



VPN Configuration Guide

ZyXEL ZyWALL 5 / 2WG

Revision 1.0.0

equinux AG and equinux USA, Inc.

© 2007 equinux USA, Inc. All rights reserved.

Under the copyright laws, this manual may not be copied, in whole or in part, without the written consent of equinux AG or equinux USA, Inc. Your rights to the software are governed by the accompanying software license agreement.

The equinux logo is a trademark of equinux AG and equinux USA, Inc., registered in the U.S. and other countries.

Every effort has been made to ensure that the information in this manual is accurate. equinux is not responsible for printing or clerical errors.

Manual Edition 1.0.0

Created using Apple Pages.

www.equinux.com

Apple, the Apple logo, iBook, Mac, Mac OS, MacBook, PowerBook are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

Finder and Mail are trademarks of Apple Computer, Inc. AppleCare is a service mark of Apple Computer, Inc., registered in the U.S. and other countries.

FileMaker is a trademark of FileMaker, Inc.

equinux shall have absolutely no liability for any direct or indirect, special or other consequential damages in connection with the use of the quick setup guide 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.

Introduction.....	5
Prerequisites.....	6
Configure your ZyXEL router.....	7
Step 1 - Add a new VPN tunnel gateway policy.....	7
Step 2 - Configure your VPN tunnel's gateway policy.....	8
Step 3 - Add a network policy.....	9
Step 3 - Configure your network policy.....	10
Step 4 - Add a New VPN User.....	11
Configure VPN Tracker.....	12
Step 1 - Create a new Connection.....	12
Step 3 - Network Settings.....	14
Step 4 - Authentication Settings.....	15
Check the VPN connection.....	16
It's time to go out!.....	16
Test your connection.....	16
Host to Everywhere.....	19
Step 2 - Add a new Gateway policy to your ZyXEL Router.....	20
Step 2 - Configure the new Gateway policy.....	21
Troubleshooting.....	22
What's next?.....	23
Introduction.....	23
Known Limitations.....	23
Accessing Files.....	24
Accessing a FileMaker Database.....	26

Acquire more Licenses.....	30
-----------------------------------	-----------

Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a ZyXEL ZyWALL VPN router.

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

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

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.

Prerequisites

First you have to make sure to use a recent firmware version. The latest release for your ZyXEL firewall can be obtained from <http://www.ZyXEL.com/>

For this document, firmware version 1.0 was used.

Please note: VPN Tracker has been only been tested with the ZyXEL ZyWALL 2WG / ZyWALL 5 and the above firmware version. Please make sure to use the latest firmware version.

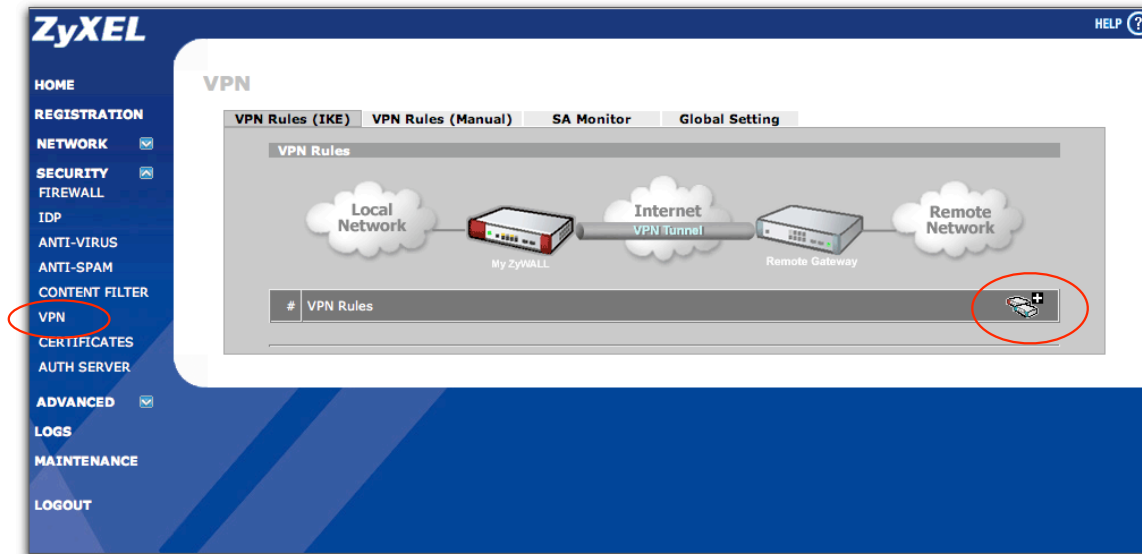
You will need one VPN Tracker Personal Edition license for each Mac connecting to your ZyXEL device.

