VPN Tracker for Mac OS X

How-to:

Interoperability

With

Netopia Cayman Routers

Rev. 1.0

1. Introduction

This document describes how VPN Tracker can be used to establish a secure connection between a Macintosh running Mac OS X and Netopia Cayman appliances.

The Gateway is configured as a router/firewall 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 Netopia Cayman appliance. Please be sure to read those instructions and understand them before starting.

2. Prerequisites

Please make sure, that your Netopia Cayman appliance has VPN support built-in. Some models come with built-in VPN Support, others have to be upgraded for VPN functionality. Please refer to the Netopia manual for details. For this document, the Netopia Cayman 3386-ENT has been used.

Furthermore you should use a recent Netopia Cayman firmware version.

On the Mac side you need one VPN Tracker Personal license for each Mac connecting to the Netopia Cayman. VPN Tracker is compatible with Mac OS X 10.2 or greater.

3. Connecting a VPN Tracker host to a Netopia Cayman Router

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

The Netopia Cayman 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 VPN Gateway use 192.168.1.1 as their default gateway and should have a working Internet connection.

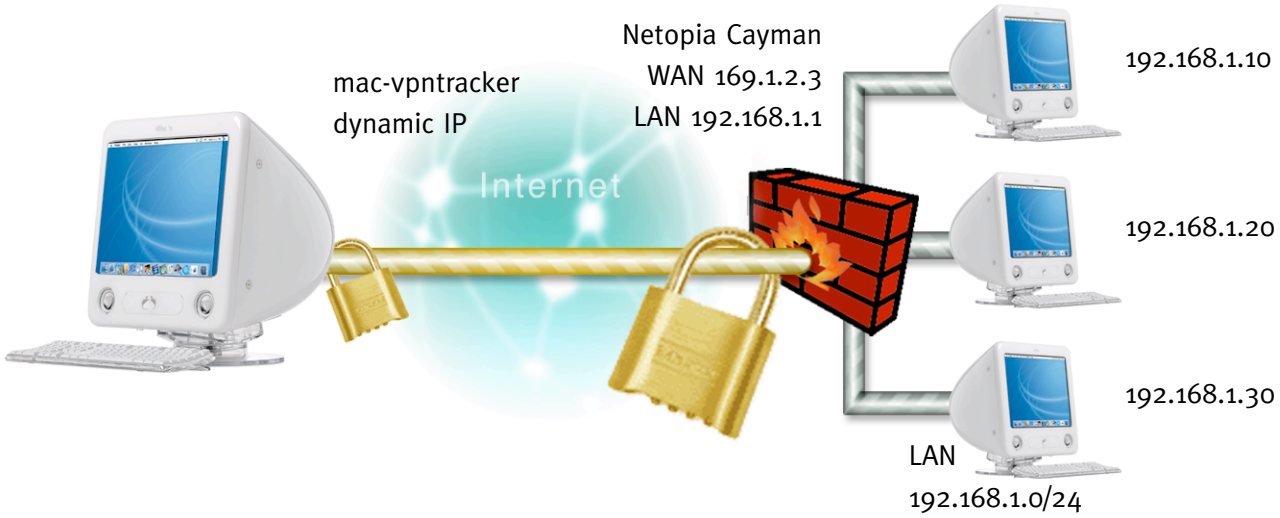

Figure 1: VPN Tracker – Netopia Cayman connection diagram

[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 Netopia Cayman Configuration

The Netopia router should be connected to the Internet and the Hosts behind the appliance should use the Netopia router as their default gateway.[2]

Step 1 Add a new Connection Profile (WAN Configuration › Add Connection Profile). Enter a "Profile Name" of your choice and select IPsec as "Encapsulation Type".

