# VPN Tracker for Mac OS X

## How-to:

## Interoperability with

## Linux FreeS/WAN

Rev. 2.0

# 1. Introduction

This document describes how VPN Tracker can be used to establish an IPSEC connection between a Macintosh running Mac OS X and a Linux box running FreeS/WAN.

The first example demonstrates a connection scenario with a dial-in Mac connecting to a FreeS/WAN gateway with subnet.

The second example demonstrates a LAN-to-LAN connection with VPN Tracker on one side and FreeS/WAN on the other side.

This manual does not cover the basic installation of FreeS/WAN. Please refer to the online documentation[1] for general FreeS/WAN configuration and installation issues.

# 2. Prerequisites

The requirements on the Linux side depend on the type of authentication you want to use. VPN Tracker supports authentication by preshared key, by RSA public/private keys and by x.509 certificates. A working installation of FreeS/WAN is required if you want to use authentication by preshared key or RSA public/private key. For authentication by x.509 certificates you need the patched version of FreeS/WAN[2] with x.509 support.

On the Mac side you need one VPN Tracker license for each Mac connecting to the Linux box. The type of the license needed (personal or professional edition) depends on the connection scenario you are using:

- If you want to use authentication by RSA keys or x.509 certificates, you need one VPN Tracker professional license for generating a CA and signing certificates.
- If you want to establish a LAN-to-LAN connection from your Mac to the Linux gateway, you need a VPN Tracker professional license.

[1] http://www.freeswan.org/

[2] http://www.freeswan.ca/

- Otherwise, if you connect a dial-in Mac without own subnet to the Linux box you need a personal license.

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

# 3. Connecting a VPN Tracker host to a FreeS/WAN gateway

In this example the Mac running VPN Tracker is directly connected to the Internet via a dialup or PPP connection.[3]

The Linux box is configured with IP masquerading turned on and has the static WAN IP address 169.1.2.3 and the private LAN IP address 10.0.0.1. The Stations in the LAN behind the Linux box use 10.0.0.1 as their default gateway and should have a working Internet connection. The Linux box is the passive side waiting for connections that are initiated from the VPN Tracker side.

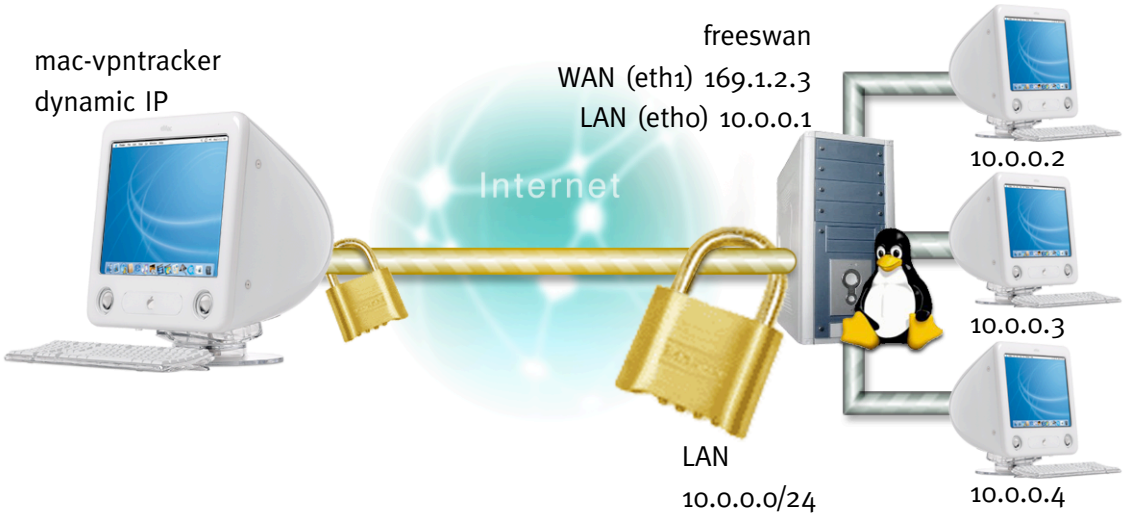


*Figure 1: VPN Tracker – FreeS/WAN host to network connection diagram*

[3] Please note that the connection via a router operating in Network Address Translation (NAT) mode only works if the NAT router supports „IPSEC passthrough“. Please contact the manufacturer of the router for details.

