



VPN Tracker for Mac OS X



How-to:
Interoperability with
Check Point
VPN-1 Gateway

Rev. 3.0

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 Check Point VPN-1 Gateway.

The Check Point Firewall is configured as an Internet Gateway 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 Check Point Firewall. 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.

2. Prerequisites

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

Furthermore you should use a recent Check Point version. Unfortunately, Check Point version 4.1 is **not** supported.

For this document, VPN-1 FP3 and FP4 has been used.

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

For certificate authentication you need a CA with private key, so one VPN Tracker Professional Edition is required in order to sign certificates. Only one VPN Tracker Professional Edition is required, other VPN users can use a Personal Edition. For further information please refer to chapter 3 in the VPN Tracker manual.

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

3. Connecting VPN Tracker to a Check Point Firewall using a Pre-shared Key

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

The Check Point Firewall 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 Check Point use 192.168.1.1 as their default gateway and should have a working Internet connection. The firewall rules are already defined and the VPN connection between the windows clients and the Check Point VPN-1 GateWay works.

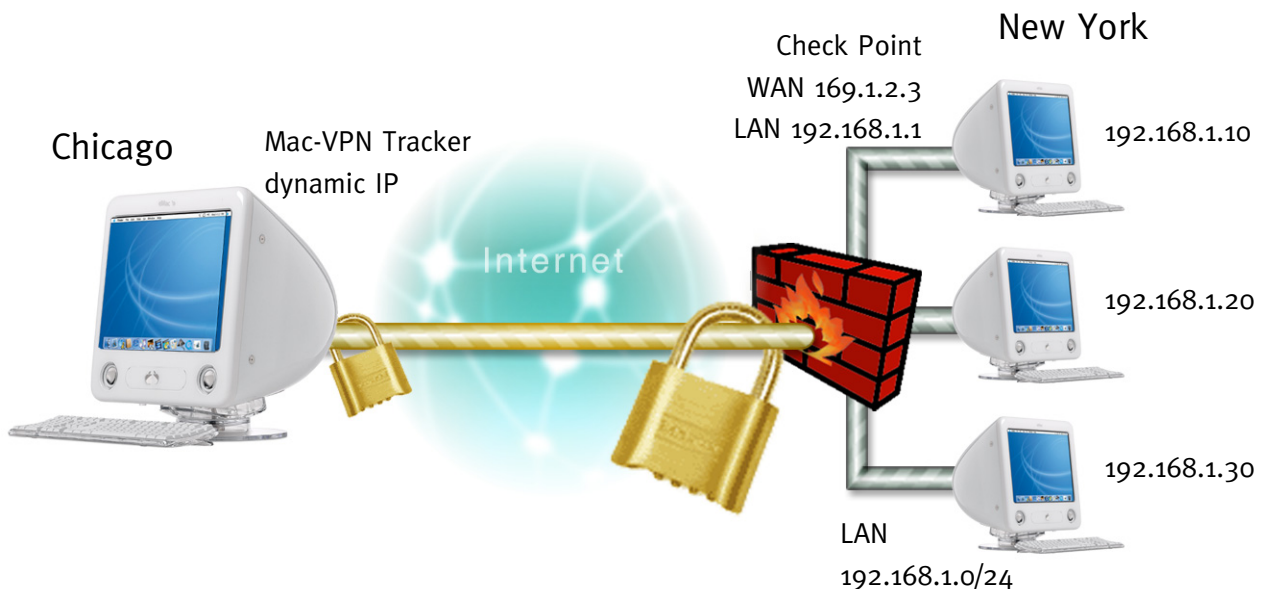


Figure 1: VPN Tracker – Check Point connection diagram

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 Check Point Configuration

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

Step 1

Adjust the VPN - Basic settings:

- Pre-shared Secret: **check**

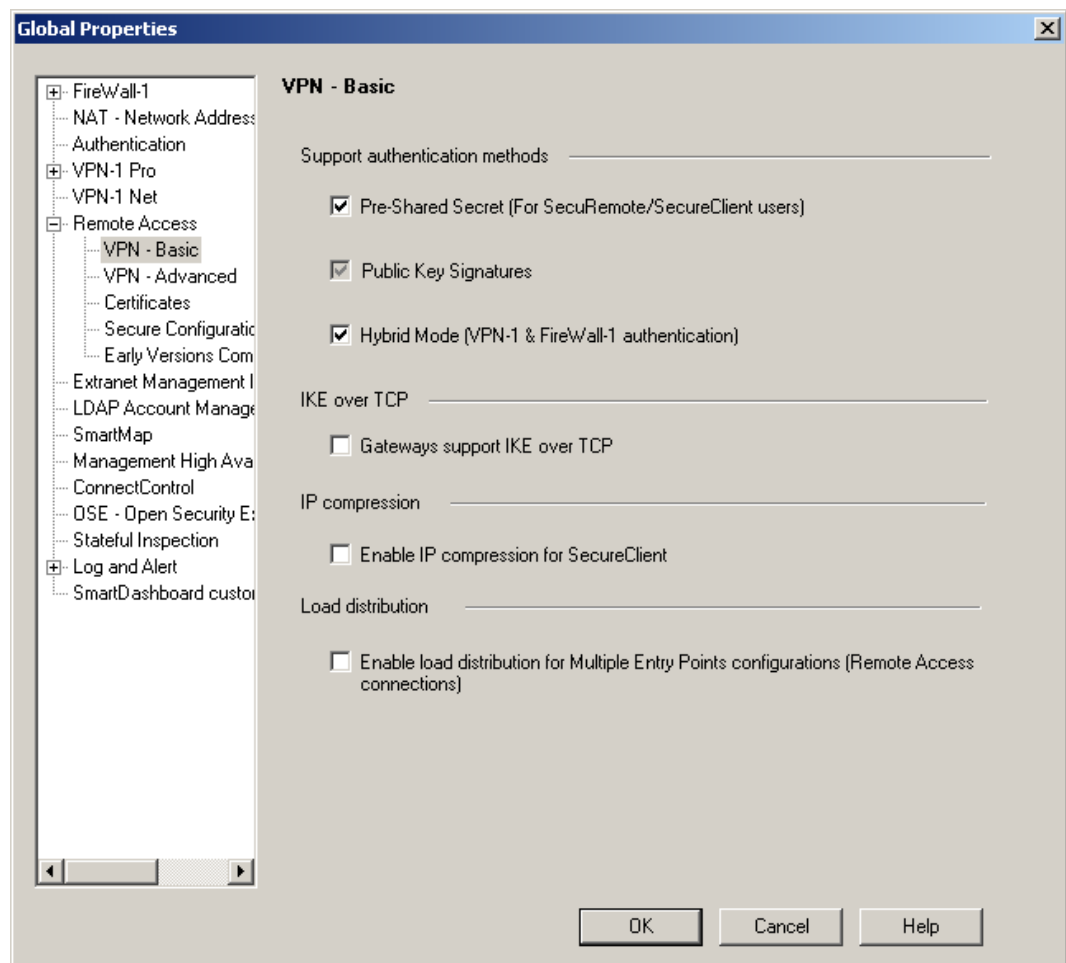


Figure 2: Check Point - VPN - Basic

3. Connecting VPN Tracker to a Check Point Firewall using a Pre-shared Key

Step 2

Adjust the VPN - Advanced settings:

- Encryption Algorithm: **AES-128**
- Data Integrity: **SHA-1**
- Support Diffie-Hellman groups: check **Group 2**

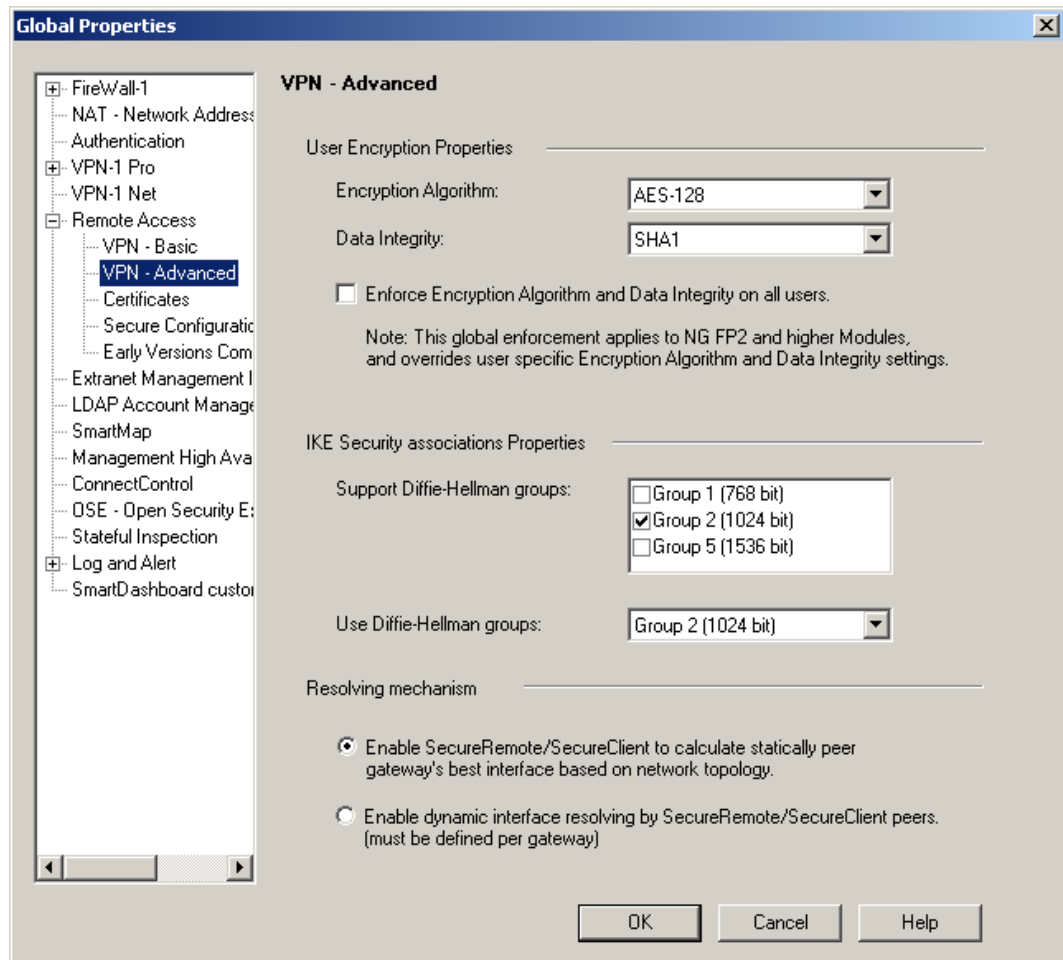


Figure 2: Check Point

3. Connecting VPN Tracker to a Check Point Firewall using a Pre-shared Key

Step 3

Adjust the User Properties:

- Login Name: enter in e-mail address format (e.g. **vpnuser@domain**)

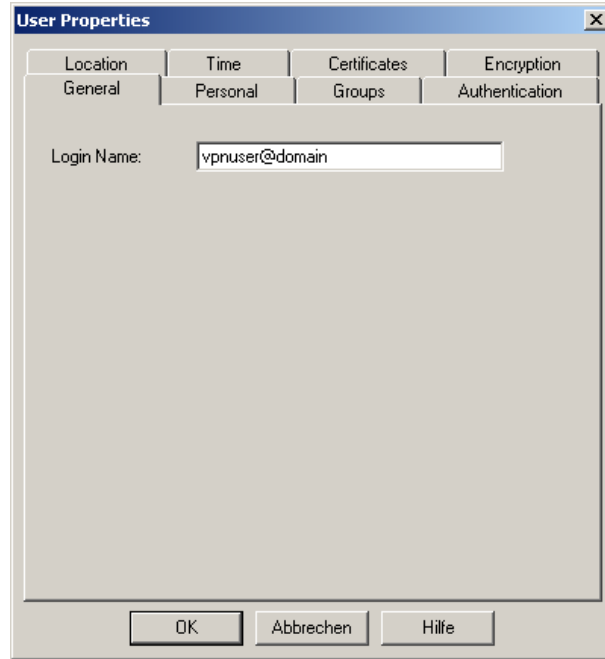


Figure 3: Check Point – User Properties

- Authentication Scheme: **Undefined**

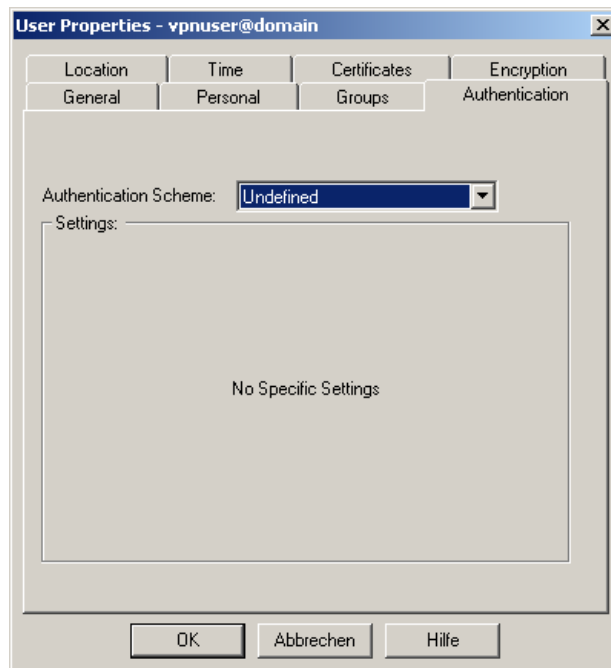


Figure 4: Check Point - User Properties - Authentication

3. Connecting VPN Tracker to a Check Point Firewall using a Pre-shared Key

- Enable the IKE Encryption Method and the Log.

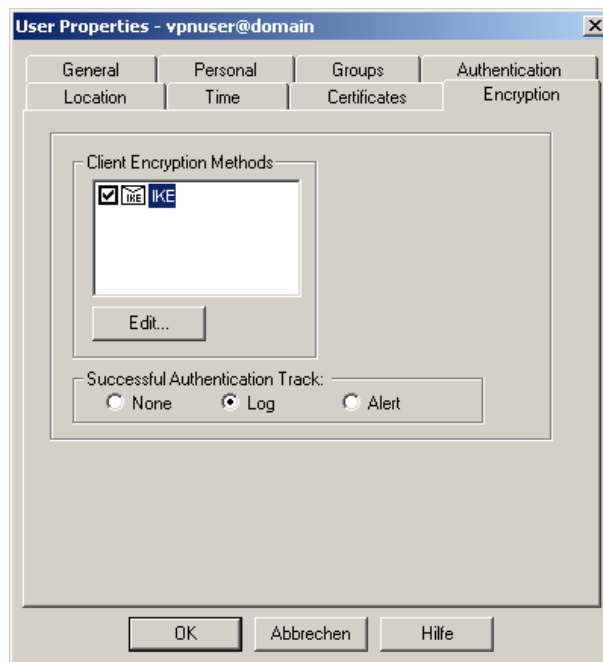


Figure 5: Check Point - User Properties - Encryption

Edit the IKE encryption method:

- Password (Pre-shared secret): the user password (e.g. **presaredkey**)

