

VPN Configuration of NETGEAR FVS318 or FVM318

This is a case study on how to configure a secure IPSec VPN tunnel on a NETGEAR FVS318 or FVM318. This case study follows the VPN Consortium interoperability profile guidelines (found at <http://www.vpnc.org/InteropProfiles/Interop-01.html>). The configuration options and screens for the FVS318 and FVM318 are the same.

Configuration Template

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Check that there are no firewall restrictions.

Table 1. Profile Summary

VPN Consortium Scenario:	Scenario 1
Type of VPN	LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway)
Security Scheme:	IKE with Preshared Secret/Key (not Certificate-based)
Date Tested:	April 2003
Model/Firmware Tested:	
Gateway A	FVS318 firmware version A1.4 or FVM318 firmware version 1.1
Gateway B	In this example, a NETGEAR FVL328 using firmware v1.4
IP Addressing:	
Gateway A	Static IP address
Gateway B	Static IP address

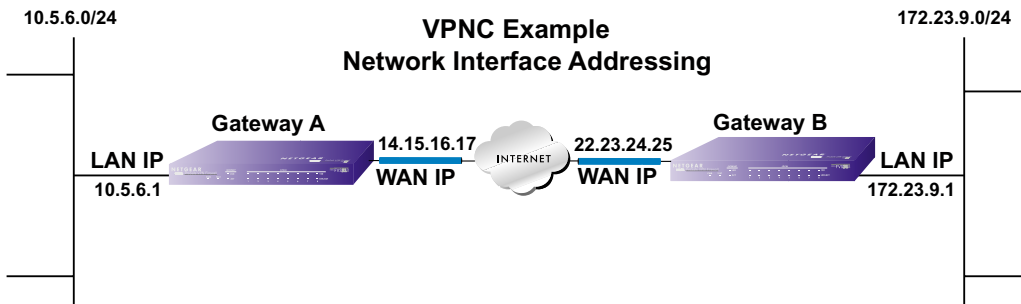


Figure 1: Addressing and Subnets Used for Examples



Note: Product updates are available on the NETGEAR, Inc. web site at <http://www.netgear.com/support/main.asp>. Documentation updates are available on the NETGEAR, Inc. web site at <http://www.netgear.com/docs>.

Step-By-Step Configuration of FVS318 or FVM318 Gateway A

1. Log in to the FVS318 or FVM318 labeled Gateway A as in the illustration.

Out of the box, the FVS318 or FVM318 is set for its default LAN address of <http://192.168.0.1> with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.

2. Click on the VPN Settings link on the left side of the main menu.
 - *For the FVS318:* Click the radio button of first available VPN tunnel. Click the Edit button below. This will take you to the VPN Settings – Main Mode Menu.
 - *For the FVM318:* Click Add. This will take you to the VPN Settings – Main Mode Menu.

VPN Settings - Main Mode

Connection Name	<input type="text" value="toFVL328"/>
Local IPSec Identifier	<input type="text" value="14.15.16.17"/>
Remote IPSec Identifier	<input type="text" value="22.23.24.25"/>
Tunnel can be accessed from	<input style="background-color: #e6f2ff; border: 1px solid #00aeeef;" type="button" value="a subnet of local address"/>
Local LAN start IP Address	<input type="text" value="10"/> <input type="text" value="5"/> <input type="text" value="6"/> <input type="text" value="0"/>
Local LAN finish IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Local LAN IP Subnetmask	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/>
Tunnel can access	<input style="background-color: #e6f2ff; border: 1px solid #00aeeef;" type="button" value="a subnet of remote address"/>
Remote LAN start IP Address	<input type="text" value="172"/> <input type="text" value="23"/> <input type="text" value="9"/> <input type="text" value="0"/>
Remote LAN finish IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Remote LAN IP Subnetmask	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/>
Remote WAN IP or FQDN	<input type="text" value="22.23.24.25"/>
Secure Association	<input style="background-color: #e6f2ff; border: 1px solid #00aeeef;" type="button" value="Main Mode"/>

