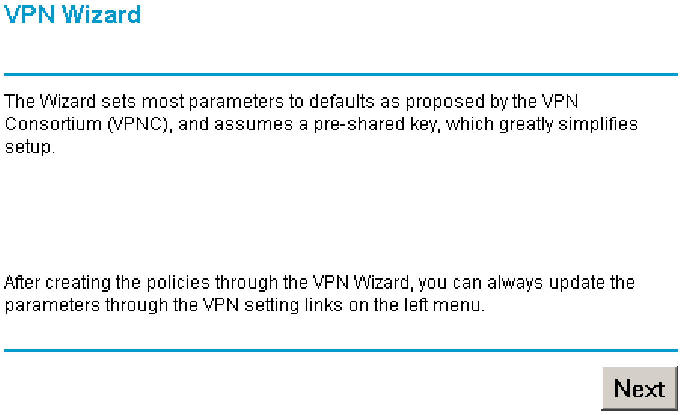
Configure VPN between ProSafe VPN Client Software and FVG318

The following configuration is tested with:
NETGEAR FVG318 with firmware version 1.0.41
NETGEAR ProSafe VPN Client Software version 10.5.1

Configure the FVG318

1. Log into the FVG318's admin GUI.
2. Click on VPN Wizard on the left panel under VPN.
3. Click Next.

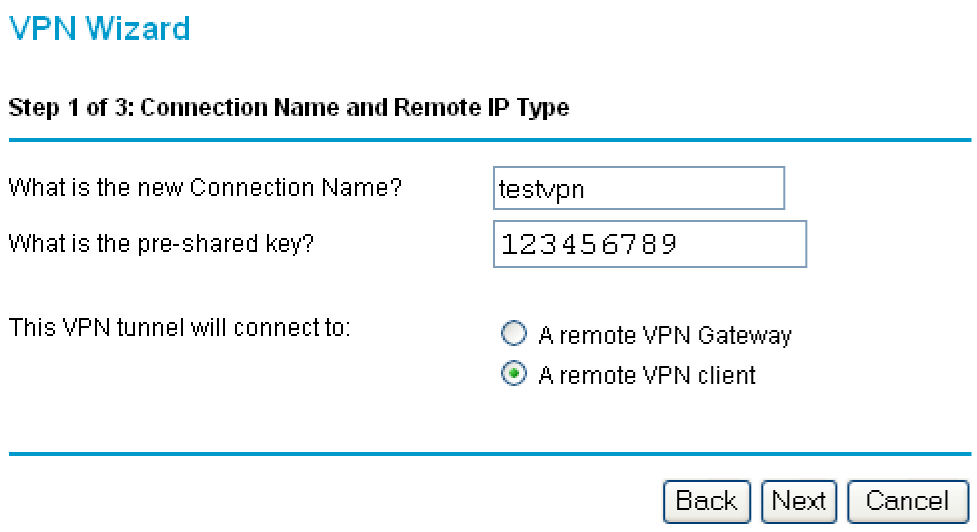


VPN Wizard

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup.

After creating the policies through the VPN Wizard, you can always update the parameters through the VPN setting links on the left menu.

4. Enter a connection name and a value for the pre-shared key. The same name and pre-shared key have to be entered when configuring the ProSafe VPN client software. Select This VPN tunnel will connect to A remote VPN client.



VPN Wizard

Step 1 of 3: Connection Name and Remote IP Type

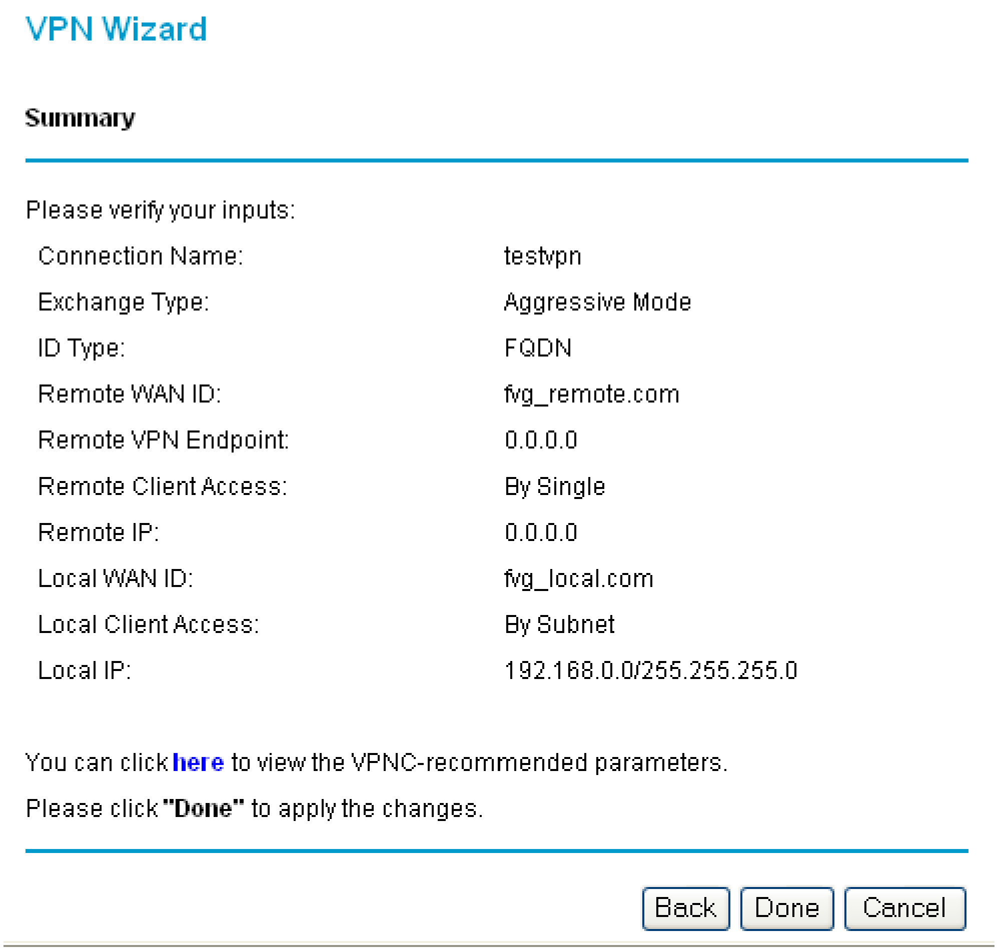
What is the new Connection Name? testvpn

