VPN Tracker for Mac OS X

How-to:

Interoperability with

NETASQ

Internet Security Appliances

Rev. 3.0

1. Introduction

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

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

2. Prerequisites

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

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

https://www.netasq.com/

For this document, NS-BSD version 5.0.10 has been used.

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

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

3. Connecting a VPN Tracker host to a NETASQ using Pre-shared Key Authentication

In this example the Mac running VPN Tracker is directly connected to the Internet via a dialup or PPP connection.[1]

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

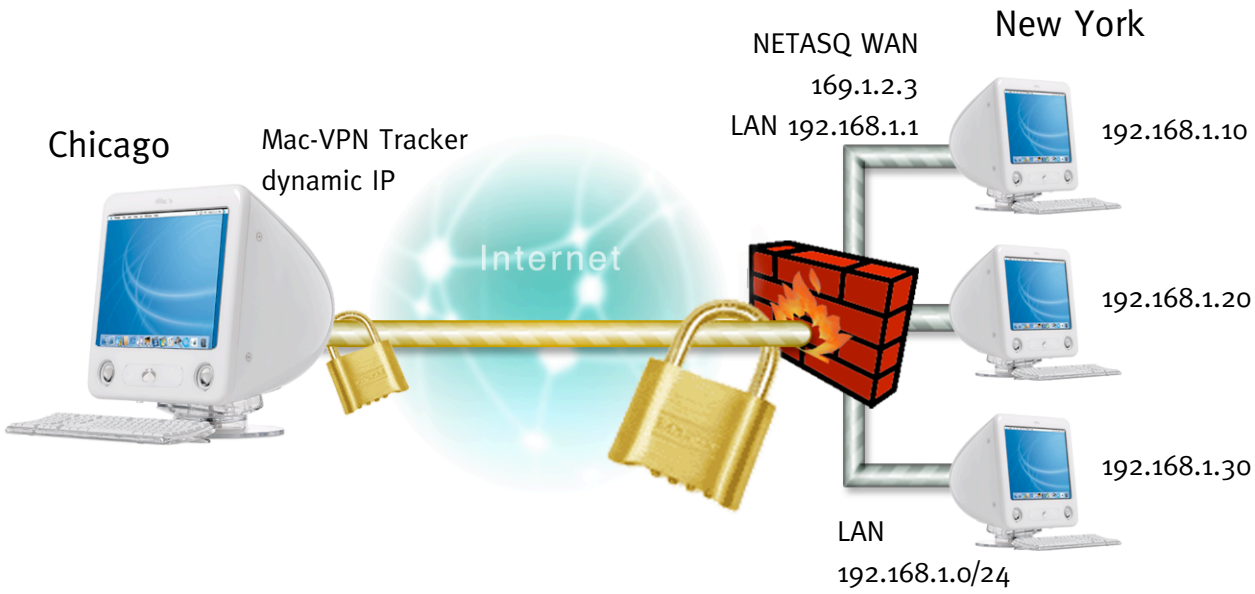

Figure 1: VPN Tracker – NETASQ connection diagram

[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.

3.1 NETASQ Configuration

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

In Firewall Manager please go to [Configuration -› VPN -› IPsec Tunnels] and edit an empty slot:

Step 1 Enter an arbitrary name for the VPN tunnel.SEQ

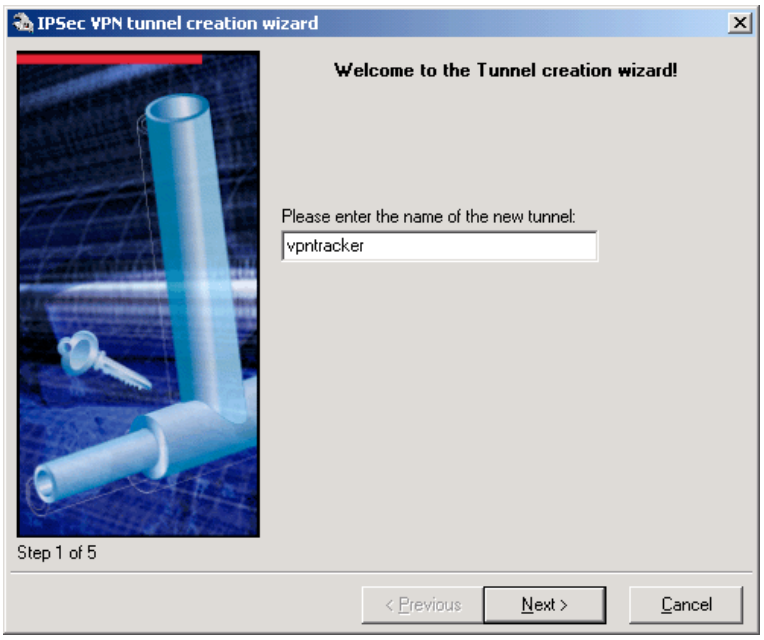

Figure 3: NETASQ - VPN Wizard - Step 1

Step 2 Check Advanced mode.

