# FortiClient in Hub-and-spoke IPSec VPN Example

## Technical Note

| *FortiClient in Hub-and-spoke IPSec VPN Example Technical Note* | |
|---|---|
| **Document Version:** | Version 1 |
| **Publication Date:** | 20 June 2005 |
| **Description:** | This technical note features a detailed configuration example that demonstrates how to include FortiClient dialup clients in a basic hub-and-spoke IPSec VPN. The VPN peers and clients use preshared keys for authentication purposes. |
| **Product:** | FortiGate v2.80 MR10 and FortiClient 1.2 MR3 |
| **Document Number:** | 01-28010-0208-20050620 |

**Fortinet Inc.**

*FortiClient in Hub-and-spoke IPSec VPN Example Technical Note*
FortiGate v2.80 MR10 and FortiClient 1.2 MR3
20 June 2005
01-28010-0208-20050620

# Table of Contents

# FortiClient in Hub-and-spoke IPSec VPN Example

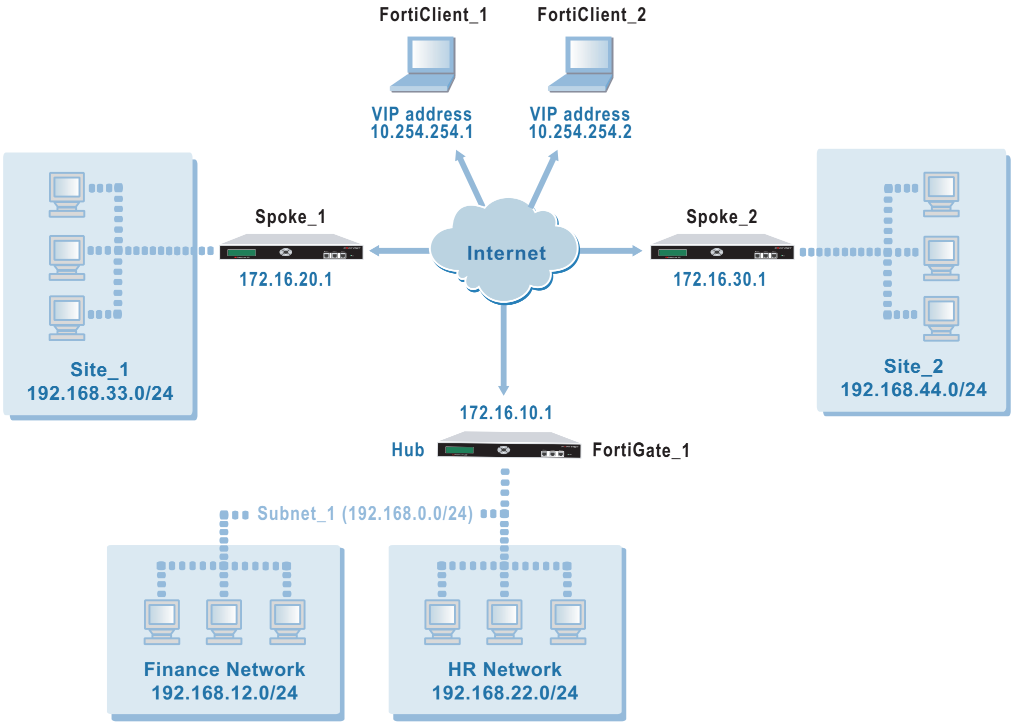
This technical note features a detailed configuration example that demonstrates how to include FortiClient dialup clients in a basic hub-and-spoke IPSec VPN. The VPN peers and clients use preshared keys for authentication purposes. The following sections are included:

## Network topology

In a hub-and-spoke configuration, connections to a number of remote peers and/or dialup clients radiate from a single, central FortiGate unit. Site-to-site connections between the VPN peers and clients do not exist; however, VPN tunnels between any two of the remote peers or clients can be set up through the FortiGate unit “hub”.

In a hub-and-spoke network, all VPN tunnels terminate at the hub. See Figure 1. The peers and/or clients that connect to the hub are known as “spokes”. The hub functions as a concentrator on the network, managing all VPN connections between the spokes. VPN traffic passes from one tunnel to the other through the hub.

Figure 1: Example hub-and-spoke configuration with FortiClient dialup clients



In the examples throughout this technical bulletin, the network devices are assigned IP addresses as shown in Figure 1. The steps for setting up the example hub-and-spoke configuration create a VPN among Site 1, Site 2, the HR Network, and the dialup users (FortiClient_1 and FortiClient_2). The Finance network is not included in the VPN.

