e·quinux

VPN Tracker 365

VPN Configuration Guide

WatchGuard Fireware XTM

Contents

Introduction

This configuration guide helps you configure VPN Tracker and your WatchGuard Firebox device to establish a VPN connection between them.

Prerequisites

Your VPN Gateway

‣ This guide applies to WatchGuard firewall/VPN appliances running Fireware XTM. Documentation for other devices may be available at http://www.vpntracker.com/interop.

‣ Make sure you have installed the newest Fireware version available to ensure that you have all security updates and bugfixes.

‣ This guide is a supplement to the documentation included with your WatchGuard device, it can't replace it. Please it before starting.

> ⚠️ 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 11.6.

Your Mac

‣ Make sure you have all available updates installed. The latest VPN Tracker updates can be obtained from http://www.vpntracker.com.

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.

> 💡 If you are setting up VPN on your WatchGuard firewall for the first time, we strongly recommend you keep to setup proposed in this guide, and make modifications only after you have tested the basic setup.

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 – Host to Everywhere Connections

The final part of this documents shows you how to set up your VPN so all traffic passes through the VPN.

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.

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.

Scenario

In our example, we need to connect an employee's Mac to an office network. The diagram below illustrates this scenario.

This guide assumes that the Mac running VPN Tracker already has Internet connectivity. The office's WatchGuard VPN appliance (the "VPN gateway") is also already connected to the Internet and can be accessed through a static IP address (here: 203.0.113.1) or a DNS host name (here: vpn.example.com).

The VPN gateway's LAN interface is connected to the internal office network. In our example, the office network is 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.
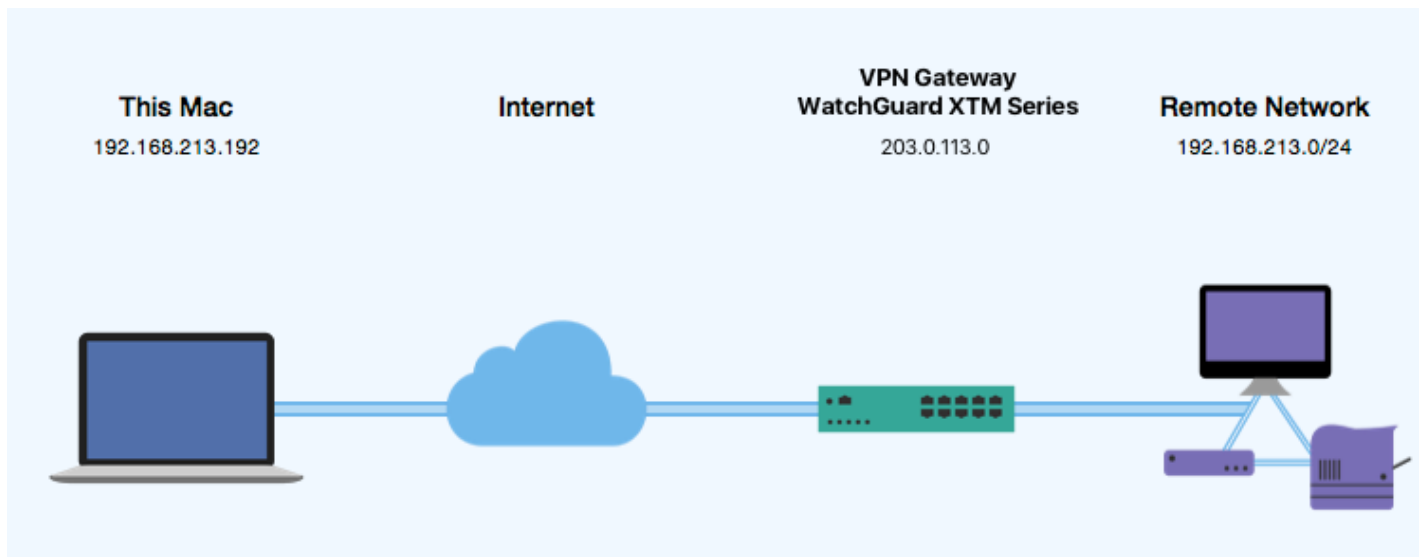
This Mac	Internet	VPN Gateway WatchGuard XTM Series	Remote Network
192.168.213.192		203.0.113.0	192.168.213.0/24

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. You can print out this checklist to help keep track of the various settings of your WatchGuard VPN appliance.

