Circumventing Ambiguous Routing in a Hub-and-spoke IPSec VPN

Technical Note

Circumventing Ambiguous Routing in a Hub-and-spoke IPSec VPN Technical Note	
Document Version:	Version 1
Publication Date:	25 August 2005
Description:	This technical note provides guidelines for circumventing ambiguous routing in a hub-and-spoke IPSec VPN. Ambiguous routing may become problematic when two or more of the private networks behind FortiGate spokes unintentionally use the same IP address space or have overlapping IP addresses.
Product:	FortiGate v2.80 MR10
Document Number:	01-28010-0226-20050825

Fortinet Inc.

Circumventing Ambiguous Routing in a Hub-and-spoke IPSec VPN Technical Note
FortiGate v2.80 MR10
25 August 2005
01-28010-0226-20050825

Table of Contents

Circumventing Ambiguous Routing in a Hub-and-spoke IPSec VPN

This technical note provides guidelines for circumventing ambiguous routing in a hub-and-spoke IPSec VPN. Ambiguous routing may become problematic when two or more of the private networks behind FortiGate spokes unintentionally use the same IP address space or have overlapping IP addresses.

This technical note contains the following sections:

How ambiguous routing affects a VPN

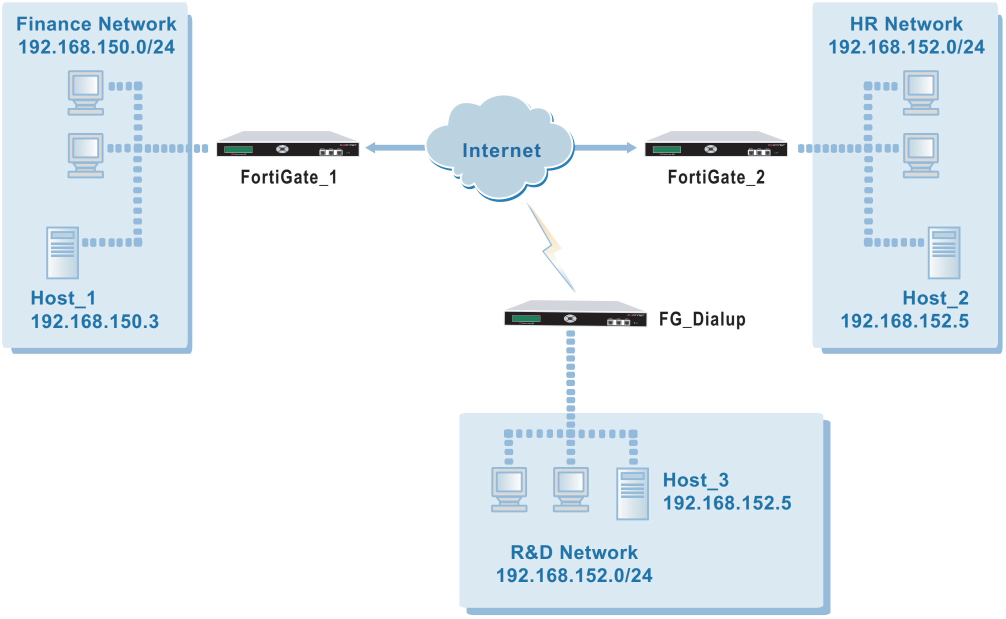
Ambiguous routing can happen when two or more physically separate networks that use the same private address space are connected through a VPN: a single private network would be created, but a packet destined for the remote network might not be forwarded to a computer on the other side of the VPN tunnel. An example of this type of network is shown in Figure 1 on page 6.

In the example hub-and-spoke configuration shown in Figure 1:

- FortiGate_1 is the hub, and FortiGate_2 and FG_Dialup are spokes.
- FortiGate_1 operates in NAT-Route mode and has static public IP address.
- FortiGate_2 has static IP address and FG_Dialup is assigned a dynamic IP address through an ISP before it initiates a connection to FortiGate_1.

