

e·quinux



VPN Tracker 365

VPN Configuration Guide

NETGEAR® FVS318v3

equinix AG and equinix USA, Inc.

© 2015 equinix 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 equinix AG or equinix 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 equinix 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. equinix is not responsible for printing or clerical errors.

www.equinix.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.

equinix 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 equinix has been advised of the possibility of such damages.

Introduction	4	Further Questions?	26
Important Prerequisites.....	5	Task 1 – Configure your NETGEAR (Alternate Configuration)	27
Scenario.....	6	Step 1 – Choosing the Local Address.....	27
Terminology.....	7	Step 2 – Create a new IKE Policy.....	29
My NETGEAR Configuration	8	Step 3 – Retrieve your NETGEAR’s LAN and WAN Configuration	31
Task 0 – Test Your Local Router Capabilities	9	31	
Run the VPN Availability Test.....	9	Step 4 – Create a new VPN Policy.....	32
Task 1 – Configure your NETGEAR	11	Task 2 – Configure VPN Tracker (Alternate Configuration)	34
Step 1 – Create a new VPN Tunnel using the VPN Wizard	11	Step 1 - Create a New Connection.....	34
Step 2 – Adjust the VPN Tunnel Settings	13	Step 2 – Configure the VPN Connection	35
Step 3 – Retrieve your NETGEAR’s WAN Configuration ...	14	Task 3 – Test the VPN Connection (Alternate Configuration)	36
Step 4 – Retrieve your NETGEAR’s Local ID	14	It’s time to go out!	36
Task 2 – Configure VPN Tracker	15	Start your connection	36
Step 1 - Create a New Connection	15	VPN Settings Explained	38
Step 2 – Configure the VPN	16	IKE Policy	38
Connection.....	16	VPN Policy.....	40
Task 3 – Test the VPN Connection	17	The Role of the Local Address in VPN Tracker	44
It’s time to go out!	17	Outgoing Network Ports.....	48
Start your connection	17		
Supporting Multiple Users	19		
Preventing IP Address and Policy Conflicts	19		
Step 2 – Adjust your NETGEAR device to work with specific Local			
Addresses	21		
Step 3 – Configuring a Local IP Address in VPN Tracker ...	22		
Step 4 - Adding Policies for Additional Users.....	22		
Troubleshooting	24		
VPN Connection Fails to Establish	24		
No Access to the Remote Network	25		

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 gateway.

Note This documentation is only a supplement to, not a replacement for, the instructions 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 a basic VPN setup that can accept incoming connections from any IP address.

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:

- ▶ instructions for setting up a VPN connection for multiple users
- ▶ troubleshooting tips
- ▶ 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 features to your connection once you have the basic setup working.

Important Prerequisites

Your NETGEAR Device

This document applies to the following NETGEAR device

- ▶ FVS318v3
 - ▶ The FVS318v1 and v2 use a different firmware. Refer to [NETGEAR's product support website](#) on how to recognize the different device revisions.

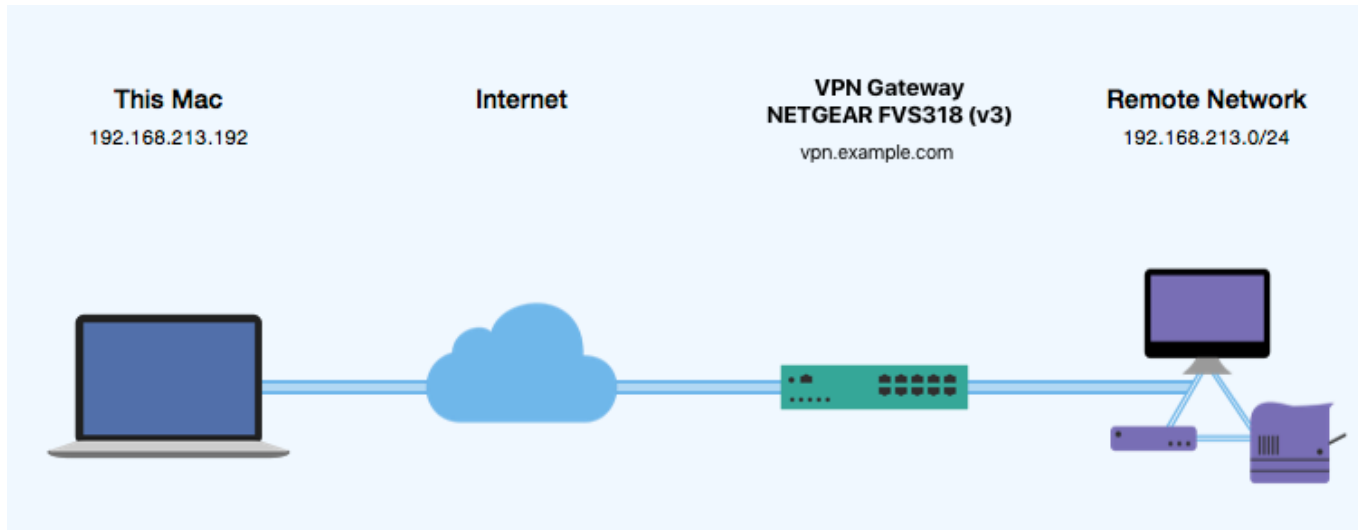
The documentation is based on firmware 3.0_27 (FVS318v3).

