



VPN Tracker Quick Setup Guide

NETGEAR® ProSafe™ FVS114 / FVS318v3

Edition 1.0

equinux AG and equinux USA, Inc.

© 2006 equinux USA, Inc. All rights reserved.

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

The equinux logo is a trademark of equinux AG and equinux USA, Inc., registered in the U.S. and other countries.

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

Manual Edition 1.0

Created using Apple Pages.

www.equinux.com

Apple, the Apple logo, iBook, Mac, Mac OS, MacBook, PowerBook are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

Finder and Mail are trademarks of Apple Computer, Inc. AppleCare is a service mark of Apple Computer, Inc., registered in the U.S. and other countries.

NETGEAR, NETGEAR Logo, Everybody's connecting. are trademarks of NETGEAR, Inc., registered in the U.S. and other countries.

FirstGear, Gear Guy Logo, ProSafe, Smart Wizard, RangeMax are trademarks of NETGEAR, Inc.

FileMaker is a trademark of FileMaker, Inc.

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

How to use this Guide.....	4
The sections of this guide.....	4
Prerequisites.....	4
The Checklist.....	4
Support.....	4
The five steps to your own VPN.....	5
Understand a VPN.....	6
What is a VPN?.....	6
Where can I use my VPN connection?.....	6
How my existing network has to be changed.....	7
Step 1: Configure your Network.....	10
1.1 Adding the VPN Router to your network.....	10
1.2 AirPort Base Station Integration.....	12
1.3 Network components are now set!.....	14
Step 2: Public IP Address Configuration.....	15
2.1 The difference between static and dynamic IP addresses....	15
2.2 What is a DynDNS service?.....	16
2.3 Create your DynDNS Account.....	16
2.4 Your DynDNS settings are now complete!.....	19
Step 3: NETGEAR Router Configuration.....	20
3.1 Check your equipment first.....	20
3.2 Configure your Public IP Address.....	23
3.3 Configure the NETGEAR VPN.....	26
Your VPN Router is now set up for your VPN connection!.....	28
Step 4: VPN Tracker Configuration.....	29
4.1 Install, start VPN Tracker and run the VPN Tracker Setup Assistant.....	29

Step 5: Check the VPN connection.....	35
5.1 It's time to go out!.....	35
5.2 Test your connection.....	35
Troubleshooting.....	37
What's next?.....	38
Introduction.....	38
Known Limitations.....	38
Accessing Files.....	39
Access your FileMaker Database.....	41
Access your IP cam.....	45
Acquire more Licenses.....	47
Your VPN Checklist.....	48

How to use this Guide

This guide has a step-by-step approach to help you set up your own Virtual Private Network.

The sections of this guide

The first section helps you to understand what a Virtual Private Network (VPN) is.

The sections **Step 1** through to **Step 5** will guide you through the VPN configuration. Each step includes a time estimate of how long it should take. The guide is designed in a way which allows you to pause the setup after major steps, then resume at a later time.

The **Troubleshooting** section will help you if anything goes wrong during the setup.

Last but not least, the **What next?** section will give you examples of how to leverage your new VPN.

Prerequisites

To setup your VPN, you'll need this Quick Setup Guide, VPN Tracker software, VPN Tracker Setup Assistant and a NETGEAR Router.

The Checklist

When setting up a VPN, you'll have to handle a couple of parameters. To make life easy, we have created a form, where you insert all parameters. Throughout the setup we will point back to those parameters - you'll always have them handy.

We call this form the **Checklist**. Please now unfold the **Checklist** on the last page of this guide.

Support

Setting up a VPN is no longer a hassle. equinux has made every effort to make the setup as easy as possible. If you still have questions, see the FAQ section of our website for more information (<http://www.equinux.com/goto/vpn-solution-faq/>).

OK. Let's get started!

The five steps to your own VPN

Setting up a VPN is easier than most people think. VPN technology is very advanced and up until now, only technically savvy people have been able to set up such a network. But now with the VPN Tracker **Quick Setup Guide**, setting up a VPN has been made easy.

This Guide will help you in 5 steps to setup a secure, remote connection to your **Private Network** (home or office). We estimate that you'll need a total of three hours to setup the whole VPN connection.

Step 1 **Configure your Network [~45 minutes]**

This step explains how you can integrate a VPN Router into your current network setup.

Step 2 **Public IP Address Configuration [~20 minutes]**

This step describes how to setup a public IP address for your VPN Router. This public address can either be static or dynamic.

Step 3 **Configure your VPN Router [~30 minutes]**

In order to connect to your Private Network from a remote location, you'll have to setup your VPN Router correctly.

Step 4 **VPN Tracker Setup Assistant [~5 minutes]**

The VPN Tracker Setup Assistant will help you setup the VPN Tracker software on your MacBook Pro.

Step 5 **Test the VPN Connection [~10 minutes]**

This is the final step and explains how to start and test your VPN connection.

Understand a VPN

This section explains the basic concept of a Virtual Private Network. It shows you how to change your existing network structure to support a VPN.

What is a VPN?

VPN is an abbreviation of **Virtual Private Network**. It allows you to connect into your Private Network (office or home) from anywhere in the world, through the Internet - Securely. You can then, for example, access your files and services, receive mails from your company, get contacts from your FileMaker database or retrieve a music file from your home/office computer. All that communication is done through a secure **tunnel** from anywhere in the world where you have an Internet connection.

Where can I use my VPN connection?

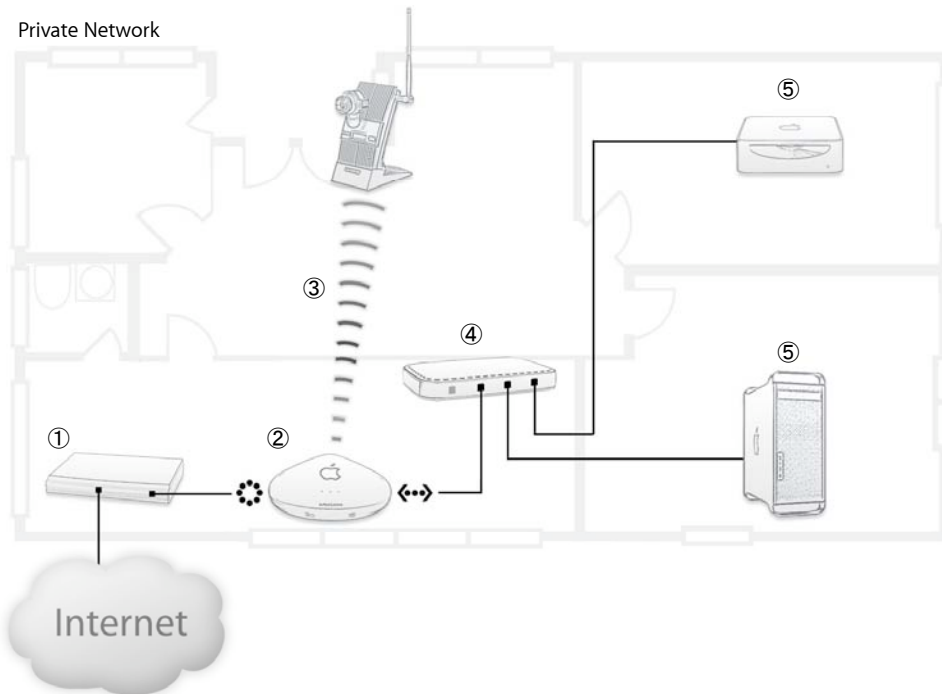
Whether you're working from a hotel, an Internet cafe or from your home office, VPN enables you to access important resources in your Private Network from any place at any time.

How my existing network has to be changed

Typically, one has an existing home or company network that is attached to the Internet using DSL or cable-modem with a standard router. This section describes how you can alter your existing network to make it VPN enabled, secure and remotely accessible.

Your current network setup

The following picture is an example of a typical network layout which can be found today in many homes or offices.



The network is usually connected to the Internet using a DSL or Cable Modem ①.

A router, in this example, is an AirPort Base Station ②, routes Internet traffic to the local network. It may also act as a WLAN base station ③.

