e·quinux

VPN Configuration Guide

WatchGuard Firebox X Series - Fireware

Revision 1.0.1

equinux AG and equinux USA, Inc.

Every effort has been made to ensure that the information in this manual is accurate. equinux is not responsible for printing or clerical errors.

Created using Apple Pages.

www.equinux.com

equinux shall have absolutely no liability for any direct or indirect, special or other consequential damages in connection with the use of the quick setup guide or any change to the router generally, including without limitation, any lost profits, business, or data, even if equinux has been advised of the possibility of such damages.

Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a WatchGuard Firebox VPN firewall.

The WatchGuard Firebox gateway is configured as a router connecting a company LAN to the Internet.

This paper is only a supplement to, not a replacement for, the instructions that have been included with your WatchGuard Firebox. Please be sure to read those instructions and understand them before starting.

EQUINUX 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 EQUINUX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Prerequisites

First you have to make sure to use a recent Fireware firmware version. The latest release for your WatchGuard Firebox firewall can be obtained from https://www.watchguard.com/archive/softwarecenter.asp/

For this document, Fireware firmware version 8.2.1 has been used.

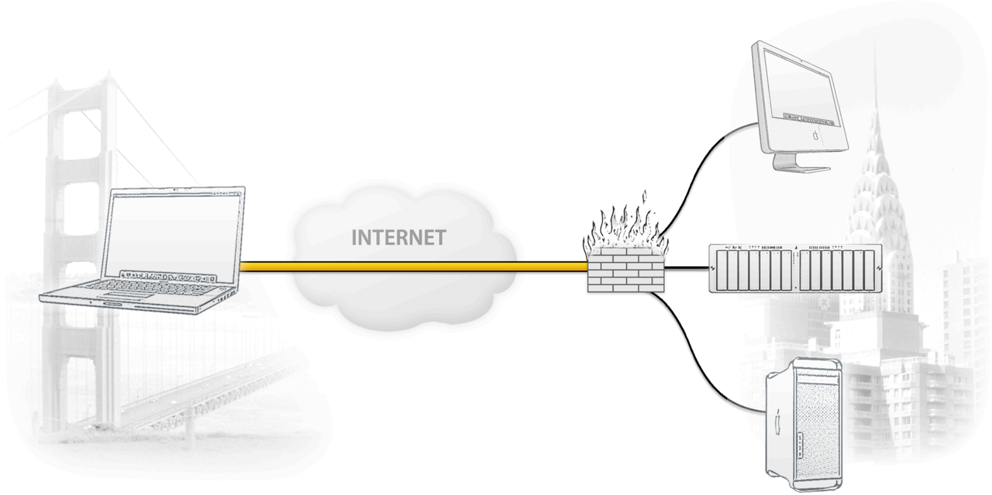
Please note: VPN Tracker has been only been tested with the WatchGuard Firebox X series and the above firmware version.

You will need one VPN Tracker Personal Edition license for each Mac connecting to the WatchGuard Firebox.

We recommend one VPN Tracker Professional Edition for the administrator's Mac in order to export configuration files to the clients. VPN Tracker is compatible with Mac OS X version 10.2.5+, 10.3 and 10.4.1+

Scenario

In our example, we need to connect an employee's Mac Book in San Francisco to an office in New York. The following diagram illustrates this scenario:



The MacBook is directly connected to the Internet and has a public IP address, assigned by an ISP.

The office's VPN gateway is also connected to the Internet and can be accessed via an static IP address. The VPN gateway also has a second interface which is connected to the internal office network. In our example, the office network has the IP range 192.168.1.0/24.

A VPN tunnel will be established between the public interfaces in San Francisco and New York. Once the VPN tunnel is up, San Francisco can access the office network behind the VPN gateway.

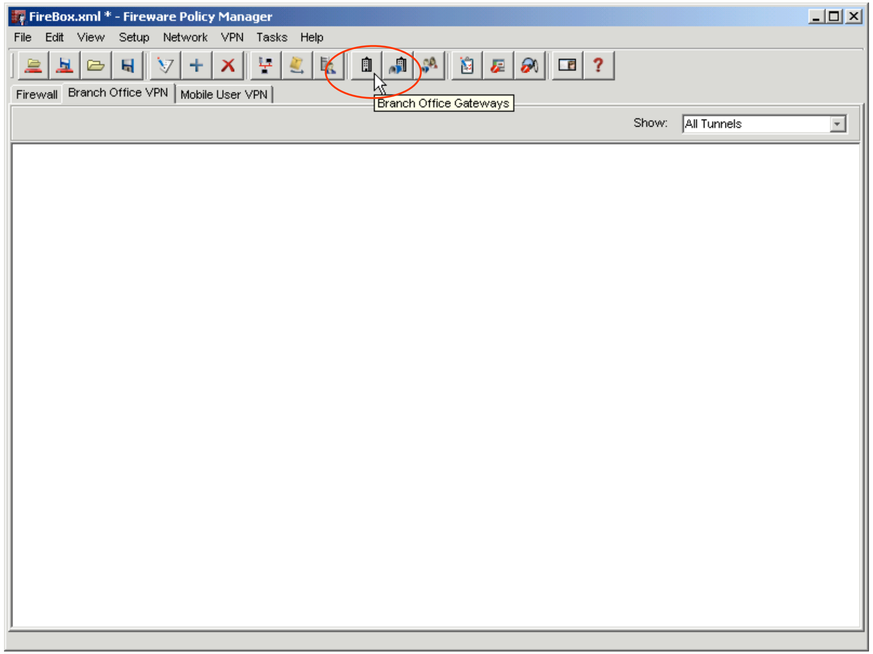
Please note that the connection from a MacBook at home to an office network is just one possible scenario. The instructions also apply to connections from a desktop computer or notebook in your office to a VPN gateway at home or at another office. Please adapt the term "office network", which is used throughout this manual, to your scenario.

