

# VPN Tracker

Secure networking made easy

**User Manual**

Version 4.9.3

## **Disclaimer**

We cannot guarantee the compatibility of VPN Tracker (“the Software”) with other IPsec products. As secure networking depends on a lot of external conditions, setting up secure connections between two VPN Tracker clients is not always possible.

You agree that equinix AG and equinix USA Inc. (“equinix”) shall have no liability whatsoever for any use you make of the Software. You shall indemnify and hold harmless equinix from any third party claims, damages, liabilities, costs and fees (including reasonable attorney fees) arising from your use of the Software as well as from your failure to comply with any term of this Agreement.

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

## Contents

<b>Chapter 1: Welcome to VPN Tracker</b>	5
Getting Started	5
What is VPN Tracker?	5
Licensing	6
System Requirements	6
Contact & Support	6
<b>Chapter 2: IPsec Concepts</b>	7
Modes	7
Transport Mode	7
Tunnel Mode	7
Protocols	8
Internet Key Exchange (IKE)	8
Security Association (SA)	8
Tunnel Negotiating	8
Phase 1	9
Phase 2	10
Public Key Cryptography	11
Certificates	11
Extended Authentication (XAUTH)	12
NAT Traversal (NAT-T)	12
Client Provisioning	13
<b>Chapter 3: Setup and Configuration</b>	14
General Concept	14
Connection List	14
Connection Status	15
Smart VPN	15
Connection Details	16
Authentication	24
Authentication using Pre-shared Keys	24
Authentication using Certificates	25
Extended Authentication (XAUTH)	26
Certificate Manager	27

Certificates	27
Requests	29
Certificate Authorities (CAs)	31
Connection Types (Vendor Database)	34
Phase 1 General	35
Phase 1 Proposal	37
Phase 2	39
The Log Window	41
Preferences	41
<b>Chapter 4: Configuration Examples</b>	<b>43</b>
Connection Between Two Macs Running VPN Tracker	43
Connecting to an Office LAN	44
Securing an AirPort Network	46
<b>Chapter 5: Interoperability</b>	<b>49</b>
Introduction	49
List of Known Compatible VPN Gateways	50
Manuals for Compatible Devices	50
<b>Appendix A: Customizing the Authorization Behavior</b>	<b>51</b>
Right Keys Used by VPN Tracker	51
Default Policies	51
Customizing the Policy Database	52
Editing the policy database file (Mac OS X 10.2)	52
Editing the policy database file (Mac OS X 10.3 and higher)	53
<b>Appendix B: Scripting</b>	<b>54</b>
The Actions Folder	54
Action Events	54
Script Parameters	55
Using AppleScript	55
<b>Appendix C: Frequently Asked Questions</b>	<b>56</b>

## Chapter 1:

# Welcome to VPN Tracker

This chapter introduces you to VPN Tracker, an application to setup secure, encrypted network connections on Mac OS X.

## Getting Started

Thank you for your selection of VPN Tracker.

If you are new to VPN Tracker, we recommend you read at least Chapter 3 of this manual to familiarize yourself with the basic concepts of VPN Tracker.

Additionally, you should read Chapter 2 for an overview of the concepts of the IPsec protocol used by VPN Tracker.

If you want to quickly configure VPN Tracker, you should look into the Configuration Examples in Chapter 4 to see if your setup is described here.

If you want to use VPN Tracker with a specific 3rd party VPN solution, please have a look at Chapter 5 to see if there is a How-To documentation which describes the configuration of VPN Tracker with your VPN product.

## What is VPN Tracker?

VPN Tracker is a versatile, user-friendly IPsec client for Mac OS X. Using industry-standard algorithms, VPN Tracker can secure all your internet-based communications, including those over wireless networks.

Our predefined connection types for a large variety of 3rd party VPN solutions make setting up secure, encrypted tunnels to remote networks easier than ever before!

Nevertheless power users will be happy to see that they are able to control even the most obscure IPsec options, opening endless opportunities of fine-tuning their VPN devices or network.

## Licensing

VPN Tracker comes in two editions: Personal and Professional.

The Personal Edition allows you to have one connection in either Host to Host or Host to Network mode. This is sufficient if you want to connect to another Mac running VPN Tracker (Host to Host) or to a network of computers (e.g. to your office LAN).

The Professional Edition also allows you to establish “Network to Network” connections (e.g. if you want to connect to branch offices) and to have an unlimited number of concurrent connections. Also, it allows the use of the AES algorithm (“Advanced Encryption Standard”) with key lengths of 192 and 256 bits, exporting of connections including the connection type, pre-shared key and certificates/CAs as necessary, execution of scripts upon certain events and to enter the pre-shared key when starting the VPN service.

For both editions, there is only one download: your VPN Tracker license key determines which edition you have.

When running in demo mode, VPN Tracker will have the same full features as the Professional Edition.

If you have already set up your connections in VPN Tracker and want to find out which edition fits your needs, just select “Order Information...” from the VPN Tracker application menu to let VPN Tracker determine which edition is appropriate for you.

Alternatively, you can use our interactive wizard to find out which edition you need:

<http://www.vpntracker.com/wizard>

Please see our web page for details on pricing.

## System Requirements

VPN Tracker requires Mac OS X 10.2.5, 10.3 or higher and the BSD subsystem from the Mac OS X installation to be installed.

## Contact & Support

Web site: <http://www.vpntracker.com>

Email: [vpntracker@equinux.com](mailto:vpntracker@equinux.com)

## Chapter 2:

# IPsec Concepts

A virtual private network (VPN) provides a means for securely communicating between remote computers across the Internet.

A VPN connection can, for example, link two local area networks (LANs) or a remote dialup user and a LAN. The traffic that flows between these two points passes through shared resources such as routers, switches and other network equipment that make up the public Internet. To secure VPN communication while passing through the Internet, the two participants create an IP Security (IPsec) tunnel. An IPsec tunnel consists of a pair of unidirectional Security Associations (SAs)—one at each end of the tunnel—that specify the security parameters and the source and destination IP addresses. Through the SA, an IPsec tunnel can provide the following security functions:

- Privacy (via encryption)
- Content integrity (via data authentication)
- Sender authentication
- non-repudiation (via data origin authentication, if using certificates)

## Modes

IPsec operates in one of two modes: transport or tunnel. When both ends of the tunnel are hosts, you can use transport mode or tunnel mode. When at least one of the endpoints of a tunnel is a security gateway, such as a router or firewall, you must use tunnel mode. VPN Tracker can operate in tunnel and transport mode for IPsec tunnels.

### Transport Mode

The original IP packet is not encapsulated within another IP packet. The entire packet can be authenticated, the payload can be encrypted (with ESP), and the original header remains in plaintext as it is sent across the Internet.

### Tunnel Mode

The entire original IP packet—payload and header—is encapsulated within another IP payload and a new header appended to it. The entire original packet can be encrypted with ESP.

In a LAN-to-LAN VPN, the source and destination addresses used in the new header are the IP addresses of the outgoing interface (in NAT or Route mode); the source and destination addresses of the encapsulated packets are the addresses of the ultimate endpoints of the connection.

## Protocols

IPsec uses two protocols to secure communications at the IP layer:

- Authentication Header (AH)—A security protocol for authenticating the source of an IP packet and verifying the integrity of its content. This protocol is not supported by VPN Tracker, because ESP provides superior capabilities.
- Encapsulating Security Payload (ESP)—A security protocol for encrypting the entire IP packet (authentication the source and ensuring the content integrity). This is the protocol used by VPN Tracker.

## Internet Key Exchange (IKE)

IKE is a protocol for securely negotiating the session key that is used for the actual payload encryption. As soon as the lifetime of the session key is reached, IKE negotiates a new session key.

## Security Association (SA)

A security association (SA) is a unidirectional agreement between the VPN participants regarding the methods and parameters to use in securing a communication channel. Full bidirectional communication requires at least two SAs, one for each direction.

## Tunnel Negotiating

To establish an IPsec tunnel, two phases of negotiation are required:

- In Phase 1, the participants establish a secure channel in which to negotiate the IPsec SAs. This secure channel is also referred to as ISAKMP-SA
- In Phase 2, the participants negotiate the IPsec SAs for encrypting and authenticating the ensuing exchanges of user data.

## Phase 1

Phase 1 of an IKE tunnel negotiation consists of the exchange of proposals for how to authenticate and secure the channel. The exchange can be in one of two modes: Aggressive mode or Main mode (see below). Using either mode, the participants exchange proposals for acceptable security services such as:

- Encryption algorithms (DES and 3DES) and authentication algorithms (MD5 and SHA-1).
- A Diffie-Hellman Group (see Diffie-Hellman Exchange)
- Pre-shared Key or RSA X.509 certificates (see Public Key Cryptography)

A successful Phase 1 negotiation concludes when both ends of the tunnel agree to accept at least one set of the Phase 1 security parameters proposed, and then processes them.

VPN Tracker provides predefined Phase 1 proposals compatible with the VPN gateway used.

### Main and Aggressive Mode

Phase 1 can take place in either Main mode or Aggressive mode. The two modes are described below.

#### Main Mode:

The initiator and recipient send three two-way exchanges (six messages in total) to accomplish the following services:

- First exchange, (messages 1 and 2): Propose and accept the encryption and authentication algorithms.
- Second exchange, (messages 3 and 4): Execute a Diffie-Hellman exchange, whereby the initiator and recipient each provide a nonce (randomly generated number).
- Third exchange, (messages 5 and 6): Send and verify their identities.

The encryption algorithm established in the first two exchanges protects the information transmitted in the third exchange of messages. Thus, the participants' identities are not transmitted openly.

#### Aggressive Mode:

The initiator and recipient accomplish the same objectives, but only in two exchanges, and a total of three messages:

- First message: The initiator proposes the SA, initiates a Diffie-Hellman exchange, and sends a nonce and its IKE identity.
- Second message: The recipient accepts the SA, authenticates the initiator and immediately sends its IKE identity, and, if using certificates, the

recipient's certificate.

- Third message: The initiator authenticates the recipient, confirms the exchange, and, if using certificates, sends the initiator's certificate.

Because the participants' identities are not exchanged securely (in the first two messages), Aggressive mode does not provide identity protection.

## **The Diffie-Hellman (DH) Key Exchange**

A Diffie-Hellman exchange allows the participants to produce a shared secret value. The strength of the technique is that it allows the participants to create the secret value over an unsecured medium without passing the secret value through the wire. There are five Diffie-Hellman groups (VPN Tracker supports groups 1, 2, and 5). The size of the prime modulus used in each group's calculation differs as follows:

- DH Group 1: 768-bit modulus
- DH Group 2: 1024-bit modulus
- DH Group 5: 1536-bit modulus

The larger the modulus, the more secure the generated key is considered to be; however, the larger the modulus, the longer the key-generation process takes. Because the modulus for each DH group is a different size, the participants must agree to use the same group.

