equinux

VPN Configuration Guide

WatchGuard Firebox X – Peak and Core Series

Introduction

This document describes how VPN Tracker can be used to establish a connection between a Mac running Mac OS X and a WatchGuard Firebox VPN router.

Note This documentation is only a supplement to, not a replacement for, the instructions that have been included with your WatchGuard device. Please be sure to read those instructions and understand them before starting.

WatchGuard Configuration

The first part of this document will show you how to configure a VPN tunnel on a WatchGuard Firebox that has not yet been configured for VPN. The configuration described is just one example for such a setup. It is not the only known working configuration, and also may not be suitable for all situations. However, it is a configuration which quickly provides you with a ready-to-use VPN tunnel, and it is still flexible enough to be easily extended if your VPN requirements grow in the future.

Advanced Users While the instructions in this document describe how to set up VPN on your WatchGuard from scratch, they also apply if you are configuring VPN Tracker for your existing WatchGuard VPN setup. In this case, we recommend you follow the instructions to understand how the WatchGuard settings relate to the VPN Tracker settings, adapting the settings in VPN Tracker to your setup, if necessary.

VPN Tracker Configuration

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

Important Prerequisites

Your WatchGuard Device

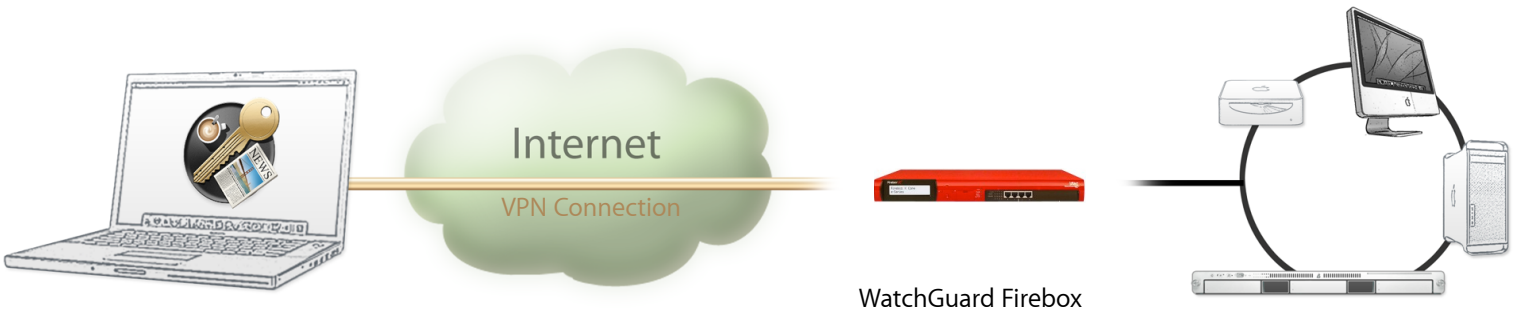
This document applies to WatchGuard Firebox Core and Peak series devices. All tests have been performed using Fireware 9.1.

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 to use a recent VPN Tracker version, if possible. The latest VPN Tracker release can always be obtained from http://www.vpntracker.com
- You will need one VPN Tracker license for each Mac running VPN Tracker

Scenario

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



This guide assumes that the Mac running VPN Tracker already has internet connectivity. The office's WatchGuard Firebox (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 Firebox has a second network interface which is connected to the internal office network (LAN). In our example, the office network has the IP range 192.168.1.0/24 (which is the same as 192.168.1.0/255.255.255.0). 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.

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.

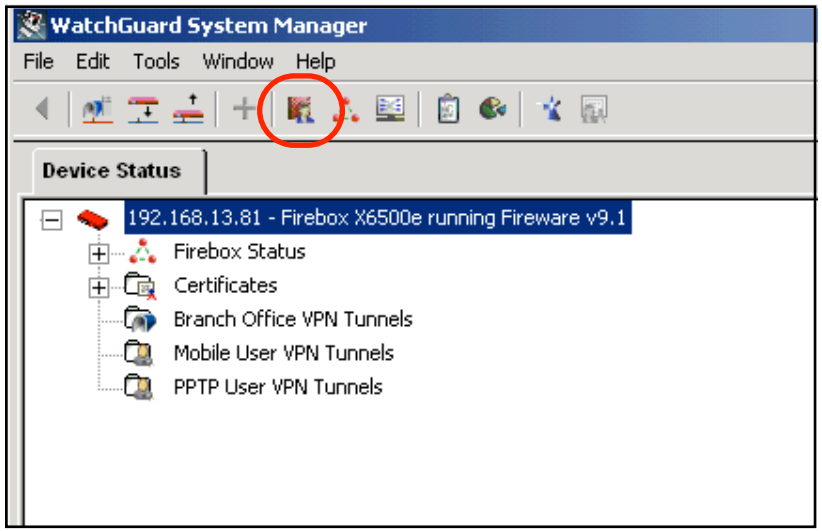
A list of terms used by WatchGuard, and their corresponding terms in VPN Tracker can be found in Appendix: Terminology Matrix.

Task 1 – Configure your VPN Device

This section describes the configuration of your WatchGuard VPN router.

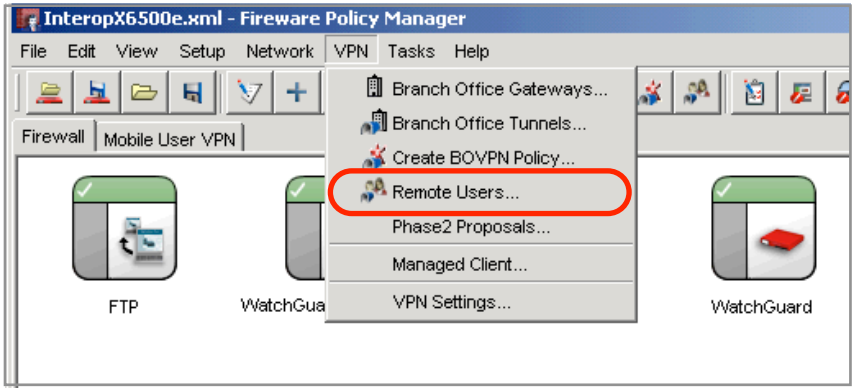
TIP To set up your VPN connection, you'll need to keep track of certain pieces of information. Those details are indicated by red numbers. Throughout this guide we will be referencing those numbers.

Step 1 – Access the WatchGuard System Manager

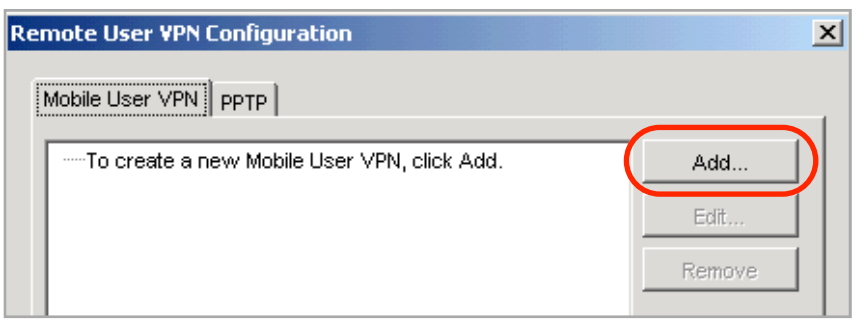


- Start WatchGuard System Manager
- Select your WatchGuard device from the list
- Start the Fireware Policy Manager by clicking its icon

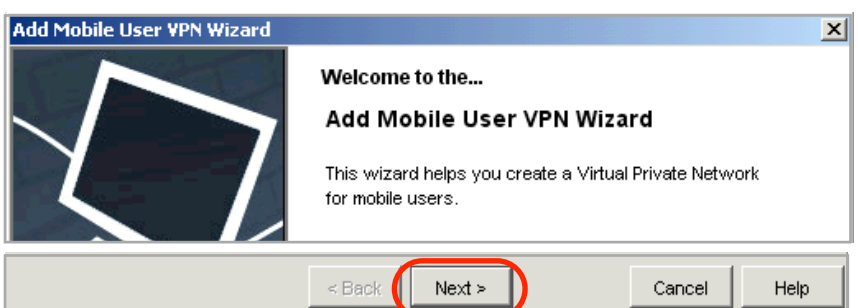
Step 2 - Add a New Mobile User VPN Group



- In the Fireware Policy Manager's menu, click "VPN" > "Remote Users..."