All FortiGate units in the example configuration operate in NAT/Route mode and have static public IP addresses.

**Note:** Any FortiGate spoke may have a dynamic IP address, or a static domain name and dynamic IP address. For more information, contact Fortinet Technical Support.

The remote hosts on which the FortiClient Host Security application is installed obtain dynamic IP addresses from an ISP when they connect to the Internet. By default, the FortiClient Host Security application encrypts IP traffic and addresses the encrypted packets to the public interface of the FortiGate hub. Encrypted packets from the FortiGate hub are addressed either to the public IP address of the remote FortiClient host, or if the host computer is behind a NAT device, the private IP address of the host computer.

**Note:** If a router with NAT capabilities is in front of the FortiClient host (for example, when the FortiClient host is located in a remote office or hotel LAN), encrypted packets from the FortiGate unit are addressed to the remote host’s IP address on the private network behind the NAT device. For encrypted traffic to pass through the NAT device, the device must be NAT_T compatible. For more information, see “NAT traversal” in the *FortiGate VPN Guide*.

When the remote host is located behind a NAT device, unintended IP-address overlap issues may arise between the remote private network and the private network behind the FortiGate unit (for details, see the “FortiClient dialup-client configurations” section of the *FortiGate VPN Guide*). To prevent IP-address overlap, a Virtual IP (VIP) configuration is recommended. A VIP configuration enables you to assign uncommonly used IP addresses (for example, 10.254.254.1 and 10.254.254.2) to FortiClient dialup clients.

**Note:** More than one dialup client can connect to the same VPN tunnel. When you need to configure access for a group of dialup clients, assign a VIP address to each dialup client from a subnet comprising VIP addresses (for example, 10.254.254.0/24). As an alternative, you may configure a VIP address range (for example, 10.254.254.[100-110]).

In the example configuration, VIP addresses are assigned to the dialup clients manually. When a VIP address is assigned, the FortiClient Host Security application and the FortiGate unit both use the VIP address as the IP address of the FortiClient dialup client for the duration of the connection. As a result, when the FortiGate unit decrypts a packet from a FortiClient dialup client that has a VIP address, the source address in the IP header will be the VIP address used by the FortiClient Host Security application.

Assigning VIP addresses manually enables you to create a firewall encryption policy that allows connections from a specific VIP address, VIP address range, or a subnet address comprising VIP addresses.

## Configuring FortiGate_1

When a FortiGate unit receives a connection request from a remote VPN peer or client, it uses IPSec phase 1 parameters to establish a secure connection and authenticate the VPN peer or client. Then, if the firewall policy permits the connection, the FortiGate unit establishes the tunnel using IPSec phase 2 parameters and applies the firewall encryption policy. Key management, authentication, and security services are negotiated dynamically through the IKE protocol.

To support these functions, the following general configuration steps must be performed at FortiGate_1:

- Define the phase 1 parameters that the FortiGate unit needs to authenticate the spokes and establish secure connections. See “Define the phase 1 parameters” on page 8.
- Define the phase 2 parameters that the FortiGate unit needs to create VPN tunnels with the spokes. See “Define the phase 2 parameters” on page 9.
- Create one firewall encryption policy for each tunnel and define the scope of permitted services between the hub and each spoke. See “Define the firewall encryption policies” on page 10.
- Define the VPN concentrator, which determines the spokes to include in the configuration. See “Define the VPN concentrator” on page 12.

## Define the phase 1 parameters

The phase 1 configuration defines the parameters that FortiGate_1 will use to authenticate spokes and establish secure connections. For the purposes of this example, preshared keys are used to authenticate the spokes.

Before you define the phase 1 parameters, you need to:

- Reserve a name for each phase 1 configuration. A phase 1 configuration is needed for each FortiGate spoke. A single phase 1 configuration is needed for the FortiClient dialup clients.
- Obtain the IP address of the public interface to each FortiGate spoke.
- Decide which VIP addresses to use for FortiClient dialup clients. To prevent IP-address overlap, choose VIP addresses from a network that is not commonly used (for example, 10.254.254.0/24).
- Reserve a unique preshared key for each tunnel.

