e·quinux

VPN Tracker for Mac OS X

How-to:

Interoperability with

ZyXEL Internet Security Gateways

Rev. 4.0

1. Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a ZyXEL Internet Security Gateway. The whole ZyWALL product range from ZyWALL 1 to ZyWALL 100 should be compatible with VPN Tracker – they only differ in the number of simultaneous IPsec connections. The ZyWALL 35 and 70 appliances also support “Extended Authentication” (XAUTH).

Additionally, the Prestige 652 / 653 product series are also compatible with VPN Tracker.

The ZyXEL gateway is configured as a router connecting a company LAN to the Internet.

The first example outlines a connection scenario of a dial-in Mac connecting to a ZyXEL Gateway.

The second example depicts a LAN-to-LAN connection of VPN Tracker on one side and ZyXEL gateway on the other side.

This paper is only a supplement to, not a replacement for, the instructions that have been included with your ZyXEL gateway. Please be sure to read those instructions and understand them before starting.

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

EQUINUX 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 EQUINUX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2. Prerequisites

First you should upgrade your ZyXEL gateway to the most recent ZyNOS firmware version.[1] The latest firmware release for your ZyXEL gateway can be obtained from

http://www.zyxel.com/support/download.php

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

- If you connect a dial-in Mac without its own subnet to the ZyXEL gateway you need a personal license.
- If you want to establish a LAN-to-LAN connection from your Mac to the ZyXEL gateway, you need a VPN Tracker professional license.
- If you connect a dial-in Mac without it's own subnet to multiple Networks on ZyXEL side you also need the professional license.

VPN Tracker is compatible with Mac OS X 10.2+5, 10.3 and 10.4.

[1] We've tested firmware version V3.50 and V.3.52 successfully.

3. Connecting a VPN Tracker host to a ZyXEL gateway

In this example the Mac running VPN Tracker is directly connected to the Internet via a dialup or PPP connection.[2]

The ZyXEL gateway is configured in NAT mode and has the static WAN IP address 169.1.2.3 and the private LAN IP address 192.168.1.1. The stations in the LAN behind the ZyXEL gateway use 192.168.1.1 as their default gateway and should have a working Internet connection.