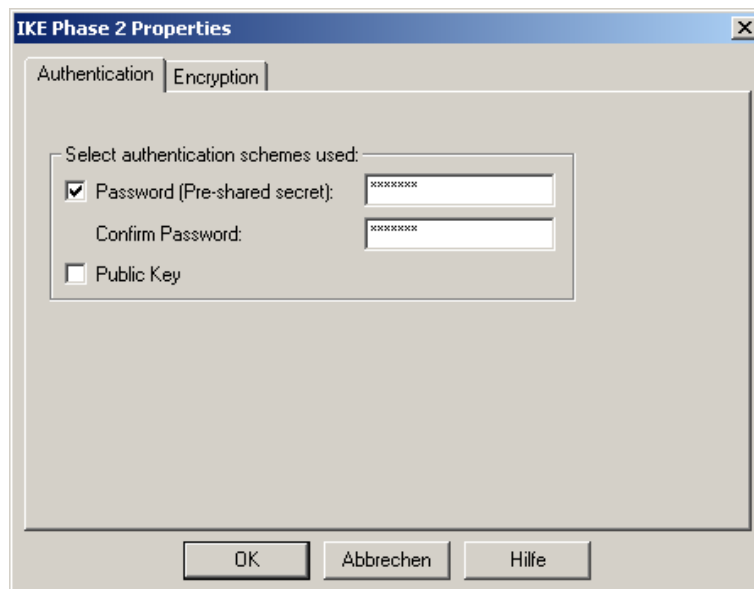


Figure 6: Check Point - IKE Phase 2 Properties

3. Connecting VPN Tracker to a Check Point Firewall using a Pre-shared Key

Step 4

Add user in a RemoteAccess Group.

The screenshots are only an example of adding the previously created user in a group called “RemoteAccessUsers”. You may already have existing Access Groups. We used the following.

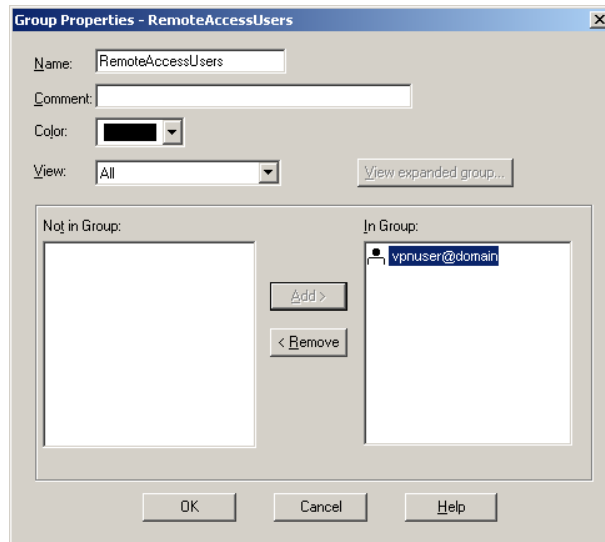


Figure 7: Check Point - Group Properties - RemoteAccessUsers

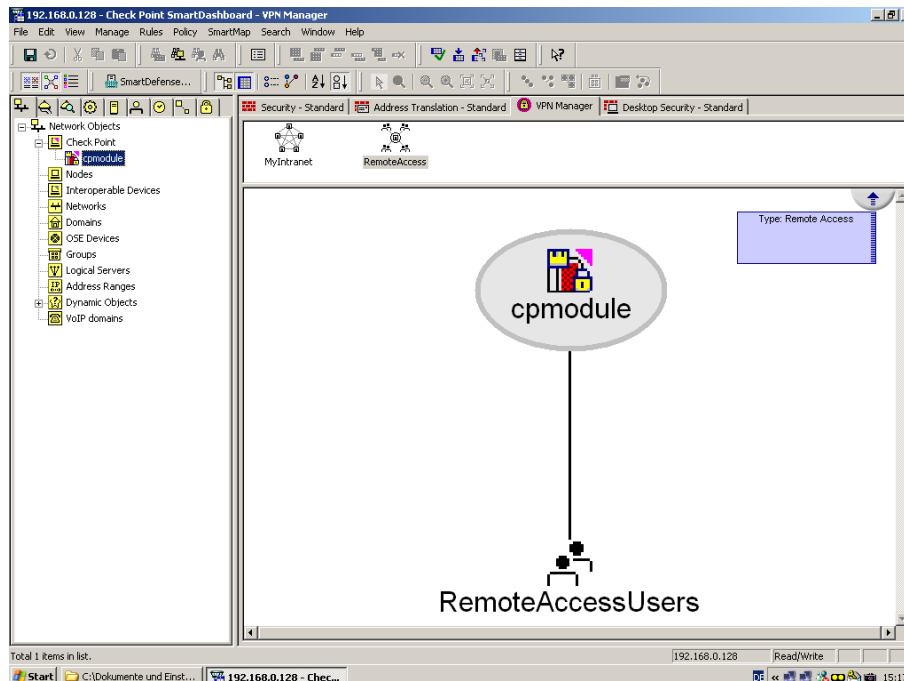


Figure 8: Check Point - Main Screen – cpmodule

3. Connecting VPN Tracker to a Check Point Firewall using a Pre-shared Key

Step 5

Please be sure that the previously created group is in the VPN community. Click on the “Traditional mode configuration” button.

