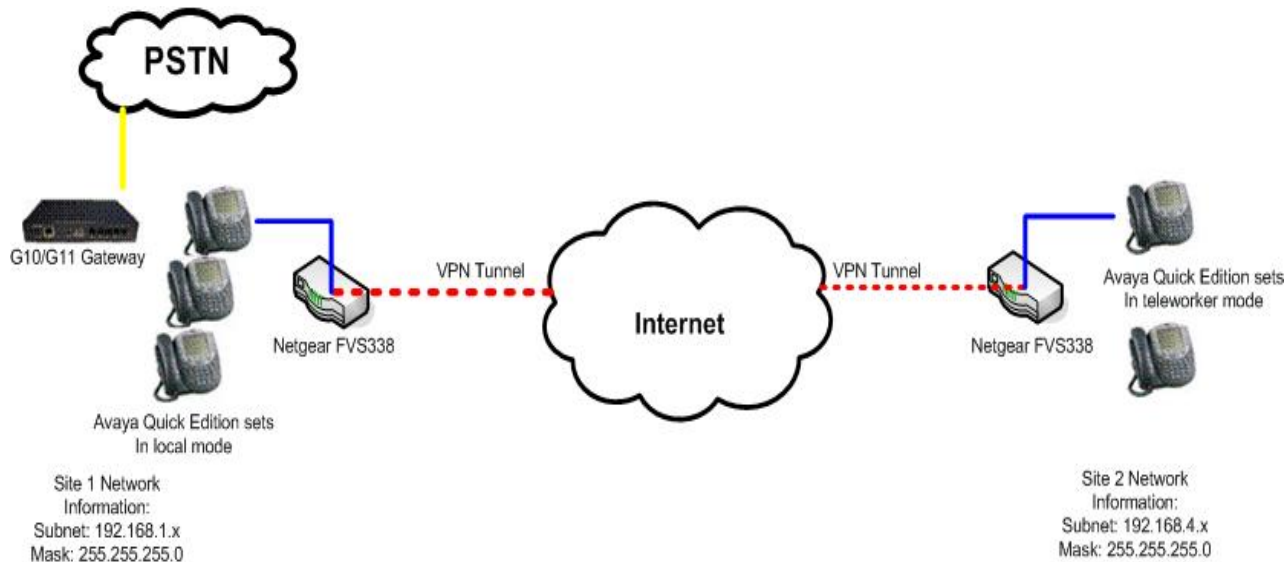


Avaya one-X™ Quick Edition

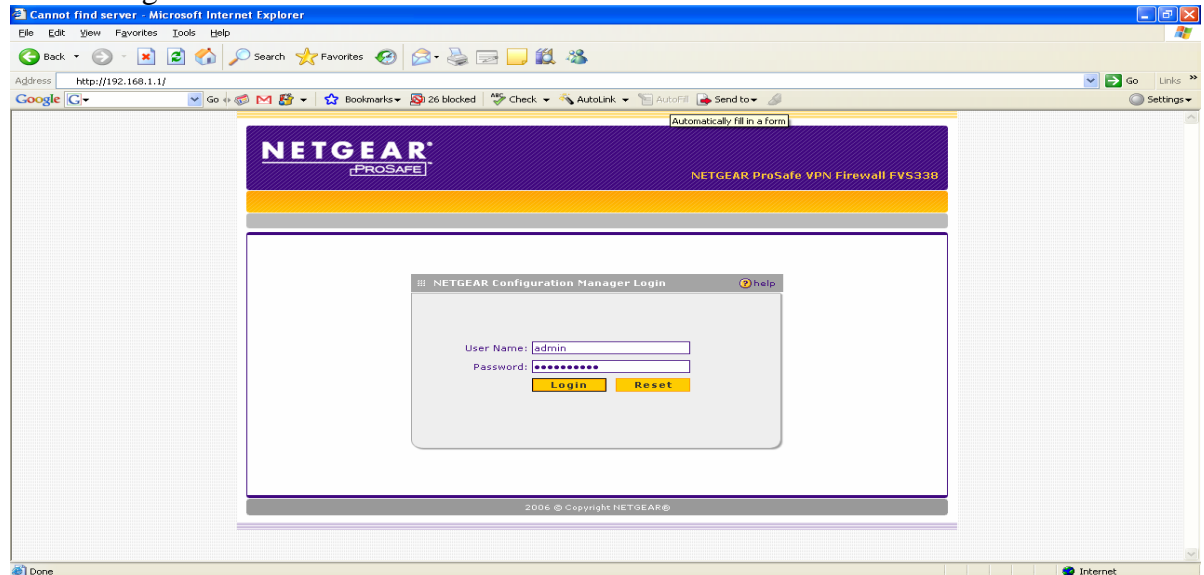
Configuring a Site-to-Site VPN on Netgear FVS338 Routers

