VPN Tracker for Mac OS X

How-to:

Interoperability with

SnapGear VPN Router Appliances

Rev. 1.0

1. Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a SnapGear VPN Appliance. The entire SnapGear product range should be compatible with VPN Tracker. equinux has tested the SnapGear SOHO+.

The SnapGear VPN Appliance 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 SnapGear VPN Appliance.

This paper is only a supplement to, not a replacement for, the instructions that have been included with your SnapGear VPN Appliance. Please be sure to read and understand those instructions before beginning.

2. Prerequisites

Firstly, you should use a recent SnapGear firmware version. The latest firmware release for your SnapGear VPN Appliance can be obtained from:

http://www.snapgear.com

For this document, firmware version 1.7.2u2 has been used.

The type of the VPN Tracker license needed (personal or professional edition) depends on the connection scenario you are using:

- If you connect a dial-in Mac without it's own subnet to the SnapGear VPN Appliance you need a Personal License.
- If you want to establish a LAN-to-LAN connection from your Mac to the SnapGear VPN Appliance, you need a VPN Tracker Professional License.

VPN Tracker is compatible with Mac OS X 10.2 or higher.

Be sure to use VPN Tracker 1.6.1 or higher.[1] For this document VPN Tracker version 2.0 has been used.

[1] All VPN Tracker versions prior to the 1.6.1 did not include a connection type for SnapGear products.

3. Connecting a VPN Tracker Host to a SnapGear VPN Appliance

In this example, the Mac running VPN Tracker is directly connected to the internet via a dialup or PPP connection.[2] The SnapGear VPN Appliance is configured in NAT mode and has the static WAN IP address 169.1.2.3 with gateway 169.1.2.1 and the private LAN IP address 192.168.1.1. The stations in the LAN behind the SnapGear VPN Appliance use 192.168.1.1 as their default gateway and should have a working Internet connection.

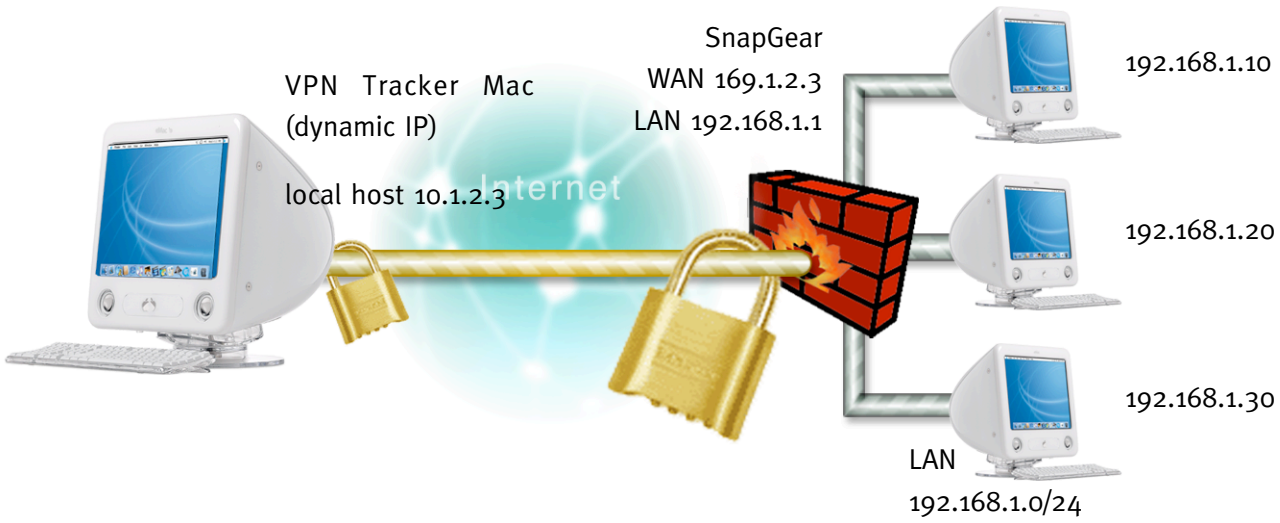


Figure 1: VPN Tracker - SnapGear VPN Appliance connection diagram (host to network)

3.1 SnapGear VPN Appliance configuration

The pre-defined VPN Tracker connection type has been created using the default settings on SnapGear VPN Appliance. If you change any of the settings on the SnapGear VPN Appliance VPN router, you will subsequently have to adjust the connection type in VPN Tracker.

