



VPN Configuration Guide

NETGEAR® FVG318 / FVS318G / FVS336G / FVS338 / DGFV338
FVX538 / SRXN3205 / SRX5308 / ProSecure™ UTM Series

© 2010 equinix AG and equinux USA, Inc. All rights reserved.

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

The equinix logo is a trademark of equinix AG and equinux USA, Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

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

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

Manual revision 3

Created using Apple Pages.

www.equinix.com

Introduction	5	VPN Settings Explained	30
Important Prerequisites.....	6	IKE Policy.....	.30
Scenario.....	7	VPN Policy33
Terminology.....	8	The Role of the Local Address in VPN Tracker37
My NETGEAR Configuration	9		
Task 1 – Configure your NETGEAR	10		
Step 1 – Start the VPN Wizard	10		
Step 2 – Configure the VPN	11		
Step 3 – Retrieve your NETGEAR’s WAN Configuration	12		
Step 4 – Check the Settings for the VPN Policy	13		
Step 5 – Check the Settings for the IKE Policy.....	15		
Task 2 – Configure VPN Tracker	16		
Step 1 – Create a New Connection.....	16		
Step 2 – Configure the VPN Connection	17		
Task 3 – Test the VPN Connection	18		
It’s time to go out!.....	18		
Start your connection	18		
Supporting Multiple Users	20		
Individual User Logins with Extended Authentication (XAUTH) ...	20		
Using Mode Config for IP Address Assignment.....	24		
Deploying VPN Connections to Your Users.....	26		
Troubleshooting	27		
VPN Connection Fails to Establish.....	27		
No Access to the Remote Network.....	28		
Further Questions?	29		

Introduction

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

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

NETGEAR Configuration

The first part of this document will show you how to configure a VPN tunnel on a NETGEAR VPN router using the NETGEAR's VPN Wizard. This is the easiest method of setting up a VPN connection on the device.

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.

Troubleshooting and Advanced Topics

Troubleshooting and advanced topics are covered in the third part of this document. There you will find

- ▶ troubleshooting tips
- ▶ instructions for setting up a VPN connection for multiple users
- ▶ an in-depth discussion of the various NETGEAR settings and how they relate to VPN Tracker

Tip If you are setting up VPN on your device for the first time, we strongly recommend you start out with the tutorial-style setup in the first and second part of this document, and only add additional users and features to your connection once you have the basic setup working.

Important Prerequisites

Your NETGEAR Device

This document applies to the following NETGEAR devices running firmware 3.0 or later:

- ▶ FVS318G
- ▶ FVS336G
- ▶ FVS338
- ▶ DGFW338
- ▶ FVG318¹
- ▶ FVX538
- ▶ SRXN3205
- ▶ SRX5308
- ▶ ProSecure UTM Series²

Documentation for other NETGEAR devices is available at <http://www.vpntracker.com/interop>.

Your Mac

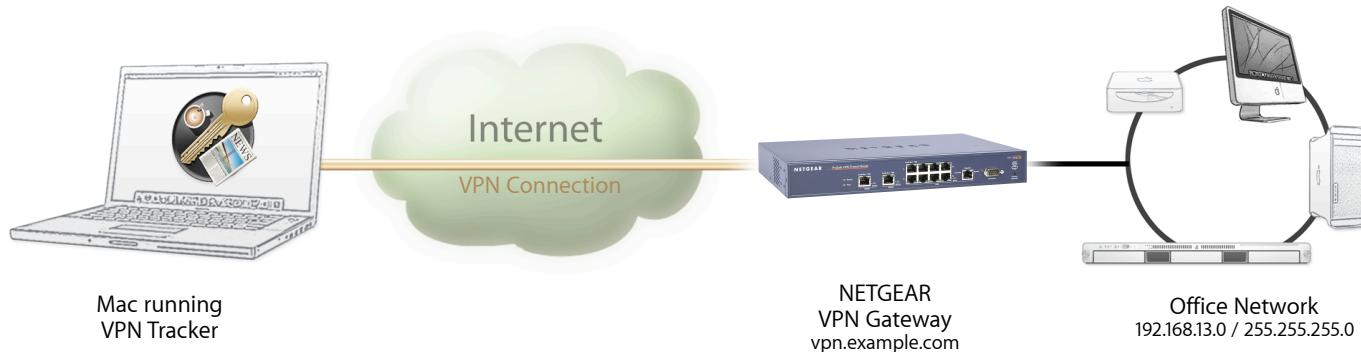
- ▶ VPN Tracker runs on Mac OS X 10.4, 10.5 and 10.6
- ▶ The configuration described in this guide requires VPN Tracker 6. Make sure to use a recent VPN Tracker version. The latest VPN Tracker release can be obtained from <http://www.vpntracker.com>
- ▶ You will need one VPN Tracker license for each Mac running VPN Tracker

¹ Using firmware 2.1.2 or higher. FVG318 devices do not support Mode Config and Extended Authentication (XAUTH).

² Using firmware 1.0.16.0 or higher.

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 NETGEAR firewall (the "VPN Gateway") is also already connected to the Internet and can be accessed through a static IP address or a (Dynamic) DNS host name. In our example setup, we will be using a host name: `vpn.example.com`.

The NETGEAR device has a second network interface which is connected to the internal office network (LAN). In our example, the office network has the IP range `192.168.13.0/24` (which is the same as `192.168.13.0/255.255.255.0`). This is the network that will be accessed from the employee's Mac through the VPN. It is called the "Remote Network" in VPN Tracker.

Terminology

A VPN connection is often called a “tunnel” (or “VPN tunnel”). Every VPN tunnel is established between two “endpoints”. In our example one endpoint is VPN Tracker and the other endpoint is the VPN gateway.

Please note that for each endpoint, the settings on the other endpoint are considered to be “remote”, while its own settings are considered to be “local”. That means a “local” setting from VPN Tracker’s perspective, is a “remote” setting from the VPN gateway’s perspective, and vice versa.

The sample configuration described in this guide is called a “Host to Network” configuration: A single computer, called a “Host” establishes a VPN tunnel to an entire “Network” behind the VPN gateway.

My NETGEAR Configuration

Throughout this guide, there are certain pieces of information that are needed later on for configuring VPN Tracker. This information is marked with red numbers to make it easier to reference it later. You can print out this form to help keep track of the various configuration settings of your NETGEAR device.

