Partially Redundant IPSec VPN Tunnel Example

Technical Note

Partially Redundant IPSec VPN Tunnel Example Technical Note	
Document Version:	Version 1
Publication Date:	15 July 2005
Description:	This technical note demonstrates how to set up a partially redundant IPSec VPN tunnel between a local FortiGate unit and a remote FortiGate unit that receives a dynamic IP address from an ISP before it connects to the local FortiGate unit. In the example, both FortiGate units use preshared keys for authentication purposes, and the FortiGate dialup client identifies itself using a unique identifier (peer ID).
Product:	FortiGate v2.80 MR10
Document Number:	01-28010-0140-20050715

Fortinet Inc.

Partially Redundant IPSec VPN Tunnel Example Technical Note
FortiGate v2.80 MR7
15 July 2005
01-28010-0140-20050715

Table of Contents

Partially Redundant IPSec VPN Tunnel Example

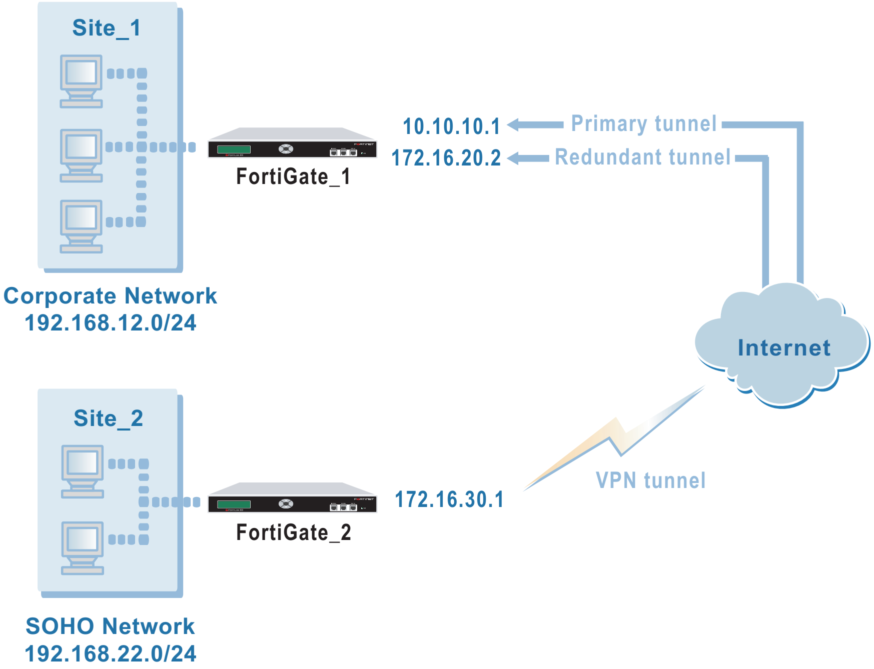
This technical note demonstrates how to set up a partially redundant IPSec VPN tunnel between a local FortiGate unit and a remote FortiGate unit that receives a dynamic IP address from an ISP before it connects to the local FortiGate unit. In the example, both FortiGate units use preshared keys for authentication purposes, and the FortiGate dialup client identifies itself using a unique identifier (peer ID).

The following sections are included:

Network topology

When a FortiGate unit has more than one interface to the Internet (for example, see FortiGate_1 in Figure 1), you can configure redundant tunnels—if the primary connection fails, the FortiGate unit can establish a tunnel using the redundant connection.

Figure 1: Example partially redundant tunnel configuration



However, a FortiGate unit such as a FortiGate dialup client may have only one connection to the Internet. If the link to the ISP were to go down, the connection to FortiGate_1 would be lost, and the tunnel would be taken down. The tunnel is said to be partially redundant because FortiGate_2 does not support a redundant connection.

This technical note provides a detailed example of how to configure a partially redundant tunnel based on the network scenario shown in Figure 1. In the configuration example:

- Both VPN peers operate in NAT/Route mode.
- Two separate interfaces to the Internet (10.10.10.1 and 172.16.20.2) are available on FortiGate_1. Each interface has a static public IP address.
- FortiGate_2 has a single connection to the Internet and obtains a dynamic public IP address (for example, 172.16.30.1) when it connects to the Internet.
- FortiGate_2 forwards IP packets from the SOHO network (192.168.22.0/24) to the corporate network (192.168.12.0/24) behind FortiGate_1 through a partially redundant IPSec VPN tunnel. Encrypted packets from FortiGate_2 are addressed to the public interface of the FortiGate unit. Encrypted packets from the FortiGate unit are addressed to the public IP address of FortiGate_2.

