equinux

VPN Tracker 365

VPN Configuration Guide

WatchGuard Firewall Appliances

Firebox T Series, Firebox M Series, Firebox XTM Series

Revised November 2020

www.equinux.com

Contents

Introduction

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 WatchGuard Firebox VPN gateway device.

IP Addresses

(1) WAN IP Address: ______._______._______._______ (or hostname ______________________________________)

(2) LAN (internal) IP Address / Subnet Mask: ______._______._______._______ / ______._______._______.

Group Authentication

(3) Group name: ___________________________

(4) Passphrase (Pre-Shared Key): ___________________________

Allowed Resources

(5) LAN Network Address / Subnet: ___________________________

User Authentication (XAUTH)

(6) Username: ___________________________

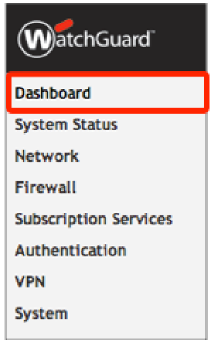
(7) Password: ___________________________

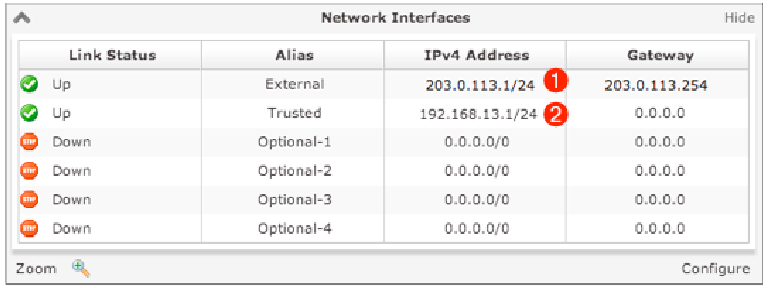
Task 1 – VPN Gateway Configuration

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

Step 1 – Retrieve Network Settings

- ➔ Log into your WatchGuard appliance’s web interface. 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, go to the Dashboard. Here you will find an overview of the IP addresses used by the device:



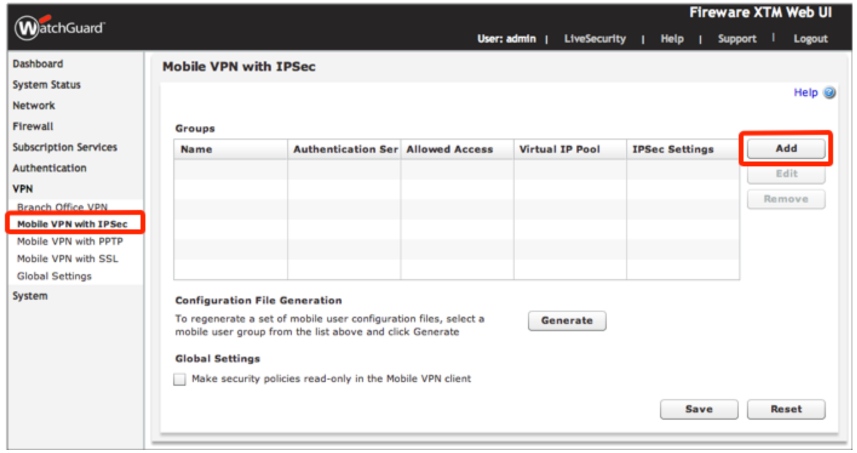


Link Status	Alias	IPv4 Address	Gateway
Up	External	203.0.113.1/24 ❶	203.0.113.254
Up	Trusted	192.168.13.1/24 ❷	0.0.0.0
Down	Optional-1	0.0.0.0/0	0.0.0.0
Down	Optional-2	0.0.0.0/0	0.0.0.0
Down	Optional-3	0.0.0.0/0	0.0.0.0
Down	Optional-4	0.0.0.0/0	0.0.0.0

- ➔ Locate the **External** entry. This is the device’s WAN IP address. Write it down as **(1)** on your Checklist. 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 **(2)**. 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.**



To regenerate a set of mobile user configuration files, select a mobile user group from the list above and click Generate

☐ Make security policies read-only in the Mobile VPN client

General Settings

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), otherwise simply choose a generic name. Write down the group name as **(3)**.