For more information about hub-and-spoke configurations and FortiGate dialup-client configurations, see the *FortiGate VPN Guide*.

Figure 1: IP-address overlap between the HR and R&D networks



Because the private networks in the example configuration are managed by different organizations (for example, FortiGate_1 may belong to a trading company and FortiGate_2 and FG_Dialup may be managed by two different suppliers), the IP addresses used by the private networks behind FortiGate_2 and FG_Dialup both—by coincidence—may use the same IP address space or have overlapping IP address.

As a result, when a host or server behind FortiGate_1 responds to traffic that originates from the private network behind FortiGate_2 or FG_Dialup, a conflict may occur in the routing table on FortiGate_1 and traffic destined for the remote network through the hub may be sent to the wrong network. In this case, you can use a combination of FortiGate IPSec phase 2 quick mode selectors and firewall encryption policy settings as described in this technical note to ensure that the response is sent back to the correct originator.

Resolving ambiguous routing

It is possible to associate substitute IP source addresses with traffic that originates from behind each remote peer. Replacing the source addresses of IP packets before they enter the tunnel at the remote end helps to circumvent ambiguous routing at FortiGate_1. This is done by specifying matching phase 2 selectors at all FortiGate units and configuring the firewall encryption policies at the spokes to translate the source addresses of outgoing IP packets into replacement addresses.

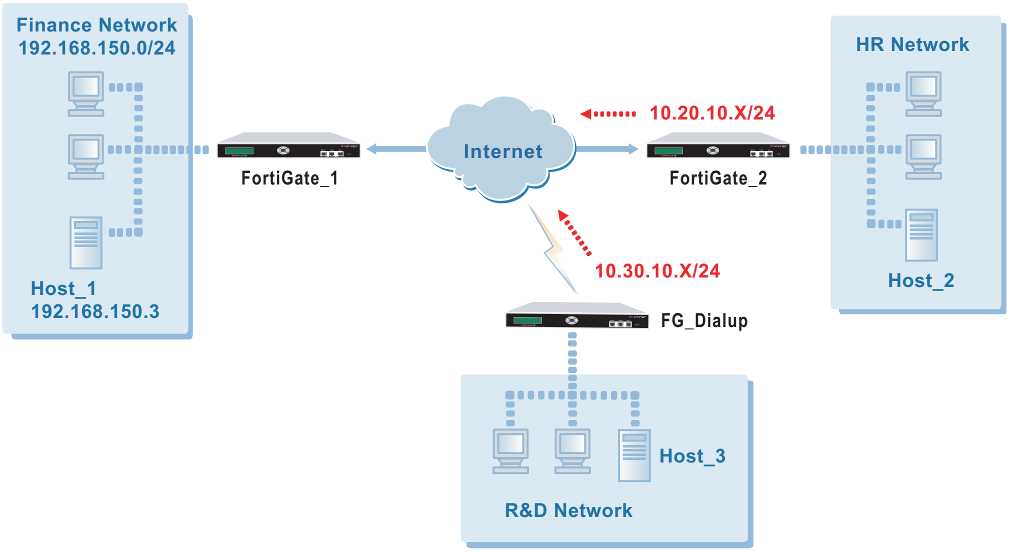
Substituting uncommonly used source addresses for IP packets from each remote private network is the key step to resolving ambiguous routing. The configuration procedures rely on the ability of FortiGate spokes to perform IP-address-substitution automatically as soon as tunnels to the hub are established.

In a hub-and-spoke configuration, each tunnel between the hub and a spoke may be considered a stand-alone (gateway-to-gateway or dialup-client) tunnel. The goal of phase 2 negotiations between each hub-spoke pair is to match the address of the private network behind the hub and the replacement address used by the spoke to represent its private network. You must configure FortiGate_1 to use the replacement addresses for IPSec phase 2 (quick mode) selector negotiations, and configure the spokes to accept the selectors proposed by FortiGate_1 during phase 2 negotiations. Afterward, when a packet from one spoke is destined for another spoke, the hub applies its concentrator function to forward the packet through the tunnel to the correct spoke.

