



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.

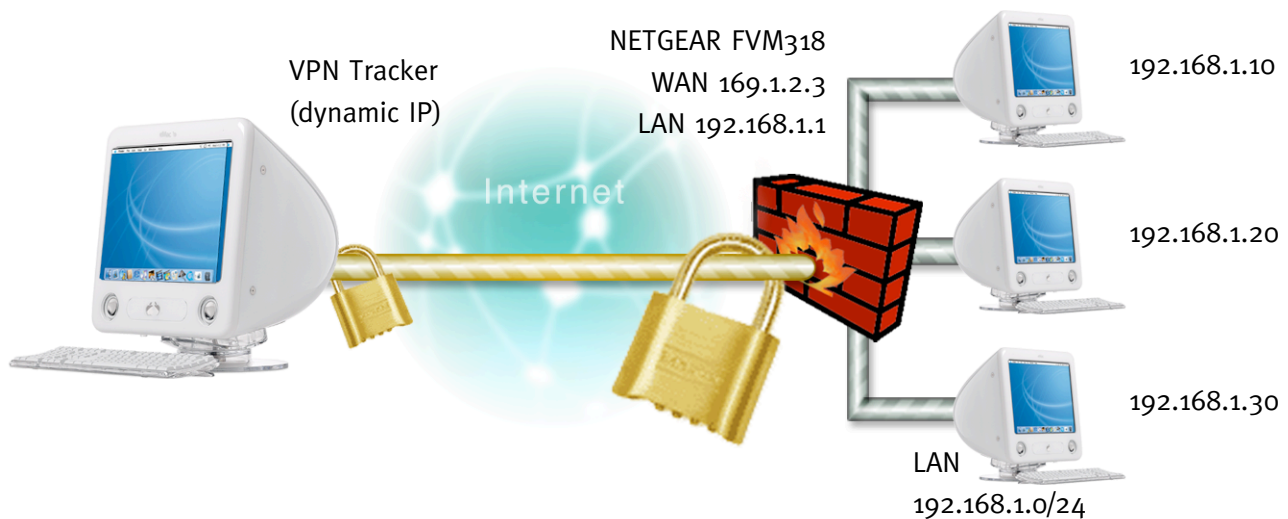


Figure 1: VPN Tracker - NETGEAR FVM318 VPN Firewall connection diagram

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.

The screenshot displays the NETGEAR FVM318 ProSafe Wireless VPN Security Firewall settings page. The left sidebar contains a navigation menu with sections: Setup Wizard, Setup, Basic Settings, VPN Settings, Wireless Settings, Security, Router Status, Attached Devices, Set Password, Settings Backup, Diagnostics, Router Upgrade, Advanced, Ports, Dynamic DNS, LAN IP Setup, Static Routes, Remote Management, and Logout. The main content area is titled "VPN Settings - Aggressive Mode" and contains the following fields:

- Connection Name: vpntracker
- Local IPsec Identifier: netgear
- Remote IPsec Identifier: vpntracker
- Remote LAN IP Address: 10.1.2.3
- Remote LAN Subnet Mask: 255.255.255.255
- Remote WAN IP Address: 0.0.0.0
- Secure Association: Aggressive Mode (selected)
- Perfect Forward Secrecy: Enabled (selected)
- Encryption Protocol: AES - 128 (selected)
- Key Group: Diffie-Hellman Group2 (selected)
- PreShared Key: 1234
- Key Life: 3600 Seconds
- IKE Life Time: 28800 Seconds
- NETBIOS Enable: ☐

At the bottom of the form are buttons for Back, Apply, and Cancel. On the right side, there is a blue informational box with text about Virtual Private Networks (VPN) and a list of steps to set up a VPN Security Association (SA). Below this box is a "Note" and a section titled "IKE Security Association".

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.

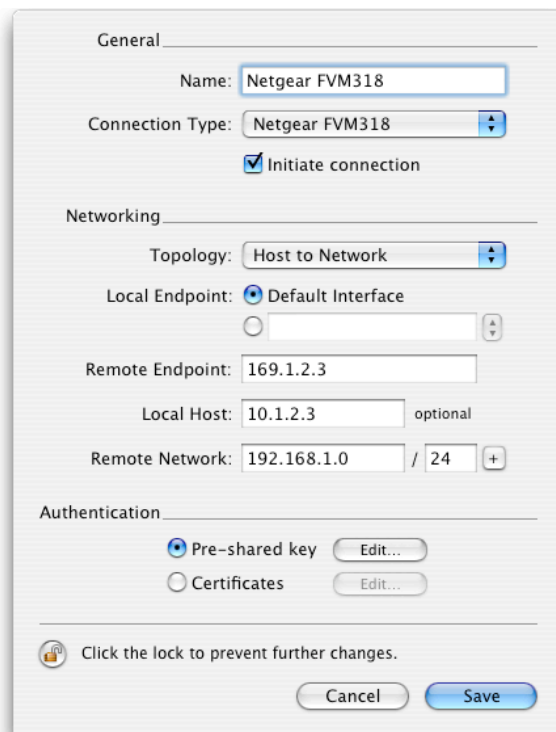
Please repeat this step for each Mac you want to connect to the NETGEAR FVM318. You need to supply a unique IP for each remote Mac connecting to the NETGEAR FVM318 Router.