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)**.

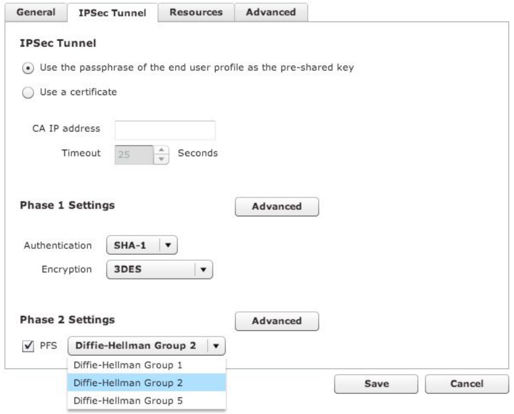
Firebox IP Addresses

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

Tip: If you make any other changes, you will have to match these settings on VPN Tracker's Advanced tab. We recommend deferring such changes until you've got the basic setup working.

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.



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

Authentication SHA-1

Encryption 3DES

Phase 2 Settings

☑ PFS Diffie-Hellman Group 2

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 365) 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**.

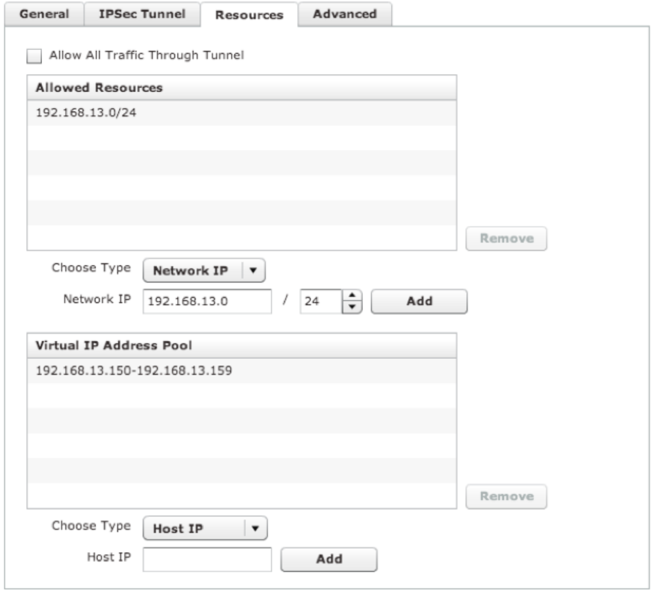
Phase 1 Advanced Settings: Diffie-Hellman Group

- ➔ 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

Allowed Resources
192.168.13.0/24

Choose Type: Network IP
Network IP: 192.168.13.0 / 24

Virtual IP Address Pool
192.168.13.150-192.168.13.159

Choose Type: Host IP
Host IP:

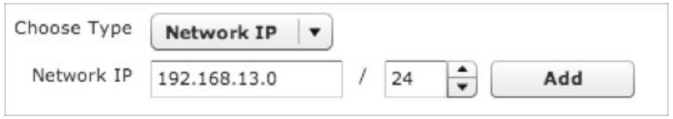
Allow All Traffic Through Tunnel

This setting should remain unchecked for now. If checked, a Host to Everywhere connection will be created.

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 **(5)**
- ➔ Click **Add**.



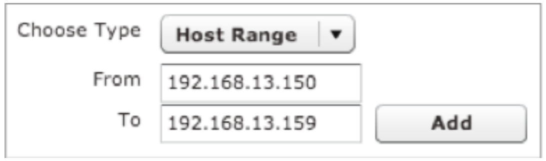
Choose Type: Network IP
Network IP: 192.168.13.0 / 24

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**.



