VPN Tracker for Mac OS X

How-to:

Interoperability with

Fortinet FortiGate

Internet Security Appliances

Rev. 4.0

1. Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a Fortinet FortiGate Internet Security Appliance.

The Fortinet FortiGate 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 Fortinet FortiGate. Please be sure to read those instructions and understand them before starting.

2. Prerequisites

First you have to make sure that your Fortinet FortiGate has VPN support built in. Please refer to your Fortinet FortiGate manual for details.

Furthermore you should use a recent Fortinet FortiGate fimware version. The latest firmware release for your Fortinet FortiGate appliance can be obtained from

http://www.Fortinet.com/

For this document, firmware version 2.80 has been used.

When using Pre-shared key authentication you need one VPN Tracker Personal Edition license for each Mac connecting to the Fortinet FortiGate.

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 10.2.5+, 10.3 and 10.4.

3. Connecting a VPN Tracker host to a Fortinet FortiGate using Extended Authentication

In this example the Mac running VPN Tracker is directly connected to the Internet via a dialup or PPP connection.

The Fortinet FortiGate 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 Fortinet FortiGate use 192.168.1.1 as their default gateway and should have a working Internet connection.

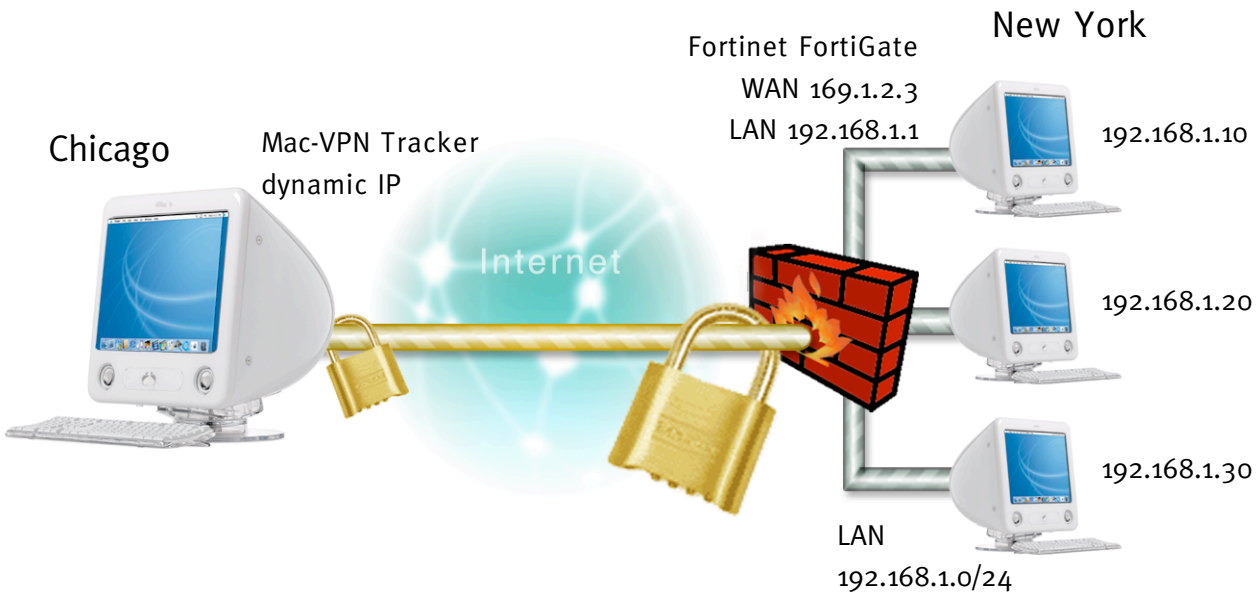

Figure 1: VPN Tracker – Fortinet FortiGate connection diagram

3.1 Fortinet FortiGate Configuration

The pre-defined VPN Tracker connection type has been created using the default settings for your Fortinet FortiGate appliance. If you change any of the settings on the Fortinet FortiGate, you will eventually have to adjust the connection type in VPN Tracker.