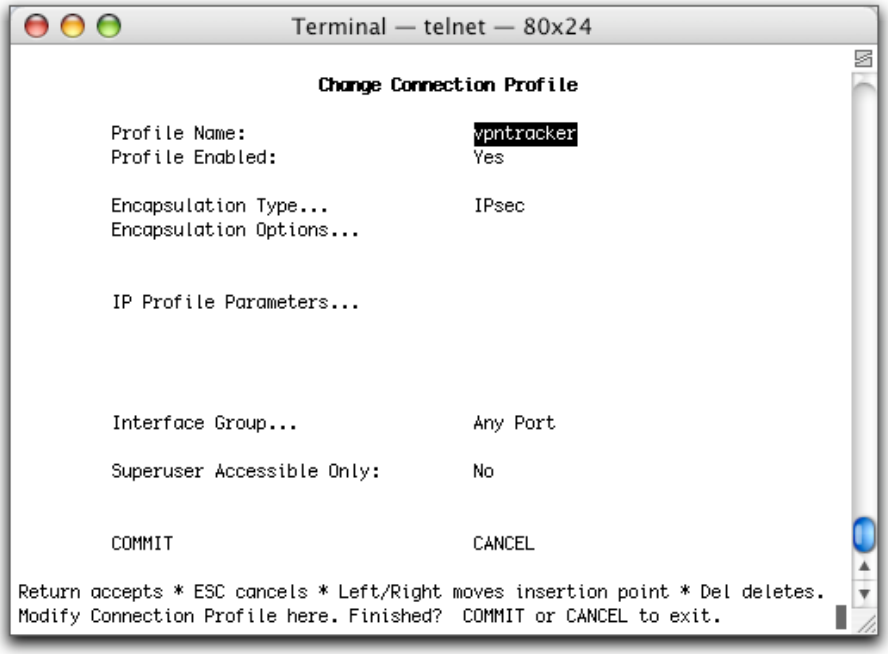

Figure 2: Netopia - Connection Profile Dialog

[2] Administration of Netopia Cayman routers is done by opening a telnet connection with your favorite telnet client (e.g. with Mac OS X's built-in Terminal application).

Step 2 Select “Encapsulation Option” and change the “ESP Encryption Transform…” to “3DES” and the “ESP Authentication Transform…” to “HMAC-SHA1-96”.

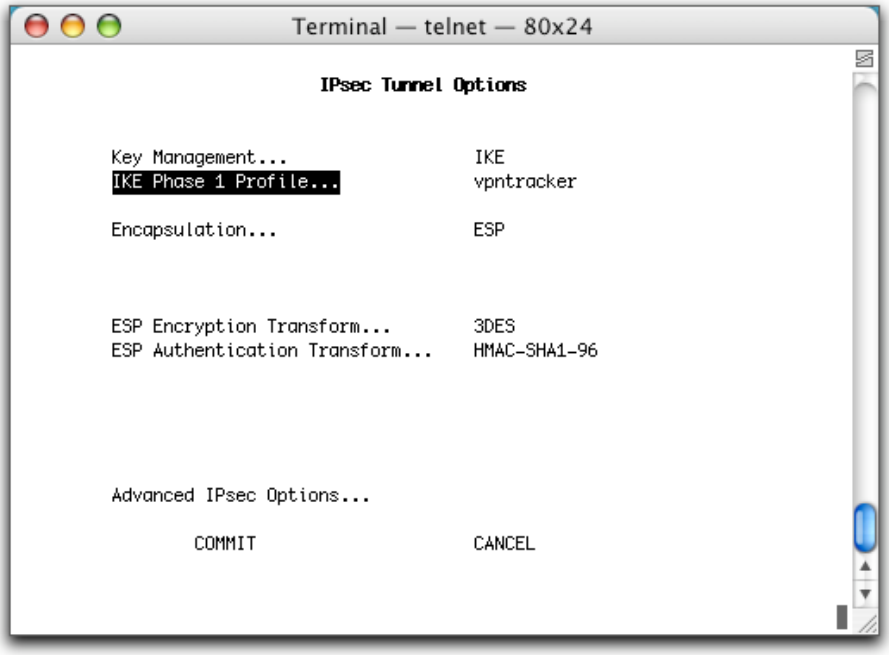

Figure 3: Netopia - IPsec Tunnel Options

Step 3

Select “IKE Phase 1 Profile“ and create a new Profile. Choose an arbitrary “Profile Name” and set “Mode” to Aggressive Mode.