In the example configuration (see Figure 2):

- FortiGate_2 replaces the source addresses of IP traffic from the HR network with a virtual IP address in the 10.20.10.0/24 address space before the packets are sent through the tunnel. FortiGate_1 accepts connections from FortiGate_2 based on its static IP address and passes associated traffic having a source address in the 10.20.10.0/24 address space. Host_1 can reach Host_2 using the destination IP address 10.20.10.5. Host_2 replies to Host_1 using a destination IP address of 192.168.150.3.
- FG_Dialup replaces the source addresses of IP traffic from the R&D network with a virtual IP address in the 10.30.10.0/24 address space before the packets are sent through the tunnel. FortiGate_1 accepts connections from FG_Dialup based on its unique identifier (local ID) and passes associated traffic having a source address in the 10.30.10.0/24 address space. Host_1 can reach Host_3 using the destination IP address 10.30.10.5. Host_3 replies to Host_1 using a destination IP address of 192.168.150.3.

Figure 2: Assigning replacement addresses to IP packets from remote networks



Configuring FortiGate_1

When a FortiGate unit receives a connection request from a remote VPN peer, it uses IPSec phase 1 parameters to establish a secure connection and authenticate the VPN peer. 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 FortiGate_1 needs to authenticate FortiGate_2 and FG_Dialup and establish secure connections. See “Define the phase 1 parameters” on page 8.
- Define the phase 2 parameters that FortiGate_1 needs to create VPN tunnels with FortiGate_2 and FG_Dialup. See “Define the phase 2 parameters” on page 9.
- Create a firewall encryption policy to control the permitted services and permitted direction of traffic between the IP source and destination addresses. The IP destination addresses will be the virtual IP addresses that the spokes assign to outgoing IP packets before the packets enter the tunnel at the remote end. See “Define the firewall encryption policy” on page 10.
- Specify the quick mode selectors that FortiGate_1 will supply to the spokes during phase 2 negotiations. The selectors associated with destination addresses have to identify the virtual source addresses that spokes assign to outgoing IP packets. See “Specifying the phase 2 quick mode selectors” on page 12.
- Define the VPN concentrator, which determines the spokes to include in the configuration. See “Define the VPN concentrator” on page 13.

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.

Note: A single phase 1 configuration may be shared by multiple dialup clients.

- Obtain the static IP address of the public interface to FortiGate_2 (for example, `172.16.87.186`).
- Reserve a unique identifier (local ID) that FG_Dialup can use to identify itself to FortiGate_1 during the IPSec phase 1 exchange (for example, `FG_Dialup`).
- Reserve a unique preshared key for each tunnel.

You need one preshared key to authenticate FortiGate_2, and a second different preshared key to authenticate FG_Dialup. 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 with FortiGate_2. Select Create New, enter the following information, and select OK:

Gateway Name	Type a name for the spoke (for example, `FortiGate_2`).
Remote Gateway	Static IP Address
IP Address	`172.16.87.186`
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 with FG_Dialup. Select Create New, enter the following information, and select OK:

Gateway Name	Type a name for the spoke (for example, `FG_Dialup`).
Remote Gateway	Select Dialup User.
Mode	Aggressive
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Select Accept this peer ID and type the identifier that you reserved for the FortiGate dialup client into the adjacent field (for example, `FG_Dialup`).

Note: Whenever you add dialup clients, it is a good practice to assign a unique identifier (local ID) to each dialup client. Be sure to select Aggressive mode on both the dialup client and the dialup server, and also specify the identifier as a peer ID on the FortiGate dialup server.

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 FortiGate_2. Select Create New, enter the following information, and select OK:

Tunnel Name	Enter a name for the tunnel (for example, `FG1toFG2_Tunnel`).
Remote Gateway	Select the gateway that you defined previously for FortiGate_2 (for example, `FortiGate_2`).