Step 1 Create a new User:

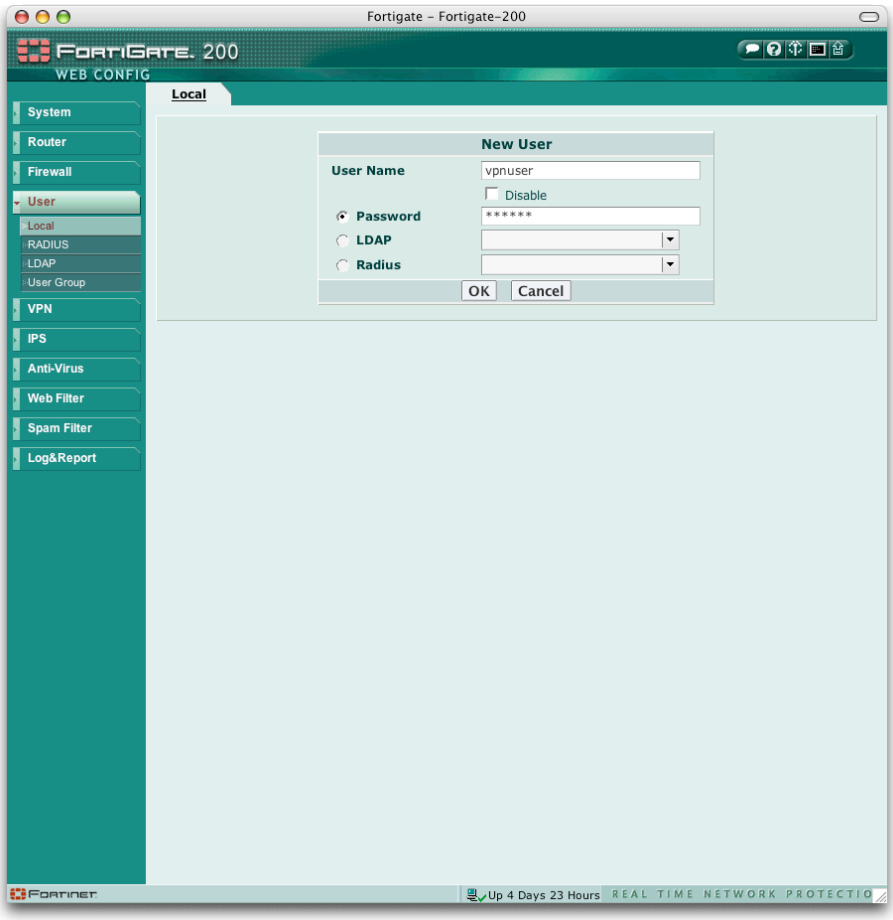

Figure 2: FortiGate - New user

Step 2

Add user to group:

Add the previously created user to your remote access user group.