## **Phase 2**

After the participants have established a secure and authenticated channel, they proceed through Phase 2, in which they negotiate the SAs to secure the data to be transmitted through the IPsec tunnel. Just as with the process for Phase 1, the participants exchange proposals to determine which security parameters to employ in the SA. A Phase 2 proposal includes the security protocol ESP and selected encryption and authentication algorithms. The proposal can also specify a Diffie-Hellman group, if Perfect Forward Secrecy (PFS, see below) is desired. Regardless of the mode used in Phase 1, Phase 2 always operates in Quick mode and involves the exchange of three messages.

VPN Tracker has many pre-defined proposals for Phase 2 negotiations, depending on the VPN gateway used.

## **Perfect Forward Security (PFS)**

Perfect Forward Security (PFS) is a method for deriving Phase 2 keys independent of and unrelated to the preceding keys. Alternatively, the Phase 1 proposal creates a key from which all Phase 2 keys are derived. If an unauthorized party gains access to the Phase 1 key, all your encryption keys are compromised. PFS addresses this security risk by forcing a new Diffie-Hellman key exchange to occur for each Phase

2 tunnel. Using PFS is thus more secure, although the rekeying procedure in Phase 2 might take slightly longer with PFS enabled and some VPN devices do not support PFS.

## Public Key Cryptography

In public key cryptography, a public/private key pair is used to encrypt and decrypt data. Data encrypted with a public key, which the owner makes available to the public, can only be decrypted with the corresponding private key, which the owner keeps secret and protected. For example, if Alice wants to send Bob an encrypted message, Alice can encrypt it with Bob's public key and send it to him. Bob then decrypts the message with his private key.

The reverse is also useful; that is, encrypting data with a private key and decrypting it with the corresponding public key. This is known as creating a digital signature. For example, if Alice wants to present her identity as the sender of a message, she can encrypt the message with her private key and send the message to Bob. Bob then decrypts the message with Alice's public key, thus verifying that Alice is indeed the sender. Public/private key pairs play an important role in the use of digital certificates.

## Certificates

A digital certificate is an electronic means for verifying your identity through the word of a trusted third party, known as a Certificate Authority (CA). The CA server you use can be owned and operated by an independent CA (e.g. VeriSign), or by your own organization, in which case you become your own CA. VPN Tracker Professional Edition provides the possibility to create and operate your own CA.

When using certificates to authenticate, each side generates a public/private key pair and acquires a certificate. As long as the issuing certificate authority (CA) is trusted by both sides, the participants can retrieve the peer's public key and verify the peer's signature.

The procedure for signing a certificate (by a CA) and then verifying the signature works as follows (by the recipient):

### Signing a Certificate

1. The Certificate Authority (CA) that issues a certificate hashes the certificate by using a hash algorithm (MD5 or SHA-1) to generate a digest.
2. The CA then "signs" the certificate by encrypting the digest with its private key. The result is a digital signature.
3. The CA then sends the digitally signed certificate to the person who requested it.

## Verifying a Digital Signature

1. When the recipient gets the certificate, he or she also generates another digest by applying the same hash algorithm (MD5 or SHA-1) on the certificate file.
2. The recipient uses the CA's public key to decrypt the digital signature.
3. The recipient compares the decrypted digest with the digest he or she just generated. If the two digests match, the recipient can confirm the integrity of the CA's signature and, by extension, the integrity of the accompanying certificate.

The procedure for digitally signing messages sent between two participants in an IPsec session works very similarly, with the following differences:

- Instead of making a digest from the CA certificate, the sender makes it from the data in the IP packet payload.
- Instead of using the CA's public/private key pair, the participants use the sender's public/private key pair.

## Extended Authentication (XAUTH)

Extended Authentication is an addition to the Internet Key Exchange (IKE) protocol, which allows user authentication in a separate phase after the IKE Phase 1 exchange. While the connection will still be authenticated using either pre-shared keys or certificates, the additional authentication step will authenticate each user separately using user name and password.

The user authentication can be checked against an internal database in the VPN device or external databases, e.g. against a RADIUS or LDAP server. This allows the user to use the same login information for the VPN connection as for other services like email or file services.

## NAT Traversal (NAT-T)

NAT Traversal is a method to detect NAT gateways between IPsec hosts and to negotiate the use of UDP encapsulation of IPsec packets. When using UDP encapsulation, the IPsec data packets (ESP packets) will be encapsulated in UDP packets, which can be handled by NAT gateways like any other UDP packets (in contrast to ESP packets).

Whether a VPN gateway is compatible with NAT Traversal will be automatically detected during connection establishment. If it is compatible, the two IPsec hosts will detect the presence of NAT gateways and enable NAT Traversal when needed. VPN Tracker also supports newer versions of NAT Traversal (version 02 and higher), which causes IPsec hosts to additionally switch the port number (from UDP port 500 to 4500) when NAT gateways have been detected ("port floating"). This is

done to prevent problems with some IPsec-aware NAT gateways (supporting “IPsec passthrough”), which cannot correctly handle UDP-encapsulated IPsec traffic. These gateways can handle non-encapsulated IPsec traffic (i.e. without using NAT Traversal) without problems, as long as only one connection is established to the same VPN gateway at a time.

When using VPN Tracker behind a NAT gateway which is incompatible with NAT Traversal to establish a connection to a VPN gateway which doesn't support port floating to UDP port 4500, it is best to disable NAT Traversal for this connection.

Examples for incompatible NAT gateways include Apple AirPort Base Stations with a current firmware. Most VPN gateways also do not currently support port floating.

## **Client Provisioning**

During SA negotiations, this option permits the exchange of configuration parameters with the VPN gateway. Client Provisioning has to be supported by the VPN gateway (e.g. Cisco, Juniper Networks/NetScreen support Mode Config, SonicWALL supports DHCP over IPsec).

Supported connection options include: Local Address (virtual IP), DNS settings and remote networks (remote network is supported for Cisco only).

## Chapter 3:

# Setup and Configuration

This chapter will show you how to setup connections and how to edit connection types.

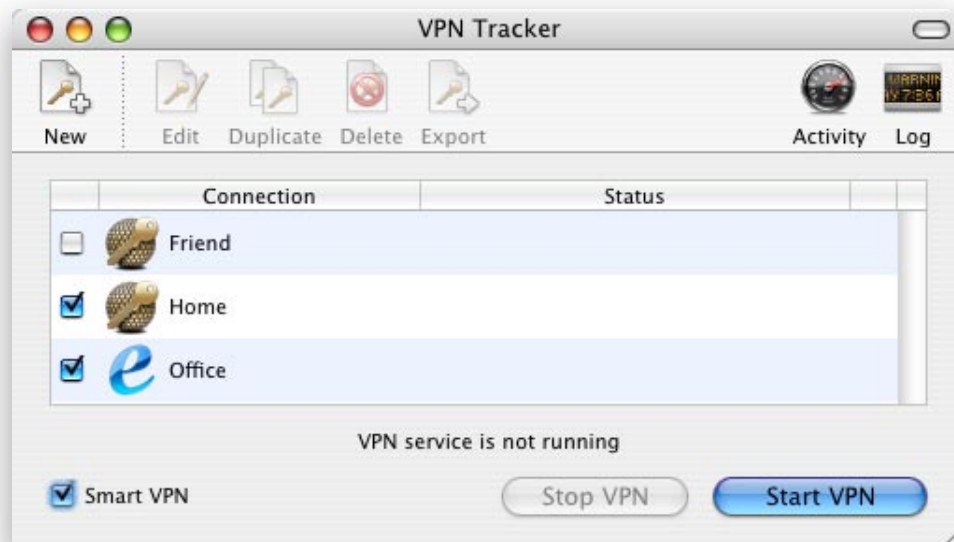
## General Concept

Settings in VPN Tracker are divided into two units: Connections and Connection Types. Connection Types specify settings like encryption algorithms and authentication method, which can apply to one or more connections.

VPN Tracker comes with pre-defined connection types for remote ends which have been verified to work with VPN Tracker. See Chapter 5 for details on interoperability with other VPN solutions.

## Connection List








The connections window will automatically open when you start VPN Tracker. It shows you the connections you have set up, the status of each connection (if the VPN service is running) and the status of the VPN service in general.



Here you can start and stop the VPN service, create and delete connections or temporarily disable specific connections. You can also enable "Always-On VPN", which will make VPN Tracker keep your VPN connections up with different network setups (see below).

## Connection Status

When the VPN service is running, the main window shows the status of every enabled connection displaying one of the following icons next to the connection entry:

-  Connection is enabled, but not yet initiated, or connection has expired.
-  Connection is about to be established.
-  Connection is being initiated, phase 1 has been started.
-  Negotiating Extended Authentication (XAUTH), only when enabled.
-  Phase 1 has been completed successfully, phase 2 has been started.
-  The connection has been established successfully.
-  The connection establishment has timed out.

Additionally, if VPN Tracker is running, it's icon in the Dock shows the general status of the VPN service:



VPN service is not running.



VPN service is running, but no connection has been established.



VPN service is running, at least one connection has been established.