Your Mac

- ▶ 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

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 DNS 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 Local Identifier: _____
- 3 NETGEAR's Remote Identifier: _____
- 4 WAN IP Address: _____ . _____ . _____ . _____ (or DNS host name _____)
- 5 LAN IP Address (*alternate configuration only*): _____ . _____ . _____ . _____
- 6 LAN Subnet Mask: _____ . _____ . _____ . _____
- 7 LAN Network Address: _____ . _____ . _____ . _____
- 8 Local IP Address (*alternate and multiple user configurations only*) _____ . _____ . _____ . _____

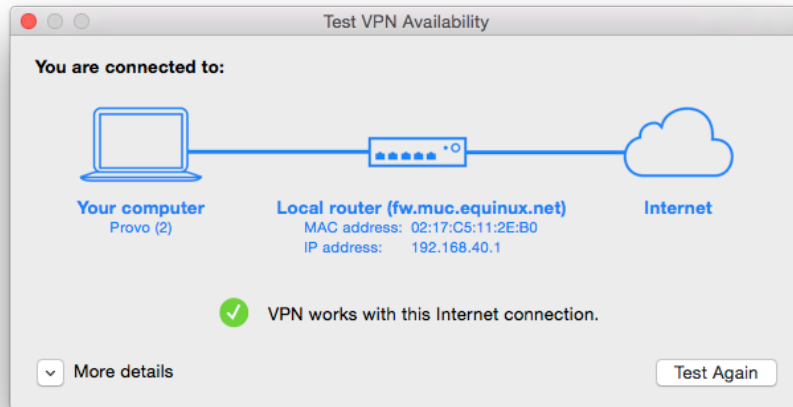
Task 0 – Test Your Local Router Capabilities

Due to an issue in the firmware in the NETGEAR FVS318v3, it may be necessary to use an alternate VPN configuration, depending on the capabilities of your local Internet router.

How to Test

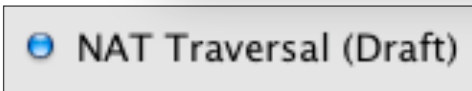
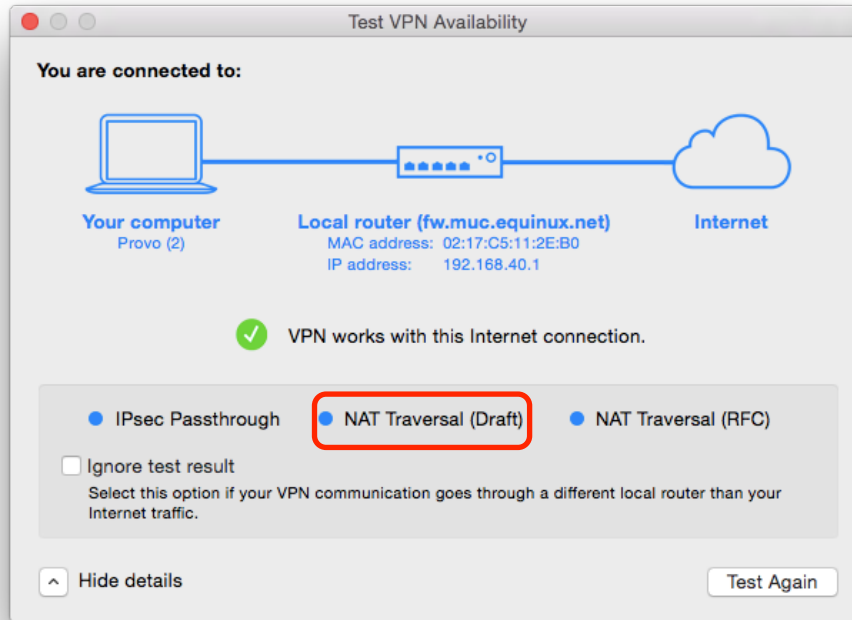
In order to perform this test, you'll need to be at the location from where you plan to be using this VPN connection from (e.g. your home, your branch office etc). If you frequently change the location from where you are using your VPN connection (e.g. traveling), please proceed directly to chapter “**Alternate Configuration**”.

Run the VPN Availability Test

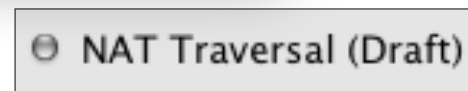


- ▶ Launch VPN Tracker
 - ▶ Select “**Tools > Test VPN Availability**” from the menu bar
- The test will run automatically (if it does not, click the “Test Again” button)
- ▶ When the test has finished, click “**More Details**” to see the results

▼ More details



If your test results show that NAT-Traversal (Draft) is **supported**, please continue with the instructions on the **next page**.



If your test results show that NAT-Traversal (Draft) is **not supported**, please go to chapter "**Alternate Configuration**".

Note Since the FVS318v3 does not support NAT-Traversal (RFC), it is necessary that either IPsec Passthrough or NAT-Traversal (Draft) are supported at the location from which you connect.

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. We will be using the NETGEAR VPN Assistant to configure your NETGEAR device's VPN settings.

Step 1 – Create a new VPN Tunnel using the VPN Wizard

The screenshot shows the NETGEAR VPN Wizard interface. On the left sidebar, the 'VPN Wizard' option is highlighted. The main content area is titled 'VPN Wizard' and displays 'Step 1 of 3: Connection Name, Connection type and Pre-Shared Key'. There are two input fields: 'What is the new Connection Name?' with the value 'vpntracker' and 'What is the pre-shared key?' with the value 'topsecret'. Below these is a section for 'This VPN tunnel will connect to.' with two radio button options: 'A remote VPN Gateway' and 'A remote VPN client', where the latter is selected. At the bottom of the form are three buttons: 'Back', 'Next', and 'Cancel'.

