



VPN Tracker for Mac OS X



How-to: Interoperability with F-Secure VPN+ gateway

Rev. 1.0

Copyright © 2003 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 F-Secure VPN+ gateway. equinix has tested the F-Secure VPN+ under Windows 2000.

The F-Secure VPN+ gateway 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 F-Secure VPN+ gateway.

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

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

Firstly, you should use a recent software version.

For this document, F-Secure VPN+ version 5.43 and F-Secure Management Agent 5.02 have 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 F-Secure VPN+ gateway you need a Personal License.
- If you want to establish a LAN-to-LAN connection from your Mac to the F-Secure VPN+ gateway, you need a VPN Tracker Professional License.
- If you connect a dial-in Mac without it's own subnet to multiple Networks on F-Secure side you also need the Professional License.

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

Be sure to use VPN Tracker 2.0.6 or higher.¹ For this document VPN Tracker version 2.0.6 has been used.

¹ All VPN Tracker versions prior to 2.0.6 did not include a connection type for F-Secure VPN+.

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

In this example, the Mac running VPN Tracker is directly connected to the Internet via a dialup or PPP connection.² The F-Secure VPN+ gateway 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 F-Secure VPN+ gateway 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 F-Secure VPN+ gateway works.

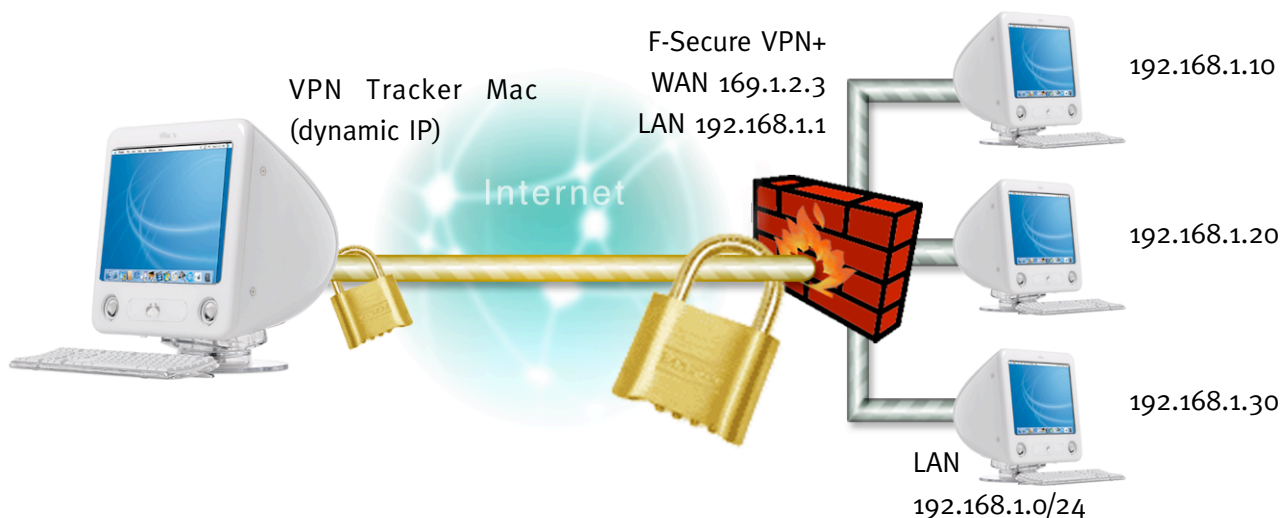


Figure 1: VPN Tracker - F-Secure VPN+ gateway connection diagram (host to network)

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.

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

3.1 F-Secure VPN+ gateway configuration

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

Step 1

New Policy Domain:

Please create a new Policy Domain with name “VPN Tracker PSK”.

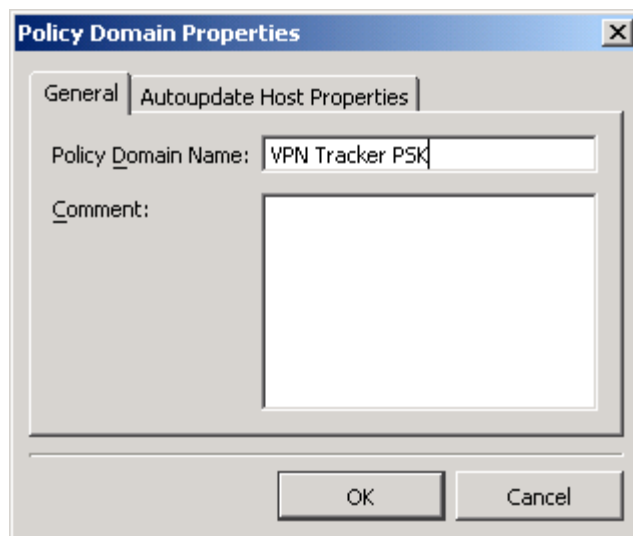


Figure 2: Policy Domain

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

Step 2

VPN – Advanced Setup:

Create a “New host” in the previously created Policy Group.