① Pre-Shared Key: _____

② NETGEAR's Remote Identifier: _____

③ NETGEAR's Local Identifier: _____

④ WAN IP Address: _____ . _____ . _____ . _____ (or DNS host name _____)

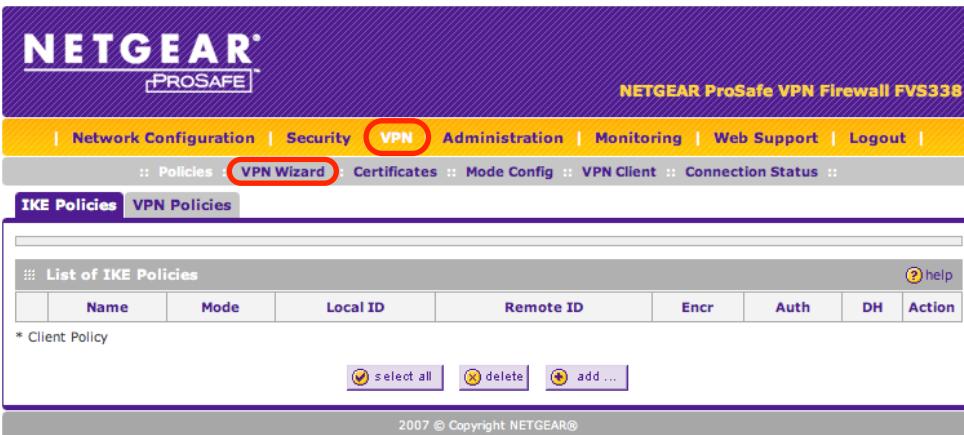
⑤ LAN Network Address: _____ . _____ . _____ . _____ / _____ . _____ . _____ . _____ (Start IP Address / Subnet Mask)

Task 1 – Configure your NETGEAR

This section describes how to set up your NETGEAR's VPN. If you do not yet have VPN configured and in use on your device, please proceed exactly as described in this section.

Advanced Users If you already have VPN in use on your device, you can skip ahead to Step 3 – 5 to verify your settings.

Step 1 – Start the VPN Wizard



The screenshot shows the NETGEAR ProSafe VPN Firewall FVS338 administration interface. The top navigation bar includes links for Network Configuration, Security, **VPN**, Administration, Monitoring, Web Support, and Logout. Below the navigation bar, there are links for Policies, **VPN Wizard**, Certificates, Mode Config, VPN Client, and Connection Status. The main content area displays a table titled "List of IKE Policies" with columns for Name, Mode, Local ID, Remote ID, Encr, Auth, DH, and Action. A note at the bottom left says "* Client Policy". At the bottom are buttons for select all, delete, and add ...

- ▶ Access your NETGEAR's administration interface
- ▶ Go to the “**VPN**” section
- ▶ If there is an “**IPsec VPN**” subsection on your device, go to “**IPsec VPN**”
- ▶ Click “**VPN Wizard**”

Note Make sure you have a current backup of your NETGEAR's configuration before making any changes.

Step 2 – Configure the VPN

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the [Policies](#) menu.

This VPN tunnel will connect to the following peers:

Gateway VPN Client

Connection Name and Remote IP Type

What is the new Connection Name? 1

What is the pre-shared key? 1 (Key Length 8 - 49 Char)

End Point Information

What is the Remote Identifier Information? 2

What is the Local Identifier Information? 3

Secure Connection Remote Accessibility

What is the remote LAN IP Address? . . .

What is the remote LAN Subnet Mask? . . .

Apply **Reset**

- ▶ **This VPN tunnel will connect to the following peers:** Select “VPN Client”
- ▶ **Connection Name:** Enter a name for the connection
- ▶ **Pre-Shared Key:** Enter a password for the connection ①
- ▶ **Remote Identifier:** Leave the identifier chosen by the VPN Wizard, or enter a different identifier. ②

Note Depending on your device and firmware revision, the identifiers chosen by the VPN Wizard may be slightly different, such as fvs_remote.com/fvs_local.com. Make sure to write down the **exact** identifiers.

- ▶ **Local Identifier Information:** Leave the identifier chosen by the VPN Wizard, or enter a different identifier. ③
- ▶ Click “Apply”

Tip Use the form on page 9 of this document to keep track of the various settings that you will configure.

Step 3 – Retrieve your NETGEAR’s WAN Configuration

The screenshot shows the 'Router Status' interface with the following details:

- System Info:**
 - System Name: FVX538
 - Firmware Version (Primary): 3.0.3-13
 - Firmware Version (Secondary): 2.0.0-139
- LAN Port:** MAC Address, IP Address, IP Subnet
- WAN1 Configuration:**
 - WAN Mode: Single Port
 - WAN State: UP
 - NAT: Enabled
 - Connection Type: Static IP
 - Connection State: Connected
 - IP Address: 194.145.236.2 (highlighted with a red oval containing the number 4)
 - Subnet Mask: 255.255.255.0
 - Gateway: 194.145.236.1
 - Primary DNS: 194.145.236.1
 - Secondary DNS: 0.0.0.0
 - MAC Address: 00:0f:b5:00:00:00
- WAN2 Configuration:** (partially visible)

- ▶ Go to “**Monitoring > Router Status**”
- ▶ Write down your NETGEAR’s **WAN IP Address** **4**
- ▶ If you use Dynamic DNS for your device, or if it has a DNS host name, **write down the host name instead**

Step 4 – Check the Settings for the VPN Policy

The screenshot shows a table with columns: !, Name, Type, Local, Remote, Auth, Encr, and Actions. A red circle highlights the 'Actions' column header. Below the table are buttons: select all, delete, enable, disable, and add ...

!	Name	Type	Local	Remote	Auth	Encr	Actions
	vpntracker*	Auto Policy	192.168.13.0/255.255.255.0	Any	SHA-1	3DES	

The 'General' tab settings include:

- Policy Name: vpntracker
- Policy Type: Auto Policy
- Remote Endpoint: FQDN: fvx_remote.com
- Enable NetBIOS? (unchecked)
- Enable Keepalive: No
- Ping IP Address: 0.0.0.0
- Detection period: 10 (Seconds)
- Reconnect after failure count: 3

The 'Traffic Selection' tab settings include:

Local IP: Subnet	5	Remote IP: Any
Start IP Address: 192.168.13.0		End IP Address: 0.0.0.0
Subnet Mask: 255.255.255.0		Subnet Mask: 0.0.0.0

- ▶ Go to “VPN > Policies”
- ▶ Make sure the “VPN Policies” tab is selected
- ▶ Click “Edit” for the VPN policy

- ▶ The settings should be exactly as shown here, with the following exceptions:
 - ▶ **Policy Name:** The policy name will be whatever you have entered earlier for the connection name
 - ▶ **Remote Endpoint:** The “Remote Endpoint” may differ, depending on the remote identifier chosen earlier by you or the VPN Wizard.
 - ▶ **Traffic Selection:** The local part of the traffic selection section is automatically configured by the VPN Wizard to reflect your NETGEAR’s LAN configuration. Therefore, this setting will be different if your NETGEAR uses a local network other than 192.168.13.0/255.255.255.0. Write down this information, as you will need it later ⑤

Advanced Users The following pages show the settings as created by the NETGEAR VPN Wizard. The device profiles in VPN Tracker are designed to match these settings. If your settings differ here, and you cannot change them, please refer to the chapter “VPN Settings Explained” for a detailed discussion of the various settings.