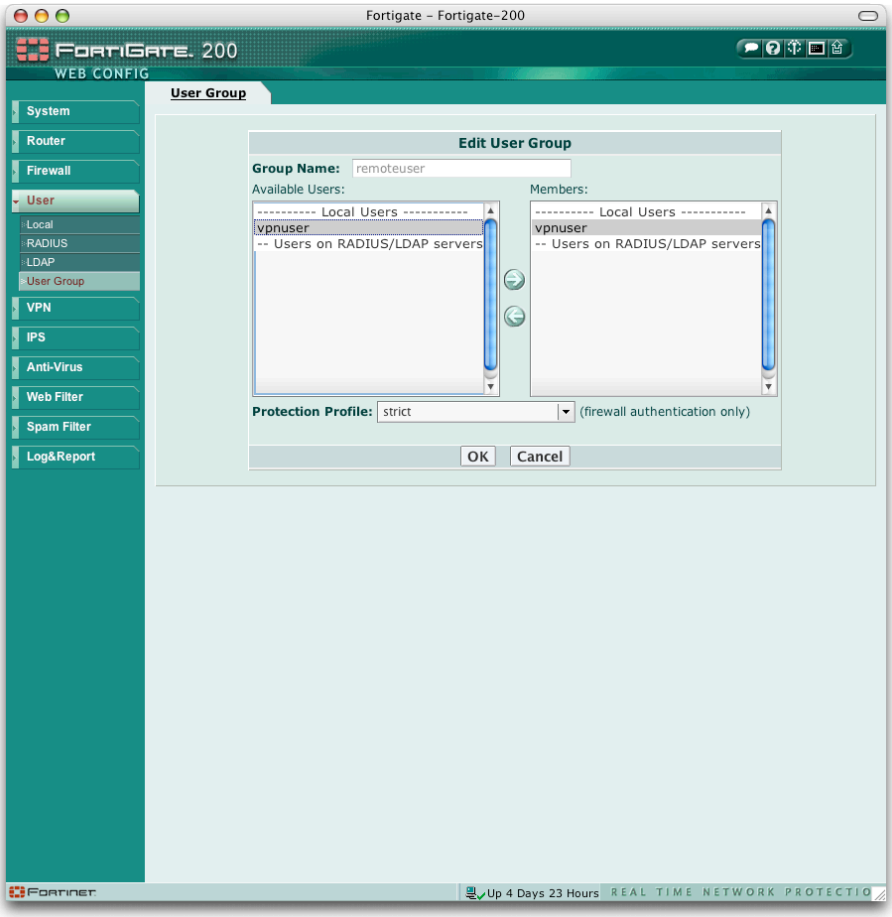

Figure 3: FortiGate - Edit User Group

Step 3

Create a new VPN Gateway:

- Gateway Name: an arbritary name (e.g. **vpntracker**)
- Remote Gateway: **Dialup User**
- Mode: **Aggressive**
- Pre-shared key: your Pre-shared key
- Xauth: **Enable as Server**
- User Group: your remote access user group (e.g. **remoteuser**)

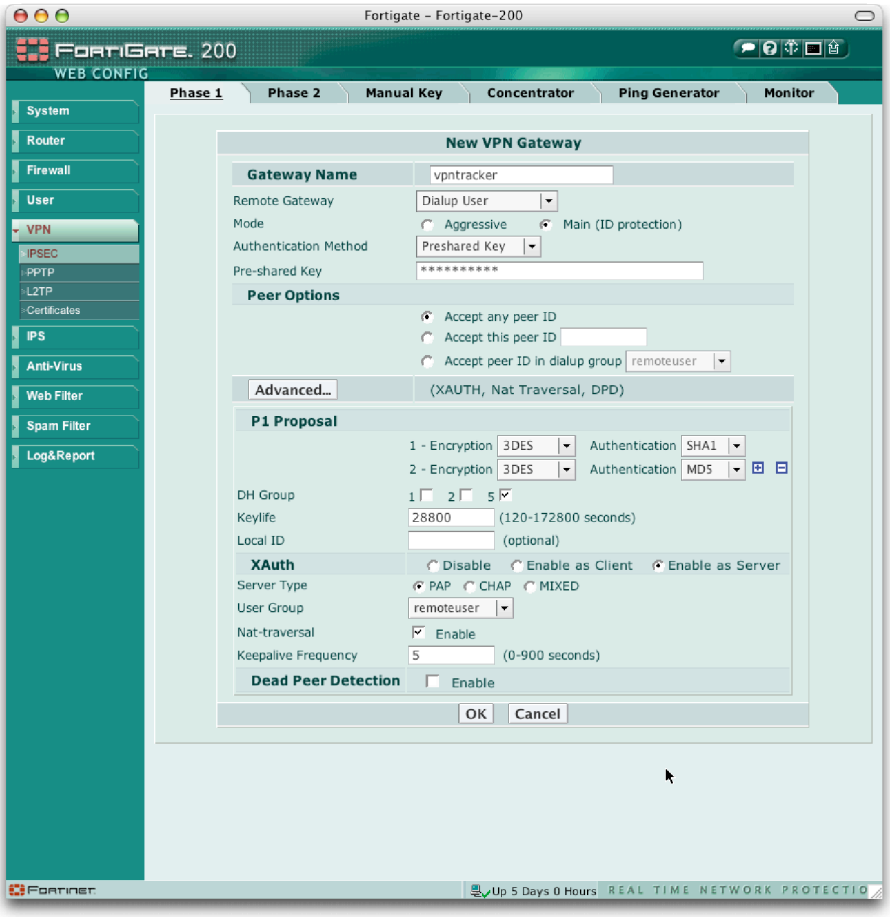

Figure 4: FortiGate - Add VPN Gateway

Step 4

Create a new VPN Tunnel:

- Tunnel Name: an arbriatary name (e.g. **vpntracker tunnel**)
- Remote Gateway: select the previously created gateway here