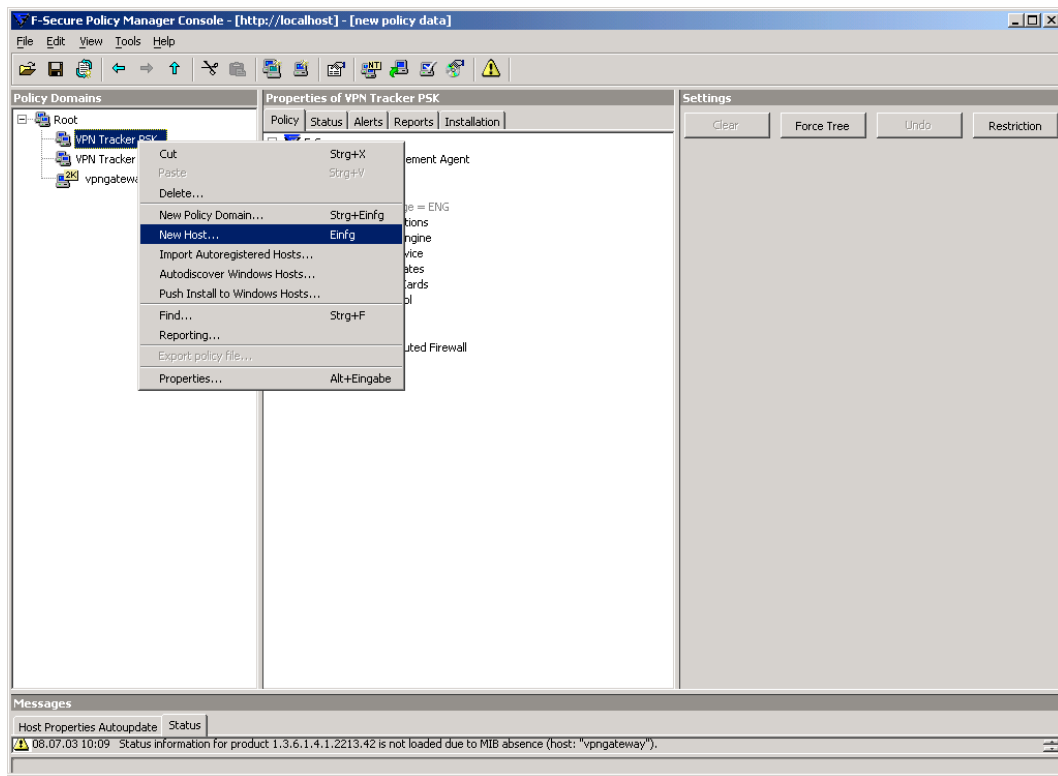
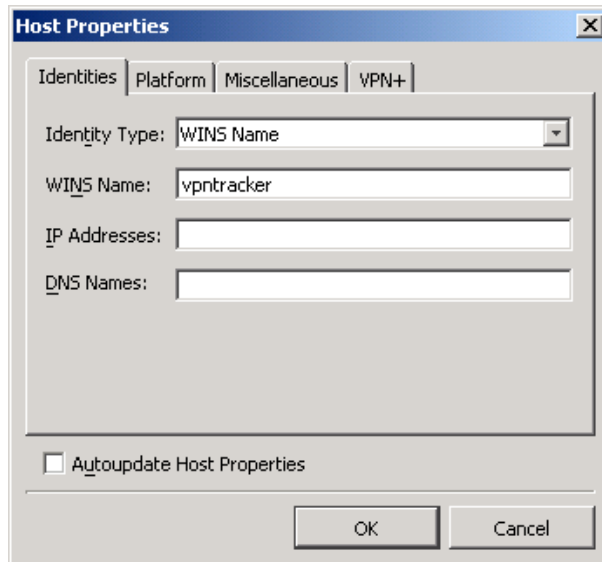


Figure 3: New Host

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

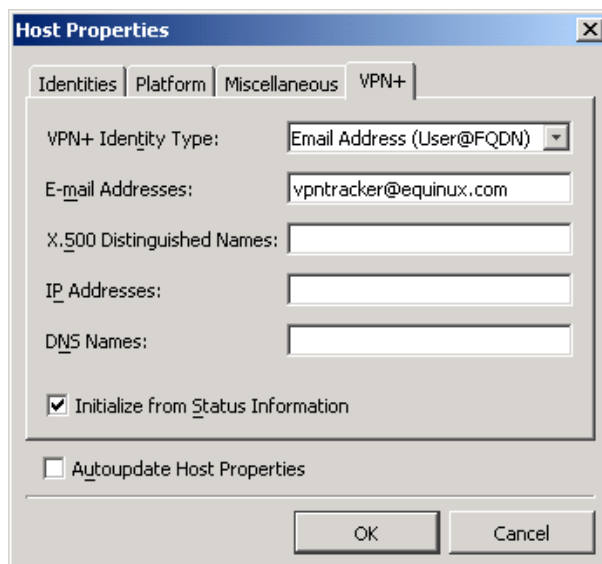
Enter an arbitrary „WINS Name“. This name will appear on the F-Secure management console.



The screenshot shows the 'Host Properties' dialog box with the 'Identities' tab selected. The 'Identity Type' dropdown is set to 'WINS Name'. The 'WINS Name' text box contains the value 'vpntracker'. Below it are empty text boxes for 'IP Addresses' and 'DNS Names'. At the bottom, there is an unchecked checkbox for 'Autoupdate Host Properties' and 'OK' and 'Cancel' buttons.

Figure 4: F-Secure VPN+ - Host Properties - Identities

Please select “Email Address (User@FQDN)” as “VPN+ Identity Type” in tab “VPN+” and enter an email Address in the form user@domain.



The screenshot shows the 'Host Properties' dialog box with the 'VPN+' tab selected. The 'VPN+ Identity Type' dropdown is set to 'Email Address (User@FQDN)'. The 'E-mail Addresses' text box contains the value 'vpntracker@equinux.com'. Below it are empty text boxes for 'X.500 Distinguished Names', 'IP Addresses', and 'DNS Names'. There is a checked checkbox for 'Initialize from Status Information' and an unchecked checkbox for 'Autoupdate Host Properties'. 'OK' and 'Cancel' buttons are at the bottom.

Figure 5: F-Secure VPN+ - Host Properties - VPN+

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

Step 3

New Connection Template Wizard:

Start the “New Connection Template Wizard” and select “VPN+ Connection”.