[2] 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.

Step 1

IPSec VPN Setup:

Go to [VPN -› IPSec] and enable “IPSec”, click the “Submit” Button to. Then specify the routes by checking “eth1” and “Restart IPsec with new configuration” under “IPSec Interfaces” and submit again.

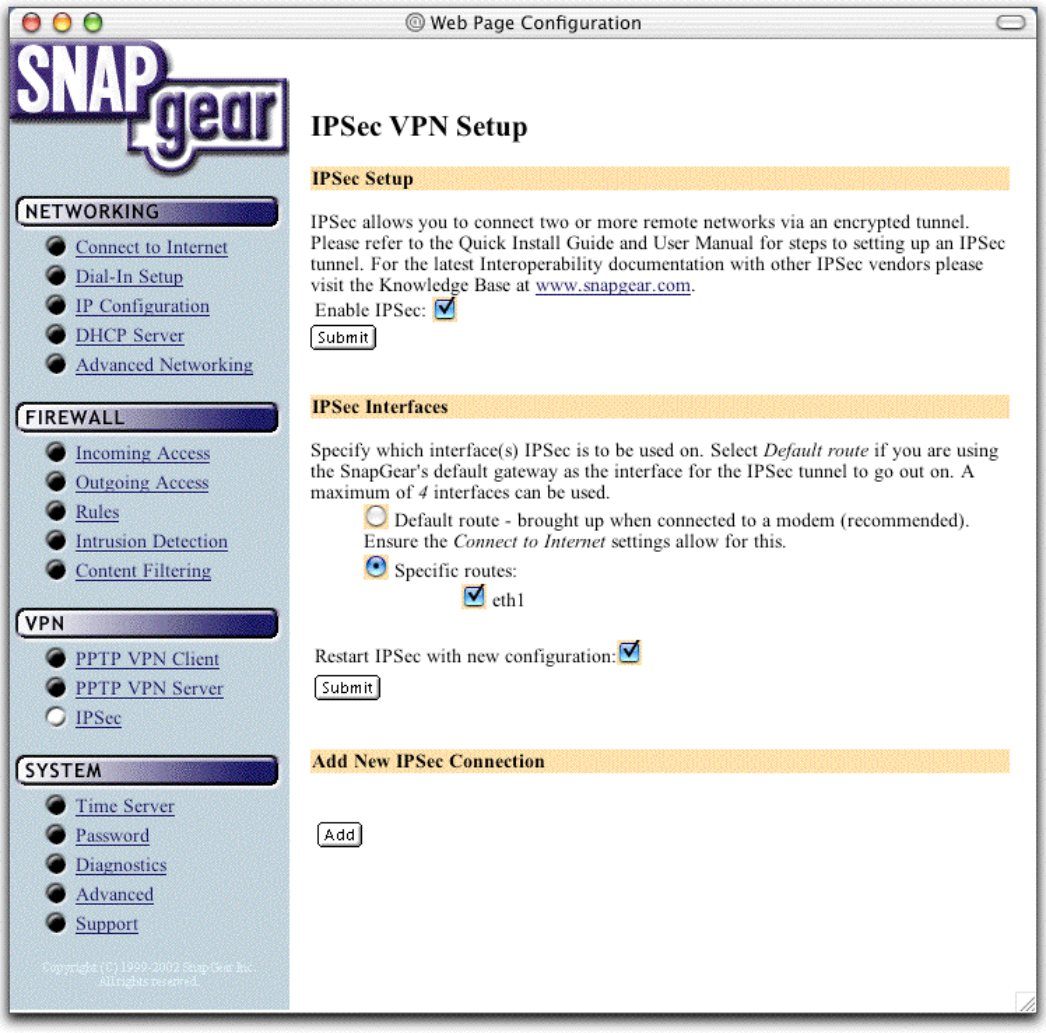


Figure 2: Enable IPSec and specify routes

Step 2

VPN IKE / IPSec Setup:

Push button “Add” on the ‘IPsec VPN Setup’ Page in order to add a new IPsec Connection.

Enter a connection name (e.g. vpntracker) and don’t use the “Aggressive Mode”.

