



VPN Configuration Guide

WatchGuard Fireware XTM

Firebox X Edge Core e-Series • Firebox X Edge Core e-Series • Firebox X Edge Peak e-Series • XTM 8 Series • XTM 10 Series

© 2010 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 | 6 |
| Scenario | 6 |
| Terminology | 7 |
| | |
| My VPN Gateway Configuration..... | 8 |
| | |
| Task 1 – VPN Gateway Configuration..... | 9 |
| Step 1 – Retrieve the WAN and LAN Addresses | 9 |
| Step 2 – Add a Mobile User VPN Group | 9 |
| Step 3 – Add a User | 14 |
| | |
| Task 2 – VPN Tracker Configuration..... | 15 |
| Step 1 – Add a Connection | 15 |
| Step 2 – Configure the VPN Connection | 15 |
| | |
| Task 3 – Test the VPN Connection..... | 16 |
| | |
| Troubleshooting..... | 18 |
| VPN Connection Fails to Establish | 18 |
| No Access to the Remote Network | 18 |
| Further Questions? | 19 |
| | |
| Host to Everywhere Connections..... | 20 |

Introduction

This configuration guide helps you configure VPN Tracker and your WatchGuard Firebox device 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 Mobile User VPN (MUVPN) connection on your WatchGuard device.



This guide is a supplement to the documentation included with your WatchGuard 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 Advanced Topics

Troubleshooting advice and additional tips 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 WatchGuard Firebox devices running Fireware XTM.

- ▶ Firebox X Edge e-Series
- ▶ Firebox X Core e-Series
- ▶ Firebox X Peak e-Series
- ▶ XTM 2 Series
- ▶ XTM 5 Series
- ▶ XTM 8 Series
- ▶ XTM 10 Series



Make sure you have the newest available firmware installed on your device. This guide describes the web-based configuration using Fireware XTM. Screenshots are based on Fireware XTM 11.1.

Your Mac

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

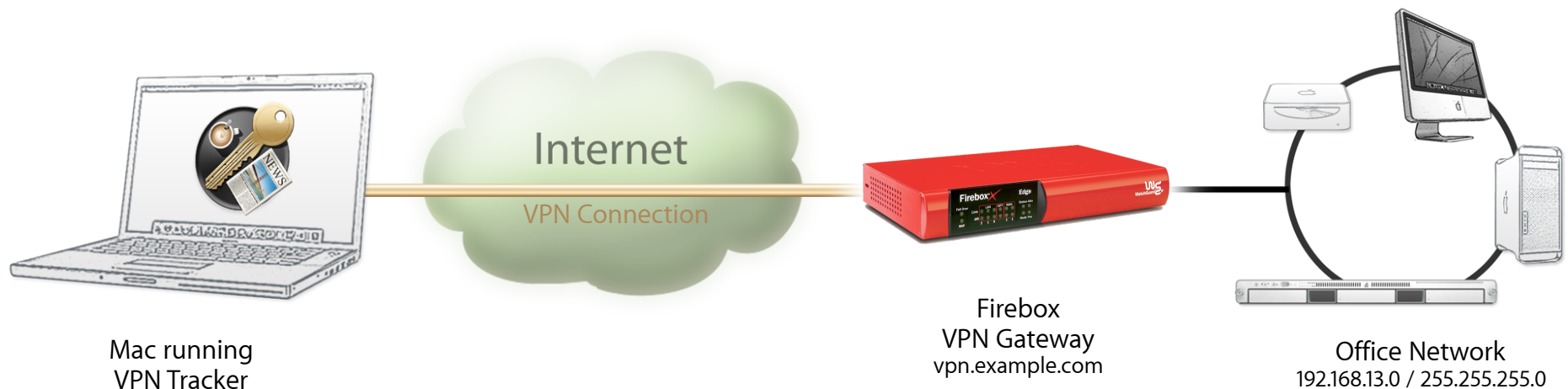
The configuration described in this guide requires VPN Tracker 6. Make sure you have all available updates installed. The latest VPN Tracker updates can always be obtained from <http://www.vpntracker.com>

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 WatchGuard 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 host name: `vpn.example.com`.

