# VPN Tracker for Mac OS X

## How-to:

## Interoperability with

## NETGEAR VPN Router Appliances

Rev. 1.4

# 1. Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a NETGEAR VPN Firewall. The entire NETGEAR product range should be compatible with VPN Tracker. equinux has tested the NETGEAR model FVL328 and FVS 318.

The NETGEAR VPN Firewall is configured as a router, connecting a company LAN to the Internet.

The example demonstrates a connection scenario, with a dial-in Mac connecting to a NETGEAR VPN Firewall.

This paper is only a supplement to, not a replacement for, the instructions that have been included with your NETGEAR VPN Firewall. Please be sure to read and understand those instructions before beginning.

All trademarks, product names, company names, logos, screenshots displayed, cited or otherwise indicated on the How-to are the property of their respective owners.

EQUINUX SHALL HAVE ABSOLUTELY NO LIABILITY FOR ANY DIRECT OR INDIRECT, SPECIAL OR OTHER CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE USE OF THE HOW-TO 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.

# 2. Prerequisites

Firstly, you should use a recent NETGEAR firmware version. The latest firmware release for your NETGEAR VPN Firewall can be obtained from:

http://www.netgear.com

For this document, firmware version 1.4 has been used.

The type of the VPN Tracker license needed (personal or professional edition) depends on the connection scenario you are using:

- If you connect a dial-in Mac without it's own subnet to the NETGEAR VPN Firewall you need a Personal License.

- If you want to establish a LAN-to-LAN connection from your Mac to the NETGEAR VPN Firewall, you need a VPN Tracker Professional License.

VPN Tracker is compatible with Mac OS X 10.2 or higher.

Be sure to use VPN Tracker 2.0.4 or higher.[1] For this document VPN Tracker version 2.0.4 has been used.

[1] All VPN Tracker versions prior to the 2.0.4 did not include a connection type for NETGEAR products.

# 3. Connecting a VPN Tracker Host to NETGEAR VPN Firewall using PSK

In this example, the Mac running VPN Tracker is directly connected to the internet via a dialup or PPP connection.[2] The NETGEAR VPN Firewall is configured in NAT mode and has the static WAN IP address 169.1.2.3 and the private LAN IP address 192.168.1.1. The stations in the LAN behind the NETGEAR VPN Firewall use 192.168.1.1 as their default gateway and should have a working Internet connection.

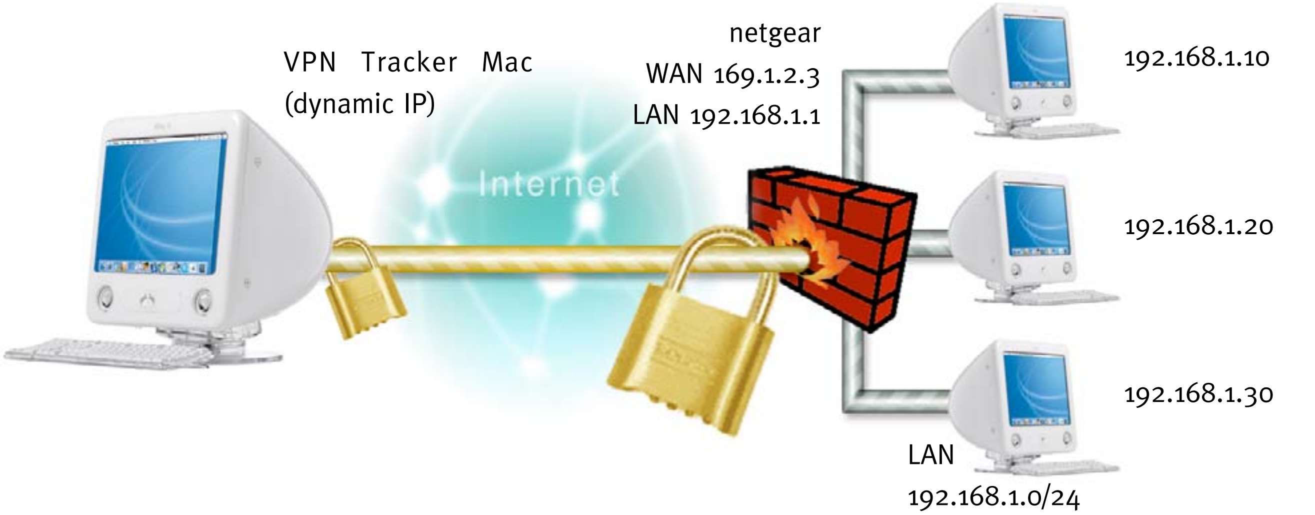


*Figure 1: VPN Tracker - NETGEAR VPN Firewall connection diagram (host to network)*

[2] Please note that the connection via a router, which uses Network Address Translation (NAT), only works if the NAT router supports „IPsec passthrough“. Please contact your router’s manufacturer for details.

NETGEAR offers 2 different types of VPN gateways, the NETGEAR FVL 328 and the FVS 318. The configuration for the FVS 318 is described in chapter 3.1. Please see chapter 3.2 for the FVL 328 configuration.

## 3.1 NETGEAR FVS 318 Firewall configuration

The pre-defined VPN Tracker connection type has been created using the default settings on NETGEAR VPN Firewall. If you change any of the settings on the NETGEAR VPN Firewall VPN router, you will subsequently have to adjust the connection type in VPN Tracker.

**Step 1** NETGEAR VPN settings:

Please go to Setup -> VPN Settings and enter a “Connection Name” e.g. vpntracker. You have to use identifiers in the  passage ‘Local’ and ‘Remote’. These settings refer to the “Local“ and “Remote identifier” settings in VPN Tracker. Please type in an arbitrary local and remote identifier (e.g. “netgear” and “vpntracker”).

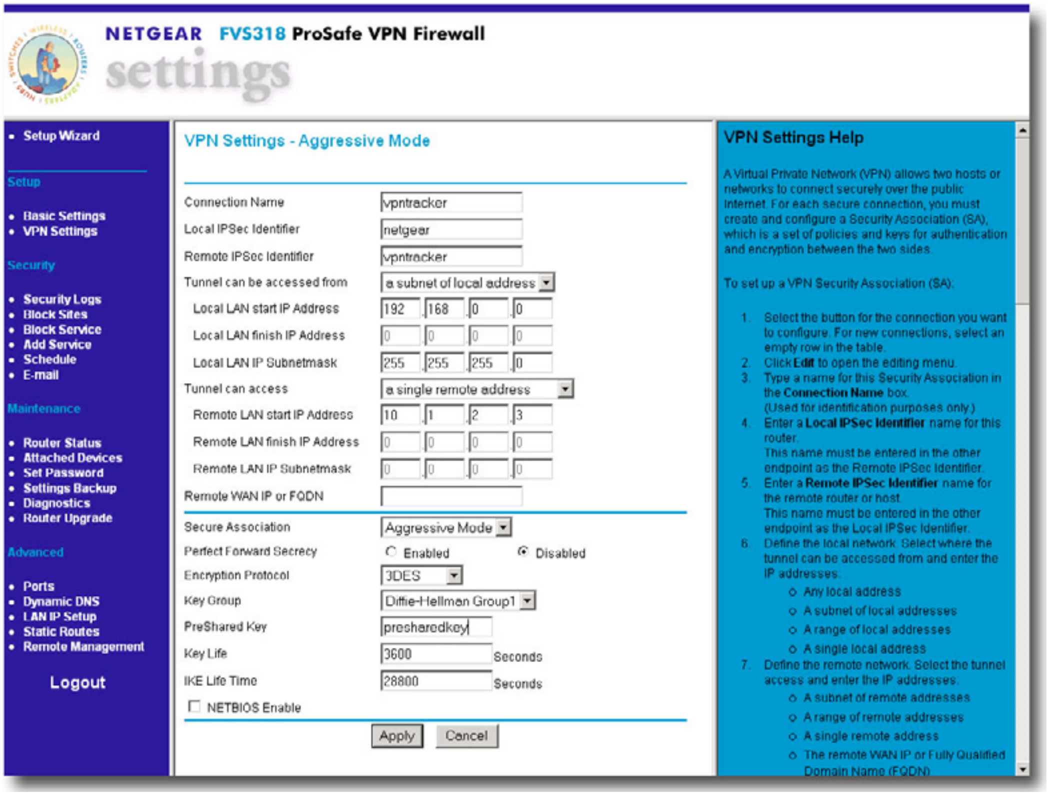
Select “a subnet of local address” where the “Tunnel can be accessed from”. Enter in the field “Local LAN start IP Address” the Network IP Address of your local network on the Netgear side. The “Local LAN IP Subnetmask” has to be entered as well.

