Redundant-tunnel IPSec VPN Example

Technical Note

Redundant-tunnel IPSec VPN Example Technical Note	
Document Version:	Version 1
Publication Date:	3 December 2004
Description:	This technical note features a detailed configuration example that demonstrates how to set up a redundant-tunnel IPSec VPN that uses preshared keys for authentication purposes.
Product:	FortiGate v2.80 MR7
Document Number:	01-28007-0136-20041203

Fortinet Inc.

Redundant-tunnel IPSec VPN Example Technical Note
FortiGate v2.80 MR7
3 December 2004
01-28007-0136-20041203

Table of Contents

Network topology 5
Infrastructure requirements 6
Configuring FortiGate_1 6
Define the phase 1 parameters 6
Define the phase 2 parameters 8
Define the firewall encryption policies 9
Configuring the ping servers 10
Configuring FortiGate_2 11

This technical note features a detailed configuration example that demonstrates how to set up a redundant-tunnel IPSec VPN that uses preshared keys for authentication purposes. The following sections are included:

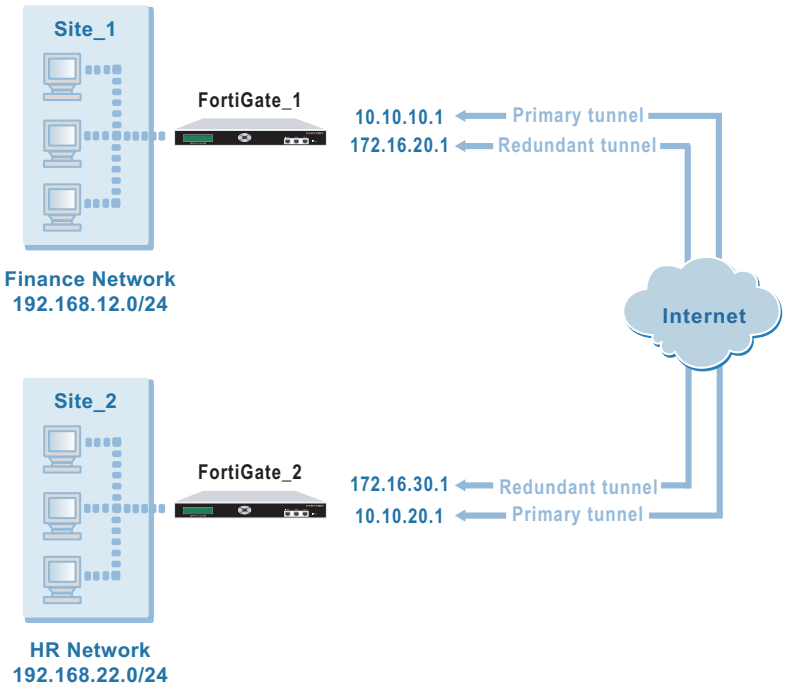
- Network topology
- Configuring FortiGate_1
- Configuring FortiGate_2

Network topology

A FortiGate unit can be configured to support redundant tunnels to the same remote peer if the FortiGate unit has more than one interface to the Internet. The remote peer must also have the same number of Internet connections.

When more than one public FortiGate interface is available, more than one VPN tunnel can be configured to ensure that a remote peer can access the FortiGate unit should the primary connection fail. If the primary connection fails, the FortiGate unit can establish a tunnel using the redundant connection.

Figure 1: Example redundant-tunnel configuration



In the example configuration, two separate interfaces to the Internet are available on both VPN peers.

Infrastructure requirements

- Both VPN peers must have at least two public interfaces and have static IP addresses for each public interface.
- Both VPN peers must be operating in NAT/Route mode.

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 the FortiGate unit:

- Define the phase 1 parameters that the FortiGate unit needs to authenticate the remote peer and establish a secure connection. See “Define the phase 1 parameters” on page 6.
- Define the phase 2 parameters that the FortiGate unit needs to create a VPN tunnel with the remote peer. See “Define the phase 2 parameters” on page 8.
- Create firewall encryption policies to control the permitted services and permitted direction of traffic between the IP source address and the IP destination address. See “Define the firewall encryption policies” on page 9.
- Configure ping servers on the local interfaces to enable the FortiGate unit to determine whether the remote interfaces are accessible. If one of the tunnels fails, a response will not be received and the FortiGate until will fail over to the other tunnel. See “Configuring the ping servers” on page 10.