- ▶ Go to **VPN > VPN Wizard**
- ▶ Click “Next”
- ▶ **Connection Name:** Enter a name for your connection (e.g. “vpntracker”)
- ▶ **Pre-shared key:**
The pre-shared key is the password that users have to enter before connecting. Make sure to set a strong password here
- ▶ Select the “**A remote VPN client**” checkbox option

The VPN Wizard will generate the appropriate settings and will then display a summary page. Be sure to make a note of the following settings

VPN - Auto Policy

Summary

Please verify your inputs:

Connection Name:	vpntracker
Remote VPN Endpoint:	fvs_remote_vpntracker 3
Remote Client Access:	Any
Remote IP:	0.0.0.0
Local WAN ID:	Either static IP or FQDN
Local Client Access:	By Subnet 7
Local IP:	192.168.13.0 / 255.255.255.0 6

You can click [here](#) to view the VPNC-recommended parameters.
Please click "**Done**" to apply the changes.

▶ **Remote VPN Endpoint:**

This is the identifier used by your NETGEAR to identify your incoming connections. It may differ from what is pictured here, so be sure to write down the exact identifier **3**

▶ **Local IP:**

▶ Write down the first part of the address (e.g. "192.168.13.0") as the **LAN Network Address** **7**

▶ Write the second part of the address (e.g. "255.255.255.0") as your **LAN Subnet Address** **6**

▶ Click "**Done**"

:

Step 2 – Adjust the VPN Tunnel Settings

Policy Table								
	#	Enable	Name	Type	Local	Remote	AH	ESP
	1	<input checked="" type="checkbox"/>	office	Auto	192.168.13.0/255.255.255.0	Any	Disabled	ESP

[Edit](#) [Move](#) [Delete](#)

The tunnel created by the VPN Wizard needs to be adjusted slightly to match VPN Tracker's default settings:

► Go to **VPN Policies** and click **“Edit”**.

VPN - Auto Policy

General

Policy Name: vpntracker

IKE policy: vpntracker

IKE Keep Alive

Remote VPN Endpoint

Address Type: IP Address

Address Data: 0.0.0.0

SA Life Time

28800 (Seconds)

0 (Kbytes)

IPsec.PFS

PFS Key Group: Group 2 (1024 Bit)

Traffic Selector

Local IP

Subnet address

Start IP address: 192 . 168 . 13 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Remote IP

Any

Start IP address: 0 . 0 . 0 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

AH Configuration

Enable Authentication

Authentication Algorithm: MD5

ESP Configuration

Enable Encryption

Encryption Algorithm: 3DES

Enable Authentication

Authentication Algorithm: SHA-1

NETBIOS Enable

[Back](#) [Apply](#) [Cancel](#)

► **SA Life Time:** Set this value to “28800” (secs)

► **IPSec PFS**

Enable this option and select “Group 2 (1024 Bit)”

► Click **“Apply”**

Step 3 – Retrieve your NETGEAR's WAN Configuration

Router Status

System Name FVS318v3
Firmware Version v3.0_27

WAN Port

MAC Address 00:14:6c: [REDACTED]
IP Address 194.145.236.2 ④
DHCP FixedIP
IP Subnet Mask 255.255.255.0
Domain Name Server 194.145.236.1

LAN Port

Go to **Maintenance > Router Status** and obtain the following information from the Router Status page:

▶ **WAN Port:**

- ▶ Write down the **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 – Retrieve your NETGEAR's Local ID

VPN

- VPN Wizard
- IKE Policies**
- VPN Policies
- CAs
- Certificates
- CRL
- VPN Status

IKE Policies

Policy Table

#	Name	Mode	Local ID	Remote ID	Encr	Auth	DH
1	vpntracker	Aggressive	ivs_local	ivs_remote_vpntracker	3DES	SHA1	Group 2 (1024 Bit)

②

Add Edit Move Delete

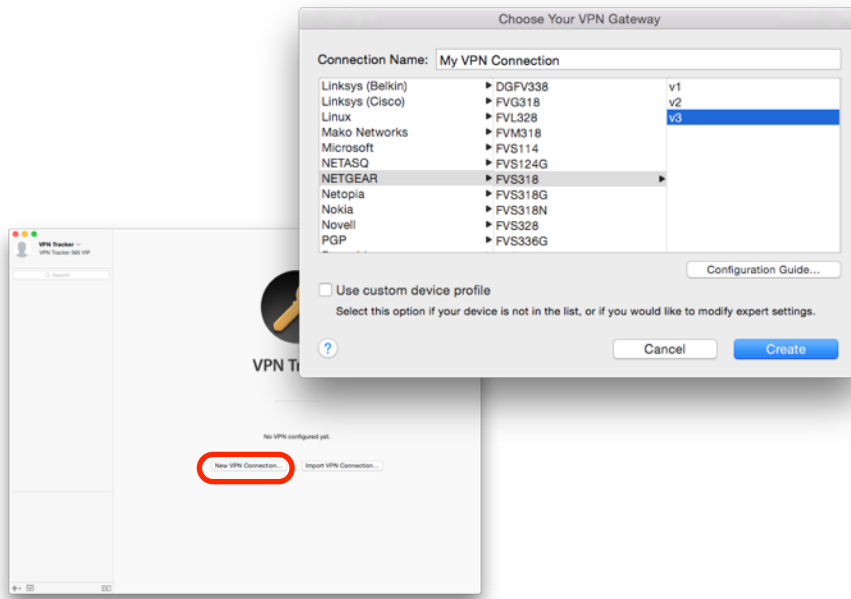
▶ Go to **IKE Policies**

- ▶ **Local ID** This is the identifier with which your NETGEAR device can be identified by VPN Tracker. Be sure to write this down exactly ②

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 “Task 1 – Configure your NETGEAR”.