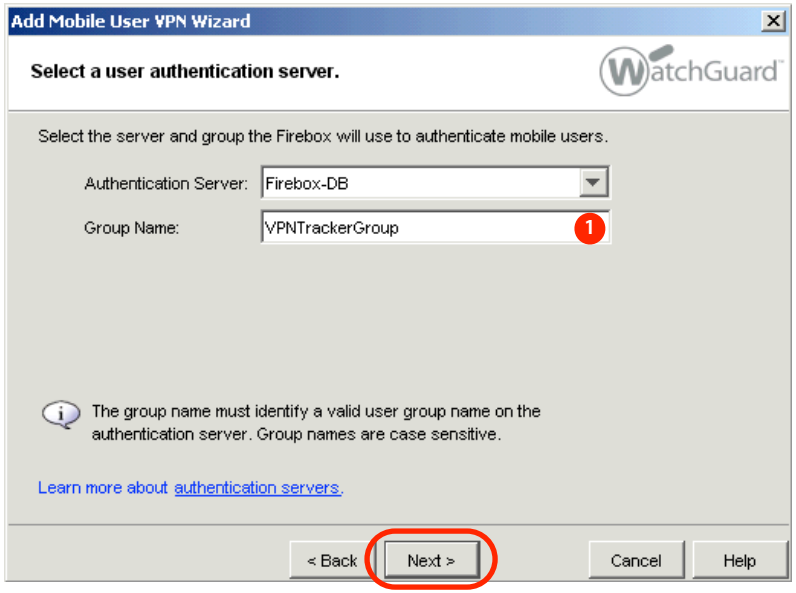


- Click "Add..."



- Click "Next"

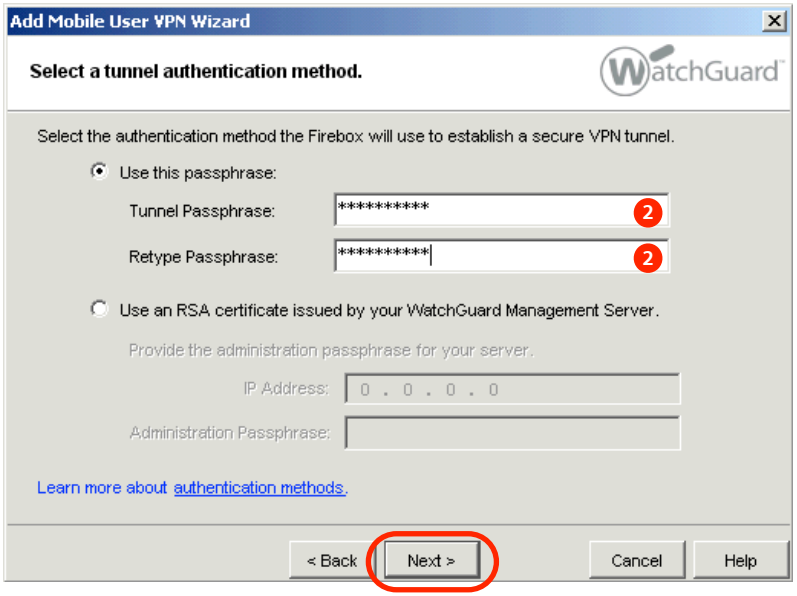
Step 3 - Set the Mobile User VPN Group Name



- **Authentication Server**: Select "Firebox-DB"
- **Group Name**: Enter a group name, e.g. "VPNTrackerGroup"
- Click "Next"

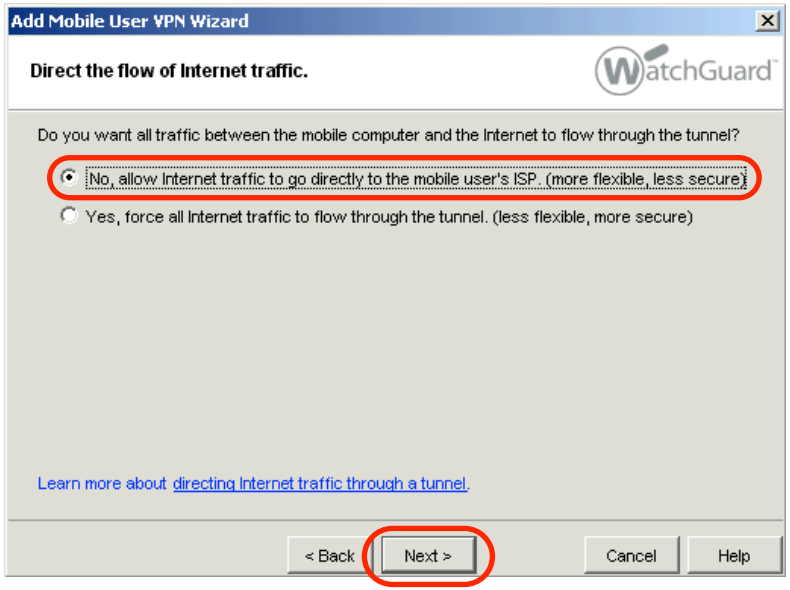
Note The group name is case-sensitive. Make sure to write down the group name, including capitalization.

Step 4 - Set the Tunnel Passphrase



- Select "Use this passphrase"
- **Tunnel Passphrase**: Enter a password for the VPN connection. The password you set here, will be entered as the pre-shared key in VPN Tracker later
- **Retype Passphrase**: Repeat the password you have entered in the previous field
- Click "Next"

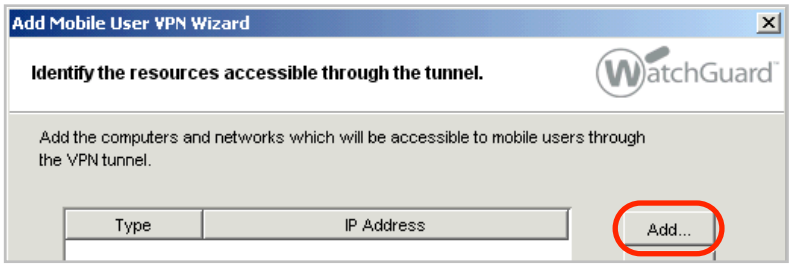
Step 5 – Select where Internet Traffic is Directed



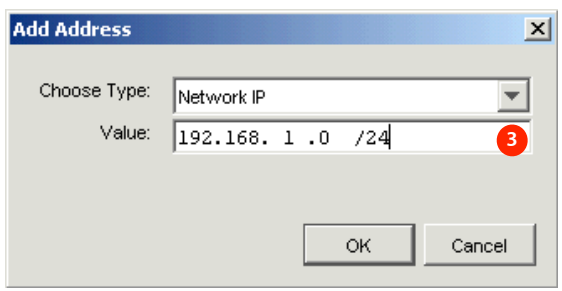
- Select "No, allow Internet traffic to go directly to the mobile user's ISP"
- Click "Next"

Tip If you rather have **all Internet traffic directed through the VPN**, please see the chapter on "Setting up a Host to Everywhere Connection".

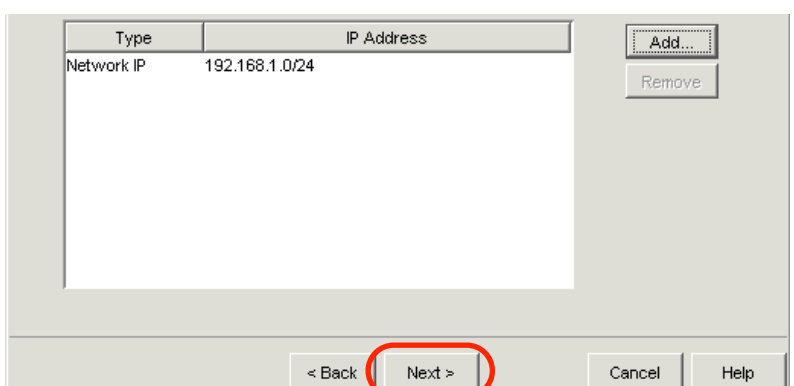
Step 6 – Set the Resources that can be accessed through the VPN Tunnel



- Click "Add" to add the network that can be accessed through the VPN tunnel



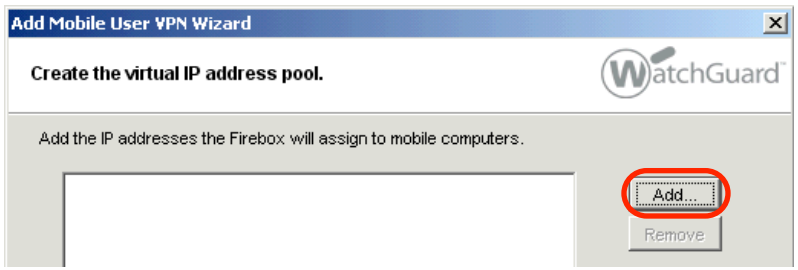
- **Choose Type**: Select "Network IP"
- **Value**: Enter the network that is to be accessed through the VPN, e.g. 192.168.1.0/24. This will in most cases be identical to the LAN network of the WatchGuard
- Click "OK"



- Click "Next"

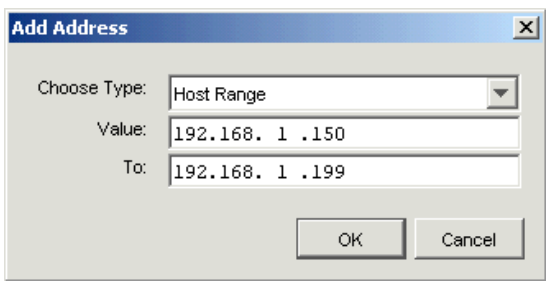
Step 7 – Set the Virtual IP Address Pool

In this step, you will be configuring the virtual IP addresses that are assigned to the VPN clients.

