VPN Configuration Guide

ZyWALL (4.x Firmware)

Configuration guide revision 1

Created using Apple Pages.

www.equinux.com

Contents

Introduction

This configuration guide helps you configure VPN Tracker and your ZyWALL VPN gateway to establish a VPN connection between them.

Using the Configuration Guide

Part 1 – VPN Gateway Configuration

The first part of this guide will show you how to configure a VPN tunnel on your ZyWALL VPN gateway device using the web configuration interface.

This guide is a supplement to the documentation included with your ZyWALL VPN gateway device, it can't replace it. Please read this documentation before starting.

Part 2 – VPN Tracker Configuration

In the second part, this guide will show you how to configure VPN Tracker to easily connect to your newly created VPN tunnel.

Part 3 – Troubleshooting and Supporting Multiple Users

Troubleshooting advice and information on supporting multiple users can be found in the final part of this guide.

If you are setting up VPN on your device for the first time, we strongly recommend you keep to the tutorial-style setup in the first and second part of this document and make modifications only after you have tested the basic setup.

Conventions Used in This Document

Links to External Websites

Sometimes you will be able to find more information on external websites. Clicking links to websites will open the website in your web browser:

http://equinux.com

Links to Other Parts of this Guide

A → *Link* will take you to another place in the configuration guide. Simply click it if you are reading this guide on your computer.

Tips and Tricks

This configuration guide contains lots of great tips. You can easily spot them by looking for the light bulb icon.

Warnings

This exclamation mark warns you when there is a setting or action where you need to take particular care.

Getting Help

VPN Tracker makes VPN simple. However, computer networking and VPNs can be complex and tricky at times, so we have also built in tools and helpful features that will assist you if you ever run into problems. Check out → *Troubleshooting* for more information.

Prerequisites

Your VPN Gateway

- This guide applies to the following ZyWALL VPN gateways
  - ZyWALL 2/2WG
  - ZyWALL 5/35/70
  - ZyWALL 5/35/70 UTM
- Make sure you have the **latest firmware** version installed that is available for your device. This configuration guide was created using a ZyWALL 5 running firmware V4.04(XD.8)

Your Mac

VPN Tracker runs on Mac OS X 10.4, 10.5 and 10.6

The configuration described in this guide requires VPN Tracker 6. Make sure you have all available updates installed. The latest VPN Tracker updates can always be obtained from http://www.vpntracker.com

Scenario

In our example, we need to connect an employee's Mac to an office network. The diagram on the bottom of this page illustrates this scenario.

This guide assumes that the Mac running VPN Tracker already has internet connectivity. The office's ZyWALL VPN gateway device (the "VPN gateway") is also already connected to the Internet and can be accessed through a static IP address or DNS host name. In our example setup, we will be using a static IP address: 203.0.113.1.

The VPN gateway has a second network interface which is connected to the internal office network (LAN). In our example, the office network is using the network 192.168.13.0/24 (which is the same as 192.168.13.0/255.255.255.0). This is the network that will be accessed from the employee's Mac through the VPN. It is called the "Remote Network" in VPN Tracker.

Terminology

A VPN connection is often called a "tunnel" (or "VPN tunnel"). Every VPN tunnel is established between two "endpoints". In our example one endpoint is VPN Tracker and the other endpoint is the VPN gateway. Each endpoint is called the other endpoint's "peer".

Please note that for each endpoint, the settings on the other endpoint are considered to be "remote", while its own settings are considered to be "local". That means a "local" setting from VPN Tracker's perspective, is a "remote" setting from the VPN gateway's perspective, and vice versa.

The sample configuration described in this guide is called a "Host to Network" configuration: a single computer, called a "Host" establishes a VPN tunnel to an entire "Network" behind the VPN gateway.

My VPN Gateway Configuration Checklist

Throughout this guide, there are certain pieces of information that are needed later on for configuring VPN Tracker. This information is marked with red numbers to make it easier to reference it later. You can print this checklist to help keep track of the various settings of your ZyWALL VPN gateway device.

IP Addresses

❶ WAN IP Address: _____._____._____._____ (or hostname _____)

❷ LAN IP Address / Subnet Mask: _____._____._____._____ / _____._____._____._____

User Authentication (XAUTH)

