e·quinux

VPN Configuration Guide

NETGEAR® FVS114 / FVS318v3

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 additional features to your connection once you have the basic setup working.

Important Prerequisites

Your NETGEAR Device

This document applies to the following NETGEAR devices

- FVS114
- FVS318v3
  - The FVS318v1 and v2 use a different firmware. Refer to NETGEAR's product support website on how to recognize the different device revisions.

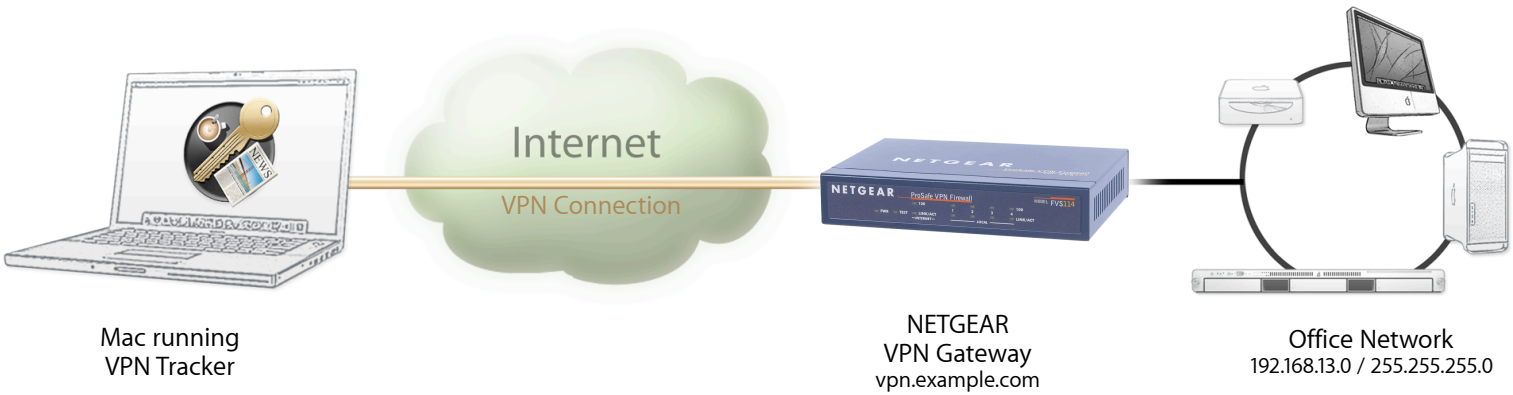
The documentation is based on firmware 1.1_15 (FVS114) and 3.0_27 (FVS318v3).

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

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.

❶ Pre-Shared Key: _____

❷ NETGEAR's Local Identifier: _____

❸ NETGEAR's Remote Identifier: _____

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

❺ LAN IP Address: _____ . _____ . _____ . _____

❻ LAN Subnet Mask: _____ . _____ . _____ . _____

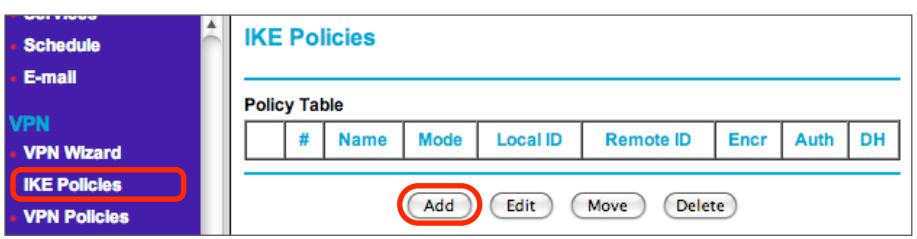
❼ LAN Network Address (calculated, see page 12): _____ . _____ . _____ . _____

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 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.

