e·quinux

VPN Tracker 365

VPN Configuration Guide

NETGEAR® FVG318 / FVS318G / FVS318N / FVS336G / FVS338 / DGFV338
FVX538 / SRXN3205 / SRX5308 / ProSecure™ UTM Series

Contents

Introduction

This configuration guide helps you configure VPN Tracker and your NETGEAR VPN Gateway to establish a VPN connection between them.

Prerequisites

Your VPN Gateway

This document applies to the following NETGEAR VPN firewalls

‣ FVG318[1]

‣ FVS318G

‣ FVS318N

‣ FVS336G

‣ FVS338

‣ DGFV338

‣ FVX538

‣ SRXN3205

‣ SRX5308

‣ ProSecure UTM Series[2]

Documentation for other NETGEAR devices may be available at http://www.vpntracker.com/interop.

Your Mac

‣ Make sure you have all available updates installed. The latest VPN Tracker updates can be obtained from http://www.vpntracker.com

Using the Configuration Guide

NETGEAR Configuration

In the first part of this guide, we'll show you how to configure your NETGEAR device for VPN access. If you already have VPN set up, use this part of the guide to see which settings you'll need for VPN Tracker.

> If you are setting up VPN on your NETGEAR firewall for the first time, we strongly recommend using the setup proposed in this guide, and making modifications once that is up and running.

VPN Tracker Configuration

In the second part, this guide will show you how to configure VPN Tracker to easily connect to your newly created VPN.

Supporting Multiple Users and Reference

In the last part of the guide you'll see how to expand your VPN to multiple users, including individual user passwords using Extended Authentication (XAUTH) and automatic IP address assignment via Mode Config. You'll also find a reference of all NETGEAR VPN settings.

Conventions Used in This Document

Links to External Websites

Sometimes you will be able to find more information on external websites. Clicking links to websites will open the website in your web browser.

---

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

[2] Using firmware 1.0.16.0 or higher.

Links to Other Parts of this Guide

A → *Link* will take you to another place in the configuration guide. Simply click it if you are reading this guide on your computer.

Scenario

In our example, we need to connect an employee's Mac to an office network. The diagram below illustrates this scenario.

This guide assumes that the Mac running VPN Tracker 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 (here: 203.0.113.1) or a DNS host name (here: vpn.example.com).
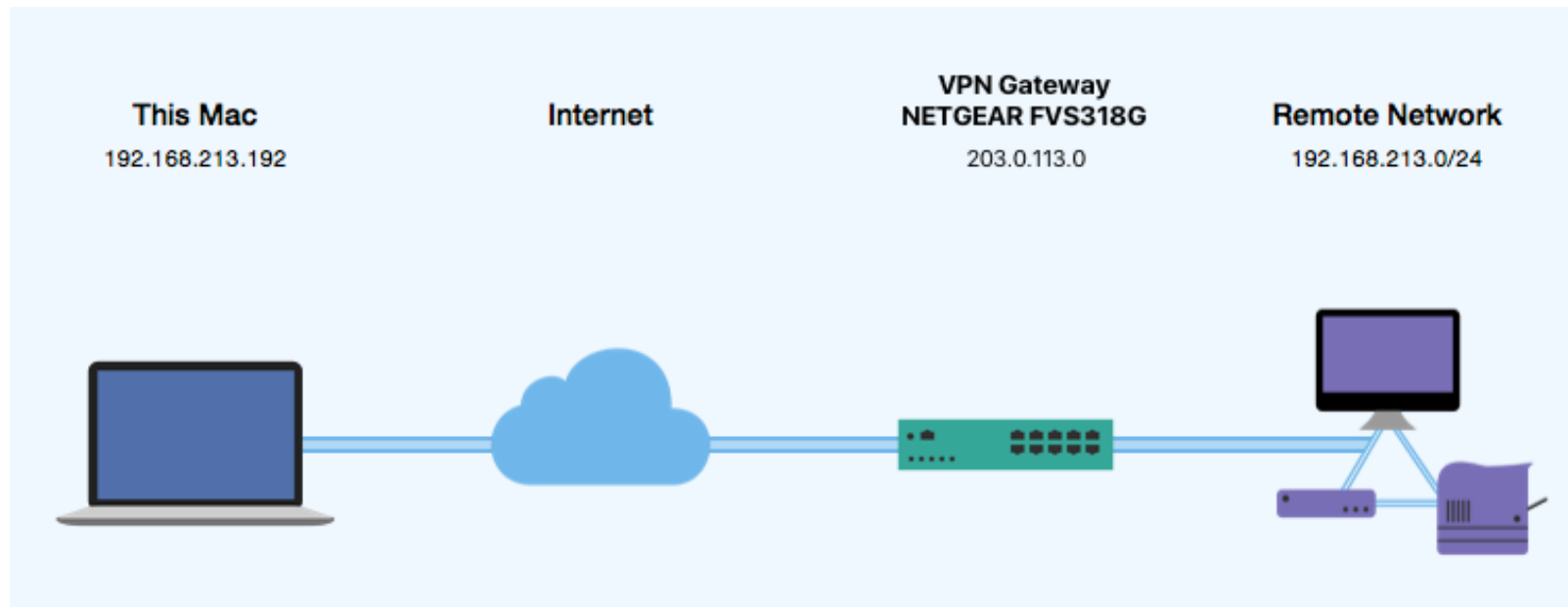
The VPN gateway's LAN interface is connected to the internal office network. In our example, the office network is 192.168.13.0 / 24 (which is the same as 192.168.13.0 / 255.255.255.0). This is the network that will be accessed from the Mac through the VPN. It is called the "Remote Network" in VPN Tracker.

