



VPN Configuration Guide

WatchGuard Firebox X – Peak and Core Series

equinux AG and equinux USA, Inc.

© 2008 equinux USA, Inc. All rights reserved.

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

The equinux logo is a trademark of equinux AG and equinux USA, Inc., registered in the U.S. and other countries.

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

Created using Apple Pages.

www.equinux.com

Apple, the Apple logo, iBook, Mac, Mac OS, MacBook, PowerBook are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

Core, Firebox, Fireware, Peak, WatchGuard are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries.

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

Introduction	5
Prerequisites	6
Scenario	7
Terminology.....	8
Task 1 – Configure your VPN Device	9
Step 1 – Access the WatchGuard System Manager.....	9
Step 2 - Add a New Mobile User VPN Group.....	10
Step 3 - Set the Mobile User VPN Group Name.....	11
Step 4 - Set the Tunnel Passphrase.....	12
Step 5 – Select where Internet Traffic is Directed.....	13
Step 6 – Set the Resources that can be accessed through the VPN Tunnel.....	14
Step 7 – Set the Virtual IP Address Pool.....	15
Step 8a – Add a User to the Mobile User VPN Group.....	16
Step 9 – Finish Adding the Mobile User VPN Group and Policy....	19
Task 2 – Configure VPN Tracker	20
Step 1 - Create a New Connection.....	20
Step 2 – Select a VPN Device.....	21
Step 3 – Configure IP Addresses.....	22
Step 4 – Configure Authentication.....	23
Step 5 – Configure Identification.....	24
Task 3 – Test the VPN Connection	25
It's time to go out!.....	25
Test your connection.....	25
Setting up a Host to Everywhere Connection	27

Steps 1 - 2: Follow Steps 1- 2 of “Task 1 – Configure Your VPN Device”	27
Step 3 - Set the Mobile User VPN Group Name.....	27
Step 4 - Set the Tunnel Passphrase.....	28
Step 5 – Select where Internet Traffic is Directed.....	29
Step 6 – Set the Resources that can be accessed through the VPN Tunnel.....	30
Step 7 – Set the Virtual IP Address Pool.....	31
Step 8a – Add a User to the Mobile User VPN Group.....	32
Step 9 – Finish Adding the Mobile User VPN Group and Policy....	35
Required Changes in VPN Tracker.....	36

Configuring VPN Tracker Personal Edition	37
Follow Task 1 and 2 for the basic configuration.....	37
Required Changes on the Firebox.....	37
Required Changes in VPN Tracker.....	38

Troubleshooting	39
VPN Connection Fails to Establish.....	39
VPN Connection Seems to Be Connected, but no Resources Can Be Accessed.....	40
Obtaining a VPN Log on the Firebox.....	42
Further Questions?	44

Appendix: Terminology Matrix	45
---	----

Introduction

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

The WatchGuard device is configured as a router connecting a company LAN to the Internet.

This paper 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.

EQUINUX SHALL HAVE ABSOLUTELY NO LIABILITY FOR ANY DIRECT OR INDIRECT, SPECIAL OR OTHER CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE USE OF THE HOW-TO OR ANY CHANGE TO THE ROUTER GENERALLY, INCLUDING WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS, OR DATA, EVEN IF EQUINUX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Prerequisites

First make sure to use a recent WatchGuard Fireware version. The latest release for your WatchGuard device can be obtained from <http://www.watchguard.com>.

For this document, Fireware 9.1 was used. Please note: VPN Tracker has been only been tested with the this firmware version.

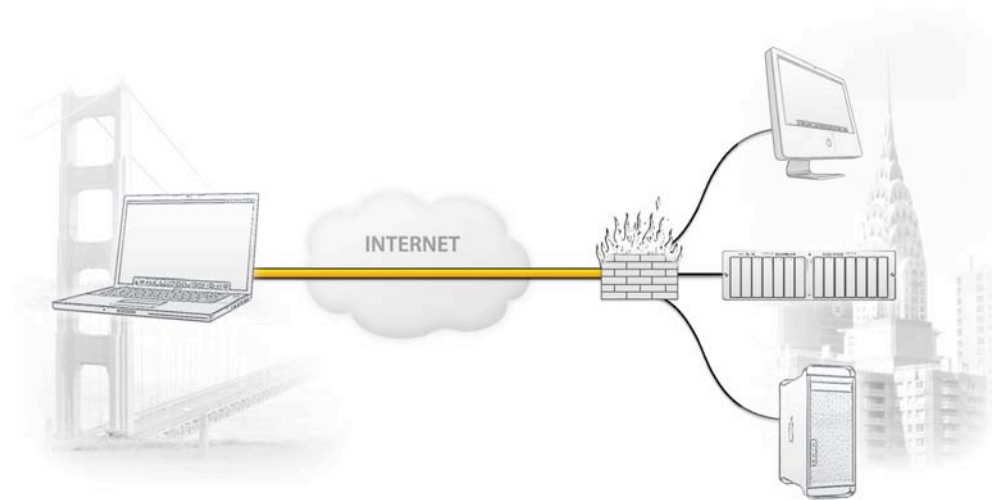
The configuration described in this guide requires VPN Tracker 5.1 or higher. Make sure to use a recent VPN Tracker version. The latest VPN Tracker release can always be obtained from <http://www.vpntracker.com>

You will need one VPN Tracker license for each Mac connecting to the WatchGuard device.

VPN Tracker is compatible with Mac OS 10.4 and 10.5.

Scenario

In our example, we need to connect an employee's Mac Book in San Francisco to an office in New York. The following diagram illustrates this scenario:



The MacBook is connected directly to the Internet, and has a public IP address, assigned by an ISP.

The office's WatchGuard VPN gateway is also connected to the Internet and can be accessed via a static IP address. The VPN gateway has a second interface which is connected to the internal office network. In our example, the office network has the IP range 192.168.1.0/24.

A VPN tunnel will be established between the public interfaces in San Francisco and New York. Once the VPN tunnel is up, San Francisco can access the office network behind the VPN gateway.

Please note that the connection from a MacBook at home to an office network is just one possible scenario. The instructions also apply to connections from a desktop computer or notebook in your office to a VPN gateway at home or at another office. Please adapt the term "office network", which is used throughout this manual, to your scenario.

Terminology

Each VPN connection is established between two peers. In the case of VPN Tracker, one peer is a Mac running VPN Tracker ("client"), the other is (usually) a gateway capable of handling VPN tunnels. Please note that for each peer, the settings on the other peer are considered to be "remote", while the own settings are called "local": a "local" setting from VPN Tracker's perspective, is a "remote" setting from the VPN gateway's perspective, and vice versa.

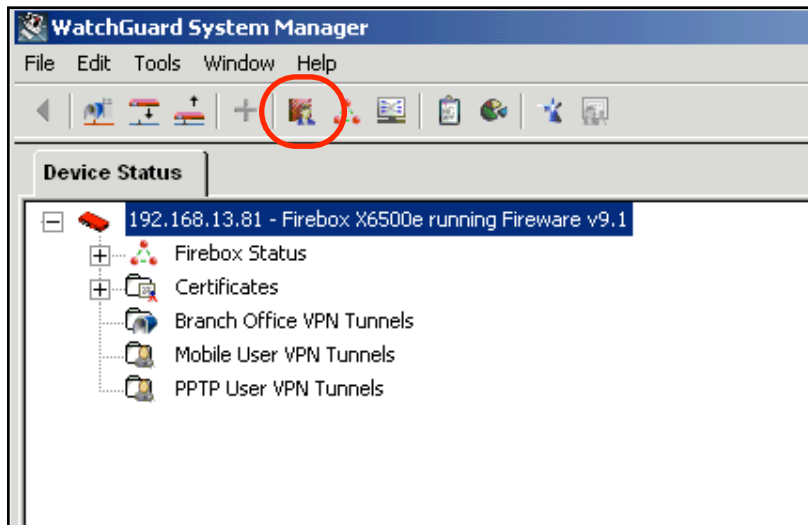
A list of terms used by WatchGuard, and their corresponding terms in VPN Tracker can be found in Appendix: Terminology Matrix.