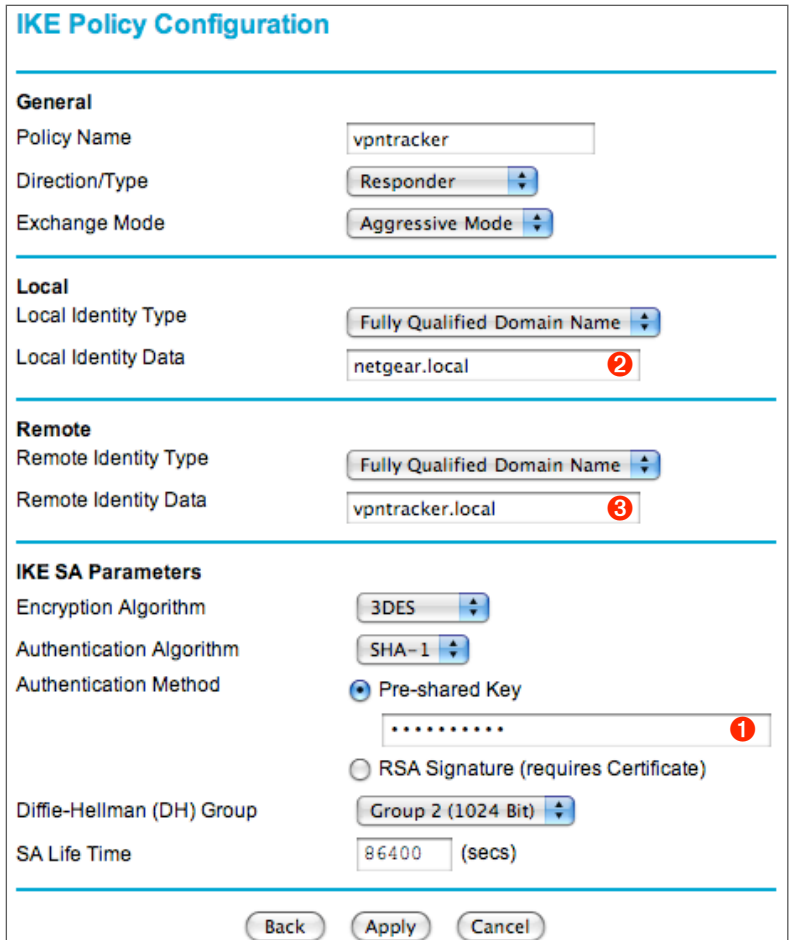
Advanced Users If you already have VPN in use on your device, you can use this chapter to verify your settings (refer to the chapter "VPN Settings Explained" for more detailed information about the settings available on your NETGEAR). If you have multiple VPN policies set up on the device, you will have to ensure that there are no unintended side-effects. Please read the chapter "Supporting Multiple Users" to learn how to set up multiple tunnels without them interfering with each other.

Step 1 – Create a new IKE policy



- Go to **VPN > IKE Policies**
- Click "Add"

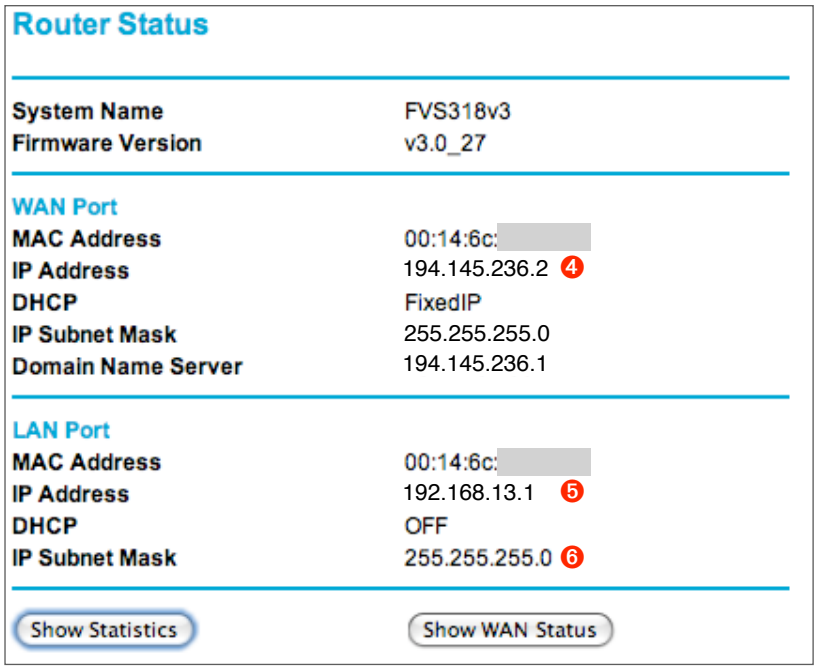
Note Make sure you have a current backup of your NETGEAR's configuration before making any changes.



