



VPN Tracker for Mac OS X



How-to:

Interoperability with

NETGEAR FVM 318

Internet Security Appliances

Rev. 1.0

Copyright © 2004 equinux USA Inc. All rights reserved.

1. Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a NETGEAR FVM318 VPN Firewall.

The NETGEAR FVM318 VPN Firewall is configured as a router, connecting a company LAN to the Internet. The example demonstrates a connection scenario, with a dial-in Mac connecting to a NETGEAR FVM318 VPN Firewall.

This paper is only a supplement to, not a replacement for, the instructions that have been included with your NETGEAR FVM318 VPN Firewall. Please be sure to read and understand those instructions before beginning.

All trademarks, product names, company names, logos, screenshots displayed, cited or otherwise indicated on the How-to are the property of their respective owners.

EQUINIX SHALL HAVE ABSOLUTELY NO LIABILITY FOR ANY DIRECT OR INDIRECT, SPECIAL OR OTHER CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE USE OF THE HOW-TO OR ANY CHANGE TO THE ROUTER GENERALLY, INCLUDING WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS, OR DATA, EVEN IF EQUINIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2. Prerequisites

Firstly, you should use a recent NETGEAR firmware version. The latest firmware release for your NETGEAR FVM318 VPN Firewall can be obtained from:

<http://www.netgear.com/>

For this document, firmware version 1.1 has been used.

VPN Tracker is compatible with Mac OS X 10.2 / 10.3.

3. Connecting a VPN Tracker Host to a NETGEAR FVM318 VPN Firewall

In this example, the Mac running VPN Tracker is directly connected to the Internet via a dialup or PPP connection.¹ The NETGEAR FVM318 VPN Firewall is configured in NAT mode and has the static WAN IP address 169.1.2.3 and the private LAN IP address 192.168.1.1. The stations in the LAN behind the NETGEAR FVM318 VPN Firewall use 192.168.1.1 as their default gateway and should have a working Internet connection.

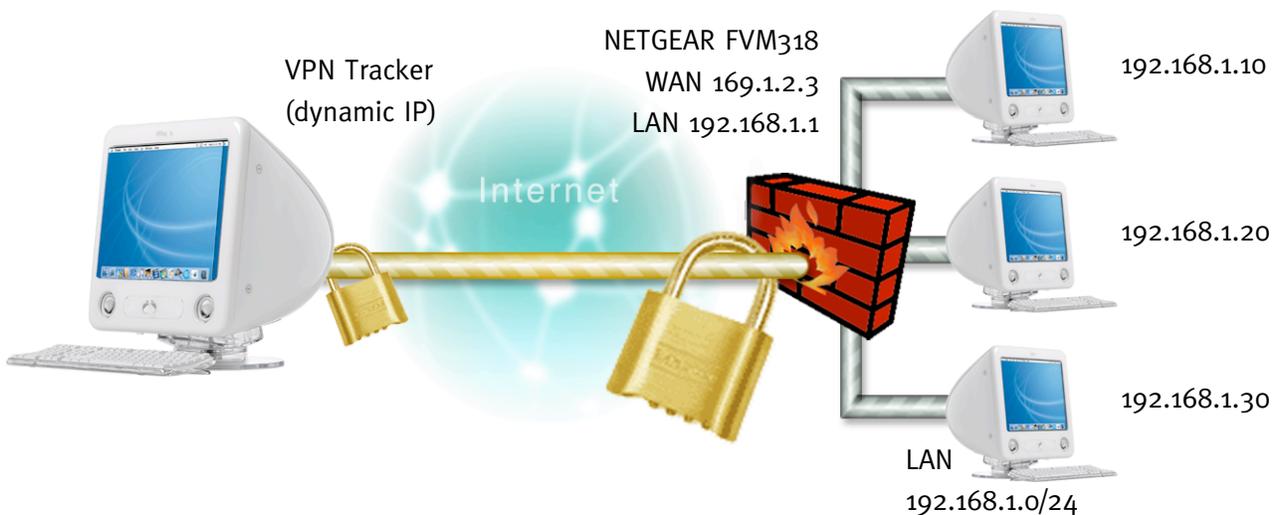


Figure 1: VPN Tracker - NETGEAR FVM318 VPN Firewall connection diagram

¹ Please note that the connection via a router, which uses Network Address Translation (NAT), only works if the NAT router supports „IPsec passthrough“. Please contact your router’s manufacturer for details.