IP Addresses

❶ WatchGuard WAN IP Address: _____._____._____._____ or hostname _____

❷ WatchGuard 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.
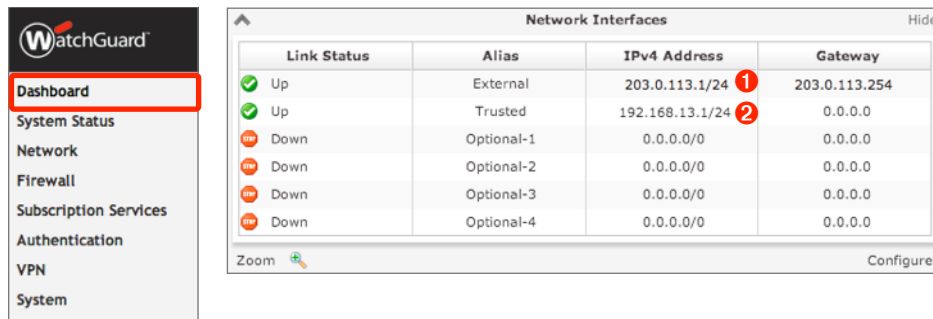
Step 1 – Retrieve the WAN and LAN Addresses

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

For example, if the device's LAN IP address is 192.168.13.1, you would access the configuration web interface at

https://192.168.13.1:8080

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

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

> If you have not done so already, you may want to print the → *Configuration Checklist*, so you can easily keep track of the various settings.

‣ Locate the **External** entry. This is the device'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: 203.0.113.1. 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, do include the part after the forward slash (/). In the example, you would write: 192.168.13.1/24

Step 2 – Add a Mobile User VPN Group

‣ Go to **VPN > Mobile VPN with IPsec.**

‣ Click **Add.**
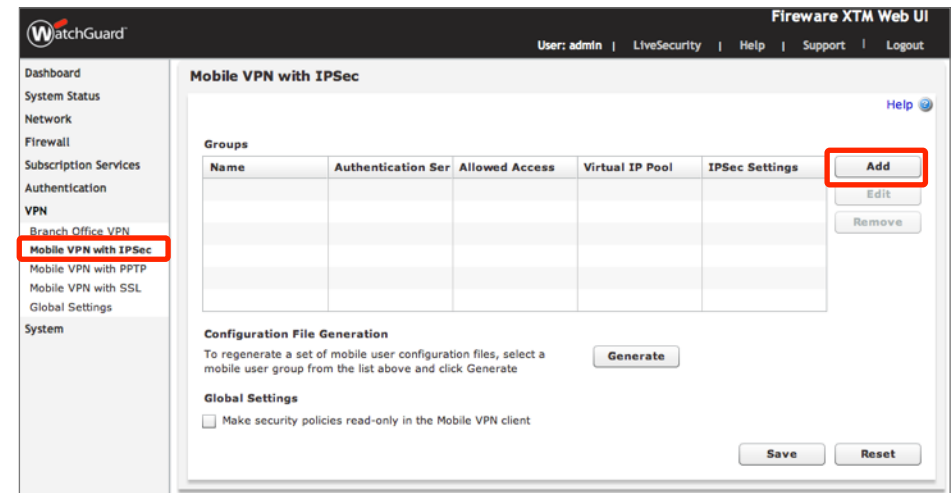
General Settings

Mobile VPN with IPSec Settings   Help

Group name VPNTrackerUsers ❸

| General | IPSec Tunnel | Resources | Advanced |

General Settings
Authentication Server Firebox-DB ▼

Passphrase

Passphrase ********** ❹
Confirm **********

Firebox IP Addresses

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

Primary 203.0.113.1 ❶
Backup

Timeouts

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

Session Timeout 480 minutes
Idle Timeout 30 minutes

Save   Cancel

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 simply choose a generic name. Write down the group name as ❸

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 ❹

Firebox IP Addresses

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

IPsec Tunnel Settings

You can leave the defaults for most IPSec Tunnel settings. However, for better security, we recommend changing the Diffie-Hellman Group for both phases to at least group 2.

| General | IPSec Tunnel | Resources | Advanced |

IPSec Tunnel

⦿ Use the passphrase of the end user profile as the pre-shared key

◯ Use a certificate

CA IP address
Timeout 25 Seconds

Phase 1 Settings   Advanced

Authentication SHA-1 ▼
Encryption 3DES ▼

Phase 2 Settings   Advanced

☑ PFS Diffie-Hellman Group 2 ▼
        Diffie-Hellman Group 1
        Diffie-Hellman Group 2
        Diffie-Hellman Group 5

Save   Cancel

Phase 2 PFS Diffie-Hellman Group

Your device likely uses Diffie-Hellman Group 1 by default. For better security, you should change this to Group 2 (the default used in VPN Tracker) or Group 5 (the most secure group available on these devices at the time of writing).