The tunnel can access “a single remote address”. Enter here your “virtual” private IP address e.g. 10.1.2.3. These settings refer to the “local host” setting in VPN Tracker.

You  have to use the “Aggressive Mode” and the Perfect Forward Secrecy must be disabled. The pre-defined connection type for NETGEAR uses 3DES and the Diffie-Hellman Group 1.

Finally you have to enter your Pre-shared key.

The pre-defined connection type “Netgear” is based on these settings. Please check all fields. The values should be exactly the same as shown on the screenshot below.



VPN Settings - Aggressive Mode

| | |
|---|---|
| Connection Name | vpntracker |
| Local IPSec Identifier | netgear |
| Remote IPSec Identifier | vpntracker |
| Tunnel can be accessed from | a subnet of local address |
| Local LAN start IP Address | 192 . 168 . 0 . 0 |
| Local LAN finish IP Address | 0 . 0 . 0 . 0 |
| Local LAN IP Subnetmask | 255 . 255 . 255 . 0 |
| Tunnel can access | a single remote address |
| Remote LAN start IP Address | 10 . 1 . 2 . 3 |
| Remote LAN finish IP Address | 0 . 0 . 0 . 0 |
| Remote LAN IP Subnetmask | 0 . 0 . 0 . 0 |
| Remote WAN IP or FQDN | |
| Secure Association | Aggressive Mode |
| Perfect Forward Secrecy | ○ Enabled ● Disabled |
| Encryption Protocol | 3DES |
| Key Group | Diffie-Hellman Group1 |
| PreShared Key | presharedkey |
| Key Life | 3600 Seconds |
| IKE Life Time | 28800 Seconds |
| □ NETBIOS Enable | |

VPN Settings Help

A Virtual Private Network (VPN) allows two hosts or networks to connect securely over the public Internet. For each secure connection, you must create and configure a Security Association (SA), which is a set of policies and keys for authentication and encryption between the two sides.

To set up a VPN Security Association (SA):

1. Select the button for the connection you want to configure. For new connections, select an empty row in the table.
2. Click **Edit** to open the editing menu.
3. Type a name for this Security Association in the **Connection Name** box. (Used for identification purposes only.)
4. Enter a **Local IPSec Identifier** name for this router. This name must be entered in the other endpoint as the Remote IPSec Identifier.
5. Enter a **Remote IPSec Identifier** name for the remote router or host. This name must be entered in the other endpoint as the Local IPSec Identifier.
6. Define the local network. Select where the tunnel can be accessed from and enter the IP addresses:
   - Any local address
   - A subnet of local addresses
   - A range of local addresses
   - A single local address
7. Define the remote network. Select the tunnel access and enter the IP addresses:
   - A subnet of remote addresses
   - A range of remote addresses
   - A single remote address
   - The remote WAN IP or Fully Qualified Domain Name (FQDN)

*Figure 2: NETGEAR FVS 318 - VPN settings*

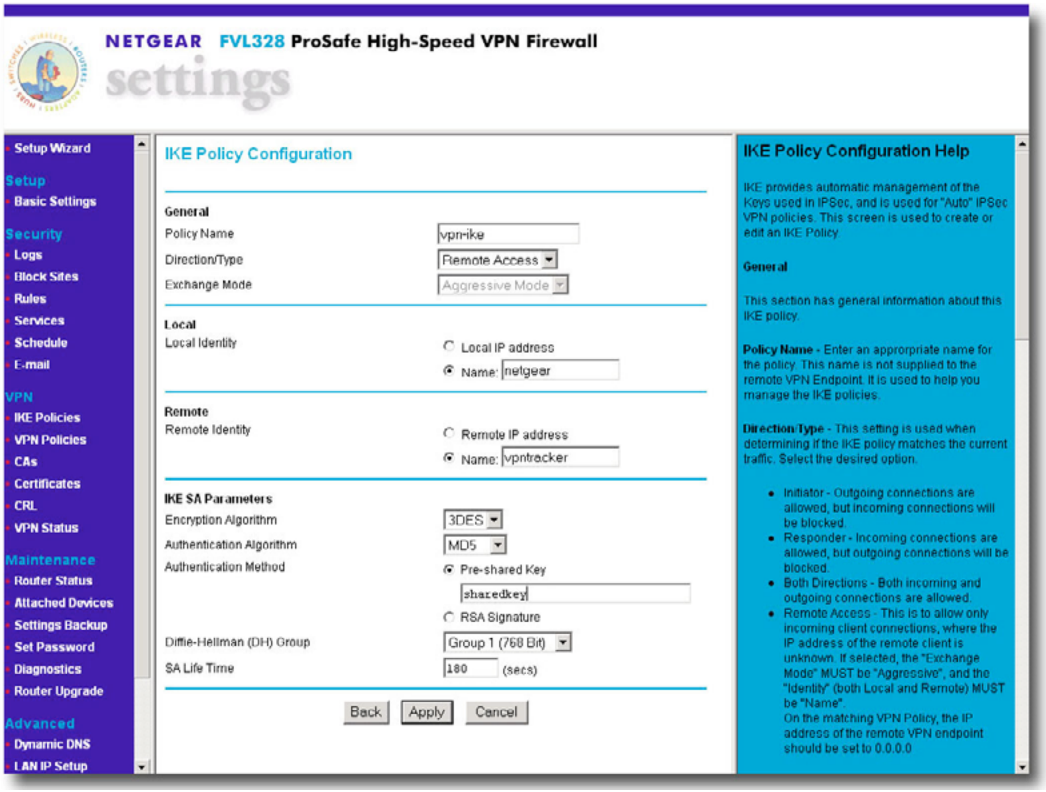
## 3.2 NETGEAR VPN FVL 328 Firewall configuration

**Step 1** IKE Policy Configuration:

Go to [VPN -> IKE Policies] and add a new policy. Enter a connection name (e.g. vpn-ike) and use “Remote Access” as Direction Mode. You have to use identifiers in the passage ‘Local’ and ‘Remote’. This settings refers to the “Local-“ and “Remote identifiers” settings in VPN Tracker. Please type in a arbitrary local and remote identifier (e.g. “netgear” and “vpntracker”).