You need one preshared key to authenticate Spoke_1, a second different preshared key to authenticate Spoke_2, and a third unique preshared key to authenticate the FortiClient dialup clients. Each key must contain at least 6 printable characters and should only be known by network administrators. For optimum protection against currently known attacks, each key should consist of a minimum of 16 randomly chosen alphanumeric characters.

### To define the phase 1 parameters

1 At FortiGate_1, go to **VPN > IPSEC > Phase 1**.

2 Define the phase 1 parameters that the hub will use to establish a secure connection to Spoke_1. Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Gateway Name** | Type a name for the spoke (for example, `Spoke_1`). |
| **Remote Gateway** | Static IP Address |
| **IP Address** | `172.16.20.1` |
| **Mode** | Main |
| **Authentication Method** | Preshared Key |
| **Pre-shared Key** | Enter the preshared key. |
| **Peer Options** | Accept any peer ID |

3 Define the phase 1 parameters that the hub will use to establish a secure connection to Spoke_2. Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Gateway Name** | Type a name for the spoke (for example, `Spoke_2`). |
| **Remote Gateway** | Static IP Address |
| **IP Address** | `172.16.30.1` |
| **Mode** | Main |
| **Authentication Method** | Preshared Key |
| **Pre-shared Key** | Enter the preshared key. |
| **Peer Options** | Accept any peer ID |

4 Define the phase 1 parameters that the hub will use to establish a secure connection with the FortiClient dialup clients. Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Gateway Name** | Type a name for the remote gateway (for example, `Dialup_clients`). |
| **Remote Gateway** | Dialup User |
| **Mode** | Main |
| **Authentication Method** | Preshared Key |
| **Pre-shared Key** | Enter the preshared key. |
| **Peer Options** | Accept any peer ID |

## Define the phase 2 parameters

The basic phase 2 settings associate IPSec phase 2 parameters with the phase 1 configuration and specify the remote end points of the VPN tunnels. Before you define the phase 2 parameters, you need to reserve a name for each tunnel.

### To define the phase 2 parameters

1 Go to **VPN > IPSEC > Phase 2**.

2 Create a phase 2 tunnel definition for Spoke_1. Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Tunnel Name** | Enter a name for the tunnel (for example, `FG1toSP1_Tunnel`). |
| **Remote Gateway** | Select the gateway that you defined previously for Spoke_1 (for example, `Spoke_1`). |

3 Create a phase 2 tunnel definition for Spoke_2. Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Tunnel Name** | Enter a name for the tunnel (for example, `FG1toSP2_Tunnel`). |
| **Remote Gateway** | Select the gateway that you defined previously for Spoke_2 (for example, `Spoke_2`). |

4 Create a phase 2 tunnel definition for the FortiClient dialup clients. Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Tunnel Name** | Enter a name for the tunnel (for example, `FG1toDialupClients`). |
| **Remote Gateway** | Select the gateway that you defined previously (for example, `Dialup_clients`). |

5 Enter the following CLI command to enable all dialup clients having VIP addresses from the designated VIP network to connect using the same phase 2 tunnel definition:

```
config vpn ipsec phase2
  edit FG1toDialupClients
  set single-source enable
  end
```

## Define the firewall encryption policies

Firewall policies control all IP traffic passing between a source address and a destination address. A firewall encryption policy is needed to allow the transmission of encrypted packets, specify the permitted direction of VPN traffic, and select the VPN tunnel that will be subject to the policy. A single encryption policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

Before you define the policy, you must first specify the IP source and destination addresses. In the example hub-and-spoke configuration:

- The IP source address corresponds to the HR network behind FortiGate_1.
- The IP destination addresses refer to the private networks behind Spoke_1 and Spoke_2, and the VIP addresses associated with FortiClient dialup clients.

### To define the IP source address of the HR network behind FortiGate_1

1 Go to **Firewall > Address**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `HR_Network`). |
| **IP Range/Subnet** | Enter the IP address of the HR network behind FortiGate_1 (for example, `192.168.22.0/24`). |

### To specify the destination address of IP packets delivered to Spoke_1

1 Go to **Firewall > Address**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `Site_1`). |
| **IP Range/Subnet** | Enter the IP address of the private network behind Spoke_1 (for example, `192.168.33.0/24`). |

### To specify the destination address of IP packets delivered to Spoke_2

1 Go to **Firewall > Address**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `Site_2`). |
| **IP Range/Subnet** | Enter the IP address of the private network behind Spoke_2 (for example, `192.168.44.0/24`). |