‣ Make sure **Phase 2 Settings > PFS** is checked.

‣ Select **Diffie-Hellman Group 2**.

Phase 1 Advanced Settings: Diffie-Hellman Group

‣ Click **Advanced** next to **Phase 1 Settings**.

‣ Change the **Key Group** to **Diffie-Hellman Group 2**.

‣ **Return to General Settings**.

Phase 2 Advanced Settings

‣ **Force Key Expiration**: Uncheck the box next to **Traffic**.

‣ **Return to General Settings**.

Resources Settings

Allow All Traffic Through Tunnel

This setting should remain un-checked for now. If checked, a Host to Everywhere connection will be created. You can find more information in → *Host to Everywhere Connections*.

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.

‣ **Choose Type**: Select **Network IP.**
‣ **Network IP**: Enter the LAN network address of WatchGuard appliance.
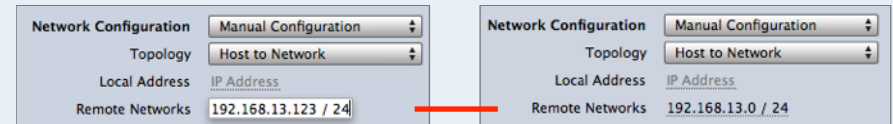‣ Write down what you entered as ❺.
‣ Click **Add**.

⚠️ Always make sure to enter a correct **network address** (with the subnet mask applied, e.g. 192.168.13.0/24, **not** 192.168.13.1/24).

What is the correct LAN network address for my WatchGuard device?

Look at the LAN IP and subnet you wrote down as ❷ Does it end in **/ 24**?

‣ If it **ends in /24**, replace the last part of the IP address with a zero (0) to get the network address, e.g.

192.168.13.**11** / 24 → 192.168.13.**0** / 24

‣ If it does **not end in /24**, open VPN Tracker and add a new connection. On the **Basic** tab under **Network Configuration**, enter the LAN IP and subnet from your checklist ❷ into the **Remote Networks** field. After pressing return, VPN Tracker will automatically transform it into a correct network address. This is the address you'll need:
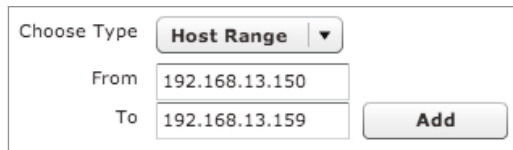
Virtual IP Address Pool

Each connecting VPN client will be assigned an IP address from a pool of addresses. The pool 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 WatchGuard's LAN.

In our example, the IP addresses 192.168.13.150 – 192.168.13.159 will be made available to VPN users.
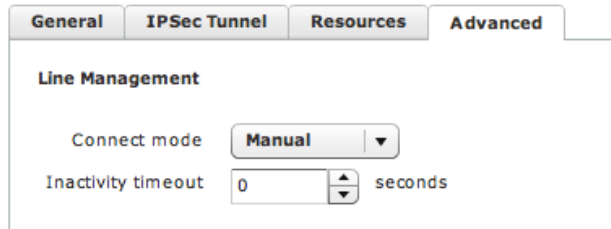
‣ **Choose Type**: Select **Host Range**.

‣ **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: 192.168.13.159).

‣ Click **Add**.