Figure 2: NETGEAR FVS318 vA1.4 VPN Settings (part 1) – Main Mode

- In the Connection Name box, enter in a unique name for the VPN tunnel to be configured between the NETGEAR devices. For this example we have used **toFVL328**.
- Enter a Local IPSec Identifier name for the NETGEAR FVS318 Gateway A. This name must be entered in the other endpoint as Remote IPSec Identifier. In this example we used **14.15.16.17** as the local identifier.
- Enter a Remote IPSec Identifier name for the remote NETGEAR FVL328 Gateway B. This name must be entered in the other endpoint as Local IPSec Identifier. In this example we used **22.23.24.25** as the remote identifier.
- Choose “a subnet from local addresses” from the “Tunnel can be accessed from” pull-down menu.
- Type the starting LAN IP Address of Gateway A (**10.5.6.1** in our example) in the Local IP Local LAN start IP Address field.
- Type the LAN Subnet Mask of Gateway A (**255.255.255.0** in our example) in the Local LAN IP Subnetmask field.
- Choose “a subnet of remote addresses” from the “Tunnel can access” pull-down menu.
- Type the starting LAN IP Address of Gateway B (**172.23.9.1** in our example) in the Local IP Remote LAN Start IP Address field.

-
- Type the LAN Subnet Mask of Gateway B (**255.255.255.0** in our example) in the Remote LAN IP Subnetmask field.
 - Type the WAN IP address (**22.23.24.25** in our example) of Gateway B in the Remote WAN IP or FQDN field.

The screenshot shows the 'Secure Association' configuration window for the NETGEAR FVS318 vA1.4 VPN. The window has a title bar and a blue border. It contains the following fields and controls:

- Secure Association:** A drop-down menu set to 'Main Mode'.
- Perfect Forward Secrecy:** Two radio buttons, with 'Enabled' selected.
- Encryption Protocol:** A drop-down menu set to '3DES'.
- PreShared Key:** A text input field containing 'hr5xb8416aa9r6'.
- Key Life:** A text input field containing '3600' with a 'Seconds' label to its right.
- IKE Life Time:** A text input field containing '28800' with a 'Seconds' label to its right.
- NETBIOS Enable:** A checked checkbox.
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom.

Figure 3: NETGEAR FVS318 vA1.4 VPN Settings (part 2) – Main Mode

- From the Secure Association drop-down box, select Main Mode.
 - Next to Perfect Forward Secrecy, select the Enabled radio button.
 - From the Encryption Protocol drop-down box, select 3DES.
 - In the PreShared Key box, type a unique text string to be used as the shared key between Gateway A and Gateway B. In this example we used **hr5xb8416aa9r6**. You must make sure the key is the same for both gateways.
 - In the Key Life box, enter **3600** seconds.
 - In the IKE Life Time, enter **28800** seconds.
 - Check the NETBIOS Enable box if you wish to pass NetBIOS traffic over the VPN tunnel, allowing functions such as Microsoft Network Neighborhood browsing.
3. Click Apply to save all changes. This will return you to the VPN Settings screen.
 4. When the screen returns to the VPN Settings, make sure the Enable checkbox is selected.