Terminology

A VPN connection is often called a **tunnel**. A VPN tunnel is established between two **endpoints**. Here one endpoint is VPN Tracker and the other endpoint is the VPN gateway. Each endpoint is the other endpoint's **peer**.

For each endpoint, the other endpoint's settings **remote**, while its own settings are **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 topology shown below is called **Host to Network**: A single computer, a **host**, establishes a VPN to an entire network "behind" the VPN gateway.

This Mac	Internet	VPN Gateway NETGEAR FVS318G	Remote Network
192.168.213.192		203.0.113.0	192.168.213.0/24

My VPN Gateway 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. You can print out this checklist to help keep track of the various settings of your NETGEAR VPN gateway. Not all settings are required for every setup, so don't worry if some stay empty.

IP Addresses

❶ NETGEAR WAN IP Address: _____._____._____._____ or host name _____

❷ NETGEAR LAN Network: _____._____._____._____ / _____._____._____._____

Identifiers

❸ NETGEAR Remote Identifier: _____ = **Local** (!) Identifier in VPN Tracker

❹ NETGEAR Local Identifier: _____ = **Remote** (!) Identifier in VPN Tracker

Pre-Shared Key

❺ Pre-Shared Key: _____

User Authentication (XAUTH)

❻ User Name: _____   ❼ Password: _____

Task 1 – NETGEAR Configuration

We will first set up VPN on the NETGEAR firewall. In case you already have VPN in use on your device, you can skip ahead to steps 3 and 4 to verify your settings.

Step 1 – WAN IP Address

‣ Go to **Monitoring > Router Status**.

‣ Write down the **WAN IP Address** as ❶ on your → *Configuration Checklist*.

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

Step 2 – Run the VPN Wizard

‣ Go to the **VPN** section (**IPsec VPN** subsection if your device has that).

‣ Click **VPN Wizard**.

Step 3 – Review the VPN Policy

‣ Go to **VPN > Policies**.

‣ Make sure the **VPN Policies** tab is selected.

‣ Click **Edit** for the VPN policy.

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

‣ **Policy Name**: The connection name from the VPN Wizard.

‣ **Remote Endpoint**: Should be the same as the remote identifier used in the VPN wizard. The actual value may differ on your device.

‣ **Traffic Selection:** The local part of the traffic selection section is automatically configured by the VPN Wizard to reflect your NETGEAR's LAN configuration. The actual value will likely differ on your device. Write down the **Start IP Address** followed by a forward slash (/) and the **Subnet Mask** as ❷ on your → Configuration Checklist. In this example, you would write: 192.168.13.0 / 255.255.255.0

If you would like to use different algorithms, we recommend changing the settings only once you've got the basic setup working. If you make any changes to the **Auto Policy Parameters**, you'll need to match these settings in VPN Tracker on the **Advanced tab** of your VPN connection (Advanced > Phase 2).

9

Step 4 – Review the IKE Policy

‣ Select the "**IKE Policies**" tab

‣ Click "Edit" for the IKE policy

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

‣ **Policy Name**: The connection name from the VPN Wizard.