## 3.1 Setting up a VPN Tunnel with Preshared Key Authentication

### FreeS/WAN Configuration

**Step 1**

On the FreeS/WAN side you have to edit the configuration file */etc/ipsec.conf* and the shared secret file */etc/ipsec.secrets*. The general settings below are independent of the authentication method used.

```
config setup
  # THIS SETTING MUST BE CORRECT or almost nothing will work;
  # %defaultroute is okay for most simple cases.
  interfaces=%defaultroute
  #interfaces="ipsec0=eth1"

  # Debug-logging controls: "none" for (almost) none, "all" for
#lots.
  klipsdebug=none
  plutodebug=none

  plutoload=%search
  plutostart=%search
  # Close down old connection when new one using same ID shows up.
  #uniqueids=yes
  dumpdir=/var/log
```

*Figure 2: /etc/ipsec.conf – general settings*

**Step 2** Please add a new connection to your */etc/ipsec.conf*.

```
conn vpntracker-psk
  left=%any
  leftsubnet=
  leftnexthop=
  right=169.1.2.3
  rightsubnet=10.0.0.0/24   # the LAN behind FreeS/WAN
  rightnexthop=169.1.2.254  # the default gateway of the Linux box
  auto=add
  authby=secret
```

*Figure 3: /etc/ipsec.conf – PSK connection*

**Step 3** Edit your */etc/ipsec.secrets* and put your PSK in here. Please use a different and longer secret key than that, which we used in our example.

```
: PSK "mysecretkey“
```

*Figure 4: /etc/ipsec.secrets – PSK Authentication*

After editing the files you have to restart IPSEC:

```
/etc/init.d/ipsec restart
```

FreeS/WAN is now ready to listen for any connection attempts from the other side.

## VPN Tracker Configuration

**Step 1** Add a new connection with the following options: Choose „FreeS/WAN“ as the Connection Type, „Host to Network“ as the mode and type in the remote host and the remote network parameters.

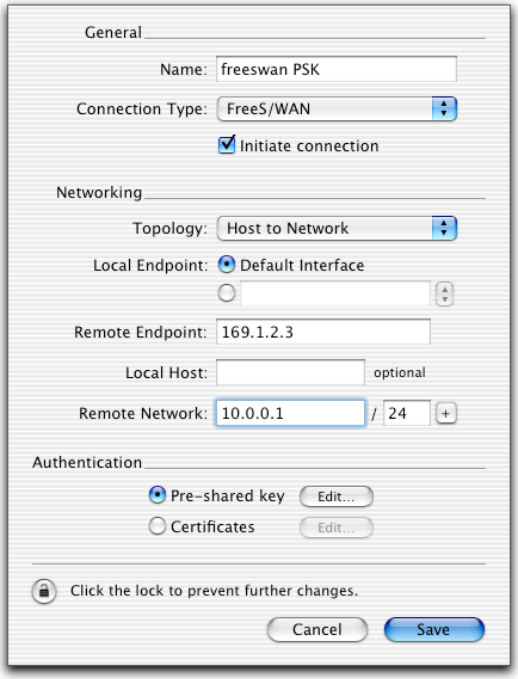


*Figure 5: PSK connection dialog*

**Step 2**

Select the authentication method „Pre-shared key“ and click “Edit...” Type in the same shared secret that you typed-in your */etc/ipsec.secrets* on your FreeS/WAN box.

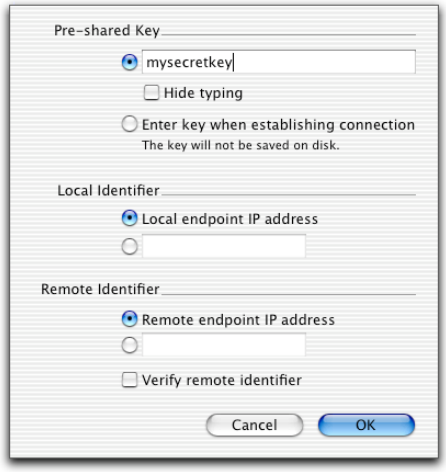


*Figure 6: Shared key dialog*

**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 FreeS/WAN host. After IPsec has been started, you may quit VPN Tracker. The IPsec service will keep running.