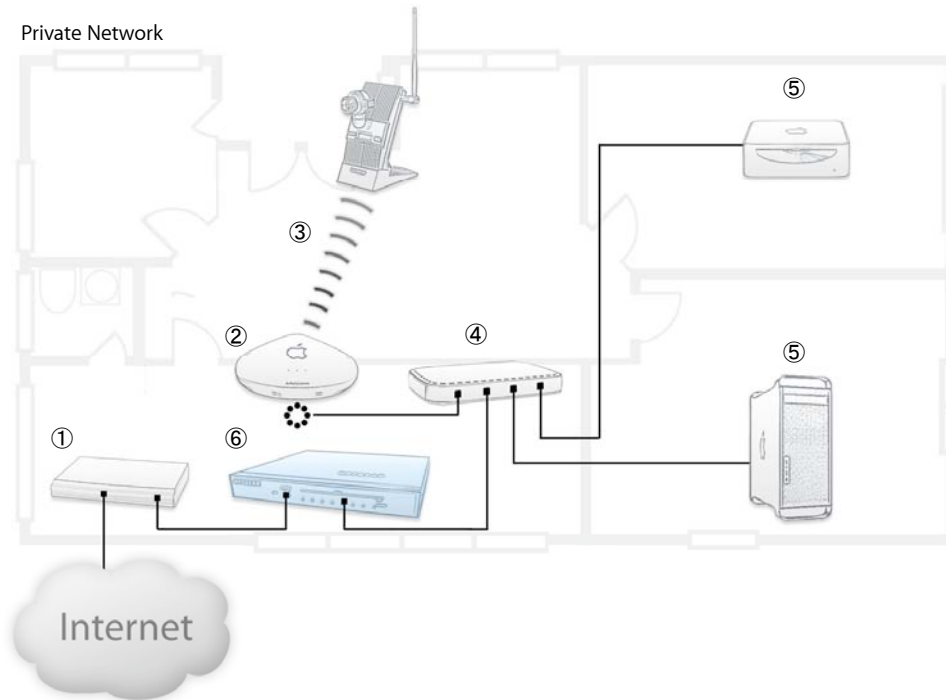
A network Hub or Switch ④ is often used for connecting other devices, like other workstations or servers ⑤ to the network.

Learn what has to be changed to get VPN functionality

The first task is to integrate the VPN NETGEAR Router into the current network setup. The basic change of this step is the replacement of the existing router with a VPN Router. The old router is then usually no longer needed, unless it is a WLAN and you need a wireless connection.

If your old router brought functionality to your network that you would like to remain using, i.e. WLAN access, then you should keep it. We'll explain how to keep and integrate the AirPort Base Station as a wireless bridge in your network (section 1.2).

See the changes after we brought in the new VPN Router:

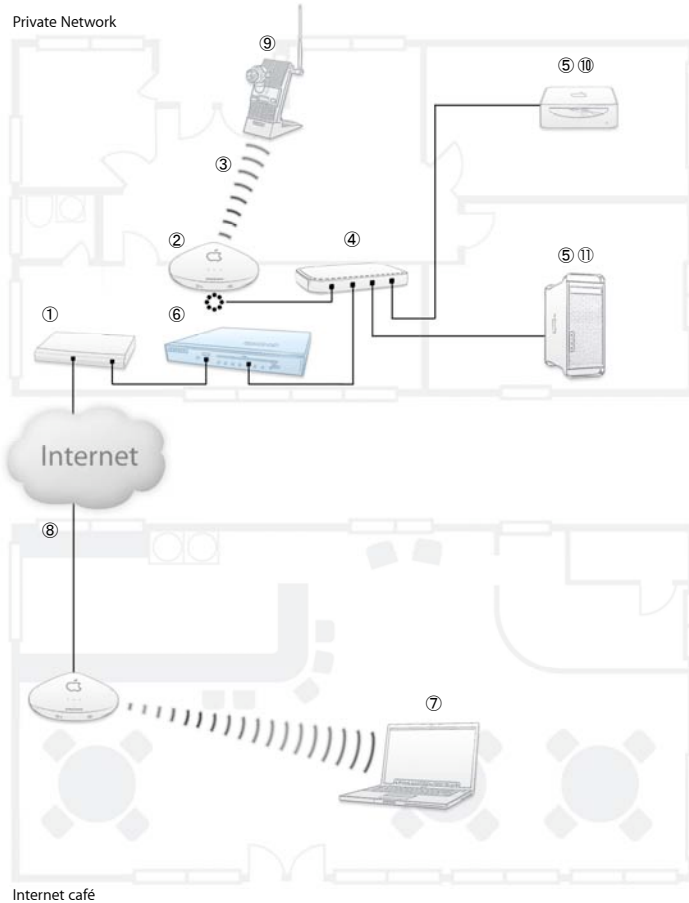


The new VPN NETGEAR Router ⑥ now replaces the AirPort Base Station and then acts as the gateway between the local network and the Internet.

To remain using the WLAN function of the AirPort Base Station ②, the station will be connected like any other network device to the hub/switch. It then acts as a simple bridge for all wireless devices.

Understand how a VPN connection works

We'll now explain how all the components in our example network communicate with each other and how VPN Tracker can be used to access our example network.



In the figure you can see a MacBook Pro (7), where VPN Tracker software is installed. It is located in an Internet café, accessing the Internet through a public Internet connection (8).

To connect to the Private Network simply start the VPN Tracker software. A secure tunnel will then be built to your VPN Router (6) in your Private Network.

Once the secure connection has been established you can access all the devices/computers (5) in the remote network through the secure VPN tunnel.

This means, for example, you can use On Air (<http://www.equinux.com/onair/>) to access a network camera (9) and observe what is going on in the office or at home.

You can also access files on your Mac mini (10) or your FileMaker database (11).

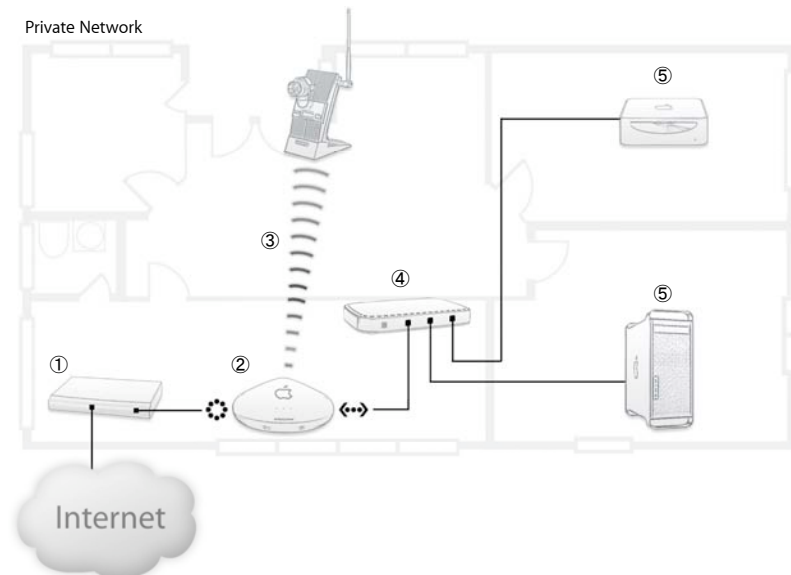
Step 1: Configure your Network

This section explains, step-by-step, how you can integrate a VPN Router into your current network setup.

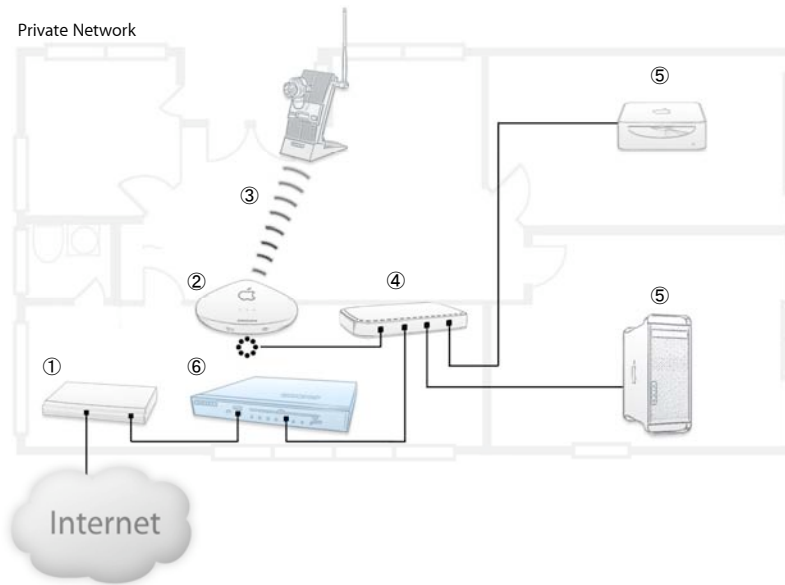
Hint: The steps might be different in your own network. You might not have a switch and instead of the AirPort Base Station there might be another router connected to your cable / DSL modem. However, remember that the VPN Router should be the first device after your cable or DSL modem and the rest of the network should be connected to the VPN Router.

1.1 Adding the VPN Router to your network

To include the VPN Router in our current network setup, please perform the following steps:



- Unplug the device ② which is connected to your cable/DSL Modem ①.
In this illustration, it's an AirPort Base Station.



- ▶ Connect your cable / DSL modem ① to the **Internet** port of your new VPN Router device ⑥.

If you have a Network Switch or Hub:

- ▶ Connect a cable from your network switch ④ to a free network port of your VPN Router device ⑥.

If you want to remain using your „old“ wireless router for WLAN functionality:

- ▶ Connect the **Internet** port of your wireless router ② to your hub / switch ④. In our illustration, we show you how to connect from your AirPort Base Station ② to your local network.