Task 1 – Configure your VPN Device

This section describes the configuration of your WatchGuard VPN router.

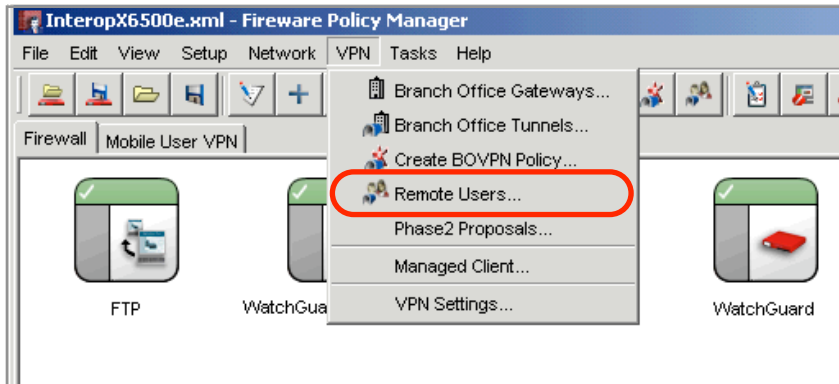
TIP To set up your VPN connection, you'll need to keep track of certain pieces of information. Those details are indicated by red numbers. Throughout this guide we will be referencing those numbers.

Step 1 – Access the WatchGuard System Manager

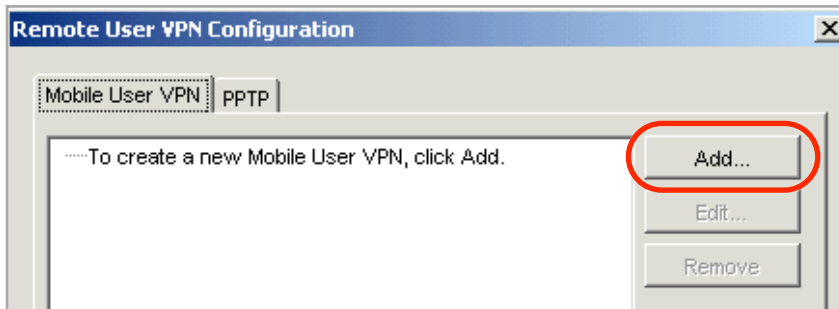


- ▶ Start WatchGuard System Manager
- ▶ Select your WatchGuard device from the list
- ▶ Start the Fireware Policy Manager by clicking its icon

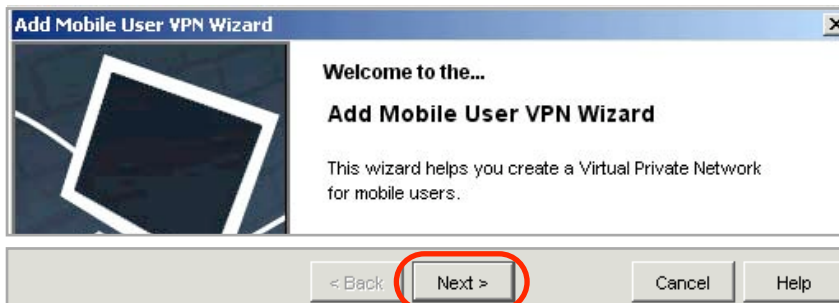
Step 2 - Add a New Mobile User VPN Group



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



- ▶ Click "Add..."



- ▶ Click "Next"

Step 3 - Set the Mobile User VPN Group Name

Add Mobile User VPN Wizard

Select a user authentication server.

Select the server and group the Firebox will use to authenticate mobile users.

Authentication Server: Firebox-DB

Group Name: VPNTrackerGroup

The group name must identify a valid user group name on the authentication server. Group names are case sensitive.

[Learn more about authentication servers.](#)

< Back Next > Cancel Help

- ▶ **Authentication Server:** Select "Firebox-DB"
- ▶ **Group Name:** Enter a group name, e.g. "VPNTrackerGroup" 1
- ▶ 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

Add Mobile User VPN Wizard

Select a tunnel authentication method.

Select the authentication method the Firebox will use to establish a secure VPN tunnel.

Use this passphrase:

Tunnel Passphrase: ***** 2

Retype Passphrase: ***** 2

Use an RSA certificate issued by your WatchGuard Management Server.

Provide the administration passphrase for your server.

IP Address: 0 . 0 . 0 . 0

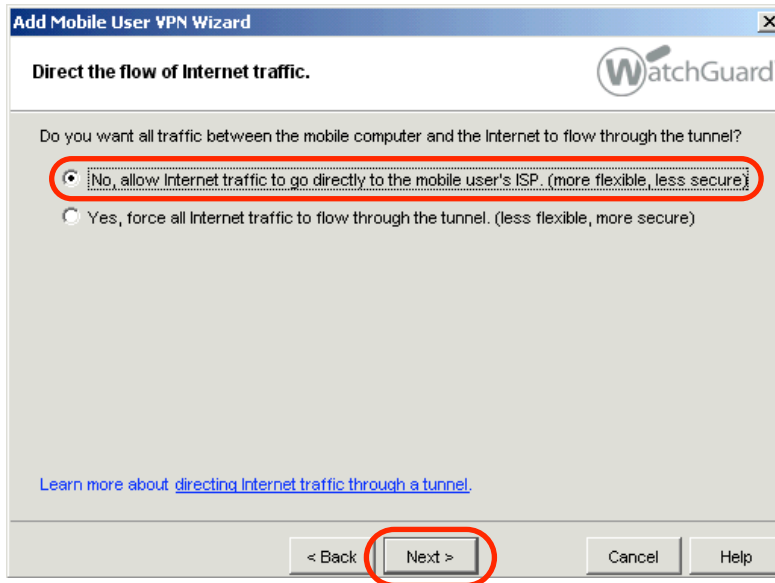
Administration Passphrase:

[Learn more about authentication methods.](#)

< Back **Next >** Cancel Help

- ▶ 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 2
- ▶ **Retype Passphrase:** Repeat the password you have entered in the previous field 2
- ▶ 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

Add Mobile User VPN Wizard

Identify the resources accessible through the tunnel.

Add the computers and networks which will be accessible to mobile users through the VPN tunnel.

Type	IP Address
------	------------

Add...

