



VPN Configuration Guide

NETGEAR® FVS336G / FVS338 / DGFV338 / FVX538 / FVG318

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.

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.

NETGEAR is a registered trademark of NETGEAR, Inc.

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
Important Prerequisites.....	6
Scenario.....	7
Terminology.....	8

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
Cannot Access Resources on the Remote Network.....	28
Further Questions?	29

VPN Settings Explained.....	30
IKE Policy.....	30
VPN Policy.....	33
The Role of the Local Address in VPN Tracker.....	33

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:

- ▶ FVS336G
- ▶ FVS338
- ▶ FVX538
- ▶ DGFV338
- ▶ FVG318¹

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

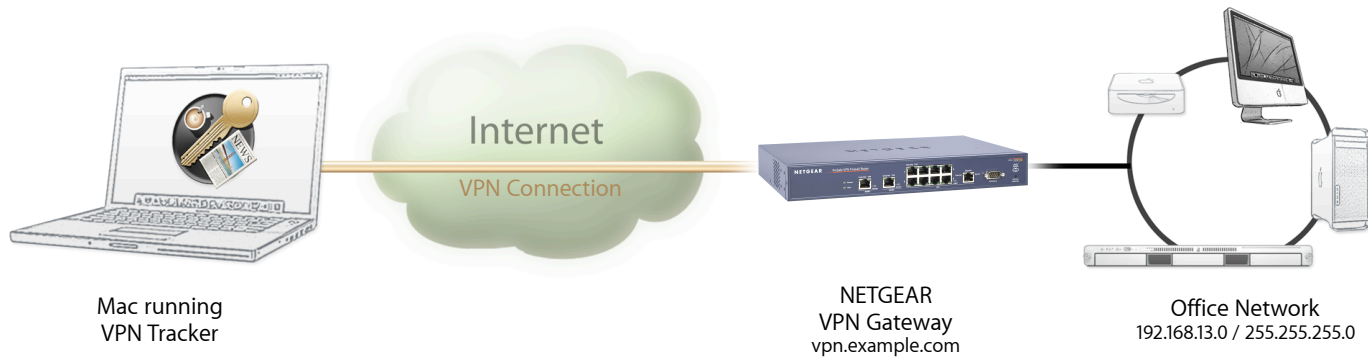
Your Mac

- ▶ VPN Tracker runs on Mac OS X 10.4 or 10.5
- ▶ The configuration described in this guide requires VPN Tracker 5.3 or higher. 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).

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.

❶ Pre-Shared Key: _____

❷ NETGEAR's Remote Identifier: _____

❸ NETGEAR's Local Identifier: _____

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

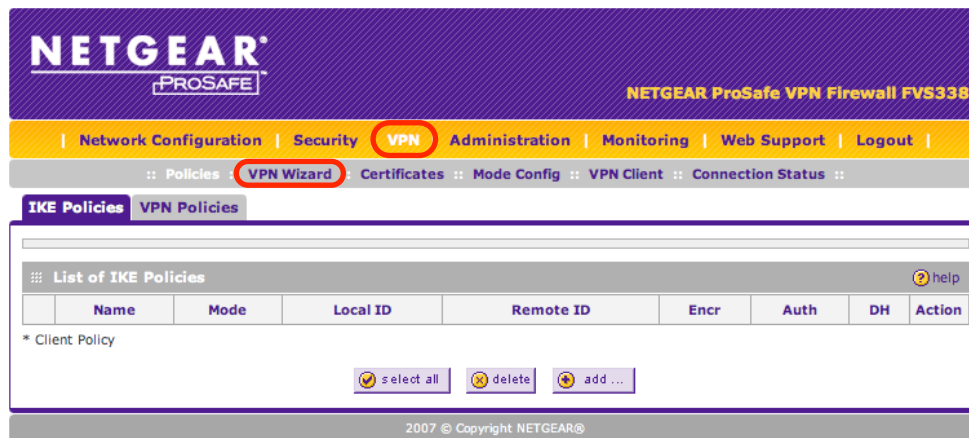
❺ LAN Network Address: _____ . _____ . _____ . _____ / _____ . _____ . _____ . _____ (Start IP Address / Subnet Mask)

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



- ▶ Access your NETGEAR's administration interface
- ▶ Go to the "VPN" section
 - ▶ FVS336G only: Go to the "IPsec VPN" section
- ▶ 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

About VPN Wizard help

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 help

What is the new Connection Name? vpntracker

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

End Point Information help

What is the Remote Identifier Information? fvx_remote.com

What is the Local Identifier Information? fvx_local.com

Secure Connection Remote Accessibility help

What is the remote LAN IP Address? . . .

