NETGEAR®
Connect with Innovation™

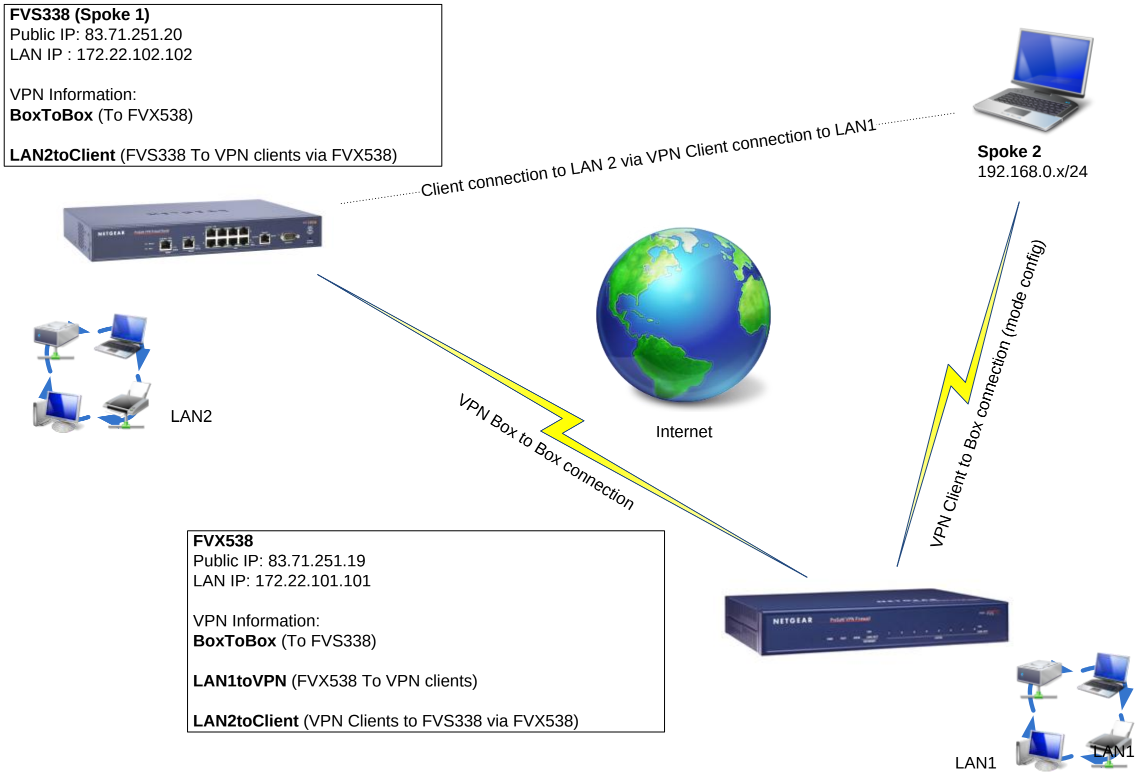
Hub and Spoke VPN using the VPN Prosafe Client

This document describes the steps to undertake in configuring a Hub-and-Spoke network over the Internet using VPNs (box-to-box and client-to-box).

In particular it describes how to allow VPN clients (**Spoke**) to access Remote LANs (**Spokes**) via a single VPN connection to a central (**Hub**) Firewall/Router.

The configuration can apply to any of the VPN Firewall/Router from firmware version 3.5.0.24 and above, and VPN clients from version 10.8.3 and above.

The diagram below shows a typical scenario.



FVS338 (Spoke 1)
Public IP: 83.71.251.20
LAN IP : 172.22.102.102

VPN Information:
BoxToBox (To FVX538)

LAN2toClient (FVS338 To VPN clients via FVX538)

FVX538
Public IP: 83.71.251.19
LAN IP: 172.22.101.101

VPN Information:
BoxToBox (To FVS338)

LAN1toVPN (FVX538 To VPN clients)

LAN2toClient (VPN Clients to FVS338 via FVX538)

Client connection to LAN 2 via VPN Client connection to LAN1
Spoke 2
192.168.0.x/24
LAN2
Internet
VPN Box to Box connection
VPN Client to Box connection (mode config)
LAN1
LAN1