The VPN gateway has a second network interface which is connected to the internal office network (LAN). In our example, the office network has the IP range 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

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 out this checklist to help keep track of the various settings of your WatchGuard Firebox device.

Firebox IP Addresses

❶ WAN IP Address: _____ or hostname _____

❷ LAN IP Address / Subnet: _____ / _____

Group Authentication

❸ Group Name: _____

❹ Passphrase (Pre-Shared Key): _____

Allowed Resources

❺ LAN Network Address / Subnet: _____ / _____

User Authentication (XAUTH)

❻ Username: _____

❼ Password: _____

Task 1 – VPN Gateway Configuration

We will start out with a fairly simple setup. If you have more complex requirements, you can always refine your configuration later.

Step 1 – Retrieve the WAN and LAN Addresses

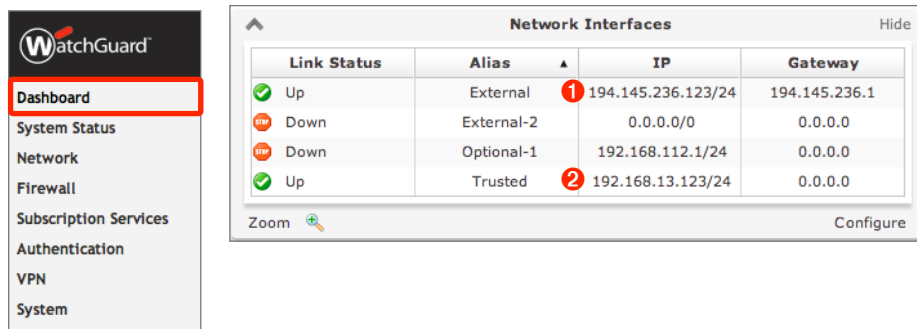
Log into your Firebox's web interface now. The web interface can usually be reached from the trusted network (LAN) of your Firebox.

For example, if your Firebox's LAN IP address is 192.168.13.123, you would access the configuration web interface at

<https://192.168.13.123:8080>

For more information, please refer to your Firebox's documentation.

Once logged in, navigate to Dashboard. On the Dashboard, you will find an overview of the IP addresses used by your Firebox:



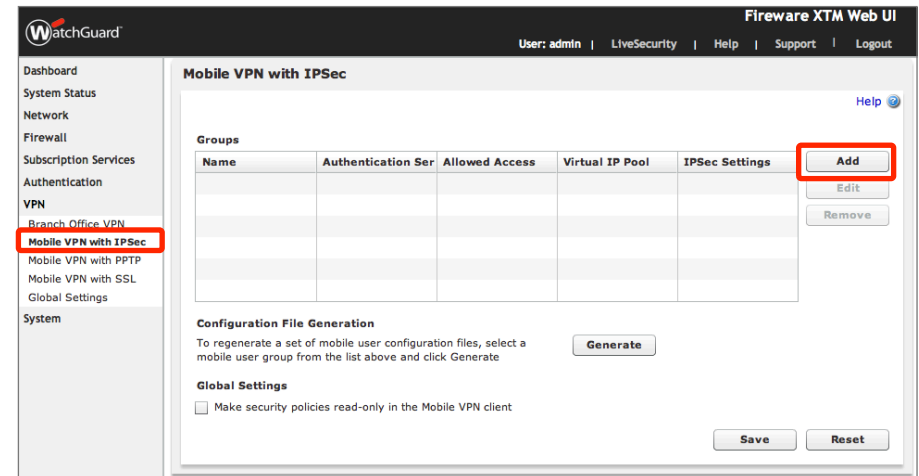
The screenshot shows the WatchGuard web interface. On the left is a navigation menu with 'Dashboard' highlighted. The main content area displays a table titled 'Network Interfaces' with columns for Link Status, Alias, IP, and Gateway. The table contains four rows of data. Red circles with numbers 1 and 2 are placed next to the IP addresses 194.145.236.123/24 and 192.168.13.123/24 respectively.