Choose Type: Host Range

From: 192.168.13.150

To: 192.168.13.159

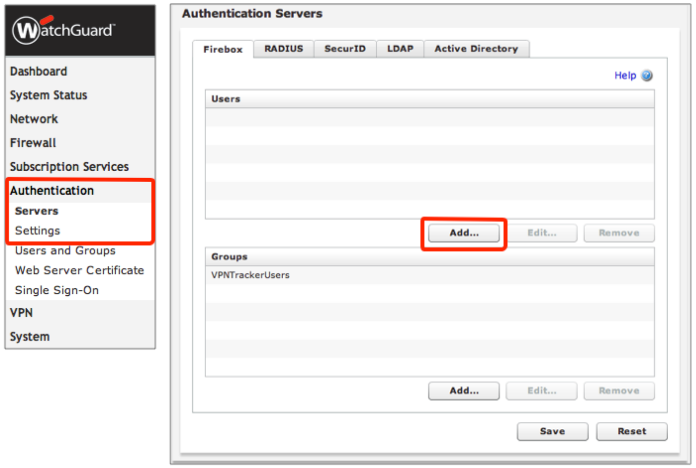
Advanced Settings

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

Tip: Don't forget to click **Save** to save your new Mobile User VPN policy.

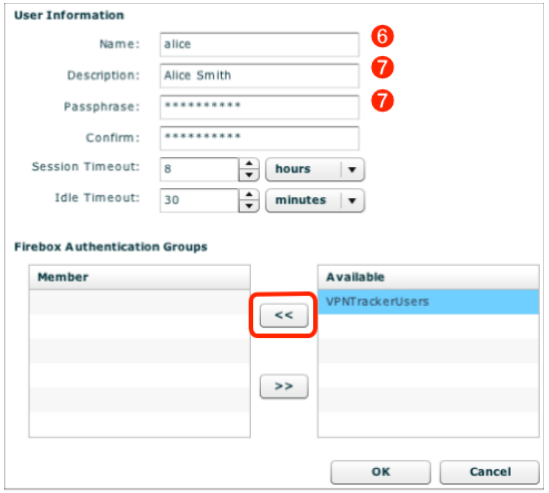
Step 3 – Add a User

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



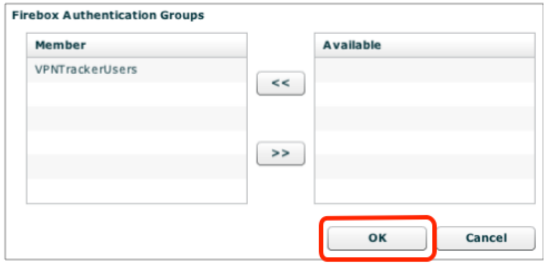
Click **Add** to begin adding a new user to the group.

- ➔ **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



User Information

Name: alice ⑥
Description: Alice Smith ⑦
Passphrase: ********** ⑦
Confirm: **********
Session Timeout: 8 hours
Idle Timeout: 30 minutes

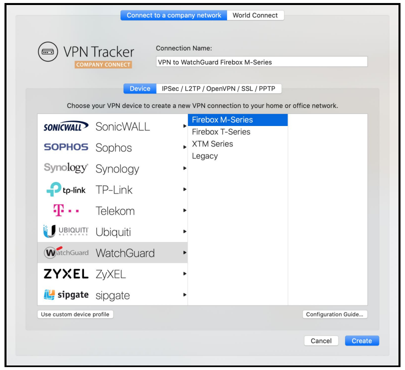


Task 2 – VPN Tracker Configuration

After finishing task 1, you should now have a completed a configuration checklist containing your WatchGuard Firebox firewall’s settings. We will now create a matching configuration in VPN Tracker 365.

Step One: Add a connection

- ➔ Open VPN Tracker 365.
- ➔ Click on the + in the bottom left corner of the app window and select “**Create new Company Connection**”
- ➔ Select **WatchGuard** from the list.
- ➔ Select your model (e.g. Firebox M-Series) and enter a name for your connection.