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 dialup server needs to authenticate the dialup client and establish a secure connection. See “Define the phase 1 parameters” on page 6.
- Define the phase 2 parameters that the dialup server needs to create a VPN tunnel with the dialup client. See “Define the phase 2 parameters” on page 7.
- Create firewall encryption policies to control the permitted services and permitted direction of traffic between the IP source address and the IP destination address. A single encryption policy per interface controls both inbound and outbound IP traffic through the VPN tunnel. See “Define the firewall encryption policies” on page 8.
- Configure a ping server on each local interface. See “Configuring the ping servers” on page 10.

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.

In addition, a peer ID for FortiGate_2 is added to the FortiGate_1 configuration to provide additional VPN connection security — the tunnel will be initiated only by FortiGate_2 when FortiGate_2 attempts to connect to FortiGate_1.

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

- Reserve a name for the phase 1 configuration.
- 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.
- Reserve a unique identifier for FortiGate_2 to identify itself to FortiGate_1. You will record the value in the FortiGate_1 configuration as described below and will need to assign the value to FortiGate_2 when you configure FortiGate_2 (see "Configuring FortiGate_2" on page 11).

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_2GW`).
Remote Gateway	Dialup User
Mode	Main
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 FortiGate_2 (for example, `FortiGate_2`).
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 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_2GW`).

3 Enter the following CLI command to bind the tunnel to the primary FortiGate_1 interface:

```
config vpn ipsec phase2
   edit FG1toFG2_Tunnel
      set bindtoif <interface-name_str>
   end
```

For `interface-name_str`, enter the name of the primary FortiGate_1 interface to the Internet (for example, `external` or `wan1`).

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 corporate network behind FortiGate_1 (for example, 192.168.12.0/24).
- The destination IP address refers to the SOHO network behind FortiGate_2 (for example, 192.168.22.0/24).

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, `Corporate_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, `SOHO_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
	`Corporate_Network`
	Destination
	`SOHO_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG1toFG2_Tunnel` Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Clear Allow outbound to prevent traffic from the local network from initiating the tunnel after the tunnel has been established.

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
	`Corporate_Network`
	Destination
	`SOHO_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG1toFG2_Tunnel` Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Clear Allow outbound to prevent traffic from the local network from initiating the tunnel after the tunnel has been established.

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 a ping server on a local interface, ICMP Echo messages are sent to the IP address that you specify to determine if a remote host is active.

Optimally, FortiGate_1 would be configured to ping FortiGate_2 to ensure that the entire path between FortiGate_1 and FortiGate_2 is tested. However, because the public IP address of FortiGate_2 is assigned dynamically when FortiGate_2 establishes a connection to the Internet (that is, the IP address is not known ahead of time), you cannot configure FortiGate_1 to ping FortiGate_2 directly. Instead, you may configure FortiGate_1 to ping an ISP gateway between FortiGate_1 and FortiGate_2. When you specify an ISP 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 public IP address of the ISP gateway.
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 public IP address of the same gateway that you specified for the primary interface.
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. You need one set of phase 1 parameters for the primary FortiGate_1 gateway, and another set for the redundant FortiGate_1 gateway.
- Define the phase 2 parameters that FortiGate_2 needs to create a VPN tunnel with FortiGate_1. You need one phase 2 definition that specifies both the primary and redundant FortiGate_1 gateways.
- Create a firewall encryption policy to define the scope of permitted services between the IP source and destination addresses. A single encryption policy is needed to control both inbound and outbound IP traffic through the VPN tunnel.

To define the phase 1 parameters for the primary FortiGate_1 gateway

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 primary FortiGate_1 gateway (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	Set these Advanced options: • In the Local ID field, type the identifier that you reserved for FortiGate_2 (for example, `FortiGate_2`). The value must be identical to the peer ID that you specified previously in the FortiGate_1 configuration. • Select Dead Peer Detection.

To define the phase 1 parameters for the redundant FortiGate_1 gateway

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 redundant FortiGate_1 gateway (for example, `FortiGate_1_redundant`).
Remote Gateway	Static IP Address
IP Address	`172.16.20.2`
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	Set these Advanced options: • In the Local ID field, type the identifier that you reserved for FortiGate_2 (for example, `FortiGate_2`). The value must be identical to the peer ID that you specified previously in the FortiGate_1 configuration. • Select Dead Peer Detection.

To define the phase 2 parameters

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_Tunnel`).
Remote Gateway	Select the primary remote gateway that you defined previously (for example, `FortiGate_1_primary`).

3 Select the add button beside the Remote Gateway list.

4 From the second list, select the redundant remote gateway (for example, `FortiGate_1_redundant`).

5 Select OK.

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, `SOHO_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, `Corporate_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**.

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 interface to the Internet.

Address Name	Source
	`SOHO_Network`
	Destination
	`Corporate_Network`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`FG2toFG1_Tunnel` Clear Allow inbound to prevent traffic from the remote network from initiating the tunnel after the tunnel has been established. Select Allow outbound to enable traffic from the local network to initiate the tunnel.

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