Task 1 – Configure your WatchGuard Firebox

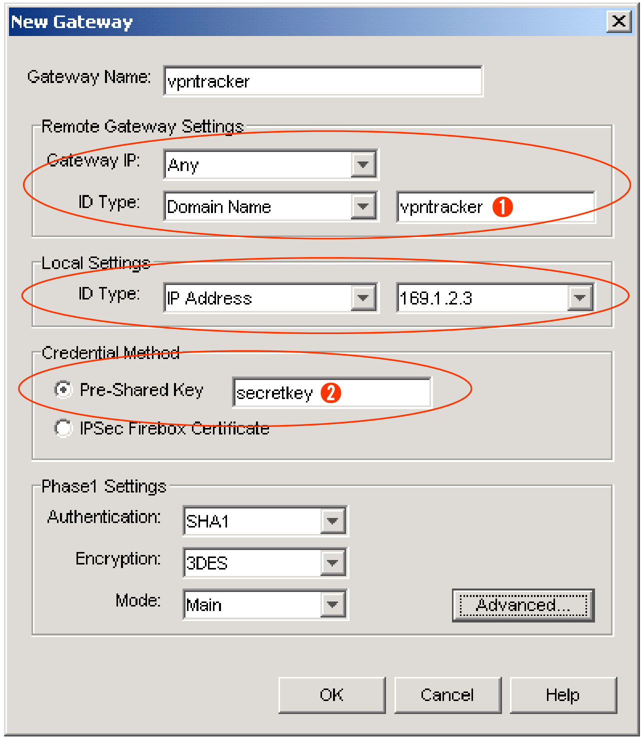
This section describes the configuration of your WatchGuard Firebox. The configuration will be created with the "Fireware Policy Manager".

TIP When setting up a VPN, you'll have to handle a couple of parameters. Those parameters are marked with red dots with little numbers in it. Throughout the setup we will point back to those parameters.

Step 1 - Add a new Branch Office Gateway



- Click on "Branch Office Gateways".
- Click on "Add" in the "Gateways" dialog.