Manual Policy Parameters

SPI-Incoming:	<input type="text"/>	(Hex, 3-8 Chars)
Encryption Algorithm:	<input type="button" value="3DES"/>	
Key-In:	<input type="text"/>	
Key-Out:	<input type="text"/>	(DES-8 Char & 3DES-24 Char)

SPI-Outgoing:

<input type="text"/>	(Hex, 3-8 Chars)	
Integrity Algorithm:	<input type="button" value="SHA-1"/>	
Key-In:	<input type="text"/>	
Key-Out:	<input type="text"/>	(MD5-16 Char & SHA-1-20 Char)

Auto Policy Parameters

SA Lifetime:	<input type="text" value="3600"/>	<input type="button" value="Seconds"/>	
Encryption Algorithm:	<input type="button" value="3DES"/>	Integrity Algorithm:	<input type="button" value="SHA-1"/>
<input checked="" type="checkbox"/> PFS Key Group: <input type="button" value="DH Group 2 (1024 bit)"/>			
Select IKE Policy:	<input type="button" value="vpntracker"/>	<input type="button" value="view selected"/>	

- If all settings match, you are ready to check the IKE Policy

Note If your device has multiple WAN interfaces, there may be more settings available. These settings should be left as configured by the VPN Wizard.

Step 5 – Check the Settings for the IKE Policy

The screenshot shows the 'IKE Policies' tab selected in a software interface. A table lists an IKE policy named 'vpntracker*' with settings: Mode: Aggressive, Local ID: fvx_local.com, Remote ID: fvx_remote.com, Encr: 3DES, Auth: SHA-1, DH: Group 2 (1024 bit). An 'edit' button is circled in red. Below the table are sections for Mode Config Record, General settings, Local and Remote identifiers, IKE SA Parameters, and Extended Authentication.

Name	Mode	Local ID	Remote ID	Encr	Auth	DH
vpntracker*	Aggressive	fvx_local.com	fvx_remote.com	3DES	SHA-1	Group 2 (1024 bit)

IKE Policies **VPN Policies**

List of IKE Policies

* Client Policy

Mode Config Record

Do you want to use Mode Config Record?

Policy Name: vpntracker

Direction / Type: Responder

Exchange Mode: Aggressive

General

Select Mode Config Record: vpntracker

Local

Select Local Gateway: WAN1

Identifier Type: FQDN

Identifier: fvx_local.com

Remote

Identifier Type: FQDN

Identifier: fvx_remote.com

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: Pre-shared key

Pre-shared key: topsecret

Diffie-Hellman (DH) Group: Group 2 (1024 bit)

SA-Lifetime (sec): 28800

Enable Dead Peer Detection: No

Detection Period: 10 (Seconds)

Reconnect after failure count: 3

Extended Authentication

XAUTH Configuration: None

Authentication Type: User Database

Username:

Password:

► Select the “IKE Policies” tab

► Click “Edit” for the IKE policy

► The settings should be exactly as shown here, with the following exceptions:

► **Policy Name:** The policy name will be whatever you have entered for the connection name earlier

► **Local / Remote Identifier:** The identifier will be whatever you configured in the VPN Wizard (or what was pre-filled by the VPN Wizard)

► **Pre-shared key:** The pre-shared key will be the pre-shared key you have entered earlier

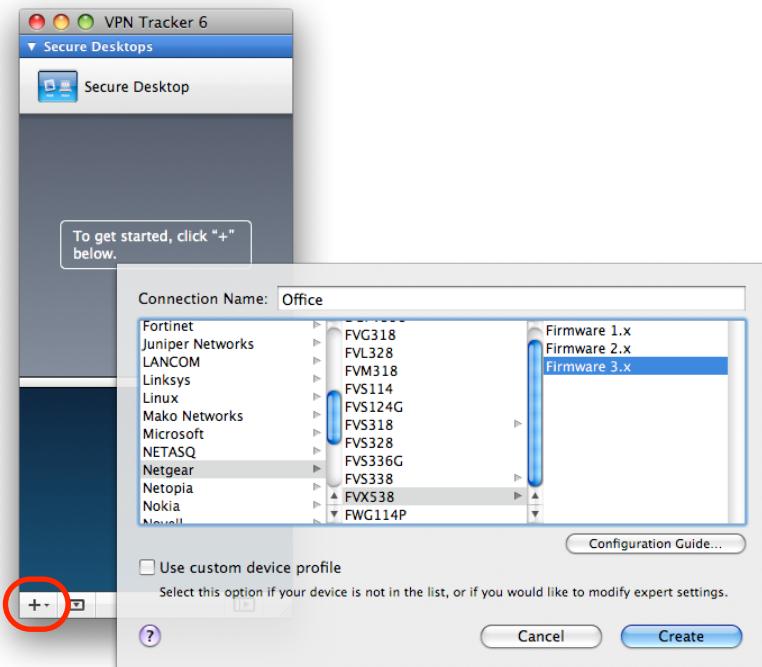
► If all settings match, you are ready to test the connection.

Note If you need to make any changes to the IKE policy, make sure to disable the VPN policy first: you will not be able to make changes to the IKE policy as long as the associated VPN policy is enabled.

Task 2 – Configure VPN Tracker

This section describes how to configure VPN Tracker to connect to your NETGEAR. You will need the configuration information you collected during Task 1. If you are missing any information, please refer back to steps 3 to 5 of “Task 1 – Configure your NETGEAR”.

