

VPN Consortium Scenario 1: Gateway-to-Gateway with Preshared Secrets

The following is a typical gateway-to-gateway VPN that uses a preshared secret for authentication.

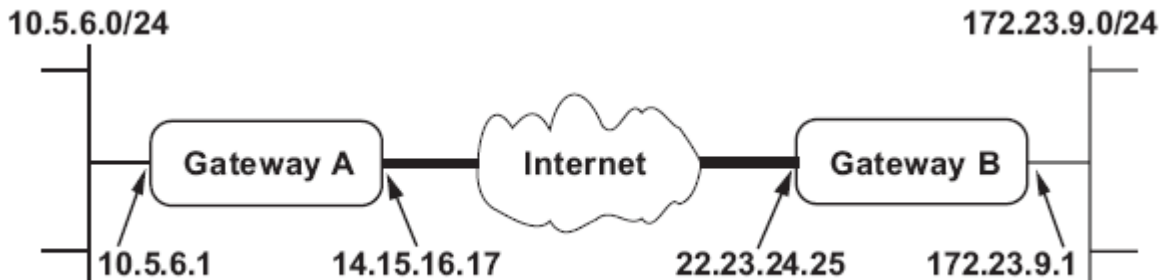


Figure 4-5: VPN Consortium Scenario 1

Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

The **IKE Phase 1 parameters** used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The **IKE Phase 2 parameters** used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

FVS336G Scenario 1: FVS336G to Gateway B with IKE and VPN Policies

Use this scenario illustration and configuration screens as a model to build your configuration.

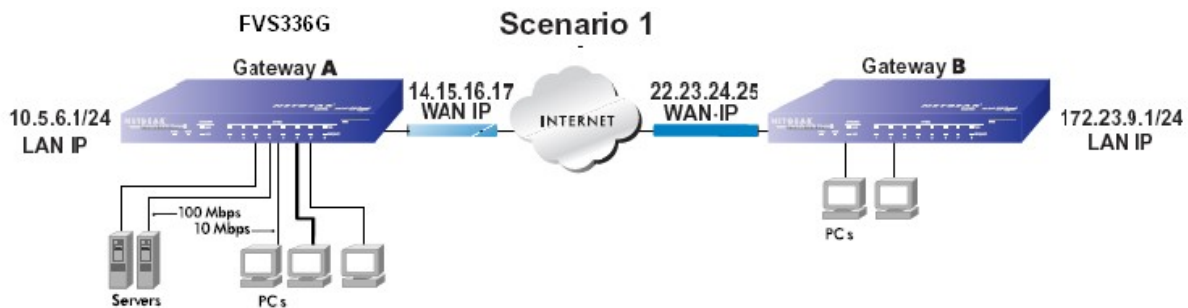


Figure 4-6: LAN to LAN VPN access from an FVS336G to an FVS336G

1. **Log in to the FVS336G labeled Gateway A in the illustration.**

Log in to the firewall at its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**, or using whatever Password and LAN address you have chosen for the firewall.

2. **Configure the WAN (Internet) and LAN IP addresses of the FVS336G.**

- a. Set up WAN:

[Network](#) | [Security](#) | [VPN](#) | [Users](#) | [Administration](#) | [Monitoring](#) | [Web Support](#) | [Logout](#)

[:: WAN Settings](#) :: [Protocol Binding](#) :: [Dynamic DNS](#) :: [LAN Setup](#) :: [Routing](#) ::

WAN1 ISP Settings | [WAN2 ISP Settings](#) | [WAN Mode](#)

[Advanced](#) | [WAN Status](#)

ISP Login ? help

Does Your Internet Connection Require a Login?

Yes No

Login:
 Password:

ISP Type ? help

Which type of ISP connection do you use?

Austria (PPTP)
 Other (PPPoE)
 BigPond Cable

Account Name:
 Domain Name:
 Login Server:
 Idle Timeout: Keep Connected
 Idle Time: Minutes
 My IP Address: ...
 Server IP Address: ...

Internet (IP) Address (Current IP Address) ? help

Get Dynamically from ISP
 Use Static IP Address

IP Address: ...
 IP Subnet Mask: ...
 Gateway IP Address: ...

Domain Name Server (DNS) Servers ? help

Get Automatically from ISP
 Use These DNS Servers

Primary DNS Server: ...
 Secondary DNS Server: ...

Internet

Figure 4-7: FVS336G Internet IP Address menu

- b. Configure the WAN Internet Address according to the settings in Figure 4-6 above and click Apply to save your settings.
- c. From the main menu Advanced section, click on the LAN IP Setup link.

[Network](#) | [Security](#) | [VPN](#) | [Users](#) | [Administration](#) | [Monitoring](#) | [Web Support](#) | [Logout](#) |

:: [WAN Settings](#) :: [Protocol Binding](#) :: [Dynamic DNS](#) :: [LAN Setup](#) :: [Routing](#) ::

[LAN Setup](#) | [LAN Groups](#) | [LAN Multi-homing](#) DHCP Log

LAN TCP/IP Setup help

IP Address:
 Subnet Mask:

DHCP help

Disable DHCP Server
 Enable DHCP Server

Domain Name:

Starting IP Address:

Ending IP Address:

Primary DNS Server:

Secondary DNS Server:

WINS Server:

Lease Time: Hours

Enable DNS Proxy:

2007 © Copyright NETGEAR®

d. Configure the LAN IP address according to the settings in figure above and click Apply to save your settings

Note: After you click Apply to change the LAN IP address settings, your workstation will be disconnected for the FVS336G. You will have to log on with <https://10.5.6.1> which is now the address you use to connect to the built-in web-based configuration manager of the FVS336G.

