USER GUIDE

FortiGate™ IPSec VPN
Version 3.0 MR5

FORTINET

www.fortinet.com

FortiGate™ IPSec VPN User Guide
Version 3.0
16 July 2007
01-30005-0065-20070716

Trademarks

Contents

Introduction

This chapter introduces you to FortiGate VPNs and the following topics:

- About FortiGate IPSec VPNs
- About this document
- Fortinet documentation
- Customer service and technical support

About FortiGate IPSec VPNs

A virtual private network (VPN) is a way to use a public network, such as the Internet, to provide remote offices or individual users with secure access to private networks. For example, a company that has two offices in different cities, each with its own private network, can use a VPN to create a secure tunnel between the offices. Similarly, telecommuters can use VPN clients to access private data resources securely from a remote location.

With the FortiGate unit's built-in VPN capabilities, small home offices, medium-sized businesses, enterprises, and service providers can ensure the confidentiality and integrity of data transmitted over the Internet. The FortiGate unit provides enhanced authentication, strong encryption, and restricted access to company network resources and services.

FortiGate units support Internet Protocol Security (IPSec), a framework for the secure exchange of packets at the IP layer, to authenticate and encrypt traffic. FortiGate units implement the Encapsulated Security Payload (ESP) protocol in tunnel mode. The encrypted packets look like ordinary packets that can be routed through any IP network. Internet Key Exchange (IKE) is performed automatically based on preshared keys or X.509 digital certificates. As an option, you can specify manual keys.

The FortiGate IPSec VPN feature is compatible with the VPN client feature of the FortiClient Host Security application. A FortiGate unit can act as a policy server, enabling FortiClient users to download and apply VPN settings automatically.

Because FortiGate units support industry standard IPSec VPN technologies, you can configure an IPSec VPN between a FortiGate unit and most third-party IPSec VPN devices or clients. There are articles about interoperation with some specific third-party devices on the Fortinet Knowledge Center. Otherwise, for more information about FortiGate VPN interoperability, contact Fortinet™ Technical Support.

Using the web-based manager and CLI to configure IPSec VPNs

The FortiGate unit provides two user interfaces to configure operating parameters: the web-based manager, and the Command Line Interface (CLI).

In the web-based manager:

- IPSec VPN operating parameters are located on the following tabs:
  - **VPN > IPSEC > Auto Key (IKE)**
  - **VPN > IPSEC > Manual Key**
  - **VPN > IPSEC > Concentrator**
  - **VPN > Certificates**

In the CLI, the following commands are available to configure comparable VPN settings:

- `config vpn ipsec phase1`
- `config vpn ipsec phase1-interface`
- `config vpn ipsec phase2`
- `config vpn ipsec phase2-interface`
- `config vpn ipsec manualkey`
- `config vpn ipsec manualkey-interface`
- `config vpn ipsec concentrator`
- `config vpn ipsec forticlient`
- `config vpn certificate`
- `execute vpn certificate`

For detailed information about these CLI commands, refer to the “vpn” and “execute” chapters of the *FortiGate CLI Reference*.

About this document

Where possible, this document explains how to configure VPNs using the web-based manager. A few options can be configured only through the CLI. You can also configure VPNs entirely through the CLI. For detailed information about CLI commands, see the *FortiGate CLI Reference*.

This document contains the following chapters:

- Configuring IPSec VPNs provides a brief overview of IPSec technology and includes general information about how to configure IPSec VPNs using this guide.
- Gateway-to-gateway configurations explains how to set up a basic gateway-to-gateway (site-to-site) IPSec VPN. In a gateway-to-gateway configuration, two FortiGate units create a VPN tunnel between two separate private networks.
- Hub-and-spoke configurations describes how to set up hub-and-spoke IPSec VPNs. In a hub-and-spoke configuration, connections to a number of remote peers and/or clients radiate from a single, central FortiGate hub.
- Dynamic DNS configurations describes how to configure a site-to-site VPN, in which one FortiGate unit has a static IP address and the other FortiGate unit has a static domain name and a dynamic IP address.

- FortiClient dialup-client configurations guides you through configuring a FortiClient dialup-client IPSec VPN. In a FortiClient dialup-client configuration, the FortiGate unit acts as a dialup server and VPN client functionality is provided by the FortiClient Host Security application installed on a remote host.
- FortiGate dialup-client configurations explains how to set up a FortiGate dialup-client IPSec VPN. In a FortiGate dialup-client configuration, a FortiGate unit with a static IP address acts as a dialup server and a FortiGate unit having a dynamic IP address initiates a VPN tunnel with the FortiGate dialup server.
- Internet-browsing configuration explains how to support secure web browsing performed by dialup VPN clients, and/or hosts behind a remote VPN peer. Remote users can access the private network behind the local FortiGate unit and browse the Internet securely. All traffic generated remotely is subject to the firewall policy that controls traffic on the private network behind the local FortiGate unit.
- Redundant VPN configurations discusses the options for supporting redundant and partially redundant tunnels in an IPSec VPN configuration. 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.
- Transparent mode VPNs describes transparent VPN configurations, in which two FortiGate units create a VPN tunnel between two separate private networks transparently. In Transparent mode, all interfaces of the FortiGate unit except the management interface are invisible at the network layer.
- Manual-key configurations explains how to manually define cryptographic keys to establish an IPSec VPN tunnel. If one VPN peer uses specific authentication and encryption keys to establish a tunnel, both VPN peers must be configured to use the same encryption and authentication algorithms and keys.
- IPv6 IPSec VPNs describes FortiGate unit VPN capabilities for networks based on IPv6 addressing. This includes IPv4-over-IPv6 and IPv6-over-IPv4 tunnelling configurations.
- Auto Key phase 1 parameters provides detailed step-by-step procedures for configuring a FortiGate unit to accept a connection from a remote peer or dialup client. The basic phase 1 parameters identify the remote peer or clients and support authentication through preshared keys or digital certificates. You can increase VPN connection security further using peer identifiers, certificate distinguished names, group names, or the FortiGate extended authentication (XAuth) option for authentication purposes.
- Phase 2 parameters provides detailed step-by-step procedures for configuring an IPSec VPN tunnel. During phase 2, the specific IPSec security associations needed to implement security services are selected and a tunnel is established.
- Defining firewall policies explains how to specify the source and destination IP addresses of traffic transmitted through an IPSec VPN tunnel, and how to define a firewall encryption policy. Firewall policies control all IP traffic passing between a source address and a destination address.
- Monitoring and testing VPNs provides some general monitoring and testing procedures for VPNs.

Document conventions

The following document conventions are used in this guide:

- In the examples, private IP addresses are used for both private and public IP addresses.
- Notes and Cautions are used to provide important information:

Note: Highlights useful additional information.

Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Typographic conventions

FortiGate documentation uses the following typographical conventions:

Convention	Example
Keyboard input	In the Gateway Name field, type a name for the remote VPN peer or client (for example, `Central_Office_1`).

Code examples	`config vpn ipsec phase2`
	`   edit FG1toDialupClients`
	`      set single-source enable`
	`   end`

CLI command syntax	`config vpn ipsec phase2`
	`   edit <tunnel_name>`
	`     set single-source enable`
	`   end`

Document names	*FortiGate Administration Guide*
File content	`<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>`
Menu commands	Go to **VPN > IPSEC > Auto Key** and select Create Phase 1.
Program output	`Initiator: tunnel 172.16.20.143, transform=ESP_3DES, HMAC_SHA1`
Variables	`<tunnel_name>`

Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at http://docs.forticare.com.

The following FortiGate product documentation is available:

- *FortiGate QuickStart Guide*

  Provides basic information about connecting and installing a FortiGate unit.

- *FortiGate Installation Guide*

  Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*

  Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*

  Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference*

  Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference*

  Available exclusively from the Fortinet Knowledge Center, the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability User Guide*

  Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS User Guide*

  Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate IPSec VPN User Guide*

  Provides step-by-step instructions for configuring IPSec VPNs using the web-based manager.
- *FortiGate SSL VPN User Guide*

  Compares FortiGate IPSec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.
- *FortiGate PPTP VPN User Guide*

  Explains how to configure a PPTP VPN using the web-based manager.
- *FortiGate Certificate Management User Guide*

  Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.
- *FortiGate VLANs and VDOMs User Guide*

  Describes how to configure VLANs and VDOMS in both NAT/Route and Transparent mode. Includes detailed examples.

Fortinet Tools and Documentation CD

All Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Technical Documentation web site at http://docs.forticare.com.

Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at http://kc.forticare.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at http://support.fortinet.com to learn about the technical support services that Fortinet provides.

Configuring IPSec VPNs

This section provides a brief overview of IPSec technology and includes general information about how to configure IPSec VPNs using this guide.

The following topics are included in this section:

- IPSec VPN overview
- Planning your VPN
- General preparation steps
- How to use this guide to configure an IPSec VPN

IPSec VPN overview

IPSec can be used to tunnel network-layer (layer 3) traffic between two VPN peers or between a VPN server and its client. When an IPSec VPN tunnel is established between a FortiGate unit and a remote VPN peer or client, packets are transmitted using Encapsulated Security Payload (ESP) security in tunnel mode.

Cleartext packets that originate from behind the FortiGate unit are encrypted as follows:

- IP packets are encapsulated within IPSec packets to form a secure tunnel
- the IP packet remains unaltered, but the header of the new IPSec packet refers to the end points of the VPN tunnel

When a FortiGate unit receives a connection request from a remote peer, it uses 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 VPN tunnel using phase 2 parameters and applies the protection profile. Key management, authentication, and security services are negotiated dynamically through the IKE protocol.

Planning your VPN

To save time later and be ready to configure a VPN correctly, it is a good idea to plan the VPN configuration ahead of time. All VPN configurations comprise a number of required and optional parameters. Before you begin, you need to determine:

- where does the IP traffic originate, and where does it need to be delivered
- which hosts, servers, or networks to include in the VPN
- which VPN devices to include in the configuration
- through which interfaces the VPN devices communicate
- through which interfaces do private networks access the VPN gateways

Once you have this information, you can select a VPN topology that meets the requirements of your situation (see "Network topologies" on page 16).

Network topologies

The topology of your network will determine how remote peers and clients connect to the VPN and how VPN traffic is routed. You can read about various network topologies and find the high-level procedures needed to configure IPSec VPNs in one of these sections:

- Gateway-to-gateway configurations
- Hub-and-spoke configurations
- Dynamic DNS configurations
- FortiClient dialup-client configurations
- FortiGate dialup-client configurations
- Internet-browsing configuration
- Redundant VPN configurations
- Transparent mode VPNs
- Manual-key configurations

These sections contain high-level configuration guidelines with cross-references to detailed configuration procedures. If you need more detail to complete a step, select the cross-reference in the step to drill-down to more detail. Return to the original procedure to complete the procedure. For a general overview of how to configure a VPN, see "General preparation steps" below.