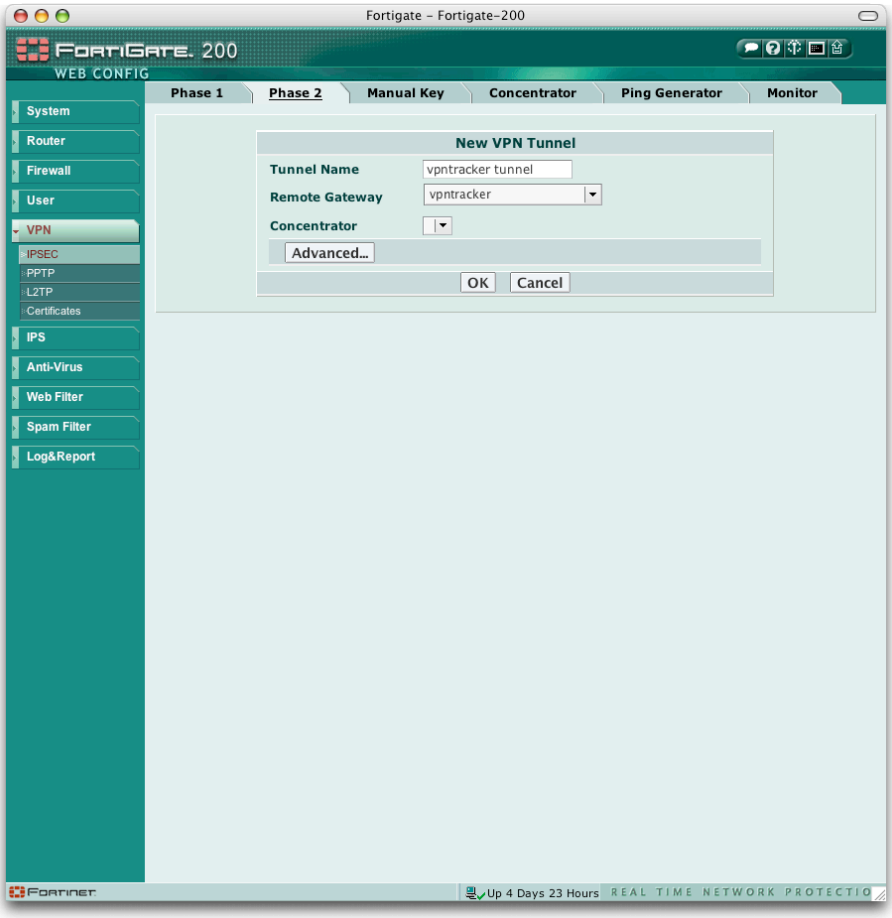

Figure 5: FortiGate - New VPN Tunnel

Step 5 (optional)

Please note: This step is only needed if a LAN address object does not exist.

Create an Address Object:

- Address Name: an arbitrary name (e.g. **LAN**)
- IP Range/Subnet: the network you want to access through your VPN tunnel (e.g. **192.168.1.0/24**)

