



VPN Tracker 365

VPN Configuration Guide

ZyWALL USG Series / ZyWALL 1050

© 2015 equinix AG and equinix USA, Inc. All rights reserved.

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

The equinix logo is a trademark of equinix AG and equinix USA, Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

equinix shall have absolutely no liability for any direct or indirect, special or other consequential damages in connection with the use of this document or any change to the router in general, including without limitation, any lost profits, business, or data, even if equinix has been advised of the possibility of such damages.

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

Configuration guide revision 2

Created using Apple Pages.

www.equinix.com

Contents

Introduction	5
Using the Configuration Guide	5
Prerequisites	7
Scenario	7
Terminology	8
My VPN Gateway Configuration Checklist	9
Task 1 – VPN Gateway Configuration	10
Step 1 – Retrieve Network Settings	10
Step 2 – Create a VPN User	11
Step 3 – Create an Authentication Method	12
Step 4 – Set up Phase 1	13
Step 5 – Set up Phase 2	15
Task 2 – VPN Tracker Configuration	17
Step 1 – Add a Connection	17
Step 2 – Configure the VPN Connection	17
Step 3 – Test the VPN Connection	18
Troubleshooting	20
VPN Connection Fails to Establish	20
No Access to the Remote Network	20
Further Questions?	21
Supporting Multiple Users	22
Preventing IP Address Conflicts	22

Introduction

This configuration guide helps you configure VPN Tracker and your ZyWALL USG 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 USG VPN gateway device using the web configuration interface.



This guide is a supplement to the documentation included with your ZyWALL USG 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 ZyWALL USG and ZyWALL 1050 VPN gateways
- ▶ Make sure you have the **latest firmware** version installed that is available for your device. This configuration guide was created using a ZyWALL USG 200 running firmware v2.20

Your Mac

VPN Tracker runs on Mac OS X 10.4, 10.5, 10.6, and 10.7

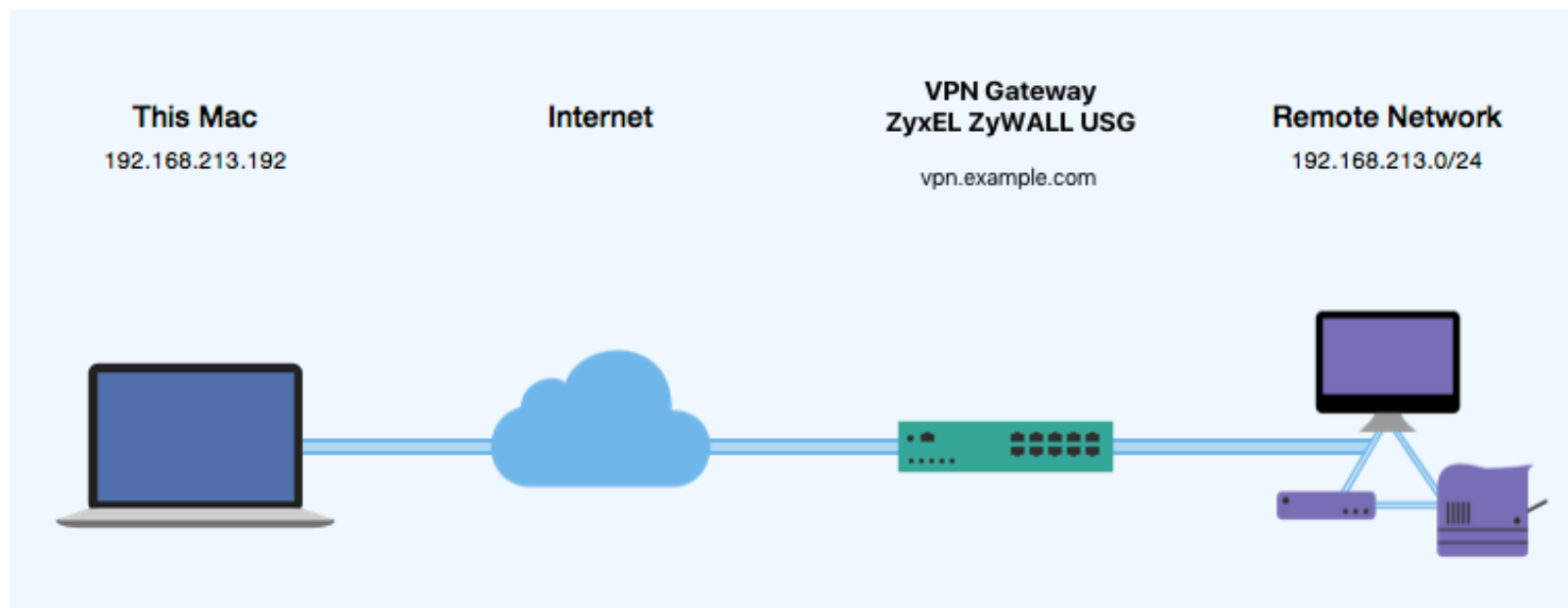
The configuration described in this guide requires VPN Tracker 6. Make sure you have all available updates installed. The latest VPN Tracker updates can always be obtained from <http://www.vpntracker.com>

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 USG 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 USG VPN gateway device.