Step 1 - Create a New Connection



- ▶ Launch 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 device or firmware revision available, be sure to select the revision/firmware matching your device
- ▶ **Connection Name:** Choose a name for your connection (e.g. “Office”)
- ▶ Click “OK”

Step 2 – Configure the VPN

Connection

Connection Name My VPN Connection
Connection based on NETGEAR FVS318 (v3)
Need help? Configuration Guide

VPN Gateway vpn.example.com ? 4

Network Configuration

Topology Host to Network ?

Local Address IP Address ?

Remote Networks 192.168.13.0 / 24 ? 7 / 6

Authentication Pre-shared key ? Pre-shared key not saved

Identifiers

Local Fully Qualified Domain Name (FQDN) ? fvs_remote_vpnt tracker ? 3

Remote Fully Qualified Domain Name (FQDN) ? fvs_local ? 2

DNS Use Remote DNS Server

Note The default value for your NETGEAR device's local identifier is "fvs_local". You can check this value under VPN > IKE Policies on the device.

- ▶ **VPN Gateway:** Enter your NETGEAR's public IP address 4. If you are using Dynamic DNS, or if the device has a DNS host name, use it instead (in our 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" for details and how to choose the address
- ▶ **Remote Networks:** Enter the network address 7 and the subnet mask 6 of the network that is being accessed through the VPN tunnel. 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. "fvs_remote_vpnt tracker") 3
 - ▶ **Remote:** Enter the **local** identifier from your NETGEAR (e.g. "fvs_local") 2

Task 3 – Test the VPN Connection

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

It's time to go out!

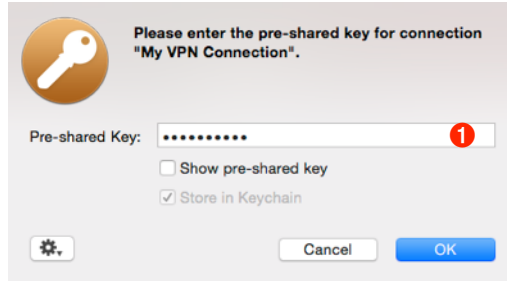
You will not be able to test and use your VPN connection from within the internal network that you want to connect to. To test your connection, you will need to connect from a different location. For example, if you are setting up a VPN connection to your office, test it from home. If you are setting 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 (or even just yourself connecting from multiple computers simultaneously), there are certain issues you will have to consider, such as using different IP addresses for each user, and making sure that one user connecting does not disconnect others. In addition to 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.

Preventing IP Address and Policy Conflicts

If multiple users connect to your NETGEAR at the same time, **you must ensure that each of them uses a different Local Address in VPN Tracker** by setting an individual Local Address for each of them.

Advanced Users A more detailed description of the Local Address setting is available in the last chapter of this document.

Step 1 – Choosing the Local Address

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.

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 (= 10.22.13.0/255.255.255.0), 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.

Once you've picked an address for a user (e.g. 10.22.13.1 for "alice"), make a note of it under **8**.

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

Step 2 – Adjust your NETGEAR device to work with specific Local Addresses

You will need to change the tunnel for the first user on your NETGEAR to work with specific local IP addresses.

Policy Table								
	#	Enable	Name	Type	Local	Remote	AH	ESP
	1	<input checked="" type="checkbox"/>	office	Auto	192.168.13.0/255.255.255.0	Any	Disabled	ESP

► Go to **VPN Policies** and click **“Edit”**.

Traffic Selector

Local IP

Subnet address: . . .

Start IP address: . . .

Finish IP address: . . .

Subnet Mask: . . .

Remote IP

Single address: . . .

Start IP address: . . .

Finish IP address: . . .

Subnet Mask: . . .

AH Configuration

Enable Authentication

Authentication Algorithm:

ESP Configuration

Enable Encryption

Encryption Algorithm:

Enable Authentication

Authentication Algorithm:

NETBIOS Enable

► **Remote IP**

► Select “Single Address” from the drop down menu

► **Start IP Address**

Enter the local address **8** you chose as your local IP (See **“Choosing the Local Address”**. (e.g. “10.22.13.1”))

Note A VPN policy that is set up to accept only a single “Remote IP” can only be used by a single user at a time.

Step 3 – Configuring a Local IP Address in VPN Tracker

The screenshot shows the configuration page for a VPN connection. The 'Connection Name' is 'Netg. FVS318 V3' and it is based on 'NETGEAR FVS318 (v3)'. The 'VPN Gateway' is 'vpn.example.com'. Under 'Network Configuration', the 'Topology' is 'Host to Network', the 'Local Address' is '10.22.13.1' (highlighted with a red circle and the number 8), and the 'Remote Networks' are '192.168.13.0 / 24'. The 'Authentication' is set to 'Pre-shared key'. Under 'Identifiers', the 'Local' is 'fvs_remote_vpntacker' and the 'Remote' is 'fvs_local'. There is a 'DNS' section with a checkbox for 'Use Remote DNS Server' which is currently unchecked.

- ▶ **Local Address:** Enter the Local IP address **8** you have configured for this VPN user.

Tip If your needs expand to more than a handful of users, you may want to consider upgrading to a VPN gateway that supports Extended Authentication (XAUTH) and multiple users sharing the same set of policies.

Step 4 - Adding Policies for Additional Users

The set of policies you have set up can be used by a single user with a fixed local IP address. To add more users, repeat the setup described in “Task 1 – Configure Your NETGEAR”, and set a specific Local Address for the newly created tunnel as described in Steps 1 – 3 of this chapter.

