



VPN Tracker for Mac OS X



How-to:
Interoperability with
Cisco PIX
Internet Security Appliances

Rev. 4.0

Copyright © 2003-2004 equinux USA Inc. All rights reserved.

1. Introduction

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

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

All trademarks, product names, company names, logos, screenshots displayed, cited or otherwise indicated on the How-to are the property of their respective owners.

EQUINIX SHALL HAVE ABSOLUTELY NO LIABILITY FOR ANY DIRECT OR INDIRECT, SPECIAL OR OTHER CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE USE OF THE HOW-TO OR ANY CHANGE TO THE ROUTER GENERALLY, INCLUDING WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS, OR DATA, EVEN IF EQUINIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

1. Prerequisites

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

Furthermore you should use a recent Cisco PIX firmware version. The latest firmware release for your Cisco PIX appliance can be obtained from your local reseller or from

<https://www.Cisco.com/>

For this document, PIX Version 6.3(1) has been used.

When using Pre-shared key / Extended authentication you need one VPN Tracker license for each Mac connecting to the Cisco PIX.

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

2. Connecting to a Cisco VPN Appliance (single user)

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

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

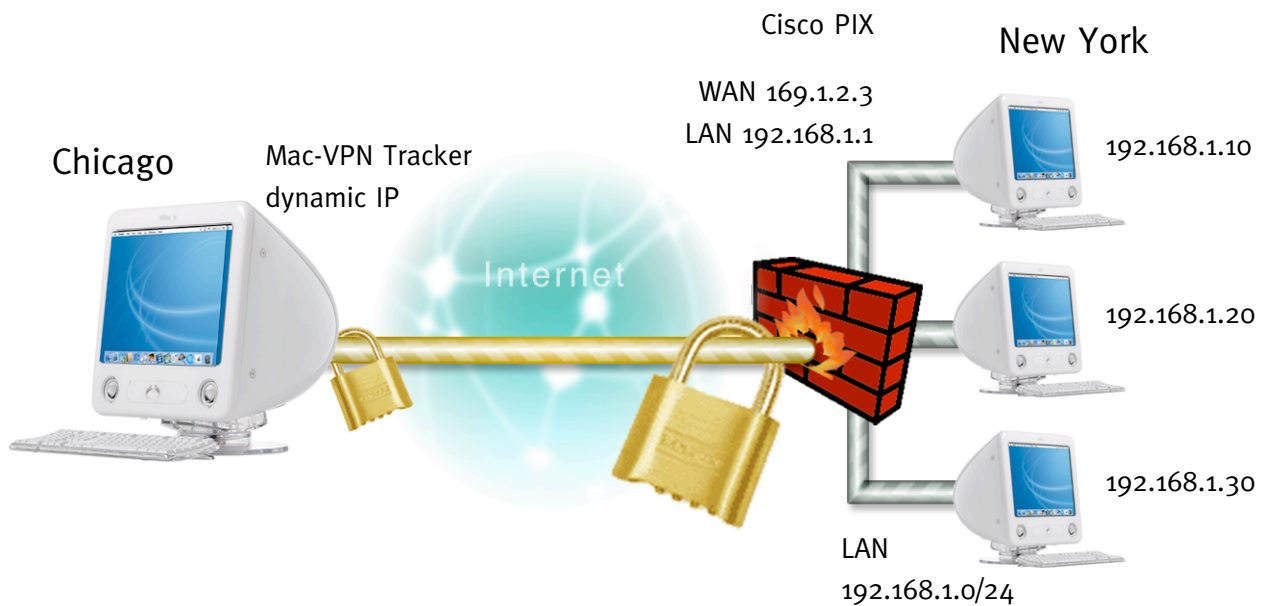


Figure 1: VPN Tracker – Cisco PIX connection diagram

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.

2. Connecting to a Cisco VPN Appliance (single user)

2.1 Cisco PIX Configuration

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

Please note: The following configuration steps were done on the console interface of the Cisco PIX device, which could be accessed through Telnet or SSH. In order to execute the following commands, admin privileges are required.