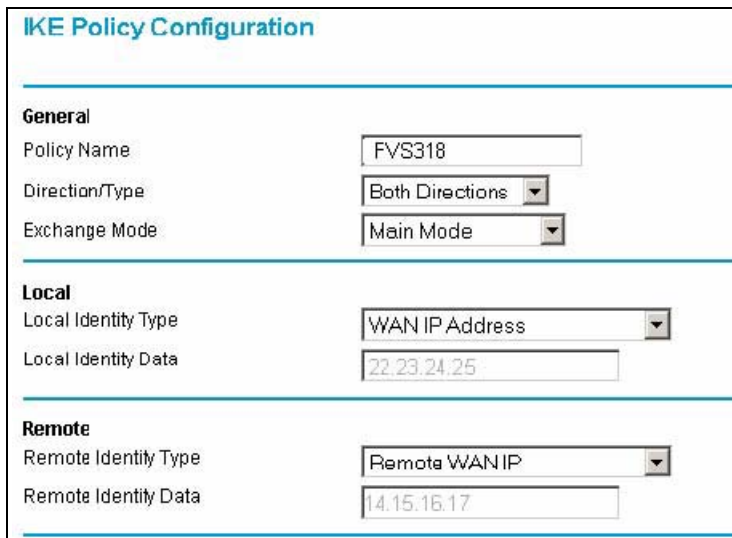
Step-By-Step Configuration of Gateway B

In this example, we are using a NETGEAR FVL328 Broadband ProSafe High-Speed VPN Firewall for gateway B.

1. Log in to the NETGEAR FVL328 labeled Gateway B as in the illustration.

Out of the box, the FVL328 is set for its default LAN address of <http://192.168.0.1> with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 172.23.9.1 for Gateway B and have set your own user name and password.

2. Click on the IKE Policies link under the VPN category link on the left side of the main menu. This will open the IKE Policies Menu. Click Add. This will open a new screen titled IKE Policy Configuration.



IKE Policy Configuration	
General	
Policy Name	<input type="text" value="FVS318"/>
Direction/Type	<input type="text" value="Both Directions"/>
Exchange Mode	<input type="text" value="Main Mode"/>
Local	
Local Identity Type	<input type="text" value="WAN IP Address"/>
Local Identity Data	<input type="text" value="22.23.24.25"/>
Remote	
Remote Identity Type	<input type="text" value="Remote WAN IP"/>
Remote Identity Data	<input type="text" value="14.15.16.17"/>

Figure 4: NETGEAR FVL328 v1.4 IKE Policy Configuration – Part 1

- Enter an appropriate name for the policy in the Policy Name field. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the IKE policies. In our example we have used FVS318 as the Policy Name. In the Policy Name field type **FVS318**.
- From the Direction/Type drop-down box, select Both Directions

- From the Exchange Mode drop-down box, select Main Mode.
- From the Local Identity drop-down box, select WAN IP Address (WAN IP address will automatically be populated into the Local Identity Data field after policy is applied).
- From the Remote Identity drop-down box, select Remote WAN IP (WAN IP address will automatically be populated into the Local Identity Data field after policy is applied).

Figure 5: NETGEAR FVL328 v1.4 IKE Policy Configuration – Part 2

- From the Encryption Algorithm drop-down box, select 3DES.
 - From the Authentication Algorithm drop-down box, select MD5.
 - From the Authentication Method radio button, select Pre-shared Key.
 - In the Pre-Shared Key field, type **hr5xb8416aa9r6**. You must make sure the key is the same for both gateways.
 - From the Diffie-Hellman (DH) Group drop-down box, select Group 1 (768 Bit).
 - In the SA Life Time field, type **28800**.
3. Click the Apply Button. This will bring you back to the IKE Policies Menu.

IKE Policies								
Policy Table								
	#	Name	Mode	Local ID	Remote ID	Encr	Auth	DH
<input checked="" type="radio"/>	1	FVS318	Main	22.23.24.25	14.15.16.17	3DES	MD5	Group 1 (768 Bit)

Figure 6: NETGEAR FVL328 v1.4 IKE Policies (Post Configuration)

The FVS318 IKE Policy is now displayed in the IKE Policies page.

4. Click on the VPN Policies link under the VPN category link on the left side of the main menu. This will take you to the VPN Policies Menu page. Click Add Auto Policy. This will open a new screen titled VPN – Auto Policy.

VPN - Auto Policy

General

Policy Name:

IKE policy:

Remote VPN Endpoint Address Type:

Address Data:

SA Life Time: (Seconds)

(Kbytes)

IPsec PFS PFS Key Group:

Traffic Selector

Local IP:

Start IP address: . . .

Finish IP address: . . .

Subnet Mask: . . .