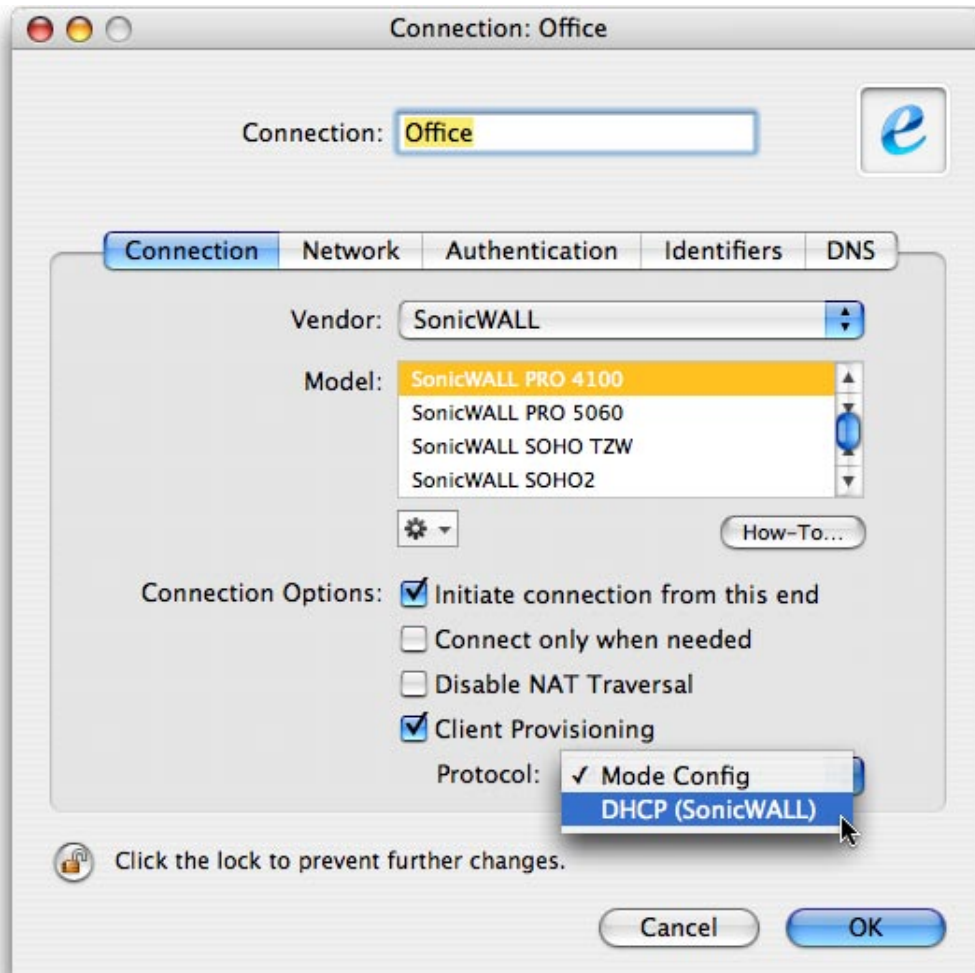
## Smart VPN

“Smart VPN” will make your VPN connections work hassle-free wherever you are, which is especially great for mobile users.

When this option is enabled, VPN Tracker will automatically follow network configuration changes and sleep/wakeup events, restarting the VPN service when necessary. If the remote network of a connection is the same as your local network, this connection is automatically skipped (e.g. your Office connection in the case when you are in the office). If your Mac currently has no active network connection, the VPN service is kept idle and will be started as soon as network connectivity is re-established.

## Connection Details

You can create a new connection by clicking the “New” button in the connection window’s toolbar and you can edit existing connections by double-clicking an entry in the list of connections. In both cases, the following window will appear.



The settings are split into five groups, accessible through the tabs Connection, Network, Authentication, Identifiers, DNS. Above these tabs you can enter a name for the connection, which is for internal purposes only.

You can also assign a custom icon to your connection, either by dragging an image file onto the icon space, or by copying an icon (e.g. from a “Get Info” dialog in the Finder) and pasting it into the icon space.

### Connection Settings

The connection settings specify general details about the connection, e.g. the vendor and model of the VPN gateway.

#### Vendor:

Select the vendor of your VPN gateway, e.g. “SonicWALL”.

Select “Custom” if you want to use a custom connection type. Select “Edit Vendor Database...” to add you own device or to edit existing devices.

**Model:**

Select the model of your VPN gateway. The contents of this list depend on the selected vendor. Each model is assigned to a specific internal connection type which defines the different parameters of the IPsec communication. Please see Connection Types for more details.

If you have selected “Custom” as vendor, this list will contain all custom connection types.

You can click the action button or right-click an entry in the list to edit the connection type of the selected model. If you have selected a built-in model (i.e. not “Custom”), you can click the “How-To” button to view a step-by-step manual which describes the setup process of VPN Tracker with your VPN gateway (this feature requires Internet access).

**Initiate connection from this end:**

Enable this option if you want to be able to establish this connection from your end. If you disable this option, the connection can only be established from the remote end. This option should normally be enabled.

**Connect only when needed:**

Enable this option if the connection should not be established when starting the VPN service. In this case, the connection will be established when the first packet is sent to the remote network. This option should normally be disabled.

**Disable NAT Traversal:**

Enable this option when you do not want VPN Tracker to try to use NAT Traversal (NAT-T) when establishing the connection. This option would be enabled when using a NAT router which is incompatible with NAT Traversal. Please see the section NAT Traversal in chapter 2 for more information.

**Client Provisioning (Mode Config or DHCP over IPsec):**

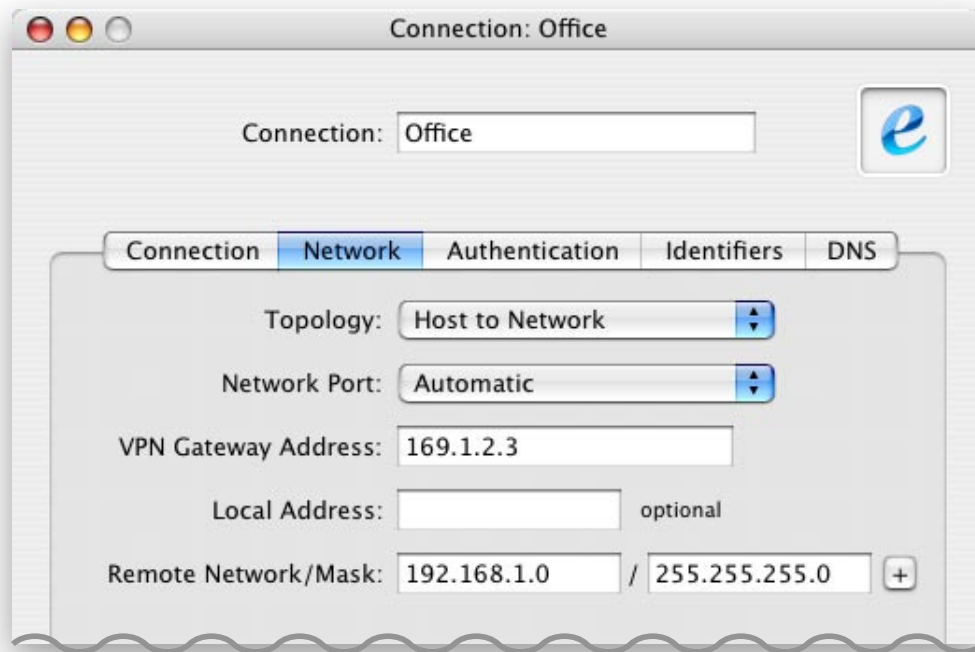
Enable this option to use the for Client Provisioning. This feature has to be supported by the VPN gateway (e.g. Cisco, Juniper Networks/NetScreen support Mode Config, SonicWALL supports DHCP over IPsec). It allows the gateway to communicate connection options to the client when establishing the connection. Supported connection options include: Local Address (virtual IP), DNS settings and remote networks (Cisco only).

Note: Manual DNS settings for a connection overwrite those received during the Client Provisioning phase. Incomplete DNS settings will be completed where possible. If the topology is Host to Network or Host to Host, split-DNS will be used if possible (that is if we received a domain name from the VPN gateway), otherwise the received DNS servers are used for all DNS queries. If the topology is Host to Everywhere, the received DNS servers are used for all DNS queries.

When connecting to a Cisco VPN gateway which has been configured using “Easy VPN”, please enable this option before selecting “Cisco Easy VPN” as the topology in the “Network” tab.

## Network Settings

The network settings specify the network details of the IPsec connection, e.g. the address of the VPN gateway and the remote network.



### Topology:

Select “Host to Host” or “Host to Host (Transport)” for connections between two hosts only. “Host to Host (Transport)” uses IPsec transport mode, “Host to Host” uses IPsec tunnel mode and enables use of virtual interfaces (“Local Address” and “Remote Address” fields, see below). Whether you should use tunnel or transport mode depends on the setting on the remote end and on whether or not you want to use virtual interfaces. We generally recommend to use tunnel mode.

Select “Host to Network” if you want to connect to another network.

Select “Host to Everywhere” if all your network traffic is to be secured. For example, this topology could be used for securing AirPort connections.

Select “Network to Network” (also known as “Tunnel”) for connections between two networks (“Network to Network” mode is only available in demo mode or if you have a Professional Edition license).

Select “Cisco Easy VPN” for connections to a Cisco VPN gateway which has been configured using Cisco Easy VPN. For this option you will need to enable “Client Provisioning (Mode-Config)” in the “Connection” tab first.

For example, you will need a “Host to Network” connection, if you want to connect to your office with a dialup connection and want to be able to see all computers in your office LAN.

1) It is recommended to use an IP address from one of the private IP address ranges 10.x.x.x, 172.16.x.x – 172.31.x.x or 192.168.x.x.

**Network Port:**

You would normally select “Automatic” here. This means that VPN Tracker will use the default network connection of your Mac for connecting to the remote endpoint.

**VPN Gateway Address:**

This field should contain the address of your VPN gateway.

If you have selected to use a “Host to Host” connection, this would be the IP address or domain name of the host you are connecting to.

If you have selected to use a “Host to Network” or “Network to Network” connection, this would normally be the address of an IPsec-compatible firewall.

**Local Address:**

This optional field is only available when mode is set to “Host to Host” or “Host to Network”.

If you enter an arbitrary<sup>1)</sup> IP address into this field, VPN Tracker will use the address to add a virtual interface to your Mac. The IPsec tunnel will then originate from this address, as opposed to the address of the interface specified under Network Port. The address should not be within your remote network range.

Users on the remote end of the connection have to use this IP address for connections to your Mac.

The other way round, after decryption at the remote end, all traffic going to the remote host respective remote network will have this source address.

Please note that the connection setting on the remote end has to reflect your setting here.

**Remote Address:**

This optional field is only available when mode is set to “Host to Host”.

If you enter an IP address into this field, any network traffic to this address will be encrypted. If left empty, the “Remote Endpoint” address will be used.

Please note that the connection setting on the remote end has to reflect your setting here.

**Local Network:**

This field is only available when mode is set to “Network to Network”. Network traffic coming from this network will get encrypted.

The first field should contain the IP address of your network (e.g. “192.168.1.0”), the second field the network mask (e.g. “255.255.255.0”).

You can use the “+” button if you have more than one local network.

**Remote Network:**

This field is only available when mode is set to “Host to Network” or “Network to Network”. Network traffic going to this network will get encrypted.

The first field should contain the IP address of your network (e.g. “192.168.1.0”), the second field the network mask (e.g. “255.255.255.0”).

For example, if you are connecting to your office, this would be the address of the LAN in your office.

You can use the “+” button if you have more than one remote network.

## Authentication Settings

The authentication settings specify how the connection should be authenticated. Available options are “Pre-shared key” and “Certificates”. Additionally, you can choose to use Extended Authentication (XAUTH). Please note that all settings have to match the settings on your VPN gateway.