- **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 ❷
- **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 ❸
- **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 ❶
- **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 2 – Retrieve your NETGEAR's LAN and WAN Configuration



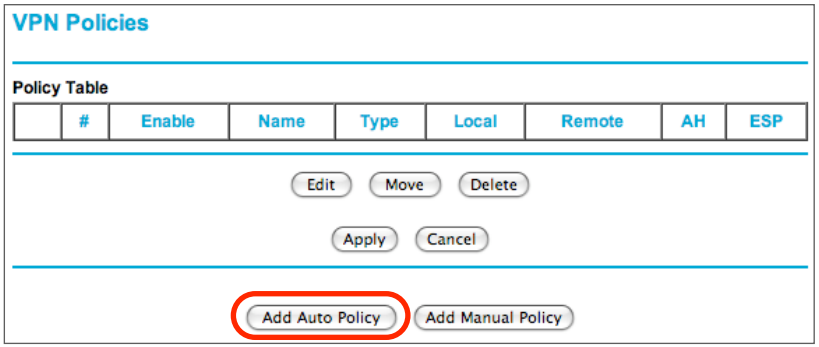
- Go to **Maintenance** > **Router Status** and obtain the following information from the Router Status page:
  - **WAN Port:**
    - Write down the **WAN IP Address** ❹
    - If you use Dynamic DNS for your device, or if it has a DNS host name, write down the host name instead
  - **LAN Port:**
    - Write down the **LAN IP Address** ❺
    - Write down the **LAN IP Subnet Mask** ❻
- Calculate your **LAN Network Address** by applying the **LAN Subnet Mask** ❻ to the **LAN IP Address** ❺:
  - 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 (*)
  - In our example:

LAN Subnet Mask	255	255	255	0
applied to	⇩	⇩	⇩	⇩
LAN IP Address	192	168	13	1
LAN Network Address	192	168	13	0

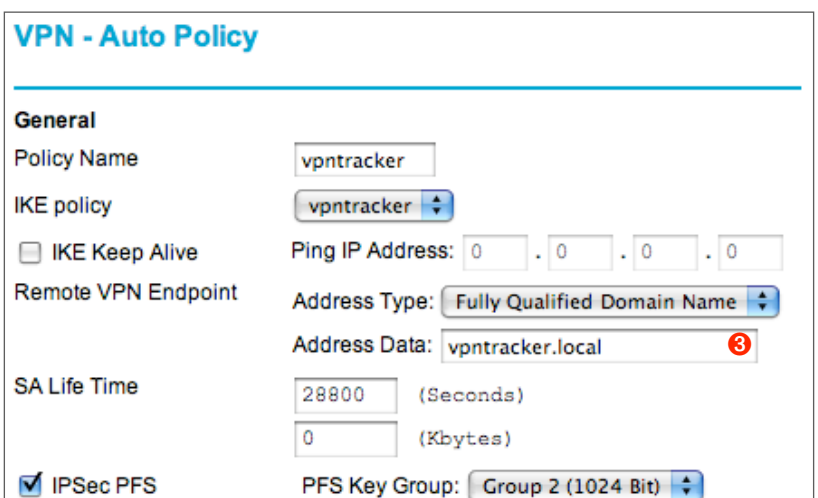
  - Write down the **LAN Network Address** you have calculated as ❼

(*) 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.