Version 1.0

Table of Contents

NETWORK SETUP

Physical setup

FVX538 connected to the Internet via a modem or modem/router

FVS338 connected to the Internet via a modem or modem/router

VPN Client PCs connected Wireless/Wired to the Internet (via a LAN allowing IPSEC traffic)

Logical setup

FVX538

LAN IP: 172.22.101.101/24
DHCP: 172.22.101.0/24
Mode Config DHCP: 192.168.0.0/24
Firmware version: 3.5.0.24

FVS338

LAN IP: 172.22.102.102/24
DHCP: 172.22.102.0/24
Firmware version: 3.5.0.24

VPN Client
Version: 10.8.3
NIC IP: 192.168.0.x/24

VPN configuration

The setup will require the creation of multiple VPN policies:

FVX538

- 1x Box-to-box policy from the FVX538 to the FVS338 (Policy name: **BoxtoBox**)
- 1x Client-to-Box policy on the FVX538 to connect to the VPN clients (Policy name: **LAN1toVPN**)
- 1x Manual VPN policy using the IKE policy used for the box-to-box connection to allow the VPN clients to connect to the LAN behind the FVS338 (Policy name: **LAN2toClient**)

FVS338

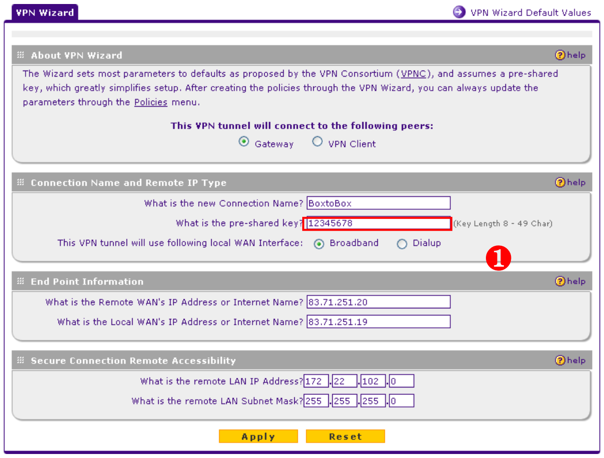
- 1x Box-to-box policy from the FVS338 to the FVX538 (Policy name: **BoxtoBox**)
- 1x Manual VPN policy using the IKE policy used for the box-to-box connection to allow the FVS338 to connect to the VPN clients (Policy name: **LAN2toClient**)

VPN Client

- 1x Policy connecting to the Public address of the FVS338 specifying as the IP range for the Remote party 172.22.0.0 mask 255.255.0.0 (class full only mask accepted)

Configuration of VPN policies on the Firewall/Routers

FVX538 VPN Config (Policy name: **BoxtoBox**)



VPN Wizard

VPN Wizard Default Values

About VPN Wizard help

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 Policies menu.

This VPN tunnel will connect to the following peers:

● Gateway ○ VPN Client

Connection Name and Remote IP Type help

What is the new Connection Name? BoxtoBox

What is the pre-shared key? 12345678 (Key Length 8 - 49 Char)

This VPN tunnel will use following local WAN Interface: ● Broadband ○ Dialup

❶

End Point Information help

What is the Remote WAN's IP Address or Internet Name? 83.71.251.20

What is the Local WAN's IP Address or Internet Name? 83.71.251.19

Secure Connection Remote Accessibility help

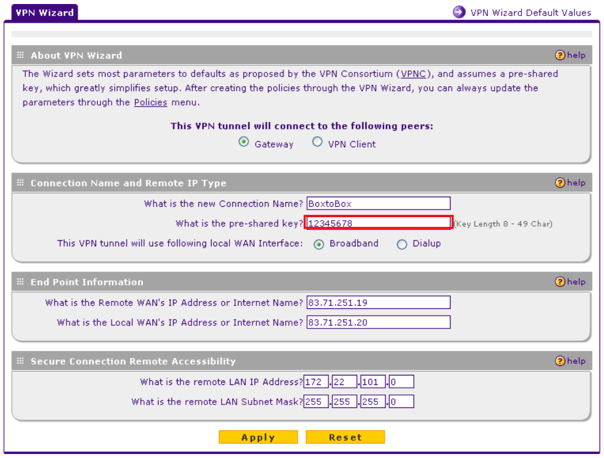
What is the remote LAN IP Address? 172 . 22 . 102 . 0