IP Addresses

- 1 WAN IP Address: _____ (or hostname _____)
- 2 LAN (internal) IP Address / Subnet Mask: _____ / _____

User Authentication (XAUTH)

- 3 Username: _____
- 4 Password: _____

Pre-Shared Key

- 5 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 the **CONFIGURATION** tab to access the device's settings
- ▶ Go to **Network > Interface** and switch to the **Ethernet** tab

The screenshot shows the Mikrotik configuration interface. The left sidebar is titled 'CONFIGURATION' and has a tree view with 'Interface' selected. The main area is titled 'Ethernet' and contains a table of network interfaces. The table has columns for '#', 'Status', 'Name', 'IP Address', and 'Mask'. The first row is 'wan1' with a status of '1' and a lightbulb icon. The fourth row is 'lan1' with a status of '2' and a lightbulb icon. The table also shows 'wan2', 'opt', 'lan2', 'ext-wlan', and 'dmz'.

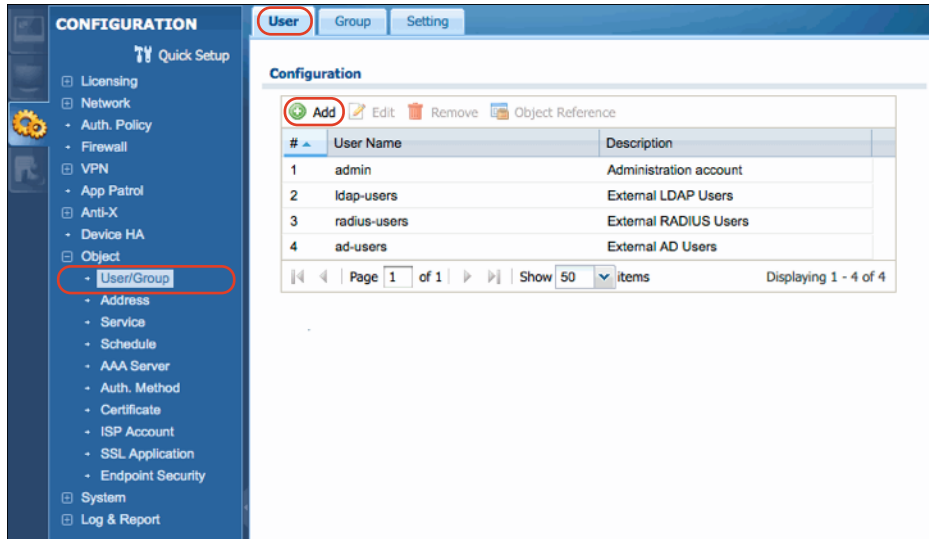
#	Status	Name	IP Address	Mask
1	1	wan1	STATIC -- 203.0.113.1	255.255.255.0
2		wan2	DHCP -- 0.0.0.0	0.0.0.0
3		opt	STATIC -- 0.0.0.0	0.0.0.0
4	2	lan1	STATIC -- 192.168.13.1	255.255.255.0
5		lan2	STATIC -- 192.168.2.1	255.255.255.0
6		ext-wlan	STATIC -- 10.59.0.1	255.255.255.0
7		dmz	STATIC -- 192.168.3.1	255.255.255.0

- ▶ Write down the IP address of the primary **WAN** network interface (here: **wan1**) as **1** on your → *Configuration Checklist*. If your device has a DNS hostname (fixed or DynDNS), write it down instead

- ▶ Write down the IP address of the **LAN** network interface (here: **lan1**), including its **subnet mask** as **2** on your → *Configuration Checklist*