What is the pre-shared key? 123456789

This VPN tunnel will connect to:

○ A remote VPN Gateway
● A remote VPN client

5. A summary of the VPN policy will be displayed. Click Done.



VPN Wizard

Summary

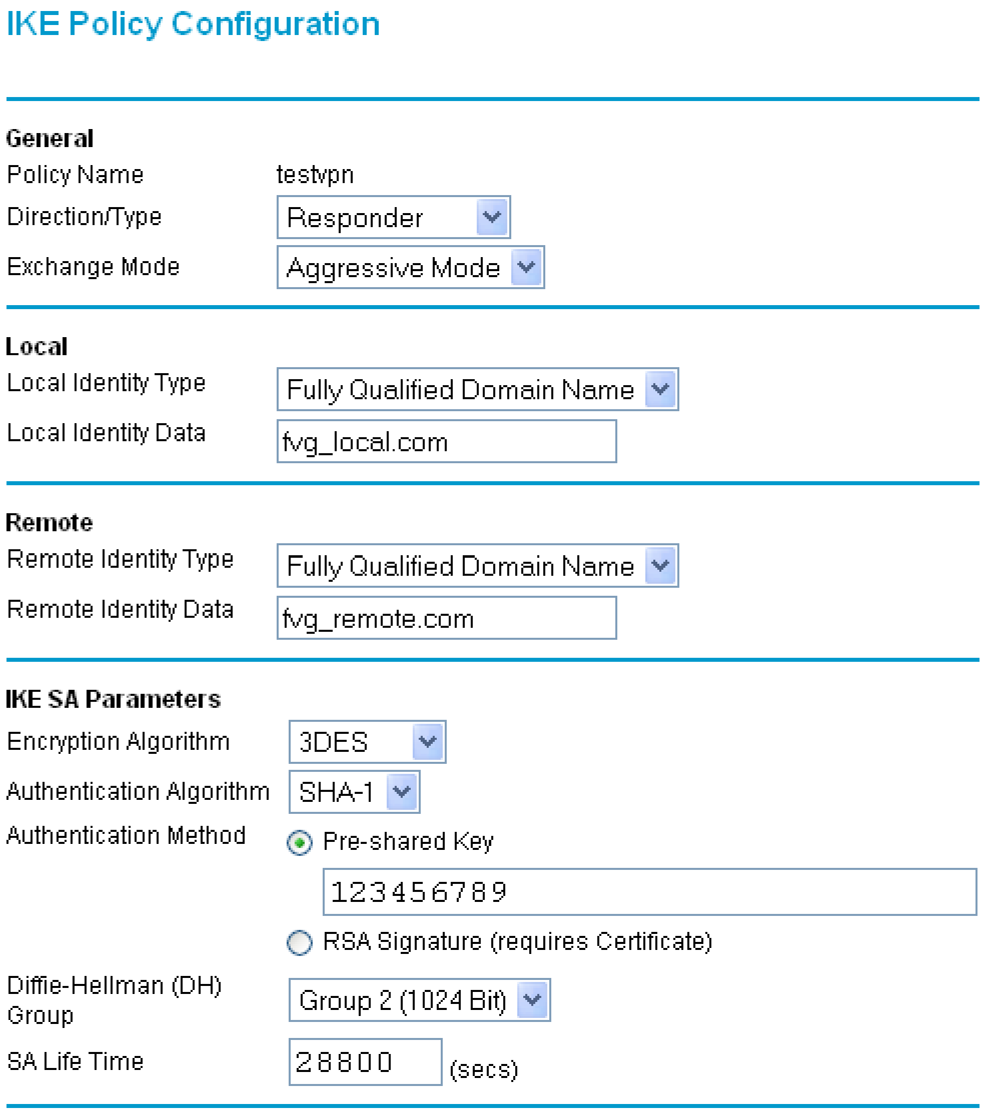
Please verify your inputs:

Connection Name:	testvpn
Exchange Type:	Aggressive Mode
ID Type:	FQDN
Remote WAN ID:	fvg_remote.com
Remote VPN Endpoint:	0.0.0.0
Remote Client Access:	By Single
Remote IP:	0.0.0.0
Local WAN ID:	fvg_local.com
Local Client Access:	By Subnet
Local IP:	192.168.0.0/255.255.255.0

You can click **here** to view the VPNC-recommended parameters.

Please click **"Done"** to apply the changes.