Step 1 – Create a New Connection

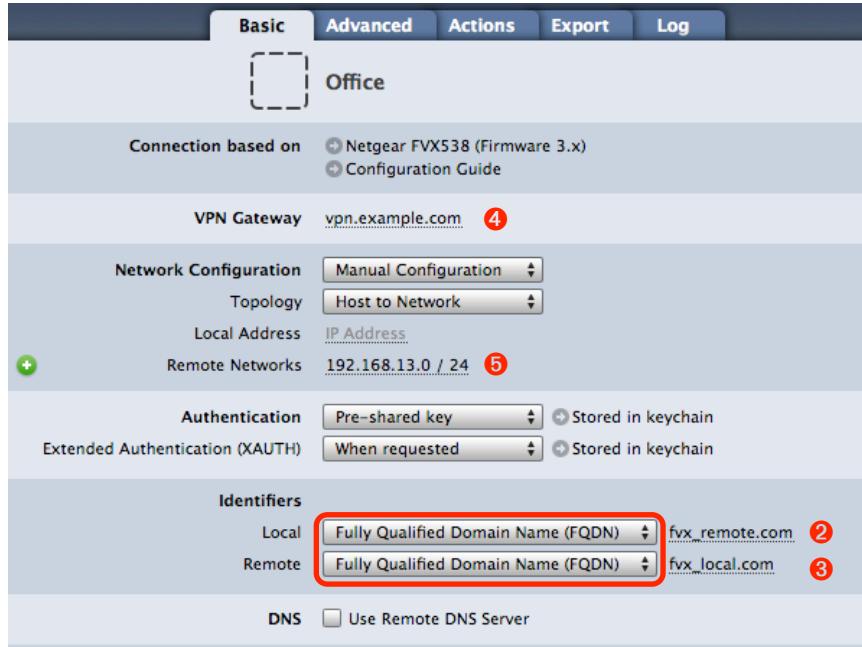


- ▶ Start VPN Tracker
- ▶ Click the “+” button in the main window

You will be asked to select a device profile for the new connection:

- ▶ Select “Netgear” from the list
- ▶ Select your device from the list of NETGEAR devices
- ▶ If your device has more than one firmware revision available, be sure to select the revision matching the firmware installed on the device
- ▶ **Connection Name:** Choose a name for your connection (e.g. “Office”)
- ▶ Click “OK”

Step 2 – Configure the VPN Connection



- ▶ **VPN Gateway:** Enter your NETGEAR's public IP address or its host name (in this example, we are using the host name "vpn.example.com")
- ▶ **Local Address:** Leave empty for now. Depending on your setup, you may have to set a specific Local Address eventually. Refer to "Supporting Multiple Users" and "The Role of the Local Address in VPN Tracker" for details and how to choose the address
- ▶ **Remote Networks:** Enter the network address of the network that is being accessed through the VPN tunnel
⑤. Separate the subnet mask with a forward slash ("/")
- ▶ **Identifiers**
 - ▶ Make sure the types for both identifiers are set to "**Fully Qualified Domain Name (FQDN)**"
 - ▶ **Local:** Enter the **remote** identifier from your NETGEAR (e.g. fvx_remote.com) ②
 - ▶ **Remote:** Enter the **local** identifier from your NETGEAR (e.g. fvx_local.com) ③

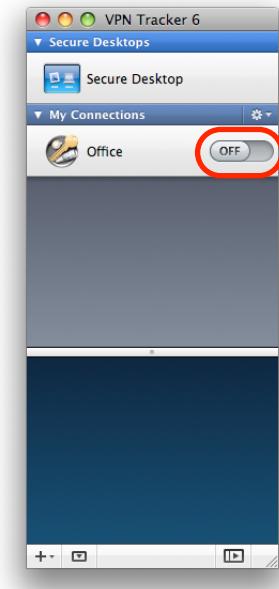
Task 3 – Test the VPN Connection

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

It's time to go out!

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

Start your connection



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

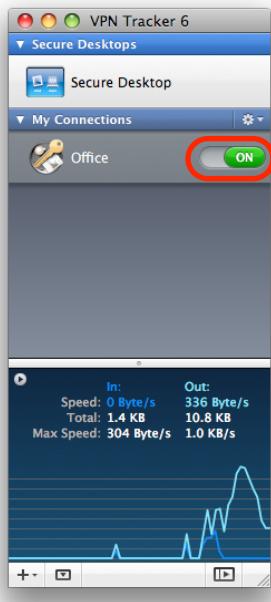
When you are prompted for your pre-shared key:



- ▶ **Pre-shared key:** Enter the pre-shared key that you configured on the NETGEAR device **1**

- ▶ 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

- ▶ Click “OK”



- ▶ If the slider goes back to **Off** after starting the connection, or after entering your pre-shared key or your XAUTH credentials, please read the **Troubleshooting** section of this document
- ▶ If the slider goes to **On** and turns green after a while, you have successfully established a connection

Congratulations!

Supporting Multiple Users

Once your VPN expands to multiple users, you will likely want to issue them individual logins, and you must ensure that IP addresses do not conflict. In addition to these purely technical considerations, VPN Tracker makes it easy to distribute pre-configured connections to your users, and prevent the modification of VPN connections and access to confidential data.

Note When multiple users use the same VPN connection, it is very important that a different Local Address is used for each VPN client. The easiest way to ensure this is Mode Config. Setting up Mode Config is described later in this chapter. If you cannot use Mode Config, please refer to "The Role of the Local Address in VPN Tracker" for alternative solutions.

Individual User Logins with Extended Authentication (XAUTH)

Once your VPN expands to multiple users, you may want to issue them each an individual user name and password to access the VPN connection, in addition to the pre-shared key that is shared among all users of a VPN connection. **This feature is not available on FVG318 devices.**

Add XAUTH Users (devices without a dedicated "Users" section)

User Name	Action
bob	[Edit]

Add New User:

User Name	Password	Confirm Password	Add
bob	(5) [Redacted]	(6) [Redacted]	[Add] (Red circle)

- ▶ Go to the "**VPN > VPN Client**" section
- ▶ Enter a user name for the new user **5**
- ▶ Enter a password for the new user **6**
- ▶ Confirm the password for the new user
- ▶ Click "Add"

Add XAUTH Users (devices with a separate “Users” section)

The screenshot shows the 'Add User' page. The 'User Name' field is filled with 'bob' (step 5). The 'User Type' dropdown is set to 'IPSEC VPN User' (step 4). The 'Select Group' dropdown is set to 'geardomain' (step 5). The 'Password' and 'Confirm Password' fields both contain '*****' (step 6). The 'Idle Timeout' is set to '10 Minutes'. The 'User' menu item is highlighted with a red circle.