The chapter Authentication below describes the details of the configuration options.



### Pre-shared Key:

Select this option if you want to connect using pre-shared keys. You can edit the pre-shared key by clicking the “Edit...” button next to this option.

### Certificates:

Select this option if you want to connect using RSA X.509 certificates. You can select the certificates by clicking the “Edit...” button next to this option.

### Enable XAUTH:

Enable this option if your VPN gateway is setup to use Extended Authentication (XAUTH).

Extended Authentication will add an extra authentication step after the connection has been authenticated using either pre-shared keys or certificates. This will allow the VPN gateway to authenticate each user separately using user name and password.

The authentication details will be requested from the user when the connection is being established and can optionally be saved in the keychain.

## Identifier Settings

The identifier settings specify the local and remote identifiers for the IPsec connection. These values are used by some VPN gateways to match the connection against different connection settings. Please see the how-to manual for your VPN gateway for details on these settings.



### Local / Remote Identifier

An identifier can be one of the following:

- an IP address
- a certificate when authenticating using certificates (own certificate for local identifiers and remote certificate for remote identifiers)
- a fully-qualified domain name (FQDN), e.g. "host". This is used as a literal string and not resolved
- a user fully-qualified domain name (email, User-FQDN), e.g. "user@host"
- a ASN.1 distinguished name (ASN.1 DN)
- a Key ID, which is used for the group name when connecting to Cisco VPN gateways

The identifier type can be selected using the popup menu next to the identifier field. Using the "Auto" setting, VPN Tracker will recognize which identifier type is used and show the result beside the field. The following types are automatically recognized: FQDN, email and ASN.1 DN.

An identifier of the form "@user" will be taken as "user" with a type of "email".

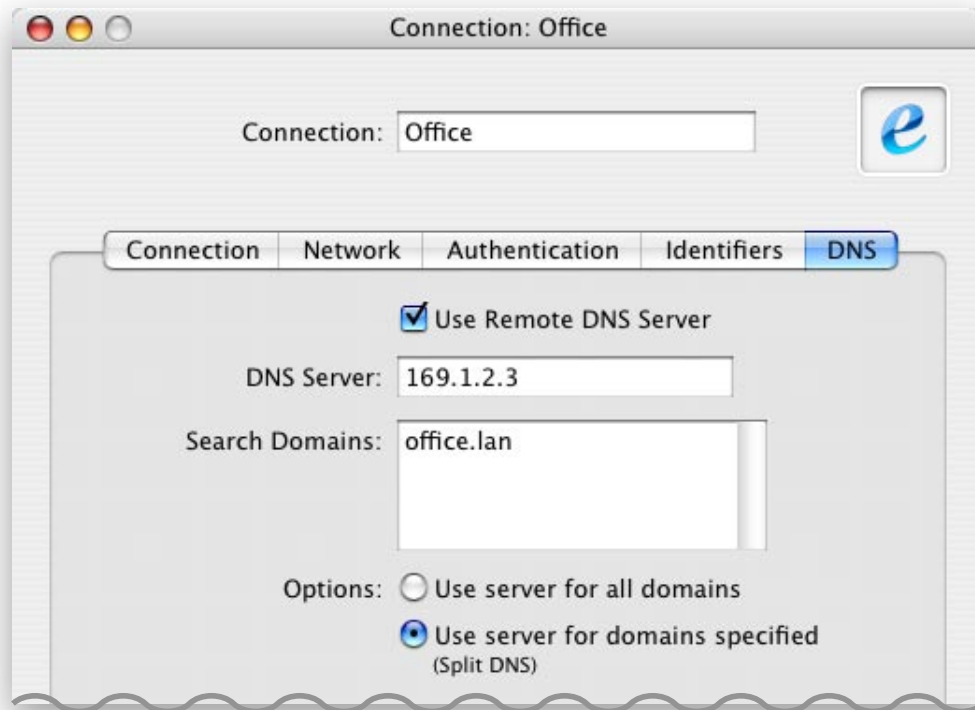
### Verify remote identifier

Enable this check box if you want to verify the identifier of the remote endpoint.

## DNS Settings

The DNS settings optionally allow you to use a DNS (Domain Name Service) server in the remote network, which enables you to access servers in the remote network by name instead of by IP address.

All settings will apply if the connection is enabled and the VPN service is started.



### Use Remote DNS Server:

Enable this option if you want to use a DNS server which is located in the remote network.

### DNS Server:

Enter the IP address of the DNS server you want to use when the VPN connection is established. This address should typically lie within the remote network range. Multiple DNS servers should be separated by a comma.

### Search Domains:

Enter the DNS domains of your remote networks, one per line.

If you want to have reverse DNS lookup, you can enter “.in-addr.arpa” entries for your remote networks, e.g. “1.168.192.in-addr.arpa” for the network “192.168.1.0/255.255.255.0”.

### Use server for all domains:

Choose this option if VPN Tracker should overwrite the system DNS settings. All DNS queries will be sent to the DNS server specified above.

The domains specified under “Search Domains” will be used to complete unqualified domain queries (i.e. queries without a domain part).

**Use server for domains specified (Split DNS):**

Choose this option if VPN Tracker should use the specified DNS server for the domains specified under “Search Domains” only.

These domains will also be used to complete unqualified domain queries (i.e. queries without a domain part), which means that they will be sent to both the system DNS server and the one specified above, in this order.

## Authentication

Select “Pre-shared key” for authentication using a pre-shared key or “Certificates” for authentication using RSA X.509 certificates.

Click the “Edit...” button next to edit the authentication details (i.e. enter the pre-shared key or select the certificates).

### Authentication using Pre-shared Keys



#### Pre-shared Key

If the first option is selected, you can enter the pre-shared key (also known as: “PSK”, “shared secret” or “password”).

The pre-shared key is case-sensitive and should not contain any special (non-ASCII) characters like umlauts or accents. As the length of the pre-shared key affects the overall security of your connection, we recommend a minimum length of 20 characters.

You can enter the pre-shared key as a hexadecimal number by adding the prefix “0x”.

By selecting the second option, the pre-shared key will not be saved on your hard disk and you will have to enter your pre-shared key every time the connection is getting established. Please note that you will also have to enter the pre-shared key every time the phase 1 and 2 expire, so a very short lifetime is not recommended in this case. This feature is only available with a VPN Tracker Professional Edition license.

When saving the pre-shared key, you will have to enter your administrator password if VPN Tracker is currently not authenticated.

## Authentication using Certificates



### Own Certificate

Select your own certificate here. Your certificate needs to have a private key.

### Remote Certificate

Choose a remote certificate here. VPN Tracker verifies this certificate against the one the VPN gateway sends. If you choose “Verify with CAs”, VPN Tracker verifies the remote Certificate against the locally stored CAs.

Please note that when using the option “Verify with CAs”, you should do either one of the following to ensure that in a group of clients, a client cannot pretend to be the server using its own certificates:

- enter the ASN.1 distinguished name of the remote certificate as remote identifier and choose to verify the remote identifier (see above)
- use different CAs for client and server certificates and make sure not to import the CA used for client certificate signing in VPN Tracker.

## Extended Authentication (XAUTH)

When Extended Authentication is enabled in the “Authentication” tab in the connection settings, the VPN gateway will ask for user authentication when the connection is being established. VPN Tracker will display the following dialog.



The VPN gateway will specify which options the user has to provide in order to authenticate the connection and might also send a custom message. If necessary, VPN Tracker will automatically adjust the authentication dialog.

If you enable the option “Remember this password”, VPN Tracker will store the user name and password in the keychain of the user which is currently logged in. The next time you will have to authenticate the connection, the options will be already filled out. This option is only available when the VPN gateway asks for user name and password only.

If you enable the option “Don’t show this dialog again”, VPN Tracker will automatically take the user name and password for this connection from the keychain without showing the dialog. This option will be automatically disabled when the connection establishment fails or when VPN Tracker is updated. You can manually reset this option for all connections by selecting “Reset Confirmation Dialogs” in the preferences.

Please see the section Extended Authentication in chapter 2 for more information.

# Certificate Manager

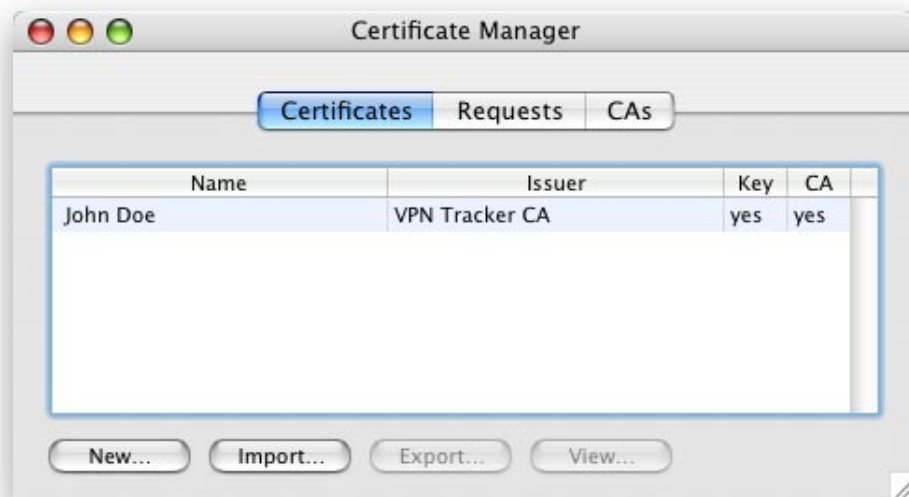
Using the “Certificates” window, you can manage all your local and foreign certificates as well as certificate authorities (CAs).

VPN Tracker supports RSA X.509 certificates in PEM, DER and PKCS#12 format.

## Certificates

Here are listed all your local and foreign Certificates.

This tab lists all important information about the certificate. The last two rows indicate if you own the private key for a certificate and if the signing CA is stored locally. You can delete a certificate using the respective option in the contextual menu or by pressing the “delete” key on the keyboard.



### New...

Starts the Certificate Wizard (see below).

### Import...

Imports a certificate with or without a private key. Certificates can be imported in PEM, DER and PKCS#12 format.

### Export... (only available with a VPN Tracker Professional Edition license)

Stores the certificate in a file in order to transfer it to another computer or device. Possible export formats are PEM, DER, PKCS#12 and Free/SWAN (for FreeS/WAN, only the public or private keys are extracted from the certificate). Optionally you can export your private key, too, but this is not recommended because of security reasons. Please note: Keep your private key safe!