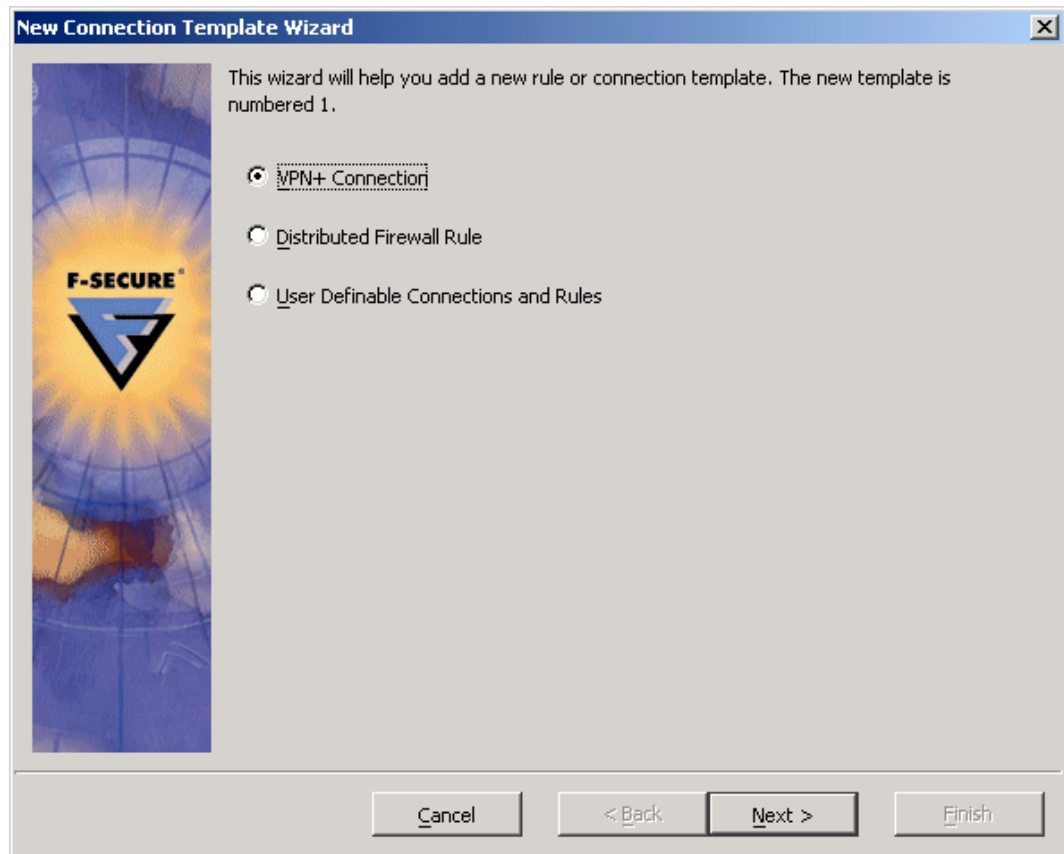


Figure 6: New Connection Template Wizard – Template

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

The Endpoint type is „Host to Gateway“.

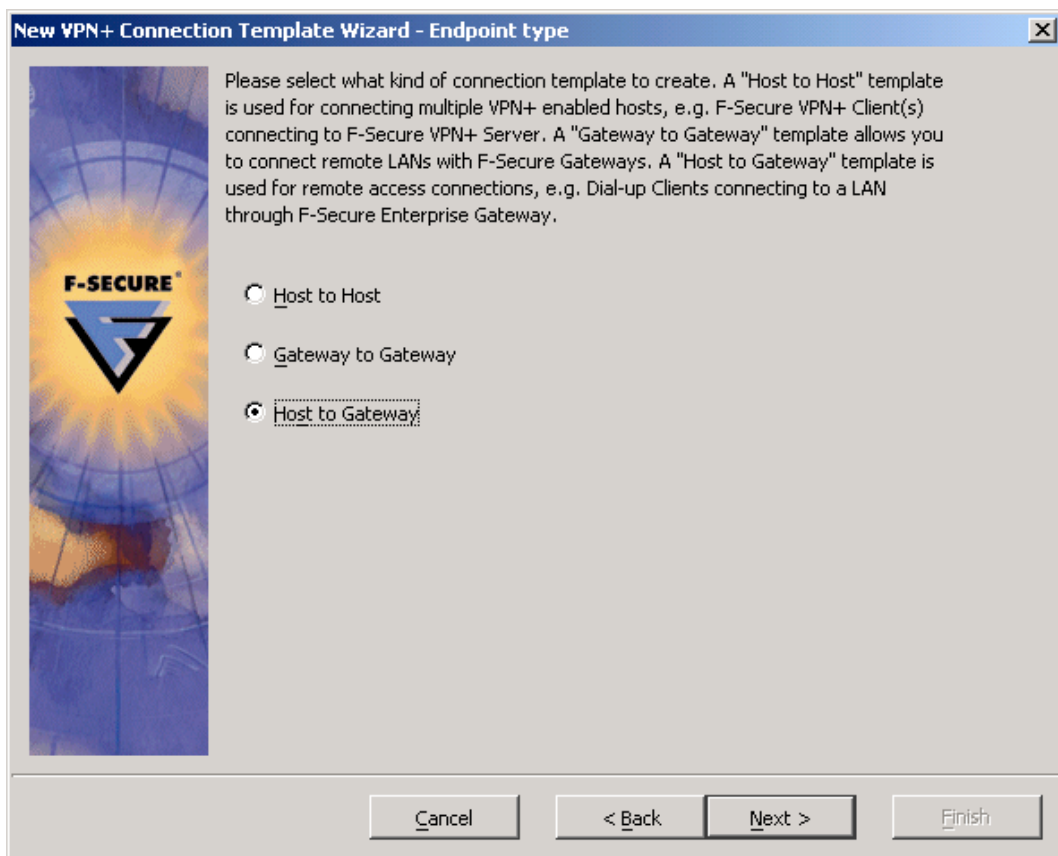


Figure 7: New Connection Template Wizard – Endpoint type

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

Select „IPsec“ for this connection.

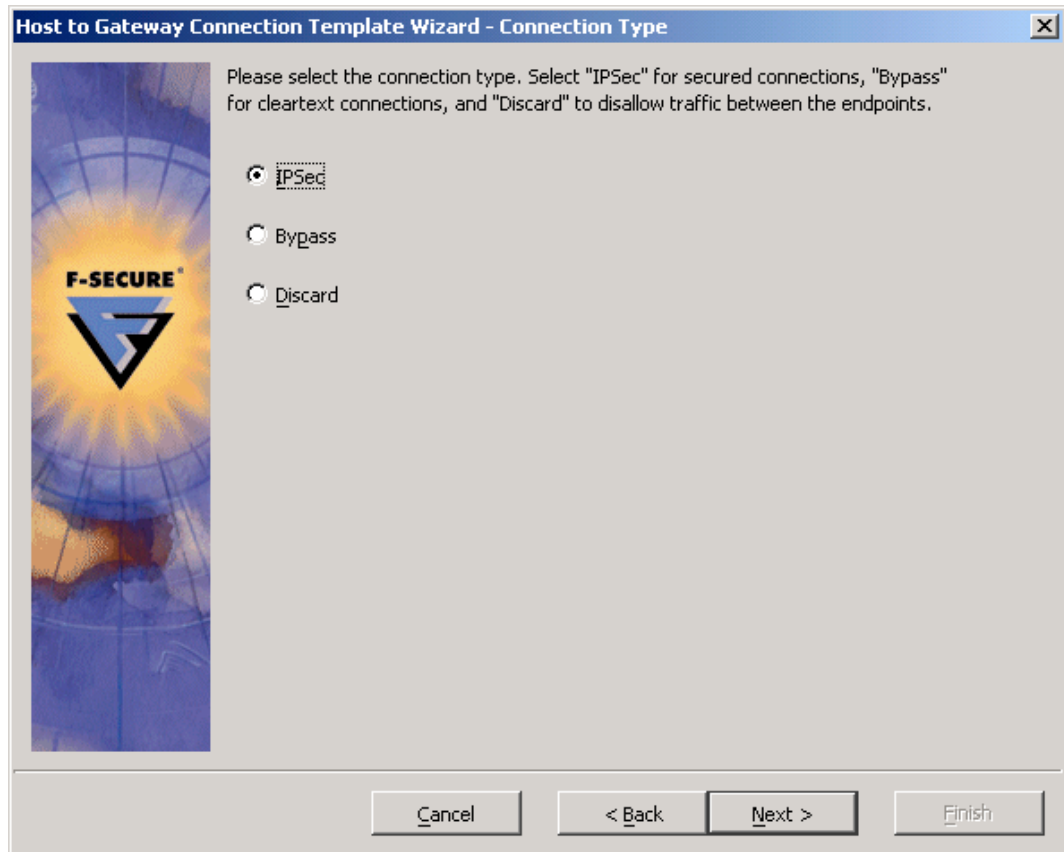


Figure 8: New Connection Template Wizard – Connection Type

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

Please don't use a "Smartcard authentication". Click on the "..." button to select the endpoint.