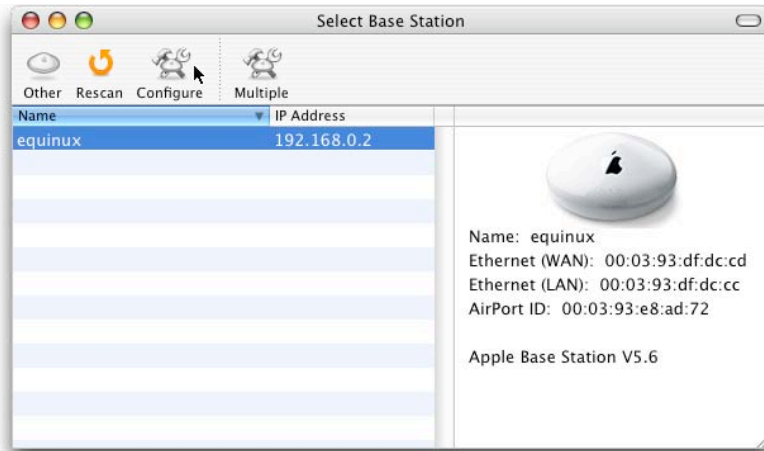
Note: Your new VPN Router ⑥ may have integrated network ports, 4 or 8. If you don't have more than 4 or 8 wired devices in your network, you could eliminate any existing hub/switch ④ and connect all your devices directly to the VPN device ⑥.

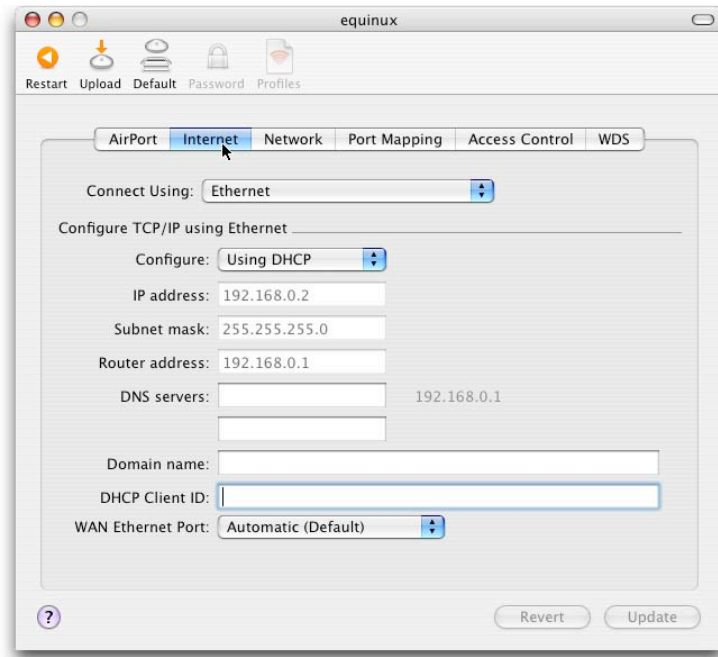
1.2 AirPort Base Station Integration

If you do have an AirPort Base Station you can still use it in your network setup, but we will have to modify its settings slightly. It will then act as a wireless „bridge“, bringing all your wireless devices into the network. This means we need to change the router operation mode to a so called **Bridging Mode**.

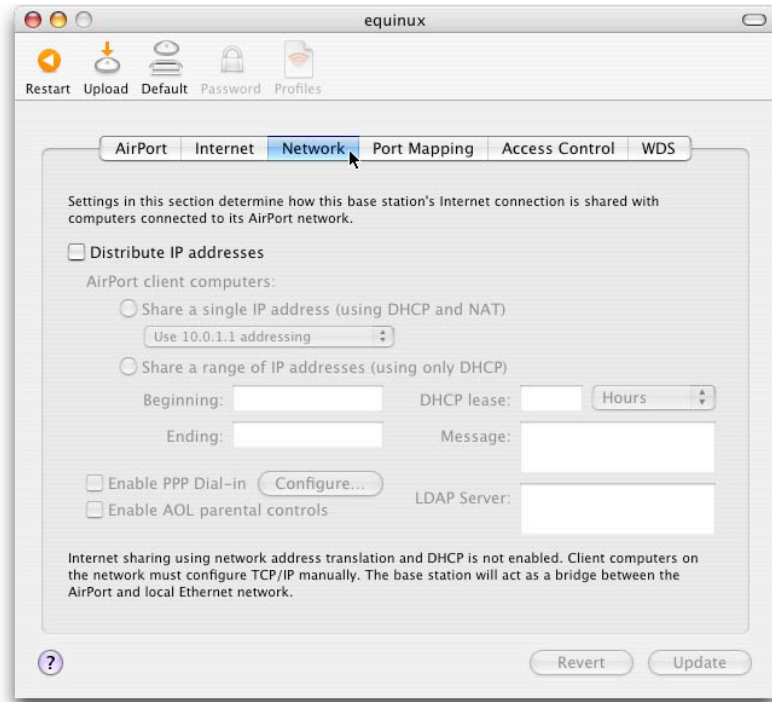
To change the AirPort Base Station to Bridging Mode, please perform the following steps:

- ▶ Open the Finder application
- ▶ Choose in the menu bar **Go>Utilities**
- ▶ Double click the **AirPort Admin Utility**
- ▶ Select your AirPort Base Station from the list and click on **Configure**





- ▶ Click on the **Internet** tab
- ▶ Change **Connect Using** to **Ethernet**
- ▶ Change **Configure** to **Using DHCP**



- ▶ Click on the **Network** tab
- ▶ Untick **Distribute IP addresses**
- ▶ Click on the **Update** button in the lower right corner

The Base Station will then reboot and receive an IP address from the VPN Router, which enables you to still have a wireless access to your network.

1.3 Network components are now set!

Your network components are now correctly setup. The next section describes the IP address setup in your Private Network. It also explains how you would be able to connect from an Internet Café to your Private Network.

Step 2: Public IP Address Configuration

In order to connect to your VPN Router from the outside, you need to configure a public IP address. In this section you will check what kind of Internet connection you use and how to configure it appropriately.

2.1 The difference between static and dynamic IP addresses

There are two different ways ISPs (Internet Service Provider) provide an IP address to your router when you connect to the Internet.

Static: If your ISP provides you with a **static** IP address, then you need to configure this IP address on the VPN Router for Internet access

Dynamic: If you receive a **dynamic** IP address, which means it changes every time you connect to the Internet, then you'll need to setup a DynDNS account.

Hint: If you are not sure, if your ISP provides you with a dynamic or static IP address, please call your ISP to find out.

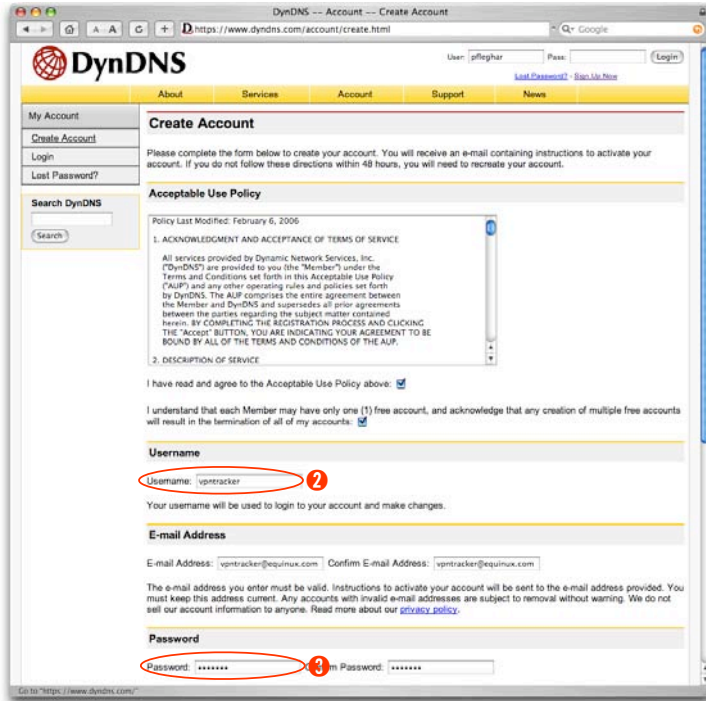
- ▶ If you have a static IP address tick the checkbox **Static IP Address** on you Checklist **1** and proceed to **Step 3**.
- ▶ If you have a dynamic IP address tick the checkbox **Dynamic IP Address** on your Checklist **1** and proceed to **the next page**.

2.2 What is a DynDNS service?

This service is provided free of charge to the Internet community. The free Dynamic DNS service allows you to alias a dynamic IP address to a static host name allowing your computer to be more easily accessed from various locations on the Internet.