| Link Status | Alias | IP | Gateway |
|-------------|------------|--------------------|---------------|
| Up | External | 194.145.236.123/24 | 194.145.236.1 |
| Down | External-2 | 0.0.0.0/0 | 0.0.0.0 |
| Down | Optional-1 | 192.168.112.1/24 | 0.0.0.0 |
| Up | Trusted | 192.168.13.123/24 | 0.0.0.0 |

- ▶ Locate the **External** entry. This is your Firebox's WAN IP address. Write it down on your → *configuration checklist* as ❶. Do **not** write down the part after the forward slash (/). In this example, you would write: 194.145.236.123. If your Firebox has a DNS hostname (e.g. vpn.example.com), write down the hostname as well.
- ▶ Locate the **Trusted** entry. This is your LAN IP and Subnet. Write it down as ❷. This time include the part after the forward slash (/). In the example, you would write: 192.168.13.123/24

Step 2 – Add a Mobile User VPN Group

- ▶ We will be using the Mobile User VPN (MUVPN) on the Firebox. To begin, access your WatchGuard's web configuration interface and log in.
- ▶ Go to VPN > Mobile VPN with IPsec
- ▶ Click Add



The screenshot shows the 'Mobile VPN with IPsec' configuration page in the WatchGuard web interface. The left navigation menu has 'VPN' > 'Mobile VPN with IPsec' selected. The main content area features a table with columns for Name, Authentication Ser, Allowed Access, Virtual IP Pool, and IPsec Settings. An 'Add' button is highlighted with a red box. Below the table are sections for 'Configuration File Generation' and 'Global Settings'.

▶



If you have not done so already, print out the → *configuration checklist*, so you can easily keep track of the various settings.

General Settings

Mobile VPN with IPSec Settings

Group name : **3**

General | **IPSec Tunnel** | **Resources** | **Advanced**

General Settings

Authentication Server :

Passphrase

Passphrase : **4**

Confirm :

Firebox IP Addresses

Mobile VPN with IPSec clients will connect to one of these External IP addresses or domains

External IP address : **1**

Backup IP address :

Timeouts

If the session and Idle timeouts are configured on your authentication server, they will take precedence over these settings

Session Timeout : minutes

Idle Timeout : minutes

Group Name

Enter a group name for the users of this VPN connection. If you plan to have multiple groups with different access privileges, you should name them so you recognize them later (e.g. Marketing, WebAdmins, Developers, ...), otherwise you can just choose a generic name. Write down the group name as **3**



The group name cannot contain spaces. As with most VPN-related settings, the group name is case-sensitive, so make sure to write down the correct capitalization.

Passphrase

The passphrase entered here is used as the pre-shared key for your VPN connection. Make sure to choose a good password, and write it down as **4**

Firebox IP Addresses

Enter the external (WAN) IP address of your Firebox that you wrote down as **1** in the last step of this configuration guide.

IPsec Tunnel Settings

The screenshot shows the 'IPSec Tunnel' configuration window with the 'Advanced' tab selected. Under 'Phase 1 Settings', the 'Advanced' button is highlighted with a red box. Under 'Phase 2 Settings', the 'Diffie-Hellman Group 2' dropdown menu is highlighted with a red box.

- ▶ In the **Phase 2 Settings**, select **Diffie-Hellman Group 2** for PFS
- ▶ Click **Phase 1 Settings > Advanced**
- ▶ Change the **Diffie-Hellman Group** to **Group 2**

The screenshot shows the 'Phase 1 Advanced Settings' window. The 'Key Group' dropdown menu is highlighted with a red box and set to 'Diffie-Hellman Group 2'.

If you are using VPN Tracker Personal Edition

VPN Tracker Personal Edition does not include support for AES-256, the default encryption algorithm for phase 2. You will have to change the algorithm to AES-128 or 3DES if you plan to access this VPN using VPN Tracker Personal Edition.