Step 2 – Create a VPN User

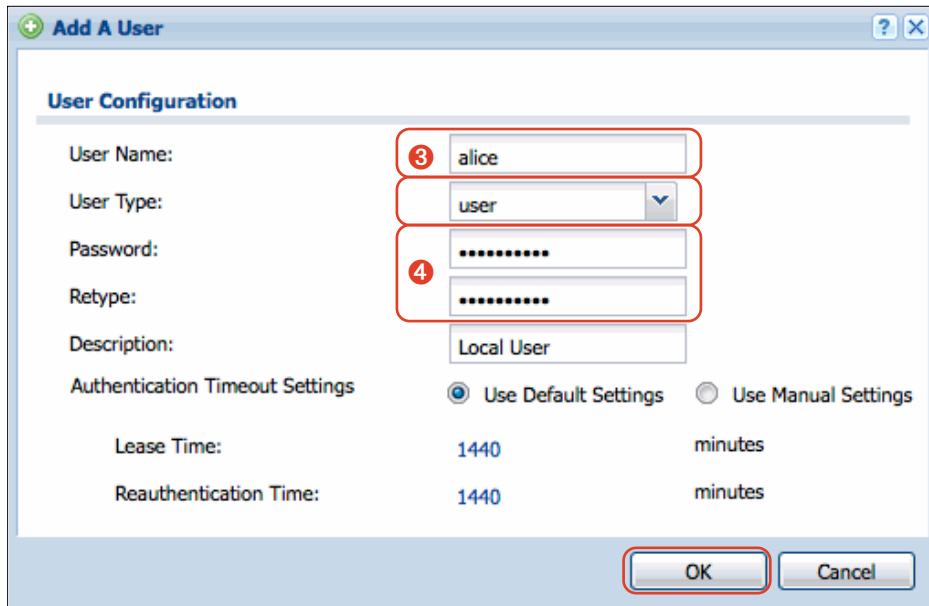
- ▶ Go to **Object > User/Group** and switch to the **User** tab



The screenshot shows the configuration interface with the **User/Group** tab selected in the left sidebar. The main area displays the **Configuration** table with the following data:

#	User Name	Description
1	admin	Administration account
2	ldap-users	External LDAP Users
3	radius-users	External RADIUS Users
4	ad-users	External AD Users

- ▶ Click the **Add** button



The screenshot shows the **Add A User** dialog box with the following configuration fields:

- User Name:** alice
- User Type:** user
- Password:** [Redacted]
- Retype:** [Redacted]
- Description:** Local User
- Authentication Timeout Settings:** Use Default Settings Use Manual Settings
- Lease Time:** 1440 minutes
- Reauthentication Time:** 1440 minutes

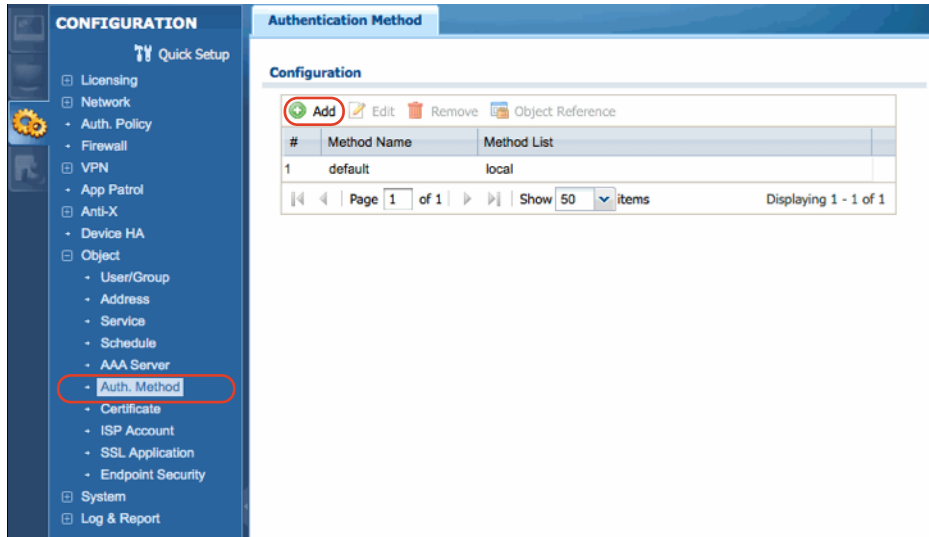
- ▶ **User Name:** Enter a username for the new user (here: **alice**). Write down the user name as ③
- ▶ **User Type:** Choose **user** from the pop-up
- ▶ **Password:** Enter a password for this new user. Make sure to remember the password, or write it down as ④
- ▶ Click **OK** to add the user



To add more users, simply repeat this step. You might want to connect the device to an existing (LDAP or RADIUS) authentication server later (remember to select the appropriate user type for the external authentication server in the **User Type** pop-up). We recommend using a local user for initial setup and testing.

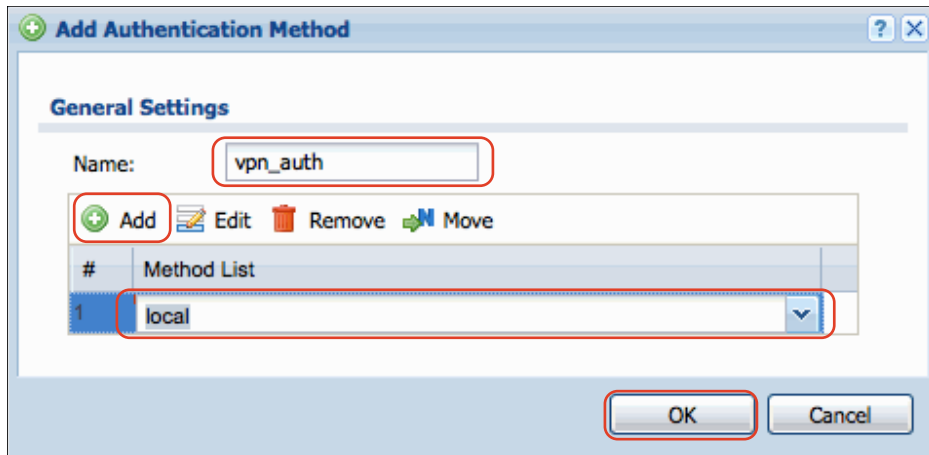
Step 3 – Create an Authentication Method