Finally you have to choose “Pre-shared Key” as “Authentication Method” and enter your pre-shared secret in the field below.

The pre-defined connection type “Netgear” is based on default settings. Please check all fields. The values should be exactly the same as shown on the screenshot below.



IKE Policy Configuration

General

Policy Name: vpn-ike
Direction/Type: Remote Access
Exchange Mode: Aggressive Mode

Local

Local Identity: ○ Local IP address ● Name: netgear

Remote

Remote Identity: ○ Remote IP address ● Name: vpntracker

IKE SA Parameters

Encryption Algorithm: 3DES
Authentication Algorithm: MD5
Authentication Method: ● Pre-shared Key sharedkey ○ RSA Signature
Diffie-Hellman (DH) Group: Group 1 (768 Bit)
SA Life Time: 180 (secs)

IKE Policy Configuration Help

IKE provides automatic management of the Keys used in IPSec, and is used for "Auto" IPSec VPN policies. This screen is used to create or edit an IKE Policy.

**General**

This section has general information about this IKE policy.

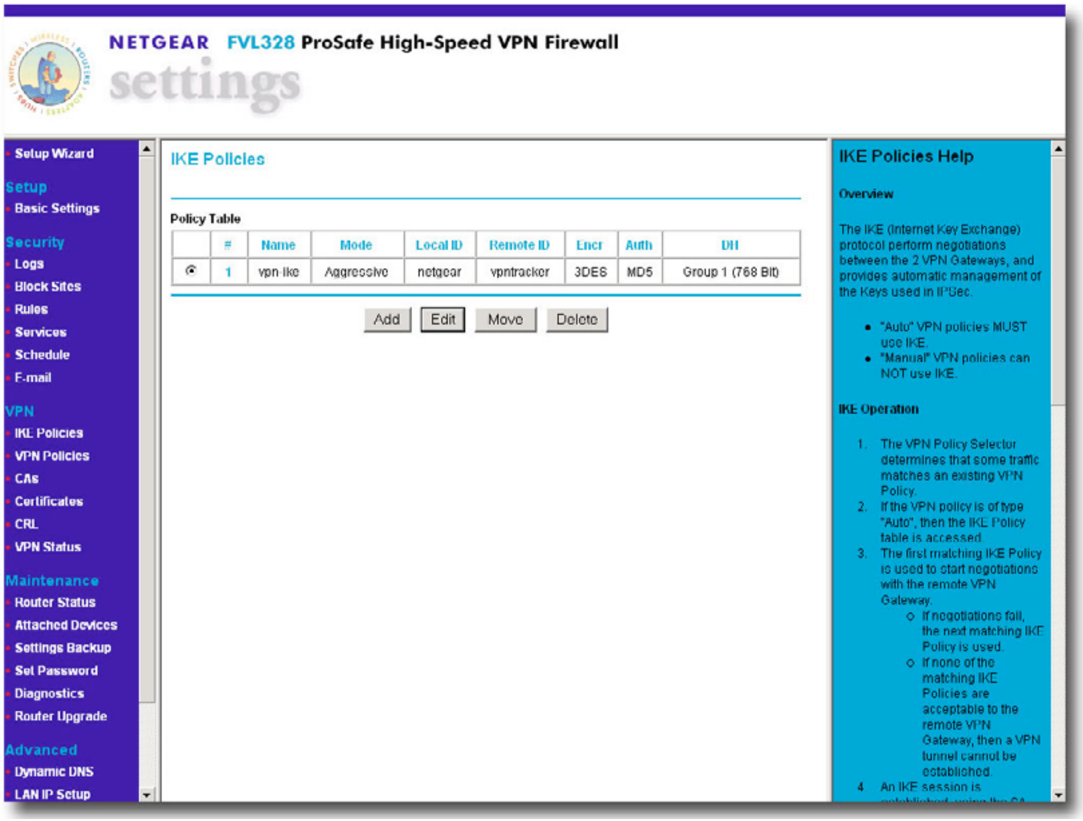
**Policy Name** - Enter an approrpriate name for the policy. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the IKE policies.

**Direction/Type** - This setting is used when determining if the IKE policy matches the current traffic. Select the desired option.

- Initiator - Outgoing connections are allowed, but incoming connections will be blocked.
- Responder - Incoming connections are allowed, but outgoing connections will be blocked.
- Both Directions - Both incoming and outgoing connections are allowed.
- Remote Access - This is to allow only incoming client connections, where the IP address of the remote client is unknown. If selected, the "Exchange Mode" MUST be "Aggressive", and the "Identity" (both Local and Remote) MUST be "Name".
  On the matching VPN Policy, the IP address of the remote VPN endpoint should be set to 0.0.0.0

*Figure 3: IKE Policy Configuration*

After this steps the configuration should look like this:



IKE Policies

Policy Table

| | # | Name | Mode | Local ID | Remote ID | Encr | Auth | DH |
|---|---|---|---|---|---|---|---|---|
| ● | 1 | vpn-ike | Aggressive | netgear | vpntracker | 3DES | MD5 | Group 1 (768 Bit) |

IKE Policies Help

**Overview**

The IKE (Internet Key Exchange) protocol perform negotiations between the 2 VPN Gateways, and provides automatic management of the Keys used in IPSec.

- "Auto" VPN policies MUST use IKE.
- "Manual" VPN policies can NOT use IKE.

**IKE Operation**

1. The VPN Policy Selector determines that some traffic matches an existing VPN Policy.
2. If the VPN policy is of type "Auto", then the IKE Policy table is accessed.
3. The first matching IKE Policy is used to start negotiations with the remote VPN Gateway.
   - If negotiations fail, the next matching IKE Policy is used.
   - If none of the matching IKE Policies are acceptable to the remote VPN Gateway, then a VPN tunnel cannot be established.
4. An IKE session is