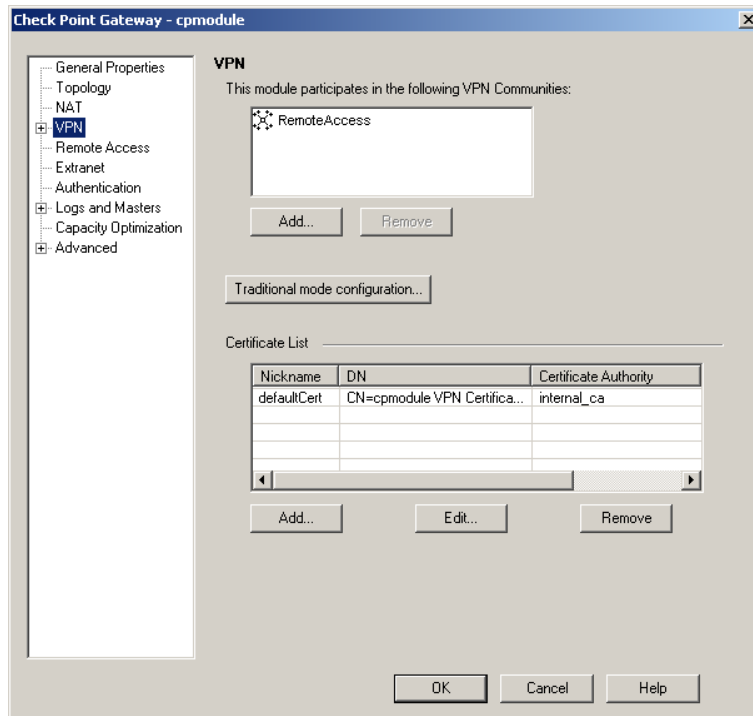


Figure 10: Check Point Gateway - cpmodule

Enable “Pre-Shared Secret” and adjust the advanced settings.

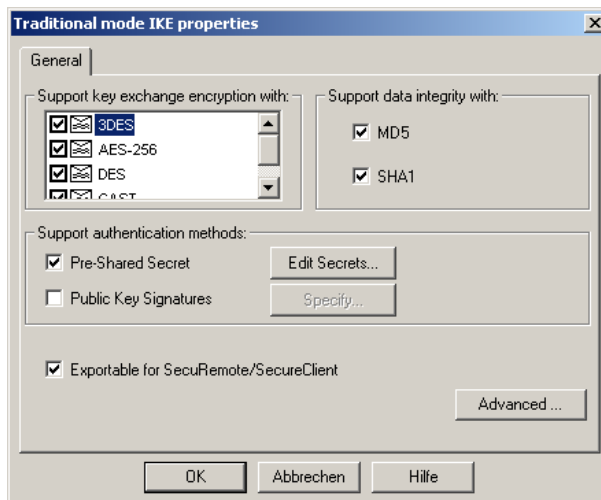


Figure 11: Traditional mode IKE Properties

3. Connecting VPN Tracker to a Check Point Firewall using a Pre-shared Key

Traditional mode advanced IKE properties:

- Support aggressive mode: **enabled**
- Support Diffie-Hellman groups: enable **Group 2**

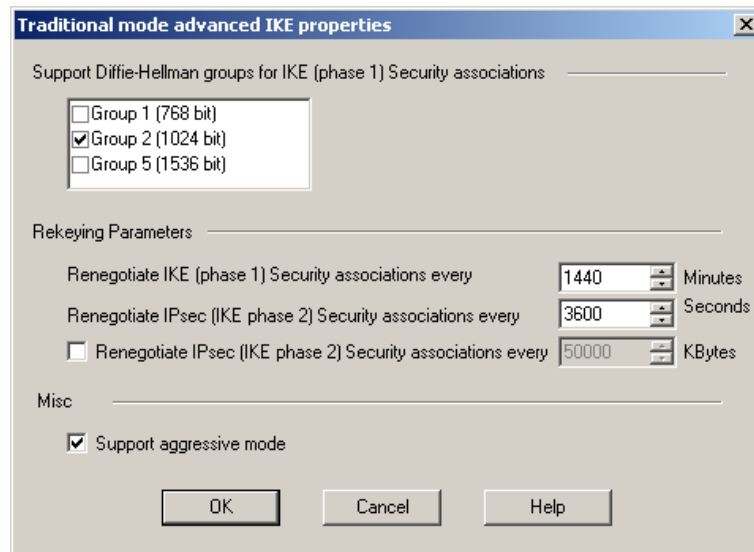


Figure 12: Traditional mode advanced IKE properties

❖ Multiple VPN Tracker Hosts

To create another user with the same settings, please repeat step 3-4.

3. Connecting VPN Tracker to a Check Point Firewall using a Pre-shared Key

3.2 VPN Tracker Configuration

Step 1

Add a new connection with the following options:

- Vendor: „Check Point“
- Model: your Check Point Software version

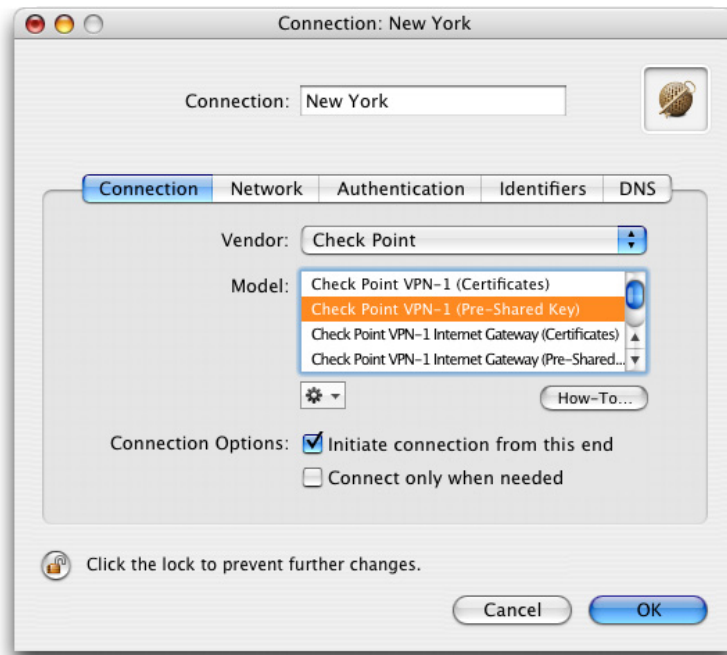


Figure 13: VPN Tracker - Connection settings

3. Connecting VPN Tracker to a Check Point Firewall using a Pre-shared Key

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**).