2.3 Create your DynDNS Account

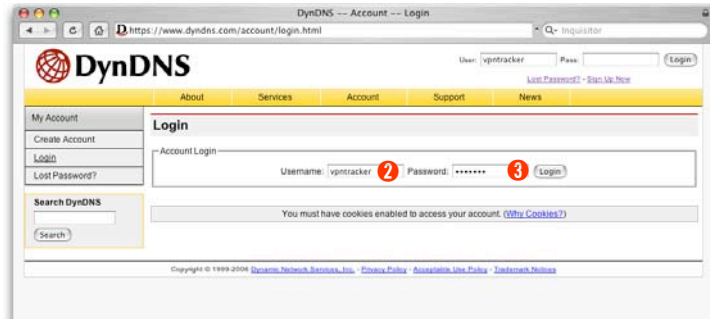
To create a DynDNS account please follow the steps below:



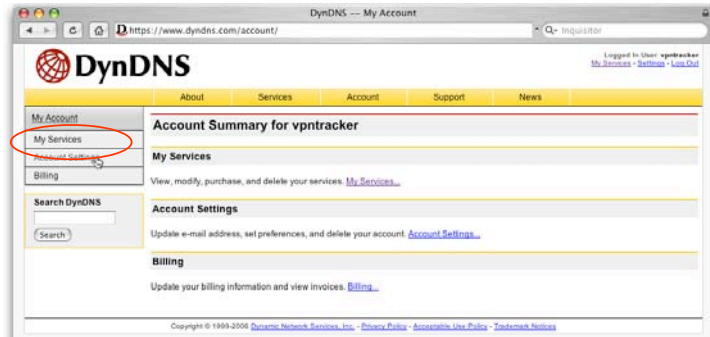
The screenshot shows the DynDNS 'Create Account' page. The page title is 'DynDNS -- Account -- Create Account'. The URL in the browser is 'https://www.dyndns.com/account/create.html'. The page has a navigation menu with 'About', 'Services', 'Account', 'Support', and 'News'. The 'Account' menu is selected. The main content area is titled 'Create Account' and contains the following text: 'Please complete the form below to create your account. You will receive an e-mail containing instructions to activate your account. If you do not follow these directions within 48 hours, you will need to recreate your account.' Below this is the 'Acceptable Use Policy' section, which includes a scrollable text area with the policy details. The form fields are: 'Username' (with the value 'vpntacker' and a red circle with the number 2), 'E-mail Address' (with the value 'vpntacker@equinux.com'), and 'Password' (with a red circle and the number 3). The 'Password' field is followed by a 'Confirm Password' field.

- ▶ Open your Internet browser
- ▶ Go to <http://www.dyndns.org>
- ▶ Click on **Account** in the top menu bar
- ▶ In the left menu bar, click on **Create Account**
- ▶ Enter your **Username** (e.g. yourname) and write it down in the Checklist **2**
- ▶ Enter your **E-mail Address**
- ▶ Enter your **Password** (e.g. mypassword) and write it down in the Checklist **3**

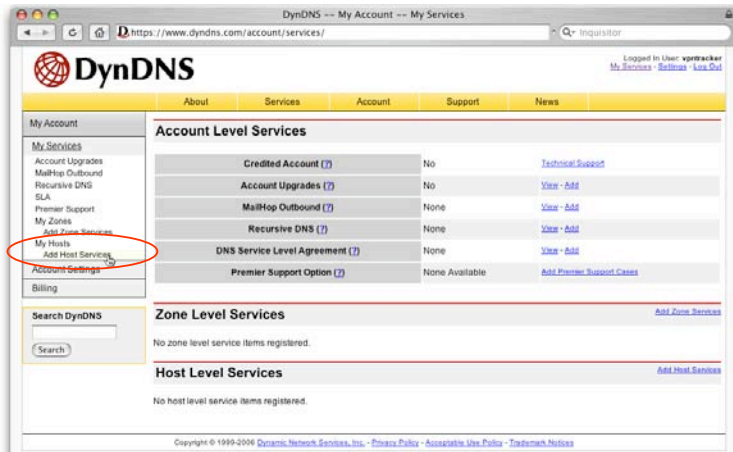
- ▶ You will receive a confirmation email from **DynDNS.org**
- ▶ Click on the **link** in the confirmation e-mail



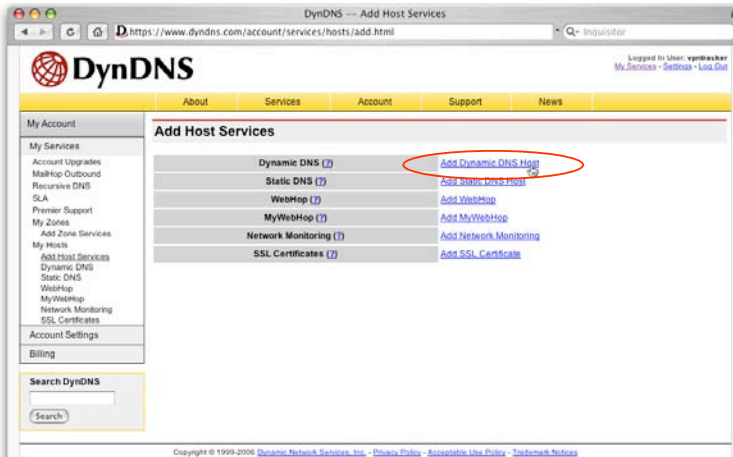
- ▶ Enter your **Username 2** and **Password 3**
- ▶ Click on the **Login** button



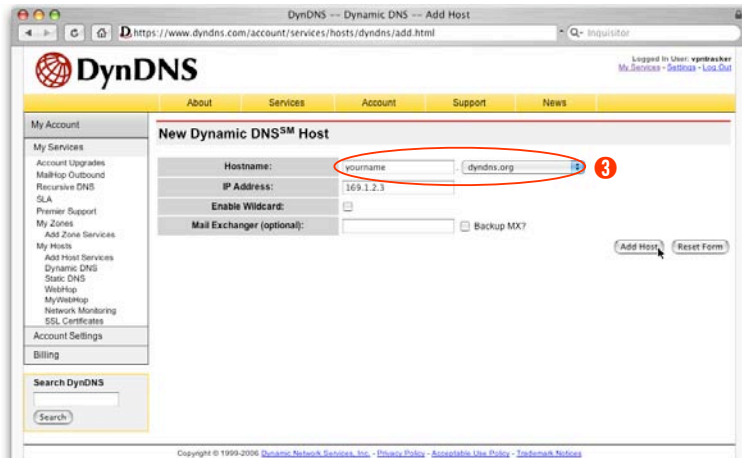
- ▶ Once logged in, click on **My Services** to add a new service



► Click on Add Host Services



► Click on Add Dynamic DNS Host



- ▶ Choose a unique name for your VPN Router (e.g. yourname) and write it down in your Checklist **4**
- ▶ Select **dyndns.org** from the drop-down list beside the name
- ▶ Leave the field **IP address** as it is
- ▶ Click on the **Add Host** button to finish up

2.4 Your DynDNS settings are now complete!

You have now successfully created your DynDNS account. You'll later need to setup the DynDNS account for the VPN Router.

Step 3: NETGEAR Router Configuration

This section explains the configuration of your NETGEAR Router in order to connect using your VPN Tracker software.

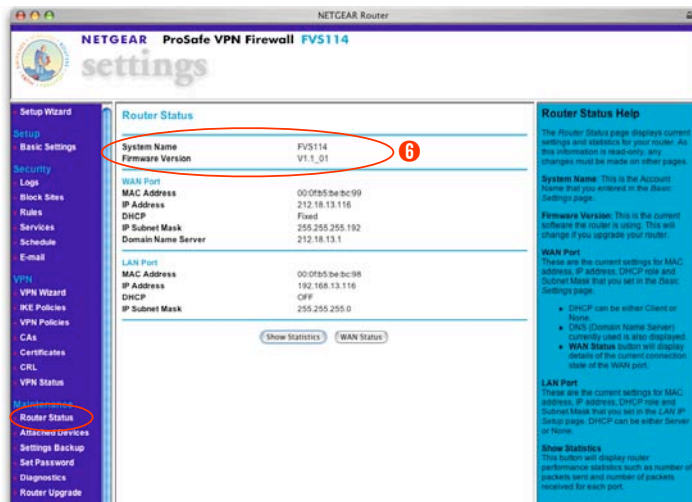
3.1 Check your equipment first

Find out what NETGEAR device you have.