What is the remote LAN Subnet Mask? . . .

Apply Reset

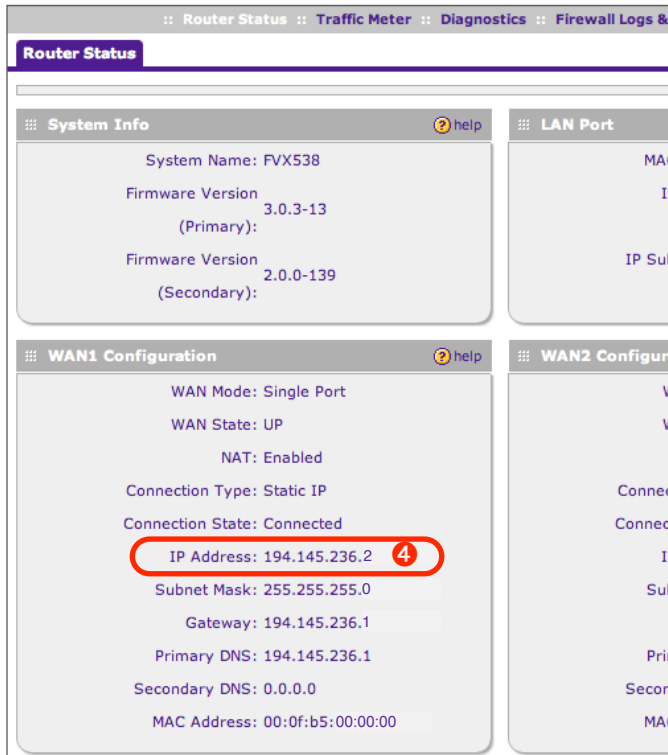
- ▶ This VPN tunnel will connect to the following peers: Select “VPN Client”
- ▶ **Connection Name:** Enter a name for the connection
- ▶ **Pre-Shared Key:** Enter a password for the connection ❶
- ▶ **Remote Identifier:** Leave the identifier chosen by the VPN Wizard, or enter a different identifier.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

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. ❸
- ▶ Click “Apply”

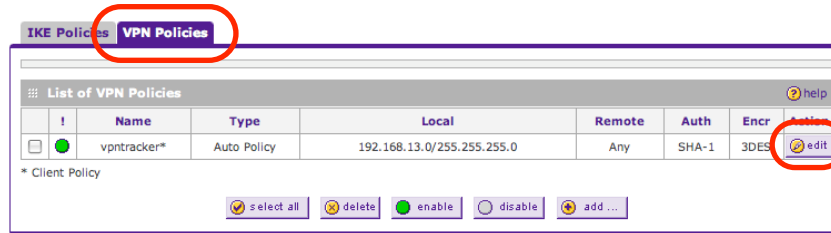
Tip Use the form on page 9 of this document to keep track of the various settings that you will configure.

Step 3 – Retrieve your NETGEAR's WAN Configuration



- ▶ 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**

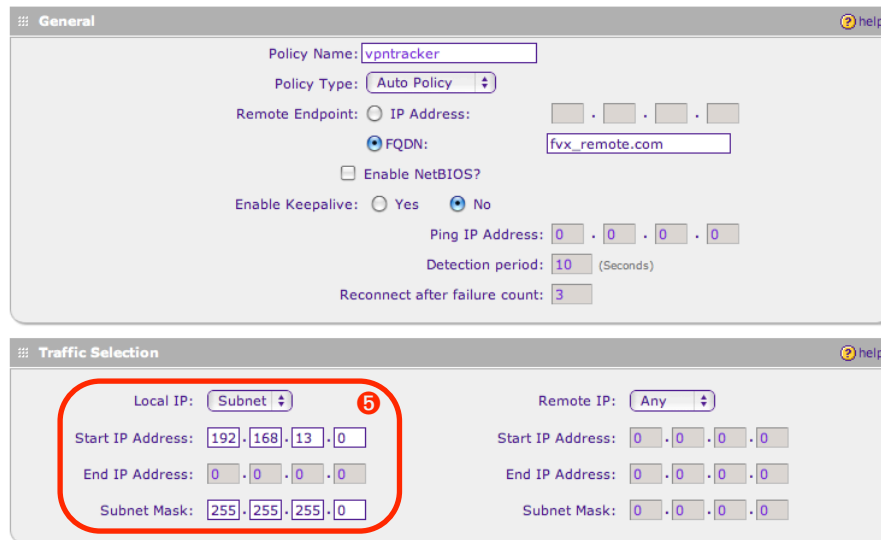
Step 4 – Check the Settings for the VPN Policy



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

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.