3. Connecting a VPN Tracker Host to a NETGEAR FVM318 VPN Firewall

3.1 NETGEAR FVM 318 Configuration

Step 1

Please go to Setup -> VPN Settings and enter a “Connection Name” e.g. vpntracker. You have to use identifiers in the passage “Local” and “Remote IPsec Identifier”. These settings refer to the “Remote” and “Local Identifier” settings in VPN Tracker. Please type in an arbitrary local and remote identifier (e.g. “netgear” and “vpntracker”).

Please set the “Remote LAN IP Address” to 10.1.2.3 and the “Remote LAN Subnet Mask” to 255.255.255.255. The “Remote WAN IP Address” should be set to 0.0.0.0.

You have to use the “Aggressive Mode” and the Perfect Forward Secrecy must be enabled. The pre-defined connection type for NETGEAR FVM318 uses AES128 and the Diffie-Hellman Group 2. Finally you have to enter your Pre-shared key.

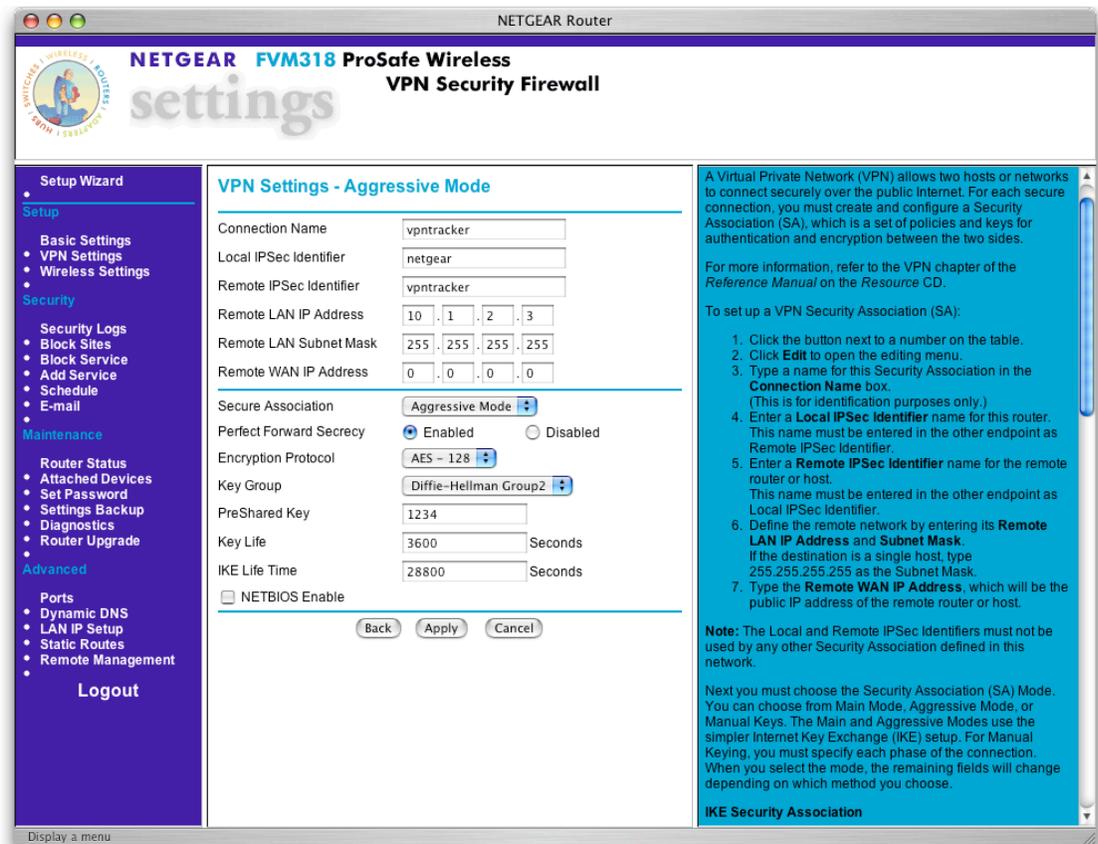


Figure 2: NETGEAR FVM318 - VPN Settings

3. Connecting a VPN Tracker Host to a NETGEAR FVM318 VPN Firewall

The pre-defined connection type “Netgear FVM318” is based on these settings. Please check all fields. The values should be exactly the same as shown on the screenshot below. Click on apply to save your settings.

Please repeat this step for each Mac you want to connect to the NETGEAR FVM318. You need to supply a unique IP for each remote Mac connecting to the NETGEAR FVM318 Router.

3.2 VPN Tracker configuration

Step 1

Add a new connection with the following options: Choose „Netgear FVM318“ as the Connection Type, „Host to Network“ as Topology, then type in the remote endpoint (169.1.2.3) and the remote network (192.168.1.0/24).