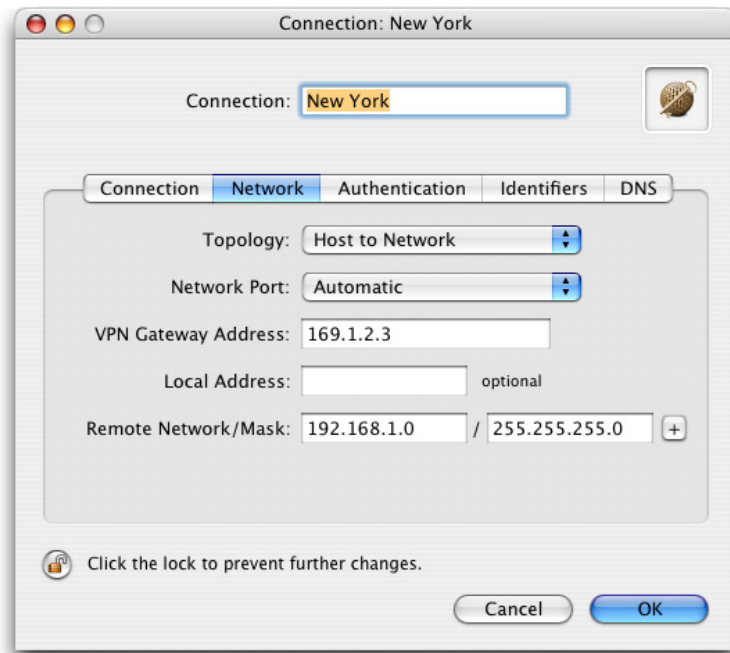


Figure 14: VPN Tracker – Network settings

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.

3. Connecting VPN Tracker to a Check Point Firewall using a Pre-shared Key

Step 3

Change your Authentication Settings:

- Pre-shared key: the same Pre-shared key as in the Check Point configuration.

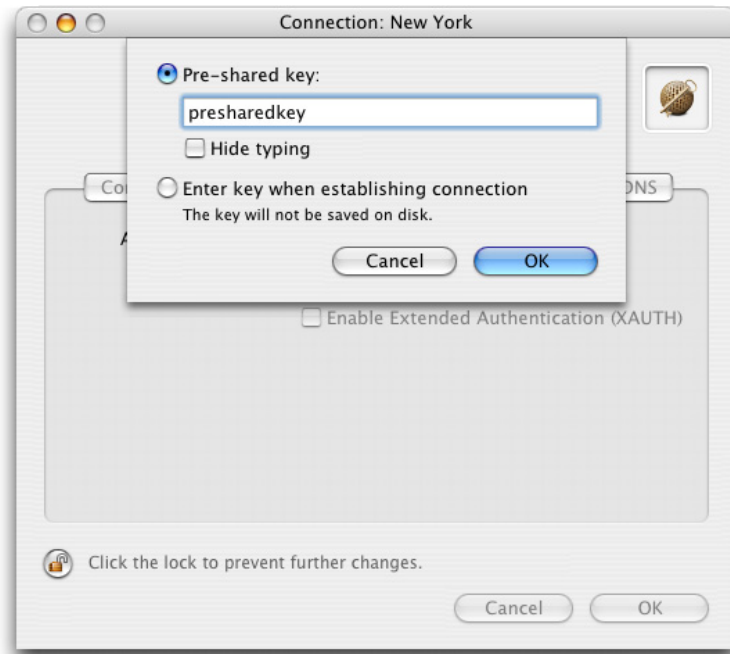


Figure 15: VPN Tracker - Authentication settings

3. Connecting VPN Tracker to a Check Point Firewall using a Pre-shared Key

Step 4

Identifier Settings:

- Local Identifier: your username (e.g. `vpnuser@example.com`).
- Remote Identifier: Remote endpoint IP address.



Figure 9: VPN Tracker - Identifier settings

Please note: If you have typed in a correct username, the word "email" should be visible beside the input field. Starting with VPN Tracker version 2.0.5 you can use a username in the form "vpntracker" but you have to type in "@vpntracker" as local identifier. An identifier of the form "@user" will be interpreted as "user" with a type of "email" (User-FQDN). This is to help all Check Point users who have usernames without an "@" in them, as Check Point always expects a User-FQDN identifier.

3. Connecting VPN Tracker to a Check Point Firewall using a Pre-shared Key

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 Check Point. 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 Check Point network from the dialed-in Mac in the "Terminal" utility:

```
ping 192.168.1.10
```

4. Connecting VPN Tracker Host to Check Point Firewall using Certificates

4.1 Check Point Configuration

Step 1 Please refer to section 3.1.