In passage ‘Local Network’, please type in the:

- “Internal subnet/netmask” (e.g 192.168.1.0/255.255.255.0)
- the “External IP” of the SnapGear Router
- and the Gateway IP address in the field “NextHop”

This settings refers to the [Networking -› Connect to Internet] settings in your SnapGear Router.

Please enter the same virtual IP (e.g. 10.1.2.3) that you will use for ‘local host’ in VPN Tracker (figure 8) on field “Internal subnet / netmask” of the “Remote Gateway”. This setting refers to the “Local Host” field in VPN Tracker. The Network Mask is ‘255.255.255.255’ and the external IP of the Remote Network is 0.0.0.0.

Finally please disable the “Dead Peer Detection’. The authentication method is “Using a Pre-Shared Secret”.

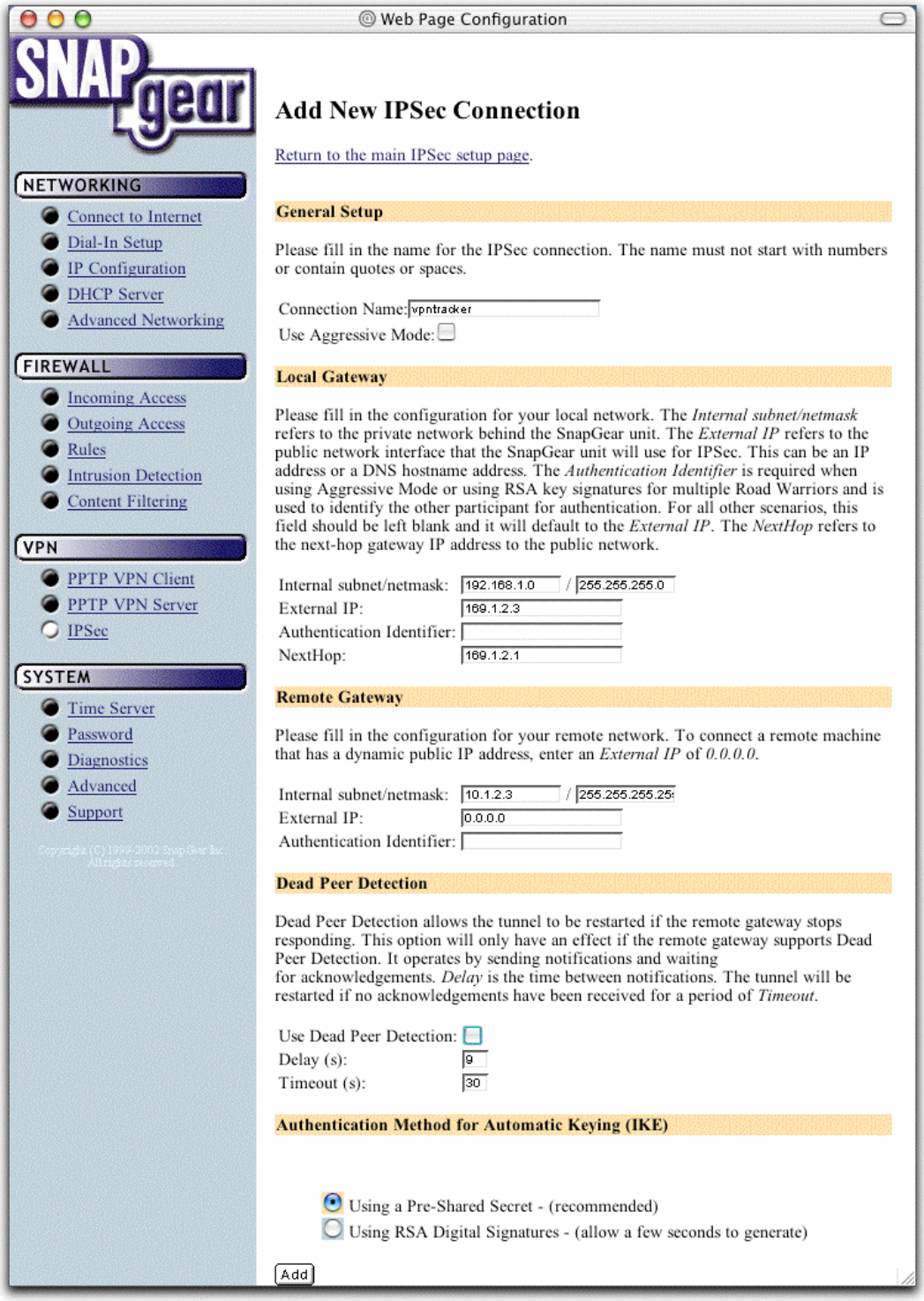


Figure 3: New IPSec Connection dialog

Step 3 Automatic Keying (IKE) Setup:

Insert a Pre-Shared Key. You can leave the other settings in their default value. And submit the changes. Please Note: Every user uses the same shared key.