Please enter an IP address in the field “local host”. This address refers to the “Remote LAN IP Address” in Figure 2 (e.g. 10.1.2.3).



The screenshot shows the 'VPN Tracker Main Window' configuration dialog. It is divided into three sections: General, Networking, and Authentication. In the General section, the Name is 'Netgear FVM318', Connection Type is 'Netgear FVM318', and 'Initiate connection' is checked. In the Networking section, Topology is 'Host to Network', Local Endpoint is 'Default Interface', Remote Endpoint is '169.1.2.3', Local Host is '10.1.2.3' (optional), and Remote Network is '192.168.1.0 / 24'. In the Authentication section, 'Pre-shared key' is selected. At the bottom, there is a lock icon with the text 'Click the lock to prevent further changes.' and 'Cancel' and 'Save' buttons.

Figure 3: VPN Tracker Main Window

3. Connecting a VPN Tracker Host to a NETGEAR FVM318 VPN Firewall

Step 2

Select as “Authentication” method „Pre-shared key“ and click “Edit...”. Type in the same shared secret that you typed-in in the NETGEAR router (Figure 2). Enter the local (e.g. vpntracker) and the remote (e.g. netgear) identifier. The local identifier in VPN tracker is the remote identifier in the NETGEAR configuration and vice versa.

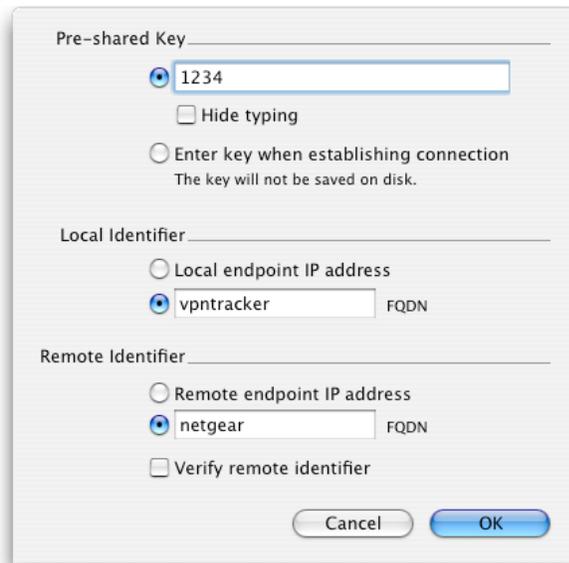


Figure 4: VPN Tracker - Authentication dialog

Step 3

Save the connection and Click „Start IPsec“ in the VPN Tracker main window.