Note Please refer to your device’s data sheet to find out the maximum number of VPN tunnels that can be set up on your device.

If you have difficulties setting up multiple tunnels on a single device, it is a good idea to check the VPN Status (VPN > VPN Status > VPN Status) to see which policies are in use. If necessary, selectively disable policies to see which policies are causing trouble.

Troubleshooting

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

VPN Connection Fails to Establish

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

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

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

If the connection ON/OFF slider goes back to “OFF” a while after attempting to start the connection, please go to the “Log” tab to get more information about the error. You can also 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.



```
2015/09/23 - 14:39:37 Not Connected
14:39:37 VPN Connection Requested
14:39:37 Preparing Connection
14:39:38 VPN Gateway Unreachable
The VPN gateway cannot be contacted.
• Make sure that you have a working internet connection
If you entered your VPN gateway as a host name (e.g. vpn.example.com) instead of an IP address (e.g. 10.23.42.1):
• Check the host name you entered to make sure it is not mistyped
• Make sure a DNS server is configured on your Mac and the host name can be looked up using this DNS server
14:39:38 About to Disconnect (Error)
14:39:38 Disconnecting (Error)
14:39:38 Not Connected
```


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

Task 1 – Configure your NETGEAR (Alternate Configuration)


This configuration is intended for situations where you are connecting from locations where NAT-Traversal (old) is not supported by the local router. 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. We will first be creating an IKE policy, which corresponds to "Phase 1" in VPN Tracker. In a second step, we will be setting up an associated VPN (IPsec) policy, which corresponds to "Phase 2" in VPN Tracker.

Step 1 – Choosing the Local Address

With the type of policy that we will be setting up, it is necessary to always set a specific Local Address to avoid unintended side-effects. The Local Address you will be choosing 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.

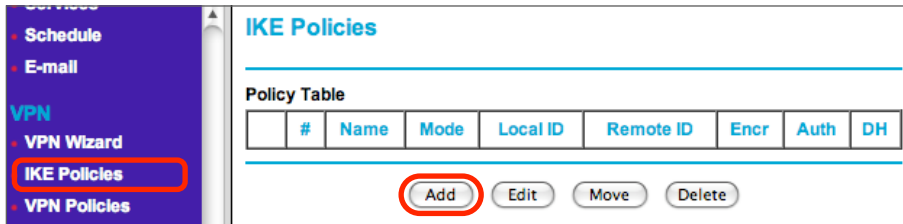
User	IP Address
alice	10.22.13.1
bob	10.22.13.2
charlie	10.22.13.3
...	10.22.13._

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 select a different IP address from that network to be used as the Local Address in VPN Tracker for each user.

Once you've picked an address for a user (e.g. 10.22.13.1), make a note of it under 

Advanced Users A more detailed description of the Local Address setting is available in the last chapter of this document.

Step 2 – Create a new IKE Policy



The screenshot shows a web-based configuration interface for VPN services. On the left is a dark blue sidebar with a menu. Under the 'VPN' section, 'IKE Policies' is highlighted with a red rectangle. The main content area is titled 'IKE Policies' and contains a 'Policy Table' with the following columns: #, Name, Mode, Local ID, Remote ID, Encr, Auth, and DH. Below the table are four buttons: 'Add', 'Edit', 'Move', and 'Delete'. The 'Add' button is circled in red.

#	Name	Mode	Local ID	Remote ID	Encr	Auth	DH
---	------	------	----------	-----------	------	------	----

Buttons: Add, Edit, Move, Delete

▶ Go to **VPN > IKE Policies**

▶ Click “Add”

IKE Policy Configuration

General

Policy Name

Direction/Type

Exchange Mode

Local

Local Identity Type

Local Identity Data ②

Remote

Remote Identity Type

Remote Identity Data ③

IKE SA Parameters

Encryption Algorithm

Authentication Algorithm

Authentication Method Pre-shared Key ①
 RSA Signature (requires Certificate)

Diffie-Hellman (DH) Group

SA Life Time (secs)

- ▶ **Policy Name:** Enter a name for the connection
- ▶ **Direction / Type:** Select “Responder”
- ▶ **Exchange Mode:** Select “Aggressive Mode”
- ▶ **Local Identity Type:** Select “Fully Qualified Domain Name”
- ▶ **Local Identity Data:** Enter the identifier to be used by the device, e.g. “netgear.local”. Make sure to write down the **exact** identifier ②
- ▶ **Remote Identity Type:** Select “Fully Qualified Domain Name”
- ▶ **Remote Identity Data:** Enter the identifier to be used by the client, e.g. “vpntracker.local”. Make sure to write down the **exact** identifier ③
- ▶ **Encryption Algorithm:** Select “3DES”
- ▶ **Authentication Algorithm:** Select “SHA-1”
- ▶ **Authentication Method:** Select “Pre-Shared Key”
 - ▶ The pre-shared key is the password that users have to enter before connecting. Make sure to set a strong password here ①
- ▶ **Diffie-Hellman (DH) Group:** Select “Group 2 (1024 Bit)”
- ▶ **SA Lifetime:** 86400 seconds
- ▶ Click “Apply” to add your new IKE policy

Tip Use the form on page 9 of this document to keep track of the various settings. You will need again them later on.