Choosing policy-based or route-based VPNs

Generally, route-based VPNs are easier to configure than policy-based VPNs. However, the two types have different requirements that limit where they can be used.

Table 1: Comparison of policy-based and route-based VPNs

Policy-based	Route-based
Available in NAT/Route or Transparent mode	Available only in NAT/Route mode
Requires a firewall policy with IPSEC action that specifies the VPN tunnel. One policy controls connections in both directions.	Requires only a simple firewall policy with ACCEPT action. A separate policy is required for connections in each direction.
Supports DHCP over IPSec	Does not support DHCP over IPSec

You create a policy-based VPN by defining an IPSec firewall policy between two network interfaces and associating it with a VPN tunnel (phase 1) configuration.

You create a route-based VPN by creating a VPN phase 1 configuration with IPSec interface mode enabled. This creates a virtual IPSec interface. You then define a firewall policy to permit traffic to flow between the virtual IPSec interface and another network interface.

A virtual IPSec interface is a subinterface to a physical interface, an aggregate or VLAN interface. You can view these virtual IPSec interfaces on the System > Network > Interface page displayed under their associated physical interface names in the Name column. For more information about the Interface page, see the System Network chapter of the *FortiGate Administration Guide*.

General preparation steps

A VPN configuration defines relationships between the VPN devices and the private hosts, servers, or networks making up the VPN. Configuring a VPN involves gathering and recording the following information. You will need this information to configure the VPN.

- Identify the private IP address(es) of traffic generated by participating hosts, servers, and/or networks. These IP addresses represent the source addresses of traffic that is permitted to pass through the VPN. A IP source address can be an individual IP address, an address range, or a subnet address.
- Identify the public IP addresses of the VPN end-point interfaces. The VPN devices establish tunnels with each other through these interfaces.
- Identify the private IP address(es) associated with the VPN-device interfaces to the private networks. Computers on the private network(s) behind the VPN gateways will connect to their VPN gateways through these interfaces.

How to use this guide to configure an IPSec VPN

This guide uses a task-based approach to provide all of the procedures needed to create different types of VPN configurations. Follow the step-by-step configuration procedures in this guide to set up the VPN.

The following configuration procedures are common to all IPSec VPNs:

1. Define the phase 1 parameters that the FortiGate unit needs to authenticate remote peers or clients and establish a secure a connection. See “Auto Key phase 1 parameters” on page 127.
2. Define the phase 2 parameters that the FortiGate unit needs to create a VPN tunnel with a remote peer or dialup client. See “Phase 2 parameters” on page 143.
3. Specify the source and destination addresses of IP packets that are to be transported through the VPN tunnel. See “Defining firewall addresses” on page 149.
4. Create an IPsec firewall policy to define the scope of permitted services between the IP source and destination addresses. See “Defining firewall policies” on page 150.

Note: The steps given above assume that you will perform Steps 1 and 2 to have the FortiGate unit generate unique IPSec encryption and authentication keys automatically. In situations where a remote VPN peer or client requires a specific IPSec encryption and/or authentication key, you must configure the FortiGate unit to use manual keys instead of performing Steps 1 and 2. For more information, see “Manual-key configurations” on page 111.

Gateway-to-gateway configurations

This section explains how to set up a basic gateway-to-gateway (site-to-site) IPSec VPN.

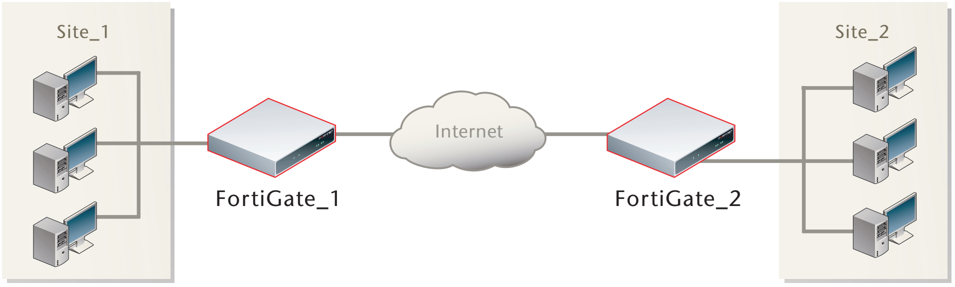
The following topics are included in this section:

- Configuration overview
- General configuration steps
- Configure the VPN peers
- Configuration example
- How to work with overlapping subnets

Configuration overview

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

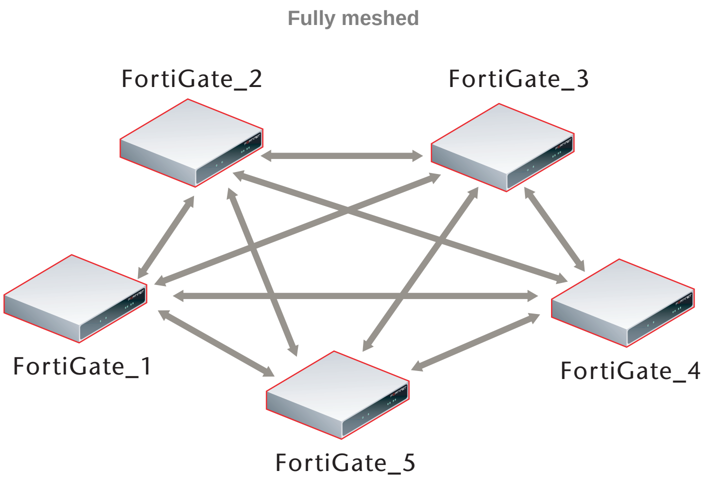
Figure 1: Example gateway-to-gateway configuration



Note: In some cases, computers on the private network behind one VPN peer may (by co-incidence) have IP addresses that are already used by computers on the network behind the other VPN peer. In this type of situation (ambiguous routing), conflicts may occur in one or both of the FortiGate routing tables and traffic destined for the remote network through the tunnel may not be sent. To resolve issues related to ambiguous routing, see “How to work with overlapping subnets” on page 29.
In other cases, computers on the private network behind one VPN peer may obtain IP addresses from a local DHCP server. However, unless the local and remote networks use different private network address spaces, unintended ambiguous routing and/or IP-address overlap issues may arise. For a discussion of the related issues, see “FortiGate dialup-client configurations” on page 71.

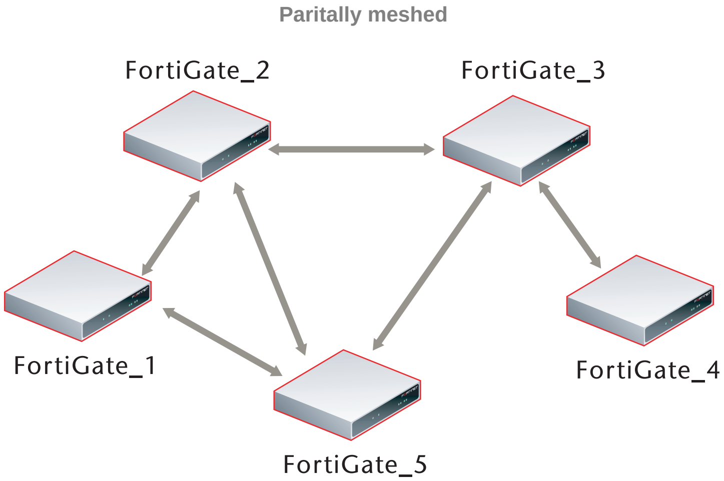
You can set up a fully meshed or partially meshed configuration (see Figure 2 and Figure 3).

Figure 2: Fully meshed configuration



In a fully meshed network, all VPN peers are connected to each other, with one hop between peers. This topology is the most fault-tolerant: if one peer goes down, the rest of the network is not affected. This topology is difficult to scale because it requires connections between all peers. In addition, unnecessary communication can occur between peers. We recommend a hub-and-spoke configuration instead (see “Hub-and-spoke configurations” on page 33).

Figure 3: Partially meshed configuration



A partially meshed network is similar to a fully meshed network, but instead of having tunnels between all peers, tunnels are only configured between peers that communicate with each other regularly.

Gateway-to-gateway infrastructure requirements

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

General configuration steps

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 IPSec firewall 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 firewall policies to control the permitted services and permitted direction of traffic between the IP source and destination addresses.

For more information, see “Configure the VPN peers” below.

Configure the VPN peers

Configure the VPN peers as follows:

1 At the local FortiGate unit, define the phase 1 configuration needed to establish a secure connection with the remote peer. See “Auto Key phase 1 parameters” on page 127. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel. This name appears in phase 2 configurations, firewall policies and the VPN monitor.
Remote Gateway	Select Static IP Address.
IP Address	Type the IP address of the remote peer public interface.
Local Interface	Select the FortiGate unit’s public interface.
Enable IPSec Interface Mode	You must select Advanced to see this setting. If IPSec Interface Mode is enabled, the FortiGate unit creates a virtual IPSec interface for a route-based VPN. Disable this option if you want to create a policy-based VPN. For more information, see “Choosing policy-based or route-based VPNs” on page 16. After you select OK to create the phase 1 configuration, you cannot change this setting.

2 Define the phase 2 parameters needed to create a VPN tunnel with the remote peer. See “Phase 2 parameters” on page 143. Enter these settings in particular:

Name	Enter a name to identify this phase 2 configuration.
Phase 1	Select the name of the phase 1 configuration that you defined.

3 Define names for the addresses or address ranges of the private networks that the VPN links. These addresses are used in the firewall policies that permit communication between the networks. For more information, see “Defining firewall addresses” on page 149.

Enter these settings in particular:

- Define an address name for the IP address and netmask of the private network behind the local FortiGate unit.

- Define an address name for the IP address and netmask of the private network behind the remote peer.

4 Define firewall policies to permit communication between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different firewall policies. For detailed information about creating firewall policies, see "Defining firewall policies" on page 150.

Policy-based VPN firewall policy

Define an IPSec firewall policy to permit communications between the source and destination addresses. Enter these settings in particular:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Destination Interface/Zone	Select the FortiGate unit's public interface.
Destination Address Name	Select the address name that you defined in Step 3 for the private network behind the remote peer.
Action	Select IPSEC.
VPN Tunnel	Select the name of the phase 1 configuration that you created in Step 1. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow outbound to enable traffic from the local network to initiate the tunnel.

Route-based VPN firewall policies

Define an ACCEPT firewall policy to permit communications between the source and destination addresses. Enter these settings in particular:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Destination Interface/Zone	Select the VPN Tunnel (IPSec Interface) you configured in Step 1.
Destination Address Name	Select the address name that you defined in Step 3 for the private network behind the remote peer.
Action	Select ACCEPT.
NAT	Disable.

To permit the remote client to initiate communication, you need to define a firewall policy for communication in that direction. Enter these settings in particular:

Source Interface/Zone	Select the VPN Tunnel (IPSec Interface) you configured in Step 1.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind the remote peer.
Destination Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Action	Select ACCEPT.
NAT	Disable.