We recommend one VPN Tracker Professional Edition for the administrator's Mac in order to export configuration files to the clients. VPN Tracker is compatible with Mac OS 10.2.5+, 10.3 and 10.4.1+

Configure your ZyXEL router

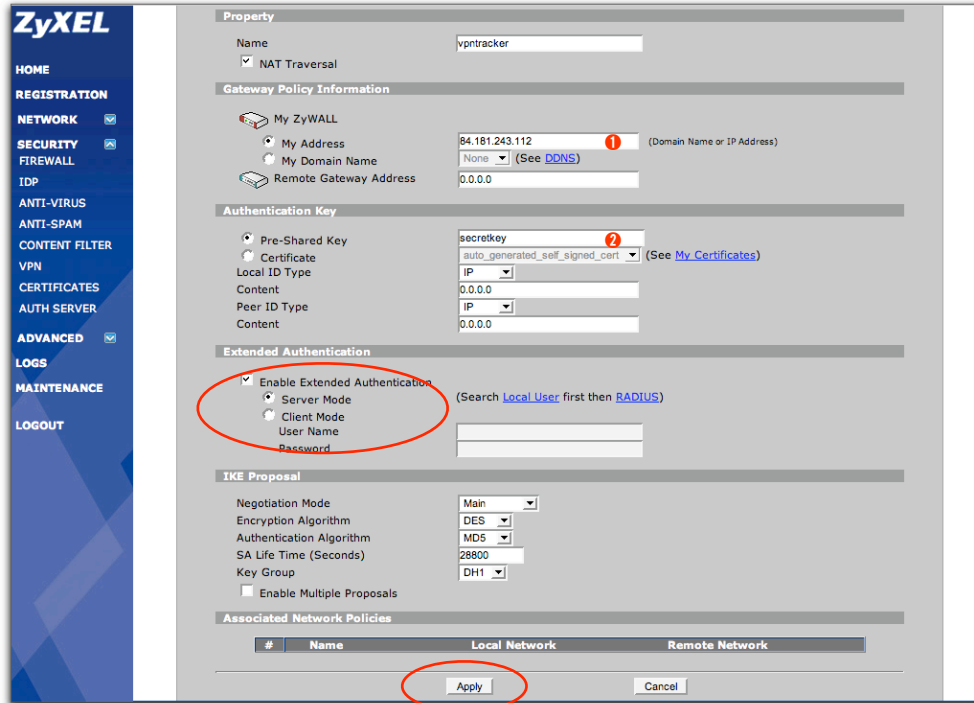
This section describes the configuration of your VPN router.

Step 1 – Add a new VPN tunnel gateway policy



- ▶ Select “VPN” from the menu
- ▶ Click the “+” icon to add a new VPN Tunnel gateway policy

Step 2 – Configure your VPN tunnel's gateway policy



The screenshot shows the ZyXEL VPN configuration interface. The left sidebar contains navigation links: HOME, REGISTRATION, NETWORK, SECURITY, FIREWALL, IDP, ANTI-VIRUS, ANTI-SPAM, CONTENT FILTER, VPN, CERTIFICATES, AUTH SERVER, ADVANCED, LOGS, MAINTENANCE, and LOGOUT. The main configuration area is divided into several sections:

- Property:** Name is set to 'vpntracker'. NAT Traversal is checked.
- Gateway Policy Information:** My ZyWALL is selected. My Address is '84.181.243.112' (marked with a red 1). My Domain Name is 'None'. Remote Gateway Address is '0.0.0.0'.
- Authentication Key:** Pre-Shared Key is selected with the value 'secretkey' (marked with a red 2). Certificate is also an option. Local ID Type and Peer ID Type are both set to 'IP'. Content for both is '0.0.0.0'.
- Extended Authentication:** 'Enable Extended Authentication' is checked and circled in red. Under it, 'Server Mode' is selected. A note says '(Search Local User first then RADIUS)'. There are input fields for User Name and Password.
- IKE Proposal:** Negotiation Mode is 'Main'. Encryption Algorithm is 'DES'. Authentication Algorithm is 'MD5'. SA Life Time (Seconds) is '28800'. Key Group is 'DH1'. 'Enable Multiple Proposals' is unchecked.
- Associated Network Policies:** A table with columns '#', 'Name', 'Local Network', and 'Remote Network' is shown. Below the table, the 'Apply' button is circled in red, along with a 'Cancel' button.

- **Name:** Enter an arbitrary name for your new tunnel
- **My Address:** Enter your ZyXEL device's IP address **1**
- **Pre-Shared Key:** Enter your desired password (pre-shared key), e.g. secretkey **2**
- **Enable Extended Authentication:** Check the box and select "Server Mode"
- Click "Apply"

Step 3 – Add a network policy

The image shows the ZyXEL web management interface for VPN configuration. On the left is a navigation menu with categories: HOME, REGISTRATION, NETWORK (checked), SECURITY (checked), FIREWALL, IDP, ANTI-VIRUS, ANTI-SPAM, CONTENT FILTER, VPN, CERTIFICATES, AUTH SERVER, ADVANCED (checked), LOGS, MAINTENANCE, and LOGOUT. The main content area is titled 'VPN' and has tabs for 'VPN Rules (IKE)', 'VPN Rules (Manual)', 'SA Monitor', and 'Global Setting'. The 'VPN Rules (IKE)' tab is active, showing a diagram of a VPN tunnel. The diagram illustrates a 'Local Network' connected to a 'My ZyXEL' router, which is connected to an 'Internet VPN Tunnel' (represented by a cloud), which is then connected to a 'Remote Gateway' router and finally to a 'Remote Network'. Below the diagram is a table of VPN Rules:

#	VPN Rules				
1	vpntracker	84.181.243.112	Dynamic		

In the table, the 'vpntracker' rule is highlighted. To the right of the rule name, there are icons for a router, an IP address, and a dynamic IP icon. At the end of the row, there are icons for editing, deleting, and adding a new rule. The 'Add' icon (a plus sign inside a cloud) is circled in red.