Simply test your connection by pinging a host in the FreeS/WAN network from the dialed-in Mac in the “Terminal” utility:

```
ping 192.168.1.1
```

## 3.2 Setting up a VPN Tunnel with RSA Authentication

### FreeS/WAN Configuration

**Step 1** Please refer to chapter 3.1 on page 4

**Step 2** Go to the VPN Tracker certificate manager (⌘ + "E") and create and sign a certificate for the FreeS/WAN host.[4]

Please note: To sign a certificate you need to create a CA as described in the VPN Tracker Manual on page 25.

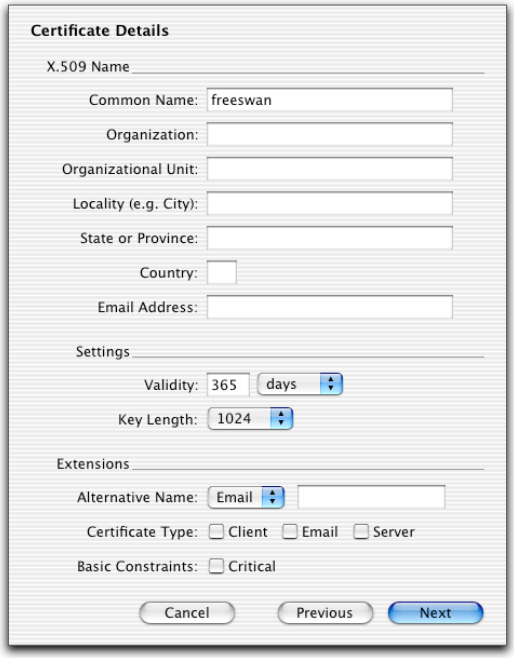


*Figure 7: FreeS/WAN certificate*

[4] Requires the VPN Tracker Professional Edition

**Step 3** Create and sign your own certificate for the VPN Tracker side.[5]

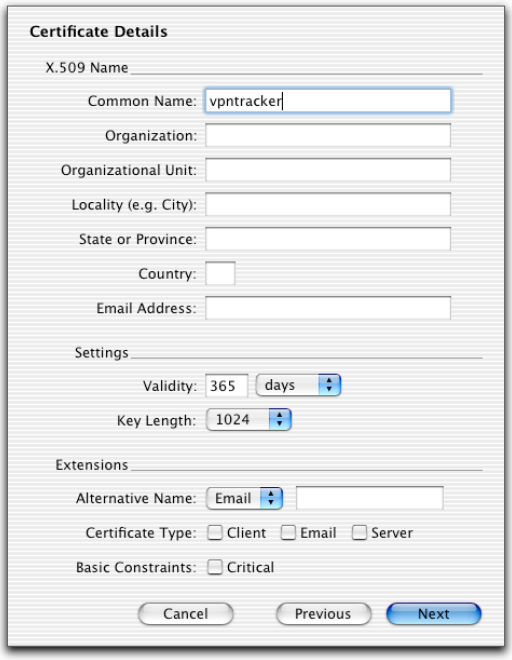


*Figure 8: VPN Tracker certificate*

**Step 4** Please export both certificates as FreeS/WAN public keys to your FreeS/WAN host. For the VPN Tracker certificate select „left“ as prefix and for the FreeS/WAN certificate „right“. Please also export the private key of the FreeS/WAN certificate.

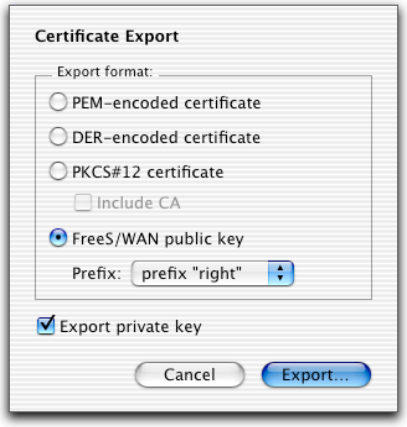


*Figure 9: FreeS/WAN public and private key export*

[5] Requires the VPN Tracker Professional Edition

**Step 5**

Copy all files to your FreeS/WAN box and edit */etc/ipsec.conf* and add the content of the public key files to your config.

```
conn vpntracker-keys
        auto=add
        keyingtries=0
        left=%any
        leftsubnet=
        leftnexthop=
        right=169.1.2.3
        rightsubnet=10.0.0.0/24
        rightnexthop=169.1.2.254
        authby=rsasig
        leftid=@vpntracker # refers to local identifier
        rightid=@freeswan  # refers to remote identifier
        leftrsasigkey=0x03010001D.... # content of vpntracker.cert
        rightrsasigkey=0x03010001B..... # content of freeswan.cert
```