Step 2 User Properties:

- Please enter an Identifier in the form **certificateUser**

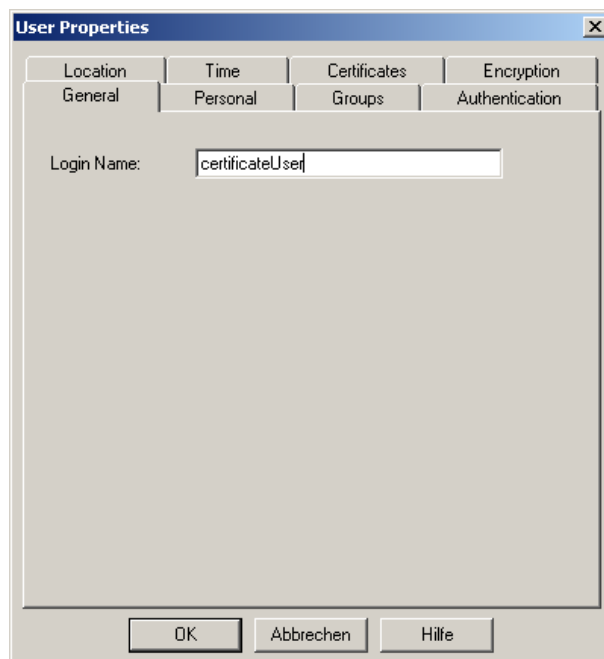


Figure 10: Check Point - User Properties - General

4. Connecting VPN Tracker Host to Check Point Firewall using Certificates

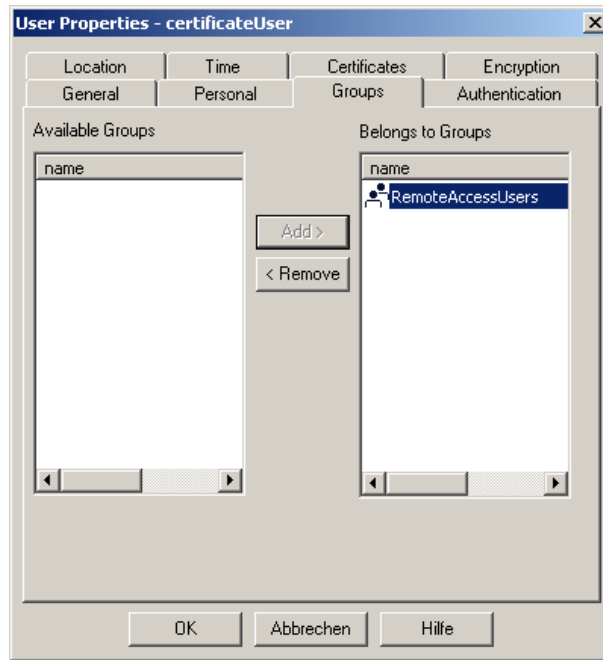


Figure 11: Check Point - User Properties - Groups

Generate and save the certificate. The PKCS#12 file contains the certificate, your private key and the CA.

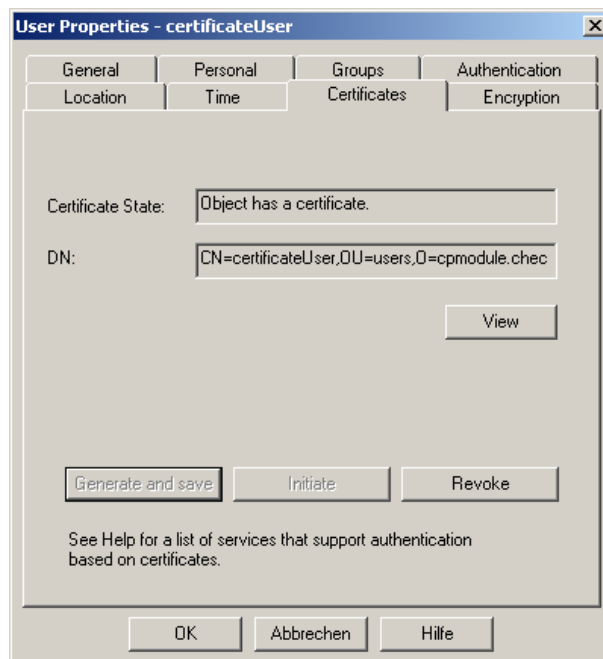


Figure 12: user Properties - Certificates

4. Connecting VPN Tracker Host to Check Point Firewall using Certificates

Please be sure that you enable the “Public Key” Authentication” in the IKE Phase 2 Properties.

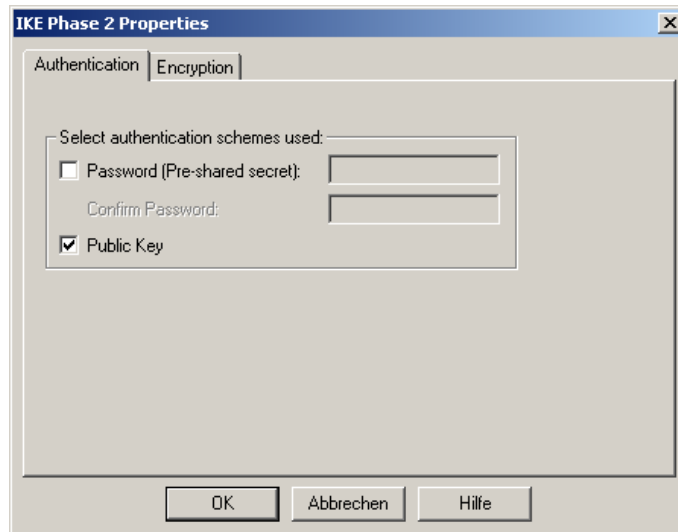


Figure 13: IKE Phase 2 Properties

Step 4

Tradition mode IKE properties:

Please enable the “Public key Signatures”. You can leave the “Pre-Shared Secrets” enabled.