- Click the “Cloud” icon to add a new network policy for your VPN connection

Step 3 – Configure your network policy

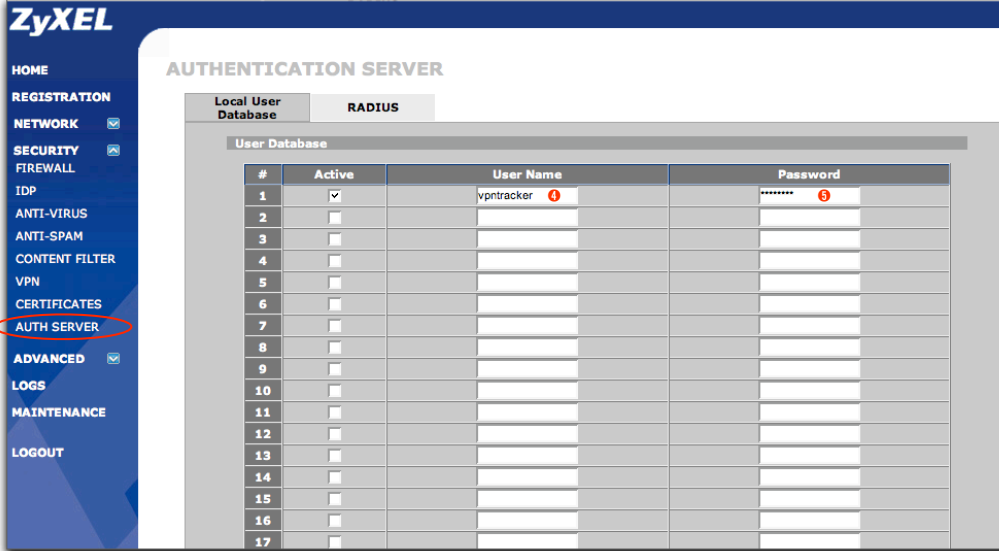
The screenshot shows the ZyXEL VPN configuration interface. The left sidebar contains navigation links: HOME, REGISTRATION, NETWORK, SECURITY, FIREWALL, IDP, ANTI-VIRUS, ANTI-SPAM, CONTENT FILTER, VPN, CERTIFICATES, AUTH SERVER, ADVANCED, LOGS, MAINTENANCE, and LOGOUT. The main content area is divided into several sections:

- Property:** Includes an ☒ **Active** checkbox, a **Name** field with the value "vpntracker_hosttonetwork", a **Protocol** dropdown set to "0", and checkboxes for "Nailed-Up", "Allow NetBIOS Traffic Through IPsec Tunnel", and "Check IPsec Tunnel Connectivity". A **Log** button and a **Ping this Address** field with the value "0 . 0 . 0 . 0" are also present.
- Gateway Policy Information:** Shows a **Gateway Policy** dropdown set to "vpntracker".
- Local Network:** Includes an **Address Type** dropdown set to "Subnet Address", a **Starting IP Address** field with the value "192 . 168 . 1 . 0", a **Ending IP Address / Subnet Mask** field with the value "255 . 255 . 255 . 0", and **Start** and **End** fields both set to "0".
- Remote Network:** Includes an **Address Type** dropdown set to "Single Address", a **Starting IP Address** field with the value "0 . 0 . 0 . 0", a **Ending IP Address / Subnet Mask** field with the value "0 . 0 . 0 . 0", and **Start** and **End** fields both set to "0".
- IPsec Proposal:** Includes a **Encapsulation Mode** dropdown set to "Tunnel", an **Active Protocol** dropdown set to "ESP", an **Encryption Algorithm** dropdown set to "DES", an **Authentication Algorithm** dropdown set to "SHA1", an **SA Life Time (Seconds)** field with the value "28800", and a **Perfect Forward Secrecy (PFS)** dropdown set to "NONE". There are also checkboxes for "Enable Replay Detection" and "Enable Multiple Proposals".

At the bottom of the configuration area, there are **Apply** and **Cancel** buttons. The status bar at the bottom left indicates "Status: Ready".

- ▶ Check the "Active" box to enable this new policy
- ▶ **Name:** Enter an arbitrary name (e.g. "vpntracker_hosttonetwork")
- ▶ **Local Network:**
 - **Address Type:** Select "Subnet Address"
 - **Starting IP Address:** Enter the IP address of your office network ③
 - **Ending IP Address / Subnet Mask:** Enter your office network's subnet mask
- ▶ Click "Apply"

Step 4 – Add a New VPN User



The screenshot shows the ZyXEL web interface for the AUTHENTICATION SERVER. The left sidebar contains a menu with options: HOME, REGISTRATION, NETWORK, SECURITY, FIREWALL, IDP, ANTI-VIRUS, ANTI-SPAM, CONTENT FILTER, VPN, CERTIFICATES, AUTH SERVER (highlighted with a red circle), ADVANCED, LOGS, MAINTENANCE, and LOGOUT. The main content area is titled 'AUTHENTICATION SERVER' and has two tabs: 'Local User Database' and 'RADIUS'. The 'Local User Database' tab is active, showing a 'User Database' table with 17 rows. The first row is pre-filled with 'vpntracker' as the username and a masked password. Red circles with numbers 4 and 5 are placed over the username and password fields respectively, indicating where to enter a new user's details.