Step 3 – Retrieve your NETGEAR's LAN and WAN Configuration

Router Status

System Name	FVS318v3
Firmware Version	v3.0_27

WAN Port

MAC Address	00:14:6c: [REDACTED]
IP Address	194.145.236.2 4
DHCP	FixedIP
IP Subnet Mask	255.255.255.0
Domain Name Server	194.145.236.1

LAN Port

MAC Address	00:14:6c: [REDACTED]
IP Address	192.168.13.1 5
DHCP	OFF
IP Subnet Mask	255.255.255.0 6

[Show Statistics](#) [Show WAN Status](#)

- ▶ Go to **Maintenance > Router Status** and obtain the following information from the Router Status page:
- ▶ **WAN Port:**
 - ▶ Write down the **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
- ▶ **LAN Port:**
 - ▶ Write down the **LAN IP Address** **5**
 - ▶ Write down the **LAN IP Subnet Mask** **6**
- ▶ Calculate your **LAN Network Address** by applying the **LAN Subnet Mask** **6** to the **LAN IP Address** **5**:
- ▶ Applying the subnet mask means setting those elements of the IP address to 0 where the subnet mask is 0, and preserving all elements where the subnet mask is 255 (*)

LAN Subnet Mask	255	.	255	.	255	.	0
<i>applied to</i>	↓		↓		↓		↓
LAN IP Address	192	.	168	.	13	.	1

LAN Network Address 192 . 168 . 13 . 0

- ▶ In our example: Write down the **LAN Network Address** you have calculated as **7**

(*) If you are using a subnet mask with elements that are not 0 or 255, you can use one of the many subnet calculators available for free on the Internet to calculate the network address.

Step 4 – Create a new VPN Policy

VPN Policies

Policy Table

#	Enable	Name	Type	Local	Remote	AH	ESP
---	--------	------	------	-------	--------	----	-----

Edit Move Delete

Apply Cancel

Add Auto Policy Add Manual Policy

- ▶ Go to **VPN > VPN Policies**
- ▶ Click “Add Auto Policy”

VPN - Auto Policy

General

Policy Name:

IKE policy:

IKE Keep Alive

Ping IP Address: . . .

Remote VPN Endpoint

Address Type:

Address Data: 3

SA Life Time

(Seconds)

(Kbytes)

IPsec PFS

PFS Key Group:

- ▶ **Policy Name:** Enter a name for the connection. It can be the same or different than the IKE Policy
- ▶ **IKE Policy:** Select the IKE Policy you have just created
- ▶ **IKE Keep Alive:** Leave this setting turned off
- ▶ **Remote VPN Endpoint:** Select “Fully Qualified Domain Name”, and enter the same identifier here that you used as the Remote Identity 3 in the IKE policy
- ▶ **SA Life Time:** 28800 seconds / 0 Kbytes
- ▶ **IPsec PFS:** Turn on IPsec PFS
- ▶ **PFS Key Group:** Select “Group 2 (1024 Bit)”

Traffic Selector

Local IP

Subnet address ▾

Start IP address: 192 . 168 . 13 . 0 **7**

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0 **6**

Remote IP

Single address ▾

Start IP address: 10 . 22 . 13 . 1 **8**

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

AH Configuration

Enable Authentication

Authentication Algorithm: MD5 ▾

ESP Configuration

Enable Encryption

Encryption Algorithm: 3DES ▾

Enable Authentication

Authentication Algorithm: SHA-1 ▾

NETBIOS Enable

Back Apply Cancel

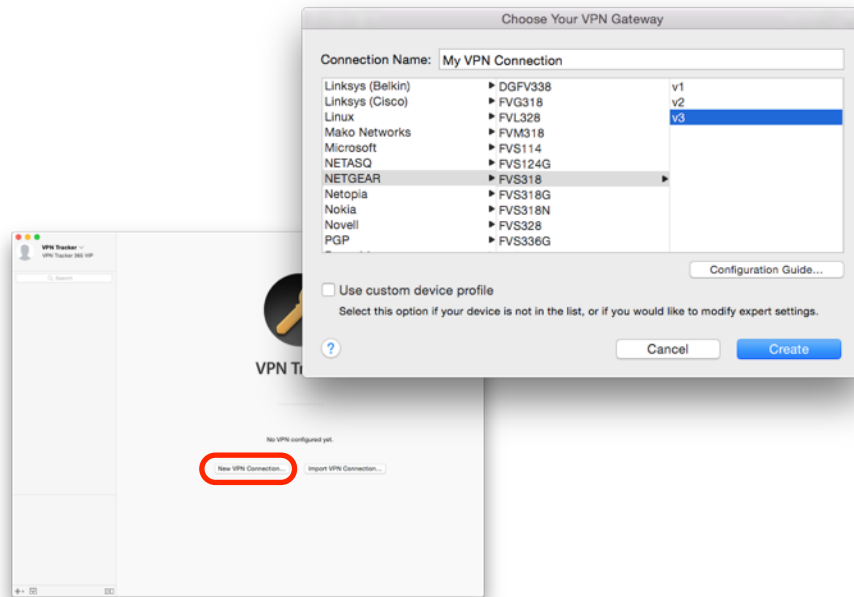
- ▶ **Local IP:** Select “Subnet Address”
- ▶ **Start IP address:** Enter the LAN Network Address **7** you calculated in Step 2 (here: 192.168.13.0)
- ▶ **Subnet Mask:** Enter the LAN subnet mask **6** you wrote down in Step 2 (here: 255.255.255.0)
- ▶ **Remote IP:**
 - ▶ Select “Single Address”
 - ▶ **Start IP Address:** Enter the Local IP address **8** you determined.
- ▶ **AH Configuration:** Leave this setting turned off
- ▶ **ESP Configuration**
 - ▶ **Enable Encryption:** Turn on encryption
 - ▶ **Encryption Algorithm:** Select “3DES”
 - ▶ **Enable Authentication:** Turn on authentication
 - ▶ **Authentication Algorithm:** Select “SHA-1”
- ▶ **NETBIOS Enable:** Leave this setting turned off
- ▶ Click “Apply” to add your new VPN policy

Task 2 – Configure VPN Tracker (Alternate Configuration)

This section describes how to configure VPN Tracker to connect to your NETGEAR FVS318v3. You will need the configuration information you collected during Task 1.