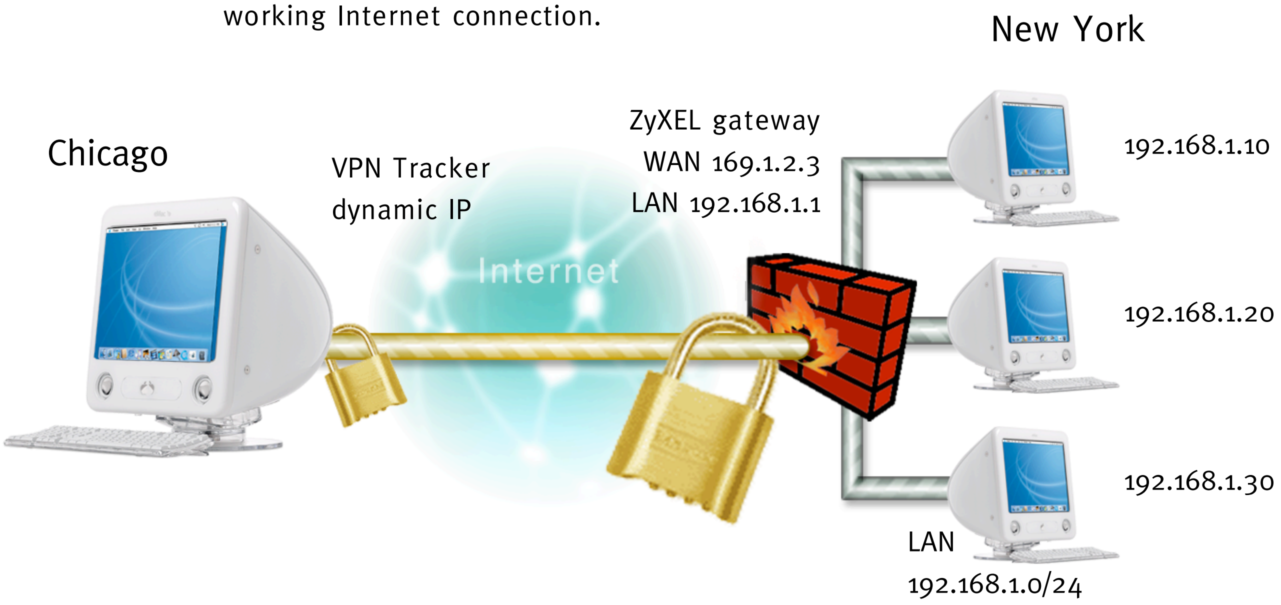
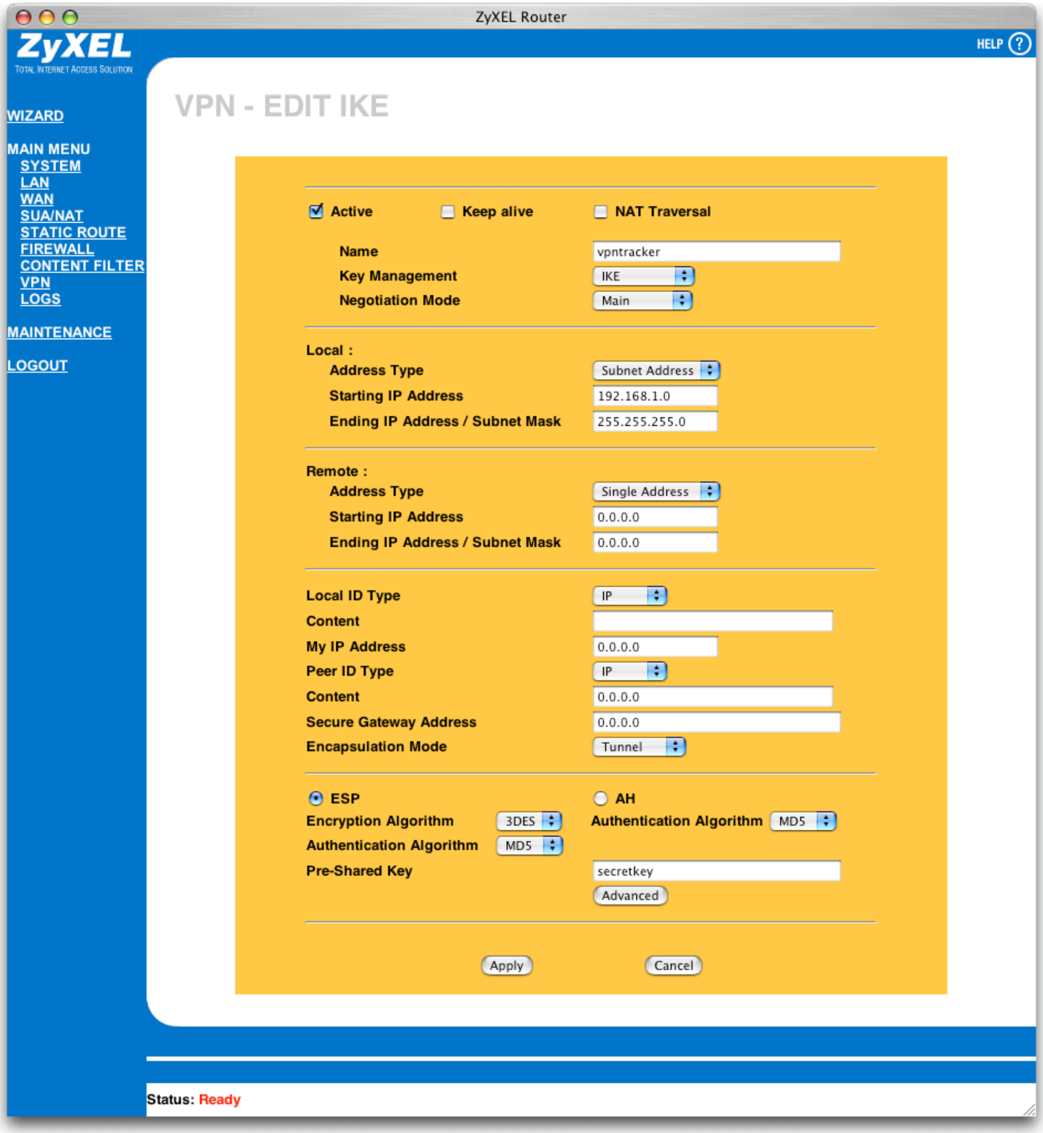


Figure 1: VPN Tracker – ZyXEL gateway connection diagram (host to network)

[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.