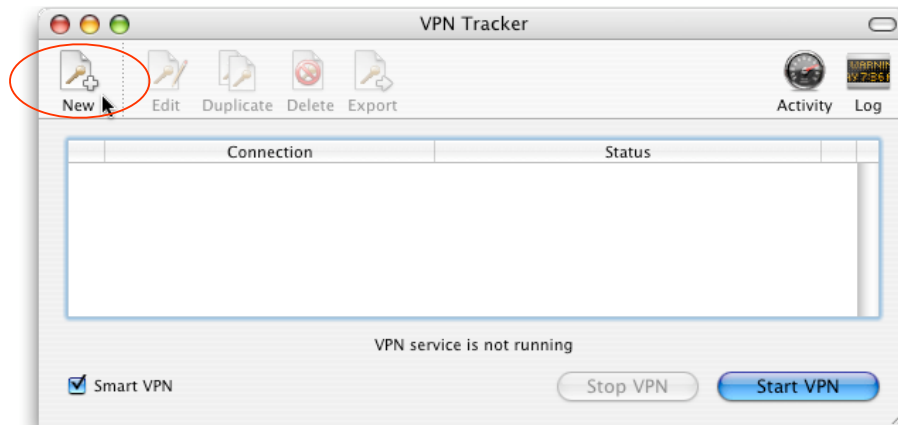
#	Active	User Name	Password
1	<input checked="" type="checkbox"/>	vpntracker 4	***** 5
2	<input type="checkbox"/>		
3	<input type="checkbox"/>		
4	<input type="checkbox"/>		
5	<input type="checkbox"/>		
6	<input type="checkbox"/>		
7	<input type="checkbox"/>		
8	<input type="checkbox"/>		
9	<input type="checkbox"/>		
10	<input type="checkbox"/>		
11	<input type="checkbox"/>		
12	<input type="checkbox"/>		
13	<input type="checkbox"/>		
14	<input type="checkbox"/>		
15	<input type="checkbox"/>		
16	<input type="checkbox"/>		
17	<input type="checkbox"/>		

- ▶ Select "AUTH SERVER" from the menu
- ▶ Activate the checkbox for the first user
- ▶ Select a unique user name 4 and password 5
- ▶ Click "Apply"

Configure VPN Tracker

This section describes the configuration of VPN Tracker for your ZyXEL router.

Step 1 – Create a new Connection



► Click on “New” in the VPN Tracker main window

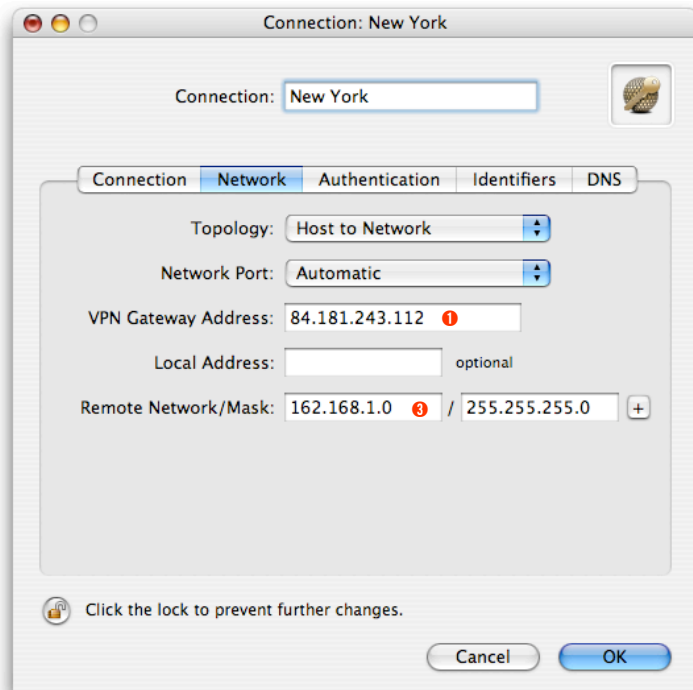
Step 2 – Connection Settings

The pre-defined VPN Tracker connection for the ZyXEL VPN router is based on the default settings for your ZyXEL VPN router. If you changed any of the settings while configuring the device, you might have to adjust the connection type in VPN Tracker.