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

Tunnel Name	Enter a name for the tunnel (for example, `FG1toFGDialup_Tunnel`).
Remote Gateway	Select the gateway name that you defined previously for FG_Dialup (for example, `FG_Dialup`).

Define the firewall encryption policy

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 Finance network behind FortiGate_1.
- The IP destination addresses refer to the substituted network-address values that the spokes assign to outgoing IP packets before the packets are sent through the tunnel at the remote end. The source addresses of packets from the HR network will be converted to the 10.20.10.0/24 address space, and the source addresses of packets from the R&D network will be converted to the 10.30.10.0/24 address space.

To specify the source address of IP packets from the Finance network

1. Go to **Firewall > Address**.
2. Select Create New, enter the following information, and select OK:

Address Name	Enter an address name (for example, `Finance_Network`).
IP Range/Subnet	Enter the IP address of the private network behind FortiGate_1 (for example, `192.168.150.0/24`).

To refer to the substituted HR network address

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 network address from which FortiGate_2 may assign IP addresses to packets from the HR network (for example, `10.20.10.0/24`).

To refer to the substituted R&D network address

1 Go to **Firewall > Address**.

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

Address Name	Enter an address name (for example, `RD_Network`).
IP Range/Subnet	Enter the network address from which FG_Dialup may assign IP addresses to packets from the R&D network (for example, `10.30.10.0/24`).

To define the firewall encryption policy for hub-to-FortiGate_2 traffic

1 Go to **Firewall > Policy**.

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

Interface/Zone	Source Select the interface to the Finance network. Destination Select the interface to the external (public) network.

Address Name	Source
	`Finance_Network`
	Destination
	`HR_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG1toFG2_Tunnel`

To define the firewall encryption policy for hub-to-FG_Dialup traffic

1. Go to **Firewall > Policy**.
2. Select Create New, enter the following information, and select OK:

Interface/Zone	Source Select the interface to the Finance network. Destination Select the interface to the external (public) network.

Address Name	Source
	`Finance_Network`
	Destination
	`RD_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG1toFGDialup_Tunnel`

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

Specifying the phase 2 quick mode selectors

Now that you have replacement IP addresses for traffic that originates from the HR and R&D networks, you can edit the phase 2 quick mode identities configuration on FortiGate_1 to refer to the replacement IP addresses.

1. Go to **VPN > IPSEC > Phase 2**.
2. Select the Edit icon in the row beside the phase 2 tunnel definition for FortiGate_2.
3. Select Advanced, enter the following information, and then select OK:

Quick Mode Identities Select Specify a selector and enter appropriate values as follows:

Source address	`Finance_Network`
Source port	`0` (all ports)
Dest address	`HR_Network`
Dest port	`0` (all ports)
Protocol	`0` (all protocol types)

4. Select the Edit icon in the row beside the phase 2 tunnel definition for FG_Dialup.
5. Select Advanced, enter the following information, and then select OK:

Quick Mode Identities Select Specify a selector and enter appropriate values as follows:

Source address	`Finance_Network`
Source port	`0` (all ports)
Dest address	`RD_Network`
Dest port	`0` (all ports)
Protocol	`0` (all protocol types)

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 `FG1toFG2_Tunnel` and select the right-pointing arrow.
4. From the Available Tunnels list, select `FG1toFGDialup_Tunnel` and select the right-pointing arrow.
5. Select OK.