## Using the Certificate Wizard



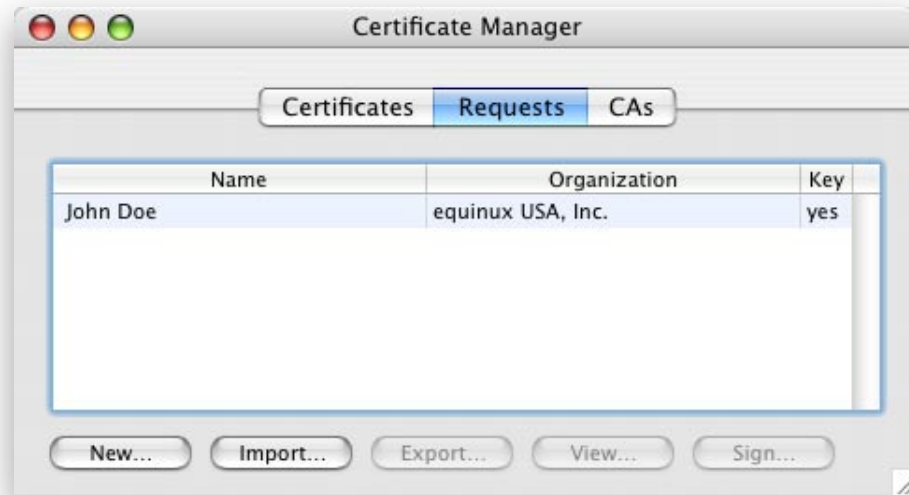
The Certificate Wizard offers the following methods for creating certificates:

- Create and export a new request for external signing
- Create and sign a new certificate with an existing CA (only available with a VPN Tracker Professional Edition)
- Create a new CA and sign a new certificate all in once (only available with a VPN Tracker Professional Edition).

Select the 3<sup>rd</sup> item if you start from scratch.

## Requests

The “Requests” tab handles all your certificate requests.



### **New...**

Creates a new Certificate Signing Request (CSR) for external or internal signing. See next screen shot.

### **Import...**

Lets you import a CSR from an external device for signing. Optionally, you can import the request with the private key. This is not recommend, as the private key of a certificate is not needed for signing.

### **Export...**

Stores the CSR locally in a file in order for it to be signed by an external CA. Possible export formats are PEM and DER. Optionally, you can export your private key, too, but this is not recommended because of security reasons. The private key is not needed for signing.

### **Sign... (only available with a VPN Tracker Professional Edition license)**

In order to generate a valid certificate out of a CSR, you have to sign it by your own CA (with an existing private key). To sign a CSR, please select the signing CA first and specify the lifetime and possible extension options for the certificate.

## **Creating a New Certificate Request**

### **X.509 Name**

Please fill out some of the fields. You only have to fill out at least a common name or an organization. You can also drag-and-drop a contact item from the Mac OS X Address Book. VPN Tracker automatically fills out the fields, which are stored in the contact item. By default, all fields are filled with the owner contact from the Address Book.

**Request Details**

X.509 Name

Common Name: John Doe

Organization: equinix USA, Inc.

Organizational Unit:

Locality (e.g. City): Lexington

State or Province: Massachusetts

Country: US

Email Address: vpntracker@equinix.com

Settings

Validity: 365 days

Key Length: 1024

Extensions

Alternative Name: Email

Certificate Type:  Client  Email  Server

Basic Constraints:  Critical

Cancel Previous Next

## Settings

### Validity:

Defines a lifetime of the certificate.

### Key Length:

You can choose 3 different values here 758, 1024 and 2048. A higher value means better security of your certificate, but also more work for the computer to process the certificate.

## Extensions

### Alternative Name:

The alternative name can be used to simplify the VPN Tunnel setup. Select “DNS”, “Email” or “IP” from the drop-down box and enter a proper value. With some devices (e.g. SonicWALL) you must use this alternative name as the peer ID if the peer’s local certificate shows one.

### Certificate Type:

For some devices you need the certificate type flag, which can be setup here.

### Basic Constraints:

Set's the "critical" flag for certificate's "Basic Constraints" option. Some devices may need this flag.

## Certificate Authorities (CAs)

The CA tab handles all your certificate authorities. You can create new and import existing CAs. Existing CAs can be exported and viewed. With a CA, you can sign requests and check whether the certificate is valid or not.



### New (only available with a VPN Tracker Professional Edition license):

Creates a new Certificate Authority (CA). See the next screenshot for details.

### Import:

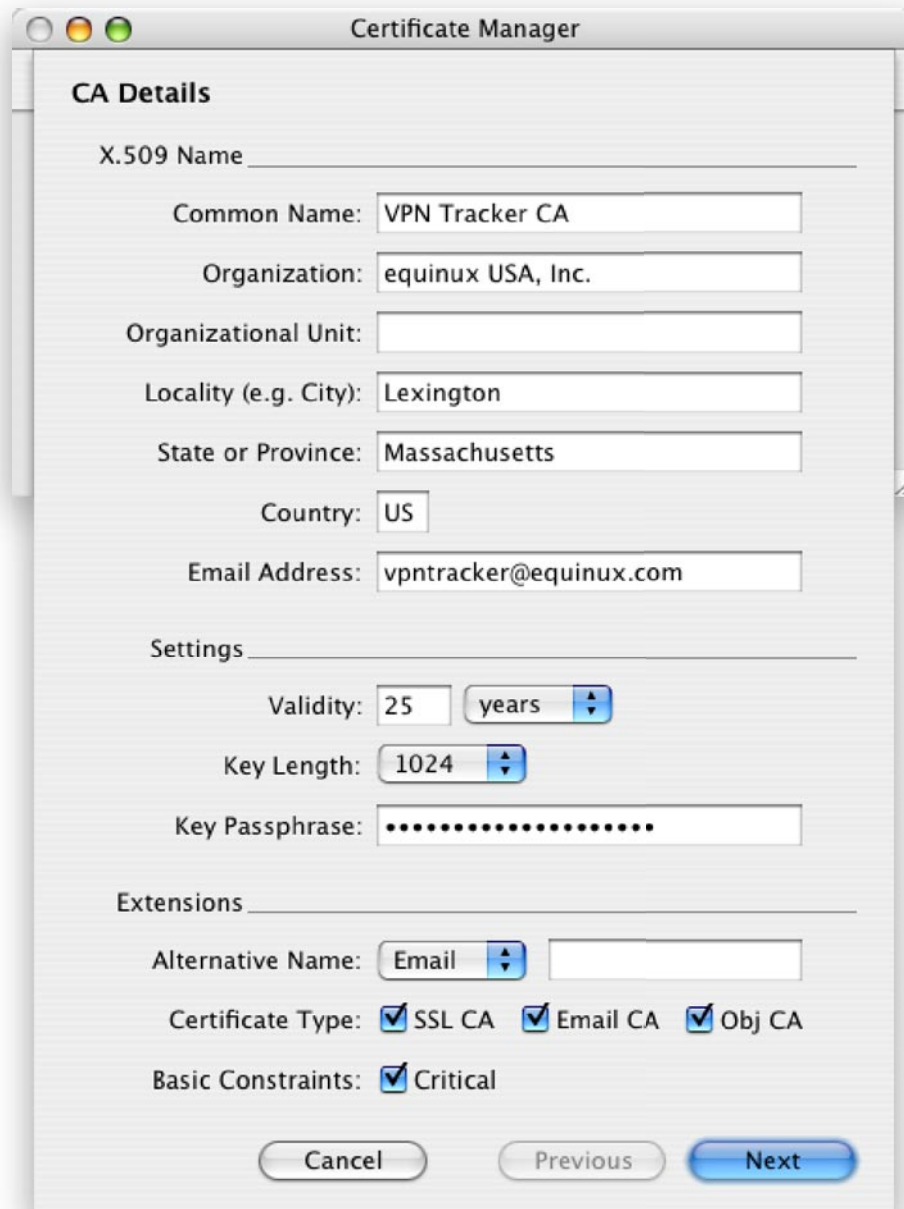
Imports a CA with or without a private key. Certificates can be imported in PEM, DER and PKCS#12 format.

### Export (only available with a VPN Tracker Professional Edition license):

You can export your certificate with your private key, but this is not recommend because of security reasons. Please note: Keep your private key safe!

## Creating a New CA

This section describes the possible settings when creating a new CA.



The screenshot shows the 'Certificate Manager' dialog box with the following fields and options:

- CA Details**
  - X.509 Name: \_\_\_\_\_
  - Common Name: VPN Tracker CA
  - Organization: equinix USA, Inc.
  - Organizational Unit: \_\_\_\_\_
  - Locality (e.g. City): Lexington
  - State or Province: Massachusetts
  - Country: US
  - Email Address: vpntracker@equinix.com
- Settings**
  - Validity: 25 years
  - Key Length: 1024
  - Key Passphrase: .....
- Extensions**
  - Alternative Name: Email \_\_\_\_\_
  - Certificate Type:  SSL CA  Email CA  Obj CA
  - Basic Constraints:  Critical

Buttons: Cancel, Previous, Next

### X.509 Name

See X.509 Name for Certificates.

### Settings

#### Validity:

Defines a lifetime of the CA.

#### Key Length:

You can choose 3 different values here 758, 1024 and 2048. A higher value means better security of your certificate, but also more work for the comput-

er to process the certificate.

**Key Passphrase:**

You have to enter a key pass phrase to protect your CA. You'll need the pass phrase for signing certificate requests.

**Extensions**

**Alternative Name:**

The alternative name can be used to simplify the VPN Tunnel setup. Select "DNS", "Email" or "IP" from the drop-down box and enter a proper value. With some devices (e.g. SonicWALL) you must use this alternative name as the peer ID if the peer's local certificate shows one.

**Certificate Type:**

For some devices you need some the CA type flags, which can be setup here.

**Basic Constraints:**

Set's the "critical" flag for certificate's "Basic Constraints" option. Some devices may need this flag.

## Connection Types (Vendor Database)

You can skip this section if you are connecting to another Mac running VPN Tracker. You should use the “VPN Tracker” connection type in this case.

However, if you are connecting to an IPsec compatible firewall, you will eventually have to create your own connection type or modify an existing one in order to have matching settings on VPN Tracker and your third-party device. See Chapter 5 for details about interoperability with other IPsec products.

Connection type settings are grouped into three sections:

### Phase 1 General:

Phase 1 of a tunnel negotiation consists of the exchange of proposals for how to authenticate and secure the channel. This group of settings specifies the details about the proposal exchange.

### Phase 1 Proposal:

Here you can specify the details of your proposal.

### Phase 2:

After the participants have established a secure and authenticated channel in phase 1, they proceed through phase 2, in which they negotiate how the data to be transmitted through the IPsec tunnel should get encrypted and authenticated.

