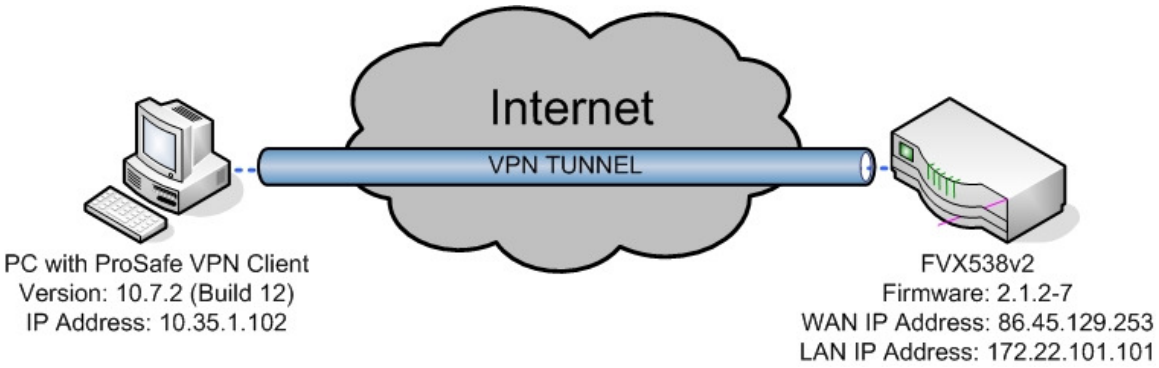
Mode Config of a VPN tunnel from ProSafe Client to FVX538v2 Router:

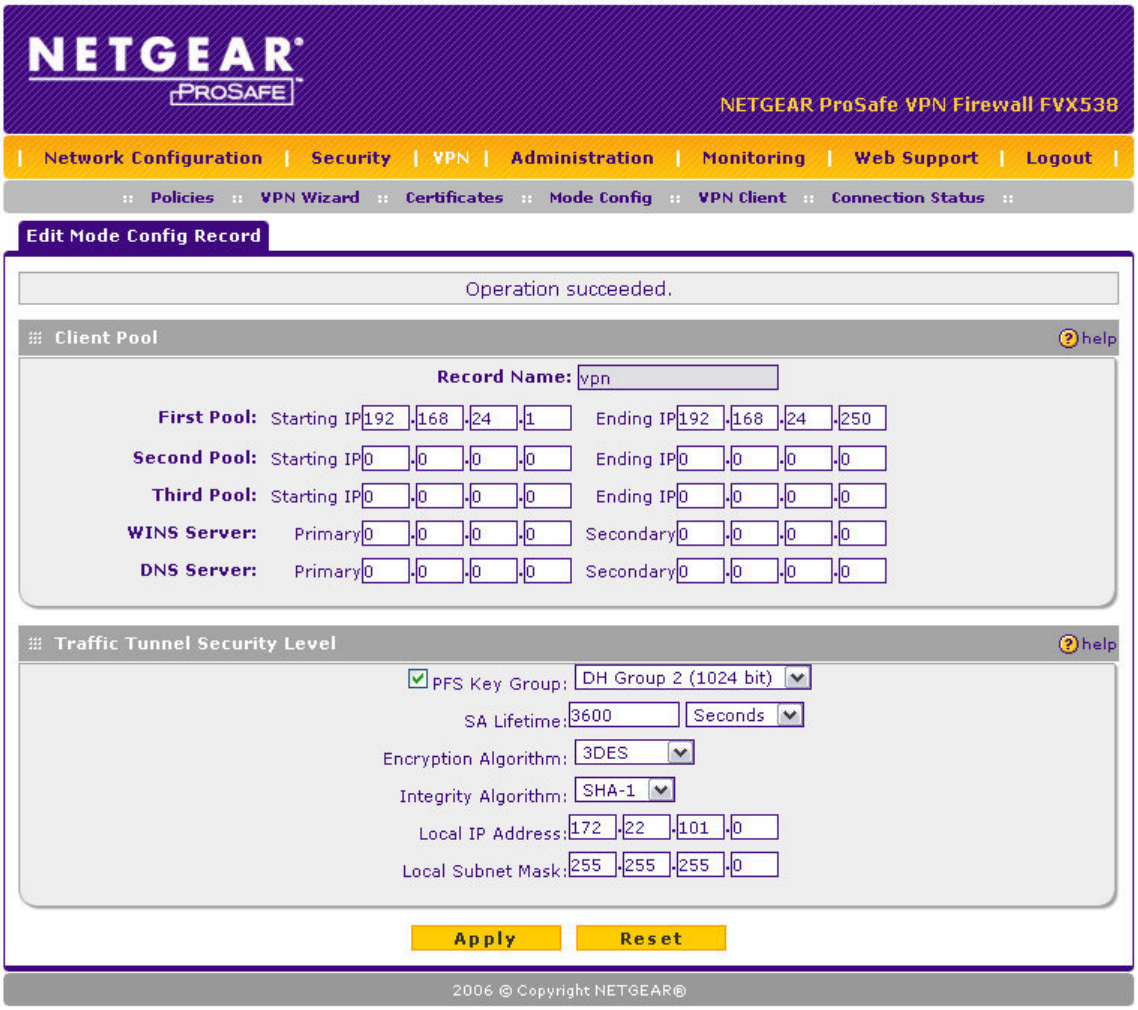
Mode Config is a feature included in some of the Netgear Routers which allows the IP addressing of the remote client devices be handled and controlled by the VPN Router by using a Virtual Adapter. This document will guide you on how to create IKE and Mode Config policies for your FVX538v2, as well as how to configure the VPN Pro-Safe VPN client in order to allow a Virtual Private Network to be established over the internet.



