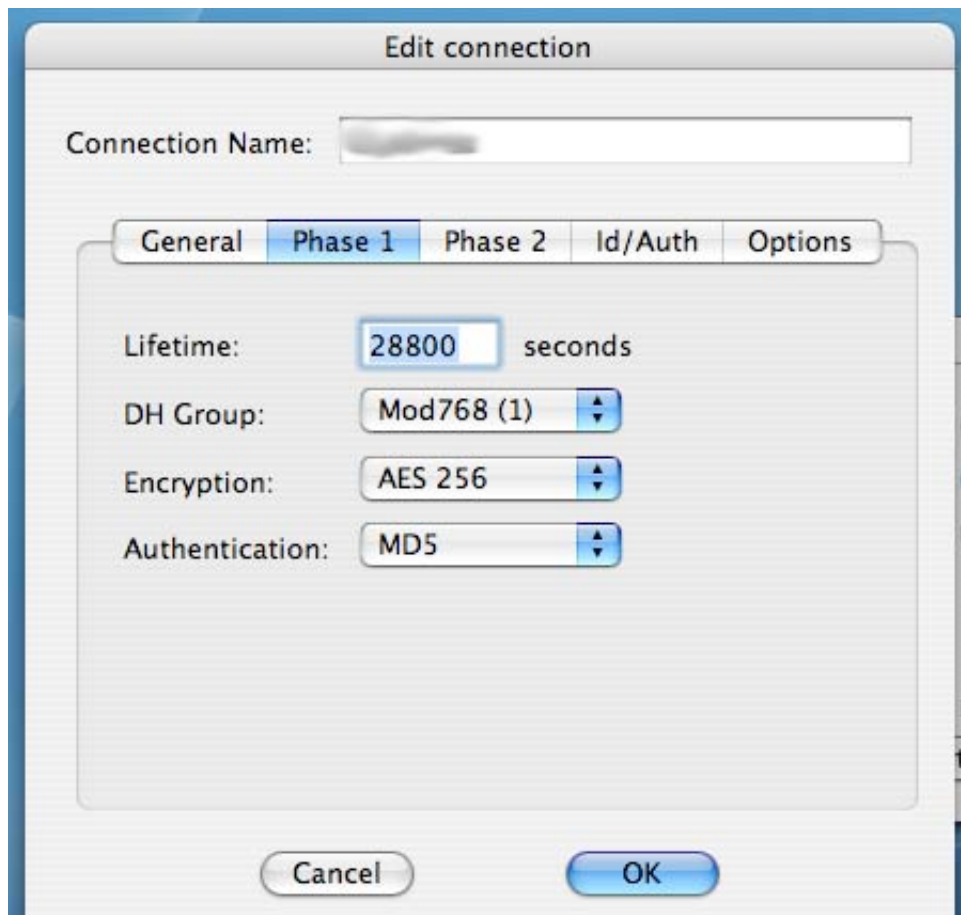
At the "General" tab:





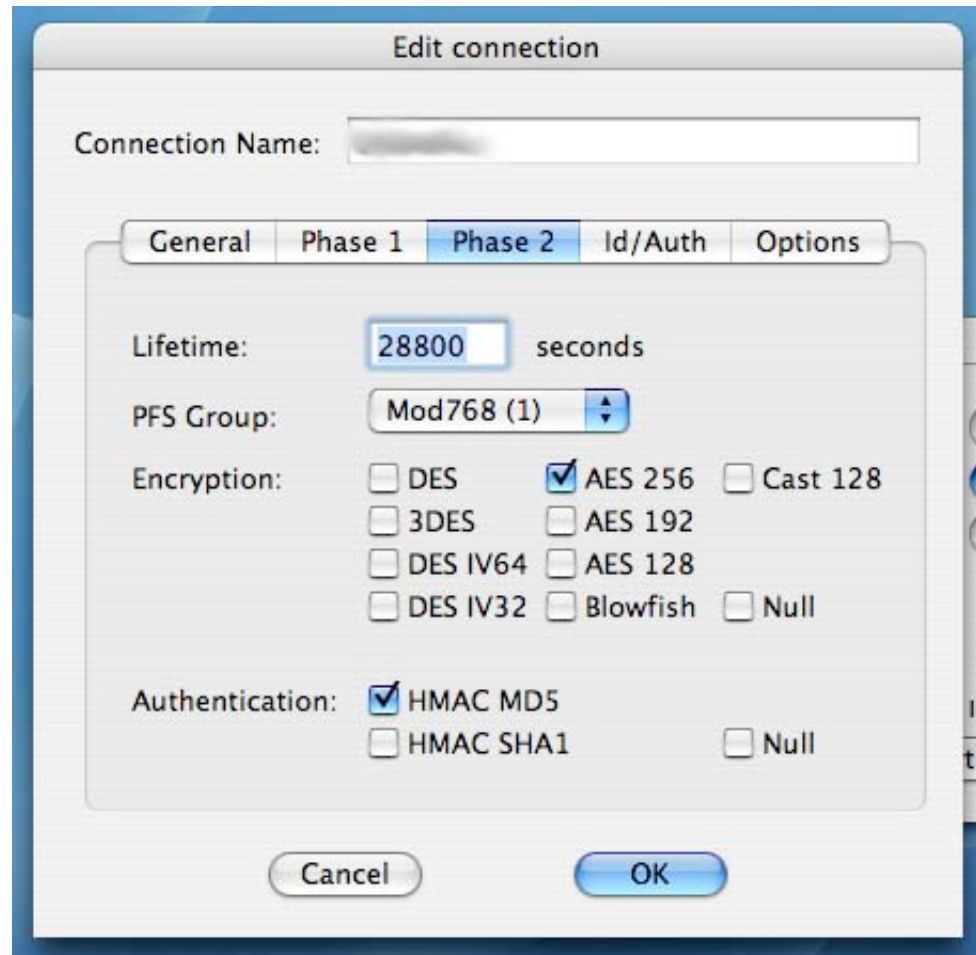
- Start IPsec and click the "New" button on the initial window.
- **Connection Name:** As on the FVS318, this is a name you give the connection that is meaningful to you. It does not affect the connection.
- **Mode of Operation:** Select "Host To Network" from the drop-down. We are a single machine (host) connecting to the firewall (network).
- **Remote IPsec Device:** Enter the IP address of the FVS318 into this box.
- **Remote Network:** Enter the IP address of the network behind the firewall into this box. We entered this information into the FVS318 in a step above as 192.168.1.0. The box to the right and after the slash is for a value called the CIDR. This is a shorthand notation for the subnet mask. Again, in a step above, we said the subnet mask was 255.255.255.0. The CIDR notation, and the value you should enter into the the box, is 24.
- **Local Address:** This is the IP address we're assigning to the Mac. This is also something we entered into the FVS318 in a step above. The value we gave it there was 10.1.2.3, and that's the same value that should be entered into this box.
- **Exchange Mode:** Check the "Aggressive" box and uncheck all others.
- **Proposal Check:** Select "Obey" from the drop-down and set the Nonce Size to 16.

At the "Phase 1" tab:



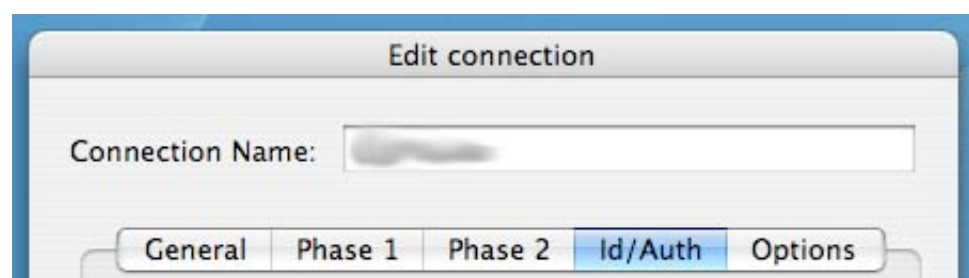
- **Lifetime:** Set to 28800 seconds.
- **DH Group:** This should be the same as the Diffie-Hellman value we set on the FVS318. Choose "Mod768 (1)" from the drop-down.
- **Encryption:** This should be the same as the encryption method we set on the FVS318. Choose "AES 256" from the drop-down.
- **Authentication:** Choose "MD5" from the drop-down.