3.1 ZyXEL Configuration

On a ZyXEL ZyWALL create a new IPsec SA with the following settings:



VPN - EDIT IKE

☑ Active ☐ Keep alive ☐ NAT Traversal

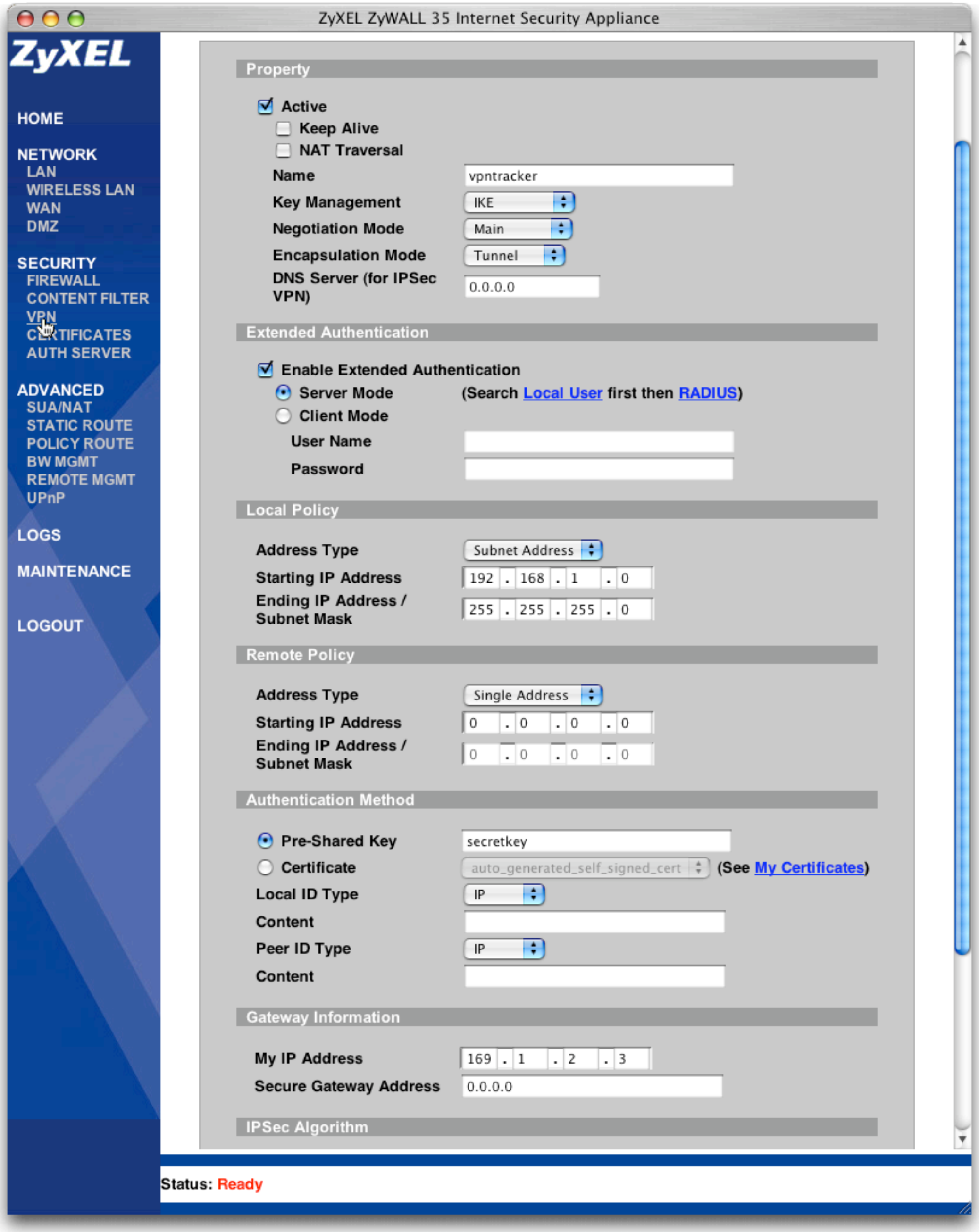
Name	vpntracker
Key Management	IKE
Negotiation Mode	Main
Local :	
Address Type	Subnet Address
Starting IP Address	192.168.1.0
Ending IP Address / Subnet Mask	255.255.255.0
Remote :	
Address Type	Single Address
Starting IP Address	0.0.0.0
Ending IP Address / Subnet Mask	0.0.0.0
Local ID Type	IP
Content	
My IP Address	0.0.0.0
Peer ID Type	IP
Content	0.0.0.0
Secure Gateway Address	0.0.0.0
Encapsulation Mode	Tunnel

● ESP ○ AH

Encryption Algorithm	3DES	Authentication Algorithm	MD5
Authentication Algorithm	MD5		
Pre-Shared Key		secretkey	

Status: Ready

Figure 2: ZyXEL ZyWALL – ZyNOS 3.52 - VPN settings



Property

☑ Active
□ Keep Alive
□ NAT Traversal

Name: vpntracker
Key Management: IKE
Negotiation Mode: Main
Encapsulation Mode: Tunnel
DNS Server (for IPSec VPN): 0.0.0.0