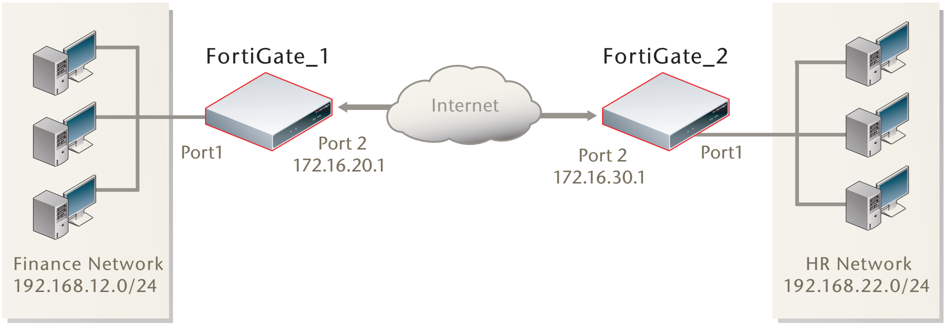
5 Place VPN policies in the policy list above any other policies having similar source and destination addresses.

6 Repeat this procedure at the remote FortiGate unit.

Configuration example

The following example demonstrates how to set up a basic gateway-to-gateway IPSec VPN that uses preshared keys to authenticate the two VPN peers.

Figure 4: Example gateway-to-gateway configuration



In this example, the network devices are assigned IP addresses as shown in Figure 4.

Define the phase 1 parameters on FortiGate_1

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 > Auto Key**.

2 Select Create Phase 1, enter the following information, and select OK:

Name	Type a name to identify the VPN tunnel (for example, `FG1toFG2_Tunnel`).
Remote Gateway	Static IP Address
IP Address	`172.16.30.1`
Local Interface	Port 2

Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Enable to create a route-based VPN. Disable to create a policy-based VPN. This example shows both policy and route-based VPNs.

Define the phase 2 parameters on FortiGate_1

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 > Auto Key**.

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

Name	Enter a name for the phase 2 configuration (for example, `FG1toFG2_phase2`).
Phase 1	Select the Phase 1 configuration that you defined previously (for example, `FG1toFG2_Tunnel`).

Define the firewall policy on FortiGate_1

Firewall policies control all IP traffic passing between a source address and a destination address.

An IPSec firewall 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 policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

Before you define firewall policies, you must first specify the IP source and destination addresses. In a gateway-to-gateway configuration:

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

To define the IP 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`).
Subnet/IP Range	Enter the IP address of the private network behind FortiGate_1 (for example, `192.168.12.0/24`).

To specify the 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`).
Subnet/IP Range	Enter the IP address of the private network behind FortiGate_2 (for example, `192.168.22.0/24`).

To define the firewall policy for a policy-based VPN

1 Go to **Firewall > Policy**.

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

Source Interface/Zone	Port 1
Source Address Name	`Finance_Network`
Destination Interface/Zone	Port 2
Destination Address Name	`HR_Network`
Schedule	As required.
Service	As required.
Action	IPSEC
VPN Tunnel	`FG1toFG2_Tunnel`
Allow Inbound	Enable
Allow Outbound	Enable
Inbound NAT	Disable

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

To define firewall policies for a route-based VPN

1 Go to **Firewall > Policy**.

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

Source Interface/Zone	Port 1
Source Address Name	`Finance_Network`
Destination Interface/Zone	`FG1toFG2_Tunnel`
Destination Address Name	`HR_Network`
Schedule	As required.
Service	As required.
Action	ACCEPT
NAT	Disable

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

Source Interface/Zone	`FG1toFG2_Tunnel`
Source Address Name	`HR_Network`
Destination Interface/Zone	Port 1
Destination Address Name	`Finance_Network`
Schedule	As required.
Service	As required.
Action	ACCEPT
NAT	Disable

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

To configure the route for a route-based VPN

1 Go to **Router > Static**.

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

Destination IP / Mask	`192.168.22.0/24`
Device	`FG1toFG2_Tunnel`
Gateway	Leave as default: 0.0.0.0.
Distance	Leave this at its default.

Configure 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 the firewall 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 > Auto Key**.

2 Select Create Phase 1, enter the following information, and select OK:

Name	Type a name for the VPN tunnel (for example, `FG2toFG1_Tunnel`).
Remote Gateway	Static IP Address
IP Address	`172.16.20.1`
Local Interface	Port 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	
Enable IPSec Interface Mode	Enable to create a route-based VPN. Disable to create a policy-based VPN. This example shows both policy and route-based VPNs.

To define the phase 2 parameters

1 Go to **VPN > IPSEC > Auto Key**.

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

Name	Enter a name for the phase 2 configuration (for example, `FG2toFG1_phase2`).
Phase 1	Select the gateway that you defined previously (for example, `FG2toFG1_Tunnel`).

To define the IP 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`).
Subnet/IP Range	`192.168.22.0/24` This is the IP address of the private network behind FortiGate_2.

To define the IP 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`).
Subnet/IP Range	Enter the IP address of the private network behind FortiGate_1 (for example, `192.168.12.0/24`).

To define the firewall policy for a policy-based VPN

1 Go to **Firewall > Policy**.

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

Source Interface/Zone	Port 2
Source Address Name	`HR_Network`
Destination Interface/Zone	Port 1
Destination Address Name	`Finance_Network`
Schedule	As required.
Service	As required.
Action	IPSEC
VPN Tunnel	`FG2toFG1_Tunnel`
Allow Inbound	Enable
Allow Outbound	Enable
Inbound NAT	Disable

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

To define the firewall policies for a route-based VPN

1 Go to **Firewall > Policy**.

2 Select Create New, enter the following information to create an outbound policy, and then select OK:

Source Interface/Zone	Port 2
Source Address Name	`HR_Network`
Destination Interface/Zone	`FG2toFG1_Tunnel`
Destination Address Name	`Finance_Network`
Schedule	As required.
Service	As required.
Action	ACCEPT
NAT	`Disable`

3 Select Create New, enter the following information to create an inbound policy, and then select OK:

Source Interface/Zone	`FG2toFG1_Tunnel`
Source Address Name	`Finance_Network`
Destination Interface/Zone	Port 2
Destination Address Name	`HR_Network`
Schedule	As required.
Service	As required.
Action	ACCEPT
NAT	`Disable`

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

To configure the route for a route-based VPN

1 Go to **Router > Static**.

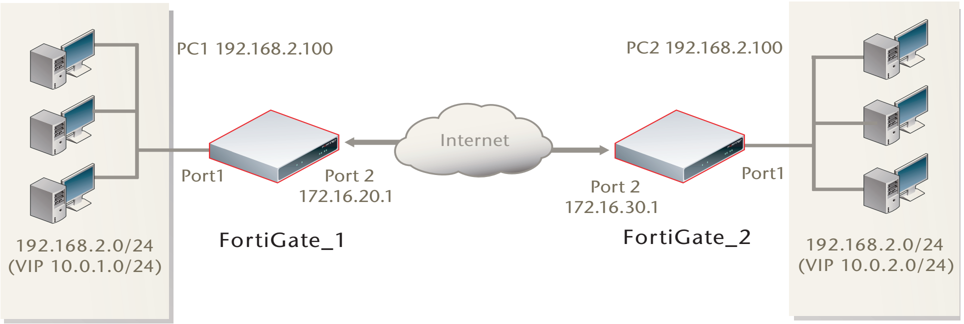
2 Select Create New, enter the following information, and then select OK:

Destination IP / Mask	`192.168.12.0/24`
Device	`FG2toFG1_Tunnel`
Gateway	Leave as default: 0.0.0.0.
Distance	Usually you can leave this at its default.

How to work with overlapping subnets

A site-to-site VPN configuration sometimes has the problem that the private subnet addresses at each end are the same. You can resolve this problem by remapping the private addresses using virtual IP addresses (VIP).

Figure 5: Overlapped subnets example



After the tunnel is established, hosts on each side can communicate with hosts on the other side using the mapped IP addresses. For example, PC1 can communicate with PC2 using IP address 10.0.2.100. FortiGate_2 maps connections for IP address 10.0.2.100 to IP address 192.168.2.100.

Solution for route-based VPN

You need to:

- Configure IPSec Phase 1 and Phase 2 as you usually would for a route-based VPN. In this example, the resulting IPSec interface is named FG1toFG2.
- Configure virtual IP (VIP) mapping:
  - the 10.0.1.0/24 network to the 192.168.2.0/24 network on FortiGate_1
  - the 10.0.2.0/24 network to the 192.168.2.0/24 network on FortiGate_2
- Configure an outgoing firewall policy with ordinary source NAT.
- Configure an incoming firewall policy with the VIP as the destination.
- Configure a route to the remote private network over the IPSec interface.

To configure VIP mapping

1 Go to **Firewall > Virtual IP**.

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

Name	Enter a name, for example, `my-vip`.
External Interface	Select the IPSec interface: FG1toFG2
Type	Static NAT
External IP Address/Range	In the first field, enter: `10.0.1.1` on FortiGate_1 `10.0.2.1` on FortiGate_2.
Mapped IP Address/Range	Enter `192.168.2.1` and `192.168.2.254`.
Port Forwarding	Disable

To configure the outbound firewall policy

1 Go to **Firewall > Policy**.

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

Source Interface/Zone	Port 1
Source Address Name	all
Destination Interface/Zone	FG1toFG2
Destination Address Name	all
Schedule	As required.
Service	As required.
Action	ACCEPT
NAT	Enable

To configure the inbound firewall policy

1 Go to **Firewall > Policy**.

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

Source Interface/Zone	FG1toFG2
Source Address Name	all
Destination Interface/Zone	Port 1
Destination Address Name	my-vip
Schedule	As required.
Service	As required.
Action	ACCEPT
NAT	Disable

To configure the route

1 Go to **Router > Static**.

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

Destination IP / Mask	`10.0.2.0/24` on FortiGate_1 `10.0.1.0/24` on FortiGate_2
Device	FG1toFG2
Gateway	Leave as default: 0.0.0.0.
Distance	Usually you can leave this at its default.

Solution for policy-based VPN

As with the route-based solution, users contact hosts at the other end of the VPN using an alternate subnet address. PC1 communicates with PC2 using IP address 10.0.2.100. PC2 communicates with PC1 using IP address 10.0.1.100. In this solution however, outbound NAT is used to translate the source address of packets from the 192.168.2.0/24 network to the alternate subnet address that hosts at the other end of the VPN use to reply. Inbound packets from the remote end have their destination addresses translated back to the 192.168.2.0/24 network.

For example, PC1 uses the destination address 10.0.2.100 to contact PC2. Outbound NAT on FortiGate_1 translates the PC1 source address to 10.0.1.100. At the FortiGate_2 end of the tunnel, the outbound NAT configuration translates the destination address to the actual PC2 address of 192.168.2.100. Similarly, PC2 replies to PC1 using destination address 10.0.1.100, with the PC2 source address translated to 10.0.2.100. PC1 and PC2 can communicate over the VPN even though they both have the same IP address.