- ▶ 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**

Manual Policy Parameters

help

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: (DES-8 Char & 3DES-24 Char)

Key-Out: (MD5-16 Char & SHA-1-20 Char)

Auto Policy Parameters

help

SA Lifetime: 3600 Seconds

Encryption Algorithm: 3DES

Integrity Algorithm: SHA-1

☒ PFS Key Group: DH Group 2 (1024 bit)

Select IKE Policy: vpntracker

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

IKE Policies VPN Policies

List of IKE Policies

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

* Client Policy

select all delete add ...

Mode Config Record

Do you want to use Mode Config Record?

☐ Yes ☒ No

Select Mode Config Record: vpntracker

view selected

General

Policy Name: vpntracker

Direction / Type: Responder

Exchange Mode: Aggressive

Local

Select Local Gateway: WAN1 ☐ WAN2 ☐

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 ☐ 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

Extended Authentication

XAUTH Configuration

☒ None ☐ Edge Device ☐ IPSec Host

Authentication Type: User Database

Username:

Password:

- ▶ Select the “IKE Policies” tab
- ▶ Click “Edit” for the IKE policy

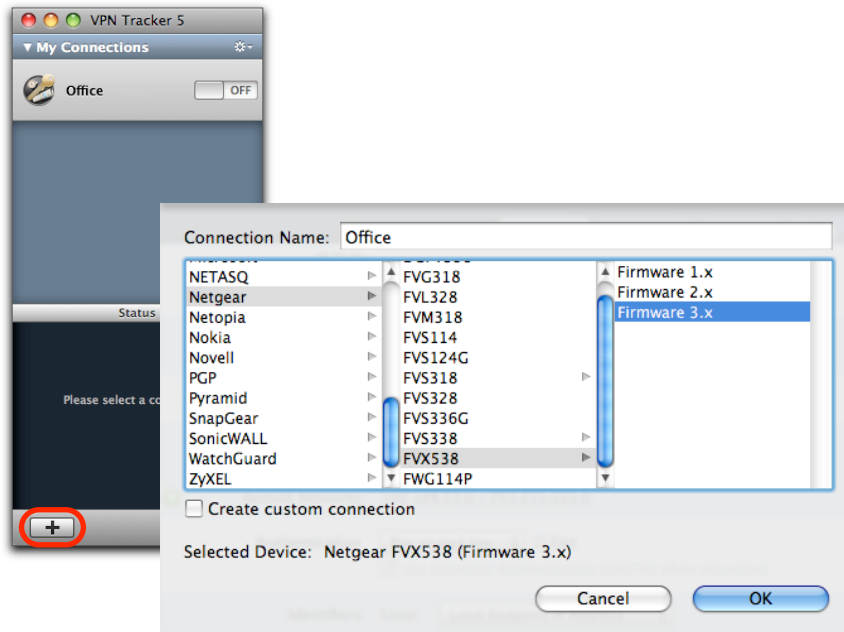
- ▶ The settings should be exactly as shown here, with the following exceptions:
- ▶ **Policy Name:** The policy name will be whatever you have entered for the connection name earlier
- ▶ **Local / Remote Identifier:** The identifier will be whatever you configured in the VPN Wizard (or what was pre-filled 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

The screenshot shows the 'Basic' tab of the Netgear VPN configuration interface. The interface is divided into several sections:

- Office**: A dashed box icon.
- Connection based on**: Netgear FVS338 (Firmware 3.x) and Configuration Guide.
- Automatic Configuration**: Mode Config (Automatic).
- Network**: Host to Network dropdown.
- VPN Gateway**: vpn.example.com (1).
- Local Address**: IP Address (2).
- Remote Networks**: 192.168.13.0 / 255.255.255.0 (3).
- Authentication**: Pre-shared key (4), Use Extended Authentication (XAUTH) (when requested), and Edit.
- Identifiers**: Local (Fully Qualified Domain Name (FQDN) fvx_remote.com (5)), Remote (Fully Qualified Domain Name (FQDN) fvx_local.com (6)), and Verify remote identifier (checked).
- DNS**: Use Remote DNS Server (unchecked).