*Figure 4: IKE Policies*

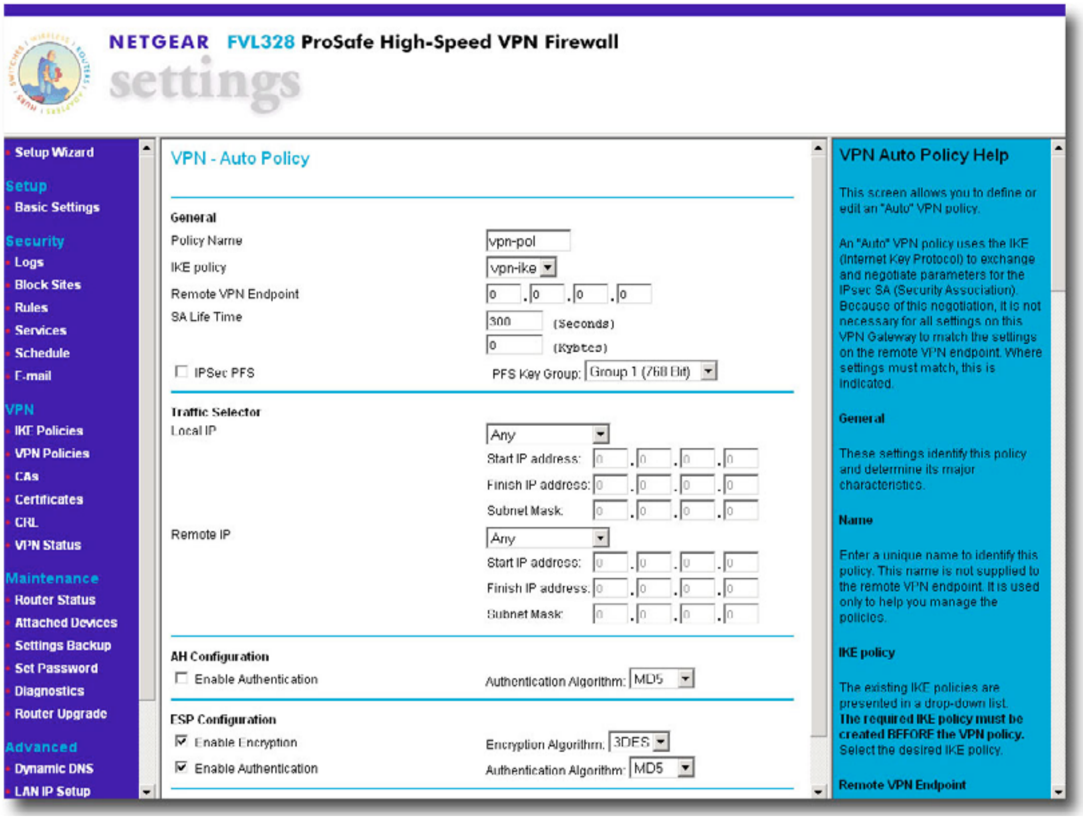
**Step 2**

VPN IKE / IPSec Setup:

Go to [VPN -> VPN Policies] and add a new “Auto Policy”. Enter a policy name (e.g. vpn-pol) and choose as “IKE policy” the previously defined policy “vpn-ike”. The “Remote VPN Endpoint” Adress is 0.0.0.0.

In the “Traffic Selector” passage choose “Any” as “Local IP” and “Remote IP”.

Enable the “ESP configuration” by checking “Enable Encryption” **and** “Enable Authentication”. Please change the “Encryption Algorithm” from “DES” to “3DES”.



VPN - Auto Policy

General

Policy Name: vpn-pol

IKE policy: vpn-ike

Remote VPN Endpoint: 0 . 0 . 0 . 0

SA Life Time: 300 (Seconds)
0 (Kybtes)

□ IPSec PFS PFS Key Group: Group 1 (768 Bit)

Traffic Selector

Local IP: Any
Start IP address: 0 . 0 . 0 . 0
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

Remote IP: Any
Start IP address: 0 . 0 . 0 . 0
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

AH Configuration

□ Enable Authentication Authentication Algorithm: MD5

ESP Configuration

☑ Enable Encryption Encryption Algorithm: 3DES

☑ Enable Authentication Authentication Algorithm: MD5

VPN Auto Policy Help

This screen allows you to define or edit an "Auto" VPN policy.

An "Auto" VPN policy uses the IKE (Internet Key Protocol) to exchange and negotiate parameters for the IPsec SA (Security Association). Because of this negotiation, it is not necessary for all settings on this VPN Gateway to match the settings on the remote VPN endpoint. Where settings must match, this is indicated.

**General**

These settings identify this policy and determine its major characteristics.

**Name**

Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.

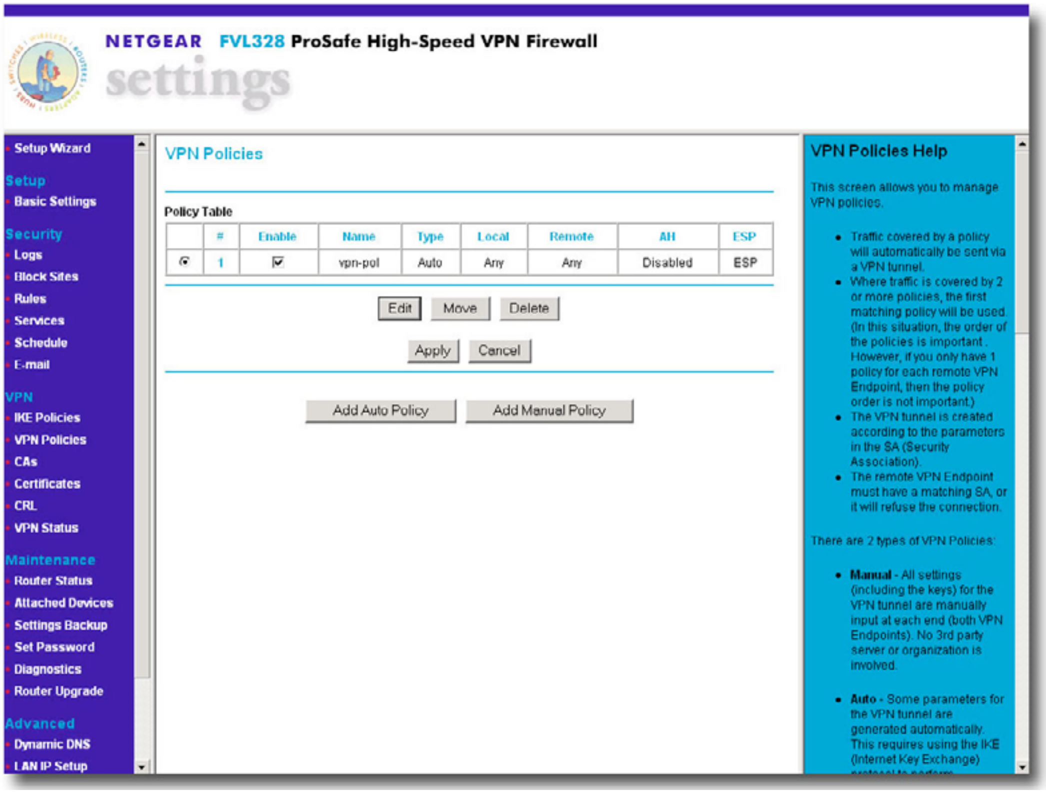
**IKE policy**

The existing IKE policies are presented in a drop-down list. **The required IKE policy must be created BEFORE the VPN policy.** Select the desired IKE policy.

**Remote VPN Endpoint**

*Figure 5: VPN - Auto Policy*

After step 2 the configuration should look like this:



VPN Policies

Policy Table

| | # | Enable | Name | Type | Local | Remote | AH | ESP |
|---|---|---|---|---|---|---|---|---|
| ● | 1 | ☑ | vpn-pol | Auto | Any | Any | Disabled | ESP |

VPN Policies Help

This screen allows you to manage VPN policies.

- Traffic covered by a policy will automatically be sent via a VPN tunnel.
- Where traffic is covered by 2 or more policies, the first matching policy will be used. (In this situation, the order of the policies is important . However, if you only have 1 policy for each remote VPN Endpoint, then the policy order is not important.)
- The VPN tunnel is created according to the parameters in the SA (Security Association).
- The remote VPN Endpoint must have a matching SA, or it will refuse the connection.