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 device or firmware revision available, be sure to select the revision/firmware matching your device
- ▶ **Connection Name:** Choose a name for your connection (e.g. “Office”)
- ▶ Click “OK”

Step 2 – Configure the VPN Connection

The screenshot shows the 'Office' VPN configuration page. It includes tabs for 'Basic', 'Advanced', 'SecureDrop', 'Actions', and 'Notes'. The configuration is divided into several sections: 'Connection Name' (Office), 'VPN Gateway' (vpn.example.com), 'Network Configuration' (Topology: Host to Network, Local Address: 10.22.13.1, Remote Networks: 192.168.13.0 / 24), 'Authentication' (Pre-shared key), and 'Identifiers' (Local and Remote, both set to Fully Qualified Domain Name (FQDN)). A red box highlights the 'Identifiers' section, and red circles with numbers 2 through 8 point to specific fields: 2 (Remote identifier), 3 (Local identifier), 4 (VPN Gateway), 6 (Subnet mask), 7 (Remote network address), and 8 (Local address).

- ▶ **VPN Gateway:** Enter your NETGEAR’s public IP address **4**. If you are using Dynamic DNS, or if the device has a DNS host name, use it instead (in our example, we are using the host name “vpn.example.com”)
- ▶ **Local Address:** Enter the Local IP address **8** you determined.
- ▶ **Remote Networks:** Enter the network address **7** and the subnet mask **6** of the network that is being accessed through the VPN tunnel 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. “vpntracker.local”) **3**
 - ▶ **Remote:** Enter the **local** identifier from your NETGEAR (e.g. “netgear.local”) **2**

Task 3 – Test the VPN Connection (Alternate Configuration)

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

It's time to go out!

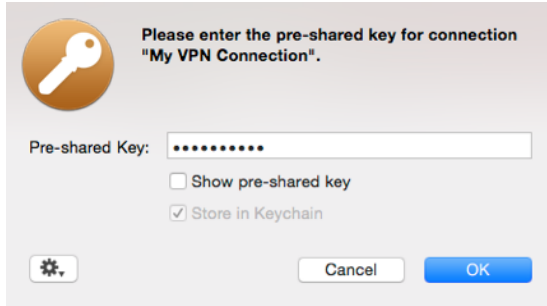
You will not be able to test and use your VPN connection from within the internal network that you want to connect to. To test your connection, you will need to connect from a different location. For example, if you are setting up a VPN connection to your office, test it from home. If you are setting 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!

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 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. **Many of the settings here correspond to settings located in VPN Tracker on the Basic tab, or under Advanced > Phase 1.**

General

General	
Policy Name	<input type="text" value="vpntracker"/>
Direction/Type	<input type="button" value="Responder"/>
Exchange Mode	<input type="button" value="Aggressive Mode"/>

Policy Name: The policy name is used only for naming connections on the device. Use a name that you will recognize later.

Direction / Type: Must be “**Remote Access**” or “**Responder**” for VPN clients to be able to connect. Remote Access policies are typically created through the device's VPN Wizard.

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	
Local Identity Type	Fully Qualified Domain Name
Local Identity Data	netgear.local
<hr/>	
Remote	
Remote Identity Type	Fully Qualified Domain Name
Remote Identity Data	vpntracker.local

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

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

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

Remote Identity Data: The remote identity data on the device must

IKE SA Parameters

IKE SA Parameters	
Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Authentication Method	<input checked="" type="radio"/> Pre-shared Key <input type="radio"/> RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group	Group 2 (1024 Bit)
SA Life Time	86400 (secs)

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.

Encryption Algorithm: The encryption algorithm 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).

Authentication Algorithm: The authentication algorithm must match the hash algorithm configured in VPN Tracker (Advanced > Phase 1 > Hash Algorithms). Do not select more hash algorithms in VPN Tracker than the one selected on the device.

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 strong 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).

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 Life Time: 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 86400 sec (24 hours) is generally a good choice. It is not recommended to set the lifetime lower than 3600 sec (1 hour).

VPN Policy

The VPN Policy contains the settings for the second phase in the process of establishing a VPN connection. **Many 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

General	
Policy Name	<input type="text" value="vpntracker"/>
IKE policy	<input type="text" value="vpntracker"/> ▾
<input type="checkbox"/> IKE Keep Alive	Ping IP Address: <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Remote VPN Endpoint	Address Type: <input type="text" value="Fully Qualified Domain Name"/> ▾ Address Data: <input type="text" value="vpntracker.local"/>
SA Life Time	<input type="text" value="28800"/> (Seconds) <input type="text" value="0"/> (Kbytes)
<input checked="" type="checkbox"/> IPSec PFS	PFS Key Group: <input type="text" value="Group 2 (1024 Bit)"/> ▾

Policy Name: The policy name is used only for naming connections on the device. Use a name that you will recognize later.

IKE Policy: Select the corresponding IKE policy. An IKE policy that is not selected in any VPN policy cannot be accessed. However, selecting an IKE policy here does not automatically mean that connections from the selected IKE policy will use this VPN policy, the VPN policy lookup on this device is independent from the IKE

policy and determined by the traffic selectors.