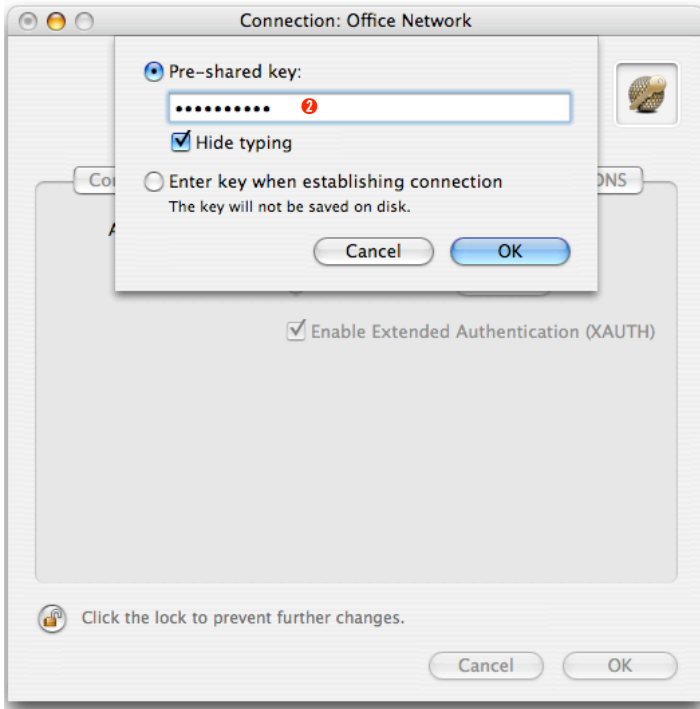
- ▶ Select the vendor "ZyXEL"
- ▶ Select your VPN model (ZyWALL 2WG / ZyWALL 5)
- ▶ Make sure to enable "Initiate connection from this end"

Step 3 – Network Settings



- ▶ **VPN Gateway Address:** the public IP address of your VPN Gateway (e.g. "84.181.243.112") ❶
- ▶ **Remote Network/Mask:** network address and subnet address of your office network ❸

Step 4 – Authentication Settings



- ▶ **Pre-shared key:** Enter the pre-shared key you used earlier when configuring your ZyXEL device **2**
- ▶ Make sure to check "Enable Extended Authentication (XAUTH)"

Check the VPN connection

This section explains how to start and test your VPN connection.

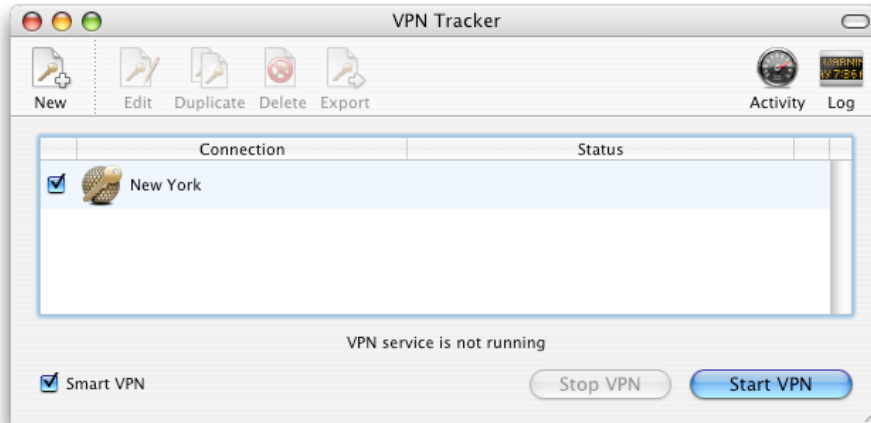
It's time to go out!

You will not be able to test and use your VPN connection from within your Private Network. In order to test your connection, you'll need to connect from a different location. That's why it's now time to go out. Take your MacBook Pro and have a coffee at your favorite Internet cafe or go visit a friend.

Test your connection

To test if everything is setup correctly please follow the steps below:

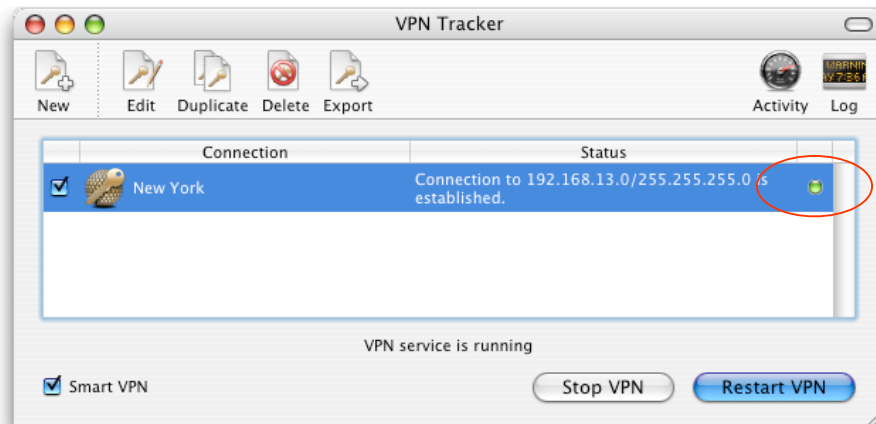
- ▶ Get access to the Internet
- ▶ Make sure the Internet connection is working; open your Internet browser and try to connect to <http://www.equinux.com>
- ▶ Start VPN Tracker if it's not already running



- ▶ Select the connection you configured for your ZyXEL device
- ▶ Click on the **Start VPN** button



- ▶ Provide the username **4** and password **5** defined earlier
- ▶ Click "OK"