- ▶ Go to the “**Users > Users**” section
- ▶ Click “Add...”
- ▶ **User Type:** Select “**IPSEC VPN User**”
- ▶ Enter a user name for the new user **⑥**
- ▶ Enter a password for the new user **⑥**
- ▶ Confirm the password for the new user
- ▶ Click “Add”

Tip You can add more users later using the same procedure.

Temporarily Disable the VPN Policy

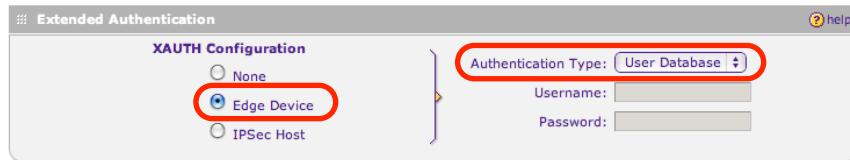
List of VPN Policies							
!	Name	Type	Local	Remote	Auth	Encr	Action
<input checked="" type="checkbox"/>	vpntracker*	Auto Policy	192.168.13.0/255.255.255.0	Any	SHA-1	3DES	

The screenshot shows the 'List of VPN Policies' table. A checkmark is placed in the 'Action' column of the row for 'vpntracker*' (step 1). The 'disable' button in the toolbar is circled in red (step 2).

In order to make changes to the IKE policy, you will first have to disable the associated VPN policy.

- ▶ Place a check mark at the row containing the VPN policy to select it
- ▶ Click “Disable”

Configure the IKE Policy to use Extended Authentication (XAUTH)



- ▶ Edit your **IKE Policy** and scroll to the “**Extended Authentication**” section

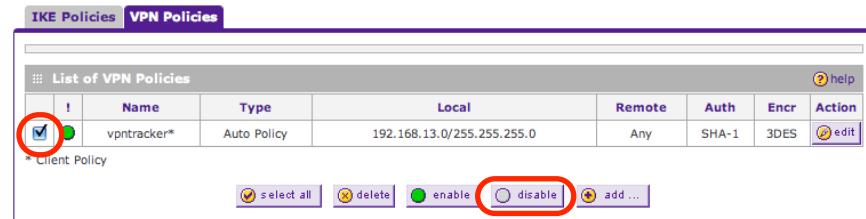
▶ **XAUTH Configuration:** Select “**Edge Device**”

▶ **Authentication Type:** Select “**User Database**”

▶ Click “**Apply**”

Advanced Users It is possible to obtain the user names and passwords from an external RADIUS server: Set the “Authentication Type” in the Extended Authentication section of the IKE policy to one of the RADIUS options, and configure your RADIUS server under VPN > VPN Client > RADIUS Client.

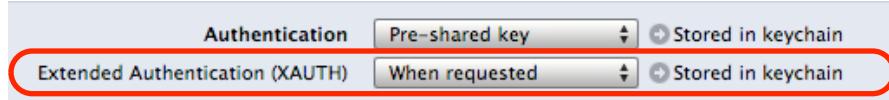
Re-Enable the VPN Policy



- ▶ Place a check mark at the row containing the VPN policy in order to select it

▶ Click “**Enable**”

Check the VPN Tracker Settings



- ▶ Make sure that “**Use Extended Authentication (XAUTH)**” is checked

Start the Connection



- ▶ After starting the connection, you will be asked for your XAUTH credentials
- ▶ **User Name:** Enter the name of a user configured on the NETGEAR **5**
- ▶ **Password:** Enter the password for this user **6**
- ▶ Optionally, check the box “**Store in Keychain**” to save the user name and password in your keychain so you are not asked for it again when connecting the next time
- ▶ Click “OK”

Using Mode Config for IP Address Assignment

When multiple users use the same VPN connection, it is very important that a different IP address is used for each VPN client. The easiest way to ensure this, is to automatically have the NETGEAR assign IP addresses to connecting clients through Mode Config. **This feature is not available on FVG318 devices** (see “The Role of the Local Address in VPN Tracker” for alternative solutions).

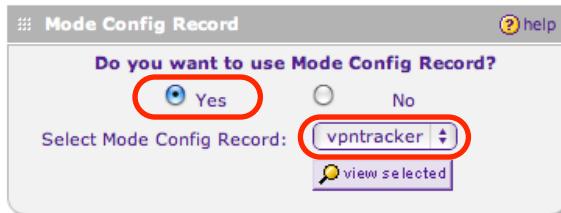
Creating an Address Pool for Mode Config

The figure consists of three screenshots of the NETGEAR device's web-based configuration interface:

- Screenshot 1: Mode Config - List of Mode Config Records**
 - Shows a table with columns: Record Name, Pool Start IP, Pool End IP, and Action.
 - Buttons at the bottom include "select all", "delete", and "add ...". The "add ..." button is circled in red.
- Screenshot 2: Client Pool**
 - Shows fields for "Record Name" (set to "vpntracker").
 - Shows "First Pool" settings: Starting IP 10.13.123.100, Ending IP 10.13.123.199. This range is circled in red.
 - Shows "Second Pool", "Third Pool", "WINS Server", and "DNS Server" fields, each with Primary and Secondary IP ranges. These fields are also circled in red.
- Screenshot 3: Traffic Tunnel Security Level**
 - Shows "PFS Key Group" set to "DH Group 2 (1024 bit)" (with a checked checkbox). This entire section is circled in red.
 - Shows "SA Lifetime" (3600 seconds), "Encryption Algorithm" (3DES), "Integrity Algorithm" (SHA-1), "Local IP Address" (0.0.0.0), and "Local Subnet Mask" (0.0.0.0).

- ▶ Go to the “**VPN > Mode Config**” section
- ▶ If there is an “**IPsec VPN**” subsection on your device, go to **VPN > IPsec VPN > Mode Config** instead
- ▶ Click “Add”
- ▶ **Record Name:** Enter a name that will later allow you to recognize this Mode Config Record
- ▶ **First Pool:** Enter an IP range that is **not** part of your NETGEAR’s LAN. It is a good idea to use an IP range from the private ([RFC1918](#)) IP address space, and to make the range large enough to support at least the maximum number of simultaneous connections expected
- ▶ **DNS Server** (optional): If you operate your own DNS server, enter it here. Otherwise, leave 0.0.0.0
- ▶ **Traffic Tunnel Security Level:** These settings correspond to the VPN Policy settings used for non-Mode Config connections. We recommend you use the default values here.