What is the remote LAN Subnet Mask? 255 . 255 . 255 . 0

Apply Reset

- Access the VPN Wizard via the VPN configuration page.
- Configure the Connection name (for admin reasons this will match the FVS338 box as **BoxtoBox**).
- ❶ Input the pre-shared key.
- Configure the Public or DNS address of the Remote location, and the LAN details (the Remote LAN IP address is intended as the subnet address).
- Click on Apply

FVS338 VPN Config (Policy name: **BoxtoBox**)



VPN Wizard

VPN Wizard Default Values

About VPN Wizard help

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 Policies menu.

This VPN tunnel will connect to the following peers:

● Gateway ○ VPN Client

Connection Name and Remote IP Type help

What is the new Connection Name? BoxtoBox

What is the pre-shared key? 12345678 (Key Length 8 - 49 Char)

This VPN tunnel will use following local WAN Interface: ● Broadband ○ Dialup

End Point Information help

What is the Remote WAN's IP Address or Internet Name? 83.71.251.19

What is the Local WAN's IP Address or Internet Name? 83.71.251.20

Secure Connection Remote Accessibility help

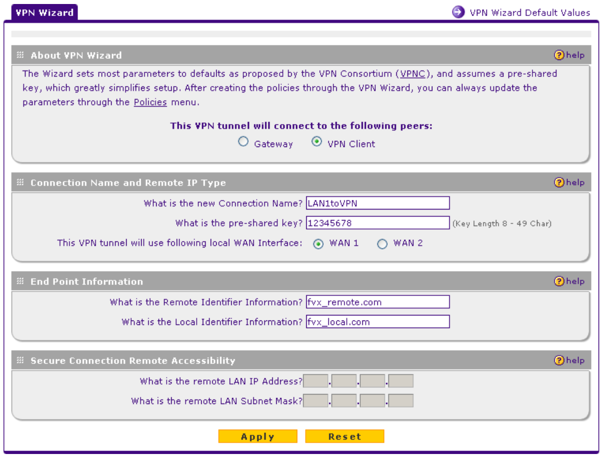
What is the remote LAN IP Address? 172 . 22 . 101 . 0

What is the remote LAN Subnet Mask? 255 . 255 . 255 . 0

Apply Reset

- Access the VPN Wizard via the VPN configuration page.
- Configure the Connection name (for admin reasons this will match the other box as **BoxtoBox**).
- Input the pre-shared key as at point ❶
- Configure the Public or DNS address of the Remote location, and the LAN details (the Remote LAN IP address is intended as the subnet address).
- Click on Apply

FVX538 VPN Config (Policy name: **LAN1toVPN**)



About 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 Policies menu.

This VPN tunnel will connect to the following peers:

○ Gateway ● VPN Client

Connection Name and Remote IP Type

What is the new Connection Name? LAN1toVPN

What is the pre-shared key? 12345678 (Key Length 8 - 49 Char)

This VPN tunnel will use following local WAN Interface: ● WAN 1 ○ WAN 2

End Point Information

What is the Remote Identifier Information? fvx_remote.com

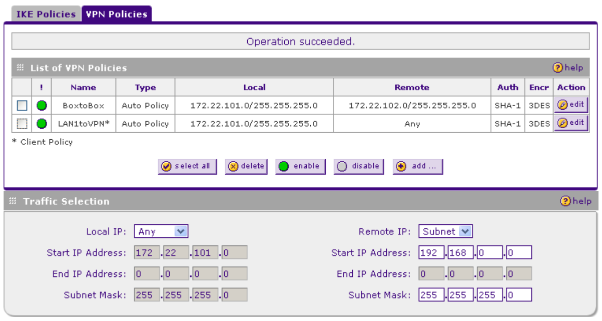
What is the Local Identifier Information? fvx_local.com

Secure Connection Remote Accessibility

What is the remote LAN IP Address? . . .

What is the remote LAN Subnet Mask? . . .

- Access the VPN Wizard via the VPN configuration page.
- Create a new VPN client policy named **LAN1toVPN** (with any pre-shared key)
- Take note of the Remote and Local identifier whether using the default ones or new ones.
- Click on Apply



Operation succeeded.