- ▶ Click “Add” to add the network that can be accessed through the VPN tunnel

Add Address

Choose Type: Network IP

Value: 192.168.1.0 /24

OK Cancel

- ▶ **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”

Type	IP Address
Network IP	192.168.1.0/24

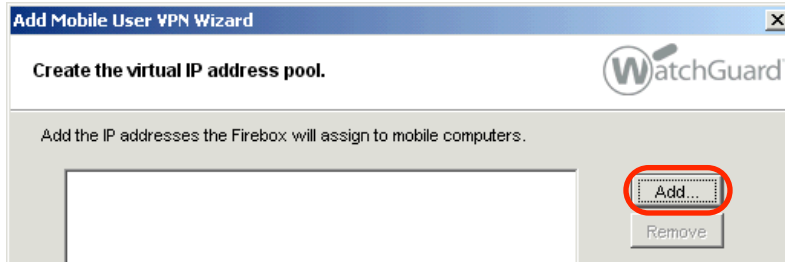
Add... Remove

< Back Next > Cancel Help

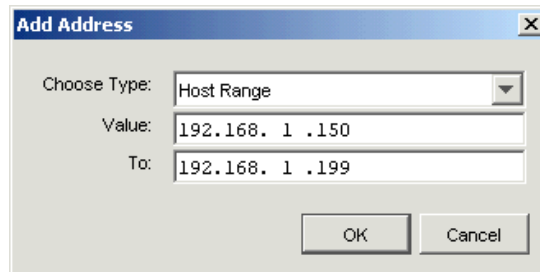
- ▶ Click “Next”

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...”

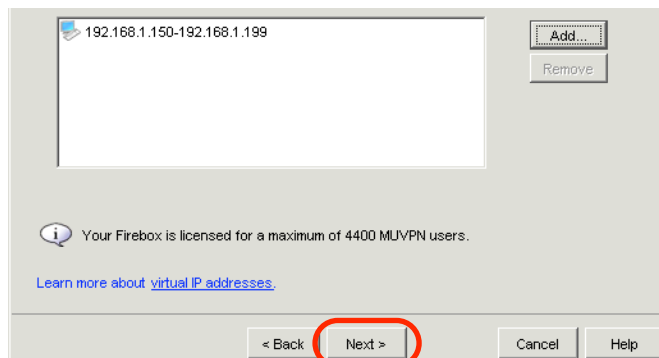


▶ **Choose Type:** Select “Host Range”

▶ Choose a range of unused IP addresses from the remote network. **3** 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

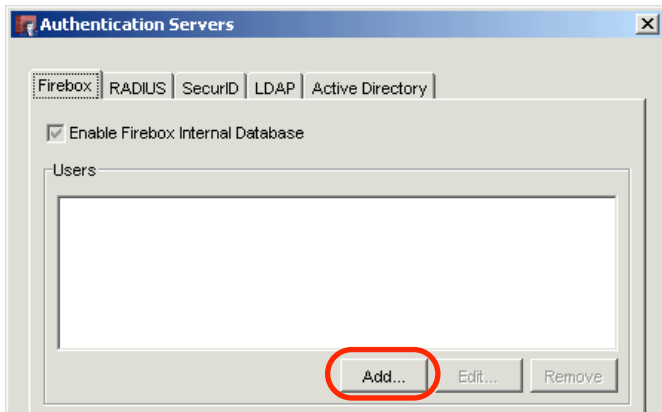


▶ Click “Next”

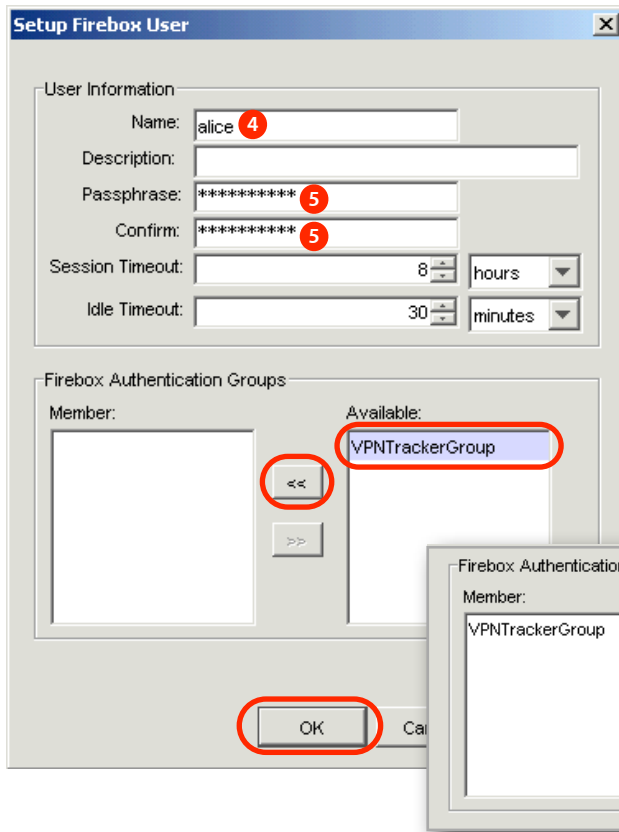
Step 8a – Add a User to the Mobile User VPN Group



- ▶ Check the box “Add users to VPNTrackerGroup”
- ▶ Click “Finish”



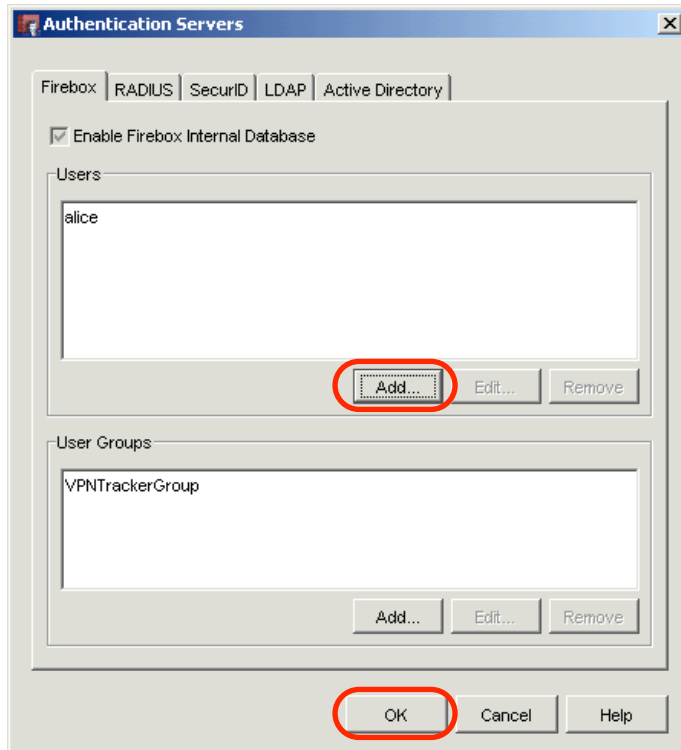
- ▶ Click “Add...”