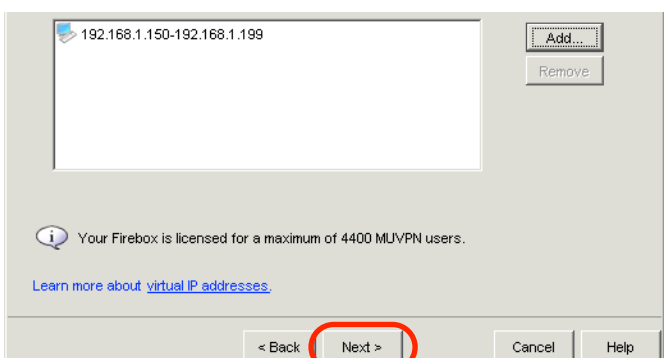


1

- Click "Add..."

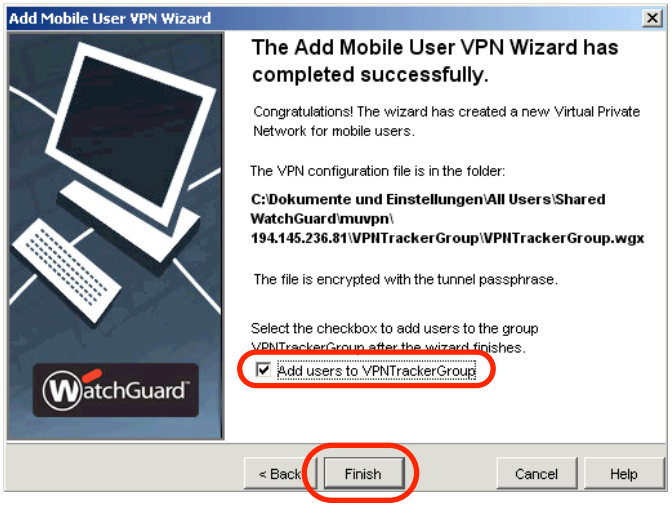


- **Choose Type**: Select "Host Range"
- Choose a range of unused IP addresses from the remote network. Make sure the range comprises at least as many IP addresses as you expect users to use this VPN connection
- **Value**: Enter the first IP address of the range
- **To**: Enter the last IP address of the range

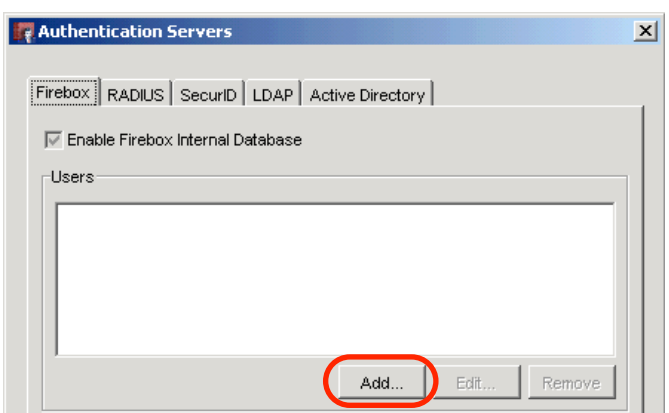


- Click "Next"

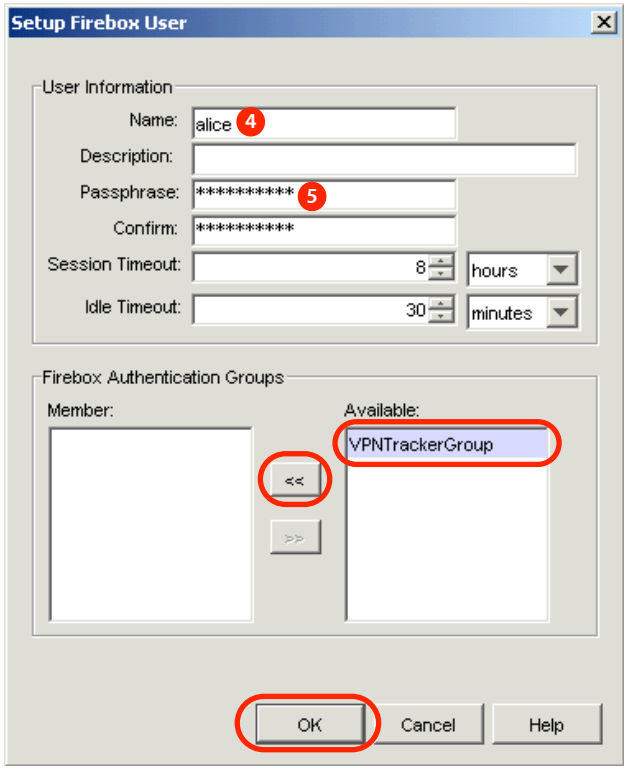
Step 8a – Add a User to the Mobile User VPN Group



- Check the box "Add users to VPNTrackerGroup"
- Click "Finish"



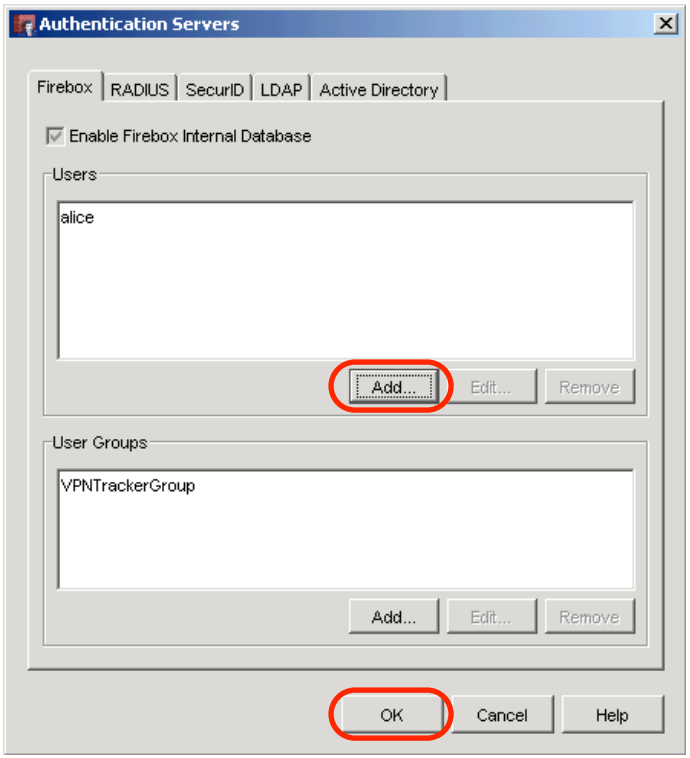
- Click "Add..."



- **Name**: Enter a user name ❹
- **Passphrase**: Enter a password for the user ❺
- **Confirm**: Repeat the password ❺
- **Firebox Authentication Groups**: Add the user to the newly added group (here: "VPNTrackerGroup") by selecting the group from the "Available" list and moving it to the "Member" list by clicking "<<"
- Click "OK"

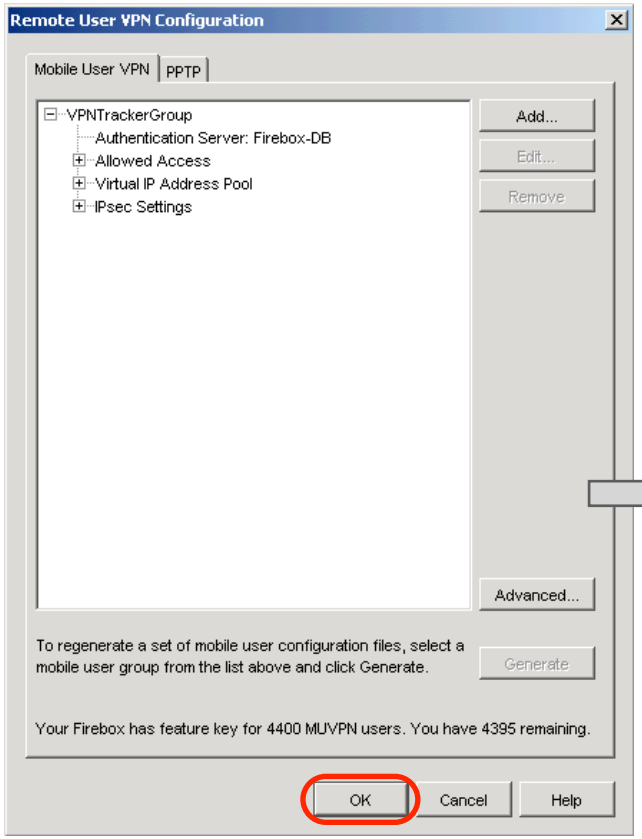
Tip To prevent the VPN connection from being **disconnected after 8 hours**, adjust the **Session Timeout**: A value of 0 means that the Firebox never forces a disconnect. .