### To specify the VIP destination addresses assigned to FortiClient dialup clients

1 Go to **Firewall > Address**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `VIP_addresses`). |
| **IP Range/Subnet** | Enter the IP address of the designated VIP network (for example, `10.254.254.0/24`). |

### To define the firewall encryption policy for hub-to-Spoke_1 traffic

1 Go to **Firewall > Policy**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Interface/Zone** | Source<br>Select the interface to the HR network.<br>Destination<br>Select the interface to the external (public) network. |
| **Address Name** | Source<br>`HR_Network`<br>Destination<br>`Site_1` |
| **Schedule** | As required. |
| **Service** | As required. |
| **Action** | ENCRYPT |
| **VPN Tunnel** | `FG1toSP1_Tunnel` |

### To define the firewall encryption policy for hub-to-Spoke_2 traffic

1 Go to **Firewall > Policy**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Interface/Zone** | Source<br>Select the interface to the HR network.<br>Destination<br>Select the interface to the external (public) network. |
| **Address Name** | Source<br>`HR_Network`<br>Destination<br>`Site_2` |
| **Schedule** | As required. |
| **Service** | As required. |
| **Action** | ENCRYPT |
| **VPN Tunnel** | `FG1toSP2_Tunnel` |

### To define the firewall encryption policy for hub-to-FortiClient traffic

1 Go to **Firewall > Policy**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Interface/Zone** | Source<br>Select the interface to the internal (private) network.<br>Destination<br>Select the interface to the external (public) network. |
| **Address Name** | Source<br>`HR_Network`<br>Destination<br>`VIP_addresses` |

| | |
|---|---|
| **Schedule** | As required. |
| **Service** | As required. |
| **Action** | ENCRYPT |
| **VPN Tunnel** | `FG1toDialupClients` |

3 In the policy list, arrange the policies in the following order:

- encryption policies that control traffic between the hub and the spokes first
- the default firewall policy last

## Define the VPN concentrator

The concentrator specifies which spokes to include in the hub-and-spoke configuration.

### To define the VPN concentrator

1 Go to **VPN > IPSec > Concentrator** and select Create New.

2 In the Concentrator Name field, type a name to identify the concentrator (for example, `Hub_1`).

3 From the Available Tunnels list, select `FG1toSP1_Tunnel` and select the right-pointing arrow.

4 From the Available Tunnels list, select `FG1toSP2_Tunnel` and select the right-pointing arrow.

5 From the Available Tunnels list, select `FG1toDialupClients` and select the right-pointing arrow.

6 Select OK.

# Configuring Spoke_1

The Spoke_1 configuration requires the following settings:

- phase 1 authentication parameters to initiate a connection with the hub
- phase 2 tunnel creation parameters to establish a VPN tunnel with the hub
- a source address that represents the network behind Spoke_1
- a destination address that represents the HR network behind the hub
- a firewall encryption policy to enable communications between Spoke_1 and the hub
- a destination address that represents the network behind Spoke_2
- a firewall encryption policy to enable communications between Spoke_1 and Spoke_2
- a destination address that represents the VIP addresses assigned to FortiClient dialup clients
- a firewall encryption policy to enable communications between Spoke_1 and the FortiClient dialup clients

### To define the phase 1 parameters

1 At Spoke_1, go to **VPN > IPSEC > Phase 1**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Gateway Name** | Type a name for the hub (for example, `FortiGate_1`). |
| **Remote Gateway** | Static IP Address |
| **IP Address** | `172.16.10.1` |
| **Mode** | Main |
| **Authentication Method** | Preshared Key |
| **Pre-shared Key** | Enter the preshared key. The value must be identical to the preshared key that you specified previously in the FortiGate_1 configuration. |
| **Peer Options** | Accept any peer ID |

### To define the phase 2 parameters

1 Go to **VPN > IPSEC > Phase 2**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Tunnel Name** | Enter a name for the tunnel (for example, `SP1toFG1_Tunnel`). |
| **Remote Gateway** | Select the name that you defined previously for the hub (for example, `FortiGate_1`). |

### To define the IP source address of the network behind Spoke_1

1 Go to **Firewall > Address**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `Site_1`). |
| **IP Range/Subnet** | Enter the IP address of the private network behind Spoke_1 (for example, `192.168.33.0/24`). |

### To specify the destination address of IP packets delivered to FortiGate_1

1 Go to **Firewall > Address**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `HR_Network`). |
| **IP Range/Subnet** | Enter the IP address of the HR network behind FortiGate_1 (for example, `192.168.22.0/24`). |