You’re done. After 10-20 seconds the red status indicator for the connection should change to green, which means you’re securely connected to the NETGEAR FVM318 VPN Firewall. After IPsec has been started, you may quit VPN Tracker. The IPsec service will keep running.

Simply test your connection by pinging a host in the NETGEAR FVM318 network from the dialed-in Mac in the “Terminal” utility:

```
ping 192.168.1.1
```

❖ Debugging

If the status indicator does not change to green please have a look at the log file on both sides. You can define the amount of information available in the log file in the VPN Tracker preferences.

4. Secure your NETGEAR FVM318 WLAN using VPN Tracker

The NETGEAR FVM318 is configured in NAT mode and has the static WAN IP address 169.1.2.3 and the private WLAN IP address 192.168.1.1.

The Macs are connected to the NETGEAR FVM318 via WLAN and use 192.168.1.1 as their default gateway. If IPsec Encryption is enabled and the VPN Tunnel is not yet established the Macs can just login into the WLAN, but you can't access any resources on the Internet or the LAN.

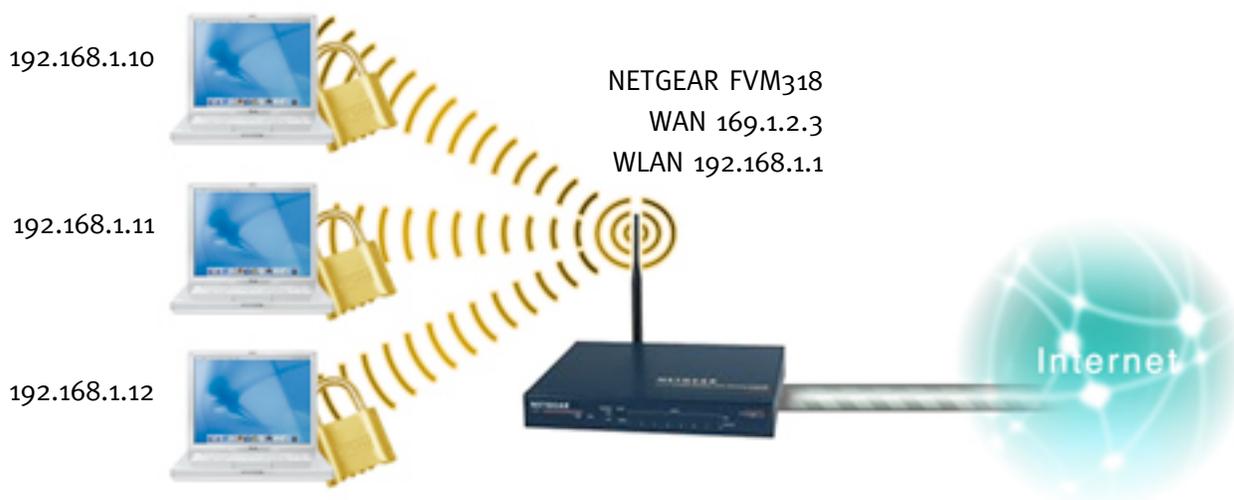


Figure 5: NETGEAR FVM318 - VPN Tracker - Wireless Encryption

4. Secure your NETGEAR FVM318 WLAN using VPN Tracker

4.1 NETGEAR FVM318 Configuration

Step 1

Please go to Wireless Settings and set the “Encryption Strength” to IPsec. Additionally, allowing access to “Trusted PCs only” is recommended.