6. You can review the IKE policy and VPN policy by clicking on IKE Policies.



IKE Policy Configuration

General

Policy Name	testvpn
Direction/Type	Responder
Exchange Mode	Aggressive Mode

Local

Local Identity Type	Fully Qualified Domain Name
Local Identity Data	fvg_local.com

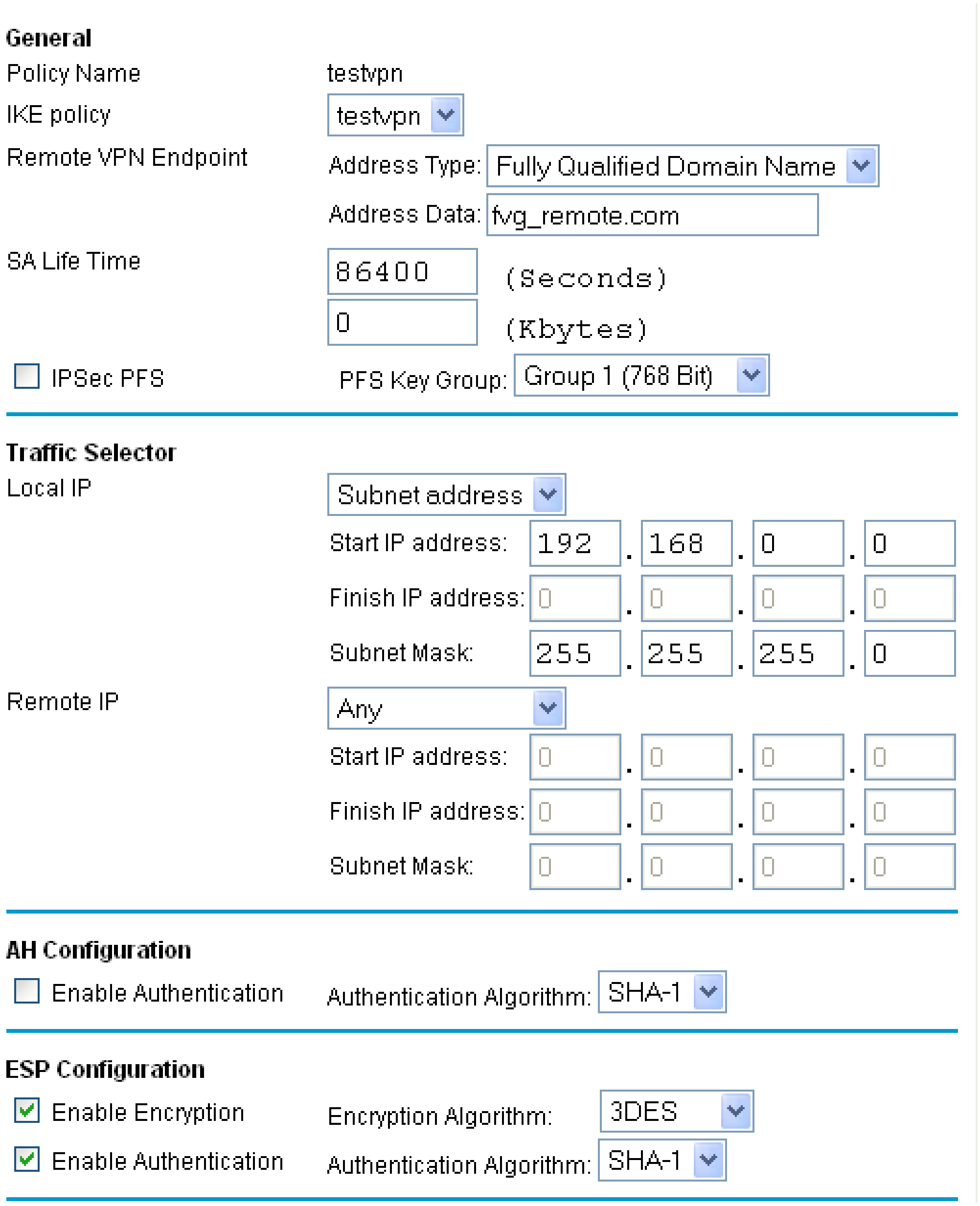
Remote

Remote Identity Type	Fully Qualified Domain Name
Remote Identity Data	fvg_remote.com

IKE SA Parameters

Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Authentication Method	● Pre-shared Key 123456789 ○ RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group	Group 2 (1024 Bit)
SA Life Time	28800 (secs)

7. And VPN Policies under VPN. In most cases, you can just leave them as it.



General

Policy Name: testvpn

IKE policy: testvpn

Remote VPN Endpoint: Address Type: Fully Qualified Domain Name

Address Data: fvg_remote.com

SA Life Time: 86400 (Seconds)

0 (Kbytes)

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

Traffic Selector

Local IP: Subnet address

Start IP address: 192 . 168 . 0 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 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: SHA-1

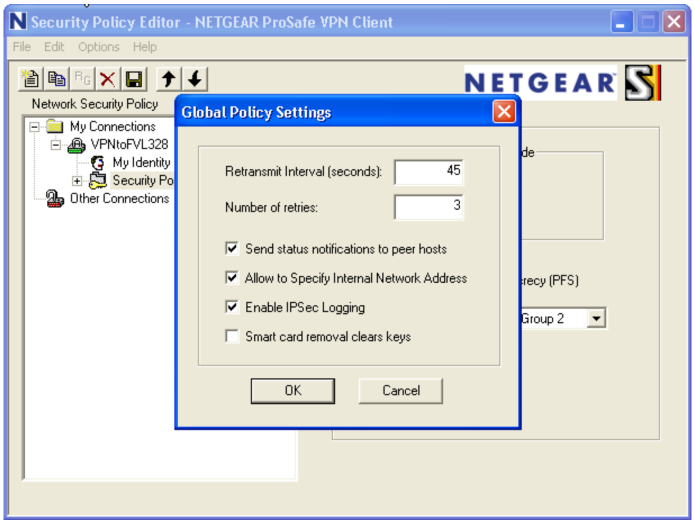
ESP Configuration

☑ Enable Encryption — Encryption Algorithm: 3DES

☑ Enable Authentication — Authentication Algorithm: SHA-1

Configure the ProSafe VPN Client Software

1. Right click on the ProSafe VPN client icon on the system tray and select Security Policy Editor.
2. Under the Options menu, select Global Policy Settings. The Global Policy Setting dialog box opens. Make sure Allow to Specify Internal Network Address is checked.