❸ Username: _____

❹ Password: _____

Pre-Shared Key

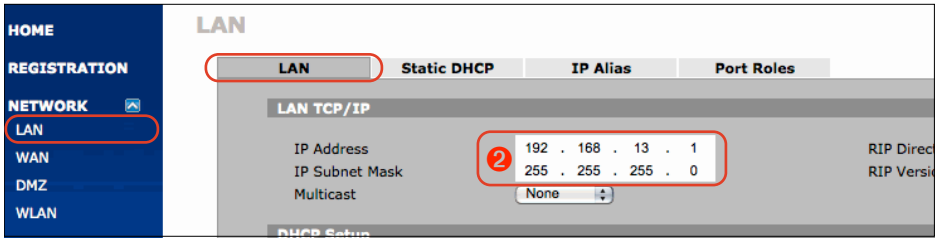
❺ Pre-Shared Key: _____

Task 1 – VPN Gateway Configuration

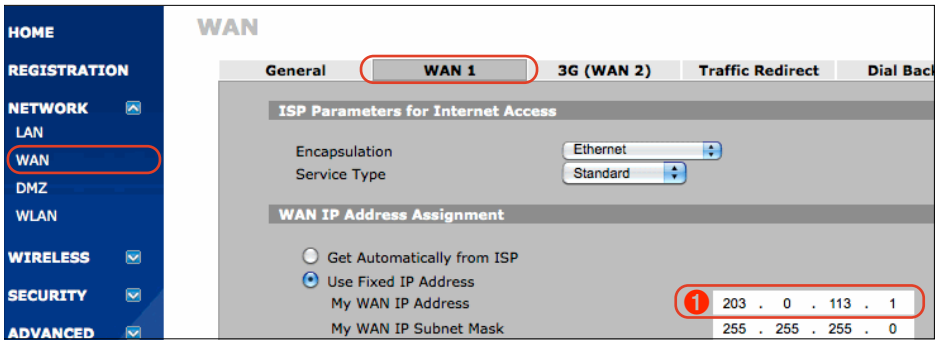
We will first set up VPN on the VPN gateway. If you already have VPN in place, it's helpful to follow along this tutorial to see how settings on the device fit together with VPN Tracker.

Step 1 – Retrieve Network Settings

- Connect to your VPN gateway through its web configuration interface
- Go to **NETWORK** > **LAN** > **LAN**



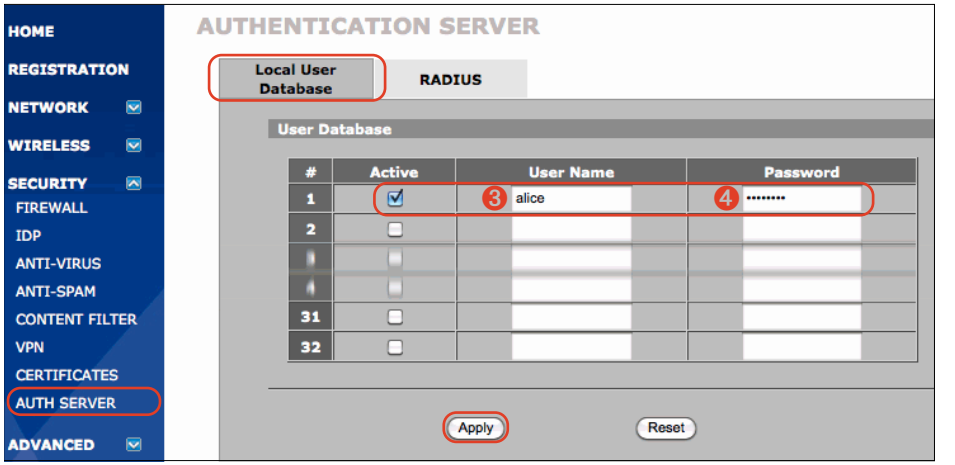
- Write down the **IP address** of the LAN network interface, including its **subnet mask** as ❷ on your → *Configuration Checklist*
- Continue to **NETWORK** > **WAN** and switch to the tab representing the device's primary WAN interface (usually **WAN 1**)



- Write down the IP address of the primary **WAN** network interface as ❶ on your → *Configuration Checklist*. If your device has a DNS hostname (fixed or DynDNS), write it down instead

Step 2 – Create a VPN User

- Go to **SECURITY** > **AUTH SERVER** > **Local User Database**



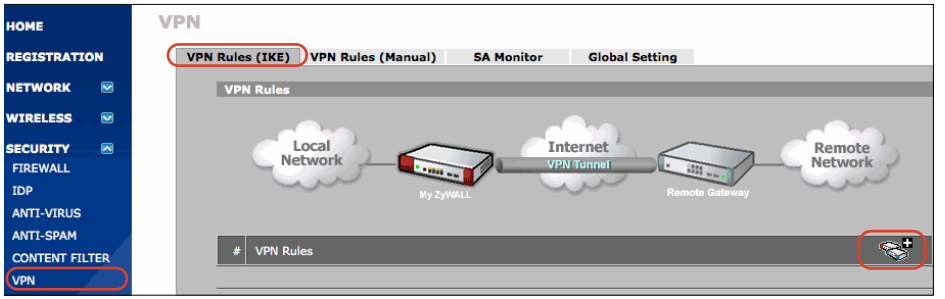
- **Active**: Click the checkbox to make the user account active
- **User Name**: Enter a username for the new user (here: **alice**). Write down the user name as ❸ on your → *Configuration Checklist*
- **Password**: Enter a password for this new user. Make sure to remember the password, or write it down as ❹ on your → *Configuration Checklist*

To add more users, simply repeat this step. You might want to connect the device to an existing (RADIUS) authentication server later. We recommend using a local user for initial setup and testing.