New Gateway

Gateway Name: vpntracker

Remote Gateway Settings

Gateway IP: Any

ID Type: Domain Name | vpntracker ❶

Local Settings

ID Type: IP Address | 169.1.2.3

Credential Method

● Pre-Shared Key: secretkey ❷

○ IPSec Firebox Certificate

Phase1 Settings

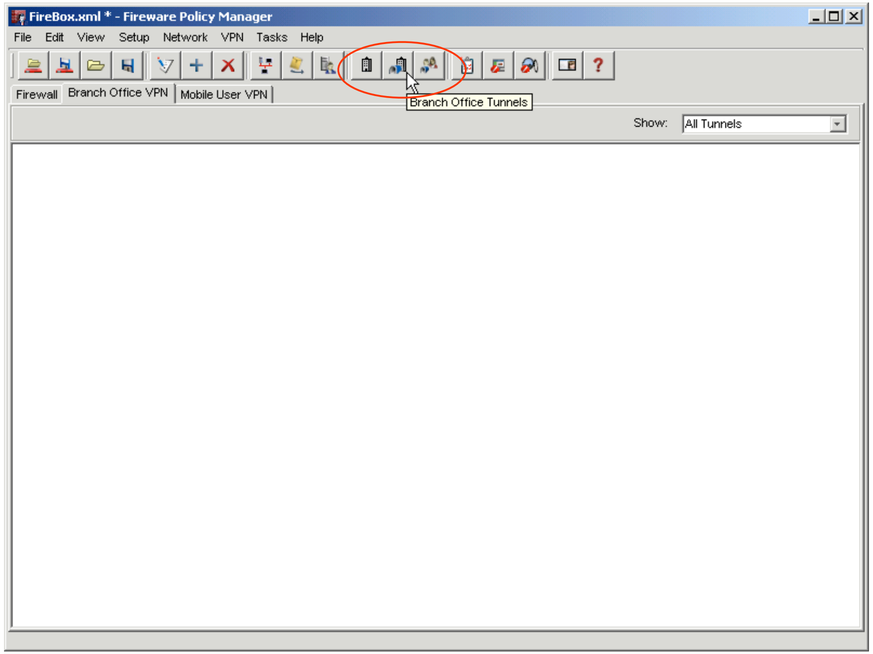
Authentication: SHA1

Encryption: 3DES

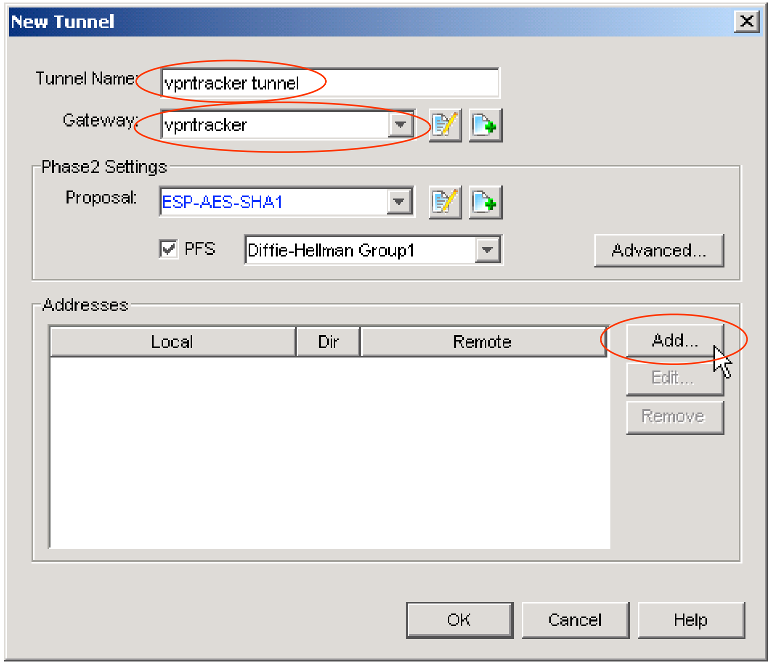
Mode: Main

- *Gateway Name*: Enter an unique name for the VPN gateway (e.g. **vpntracker**).
- *Remote Gateway Settings:*
  - Gateway IP: Select **Any**.
  - *ID Type:* Select **Domain Name** and enter an unique name (e.g **vpntracker**). ❶
- *Local Settings:*
  - *ID Type:* Select the IP address of the untrusted interface from your WatchGuard Firebox.
- *Pre-shared Key:* Enter a secure password for the connection (e.g. **secretkey**). ❷
- Leave the Phase1 Settings untouched.
- Click on Ok, when you're done.

Step 2 - Create a Branch Office Tunnel



- Click on “Branch Office” Tunnels.
- Click on “Add…” in the “Branch Office IPsec Tunnels” interface.



New Tunnel

Tunnel Name: vpntracker tunnel

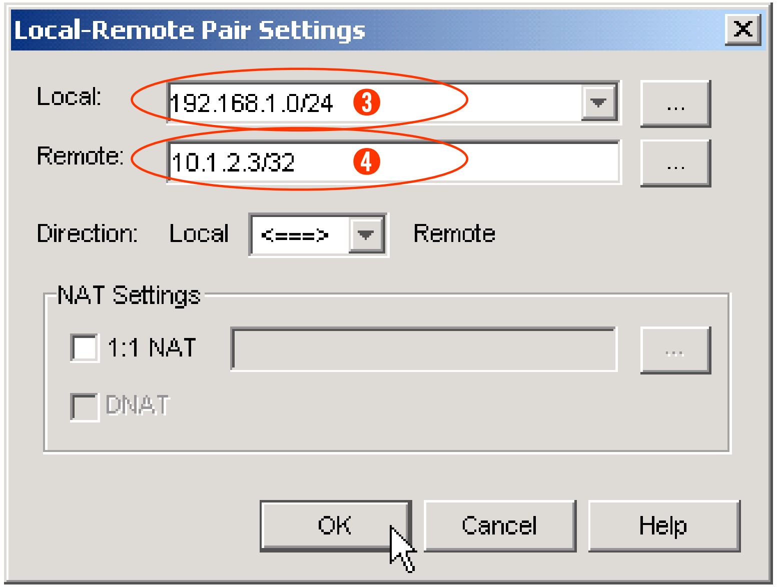
Gateway: vpntracker

Phase2 Settings

Proposal: ESP-AES-SHA1

☑ PFS Diffie-Hellman Group1

- *Tunnel Name:* Enter an unique name for the VPN tunnel (e.g. **vpntracker tunnel**)
- *Gateway:* Select the previously created VPN gateway (**vpntracker**)
- Leave the Phase2 Settings untouched.
- Create a new addresses entry by clicking on “Add…”.



Local-Remote Pair Settings

Local: 192.168.1.0/24 ❸

Remote: 10.1.2.3/32 ❹

Direction: Local <===> Remote

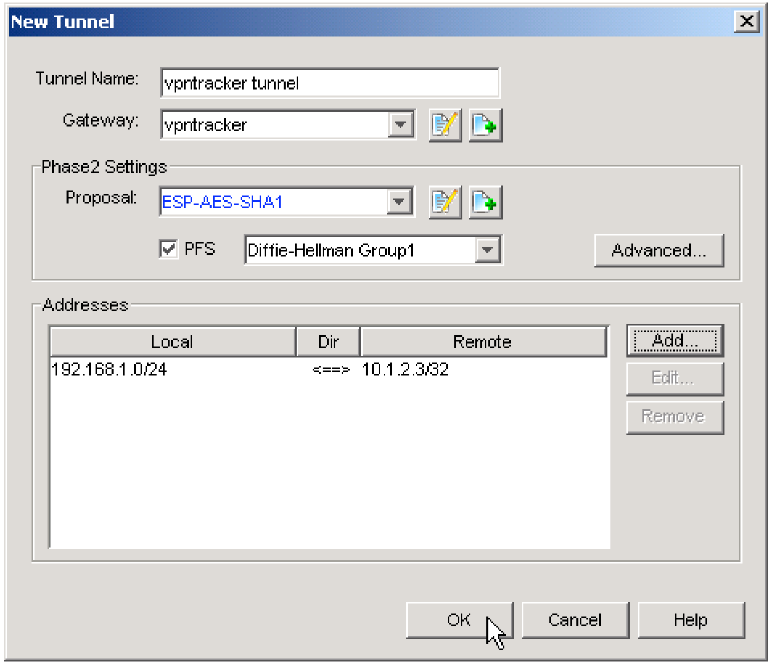
NAT Settings

□ 1:1 NAT

□ DNAT

- *Local:* Enter the network address, which should be reached through the VPN tunnel. (e.g. **192.168.1.0/24**) ❸
- *Remote:* Enter an unique virtual IP address for the VPN Tracker client. (e.g. **10.1.2.3/32**). ❹
- Click on "OK".