Now change the “Local/Remote Identity Type” to Host name and supply a descriptive name. This setting refers to “Remote/Local Identifier” in the VPN Tracker configuration.

Please enter your “Shared Secret“ and change the “Encryption Algorithm“ to 3des and the “Hash Algorithm“ to sha1.

When you’re finished, submit your changes and go back to the Connection Profile.

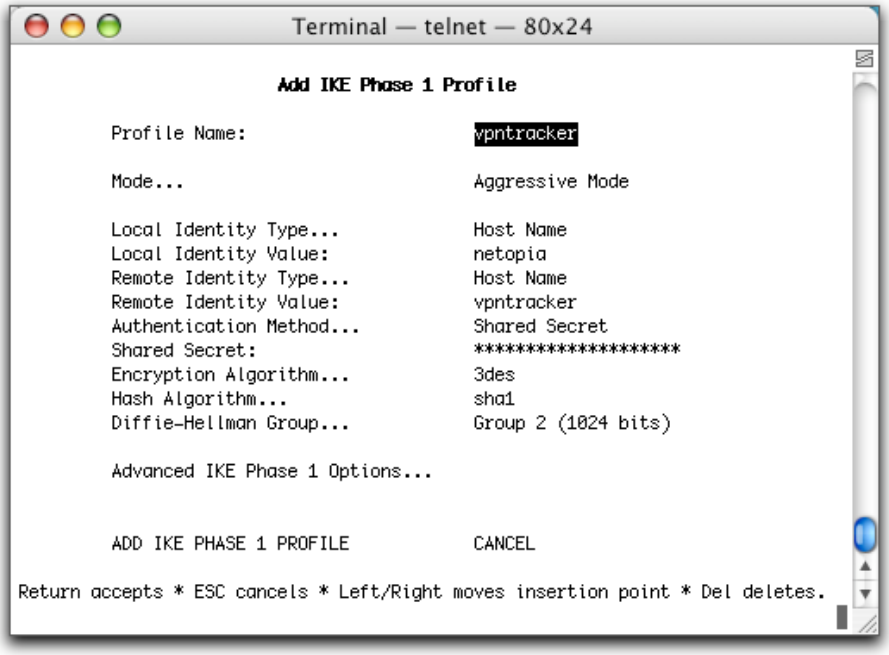

Figure 4: Netopia – Add IKE Phase 1 Profile

Step 4 Back in the Connection Profile screen, change the “IP Profile Parameters“.

Please select Host Address as “Remote Member Format“ and enter an IP address. This setting refers to the “Local Host“ in your VPN Tracker configuration.

Please enter the network address of your LAN subnet as “Local Member Address“.

Finally commit your IP Profile and your Connection Profile configuration.