Global Policy Settings

Retransmit Interval (seconds): 45

Number of retries: 3

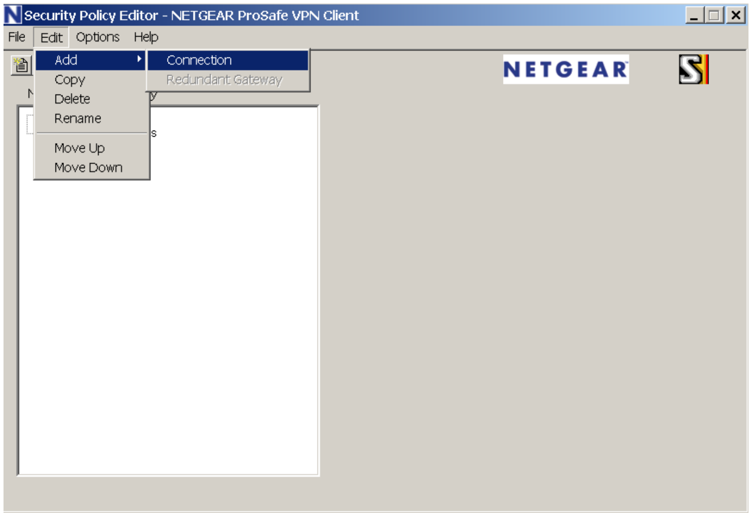
☑ Send status notifications to peer hosts

☑ Allow to Specify Internal Network Address

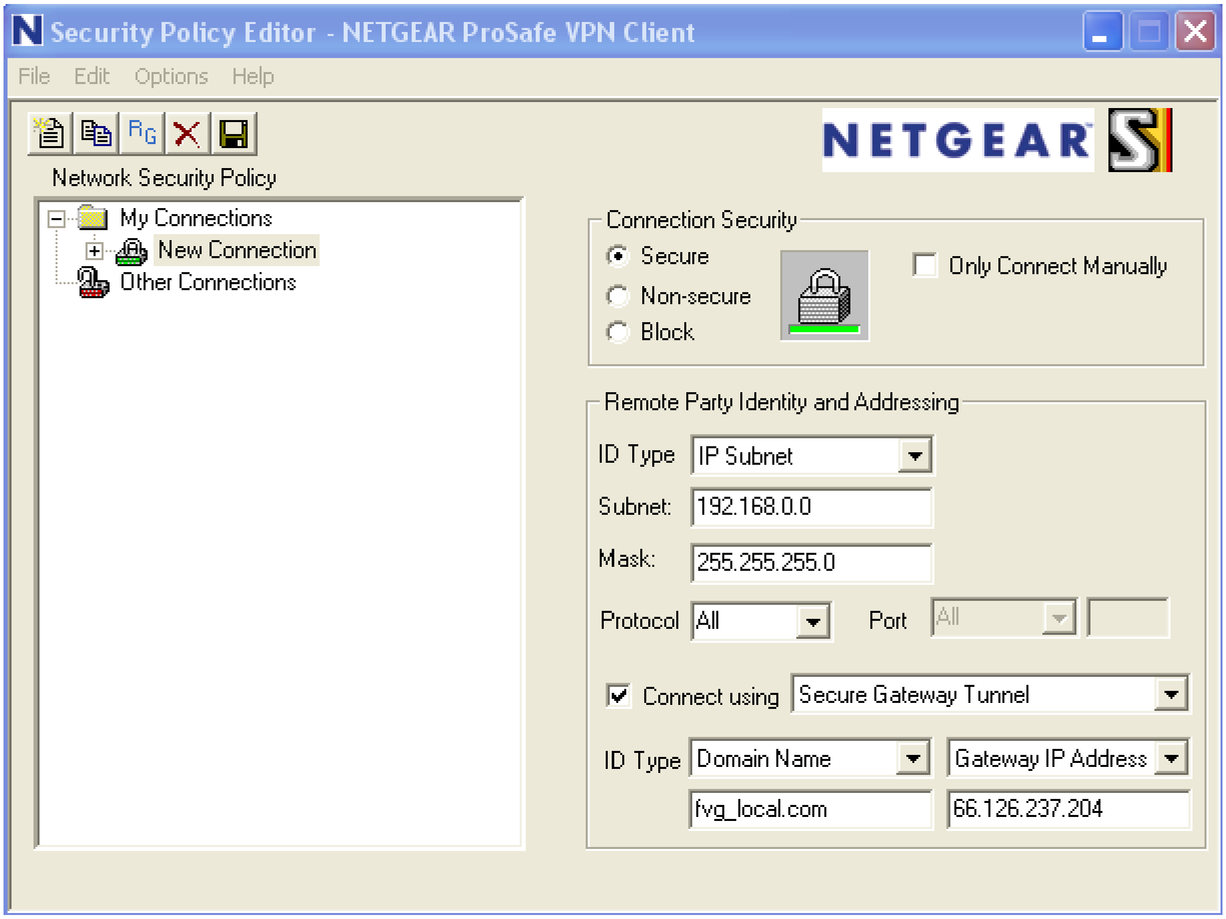
☑ Enable IPSec Logging

☐ Smart card removal clears keys

3. Under the Edit menu, select Add and select Connection.



4. A new connection will be created. You can rename the connection name by double click on the name. On the right panel, under Remote Party Identity and Addressing, select IP Subnet as ID Type, enter the LAN subnet on the FVG318 as Subnet and enter the LAN subnet mask as Mask. Choose All for Protocol. Check the box Connect using and select Secure Gateway Tunnel. For ID Type, choose Domain Name and enter fvx_local.com under Domain Name. Select Gateway IP Address and enter the WAN IP address of the FVG318.