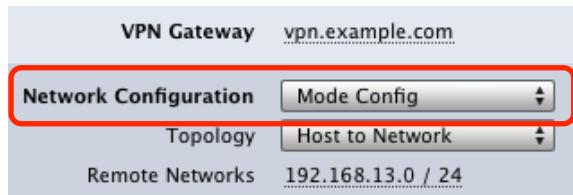
Configure the IKE Policy to use Mode Config



- ▶ Edit your **IKE Policy**
- ▶ In the “**Mode Config Record**” section, turn on Mode Config by clicking “**Yes**”
- ▶ Make sure the record you created earlier (in our example, “vpntracker”) is selected
- ▶ Click “**Apply**”

Tip Once your IKE Policy is properly set up for Mode Config, a VPN Policy is no longer needed for this connection and can be disabled or deleted.

Enable Mode Config in VPN Tracker



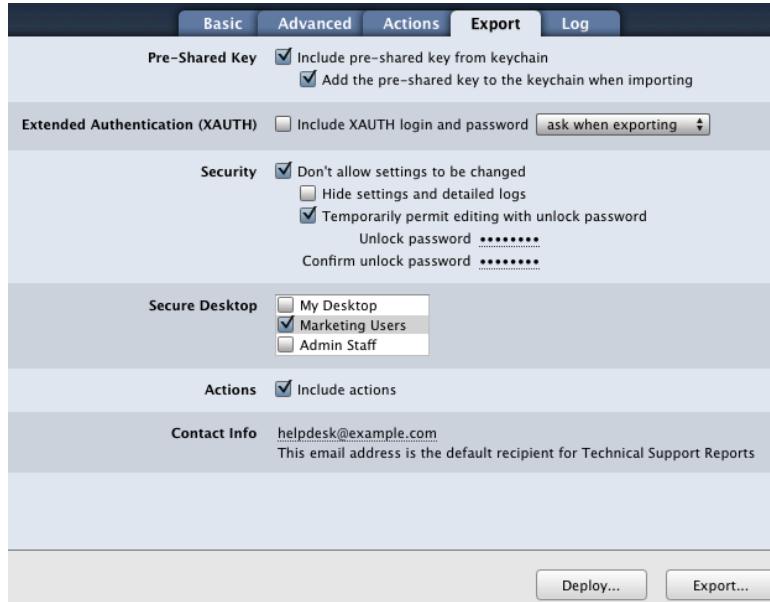
- ▶ On the Basic tab in VPN Tracker, switch “**Network Configuration**” to “**Mode Config**”. If you cannot find this setting for your device, make sure you have selected the correct device and firmware revision

Advanced Users It is very important to initially set up Mode Config as “automatic” instead of “active” or “passive”. While this may mean a short delay when connecting (if the device actually requires “active” mode config), it will ensure that it works in both cases. You can later try passive or active to see which mode your device and particular firmware revision actually uses

Deploying VPN Connections to Your Users

VPN Tracker Professional Edition offers a number of ways to easily distribute pre-configured connections to users. It is even possible to create a custom VPN Tracker application that contains a pre-configured connection and a license voucher for your users.

Further information on deploying connections to users is available in the VPN Tracker manual.



Tip To deploy VPN Tracker to many users, you can create a custom VPN Tracker application with a pre-configured connection and a license voucher. Simply click "Deploy..." to get started.

Troubleshooting

In most cases, your connection should work fine if you follow the instructions above. If you cannot connect, please read on.

VPN Connection Fails to Establish

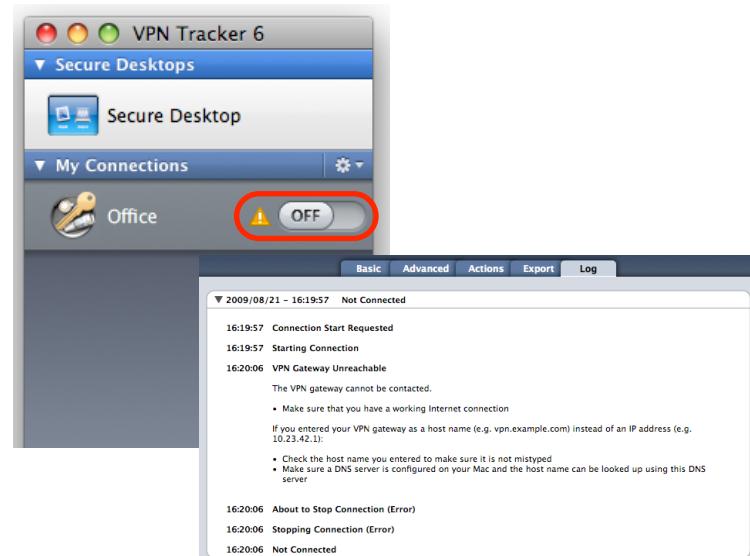
On/Off Slider goes back to “Off” right away

If the slider goes back to “Off” right away, please make sure you have entered all the required information. VPN Tracker will highlight fields that are missing or obviously incorrect information.

On/Off Slider goes back to “Off” after a while

If the connection ON/OFF slider goes back to “OFF” a while after attempting to start the connection, please go to the “Log” tab to get more information about the error (or click the warning triangle to be automatically taken to the “Log” tab).

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.

Test VPN Availability again

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

VPN Tracker automatically runs a test to detect the proper method for your particular Internet connection when you first connect using this Internet connection. However, test results could become outdated by changes to the local router, so it is a good idea to test again if there are problems.

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

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

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

Further Questions?

You can find the latest news and compatibility information on our support and FAQ website:

<http://www.equinux.com/support>

If you need to contact equinux Technical Support

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

- ▶ The manufacturer and model and firmware revision of the VPN gateway
- ▶ A Technical Support Report from VPN Tracker (Help > Generate Technical Support Report)
- ▶ Screenshots of what you have configured on your VPN gateway, in particular all VPN settings
- ▶ A detailed description of the problem and the troubleshooting steps you have taken

VPN Settings Explained

This section explains the various settings found on your NETGEAR, and how they relate to VPN Tracker's settings. We will first go through the IKE policy settings from left to right, and from top to bottom, then through the VPN policy settings. In the end, a few selected VPN Tracker settings that have no matching setting on the NETGEAR, or are found elsewhere, are explained.

IKE Policy

The IKE Policy contains the settings for the first phase in the process of establishing a VPN connection. **Most of the settings here correspond to settings located in VPN Tracker on the Basic tab, or under Advanced > Phase 1.**

Mode Config Record



Mode Config is a way to automatically distribute IP addresses to VPN clients. If Mode Config is to be used, it must be enabled on the NETGEAR, as well as in VPN Tracker (Basic > Automatic Configuration). See the chapter "Supporting Multiple Users" for more information about Mode Config. **Mode Config is not available on FVG318 devices.**

General



Policy Name: The policy name is used only for naming connections on the device.