Extended Authentication

☑ Enable Extended Authentication
● Server Mode (Search Local User first then RADIUS)
○ Client Mode
User Name:
Password:

Local Policy

Address Type: Subnet Address
Starting IP Address: 192 . 168 . 1 . 0
Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0

Remote Policy

Address Type: Single Address
Starting IP Address: 0 . 0 . 0 . 0
Ending IP Address / Subnet Mask: 0 . 0 . 0 . 0

Authentication Method

● Pre-Shared Key: secretkey
○ Certificate: auto_generated_self_signed_cert (See My Certificates)
Local ID Type: IP
Content:
Peer ID Type: IP
Content:

Gateway Information

My IP Address: 169 . 1 . 2 . 3
Secure Gateway Address: 0.0.0.0

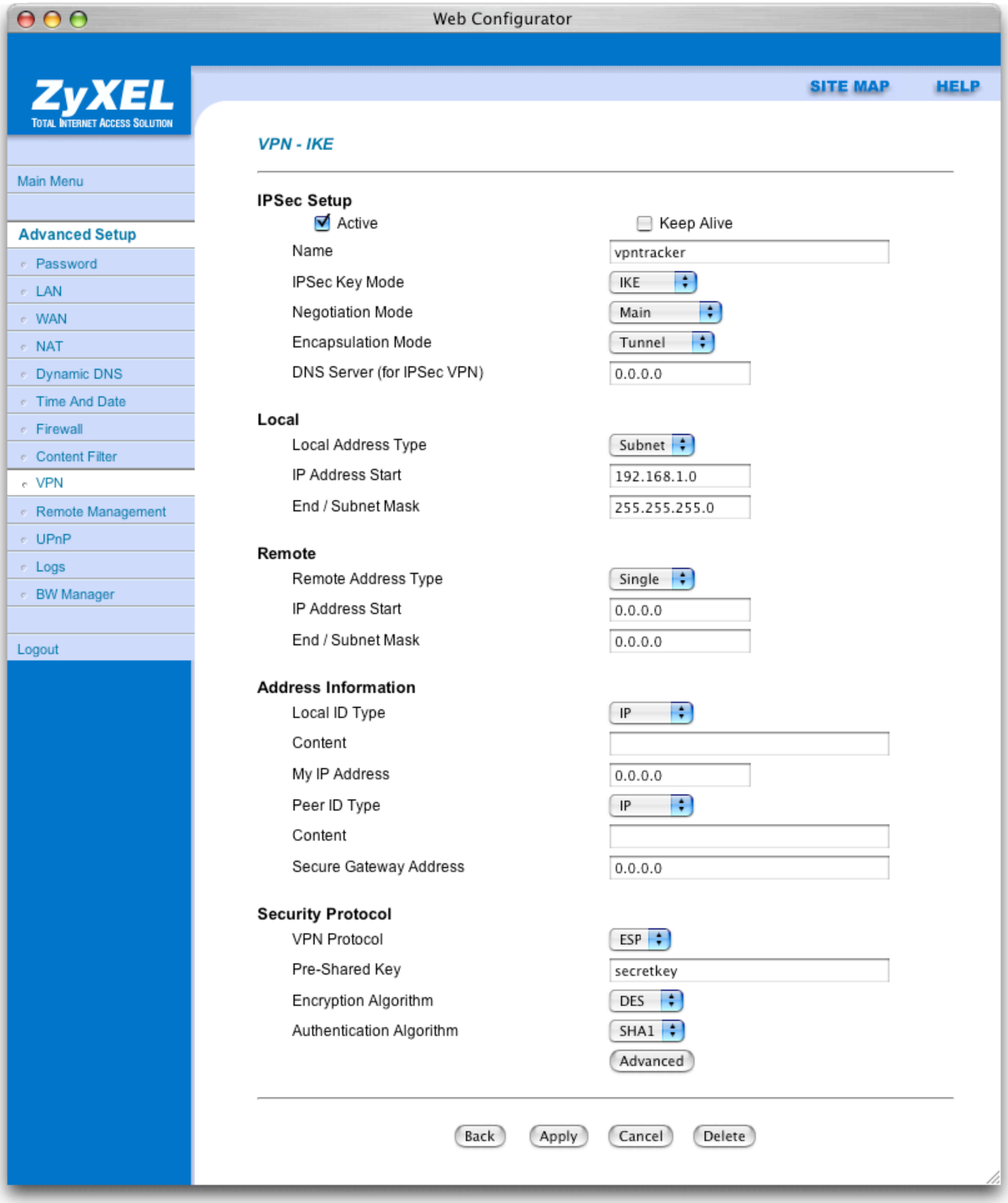
IPSec Algorithm

Status: Ready

Figure 3: ZyXEL ZyWALL - ZyNOS 3.62 - VPN settings

Please note: In order to authenticate multiple clients with different credentials, please „Enable”. In this case you'll also need to check “XAUTH” in your VPN Tracker Authentication settings. Please refer to the ZyXEL manual for further assistance regarding User management.