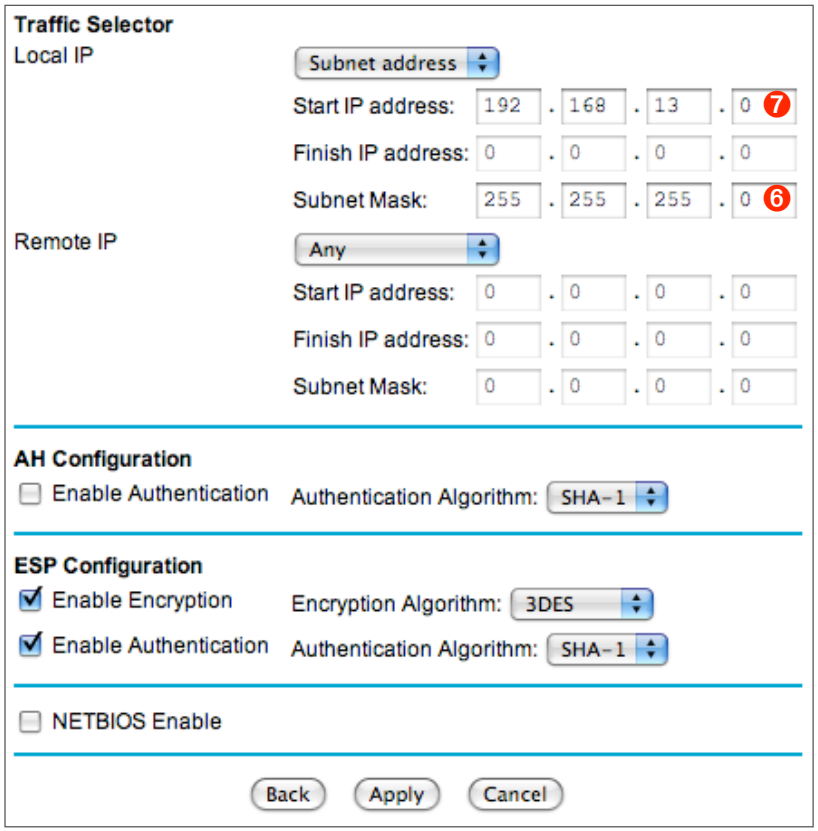
Step 3 – Create a new VPN Policy



- Go to **VPN > VPN Policies**
- Click "Add Auto Policy"



- **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 ❸ 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)"