- ▶ Go to **Object > Auth. Method**



- ▶ Click the **Add** button and choose **local** from the pop-up
- ▶ Click **OK** to save the authentication method

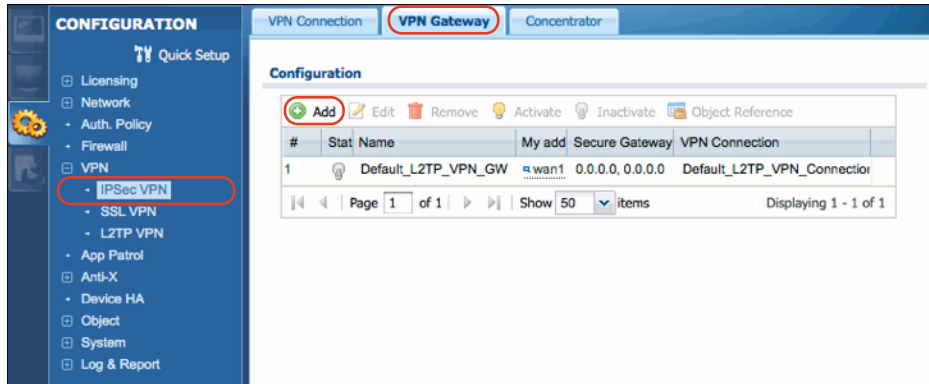
- ▶ Click the **Add** button



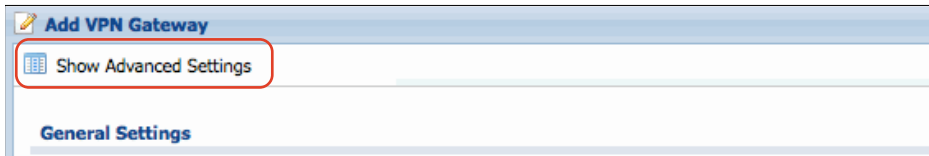
- ▶ **Name:** Enter a name for the new authentication method (here: **vpn_auth**)

Step 4 – Set up Phase 1

- ▶ Go to **VPN > IPsec VPN** and switch to the **VPN Gateway** tab

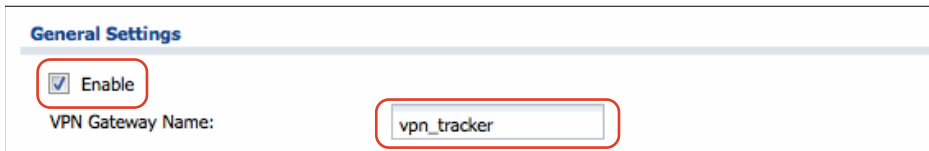


- ▶ Click the **Add** button



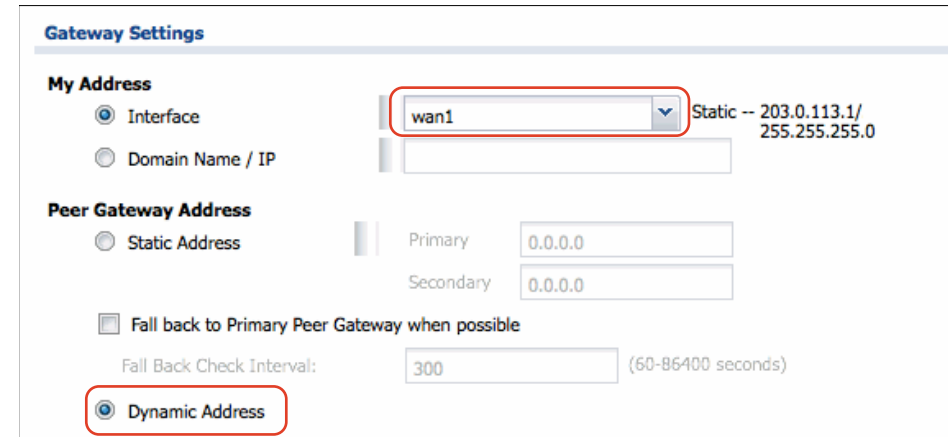
- ▶ Click the **Show Advanced Settings** button to be able to access all settings