Network Security Policy

- My Connections
  - New Connection
- Other Connections

Connection Security

● Secure

○ Non-secure

○ Block

□ Only Connect Manually

Remote Party Identity and Addressing

ID Type: IP Subnet

Subnet: 192.168.0.0

Mask: 255.255.255.0

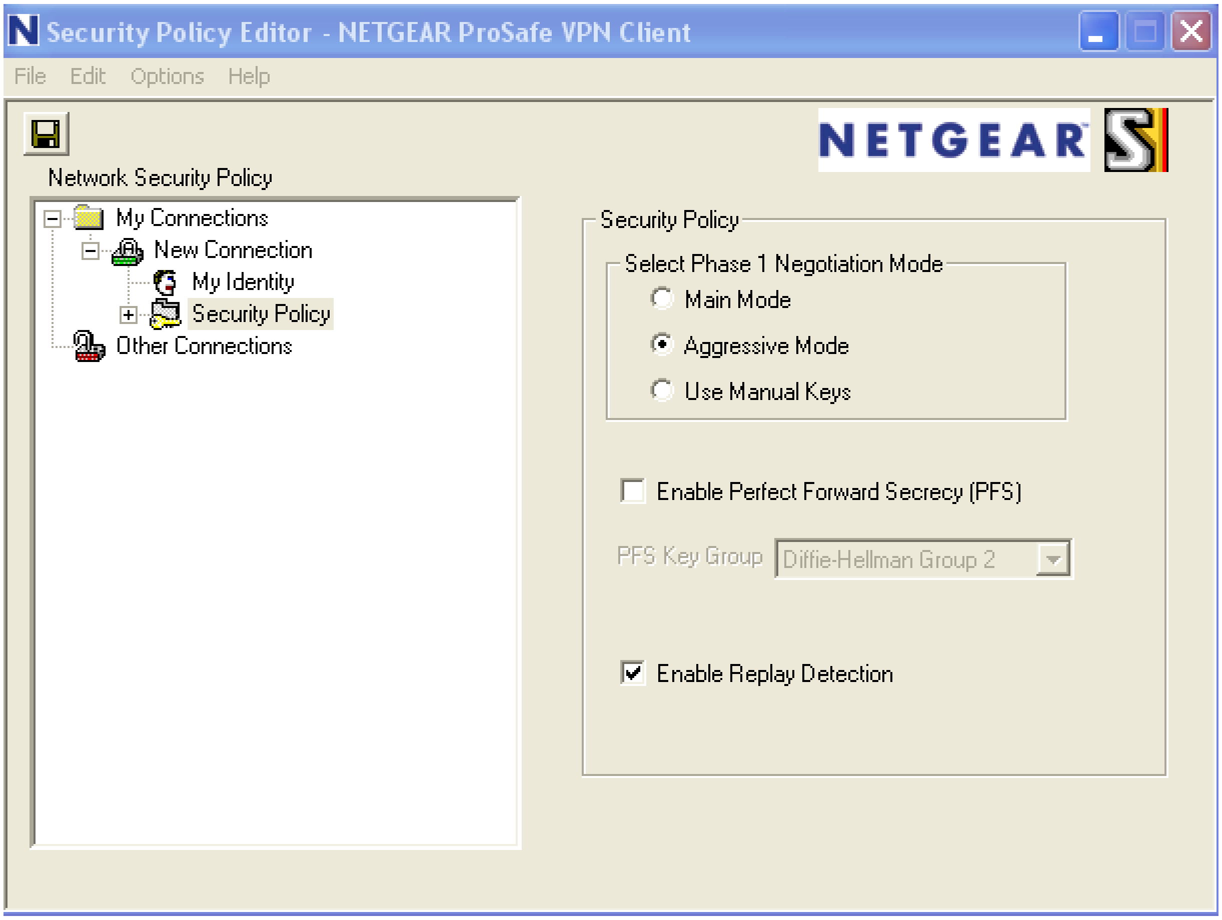
Protocol: All   Port: All

☑ Connect using: Secure Gateway Tunnel

ID Type: Domain Name   Gateway IP Address

fvg_local.com   66.126.237.204

5. On the left panel, click on Security Policy. On the right panel, select Aggressive Mode under Phase 1 Negotiation Mode. Make sure Enable Perfect Forward Secrecy is unchecked. Leave Enable Replay Detection checked.