Step 8b (optional) – Add Additional Users

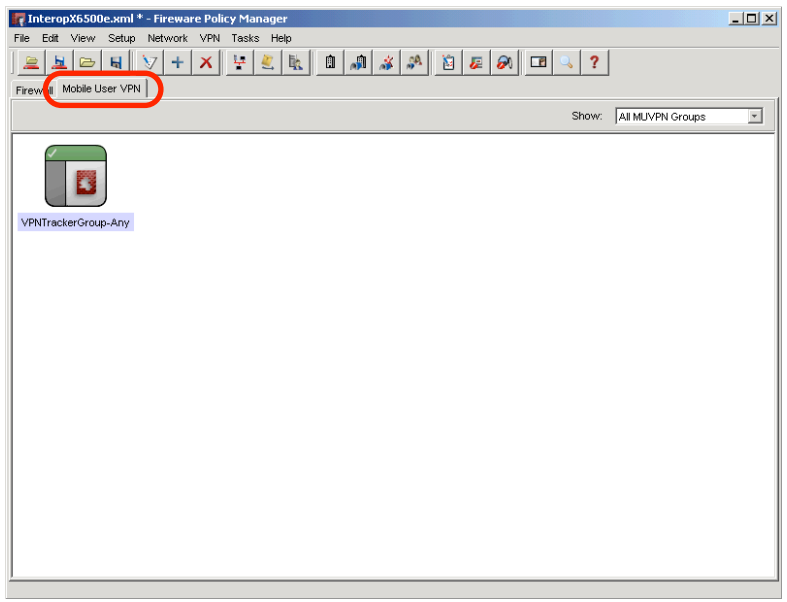


- If desired, add additional users for this VPN connection by clicking "Add..."
- Click "OK" when you are done adding users

Step 9 – Finish Adding the Mobile User VPN Group and Policy



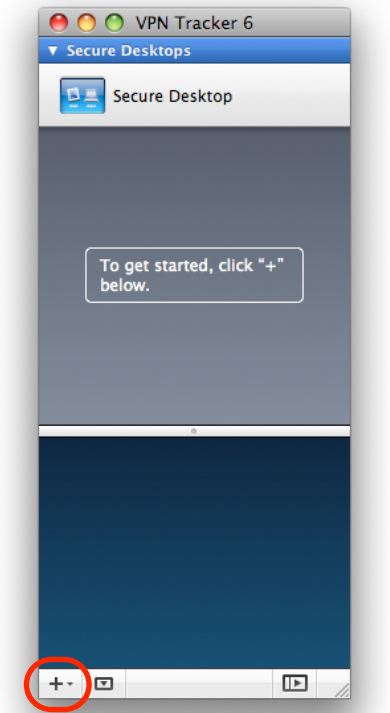
- Click "OK" to finish adding the Mobile User VPN group
- Switch to the "Mobile User VPN" tab in the Fireware Policy Manager to see the Mobile User VPN Policy that has automatically been added for your new Mobile User VPN group
- **Do not forget to save the new settings to your Firebox!**



Task 2 – Configure VPN Tracker

This section describes how to configure VPN Tracker.

Step 1 - Create a New Connection

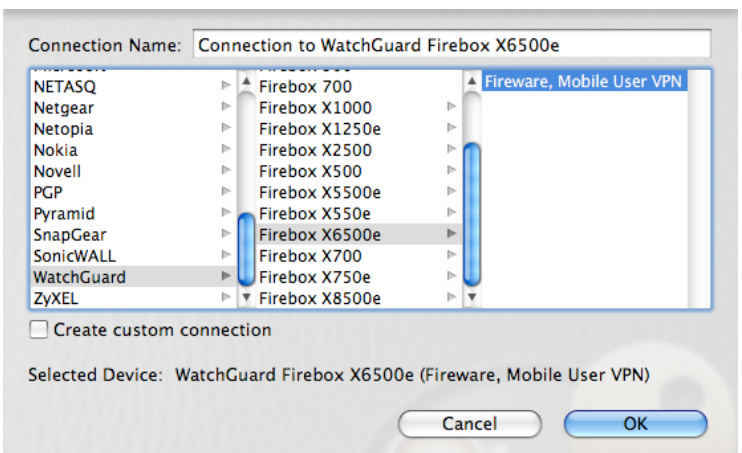


- Start VPN Tracker 6
- Click the "+" button in the main window

Step 2 – Select a VPN Device

For many VPN gateways, VPN Tracker 6 provides pre-defined profiles, based on the device's default settings.

Note If you have changed any of the factory settings while configuring the device (other than as described in this document), you might have to adjust the "Advanced" settings in VPN Tracker. This is explained in detail in the VPN Tracker 6 manual. Please see the appendix of this document for a mapping of WatchGuard terms to VPN Tracker terms.

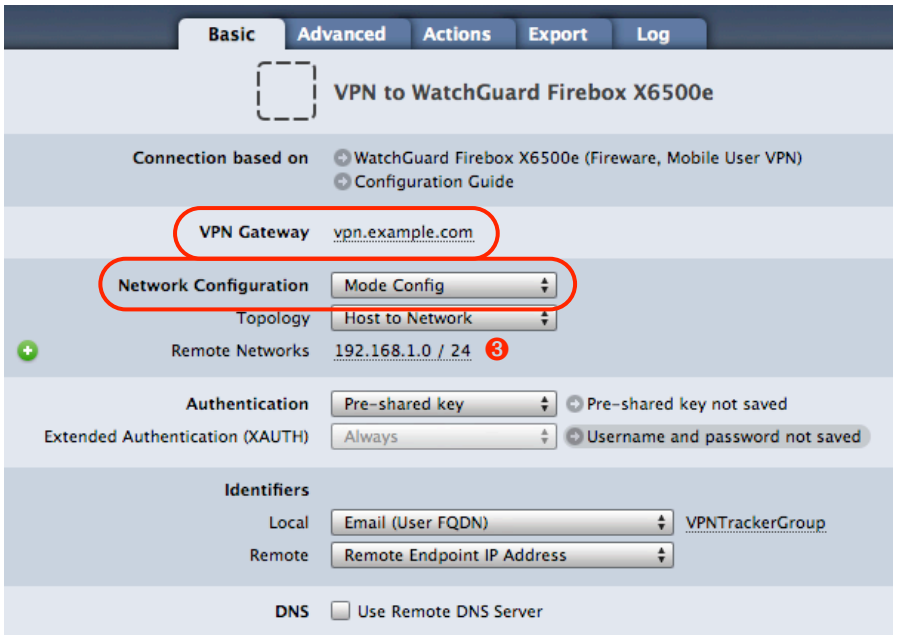


- Select "WatchGuard" from the list
- Select your device from the list of WatchGuard devices
- Select the "Fireware, Mobile User VPN" profile
- **Connection Name**: Choose a name for your connection (e.g. "New York Office")
- Click "OK"

Step 3 – Configure IP Addresses

There are two important addresses involved in a VPN tunnel:

- The VPN gateway's public address (aka WAN IP)
- Your office (intranet) network's IP address at the gateway's end of your VPN tunnel (i.e. the network you want to access through the VPN gateway)



- Make sure the **Mode Config** box is chosen under Network Configuration
- **VPN Gateway:** Enter your Firebox's public IP address (WAN IP) or its host name
- **Remote Networks**: Enter the Firebox's LAN network address and network mask ❸, separated by a slash

Step 4 – Configure Authentication

Each VPN tunnel requires mutual authentication of both the client and the gateway. This authentication can be provided by a pre-shared key.

- Click the "Edit" arrow next to **Pre-shared key**
- Enter the pre-shared key ❷
- Make sure **"Store in Keychain"** is checked
- Click "OK"

Step 5 – Configure Identification

In addition to the authentication, client and gateway need to identify themselves. Each identifier has a type and a value.

- **Local Identifier:** Enter the Mobile User VPN group name from the Firebox ❶

You're done! The next task is to test the connection you just configured.