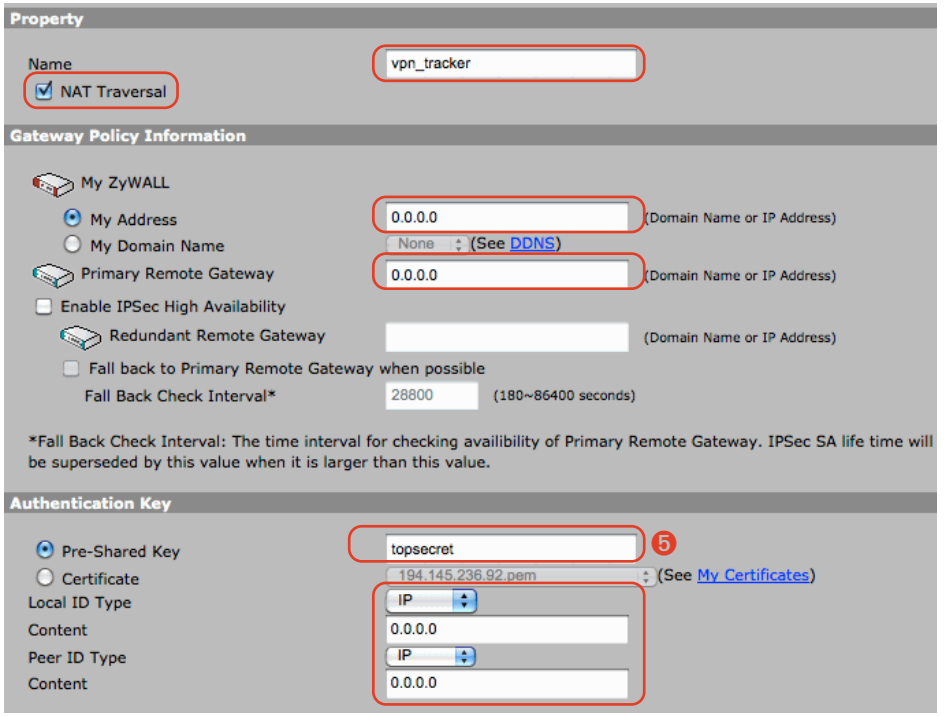
- Click **Apply** button to save your configured user(s)

Step 3 – Set up Phase 1

- Go to **SECURITY** > **VPN** > **VPN Rules (IKE)**



- Click the **Add Gateway Policy** button to add a new gateway policy. The gateway policy corresponds to the phase 1 settings in VPN Tracker



Property

- **Name**: Enter a name for the gateway policy (here: **vpn_tracker**)
- Click the **NAT Traversal** checkbox to select it

Gateway Policy Information

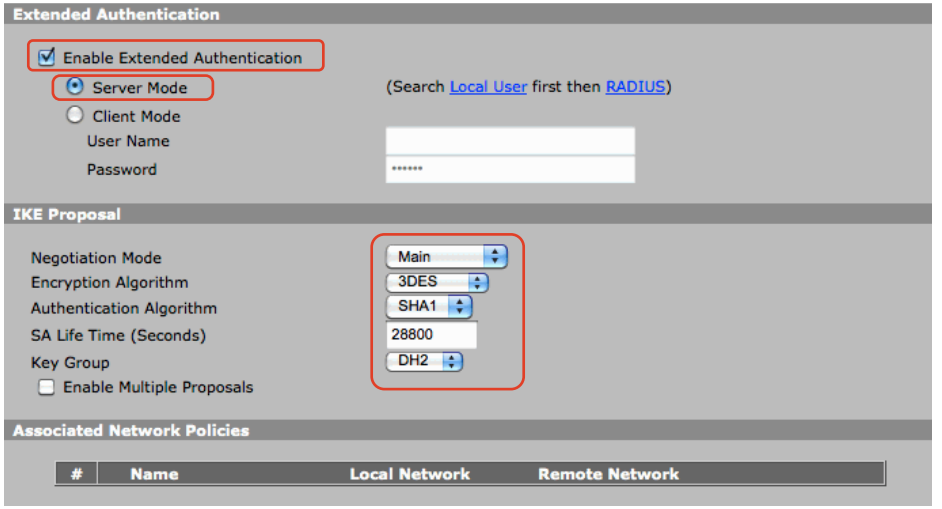
- Select **My ZyWALL** > **My Address**. A value of **0.0.0.0** means that the VPN gateway will automatically use its current **WAN IP address**
- Set the **Primary Remote Gateway** to **0.0.0.0** to let VPN Tracker connect from any IP address

Authentication Key

- Enter a **Pre-Shared Key**. Make sure to choose a good pre-shared key and remember it, or write it down as 5
- **Local ID Type**: Make sure **IP** is chosen from the pop-up menu
- **Content**: Leave the default of **0.0.0.0**. This means that the IP address entered for **My Address** will automatically be used as the device's identifier
- **Peer ID Type**: Make sure **IP** is chosen from the pop-up menu
- **Content**: Enter **0.0.0.0** to allow VPN clients to identify using any IP address

It is possible to select a **specific identifier** that VPN clients need to use. However, please note that if you choose to do this, you will probably have to use **Aggressive Mode** instead of **Main Mode** as the Exchange Mode (Negotiation Mode), both on the ZyWALL and in VPN Tracker.