‣ **Local ❹ and Remote ❸ Identifiers:** May differ from the ones shown here if your device uses different default identifiers in the VPN Wizard or if you modified those values.

‣ **Pre-shared key ❺:** The pre-shared key from the VPN Wizard.

If you skipped the VPN Wizard and are working with an existing setup, please write down the identifiers and the pre-shared key on your → *Configuration Checklist* now.

⚠ If you would like to use different algorithms, we recommend changing the settings only once you've got the basic setup working. If you make any changes to the **IKE SA Parameters**, you'll need to match these settings in VPN Tracker on the **Advanced tab** of your VPN connection (Advanced > Phase 1).

Task 2 – VPN Tracker Configuration

After finishing Task 1, you should have a completed → *Configuration Checklist* containing your NETGEAR's settings. We'll now create a matching setup in VPN Tracker.

Step 1 – Add a Connection

‣ Click **Create**.

For some devices, more than one firmware revision is available. Please select the one corresponding to the firmware installed on your device.
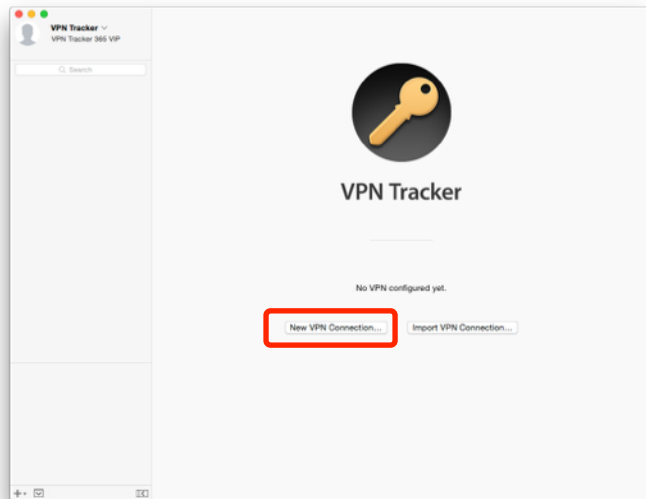
‣ Open VPN Tracker.
‣ Click **New VPN Connection…** (or click the + button in the lower left corner).
‣ Select **NETGEAR** from the list.
‣ Select your NETGEAR **model** (e.g. FVS318G).

Step 2 – Configure the VPN Connection

Please double-check your identifiers: The **Local** Identifier on your NETGEAR is the **Remote** Identifier in VPN Tracker, and vice versa.

- ▸ Click **Configure** and switch to the **Basic** tab if it is not already displayed.

- ▸ **VPN Gateway**: Enter your NETGEAR's public IP address or its host name ❶ from your → *Configuration Checklist*.

- ▸ **Remote Networks**: Enter your NETGEAR's LAN network ❷.

- ▸ **Local Identifier**: Enter your NETGEAR's remote (!) identifier ❹.

- ▸ **Remote Identifier**: Enter your NETGEAR's local (!) identifier ❸.

- ▸ Click **Done**.

Task 3 – Test the VPN Connection

Connect to your VPN

‣ Make sure that your Internet connection is working – open your Internet browser and check that you can open http://www.equinux.com

‣ Open VPN Tracker.

‣ Click the On/Off slider for your connection.

‣ If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection. Wait for the test to complete.
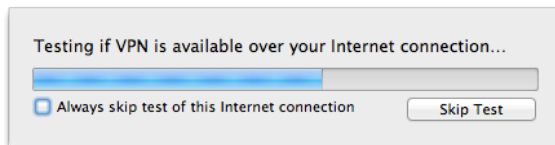
‣ You will be prompted to enter your pre-shared key ❺. Optionally, check the box **"Store in Keychain"** to save the password in your keychain so you are not asked for it again when connecting the next time.
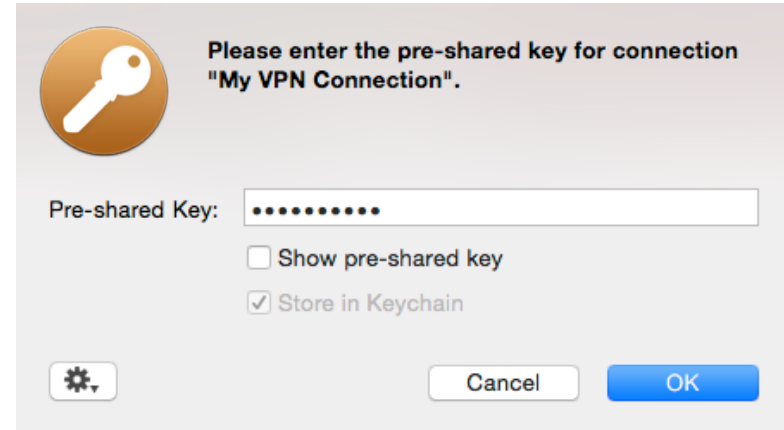
Connected!