- ▶ If you have the smaller, 4-Port NETGEAR FVS114 device, tick the FVS114 box in your Checklist **5**, and continue to section 3.1.1
- ▶ If you have the larger, 8-Port NETGEAR FVS318 device, tick the FVS318v3 box in your Checklist **5**, and jump to section 3.1.2

3.1.1 FVS114: Update your firmware version

You have to make sure that you are using the current firmware version 1.1_01 or higher to be able to use your Router:



- ▶ Open your Internet browser
- ▶ Login to your router's web interface (<http://192.168.0.1>)
- ▶ Enter your Username (default: admin) and Password (default: password)
- ▶ In the Maintenance section, click on Router Status
- ▶ Write down the Firmware Version in your Checklist **6**

If you're using a previous firmware version, please follow the the steps below to upgrade to the latest version:

- ▶ Write <http://kbserver.netgear.com/products/FVS114.asp> in your Internet browser and download the Firmware Version 1.1_01 or higher
- ▶ Login to your router's web interface
- ▶ In the **Maintenance** section, click on the **Router Upgrade**
- ▶ Click on **Browse** and select the firmware file
- ▶ Click on the **Upload** button

3.1.2 FVS318: Check your model's serial number and firmware version

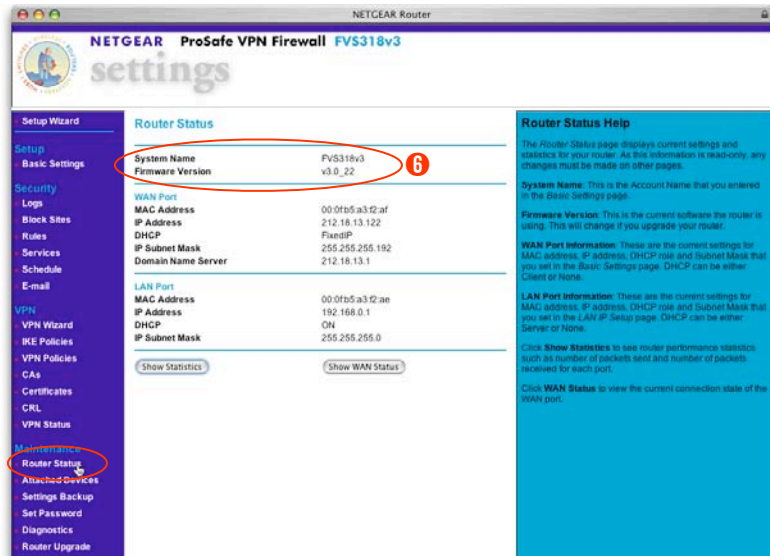
NETGEAR has released three different models of the FVS318 device. This guide only supports the FVS318v3. Previous models, like the FVS318v2 or FVS318 are not supported in this configuration.

To be sure, if you have the right device:



- ▶ Check the serial number on the unit. If it starts with FVS9 or 14A, then you have the correct model.

Now we have to make sure that you are using firmware version 3.0_22 or higher:



- ▶ Open your Internet browser
- ▶ Login to your router's web interface (<http://192.168.0.1>)
- ▶ Enter your **Username** (default: **admin**) and **Password** (default: **password**)
- ▶ In the **Maintenance** section, click on **Router Status**
- ▶ Write down the **Firmware Version** in your Checklist **6**

If you're using a previous firmware version, please follow the the steps below to upgrade to a recent version:

- ▶ Open your Internet browser
- ▶ Go to <http://kbserver.netgear.com/products/FVS318v3.asp> and download the Firmware Version 3.0_22 or higher
- ▶ Login to your router's web interface
- ▶ In the **Maintenance** section, click on **Router Status**
- ▶ Click on **Browse** and select the firmware file
- ▶ Click on **Upload**

3.2 Configure your Public IP Address

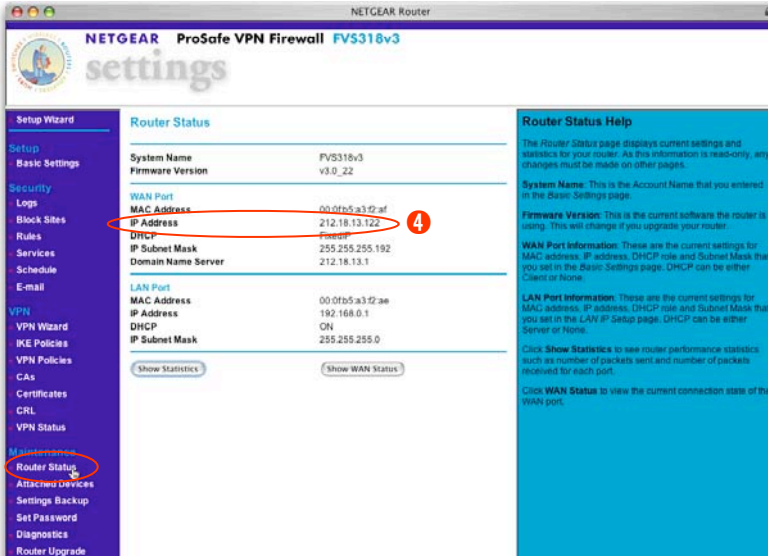
You will now configure your public IP address depending on the type of your Internet connection.

- ▶ If you checked the box **Static IP Address** in your Checklist, proceed to the next section 3.2.1 **Static IP Address**.
- ▶ If you checked the box **Dynamic IP Address** in your Checklist, jump to the section 3.2.2 **Dynamic IP Address**.

3.2.1 Static IP Address

As we need to configure the public IP address of the NETGEAR Router later on in the VPN Tracker Setup Assistant, you need to write it down now. This step is the same for FVS318 or FVS114.

To find our the public IP address please follow the steps below:



The screenshot shows the NETGEAR ProSafe VPN Firewall FVS318v3 settings page. The left sidebar has 'Maintenance' selected, with 'Router Status' highlighted. The main content area shows the 'Router Status' section with the following information:

Router Status	
System Name	FVS318v3
Firmware Version	v3.0_22
WAN Port	
MAC Address	00:0f:b5:a3:12:af
IP Address	212.18.13.122
DHCP	Enabled
IP Subnet Mask	255.255.255.192
Domain Name Server	212.18.13.1
LAN Port	
MAC Address	00:0f:b5:a3:12:ae
IP Address	192.168.0.1
DHCP	On
IP Subnet Mask	255.255.255.0

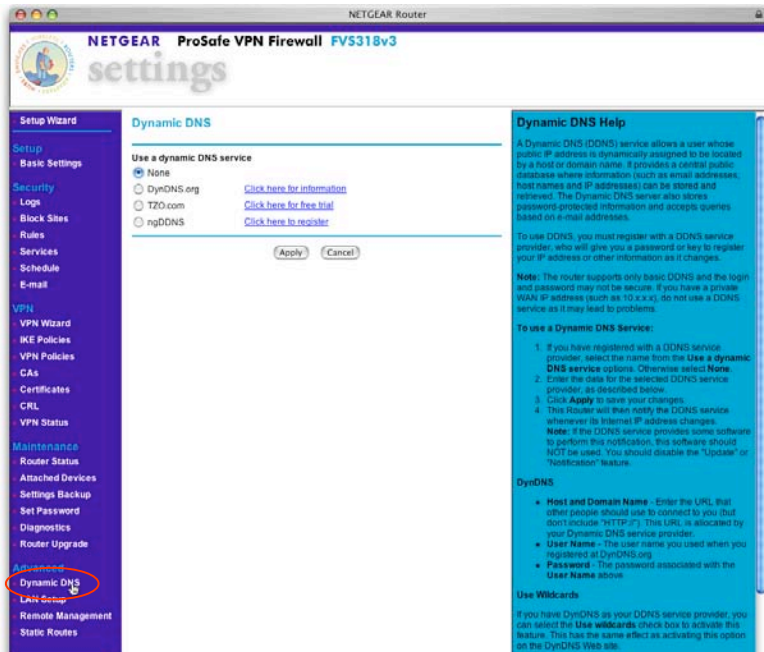
Below the table are two buttons: 'Show Statistics' and 'Show WAN Status'. The 'Router Status Help' section on the right provides additional information about the Router Status page, including details about System Name, Firmware Version, WAN Port Information, and LAN Port Information.

- ▶ Open your Internet browser
- ▶ Login to your router's web interface (<http://192.168.0.1>)
- ▶ Enter your **Username** (default: **admin**) and **Password** (default: **password**)
- ▶ In the **Maintenance** section, click on **Router Status**
- ▶ Write down the **IP Address** of your WAN Port in the Checklist **4**
- ▶ Now proceed to section 3.3 **Configure the NETGEAR VPN**

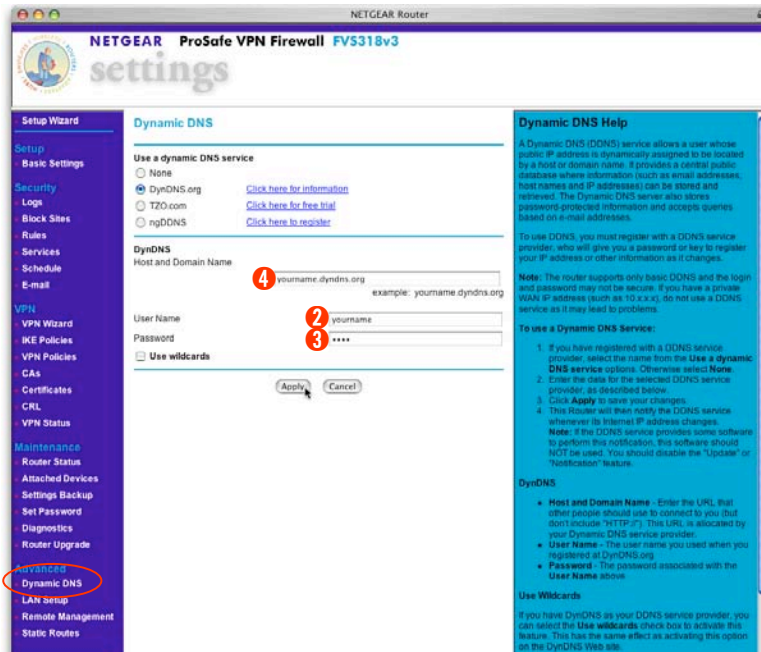
3.2.2 Dynamic IP Address

If you ticked Dynamic IP Address in your Checklist, then we now need to configure the a DynDNS service on the NETGEAR device.