This is because Main Mode identifies VPN clients based on their IP address. For a VPN client connecting from dynamic IP addresses and/or from behind NAT routers, its IP address can obviously not be used to uniquely and consistently identify it.



Extended Authentication

- Select **Enable Extended Authentication** and select **Server Mode**

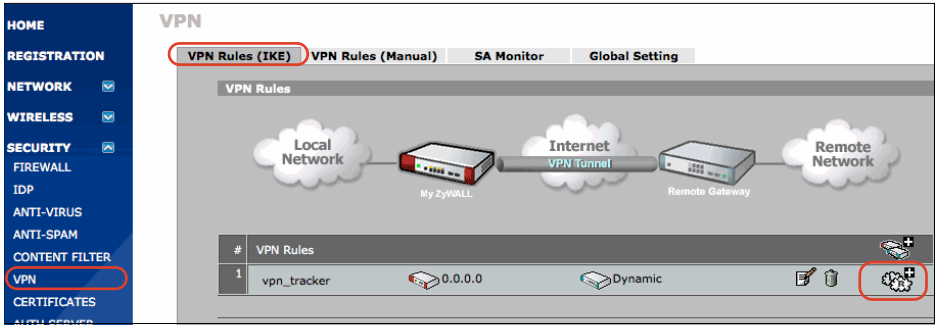
IKE Proposal

- **Negotiation Mode**: Leave the default of **Main** Mode
- **Encryption/Authentication Algorithms**: For security reasons, we recommend changing the default settings to use at least **3DES** and **SHA1** as shown
- **SA Life Time**: Leave the default of 28800 seconds
- **Key Group**: Choose **DH2** from the pop-up menu

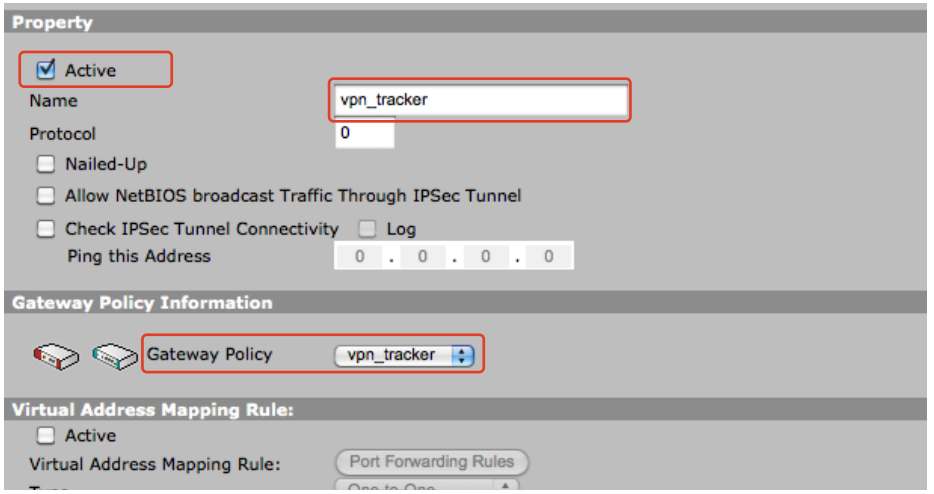
It is possible to use different phase 1 settings. Please note that any changes you make here must be matched in VPN Tracker (Advanced > Phase 1). We recommend using the settings shown here for initial setup and testing.

- Click the **Apply** button to complete the phase 1 setup

Step 4 – Set up Phase 2



- Click the **Add Network Policy** button to add a network policy. The network policy corresponds to the phase 2 settings in VPN Tracker.