- ▶ **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)

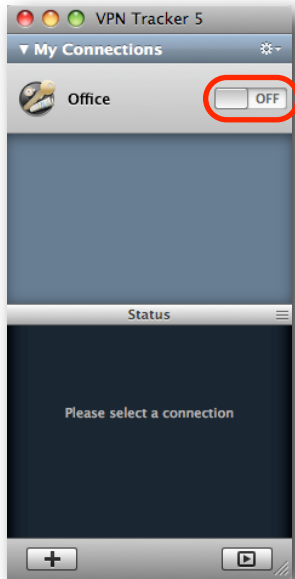
Task 3 – Test the VPN Connection

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

It's time to go out!

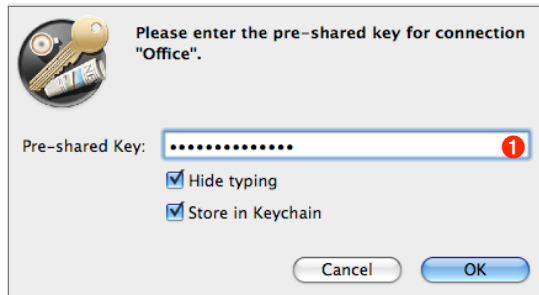
You will not be able to test and use your VPN connection from within the internal network that you want to connect to. In order to test your connection, you will need to connect from a different location. For example, if you are setting up a VPN connection to your office, test it from home. If you are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

Start your connection

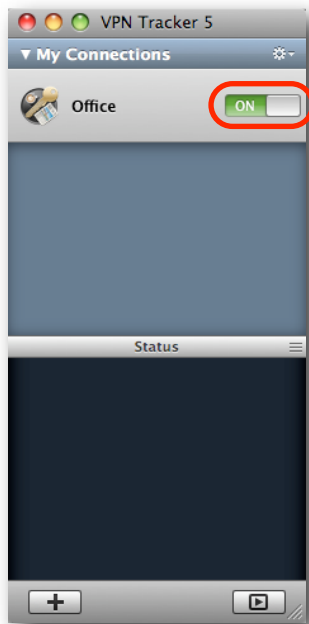


- ▶ Connect to the Internet
- ▶ Make sure that your Internet connection is working – open your Internet browser and try to connect to <http://www.equinux.com>
- ▶ Start VPN Tracker if it's not already running
- ▶ Slide the On/Off slider for the connection you have just configured to **On**

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, 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 (FVS338/DGFV338/FVX538)

The screenshot shows the VPN Tracker web interface. The top navigation bar includes 'Network Configuration', 'Security', 'VPN', 'Administration', 'Monitoring', 'Web Support', and 'Logout'. The 'VPN' tab is selected, and the 'VPN Client' sub-tab is highlighted. Below the navigation bar, there is a 'User Database' section with a 'RADIUS Client' sub-tab. The 'Configured Users' table is empty. Below the table, there is an 'Add New User' form with fields for 'User Name', 'Password', and 'Confirm Password'. The 'Add' button is highlighted. Red circles with numbers 5, 6, and 7 are placed over the 'User Name' field, the 'Password' field, and the 'Add' button respectively.

User Name	Password	Confirm Password	Action
bob	*****	*****	add

- ▶ 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 (FVS336G)

Network Configuration | Security | VPN | **Users** | Administration | Monitoring | Web Support | Logout

Users :: Groups :: Domains ::

Add User

Add User help

User Name: bob 5

User Type: IPSEC VPN User

Select Group: geardomain

Password: 6

Confirm Password:

Idle Timeout: 10 Minutes

- ▶ Go to the “Users > Users” section
- ▶ Click “Add...”
- ▶ **User Type:** Select “IPSEC VPN User”
- ▶ 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”

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

Temporarily Disable the VPN Policy

IKE Policies | **VPN Policies**

List of VPN Policies help

	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	edit

* Client Policy

select all delete enable **disable** add ...