### To define the firewall encryption policy to enable communications with the hub

1 Go to **Firewall > Policy**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Interface/Zone** | Source<br>Select the interface to the internal (private) network.<br>Destination<br>Select the interface to the external (public) network. |
| **Address Name** | Source<br>`Site_1`<br>Destination<br>`HR_Network` |
| **Schedule** | As required. |
| **Service** | As required. |
| **Action** | ENCRYPT |
| **VPN Tunnel** | `SP1toFG1_Tunnel` |

### To specify the IP address of the network behind Spoke_2

1 Go to **Firewall > Address**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `Site_2`). |
| **IP Range/Subnet** | Enter the IP address of the network behind Spoke_2 (for example, `192.168.44.0/24`). |

### To define the firewall encryption policy for Spoke_1-to-Spoke_2 traffic

1 Go to **Firewall > Policy**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Interface/Zone** | Source<br>Select the interface to the internal (private) network.<br>Destination<br>Select the interface to the external (public) network. |
| **Address Name** | Source<br>`Site_1`<br>Destination<br>`Site_2` |
| **Schedule** | As required. |
| **Service** | As required. |
| **Action** | ENCRYPT |
| **VPN Tunnel** | `SP1toFG1_Tunnel` |

### To specify the VIP destination addresses assigned to FortiClient dialup clients

1 Go to **Firewall > Address**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `VIP_addresses`). |
| **IP Range/Subnet** | Enter the IP address of the designated VIP network (for example, `10.254.254.0/24`). |

### To define the firewall encryption policy for Spoke_1-to-FortiClient traffic

1 Go to **Firewall > Policy**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Interface/Zone** | Source<br>Select the interface to the internal (private) network.<br>Destination<br>Select the interface to the external (public) network. |
| **Address Name** | Source<br>`Site_1`<br>Destination<br>`VIP_addresses` |
| **Schedule** | As required. |
| **Service** | As required. |
| **Action** | ENCRYPT |
| **VPN Tunnel** | `SP1toFG1_Tunnel` |

3 In the policy list, arrange the policies in the following order:

- encryption policies that control traffic between Spoke_1 and the hub first
- the default firewall policy last

## Configuring Spoke_2

The Spoke_2 configuration requires the following settings:

- phase 1 authentication parameters to initiate a connection with the hub
- phase 2 tunnel creation parameters to establish a VPN tunnel with the hub
- a source address that represents the network behind Spoke_2
- a destination address that represents the HR network behind the hub
- a firewall encryption policy to enable communications between Spoke_2 and the hub
- a destination address that represents the network behind Spoke_1
- a firewall encryption policy to enable communications between Spoke_2 and Spoke_1
- the destination address that represents the VIP addresses assigned to FortiClient dialup clients
- a firewall encryption policy to enable communications between Spoke_2 and the FortiClient dialup clients

### To define the phase 1 parameters

**1** At Spoke_2, go to **VPN > IPSEC > Phase 1**.

**2** Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Gateway Name** | Type a name for the hub (for example, `FortiGate_1`). |
| **Remote Gateway** | Static IP Address |
| **IP Address** | `172.16.10.1` |
| **Mode** | Main |
| **Authentication Method** | Preshared Key |
| **Pre-shared Key** | Enter the preshared key. The value must be identical to the preshared key that you specified previously in the FortiGate_1 configuration. |
| **Peer Options** | Accept any peer ID |

### To define the phase 2 parameters

**1** Go to **VPN > IPSEC > Phase 2**.

**2** Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Tunnel Name** | Enter a name for the tunnel (for example, `SP2toFG1_Tunnel`). |
| **Remote Gateway** | Select the name that you defined previously for the hub (for example, `FortiGate_1`). |

### To define the IP source address of the network behind Spoke_2

1 Go to **Firewall > Address**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `Site_2`). |
| **IP Range/Subnet** | Enter the IP address of the private network behind Spoke_2 (for example, `192.168.44.0/24`). |

### To specify the destination address of IP packets delivered to FortiGate_1

1 Go to **Firewall > Address**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `HR_Network`). |
| **IP Range/Subnet** | Enter the IP address of the HR network behind FortiGate_1 (for example, `192.168.22.0/24`). |