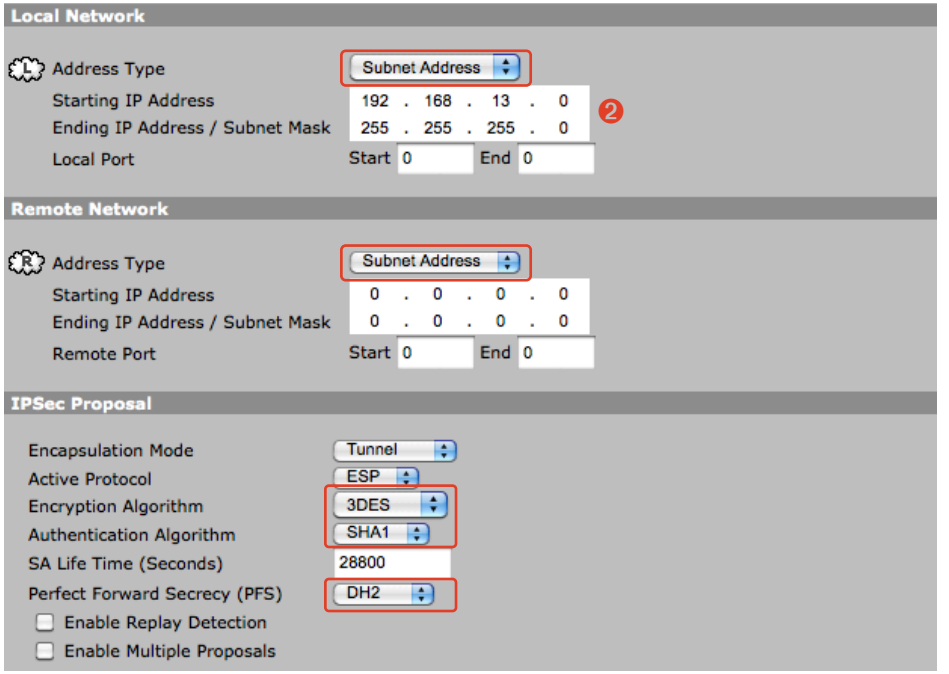


Property

- Select **Active** to enable the network policy that you are about to configure
- **Name**: Enter a name for the phase 2 setup (here: **vpn_tracker**)

Gateway Policy Information

- **Gateway Policy**: Select the gateway policy that you configured during → *Step 3* (here: **vpn_tracker**)



Local Network

- **Address Type**: Choose **Subnet Address** from the pull-down menu
- **Starting IP Address / Subnet Mask**: Enter the LAN network address and its subnet mask.
  You can easily obtain the LAN network address from the LAN IP address you have written down as ❷: Simply apply the subnet mask to the LAN IP. In most cases, this will mean setting those parts of the IP address to zero where the subnet mask is zero. In our example:
  192.168.13.1/255.255.255.0 → 192.168.13.0/255.255.255.0

Remote Network

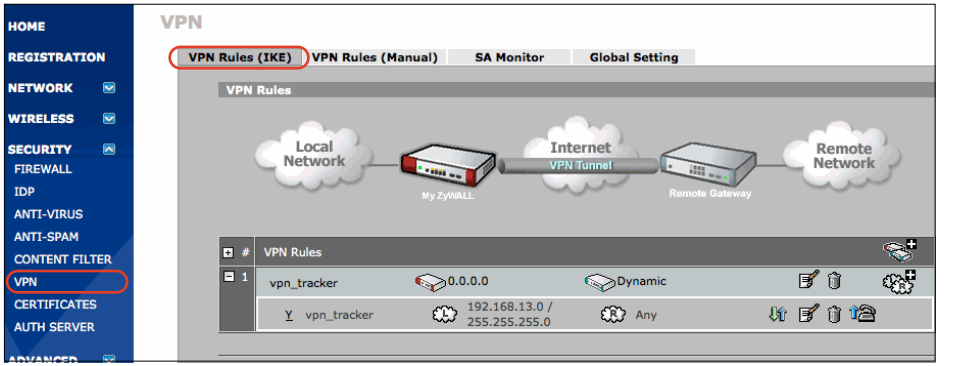
- **Address Type**: Choose **Subnet Network** from the pop-up menu
- **Subnet IP Address**: Leave the default of **0.0.0.0** to allow VPN Tracker clients with any local address

IPSec Proposal

- **Encapsulation Mode**: Leave the default of **Tunnel**
- **Active Protocol**: Leave the default of **ESP**
- **Encryption/Authentication Algorithms**: For security reasons, we recommend changing the default settings to use at least **3DES** and **SHA1** as shown
- **SA Life Time**: Leave the default of 28800 seconds
- **Perfect Forward Secrecy (PFS)**: Choose **DH2** from the pop-up menu

It is possible to use different phase 2 settings. Please note that any changes you make here must be matched in VPN Tracker (Advanced > Phase 2). We recommend using the settings shown here for initial setup and testing.

- Click the **Apply** button to complete the phase 2 setup.You should now have a setup similar to the one shown in the following screenshot:

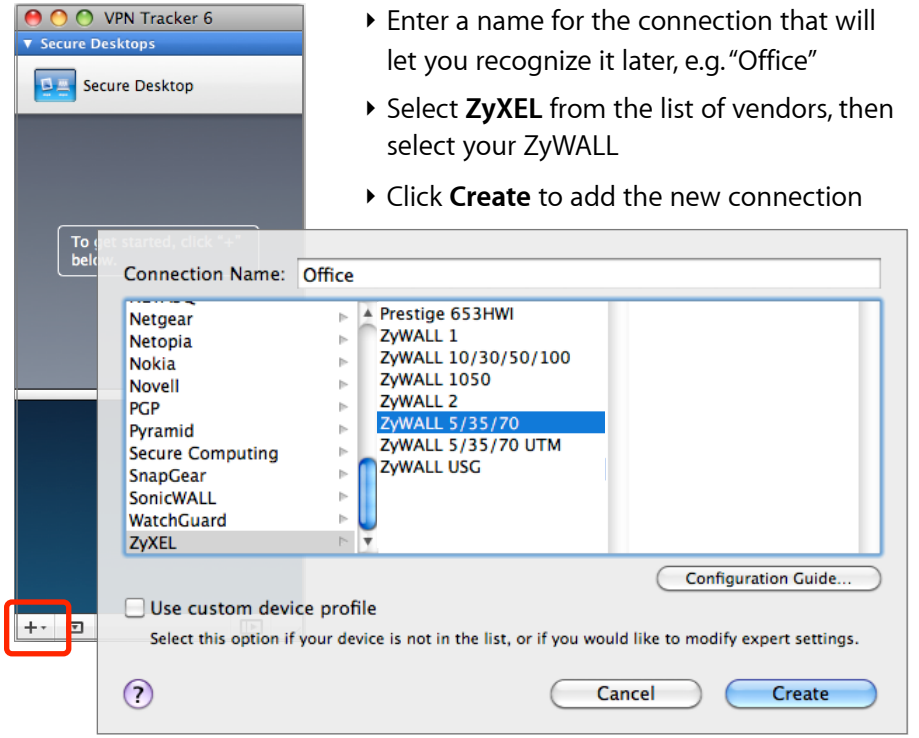


Task 2 – VPN Tracker Configuration

After finishing task 1, you should now have a completed → *configuration checklist* containing your ZyWALL's settings. We will now create a matching configuration in VPN Tracker.

Step 1 – Add a Connection

Open VPN Tracker, and click the plus button in the bottom left corner of the window to add a new connection:



- Enter a name for the connection that will let you recognize it later, e.g. "Office"
- Select **ZyXEL** from the list of vendors, then select your ZyWALL
- Click **Create** to add the new connection

Step 2 – Configure the VPN Connection

Once you have added the new connection, there are a few settings that need to be customized to match what is configured on your VPN gateway.

- **VPN Gateway**: Enter the WAN IP address (or hostname) of your VPN gateway that you wrote down as 1
- **Local Address**: Leave empty for now. Depending on your setup, you may have to set a specific local address later. Refer to → *Supporting Multiple Users* on when and how to set a specific local address
- **Remote Networks**: Enter the network address of the network that is being accessed through the VPN tunnel 2. Separate the subnet mask with a forward slash („/")

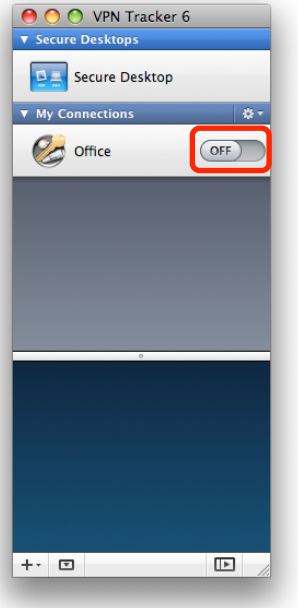
VPN Tracker will automatically turn the IP address into a network address. Double-check that the result is the same as the "Local Network" configured in the network policy in → *Step 4*

Step 3 – Test the VPN Connection

It 's time to go out!

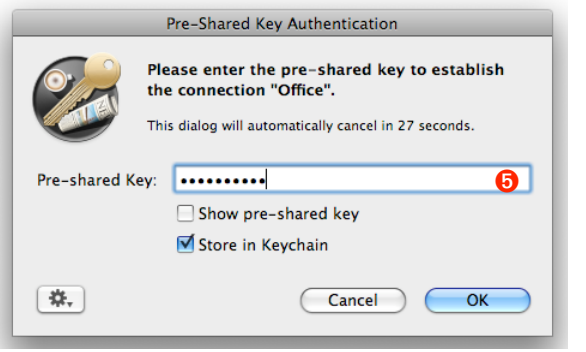
You will not be able to test and use your VPN connection from within the internal network that you want to connect to. To test your connection, you will need to connect from a different location. For example, if you are setting up a VPN connection to your office, test it from home. If you are setting up a VPN connection to your home network, test it from an Internet cafe, or go visit a friend.

Start your connection



- Connect to the Internet
- Make sure that your Internet connection is working – open your Internet browser and try to connect to http://www.equinux.com
- Open VPN Tracker if it's not already running
- Slide the ON/OFF slider for the connection you have just configured to **ON**