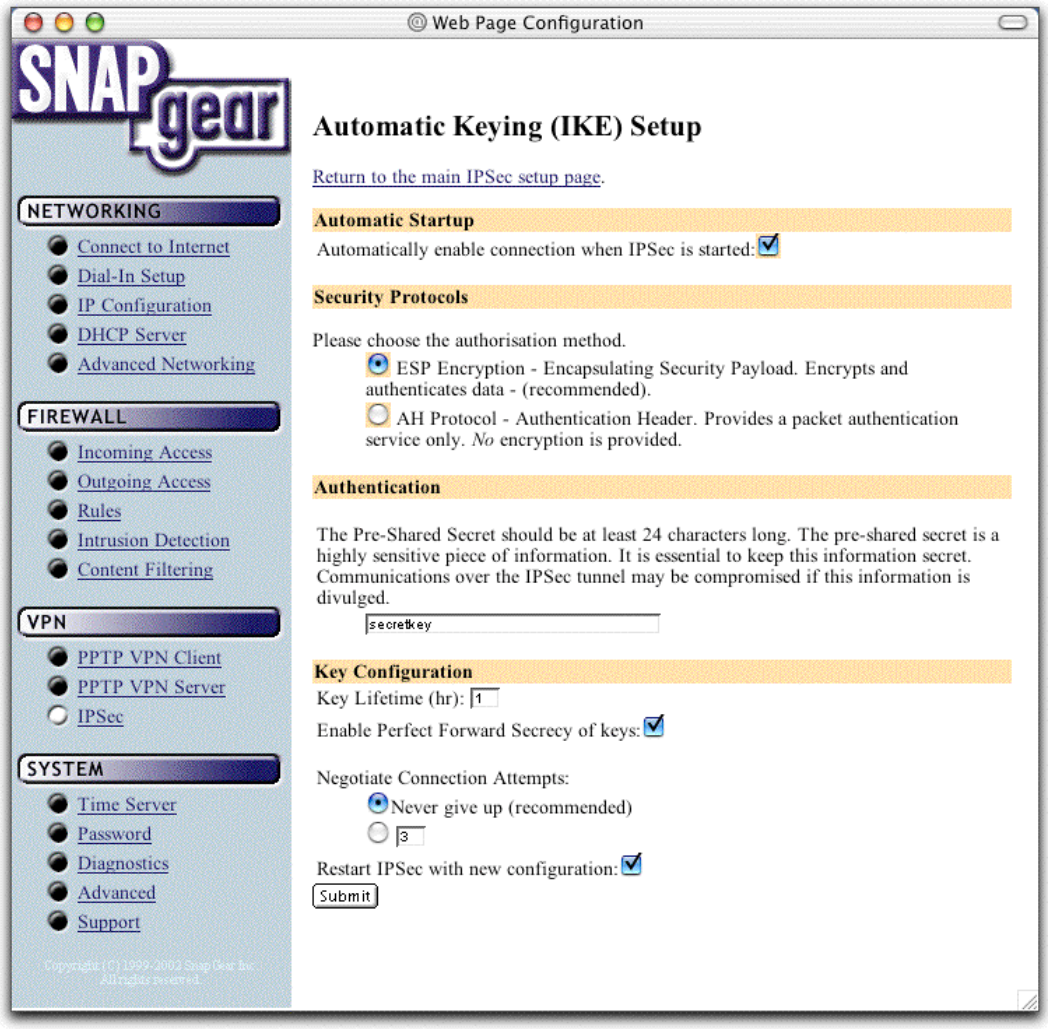


Figure 4: Automatic Keying Setup dialog

After the steps 1-4 the configuration should look like this:

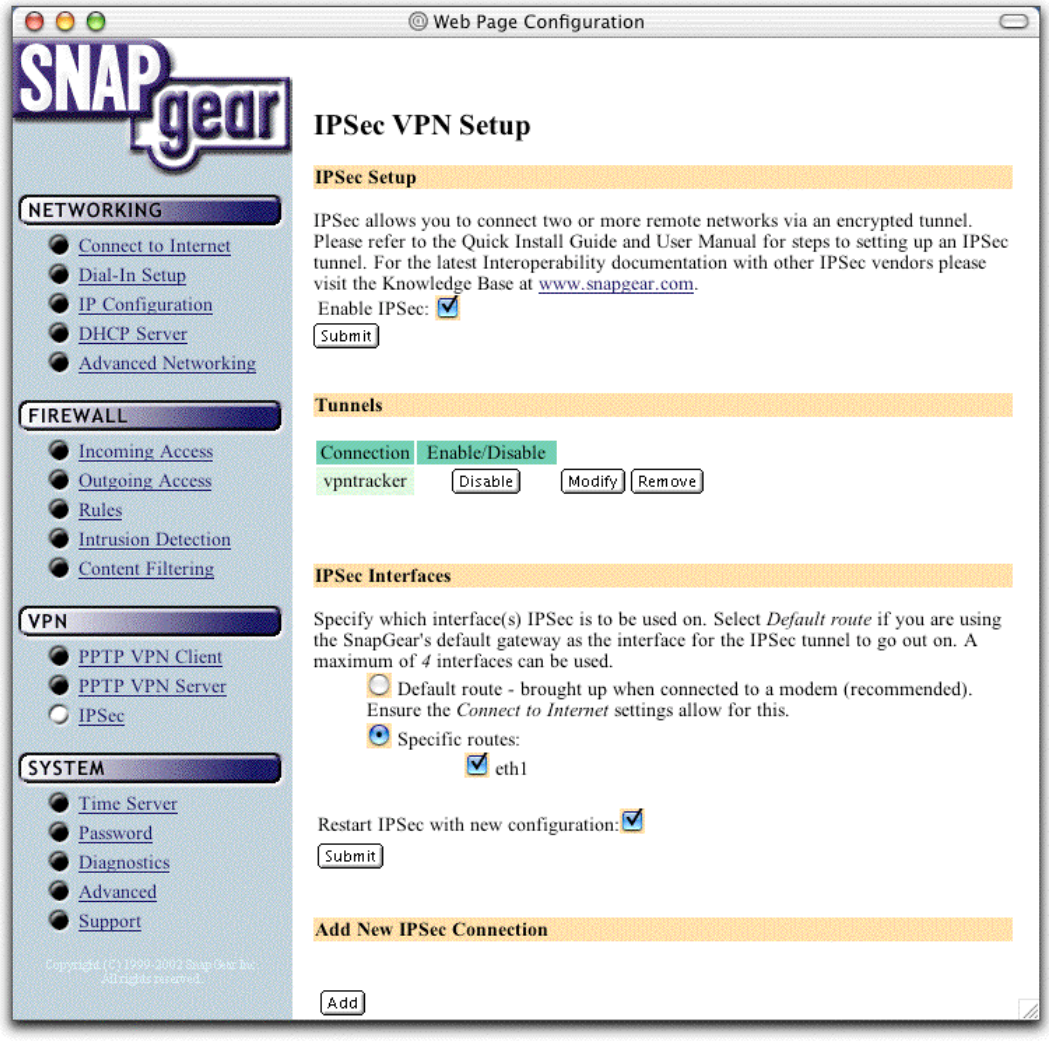


Figure 5: IPSec VPN Setup dialog

Multiple VPN Tracker Hosts

Repeat steps 1 to 3, using different names e.g. vpn2 and a different virtual IP in field ‘Internal Subnet/Netmask’ addresses (e.g. 10.1.2.4) in paragraph ‘Remote Gateway’.

3.2 VPN Tracker configuration

Step 1

Add a new connection with the following options: Choose „SnapGear “ 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). Enter the same “local host” that you typed-in in Figure 5, which will be the virtual IP address of your Mac (10.1.2.3).