You need to:

- Configure IPSec Phase 1 as you usually would for a policy-based VPN.
- Configure IPSec Phase 2 with the `use-natip disable` CLI option.
- Define a firewall address for the local private network, 192.168.2.0/24.
- Define a firewall address for the remote private network:
  - define a firewall address for 10.0.2.0/24 on FortiGate_1
  - define a firewall address for 10.0.1.0/24 on FortiGate_2
- Configure an outgoing IPSec firewall policy with outbound NAT to map 192.168.2.0/24 source addresses:
  - to the 10.0.1.0/24 network on FortiGate_1
  - to the 10.0.2.0/24 network on FortiGate_2

To configure IPSec Phase 2

In the CLI, enter the following commands:

```
config vpn ipsec phase2
   edit "FG1FG2_p2"
      set keepalive enable
      set pfs enable
      set phase1name FG1toFG2
      set proposal 3des-sha1 3des-md5
      set replay enable
      set use-natip disable
end
```

In this example, your phase 1 definition is named FG1toFG2. Because `use-natip` is set to `disable`, you can specify the source selector using the `src-addr-type`, `src-start-ip` / `src-end-ip` or `src-subnet` keywords. This example leaves these keywords at their default values, which specify the subnet `0.0.0.0/0`.

To define the local private network firewall address

1 Go to **Firewall > Address**.

2 Select Create New and enter the following information:

Address Name	Enter a name, `vpn-local`, for example.
Type	`Subnet / IP Range`
Subnet / IP Range	`192.168.2.0 255.255.255.0`
Interface	`Any`

To define the remote private network firewall address

1 Go to **Firewall > Address**.

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

Address Name	Enter a name, `vpn-remote`, for example.
Type	`Subnet / IP Range`
Subnet / IP Range	`10.0.2.0 255.255.255.0` on FortiGate_1 `10.0.1.0 255.255.255.0` on FortiGate_2
Interface	`Any`

To configure the IPSec firewall policy

In the CLI, enter the following commands:

```
config firewall policy
   edit 1
      set srcintf "port1"
      set dstintf "port2"
      set srcaddr "vpn-local"
      set dstaddr "vpn-remote"
      set action ipsec
      set schedule "always"
      set service "ANY"
      set inbound enable
      set outbound enable
      set vpntunnel "FG1toFG2"
      set natoutbound enable
      set natip 10.0.1.0 255.255.255.0 (on FortiGate_1)
      set natip 10.0.2.0 255.255.255.0 (on FortiGate_2)
end
```

Optionally, you can set everything except `natip` in the web-based manager and then use the CLI to set `natip`.

Hub-and-spoke configurations

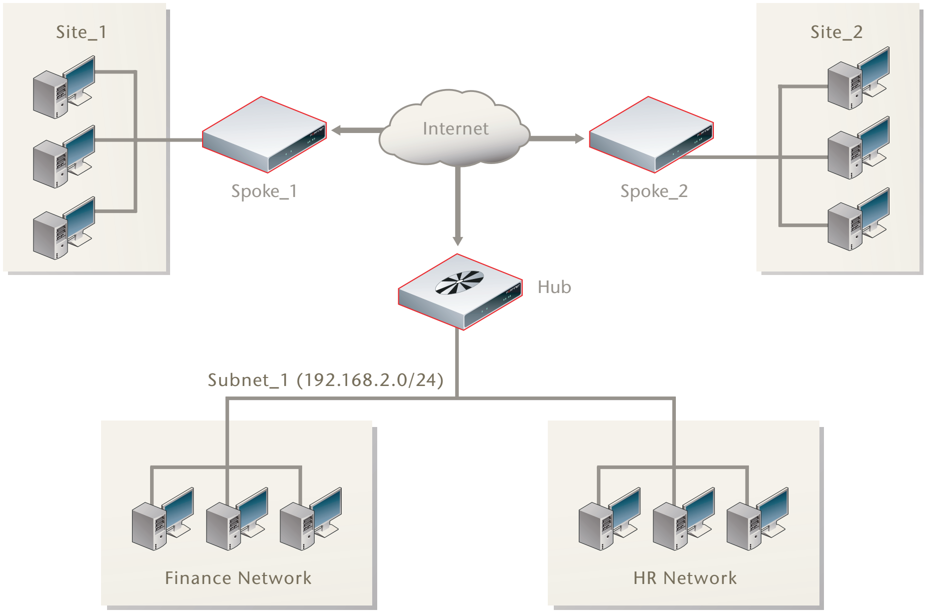
This section describes how to set up hub-and-spoke IPSec VPNs. The following topics are included in this section:

- Configuration overview
- Configure the hub
- Configure the spokes
- Dynamic spokes configuration example

Configuration overview

In a hub-and-spoke configuration, VPN connections radiate from a central FortiGate unit (the hub) to a number of remote peers (the spokes). Traffic can pass between private networks behind the hub and private networks behind the remote peers. Traffic can also pass between remote peer private networks through the hub.

Figure 6: Example hub-and-spoke configuration



The actual implementation varies in complexity depending on

- whether the spokes are statically or dynamically addressed
- the addressing scheme of the protected subnets
- how peers are authenticated

This guide discusses the issues involved in configuring a hub-and-spoke VPN and provides some basic configuration examples.

Hub-and-spoke infrastructure requirements

- The FortiGate hub must be operating in NAT/Route mode and have a static public IP address.
- Spokes may have static IP addresses, dynamic IP addresses (see “FortiGate dialup-client configurations” on page 71), or static domain names and dynamic IP addresses (see “Dynamic DNS configurations” on page 49).

Spoke gateway addressing

The public IP address of the spoke is the VPN remote gateway as seen from the hub. Statically addressed spokes each require a separate VPN phase 1 configuration on the hub. When there are many spokes, this becomes rather cumbersome.

Using dynamic addressing for spokes simplifies the VPN configuration because then the hub requires only a single phase 1 configuration with “dialup user” as the remote gateway. You can use this configuration even if the remote peers have static IP addresses. A remote peer can establish a VPN connection regardless of its IP address if its traffic selectors match and it can authenticate to the hub. See “Dynamic spokes configuration example” on page 42 for an example of this configuration.

Protected networks addressing

The addresses of the protected networks are needed to configure destination selectors and sometimes for firewall policies and static routes. The larger the number of spokes, the more addresses there are to manage. You can

- assign spoke subnets as part of a larger subnet, usually on a new network

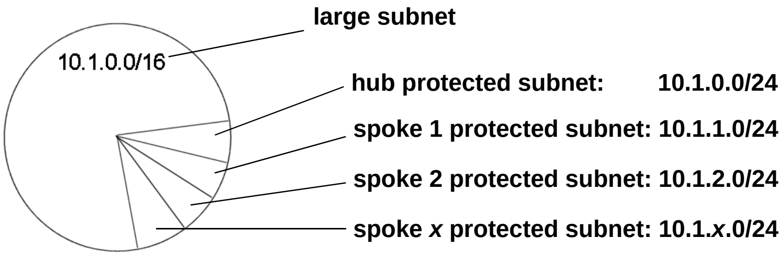
or

- create address groups that contain all of the needed addresses

Using aggregated subnets

If you are creating a new network, where subnet IP addresses are not already assigned, you can simplify the VPN configuration by assigning spoke subnets that are part of a large subnet.

Figure 7: Aggregated subnets


large subnet
10.1.0.0/16
hub protected subnet: 10.1.0.0/24
spoke 1 protected subnet: 10.1.1.0/24
spoke 2 protected subnet: 10.1.2.0/24
spoke *x* protected subnet: 10.1.*x*.0/24

All spokes use the large subnet address, 10.1.0.0/16 for example, as

- the IPsec destination selector
- the destination of the firewall policy from the private subnet to the VPN (required for policy-based VPN, optional for interface-based VPN)
- the destination of the static route to the VPN (interface-based)

Each spoke uses the address of its own protected subnet as the IPsec source selector and as the source address in its VPN firewall policy. The remote gateway is the public IP address of the hub FortiGate unit.

Using an address group

If you want to create a hub-and-spoke VPN between existing private networks, the subnet addressing usually does not fit the aggregated subnet model discussed earlier. All of the spokes and the hub will need to include the addresses of all the protected networks in their configuration.

On FortiGate units, you can define a named firewall address for each of the remote protected networks and add these addresses to a firewall address group. For a policy-based VPN, you can then use this address group as the destination of the VPN firewall policy.

For an interface-based VPN, the destination of the VPN firewall policy can be set to All. You need to specify appropriate routes for each of the remote subnets.

Authentication

Authentication is by a common preshared key or by certificates. For simplicity, the examples in this chapter assume that all spokes use the same preshared key.

Configure the hub

At the FortiGate unit that acts as the hub, you need to

- configure the VPN to each spoke
- configure communication between spokes

You configure communication between spokes differently for a policy-based VPN than for a route-based VPN. For a policy-based VPN, you configure a VPN concentrator. For a route-based VPN, you must either define firewall policies or group the IPSec interfaces into a zone

Define the hub-spoke VPNs

Perform these steps at the FortiGate unit that will act as the hub. Although this procedure assumes that the spokes are all FortiGate units, a spoke could also be VPN client software, such as FortiClient Host Security.

To configure the VPN hub

1 At the hub, define the phase 1 configuration for each spoke. See “Auto Key phase 1 parameters” on page 127. Enter these settings in particular:

Name	Enter a name to identify the VPN in phase 2 configurations, firewall policies and the VPN monitor.

Remote Gateway The remote gateway is the other end of the VPN tunnel. There are three options:

- **Static IP Address** Enter the spoke's public IP address. You will need to create a phase 1 configuration for each spoke.

  Either the hub or the spoke can establish the VPN connection.

- **Dialup User** No additional information is needed. The hub accepts connections from peers with appropriate encryption and authentication settings. Only one phase 1 configuration is needed for multiple dialup spokes.

  Only the spoke can establish the VPN tunnel.

- **Dynamic DNS** If the spoke subscribes to a dynamic DNS service, enter the spoke's domain name. Either the hub or the spoke can establish the VPN connection. For more information, see "Dynamic DNS configurations" on page 49.

Local Interface Select the FortiGate interface that connects to the remote gateway. This is usually the FortiGate unit's public interface.

Enable IPSec Interface Mode You must select Advanced to see this setting. If IPSec Interface Mode is enabled, the FortiGate unit creates a virtual IPSec interface for a route-based VPN. Disable this option if you want to create a policy-based VPN. For more information, see "Choosing policy-based or route-based VPNs" on page 16.

After you select OK to create the phase 1 configuration, you cannot change this setting.

2 Define the phase 2 parameters needed to create a VPN tunnel with each spoke. See "Phase 2 parameters" on page 143. Enter these settings in particular:

Name Enter a name to identify this spoke phase 2 configuration.