Host to Gateway Connection Template Wizard - Host Endpoint

Specify the host endpoint. You can select any policy domain or host to be the endpoint. Alternatively, you can specify the host endpoint as an IP address or DNS name. IP address can be a host IP address (e.g. 192.168.100.100), a network (e.g. 192.168.100.0/24), or a range of IP addresses (e.g. 192.168.100.1-192.168.100.10). If you want to use smartcard-based user authentication for remote access, please fill in the organizational information for smartcard users. Empty fields are treated as wildcards. With smartcard authentication, the use of a policy domain as host endpoint is recommended.

Smartcard authentication

Country: Don't care

Organization:

Organization Unit:

Common Name:

Additional Fields:

Host Endpoint: vpntracker

Cancel < Back Next > Finish

Figure 9: New Connection Template Wizard – Host Endpoint

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

Select the host “vpntracker” which was created in step 2.

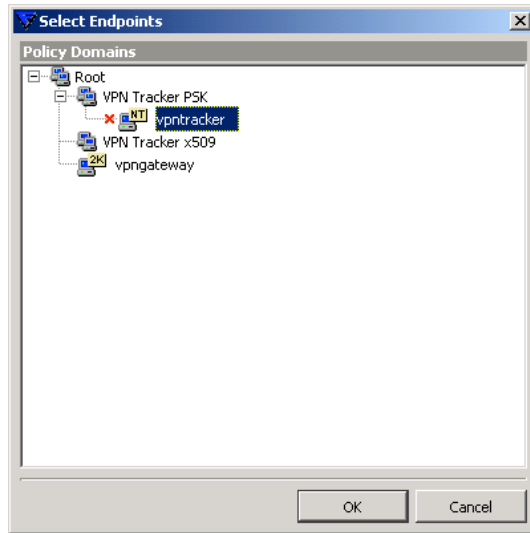


Figure 10: Select Endpoints

Select the “vpngateway”, this is the F-Secure VPN+ side endpoint. Enter the official IP address of your router in the field identity and the network address of your local network on the F-Secure VPN+ side.

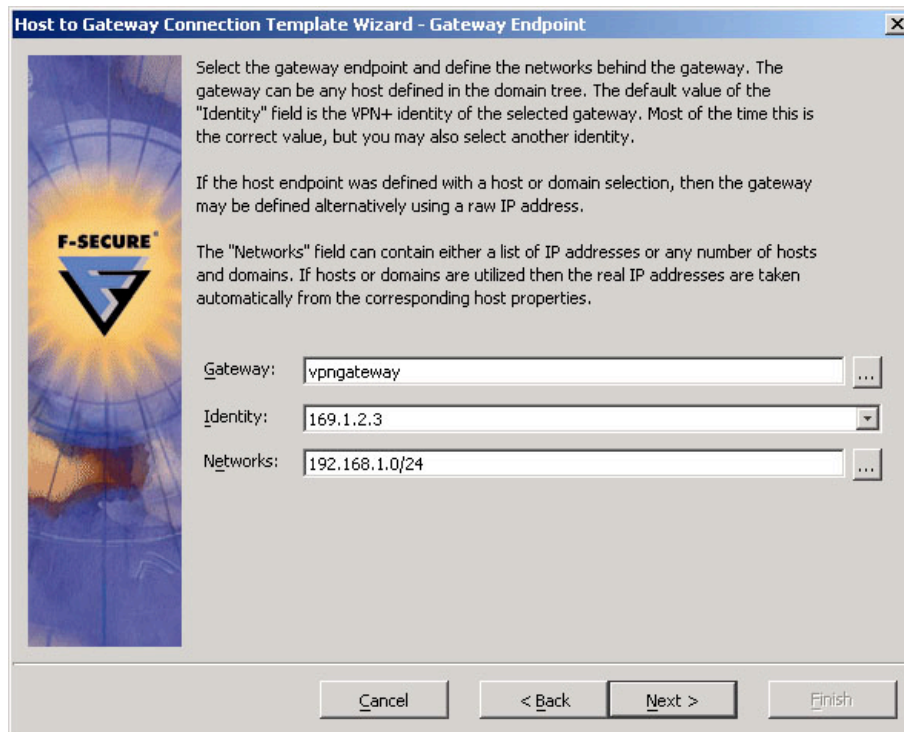
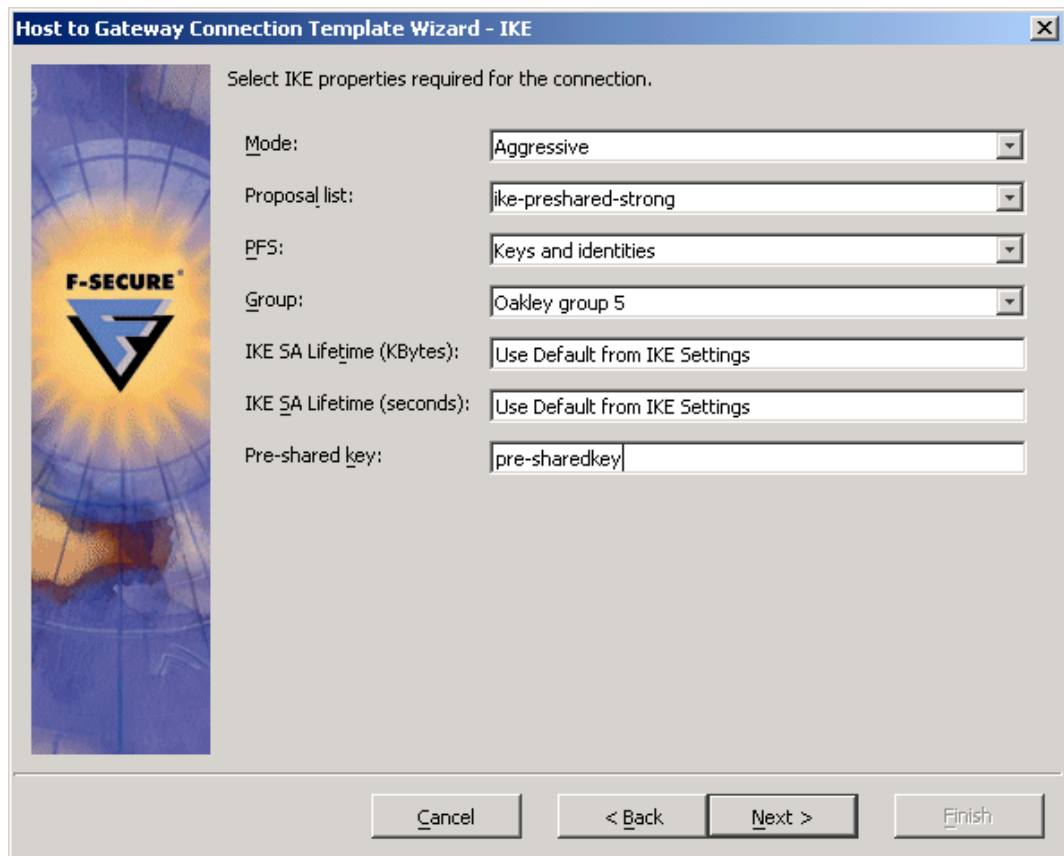