Please follow the steps below to setup DynDNS on your device:



- ▶ Open your Internet browser
- ▶ Open your NETGEAR web interface (<http://192.168.0.1>)
- ▶ Enter your Username (default: admin) and Password (default: password)
- ▶ In the Advanced section click on Dynamic DNS



- ▶ Select DynDNS.org as dynamic DNS service
- ▶ Enter the Host Name from your Checklist **4**
- ▶ Enter your DynDNS Username from your Checklist **2**
- ▶ Enter your DynDNS Password from your Checklist **3**
- ▶ Click on the Apply button

Advanced Users only

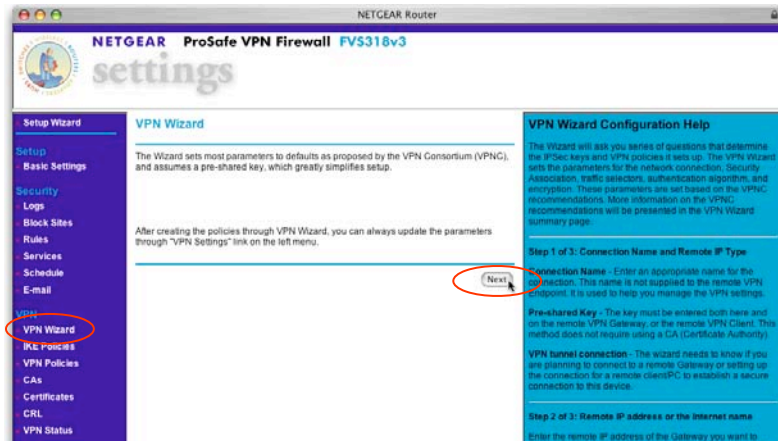
We assume that you are using your NETGEAR device with factory settings. If you are an advanced user and you want to change the IP Address of the NETGEAR device and (or) change the IP range of your private network, choose **LAN Setup** in the **Advanced Section** of the NETGEAR web interface and make the desired changes.

3.3 Configure the NETGEAR VPN

Now we'll create the VPN settings on your NETGEAR Router. After this step your NETGEAR device will allow secure connections from the outside world.

3.3.1 Using the VPN Wizard of your NETGEAR device

This section explains how you will setup your VPN connection on you NETGEAR device:

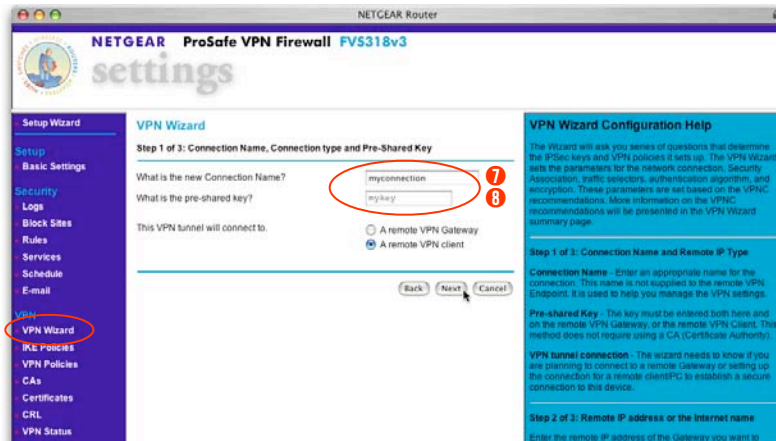


- ▶ Open your Internet browser
- ▶ Open your NETGEAR web interface (<http://192.168.0.1>)
- ▶ Enter your **Username** (default: **admin**) and **Password** (default: **password**)
- ▶ In the left menu section, click on **VPN Wizard**
- ▶ Click on the **Next** button to proceed

3.3.2 Enter your Connection Name, Type and Password

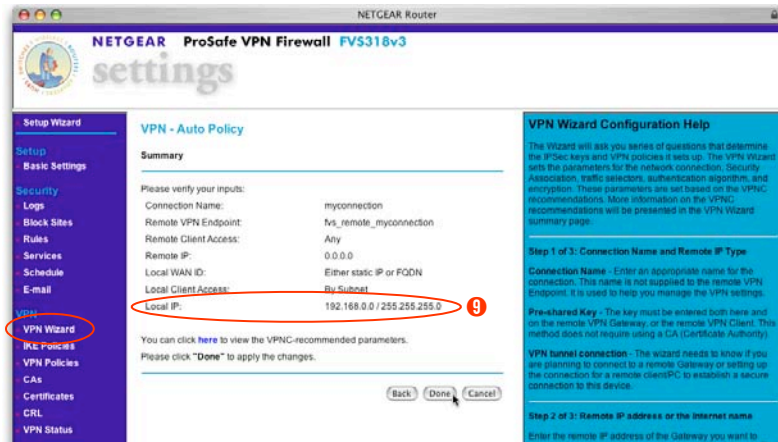
You need now to setup a connection name and a so called **pre-shared key**. In the language of VPN, the term **pre-shared key** means **password**.

To setup the connection please follow the steps below:



- ▶ Enter a **Connection Name** for the connection(e.g. **myconnection**). Write your connection name down in your Checklist **7** . You can use any name you wish, avoid using spaces and special characters.
- ▶ Enter your desired **Pre-shared key** for the connection (e.g. **mykey**). Write it down in your Checklist **8**
- ▶ Select **A remote VPN client**
- ▶ Click on the **Next** button

3.3.3 Find out the local IP settings



- ▶ Now write down the **Remote Network/Mask** in your Checklist **9**
- ▶ Click on the **Done** button

Advanced Users only

FV5318v3 only - If you want to allow multiple users to access your devices.

If you want to connect multiple users to your NETGEAR FV5318v3 VPN Router, you just need to repeat the VPN Wizard steps, creating for every new user, a different *Connection Name* and *Password* (pre-shared key).

Your VPN Router is now set up for your VPN connection!

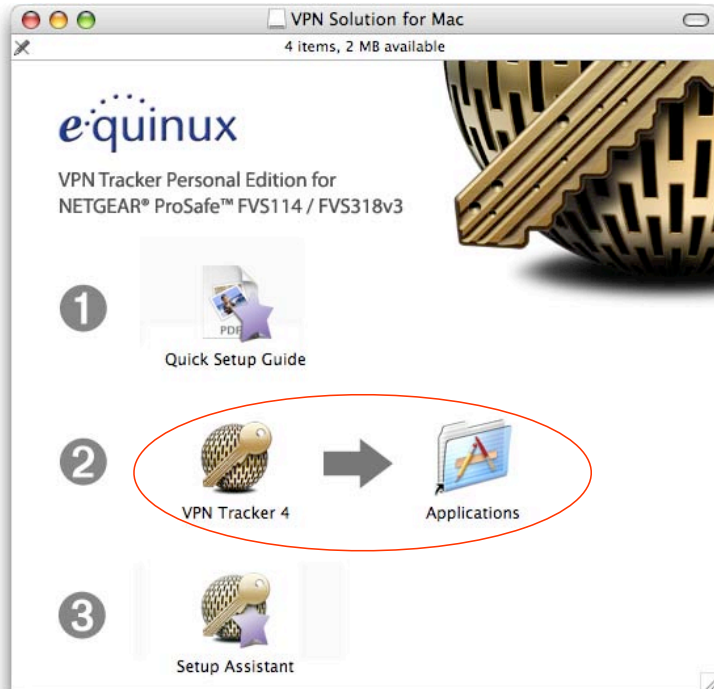
The NETGEAR Router is now correctly configured and we can go on with the VPN Tracker software configuration.

Step 4: VPN Tracker Configuration

This section describes the configuration of VPN Tracker based on the VPN Tracker Setup Assistant.