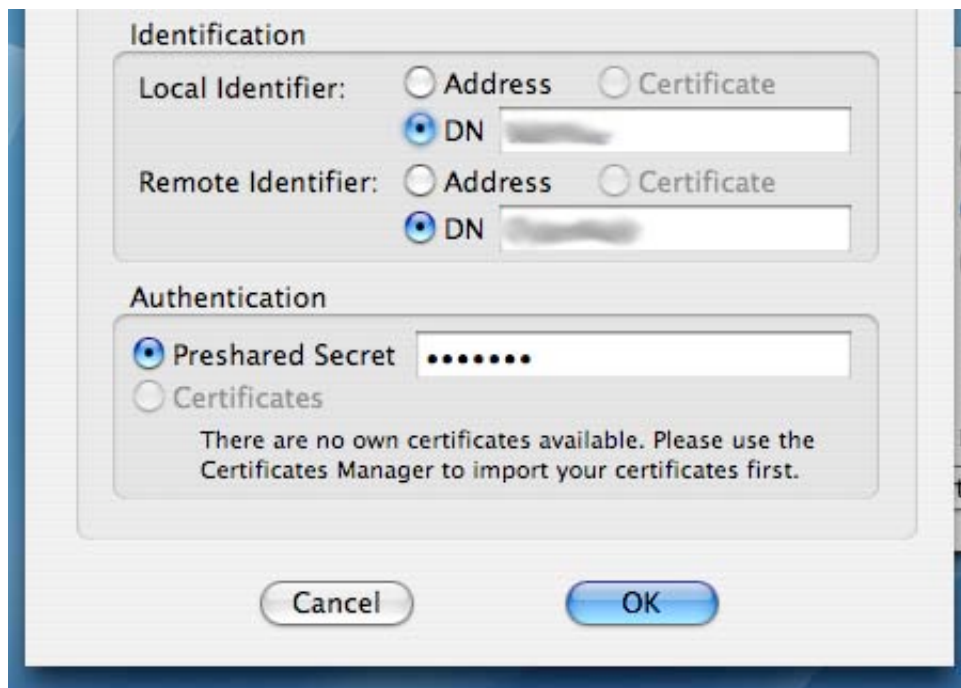
At the "Phase 2" tab:



- **Lifetime:** Enter 28800 seconds
- **PFS Group:** This corresponds to the "Perfect Forward Secrecy" option we enabled at the FVS318. Choose "Mod768 (1)" from the drop-down.
- **Encryption:** Again, corresponding with settings on the FVS318, check "AES 256" and uncheck all others.
- **Authentication:** Check "HMAC MD5" and uncheck all others.

At the "Id/Auth" tab:





- **Local Identifier:** This is the identifier that is assigned to your Mac. This name *must* be the same as the remote identifier value entered on the FVS318, which if you remember, was "Mac".
- **Remote Identifier:** This is the identifier that is assigned to the firewall. This name *must* be the same as the local identifier value entered on the FVS318, which if you remember, was "Firewall".
- **Preshared Secret:** This *must* be the same as the preshared secret key entered on the FVS318.

The "Options" tab contains things that are not important for the purposes of this example. You can click OK and the connection will be saved.

At the initial IPsecrutas screen, click the "Start IPsec" button. It will take several seconds, but the red X next to your newly created connection will change to a green check mark and your VPN will be ready to go!

What's Related

- [More by Aaron](#)
- [More from Mac OS X](#)

Story Options

- [Mail Story to a Friend](#)
- [Printable Story Format](#)

Establishing a VPN with IPsecrutas and the Netgear FVS318 | 0 comments | [Create New Account](#)

Oldest First | Threaded | Refresh | Reply

The following comments are owned by whomever posted them. This site is not responsible for what they say.