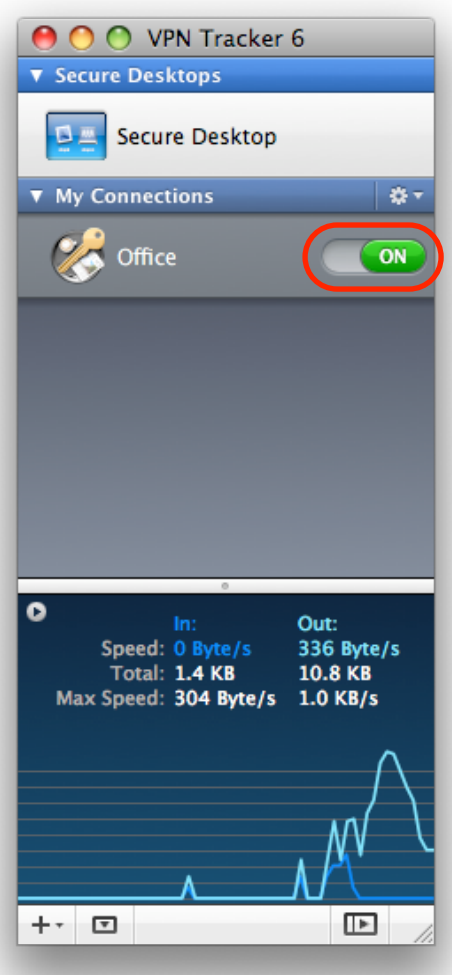
When prompted for your pre-shared key:



- **Pre-shared key**: Enter the pre-shared key that you configured on the VPN gateway in the phase 1 settings ❺
- Optional: Check the box **Store in Keychain** to save the password in your keychain so you are not asked for it again when connecting the next time
- Click **OK**

When prompted for your Extended Authentication (XAUTH) credentials:

- **User Name**: Enter the name of the user you have added on the VPN gateway (here: **alice**) ❸
- **Password**: Enter the password for the user ❹
- Optional: Check the box **Store in Keychain** to save the password in your keychain so you are not asked for it again when connecting the next time
- Click **OK**



- If the slider goes back to **OFF** after starting the connection, or after entering your pre-shared key or your XAUTH credentials, please read the → *Troubleshooting* section of this document
- If the slider goes to **ON** and turns green after a while, you have successfully established a connection
- **Congratulations**!

Troubleshooting

In most cases, your connection should work fine if you follow the instructions above. If you cannot connect, please read on.

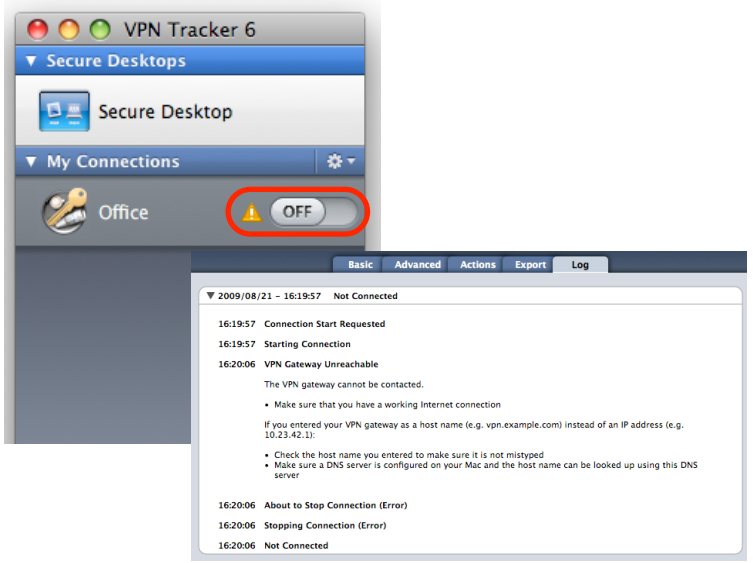
VPN Connection Fails to Establish

ON/OFF slider goes back to OFF right away

If the slider goes back to **OFF** right away, please make sure you have entered all the required information. VPN Tracker will highlight fields that are missing or obviously incorrect information.

ON/OFF slider goes back to OFF after a while

If the connection **ON**/**OFF** slider goes back to **OFF** a while after attempting to start the connection, please go to the **Log** tab to get more information about the issue (or click the warning triangle to be automatically taken to the **Log** tab). VPN Tracker will display detailed suggestions for a solution:



No Access to the Remote Network

If the connection slider goes to **ON** and turns green, but you cannot access resources (servers, email, etc.) through the VPN connection please check the following points.

Connect to an IP address (instead of a host name)

If you are not connecting to the resource by IP address (e.g. 192.168.13.42), but are using a host name (e.g. server.example.com), please try using the resource's IP address instead. If the connection works when using the IP address, but not when using a host name, please make sure that your Mac's DNS server or the "Remote DNS" server that you have configured on your VPN gateway is able to resolve this host name to an IP address.

Test VPN Availability again

In many networks your Mac will be behind a router that performs Network Address Translation (NAT). For a VPN connection to be established through such a router, VPN Tracker can use different methods, but not all of them may be supported by your local router or your VPN gateway.

VPN Tracker automatically runs a test to detect the proper method for your particular Internet connection when you first connect using this Internet connection. However, test results could become outdated by changes to the local router, so it is a good idea to test again if there are problems.

- Select **Tools** > **Test VPN Availability** from the menu
- Click **Test Again** and wait until the test has completed
- Try connecting again

Check that the IP address you are connecting to is part of the network(s) permitted in the split tunneling setup

Check that the IP address you are connecting to is actually part of the network(s) you permitted in the network policy in → *Step 4 – Set up Phase 2*. Also double-check the network mask.