TIP The virtual IP address in the remote field must not be within the same range of the local network or the clients real home network. You later need to enter this IP address as "Local Address" in your VPN Tracker configuration.



New Tunnel

Tunnel Name: vpntracker tunnel

Gateway: vpntracker

Phase2 Settings

Proposal: ESP-AES-SHA1

☑ PFS Diffie-Hellman Group1

Addresses

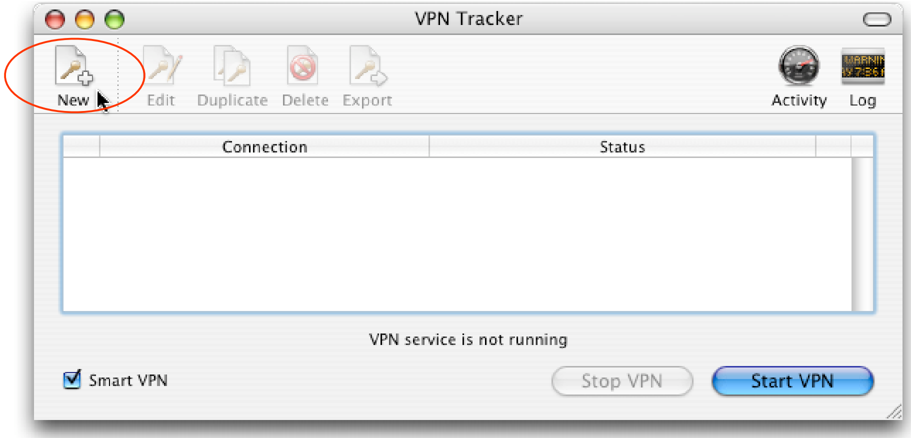
Local	Dir	Remote
192.168.1.0/24	<==>	10.1.2.3/32

- Click on “OK” in the “New Tunnel” dialog.

Task 2 – Configure VPN Tracker

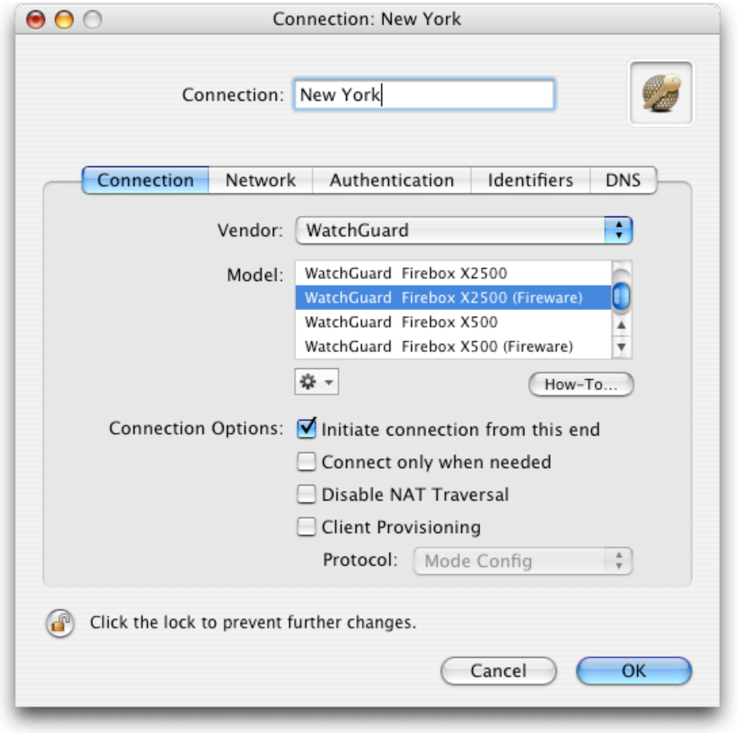
This section describes the configuration of VPN Tracker for your WatchGuard Firebox router.

Step 1 - Create a new Connection



- Click on “New” in the VPN Tracker main window.

Step 2 - Connection Settings



Connection: New York

Vendor: WatchGuard

Model:
- WatchGuard Firebox X2500
- WatchGuard Firebox X2500 (Fireware)
- WatchGuard Firebox X500
- WatchGuard Firebox X500 (Fireware)

Connection Options:
- ☑ Initiate connection from this end
- □ Connect only when needed
- □ Disable NAT Traversal
- □ Client Provisioning