4.1 Install, start VPN Tracker and run the VPN Tracker Setup Assistant

Before using the VPN Tracker Setup Assistant, you'll first need to install the latest version of VPN Tracker:

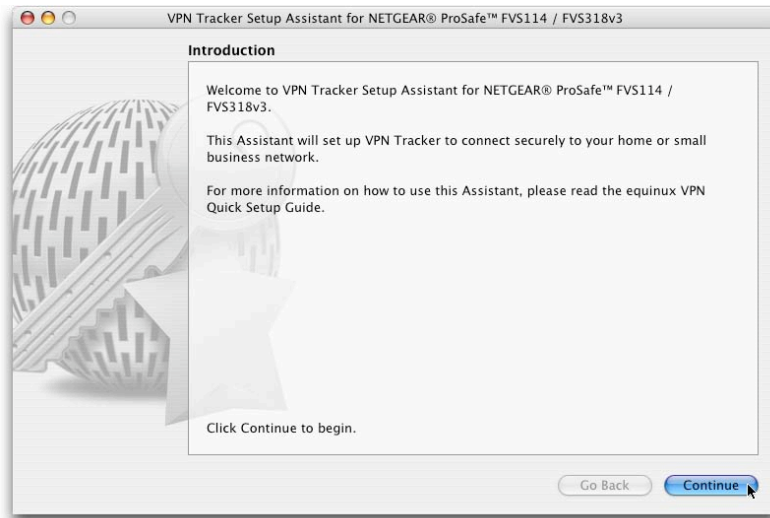


- ▶ Open the VPN Tracker disk image on your Desktop
- ▶ Drag the **VPN Tracker 4** icon into the **Applications** folder (2 in the screenshot)
- ▶ Navigate to your Applications folder in Finder
- ▶ Double click on the **VPN Tracker** icon in your **Applications** folder



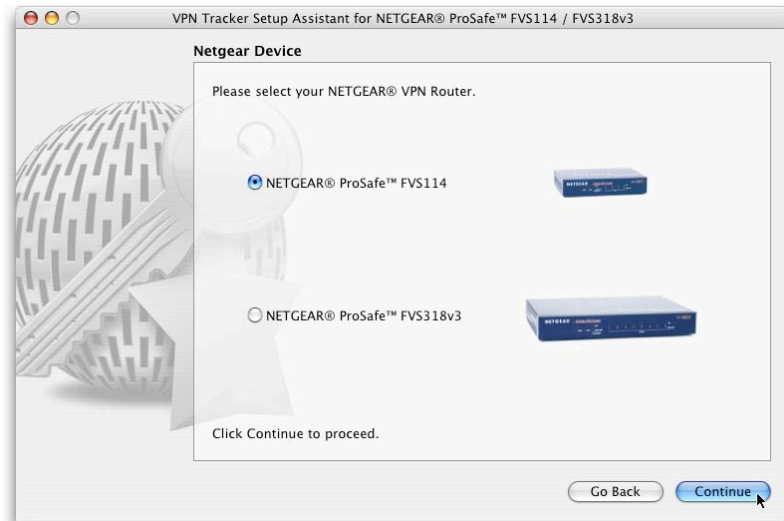
▶ Double click the **Setup Assistant** in the disk image (3 in the screenshot)

4.1.1 Introduction



- ▶ The VPN Tracker Setup Assistant will open up. Click on the **Continue** button

4.1.2 NETGEAR Device



- ▶ Select your NETGEAR VPN Router depending on your Checklist **5**
- ▶ Click on the **Continue** button

4.1.3 Connection Settings

VPN Tracker Setup Assistant for NETGEAR® ProSafe™ FVS114 / FVS318v3

Connection Settings

Please enter the following settings and make sure they match your current NETGEAR device configuration.

Connection Name: 7

Pre-Shared Key: 8

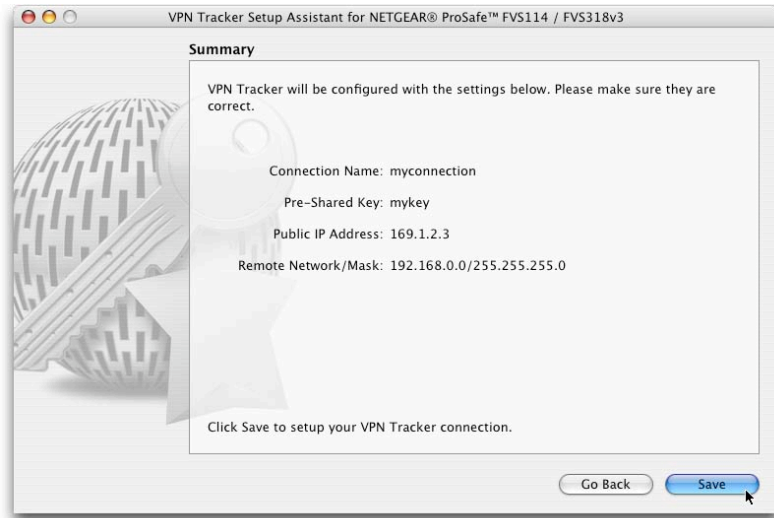
Public IP Address: 4

Remote Network/Mask: 9

Click Continue to proceed.

- ▶ Enter the **Connection Name** from the Checklist 7
- ▶ Enter the **Pre-shared Key** from the Checklist 8
- ▶ Enter the **Public IP Address** from the Checklist 4
- ▶ Enter the **Remote Network / Mask** from the Checklist 9
- ▶ Click on the **Continue** button

4.1.3 Summary



- ▶ Verify that the settings you've entered match with those on the Checklist
- ▶ Click the **Save** button to finish the setup

A new connection will now be added to VPN Tracker

Step 5: Check the VPN connection

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

5.1 It's time to go out!

You will not be able to test and use your VPN connection within your Private Network. In order to test your connection to your Private Network, you'll need to connect from a different location. That's why it's now time to go out. Take your MacBook Pro and have a coffee at your favorite Internet cafe or go visit a friend.

5.2 Test your connection

To test if everything is setup correctly please follow the steps below:

- ▶ Get access to the network from an Internet café, a friend's house or some place else where you can find an Internet connection
- ▶ Make sure the 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



- ▶ Select the previously configured connection
- ▶ Click on the **Start VPN** button



- ▶ If the light turns red after a few seconds, then please read the **Troubleshooting** section on the next page
- ▶ If you get a **Green** light, that means you've successfully established a connection

Congratulations! You did it!

Troubleshooting

I don't get a green light in the VPN Tracker main window

- ▶ Make sure that your computer is not connected to the Private Network you want to connect to.
- ▶ Make sure, that the **Connection Name** **7** and the **Pre-shared key** **8** you've entered in the NETGEAR VPN wizard match the settings you entered in the VPN Tracker Setup Assistant.
- ▶ Verify that the **Public IP address** **4** you entered in the VPN Tracker Setup Assistant matches the public IP address of your NETGEAR Router and the setting in your Checklist.
- ▶ If all those settings are correct, then please contact our support team at vpntracker@equinux.com

What's next?

This section explains the usage of your newly configured VPN connection.

Introduction

As the VPN connection has now been established, you should be able to access all resources in your Private Network.

Known Limitations

Except the limitations below, you should be able to access all resources as if you were actually in your Private Network.

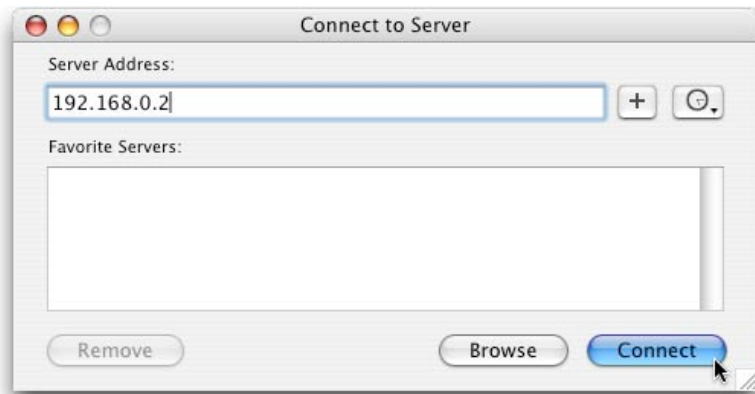
- ▶ **Bonjour:** As Bonjour Chat is not supported over a VPN tunnel, you'll need to use iChat server in order to chat remotely.
- ▶ **Browsing the network:** You can't "browse" the remote network as you're normally used to. You need to connect to the machine manually, as described on the next page.

Accessing Files

To access files in the remote network, just follow the steps below:



- ▶ Go to the **Finder** application
- ▶ In the menu bar, click on **Go->Connect To Server...**