- ▶ Click **Phase 2 > Advanced**
- ▶ Change the **Encryption Algorithm** to **AES (128-bit)**

The screenshot shows the 'Phase 2 Advanced Settings' window. The 'Encryption' dropdown menu is highlighted with a red box and set to 'AES(256-bit)'. A red arrow points from this menu down to the next screenshot.

The screenshot shows the 'Phase 2 Advanced Settings' window. The 'Encryption' dropdown menu is highlighted with a red box and set to 'AES(128-bit)'. A red arrow points from the previous screenshot to this one.



If you make any other changes (e.g. selecting a different encryption algorithm or a different Diffie-Hellman group), you will have to match these settings on VPN Tracker's Advanced tab. As you can always make such changes later, we recommend using the above settings for your first connection attempt.

Resources Settings

Mobile VPN with IPSec Settings

Group name :

General | **IPSec Tunnel** | **Resources** | **Advanced**

Allow All Traffic Through Tunnel

Allowed Resources

| Allowed Resources |
|-------------------|
| |
| |
| |
| |

Choose Type : **Network IP** ▼

Network IP: /

Virtual IP Address Pool

| Virtual IP Address Pool |
|-------------------------|
| |
| |
| |
| |

Choose Type : **Host Range** ▼

From: to:

Allowed Resources

This setting indicates which IP addresses can be accessed by VPN users. In most cases, you will add the Firebox's LAN network address here.



When choosing the type **Network IP**, always make sure to enter a correct **network address** (with the subnet mask applied, e.g. 192.168.13.0 / 24, **not** 192.168.13.123 / 24).

- ▶ Choose Type: Select **Network IP**
- ▶ **Network IP**: Enter the network address of your Firebox's LAN and its network mask (in CIDR notation).
- ▶ Write down what you entered as ⑤
- ▶ Click **Add**

If you don't know how to get your LAN's network address:

Go back to the LAN IP and subnet you wrote down as ② Does it end in /24?

- ▶ If it **ends in /24**, simply replace the last part of the IP address with a zero (0) to get the network address. In our example:

192.168.13.123 / 24 → 192.168.13.0 / 24

- ▶ If it does **not end in /24**, open VPN Tracker and add a new connection. In the new connection, enter your Firebox's LAN IP and subnet ② into the "Remote Networks" field. When you press return, VPN Tracker will automatically transform it into a correct network address:

| | | | |
|-----------------------|------------------------|-----------------------|------------------------|
| Network Configuration | Manual Configuration ▼ | Network Configuration | Manual Configuration ▼ |
| Topology | Host to Network ▼ | Topology | Host to Network ▼ |
| Local Address | IP Address | Local Address | IP Address |
| Remote Networks | 192.168.13.123 / 24 | Remote Networks | 192.168.13.0 / 24 |

Once you're done, you can delete this VPN connection again, or keep it around until you are ready to set up VPN Tracker in part two of this guide.



The setting **Allow All Traffic Through Tunnel** corresponds to a **Host to Everywhere** connection in VPN Tracker. Refer to → *Host to Everywhere Connections* to learn more.

Virtual IP Address Pool

Each connecting VPN client will be assigned an IP address from this pool of addresses. It therefore needs to contain at least as many IP addresses as VPN users are expected. Make sure to choose IP addresses that are not used for anything else on your Firebox's LAN.

In our example, the IP addresses 192.168.13.150 – 192.168.13.199 will be made available to VPN users.

- ▶ **Choose Type:** Select **Host Range**
- ▶ **From:** Enter the first IP address available to VPN clients (here: 192.168.13.150)
- ▶ **To:** Enter the last IP address for VPN client (here: 192.168.13.199)
- ▶ Click **Add**

Advanced Settings

Mobile VPN with IPSec Settings Help ?