> **Note** If you are running VPN Tracker **Personal Edition**, please see the section "Configuring VPN Tracker Personal Edition" for additional information.

p

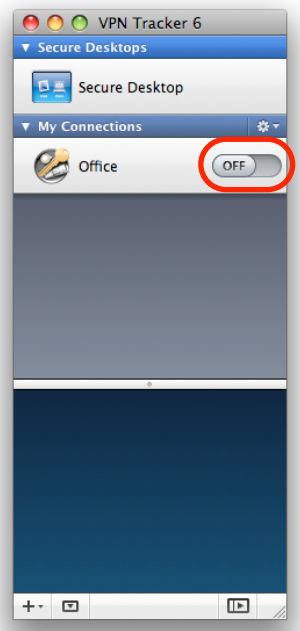
Task 3 – Test the VPN Connection

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

It's time to go out!

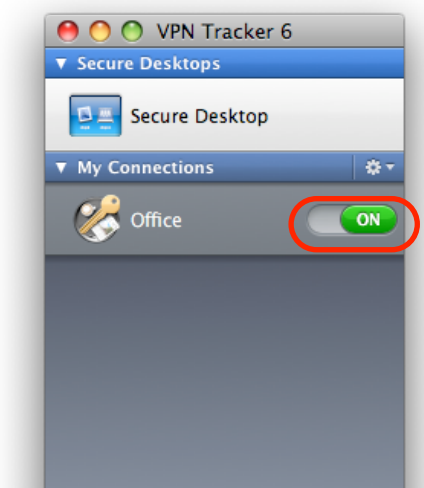
You will not be able to test and use your VPN connection from within the intranet that you want to connect to. In order to test your connection, you'll need to connect from a different location. For example, if you are setting up a VPN connection to your office, try it from home. If you are setting up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

Test your connection



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

- After a short while, you will be asked for your XAUTH credentials
- **User Name**: Enter the name of the user that you added to the "VPNTrackerGroup" Mobile User VPN Group earlier ❹
- **Password**: Enter the password that you set for this user ❺
- **Store in Keychain** (optional): Check this box to store the user name and password for this user in the Mac OS X keychain
- Click "OK"



- If the slider goes back to **Off** after starting the connection, or after entering 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

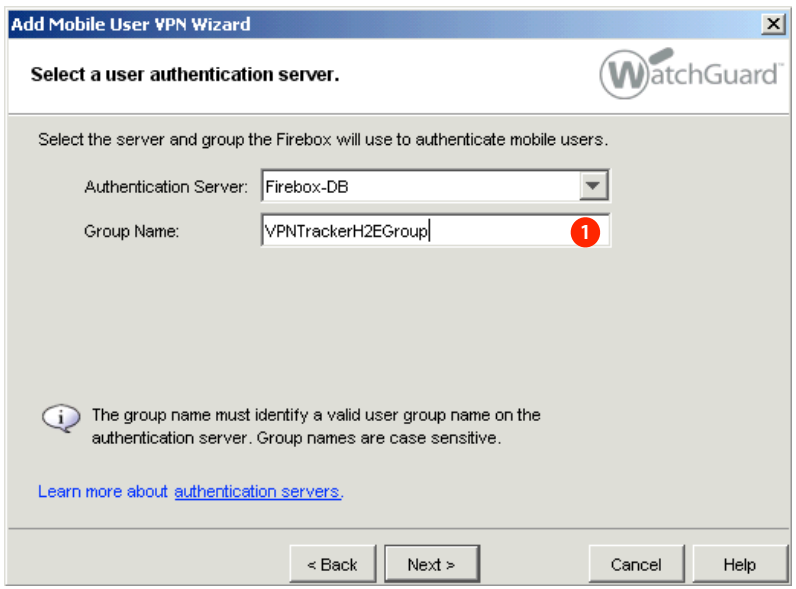
Congratulations!

Setting up a Host to Everywhere Connection

This section explains how to set up the VPN so all Internet traffic is directed through the VPN. This can be useful when connected to insecure public networks (e.g. public WiFi networks).

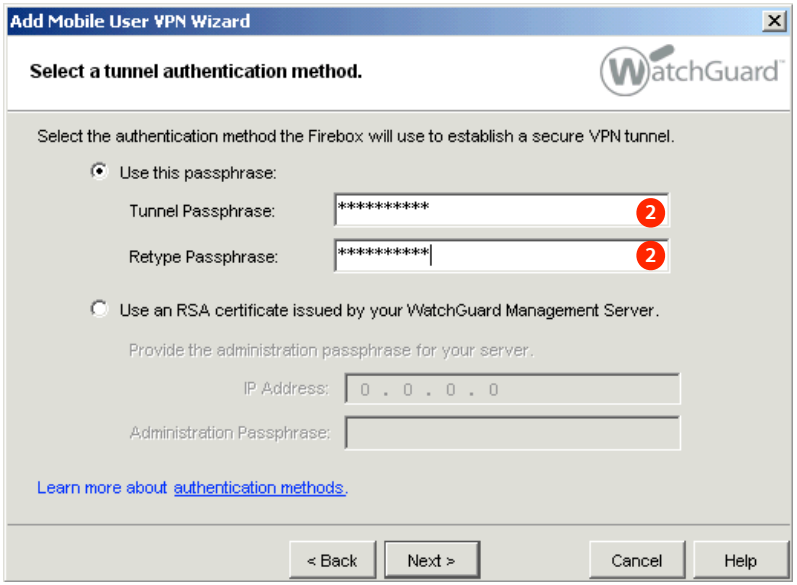
Steps 1 - 2: Follow Steps 1- 2 of "Task 1 – Configure Your VPN Device"

Step 3 - Set the Mobile User VPN Group Name



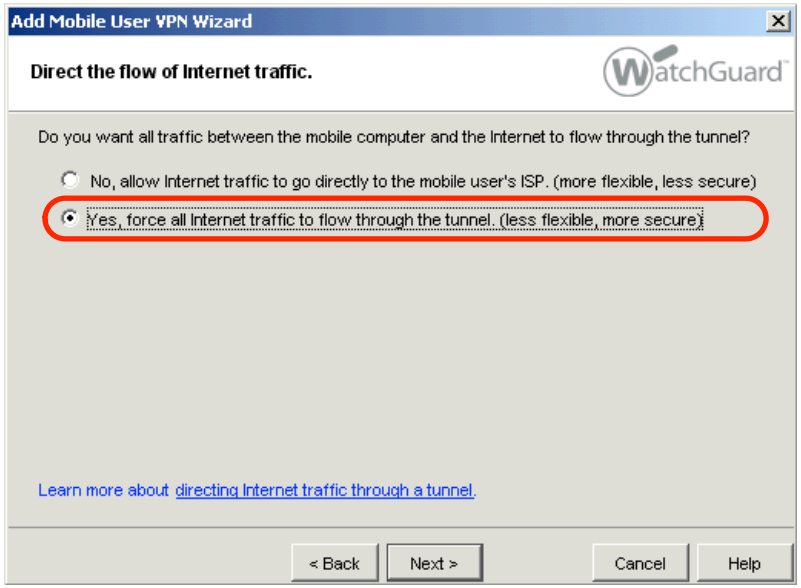
- **Authentication Server**: Select "Firebox-DB"
- **Group Name**: Enter a group name, e.g. "VPNTrackerH2EGroup" ❶
- Click "Next"

Step 4 - Set the Tunnel Passphrase



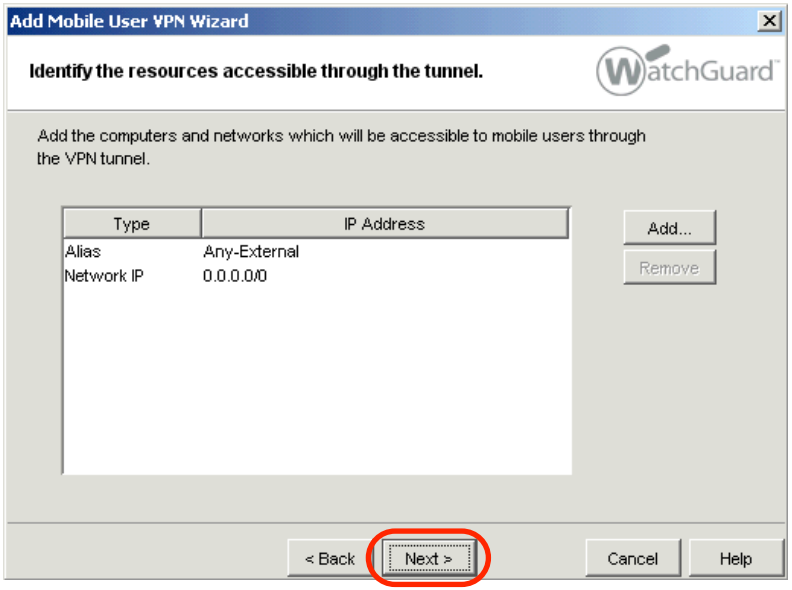
- Select "Use this passphrase"
- **Tunnel Passphrase**: Enter a password for the VPN connection. The password you set here, will be entered as the pre-shared key in VPN Tracker later ❷
- **Retype Passphrase**: Repeat the password you have entered in the previous field ❷
- Click "Next"