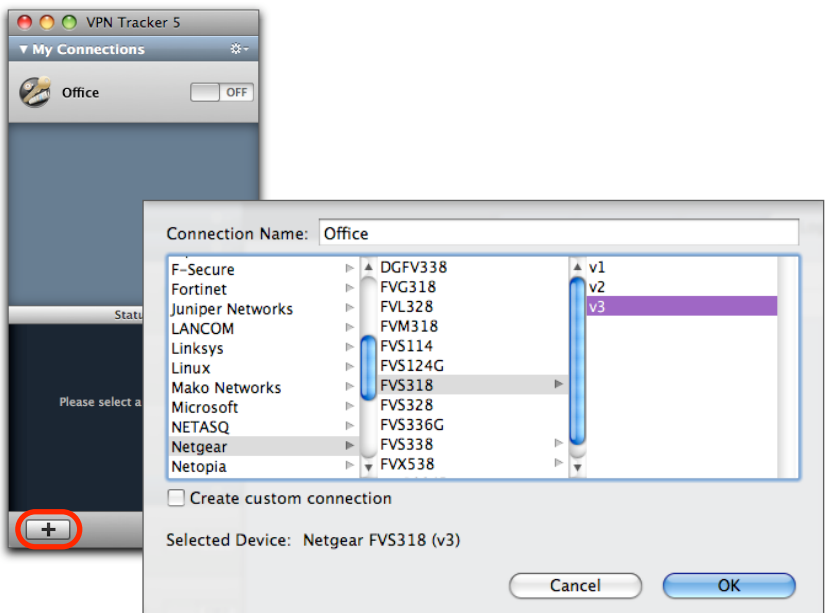


- **Local IP**: Select "Subnet Address"
  - **Start IP address**: Enter the LAN Network Address 7 you calculated in Step 2 (here:192.168.13.0)
  - **Subnet Mask**: Enter the LAN subnet mask 6 you wrote down in Step 2 (here: 255.255.255.0)
- **Remote IP**: Select "Any"
- **AH Configuration**: Leave this 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

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

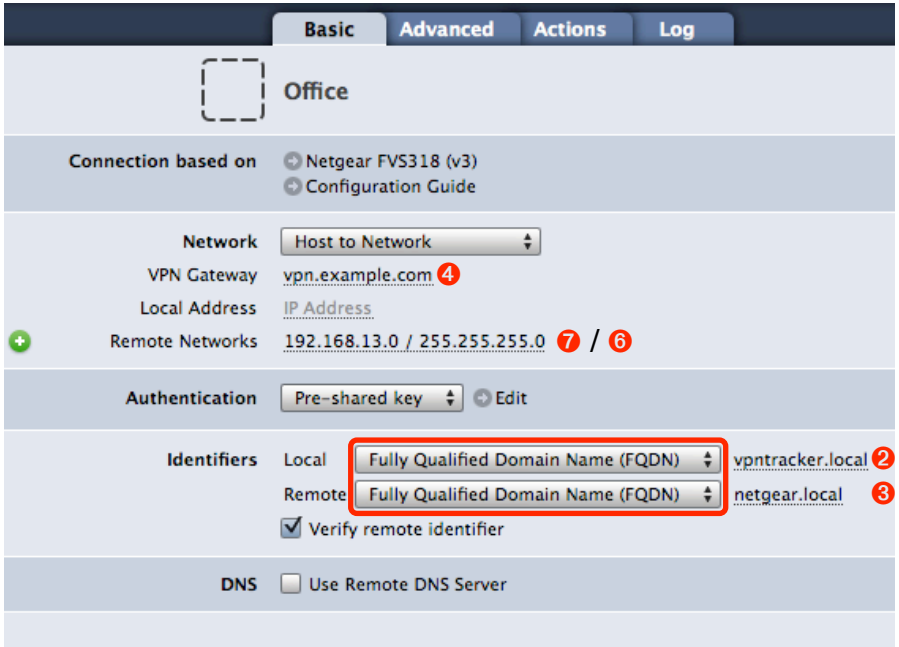


- Start VPN Tracker
- Click the "+" button in the main window

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 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



- **VPN Gateway**: Enter your NETGEAR's public IP address ❹. 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 ❼ and the subnet mask ❻ 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") ❸
  - **Remote**: Enter the **local** identifier from your NETGEAR (e.g. "netgear.local") ❷

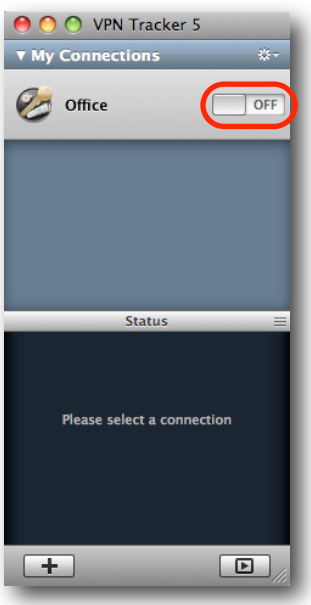
Task 3 – Test the VPN Connection

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

It's time to go out!