On a ZyXEL Prestige create a new IPsec SA with the following settings:



VPN - IKE

IPSec Setup

☑ Active ☐ Keep Alive

Name	vpntracker
IPSec Key Mode	IKE
Negotiation Mode	Main
Encapsulation Mode	Tunnel
DNS Server (for IPSec VPN)	0.0.0.0

Local

Local Address Type	Subnet
IP Address Start	192.168.1.0
End / Subnet Mask	255.255.255.0

Remote

Remote Address Type	Single
IP Address Start	0.0.0.0
End / Subnet Mask	0.0.0.0

Address Information

Local ID Type	IP
Content	
My IP Address	0.0.0.0
Peer ID Type	IP
Content	
Secure Gateway Address	0.0.0.0

Security Protocol

VPN Protocol	ESP
Pre-Shared Key	secretkey
Encryption Algorithm	DES
Authentication Algorithm	SHA1

Figure 4: ZyXEL Prestige - VPN settings

Make sure to check the „Active“ box at the top of the page.

The „Secure Gateway Address“ field should be set to 0.0.0.0 to grant access to arbitrary dynamic remote IP addresses. In this case the options in the „Remote“ part are irrelevant for the ZyXEL gateway.

The advanced options can be left at the default setting.

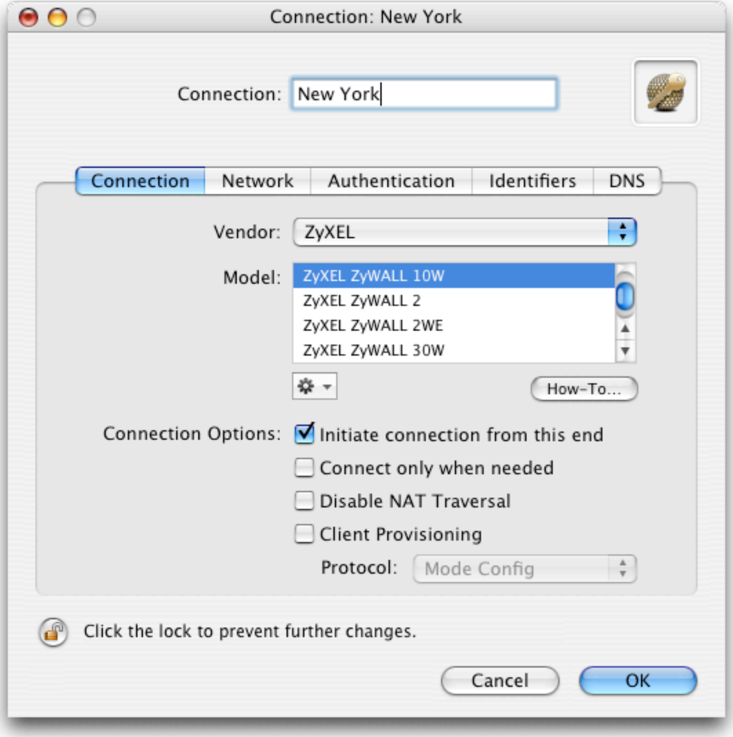
Please note: The ZyXEL gateway by default uses relatively weak encryption settings. If you want to have maximal security you should change the encryption settings in the advanced options to 3DES and SHA1 for both phase 1 and phase 2. Caution: If you change the encryption algorithms for phase 1 in the advanced options you have to change these options in the Connection Type definition in VPN Tracker as well to match the selected algorithms.

3.2 VPN Tracker Configuration

Step 1

Add a new connection with the following options:

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



Connection: New York

Connection: New York

Vendor: ZyXEL

Model: ZyXEL ZyWALL 10W

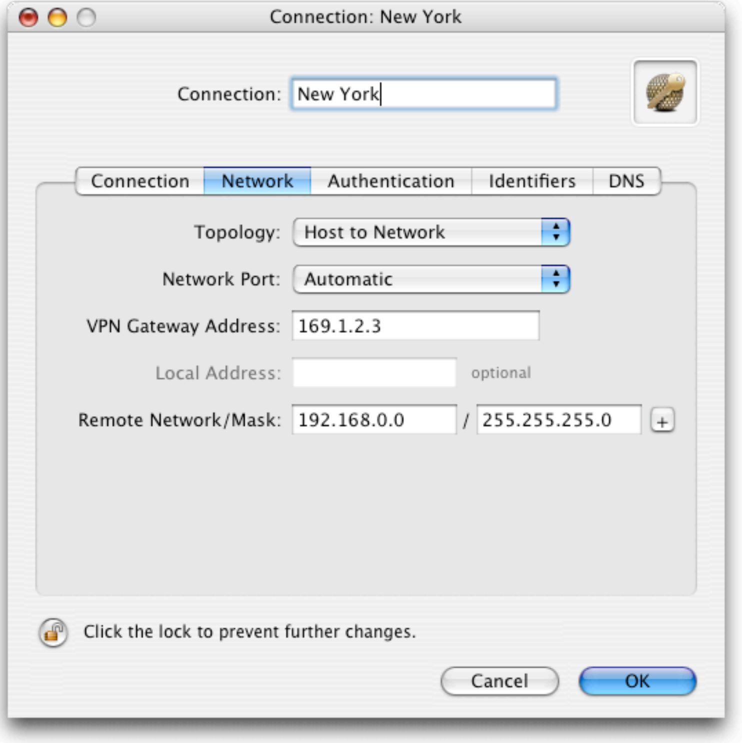
Connection Options:
☑ Initiate connection from this end
□ Connect only when needed
□ Disable NAT Traversal
□ Client Provisioning
Protocol: Mode Config

Click the lock to prevent further changes.

Figure 5: VPN Tracker - Connection settings

Step 2 Change your Network Settings:

- VPN Server Address: public IP address of your VPN Gateway (e.g. 169.1.2.3)
- Remote Network/Mask: network address and netmask of the remote network (eg. 192.168.1.0/255.255.255.0).


Connection: New York
Connection | Network | Authentication | Identifiers | DNS
Click the lock to prevent further changes.
Cancel
OK

Connection: New York

Topology: Host to Network

Network Port: Automatic

VPN Gateway Address: 169.1.2.3

Local Address: optional

Remote Network/Mask: 192.168.0.0 / 255.255.255.0 +

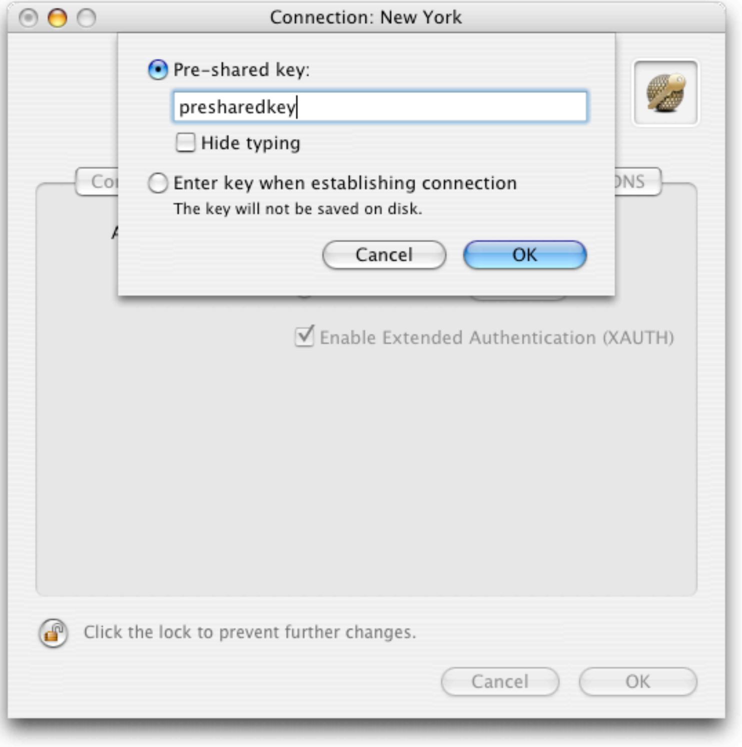
Figure 6: VPN Tracker – Network settings

Please note: In order to access multiple remote networks simultaneously, just add them by pressing the Plus-button.[3]

[3] For this step VPN Tracker Professional Edition is needed.

Step 3 Change your Authentication Settings:

- Pre-shared key: the same Pre-shared key as in the ZyXEL configuration.
- Enable XAUTH if the corresponding option is enabled on the ZyXEL.


Connection: New York

● Pre-shared key:

presharedkey

□ Hide typing

○ Enter key when establishing connection

The key will not be saved on disk.