Connecting may take a couple of seconds. If the On/Off button turns blue that's great – you're connected!
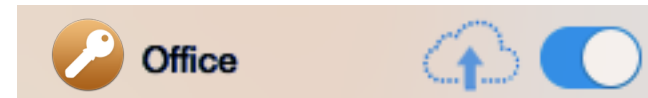
Now is a great time to take a look at the VPN Tracker Manual. It shows you how to use your newly established VPN and how to get the most out of it.

Troubleshooting

In case there's a problem connecting, a yellow warning triangle will show up:

Click the yellow warning triangle to be taken to the log. The log will explain exactly what the problem is. Follow the steps listed in the log.

💡 Press Cmd-L to open the log in a new window. That way, you can have the log side-by-side with your VPN configuration while making changes to troubleshoot a problem.

In most cases, the advice in the log should be sufficient to resolve the issue. However, VPNs are a complex topic and there might be trickier issues with which you need additional help.

VPN Tracker Manual

The [VPN Tracker Manual](#) contains detailed troubleshooting advice.

Frequently Asked Questions (FAQs)

Answers to frequently asked questions can be found at

http://www.vpntracker.com/support

Technical Support

If you're stuck, the technical support team at equinux is here to help. Contact information can be found at

http://www.vpntracker.com/support

Please include the following information with any request for support:

‣ A description of the problem and any troubleshooting steps that you have already taken.
‣ A VPN Tracker Technical Support Report (Log > Technical Support Report).
‣ NETGEAR model and the firmware version running on it.
‣ Screenshots of the VPN and IKE policy on your NETGEAR (please blank out the pre-shared key before sending screenshots).

💡 A Technical Support Report contains the settings and logs necessary for resolving technical problems. Confidential information (e.g. passwords, private keys for certificates) is **not** included in a Technical Support Report.

Supporting Multiple Users

Once your VPN expands to multiple users, two things are important: Individual logins so you don't have to change everyone's VPN password if someone leaves your organization, and distinct IP addresses for each user.

Individual User Logins Using XAUTH[3]

Extended Authentication (XAUTH) requires each user of the VPN to enter an individual username and password, in addition to the pre-shared key that is shared among all users of a VPN connection.

Add Users

Depending on your device, you'll find the user database in different locations:

‣ **VPN > VPN Client > User Database** or
‣ **Users > Users**

Go to the appropriate section on your device to add a new user.

---

[3] This feature is not available on FVG318 devices.

‣ **User Name**: Enter the user name for the new user ❻.
‣ **Password:** Enter a password for the new user ❼.
‣ **Confirm Password**: Re-enter the password for the new user.
‣ **User Type** (some devices): Select **IPSEC VPN User**.
‣ Click **Add**.

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

Configure the VPN Gateway to Use XAUTH

Disable the VPN Policy

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

‣ Go to **VPN > VPN Policies**.
‣ Place a checkmark at the row containing your VPN policy.
‣ Click **Disable**.

Modify the IKE Policy

‣ Go to **VPN > IKE Policies**.

- ▸ Click the **Edit** button in the row containing your IKE policy.
- ▸ Go to the **Extended Authentication** section.
- ▸ **XAUTH Configuration**: Select **Edge Device**.
- ▸ **Authentication Type:** Select **User Database**.
- ▸ Click **Apply**.

> It is possible to obtain the user names and passwords from an external RADIUS server: Set the authentication type to one of the RADIUS options instead of "User Database", and configure your RADIUS server under VPN > VPN Client > RADIUS Client.

Re-Enable the VPN Policy

- ▸ Place a checkmark at the row containing your VPN policy.
- ▸ Click **Enable**.

Configure VPN Tracker to use XAUTH

VPN Tracker should already have XAUTH set to **Automatic**. Check the **Basic** tab in VPN Tracker to make sure that this is the case.

Then connect the VPN. You should be asked for your XAUTH credentials.