General Settings



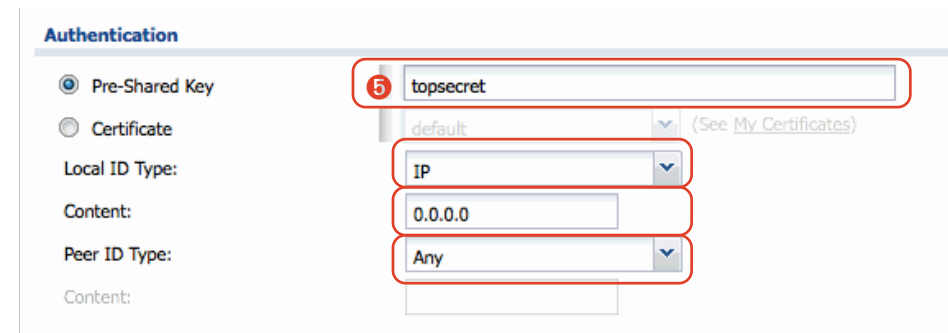
- ▶ Select the **Enable** checkbox to enable the VPN gateway settings that you are about to configure
- ▶ **VPN Gateway Name:** Enter a name for the phase 1 setup (here: **vpn_tracker**)

Gateway Settings



- ▶ **My Address:** Select **Interface** and select your primary **WAN** network interface (here: **wan1**) from the pop-up menu
- ▶ **Peer Gateway Address:** Select **Dynamic Address**

Authentication



- ▶ Enter a **Pre-Shared Key** (here: **topsecret**). 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 selected

- ▶ **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 **Any** is selected. This means that connecting VPN clients can use any identifier type



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.

Phase 1 Settings

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Proposal

#	Encryption	Authentication
1	3DES	SHA1
2	AES128	SHA1

Key Group: DH2

NAT Traversal

Dead Peer Detection (DPD)

- ▶ **SA Life Time:** Leave the default of 86400 seconds
- ▶ **Negotiation Mode:** Leave the default of **Main Mode**

- ▶ **Proposal:** For security reasons, we recommend changing the default proposal settings to use at least **3DES** and **SHA-1** (with the option of using **AES-128** and **SHA-1**) as shown here
- ▶ **Key Group:** Choose **DH2** from the pop-up
- ▶ Select the **NAT Traversal** checkbox
- ▶ Make sure the **Dead Peer Detection (DPD)** checkbox is selected



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.

Extended Authentication

Extended Authentication

Enable Extended Authentication

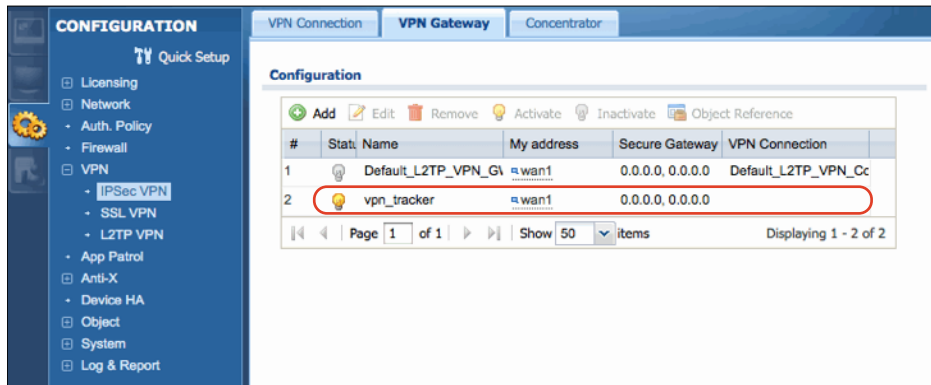
Server Mode (vpn_auth)

Client Mode

User Name:

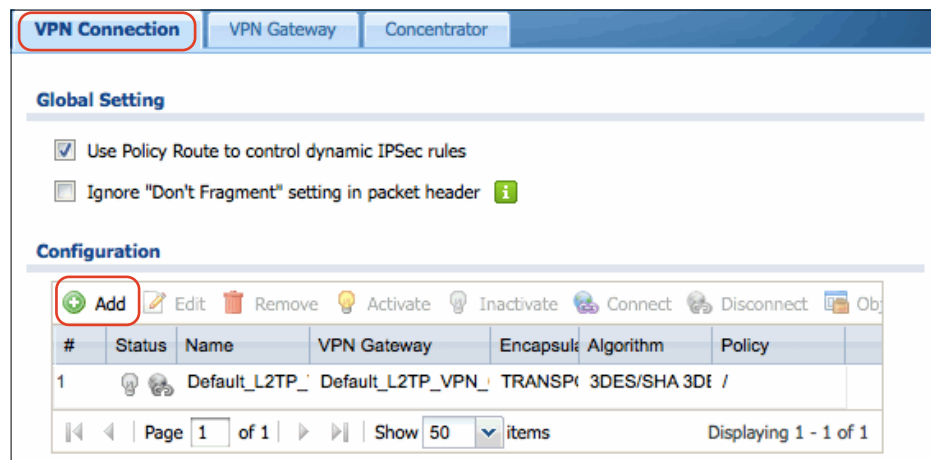
Password:

- ▶ Select the **Enable Extended Authentication** checkbox
- ▶ **Server Mode:** Choose **vpn_auth** from the pop-up. If you do not see the vpn_auth entry here, you may have skipped → *Step 3 – Create an Authentication Method*
- ▶ Click **OK** to complete the phase 1 setup. The result should look similar to what is shown in the following screenshot:

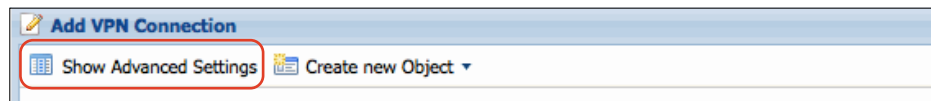


Step 5 – Set up Phase 2

- ▶ Switch to the **VPN Connection** tab (under **VPN > IPsec VPN**)

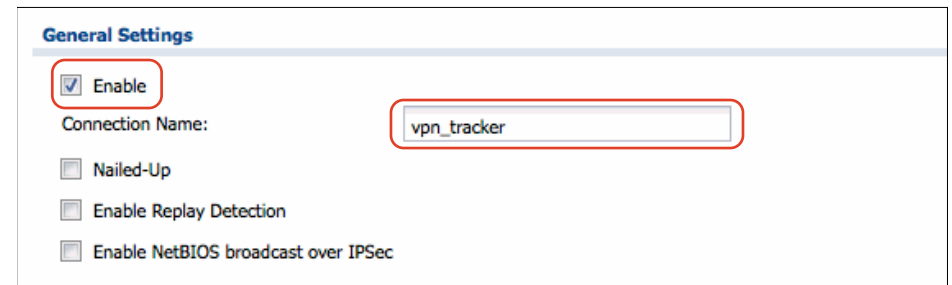


- ▶ Click the **Add** button



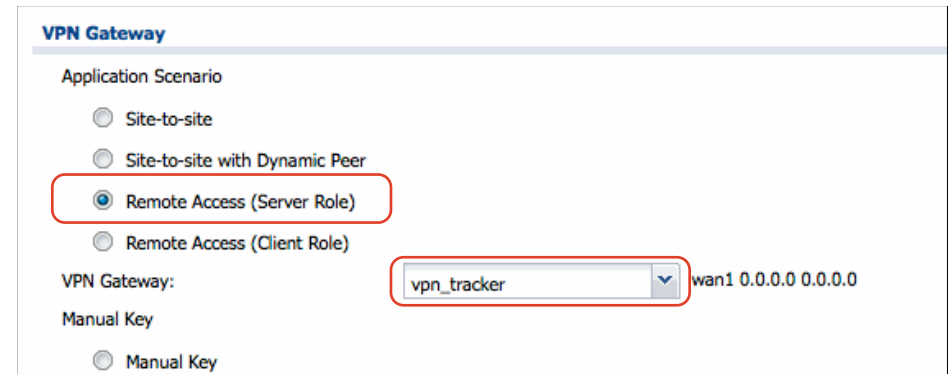
- ▶ Click the **Show Advanced Settings** button to be able to access all settings

General Settings



- ▶ Select the **Enable** checkbox to enable the VPN connection settings that you are about to configure
- ▶ **Connection Name:** Enter a name for the phase 2 setup (here: **vpn_tracker**)

VPN Gateway



- ▶ **Application Scenario:** Select **Remote Access (Server Role)**
- ▶ **VPN Gateway:** Choose the phase 1 (VPN gateway) setup you have created in → *Step 4* (here: **vpn_tracker**) from the pop-up

Policy

Local policy: LAN1_SUBNET INTERFACE SUBNET, 192.168.13.0/24

Policy Enforcement

- ▶ **Local policy:** Choose the address object corresponding to the network(s) VPN clients are permitted to access. Here, **LAN1_SUBNET**, i.e. the ZyWALL's LAN network, is being used. This selection will be appropriate in most cases.
- ▶ Select the checkbox **Policy Enforcement** to restrict VPN client access to the network(s) chosen under **Local Policy**

Phase 2 Settings

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

#	Encryption	Authentication
1	3DES	SHA1
2	AES128	SHA1

Perfect Forward Secrecy (PFS): DH2

- ▶ **SA Life Time:** Leave the default of 86400 seconds
- ▶ **Active Protocol:** Leave the default of **ESP**
- ▶ **Encapsulation:** Leave the default of **Tunnel**
- ▶ **Proposal:** For security reasons, we recommend changing the default proposal settings to use at least **3DES** and **SHA-1** (with the option of using **AES-128** and **SHA-1**) as shown here
- ▶ **Perfect Forward Secrecy (PFS):** Choose **DH2** from the pop-up



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.