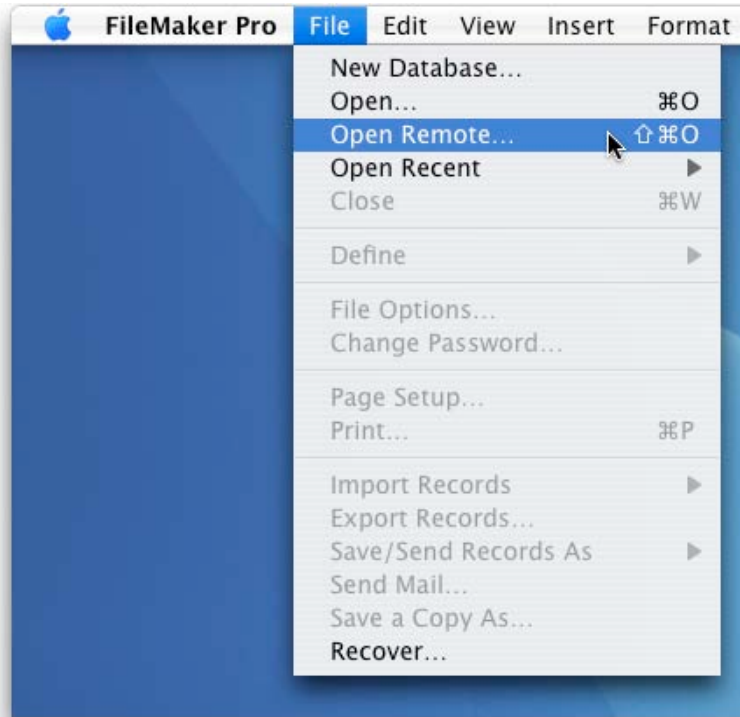


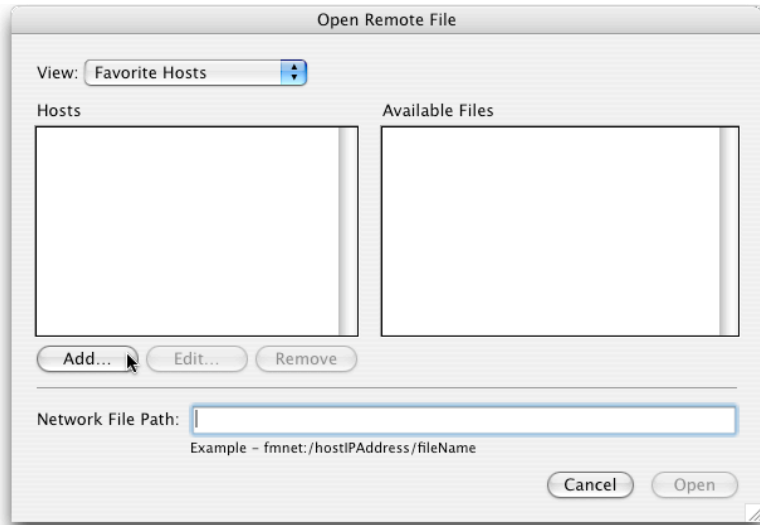
- ▶ Enter the IP address of the machine you want to connect to. In our example network this would be the IP address **192.168.0.2**
- ▶ Click on the **Connect** button
- ▶ Enter your **Username** and **Password** to access the files

Access your FileMaker Database

To access files in your Private Network, just follow the steps below:

- ▶ Start the **FileMaker** application
- ▶ In the menu bar, click on **File->Open Remote**





▶ Click on the **Add...** button

Edit Favorite Host

Favorite Settings

Host's Internet Address:
(Example - host.domain.com or 192.168.10.0)

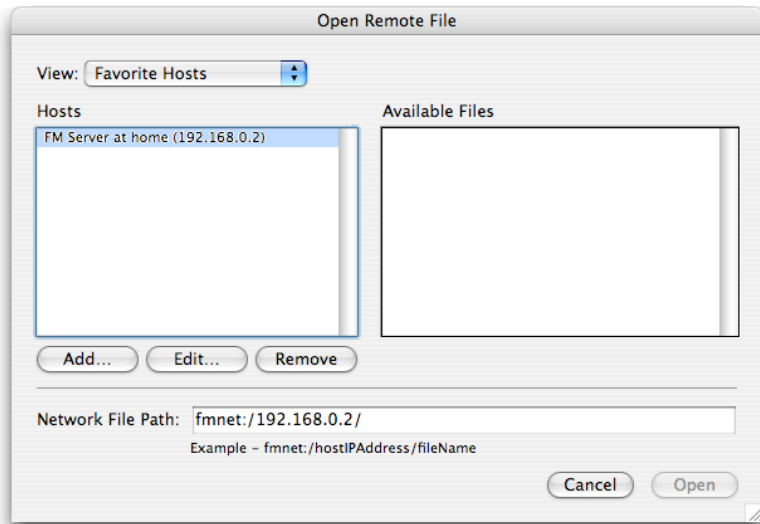
Favorite Host's Name:
(optional)

File Settings

Show all available files for this host
 Show only these files

Enter one file name per line, separated by a carriage return

- ▶ Enter the **IP address** of the the FileMaker Server machine
- ▶ Enter the **Favorite Host's Name** for this machine
- ▶ Click on the **Save** button



- ▶ Select a database from the list of **Available Files** and click **Open**
- ▶ You're now able to access your FileMaker databases as usual

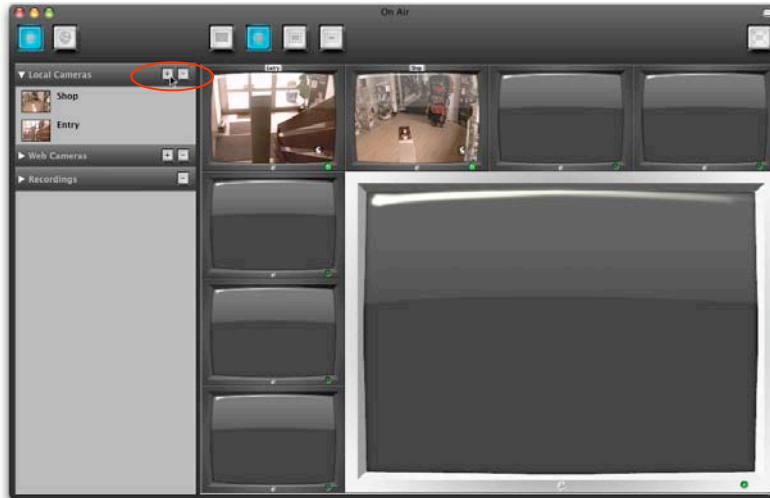
Access your IP cam

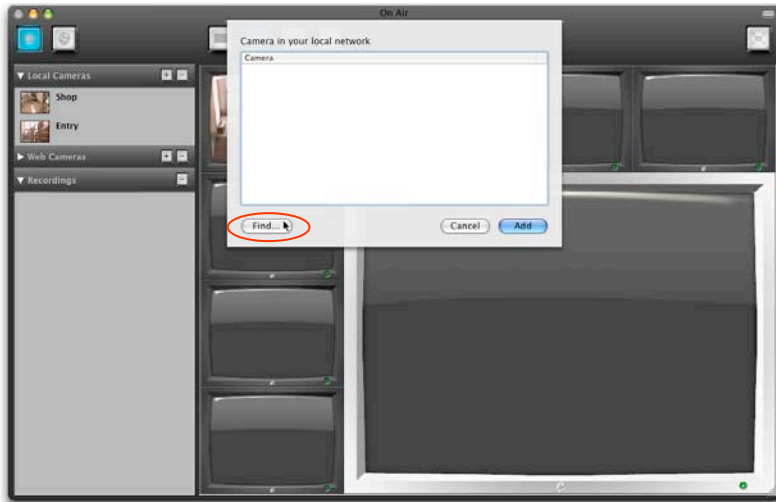
With equinux software On Air, you can access all cameras in your Private Network.

Download the On Air FREE demo at <http://www.equinux.com/onair/download/>

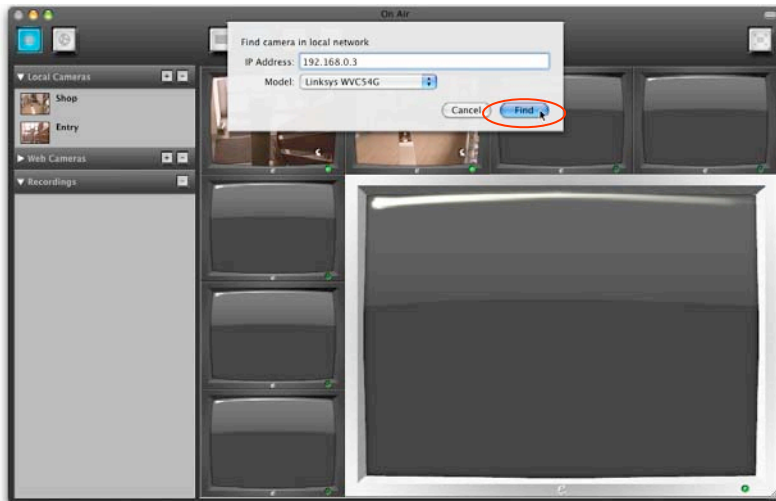
To access your IP cam, just follow the steps below:

- ▶ Start the On Air application
- ▶ Click on + next to **Local Cameras**





▶ Click on **Find**



- ▶ Enter the **IP Address** of the Linksys IP cam (e.g. **192.168.0.3**)
- ▶ Select the **Model: Linksys WVC54G**
- ▶ Click on the **Find** button
- ▶ The camera will be added to the **Local Cameras** list and you can now drop it on to you video wall

Acquire more Licenses

If two or more people need to access your Private Network, then you need to acquire more VPN Tracker licenses.

To get more licenses please contact your reseller and inquire about „VPN Tracker Personal Edition“.

Or point your browser to <http://store.equinux.com> and buy additional VPN Tracker Personal Edition Licenses.

Your VPN Checklist

In certain sections of the manual, you'll be asked to fill out this Checklist. It will also be used as a reference for filling out other sections. The red numbers will be your guide **1**, **2**, ...

- 1** My ISP provides me with a Static IP address Dynamic IP address
- 2** DynDNS Username: _____
- 3** DynDNS Password: _____
- 4** Public IP Address: Dynamic: _____ .dyndns.org OR Static: _____._____._____._____
- 5** Model Version: FVS114 FVS318v3
- 6** Firmware: _____
- 7** Connection Name: _____
- 8** Pre-shared key: _____
- 9** Remote Network/Mask: _____ / 255 . 255 . _____ . _____