3. **Set up the IKE Policy illustrated below on the FVS336G.**

a. From the main menu VPN section, click on the IKE Policies link, and then click the Add button to display the screen below.

[Network](#) | [Security](#) | [VPN](#) | [Users](#) | [Administration](#) | [Monitoring](#) | [Web Support](#) | [Logout](#)

[IPSec VPN](#) :: [SSL VPN](#) :: [Certificates](#) :: [Connection Status](#) ::

Add IKE Policy [Add New VPN Policy](#)

Mode Config Record ? help

Do you want to use Mode Config Record?

Yes No

Select Mode Config Record:

[view selected](#)

General ? help

Policy Name:

Direction / Type:

Exchange Mode:

Local ? help

Identifier Type:

Identifier:

Remote ? help

Identifier Type:

Identifier:

IKE SA Parameters ? help

Encryption Algorithm:

Authentication Algorithm:

Authentication Method: Pre-shared key RSA-Signature

Pre-shared key: (Key Length 8 - 49 Char)

Diffie-Hellman (DH) Group:

SA-Lifetime (sec):

Extended Authentication ? help

XAUTH Configuration

None
 Edge Device
 IPSec Host

Authentication Type:

Username:

Password:

Apply
Reset

Figure 4-8: Scenario 1 IKE Policy

b. Configure the IKE Policy according to the settings in the illustration above and click Apply to save your settings.

4. Set up the FVS336G VPN -Auto Policy illustrated below.

- a. From the main menu VPN section, click on the VPN Policies link, and then click on the Add Auto Policy button.

The screenshot displays the configuration interface for an Auto Policy, divided into four sections:

- General:** Policy Name: scenario1a; Policy Type: Auto Policy; Select Local Gateway: WAN1 (selected); Remote Endpoint: IP Address (selected) with fields 22, 23, 24, 25; Enable NetBIOS? (unchecked); Enable RollOver? (unchecked).
- Traffic Selection:** Local IP: Subnet; Remote IP: Subnet; Start IP Address: 10, 5, 6, 0; End IP Address: (empty); Subnet Mask: 255, 255, 255, 0; Remote Start IP Address: 172, 23, 9, 0; Remote End IP Address: (empty); Remote Subnet Mask: 255, 255, 255, 0.
- Manual Policy Parameters:** SPI-Incoming: (empty) (Hex, 3-8 Chars); SPI-Outgoing: (empty) (Hex, 3-8 Chars); Encryption Algorithm: 3DES; Integrity Algorithm: SHA-1; Key-In: (empty); Key-Out: (empty) (DES-8 Char & 3DES-24 Char); Key-In: (empty); Key-Out: (empty) (MD5-16 Char & SHA-1-20 Char).
- Auto Policy Parameters:** SA Lifetime: 3600; Seconds (selected); Encryption Algorithm: 3DES; Integrity Algorithm: SHA-1; PFS Key Group: checked, DH Group 2 (1024 bit); Select IKE Policy: Scenario_1; view selected button.

Figure 4-9: Scenario 1 VPN - Auto Policy

- b. Configure the IKE Policy according to the settings in the illustration above and click Apply to save your settings.

5. After applying these changes, you will see a new table entry listed under VPN policies.

Now, all traffic from the range of LAN IP addresses specified on FVS336G A and FVS336G B will flow over a secure VPN tunnel.

Procedure 4-1: Checking VPN Connections

You can test connectivity and view VPN status information on the FVS336G.

1. To test connectivity between the Gateway A FVS336G LAN and the Gateway B LAN, follow these steps:

- a. Using our example, from a PC attached to the FVS336G on LAN A, on a Windows PC click the Start button on the taskbar and then click Run.
- b. Type `ping -t 172.23.9.1`, and then click OK.
- c. This will cause a continuous ping to be sent to the LAN interface of Gateway B. After between several seconds and two minutes, the ping response should change from “timed out” to “reply.”
- d. At this point the connection is established.

2. To test connectivity between the FVS336G Gateway A and Gateway B WAN ports, follow these steps:

- a. Using our example, log in to the FVS336G on LAN A, go to the main menu Maintenance section and click the Diagnostics link.
- b. To test connectivity to the WAN port of Gateway B, enter `22.23.24.25`, and then click Ping.
- c. This will cause a ping to be sent to the WAN interface of Gateway B. After between several seconds and two minutes, the ping response should change from “timed out” to “reply.” You may have to run this test several times before you get the “reply” message back from the target FVS336G.
- d. At this point the connection is established.

Note: If you want to Ping the FVS336G as a test of network connectivity, be sure the FVS336G is configured to respond to a Ping on the Internet WAN port by checking the checkbox seen in “Rules menu“. However, to preserve a high degree of security, you should turn off this feature when you are finished with testing.

3. To view the FVS336G event log and status of Security Associations, follow these steps:

- a. Go to the FVS336G main menu VPN section and click the Connection Status link. The log screen will display a history of the VPN connections, and the IPSec SA and IKE SA tables will report the status and data transmission statistics of the VPN tunnels for each policy.

- b. Go to “Monitoring” main menu and “VPN logs” submenu, and you’ll see all even log entries.