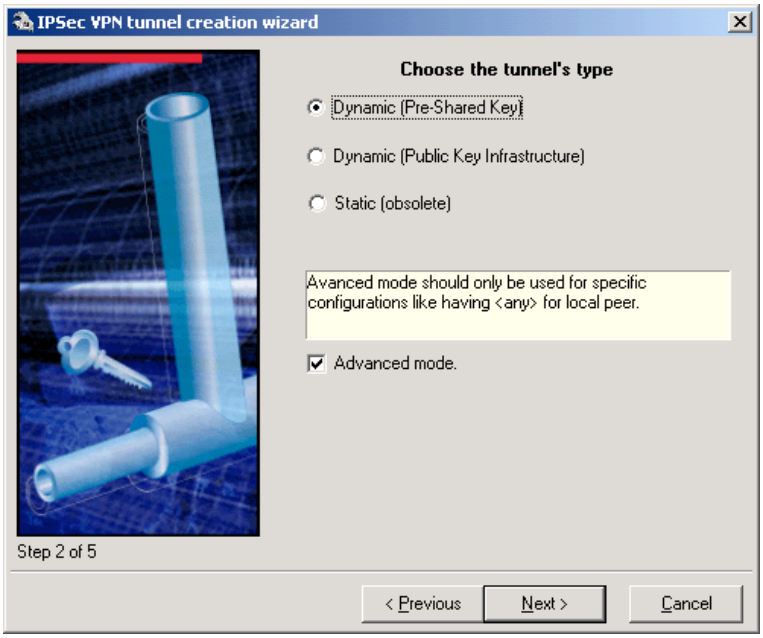

Figure 4: NETASQ - VPN Wizard - Step 2

Step 3 Adjust the Tunnel Endpoints:

- Local IPS-Firewall interface: **Firewall_bridge**
- Peer IP address: **any**

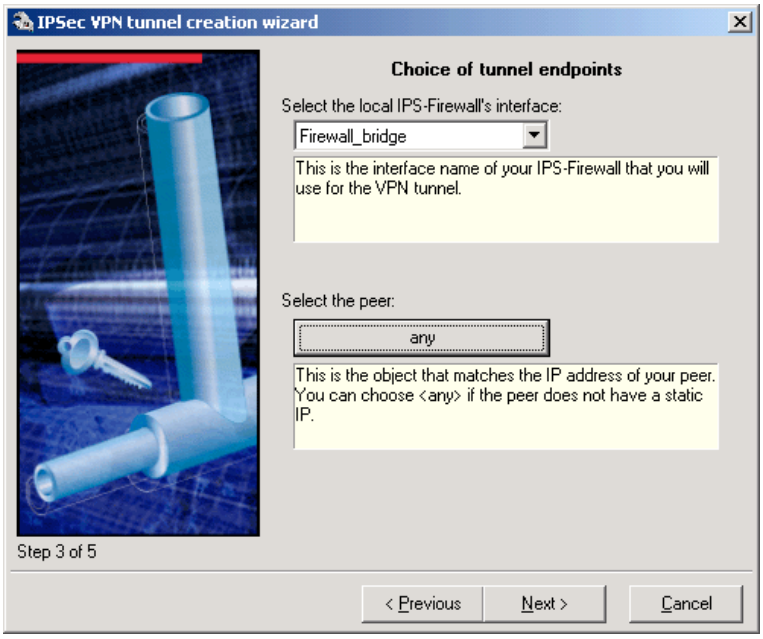

Figure 6: NETASQ - VPN Wizard - Step 3

Step 4 Adjust the Traffic endpoints:

- Local host at traffic end point: **Network_bridge**
- Remote host at traffic end point: **any**