Security Policy

Select Phase 1 Negotiation Mode

○ Main Mode

● Aggressive Mode

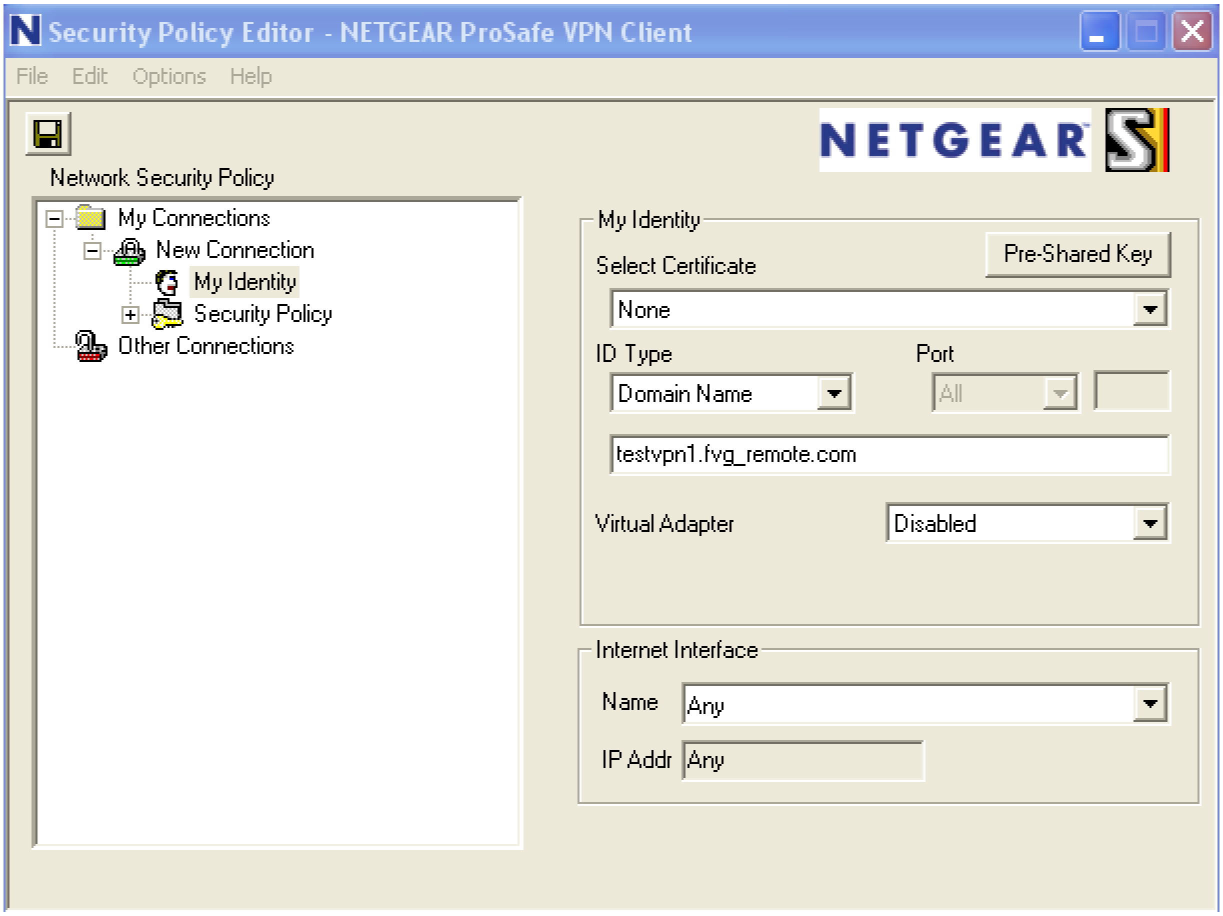
○ Use Manual Keys

□ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 2

☑ Enable Replay Detection

6. Click on My Identity on the left panel. On the right panel, select None under Select Certificate. For ID Type, select Domain Name and enter <policy name><digit>.fvg_remote.com where the policy name is the VPN policy name you entered when configure VPN Wizard on the FVG318 and digit can be any digit, it is being used to distinguish multiple VPN client user connected to the FVG318 at the same time. In our example, the domain name will be testvpn1.fvg_remote.com. Another VPN client user can use testvpn2.fvg_remote.com as domain name. For Virtual Adapter, select Disabled. Enter 0.0.0.0 for Internal Network IP Address. Select Any for Internet Interface. If you cannot find Domain Name under ID Type, you may not have select Aggressive mode under Security Policy as indicated on Step (5).



Security Policy Editor - NETGEAR ProSafe VPN Client

Select Certificate: None

ID Type: Domain Name

Port: All

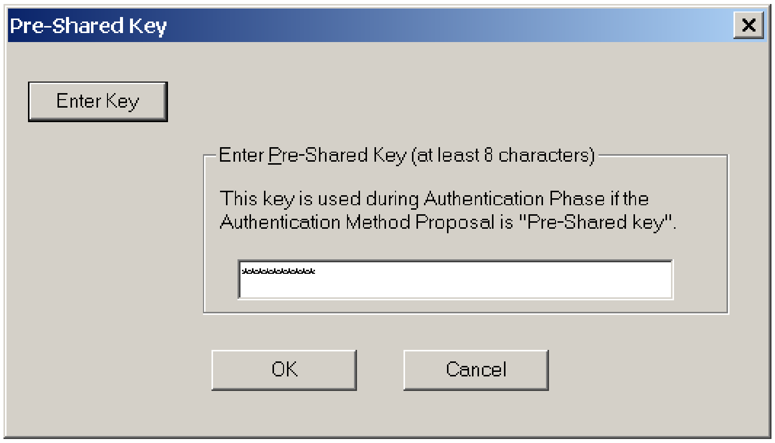
testvpn1.fvg_remote.com

Virtual Adapter: Disabled

Name: Any

IP Addr: Any

7. Click on the Pre-Shared Key button, and Click Enter Key. Enter the same pre-shared key you've entered when configure the FVG318. Click OK.

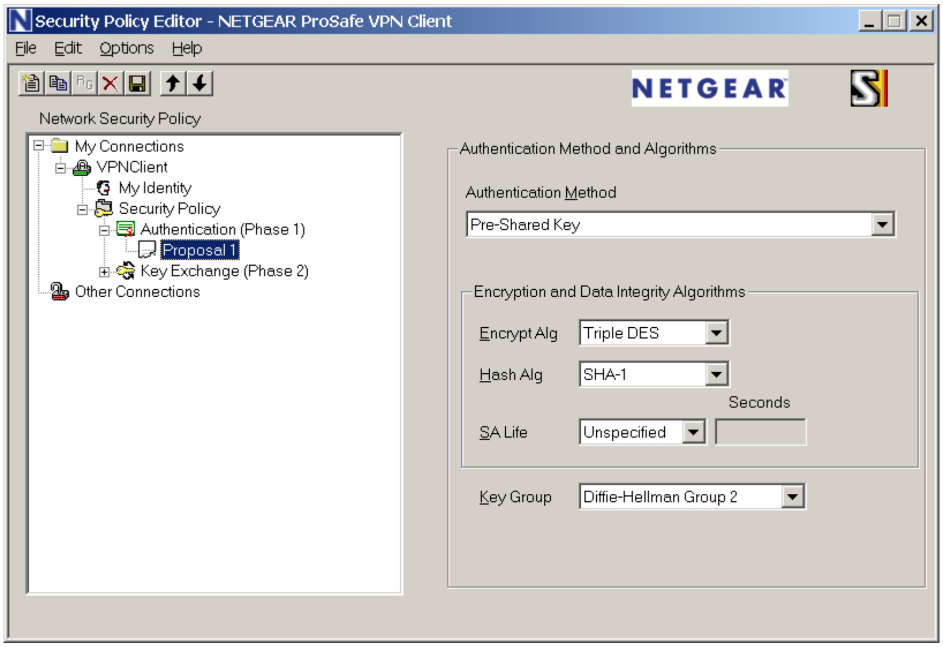


Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

****

8. On the left panel, expand Security Policy and Authentication (Phrase 1) and click on Proposal 1. On the right panel, you can keep everything as default. Make sure they match the screen below.