There are 2 types of VPN Policies:

- **Manual** - All settings (including the keys) for the VPN tunnel are manually input at each end (both VPN Endpoints). No 3rd party server or organization is involved.
- **Auto** - Some parameters for the VPN tunnel are generated automatically. This requires using the IKE (Internet Key Exchange)

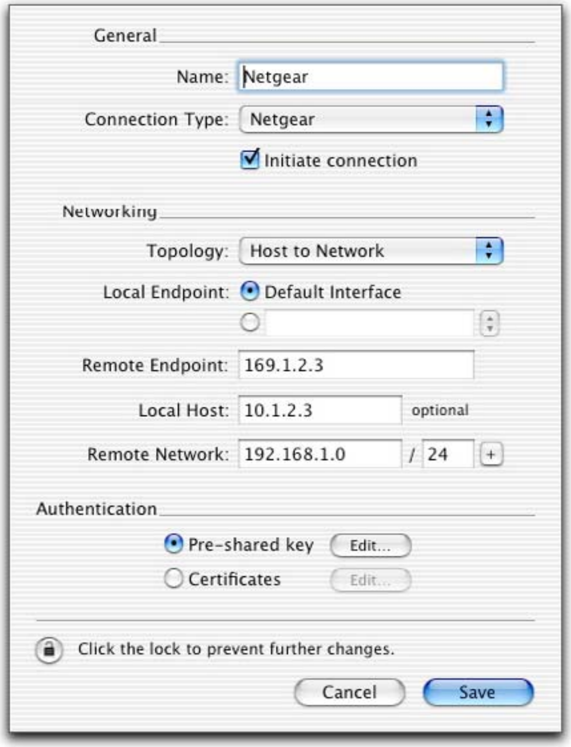
*Figure 6: VPN Policies*

## 3.3 VPN Tracker configuration

**Step 1**

Add a new connection with the following options: Choose „Netgear“ as the Connection Type, „Host to Network“ as Topology, then type in the remote endpoint (169.1.2.3) and the remote network (192.168.1.0/24).

If you are using the NETGEAR FVS 318 VPN Firewall, you have to enter an IP address in the field “local host”. This address must be the same as that which you entered in chapter 3.1 figure 2 (e.g. 10.1.2.3). If you are using the FVL 328 router, you could leave this field empty.



General

Name: Netgear

Connection Type: Netgear

☑ Initiate connection

Networking

Topology: Host to Network

Local Endpoint: ● Default Interface

○

Remote Endpoint: 169.1.2.3

Local Host: 10.1.2.3 optional

Remote Network: 192.168.1.0 / 24

Authentication

● Pre-shared key

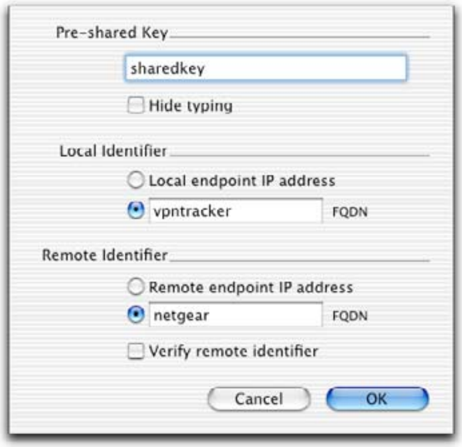
○ Certificates

Click the lock to prevent further changes.

*Figure 7: VPN Tracker Main Window*

**Step 2**

Select as “Authentication” method „Pre-shared key“ and click “Edit...”. Type in the same shared secret that you typed-in in the NETGEAR router (Figure 2). Type in your local identifiers (e.g. vpntracker) and the remote one (e.g. netgear). The local identifier in VPN tracker is the remote identifier in the NETGEAR configuration and vice versa.



Pre-shared Key

sharedkey

□ Hide typing

Local Identifier

○ Local endpoint IP address

● vpntracker FQDN

Remote Identifier

○ Remote endpoint IP address

● netgear FQDN

□ Verify remote identifier

*Figure 8: VPN Tracker - Authentication dialog*

**Step 3**

Save the connection and Click „Start IPsec“ in the VPN Tracker main window.

You’re done. After 10-20 seconds the red status indicator for the connection should change to green, which means you’re securely connected to the NETGEAR VPN Firewall. After IPsec has been started, you may quit VPN Tracker. The IPsec service will keep running.

Simply test your connection by pinging a host in the NETGEAR VPN Firewall network from the dialed-in Mac in the “Terminal” utility:

```
ping 192.168.1.1
```

### Debugging

If the status indicator does not change to green please have a look at the log file on both sides.  You can define the amount of information available in the log file in the VPN Tracker preferences.

# 4. Connecting a VPN Tracker Host to a NETGEAR VPN Firewall using Certificates

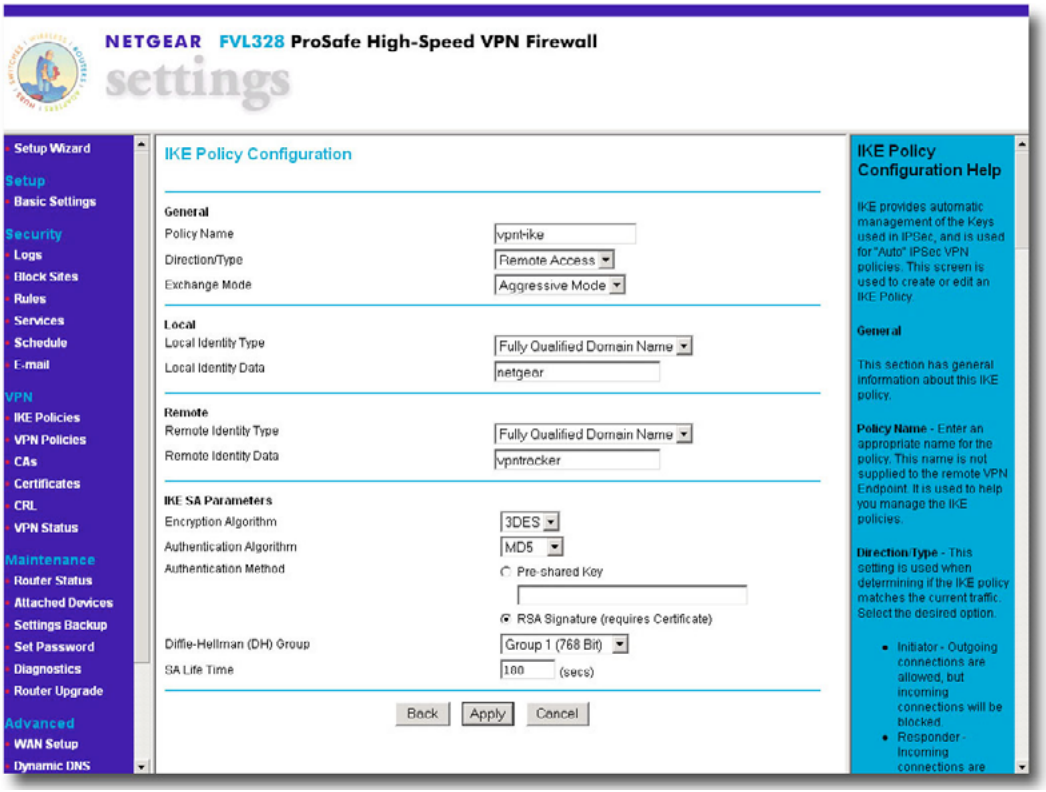
First, make sure to use VPN Tracker 2.0.5 or higher, because of major updates in Certificate management. You need a CA with private key, so one VPN Tracker Professional Edition is required if you don't actually have a signing CA. Only one VPN Tracker Professional Edition is required, other VPN users can use a Personal Edition. For further information please refer to chapter 3 in the VPN Tracker manual.