Direction / Type: Must be "**Responder**" for VPN clients to be able to connect.

Exchange Mode: Always use "**Aggressive**" Mode if VPN clients connect from dynamic IP addresses. The Exchange Mode configured here must match the Advanced > Exchange Mode setting in VPN Tracker. If you must for some reason use Main Mode here, please refer to your device's documentation for any prerequisites for using Main Mode.

Local and Remote Identifier

Local
Select Local Gateway: WAN1 WAN2
Identifier Type: FQDN
Identifier: fvx_local.com

Select Local Gateway: (only if the device has more than one WAN interface): The WAN interface that is used if the identifier type is "Local WAN IP"

Local Identifier Type: The local identifier's type on the device must match the **Remote Identifier Type** (Basic > Identifiers) in VPN Tracker.

Local Identifier: The local identifier on the device must match the **Remote Identifier** (Basic > Identifiers) in VPN Tracker.

Remote
Identifier Type : FQDN
Identifier: fvx_remote.com

Remote Identifier Type: The remote identifier's type on the device must match the **Local Identifier Type** (Basic > Identifiers) in VPN Tracker.

Remote Identifier: The remote identifier on the device must match the **Local Identifier** (Basic > Identifiers) in VPN Tracker.

IKE SA Parameters

IKE SA Parameters
Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Authentication Method: Pre-shared key RSA-Signature
Pre-shared key: topsecret (Key Length 8 - 49 Char)
Diffie-Hellman (DH) Group: Group 2 (1024 bit)
SA-Lifetime (sec): 28800
Enable Dead Peer Detection: Yes No
Detection Period: 10 (Seconds)
Reconnect after failure count: 3

Encryption Algorithm: The encryption algorithm here must match the encryption algorithm configured in VPN Tracker in Advanced > Phase 1 > Encryption Algorithms. The device uses 3DES by default, which is generally a good choice. AES-128/192/256 are considered to be even more secure (AES-192/AES-256 are only available in the Professional Edition of VPN Tracker).

Note While it is possible to set more than one encryption algorithm in VPN Tracker (as long as the one actually used by the device is among them), setting more than two or three algorithms (or algorithms not known to the device) may cause the connection to fail

Authentication Algorithm: The authentication algorithm here must match the hash algorithm configured in VPN Tracker (Advanced > Phase 1 > Hash Algorithms). It is ok to check both algorithms (MD5 and SHA-1) in VPN Tracker.

Authentication Method: Unless you already have a Public-Key Infrastructure (PKI) in place for your users, you will probably want to start out using pre-shared key (i.e. password-based) authentication. The method must match Basic > Authentication in VPN Tracker.

Pre-shared key: This is the password for the VPN connection, and corresponds to the same setting in VPN Tracker (Basic > Authentication). This password is shared among all users. Make sure to choose a good password here that is long enough and contains a mix of letters and numbers (but be aware that your Mac and your Netgear may not use the same character encoding, so try to avoid accented characters). To require a user name and password for each user, in addition to the pre-shared key, it is possible to use Extended Authentication (XAUTH). The chapter "Supporting Multiple Users" has more information on using XAUTH.

Diffie-Hellman (DH) Group: The Diffie-Hellman (DH) group defined here must match the group selected for phase 1 in VPN Tracker (Advanced > Phase 1 > Diffie-Hellman). Using a longer key (= higher number) is more secure, but may also be slower.

SA Lifetime: The IKE SA lifetime indicates when the phase 1 of the connection needs to be re-established. The lifetime must match the lifetime for phase 1 in VPN Tracker (Advanced > Phase 1 > Lifetime). A value of 28800 sec (8 hours) is generally a good choice. It is not recommended to set the lifetime lower than 3600 sec (1 hour).

Dead Peer Detection (DPD): A mechanism to detect if the peer on the other side of the VPN connection is no longer responding. VPN Tracker 6 supports Dead Peer Detection, so you can enable it if you wish.

Extended Authentication (XAUTH)



XAUTH Configuration: When XAUTH is used, individual user names and passwords are required, in addition to the pre-shared key. **XAUTH is not available on FVG318 devices.**

- ▶ To use a pre-shared key only, leave XAUTH turned off.
- ▶ To use XAUTH, set XAUTH Configuration to "Edge Device"

The VPN Tracker configuration is independent of the XAUTH setting: On the Basic tab, set Extended Authentication (XAUTH) to "When requested" to automatically use XAUTH if it is configured on the NETGEAR:

The **Authentication Type** determines where XAUTH user names and passwords are taken from – either from the device's user database (VPN > VPN Client > User Database) or from an external RADIUS server (VPN > VPN Client > RADIUS Client).

VPN Policy

The VPN Policy contains the settings for the second phase in the process of establishing a VPN connection. **Most of the settings here correspond to settings located in VPN Tracker in the Network section of the Basic tab, or in Advanced > Phase 2.**

General

Policy Name: The policy name is used only for naming connections on the device.

Policy Type: The policy type must always be "Auto Policy".

Select Local Gateway (only if the device has more than one WAN interface): This is the interface that the device expects incoming VPN connections to arrive on. The IP address (or corresponding host name) of this interface is the **VPN Gateway** address in VPN Tracker.

Remote Endpoint: This is the (public) IP address of the connecting client. With clients connecting from dynamic IP addresses, it should be set to **FQDN**. Enter the same FQDN that is used for the Remote Identifier in the IKE Policy.

Enable NetBIOS: This setting has no effect on the VPN Tracker configuration.

Enable RollOver (only if the device has more than one WAN interface): If enabled, VPN connections will be possible to the secondary WAN interface if RollOver (fail-over) occurs.

Enable Keepalive: Keepalive should be turned off for a setup where a client is connecting to the NETGEAR.

Traffic Selection

The Traffic Selection settings determine the endpoints of the VPN tunnel.

- ▶ If you are using the **VPN Wizard** on the device, it will automatically fill in the correct values.
- ▶ If you are setting up your configuration manually, the **local** (=NETGEAR) side of the tunnel needs to be configured to be a subnet matching the NETGEAR's LAN (192.168.13.0/255.255.255.0 is the NETGEAR's LAN in our example)
- ▶ The **remote** part should be set to "Any"



Advanced Users If you are not setting the remote part of the Traffic Selection to "Any", it must match exactly what is configured in VPN Tracker as the Local Address (or Local Network, if using a Network to Network connection). Range type addresses are not supported in VPN Tracker.