The redundant-tunnel configuration on FortiGate_1 must include:

- one set of phase 1 parameters for the primary remote interface, and another set for the redundant remote interface
- one phase 2 definition for the primary tunnel and another for the redundant tunnel
- one firewall encryption policy per local interface — a single encryption policy per interface controls both inbound and outbound IP traffic through the VPN tunnel
- a ping server configured on each local interface

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 primary remote interface.
- Reserve a name for the redundant remote interface.
- Obtain the IP addresses of the two remote interfaces.
- 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 for the primary remote interface

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

2 Select Create New, enter the following information for the primary interface of the remote peer, and select OK:

Gateway Name	Type a name for the primary remote interface (for example, `FortiGate_2_primary`).
Remote Gateway	Static IP Address
IP Address	`10.10.20.1`
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	Select Dead Peer Detection.

To define the phase 1 parameters for the redundant remote interface

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

2 Select Create New, enter the following information for the redundant interface of the remote peer, and select OK:

Gateway Name	Type a name for the redundant remote interface (for example, `FortiGate_2_redundant`).
Remote Gateway	Static IP Address
IP Address	`172.16.30.1`
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 for the primary remote interface.
Peer Options	Accept any peer ID
Advanced	Select Dead Peer Detection.

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 each tunnel. One phase 2 definition is needed for the primary tunnel, and another is needed for the redundant tunnel.

To define the phase 2 parameters for the primary tunnel

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

2 Select Create New and enter the following information:

Tunnel Name	Enter a name for the primary tunnel (for example, `FG1toFG2_PTunnel`).
Remote Gateway	Select the primary remote interface that you defined previously (for example, `FortiGate_2_primary`).

3 Select OK.

4 Enter the following CLI command to bind the tunnel to the local FortiGate_1 interface to the private network:

```
config vpn ipsec phase2
  edit FG1toFG2_PTunnel
  set bindtoif <interface-name_str>
  end
```

For `interface-name_str`, enter the name of the interface that the tunnel connects to the VPN.

To define the phase 2 parameters for the redundant tunnel

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

2 Select Create New and enter the following information:

Tunnel Name	Enter a name for the tunnel (for example, `FG1toFG2_RTunnel`).
Remote Gateway	Select the primary remote interface that you defined previously (for example, `FortiGate_2_redundant`).

3 Select OK.

4 Enter the following CLI command to bind the tunnel to the local FortiGate_1 interface to the private network:

```
config vpn ipsec phase2
  edit FG1toFG2_RTunnel
  set bindtoif <interface-name_str>
  end
```

For `interface-name_str`, enter the same interface name that you specified previously in Step 4 for the primary tunnel.

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 for each interface in the redundant-tunnel configuration 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 per interface is needed to control both inbound and outbound IP traffic through the VPN tunnel.

Before you define the policies, you must first specify the associated IP source and destination addresses. The source addresses specified in both firewall encryption policies must be identical. Similarly, the destination addresses specified in both firewall encryption policies must be identical. In both cases:

- 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**.

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**.

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 for the local primary interface

1 Go to **Firewall > Policy**.

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

Interface/Zone	Source Select the local interface to the internal (private) network. Destination Select the local primary interface to the Internet.

Address Name	Source
	`Finance_Network`
	Destination
	`HR_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG1toFG2_PTunnel`

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 the local redundant interface

1 Go to **Firewall > Policy**.

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

Interface/Zone	Source Select the local interface to the internal (private) network. Destination Select the local redundant interface to the Internet.

Address Name	Source
	`Finance_Network`
	Destination
	`HR_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG1toFG2_RTunnel`

3 Place the policy in the policy list directly beneath the policy that you created for the primary interface.

Configuring the ping servers

When you enable ping servers on the local interfaces, ping commands are sent periodically to the remote interfaces that you specify. If a response is not received, the FortiGate unit switches over to the redundant tunnel automatically.

The procedure below configures FortiGate_1 to ping the public interfaces of FortiGate_2. This configuration ensures that the entire path between FortiGate_1 and FortiGate_2 is tested.

Note: If required for your situation, you may ping an ISP gateway or another major gateway instead. When you specify an ISP gateway or another major gateway, the tunnel fails over when the specified gateway fails to respond.