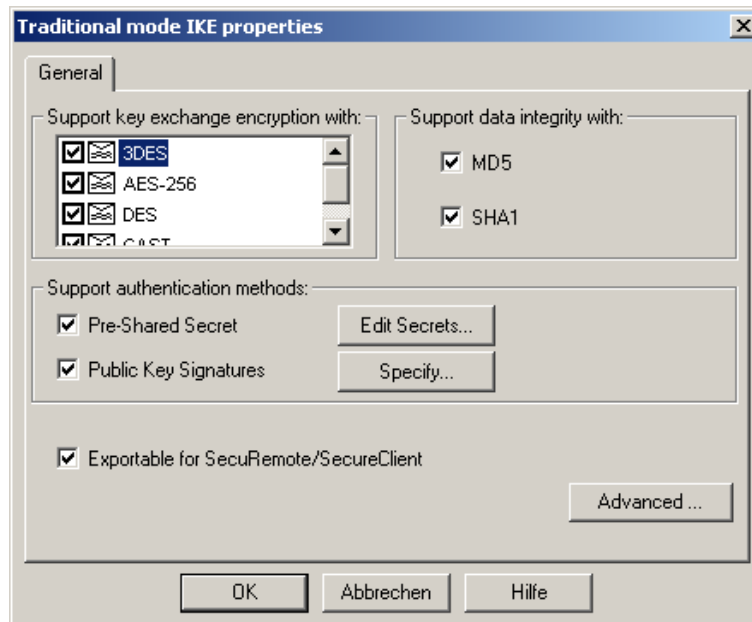


Figure 14: Check Point - Traditional mode IKE properties

4.2 VPN Tracker Configuration

Step 1

Go to the VPN Tracker certificate manager (⌘ + “E”) and import the PKCS#12 file you’ve previously exported.

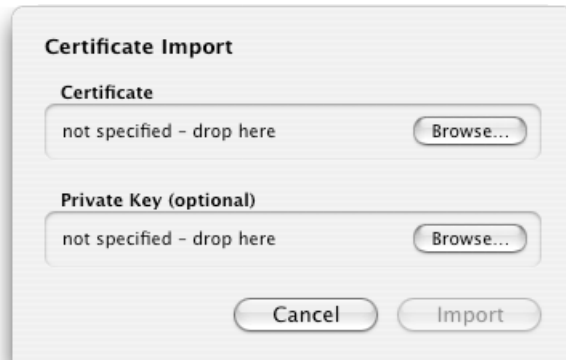


Figure 15: VPN Tracker - Certificate Import

Step 2-3

Please refer to section 3.2 step 1-2.

Step 4

Change your Authentication Settings:

- Own Certificate: imported certificate from step 1
- Remote Certificate: **Verify with CA's**

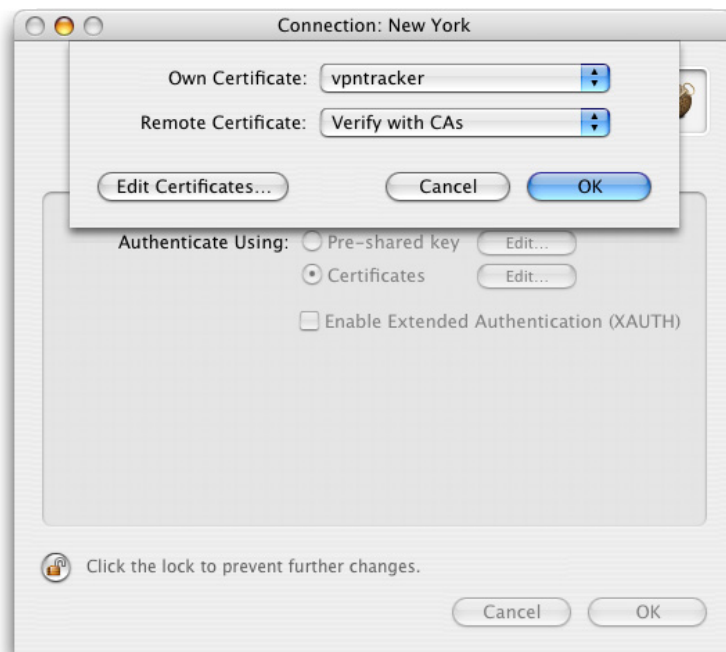


Figure 16: VPN Tracker - Authentication Settings

4. Connecting VPN Tracker Host to Check Point Firewall using Certificates

Step 5

Change your Identifier Settings:

- Local Identifier: **Own Certificate**
- Remote Identifier: Remote endpoint IP address
- Verify remote identifier: **unchecked**



Figure 17: VPN Tracker - Identifier Settings

Step 6

Please refer to section 3.2 step 5.