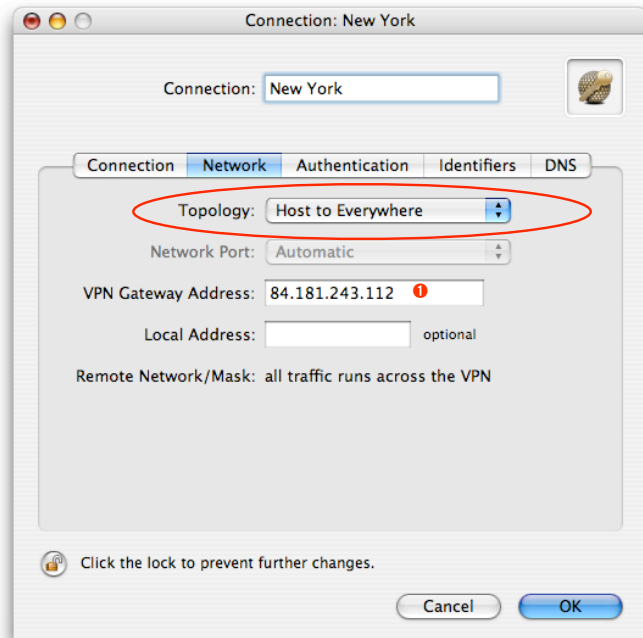
- ▶ If the light turns red after a few seconds, then please read the **Troubleshooting** section on the next page
- ▶ If the light turns green, that means you've successfully established a connection

Congratulations! You did it!

Host to Everywhere

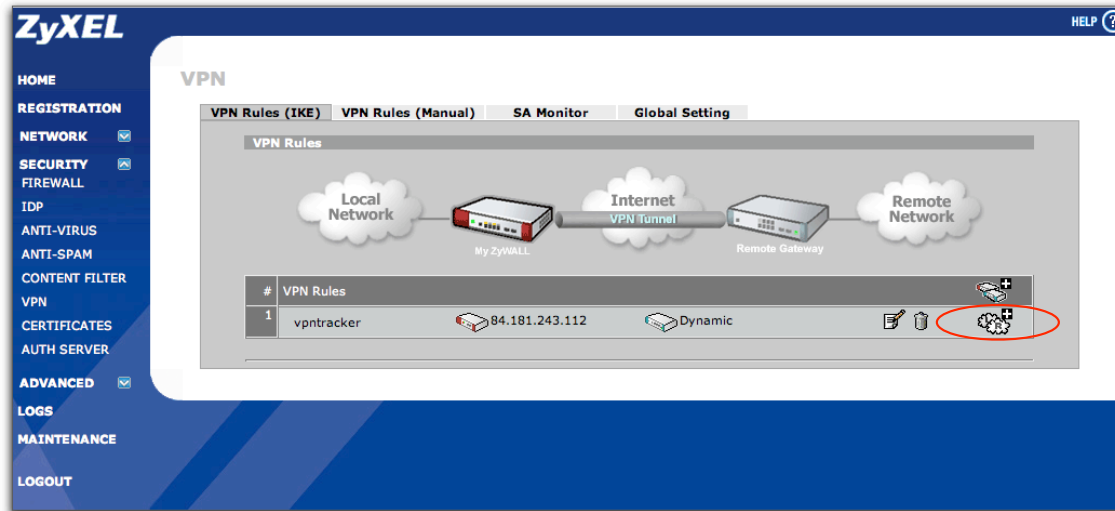
Sometimes, you will want to secure all your IP traffic. Both VPN Tracker and your ZyXEL router support this mode.

Step 1 – Adjust your VPN Connection




- **Topology:** Select “Host to Everywhere” from the drop down menu

Step 2 – Add a new Gateway policy to your ZyXEL Router



The screenshot shows the ZyXEL web interface for VPN configuration. The left sidebar contains navigation links: HOME, REGISTRATION, NETWORK, SECURITY, FIREWALL, IDP, ANTI-VIRUS, ANTI-SPAM, CONTENT FILTER, VPN, CERTIFICATES, AUTH SERVER, ADVANCED, LOGS, MAINTENANCE, and LOGOUT. The main content area is titled 'VPN' and has tabs for 'VPN Rules (IKE)', 'VPN Rules (Manual)', 'SA Monitor', and 'Global Setting'. The 'VPN Rules (IKE)' tab is active, displaying a diagram of a VPN tunnel connecting a 'Local Network' (My ZyWALL) to a 'Remote Network' (Remote Gateway) via an 'Internet VPN Tunnel'. Below the diagram is a table of VPN Rules:

#	VPN Rules				
1	vpntracker	84.181.243.112	Dynamic		

The 'Add new rule' icon (a cloud with a plus sign) is circled in red.

- Click the “cloud” icon to add a new VPN gateway policy

Step 3 – Configure the new Gateway policy

The screenshot shows the ZyXEL web interface for configuring a new Gateway policy. The 'Active' checkbox is checked. The policy name is 'vpntracker_hosttoeverywhere'. The Local Network is configured with Subnet Address, Starting IP Address 0.0.0.0, Ending IP Address / Subnet Mask 0.0.0.0, and Local Port 0. The Remote Network is configured with Single Address, Starting IP Address 0.0.0.0, Ending IP Address / Subnet Mask 0.0.0.0, and Remote Port 0. The IPSec Proposal is configured with Tunnel, ESP, DES, SHA1, 28800, and NONE. The 'Apply' button is highlighted.