Figure 11: New Connection Template Wizard – Gateway Endpoint

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

Select the IKE properties exactly as shown on the next screenshot. The pre-defined connection type in VPN tracker uses these settings. Finally enter your pre-shared key (password) in the field “Pre-shared key”.



The screenshot shows a dialog box titled "Host to Gateway Connection Template Wizard - IKE". The dialog contains a vertical banner on the left with the F-SECURE logo and a globe. The main area is titled "Select IKE properties required for the connection." and contains the following fields:

| | |
|----------------------------|-------------------------------|
| Mode: | Aggressive |
| Proposal list: | ike-preshared-strong |
| PFS: | Keys and identities |
| Group: | Oakley group 5 |
| IKE SA Lifetime (KBytes): | Use Default from IKE Settings |
| IKE SA Lifetime (seconds): | Use Default from IKE Settings |
| Pre-shared key: | pre-sharedkey |

At the bottom of the dialog are four buttons: "Cancel", "< Back", "Next >", and "Finish".

Figure 12: New Connection Template Wizard - IKE properties

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

Please select “esp-tunnel-strong” as proposal list and disable the “Keep IPsec SA alive” feature.

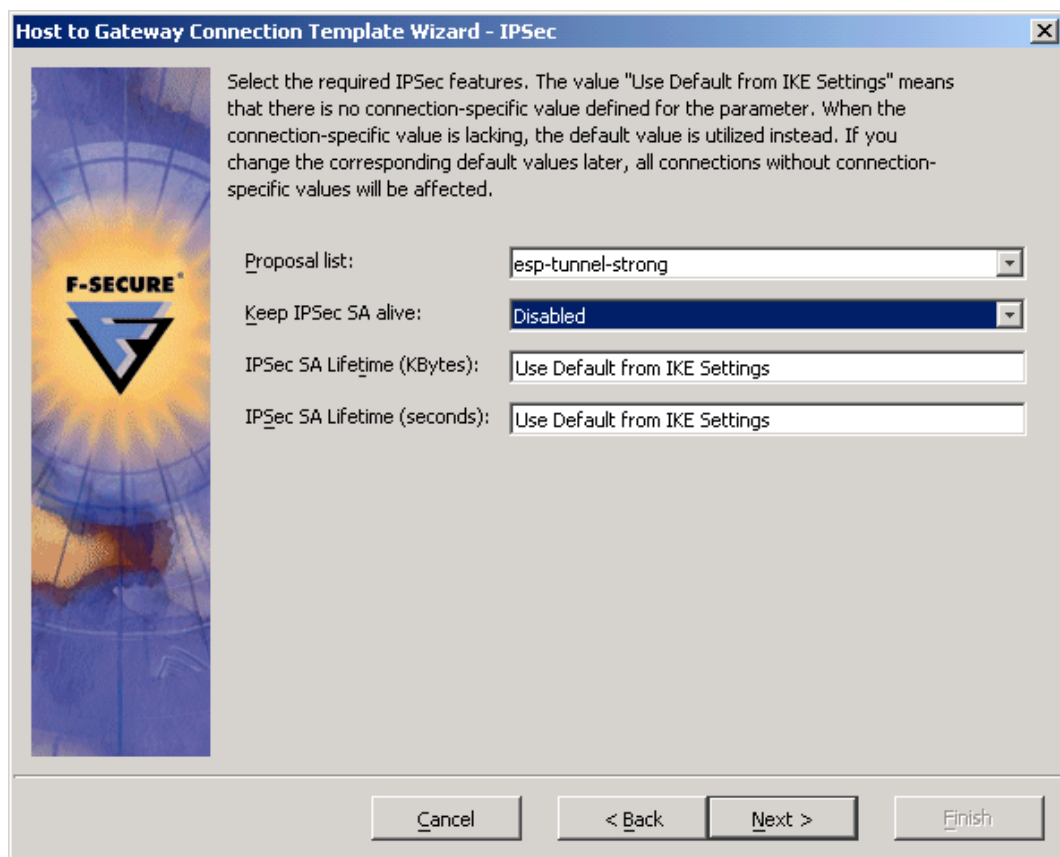


Figure 13: New Connection Template Wizard - IPsec

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

Here you can specify services here. We selected “include all traffic“. You may change it if you need to.