Related Settings

Related Settings

Add this VPN connection to IPSec_VPN zone.

- ▶ Make sure **Add this VPN connection to IPSec_VPN zone** is selected. This means that any security rules or settings configured for the IPSec_VPN zone will apply to this VPN connection. **Some devices may not have this option**, in that case, please add the connection manually to **Network > Zone**
- ▶ It is not necessary to make any changes to the **Connectivity Check** and **Inbound/Outbound traffic NAT** settings
- ▶ Click **OK** to complete the phase 2 setup. The result should look similar to what is shown in the following screenshot:

CONFIGURATION

VPN Connection | VPN Gateway | Concentrator

Global Setting

Use Policy Route to control dynamic IPSec rules

Ignore "Don't Fragment" setting in packet header

Configuration

#	Status	Name	VPN Gateway	Encapsula	Algorithm	Policy
1		Default_L2TI	Default_L2TI	TRANSPC	3DES/SHA	3DES/MI /
2		vpn_tracker	vpn_tracker	TUNNEL	3DES/SHA	AES128 LAN1_SUBNET/0.0

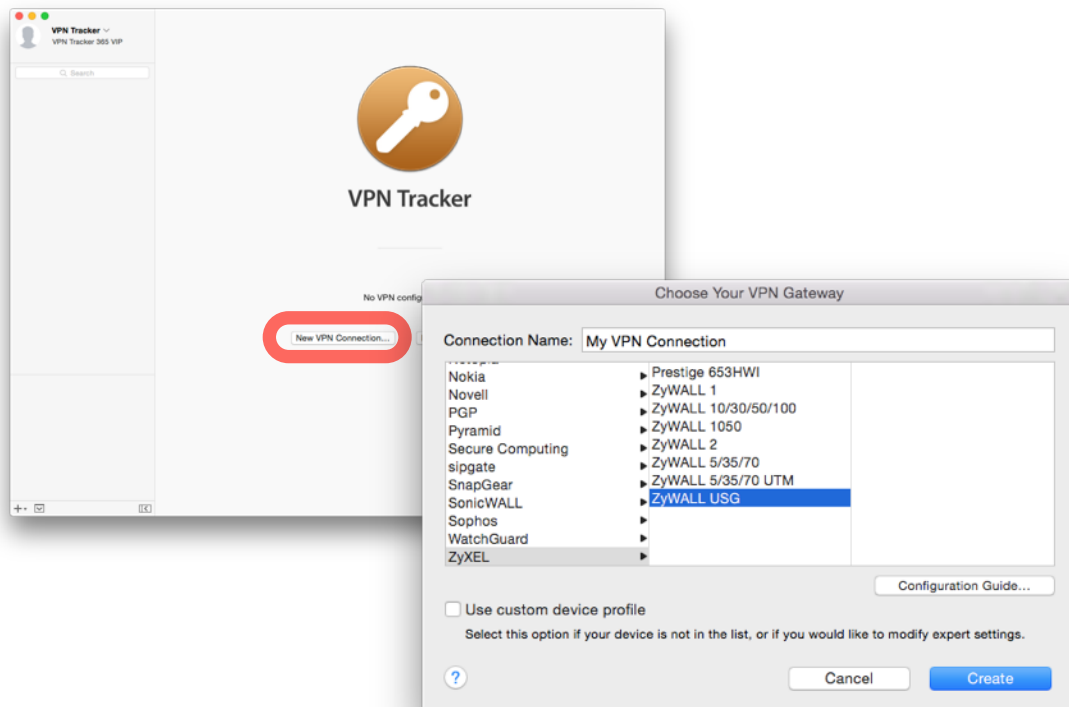
Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