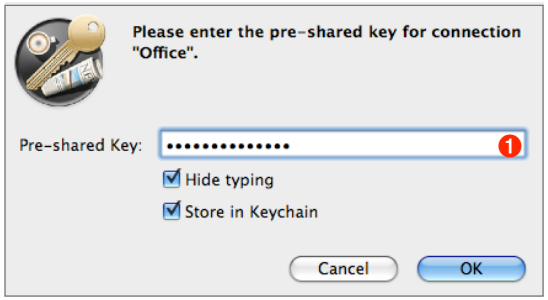
You will not be able to test and use your VPN connection from within the internal network that you want to connect to. To test your connection, you will need to connect from a different location. For example, if you are setting up a VPN connection to your office, test it from home. If you are setting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

Start your connection

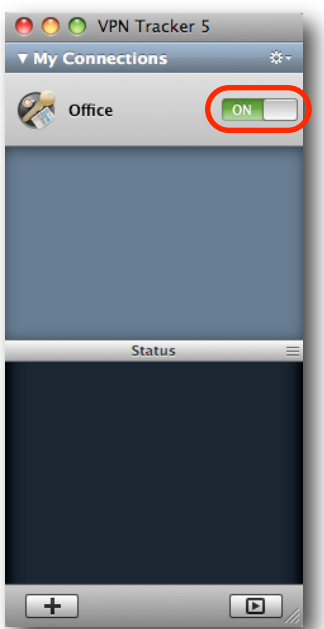


- Connect to the Internet
- Make sure that your Internet connection is working – open your Internet browser and try to connect to http://www.equinux.com
- Start VPN Tracker if it's not already running
- Slide the On/Off slider for the connection you have just configured to **On**

When you are prompted for your pre-shared key:



- **Pre-shared key**: Enter the pre-shared key that you configured on the NETGEAR device ❶
- 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 (or even just yourself connecting from multiple computers simultaneously), there are certain issues you will have to consider. Primarily, you must ensure that IP addresses do not conflict. 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 Conflicts

If multiple users connect using the same policy on 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.

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, 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.

Adding more VPN Tunnels

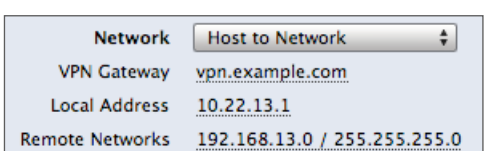
The tunnel you have set up in the first part of this document can be used by multiple users if you set an individual Local Address for each of them, as described in "Choosing the Local Address". **This is the recommended setup**.

However, there may be situations where it is necessary to create additional VPN tunnels, instead of reusing one tunnel. For example, if you need to issue users individual pre-shared keys, you can add multiple VPN tunnels with different pre-shared keys. Or you may require a static gateway-to-gateway tunnel, in addition to a tunnel used by VPN clients.

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) in order to avoid having to set up an individual VPN tunnel on the device for each user, just to be able to issue them individual passwords.

When more than one tunnel is configured and enabled on the device, you will have to ensure that there are no conflicts:

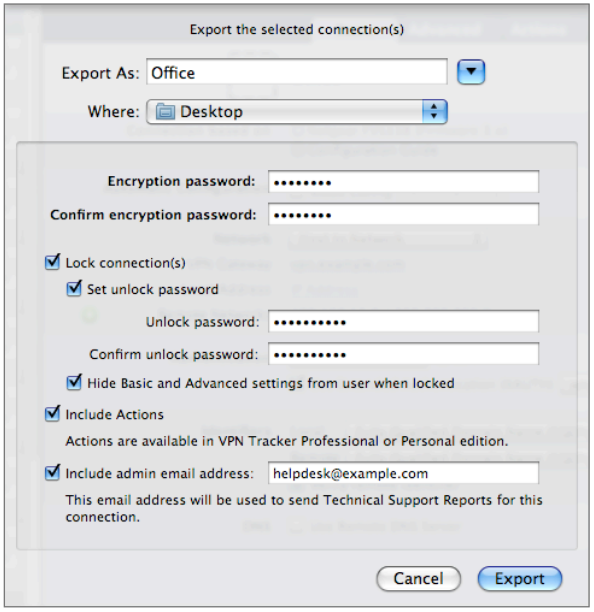
- For the IKE policies, make sure that the identifiers for each tunnel are different.
- If you have more than one tunnel used by clients connecting from dynamic IP addresses, make sure that the "Remote IP" is "Any" for **only one** of the policies. The "Any" policy should be **at the bottom of the list** since the device will try matching VPN policies from top to bottom, and use the first matching VPN policy. For the other tunnels, set a fixed remote IP that is the same as the "Local Address" in VPN Tracker. In the following example, the address "10.22.13.1" is used both on the device and in VPN Tracker:



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.