Manual Policy Parameters

An Auto Policy does not use Manual Policy Parameters. This section should always be disabled (if it is not, make sure you have set up this VPN policy as an "Auto Policy" in the "General" section).

Manual Policy Parameters

SPI-Incoming:	(Hex, 3-8 Chars)	SPI-Outgoing:	(Hex, 3-8 Chars)
Encryption Algorithm:	3DES	Integrity Algorithm:	SHA-1
Key-In:		Key-In:	
Key-Out:		Key-Out:	
(DES-8 Char & 3DES-24 Char)		(MD5-16 Char & SHA-1-20 Char)	

Auto Policy Parameters

Auto Policy Parameters

SA Lifetime:	3600	Seconds	
Encryption Algorithm:	3DES	Integrity Algorithm:	SHA-1
<input checked="" type="checkbox"/> PFS Key Group: DH Group 2 (1024 bit)			
Select IKE Policy:	vpntracker	view selected	

SA Lifetime: The lifetime determines how long a client can be connected before the encryption keys must be renegotiated. The lifetime must match the lifetime for phase 2 in VPN Tracker (Advanced > Phase 2 > Lifetime). A value of 3600 sec (1 hour) is generally a good choice. It is not recommended to set the lifetime lower than 1 hour. Due to the complications involved with a lifetime that depends on data transfer amounts, we recommend to set the lifetime in "Seconds" (not in "KBytes").

Encryption Algorithm: The encryption algorithm selected here must match the encryption algorithm selected in VPN Tracker for phase 2. The device uses 3DES by default, which is generally a good choice. AES-128/192/256 are considered to be even more secure (AES-192/AES-256 are only available in the Professional Edition of VPN Tracker).

Note While it is possible to set more than one encryption algorithm in VPN Tracker (as long as the one used by the device is among them), setting more than two or three algorithms (or algorithms not known to the device) may cause the connection to fail

Integrity Algorithm: The algorithm selected here must match the selection in VPN Tracker for the Phase 2 Authentication Algorithm. NETGEAR uses SHA-1 by default (which corresponds to HMAC SHA-1 in VPN Tracker).

PFS Key Group: This setting must match the Perfect Forward Secrecy (PFS) setting in VPN Tracker (Advanced > Phase 2 > Perfect Forward Secrecy (PFS)). Using PFS is more secure. The selected group must match the PFS Diffie-Hellman (DH) group in VPN Tracker (Advanced > Phase 2 > Perfect Forward Secrecy (PFS)). Using a longer key (= higher number) is more secure, but may also be slower.

Select IKE Policy: Select the corresponding IKE Policy for the connection here (unless you are manually adding your policy the correct policy will already be selected).

The Role of the Local Address in VPN Tracker

The local address is the IP address that your Mac uses in the remote network when connected through VPN.

- ▶ If the Local Address field is left empty, the Mac's actual local IP address (as shown in System Preferences > Network) is used
- ▶ When Mode Config is used, the Local Address is assigned automatically by the VPN gateway

Advanced Users The Local Address is used as the endpoint of the IPsec Security Association (SA) on the VPN Tracker side that is established in phase 2 of the connection process.

When to Set the Local Address in VPN Tracker

If Mode Config is not being used, it is beneficial to use fixed Local Addresses in VPN Tracker, instead of leaving the Local Address field empty. **Always use a fixed Local Address if:**

- ▶ multiple clients (users/computers) use the VPN, and you cannot use Mode Config (see "Supporting Multiple Users")
- ▶ the NETGEAR device is not the default gateway (router) in the remote network

Choosing the Local Address

When connecting to a NETGEAR device, the Local Address **must not be part of the remote network** (i.e. the NETGEAR's LAN) and the **same Local Address may not be used by two VPN clients** at the same time. If there is only a single user of the VPN, this will often automatically be the case if the Local Address field is simply left empty, and VPN Tracker therefore uses the Macs local IP address. However, in all other circumstances, you should configure a specific address.

Example: The NETGEAR's LAN in this example is the network 192.168.13.0/24 (= 192.168.13.0/255.255.255.0). Choose an arbitrary [private network](#) that is not part of this network, such as 10.22.13.0/24, and manually assign each user of the VPN a different IP address from that network to be used as the Local Address in VPN Tracker.

User	IP Address
alice	10.22.13.1
bob	10.22.13.2
charlie	10.22.13.3
...	10.22.13._

Local Addresses for the More Curious

Why can't I use a Local Address from my NETGEAR's LAN?

It may sound a bit unusual to use IP addresses that are not part of the NETGEAR's LAN. The reason for this is that the NETGEAR cannot act as a so-called "ARP Proxy" for its VPN clients. Computers on the NETGEAR's LAN therefore must be "tricked" into sending replies for VPN clients to the NETGEAR by using IPs from outside the local network (for which replies are sent to the default gateway).

My users connect from different places, from different IPs. Why do I still need to give them different Local Addresses?

In most cases, the connecting Macs will be behind routers (DSL routers, wireless access points, ...) that perform Network Address Translation (NAT), meaning they map several [private IP addresses](#) onto a single public IP address. The Macs themselves will have such a private IP address for their Ethernet or AirPort interface, and this is the IP address that is used by VPN Tracker if the Local Address field is empty.

Because of this, the likelihood of two Macs using the same local address is very high: Many NAT routers are by default configured to use the same private networks (192.168.1.0/24 and 10.0.0.0/24 are popular choices), and therefore there is a good chance that two clients connecting from entirely different places will have the same local IP address assigned by their respective local router. Therefore it is essential to configure a different Local Address in VPN Tracker for each VPN user if multiple users connect concurrently.

Why do I have to set a fixed Local Address when my NETGEAR is not the default gateway (router) in its LAN?

If the NETGEAR is not the default gateway, this means that computers the VPN clients communicate with do not connect to the Internet through the NETGEAR.

In such an environment, you will have to ensure that those computers (and all other resources accessed through the VPN, such as printers and NAS drives) know where to send replies for VPN clients. This is much easier, if you know what IP addresses your VPN clients will be using, and therefore you should enter an individual fixed IP address in the Local Address field on each VPN client.

Once you have decided on a range of IP address to be used for VPN clients, you can either

- ▶ set a route to the NETGEAR for the VPN clients' IP addresses on each host that needs to communicate with VPN clients, or
- ▶ have the default gateway redirect all traffic for the VPN clients' IP addresses to the NETGEAR