## 4.1 NETGEAR VPN Firewall configuration

**Step 1** IKE Policy Configuration:

Go to [VPN -> IKE Policies] and add a new policy. Enter a connection name (e.g. vpn-ike) and use "Remote Access" as Direction Mode (this implicates the "Aggressive Mode"). You have to use identifiers in the  passage 'Local' and 'Remote'. This settings refers to the "Local-" and "Remote identifiers" settings in VPN Tracker and the optional domain name field in the certificates. Please type in a arbitrary "Full Qualified Domain name" identifier (e.g. "netgear" and "vpntracker").

Finally you have to choose "RSA Signature" as "Authentication Method".



IKE Policy Configuration

General

Policy Name: vpnt-ike

Direction/Type: Remote Access

Exchange Mode: Aggressive Mode

Local

Local Identity Type: Fully Qualified Domain Name

Local Identity Data: netgear

Remote

Remote Identity Type: Fully Qualified Domain Name

Remote Identity Data: vpntracker

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

Authentication Method: ○ Pre-shared Key ● RSA Signature (requires Certificate)

Diffie-Hellman (DH) Group: Group 1 (768 Bit)

SA Life Time: 180 (secs)

IKE Policy Configuration Help

IKE provides automatic management of the Keys used in IPSec, and is used for "Auto" IPSec VPN policies. This screen is used to create or edit an IKE Policy.

General

This section has general information about this IKE policy.

**Policy Name** - Enter an appropriate name for the policy. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the IKE policies.

**Direction/Type** - This setting is used when determining if the IKE policy matches the current traffic. Select the desired option.

- Initiator - Outgoing connections are allowed, but incoming connections will be blocked.
- Responder - Incoming connections are

*Figure 9: IKE Policy Configuration*

**Step 2**

VPN IKE / IPSec Setup:

The setup of adding a Auto VPN Policy works the same way as described in step 2 in section 3.

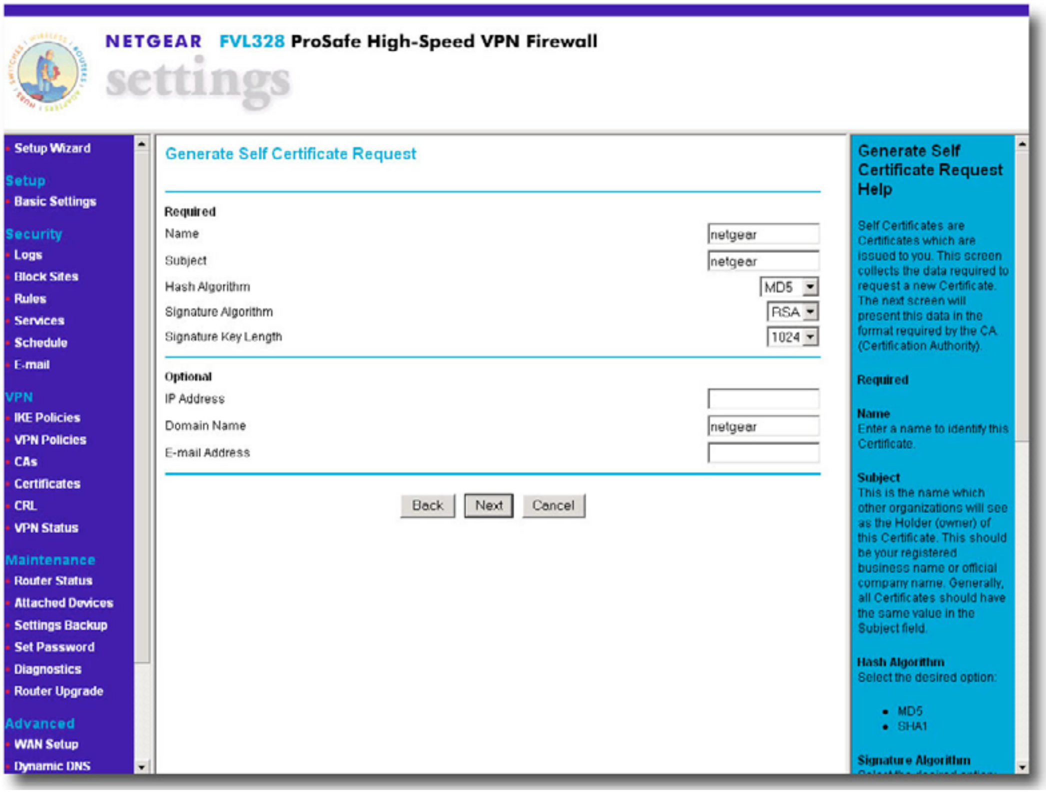
**Step 3**

Certificates Setup:

Please go to [VPN -> Certificates] and generate a “Certificate Request”. Enter a name and a subject for the Certificate. Choose a “Signature key length” of “1024” Bit.

You have to use a “Optional” “Domain Name”. This setting refers to the “Local Identifier” in the IKE Policies and the remote identifier in VPN Tracker.

**Note:** Please make sure, that the time in [Security -> Schedule -> Date/Time] is set to your local time zone, otherwise you can’t generate and sign the self certificate, explained in step 4-6.



Generate Self Certificate Request

Required

| | |
|---|---|
| Name | netgear |
| Subject | netgear |
| Hash Algorithm | MD5 |
| Signature Algorithm | RSA |
| Signature Key Length | 1024 |

Optional

| | |
|---|---|
| IP Address | |
| Domain Name | netgear |
| E-mail Address | |

Generate Self Certificate Request Help

Self Certificates are Certificates which are issued to you. This screen collects the data required to request a new Certificate. The next screen will present this data in the format required by the CA (Certification Authority).

Required

Name
Enter a name to identify this Certificate.

Subject
This is the name which other organizations will see as the Holder (owner) of this Certificate. This should be your registered business name or official company name. Generally, all Certificates should have the same value in the Subject field.

Hash Algorithm
Select the desired option:

- MD5
- SHA1

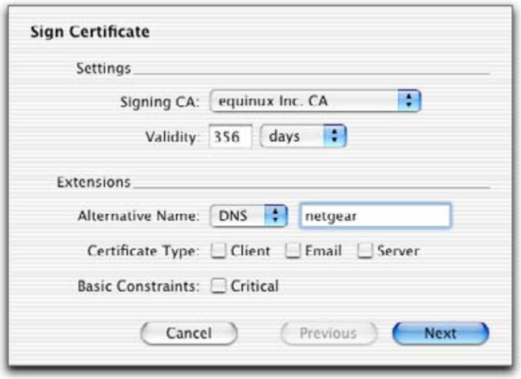
Signature Algorithm

*Figure 10: Generate Self Certificate Request*

**Step 4**

Save the certificate request in a text file. Import the Request in the "Request" tab in VPN Tracker. Finally "Sign" the request with a CA. The "Alternative Name" field is predefined with the value you entered in the certificate signing request. It should be the same as the "Alternate Subject Name", defined before.