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.



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 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 will not be displayed to users
- **Set Unlock Password**: In case you need to make a quick modification to a locked connection on a user's Mac, you can add an unlock password that will allow 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 followed the instructions above. If you cannot connect, please read on.

VPN Connection Fails to Establish

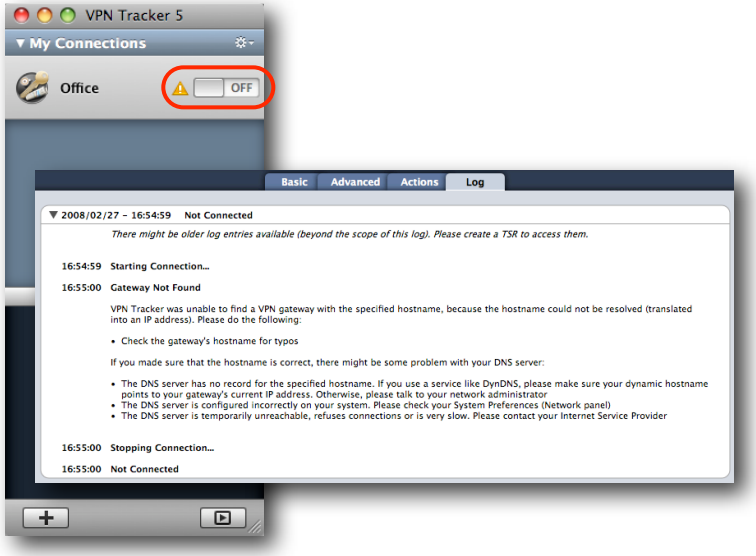
On/Off Slider goes back to "Off" right away

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.



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 whether the IP address is part of the remote network

Please make sure that the IP address of the resource that you are connecting to is actually contained in the remote network(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.

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

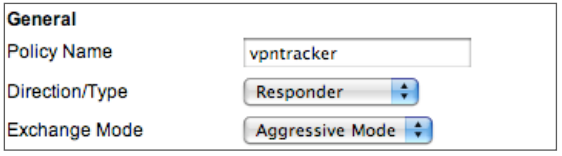
VPN Settings Explained

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 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

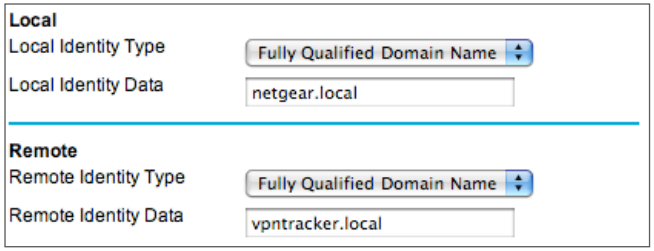


Policy Name: The policy name is used only for naming connections on the device. Use a name that you will recognize later.

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

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

Local and Remote Identifier



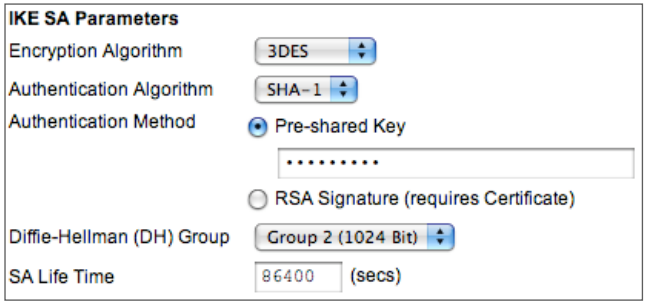
Local Identity Type: The local identity's type on the device must match the **Remote** Identifier Type (Basic > Identifiers) in VPN Tracker.