Figure 7: NETGEAR FVL328 VPN v1.4 – Auto Policy (part 1)

- Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. In our example we have used “to318” as the Policy Name. In the Policy Name field type **to318**.
- From the IKE policy drop-down box, select the IKE Policy that was set up in the earlier step – this being the FVS318 IKE Policy.
- From the Remote VPN Endpoint Address Type drop-down box, select IP Address.
- Type the WAN IP Address of Gateway A (**14.15.16.17** in our example) in the **Remote VPN Endpoint Address Data** field.
- Type **300** in the SA Life Time (Seconds) field.
- Type **0** in the SA Life Time (Kbytes) field.
- Check the IPsec PFS checkbox to enable Perfect Forward Secrecy.
- From the PFS Key Group drop-down box, select Group 2 (1024 Bit).
- From the Traffic Selector Local IP drop-down box, select “Subnet address”.
- Type the starting LAN IP Address of Gateway B (**172.23.9.1** in our example) in the Local IP Start IP Address field.

-
- Type the LAN Subnet Mask of Gateway B (**255.255.255.0** in our example) in the Local IP Subnet Mask field.

The screenshot shows a configuration window for a VPN policy. At the top, under 'Remote IP', there is a dropdown menu set to 'Subnet address'. Below it are four input fields: 'Start IP address' (10.5.6.1), 'Finish IP address' (0.0.0.0), and 'Subnet Mask' (255.255.255.0). The 'AH Configuration' section has an unchecked 'Enable Authentication' checkbox and an 'Authentication Algorithm' dropdown set to 'MD5'. The 'ESP Configuration' section has three checked checkboxes: 'Enable Encryption', 'Enable Authentication', and 'NETBIOS Enable'. The 'Encryption Algorithm' dropdown is set to '3DES' and the 'Authentication Algorithm' dropdown is set to 'MD5'. At the bottom are 'Back', 'Apply', and 'Cancel' buttons.

Figure 8: NETGEAR FVL328 VPN v1.4 – Auto Policy (part 2)

- From the Traffic Selector Remote IP drop-down box, select Subnet address.
 - Type the starting LAN IP Address of Gateway A (**10.5.6.1** in our example) in the Remote IP Start IP Address field.
 - Type the LAN Subnet Mask of Gateway A (**255.255.255.0** in our example) in the Remote IP Subnet Mask field.
 - Select Enable Encryption in the ESP Configuration Enable Encryption checkbox.
 - From the ESP Configuration Encryption Algorithm drop-down box, select 3DES.
 - Select Enable Authentication in the ESP Configuration Enable Authentication checkbox.
 - From the ESP Configuration Authentication Algorithm drop-down box, select MD5.
 - Select NETBIOS Enable in the NETBIOS Enable checkbox to enable networking features such as Windows Network Neighborhood.
5. Click Apply. You will be taken back to the VPN Policies Menu page.
 6. When the screen returns to the VPN Policies, make sure the Enable checkbox is selected. Click the Apply button.