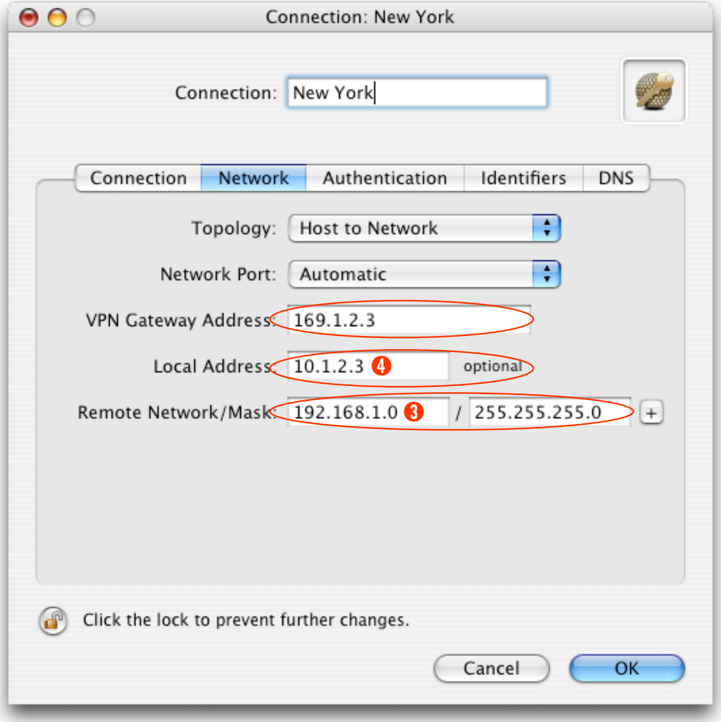
Protocol: Mode Config

Click the lock to prevent further changes.

- *Vendor:* Select the vendor (**WatchGuard)**
- *Model:* Select your VPN router model with (e.g. **WatchGuard Firebox X2500 (Fireware)**)
- Make sure to enable "**Initiate connection from this end**"

TIP The pre-defined VPN Tracker connection for the WatchGuard Firebox is based on the default settings for the WatchGuard Firebox X series with Fireware firmware versions. If you or the administrator changed any of the settings while configuring the device, you might have to adjust the connection type in VPN Tracker by double-clicking on the model.

Step 3 - Network Settings



Connection: New York

Topology: Host to Network

Network Port: Automatic

VPN Gateway Address: 169.1.2.3

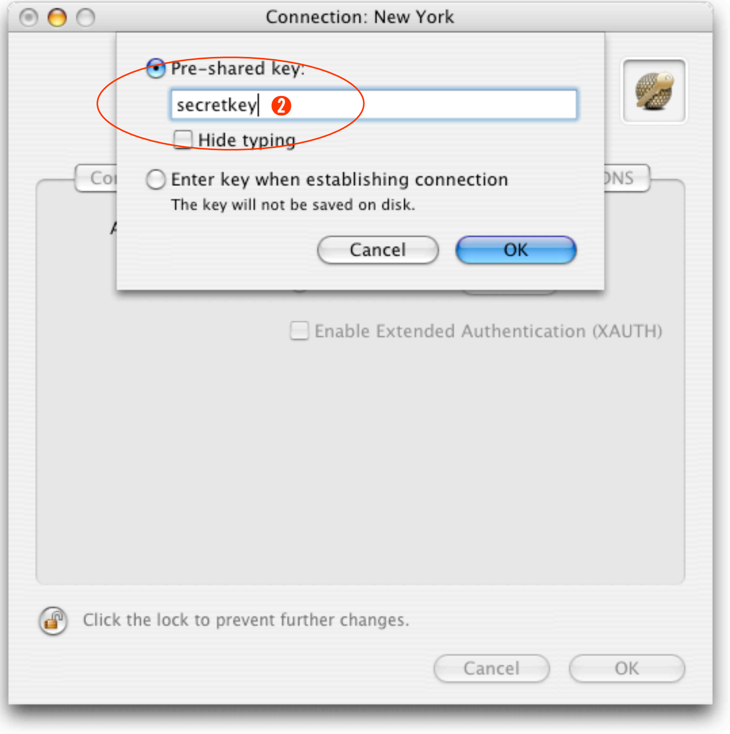
Local Address: 10.1.2.3 ❹ optional

Remote Network/Mask: 192.168.1.0 ❸ / 255.255.255.0

Click the lock to prevent further changes.

- *VPN Server Address*: Enter the public IP address of your VPN Gateway (e.g. **169.1.2.3**)
- *Local Address:* Enter the virtual IP address, you've chosen in your WatchGuard configuration (e.g. **10.1.2.3**). ❹
- *Remote Network/Mask*: Enter the network address and netmask of your office network. ❸

Step 4 - Authentication Settings



Connection: New York

● Pre-shared key:

secretkey ❷

□ Hide typing

○ Enter key when establishing connection

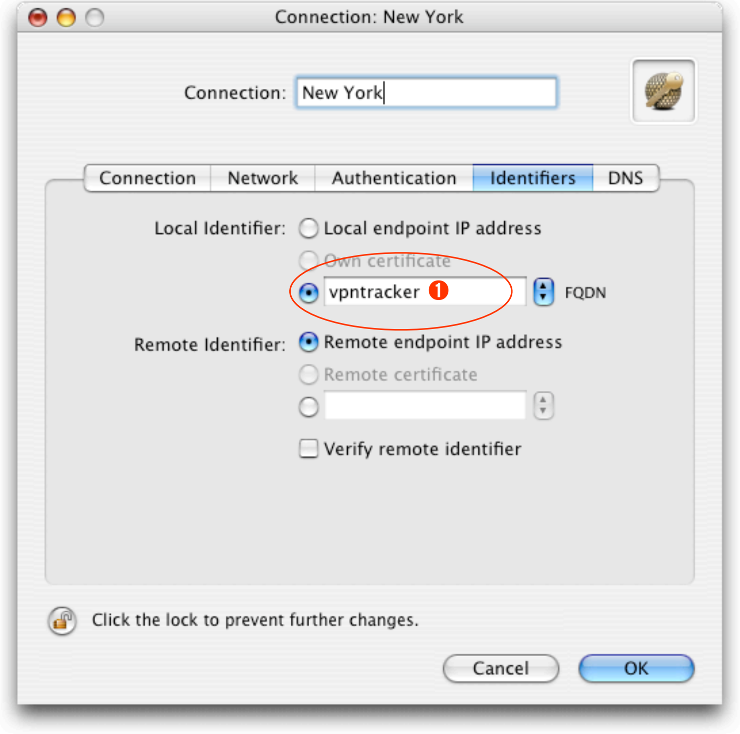
The key will not be saved on disk.