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 match the **Local** Identifier (Basic > Identifiers) in VPN Tracker.

IKE SA Parameters



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.

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).

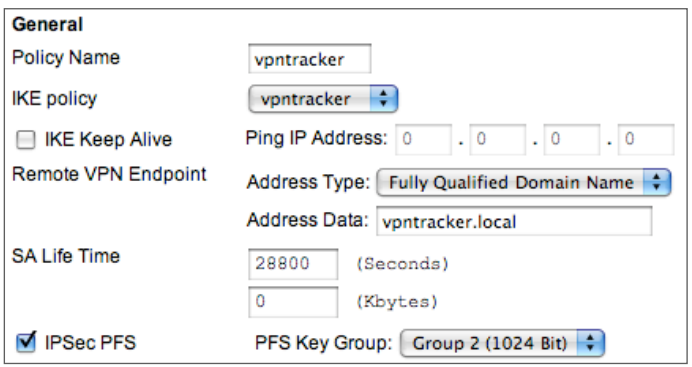
Diffie-Hellman (DH) Group: The Diffie-Hellman (DH) group defined here must match the group selected for phase 1 in VPN Tracker (Advanced > Phase 1 > Diffie-Hellman). Using a longer key (= higher number) is more secure, but may also be slower.

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



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.

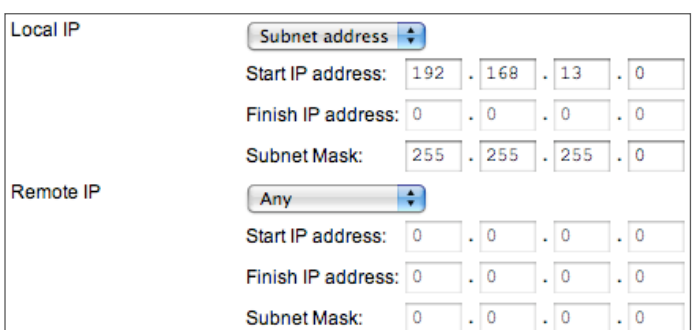
Remote VPN Endpoint: This is the (public) IP address of the connecting client. With clients connecting from different IP addresses, it should be set to "Fully Qualified Domain Name". Enter the same Fully Qualified Domain Name (FQDN) that is used for the "Remote Identity Data" in the IKE Policy.

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

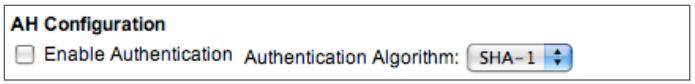


The Traffic Selection settings determine the endpoints of the VPN tunnel.

- 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".

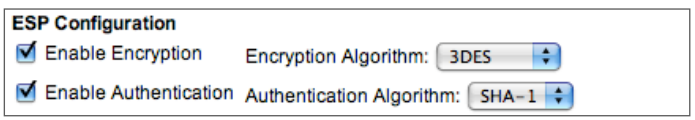
Advanced Users	If you are not setting the remote part of the Traffic Selection to "Any" (for example, because you have different VPN policies all used by clients connecting from dynamic IP addresses), it must match exactly what is configured in VPN Tracker as the Local Address (or Local Network, if using a Network to Network connection). Range type addresses are not supported in VPN Tracker.

AH Configuration



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



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 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: 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 FVS114 and FVS318v3 require 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 can optionally use any available non-standard network port for outgoing VPN connections. **Using non-standard network ports for outgoing VPN connections is not possible when connecting to FVS114 or FVS318v3 VPN gateways.**

To ensure that VPN Tracker uses only the standard network port 500 for outgoing VPN connections:

- Go to "**VPN Tracker 5 > 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