Authentication Method and Algorithms

Authentication Method: Pre-Shared Key

Encryption and Data Integrity Algorithms

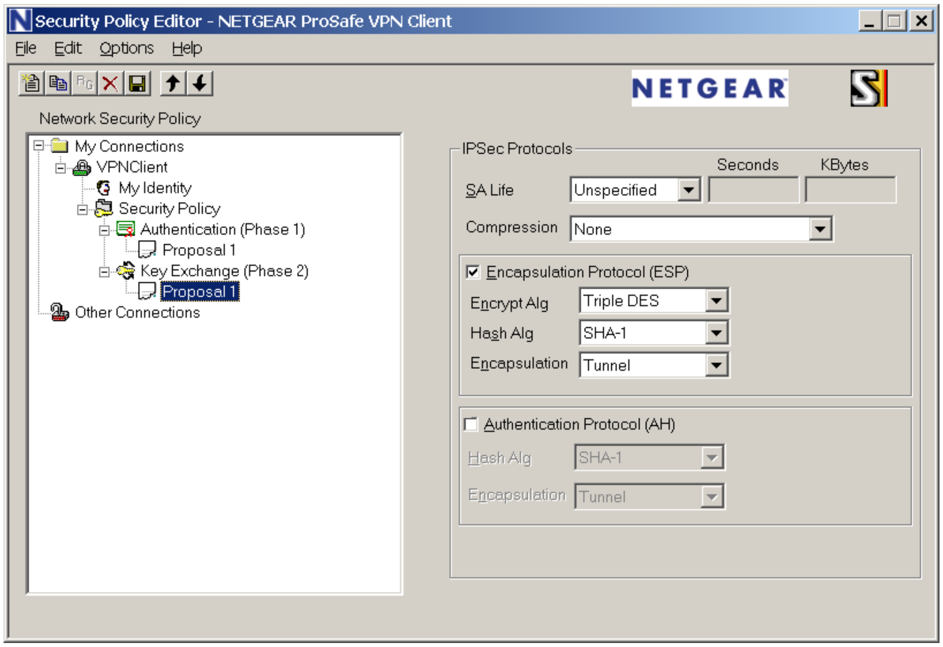
Encrypt Alg: Triple DES

Hash Alg: SHA-1

SA Life: Unspecified — Seconds:

Key Group: Diffie-Hellman Group 2

9. On the left panel, expand on Key Exchange (Phrase 2) and click on Proposal 1. On the right panel, left everything as default. Make sure they mach the screen below.



IPSec Protocols

SA Life: Unspecified — Seconds: — KBytes:

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: Triple DES

Hash Alg: SHA-1

Encapsulation: Tunnel

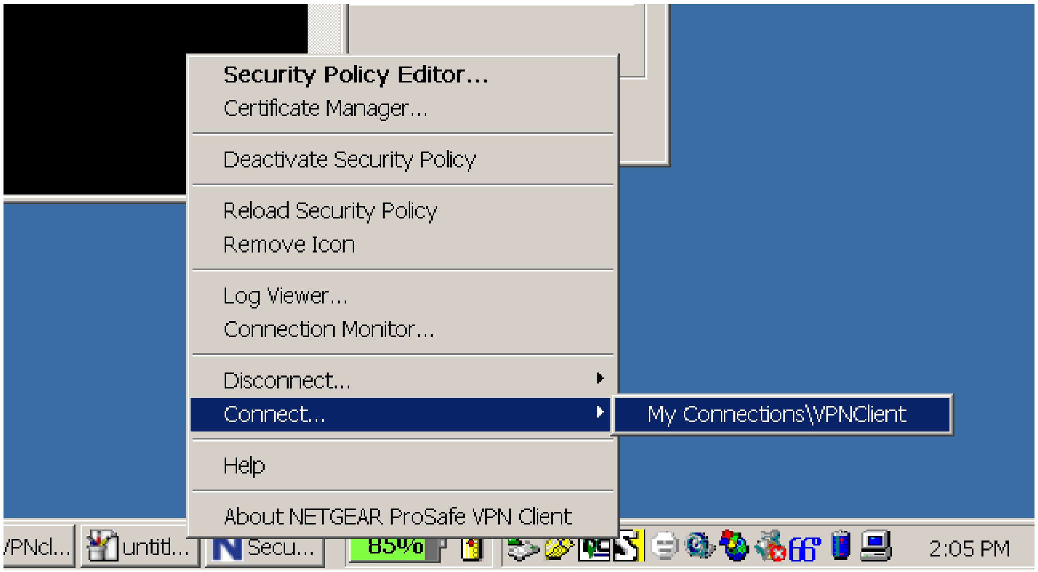
☐ Authentication Protocol (AH)

Hash Alg: SHA-1

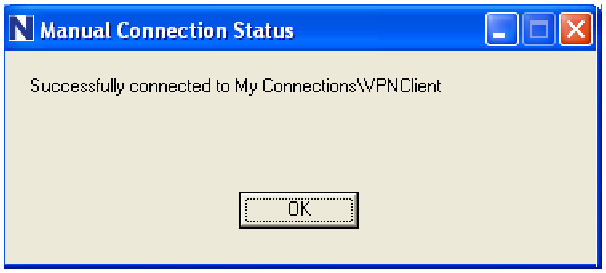
Encapsulation: Tunnel

10. Save the policy by click on the save button or choose File->Save.

11. To connect, right click on the ProSafe VPN client icon on the system tray and choose Connect, select the Connection Profile you just created.