You can select the connection type you want to edit in the “Vendor Database” window (available from the “File” menu). After selecting a vendor in the popup menu at the top, you can double-click the appropriate device in the list below. Select “Custom” in the popup menu to show your custom connection types.

If you alter a pre-defined connection type which is associated with a model of a third-party VPN device, you can always restore the default settings for this connection type by clicking the “Restore Defaults” button. Please note that some models share the same connection type. Changes to a connection type might therefore change the setting of more than one model.

## Phase 1 General



### Exchange mode:

Phase 1 can take place in two modes: Main mode and Aggressive mode. Main mode is recommended for maximum security, however, many gateways require Aggressive mode for user-based authentication.

### Proposal check:

Specifies how VPN Tracker should handle connections in which the remote endpoint proposes a different phase 2 lifetime or PFS (Perfect Forward Secrecy) setting. The recommended setting is “claim”.

- obey: The responder will obey the initiator anytime.
- strict: If the responder’s lifetime is longer than the initiator’s, the responder uses the initiator’s one. Otherwise it rejects the proposal. If PFS is not required by the responder, the responder will obey the proposal. If PFS is required by both sides and if the responder’s PFS group is not equal to the initiator’s one, then the responder will reject the proposal.
- claim: If the responder’s lifetime is longer than the initiator’s, the responder will use the initiator’s one. If the responder’s lifetime is shorter than the initiator’s, the responder uses its own length and sends a

RESPONDER-LIFETIME notify message to the initiator in the case of lifetime. About PFS, this directive is same as strict.

- exact: If the initiator's lifetime is not equal to the responder's, the responder will reject the proposal. If PFS is required by both sides and if the responder's PFS group is not equal to the initiator's, then the responder will reject the proposal.

**Nonce Size:**

Defines the byte size of the nonce value. You should normally leave this value at 16.

**Send INITIAL-CONTACT message:**

Enable this to send an INITIAL-CONTACT message. This message is useful only when the implementation of the responder chooses an old SA (Security Association) where there are multiple SAs, and the initiator reboots. If this message were not used, the responder would use an old SA even when a new SA was established. It is recommended to enable this option.

**Support MIP6:**

If this option is enabled, then both values of ID payloads in phase 2 exchange are always used as the addresses of end-point of IPsec-SAs. You should enable this option for compatibility reasons.

**Send certificate:**

If certificates are being used for authentication, send own certificate to remote side for verification if enabled.

This option should be enabled for most configurations.

**Send request for remote certificate:**

If certificates are being used for authentication, request certificate from remote side for verification if enabled.

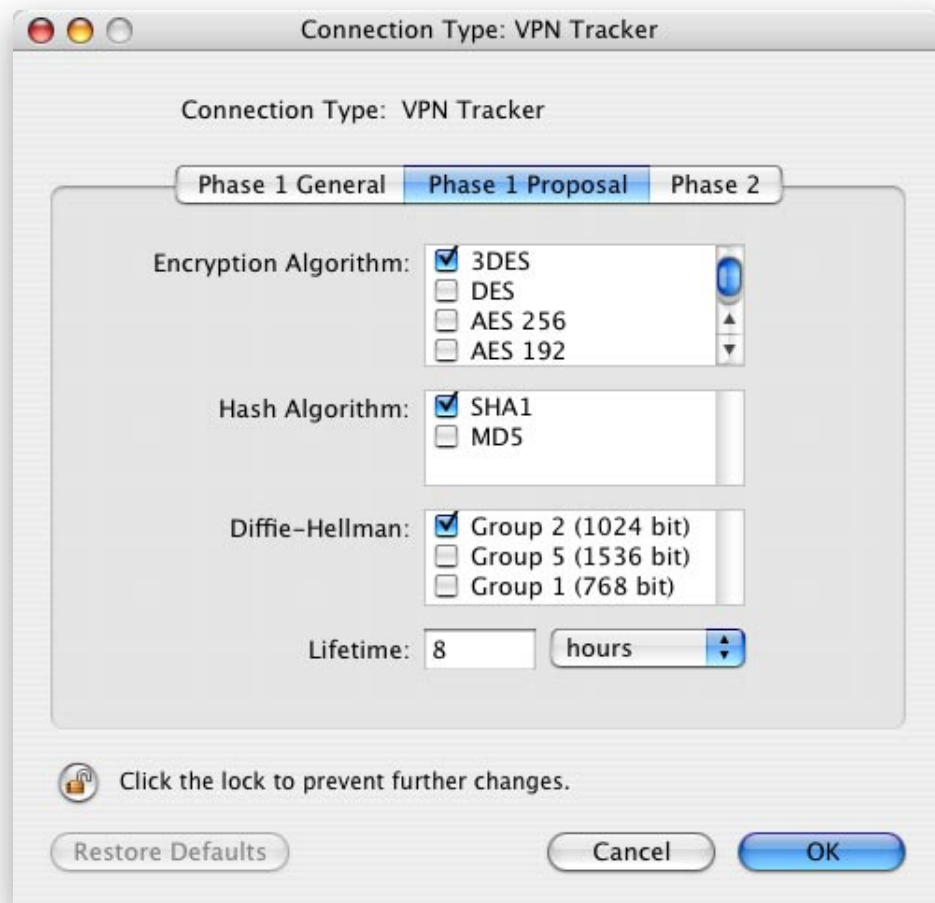
This option should be enabled for most configurations.

**Verify certificate:**

If certificates are being used for authentication, verify the remote certificate if enabled.

This option should be enabled for most configurations.

## Phase 1 Proposal



The following two settings specify the algorithms to be proposed to the VPN gateway for phase 1. It is recommended to enable all algorithms which are supported by your VPN gateway. You can rearrange the order in which the algorithms are proposed using drag and drop.

### Encryption Algorithm:

Specifies the encryption algorithms proposed for the phase 1 negotiation. Enable “3DES” and “DES” for maximum compatibility. Enable the AES algorithm and drag it to the top of the list for highest security.

Please note that the AES algorithm with key lengths of 192 and 256 bits is only available with a VPN Tracker Professional Edition license.

### Hash Algorithm:

Defines the hash algorithms proposed for the phase 1 negotiation. It is recommended to enable both options in the order “SHA1”, “MD5”.

### Diffie-Hellman:

Defines the groups proposed for the Diffie-Hellman exponentiations. Please note that only one group can be proposed when using Aggressive mode.

The majority of gateways use “Group 2 (1024 bit)”.

**Lifetime:**

Defines a lifetime for the ISAKMP-SA, after which the SA will expire and be renegotiated when necessary.

A value of 8 hours is recommended here.

## Phase 2



### Enable PFS:

Specifies the group of Diffie-Hellman exponentiations for PFS (Perfect Forward Secrecy) in phase 2. Uncheck the check box to disable PFS.

It is recommended to enable PFS using “Group 2 (1024 bit)” for increased security, if supported by the VPN gateway.

### Lifetime:

Defines a lifetime for the IPsec-SA. The connection will expire and be re-established after this period of time.

A lifetime of one hour is recommended.

The following two settings specify the algorithms to be used in the phase 2 proposals. It is recommended to enable all algorithms which are supported by your VPN gateway. You can rearrange the order in which the algorithms are proposed using drag and drop.

### Encryption Algorithm:

The algorithm to be used with ESP. You can enable all options except “No Encryption” for maximum compatibility. Drag “AES” or “Blowfish” to the top of this list for maximum security.

Please note that the AES algorithm with key lengths of 192 and 256 bits is only available with a VPN Tracker Professional Edition license.

**Authentication Algorithm:**

The algorithm to be used with ESP authentication and AH. It is recommended to enable both options in the order “HMAC SHA1”, “HMAC MD5”.

**Establish unique SAs for multiple networks:**

If enabled, VPN Tracker will establish a unique SA (Security Association) for each network when multiple local or remote networks are specified for a connection. Otherwise, the same SA will be used for all networks of a connection.

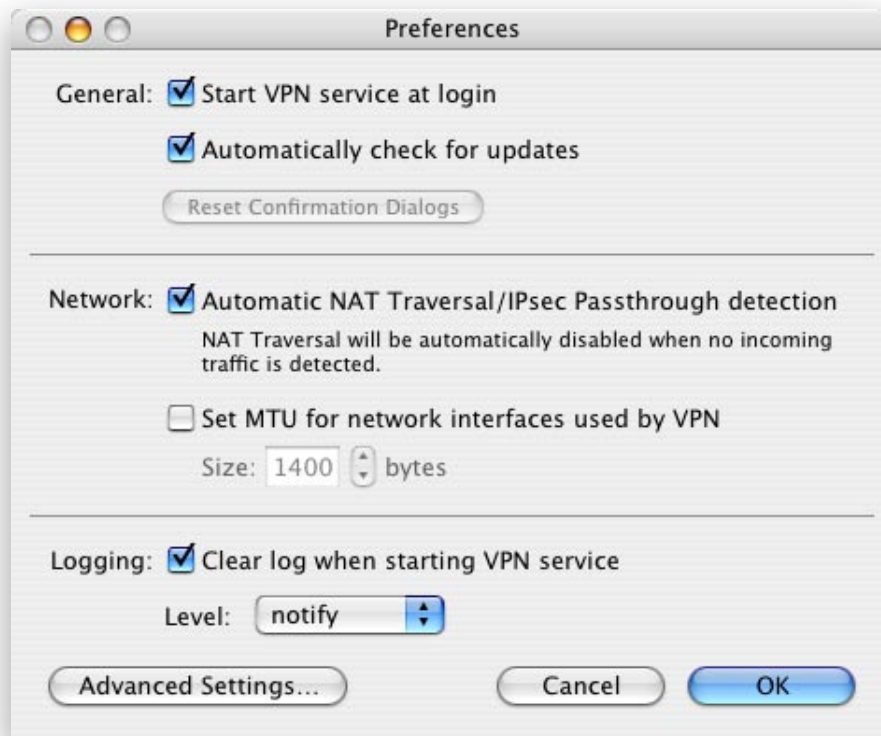
For VPN Tracker endpoints and most third-party VPN solutions, this option should be enabled. However, some vendors such as Watch Guard and Dray-Tek do not support unique SAs and this option should be disabled in order for multiple remote networks to work.

## The Log Window

Select “Show Log...” from the file menu to see details about the connection process. This is a valuable tool if you want to connect to VPN solutions which have not yet to be tested for interoperability with VPN Tracker.

Select “Clear Log” from the file menu to clear all log entries.

## Preferences



### General

#### Start VPN service at login:

Check this option to automatically start the VPN service when logging into your computer.