*Figure 10: /etc/ipsec.conf – RSA Authentication*

**Step 6**

Append the content of the FreeS/WAN private key to your */etc/ipsec.secrets*.

```
: RSA {
        Modulus:
0xB0B6ABBF9EBDC3F87BC78654B6221E98D43B90A398838EE4C76BC
A84B6BE815C737475E0F0F95D8413C8F08FB9265C2608FB2740D29B777BD68A54A
2F4A97798BB027
B871D51D7DF86CA20CAFA82B052F5D644A9DDB94394302D17F9CE159F6365DAB7B
B83A2A4C2CDFDC
4C329FA9541F363603ECAD9F425276716D478EC516F
        PublicExponent:  0x010001
        PrivateExponent: ........
...........
```

*Figure 11: /etc/ipsec.secrets – RSA Authentication*

After editing the files you have to restart IPSEC:

```
/etc/init.d/ipsec restart
```

FreeS/WAN is now ready to listen for any connection attempts from the other side.

## VPN Tracker Configuration

**Step 1** Please refer to chapter 3.1 on page 6.

**Step 2** Select the authentication method “Certificates“ and click “Edit...”

Choose as “own certificate” the self-signed certificate, you created with VPN Tracker and verify the remote certificate “with CAs”. Type in your local identifier (e.g. vpntracker) and the remote one (e.g. freeswan).

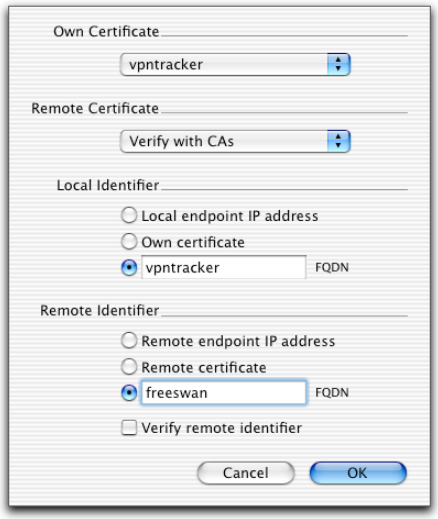


*Figure 12: Certificate dialog*

**Step 3** Please refer to chapter 3.1 on page 7.

## 3.3 Configuring a VPN Tunnel with x.509 Certificate Authentication

### FreeS/WAN Configuration

**Step 1** Please refer to chapter 3.1 on page 4

**Step 2** Create a new certificate-signing request at your Linux box running FreeS/WAN.

```
~# openssl req –newkey rsa:1024 –keyout freeswan.key.pem \
   -out freeswan.req.pem
~# cp freeswan.key.pem /etc/ipsec.d/private/
```

**Step 3** Import the Request in the “Request” tab in VPN Tracker and “Sign” the request with your CA.

Please note: This feature requires the VPN Tracker Professional Edition.