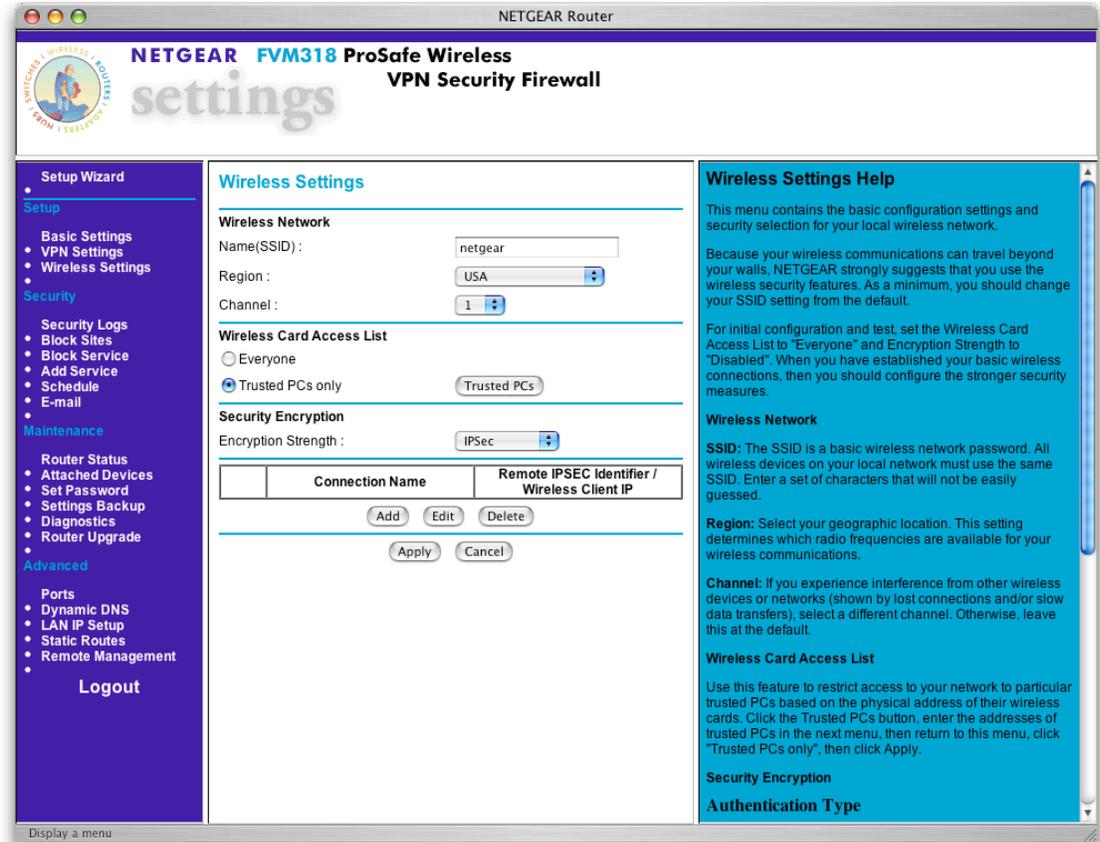


Figure 6: NETGEAR FVM318 - Wireless Settings

4. Secure your NETGEAR FVM318 WLAN using VPN Tracker

Step 2

Please add a new connection and enter a User Name (refers to Local Identifier in VPN Tracker Configuration) and a Pre-shared Key. The “Encryption Protocol” must be set to “AES – 128”. Then click on apply to save these settings.