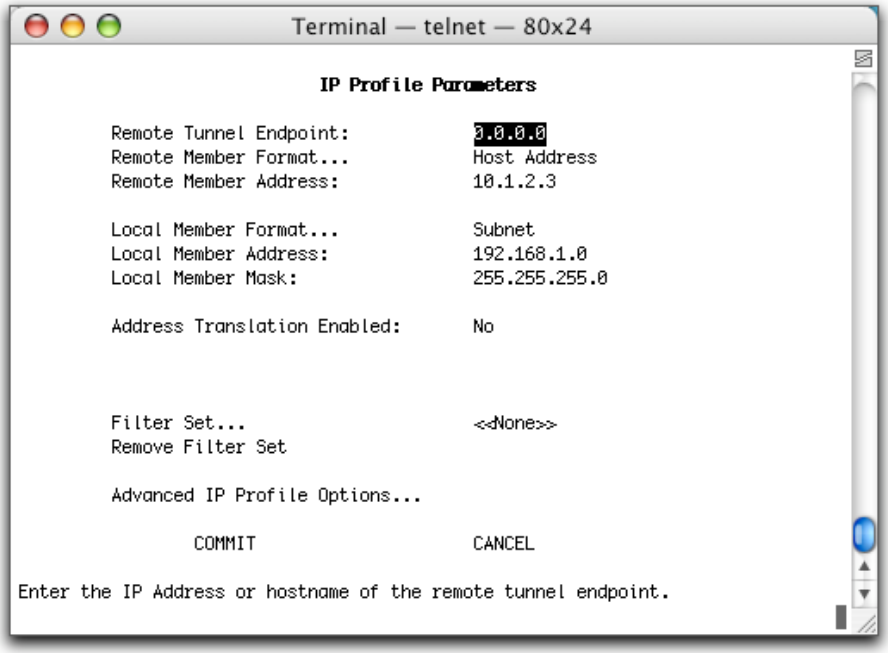

Figure 5: Netopia - IP Profile Parameters

Multiple VPN Tracker Hosts

Please create a new “Connection Profile“ for each VPN Tracker host (Step 1). Each host should have a unique “Remote Member Address“ (Step 4).

If every client should use the same Pre-shared key, you can use the same “IKE Phase 1 Profile“ for each host, otherwise create one profile for each client (Step 3).

The advantage of this setup is, that the VPN Tunnel can be accessed from both sides, so you can, for example, control the clients with Timbuktu.

VPN Tracker Configuration

Step 1 Add a new connection with the following options: Choose „Netopia“ as the Connection Type, „Host to Network“ as Topology, then type in the remote endpoint (169.1.2.3), the local host (10.1.2.3) and the remote network (192.168.1.0/24).

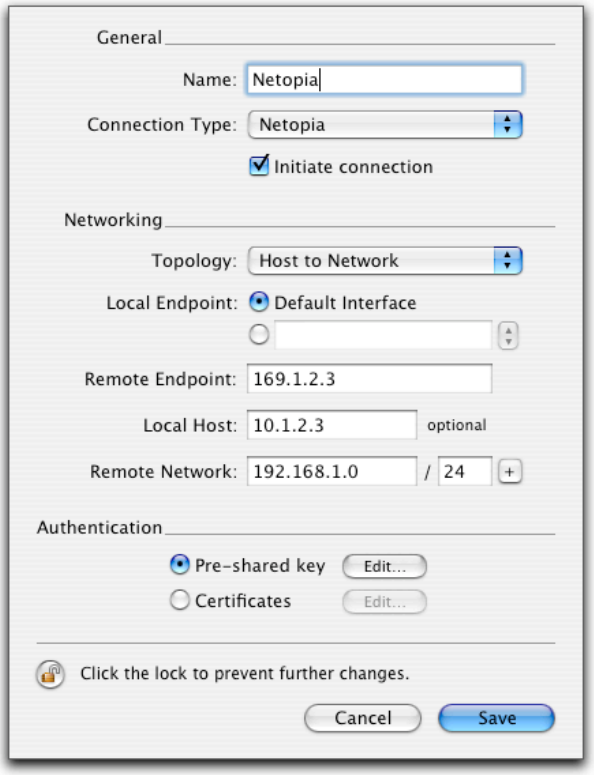

Figure 6: VPN Tracker Connection Dialog

Step 2

Select as “Authentication” method „Pre-shared key“ and click “Edit...”. Type in your Pre-shared key and your Local/Remote Identifier.

Please note: The content of these fields refer to the settings in chapter 3.1 step 3.

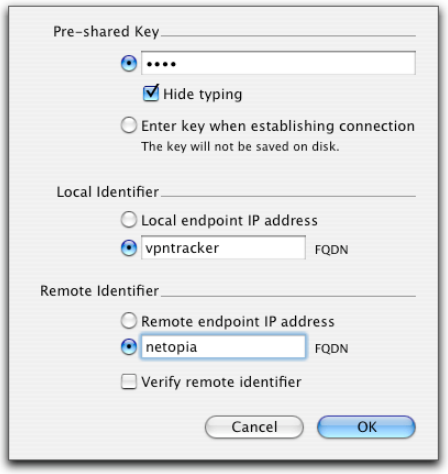

Figure 7: VPN Tracker - PSK Dialog

Step 3

Save the connection and Click on „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 Netopia Cayman. 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 Netopia Cayman network from the dialed-in Mac in the “Terminal” utility:

```
ping 192.168.1.10
```

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.