Phase 1 Select the name of the phase 1 configuration that you defined for this spoke.

Define the hub-spoke firewall policies

1 Define a name for the address of the private network behind the hub. For more information, see "Defining firewall addresses" on page 149.

2 Define names for the addresses or address ranges of the private networks behind the spokes. For more information, see "Defining firewall addresses" on page 149.

3 Define the VPN concentrator. See "To define the VPN concentrator" on page 37.

4 Define firewall policies to permit communication between the hub and the spokes. For more information, see "Defining firewall policies" on page 150.

Policy-based VPN firewall policy

Define an IPSec firewall policy to permit communications between the hub and the spoke. Enter these settings in particular:

Source Interface/Zone Select the hub's interface to the internal (private) network.

Source Address Name Select the source address that you defined in Step 1.

Destination Interface/Zone Select the hub's public network interface.

Destination Address Name Select the address name you defined in Step 2 for the private network behind the spoke FortiGate unit.

Action	IPSEC
VPN Tunnel	Select the name of the phase 1 configuration that you created for the spoke in Step 1. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow outbound to enable traffic from the local network to initiate the tunnel.

Route-based VPN firewall policies

Define ACCEPT firewall policies to permit communications between the hub and the spoke. You need one policy for each direction. Enter these settings in particular:

Source Interface/Zone	Select the VPN Tunnel (IPSec Interface) you configured in Step 1.
Source Address Name	Select the address name you defined in Step 2 for the private network behind the spoke FortiGate unit.
Destination Interface/Zone	Select the hub’s interface to the internal (private) network.
Destination Address Name	Select the source address that you defined in Step 1.
Action	Select ACCEPT.
NAT	Enable.

Source Interface/Zone	Select the address name you defined in Step 2 for the private network behind the spoke FortiGate units.
Source Address Name	Select the VPN Tunnel (IPSec Interface) you configured in Step 1.
Destination Interface/Zone	Select the source address that you defined in Step 1.
Destination Address Name	Select the hub’s interface to the internal (private) network.
Action	Select ACCEPT.
NAT	Enable.

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

- IPSec policies that control traffic between the hub and the spokes first
- the default firewall policy last

Configuring communication between spokes (policy-based VPN)

For a policy-based hub-and-spoke VPN, you define a concentrator to enable communication between the spokes.

To define the VPN concentrator

1 At the hub, go to **VPN > IPSEC > Concentrator** and select Create New.

2 In the Concentrator Name field, type a name to identify the concentrator.

3 From the Available Tunnels list, select a VPN tunnel and then select the right-pointing arrow.

Note: To remove tunnels from the VPN concentrator, select the tunnel in the Members list and select the left-pointing arrow.

4 Repeat Step 3 until all of the tunnels associated with the spokes are included in the concentrator.

5 Select OK.

Configuring communication between spokes (route-based VPN)

For a route-based hub-and-spoke VPN, there are several ways you can enable communication between the spokes:

- put all of the IPSec interfaces into a zone and enable intra-zone traffic. This eliminates the need for any firewall policy for the VPN, but you cannot apply a protection profile to scan the traffic for security threats.
- put all of the IPSec interfaces into a zone and create a single zone-to-zone firewall policy
- create a firewall policy for each pair of spokes that are allowed to communicate with each other. The number of policies required increases rapidly as the number of spokes increases.

Using a zone as a concentrator

A simple way to provide communication among all of the spokes is to create a zone and allow intra-zone communication. You cannot apply a protection profile using this method.

1. Go to **System > Network > Zone**.
2. In the Zone Name field, enter a name, such as Our_VPN_zone.
3. Clear Block intra-zone traffic.
4. In the Interface Members list, select the IPSec interfaces that are part of your VPN.
5. Select OK.

Using a zone with a policy as a concentrator

If you put all of the hub IPSec interfaces involved in the VPN into a zone, you can enable communication among all of the spokes and apply a protection profile with just one firewall policy.

To create a zone for the VPN

1. Go to **System > Network > Zone**.
2. In the Zone Name field, enter a name, such as Our_VPN_zone.
3. Select Block intra-zone traffic.
4. In the Interface Members list, select the IPSec interfaces that are part of your VPN.
5. Select OK.

To create a firewall policy for the zone

1. Go to **Firewall > Policy**. Select Create New and enter these settings:

Source Interface/Zone	Select the zone you created for your VPN.
Source Address Name	Select All.
Destination Interface/Zone	Select the zone you created for your VPN.
Destination Address Name	Select All.
Action	Select ACCEPT.

NAT	Enable.
Protection profile	If you want to apply a protection profile to this traffic, select the appropriate profile.

2 Select OK.

Using firewall policies as a concentrator

To enable communication between two spokes, you need to define an ACCEPT firewall policy for them. To allow either spoke to initiate communication, you must create a policy for each direction. This procedure describes a firewall policy for communication from Spoke 1 to Spoke 2. Others are similar.

1 Define names for the addresses or address ranges of the private networks behind each spoke. For more information, see “Defining firewall addresses” on page 149.

2 Go to **Firewall > Policy**. Select Create New and enter these settings in particular:

Source Interface/Zone	Select the IPSec interface that connects to Spoke 1.
Source Address Name	Select the address of the private network behind Spoke 1.
Destination Interface/Zone	Select the IPSec interface that connects to Spoke 2.
Destination Address Name	Select the address of the private network behind Spoke 2.
Action	Select ACCEPT.
NAT	Enable.
Protection profile	If you want to apply a protection profile to this traffic, select the appropriate profile.

3 Select OK.

Configure the spokes

Although this procedure assumes that the spokes are all FortiGate units, a spoke could also be VPN client software, such as FortiClient Host Security.

Perform these steps at each FortiGate unit that will act as a spoke.

To create the phase 1 configuration

1 At the spoke, define the phase 1 parameters that the spoke will use to establish a secure connection with the hub. See "Auto Key phase 1 parameters" on page 127. Enter these settings in particular:

Remote Gateway	Select Static IP Address.
IP Address	Type the IP address of the interface that connects to the hub.
Enable IPSec Interface Mode	Enable if you are creating a route-based VPN. Clear if you are creating a policy-based VPN.

2 Create the phase 2 tunnel definition. See "Phase 2 parameters" on page 143. Enter these settings in particular:

Remote Gateway	Select the set of phase 1 parameters that you defined for the hub. You can select the name of the hub from the Static IP Address part of the list.

Configuring firewall policies for hub-to-spoke communication

1 Create an address for this spoke. See "Defining firewall addresses" on page 149. Enter the IP address and netmask of the private network behind the spoke.

2 Create an address to represent the hub. See "Defining firewall addresses" on page 149. Enter the IP address and netmask of the private network behind the hub.

3 Define the firewall policy to enable communication with the hub.

Policy-based VPN firewall policy

Define an IPSec firewall policy to permit communications with the hub. See "Defining firewall policies" on page 150. Enter these settings in particular:

Source Interface/Zone	Select the spoke's interface to the internal (private) network.
Source Address Name	Select the spoke address you defined in Step 1.
Destination Interface/Zone	Select the spoke's interface to the external (public) network.
Destination Address Name	Select the hub address you defined in Step 2.
Action	Select IPSEC
VPN Tunnel	Select the name of the phase 1 configuration you defined. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow outbound to enable traffic from the local network to initiate the tunnel.

Route-based VPN firewall policy

Define two firewall policies to permit communications to and from the hub. Enter these settings in particular:

Source Interface/Zone	Select the virtual IPSec interface you created.
Source Address Name	Select the hub address you defined in Step 1.

Destination Interface/Zone	Select the spoke's interface to the internal (private) network.
Destination Address Name	Select the spoke addresses you defined in Step 2.
Action	Select ACCEPT
NAT	Enable

Source Interface/Zone	Select the spoke's interface to the internal (private) network.
Source Address Name	Select the spoke address you defined in Step 1.
Destination Interface/Zone	Select the virtual IPSec interface you created.
Destination Address Name	Select the hub destination addresses you defined in Step 2.
Action	Select ACCEPT
NAT	Enable

Configuring firewall policies for spoke-to-spoke communication

Each spoke requires firewall policies to enable communication with the other spokes. Instead of creating separate firewall policies for each spoke, you can create an address group that contains the addresses of the networks behind the other spokes. The firewall policy then applies to all of the spokes in the group.

1 Define destination addresses to represent the networks behind each of the other spokes. Add these addresses to an address group. For more information, see "Configuring Address Groups" section in the "Firewall Address" chapter of the *FortiGate Administration Guide*.

2 Define the firewall policy to enable communication between this spoke and the spokes in the address group you created.

Policy-based VPN firewall policy

Define an IPSec firewall policy to permit communications with the other spokes. See "Defining firewall policies" on page 150. Enter these settings in particular:

Source Interface/Zone	Select this spoke's internal (private) network interface.
Source Address Name	Select this spoke's source address.
Destination Interface/Zone	Select the spoke's interface to the external (public) network.
Destination Address Name	Select the spoke address group you defined in Step 1.
Action	Select IPSEC
VPN Tunnel	Select the name of the phase 1 configuration you defined. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow outbound to enable traffic from the local network to initiate the tunnel.

Route-based VPN firewall policy

Define two firewall policies to permit communications to and from the other spokes. Enter these settings in particular:

Source Interface/Zone	Select the virtual IPSec interface you created.
Source Address Name	Select the spoke address group you defined in Step 1.
Destination Interface/Zone	Select the spoke's interface to the internal (private) network.
Destination Address Name	Select this spoke's address name.

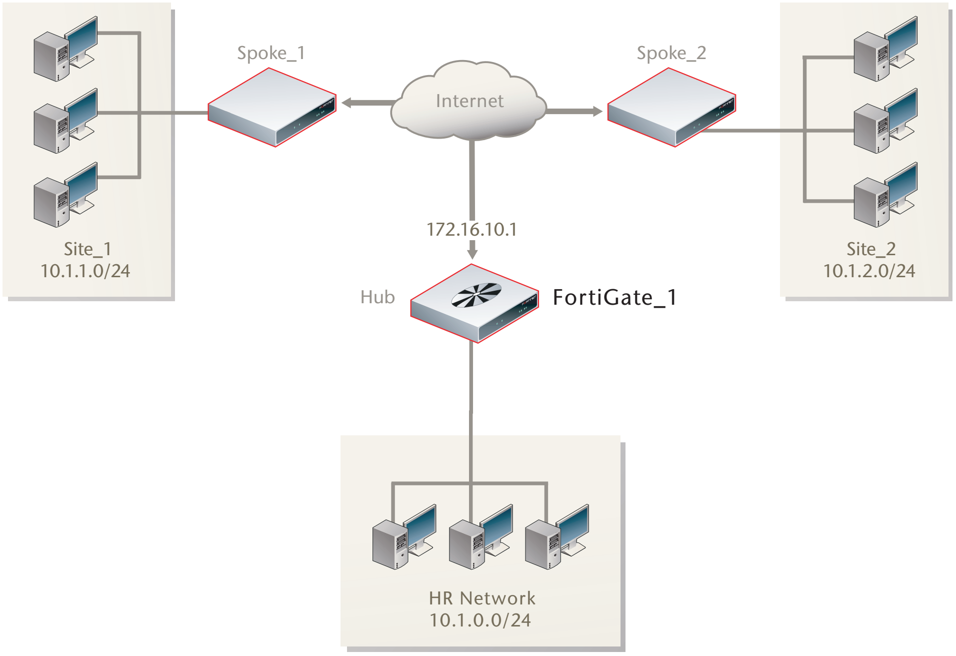
Action	Select ACCEPT
NAT	Enable
Source Interface/Zone	Select the spoke's interface to the internal (private) network.
Source Address Name	Select this spoke's address name.
Destination Interface/Zone	Select the virtual IPSec interface you created.
Destination Address Name	Select the spoke address group you defined in Step 1.
Action	Select ACCEPT
NAT	Enable

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

Dynamic spokes configuration example

This example demonstrates how to set up a basic route-based hub-and-spoke IPSec VPN that uses preshared keys to authenticate VPN peers.