Group name

General | **IPSec Tunnel** | **Resources** | **Advanced**

Line Management

Connect mode ▼

Inactivity timeout ▲ ▼ seconds

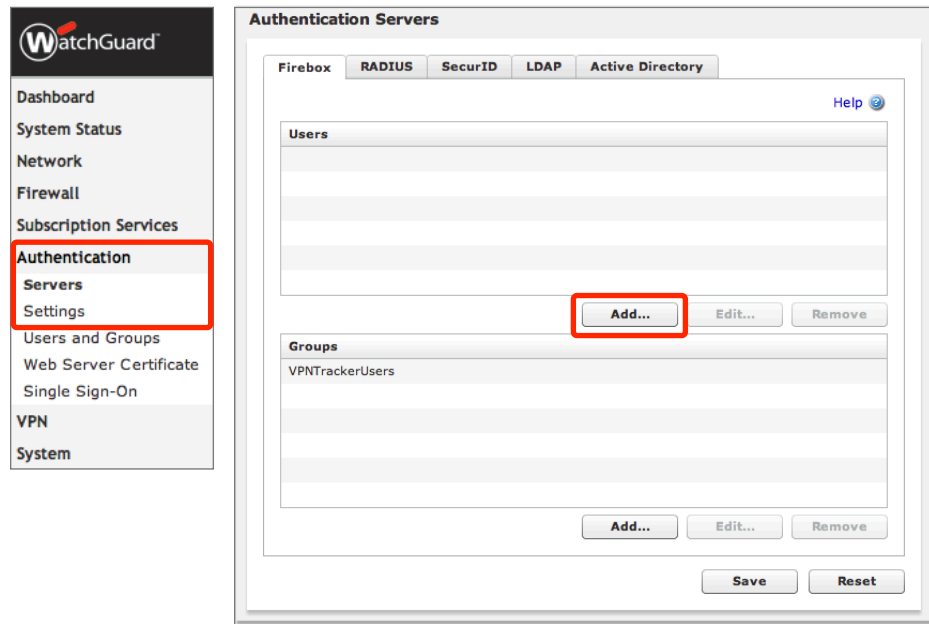
You do not have to make any changes to the Advanced settings.



Don't forget to click **Save** to save your new MUVPN policy!

Step 3 – Add a User

To add users to your VPN go to **Authentication > Servers > Settings**. You will already see your Mobile User VPN group there:



Click **Add** to begin adding a new user to the group.

- ▶ **Name:** Enter the user name (login) of the new user and write it down as ⑥
- ▶ **Description:** Enter an optional description
- ▶ **Passphrase:** Enter the user's password and write it down as ⑦. Enter it again in the **Confirm** text field.
- ▶ **Session/Idle Timeout:** Use the default values, or change them as necessary
- ▶ **Firebox Authentication Groups:** Select your MUVPN's group and click the button "<<" to make your new user a member of this group.
- ▶ Click **OK** to add the new user



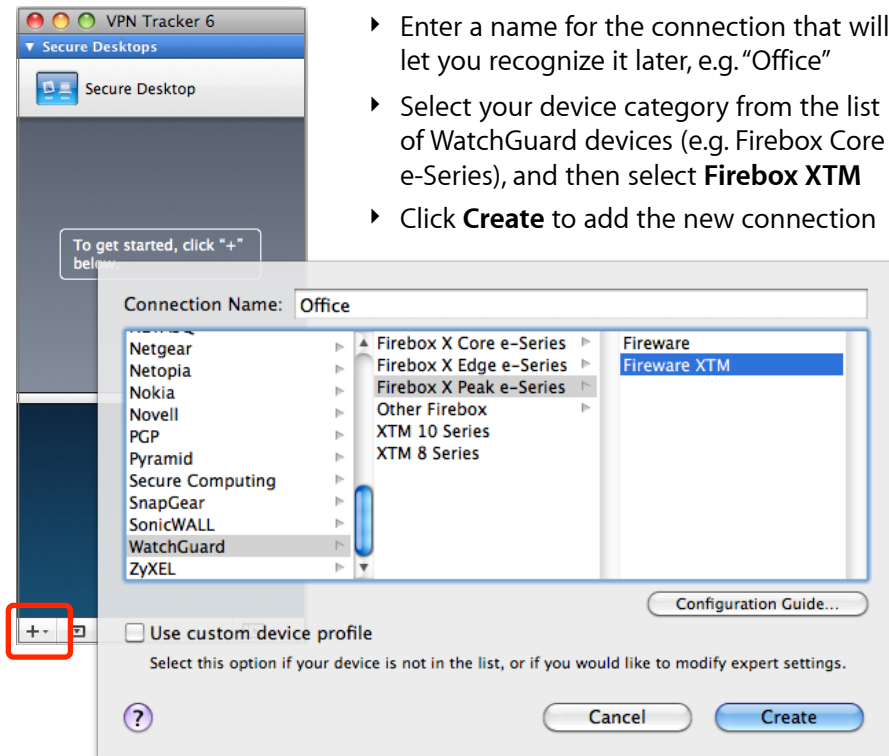
Just like you added this first user, you can add more users to your group later. Also check out the VPN Tracker manual to learn how to easily roll out VPN Tracker to users in your organization.