This document explains how to configure a basic site-to-site VPN (virtual private network) configuration using Netgear FVS338 routers for remote teleworker connectivity. The document assumes that basic LAN and WAN setup and connectivity has been established. The diagram below is an overview of the network used in this example.



VPN Configuration

1. Log on to the router web administration tool.



2. Set up the local subnet ranges that you want the devices on the Site 1 network segment to use. In our example we are using 192.168.1.0/24 for site 1, and 192.168.4.0/24 for site 2. Click the LAN setup link and make a note of your network IP range and subnet.

NOTE Site 1 and Site 2 subnet ranges must be different and cannot conflict or overlap. If you change the LAN IP range and are using a DHCP server, change the DHCP server subnet ranges to match the subnet IP addresses used in the router's LAN TCP/IP settings.

NETGEAR PROSAFE
NETGEAR ProSafe VPN Firewall FVS338

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

WAN Settings | WAN Mode | Dynamic DNS | LAN Setup | LAN Groups | Routing

LAN Setup Multi Home LAN IPs Setup DHCP Log

LAN TCP/IP Setup help

IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

DHCP help

Disable DHCP Server
 Enable DHCP Server

Domain Name: my.company.com

Starting IP Address: 192.168.1.2

Ending IP Address: 192.168.1.100

WINS Server: . . .

Lease Time: 3000 Hours

Enable DNS Proxy:

Apply Reset

2006 © Copyright NETGEAR®

3. Click VPN and then click the VPN Wizard tab at the top of the admin tool to complete the initial VPN setup.

NETGEAR PROSAFE
NETGEAR ProSafe VPN Firewall FVS338

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

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

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

4. The VPN Tunnel will connect to the following Peers:

- When connecting a LAN-to-LAN VPN you will use “gateway” mode.

Connection Name and Remote IP Type:

- Name the new connection. We simply used “VPN” in the below example.
- The pre-shared key is a unique alpha-numeric string that must be common between your two routers. This key is thought of as a common pass phrase that is used for initial authentication and encryption when the tunnel is established. In the example below we chose a random passkey of “14524567”.

Endpoint Information:

- The remote WAN IP Address or Internet Name is the public IP (Internet accessible) address that is assigned to the remote peer router.
- The Local WAN IP address or Internet Name is the public IP (Internet accessible) address that is assigned to the current router.

Secure Connection Remote Accessibility:

- The Remote LAN IP address is the network subnet assigned to the remote network. This will be the “trusted” range of IPs.
- The remote subnet IP address is the subnet mask assigned to the remote network.

NETGEAR
PROSAFE

NETGEAR ProSafe VPN Firewall FV5338

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

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

VPN Wizard VPN Wizard Default Values

About VPN Wizard help

The Wizard sets most parameters to defaults as proposed by the VPN Consortium ([VPN](#)), 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?

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

End Point Information help

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

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

Secure Connection Remote Accessibility help

What is the remote LAN IP Address?

What is the remote LAN Subnet Mask?

Apply **Reset**

2006 © Copyright NETGEAR®

5. When the required fields are completed, click Apply. This will automatically create a VPN policy and an IKE policy for your tunnel.