- ▶ **Name:** Enter a user name 4
- ▶ **Passphrase:** Enter a password for the user 5
- ▶ **Confirm:** Repeat the password 5
- ▶ **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"

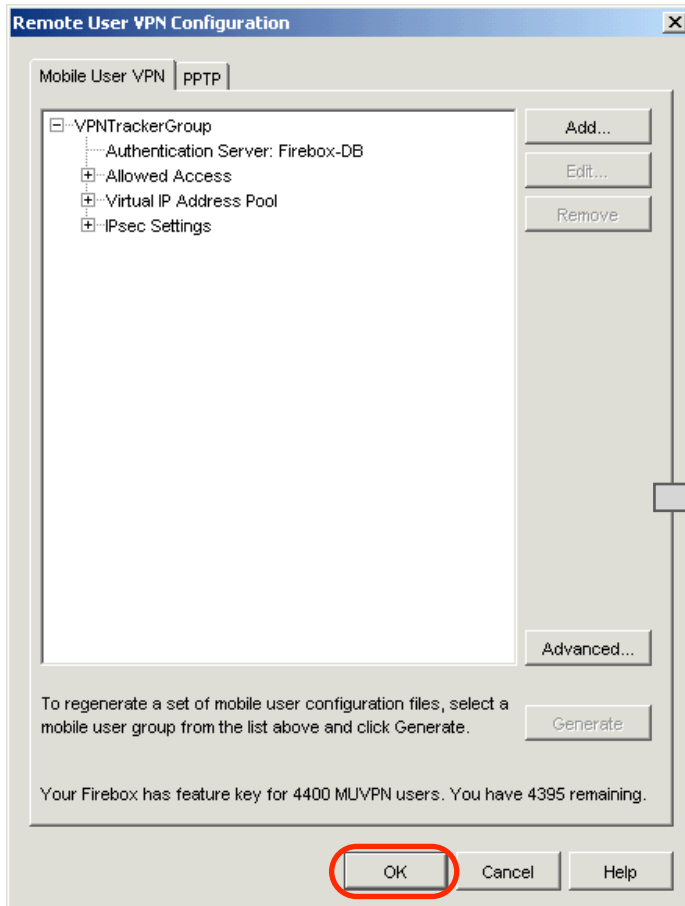
Tip To prevent the VPN connection from being **disconnected after 8 hours**, adjust the **Session Timeout**: A value of 0 means that the Firebox never forces a disconnect. .

Step 8b (optional) – Add Additional Users

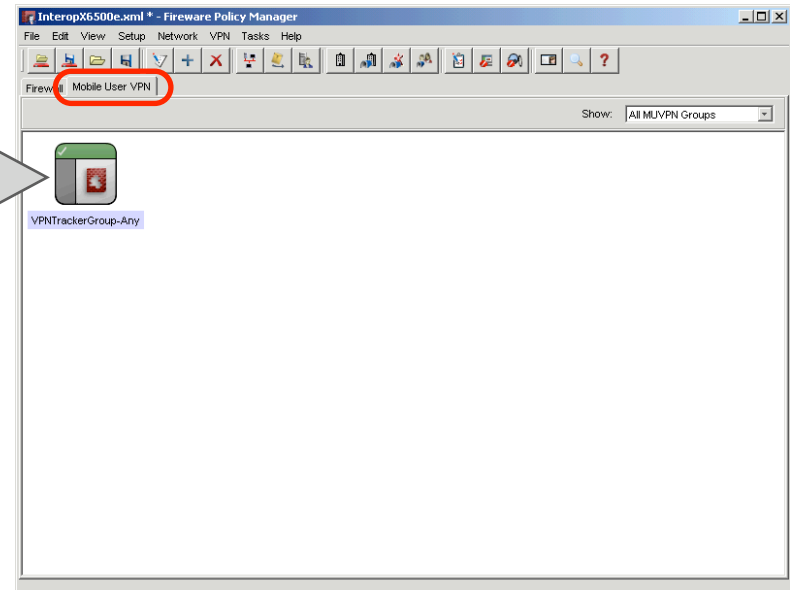


- ▶ If desired, add additional users for this VPN connection by clicking "Add..."
- ▶ Click "OK" when you are done adding users

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



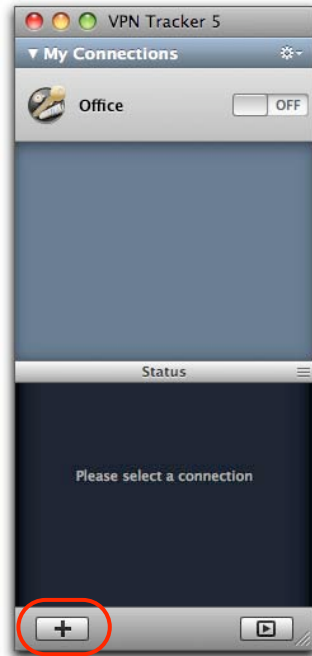
- ▶ Click "OK" to finish adding the Mobile User VPN group
- ▶ Switch to the "Mobile User VPN" tab in the Fireware Policy Manager to see the Mobile User VPN Policy that has automatically been added for your new Mobile User VPN group
- ▶ **Do not forget to save the new settings to your Firebox!**



Task 2 – Configure VPN Tracker

This section describes how to configure VPN Tracker.

Step 1 - Create a New Connection

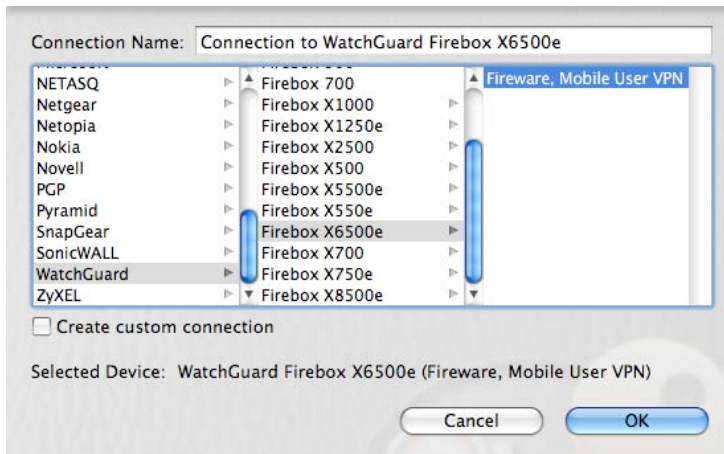


- ▶ Start VPN Tracker 5
- ▶ Click the "+" button in the main window

Step 2 – Select a VPN Device

For many VPN gateways, VPN Tracker 5 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 5 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)

Basic Advanced Actions Log

Office

Connection based on WatchGuard Firebox X6500e (Fireware, Mobile User VPN)
Configuration Guide

Client Provisioning Mode Config

Network Host to Network

VPN Gateway vpn.example.com

Remote Networks 192.168.1.0 / 255.255.255.0 3

Authentication Pre-shared key Edit
 Use Extended Authentication (XAUTH) when requested

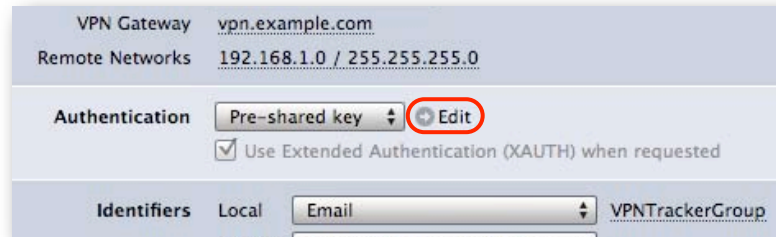
Identifiers Local Email VPNTTrackerGroup
Remote Remote Endpoint IP Address
 Verify remote identifier

DNS Use Remote DNS Server

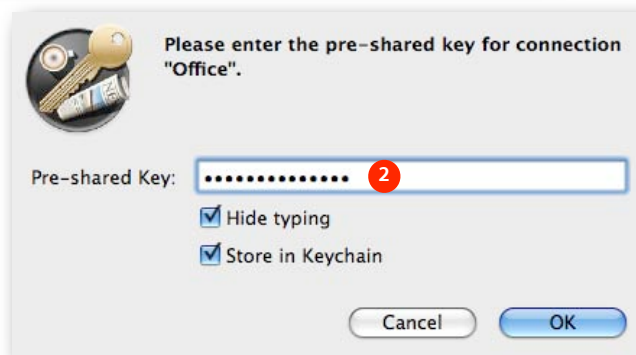
- ▶ Make sure the **Mode Config** box is checked
- ▶ **VPN Gateway:** Enter your Firebox's public IP address (WAN IP) or its host name
- ▶ **Remote Networks:** Enter the Firebox's LAN network address and network mask 3, separated by a slash

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.