List of VPN Policies

	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	BoxtoBox	Auto Policy	172.22.101.0/255.255.255.0	172.22.102.0/255.255.255.0	SHA-1	3DES	edit
□	●	LAN1toVPN*	Auto Policy	172.22.101.0/255.255.255.0	Any	SHA-1	3DES	edit

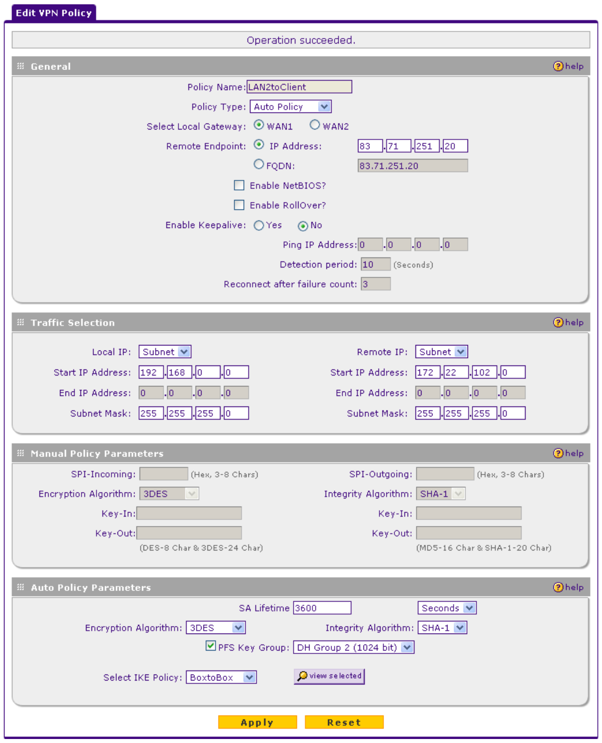
* Client Policy

Traffic Selection

Local IP:	Any	Remote IP:	Subnet
Start IP Address:	172.22.101.0	Start IP Address:	192.168.0.0
End IP Address:	0.0.0.0	End IP Address:	0.0.0.0
Subnet Mask:	255.255.255.0	Subnet Mask:	255.255.255.0

- Edit the **LAN1toVPN**.
- Change the Local IP setting to **any** and the Remote IP to **subnet**, modifying the Start IP address to **192.168.0.0** with subnet mask **255.255.255.0**
- Click on Apply

FVX538 VPN Config (Policy name: **LAN2Client**)



Operation succeeded.

General

Policy Name: LAN2toClient
Policy Type: Auto Policy
Select Local Gateway: ● WAN1 ○ WAN2
Remote Endpoint: ● IP Address: 83.71.251.20
○ FQDN: 83.71.251.20
□ Enable NetBIOS?
□ Enable RollOver?
Enable Keepalive: ○ Yes ● No
Ping IP Address: 0.0.0.0
Detection period: 10 (Seconds)
Reconnect after failure count: 3

Traffic Selection

Local IP: Subnet | Remote IP: Subnet
Start IP Address: 192.168.0.0 | Start IP Address: 172.22.102.0
End IP Address: 0.0.0.0 | End IP Address: 0.0.0.0
Subnet Mask: 255.255.255.0 | Subnet Mask: 255.255.255.0

Manual Policy Parameters

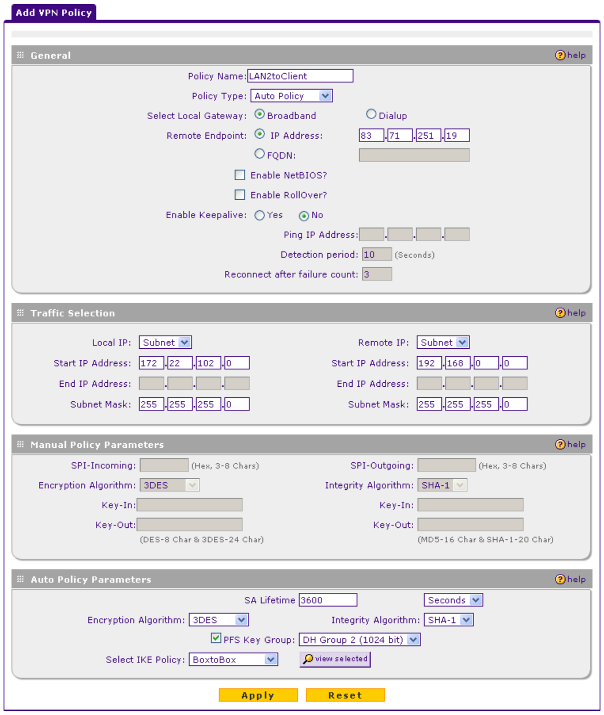
SPI-Incoming: (Hex, 3-8 Chars) | SPI-Outgoing: (Hex, 3-8 Chars)
Encryption Algorithm: 3DES | Integrity Algorithm: SHA-1
Key-In: | Key-In:
Key-Out: | Key-Out:
(DES-8 Char & 3DES-24 Char) | (MD5-16 Char & SHA-1-20 Char)