NOTE Automatic VPN policies, when created thru the wizard, use SHA-1 authentication with 3DES encryption.

NETGEAR PROSAFE
NETGEAR ProSafe VPN Firewall FVS338

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

Polices :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: **Connection Status**

IKE Policies | **VPN Policies**

Operation succeeded.

List of VPN Policies help

	!	Name	Type	Local	Remote	Auth	Encr	Action
<input type="checkbox"/>	<input checked="" type="radio"/>	VPN	Auto Policy	192.168.1.0/255.255.255.0	192.168.4.0/255.255.255.0	SHA-1	3DES	

* Client Policy

select all delete enable disable

2006 © Copyright NETGEAR®

6. Next, complete configuration steps 1-5 on the remote router.

Confirming Connectivity

7. When both routers have a VPN policy created and physical connectivity is established, the routers should link and automatically connect the VPN tunnel. You can confirm the tunnel connectivity through the VPN logs screen.

NETGEAR PROSAFE
NETGEAR ProSafe VPN Firewall FVS338

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

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

IPsec Connection Status

Operation succeeded.

Active IPsec SA(s) help

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
VPN	61.34.56.20	783.10	2187	IPsec SA Established	

* Client Policy

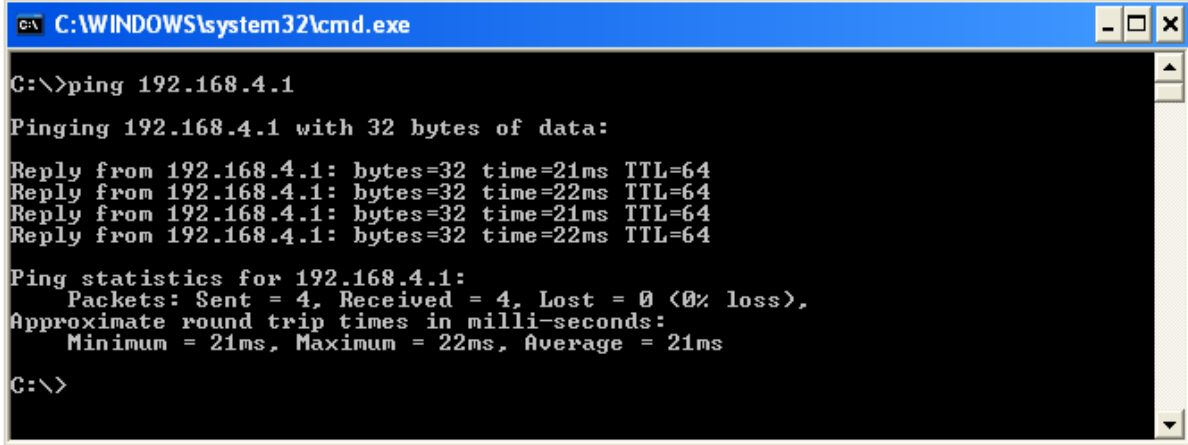
Poll Interval: (Seconds)

2006 © Copyright NETGEAR®

8. You can also perform a ping test. From a device on the local network ping a device (router endpoint) on the remote network. If you get a ping response the tunnel is set up and functioning properly. If there is no response check the settings and confirm that step 7 shows “IPSec SA Established”.

To perform a ping test from a windows PC on the local network:

1. Click Start and the click Run.
2. Type “cmd” in the Run dialog box.
3. At the DOS Prompt, type “ping 192.168.4.1” (replacing 192.168.4.1 with the subnet range that you used).



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.4.1
Pinging 192.168.4.1 with 32 bytes of data:
Reply from 192.168.4.1: bytes=32 time=21ms TTL=64
Reply from 192.168.4.1: bytes=32 time=22ms TTL=64
Reply from 192.168.4.1: bytes=32 time=21ms TTL=64
Reply from 192.168.4.1: bytes=32 time=22ms TTL=64
Ping statistics for 192.168.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 22ms, Average = 21ms
C:\>
```