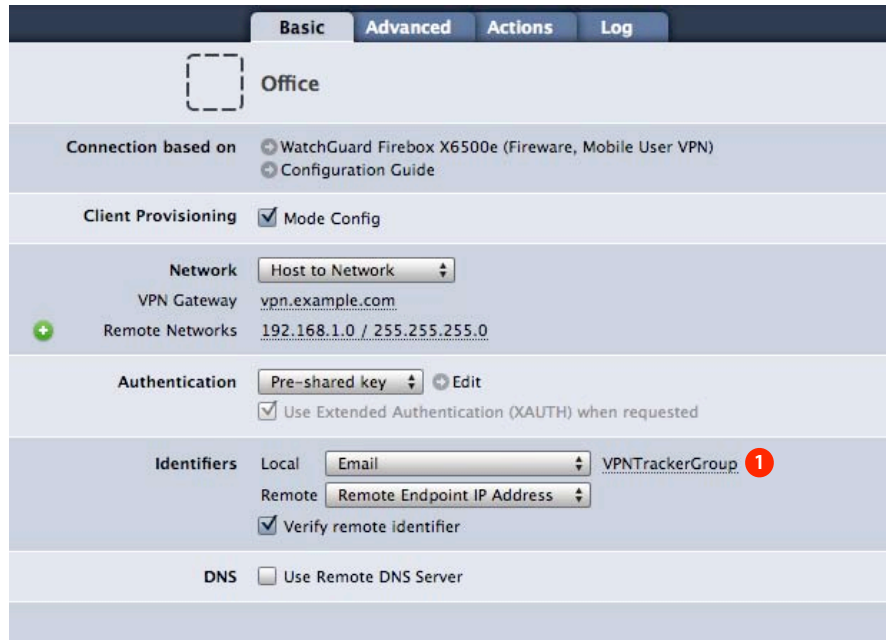


- ▶ Click the "Edit" arrow next to **Pre-shared key**
- ▶ Enter the pre-shared key **2**
- ▶ Make sure **"Store in Keychain"** is checked
- ▶ Click "OK"



Step 5 – Configure Identification

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



The screenshot shows the 'Advanced' configuration tab for a VPN connection. The connection is named 'Office'. It is based on a WatchGuard Firebox X6500e. Client provisioning is set to 'Mode Config'. The network is 'Host to Network' with a VPN Gateway of 'vpn.example.com' and Remote Networks of '192.168.1.0 / 255.255.255.0'. Authentication is set to 'Pre-shared key' with 'Use Extended Authentication (XAUTH) when requested' checked. In the 'Identifiers' section, the 'Local' identifier is 'Email' with the value 'VPNTrackerGroup' (marked with a red '1'), and the 'Remote' identifier is 'Remote Endpoint IP Address'. The 'Verify remote identifier' checkbox is checked. The 'DNS' section has 'Use Remote DNS Server' unchecked.

► **Local Identifier:** Enter the Mobile User VPN group name from the Firebox **1**

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.

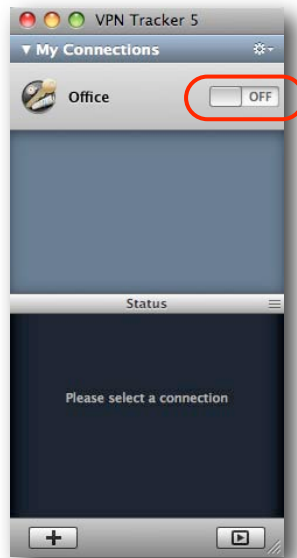
Task 3 – Test the VPN Connection

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 **4**
- ▶ **Password:** Enter the password that you set for this user **5**
- ▶ **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

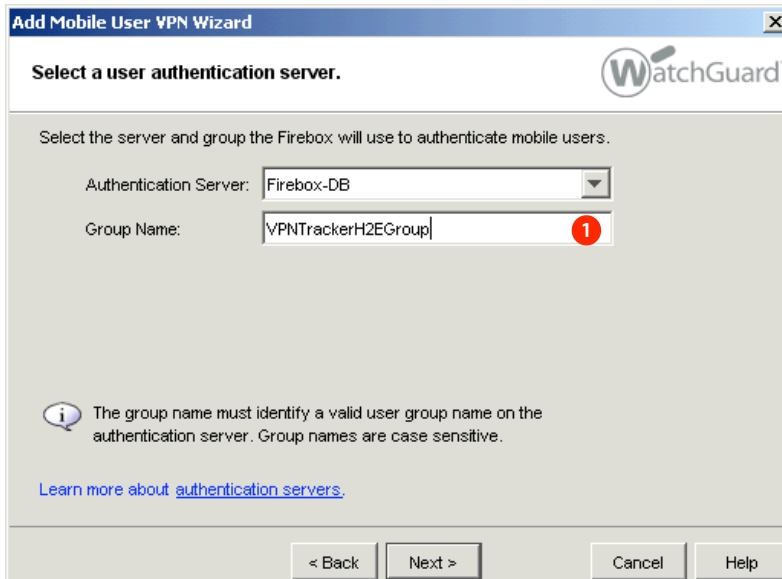
Congratulations!

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



Add Mobile User VPN Wizard

Select a user authentication server.

Select the server and group the Firebox will use to authenticate mobile users.

Authentication Server: Firebox-DB

Group Name: VPNTrackerH2EGroup 1

The group name must identify a valid user group name on the authentication server. Group names are case sensitive.

[Learn more about authentication servers.](#)

< Back Next > Cancel Help

- ▶ **Authentication Server:** Select “Firebox-DB”
- ▶ **Group Name:** Enter a group name, e.g. “VPNTrackerH2EGroup” 1
- ▶ Click “Next”

Step 4 - Set the Tunnel Passphrase

Add Mobile User VPN Wizard

Select a tunnel authentication method.

Select the authentication method the Firebox will use to establish a secure VPN tunnel.

Use this passphrase:

Tunnel Passphrase: ***** 2

Retype Passphrase: ***** 2

Use an RSA certificate issued by your WatchGuard Management Server.

Provide the administration passphrase for your server.

IP Address: 0 . 0 . 0 . 0

Administration Passphrase:

[Learn more about authentication methods.](#)

< Back Next > Cancel Help

- ▶ 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 2
- ▶ **Retype Passphrase:** Repeat the password you have entered in the previous field 2
- ▶ Click “Next”

Step 5 – Select where Internet Traffic is Directed

Add Mobile User VPN Wizard

Direct the flow of Internet traffic. WatchGuard

Do you want all traffic between the mobile computer and the Internet to flow through the tunnel?

No, allow Internet traffic to go directly to the mobile user's ISP. (more flexible, less secure)

Yes, force all Internet traffic to flow through the tunnel. (less flexible, more secure)

[Learn more about directing Internet traffic through a tunnel.](#)

< Back Next > Cancel Help

- ▶ 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

Add Mobile User VPN Wizard

Identify the resources accessible through the tunnel.

Add the computers and networks which will be accessible to mobile users through the VPN tunnel.