Auto Policy Parameters

SA Lifetime 3600 Seconds
Encryption Algorithm: 3DES | Integrity Algorithm: SHA-1
☑ PFS Key Group: DH Group 2 (1024 bit)
Select IKE Policy: BoxtoBox

- Access the VPN Wizard via the VPN configuration page.
- In the VPN Policy section click on Add (this will create a new manual VPN policy which will use an existing IKE policy)
- Create a new VPN client policy named **LAN2toClient**
- Specify the Remote Endpoint IP address to be the Public address of the FVS338
- Specify the Local IP subnet to be the one of the VPN clients as **192.168.0.0/24** and the Remote IP subnet to be the LAN of the FVS338 as **172.22.102.0/24**
- Ensure that the Select IKE Policy is set to **BoxtoBox**
- Click on Apply

FVS338 VPN Config (Policy name: **LAN2Client**)



General

Policy Name: LAN2toClient
Policy Type: Auto Policy
Select Local Gateway: ● Broadband ○ Dialup
Remote Endpoint: ● IP Address: 83.71.251.19
○ FQDN:
□ Enable NetBIOS?
□ Enable RollOver?
Enable Keepalive: ○ Yes ● No
Ping IP Address: . . .
Detection period: 10 (Seconds)
Reconnect after failure count: 3

Traffic Selection

Local IP: Subnet | Remote IP: Subnet
Start IP Address: 172.22.102.0 | Start IP Address: 192.168.0.0
End IP Address: . . . | End IP Address: . . .
Subnet Mask: 255.255.255.0 | Subnet Mask: 255.255.255.0

Manual Policy Parameters

SPI-Incoming: (Hex, 3-8 Chars) | SPI-Outgoing: (Hex, 3-8 Chars)
Encryption Algorithm: 3DES | Integrity Algorithm: SHA-1
Key-In: | Key-In:
Key-Out: | Key-Out:
(DES-8 Char & 3DES-24 Char) | (MD5-16 Char & SHA-1-20 Char)

Auto Policy Parameters

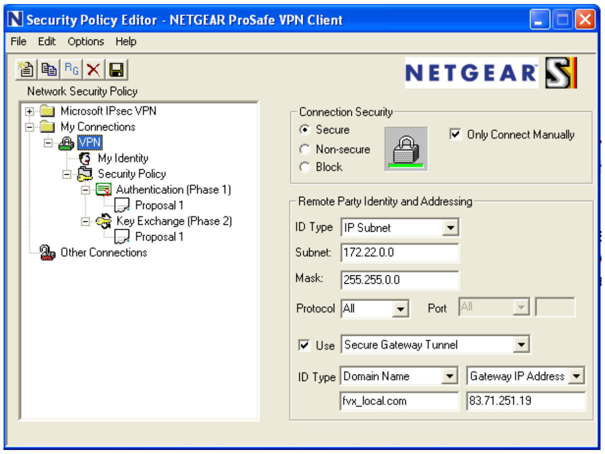
SA Lifetime 3600 Seconds
Encryption Algorithm: 3DES | Integrity Algorithm: SHA-1
☑ PFS Key Group: DH Group 2 (1024 bit)
Select IKE Policy: BoxtoBox

- Access the VPN Wizard via the VPN configuration page.
- In the VPN Policy section click on Add (this will create a new manual VPN policy which will use an existing IKE policy)
- Create a new VPN client policy named **LAN2toClient**
- Specify the Remote Endpoint IP address to be the Public address of the FVX538
- Specify the Local IP subnet to be the one of the FVS338 **172.22.102.0/24** and the Remote IP subnet to be the VPN clients one 192.168.0.0/24
- Ensure that the Select IKE Policy is set to **BoxtoBox**
- Click on Apply

VPN client configuration

This configuration requires advanced IP address planning. The VPN client policy needs to be able to address both Local Area Network #1 and Local Area Network #2 in the same client policy profile, therefore, the two networks must be presentable as one subnet or one address range.