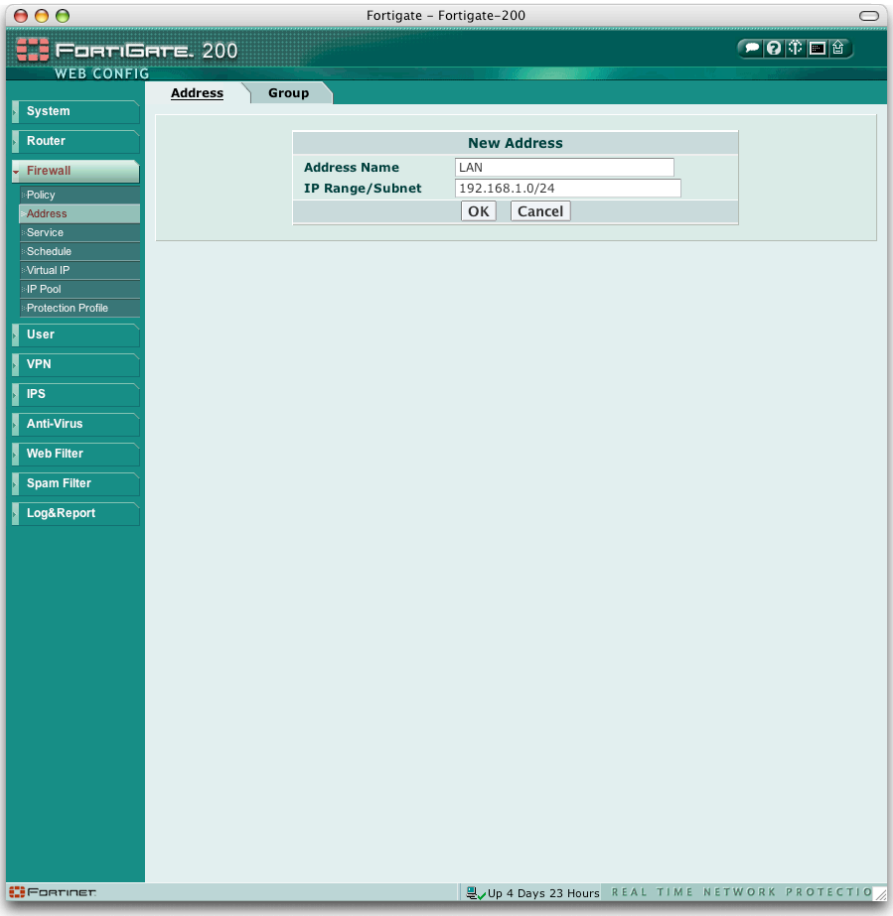

Figure 6: FortiGate - New Address

Step 6

Create a new Firewall Policy:

- Address Name Source: the local LAN address object (e.g. **LAN**)
- Address Name Destination: **all**
- Action: **ENCRYPT**

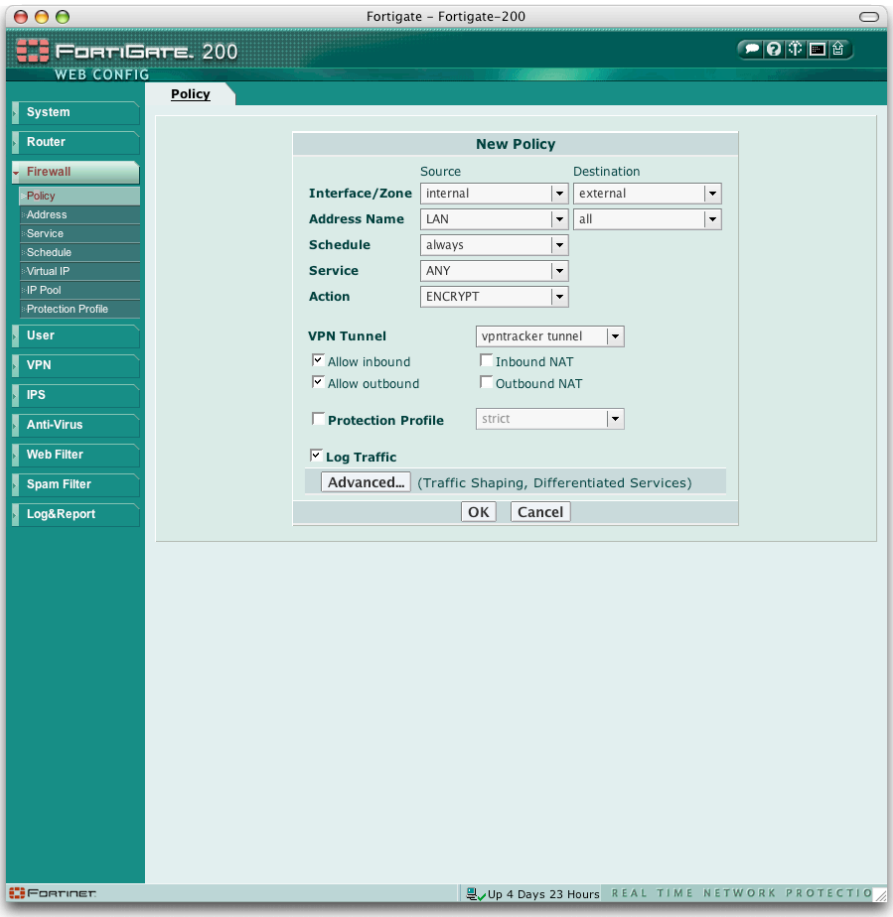

Figure 7: FortiGate - New Policy

Please note: VPN Tunnel Policies always direct from the "internal" to the "external" Zone.