#### Automatically check for updates:

Enable this option to let VPN Tracker automatically check if your VPN Tracker installation is up to date.

#### Reset Confirmation Dialogs:

Click this button to reset all confirmation dialogs. This includes the “Don’t show again” option in XAUTH authentication dialogs and the “Remember selection for this router” option in the warning dialog for incompatible NAT routers.

The button is disabled if all confirmation dialogs are in their default state.

## **Network**

### **Automatic NAT Traversal/IPsec Passthrough detection:**

When you have enabled this option, VPN Tracker will automatically restart the VPN service with NAT Traversal disabled when no incoming traffic can be detected for a connection which is using NAT Traversal over UDP port 500 (i.e. older NAT Traversal implementations). This can happen when your NAT router is doing IPsec passthrough but is incompatible with NAT Traversal packets (e.g. Apple AirPort base stations).

This information is saved for each connection and router, which will automatically disable NAT Traversal the next time you use the connection with this router without the need to restart the VPN service.

Disable this checkbox to display a confirmation dialog instead of automatically performing the VPN service restart.

### **Set MTU for network interfaces used by VPN:**

Check this option if VPN Tracker should set the MTU (maximum transfer unit) value of all network interfaces which are being used for IPsec connections.

The value will be reset to the original value when you stop the VPN service. Setting a MTU value lower than the original (e.g. 1400 for Ethernet) often fixes problems with dropping or unstable connections.

## **Logging**

### **Clear log when starting VPN service:**

Check this option if VPN Tracker should clear the log windows every time you start or restart the VPN service.

### **Logging level:**

Here you can set the amount of data which will be written to the log file.

Select “notify” for normal logging, “debug” for extended logging (recommended if you want to get VPN Tracker working with a 3rd party VPN device or for support inquiries).

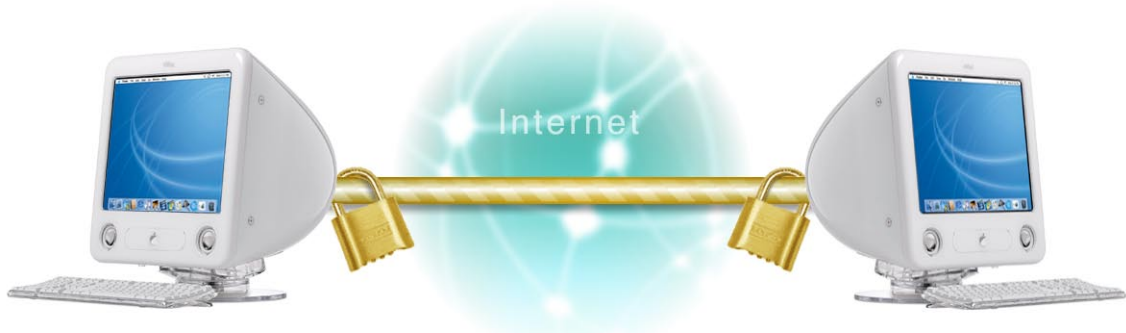
## Chapter 4:


# Configuration Examples

This chapter will show you how to configure popular VPN setup scenarios.

## Connection Between Two Macs Running VPN Tracker

VPN Tracker is a great solution if you want to exchange sensitive data between two Macs. The computers could both be in a Local Area Network (LAN), or connected to the internet with a dialup connection.



 = 2 x VPN Tracker Personal Edition

Please note that both Macs need to have a public IP address, i.e. they cannot be connected to the Internet through a router.

The steps required to setup the connection are the same for both sides:

- 1.) Create a new connection by clicking the “New...” button in the main window.
- 2.) Select “equinux” and “VPN Tracker” as the “Vendor” and “Model” in the “Connection” tab.
- 3.) In the “Network” tab, select “Host to Host” as the topology and enter the public IP address of the Mac you want to connect to as the “VPN Gateway Address”. Enter the IP address or host name of the remote host running VPN Tracker. If the remote host is on a dialup connection, you will have to get his IP address by phone, email etc.
- 4.) In the “Authentication” tab, choose “Pre-shared key” and click the “Edit...” button. Enter a pre-shared key, which must be the same for both sides of the connection.
- 5.) Click “OK”, dial into the internet if you are not connected already, and click “Start VPN” to establish the VPN connection.

## Connecting to an Office LAN

Using VPN Tracker, connecting to an office network when you are on the road or from your dialup or DSL internet connection at home is both easy and secure.



 = 1 x VPN Tracker Personal Edition

For this scenario, you will need a VPN gateway on the office side, acting as the internet gateway for the computers in your office LAN. We have tested VPN Tracker with a large number of VPN gateways and provide device specific step-by-step guides on our website, which describe the setup process in more detail:

<http://www.vpntracker.com/interop>

*Tip: When editing a connection in VPN Tracker, you can use the “How-To” button to show the manual of the selected device.*

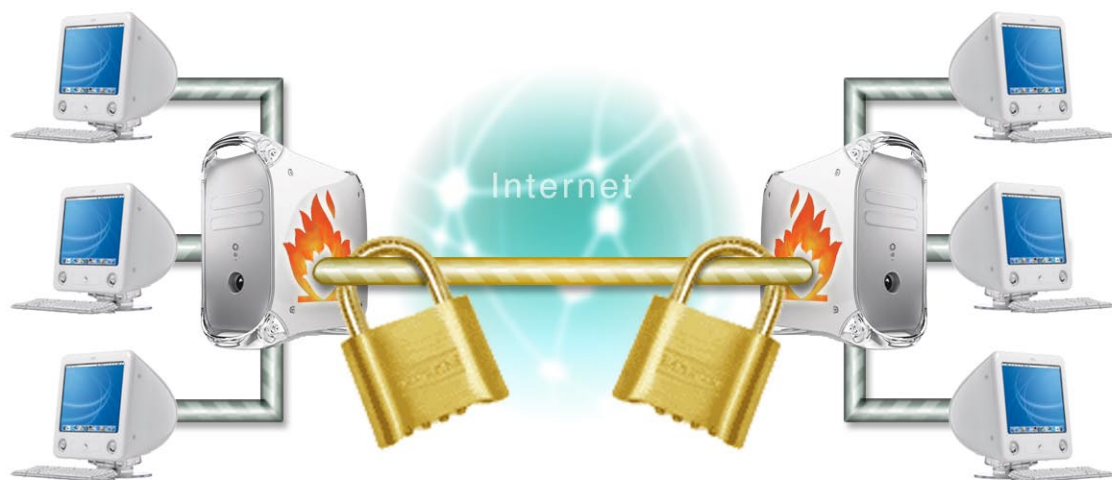
The following steps outline the general procedure when setting up a VPN connection to a office network. Please also see Chapter 3 and our step-by-step guide if available for your device.


- 1.) Create a new connection by clicking the “New...” button in the main window and enter a name for the connection (e.g. “Office”).
- 2.) Select the vendor and device name of your VPN gateway in the “Connection” tab.
- 3.) Go to the “Network” tab and enter the public IP address or DNS name of your VPN gateway as the “VPN Gateway Address”.
- 4.) Enter the address and subnet mask of your office LAN in the “Remote Network/ Mask” fields (e.g. “192.168.1.0” and “255.255.255.0”).
- 5.) Go to the “Authentication” tab and enter your manner of authentication, e.g. enter your pre-shared key.
- 6.) Click “OK” and start the VPN service in order to establish the VPN connection.

After finishing the connection process, VPN Tracker should show a green status indicator next to your new connection, which indicates that the connection has been established. You can now access any network service in your office LAN. If you want to mount a file share from your office file server, select “Connect to Server...” from the “Go To” menu in the Finder and enter the IP address of your file server.

## Connecting Branch Offices

VPN Tracker makes it easy to connect the Local Area Networks (LANs) of branch offices with each other. While having maximum security, VPN Tracker eliminates the high costs of leased lines.



 = 2 x VPN Tracker Professional Edition

For this scenario, VPN Tracker needs to be installed on both sides on Macs acting as the default Internet gateway for all computers in the respective branch office LAN. Also, both Macs need to have a direct Internet connection (i.e. not connected to a NAT router) and a public static IP address.

- 1.) Create a new connection by clicking the “New...” button in the main window and enter a name for the connection (e.g. “Branch office”).
- 2.) Select “equinux” and “VPN Tracker” as the “Vendor” and “Model” in the “Connection” tab.
- 3.) Go to the “Network” tab and select “Network to Network” as the “Topology”.
- 4.) Enter the public IP address or DNS name of the Mac in the other office as the “VPN Gateway Address”.
- 5.) Enter the address and subnet mask of your local LAN in the “Local Network/Mask” fields (e.g. “192.168.1.0” and “255.255.255.0”).
- 6.) Enter the address and subnet mask of the remote LAN in the “Remote Network/Mask” fields (e.g. “192.168.2.0” and “255.255.255.0”).
- 7.) If you do not want VPN Tracker to establish the connection from this end,

uncheck the “Initiate Connection from this end” check box in the “Connection” tab to tell VPN Tracker to wait for a connection request from the other office.

8.) Click “OK” and start the VPN service.

Repeat this process for the Mac running VPN Tracker in the other branch office.

After finishing the connection process, VPN Tracker should show a green status indicator next to your new connection if VPN Tracker has already been started in the other branch office. This indicates that the VPN connection has been established. You should now be able to access the remote network from all computers in your local network, including the Mac running VPN Tracker.

## Securing an AirPort Network

Did you know that the security algorithms built into AirPort have already been hacked? This means that it is possible to intercept your WEP-encrypted AirPort traffic!

VPN Tracker helps you to once again secure your AirPort network. And here is how. All you need is another wired Mac client connected to the AirPort base station. This Mac will decrypt the traffic going to itself, to other computers in the LAN and to the Internet.



Please note that you will need one VPN Tracker Professional license for the wired Mac client. For each Mac in the AirPort network, a VPN Tracker Personal license is adequate.

Here is our example setup:

- We have three iBooks which are connected to the base station via AirPort. Their IP addresses are 192.168.1.3, 192.168.1.4 and 192.168.1.5.
- We have a PowerMac which is connected to the base station with a network cable. It's IP address is 192.168.1.2
- The base station itself has the internal IP address 192.168.1.1 and it is connected to the Internet with a dial-up connection.

First we have to prepare the PowerMac for decrypting the network traffic and to forward Internet traffic to the base station. Go to the System Preference's Network pane and make sure you have entered the base station's IP address as the router and DNS server. Go to the Sharing pane of the System Preferences and enable Internet sharing in the Internet tab panel. The PowerMac is now able to route network traffic going to the internet through the base station.

Take the iBooks and make sure that all of them have set the IP address of the PowerMac as router and DNS server.