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)



Extended Authentication

XAUTH Configuration

☐ None

☒ Edge Device

☐ IPSec Host

Authentication Type: User Database

Username:

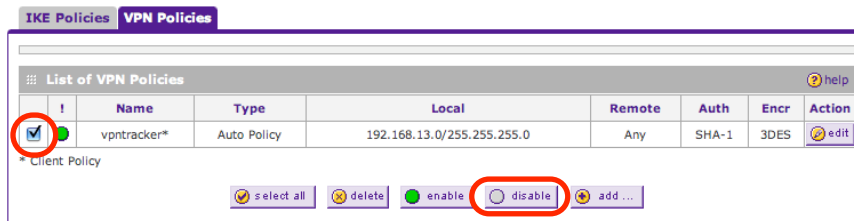
Password:

- ▶ 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



IKE Policies VPN Policies

List of VPN Policies

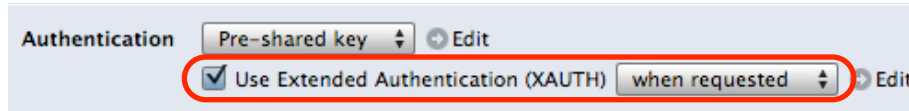
	Name	Type	Local	Remote	Auth	Encr	Action
<input checked="" type="checkbox"/>	vpntracker*	Auto Policy	192.168.13.0/255.255.0	Any	SHA-1	3DES	

* Client Policy

select all delete enable disable add ...

- ▶ 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

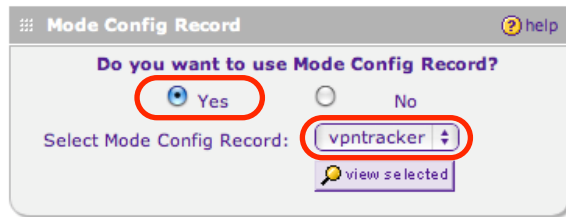
When multiple users use the same VPN connection, it is very important that a different IP address is used for each VPN client. The easiest way to ensure this, is to automatically have the NETGEAR assign IP addresses to connecting clients through Mode Config. **This feature is not available on FVG318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

Creating an Address Pool for Mode Config

The screenshot displays the NETGEAR VPN configuration interface. The top navigation bar includes links for Network Configuration, Security, VPN, Administration, Monitoring, Web Support, and Logout. The 'VPN' tab is selected, and the 'Mode Config' sub-tab is highlighted. Below the navigation bar, the 'Mode Config' section shows a table with columns for Record Name, Pool Start IP, Pool End IP, and Action. The 'add...' button is highlighted. Below the table, the 'Client Pool' section is shown, where the 'Record Name' is set to 'vpntracker'. The 'First Pool' is configured with a starting IP of 10.13.123.100 and an ending IP of 10.13.123.199. The 'DNS Server' is set to 0.0.0.0. The 'Traffic Tunnel Security Level' section shows the 'PFS Key Group' set to 'DH Group 2 (1024 bit)', 'SA Lifetime' set to 3600 seconds, 'Encryption Algorithm' set to '3DES', and 'Integrity Algorithm' set to 'SHA-1'.

- ▶ Go to the “VPN > Mode Config” section
 - ▶ FVS336G only: Go to VPN > IPsec VPN > Mode Config
 - ▶ 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 recommended you use the default values here.

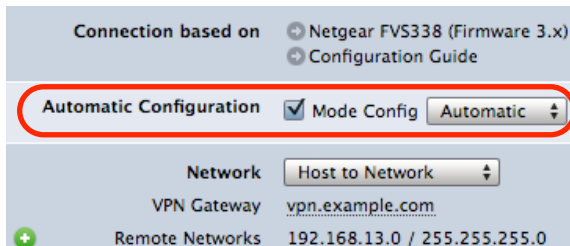
Configure the IKE Policy to use Mode Config



- ▶ 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



- ▶ Check **"Mode Config"** in the **"Automatic Configuration"** section. If you cannot find this setting for your device, make sure you have selected the correct device and firmware revision
- ▶ Make sure Mode Config is set to **"automatic"**

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.

Export the selected connection(s)

Export As: Office

Where: Desktop

Encryption password:

Confirm encryption password:

☒ Lock connection(s)

☒ Set unlock password

Unlock password:

Confirm unlock password:

☒ Hide Basic and Advanced settings from user when locked

☒ Include Actions

Actions are available in VPN Tracker Professional or Personal edition.