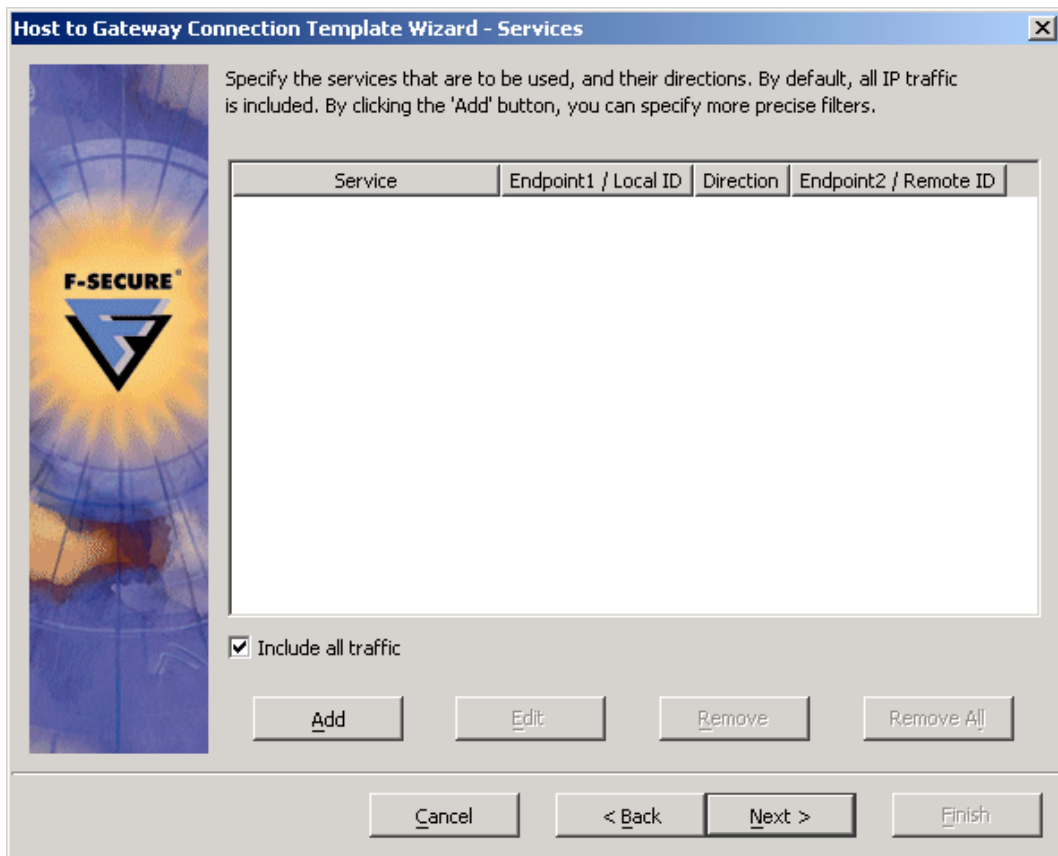


Figure 14: New Connection Template Wizard – Services

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

We didn't use flags in this scenario, but you can specify one if you wish.

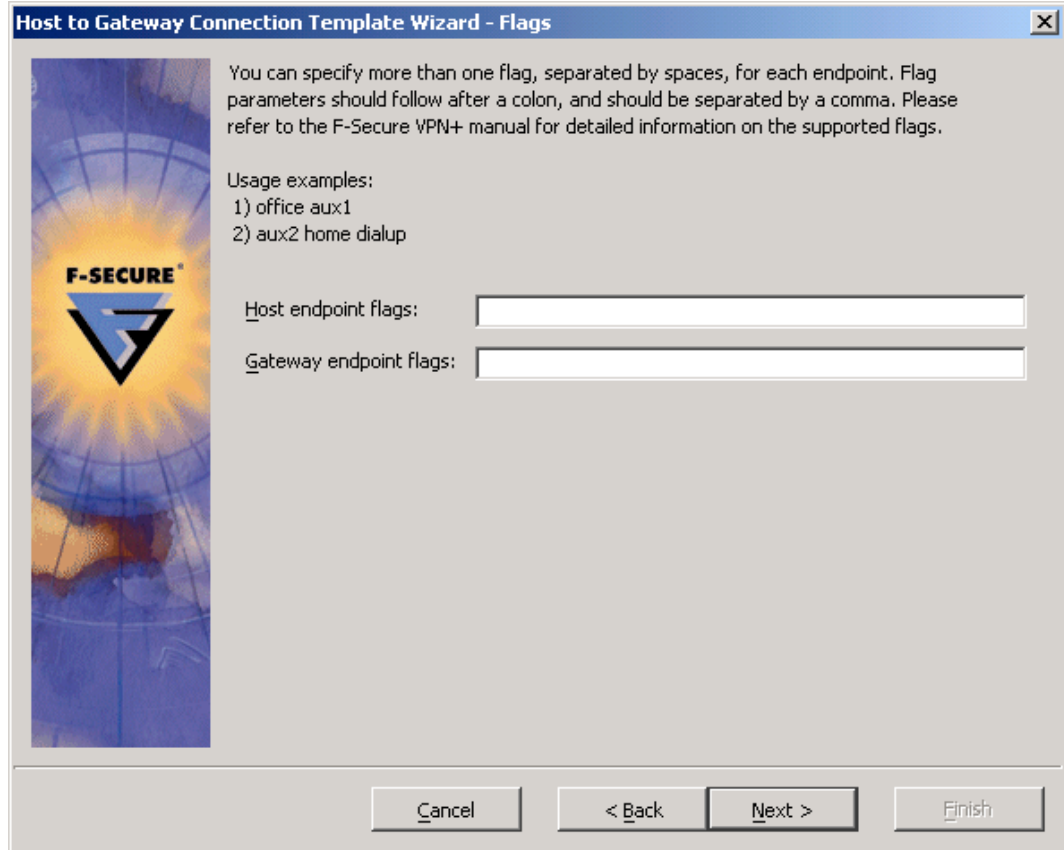


Figure 15: New Connection Template Wizard – Flags

The last step of the “Connection Template Wizard” shows you a summary of all your settings. Please check these settings once again.

Please note: You have to save and “distribute” all changes, every time you change the configuration.

❖ Multiple VPN Tracker Hosts

Just create another host with a different email address.

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

3.2 VPN Tracker configuration

Step 1

Add a new connection with the following options: Choose “F-Secure VPN+ gateway” 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).

The screenshot shows the 'VPN Tracker' configuration dialog box. It is divided into three main sections: General, Networking, and Authentication. In the 'General' section, the 'Name' field is set to 'F-secure PSK', the 'Connection Type' is 'F-Secure VPN+', and the 'Initiate connection' checkbox is checked. The 'Networking' section shows 'Topology' set to 'Host to Network', 'Local Endpoint' set to 'Default Interface', 'Remote Endpoint' set to '169.1.2.3', 'Local Host' is empty with 'optional' text, and 'Remote Network' set to '192.168.13.0 / 24'. The 'Authentication' section has 'Pre-shared key' selected with an 'Edit...' button, and 'Certificates' is unselected with an 'Edit...' button. At the bottom, there is a lock icon with the text 'Click the lock to prevent further changes.', and 'Cancel' and 'Save' buttons.

Figure 16: VPN Tracker main dialog (with PSK)

3. Connecting to a F-Secure VPN+ using Pre-shared secrets

Step 2

Click select “Pre-shared key“ and click “Edit...”. Type in the same pre-shared secret that you typed-in in the F-Secure VPN+ gateway configuration (Figure 2). Use the “VPN+ email address” as local identifier (Step 2). If you have typed in a correct local identifier, the word "Email" should be visible beside the input field.