3.2 VPN Tracker Configuration

Step 1

Add a new connection with the following options:

- Vendor: **Fortinet**
- Model: your VPN device

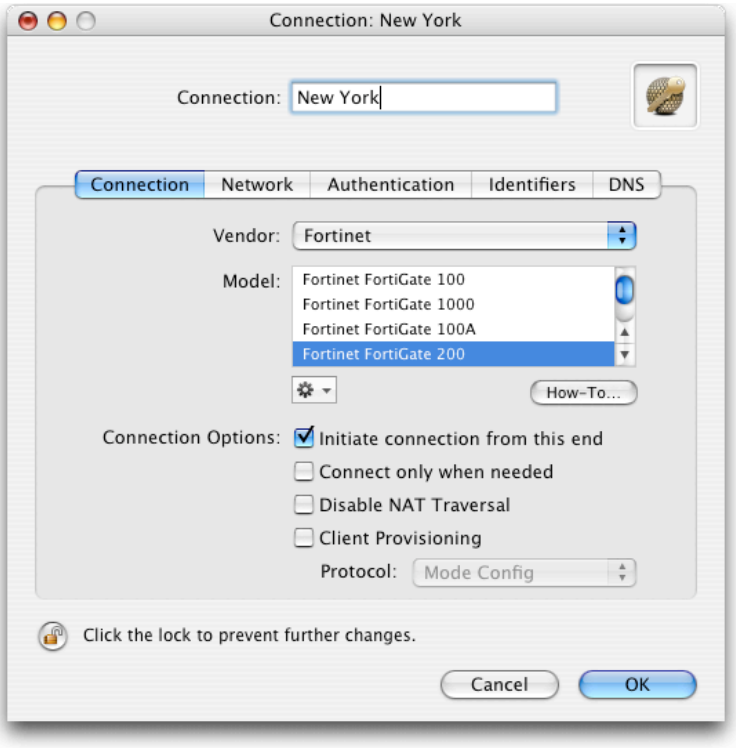

Figure 8: VPN Tracker - Connection Settings

Step 2 Change your Network Settings:

- VPN Server Address: public IP address of your VPN Gateway (e.g. **169.1.2.3**)
- Remote Network/Mask: network address and netmask of the remote network (eg. **192.168.1.0/255.255.255.0**).

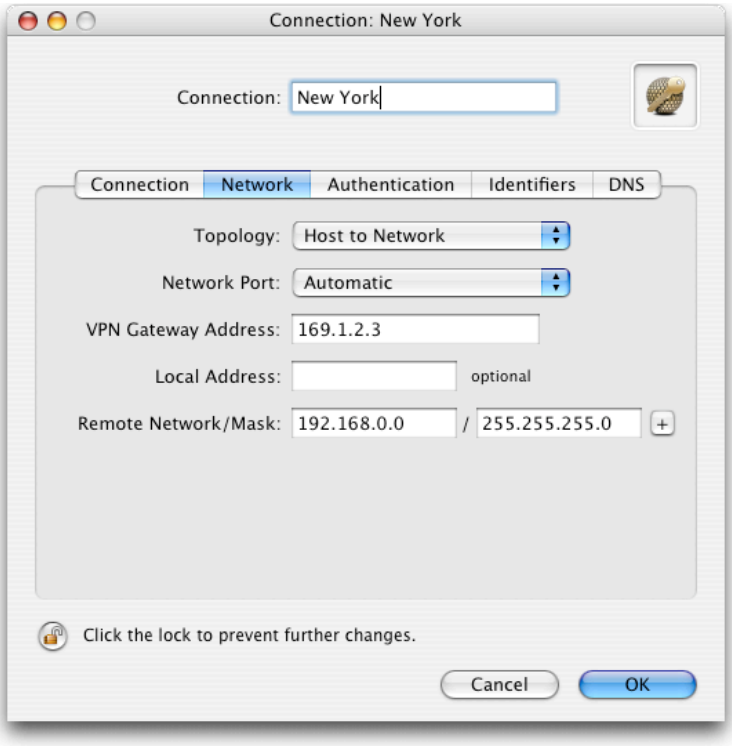

Figure 9: VPN Tracker - Network Settings

Please note: In order to access multiple remote networks simultaneously, just add them by pressing the Plus-button.[1]

[1] For this step VPN Tracker Professional Edition is needed.