NOTE: This document assumes that your FVX538v2 is either receiving a public IP address on the WAN interface or that the gateway device(s) have the correct port forwarding or DMZ configured so that port 500 UDP is open for the FVX538v2, these gateway devices must also allow VPN pass-through.

FVX538v2 – Mode Config:

To configure it, go to the VPN section and then select Mode Config. For our example we'll use the following settings:



The first pool of IP addresses, 192.168.24.1 to 192.168.24.250, lists the addresses that the clients will acquire when they connect. Notice that you can add up to three pools, addresses from the second pool will be used when the addresses of the first pool are all in use. Likewise for the third pool, it'll be used when the first and second pools are exhausted. Notice that you can also set particular DNS servers or WINS for the client virtual adapters.

(**Note: DO NOT** add IP addresses that are currently in use in any of the networks at either side of the VPN tunnel – Use completely different subnets.)

FVX538v2 – IKE Policy:

With the Mode Config policy created, go to VPN, Policies, IKE policies and create a new one. For our example, we'll use the following settings.

NETGEAR ProSafe
NETGEAR ProSafe VPN Firewall FVX538

Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout

Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status

Edit IKE Policy — Add New VPN Policy

Operation succeeded.

Mode Config Record (help)
Do you want to use Mode Config Record? Yes / No
Select Mode Config Record: vpn
view selected

General (help)
Policy Name: vpn
Direction / Type: Responder
Exchange Mode: Aggressive

Local (help)
Select Local Gateway: WAN1 / WAN2
Identifier Type: FQDN
Identifier: fvx_local.com

Remote (help)
Identifier Type : FQDN
Identifier: fvx_remote.com

IKE SA Parameters (help)
Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Authentication Method: Pre-shared key / RSA-Signature
Pre-shared key: 123456789 (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

Extended Authentication (help)
XAUTH Configuration: None / Edge Device / IPSec Host
Authentication Type: User Database
Username:
Password:

Apply Reset

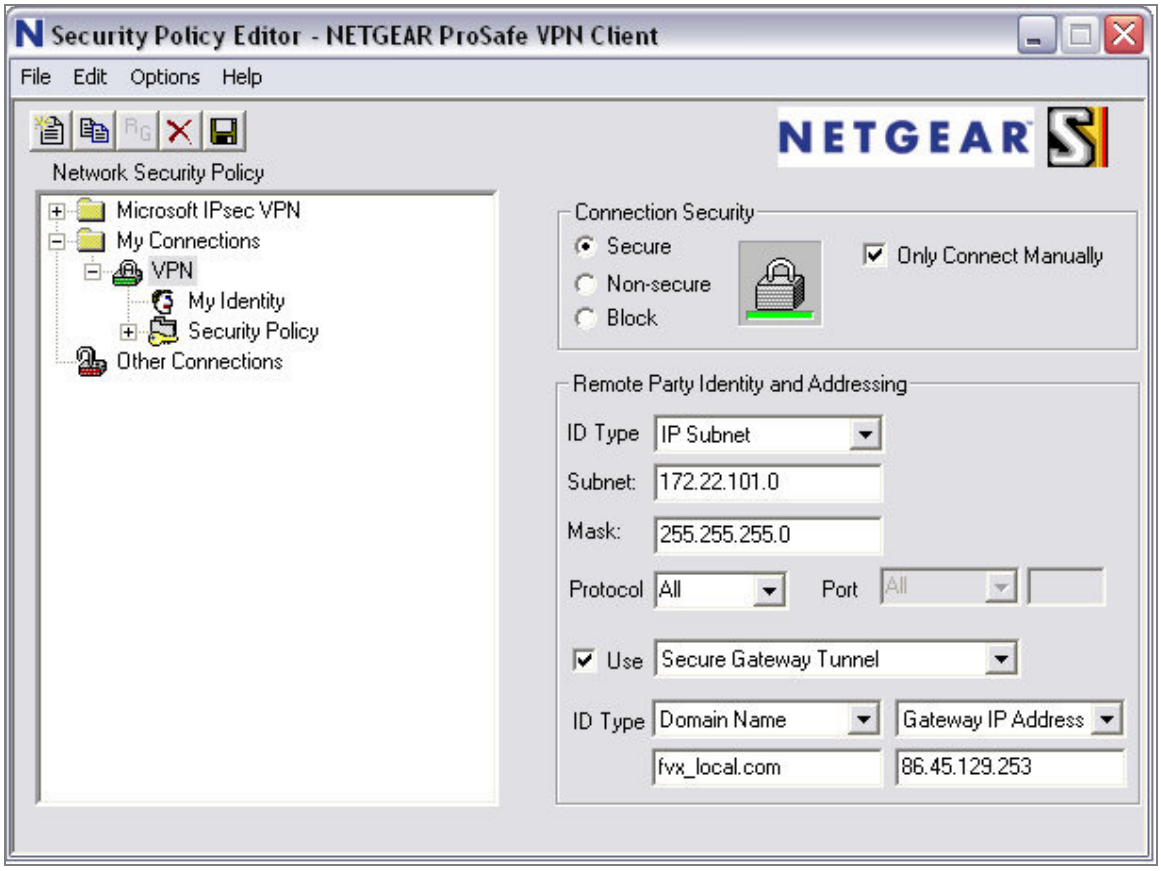
2006 © Copyright NETGEAR®

(**Note:** The pre-shared key could be any alphanumeric string)

Pro-Safe VPN Client - Configuration:

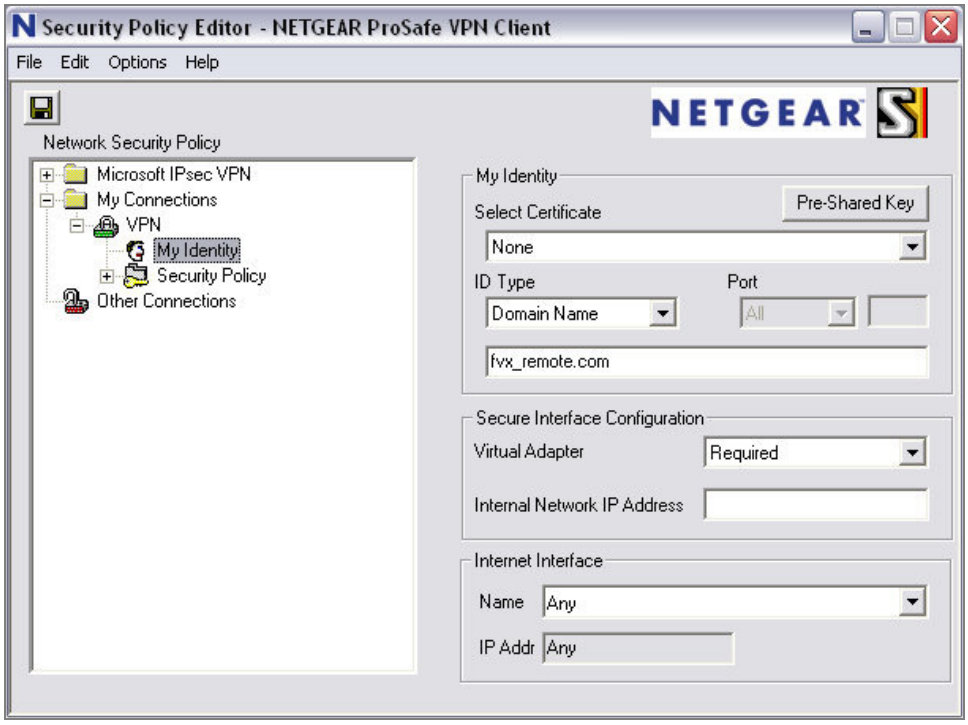
Right click on **"My Connections"** and add a new connection. Use the same name you used to name the VPN policy in your VPN gateway. In this example the name will be "VPN".

Click on the name of the new created connection and fill the parameters accordingly, for this example we'll use these:

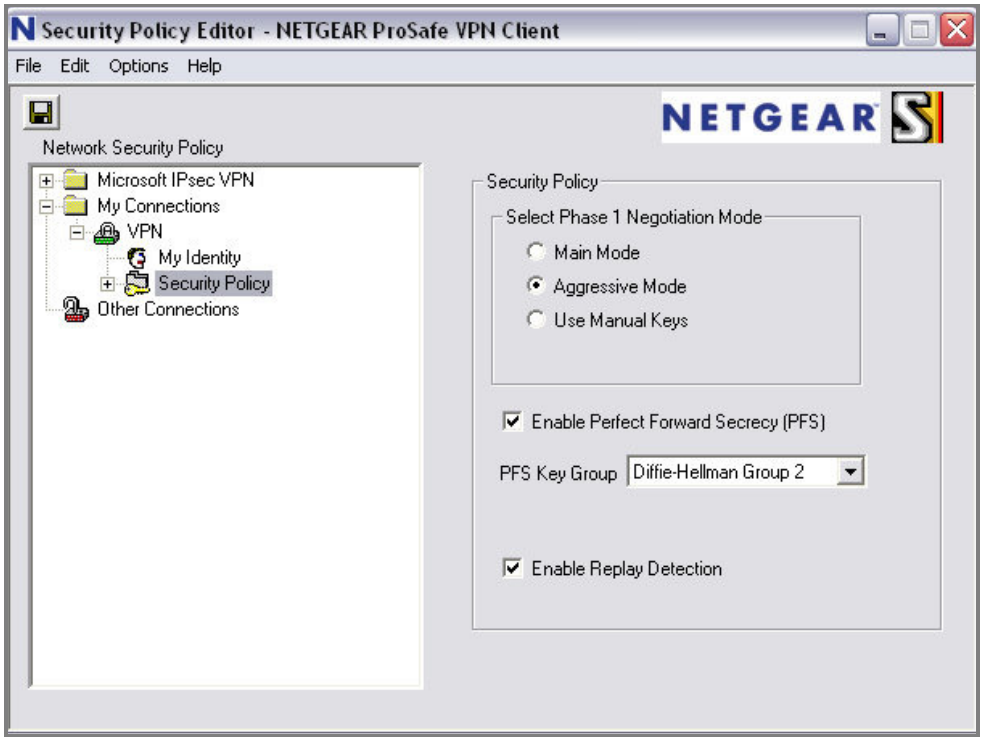


(**NOTE:** The Subnet and Mask must be those of the LAN side of your FVX538. The Gateway IP address field must be the WAN IP address of the FVX538.)