- ▸ **User Name:** Enter the name of the user configured on the NETGEAR ❻.
- ▸ **Password**: Enter the password for this user ❼.
- ▸ Optionally, check **Store in Keychain** to save the user name and password so you are not asked for it again when connecting the next time.
- ▸ Click **OK**.

Assigning IP Addresses Using Mode Config[4]

When multiple users connect to the same VPN, it is very important that a unique IP address is used for each VPN client. The easiest way to ensure this, is to let the NETGEAR assign IP addresses to connecting VPN clients through Mode Config (see → *The Role of the Local Address in VPN Tracker* for alternative solutions).

Create an Address Pool for Mode Config
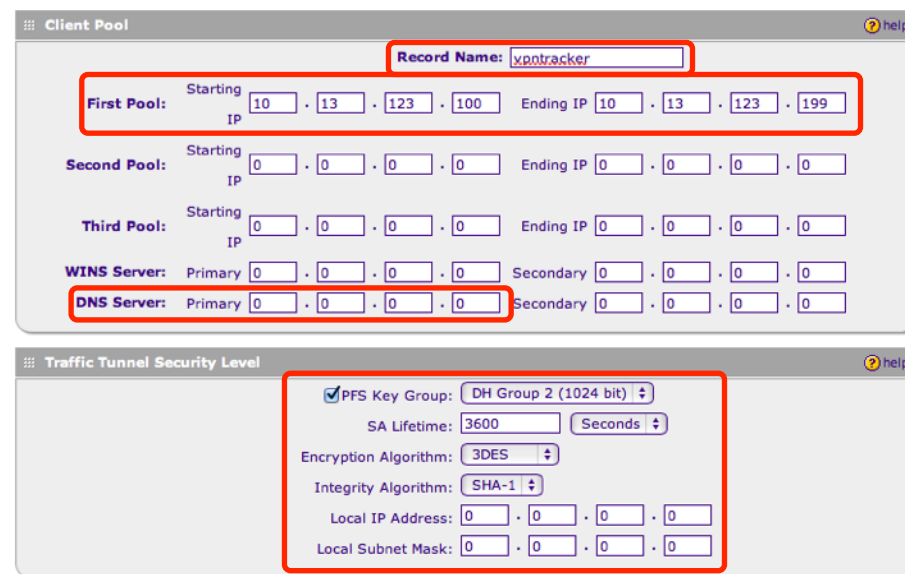
‣ Go to **VPN > Mode Config**. If there is an **IPsec VPN** subsection on your device, go to **VPN > IPsec VPN > Mode Config** instead.

‣ Click **Add**.

‣ **Record Name**: Enter a name for the address pool.

‣ **First Pool**: Enter an IP range that is **not (!)** part of your NETGEAR's LAN. It is a good idea to use an IP range from the private (RFC1918) IP address space, and to make the range large enough to support at least the maximum number of simultaneous connections expected.

‣ **DNS Server** (optional): If you operate your own DNS server, enter it here. Otherwise, leave 0.0.0.0.

‣ **Traffic Tunnel Security Level**: These settings correspond to the VPN Policy settings used for non-Mode Config connections. If you make changes here, you'll also need to change the corresponding settings in VPN Tracker (Advanced > Phase 2).

---

[4] This feature is not available on FVG318 devices.

‣ Click **Apply**.

Configure the IKE Policy to use Mode Config

Disable the VPN Policy

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

‣ Go to **VPN > VPN Policies**.

‣ Place a checkmark at the row containing your VPN policy.

‣ Click **Disable**.

Modify the IKE Policy

‣ Go to **VPN > IKE Policies**.

‣ Click the **Edit** button in the row containing your IKE policy.

‣ In the **Mode Config Record** section, turn on Mode Config by clicking **Yes**.

- Make sure the record you created earlier (in our example, "vpntracker") is selected.
- Click **Apply**.

> Once your IKE Policy is properly set up for Mode Config, a VPN Policy is no longer needed and can be removed.
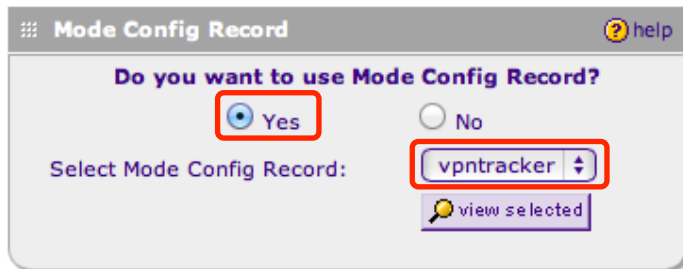
> Once you've confirmed that everything is working, you can try the "active" or "passive" variants to see if they let you connect more quickly.