Task 2 – VPN Tracker Configuration

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

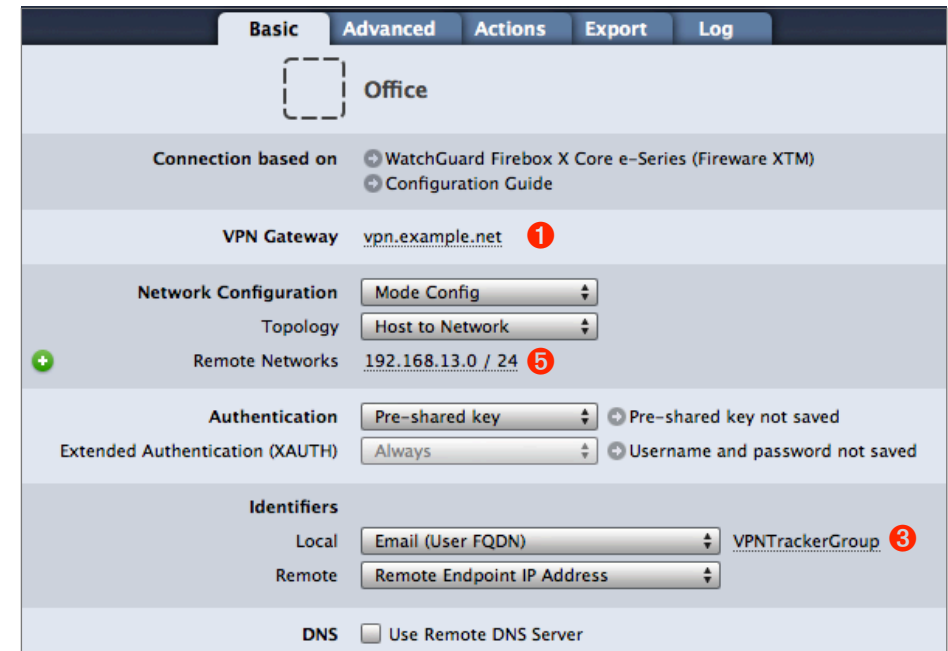
Step 1 – Add a Connection

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



Step 2 – Configure the VPN Connection

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



VPN Gateway

Enter the external (WAN) IP address of your Firebox that you wrote down as **1**. If your Firebox has a DNS host name (such as vpn.example.com in our example), you can use it instead.

Remote Networks

Enter your Firebox's internal (LAN) network address **5**. Now would be a good time to check that it looks exactly like what you have configured for the **Allowed Resources** on your Firebox. If it's not the same, make sure you have actually used a network address for this setting (see → *Resources Settings*)

Local Identifier

Enter the group name you configured on your Firebox **3**. Make sure the capitalization is the same as on your Firebox.

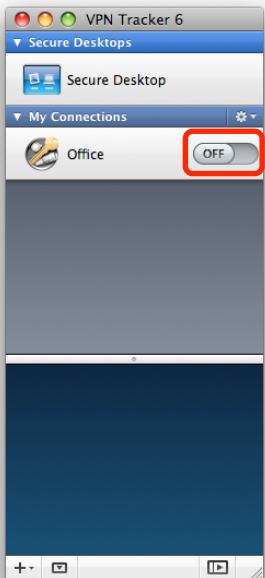
Task 3 – Test the VPN Connection

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

It's time to go out!