Task 2 – VPN Tracker Configuration

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

Step 1 – Add a Connection

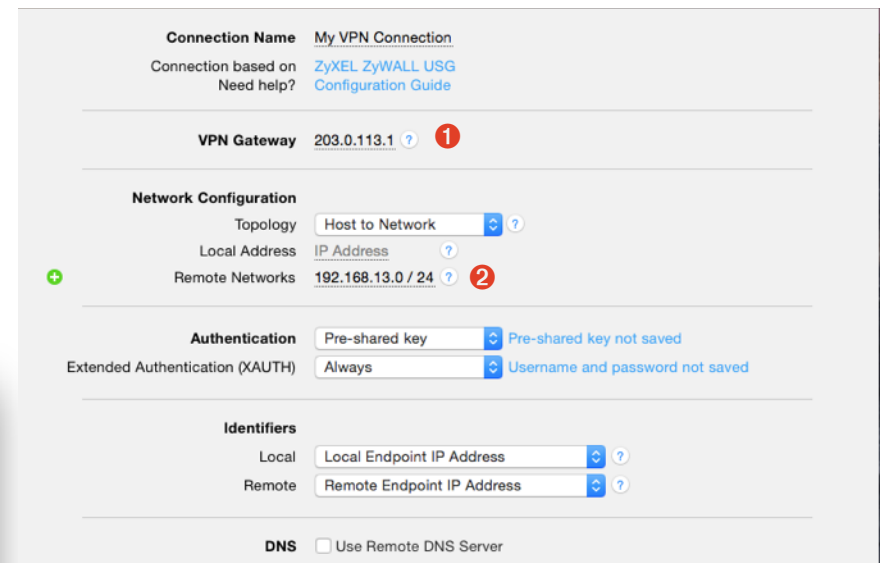
Open VPN Tracker, and click the plus button in the bottom left corner of the window to add a new connection:



- ▶ 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 (,/)”



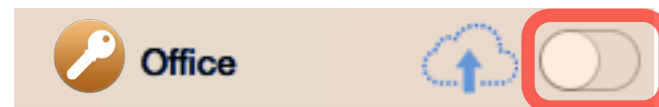
VPN Tracker will automatically turn the IP address into a network address. Double-check that the result is the same as the LAN address object configured for the Local Policy in → *Step 5*

Step 3 – Test the VPN Connection

It ‘s time to go out!

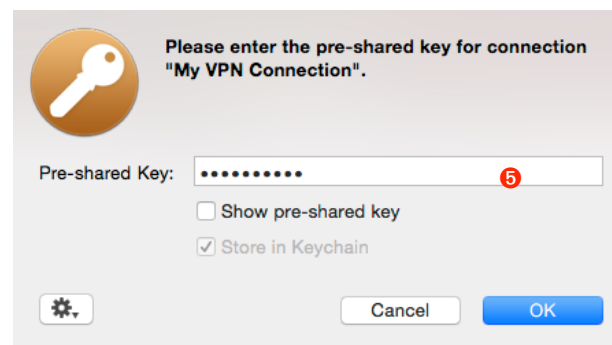
You will not be able to test and use your VPN connection from within the internal network that you want to connect to. To test your connection, you will need to connect from a different location. For example, if you are setting up a VPN connection to your office, test it from home. If you are setting 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 ⑤
- ▶ 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:

- ▶ **Congratulations!**

Please enter the XAUTH credentials for connection "Office".


Domain: optional

User Name: alice 3

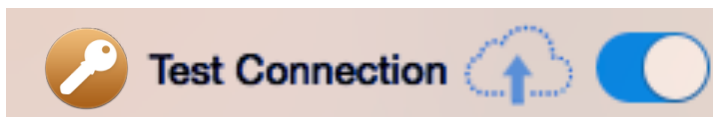
Password: 4

Show typing

Store in Keychain



- ▶ **User Name:** Enter the name of the user you have added on the VPN gateway (here: **alice**) 3
- ▶ **Password:** Enter the password for the user 4
- ▶ 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



Troubleshooting

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

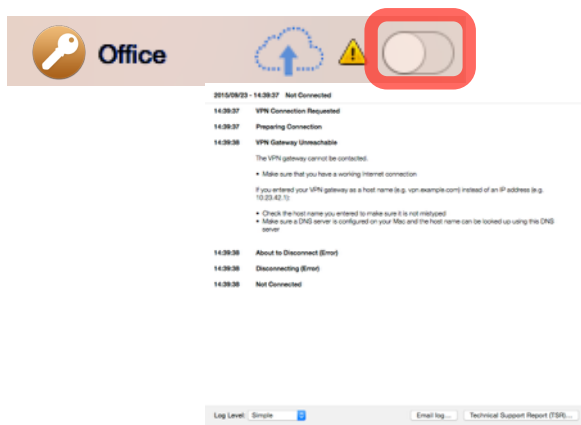
VPN Connection Fails to Establish

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 remote network(s) you permitted in the Local Policy in → *Step 5 – 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

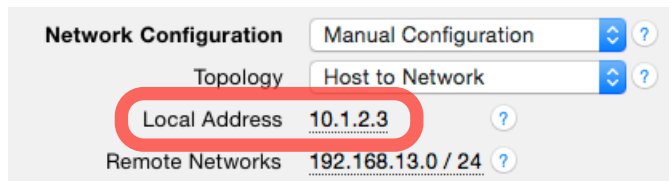
Supporting Multiple Users

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

VPN Gateway	203.0.113.1 ?
Network Configuration	Manual Configuration ?
Topology	Host to Network ?
Local Address	10.1.2.1 ?
Remote Networks	192.168.13.0 / 24 ?

- ▶ **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).