Enable Mode Config in VPN Tracker

- Click "**Configure**" and switch to the **Basic** tab if it is not already displayed.
- On the Basic tab in VPN Tracker, switch **Network Configuration** to **Mode Config**. If you cannot find this setting for your device, make sure you have selected the correct device and firmware revision
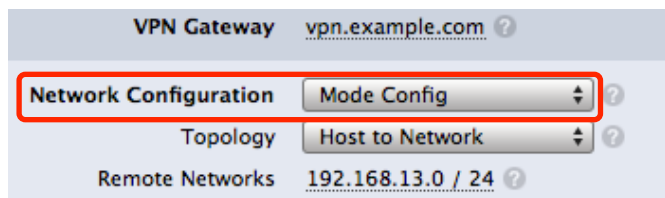
The Role of the Local Address in VPN Tracker

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

‣ If the Local Address field on VPN Tracker's Basic tab is left empty, the Mac's actual local IP address (as shown in System Preferences > Network) is used.

‣ If Mode Config is used, the local address is assigned automatically by the VPN gateway. The Local Address field will not be displayed.

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

When to Set the Local Address in VPN Tracker

When not using Mode Config, it can be beneficial to use fixed local addresses in VPN Tracker, instead of leaving the Local Address field empty.

There are some cases where you should always set a local address:

‣ Multiple clients (users/computers) connect to the VPN, and you cannot use Mode Config to assign IP addresses to them.

‣ The NETGEAR device is not the default gateway (router) of its LAN 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 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). Take the local addresses from an arbitrary [private network](#) that is not part of this network. Here we are using 10.22.13.0/24. Each user is assigned their own IP address from that network:

User	IP Address
alice	10.22.13.**1**
bob	10.22.13.**2**
charlie	10.22.13.**3**
...	10.22.13.**_**

Local Addresses for the More Curious

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

It may seem counter-intuitive to use IP addresses for VPN clients that are not part of the NETGEAR's LAN. The reason for this is that the NETGEAR cannot act as an ARP proxy for its VPN clients (ARP is the protocol used for turning IP addresses into Ethernet addresses). Not having an ARP proxy means that nobody will be responding to ARP requests on behalf of VPN clients (VPN clients themselves won't see ARP requests because they don't go through the VPN).

If IP addresses from outside the NETGEAR's LAN are being used, computers on its LAN will automatically send replies for VPN clients to

the NETGEAR (assuming that it is their default gateway), and therefore no ARP is required (for VPN client IP addresses).

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). The Macs themselves will use a private IP address for their Ethernet or Wi-Fi interface, and this is the IP address that is used by VPN Tracker if the local address field is empty.

The likelihood of two Macs ending up 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 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. It is therefore 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, computers that 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 give each VPN client a fixed local address.

Once you know which IP addresses VPN clients will be using, you can either

‣ set a route to the NETGEAR device 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.

VPN Settings Explained

This section explains the various settings found on your NETGEAR, and how they relate to VPN Tracker's settings. We will first go through the IKE policy settings from left to right, and from top to bottom, then we'll cover the VPN policy.

IKE Policy

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

Mode Config Record[5]

Mode Config is a way to automatically distribute IP addresses to VPN clients. If Mode Config is to be used, it must be enabled on the NETGEAR, as well as in VPN Tracker (Basic > Network Configuration).
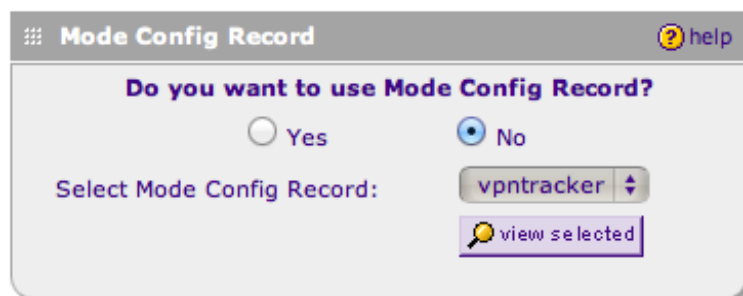
General

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

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

Exchange Mode: While Main Mode is considered to be more secure, Aggressive Mode works best for VPN clients connect from dynamic IP addresses.