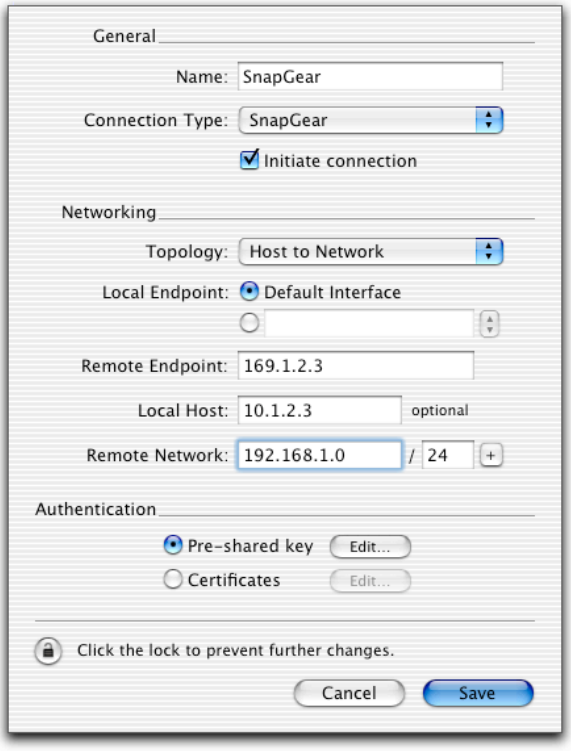


Figure 6: VPN Tracker connection dialog

Step 2

Click select „Pre-shared key“ and click “Edit...”. Type in the shared secret key that you typed-in in the SnapGear router (Figure 2).

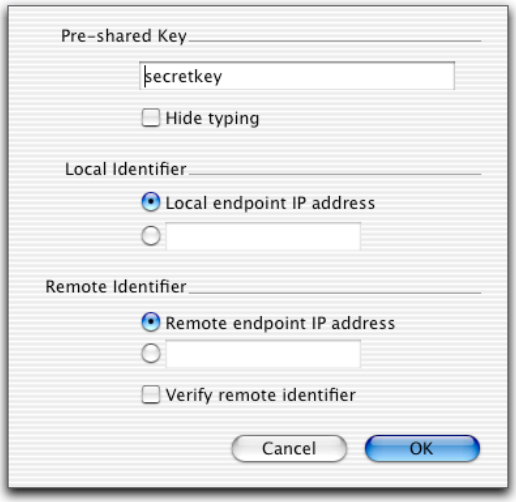


Figure 7: Pre-shared Key Authentication dialog

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 SnapGear VPN Appliance. 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 SnapGear VPN Appliance network from the dialed-in Mac in the “Terminal” utility:

```
ping 192.168.1.10
```

And from the SnapGear network (192.168.1.0/24) you can:

```
ping 10.1.2.3
```

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. Setting up a LAN-to-LAN connection

In this example the Mac running VPN Tracker Professional is directly connected to the Internet via a second Ethernet card or via a dialup or PPP connection. The WAN side IP address can be dynamically or statically assigned.

The gateway Mac running VPN Tracker is configured as a router that connects the LAN behind the gateway Mac (10.1.0.0/24) to the Internet. Therefore, Internet Sharing must be enabled on the gateway Mac. It can be enabled in the „Sharing“ control panel under the Tab „Internet“. If you are using Mac OS X Server, VPN Tracker will automatically enable routing.

The LAN IP address of the gateway Mac is 10.1.0.1 in our example. The client workstations in the LAN must be configured with the gateway Mac as their router.

The SnapGear VPN Appliance is permanently connected to the Internet and has the static WAN IP address 169.1.2.3 with Gateway 169.1.2.1 and the private LAN IP address 192.168.1.1. The stations in the LAN behind the SnapGear VPN Appliance use 192.168.1.1 as their default gateway and should have a working Internet connection.

The SnapGear VPN Appliance is the passive side waiting for connections that are initiated from the VPN Tracker side.