Further Questions?

You can find the latest news and compatibility information on our support and FAQ website:

http://www.equinux.com/support

If you need to contact equinux Technical Support

If you can't resolve your issue with the information available on our website or in this guide and would like to contact Technical Support through our website, please be sure to include at least the following information:

- The manufacturer and model and firmware revision of the VPN gateway
- A Technical Support Report from VPN Tracker (Help > Generate Technical Support Report)
- Screenshots of what you have configured on your VPN gateway, in particular all VPN-related settings
- A description of the problem and the troubleshooting steps you have taken

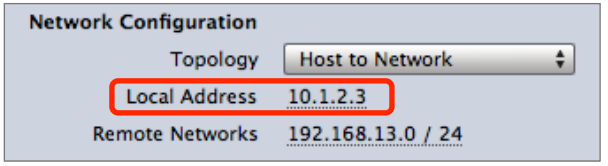
Supporting Multiple Users

Once your VPN expands to multiple users you must ensure that IP addresses do not conflict by assigning each user their own IP address. In addition to these purely technical considerations, VPN Tracker makes it easy to distribute pre-configured connections to your users, and prevent the modification of VPN connections and access to confidential data.

Preventing IP Address Conflicts

How IP Addresses are Assigned to VPN Clients

The **Local Address** in VPN Tracker is the IP address that the Mac will be using in the remote network when connected through VPN.



- If the Local Address field is left **empty**, the Mac's actual local IP address (as shown in System Preferences > Network) is used. With multiple users, it's easily possible that two users end up with the same local IP address on their respective Macs (e.g. the private IP address 192.168.1.2). You will therefore have to **use a fixed address when multiple users connect to the VPN**
- If the Local Address field contains a **fixed address** this address is used. The address must be unique among all users of the VPN connection

Step 1 – Choose the Local Addresses

Choose the local addresses for your VPN clients so that

- the local addresses are **not** part of the VPN's remote network (= usually the ZyWALL's LAN)
- each client has its **own, unique** IP address

The IP addresses may **not** come from the remote network because the ZyWALL cannot act as an ARP proxy

Example: The VPN gateway 's LAN in our example is the network 192.168.13.0/24 (= 192.168.13.0/255.255.255.0). For the local addresses, choose an arbitrary private network that is not part of this network, such as 10.1.2.0/24. For each user, pick a different IP address from that network to be used as the Local Address in VPN Tracker:

User	IP Address
alice	10.1.2.1
bob	10.1.2.2
charlie	10.1.2.3
…	10.1.2...

Step 2 – Configure the Local Address in VPN Tracker

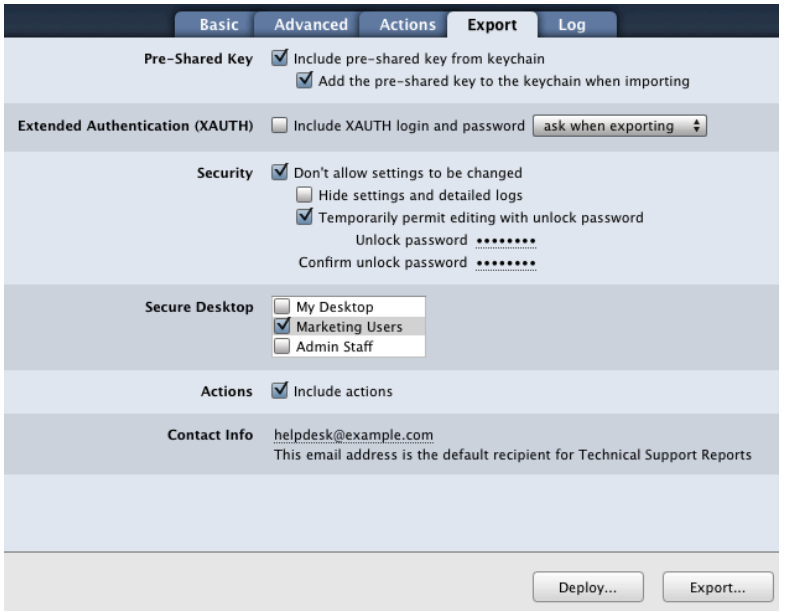
- **Local Address**: Enter the IP address that you have chosen for this user (here: 10.1.2.1 for the user **alice**)

If your ZyWALL is **not** the default gateway (router) of its network, you will have to ensure that traffic for the chosen IP addresses is routed back to the ZyWALL instead of to the usual default gateway (e.g. by adding a route on the default gateway to the ZyWALL for these IPs).

Deploying VPN Connections to Your Users

VPN Tracker Professional Edition offers a number of ways to easily distribute pre-configured connections to users. It is even possible to create a custom VPN Tracker application that contains a pre-configured connection and a license voucher for your users.

Further information on deploying connections to users is available in the VPN Tracker manual.



To deploy VPN Tracker to many users, you can create a custom VPN Tracker application with a pre-configured connection and a license voucher. Simply click "Deploy…" to get started.