Type	IP Address
Alias	Any-External
Network IP	0.0.0.0/0

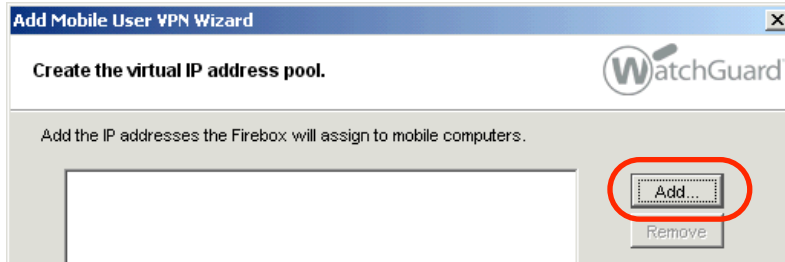
Buttons: Add... Remove

Navigation: < Back **Next >** Cancel Help

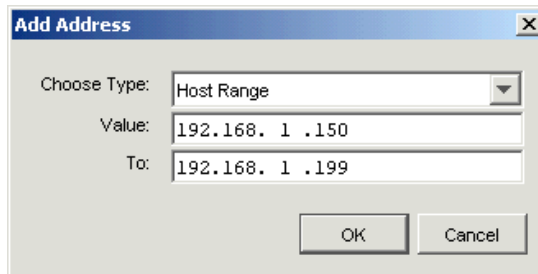
- ▶ The correct resources for a Host-to-Everywhere connection are automatically added to the tunnel definition.
- ▶ Click “Next”

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...”

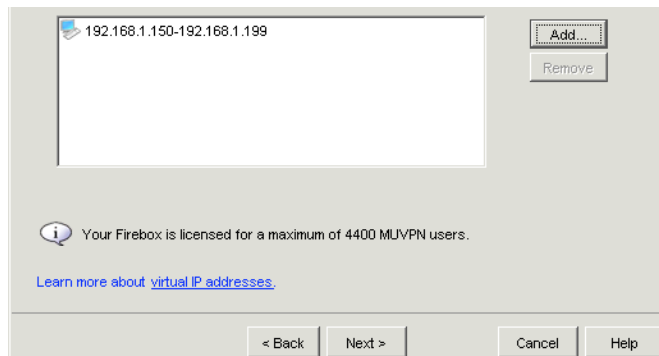


▶ **Choose Type:** Select “Host Range”

▶ Choose a range of unused IP addresses from the remote network. **3** 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

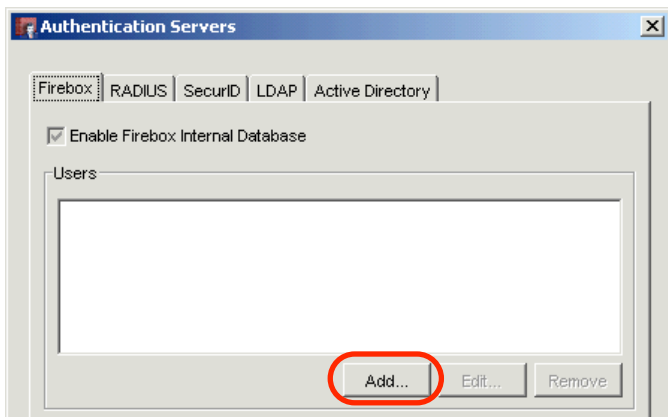


▶ Click “Next”

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



- ▶ Check the box “Add users to VPNTrackerH2EGroup”
- ▶ Click “Finish”



- ▶ Click “Add...”

Setup Firebox User

User Information

Name: bob **4**

Description:

Password: ***** **5**

Confirm: ***** **5**

Session Timeout: 8 hours

Idle Timeout: 30 minutes

Firebox Authentication Groups

Member:

Available: VPNTrackerH2EGroup

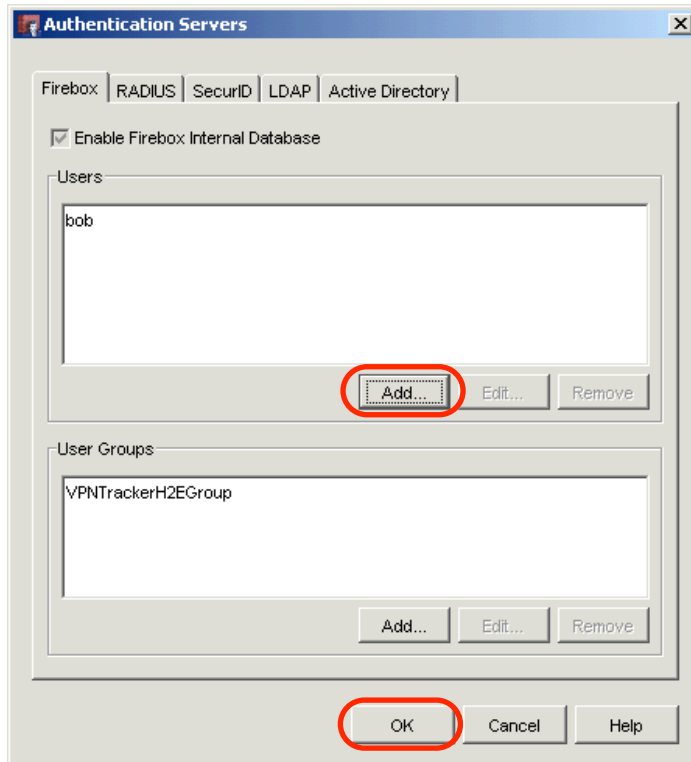
<<

>>

OK

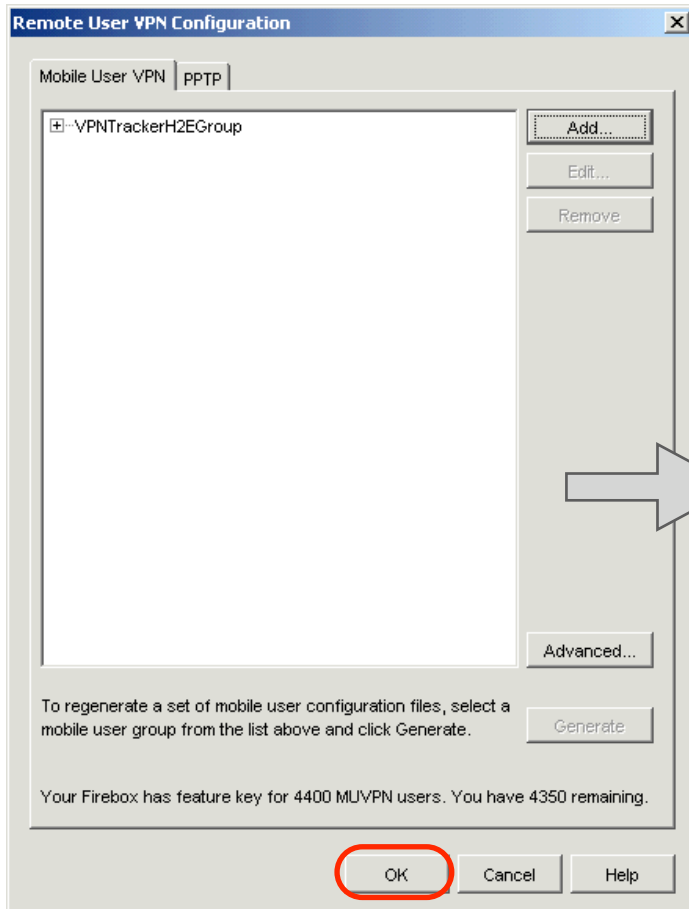
- ▶ **Name:** Enter a user name **4**
- ▶ **Password:** Enter a password for the user **5**
- ▶ **Confirm:** Repeat the password **5**
- ▶ **Firebox Authentication Groups:** Add the user to the newly added group (here: "VPNTrackerH2EGroup") by selecting the group from the "Available" list and moving it to the "Member" list by clicking "<<"
- ▶ Click "OK"