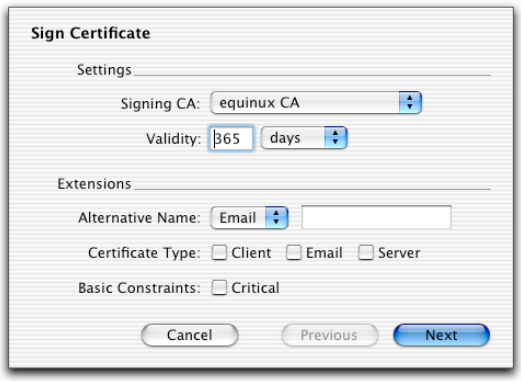


*Figure 13: VPN Tracker - Sign Certificate*

**Step 4** Create and sign a certificate for the VPN Tracker side.

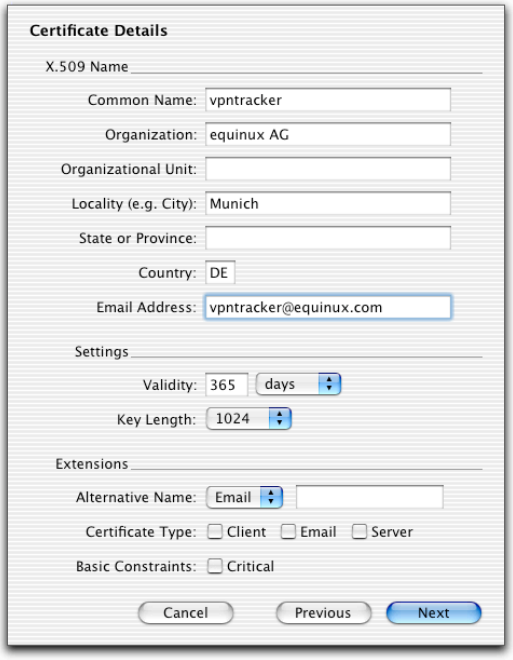


*Figure 14: VPN Tracker certificate*

**Step 5** Export both signed certificates in PEM format and copy them to /etc/ipsec.d/ on your Linux box and edit your */etc/ipsec.conf*.

```
conn vpntracker-cert
        auto=add
        authby=rsasig
        left=%any
        right=169.1.2.3
        rightsubnet=10.0.0.0/24
        rightnexthop=169.1.2.254
        leftcert=vpntracker.cert.pem
        rightcert=freeswan.cert.pem
```

*Figure 15: /etc/ipsec.conf - x.509 Certificate Authentication*

**Step 6** Edit your /etc/ipsec.secrets and add the following line:

```
:RSA freeswan.cert.pem "key.entered.in.step1"
```

After editing the files you have to restart IPSEC:

```
/etc/init.d/ipsec restart
```

FreeS/WAN is now ready to listen for any connection attempts from the other side.

## VPN Tracker Configuration

**Step 1** Add a new connection with the following options: Choose „FreeS/WAN (x.509)“ as the Connection Type, „Host to Network“ as the mode and type in the remote host and the remote network parameters.


*Figure 16: x.509 connection dialog*

**Step 2** Select the authentication method “Certificates“ and click “Edit...”

Choose as “own certificate” the self-signed certificate, you created with VPN Tracker and verify the remote certificate “with CAs”. Please set the “Local/Remote Identifier” to “Own/Remote certificate”.

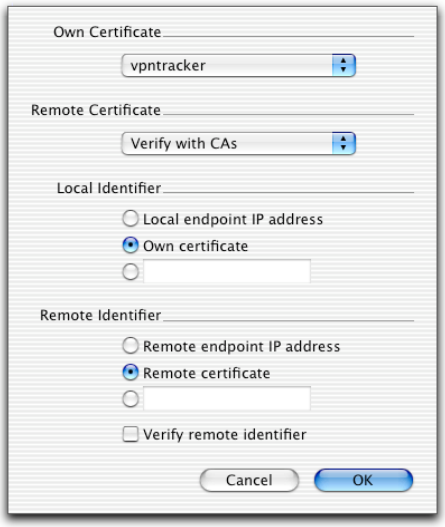


*Figure 17: Certificate dialog*

**Step 3** Please refer to chapter 3.1 on page 7

## Debugging

If the status indicator does not change to green please have a look in the log on both sides. The level of verbosity can be configured in the VPN Tracker preferences and in `/etc/ipsec.conf` for FreeS/WAN. The location of the log file on the Linux side depends on your Syslog configuration. If you can’t find any log output you should configure a catch-all logfile in your syslog configuration by adding the following line to your `/etc/syslog.conf`:

```
*.*        -/var/log/debug
```

Restart your syslog demon afterwards by executing

```
/etc/init.d/syslog restart
```

# 4. Setting up a LAN-to-LAN connection

In this example the Mac running VPN Tracker is directly connected to the Internet via an Ethernet or dialup or PPP connection.[6] 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“.

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 Linux box is configured with IP masquerading turned on and has the static WAN IP address 169.1.2.3 and the private LAN IP address 10.0.0.1. The Stations in the LAN behind the Linux box use 10.0.0.1 as their default gateway and should have a working Internet connection. The Linux box is the passive side waiting for connections that are initiated from the VPN Tracker side.