Advanced Settings

You do not have to make any changes to the Advanced settings.
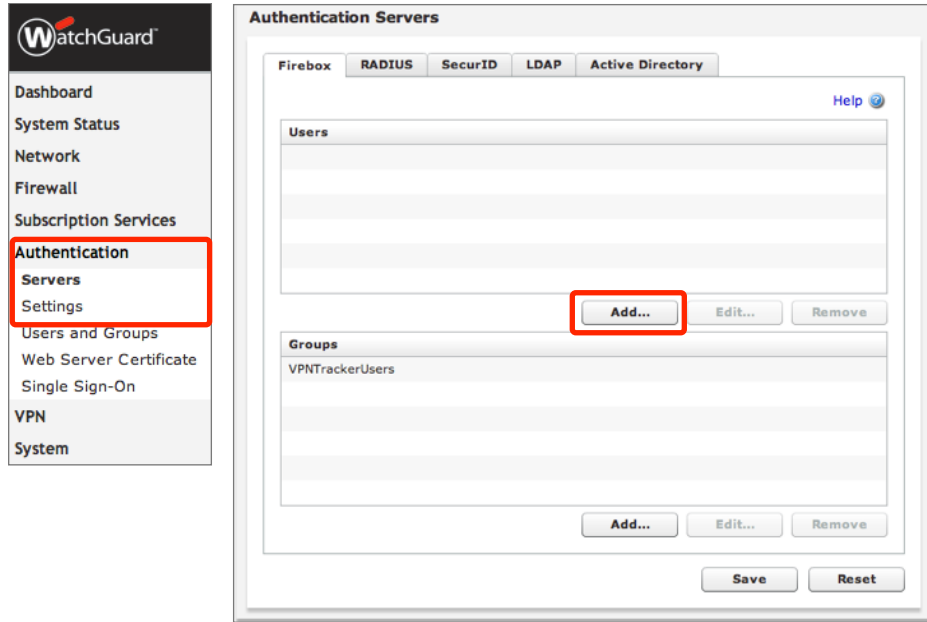
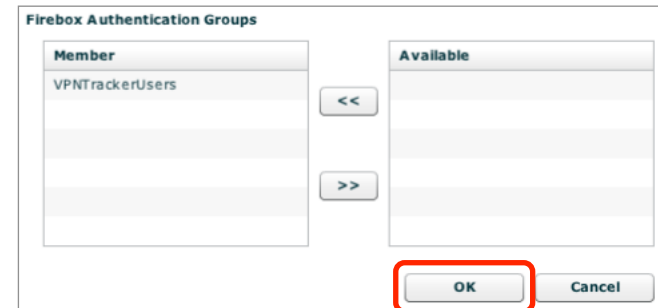⚠️ Don't forget to click **Save** to save your new MUVPN policy.
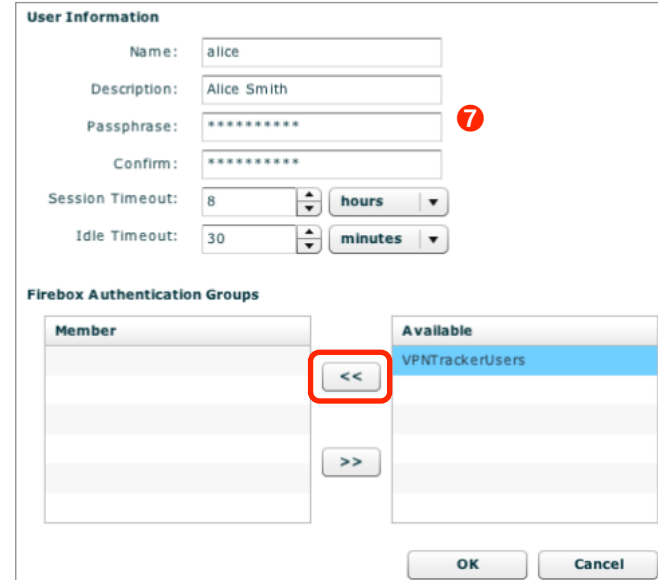
Step 3 – Add a User

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 ❻

‣ **Description**: Enter an optional description

‣ **Passphrase**: Enter the user's password and write it down as ❼. 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 the settings of your WatchGuard VPN appliance. We will now create a matching configuration in VPN Tracker.

Step 1 – Add a Connection

‣Open VPN Tracker.

‣Click **Add Connection** (or click the + button in the lower left corner).

‣Select **WatchGuard** from the list.

‣Select your device (and firmware, if multiple versions are listed).

‣Click **Create**.

For some devices, multiple firmware versions are listed. Please select "Fireware XTM" if multiple versions are listed.
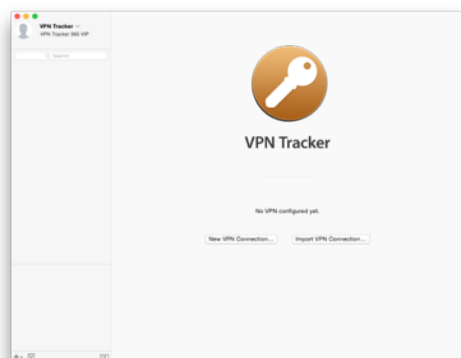
Step 2 – Configure the VPN Connection

VPN Gateway

Enter the external (WAN) IP address of your WatchGuard appliance that you wrote down as ❶. If the device has a DNS host name (e.g. vpn.example.com), use that instead.