Step 8b (optional) – Add Additional Users

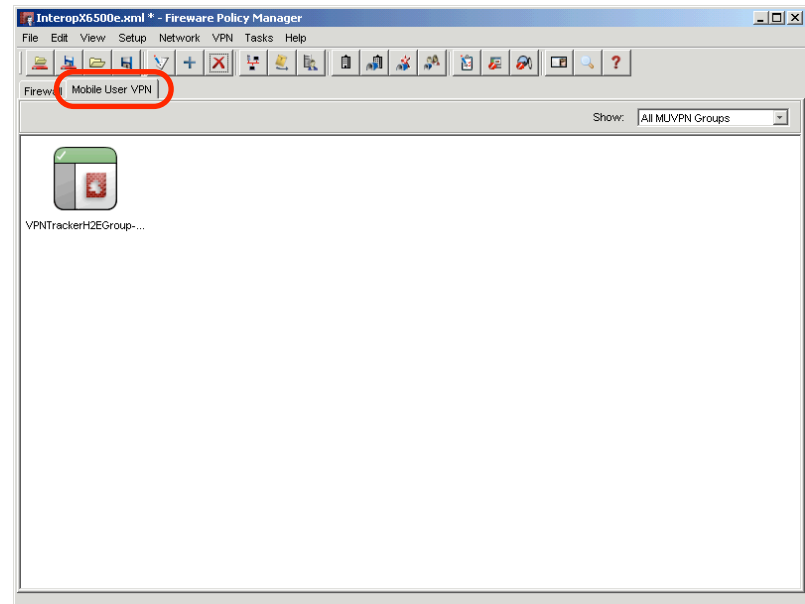


- ▶ If desired, add additional users for this VPN connection by clicking "Add..."
- ▶ Click "OK" when you are done adding users

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

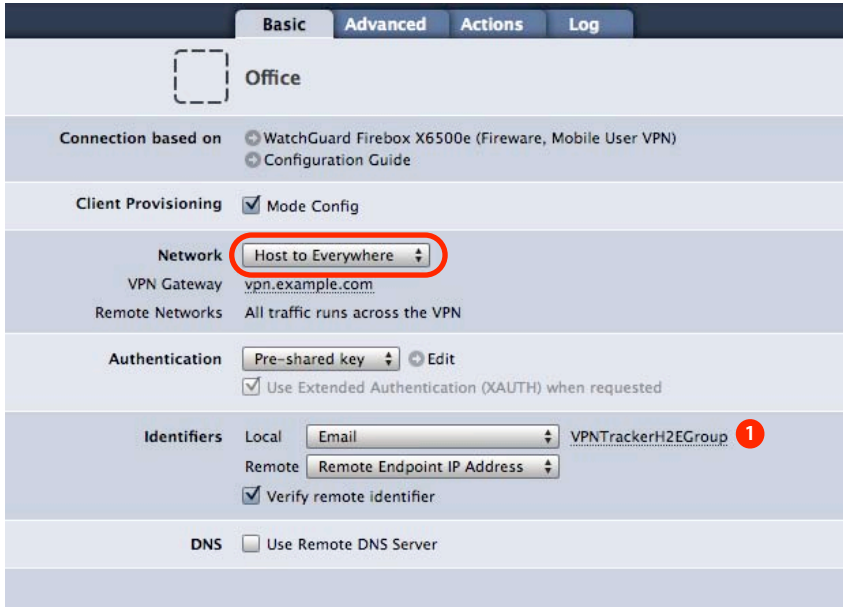


- ▶ Click "OK" to finish adding the Mobile User VPN group
- ▶ Switch to the "Mobile User VPN" tab in the Fireware Policy Manager to see the Mobile User VPN Policy that has automatically been added for your new Mobile User VPN group
- ▶ **Do not forget to save the new settings to your Firebox!**



Required Changes in VPN Tracker

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



The screenshot displays the configuration interface for a VPN Tracker. The interface is divided into several sections:

- Basic** (selected tab): Shows the name "Office" and a dashed box icon.
- Connection based on**: Includes "WatchGuard Firebox X6500e (Fireware, Mobile User VPN)" and "Configuration Guide".
- Client Provisioning**: Includes a checked checkbox for "Mode Config".
- Network**: Includes a dropdown menu for "Network" set to "Host to Everywhere" (circled in red), "VPN Gateway" set to "vpn.example.com", and "Remote Networks" set to "All traffic runs across the VPN".
- Authentication**: Includes a dropdown for "Pre-shared key" and a checked checkbox for "Use Extended Authentication (XAUTH) when requested".
- Identifiers**: Includes "Local" set to "Email" and "Remote" set to "Remote Endpoint IP Address". A red circle with the number "1" is next to the "Local" dropdown.
- DNS**: Includes an unchecked checkbox for "Use Remote DNS Server".

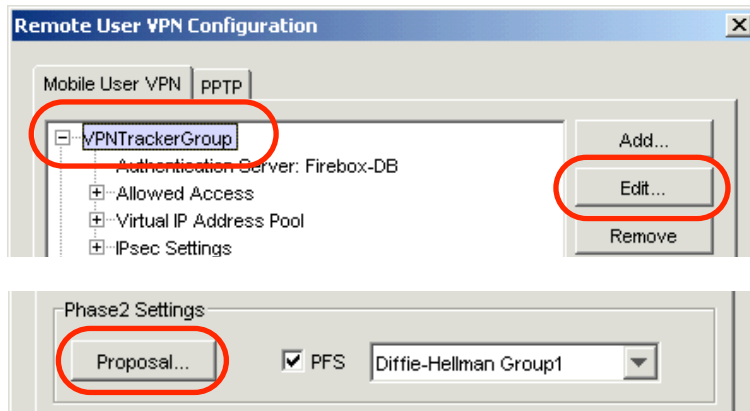
- ▶ **Network**: Select “Host to Everywhere” from the pop-up list.
- ▶ You will not have to enter anything in the **Remote Networks** field, as this field will be automatically removed once you select “Host to Everywhere”
- ▶ **Local Identifier**: Enter the Mobile User VPN Group name that you configured in step 3 **1**

Configuring VPN Tracker Personal Edition

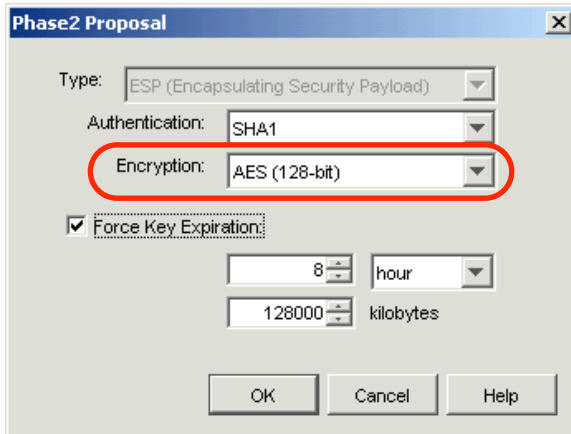
Since the AES-256 encryption algorithm is not available in VPN Tracker Personal Edition, it is necessary to change the Firebox's phase 2 encryption algorithm to an algorithm that is available in this edition (e.g. AES-128).