The Exchange Mode configured here must match Advanced > Exchange Mode in VPN Tracker. If you must for some reason use Main Mode, please refer to your device's documentation for any prerequisites for using Main Mode.
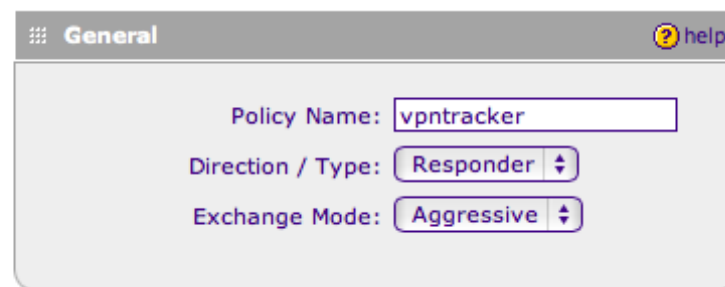
Local and Remote Identifier

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

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

---

[5] This feature is not available on FVG318 devices.

Local

Identifier Type: FQDN

Identifier: fvs_local.com

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

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

Remote

Identifier Type : FQDN

Identifier: fvs_remote.com

IKE SA Parameters

IKE SA Parameters

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

Encryption Algorithm: The encryption algorithm here must match the encryption algorithm configured in VPN Tracker (Advanced > Phase 1 > Encryption Algorithm). The device uses 3DES by default. AES-128/192/256 are considered to be even more secure.

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), using more than 2-3 algorithms (or algorithms not known to the device) may cause the connection to fail.

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

Authentication Method: Unless you already have a Public-Key In-frastructure (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. Please see your device's documentation for details.

Pre-shared key: This is the password for the VPN connection, and cor-responds to the same setting in VPN Tracker (Basic > Authentication). This password is shared among all users of the VPN connection.

Make sure to choose a good password here that is long and random (but be aware that your Mac and your NETGEAR may not use the same character encoding, so use only ASCII characters).

To require a user name and password for each user, in addition to the pre-shared key, use Extended Authentication (XAUTH).

Diffie-Hellman (DH) Group: The Diffie-Hellman (DH) group defined here must match the group selected for phase 1 in VPN Tracker (Ad-vanced > Phase 1 > Diffie-Hellman). Higher DH group numbers provide additional security but may have a performance impact on lower-end VPN gateways.

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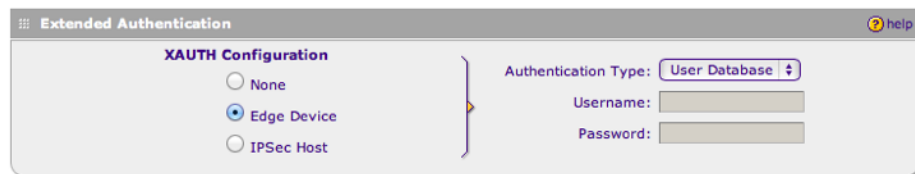
time for phase 1 in VPN Tracker (Advanced > Phase 1 > Lifetime). A value of 28800 sec (8 hours) is generally a good choice. It is not recommended to set the lifetime lower than 3600 sec (1 hour).

Dead Peer Detection (DPD): A mechanism to detect if the peer on the other side of the VPN connection is no longer responding.

Extended Authentication (XAUTH) [6]

XAUTH Configuration: When XAUTH is used, individual user names and passwords are required, in addition to the pre-shared key.

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

The **Authentication Type** determines where XAUTH user names and passwords are taken from – either from the device's user database or from an external RADIUS server.

The VPN Tracker works with or without XAUTH, simply set XAUTH to "Automatic" in VPN Tracker and VPN Tracker will do the right thing.

VPN Policy

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

---

[6] This feature is not available on FVG318 devices.

General

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

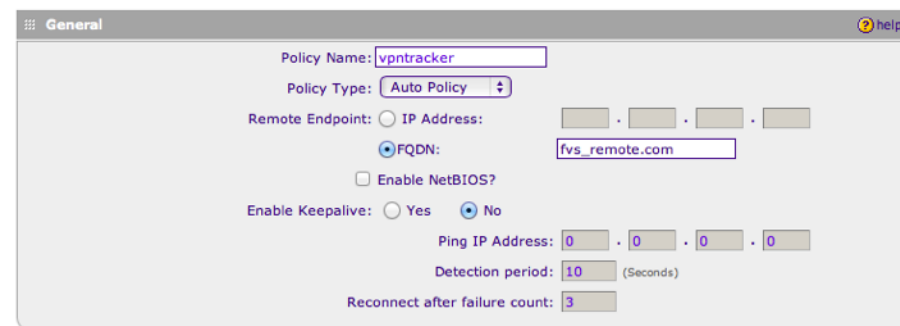**Policy Type**: The policy type must always be "Auto Policy".