☑ Enable Extended Authentication (XAUTH)

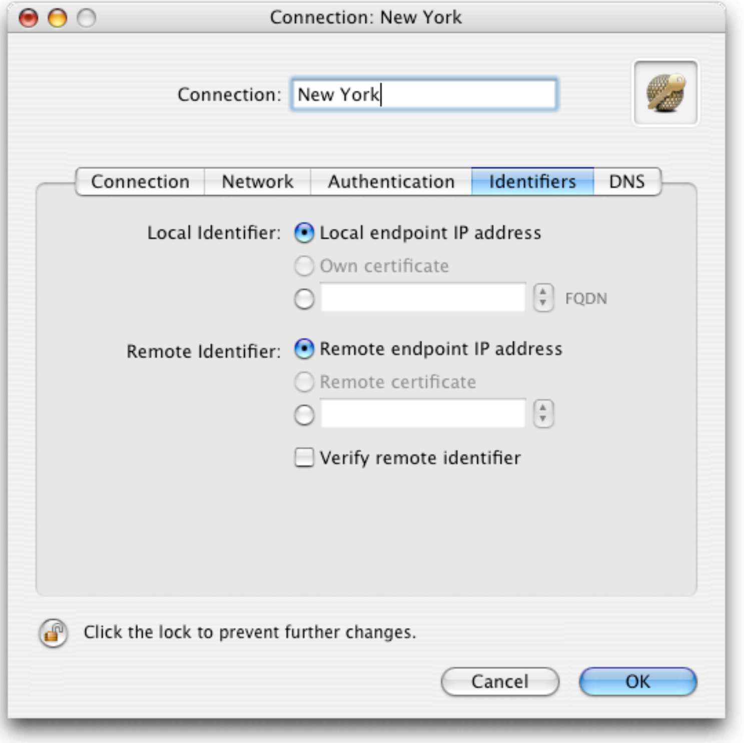
Click the lock to prevent further changes.

Figure 7: VPN Tracker - Authentication settings

Step 4

Identifier Settings:

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



Connection: New York

Connection: New York

Local Identifier: ● Local endpoint IP address

○ Own certificate

○ FQDN

Remote Identifier: ● Remote endpoint IP address

○ Remote certificate

○

□ Verify remote identifier

Click the lock to prevent further changes.

Figure 8: VPN Tracker - Identifier settings

Step 5

Save the connection and Click „Start IPsec“ in the VPN Tracker main window.

You're done. After 10-20 seconds the red status indicator for the connection should change to green, which means you're securely connected to the ZyXEL. 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 ZyXEL network from the dialed-in Mac in the "Terminal" utility:

```
ping 192.168.1.10
```

⇢ Troubleshooting

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. Below you can find a list of common error messages in the ZyXEL log file:

Log message:

```
!!No proposal chosen
```

Solution: ⇢ Check the Phase 1 algorithm and authentication settings.

Log message:

```
Start Phase 2: Quick Mode
!!No proposal chosen
```

Solution: ⇢ Check the Phase 2 Perfect Forward Secrecy settings.

Log message:

```
Rule [1] Verifying Local ID failed:
```

Solution: ⇢ Check the Remote Network settings in VPN Tracker.

4. Setting up a LAN-to-LAN connection

In this example the Mac running VPN Tracker Professional is directly connected to the Internet via an Ethernet or dialup or PPP connection. The WAN side IP address can be dynamically or statically assigned.

The gateway Mac running VPN Tracker is configured as a router that connects the LAN behind the gateway Mac (10.0.0.0/24) to the Internet. Therefore, Internet Sharing must be enabled on the gateway Mac.

The LAN IP address of the gateway Mac is 10.0.0.1 in our example. The client workstations in the LAN must be configured with the gateway Mac as their router.

The ZyXEL gateway is permanently connected to the Internet and has the static WAN IP address 169.1.2.3 and the private LAN IP address 192.168.1.1. The Stations in the LAN behind the ZyXEL gateway use 192.168.1.1 as their default gateway and should have a working Internet connection.