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' field is set to 'Netgear FVM318', the 'Connection Type' is 'Netgear FVM318', and the 'Initiate connection' checkbox is checked. In the Networking section, the 'Topology' is 'Host to Network', the 'Local Endpoint' is 'Default Interface', the 'Remote Endpoint' is '169.1.2.3', the 'Local Host' is '10.1.2.3' (marked as optional), and the 'Remote Network' is '192.168.1.0 / 24'. In the Authentication section, the 'Pre-shared key' radio button is selected, and there are 'Edit...' buttons for both 'Pre-shared key' and 'Certificates'. 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.

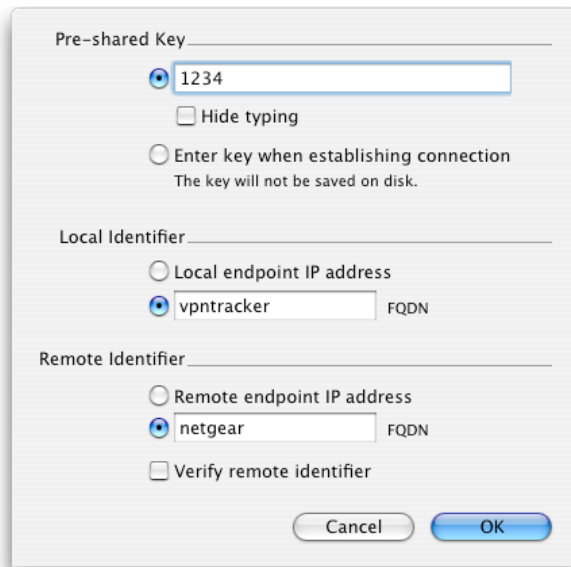


Figure 4: VPN Tracker - Authentication dialog

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.

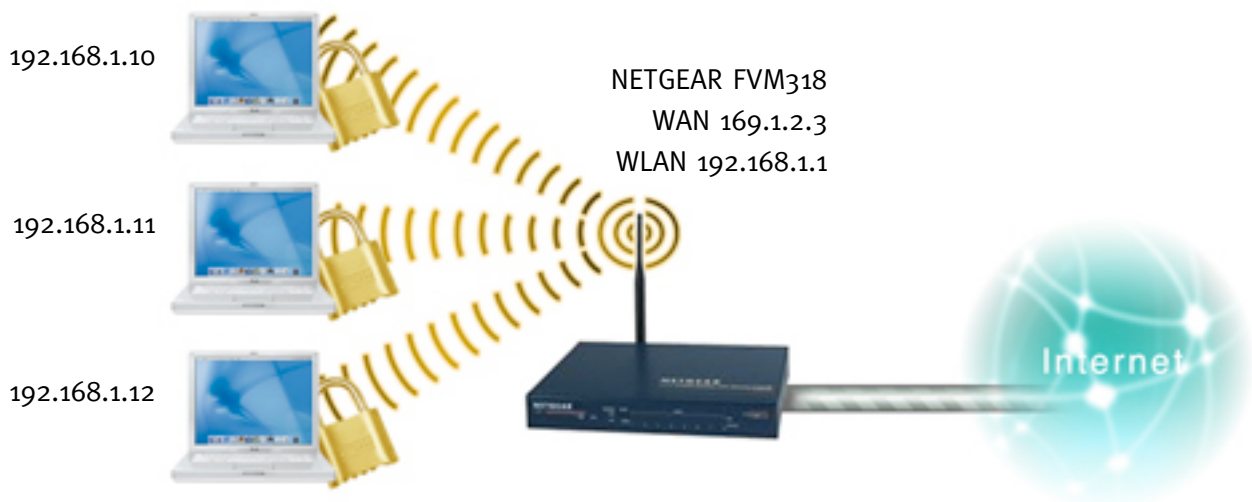


Figure 5: NETGEAR FVM318 - VPN Tracker - Wireless Encryption

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.

NETGEAR Router

NETGEAR FVM318 ProSafe Wireless
settings VPN Security Firewall

Setup Wizard

Setup

- Basic Settings
- VPN Settings
- Wireless Settings

Security

- Security Logs
- Block Sites
- Block Service
- Add Service
- Schedule
- E-mail

Maintenance

- Router Status
- Attached Devices
- Set Password
- Settings Backup
- Diagnostics
- Router Upgrade

Advanced

- Ports
- Dynamic DNS
- LAN IP Setup
- Static Routes
- Remote Management

Logout

Wireless Settings

Wireless Network

Name(SSID) : netgear

Region : USA

Channel : 1

Wireless Card Access List

☐ Everyone

☒ Trusted PCs only Trusted PCs

Security Encryption

Encryption Strength : IPSec

Connection Name	Remote IPSEC Identifier / Wireless Client IP
-----------------	--

Add Edit Delete

Apply Cancel

Wireless Settings Help

This menu contains the basic configuration settings and security selection for your local wireless network.