Step 1

General Settings:

- Enable bypass of access-list check for ipsec traffic:

```
sysopt connection permit-ipsec
```

- Allow IPsec to bypass the firewall engine:

```
sysopt ipsec pl-compatible
```

2. Connecting to a Cisco VPN Appliance (single user)

Step 2

IKE (Phase 1) Settings:

- Enable IKE on WAN interface:

```
isakmp enable wan2
```

- Set the Identifier type to IP Address:

```
isakmp identity address
```

- Create a IKE policy for VPN Tracker clients:

```
isakmp policy 10 authen pre-share  
isakmp policy 10 encrypt 3des  
isakmp policy 10 group 2
```

- Set a pre-shared key for general remote access with XAUTH:

```
isakmp key secretkey address 0.0.0.0 netmask 0.0.0.0
```

² wan is a alias name for the network interface attached to the Internet.

2. Connecting to a Cisco VPN Appliance (single user)

Step 3

IPsec (Phase 2) Settings:

- Please make sure that at least one of the following transform sets is configured on your Cisco PIX appliance:

```
show crypto ipsec transform-set
```

```
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
```

- Create a dynamic map and assign one of the above transform sets:

```
crypto dynamic-map wan_dyn_map 10 set transform-set ESP-3DES-SHA
```

- Create a regular ipsec/isakmp map based on the dynamic map, enable XAUTH and assign it to the wan interface:

```
crypto map wan_map 5 ipsec-isakmp dynamic wan_dyn_map
crypto map wan_map client authentication LOCAL3
crypto map interface wan
```

³ If you're using external authentication you should use a different authentication server group here.

2. Connecting to a Cisco VPN Appliance (single user)

Step 4 (Optional)

Create Local XAUTH Users:

Please note: This step is only needed if you're using a local user database for authentication.

```
username test password 1234 privilege 1
```

2.2 VPN Tracker Configuration

Step 1

Add a new connection with the following options:

- Vendor: „Cisco“
- Model: your VPN device

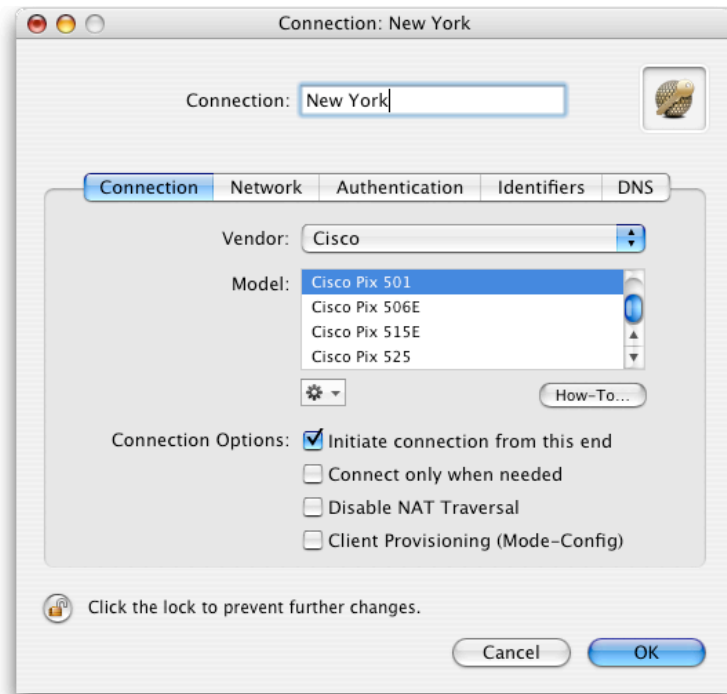


Figure 2: VPN Tracker - Connection Settings

2. Connecting to a Cisco VPN Appliance (single user)

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**).