Configuring FortiGate_2

The FortiGate_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 HR network behind FortiGate_2 (for example, `192.168.152.0/24`)
- a destination address that represents the Finance network behind the hub (for example, `192.168.150.0/24`)
- a firewall encryption policy to enable communications between FortiGate_2 and the hub
- a destination address that corresponds to the IP addresses that FG_Dialup may assign to packets from the R&D network (for example, `10.30.10.0/24`)
- a firewall encryption policy to enable communications between FortiGate_2 and FG_Dialup through the hub
- a replacement address, to be used as an IPSec phase 2 quick mode selector in the phase 2 exchange (for example, `10.20.10.0/24`)

In addition, to ensure that packets from the HR network have an unambiguous source IP address, you must enable subnet-address translation on outbound packets through the Outbound NAT option in the firewall encryption policy in conjunction with the `set natip` attribute of the `config firewall policy` command. When you specify a `natip` value, the FortiGate unit uses a static subnetwork-to-subnetwork mapping scheme to translate IP source addresses into virtual IP addresses from the network address space that you specify. You specify a 32-bit subnet mask in the `natip` value to translate the source addresses to a single network address space. For example, if the IP source address of a packet leaving the HR network is 192.168.152.5/24 and the `natip` value is 10.20.10.0/24, the source address will be translated to 10.20.10.5.

To define the phase 1 parameters

1 At FortiGate_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	`172.16.87.183`
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 for FortiGate_2 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, `FG2toFG1_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 FortiGate_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, `HR_Network`).
IP Range/Subnet	Enter the IP address of the private network behind FortiGate_2 (for example, `192.168.152.0/24`).

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, `Finance_Network`).
IP Range/Subnet	Enter the IP address of the Finance network behind FortiGate_1 (for example, `192.168.150.0/24`).

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 Select the interface to the HR network. Destination Select the interface to the external (public) network.

Address Name	Source
	`HR_Network`
	Destination
	`Finance_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG2toFG1_Tunnel` Select Outbound NAT, which in combination with the `natip` CLI attribute, will replace the source addresses of IP packets sent through the tunnel with substitute IP addresses.

To refer to the substituted R&D network address

1 Go to **Firewall > Address**.

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

Address Name	Enter an address name (for example, `RD_Network`).
IP Range/Subnet	Enter the network address from which FG_Dialup may assign IP addresses to packets from the R&D network (for example, `10.30.10.0/24`).

To define the firewall encryption policy for FortiGate_2-to-FG_Dialup traffic

1 Go to **Firewall > Policy**.

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

Interface/Zone	Source Select the interface to the HR network. Destination Select the interface to the external (public) network.

Address Name	Source
	`HR_Network`
	Destination
	`RD_Network`

Schedule	As required.
Service	As required.

Action	ENCRYPT
VPN Tunnel	FG2toFG1_Tunnel Select Outbound NAT, which in combination with the natip CLI attribute, will replace the source addresses of IP packets sent through the tunnel with substitute IP addresses.

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

- encryption policies that control traffic between FortiGate_2 and the hub first
- the default firewall policy last

To define a substitute address for the quick mode selector

1 Go to **Firewall > Address**.

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

Address Name	Enter an address name (for example, Sub_HR_Network).
IP Range/Subnet	Enter the IP address that FortiGate_2 will use as a quick mode selector during phase 2 negotiations (for example, 10.20.10.0/24).

To specify the phase 2 quick mode selectors

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

2 Select the Edit icon in the row beside the phase 2 tunnel definition.

3 Select Advanced, enter the following information, and then select OK:

Quick Mode Identities	Select Specify a selector and enter appropriate values as follows:	
	Source address	Sub_HR_Network
	Source port	0 (all ports)
	Dest address	Finance_Network
	Dest port	0 (all ports)
	Protocol	0 (all protocol types)

To specify the replacement IP address to combine with outbound NAT

Enter the following CLI command to set the natip attribute on FortiGate_2:

```
config firewall policy
   edit 1
      set natip 10.20.10.0 255.255.255.0
   end
```

This setting will cause the IP source addresses of packets from the local 192.168.152.0/24 network to be converted to the 10.20.10.0/24 network address space.

