Gateway-to-gateway IPSec VPN Example

Technical Note

Gateway-to-gateway IPSec VPN Example Technical Note	
Document Version:	Version 1
Publication Date:	22 October 2004
Description:	This technical note features a detailed configuration example that demonstrates how to set up a basic gateway-to-gateway IPSec VPN that uses preshared keys to authenticate the two VPN peers.
Product:	FortiGate v2.80 MR6
Document Number:	01-28006-0119-20041022

Fortinet Inc.

Gateway-to-gateway IPSec VPN Example Technical Note
FortiGate v2.80 MR6
22 October 2004
01-28006-0119-20041022

Table of Contents

Network topology 5
Infrastructure requirements 5
Configuring FortiGate_1.. 6
Define the phase 1 parameters.. 6
Define the phase 2 parameters.. 7
Define the firewall encryption policy.. 7
Configuring FortiGate_2.. 8

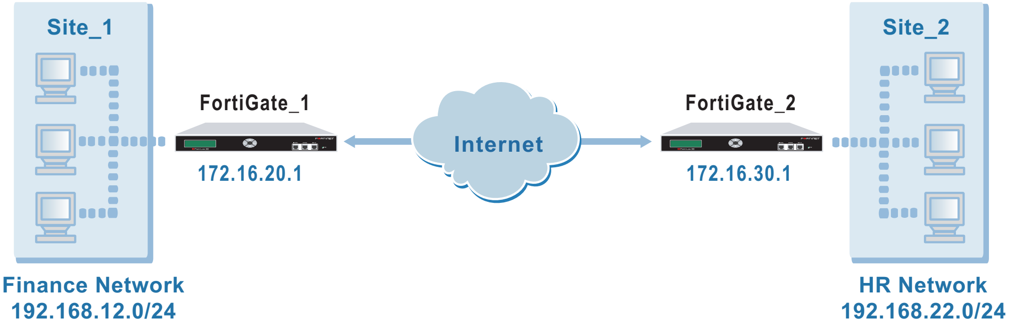
This technical note features a detailed configuration example that demonstrates how to set up a basic gateway-to-gateway IPSec VPN that uses preshared keys to authenticate the two VPN peers. The following sections are included:

- Network topology
- Configuring FortiGate_1
- Configuring FortiGate_2

Network topology

In a gateway-to-gateway configuration, two FortiGate units create an IPSec tunnel between two separate private networks. All traffic between the two networks is encrypted and protected by FortiGate firewall policies. See Figure 1.

Figure 1: Example gateway-to-gateway configuration



In the examples throughout this technical bulletin, the network devices are assigned IP addresses as shown in Figure 1.

Infrastructure requirements

- The FortiGate units at both ends of the tunnel must be operating in NAT mode and have static public IP addresses.

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 both FortiGate units:

- Define the phase 1 parameters that the FortiGate unit needs to authenticate the remote peer and establish a secure connection.
- Define the phase 2 parameters that the FortiGate unit needs to create a VPN tunnel with the remote peer.
- Create a firewall encryption policy to control the permitted services and permitted direction of traffic between the IP source and destination addresses. A single encryption policy controls both inbound and outbound IP traffic through the VPN tunnel.

Define the phase 1 parameters

The phase 1 configuration defines the parameters that FortiGate_1 will use to authenticate FortiGate_2 and establish a secure connection. For the purposes of this example, a preshared key will be used to authenticate FortiGate_2. The same preshared key must be specified at both FortiGate units.

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

- Reserve a name for the remote gateway.
- Obtain the IP address of the public interface to the remote peer.
- Reserve a unique value for the preshared key.

The key must contain at least 6 printable characters and should only be known by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.

To define the phase 1 parameters

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 remote gateway (for example, `FortiGate_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 point of the VPN tunnel. Before you define the phase 2 parameters, you need to reserve a name for the tunnel.

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, `FG1toFG2_Tunnel`).
Remote Gateway	Select the gateway that you defined previously (for example, `FortiGate_2`).

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 a gateway-to-gateway configuration:

- The source IP address corresponds to the private network behind the local FortiGate unit.
- The destination IP address refers to the private network behind the remote VPN peer.

To define the IP source address of the network behind FortiGate_1

1 Go to **Firewall > Address > 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, `192.168.12.0/24`).

To specify the destination address of IP packets delivered to FortiGate_2

1 Go to **Firewall > Address > 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, `192.168.22.0/24`).

To define the firewall encryption policy

1. Go to **Firewall > Policy > 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
	`Finance_Network`
	Destination
	`HR_Network`

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

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

Configuring FortiGate_2

The configuration of FortiGate_2 is similar to that of FortiGate_1. You must:

- Define the phase 1 parameters that FortiGate_2 needs to authenticate FortiGate_1 and establish a secure connection.
- Define the phase 2 parameters that FortiGate_2 needs to create a VPN tunnel with FortiGate_1.
- Create a firewall encryption policy and define the scope of permitted services between the IP source and destination addresses.

To define the phase 1 parameters

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 remote gateway (for example, `FortiGate_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. 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, `FG2toFG1_Tunnel`).
Remote Gateway	Select the gateway that you defined previously (for example, `FortiGate_1`).

To define the IP source address of the network behind FortiGate_2

1. Go to **Firewall > Address > 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, `192.168.22.0/24`).

To specify the destination address of IP packets delivered to FortiGate_1

1. Go to **Firewall > Address > 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, `192.168.12.0/24`).

To define the firewall encryption policy

1. Go to **Firewall > Policy > 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
	`HR_Network`
	Destination
	`Finance_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG2toFG1_Tunnel`

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