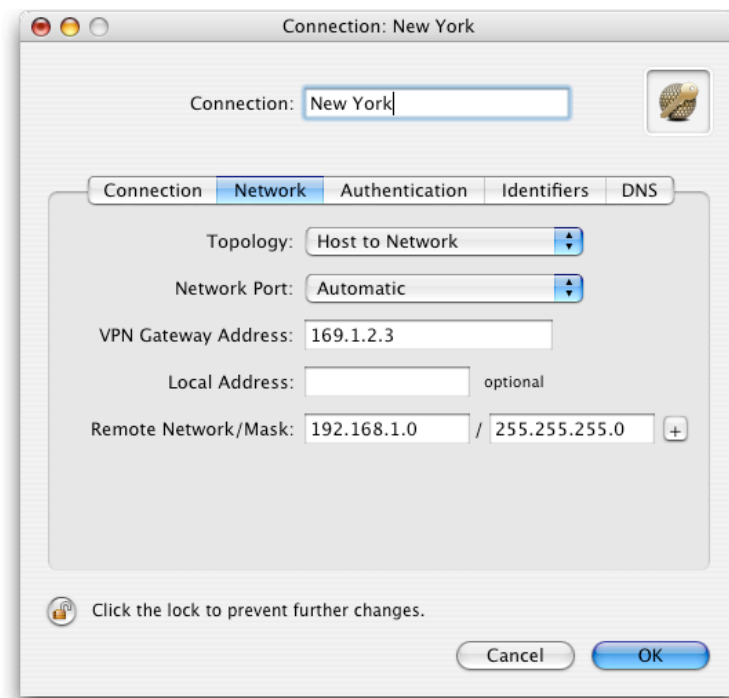


Figure 3: VPN Tracker - Network Settings

Please note: In order to access multiple remote networks simultaneously, just add them by pressing the “+” button.⁴

⁴ For this step VPN Tracker Professional Edition is needed.

2. Connecting to a Cisco VPN Appliance (single user)

Step 3

Change your Authentication Settings:

- Pre-shared key: the same Pre-shared key as in your Cisco PIX configuration.
- Enable Extended Authentication (XAUTH): **checked**

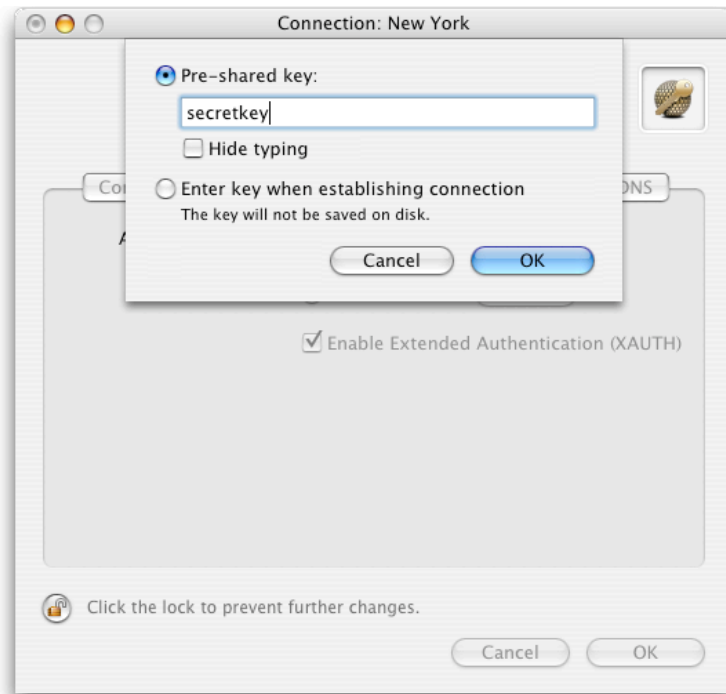


Figure 4: VPN Tracker - Authentication Settings

2. Connecting to a Cisco VPN Appliance (single user)

Step 4

Identifier Settings:

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

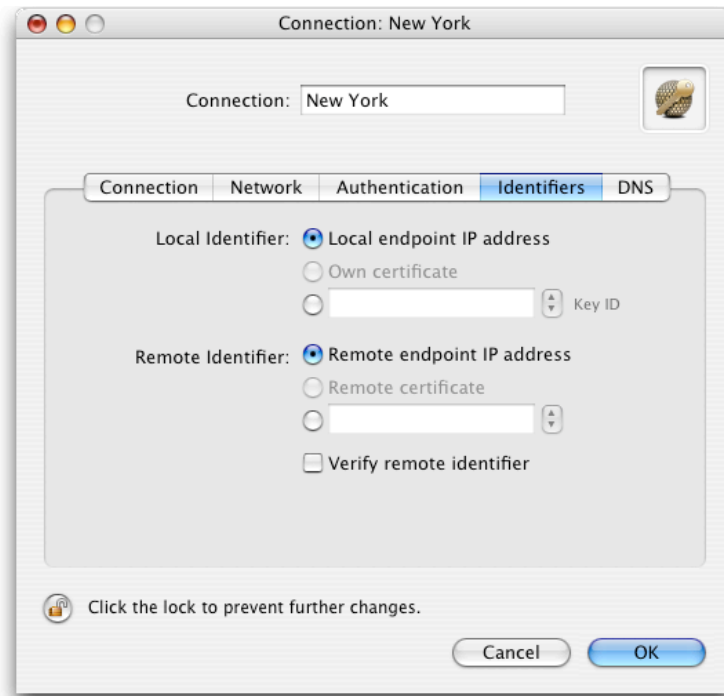


Figure 5: VPN Tracker - Identifier Settings

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

By running following commands you should see statistics of the established VPN tunnel:

```
show crypto isakmp sa
show crypto ipsec sa
```

3. Connecting to a Cisco PIX VPN Appliance (multiple user)

When connecting with multiple users we recommend, using Cisco's Easy VPN (Mode Config) facility, in order to minimize the configuration effort.

3.1 Cisco PIX Configuration

Step 1-4 Please refer to step 1-4 in section 3.1.

Step 5 Access list settings:

- Create an IP pool for VPN Tracker client connections:

```
ip local pool vpntracker-pool 10.0.1.1-10.0.1.254
```

- Create an access list that defines the VPN Tracker IP pool:

```
access-list vpntracker-user permit ip 10.0.1.0 255.255.255.0
```

- Assign this access list to the dynamic crypto map created in step 3 in section 3.1 and create a nat rule:

```
crypto wan_dyn_map 10 match address vpntracker-user  
nat 0 access-list vpntracker-user
```

3. Connecting to a Cisco PIX VPN Appliance (multiple user)

Step 6

VPN Group settings:

- Create a user group for group authentication and supply it with a password:

```
vpngroup vpntracker password secretkey
```

- Assign the IP address pool to the group:

```
vpngroup vpntracker address-pool vpntracker-pool
```

3.2 VPN Tracker Configuration

Step 1

Add a new connection with the following options:

- Vendor: „Cisco“
- Model: your VPN device
- Client Provisioning (Mode-Config): **Enabled**

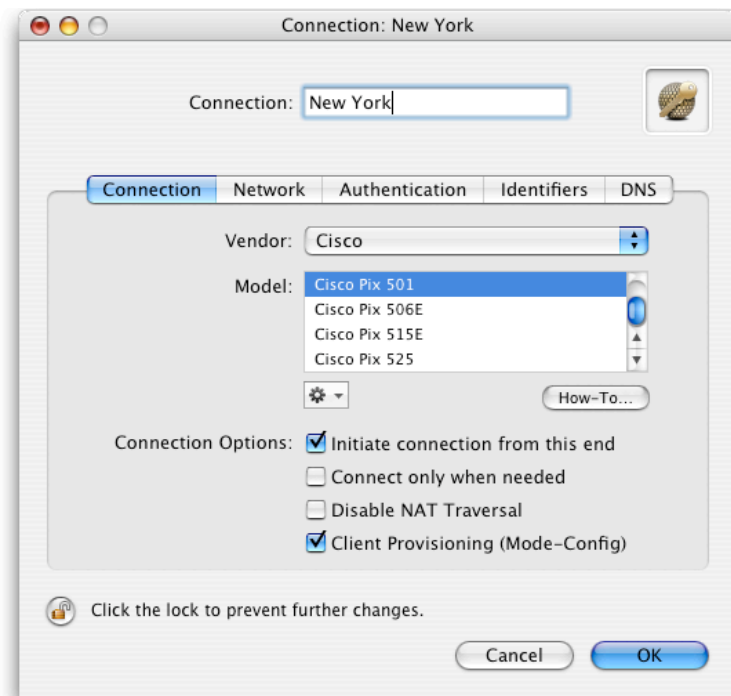


Figure 6: VPN Tracker - Connection Settings

3. Connecting to a Cisco PIX VPN Appliance (multiple user)

Step 2

Change your Network Settings:

- Topology: **Cisco Easy VPN**
- VPN Server Address: public IP address of your VPN Gateway (e.g. **169.1.2.3**)