Figure 8: Example hub-and-spoke configuration



In the example configuration, the protected networks 10.1.0.0/24, 10.1.1.0/24 and 10.1.2.0/24 are all part of the larger subnet 10.1.0.0/16. The steps for setting up the example hub-and-spoke configuration create a VPN among Site 1, Site 2, and the HR Network.

The spokes are dialup. Their addresses are not part of the configuration on the hub, so only one spoke definition is required no matter the number of spokes. For simplicity, only two spokes are shown.

Configure the hub (FortiGate_1)

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, one preshared key will be used to authenticate all of the spokes. 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.

Define the IPsec configuration

To define the phase 1 parameters

1 At FortiGate_1, go to **VPN > IPSEC > Auto Key**.

2 Define the phase 1 parameters that the hub will use to establish a secure connection to the spokes. Select Create Phase 1, enter the following information, and select OK:

Name	Type a name (for example, `toSpokes`).
Remote Gateway	Dialup user
Local Interface	External
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID

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.

To define the phase 2 parameters

1 Go to **VPN > IPSEC > Auto Key**.

2 Create a phase 2 tunnel definition for the spokes. Select Create Phase 2, enter the following information, and select OK:

Name	Enter a name for the phase 2 definition (for example, `toSpokes_ph2`).
Phase 1	Select the Phase 1 configuration that you defined previously (for example, `toSpokes`).

Define the firewall policies

Firewall policies control all IP traffic passing between a source address and a destination address. For a route-based VPN, the policies are simpler than for a policy-based VPN. Instead of an IPSEC policy, you use an ACCEPT policy with the virtual IPSec interface as the external interface.

Before you define firewall policies, you must first define firewall addresses to use in those policies. You need addresses for:

- the HR network behind FortiGate_1
- the aggregate subnet address for the protected networks

To define the IP 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`).
Subnet/IP Range	Enter the IP address of the HR network behind FortiGate_1 (for example, `10.1.0.0/24`).

To specify the IP address the aggregate protected subnet

1 Go to **Firewall > Address**.

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

Address Name	Enter an address name (for example, `Spoke_net`).
Subnet/IP Range	Enter the IP address of the aggregate protected network, `10.1.0.0/16`

To define the firewall policy for traffic from the hub to the spokes

1 Go to **Firewall > Policy**.

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

Source	Interface/Zone Select the interface to the HR network, port 1. Address Name `HR_Network`
Destination	Interface/Zone Select the virtual IPSec interface that connects to the spokes, `toSpokes` Address Name `Spoke_net`
Schedule	As required.
Service	As required.
Action	ACCEPT

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

Configure communication between spokes

Spokes communicate with each other through the hub. You need to configure the hub to allow this communication. An easy way to do this is to create a zone containing the virtual IPSec interfaces (even if there is only one) and create a zone-to-zone firewall policy.

To create a zone for the VPN

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

2 In the Zone Name field, enter a name, such as Our_VPN_zone.

3 Select Block intra-zone traffic.

You could enable intra-zone traffic and then you would not need to create a firewall policy. But, you would not be able to apply a protection profile.

4 In the Interface Members list, select the virtual IPSec interface, `toSpokes`.

5 Select OK.

To create a firewall policy for the zone

1 Go to **Firewall > Policy**. Select Create New and enter these settings:

Source Interface/Zone	Select `Our_VPN_zone`.
Source Address Name	Select All.
Destination Interface/Zone	Select `Our_VPN_zone`.
Destination Address Name	Select All.
Action	Select ACCEPT.
NAT	Enable.
Protection profile	Select the appropriate protection profile.

2 Select OK.

Configure the spokes

In this example, all spokes have nearly identical configuration, requiring the following:

- 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 the spoke. This is the only part of the configuration that is different for each spoke.
- a destination address that represents the aggregate protected network
- a firewall policy to enable communications between the spoke and the aggregate protected network

Define the IPsec configuration

At each spoke, create the following configuration.

To define the phase 1 parameters

1 At the spoke, go to **VPN > IPSEC > Auto Key**.

2 Select Create Phase 1, enter the following information, and select OK:

Name	Type a name, for example, `toHub`).
Remote Gateway	Static IP Address
IP Address	`172.16.10.1`
Local Interface	Port2
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
Enable IPSec Interface Mode	Select Advanced to see this option. Enable the option to create a route-based VPN.

To define the phase 2 parameters

1 Go to **VPN > IPSEC > Auto Key**.

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

Name	Enter a name for the tunnel (for example, `toHub_ph2`).
Phase 1	Select the name of the phase 1 configuration that you defined previously, for example, `toHub`.
Advanced	Select to show the following Quick Mode Selector settings.
Source	Enter the address of the protected network at this spoke. For spoke_1, this is 10.1.1.0/24. For spoke_2, this is 10.1.2.0/24.
Destination	Enter the aggregate protected subnet address, 10.1.0.0/16.

Define the firewall policies

You need to define firewall addresses for the spokes and the aggregate protected network and then create a firewall policy to enable communication between them.

To define the IP address of the network behind the spoke

1 Go to **Firewall > Address**.

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

Address Name	Enter an address name (for example, `LocalNet`).
Subnet/IP Range	Enter the IP address of the private network behind the spoke. For spoke_1, this is 10.1.1.0/24. For spoke_2, this is 10.1.2.0/24.

To specify the IP address of the aggregate protected 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, `Spoke_net`).
Subnet/IP Range	Enter the IP address of the aggregate protected network, `10.1.0.0/16`).

To define the firewall policy

1 Go to **Firewall > Policy**.

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

Source	Interface/Zone Select the virtual IPSec interface, `toHub`. Address Name Select the aggregate protected network address `Spoke_net`
Destination	Interface/Zone Select the interface to the internal (private) network, `port1`. Address Name Select the address for this spoke's protected network `LocalNet`
Schedule	As required.

Service	As required.
Action	ACCEPT

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

Source	Interface/Zone Select the interface to the internal (private) network, `port1`. Address Name Select the address for this spoke's protected network `LocalNet`
Destination	Interface/Zone Select the virtual IPSec interface, `toHub`. Address Name Select the aggregate protected network address `Spoke_net`
Schedule	As required.
Service	As required.
Action	ACCEPT

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

Dynamic DNS configurations

This section describes how to configure a site-to-site VPN, in which one FortiGate unit has a static IP address and the other FortiGate unit has a static domain name and a dynamic IP address.

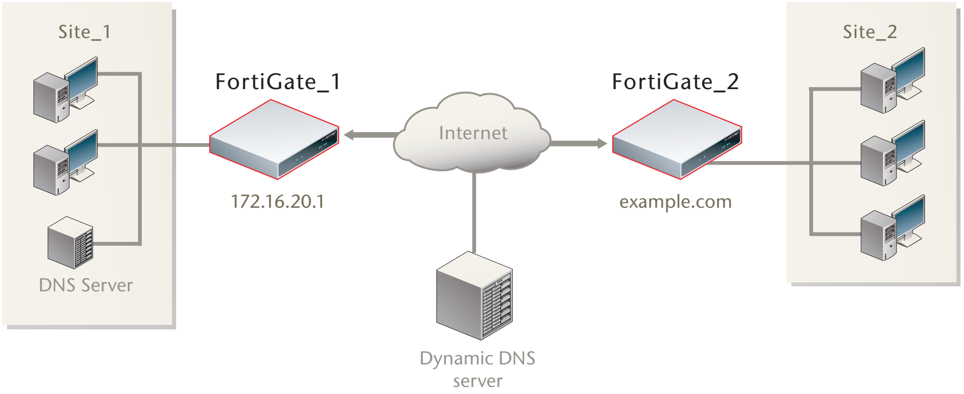
The following topics are included in this section:

- Configuration overview
- General configuration steps
- Configure the dynamically-addressed VPN peer
- Configure the fixed-address VPN peer

Configuration overview

In this type of scenario, one of the FortiGate units in a gateway-to-gateway configuration has a static domain name (for example, example.com) and a dynamic IP address. See FortiGate_2 in Figure 9. Whenever that FortiGate unit connects to the Internet (and possibly also at predefined intervals set by the ISP), the ISP may assign a different IP address to the FortiGate unit. Therefore, remote peers have to locate the FortiGate unit through DNS lookup.

Figure 9: Example dynamic DNS configuration



When a remote peer (such as FortiGate_1 in Figure 9) initiates a connection to the domain name, a DNS server looks up and returns the IP address that matches the domain name. The remote peer uses the retrieved IP address to establish a connection with the FortiGate unit.

To ensure that DNS servers are able to discover the current IP address associated with a FortiGate domain name, the FortiGate unit with the domain name subscribes to a dynamic DNS service. A dynamic DNS service ensures that any changes to IP addresses are propagated to all Internet DNS servers.

Whenever the FortiGate unit detects that its IP address has changed, it notifies the dynamic DNS server and provides the new IP address to the server. The dynamic DNS server makes the updated IP address available to all DNS servers and the new IP address remains in effect until the FortiGate unit detects that its IP address has changed again.

A FortiGate unit that has static domain name and a dynamic IP address can initiate VPN connections anytime—the remote peer replies to the FortiGate unit using the source IP address that was sent in the packet header. However, changes to a dynamic IP address must be resolved before a remote peer can establish a VPN connection to the domain name—the remote peer must request a DNS lookup for the matching IP address before initiating the connection.

Dynamic DNS infrastructure requirements

- A basic gateway-to-gateway configuration must be in place (see “Gateway-to-gateway configurations” on page 19) except one of the FortiGate units has a static domain name and a dynamic IP address instead of a static IP address.
- A DNS server must be available to VPN peers that initiate connections to the domain name. For instructions about how to configure FortiGate units to look up the IP address of a domain name, see the “System Network DNS” section of the *FortiGate Administration Guide*.
- The FortiGate unit with the domain name must subscribe to one of the supported dynamic DNS services. Contact one of the services to set up an account. For more information and instructions about how to configure the FortiGate unit to push its dynamic IP address to a dynamic DNS server, see the “System Network Interface” section of the *FortiGate Administration Guide*.