Follow Task 1 and 2 for the basic configuration

Required Changes on the Firebox

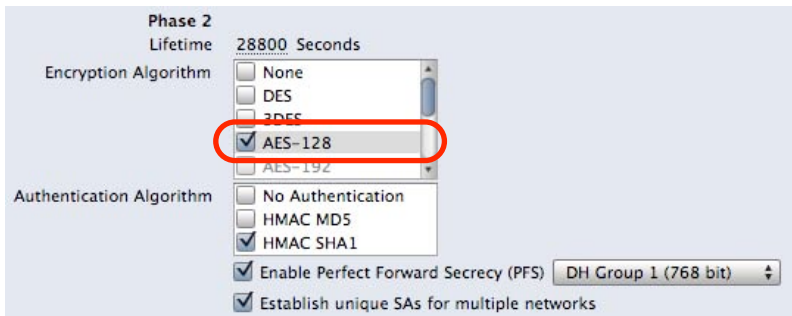


- ▶ In the Fireware Policy Manager, select "VPN > Remote Users..." from the menu
- ▶ Select the Mobile User VPN group created in Task 1
- ▶ Click "Edit..."
- ▶ Click "Proposal..."



- ▶ **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

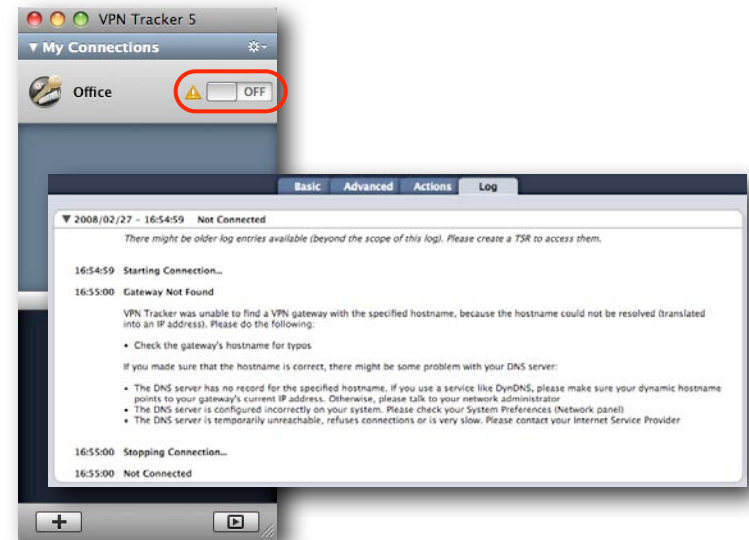
On/Off Slider goes back to “Off” right away

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.



VPN Connection Seems to Be Connected, but no Resources Can Be Accessed

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 by IP address instead of 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 if the IP address is part of the 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.

Tip The network mask (e.g. 255.255.255.0) determines the size of a network. Some examples: The network 192.168.1.0/255.255.255.0 contains **all** IP addresses starting with 192.168.1.x. The network 192.168.1.0/255.255.255.255 contains only a single IP address, 192.168.1.0.

Run the VPN Environment Manager

In many local network 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 one of three different methods, but not all of them may be supported by your local router or your VPN gateway. In that case, your VPN connection may seem connected, but no connections to servers or other resources in the VPN are possible. VPN Tracker includes a tool to detect the right method for the local network:

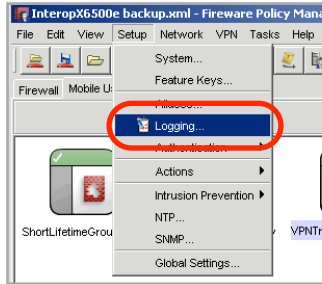
- ▶ Stop all running VPN connections
- ▶ Select "Help > VPN Environment Manager"
- ▶ Click on "Continue"

- ▶ Wait until VPN Tracker has performed the tests
- ▶ Try to start the connection again

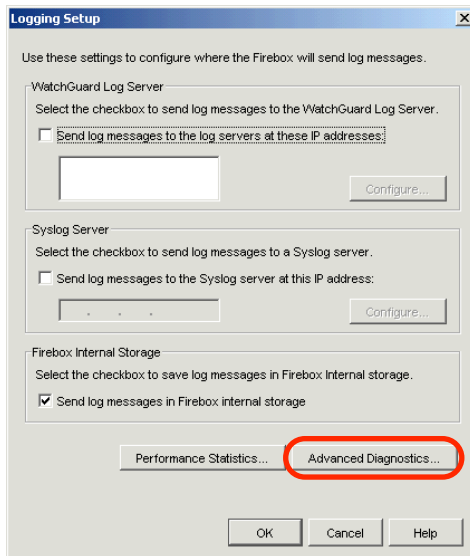
Tip You will only have to run the VPN Environment Manager once for each location that you are using VPN Tracker at.

Obtaining a VPN Log on the Firebox

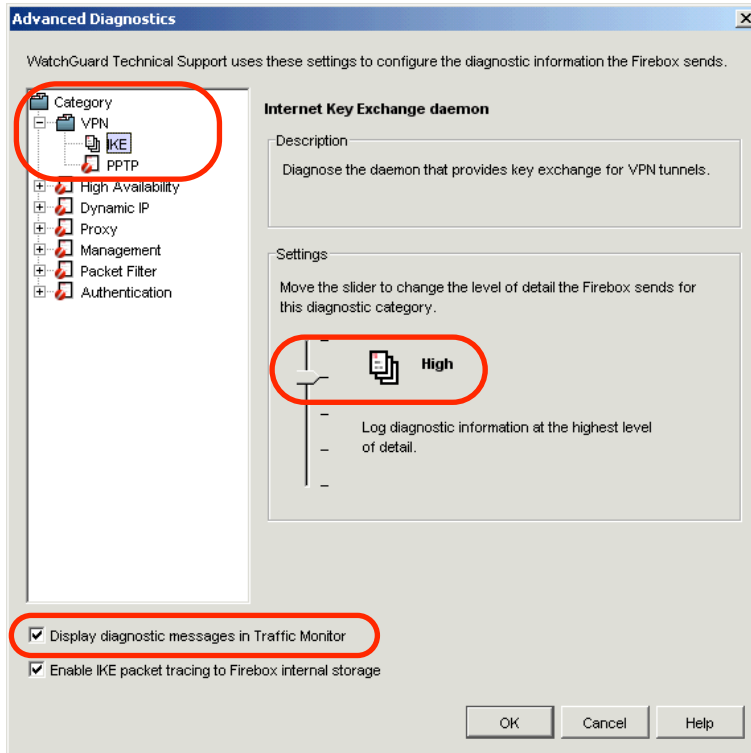
Sometimes it may be necessary to see the VPN log on the Firebox side. Follow these steps to enable VPN logging on the Firebox.



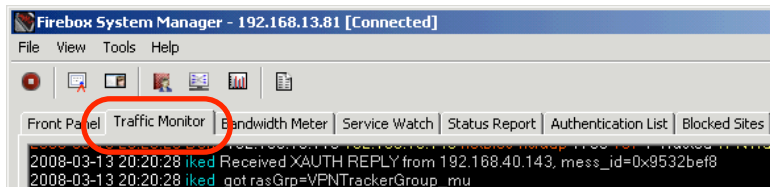
- ▶ In the Fireware Policy Manager's menu, click "Setup" > "Logging..."



- ▶ 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