- ▶ Check the “Active” box to enable this new policy
- ▶ **Name:** Enter an arbitrary name (e.g. “vpntracker_everywhere”)
- ▶ **Local Network:**
 - **Address Type:** Select “Subnet Address”
 - **Starting IP Address:** Enter “0.0.0.0”
 - **Ending IP Address / Subnet Mask:** Enter “0.0.0.0”
- ▶ Click “Apply”

Congratulations! You have now secured all of your network traffic.

Troubleshooting

I don't get a green light in the VPN Tracker main window

- ▶ Make sure that your computer is not connected directly to the Private Network you want to connect to.
- ▶ Make sure, that the Identifiers and the **Pre-shared key** you've entered in the router configuration match the settings you entered in VPN Tracker.
- ▶ Verify that the **public IP address** you entered in VPN Tracker matches the public IP address of your router.
- ▶ Download our sample configuration and connect to our test device at <http://www.vpntracker.com/connectiontest/>
 - If the test connection could **not** be established: Make sure, that the internet connection is working and verify, that your local router is not blocking any connection attempts.
 - If the test connection could be established: Check the log file of your remote VPN router for any error messages.
- ▶ If you're still having issues with your connection, then please create some screenshots of your settings on both ends, gather the log files and send them over to our support team at vpntracker@equinux.com.

What's next?

This section explains the usage of your newly configured VPN connection.

Introduction

As the VPN connection has now been established, you should be able to access all resources in your Private Network.

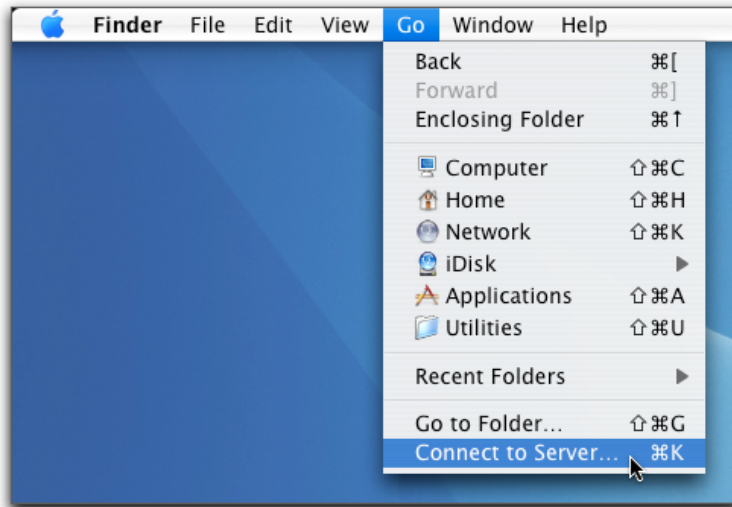
Known Limitations

There are some limitations of a VPN connection compared to a direct connection to a Private Network.

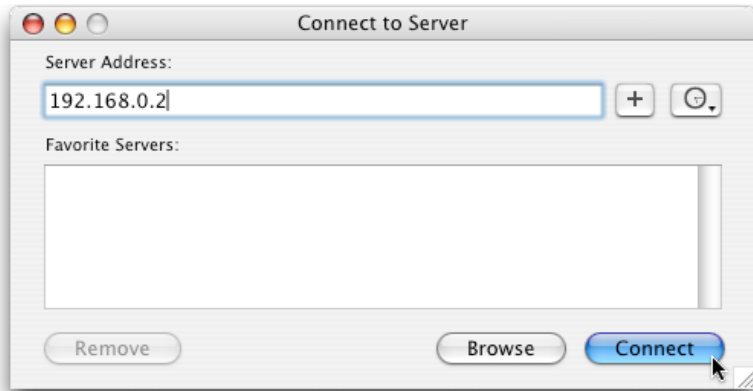
- ▶ **Bonjour:** As Bonjour Chat is not supported over a VPN tunnel, you'll need to use iChat server in order to chat remotely.
- ▶ **Browsing the network:** You can't "browse" the remote network as you're normally used to. You need to connect to each machine manually, as described on the next page.

Accessing Files

To access files in your Private Network, just follow the steps below:



- ▶ Go to the **Finder** application
- ▶ In the menu bar, click on **Go->Connect To Server...**