Step 3

Change your Authentication Settings:

- Pre-shared key: the same Pre-shared key as in the Fortinet FortiGate configuration.
- Enable Extended Authentication (XAUTH): **checked**

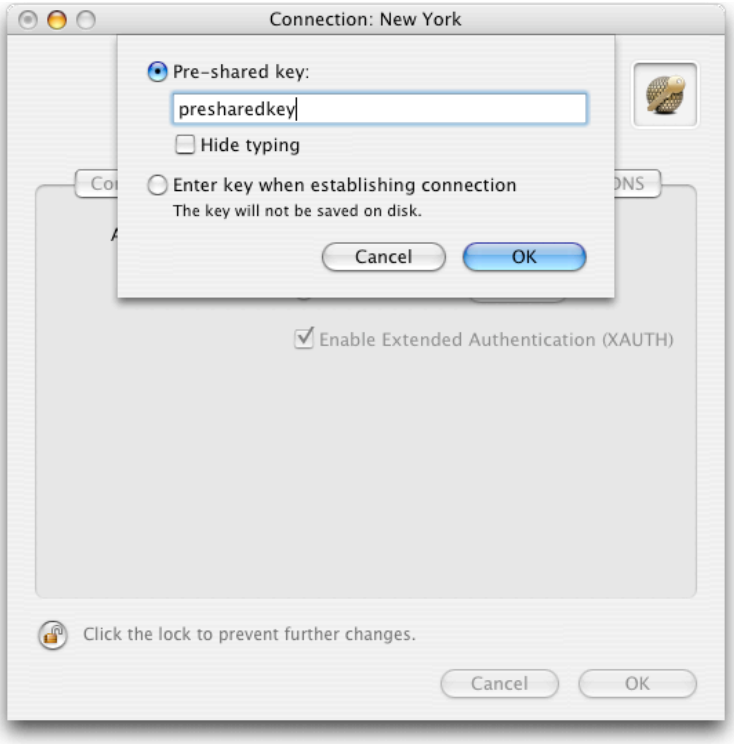

Figure 10: VPN Tracker - Authentication Settings

Step 4

Identifier Settings:

- Local Identifier: **Local endpoint IP address.**
- Remote Identifier: **Remote endpoint IP address.**

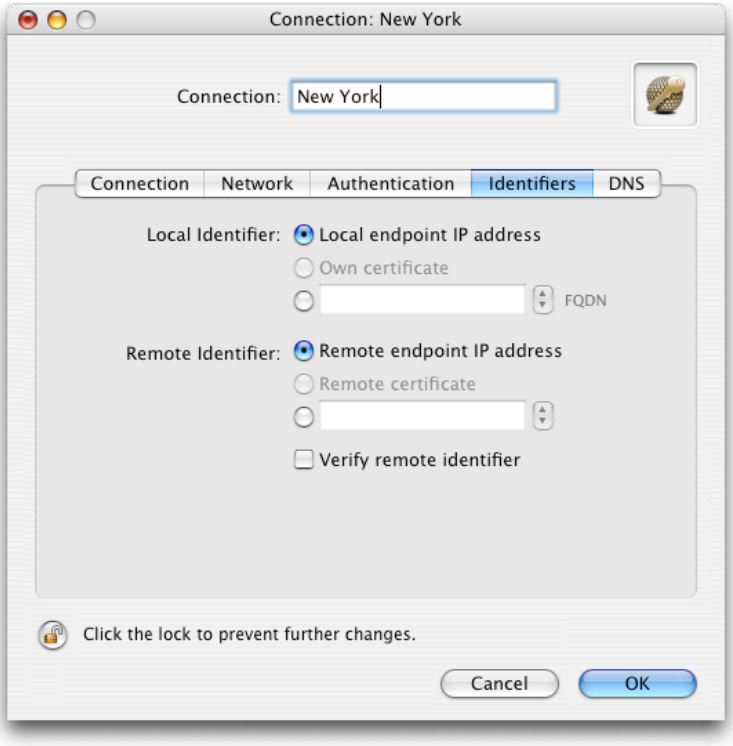

Figure 11: VPN Tracker - Identifiers Settings

Step 5

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 Fortinet FortiGate. After IPsec has been started, you may quit VPN Tracker. The IPsec service will keep running.

Now to test your connection simply ping a host in the Fortinet FortiGate network from the dialed-in Mac in the “Terminal” utility:

```
ping 192.168.1.10
```

> Troubleshooting

For further debug output, please run following commands in the Fortinet command line interface:

```
# diag debug enable
# diag debug application ike 3
```

The previous commands enable verbose debug output to the Fortinet command line.

You can change the VPN Tracker log verbosity in the preferences menu.