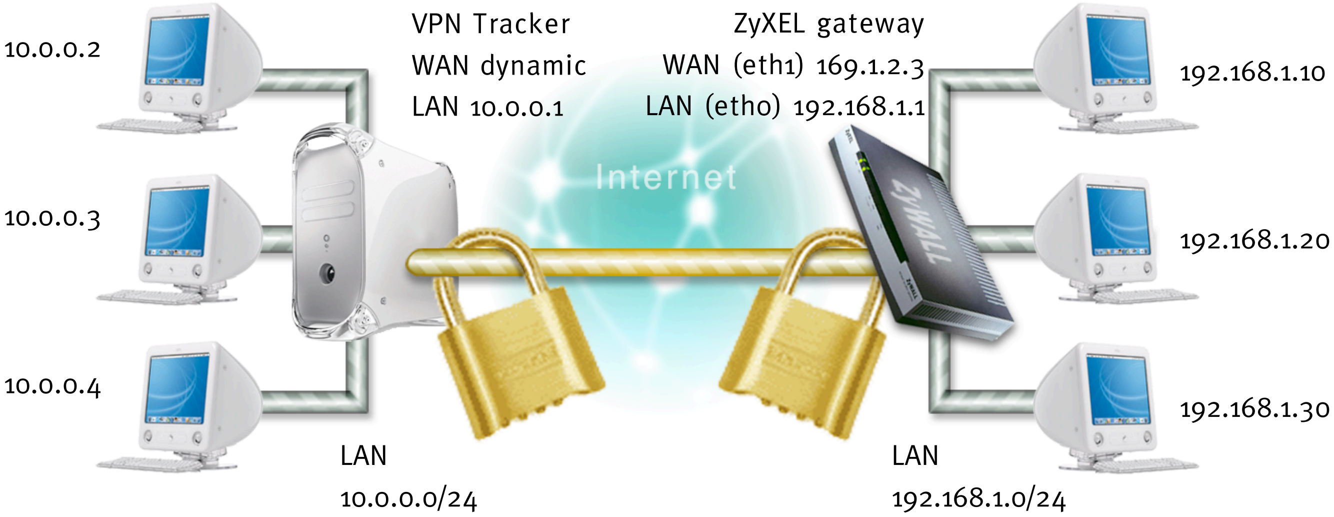


Figure 9: VPN Tracker - ZyXEL - Connection diagram

4.1 ZyXEL Configuration

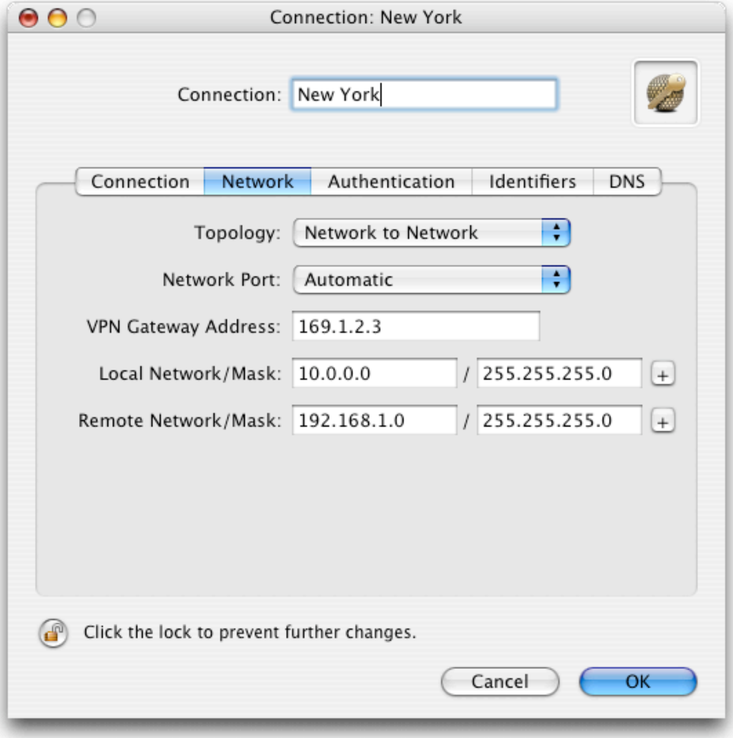
Please refer to section 3.1 for the ZyXEL configuration. Please make sure, that the remote network is set to 0.0.0.0 in order to allow arbitrary remote networks to connect. If the remote gateway has a static IP address you can enter it in the ZyXEL configuration.

4.2 VPN Tracker Configuration

Step 1 Please refer to section 3.2 for Pre-shared key authentication.

Step 2 Change your Network Settings:

- Topology: Network to Network
- VPN Server Address: public IP address of your VPN Gateway (e.g. 169.1.2.3)
- Local Network Mask: network address and netmask of the local network (e.g 10.0.0.0/255.255.255.0)
- Remote Network/Mask: network address and netmask of the remote network (eg. 192.168.1.0/255.255.255.0).



Connection: New York

Connection: New York

Topology: Network to Network

Network Port: Automatic

VPN Gateway Address: 169.1.2.3

Local Network/Mask: 10.0.0.0 / 255.255.255.0

Remote Network/Mask: 192.168.1.0 / 255.255.255.0

Click the lock to prevent further changes.

Figure 10: VPN Tracker - Network settings

Step 3-5 Please refer to section 3.2.