Step 5 – Select where Internet Traffic is Directed



- Select "Yes, force all Internet traffic to flow through the tunnel"
- Click "Next"

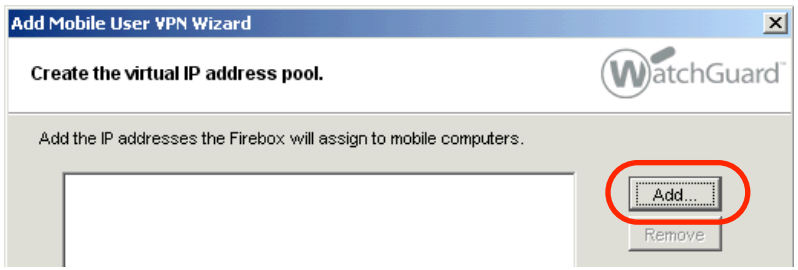
Step 6 – Set the Resources that can be accessed through the VPN Tunnel



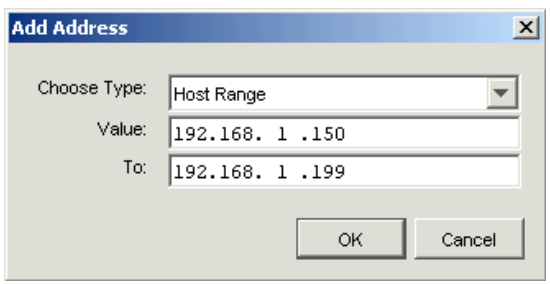
- The correct resources for a Host-to-Everywhere connection are automatically added to the tunnel definition.
- Click "Next"

Step 7 – Set the Virtual IP Address Pool

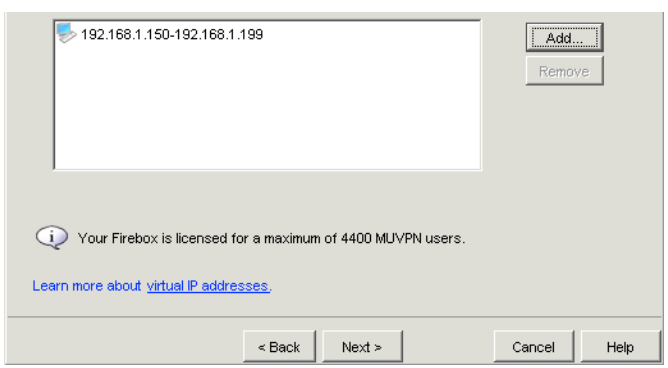
In this step, you will be configuring the virtual IP addresses that are assigned to the VPN clients.



- Click "Add..."

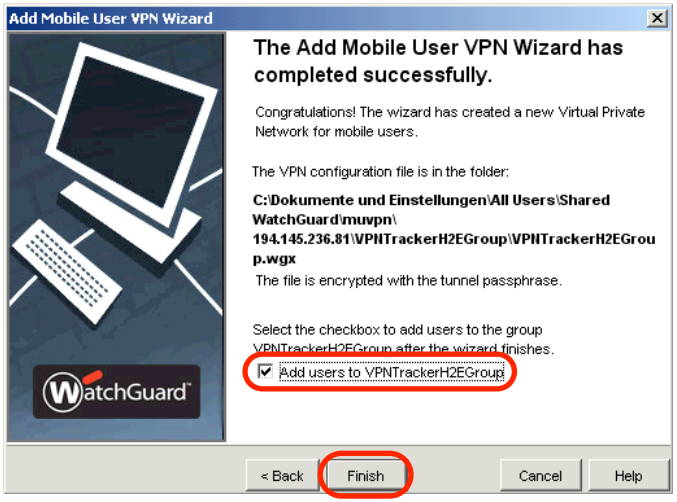


- **Choose Type**: Select "Host Range"
- Choose a range of unused IP addresses from the remote network ❸. Make sure the range comprises at least as many IP addresses as you expect users to use this VPN connection
- **Value**: Enter the first IP address of the range
- **To**: Enter the last IP address of the range

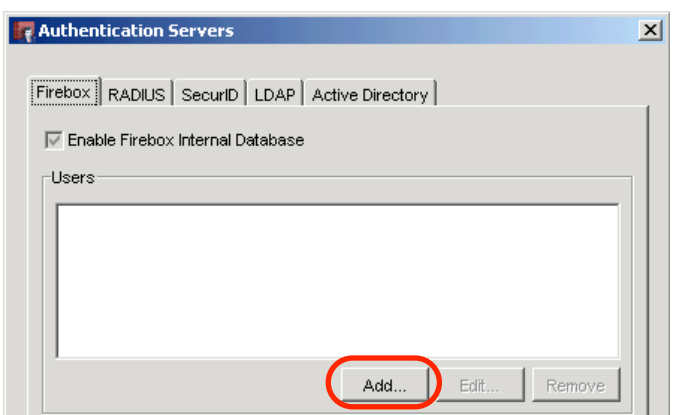


- Click "Next"

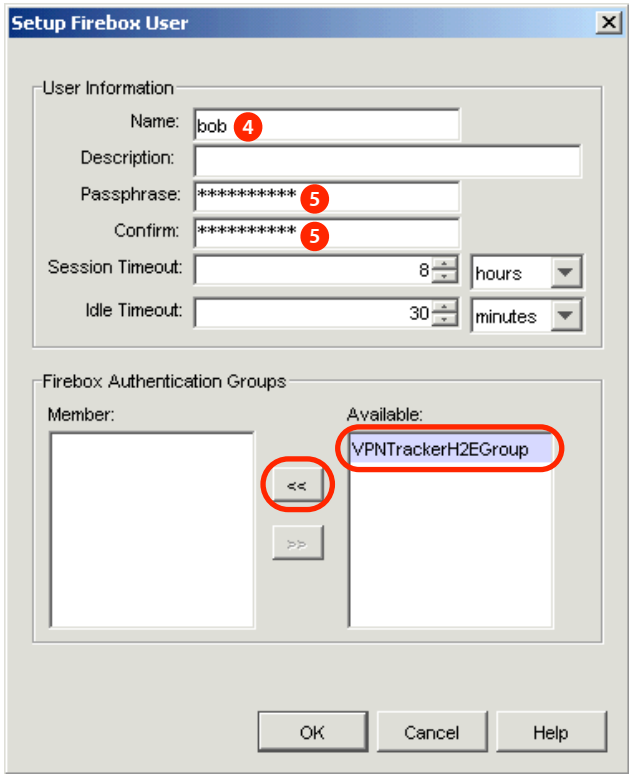
Step 8a – Add a User to the Mobile User VPN Group



- Check the box "Add users to VPNTrackerH2EGroup"
- Click "Finish"

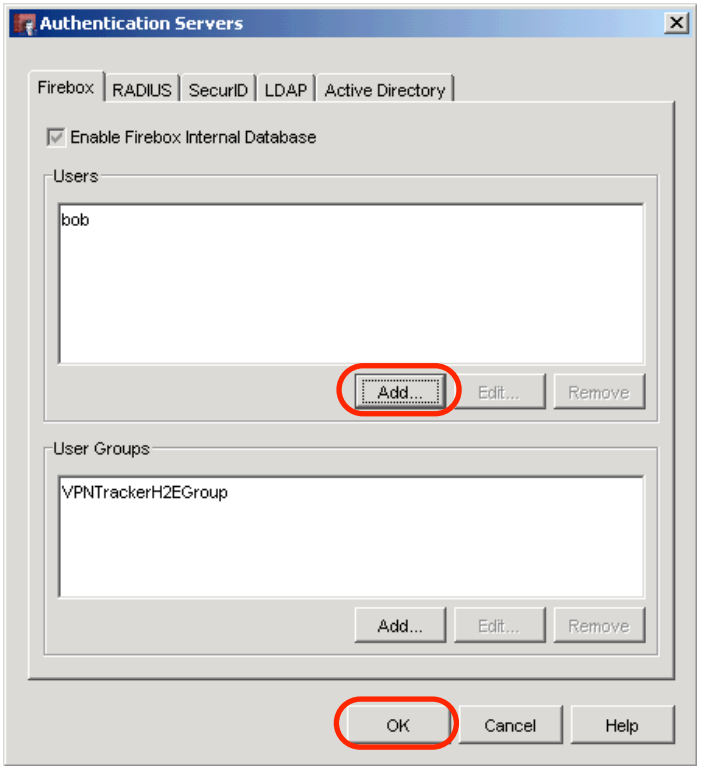


- Click "Add..."