### To define the firewall encryption policy to enable communications with the hub

1 Go to **Firewall > Policy**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Interface/Zone** | Source<br>Select the interface to the internal (private) network.<br>Destination<br>Select the interface to the external (public) network. |
| **Address Name** | Source<br>`Site_2`<br>Destination<br>`HR_Network` |
| **Schedule** | As required. |
| **Service** | As required. |
| **Action** | ENCRYPT |
| **VPN Tunnel** | `SP2toFG1_Tunnel` |

### To specify the IP address of the network behind Spoke_1

1 Go to **Firewall > Address**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `Site_1`). |
| **IP Range/Subnet** | Enter the IP address of the network behind Spoke_1 (for example, `192.168.33.0/24`). |

### To define the firewall encryption policy for Spoke_2-to-Spoke_1 traffic

1 Go to **Firewall > Policy**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Interface/Zone** | Source<br>Select the interface to the internal (private) network.<br>Destination<br>Select the interface to the external (public) network. |
| **Address Name** | Source<br>`Site_2`<br>Destination<br>`Site_1` |
| **Schedule** | As required. |
| **Service** | As required. |
| **Action** | ENCRYPT |
| **VPN Tunnel** | `SP2toFG1_Tunnel` |

### To specify the VIP destination addresses assigned to FortiClient dialup clients

1 Go to **Firewall > Address**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Address Name** | Enter an address name (for example, `VIP_addresses`). |
| **IP Range/Subnet** | Enter the IP address of the designated VIP network (for example, `10.254.254.0/24`). |

### To define the firewall encryption policy for Spoke_2-to-FortiClient traffic

1 Go to **Firewall > Policy**.

2 Select Create New, enter the following information, and select OK:

| | |
|---|---|
| **Interface/Zone** | Source<br>Select the interface to the internal (private) network.<br>Destination<br>Select the interface to the external (public) network. |
| **Address Name** | Source<br>`Site_2`<br>Destination<br>`VIP_addresses` |
| **Schedule** | As required. |
| **Service** | As required. |
| **Action** | ENCRYPT |
| **VPN Tunnel** | `SP2toFG1_Tunnel` |

3 In the policy list, arrange the policies in the following order:

- encryption policies that control traffic between Spoke_2 and the hub first
- the default firewall policy last

## Configuring the FortiClient software

The following procedure explains how to configure the FortiClient Host Security application to connect to FortiGate_1. Each FortiClient dialup client uses its assigned VIP address as its IP source address for the duration of the connection.

### To configure FortiClient

1. At the remote host, start FortiClient.
2. Go to **VPN > Connections** and select Add.
3. In the Connection Name field, type a descriptive name for the connection (for example, `FortiGate_1`).
4. In the Remote Gateway field, type the public static IP address of the FortiGate hub (for example, `172.16.10.1`).
5. In the Remote Network fields, type the private IP address and netmask of the HR network behind the FortiGate unit (for example, `192.168.22.0/255.255.255.0`).
6. From the Authentication Method list, select Preshared Key.
7. In the Preshared Key field, type the preshared key. The value must be identical to the preshared key that you specified previously for FortiClient dialup clients in the FortiGate_1 configuration.
8. Select Advanced.
9. In the Advanced Settings dialog box, select Acquire virtual IP address and then select Manually Set.
10. In the IP and Subnet Mask fields, enter the VIP address and netmask that the FortiClient Host Security application will use as its source address for transmitting IP packets through the tunnel (for example, `10.254.254.1/255.255.255.0`).

**Note:** FortiClient settings determine which DNS server and Windows Internet Service (WINS) server the client can access after the tunnel has been established. For more information, see *FortiClient online Help*.

11. Select OK.
12. Retain the default advanced settings unless changes are needed to make the IKE and IPSec proposals match the phase 1 and 2 settings on the FortiGate hub.
13. In the Remote Network group, select Add.
14. In the IP and Subnet Mask fields, type the IP address of the private network behind Spoke_1 (for example, `192.168.33.0/255.255.255.0`) and select OK.
15. In the Remote Network group, select Add.
16. In the IP and Subnet Mask fields, type the IP address of the private network behind Spoke_2 (for example, `192.168.44.0/255.255.255.0`) and select OK.
17. Select OK twice to close the dialog boxes.
18. Exit FortiClient and repeat this procedure at all other remote FortiClient hosts. When you assign a VIP address to the next remote FortiClient host in Step 10, ensure that you use a different VIP address from the designated VIP network.