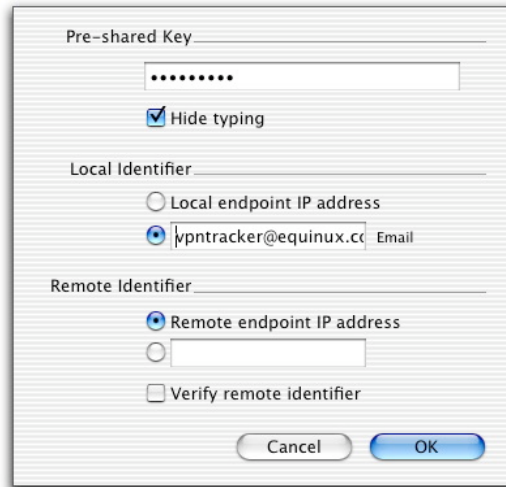


Figure 17: Pre-shared key dialog

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 F-Secure VPN+ gateway. 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 F-Secure VPN+ gateway 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.

4. Connecting to a F-Secure VPN+ gateway using RSA X.509 certificates

4.1 F-Secure VPN+ gateway configuration

Step 1

New Policy Domain:

Please create a new Policy Domain with name “VPN Tracker x509”.

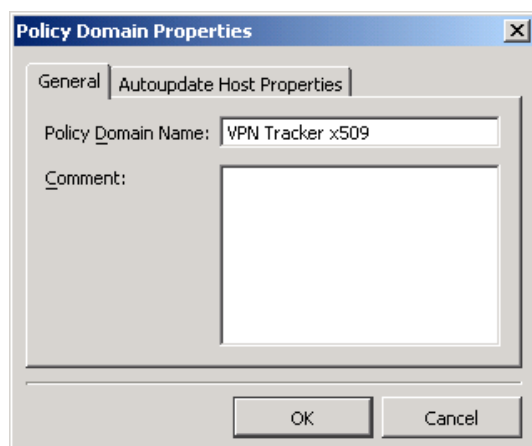


Figure 18: Policy Domain

4. Connecting to a F-Secure VPN+ gateway using RSA X.509 certificates

Step 2

VPN – Advanced Setup:

Create a “New host” in the previously created Policy Group. In tab “identities” enter an arbitrary “WINS Name“. This name will appear on the F-Secure management Console. In tab “VPN+” please select “X.500 Distinguished Name” as “VPN+ Identity Type” and enter an email Address in the field “X.500 Distinguished Names”. This field refers to the “Subject Alternative Name” in the VPN Tracker Certificate request.

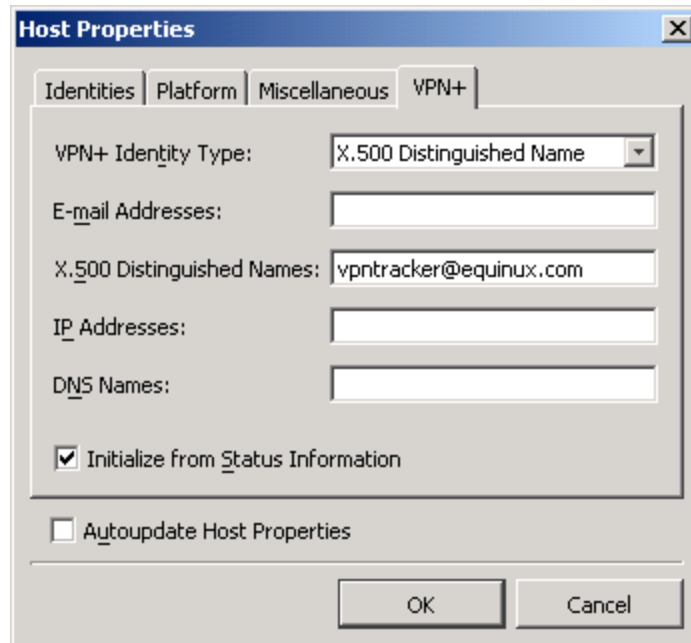


Figure 19: Host Properties - X.509

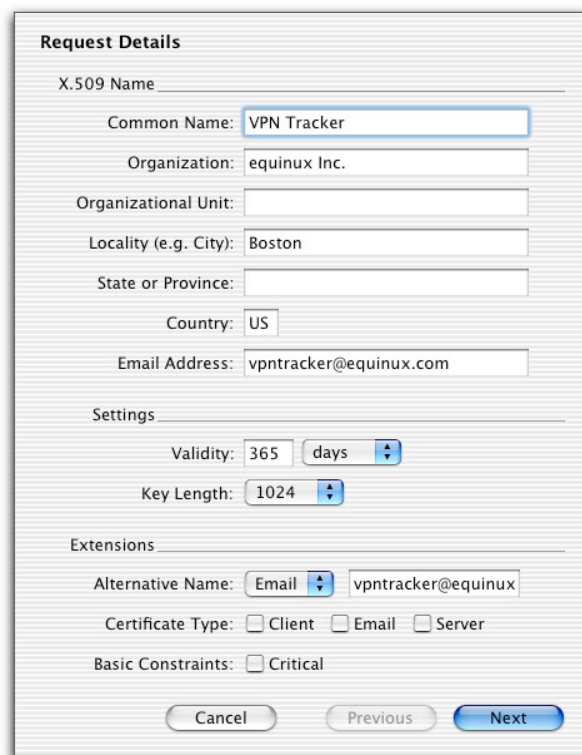
4. Connecting to a F-Secure VPN+ gateway using RSA X.509 certificates

Step 3 Create Certificate Request with VPN Tracker:

Go to the VPN Tracker certificate manager (⌘ + “E”) and create a new certificate request (in tab “Requests”). Type in the your certificate data.

You have to use an “Alternative Name”. Choose “email” from the drop-down box and enter an email address.

Export the request as PEM file without the private key and name it *host.req*. It essential that the file extension is “.req”.



The screenshot shows a dialog box titled "Request Details" for creating a certificate request. It is divided into several sections:

- X.509 Name:** Contains fields for Common Name (VPN Tracker), Organization (equinux Inc.), Organizational Unit, Locality (e.g. City) (Boston), State or Province, Country (US), and Email Address (vpntracker@equinux.com).
- Settings:** Includes a Validity field set to 365 days and a Key Length field set to 1024.
- Extensions:** Features an Alternative Name dropdown menu set to "Email" with the value vpntracker@equinux, and radio buttons for Certificate Type (Client, Email, Server) and Basic Constraints (Critical).