Remote Networks

Enter the WatchGuard appliance's internal (LAN) network address ❺.

> VPN Tracker automatically corrects remote networks to be a properly formatted network address. Now would be a good time to check that it looks exactly like what you have configured for the **Allowed Resources** on the device (→ *Resources Settings*)

Local Identifier

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

Connection Name	My VPN Connection
Connection based on Need help?	DELL SonicWALL TZ 210 Configuration Guide
VPN Gateway	203.0.113.1 (?) ❶
Network Configuration	DHCP over VPN
Topology	Host to Network
Remote Networks	19.168.13.0 / 24 (?) ❺
Authentication	Pre-shared key — Stored in connection
Extended Authentication (XAUTH)	Automatic — Username and password not saved
Identifiers	
Local	Email (User FQDN) — VPNTrackerUser (?) ❸
Remote	Remote Endpoint IP Address (?)
DNS	☐ Use Remote DNS Server

Task 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 WatchGuard appliance's network. 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, try it out at home. If you are setting up a VPN connection to your home network, try it from an Internet cafe, or go visit a friend.

Connect to your VPN

‣ Make sure that your Internet connection is working – open your Internet browser and check that you can open http://www.equinux.com

‣ Open VPN Tracker.
‣ Click the On/Off slider for your connection.
‣ If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection. Wait for the test to complete.
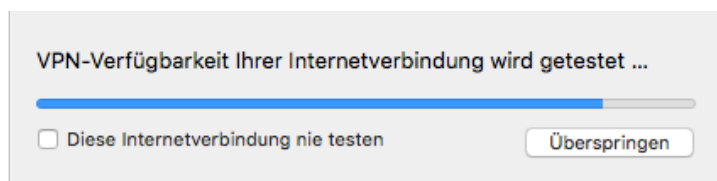

‣ Depending on your setup, you will be prompted to enter your pre-shared key ❹ and Extended Authentication (XAUTH) user name ❺ and password ❻. Optionally, check the box **"Store in Keychain"** to save the password in your keychain so you are not asked for it again when connecting the next time.
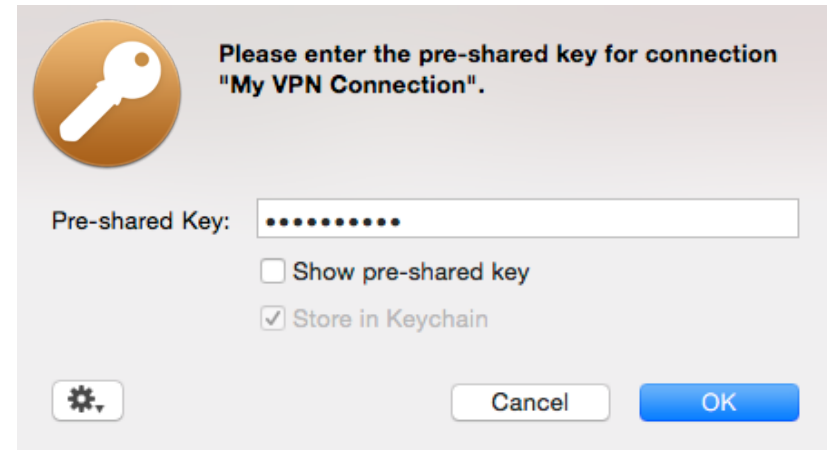
Connected!

Connecting may take a couple of seconds. If the On/Off button turns blue that's great – you're connected!
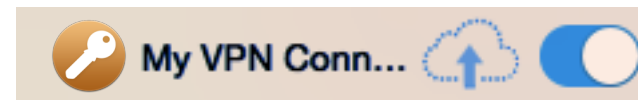
Now is a great time to take a look at the VPN Tracker Manual. It shows you how to use your newly established VPN and how to get the most out of it.

Troubleshooting

In case there's a problem connecting, a yellow warning triangle will show up:

Click the yellow warning triangle to be taken to the log. The log will explain exactly what the problem is. Follow the steps listed in the log.

Press Cmd-L to open the log in a new window. That way, you can have the log side-by-side with your VPN configuration while making changes to troubleshoot a problem.

In most cases, the advice in the log should be sufficient to resolve the issue. However, VPNs are a complex topic and there might be trickier issues with which you need additional help.

VPN Tracker Manual

The [VPN Tracker Manual](http://www.vpntracker.com) contains detailed troubleshooting advice.