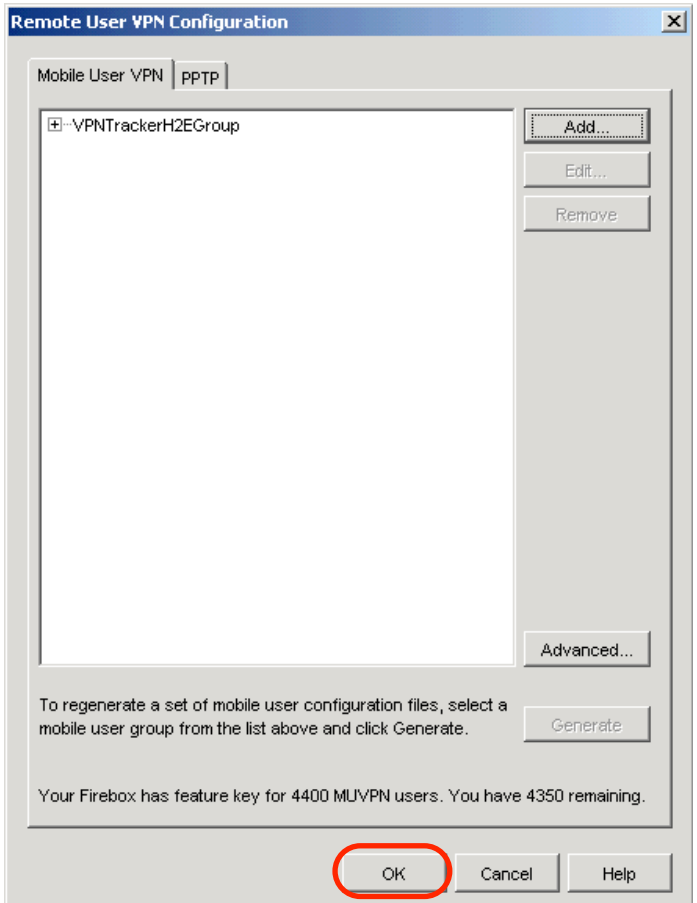
- **Name**: Enter a user name ❹
- **Passphrase**: Enter a password for the user ❺
- **Confirm**: Repeat the password ❺
- **Firebox Authentication Groups**: Add the user to the newly added group (here: "VPNTrackerH2EGroup") by selecting the group from the "Available" list and moving it to the "Member" list by clicking "<<"
- Click "OK"

Step 8b (optional) – Add Additional Users

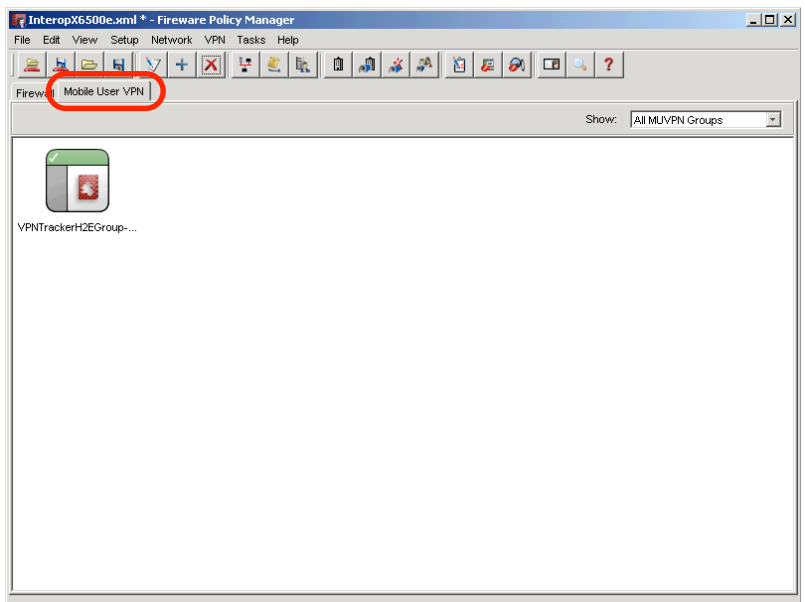


- If desired, add additional users for this VPN connection by clicking "Add..."
- Click "OK" when you are done adding users

Step 9 – Finish Adding the Mobile User VPN Group and Policy

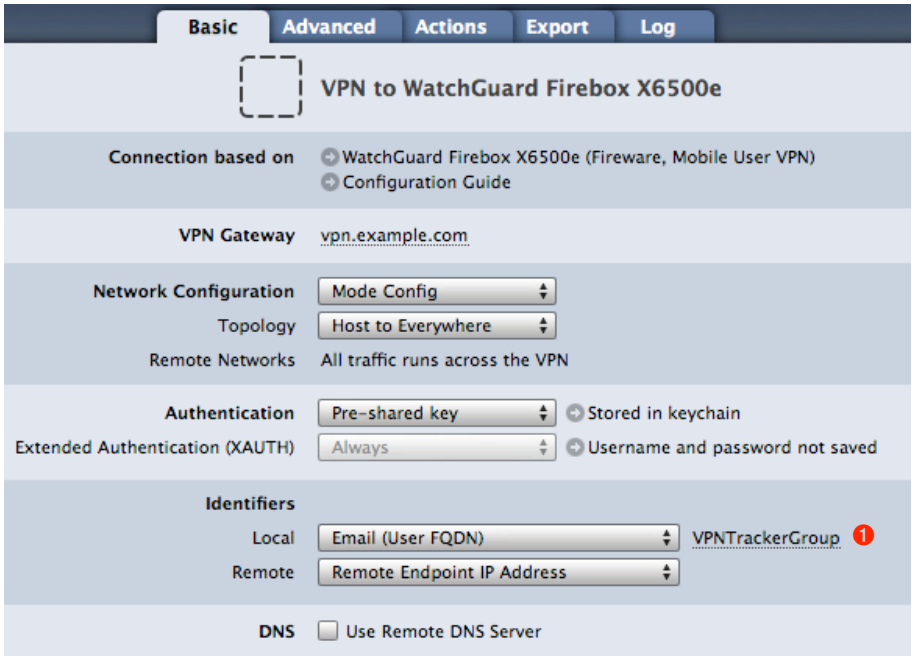


- Click "OK" to finish adding the Mobile User VPN group
- Switch to the "Mobile User VPN" tab in the Fireware Policy Manager to see the Mobile User VPN Policy that has automatically been added for your new Mobile User VPN group
- **Do not forget to save the new settings to your Firebox!**



Required Changes in VPN Tracker

Please follow the configuration instructions in "Task 2: Configure VPN Tracker", with the following exceptions:



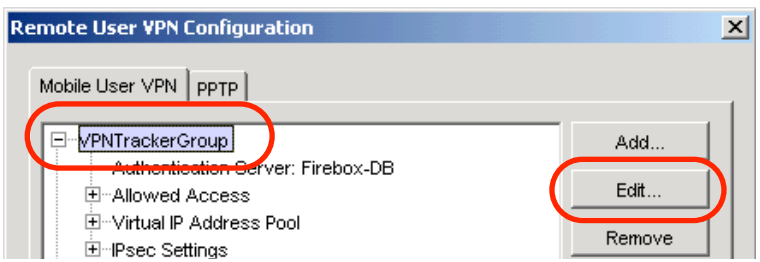
- **Network**: Select "Host to Everywhere" from the pop-up list.
- You will not have to enter anything in the **Remote Networks** field, as this field will be automatically removed once you select "Host to Everywhere"
- **Local Identifier:** Enter the Mobile User VPN Group name that you configured in step 3 ❶

Configuring VPN Tracker Personal Edition

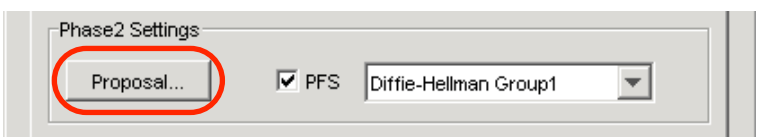
Since the AES-256 encryption algorithm is not available in VPN Tracker Personal Edition, it is necessary to change the Firebox's phase 2 encryption algorithm to an algorithm that is available in this edition (e.g. AES-128).