General configuration steps

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 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:

- Configure the FortiGate unit that has a domain name with a dynamic IP address. This unit uses a Local ID string to identify itself to the remote peer. See “Configure the dynamically-addressed VPN peer” on page 51.
- Configure the fixed-address VPN peer. To initiate a VPN tunnel with the dynamically-addressed peer, this unit must retrieve the IP address for the domain from the dynamic DNS service. See “Configure the fixed-address VPN peer” on page 53.

Configure the dynamically-addressed VPN peer

Configure the FortiGate unit that has a domain name as follows:

1 Define the phase 1 parameters needed to establish a secure connection with the remote peer. See “Auto Key phase 1 parameters” on page 127. Select Advanced, enter these settings and then select OK:

Name	Enter a name to identify the VPN tunnel. This name appears in phase 2 configurations, firewall policies and the VPN monitor.
Remote Gateway	Select Static IP Address.
IP Address	Type the IP address of the public interface to the remote peer.
Mode	Select Aggressive.
Enable IPSec Interface Mode	Enable for a route-based VPN. Disable for a policy-based VPN.
Local ID	Type a character string that the local FortiGate unit can use to identify itself to the remote peer (for example, you could type the fully qualified domain name of the FortiGate unit, `example.com`). This value must be identical to the value in the Accept this peer ID field of the phase 1 remote gateway configuration on the remote peer.

2 Define the phase 2 parameters needed to create a VPN tunnel with the remote peer. See “Phase 2 parameters” on page 143. Enter these settings in particular:

Name	Enter a name to identify this phase 2 configuration.
Phase 1	Select the name of the phase 1 configuration that you defined.

3 Define names for the addresses or address ranges of the private networks that the VPN links. These addresses are used in the firewall policies that permit communication between the networks. For more information, see “Defining firewall addresses” on page 149.

Enter these settings in particular:

- Define an address name for the IP address and netmask of the private network behind the local FortiGate unit.
- Define an address name for the IP address and netmask of the private network behind the remote peer.

4 Define firewall policies to permit communications between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different firewall policies. For detailed information about creating firewall policies, see “Defining firewall policies” on page 150.

Policy-based VPN firewall policy

Define an IPSec policy to permit communication between the private networks. Enter these settings in particular, and then select OK:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Destination Interface/Zone	Select the FortiGate unit’s public interface.
Destination Address Name	Select the address name that you defined in Step 3 for the private network behind the remote peer.

Action	Select IPSEC.
VPN Tunnel	Select the name of the phase 1 configuration that you created in Step 1. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow outbound to enable traffic from the local network to initiate the tunnel.

Route-based VPN firewall policies

Define ACCEPT firewall policies to permit communication between the private networks. To define a policy to permit the local FortiGate unit to initiate communication, enter these settings in particular:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Destination Interface/Zone	Select the VPN Tunnel (IPSec Interface) you configured in Step 1.
Destination Address Name	Select the address name that you defined in Step 3 for the private network behind the remote peer.
Action	Select ACCEPT.
NAT	Disable.

To permit the remote peer to initiate communication, you need to define a firewall policy for communication in that direction. Enter these settings in particular:

Source Interface/Zone	Select the VPN Tunnel (IPSec Interface) you configured in Step 1.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind the remote peer.
Destination Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Action	Select ACCEPT.
NAT	Disable.

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

Configure the fixed-address VPN peer

The fixed-address VPN peer needs to retrieve the IP address from the dynamic DNS service to initiate communication with the dynamically-addressed peer that has domain name. Configure the fixed-address peer as follows:

1 Define the phase 1 parameters needed to establish a secure connection with the remote peer. For more information, see “Auto Key phase 1 parameters” on page 127. Select Advanced, enter these settings and then select OK:

Name	Enter a name to identify the VPN tunnel. This name appears in phase 2 configurations, firewall policies and the VPN monitor.
Remote Gateway	Select Dynamic DNS.
Dynamic DNS	Type the fully qualified domain name of the remote peer (for example, `example.com`).
Mode	Select Aggressive.
Peer Options	Select Accept this peer ID, and type the identifier of the dynamically-addressed FortiGate unit. This is the value you entered in the Local ID field of the other unit’s phase 1 remote gateway configuration.
Enable IPSec Interface Mode	Enable for a route-based VPN. Disable for a policy-based VPN.

2 Define the phase 2 parameters needed to create a VPN tunnel with the remote peer. See “Phase 2 parameters” on page 143. Enter these settings in particular:

Name	Enter a name to identify this phase 2 configuration.
Phase 1	Select the name of the phase 1 configuration that you defined for the remote peer. You can select the name of the remote gateway from the Dynamic DNS part of the list.

3 Define names for the addresses or address ranges of the private networks that the VPN links. See “Defining firewall addresses” on page 149. Enter these settings in particular:

- Define an address name for the IP address and netmask of the private network behind the local FortiGate unit.
- Define an address name for the IP address and netmask of the private network behind the remote peer.

4 Define the firewall policies to permit communications between the source and destination addresses. See “Defining firewall policies” on page 150. Enter these settings in particular and then select OK:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Destination Interface/Zone	Select the FortiGate unit’s public interface.
Destination Address Name	Select the address name that you defined in Step 3 for the private network behind the remote peer.

Action	Select IPSEC.
VPN Tunnel	Select the name of the phase 1 configuration that you created in Step 1. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow outbound to enable traffic from the local network to initiate the tunnel.

Route-based VPN firewall policies

Define an ACCEPT firewall policy to permit communications between the source and destination addresses. Enter these settings in particular:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Destination Interface/Zone	Select the VPN Tunnel (IPSec Interface) you configured in Step 1.
Destination Address Name	Select the address name that you defined in Step 3 for the private network behind the remote peer.
Action	Select ACCEPT.
NAT	Disable.

To permit the remote client to initiate communication, you need to define a firewall policy for communication in that direction. Enter these settings in particular:

Source Interface/Zone	Select the VPN Tunnel (IPSec Interface) you configured in Step 1.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind the remote peer.
Destination Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Action	Select ACCEPT.
NAT	Disable.

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

FortiClient dialup-client configurations

The FortiClient Host Security application is a VPN client with antivirus, antispam and firewall capabilities. This section explains how to configure dialup VPN connections between a FortiGate unit and one or more FortiClient Host Security applications.

FortiClient users are usually mobile or remote users who need to connect to a private network behind a FortiGate unit. For example, the users might be employees who connect to the office network while traveling or from their homes.

For greatest ease of use, the FortiClient application can download the VPN settings from the FortiGate unit to configure itself automatically. This section covers both automatic and manual configuration.

Note: The FortiClient configurations in this guide do not apply to the FortiClient Consumer Edition, which does not include the IPSec VPN feature.

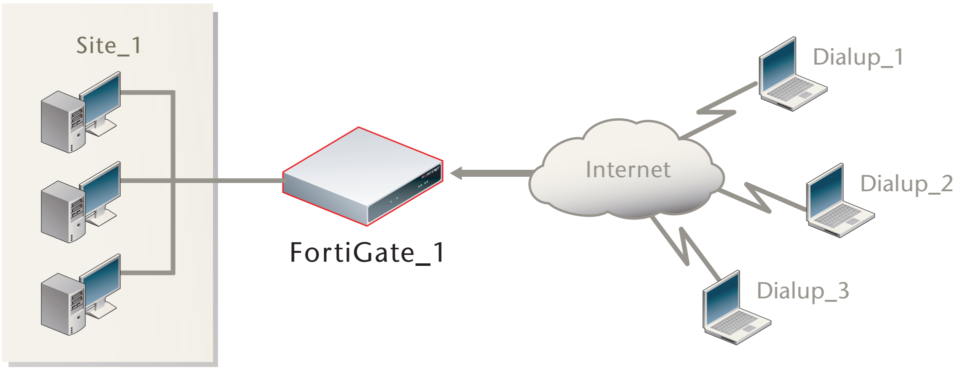
The following topics are included in this section:

- Configuration overview
- FortiClient-to-FortiGate VPN configuration steps
- Configure the FortiGate unit
- Configure the FortiClient Host Security application
- FortiClient dialup-client configuration example

Configuration overview

Dialup users typically obtain dynamic IP addresses from an ISP through Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol over Ethernet (PPPoE). Then, the FortiClient Host Security application initiates a connection to a FortiGate dialup server.

Figure 10: Example FortiClient dialup-client configuration



By default the FortiClient dialup client has the same IP address as the host PC on which it runs. If the host connects directly to the Internet, this is a public IP address. If the host is behind a NAT device, such as a router, the IP address is a private IP address. The NAT device must be NAT-T compatible to pass encrypted packets (see "NAT traversal" on page 140). The FortiClient application also can be configured to use a virtual IP address (VIP). For the duration of the connection, the FortiClient application and the FortiGate unit both use the VIP address as the IP address of the FortiClient dialup client.

The FortiClient application sends its encrypted packets to the VPN remote gateway, which is usually the public interface of the FortiGate unit. It also uses this address to download VPN settings from the FortiGate unit. See "Automatic configuration of FortiClient dialup clients" on page 56.

Peer identification

The FortiClient application can establish an IPSec tunnel with a FortiGate unit configured to act as a dialup server. When the FortiGate unit acts as a dialup server, it does not identify the client using the phase 1 remote gateway address. The IPSec tunnel is established if authentication is successful and the IPSec firewall policy associated with the tunnel permits access. There are several different ways to authenticate dialup clients and restrict access to private networks based on client credentials. For more information, see "Authenticating remote peers and clients" on page 131.

Automatic configuration of FortiClient dialup clients

The FortiClient application can obtain its VPN settings from the FortiGate VPN server. FortiClient users need to know only the FortiGate VPN server IP address and their user name and password on the FortiGate unit.

The FortiGate unit listens for VPN policy requests from clients on TCP port 8900. When the dialup client connects:

- The client initiates a Secure Sockets Layer (SSL) connection to the FortiGate unit.
- The FortiGate unit requests a user name and password from the FortiClient user. Using these credentials, it authenticates the client and determines which VPN policy applies to the client.
- Provided that authentication is successful, the FortiGate unit downloads a VPN policy to the client over the SSL connection. The information includes IPSec phase 1 and phase 2 settings, and the IP addresses of the private networks that the client is authorized to access.
- The client uses the VPN policy settings to establish an IPSec phase 1 connection and phase 2 tunnel with the FortiGate unit.

How the FortiGate unit determines which settings to apply

The FortiGate unit checks the virtual domain associated with the connection to determine which VPN policies have been configured in that domain. Each VPN policy specifies a user group and an IPSec tunnel.