□ Enable Extended Authentication (XAUTH)

Click the lock to prevent further changes.

- *Pre-shared key:* Enter the Pre-shared key you used earlier when configuring the WatchGuard Firebox. ❷

Step 5 - Identifiers Settings



Connection: New York

Local Identifier: ○ Local endpoint IP address
○ Own certificate
● vpntracker ❶ FQDN

Remote Identifier: ● Remote endpoint IP address
○ Remote certificate
○

□ Verify remote identifier

Click the lock to prevent further changes.

- *Local Identifier:* Enter the domain name you used when configuring the WatchGuard Firebox. ❶

Task 3 - Check the VPN connection

This section explains how to start and test your VPN connection.

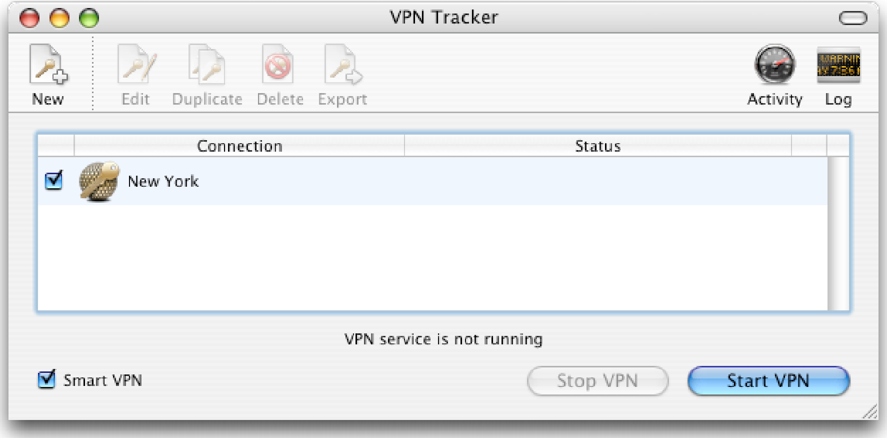
It‘s time to go out!

You will not be able to test and use your VPN connection from within your office network. In order to test your connection, you'll need to connect from a different location. That’s why it’s now time to go out. Take your MacBook Pro and have a coffee at your favorite Internet cafe or go visit a friend.

Test your connection

To test if everything is setup correctly please follow the steps below:

- Get access to the Internet
- Make sure the Internet connection is working; open your Internet browser and try to connect to http://www.equinux.com
- Start VPN Tracker if it’s not already running

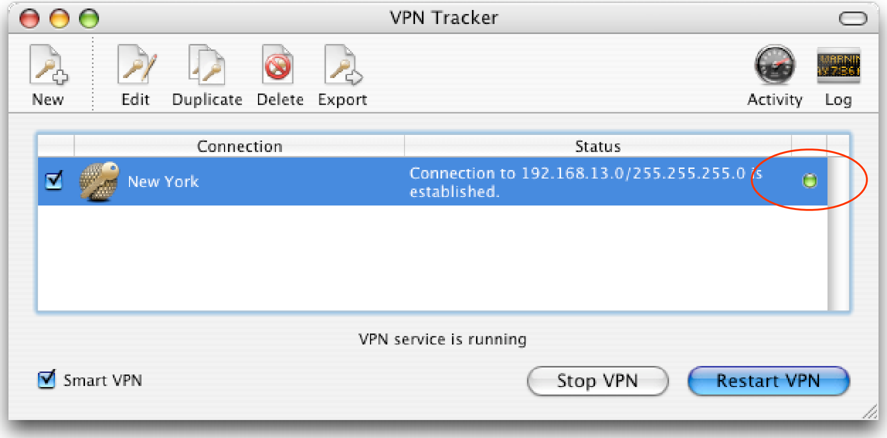

VPN Tracker

	Connection	Status
☑	New York	

VPN service is not running

☑ Smart VPN

- Select the connection you configured for your WatchGuard Firebox device
- Hit the **Start VPN** button


VPN Tracker

	Connection	Status
☑	New York	Connection to 192.168.13.0/255.255.255.0 is established. ●

VPN service is running

☑ Smart VPN

- If the light turns red after a few seconds, then please read the **Troubleshooting** section on the next page
- If the light turns green, that means you've successfully established a connection

Congratulations! You did it!

Troubleshooting

I don’t get a green light in the VPN Tracker main window

- Make sure that your computer is not connected directly to the office network you want to connect to.
- Make sure, that the **Identifier** and the **Pre-shared key** you've entered in the router configuration match the settings you entered in VPN Tracker.
- Verify that the **public IP address** you entered in VPN Tracker matches the public IP address of your router.
- Download our sample configuration and connect to our test device at http://www.vpntracker.com/connectiontest/
  - If the test connection cannot be established: Make sure, that the internet connection is working and verify that your local router is not blocking any connection attempts.
  - If the test connection is established successfully: Your internet connection is working and does not block VPN connections. Please check the log file of your WatchGuard Firebox for error messages.
- If you’re still having issues with your connection, please create some screenshots of your settings on both ends, gather the log files and send them over to our support team via http://www.equinux.com/us/products/vpntracker/contactus.html.

What’s next?

This section explains how to use your VPN connection.