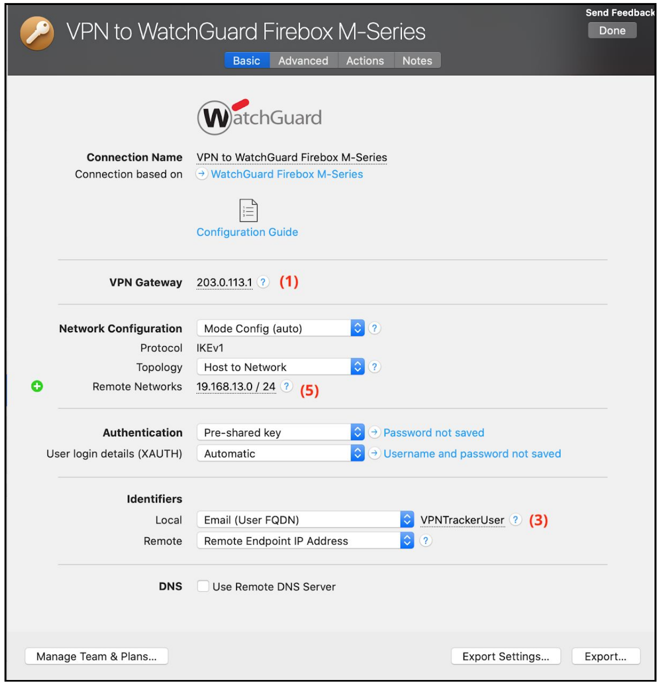
Connection Name: VPN to WatchGuard Firebox M-Series

Choose your VPN device to create a new VPN connection to your home or office network.

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)**. 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 **(5)**.
- ➔ **Local Identifier:** Enter the group name you configured on your Firebox **(3)**. Make sure the capitalization is the same as on your device.



VPN to WatchGuard Firebox M-Series

Connection Name VPN to WatchGuard Firebox M-Series
Connection based on WatchGuard Firebox M-Series

VPN Gateway 203.0.113.1 (1)

Network Configuration Mode Config (auto)
Protocol IKEv1
Topology Host to Network
Remote Networks 19.168.13.0 / 24 (5)

Authentication Pre-shared key → Password not saved
User login details (XAUTH) Automatic → Username and password not saved

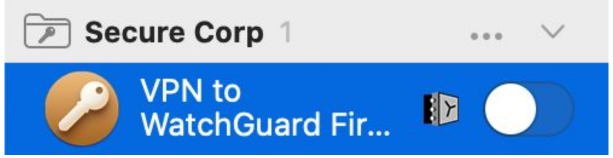
Identifiers
Local Email (User FQDN) VPNTrackerUser (3)
Remote Remote Endpoint IP Address

DNS ☐ Use Remote DNS Server

Task Three - Testing the VPN connection

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, or from an Internet cafe, or go visit a friend.

Connect to your VPN



- ➔ Check first of all that your internet connection is working as it should be. Use this link as a test: http://www.equinux.com
- ➔ Start the VPN Tracker 365 app.
- ➔ Click on the On/Off slider to turn on your connection.

IMPORTANT:

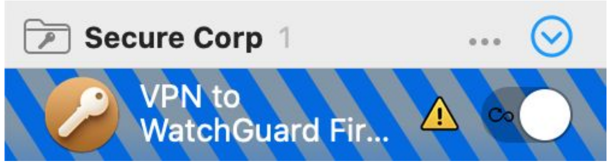
If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection. Wait for the test to complete.

- ➔ Depending on your setup, You will be prompted to enter your pre-shared key **(4)** and your XAUTH username **(6)** and password **(7)**. To save time for the future, 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 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.
TIP: 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.

VPN Tracker Manual

The VPN Tracker Manual contains detailed troubleshooting advice. Answers to frequently asked questions (FAQs) 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 us via 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).
- ➔ Device model and the firmware version running on it.
- ➔ Screenshots of the VPN settings on your VPN gateway.

IMPORTANT: 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.