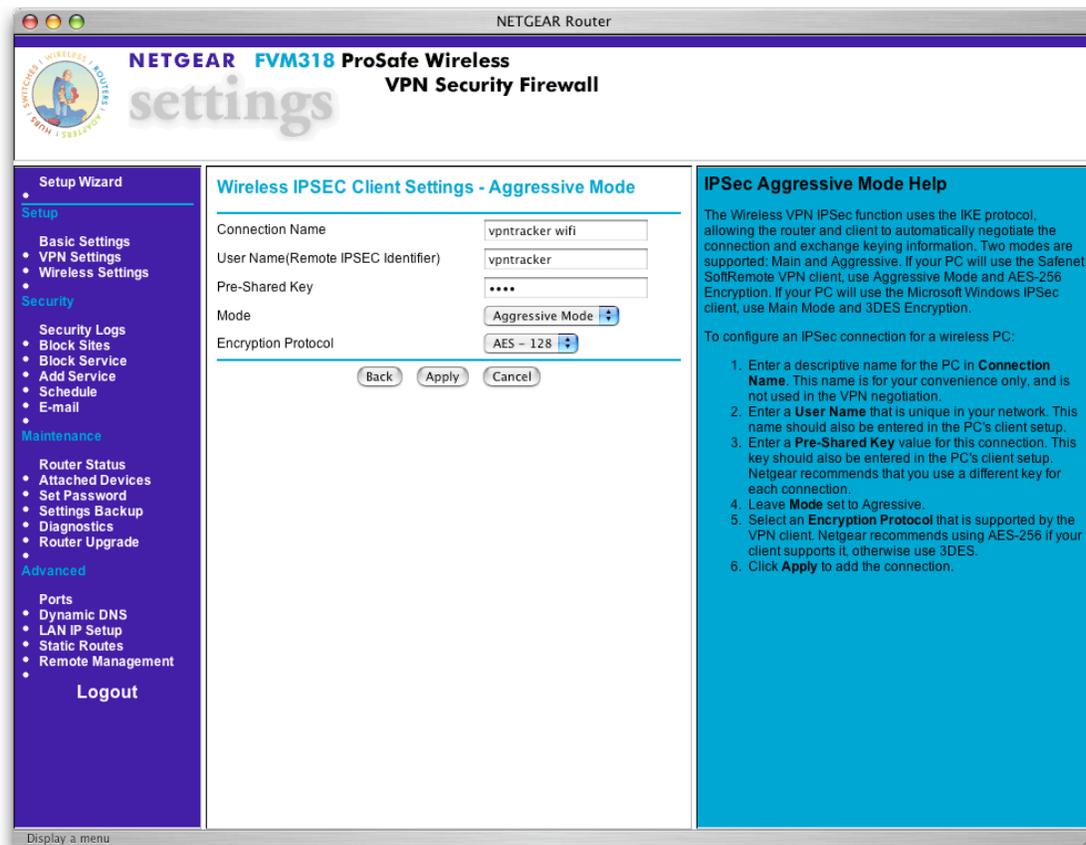


Figure 7: NETGEAR FVM318 - Wireless IPsec Settings

4.2 VPN Tracker Configuration

Step 1

Add a new connection with the following options: Choose „NETGEAR FVM318“ as the Connection Type, „Host to Everywhere“ as Topology, then type in the remote endpoint (192.168.1.1).

The screenshot shows the main configuration window for a VPN connection in VPN Tracker. The window is titled "General" and contains the following fields and options:

- Name:** Netgear FVM318 WiFi
- Connection Type:** Netgear FVM318
- Initiate connection**
- Networking**
 - Topology:** Host to Everywhere
 - Local Endpoint:** Default Interface
 - Remote Endpoint:** 192.168.1.1
 - Local Host:** optional
 - Remote Network:** all traffic runs across the VPN
- Authentication**
 - Pre-shared key** Edit...
 - Certificates** Edit...

At the bottom, there is a lock icon with the text "Click the lock to prevent further changes." and two buttons: "Cancel" and "Save".

Figure 8: VPN Tracker - Host To Everywhere - Main Window

4. Secure your NETGEAR FVM318 WLAN using VPN Tracker

Step 2

Select as “Authentication” method „Pre-shared key“ and click “Edit...”. Type in the same shared secret that you typed-in in the Wireless IPsec settings and enter the User Name as “Local Identifier” (Figure 7).



Figure 9: VPN Tracker - Host To Everywhere - Main Window

You're done. After 10-20 seconds the red status indicator for the connection should change to green, which means you're securely connected to the NETGEAR FVM318. After IPsec has been started, you may quit VPN Tracker. The IPsec service will keep running.

Now to test your connection simply ping a Internet host in the “Terminal” utility:

```
ping www.google.com
```