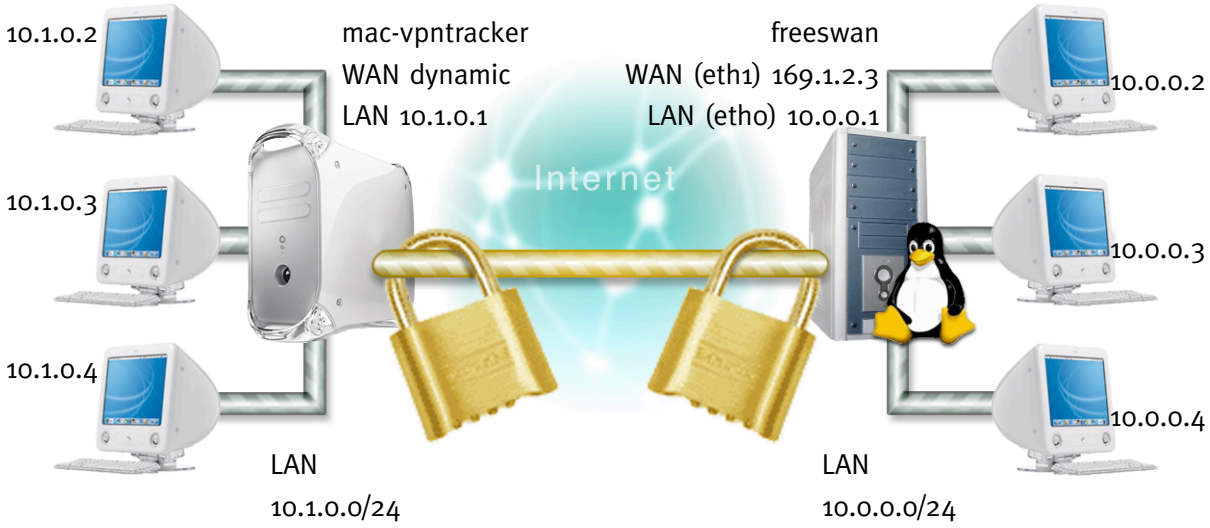


*Figure 18: VPN Tracker – FreeS/WAN network to network connection diagram*

[6] Please note that the connection via a router doing Network Address Translation (NAT) only works if the NAT router supports „IPSEC passthrough“. Please contact the manufacturer of the router for details.

## 4.1 FreeS/WAN Configuration

Please refer to chapter 3.1 for Preshared Key Authentication, chapter 3.2 for RSA Authentication or chapter 3.3 for x.509 Certificate Authentication.

Difference between a “Host to Network” and a “Network to Network” connection:

```
...
leftsubnet=10.1.0.0/24 # local  network
...
```

*Figure 19: /etc/ipsec.conf – “Network to Network” connection*

## 4.2 VPN Tracker Configuration

Please refer to chapter 3.1 for Preshared Key Authentication, chapter 3.2 for RSA Authentication or chapter 3.3 for x.509 Certificate Authentication.

Difference between a “Host to Network” and a “Network to Network” connection:

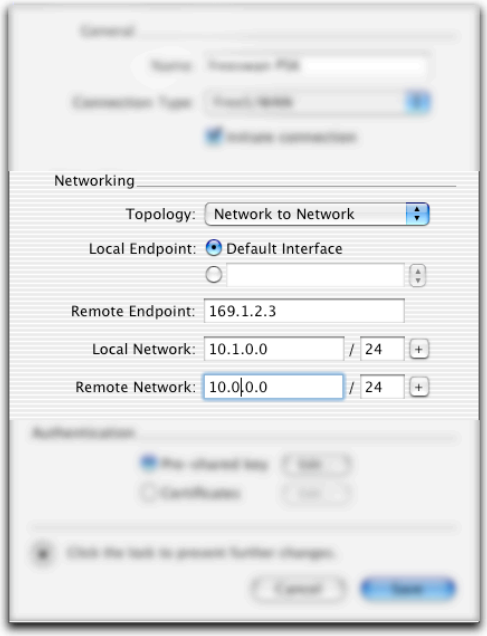


*Figure 20: Connection dialog*

### Debugging

Please refer to the debugging techniques described in chapter 3.