Introduction

As the VPN connection has now been established, you should be able to access most of the resources in your office network.

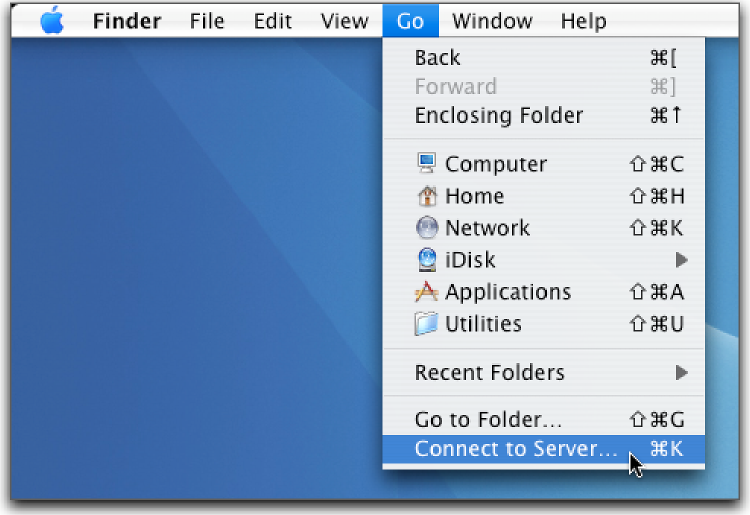
Known Limitations

There are some limitations of a VPN connection compared to a direct connection to a office network.

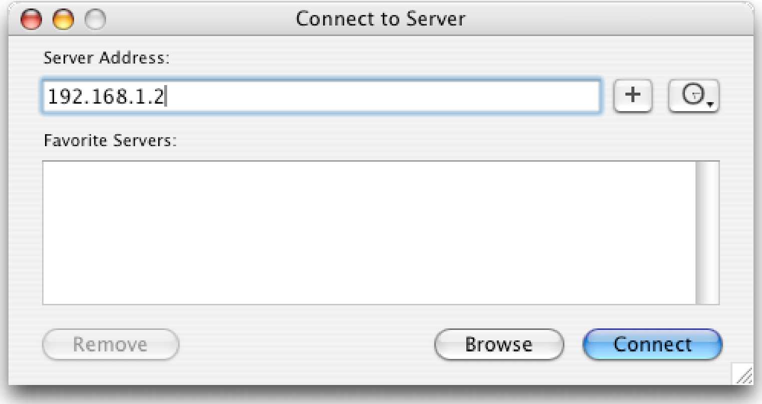
- **Bonjour**: As Bonjour Chat is not supported over a VPN tunnel, you’ll need to use iChat server in order to chat remotely.
- **Browsing the network**: You can’t “browse” the remote network as you’re normally used to. You need to connect to each machine manually, as described on the next page.

Accessing Files

To access files in your office network, just follow the steps below:



- Go to the **Finder** application
- In the menu bar, click on **Go->Connect To Server...**



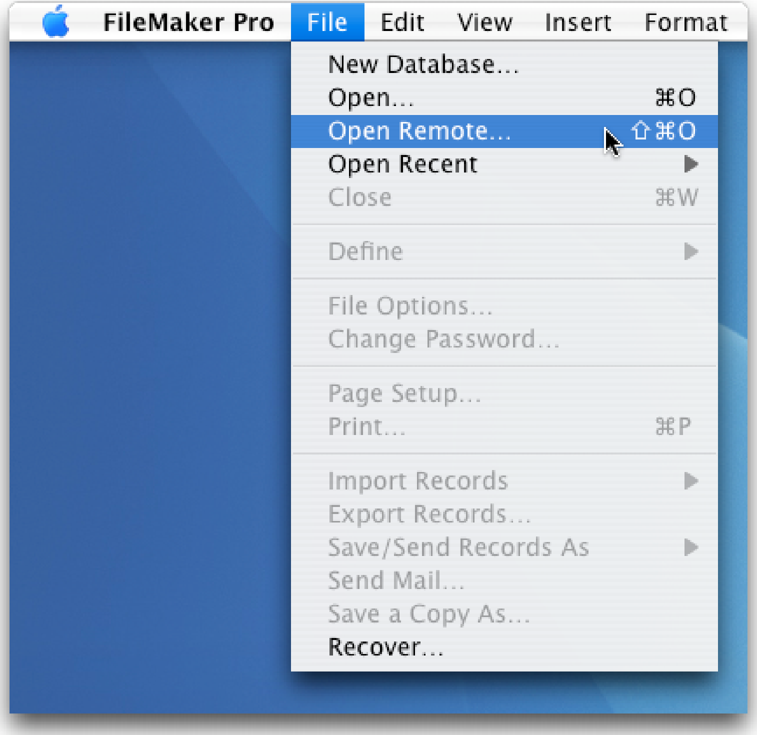
Server Address: 192.168.1.2

- Enter the IP address of the machine you want to connect to. In our example network this would be the IP address **192.168.1.2**
- Click on the **Connect** button
- Enter your **Username** and **Password** to access the files