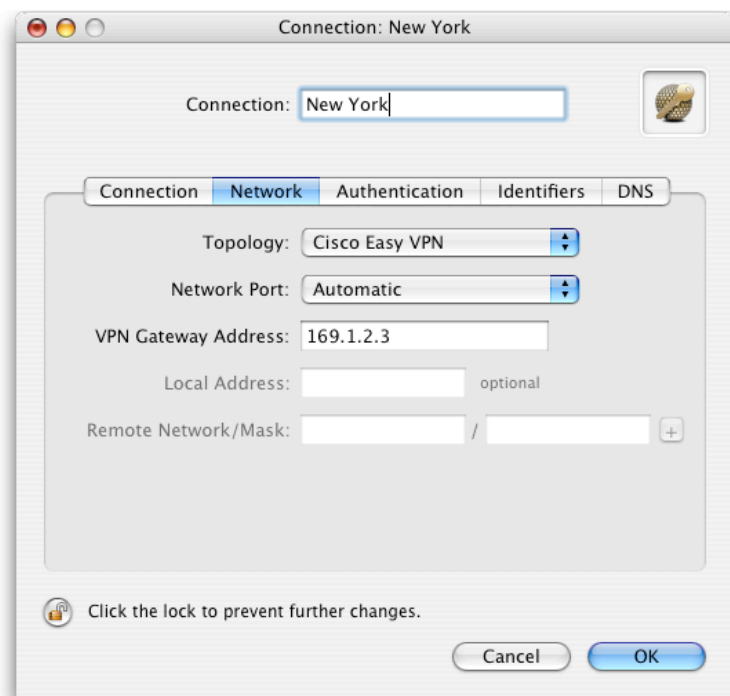


Figure 7: VPN Tracker - Network Settings

Please note: In order to access multiple remote networks simultaneously, just add them by pressing the “+” button.⁵

⁵ For this step VPN Tracker Professional Edition is needed.

3. Connecting to a Cisco PIX VPN Appliance (multiple user)

Step 3

Change your Authentication Settings:

- Pre-shared key: the same Pre-shared key as in your Cisco PIX configuration.
- Enable Extended Authentication (XAUTH): **checked**



Figure 8: VPN Tracker - Authentication Settings

3. Connecting to a Cisco PIX VPN Appliance (multiple user)

Step 4

Identifier Settings:

- Local Identifier: Groupname (e.g. **vpntracker**) and select **Key ID** as type.
- Remote Identifier: Remote endpoint IP address.

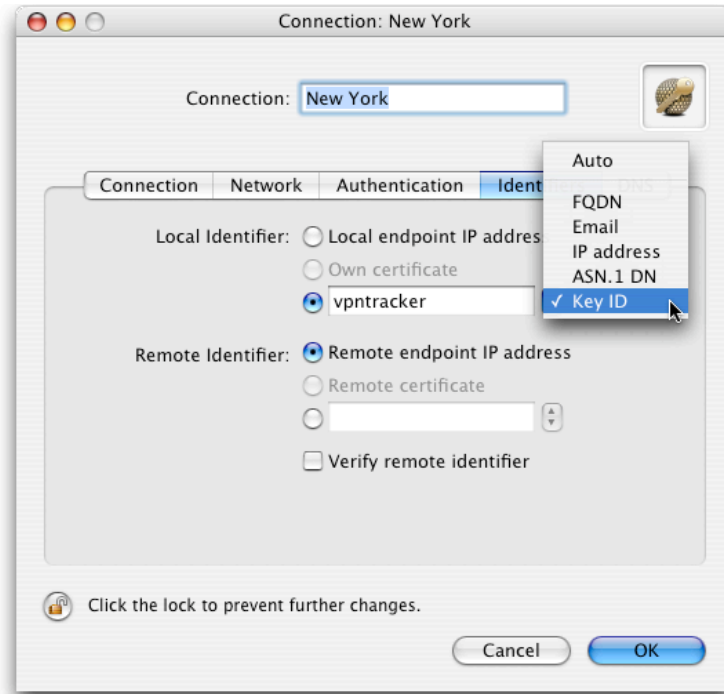


Figure 9: VPN Tracker - Identifier Settings

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

By running following commands you should see statistics of the established VPN tunnel:

```
show crypto isakmp sa
show crypto ipsec sa
```