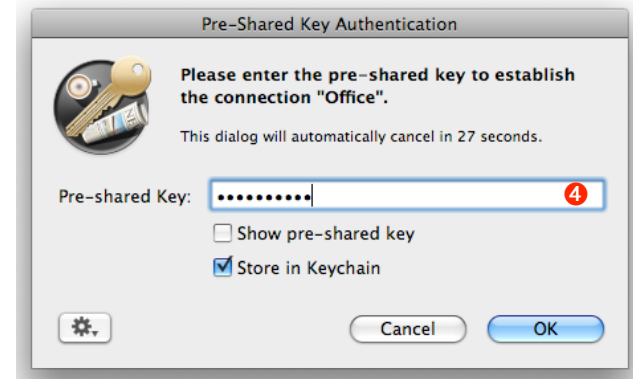
You will not be able to test and use your VPN connection from within the internal network that you want to connect to. In order to test your connection, you will need to connect from a different location. For example, if you are setting up a VPN connection to your office, test it from home. If you are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

If you are prompted for your pre-shared key:

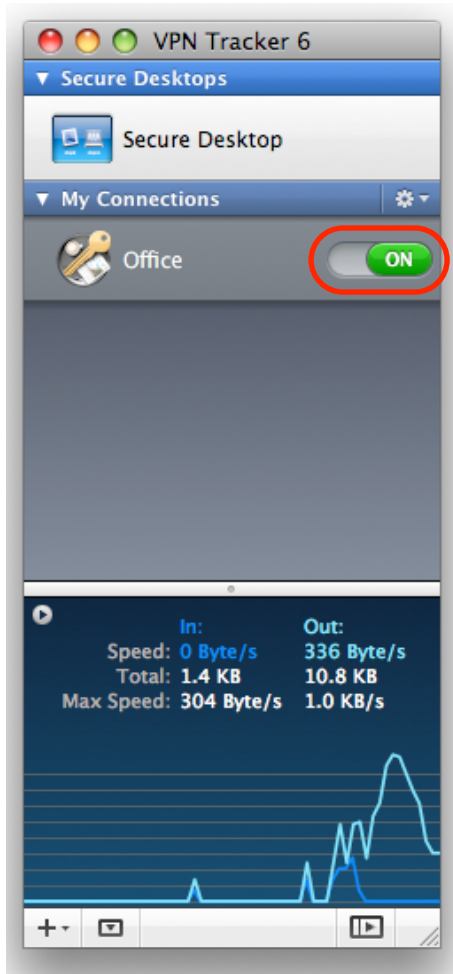


- ▶ **Pre-shared key:** Enter the passphrase that you configured on the Firebox for the Mobile User VPN 4
- ▶ Optional: Check the box **Store in Keychain** to save the password in your keychain so you are not asked for it again when connecting the next time
- ▶ Click **OK**

If you are prompted for your Extended Authentication (XAUTH) credentials:



- ▶ User Name: Enter the name of the user you have added on the Firebox 2
- ▶ Password: Enter the password for the user 3
- ▶ 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.