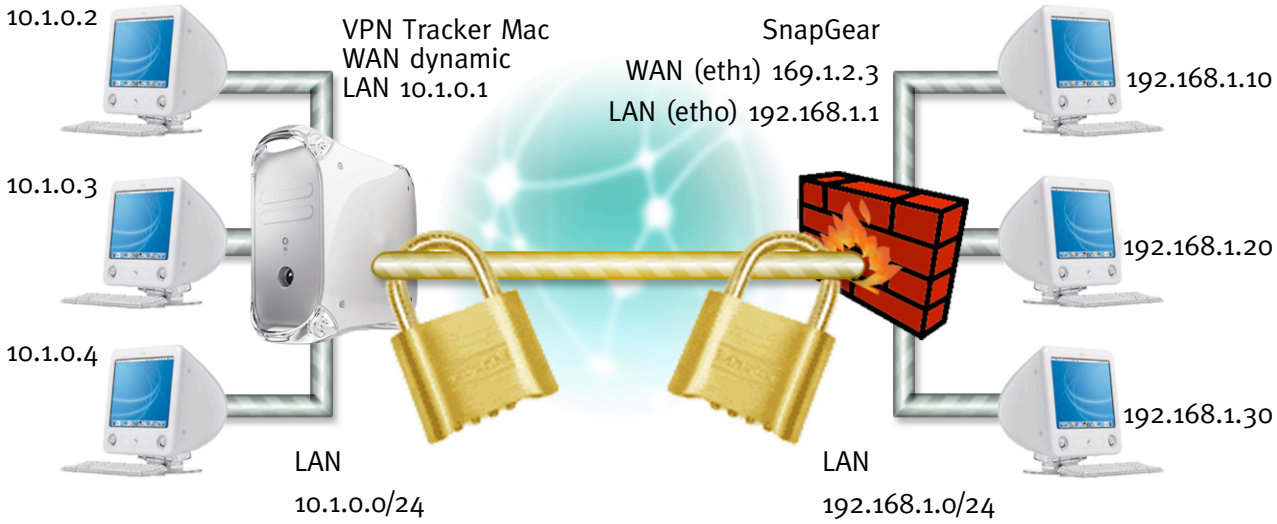


Figure 8: VPN Tracker – SnapGear connection diagram (network to network)

4.1 SnapGear VPN Appliance configuration

Step 1 The setup of enable IPsec works the same way as described in section 4.

Step 2 VPN IKE / IPSec Setup:

Enter a connection name (e.g. vpntracker-ntn) and don't use the "Aggressive Mode".

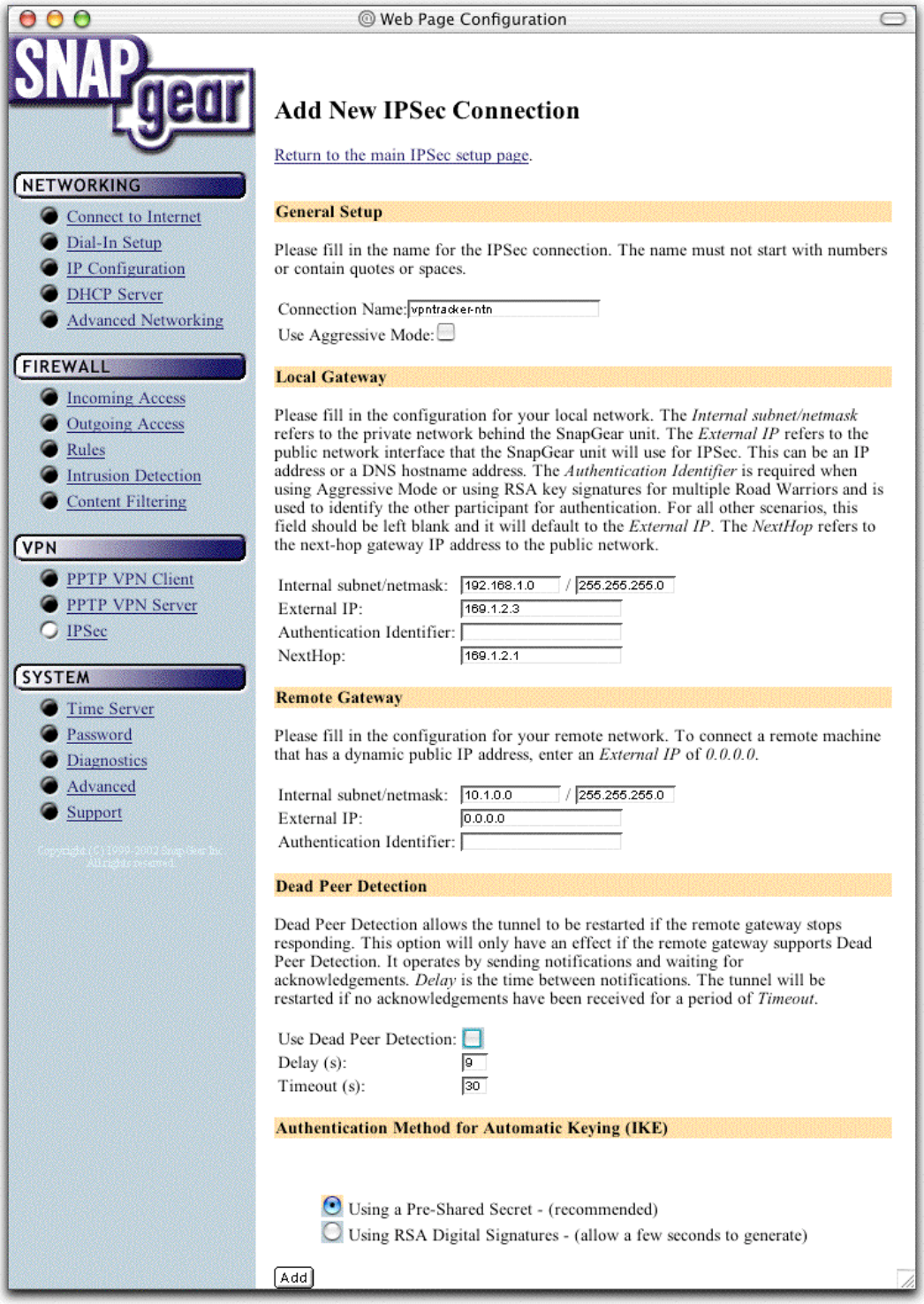
In passage 'Local Network', please type in the:

- "Internal subnet/netmask" (e.g 192.168.1.0/255.255.255.0)
- the "External IP" of the SnapGear Router
- and the Gateway IP address in the field "NextHop"

This settings refers to the [Networking -› Connect to Internet] settings in your SnapGear Router.

Please enter the same network IP (e.g. 10.1.0.0/255.255.255.0) that you will use for 'local network' in VPN Tracker (figure 8) on field "Internal subnet / netmask" in the "Remote Gateway" passage. The external IP of the Remote Network is 0.0.0.0.

Finally please disable the "Dead Peer Detection'. The authentication method is "Using a Pre-Shared Secret".



Step 3 Automatic Keying (IKE) Setup:

The SnapGear has to be configured the same way as in step 3 of chapter 3.1.

4.2 VPN Tracker configuration

Step 1 Add a new connection with the following options. Choose „SnapGear“ as Connection Type, „Network to Network“ as mode and type in the remote endpoint and the remote network parameters.

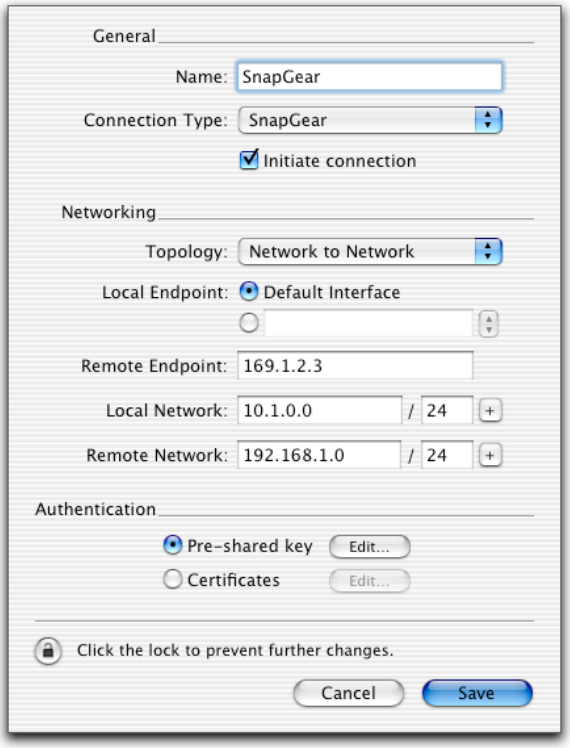


Figure 9: VPN Tracker connection dialog

Step 2, 3 The setup of the shared key and the startup of the connection works the same way as described in section 4.