12. A connection status window should be displayed and eventually, it should said Successfully connect to your connection profile.

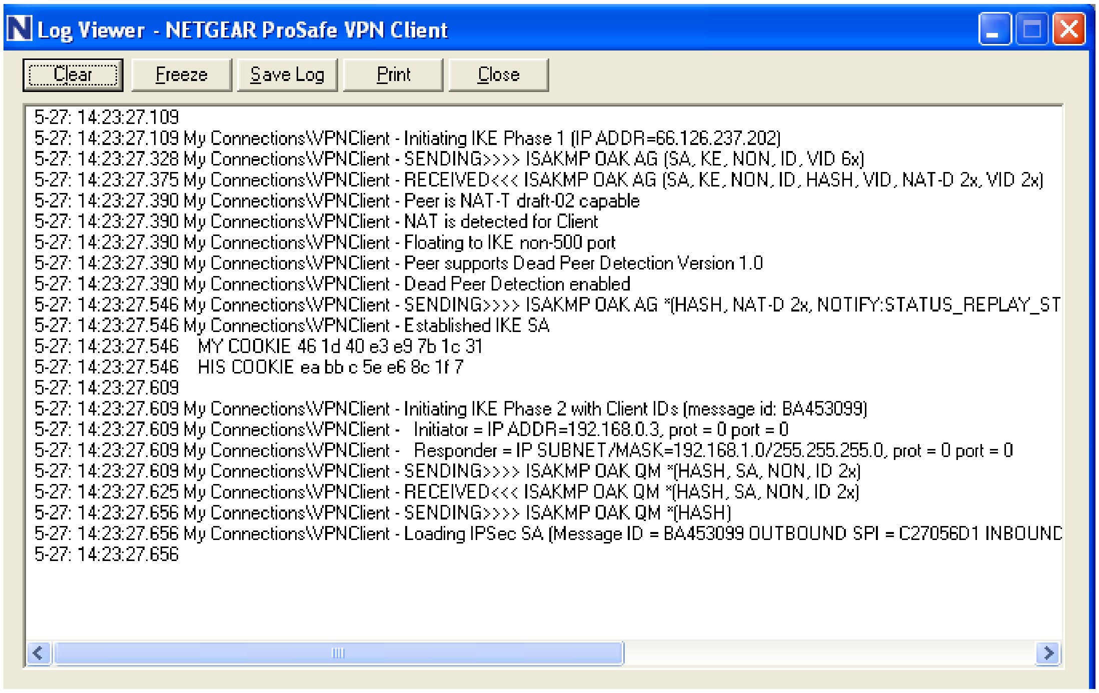


Successfully connected to My Connections\VPNClient

13. You can test the VPN by pinging resources behind the FVG318. Note that if you have not enable Response to ping on Internet port in the FVG318 WAN option menu, you won't be able to ping the LAN interface IP address of the FVG318.

14. If the VPN will not connect, double check the parameters in both the FVG318 and the VPN Client Policy, make sure they are matching on both side.

15. For more troubleshooting, you can review the VPN log on the FVG318 and the Log Viewer on the ProSafe VPN client by right click on the ProSafe VPN client icon on the system tray and select Log Viewer. A successful connection should appear as follow in the Log Viewer.



```
5-27: 14:23:27.109
5-27: 14:23:27.109 My Connections\VPNClient - Initiating IKE Phase 1 (IP ADDR=66.126.237.202)
5-27: 14:23:27.328 My Connections\VPNClient - SENDING>>>> ISAKMP OAK AG (SA, KE, NON, ID, VID 6x)
5-27: 14:23:27.375 My Connections\VPNClient - RECEIVED<<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID, NAT-D 2x, VID 2x)
5-27: 14:23:27.390 My Connections\VPNClient - Peer is NAT-T draft-02 capable
5-27: 14:23:27.390 My Connections\VPNClient - NAT is detected for Client
5-27: 14:23:27.390 My Connections\VPNClient - Floating to IKE non-500 port
5-27: 14:23:27.390 My Connections\VPNClient - Peer supports Dead Peer Detection Version 1.0
5-27: 14:23:27.390 My Connections\VPNClient - Dead Peer Detection enabled
5-27: 14:23:27.546 My Connections\VPNClient - SENDING>>>> ISAKMP OAK AG *(HASH, NAT-D 2x, NOTIFY:STATUS_REPLAY_ST
5-27: 14:23:27.546 My Connections\VPNClient - Established IKE SA
5-27: 14:23:27.546    MY COOKIE 46 1d 40 e3 e9 7b 1c 31
5-27: 14:23:27.546    HIS COOKIE ea bb c 5e e6 8c 1f 7
5-27: 14:23:27.609
5-27: 14:23:27.609 My Connections\VPNClient - Initiating IKE Phase 2 with Client IDs (message id: BA453099)
5-27: 14:23:27.609 My Connections\VPNClient -   Initiator = IP ADDR=192.168.0.3, prot = 0 port = 0
5-27: 14:23:27.609 My Connections\VPNClient -   Responder = IP SUBNET/MASK=192.168.1.0/255.255.255.0, prot = 0 port = 0
5-27: 14:23:27.609 My Connections\VPNClient - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID 2x)
5-27: 14:23:27.625 My Connections\VPNClient - RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NON, ID 2x)
5-27: 14:23:27.656 My Connections\VPNClient - SENDING>>>> ISAKMP OAK QM *(HASH)
5-27: 14:23:27.656 My Connections\VPNClient - Loading IPSec SA (Message ID = BA453099 OUTBOUND SPI = C27056D1 INBOUND
5-27: 14:23:27.656
```