To add a ping server to the local primary interface

1 Go to **System > Network > Interface**.

2 In the row that corresponds to the primary interface, select the Edit button.

3 In the Ping Server field, type the IP address of the primary remote interface on FortiGate_2.

4 Select Enable.

5 In the Administrative Access group, ensure that PING is selected.

6 Select OK.

To add a ping server to the local redundant interface

1 Go to **System > Network > Interface**.

2 In the row that corresponds to the redundant interface, select the Edit button.

3 In the Ping Server field, type the IP address of the redundant remote interface on FortiGate_2.

4 Select Enable.

5 In the Administrative Access group, ensure that PING is selected.

6 Select OK.

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 for each interface in the redundant-tunnel configuration and define the scope of permitted services between the IP source and destination addresses.
- Configure ping servers on the local interfaces to enable FortiGate_2 to determine whether the FortiGate_1 interfaces are accessible.

To define the phase 1 parameters for the primary remote interface

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

2 Select Create New, enter the following information for the primary interface of the remote peer, and select OK:

Gateway Name	Type a name for the primary remote interface (for example, `FortiGate_1_primary`).
Remote Gateway	Static IP Address
IP Address	`10.10.10.1`
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
Advanced	Select Dead Peer Detection.

To define the phase 1 parameters for the redundant remote interface

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

2 Select Create New, enter the following information for the redundant interface of the remote peer, and select OK:

Gateway Name	Type a name for the redundant remote interface (for example, `FortiGate_1_redundant`).
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
Advanced	Select Dead Peer Detection.

To define the phase 2 parameters for the primary tunnel

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

2 Select Create New and enter the following information:

Tunnel Name	Enter a name for the primary tunnel (for example, `FG2toFG1_PTunnel`).
Remote Gateway	Select the primary remote interface that you defined previously (for example, `FortiGate_1_primary`).

3 Select OK.

4 Enter the following CLI command to bind the tunnel to the local FortiGate_2 interface to the private network:

```
config vpn ipsec phase2
  edit FG2toFG1_PTunnel
  set bindtoif <interface-name_str>
  end
```

For `interface-name_str`, enter the name of the interface that the tunnel connects to the VPN.

To define the phase 2 parameters for the redundant tunnel

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

2 Select Create New and enter the following information:

Tunnel Name	Enter a name for the tunnel (for example, `FG2toFG1_RTunnel`).
Remote Gateway	Select the primary remote interface that you defined previously (for example, `FortiGate_1_redundant`).

3 Select OK.

4 Enter the following CLI command to bind the tunnel to the local FortiGate_2 interface to the private network:

```
config vpn ipsec phase2
  edit FG2toFG1_RTunnel
  set bindtoif <interface-name_str>
  end
```

For `interface-name_str`, enter the same interface name that you specified previously in Step 4 for the primary tunnel.

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, `192.168.22.0/24`).

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 private network behind FortiGate_1 (for example, `192.168.12.0/24`).

To define the firewall encryption policy for the local primary interface

1 Go to **Firewall > Policy**.

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

Interface/Zone	Source Select the local interface to the internal (private) network. Destination Select the local primary interface to the Internet.

Address Name	Source
	`HR_Network`
	Destination
	`Finance_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG2toFG1_PTunnel`

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 the local redundant interface

1 Go to **Firewall > Policy**.

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

Interface/Zone	Source Select the local interface to the internal (private) network. Destination Select the local redundant interface to the Internet.

Address Name	Source
	`HR_Network`
	Destination
	`Finance_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG2toFG1_RTunnel`

3 Place the policy in the policy list directly beneath the policy that you created for the primary interface.

To add a ping server to the local primary interface

1. Go to **System > Network > Interface**.
2. In the row that corresponds to the primary interface, select the Edit button.
3. In the Ping Server field, type the IP address of the primary remote interface on FortiGate_1.
4. Select Enable.
5. In the Administrative Access group, ensure that PING is selected.
6. Select OK.

To add a ping server to the local redundant interface

1. Go to **System > Network > Interface**.
2. In the row that corresponds to the redundant interface, select the Edit button.
3. In the Ping Server field, type the IP address of the redundant remote interface on FortiGate_1.
4. Select Enable.
5. In the Administrative Access group, ensure that PING is selected.
6. Select OK.