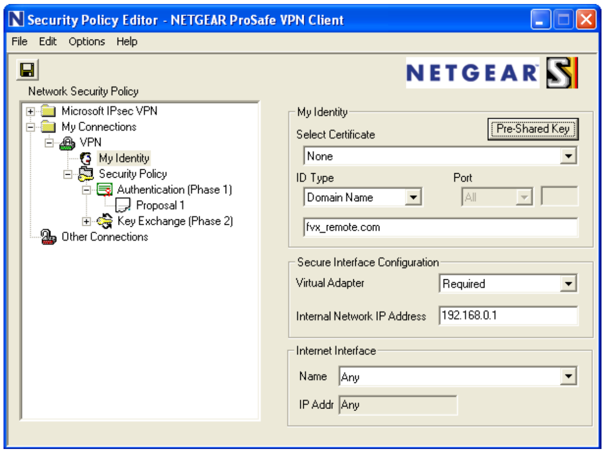
This has been considered in our scenario.



Connection Security
● Secure
○ Non-secure
○ Block
☑ Only Connect Manually

Remote Party Identity and Addressing
ID Type: IP Subnet
Subnet: 172.22.0.0
Mask: 255.255.0.0
Protocol: All Port: All
☑ Use: Secure Gateway Tunnel
ID Type: Domain Name — Gateway IP Address
fvx_local.com — 83.71.251.19

- Create a new VPN client policy
- Specify the Remote Party ID type as **IP Subnet** and the subnet and mask as **172.22.0.0 255.255.255.0** (this will address both LAN1 and LAN2)
- The gateway IP address will be specified at the WAN address of the FVX538 in our case

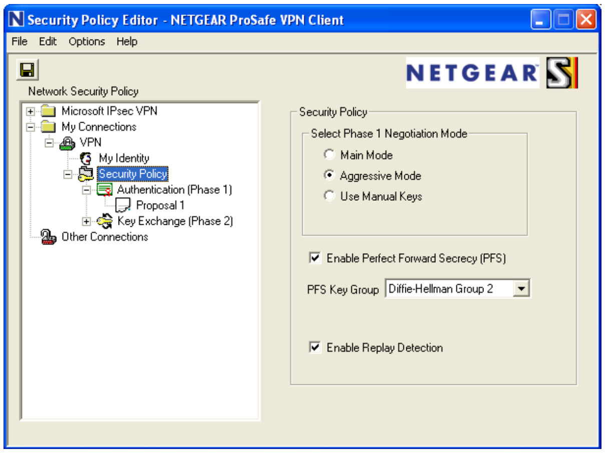


My Identity
Select Certificate: None
ID Type: Domain Name Port: All
fvx_remote.com

Secure Interface Configuration
Virtual Adapter: Required
Internal Network IP Address: 192.168.0.1

Internet Interface
Name: Any
IP Addr: Any

- In My identity change the pre-shared key to match the VPN policy **LAN1toVPN** created on the FVX538 (**12345678**)
- Set the Virtual adapter as Required as specify a unique value for the Internal network IP address (this will be different on each PC running the VPN client

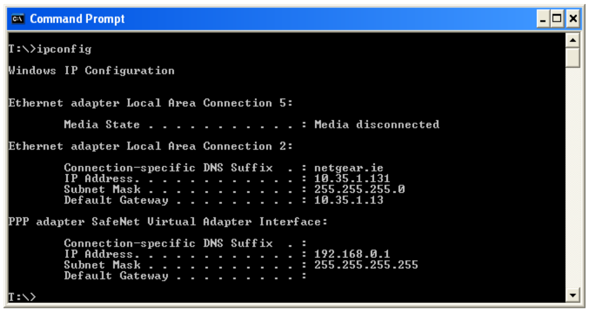


Security Policy
Select Phase 1 Negotiation Mode
○ Main Mode
● Aggressive Mode
○ Use Manual Keys
☑ Enable Perfect Forward Secrecy (PFS)
PFS Key Group: Diffie-Hellman Group 2
☑ Enable Replay Detection