Follow Task 1 and 2 for the basic configuration

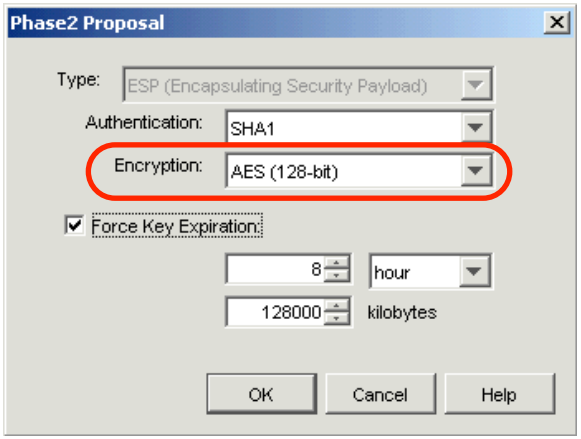
Required Changes on the Firebox



- In the Fireware Policy Manager, select "VPN > Remote Users..." from the menu
- Select the Mobile User VPN group created in Task 1
- Click "Edit..."

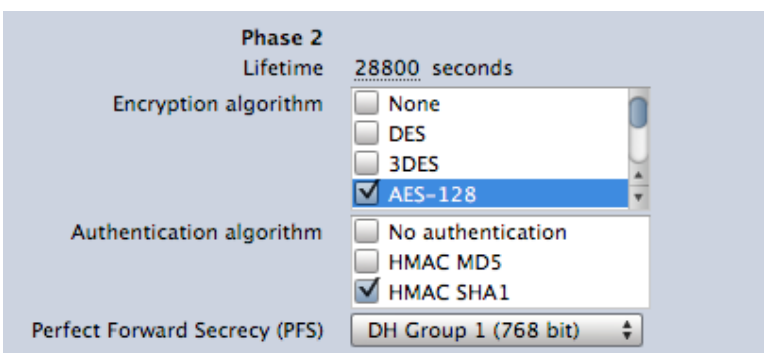


- Click "Proposal..."



- **Encryption**: Select "AES-128" from the popup list (instead of "AES-256")
- Click "OK"
- **Do not forget to save the new settings to your Firebox!**

Required Changes in VPN Tracker



- Select the connection created in Task 2
- Switch to the "Advanced" tab
- **Phase 2 Encryption Algorithm**: Check the box next to "AES-128"

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

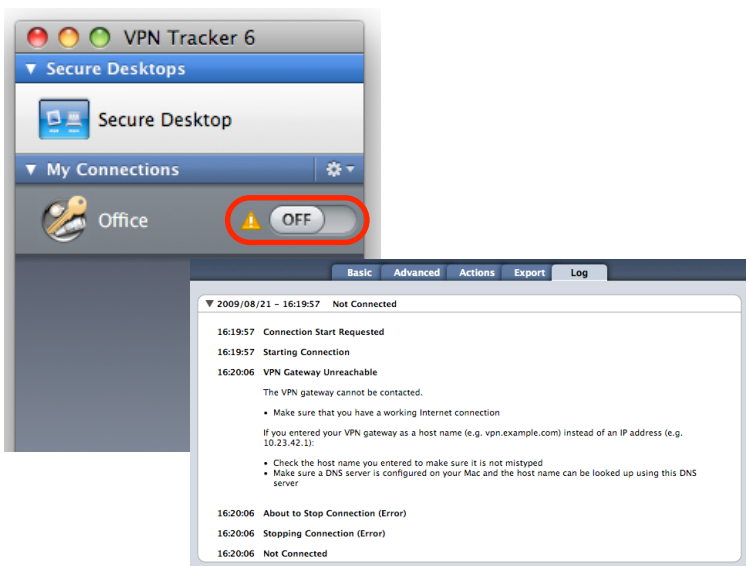
On/Off Slider goes back to "Off" right away

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 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).

Depending on the actual problem, 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. 192.168.1.42), 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.

Check that the IP address you are connecting to is part of the VPN's remote network

Please make sure that the IP address of the resource that you are connecting to is actually contained in the remote network. Also double-check the network mask that you have configured for the remote network in VPN Tracker.

Test VPN Availability again

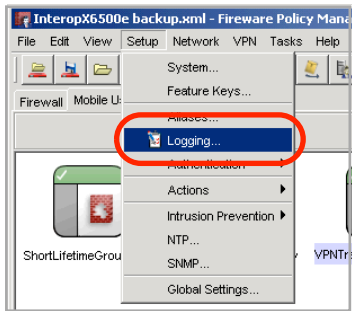
In many networks your Mac will be behind a router that performs Network Address Translation (NAT). For a VPN connection to be established through such a router, VPN Tracker can use different methods, but not all of them may be supported by your local router or your VPN gateway.

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.

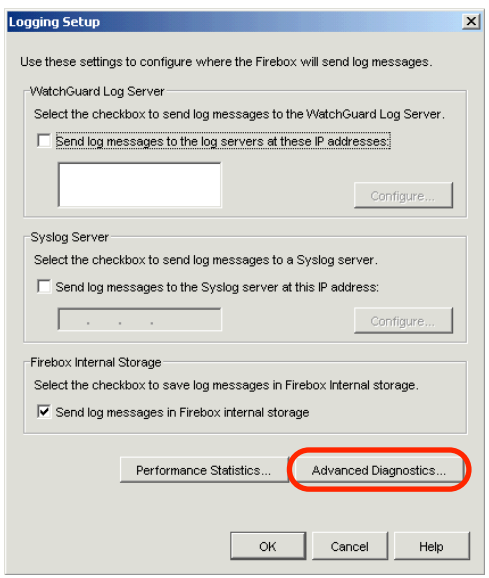
- Select "Tools > Test VPN Availability" from the menu
- Click "Test Again" and wait until the test has completed
- Try connecting again

Obtaining a VPN Log on the Firebox

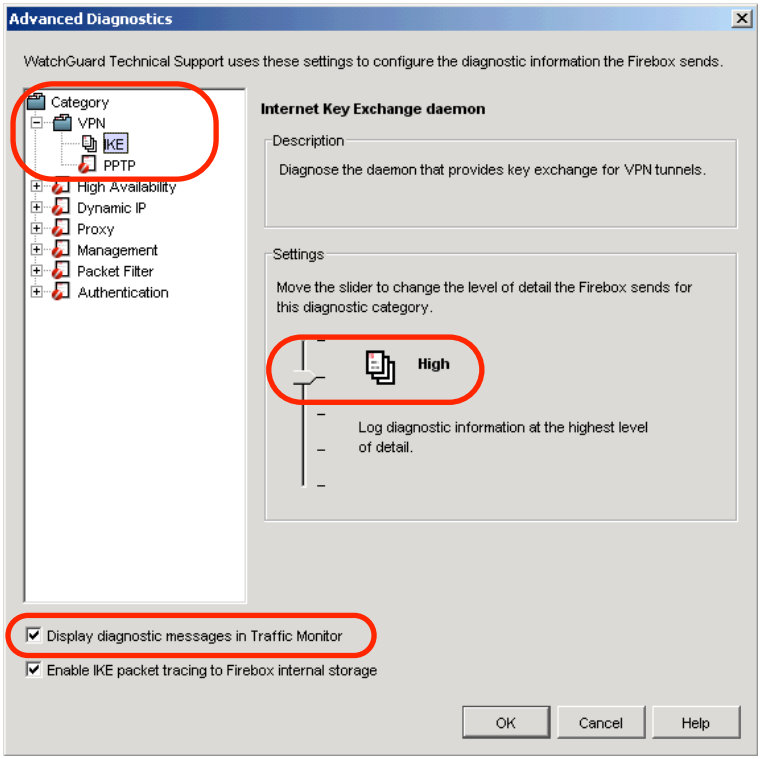
Sometimes it may be necessary to see the VPN log on the Firebox side. Follow these steps to enable VPN logging on the Firebox.



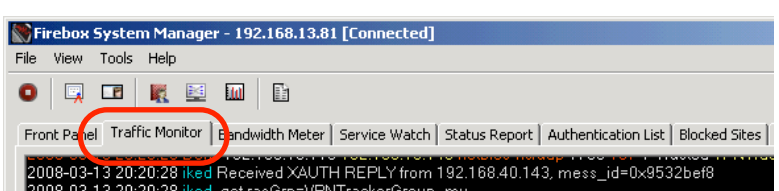
- In the Fireware Policy Manager's menu, click "Setup" > "Logging..."



- Click "Advanced Diagnostics..."



- Select the "VPN > IKE" category
- Move the detail level for the "VPN > IKE" category to "High"
- Check the box "Display diagnostic messages in Traffic Monitor"
- Click "OK"



- After saving the settings to your Firebox, you will be able to view the VPN log in the Firebox System Manager's "Traffic Monitor" tab

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 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 settings
- A detailed description of the problem and the troubleshooting steps you have taken

Appendix: Terminology Matrix

WatchGuard	VPN Tracker
allow Internet traffic to go directly to the mobile user's ISP	Host to Network
force all Internet traffic to flow through the tunnel	Host to Everywhere
MUVPN Group Name	Local Identifier
MUVPN User	XAUTH User
Tunnel Passphrase	Pre-Shared Key