Next, create one connection on the PowerMac for each iBook:

- 1.) Click the "New..." button in the VPN Tracker main window to create a new connection and enter a name for the connection (e.g. "iBook 1").
- 2.) Select "equinux" and "VPN Tracker" as the "Vendor" and "Model" in the "Connection" tab and uncheck the "Initiate connection from this end" check box.
- 3.) Go to the "Network" tab and select "Network to Network" as the "Topology".
- 4.) Enter the IP address of the iBook you are configuring as both the "VPN Gateway Address" and the "Remote Network". Enter "255.255.255.255" as the "Mask" for the remote network.
- 5.) Enter "0.0.0.0" and "0.0.0.0" in the "Local Network/Mask" fields.
- 6.) Go to the "Authentication" tab and enter a pre-shared key for this connection.
- 7.) Click "OK" to save the connection.

Repeat steps 1 through 7 for each iBook. Click "Start VPN" when you are finished. Please note that these connections are always established from the iBook end.

On each iBook, please configure VPN Tracker as follows:

- 1.) Click the "New..." button in the VPN Tracker main window to create a new connection and enter a name for the connection (e.g. "Secure AirPort").
- 2.) Select "equinux" and "VPN Tracker" as the "Vendor" and "Model" in the "Connection" tab and uncheck the "Initiate connection from this end" check box.
- 3.) Go to the "Network" tab and select "Host to Everywhere" as the "Topology".
- 4.) Enter the IP address of the PowerMac (e.g. "192.168.1.2") as the "VPN Gateway Address".
- 5.) Go to the "Authentication" tab and enter the pre-shared key for this connection. The pre-shared key needs to be the same as the one you have entered for this

connection on the PowerMac.

6.) Click “OK” to save the connection.

You can now start the VPN service on the iBook. After finishing the connection process, VPN Tracker should show a green status indicator next to your new connection. You now have a 100% secure AirPort network!

## Chapter 5:

# Interoperability

This chapter will show you how VPN Tracker works with other IPsec solutions.

## Introduction

As there are many different IPsec based solutions (hard- and software) on the market and new solutions emerge daily, we can't provide a complete list of all VPN Tracker compatible devices.

Moreover, compatible for one operational area doesn't mean compatible in a slightly different configuration. That implies two important conclusions:

First, if we name a hard- or software to be "compatible" with VPN Tracker, that means we successfully tested the given system in our labs with VPN Tracker. It does NOT mean that VPN Tracker works in your particular configuration of the given system.

Second, if we do not state your device as compatible to VPN Tracker, that does NOT mean that it isn't. IPsec is a standard protocol for network encryption, so VPN Tracker is likely to work with your IPsec-compatible devices. Download the demo version and try out different settings starting with the "Other" connection type or discuss your issues with users and developers on the VPN Tracker talk mailing list

<http://www.vpntracker.com/community>

We are glad to hear from you.

## List of Known Compatible VPN Gateways

With the release of this manual, VPN Tracker has been successfully tested in our labs with the following VPN gateways.

### Compatible Software

- Check Point
- Clavister
- FreeBSD/OpenBSD/NetBSD
- FreeS/WAN (Linux)
- F-Secure
- PGPnet
- Symantec
- Windows 2000/XP
- Novell BorderManager

### Compatible Hardware

- Amaranten
- Asanté
- Cisco
- CyberGuard
- DrayTek
- Fortinet
- Ingate
- LANCOM
- NETGEAR
- Netopia
- NetScreen
- NETASQ
- Nokia (Check Point)
- Nortel
- Pyramid BenHur II
- SnapGear
- SonicWALL
- WatchGuard
- ZyXEL

## Manuals for Compatible Devices

The list of VPN Tracker compatible devices is growing daily. Due to the large number of parameters for IPsec connections and the increasing complexity of VPN gateways, it's often difficult to setup a VPN connection. That is why we offer device specific manuals as appendices to this core manual. These appendices are available separately on our web site:

<http://www.vpntracker.com/interop>

*Tip: When editing a connection in VPN Tracker, you can use the “How-To” button to show the manual of the selected device.*

We are continually extending the list of tested devices, please check back often.

## Appendix A:

# Customizing the Authorization Behavior

VPN Tracker uses the Mac OS X Authorization Services to carry out restricted operations and to lock connection settings from being modified. This appendix describes how a system administrator can customize the authorization services for different use cases of VPN Tracker, e.g. to disallow a non-admin user to start and stop the VPN service.

## Right Keys Used by VPN Tracker

The Mac OS X Authorization Services are using so-called “rights” which are specified by “keys” in order to distinguish different actions from different applications. VPN Tracker uses the following right keys to carry out the different actions requiring authorization:

- `com.equinux.VPNTracker.run`  
This right is checked when the VPN service is started, stopped or restarted.
- `com.equinux.VPNTracker.edit`  
This right is checked when editing, deleting or duplicating a connection or connection type as well as when importing or exporting a connection.
- `com.equinux.VPNTracker.secrets`  
This right is checked when editing the pre-shared key or the certificate authentication settings. It is also checked for all actions in the Certificate Manager, e.g. when creating certificates, and when creating a new connection.

## Default Policies

Under Mac OS X 10.3 and higher, VPN Tracker installs entries in the policy database for the following keys:

- `com.equinux.VPNTracker.run`  
The default policy allows any user (admin and non-admin) to start, stop and restart the VPN service.
- `com.equinux.VPNTracker.edit`  
The default policy allows administrators to do edit actions (as specified above). After authenticating, the authorization stays valid forever.

- `com.equinux.VPNTracker.secrets`  
This right is governed by the system's default policy: only administrators are allowed to edit secrets. Authentication stays valid for 5 minutes.

For Mac OS X 10.2, all rights are governed by the system's default policy: all actions have to be authenticated. Authentication stays valid for 5 minutes.

## Customizing the Policy Database

The policy database contains a set of rules the system uses to authorize rights for a user. Each rule consists of a set of attributes which may be changed by the system administrator and determine the level of security on his computer.

This section describes how a user can modify the policy database. For more information on the policy database and the Authorization Services in general, please refer to the Mac OS X Authorization Services documentation which can be found at:

[http://developer.apple.com/documentation/Security/Conceptual/authorization\\_concepts/](http://developer.apple.com/documentation/Security/Conceptual/authorization_concepts/)

The policy database is stored as the XML property list file `/etc/authorization`. As the format of this file has changed between Mac OS X 10.2 and 10.3, please refer to the section below appropriate to your system version.

### Editing the policy database file (Mac OS X 10.2)

In order to edit the policy database file, please issue the following command in a new terminal window:

```
sudo pico /etc/authorization
```

After entering your admin password, the contents of the `/etc/authorization` file will be displayed in the terminal window. Please move the cursor down to the very bottom of the file by using the arrow down or page down key.

On the bottom of the file you will find a comment as follows:

```
<!-- All other rights will be matched by this rule.  
      Credentials remain valid 5 minutes after they've been obtained.  
      An acquired credential is shared amongst all clients.  
-->
```

Place the cursor in the empty line above this comment and type in the following text:

```
<key>com.equinux.VPNTracker.run</key>  
<dict>  
  <key>group</key>
```

```
    <string>staff</string>
    <key>shared</key>
    <true/>
    <key>allow-root</key>
    <true/>
</dict>
```

Please make sure to type in the text exactly as specified above. When finished, press Control-X, then “Y” and enter.

All users of the group “staff” (to which every user on Mac OS X is automatically added) will now be able to authenticate for starting/stopping/restarting VPN service. This authentication is only required for the first action performed. For all subsequent actions, the system will remember the authorization, even across reboots.

Please note that all other actions like editing connections or connection types are still protected by the Authorization Services. If you want all VPN Tracker actions to be available without authorization, just replace the key “com.equinux.VPNTracker.run” with “com.equinux.VPNTracker.”. Make sure to end this string with a single dot.

## **Editing the policy database file (Mac OS X 10.3 and higher)**

Please refer to the Mac OS X Authorization Services reference for details on editing the policy database under Mac OS X 10.3 and higher.

## Appendix B:

# Scripting

This appendix describes how VPN Tracker can be configured to execute shell or perl scripts when certain events occur.

Please note that a VPN Tracker Professional Edition license is required to use the scripting feature.

## The Actions Folder

The actions folder is a folder within the VPN Tracker Application Support folder where a user can store the event scripts. To enable event actions, create a folder named “actions” (all lowercase) with the following path:

```
/Library/Application Support/VPN Tracker/actions
```

## Action Events

For each event you want to handle, you will have to place an executable script (e.g. shell script) within the actions folder. This script needs to have the name of the event as specified below. Please note that all scripts will be executed as the “root” user, which means that you have full access to the system.

VPN Tracker will dispatch the following events:

- **connection-pre**  
This script is executed right before connection establishment is being initiated.
- **connection-phase1**  
This script is executed when IPsec phase 1 (ISAKMP-SA) has been completed successfully.
- **connection-up**  
This script is executed when a connection has been established successfully.
- **connection-error**  
This script is executed when an error has occurred during connection establishment.
- **connection-expired**  
This script is executed when IPsec phase 2 (IPsec-SA) has expired. The connection will automatically be re-established once you try to access any remote services.

- **init**  
This script is executed right before the VPN service will be initialized.
- **quit-pre**  
This script is executed right before the VPN service is stopped. At this time, all established connections will still be working.
- **quit-post**  
This script is executed when the VPN service has been stopped.

## Script Parameters

The scripts will be called with the following parameters:

```
scriptname source-endpoint destination-endpoint source-network destination-network
```

For example, when a connection has been established, the command line could look something like this:

```
connection-up 192.168.1.1 212.18.13.66 10.1.2.3/32 192.168.0.0/24
```

If for a specific event a parameter is not available or not applicable, the parameter “n/a” will be passed. For example, the quit events will have four parameters of “n/a”.

## Using AppleScript

By default, VPN Tracker can only execute command-line scripts, i.e. shell and perl scripts. However, using the command-line tool `osascript`, it is possible to execute AppleScripts from within a shell script. For example, if you want to execute an AppleScript upon connection establishment, your connection-up script could look like this:

```
#!/bin/bash  
/usr/bin/osascript /Users/username/connection-up.scpt
```

You will need to replace “username” with your Mac OS X user account name. This script assumes that you have an AppleScript script file named “connection-up” within your home folder.

Please note that AppleScripts will only work if a user is logged in while the script is being executed.

Appendix C:

# Frequently Asked Questions

For an up-to-date list of our frequently asked questions (FAQ) about VPN Tracker and equinux software in general, please visit our web site at:

<http://www.vpntracker.com/faq>