☒ Include admin email address: helpdesk@example.com

This email address will be used to send Technical Support Reports for this connection.

Cancel Export

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, choose File > Prepare Deployment.

- ▶ **Encryption Password:** Exported connections are always encrypted. The password must be entered by the recipient of the exported connection in order to be able to import the connection
- ▶ **Lock Connections:** Locked connections cannot be edited by users. This prevents accidental changes to a connection. In addition, the pre-shared key of a locked connection cannot be revealed by users
- ▶ **Set Unlock Password:** In case you need to make a quick modification to a locked connection at a user's Mac, you can add an unlock password that will enable you to modify the connection. Click the padlock icon in the upper right corner of the VPN Tracker window to unlock a connection
- ▶ **Hide Basic and Advanced settings from users when locked:** This setting can be used to hide all connection information from users
- ▶ **Include Actions:** If you wish, you can define actions to be performed upon connection start / stop, such as connecting to a database, or disconnecting from all file servers in the VPN when the connection is stopped. These actions can optionally be included in an exported connection
- ▶ **Email:** If you specify an email address here, Technical Support Reports created by your users will be sent to this email address

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

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

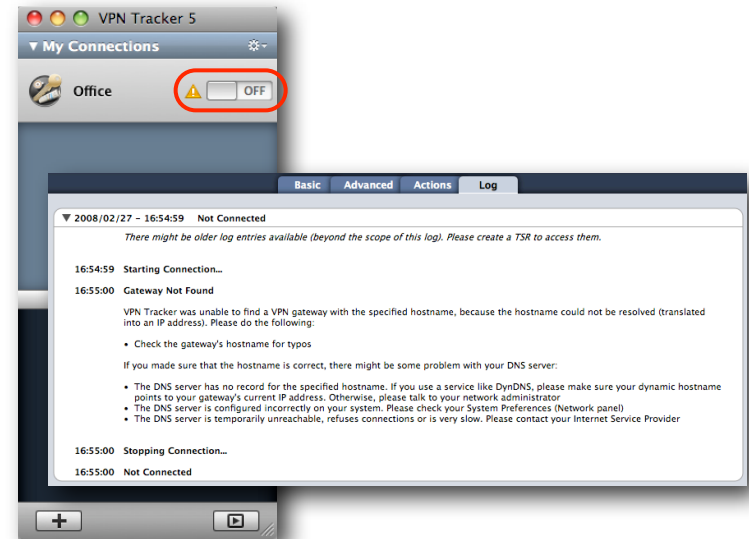
On/Off Slider goes back to “Off” right away

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.



Cannot Access Resources on the Remote Network

If the connection slider goes to ON and turns green, but you cannot access resources (servers, email, etc.) in the remote network, 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. 192.168.13.42), 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 the DNS server configured on your Mac's is able to resolve this host name to an IP address, or configure a "Remote DNS" server in VPN Tracker.

Run the VPN Environment Manager

In many local 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 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.

Check if the IP address of the resource 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(s). Also double-check the network mask that you have configured for the remote network(s) 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.

Make sure the NETGEAR device is the default gateway in the remote network

Please see “The Role of the Local Address in VPN Tracker” for the consequences of your NETGEAR device not being the default gateway in the remote network.

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

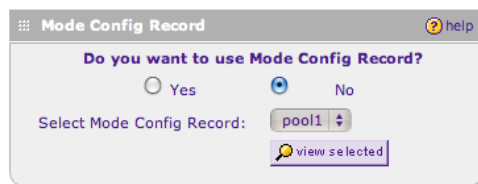
VPN Settings Explained

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

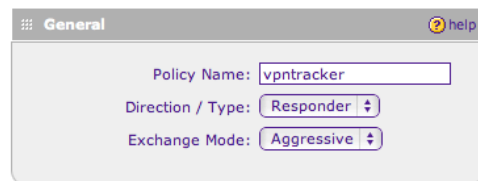
The IKE Policy contains the settings for the first phase in the process of establishing a VPN connection. **Most of the settings here correspond to settings located in VPN Tracker on the Basic tab, or under Advanced > Phase 1.**

Mode Config Record

The screenshot shows a configuration window titled "Mode Config Record" with a help icon. It contains a question "Do you want to use Mode Config Record?" with "Yes" and "No" radio buttons. The "No" button is selected. Below this is a label "Select Mode Config Record:" followed by a dropdown menu showing "pool1" and a "view selected" button.