Configuring FG_Dialup

The FG_Dialup 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 R&D network behind FG_Dialup (for example, `192.168.152.0/24`)
- a destination address that represents the Finance network behind the hub (for example, `192.168.150.0/24`)
- a firewall encryption policy to enable communications between FG_Dialup and the hub
- a destination address that corresponds to the IP addresses that FortiGate_2 may assign to packets from the HR network (for example, `10.20.10.0/24`)
- a firewall encryption policy to enable communications between FG_Dialup and FortiGate_2 through the hub
- a replacement address, to be used as an IPSec phase 2 quick mode selector in the phase 2 exchange (for example, `10.30.10.0/24`)

In addition, to ensure that packets from the R&D network have an unambiguous source IP address, you must enable subnet-address translation on outbound packets through the Outbound NAT option in the firewall encryption policy in conjunction with the `set natip` attribute of the `config firewall policy` command. Afterward, if the IP source address of a packet leaving the R&D network is 192.168.152.5/24 and the `natip` value is 10.30.10.0/24, the source address will be translated to 10.30.10.5.

To define the phase 1 parameters

1. At FG_Dialup, go to **VPN > IPSEC > Phase 1**.
2. Select Create New, and then select Advanced.
3. 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	`172.16.87.183`
Mode	Aggressive
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key. The value must be identical to the preshared key that you specified previously for FG_Dialup in the FortiGate_1 configuration.
Peer Options	Accept any peer ID
Advanced	In the Local ID field, type the identifier that you reserved for FG_Dialup (for example, `FG_Dialup`). The value must be identical to the peer ID that you specified previously in the FortiGate_1 configuration.

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, `FGDialuptoFG1_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 FG_Dialup

1 Go to **Firewall > Address**.

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

Address Name	Enter an address name (for example, `RD_Network`).
IP Range/Subnet	Enter the IP address of the private network behind FG_Dialup (for example, `192.168.152.0/24`).

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, `Finance_Network`).
IP Range/Subnet	Enter the IP address of the Finance network behind FortiGate_1 (for example, `192.168.150.0/24`).

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 Select the interface to the R&D network. Destination Select the interface to the external (public) network.

Address Name	Source
	`RD_Network`
	Destination
	`Finance_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FGDialuptoFG1_Tunnel` Select Outbound NAT, which in combination with the `natip` CLI attribute, will replace the source addresses of IP packets sent through the tunnel with substitute IP addresses.

To refer to the substituted HR network address

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 network address from which FortiGate_2 may assign IP addresses to packets from the HR network (for example, `10.20.10.0/24`).

To define the firewall encryption policy for FG_Dialup-to-FortiGate_2 traffic

1 Go to **Firewall > Policy**.

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

Interface/Zone	Source Select the interface to the R&D network. Destination Select the interface to the external (public) network.

Address Name	Source
	`RD_Network`
	Destination
	`HR_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FGDialuptoFG1_Tunnel` Select Outbound NAT, which in combination with the `natip` CLI attribute, will replace the source addresses of IP packets sent through the tunnel with substitute IP addresses.

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

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

To define a substitute address for the quick mode selector

1 Go to **Firewall > Address**.

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

Address Name	Enter an address name (for example, `Sub_RD_Network`).
IP Range/Subnet	Enter the IP address that FG_Dialup will use as a quick mode selector during phase 2 negotiations (for example, `10.30.10.0/24`).

To specify the phase 2 quick mode selectors

1. Go to **VPN > IPSEC > Phase 2**.
2. Select the Edit icon in the row beside the phase 2 tunnel definition.
3. Select Advanced, enter the following information, and then select OK:

Quick Mode Identities	Select Specify a selector and enter appropriate values as follows:	
	Source address	`Sub_RD_Network`
	Source port	`0` (all ports)
	Dest address	`Finance_Network`
	Dest port	`0` (all ports)
	Protocol	`0` (all protocol types)

To specify the replacement IP address to combine with outbound NAT

Enter the following CLI command to set the `natip` attribute on FG_Dialup:

```
config firewall policy
   edit 1
      set natip 10.30.10.0 255.255.255.0
   end
```

This setting will cause the IP source addresses of packets from the local 192.168.152.0/24 network to be converted to the 10.30.10.0/24 network address space.