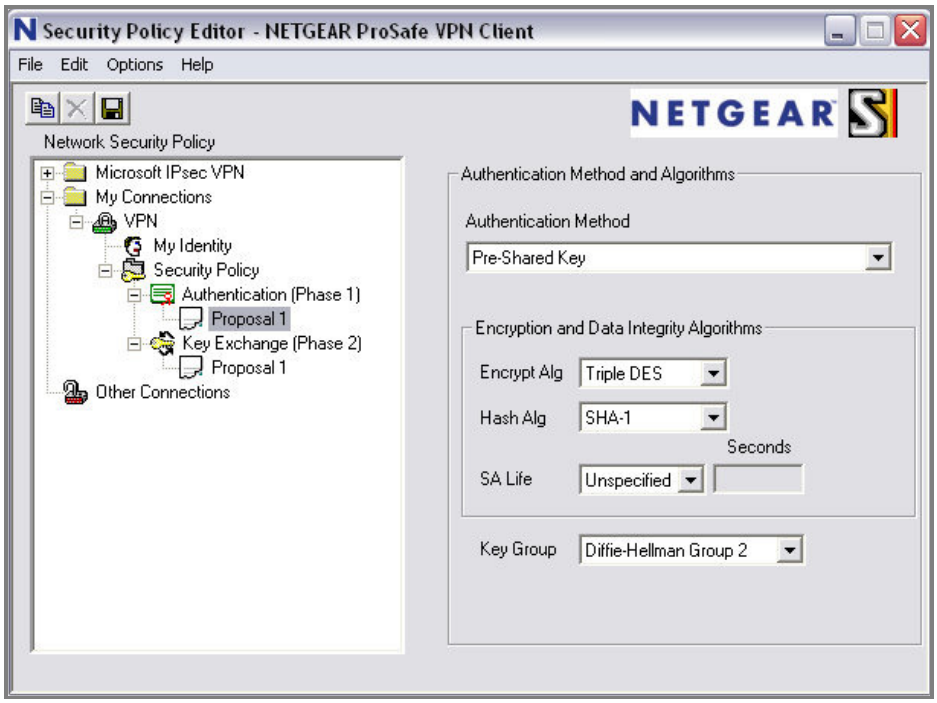
Click on **"My Identity"** and fill the fields accordingly, be sure to click on the Pre-Shared Key button and input your own pre shared key. Here are the settings used in our example:



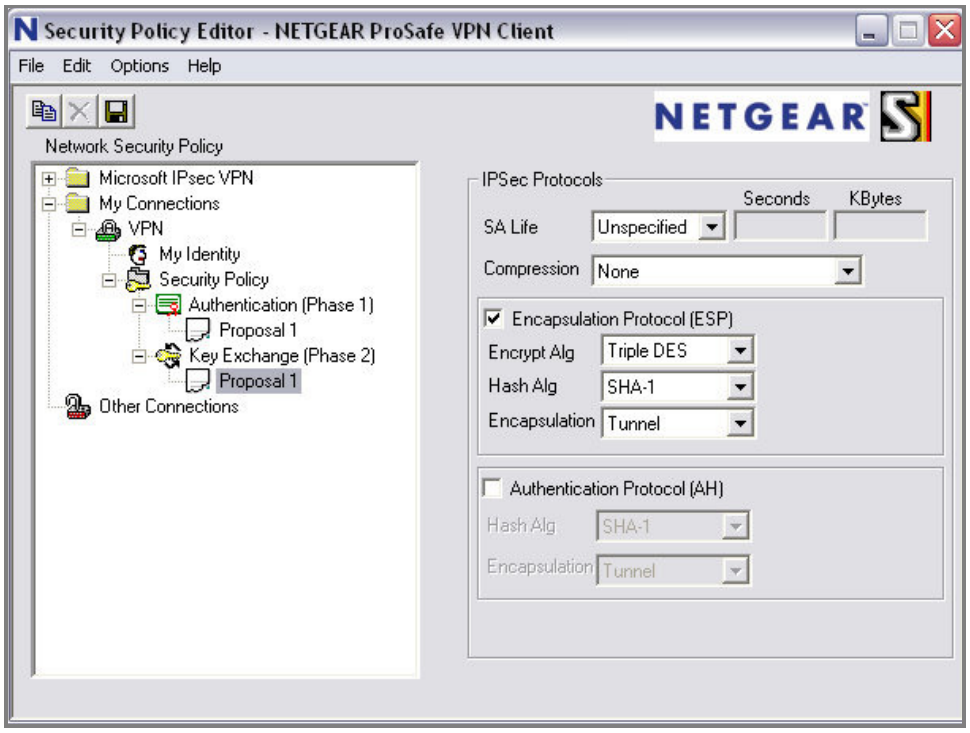
Click on "Security Policy" and verify the following settings:



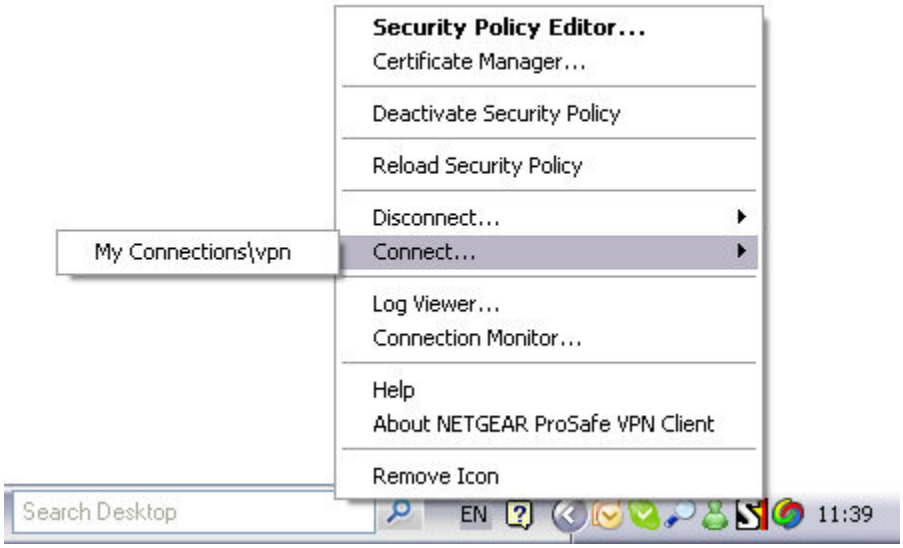
Next, expand **"Security Policy"** and **"Authentication (Phase 1)"** – Click on **"Proposal 1"** and verify the settings contained to match the ones of your policy. Functional settings in our example:



Open the **"Key Exchange (Phase 2)"** category – Click on **"Proposal 1"** and verify the settings contained to match the ones of your policy. Functional settings in our example:



For last, right click on the tray icon of the Netgear VPN client with your mouse, select connect and select the connection you just created.



If your settings are correct you'll receive a message confirming the connection.

FVX538v2 – Verifying connection:

If you wish to verify that the connection is established, which IP did you receive from the Mode Config pools and whether you can access the LAN side of the VPN router, open a command console and use the **IPCONFIG** command to see the IP address of the Virtual Adapter. You can also use the command **PING** towards the LAN address of your router to verify connectivity.