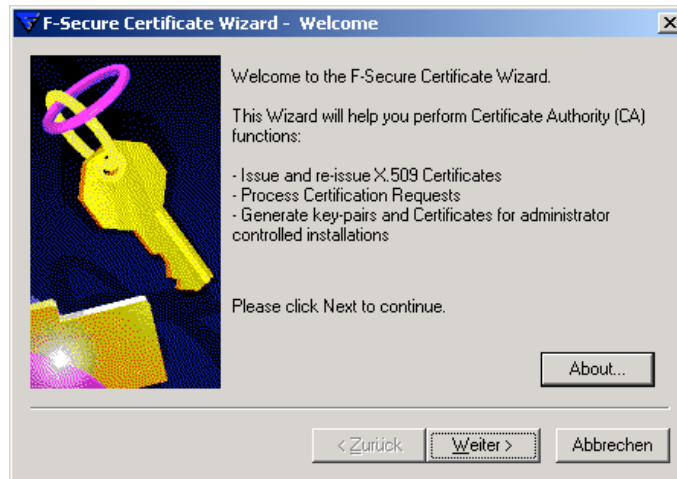
At the bottom of the dialog are three buttons: "Cancel", "Previous", and "Next".

Figure 20: VPN Tracker - Certificate Request

4. Connecting to a F-Secure VPN+ gateway using RSA X.509 certificates

Step 4

Sign the certificate request with the F-Secure certificate wizard:



Please select “Process Certification Requests (PKCS#10)”. The PKCS#10 Format is compatible to the PEM Format.

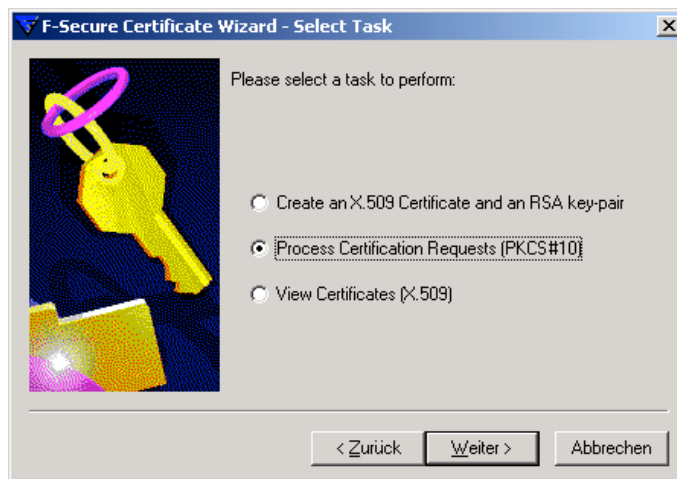


Figure 21: Certificate Wizard - Select Task

4. Connecting to a F-Secure VPN+ gateway using RSA X.509 certificates

Please choose the directory, which contains the certificate request from VPN Tracker.



Figure 22: Certificate Wizard - Choose directory

You can enter a unique serial number here. Furthermore you can change the validity for the certificate.



Figure 23: Certificate Wizard - Validity Period

4. Connecting to a F-Secure VPN+ gateway using RSA X.509 certificates

Finally please enter the pass phrase of your CA.



Figure 24: Certificate Wizard - CA Passphrase

Step 5

The setup of the IPsec Gateway works similar to the process described in section 3, step 3. There is only one difference.

Please choose “ike-rsassigned-strong” as “Proposal list” and do **not** enter a pre-shared key.

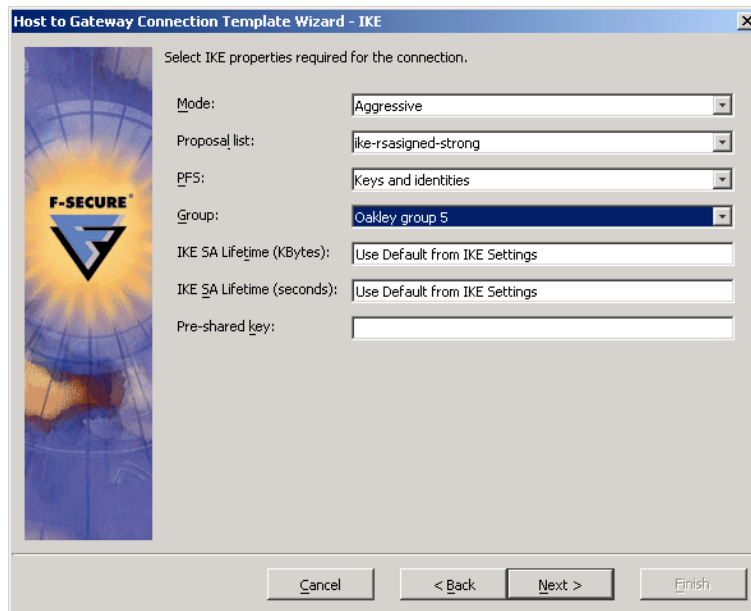


Figure 25: New Connection Template Wizard – IKE with X.509

Please note: You have to save and “distribute” all changes, every time you change the configuration.

4. Connecting to a F-Secure VPN+ gateway using RSA X.509 certificates

4.2 VPN Tracker configuration

Step 1

Import the certificate and the CA into VPN Tracker:

Copy the signed certificate and the Ca.pem from the directory you selected in the F-Secure Certificate Wizard to your Mac running VPN Tracker.

Open the Certificate Manager (File -> Show certificates) of VPN Tracker and go to the certificates tab. Import the PEM file you previously copied from your F-Secure managing workstation.



Figure 26: VPN Tracker – Certificate Import

Go to the CA tab and import the CA.pem file you previously copied from the F-Secure managing workstation.

4. Connecting to a F-Secure VPN+ gateway using RSA X.509 certificates

Step 2

Add a new connection with the following options: Choose “F-Secure VPN+ gateway“ 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).

The image shows a screenshot of the VPN Tracker main dialog box. The dialog is titled "General" and is divided into three sections: "General", "Networking", and "Authentication".

- General:**
 - Name: F-secure x509
 - Connection Type: F-Secure VPN+ (dropdown menu)
 - Initiate connection
- Networking:**
 - Topology: Host to Network (dropdown menu)
 - Local Endpoint: Default Interface
 - Remote Endpoint: 169.1.2.3
 - Local Host: optional
 - Remote Network: 192.168.1.0 / 24
- Authentication:**
 - Pre-shared key
 - Certificates

At the bottom of the dialog, there is a lock icon and the text "Click the lock to prevent further changes." Below this are two buttons: "Cancel" and "Save".

Figure 27: VPN Tracker main dialog (with certificates)

4. Connecting to a F-Secure VPN+ gateway using RSA X.509 certificates

Step 3

Choose as “own certificate” the certificate you imported in step 1 and verify the remote certificate “with CAs”. Type-in the same email Address you used in the field “X.500 Distinguished Names” in the F-Secure VPN+ configuration. If you have typed in a correct local identifier, the word "Email" should be visible beside the input field.

Select IP address as remote identifier. Do not “Verify the remote certificate”.



Figure 28: Certificate dialog

Step 4

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 F-Secure VPN+ gateway. 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 F-Secure VPN+ gateway 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.