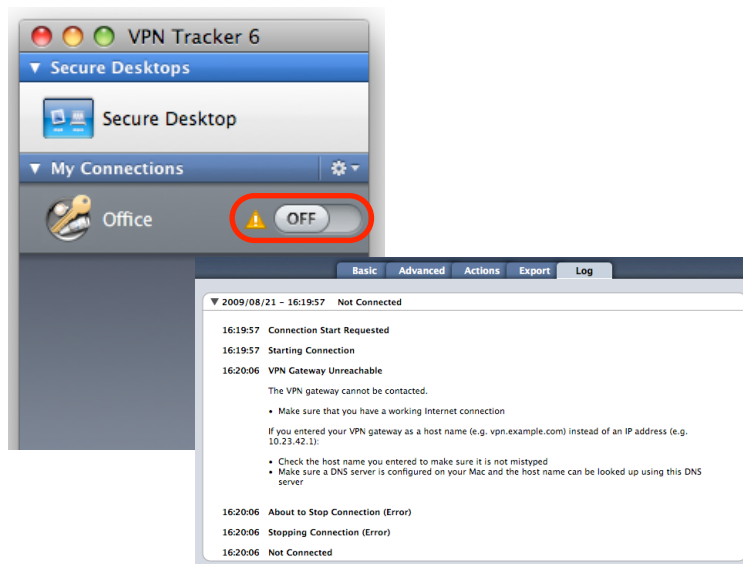
VPN Connection Fails to Establish

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 error (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.) in the VPN, 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 in VPN Tracker 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 VPN's remote network

Check that the IP address you are connecting to is actually part of the remote network(s). Also double-check the network mask that you have configured for the remote network(s) in VPN Tracker.

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

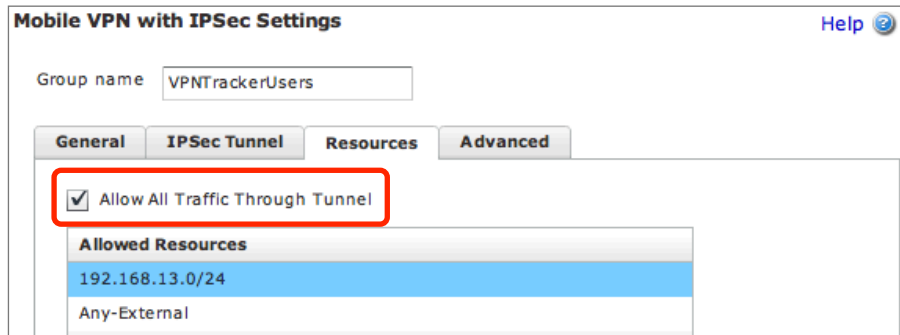
If you can't resolve your issue with the information available on our website or in this guide and would like to contact Technical Support through our website, please be sure to include at least the following information:

- ▶ 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

Host to Everywhere Connections

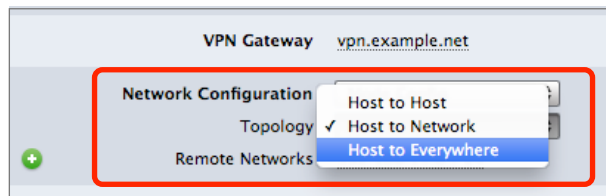
In some situations, such as when connecting from a public wireless network, it can be useful to direct all Internet traffic through the VPN. The following changes are necessary to tunnel all Internet traffic through the VPN:

Change the Allowed Resources



- ▶ On your **Firebox**, edit the Mobile User VPN group you created in Task 1
- ▶ Go to **Resources**
- ▶ Check the box **Allow All Traffic Through Tunnel**
- ▶ Click **Save**

Change the Topology to Host to Everywhere

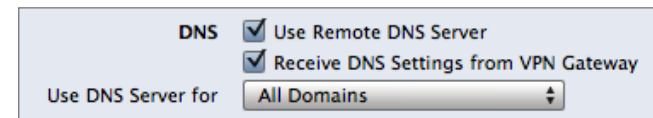


- ▶ In **VPN Tracker** select your VPN connection and go to the **Basic** tab
- ▶ Change the **Topology** setting to **Host to Everywhere**

Configure DNS

Since all your Internet traffic will be going through the VPN, you will need to ensure that DNS resolution (looking up host names, such as www.google.com, and translating them to IP addresses) still works. Otherwise, it will seem as if you are cut off from the Internet.

If DNS on your Firebox is properly configured, it will automatically transmit a suitable DNS server through Mode Config. To use this DNS server, check the boxes **Use Remote DNS Server** and **Receive DNS Setting from VPN Gateway**, and set this DNS server to be used for **All Domains**:



If you already have a **working Remote DNS setup** in VPN Tracker, you will normally not have to change it.