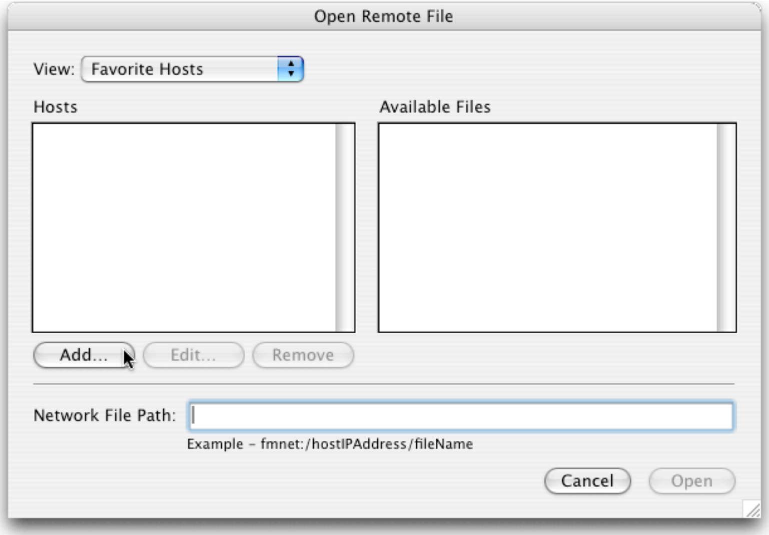
TIP When connecting to a Windows fileserver, you'll need to prefix the IP address with "*smb://*", e.g. "*smb://192.168.1.2*".

Accessing a FileMaker Database

To access a database available in your office network, just follow the steps below:



- Start the **FileMaker** application
- In the menu bar, click on **File->Open Remote...**



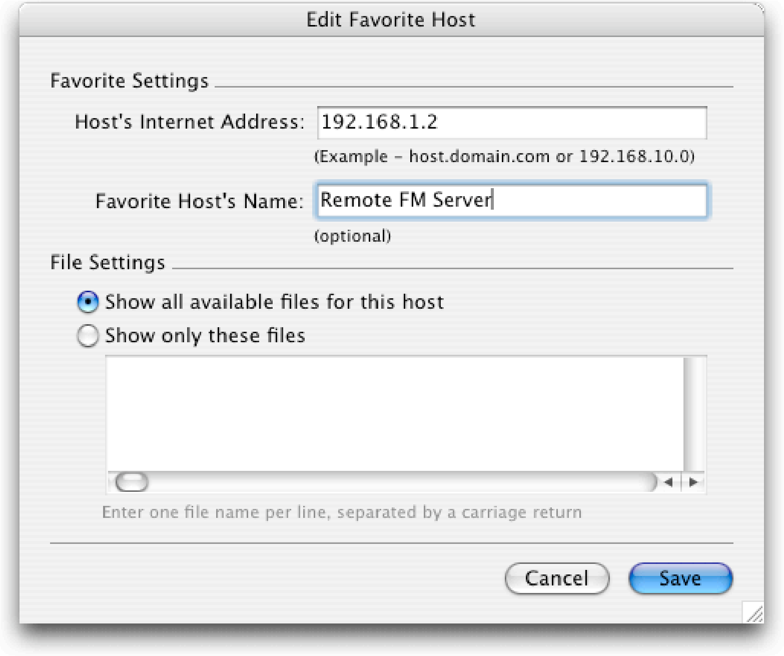
Open Remote File

View: Favorite Hosts

Network File Path:

Example – fmnet:/hostIPAddress/fileName

- Click on the **Add...** button



Edit Favorite Host

Favorite Settings

Host's Internet Address: 192.168.1.2

(Example – host.domain.com or 192.168.10.0)

Favorite Host's Name: Remote FM Server

(optional)

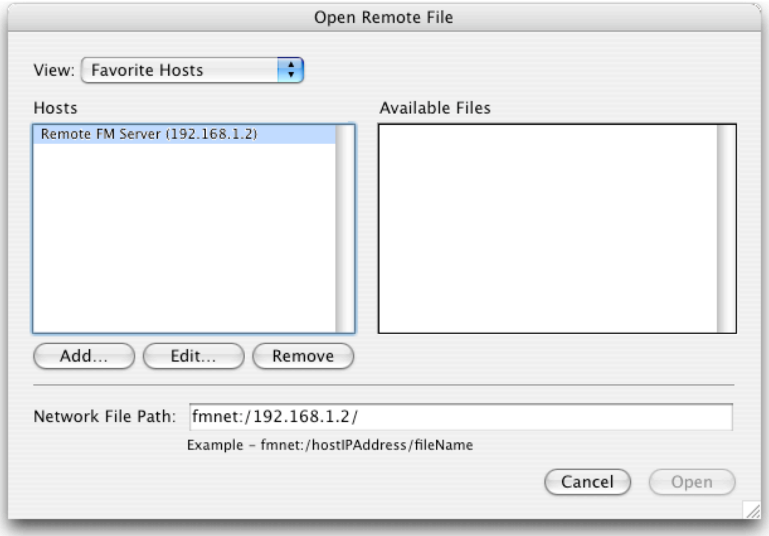
File Settings

● Show all available files for this host

○ Show only these files

Enter one file name per line, separated by a carriage return

- Enter the **IP address** of the FileMaker server machine
- Enter a hostname for this machine (optional)
- Click on the **Save** button



View: Favorite Hosts

Remote FM Server (192.168.1.2)

Network File Path: fmnet:/192.168.1.2/

Example – fmnet:/hostIPAddress/fileName

- Select a database from the list of **Available Files** and click **Open**
- You are now able to access your FileMaker databases as usual

Acquire more Licenses

If two or more people need to access your office network via VPN, then you need to acquire more VPN Tracker licenses.

To get more licenses, please contact your reseller and inquire about „VPN Tracker Personal Edition“.

Or point your browser to http://store.equinux.com and buy additional VPN Tracker Personal Edition Licenses online.