Frequently Asked Questions (FAQs)

Answers to frequently asked questions can be found at

http://www.vpntracker.com/support

Technical Support

If you're stuck, the technical support team at equinux is here to help. Contact information can be found at

http://www.vpntracker.com/support

Please include the following information with any request for support:

‣ A description of the problem and any troubleshooting steps that you have already taken.
‣ A VPN Tracker Technical Support Report (Log > Technical Support Report).
‣ WatchGuard model and the Fireware XTM version running on it.
‣ Screenshots of the Mobile User VPN settings on your WatchGuard device.

A Technical Support Report contains the settings and logs necessary for resolving technical problems. Confidential information (e.g. passwords, private keys for certificates) is **not** included in a Technical Support Report.

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. A few changes are necessary to tunnel all Internet traffic through the VPN.

Change the Allowed Resources on the VPN Gateway

‣ On your **WatchGuard VPN appliance**, edit the Mobile User VPN group you created in → *Task 1.*

‣ Go to the **Resources** tab.

‣ Check the box **Allow All Traffic Through Tunnel**.

‣ Click **Save**.
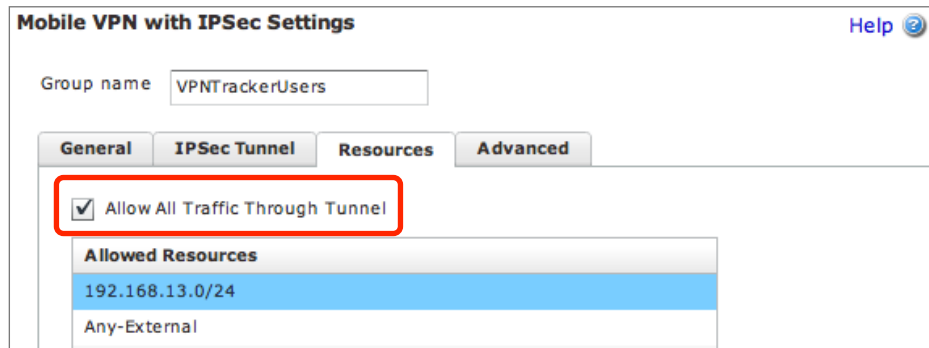
Change the Topology to Host to Everywhere in VPN Tracker

‣ Click **Configure** and switch to the **Basic** tab if it is not already displayed.

‣ Change the **Topology** setting to **Host to Everywhere**.
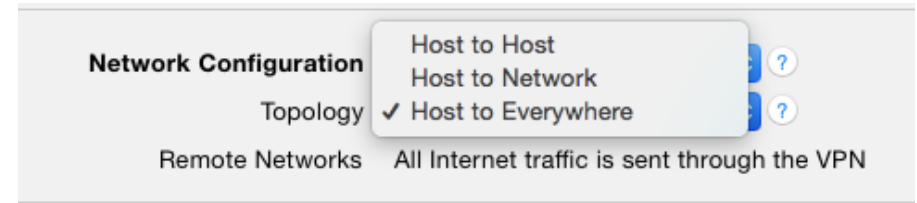
Configure DNS

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 whenever you connect the VPN.

If you already have a **working Remote DNS setup** in VPN Tracker, you will normally not have to change it.
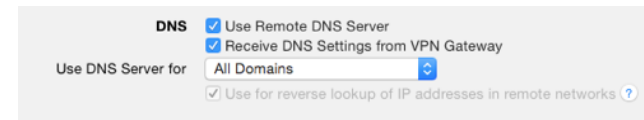
If you don't have a working remote DNS setup yet, you might be able to obtain one from your VPN gateway through Mode Config. Check the boxes **Use Remote DNS Server** and **Receive DNS Setting from VPN Gateway**, and set this DNS server to be used for **All Domains**:

What if the DNS server I receive from my VPN gateway does not work?

You can set up remote DNS using public DNS servers, e.g.

‣ Google DNS: 8.8.8.8
‣ OpenDNS: See the OpenDNS website for IP addresses.

When using a public remote DNS server with a Host to Everywhere VPN, VPN Tracker will send DNS requests through the (encrypted) VPN, and the VPN gateway will send them back out (unencrypted) on the Internet to the public DNS server.

The following setup uses Google's public DNS server to ensure that your Mac can reach a DNS server when you're connected to your Everywhere VPN:

	DNS	☑ Use Remote DNS Server
		☐ Receive DNS Settings from VPN Gateway
⊕	DNS Servers	8.8.8.8
⊕	Search Domains	Domain
	Use DNS Server for	All Domains ⬍
		☑ Use for reverse lookup of IP addresses in remote networks