Test the VPN Connection

1. From a PC behind the NETGEAR FVS318 or FVM318 gateway A attempt to ping the remote FVL328 gateway B LAN Interface address (example address 172.23.9.1).
Note: You can run ping tests from the Diagnostics link of the NETGEAR main menu or from a DOS prompt on a PC.
2. From a PC behind the FVL328 gateway B attempt to ping the remote NETGEAR FVS318 or FVM318 gateway A LAN Interface address (example address 10.5.6.1).
3. On either NETGEAR router, click the Router Status link on the left side of the main menu. Click the Show VPN Status button below. This will take you to the IPSec Connection Status Screen. If the connection is functioning properly, the State fields will show “Estab.”
4. On either NETGEAR router, click the Router Status link on the left side of the main menu. Click the Show VPN Logs button below. The log file for the FVS318 or the FVM318 should be similar to the example below.

```
13:19:02 - FVS318 IPsec:sizeof(connection)=1724 sizeof(state)=10048 sizeof(SA)=732
13:19:42 - FVS318 IPsec:call ipsecdoi_initiate
13:19:42 - FVS318 IPsec:New State index:0, sno:1
13:19:42 - FVS318 IPsec:Initiating Main Mode
13:19:42 - FVS318 IPsec:main_out1() policy=65
13:19:42 - FVS318 IKE:[toFVL328] Initializing IKE Main Mode
13:19:42 - FVS318 IKE:[toFVL328] TX >> MM_I1: 22.23.24.25
13:19:42 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10 seconds for #1
13:19:42 - FVS318 IPsec:Receive Packet address:0x1806f14 from 22.23.24.25
13:19:42 - FVS318 IPsec:main_inR1_out2()
13:19:42 - FVS318 IKE:[toFVL328] RX << MM_R1: 22.23.24.25
13:19:42 - FVS318 IPsec:Oakley Transform 1 accepted
13:19:42 - FVS318 IKE:OAKLEY_PRESHARED_KEY/OAKLEY_3DES_CBC/MODP1536
13:19:42 - FVS318 IKE:[toFVL328] TX >> MM_I2: 22.23.24.25
13:19:42 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10 seconds for #1
13:19:44 - FVS318 IPsec:Receive Packet address:0x1806f14 from 22.23.24.25
13:19:44 - FVS318 IPsec:main_inR2_out3()
13:19:44 - FVS318 IKE:[toFVL328] RX << MM_R2: 22.23.24.25
13:19:44 - FVS318 IKE:[toFVL328] TX >> MM_I3: 22.23.24.25
13:19:44 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10 seconds for #1
13:19:46 - FVS318 IPsec:Receive Packet address:0x1806f14 from 22.23.24.25
13:19:46 - FVS318 IPsec:main_inR3()
13:19:46 - FVS318 IKE:[toFVL328] RX << MM_R3: 22.23.24.25
13:19:46 - FVS318 IPsec:Decoded Peer's ID is ID_IPV4_ADDR:22.23.24.25and 22.23.24.25in st
13:19:46 - FVS318 IPsec:inserting event EVENT_SA_REPLACE, timeout in 28740 seconds for #1
13:19:46 - FVS318 IPsec:STATE_MAIN_I4: ISAKMP SA established
13:19:46 - FVS318 IPsec:New State index:1, sno:2
13:19:46 - FVS318 IPsec:quick_out1()
13:19:46 - FVS318 IPsec:New Message ID generated:570001
13:19:46 - FVS318 IPsec:initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS
13:19:46 - FVS318 IKE:[toFVL328] TX >> QM_I1: 211.26.0.186
13:19:46 - FVS318 IPsec:in get_ipsec_spi() spi=cf01ea7d
13:19:46 - FVS318 IPsec:My generated SPI=cf01ea7d
13:19:46 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10 seconds for #2
13:19:48 - FVS318 IPsec:Receive Packet address:0x1806f14 from 22.23.24.25
13:19:48 - FVS318 IPsec:loglog[3] ignoring informational payload, type IPSEC_RESPONDER_LIFETIME
13:19:48 - FVS318 IPsec:quick_inR1_out2()
13:19:48 - FVS318 IKE:[toFVL328] RX << QM_R1: 22.23.24.25
13:19:48 - FVS318 IKE:[ESP_3DES/AUTH_ALGORITHM_HMAC_SHA1/In SPI:cf01ea7d,Out SPI:e51e148d]
13:19:48 - FVS318 IPsec:****Install OUTBOUND SA:
13:19:48 - FVS318 IPsec: ESP(3DES-CBC SHA-1)
13:19:48 - FVS318 IPsec:****Install INBOUND SA:
13:19:48 - FVS318 IPsec: ESP(3DES-CBC SHA-1)
13:19:48 - FVS318 IKE:[toFVL328] TX >> QM_I2: 22.23.24.25
13:19:48 - FVS318 IKE:[toFVL328] established with 22.23.24.25 successfully
13:19:48 - FVS318 IPsec:inserting event EVENT_SA_REPLACE, timeout in 3540 seconds for #2
13:19:48 - FVS318 IPsec:STATE_QUICK_I2: sent QI2, IPsec SA established
```

End of Log -----