Because your wireless communications can travel beyond your walls, NETGEAR strongly suggests that you use the wireless security features. As a minimum, you should change your SSID setting from the default.

For initial configuration and test, set the Wireless Card Access List to "Everyone" and Encryption Strength to "Disabled". When you have established your basic wireless connections, then you should configure the stronger security measures.

Wireless Network

SSID: The SSID is a basic wireless network password. All wireless devices on your local network must use the same SSID. Enter a set of characters that will not be easily guessed.

Region: Select your geographic location. This setting determines which radio frequencies are available for your wireless communications.

Channel: If you experience interference from other wireless devices or networks (shown by lost connections and/or slow data transfers), select a different channel. Otherwise, leave this at the default.

Wireless Card Access List

Use this feature to restrict access to your network to particular trusted PCs based on the physical address of their wireless cards. Click the Trusted PCs button, enter the addresses of trusted PCs in the next menu, then return to this menu, click "Trusted PCs only", then click Apply.

Security Encryption

Authentication Type

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.

NETGEAR Router

NETGEAR FVM318 ProSafe Wireless
settings VPN Security Firewall

Setup Wizard
• Setup
• Basic Settings
• VPN Settings
• Wireless Settings
• Security
• Security Logs
• Block Sites
• Block Service
• Add Service
• Schedule
• E-mail
• Maintenance
• Router Status
• Attached Devices
• Set Password
• Settings Backup
• Diagnostics
• Router Upgrade
• Advanced
• Ports
• Dynamic DNS
• LAN IP Setup
• Static Routes
• Remote Management
• Logout

Wireless IPSEC Client Settings - Aggressive Mode

Connection Name: vpntracker wifi
User Name(Remote IPSEC Identifier): vpntracker
Pre-Shared Key: ****
Mode: Aggressive Mode
Encryption Protocol: AES - 128

Back Apply Cancel

IPSec Aggressive Mode Help

The Wireless VPN IPSec function uses the IKE protocol, allowing the router and client to automatically negotiate the connection and exchange keying information. Two modes are supported: Main and Aggressive. If your PC will use the Safenet SoftRemote VPN client, use Aggressive Mode and AES-256 Encryption. If your PC will use the Microsoft Windows IPSec client, use Main Mode and 3DES Encryption.

To configure an IPSec connection for a wireless PC:

1. Enter a descriptive name for the PC in **Connection Name**. This name is for your convenience only, and is not used in the VPN negotiation.
2. Enter a **User Name** that is unique in your network. This name should also be entered in the PC's client setup.
3. Enter a **Pre-Shared Key** value for this connection. This key should also be entered in the PC's client setup. Netgear recommends that you use a different key for each connection.
4. Leave **Mode** set to Aggressive.
5. Select an **Encryption Protocol** that is supported by the VPN client. Netgear recommends using AES-256 if your client supports it, otherwise use 3DES.
6. Click **Apply** to add the connection.

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 'VPN Tracker' configuration window. It is divided into three main sections: 'General', 'Networking', and 'Authentication'.
In the 'General' section, the 'Name' field is set to 'Netgear FVM318 WiFi'. The 'Connection Type' dropdown menu is set to 'Netgear FVM318'. The 'Initiate connection' checkbox is checked.
In the 'Networking' section, the 'Topology' dropdown menu is set to 'Host to Everywhere'. The 'Local Endpoint' is set to 'Default Interface'. The 'Remote Endpoint' field contains the IP address '192.168.1.1'. The 'Local Host' field is empty, with the word 'optional' next to it. Below this, it says 'Remote Network: all traffic runs across the VPN'.
In the 'Authentication' section, the 'Pre-shared key' radio button is selected, and there is an 'Edit...' button next to it. The 'Certificates' radio button is unselected, also with an 'Edit...' button next to it.
At the bottom of the window, there is a lock icon and the text 'Click the lock to prevent further changes.' Below this are 'Cancel' and 'Save' buttons.

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).

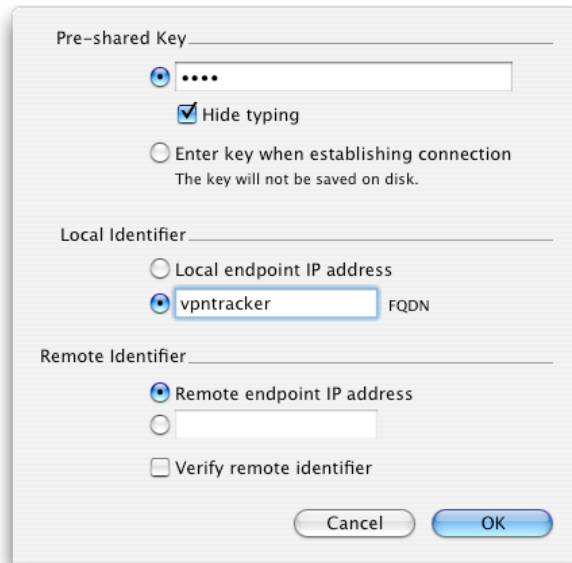


Figure 9: VPN Tracker - Host To Everywhere - Main Window

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