Please note: This feature requires the VPN Tracker Professional Edition.



Sign Certificate

Settings

Signing CA: equinux Inc. CA

Validity: 356 days

Extensions

Alternative Name: DNS netgear

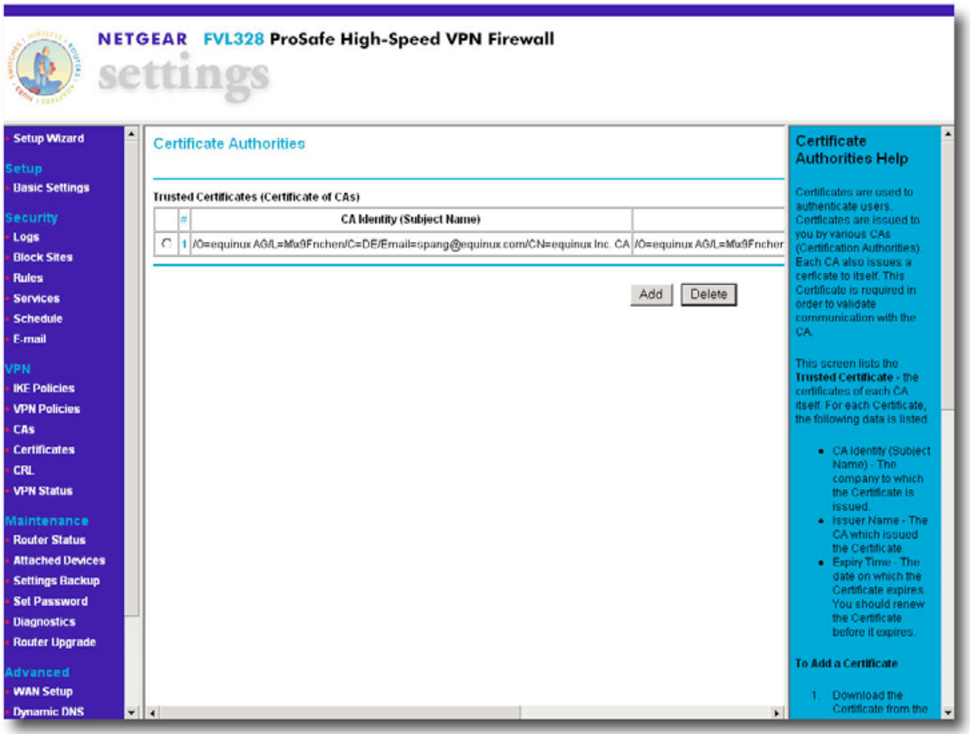
Certificate Type: □ Client □ Email □ Server

Basic Constraints: □ Critical

*Figure 11: VPN Tracker - Sign Certificate*

**Step 5**

Go to [VPN -> CAs] and import the CA which you used for signing into the NETGEAR router. The CA file must be exported in the PEM- format.



Certificate Authorities

Trusted Certificates (Certificate of CAs)

| | # | CA Identity (Subject Name) | |
|---|---|---|---|
| ○ | 1 | /O=equinux AG/L=Mu9Fnchen/C=DE/Email=spang@equinux.com/CN=equinux Inc. CA | /O=equinux AG/L=Mu9Fncher |

Certificate Authorities Help

Certificates are used to authenticate users. Certficates are issued to you by various CAs (Certification Authorities). Each CA also issues a cerficate to itself. This Certificate is required in order to validate communication with the CA.

This screen lists the **Trusted Certificate** - the certificates of each CA itself. For each Certificate, the following data is listed.

- CA Identity (Subject Name) - The company to which the Certificate is issued.
- Issuer Name - The CA which issued the Certificate.
- Expiry Time - The date on which the Certificate expires. You should renew the Certificate before it expires.

**To Add a Certificate**

1. Download the Certificate from the

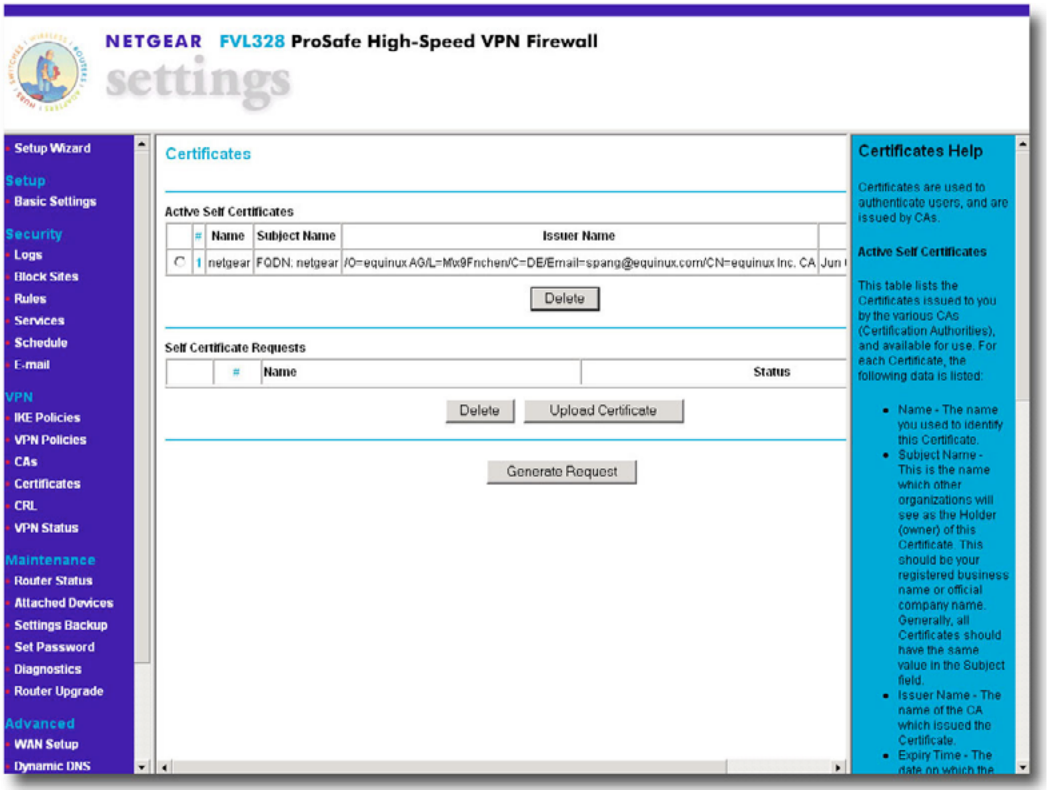
*Figure 12: Netgear Certficate Authorities window*

**Step 6**

Export the signed certificate in the PEM- format and "upload the Certificate" in the NETGEAR router.

Please note: The subject name of the certificate must look like this: "FQDN: netgear"

After step 6 the configuration should look like this:



Certificates

Active Self Certificates

|  | # | Name | Subject Name | Issuer Name |  |
|---|---|---|---|---|---|
| ○ | 1 | netgear | FQDN: netgear | /O=equinux AG/L=M\x9Fnchen/C=DE/Email=spang@equinux.com/CN=equinux Inc. CA | Jun |

Self Certificate Requests

|  | # | Name | Status |
|---|---|---|---|

Certificates Help

Certificates are used to authenticate users, and are issued by CAs.