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

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

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

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

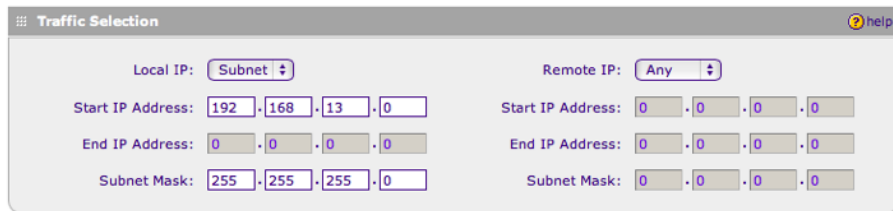**Enable Keepalive**: Keepalive should be turned off for a setup where a client is connecting to the NETGEAR.

Traffic Selection

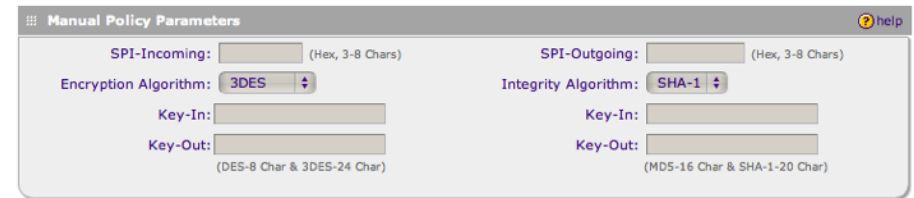The Traffic Selection settings determine the endpoints of the VPN tunnel.

‣ **If you are using the VPN Wizard** on the device, it will automatically fill in the correct values.

‣ If you are not using the wizard, the **local** (=NETGEAR) side of the tunnel needs to be configured to be a subnet matching the NETGEAR's LAN (192.168.13.0/255.255.255.0 is the NETGEAR's LAN in our example)

‣ The **remote** part should be set to "Any"

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

Manual Policy Parameters

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

Auto Policy Parameters

SA Lifetime: The lifetime determines how long a client can be connected before the encryption keys must be renegotiated. The lifetime must match the lifetime for phase 2 in VPN Tracker (Advanced > Phase 2 > Lifetime).

A value of 3600 sec (1 hour) is generally a good choice. It is not recommended to set the lifetime lower than 1 hour. Due to the complications involved with a lifetime that depends on data transfer amounts, we recommend to set the lifetime in "Seconds" (not in "KBytes").

Encryption Algorithm: The encryption algorithm selected here must match the encryption algorithm selected in VPN Tracker for phase 2. The device uses 3DES by default. AES-128/192/256 are considered to be even more secure.
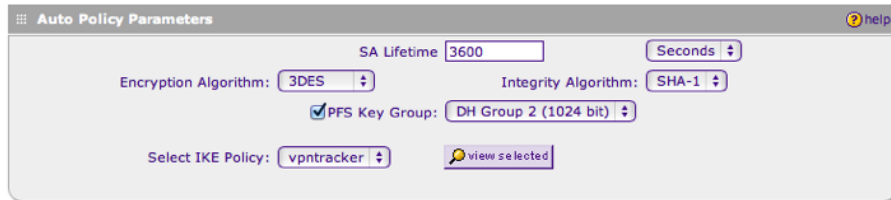
While is possible to set more than one encryption algorithm in VPN Tracker (as long as the one actually used by the device is among them), using more than 2-3 algorithms (or algorithms not known to the device) may cause the connection to fail.

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

PFS Key Group: This setting must match the Perfect Forward Secrecy (PFS) setting in VPN Tracker (Advanced > Phase 2 > Perfect Forward

Secrecy (PFS)). Using PFS is more secure. The selected group must match the PFS Diffie-Hellman (DH) group in VPN Tracker. Higher DH group numbers provide additional security.

Select IKE Policy: The corresponding IKE Policy for the connection.