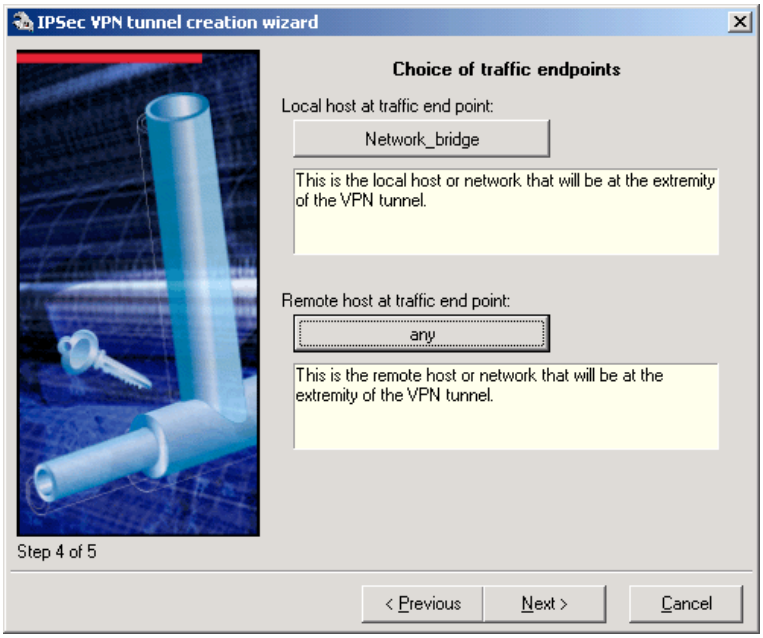

Figure 8: NETASQ - VPN Wizard - Step 4

Step 5 Adjust your IPSec VPN Tunnel configuration:

- Phase 1 negotiation mode: **Aggressive mode**
- Identity type: **IP Address**
- Identity: the public IP address of your NETASQ gateway

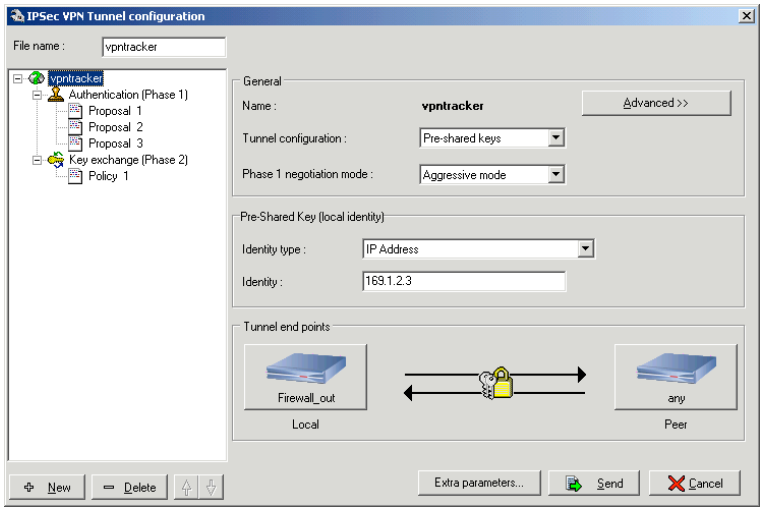

Figure 11: NETASQ - IPSec Tunnel Configuration

Step 6 Create a new Pre-shared key for this this identity:

- Type: **user@fqdn(E-mail)**
- Peer Identity: a e-mail address (e.g. **vpntracker@equinux.com**)
- Share key: your Pre-shared key

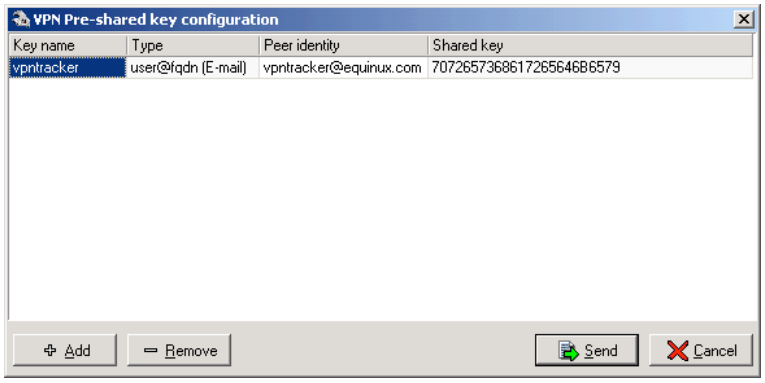

Figure 12: NETASQ - Pre-shared key configuration

Finally, send your configuration and activate the previously created tunnel.

3.2 VPN Tracker Configuration

Step 1 Add a new connection with the following options:

- Vendor: **„NETASQ“**
- Model: your VPN device

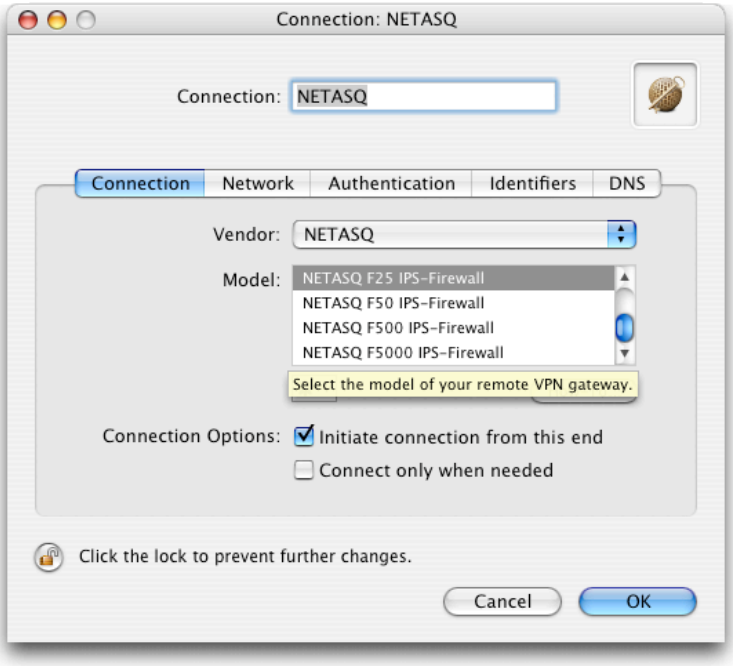

Figure 16: VPN Tracker - Connection settings

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**).

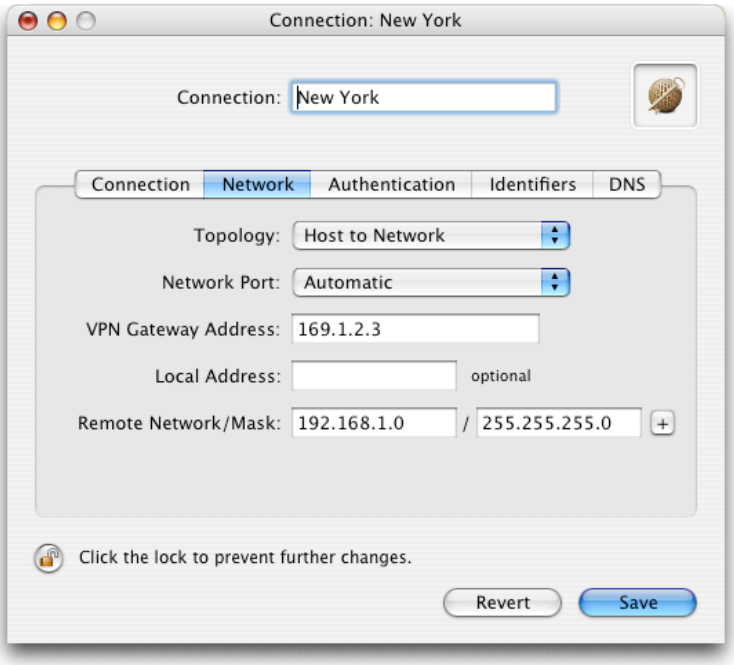

Figure 17: VPN Tracker – Network settings

Please note: In order to access multiple remote networks simultaneously, just add them by pressing the Plus-button.[2]

[2] 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 NETASQ configuration.

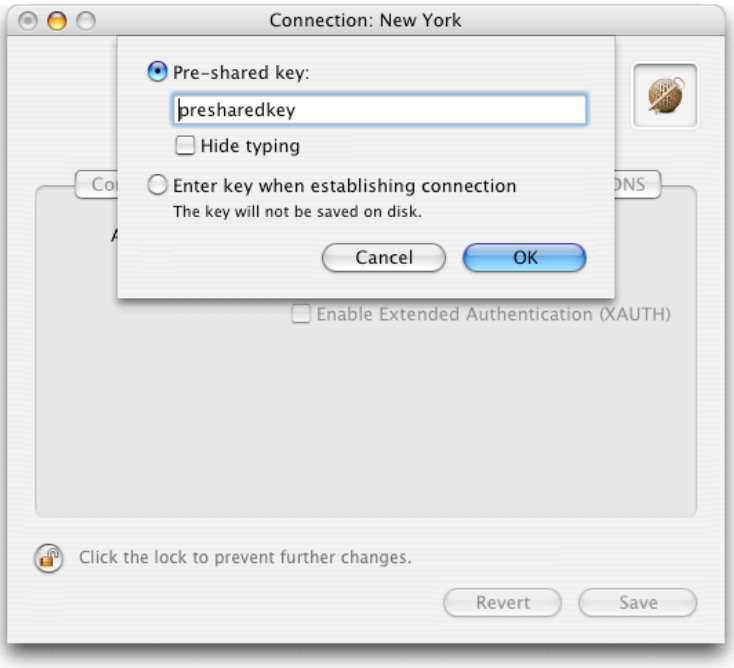

Figure 18: VPN Tracker - Authentication settings

Step 4 Identifier Settings:

- Local Identifier: E-mail address (e.g. **vpntracker@equinux.com**).
- Remote Identifier: Remote endpoint IP address.

Figure 19: VPN Tracker - Identifier 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 NETASQ. 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 NETASQ network from the dialed-in Mac in the “Terminal” utility:

```
ping 192.168.1.10
```