Hub-and-spoke IPSec VPN Example

Technical Note

Hub-and-spoke IPSec VPN Example Technical Note	
Document Version:	Version 2
Publication Date:	4 July 2005
Description:	This technical note features a detailed configuration example that demonstrates how to set up a basic hub-and-spoke IPSec VPN that uses preshared keys to authenticate VPN peers.
Product:	FortiGate v2.80 MR10
Document Number:	01-28010-0120-20050704

Fortinet Inc.

Hub-and-spoke IPSec VPN Example Technical Note
FortiGate v2.80 MR10
4 July 2005
01-28010-0120-20050704

Table of Contents

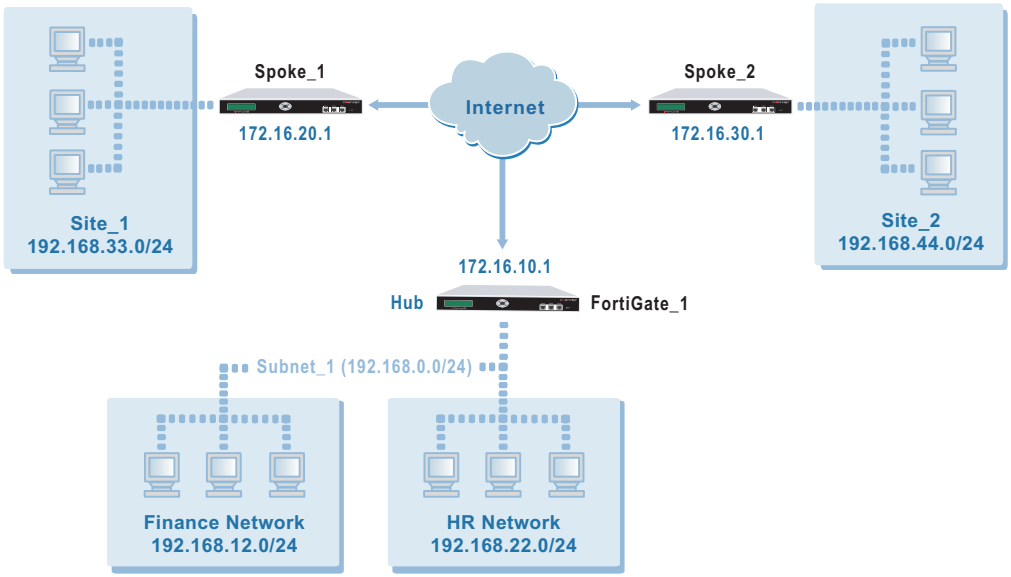
This technical note features a detailed configuration example that demonstrates how to set up a basic hub-and-spoke IPSec VPN that uses preshared keys to authenticate VPN peers. The following sections are included:

Network topology

In a hub-and-spoke configuration, connections to a number of remote peers radiate from a single, central FortiGate unit. Site-to-site connections between the remote peers do not exist; however, VPN tunnels between any two of the remote peers 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 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



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, and the HR Network. The Finance network is not included in the VPN.

Infrastructure requirements

- All FortiGate units must be operating in NAT mode and have static public IP addresses.

Note: Many hub-and-spoke configurations require static IP addresses. However, a spoke may have a dynamic IP address, or a static domain name and dynamic IP address. For more information, contact Fortinet Technical Support.

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 the FortiGate unit needs to authenticate the spokes and establish secure connections. See “Define the phase 1 parameters” on page 6.
- 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 7.
- Create one firewall encryption policy for each spoke and define the scope of permitted services between the hub and each spoke. See “Define the firewall encryption policies” on page 8.
- Define the VPN concentrator, which determines the spokes to include in the configuration. See “Define the VPN concentrator” on page 10.

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 will be used to authenticate the spokes.

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

- Reserve a name for each spoke.
- Obtain the IP address of the public interface to each spoke.
- Reserve a unique preshared key for each tunnel.

You need one preshared key to authenticate Spoke_1 and a different preshared key to authenticate Spoke_2. 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

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`).

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 source IP address corresponds to the HR network behind FortiGate_1.
- The destination IP addresses refer to the private networks behind Spoke_1 and Spoke_2.

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

Address Name	Source
	`HR_Network`
	Destination
	`Site_1`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG1toSP1_Tunnel`

3 Place the policy in the policy list above any other policies having similar source and destination addresses.

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

Address Name	Source
	`HR_Network`
	Destination
	`Site_2`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG1toSP2_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

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. 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

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 Select the interface to the internal (private) network. Destination Select the interface to the external (public) network.

Address Name	Source
	`Site_1`
	Destination
	`HR_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`SP1toFG1_Tunnel`

3 Place the policy in the policy list above any other policies having similar source and destination addresses.

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 Select the interface to the internal (private) network. Destination Select the interface to the external (public) network.

Address Name	Source
	`Site_1`
	Destination
	`Site_2`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`SP1toFG1_Tunnel`

3 Place the policy in the policy list above any other policies having similar source and destination addresses.

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

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 Select the interface to the internal (private) network. Destination Select the interface to the external (public) network.

Address Name	Source
	`Site_2`
	Destination
	`HR_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`SP2toFG1_Tunnel`

3 Place the policy in the policy list above any other policies having similar source and destination addresses.

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 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 Select the interface to the internal (private) network. Destination Select the interface to the external (public) network.

Address Name	Source
	`Site_2`
	Destination
	`Site_1`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`SP2toFG1_Tunnel`

3 Place the policy in the policy list above any other policies having similar source and destination addresses.