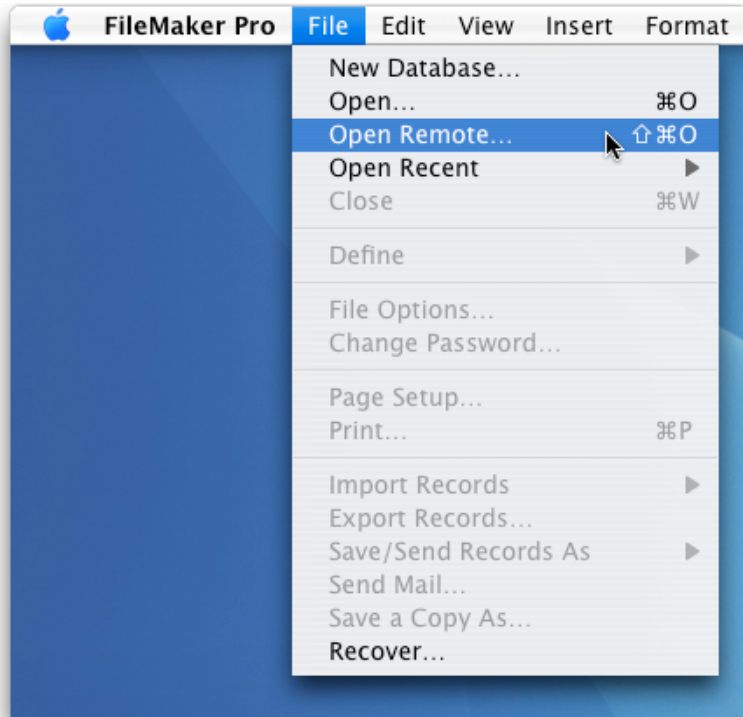
- Enter the IP address of the machine you want to connect to. In our example network this would be the IP address **192.168.0.2**
- Click on the **Connect** button
- Enter your **Username** and **Password** to access the files

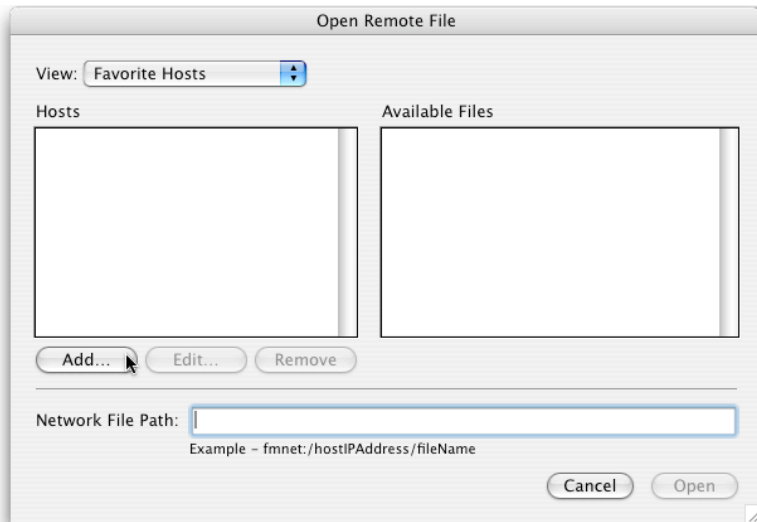
When connecting to a Windows fileserver you'll need to prefix the IP address with "*smb://*", e.g. "*smb://192.168.0.2*".

Accessing a FileMaker Database

To access a database available in your Private Network, just follow the steps below:

- ▶ Start the **FileMaker** application
- ▶ In the menu bar, click on **File->Open Remote**





► Click on the **Add...** button

Edit Favorite Host

Favorite Settings

Host's Internet Address:
(Example - host.domain.com or 192.168.10.0)

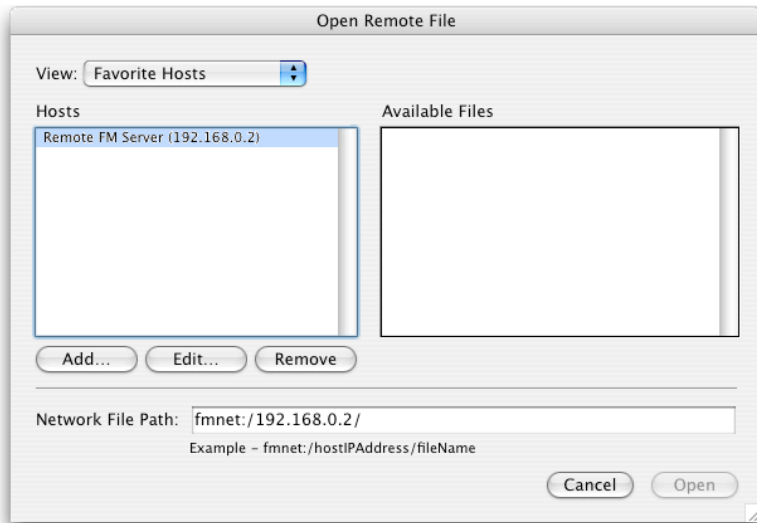
Favorite Host's Name:
(optional)

File Settings

☒ Show all available files for this host
☐ Show only these files

Enter one file name per line, separated by a carriage return

- ▶ Enter the **IP address** of the FileMaker Server machine
- ▶ Enter the **Favorite Host's Name** for this machine
- ▶ Click on the **Save** button



- ▶ Select a database from the list of **Available Files** and click **Open**
- ▶ You're now able to access your FileMaker databases as usual

Acquire more Licenses

If two or more people need to access your Private Network, then you need to acquire more VPN Tracker licenses.

To get more licenses, please contact your reseller and inquire about „VPN Tracker Personal Edition“.

Or point your browser to <http://store.equinux.com> and buy additional VPN Tracker Personal Edition Licenses online.