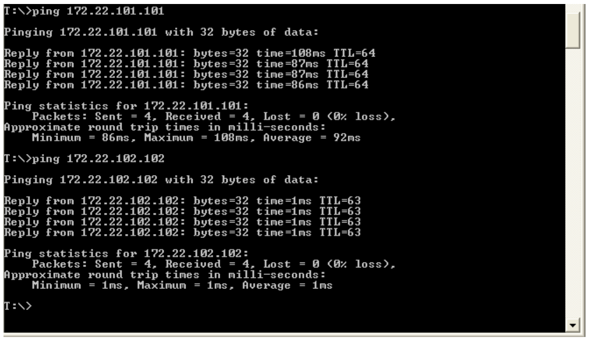
- In the Security policy section ensure the Phase 1 negotiation mode is set to aggressive , PFS is enabled and Enable Replay Detection is ticked

Testing the connection

VPN Client



```
T:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 5:

        Media State . . . . . . . . . . . : Media disconnected

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : netgear.ie
        IP Address. . . . . . . . . . . . : 10.35.1.131
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.35.1.13

PPP adapter SafeNet Virtual Adapter Interface:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . :

T:\>
```

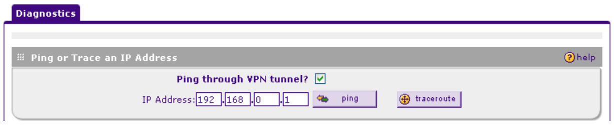


```
T:\>ping 172.22.101.101

Pinging 172.22.101.101 with 32 bytes of data:

Reply from 172.22.101.101: bytes=32 time=108ms TTL=64
Reply from 172.22.101.101: bytes=32 time=87ms TTL=64
Reply from 172.22.101.101: bytes=32 time=87ms TTL=64
Reply from 172.22.101.101: bytes=32 time=86ms TTL=64

Ping statistics for 172.22.101.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 86ms, Maximum = 108ms, Average = 92ms

T:\>ping 172.22.102.102

Pinging 172.22.102.102 with 32 bytes of data:

Reply from 172.22.102.102: bytes=32 time=1ms TTL=63
Reply from 172.22.102.102: bytes=32 time=1ms TTL=63
Reply from 172.22.102.102: bytes=32 time=1ms TTL=63
Reply from 172.22.102.102: bytes=32 time=1ms TTL=63

Ping statistics for 172.22.102.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

T:\>
```

- From the VPN client run **ipconfig** to confirm once the VPN is established that the Virtual adapter interface is assigned with the IP address specified in the policy (in this case **192.168.0.1**)

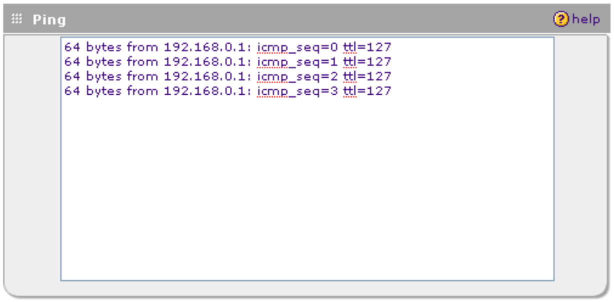
- Test the VPN connection to both the FVX538 and FVS338 by pinging each box LAN IP address

FVS338



Ping through VPN tunnel? ☑

IP Address: 192 . 168 . 0 . 1



```
64 bytes from 192.168.0.1: icmp_seq=0 ttl=127
64 bytes from 192.168.0.1: icmp_seq=1 ttl=127
64 bytes from 192.168.0.1: icmp_seq=2 ttl=127
64 bytes from 192.168.0.1: icmp_seq=3 ttl=127
```

- From Monitoring, Diagnostic on the FVS338 ping the VPN client IP address **1902.168.0.1**