IKE Keep Alive: This setting is relevant for VPN connections established between the NETGEAR and another gateway. For client connections such as VPN Tracker, it should be left disabled.

Remote VPN Endpoint: This is the (public) IP address of the connecting client. With clients connecting from different IP addresses, it should be set to “Fully Qualified Domain Name”. Enter the same Fully Qualified Domain Name (FQDN) that is used for the “Remote Identity Data” in the IKE Policy.

SA Life Time: 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 28800 sec (8 hours) is generally a good choice. It is not recommended to set the lifetime lower than 3600 sec (1 hour). Due to the complications involved with a lifetime that depends on data transfer amounts, we recommend setting the lifetime in “Seconds” only, and setting the “Kbytes” field to 0.

IPsec PFS: The setting must match the Perfect Forward Secrecy (PFS) setting in VPN Tracker (Advanced > Phase 2 > Perfect Forward Secrecy (PFS)). Using PFS is more secure.

IPsec PFS Key Group: The PFS key 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.

Traffic Selector

Local IP	Subnet address ▾
	Start IP address: 192 . 168 . 13 . 0
	Finish IP address: 0 . 0 . 0 . 0
	Subnet Mask: 255 . 255 . 255 . 0
Remote IP	Any ▾
	Start IP address: 0 . 0 . 0 . 0
	Finish IP address: 0 . 0 . 0 . 0
	Subnet Mask: 0 . 0 . 0 . 0

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

- ▶ The **local** (=NETGEAR) side of the tunnel should 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” for Remote Access policies

with a single concurrent user. Responder policies or Remote Access policies for multiple users should have a fixed single IP address here (see “The Role of the Local Address in VPN Tracker” for more information).

Advanced Users If you are not setting the remote part of the Traffic Selection to “Any” (for example, because you have different VPN policies all used by clients connecting from dynamic IP addresses), 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.

AH Configuration

AH Configuration
 Enable Authentication Authentication Algorithm: SHA-1

Enable Authentication: VPN Tracker uses Encapsulating Security Payload (ESP) with authentication. Using Authentication Header (AH) is not necessary and not supported. It should be turned off.

ESP Configuration

ESP Configuration
 Enable Encryption Encryption Algorithm: 3DES
 Enable Authentication Authentication Algorithm: SHA-1

Enable Encryption: This setting ensures that data transferred through the VPN tunnel is encrypted. It should always be turned on, and must match the corresponding setting in VPN Tracker (Advanced > Phase 2 > 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 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

Enable Authentication: This setting ensures that data sent through the VPN tunnel is authenticated. It should always be turned on, and must match the corresponding setting in VPN Tracker (Advanced > Phase 2 > Authentication Algorithms). Do not select more authentication algorithms in VPN Tracker than the one selected on the device. NETGEAR uses SHA-1 by default (which corresponds to HMAC SHA-1 in VPN Tracker, MD5 on the NETGEAR corresponds to HMAC MD5 in VPN Tracker).

NETBIOS

NETBIOS Enable

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

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

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

Setting a (suitably chosen) fixed Local Address is always a good idea. You **must** use a fixed Local Address in VPN Tracker if

- ▶ multiple clients (users/computers) use the VPN
- ▶ 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._

Tip If your VPN needs expand to more than a handful of users, you may want to consider upgrading to a VPN gateway that can automatically distribute IP addresses through Mode Config.

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

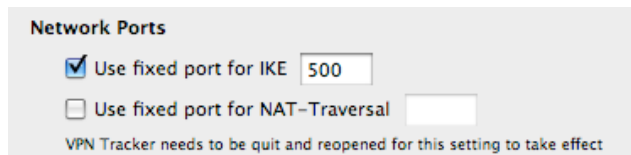
- ▶ set a route to the NETGEAR for the VPN clients' IP addresses on each host that needs to communicate with VPN clients, or
- ▶ have the default gateway redirect all traffic for the VPN clients' IP addresses to the NETGEAR

Outgoing Network Ports

The FVS318v3 requires VPN connections to originate from network port 500. This is the default network port used by VPN Tracker. However, there are some circumstances under which VPN Tracker connections will not originate from port 500, resulting in the VPN connection timing out right at the beginning of the connection process.

Outgoing Network Ports Changed by VPN Tracker

To increase compatibility with other VPN-related software (such as “Back to My Mac” in Mac OS X 10.5 Leopard), VPN Tracker has an option to use different outgoing network ports. **This option cannot be used when connecting to FVS318v3 VPN gateways.**



▶ Go to “VPN Tracker 6 > Preferences”

▶ Make sure that your settings are as shown in the screenshot. You will have to restart VPN Tracker for any changes to take effect.

Outgoing Network Ports Changed by the Local Router

Some local routers will modify the network ports of outgoing VPN connections while performing Network Address Translation (NAT). If you suspect that this is happening with your local (!) router, you should try the VPN connection from an Internet connection where you are not “behind” a NAT router, i.e. your Mac has a public IP address (instead of a [private IP address](#)).

You will likely receive a public IP address directly from your ISP if:

- ▶ Your Mac is connected directly to a DSL modem using PPoE
- ▶ Your Mac is connected directly to a modem using PPP
- ▶ Your Mac is connected directly to a cable modem

Tip You may be able to influence your local router's NAT behavior by setting a port forwarding of port 500 on your router to port 500 on your Mac. Please note that the port forwarding itself is not necessary for VPN Tracker to work, but it may cause your router to preserve outgoing port numbers for your Mac and port 500, which is exactly