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

The screenshot shows a configuration window titled "General" with a help icon. It contains three settings: "Policy Name:" with a text input field containing "vpntracker", "Direction / Type:" with a dropdown menu showing "Responder", and "Exchange Mode:" with a dropdown menu showing "Aggressive".

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

The screenshot shows the 'Local' configuration window. It has a title bar with a menu icon, the word 'Local', and a help icon. Inside, there are two radio buttons for 'Select Local Gateway': 'WAN1' (selected) and 'WAN2'. Below this is a dropdown menu for 'Identifier Type' set to 'FQDN'. At the bottom is a text field for 'Identifier' containing '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.

The screenshot shows the 'Remote' configuration window. It has a title bar with a menu icon, the word 'Remote', and a help icon. Inside, there is a dropdown menu for 'Identifier Type' set to 'FQDN'. At the bottom is a text field for 'Identifier' containing '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

The screenshot shows the 'IKE SA Parameters' configuration window. It has a title bar with a menu icon, the text 'IKE SA Parameters', and a help icon. The settings are as follows: 'Encryption Algorithm' is set to '3DES'; 'Authentication Algorithm' is set to 'SHA-1'; 'Authentication Method' has 'Pre-shared key' selected and 'RSA-Signature' unselected; 'Pre-shared key' is 'topsecret' with a note '(Key Length 8 - 49 Char)'; 'Diffie-Hellman (DH) Group' is 'Group 2 (1024 bit)'; 'SA-Lifetime (sec)' is '28800'; 'Enable Dead Peer Detection' has 'Yes' unselected and 'No' selected; 'Detection Period' is '10' with a note '(Seconds)'; and 'Reconnect after failure count' is '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 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: Make sure Dead Peer Detection is turned off.

Extended Authentication (XAUTH)

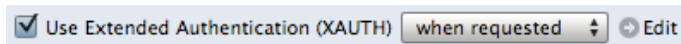


XAUTH Configuration: When XAUTH is used, individual user names and passwords are required, in addition to the pre-shared key. **XAUTH is not available on FVG318 devices.**

► 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: Turn on “Basic > Extended Authentication (XAUTH)”, and set it 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"

The screenshot shows the 'Traffic Selection' configuration window. It has a title bar with a menu icon and a 'help' button. The window is divided into two columns. The left column is for the 'Local' side and the right column is for the 'Remote' side. Each column has a dropdown for the IP type, followed by input fields for Start IP Address, End IP Address, and Subnet Mask. The Local IP is set to 'Subnet' with a dropdown arrow. Its Start IP Address is 192.168.13.0, End IP Address is 0.0.0.0, and Subnet Mask is 255.255.255.0. The Remote IP is set to 'Any' with a dropdown arrow. Its Start IP Address, End IP Address, and Subnet Mask are all 0.0.0.0.

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

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).

The screenshot shows the 'Manual Policy Parameters' configuration window. It has a title bar with a menu icon and a 'help' button. The window is divided into two columns. The left column is for 'SPI-Incoming' and the right column is for 'SPI-Outgoing'. Each column has input fields for SPI-Incoming, SPI-Outgoing, Encryption Algorithm, Integrity Algorithm, Key-In, and Key-Out. The SPI-Incoming field is empty with a hint '(Hex, 3-8 Chars)'. The SPI-Outgoing field is empty with a hint '(Hex, 3-8 Chars)'. The Encryption Algorithm is set to '3DES' with a dropdown arrow. The Integrity Algorithm is set to 'SHA-1' with a dropdown arrow. The Key-In and Key-Out fields are empty. The Key-In field has a hint '(DES-8 Char & 3DES-24 Char)' and the Key-Out field has a hint '(MD5-16 Char & SHA-1-20 Char)'.

SPI-Incoming:	SPI-Outgoing:
(Hex, 3-8 Chars)	(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

The screenshot shows the 'Auto Policy Parameters' configuration window. It contains the following settings:

- SA Lifetime:** 3600, with a unit dropdown set to 'Seconds'.
- Encryption Algorithm:** 3DES.
- Integrity Algorithm:** SHA-1.
- PFS Key Group:** Checked, with a dropdown set to 'DH Group 2 (1024 bit)'.
- Select IKE Policy:** vpntracker.
- view selected:** A button with a magnifying glass icon.

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