Active Self Certificates

This table lists the Certificates issued to you by the various CAs (Certification Authorities), and available for use. For each Certificate, the following data is listed:

- Name - The name you used to identify this Certificate.
- Subject Name - This is the name which other organizations will see as the Holder (owner) of this Certificate. This should be your registered business name or official company name. Generally, all Certificates should have the same value in the Subject field.
- Issuer Name - The name of the CA which issued the Certificate.
- Expiry Time - The date on which the

*Figure 13: Netgear Certificate window*

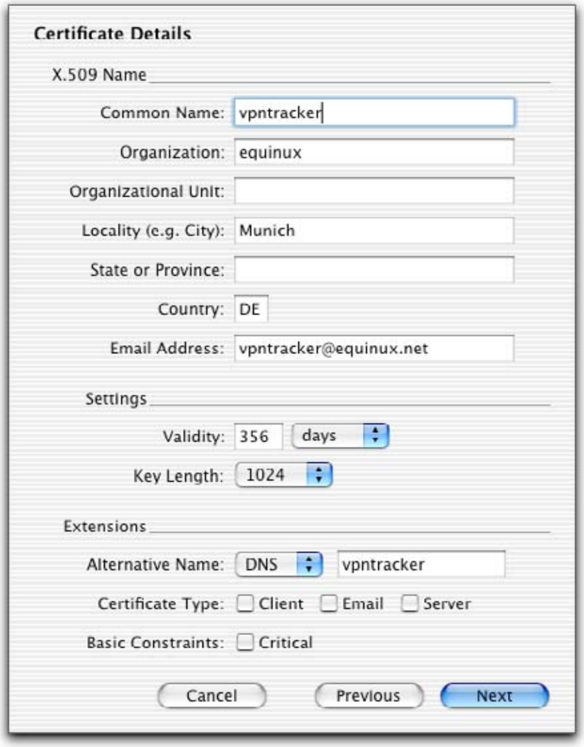
## 4.2 VPN Tracker configuration

**Step 1**

Create a new "Own certificate" for VPN Tracker.

Go to the VPN Tracker certificate manager (⌘ + "E") and create and sign a new certificate. Type in the certificate data.

You have to use an "Alternative Name". Choose DNS from the drop-down box and enter the alternative name. Please note: This name must be the same as the remote identifier in the NETGEAR IKE settings.



Certificate Details

X.509 Name

Common Name: vpntracker

Organization: equinux

Organizational Unit:

Locality (e.g. City): Munich

State or Province:

Country: DE

Email Address: vpntracker@equinux.net

Settings

Validity: 356 days

Key Length: 1024

Extensions

Alternative Name: DNS vpntracker

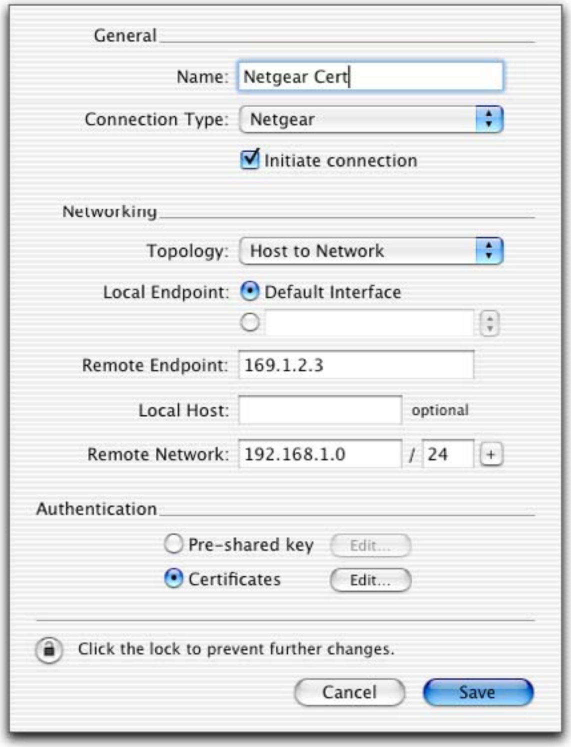
Certificate Type: □ Client □ Email □ Server

Basic Constraints: □ Critical

*Figure 14: Own certificate*

**Step 2**

Add a new connection with the following options: Choose „Netgear “ as Connection Type, „Host to Network“ as Topology, then type in the remote endpoint (169.1.2.3) and the remote network (192.168.1.0/24).



General

Name: Netgear Cert

Connection Type: Netgear

☑ Initiate connection

Networking

Topology: Host to Network

Local Endpoint: ● Default Interface

○

Remote Endpoint: 169.1.2.3

Local Host: optional

Remote Network: 192.168.1.0 / 24

Authentication

○ Pre-shared key

● Certificates

*Figure 15: VPN Tracker Main Window*

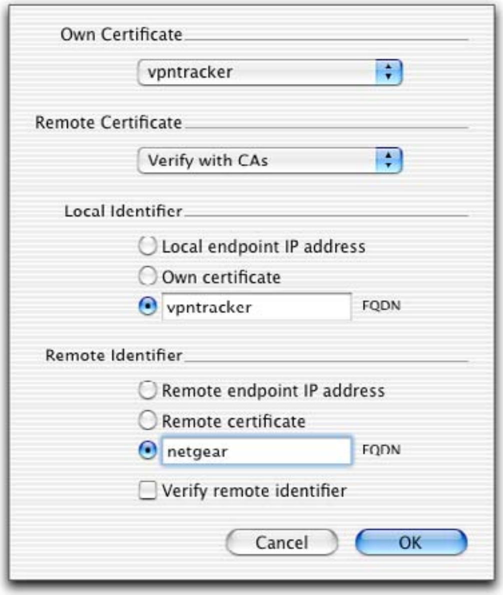
**Step 3**

Select „Certificates“ as “Authentication” method and click “Edit...”.

Choose as “own certificate” a self-signed certificate, you created with VPN Tracker and verify the remote certificate “with CAs”.

Type in your local identifier (e.g. vpntracker) and the remote one (e.g. netgear). The local identifier in VPN tracker is the remote identifier in the NETGEAR configuration and vice versa.

Do <u>not</u> “Verify the remote certificate”.



Own Certificate

vpntracker

Remote Certificate

Verify with CAs

Local Identifier

○ Local endpoint IP address
○ Own certificate
● vpntracker FQDN

Remote Identifier

○ Remote endpoint IP address
○ Remote certificate
● netgear FQDN

□ Verify remote identifier

*Figure 16: VPN Tracker Authentication dialog*

**Step 4**

Save the connection and Click „Start IPsec“ in the VPN Tracker main window.

You’re done. After 10-20 seconds the red status indicator for the connection should change to green, which means you’re securely connected to the NETGEAR VPN Firewall. After IPsec has been started, you may quit VPN Tracker. The IPsec service will keep running.

Now to test your connection simply ping a host in the NETGEAR VPN Firewall network from the dialed-in Mac in the “Terminal” utility:

```
ping 192.168.1.1
```

### Debugging

If the status indicator does not change to green please have a look at the log file on both sides.  You can define the amount of information available in the log file in the VPN Tracker preferences.