Next, the FortiGate unit selects the VPN policy that matches the dialup client's user group and determines which tunnel is specified in the VPN policy. The FortiGate unit searches all IPSec firewall polices to determine which policies specify the tunnel.

Finally, the FortiGate unit searches the implicated IPSec firewall policies to determine which private network(s) the dialup clients may access. The rest of the VPN policy information is retrieved from the existing IPSec phase 1 and phase 2 parameters in the dialup-client configuration.

Using virtual IP addresses

When the FortiClient host PC is located behind a NAT device, unintended IP address overlap issues may arise between the private networks at the two ends of the tunnel. For example, the client's host might receive a private IP address from a DHCP server on its network that by co-incidence is the same as a private IP address on the network behind the FortiGate unit. A conflict will occur in the host's routing table and the FortiClient Host Security application will be unable to send traffic through the tunnel. Configuring virtual IP (VIP) addresses for FortiClient applications prevents this problem.

Using VIPs ensures that client IP addresses are in a predictable range. You can then define firewall policies that allow access only to that source address range. If you do not use VIP, the firewall policies must allow all source addresses because you cannot predict the IP address for a remote mobile user.

The FortiClient application must not have the same IP address as any host on the private network behind the FortiGate unit or any other connected FortiClient application. You can ensure this by reserving a range of IP addresses on the private network for FortiClient users. Or, you can assign FortiClient VIPs from an uncommonly used subnet such as 10.254.254.0/24 or 192.168.254.0/24.

You can reserve a VIP address for a particular client according to its device MAC address and type of connection. The DHCP server then always assigns the reserved VIP address to the client. For more information about this feature, see the "dhcp reserved-address" section in the "system" chapter of the *FortiGate CLI Reference*.

Note: To determine the VIP address that the FortiClient Host Security application is using, type `ipconfig /all` at the Windows Command Prompt on the FortiClient host. The output will also show the IP address that has been assigned to the host Network Interface Card (NIC).

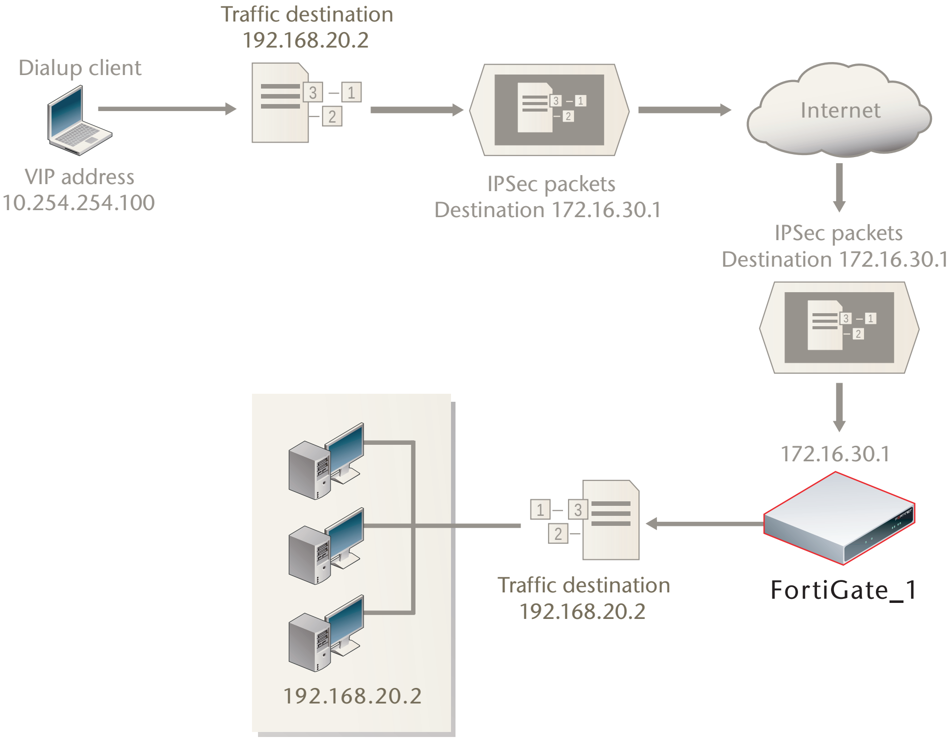
It is best to assign VIPs using DHCP over IPSec. The FortiGate dialup server can act as a DHCP server or relay requests to an external DHCP server. You can also configure VIPs manually on FortiClient applications, but it is more difficult to ensure that all clients use unique addresses.

Note: If you assign a VIP on the private network behind the FortiGate unit and enable DHCP-IPsec (a phase 2 advanced option), the FortiGate unit acts as a proxy on the local private network for the FortiClient dialup client. Whenever a host on the network behind the dialup server issues an ARP request for the device MAC address of the FortiClient host, the FortiGate unit answers the ARP request on behalf of the FortiClient host and forwards the associated traffic to the FortiClient host through the tunnel. For more information, see "DHCP-IPSec" on page 145.

Note: FortiGate units fully support RFC 3456, *Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode*. The FortiGate DHCP over IPSec feature can be enabled to allocate VIP addresses to FortiClient dialup clients using a FortiGate DHCP server if a policy-based VPN is configured. DHCP over IPSec is not compatible with FortiGate route-based VPNs.

Figure 11 shows an example of a FortiClient-to-FortiGate VPN where the FortiClient application is assigned a VIP on an uncommonly used subnet. The diagram also shows that while the destination for the information in the encrypted packets is the private network behind the FortiGate unit, the destination of the IPSec packets themselves is the public interface of the FortiGate unit that acts as the end of the VPN tunnel.

Figure 11: IP address assignments in a FortiClient dialup-client configuration



FortiClient dialup-client infrastructure requirements

- To support policy-based VPNs, the FortiGate dialup server may operate in either NAT/Route mode or Transparent mode. NAT/Route mode is required if you want to create a route-based VPN.
- If the FortiClient dialup clients will be configured to obtain VIP addresses through FortiGate DHCP relay, a DHCP server must be available on the network behind the FortiGate unit and the DHCP server must have a direct route to the FortiGate unit.
- If the FortiGate interface to the private network is not the default gateway, the private network behind the FortiGate unit must be configured to route IP traffic destined for dialup clients back (through an appropriate gateway) to the FortiGate interface to the private network. As an alternative, you can configure the IPSec firewall policy on the FortiGate unit to perform inbound NAT on IP packets. Inbound NAT translates the source addresses of inbound decrypted packets into the IP address of the FortiGate interface to the local private network.

FortiClient-to-FortiGate VPN configuration steps

Configuring dialup client capability for FortiClient dialup clients involves the following general configuration steps:

- If you will be using VIP addresses to identify dialup clients, determine which VIP addresses to use. As a precaution, consider using VIP addresses that are not commonly used.
- Configure the FortiGate unit to act as a dialup server. See “Configure the FortiGate unit” on page 59.
- If the dialup clients will be configured to obtain VIP addresses through DHCP over IPSec, configure the FortiGate unit to act as a DHCP server or to relay DHCP requests to an external DHCP server.
- Configure the dialup clients. See “Configure the FortiClient Host Security application” on page 64.

Note: When a FortiGate unit has been configured to accept connections from FortiClient dialup-clients, you can optionally arrange to have an IPSec VPN configuration downloaded to FortiGate dialup clients automatically. For more information, see “Configuring the FortiGate unit as a VPN policy server” on page 62.

Configure the FortiGate unit

Configuring the FortiGate unit to establish VPN connections with FortiClient Host Security users involves the following steps:

- configure the VPN settings
- if the dialup clients use automatic configuration, configure the FortiGate unit as a VPN policy server
- if the dialup clients obtain virtual IP addresses by DHCP over IPSec, configure an IPSec DHCP server or relay (policy-based VPN only)

The procedures in this section cover basic setup of policy-based and route-based VPNs compatible with FortiClient Host Security. A route-based VPN is simpler to configure, but it does not support DHCP over IPSec assignment of virtual addresses to FortiClient users

Only common preshared key and certificate authentication is shown here. For information about other types of authentication, see the *Authenticating FortiClient Dialup Clients Technical Note*.

The default FortiGate phase 1 and 2 VPN settings match the default FortiClient VPN settings if you have registered (licensed) your FortiClient application.

Configuring FortiGate unit VPN settings

To configure FortiGate unit VPN settings to support FortiClient users, you need to:

- configure the FortiGate Phase 1 VPN settings
- configure the FortiGate Phase 2 VPN settings
- add the firewall policy

1 At the local FortiGate unit, define the phase 1 configuration needed to establish a secure connection with the FortiClient peer. See “Auto Key phase 1 parameters” on page 127. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel. This name appears in phase 2 configurations, firewall policies and the VPN monitor.
Remote Gateway	Select Dialup User.
Local Interface	Select the interface through which clients connect to the FortiGate unit.
Mode	Select Main (ID Protection).
Authentication Method	Select Pre-shared Key.
Pre-shared Key	Enter the pre-shared key. This must be the same preshared key provided to the FortiClient users.
Peer option	Select Accept any peer ID.
Enable IPSec Interface Mode	You must select Advanced to see this setting. If IPSec Interface Mode is enabled, the FortiGate unit creates a virtual IPSec interface for a route-based VPN. Disable this option if you want to create a policy-based VPN. After you select OK to create the phase 1 configuration, you cannot change this setting.

2 Define the phase 2 parameters needed to create a VPN tunnel with the FortiClient peer. See “Phase 2 parameters” on page 143. Enter these settings in particular:

Name	Enter a name to identify this phase 2 configuration.
Phase 1	Select the name of the phase 1 configuration that you defined.
Advanced	Select to configure the following optional setting.
DHCP-IPsec	Select if you provide virtual IP addresses to clients using DHCP.

3 Define names for the addresses or address ranges of the private networks that the VPN links. These addresses are used in the firewall policies that permit communication between the networks. For more information, see “Defining firewall addresses” on page 149.

Enter these settings in particular:

- Define an address name for the individual address or the subnet address that the dialup users access through the VPN.
- If FortiClient users are assigned virtual IP addresses, define an address name for the subnet to which these VIPs belong.

4 Define firewall policies to permit communication between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different firewall policies. For detailed information about creating firewall policies, see “Defining firewall policies” on page 150.

Policy-based VPN firewall policy

Define an IPSec firewall policy to permit communications between the source and destination addresses. Enter these settings in particular:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Destination Interface/Zone	Select the FortiGate unit’s public interface.
Destination Address Name	If FortiClient users are assigned VIPs, select the address name that you defined in Step 3 for the VIP subnet. Otherwise, select All.
Action	Select IPSEC.
VPN Tunnel	Select the name of the phase 1 configuration that you created in Step 1. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow Outbound if you want to allow hosts on the private network to initiate communications with the FortiClient users after the tunnel is established.

Route-based VPN firewall policies

Define an ACCEPT firewall policy to permit communications between the source and destination addresses. Enter these settings in particular:

Source Interface/Zone	Select the VPN Tunnel (IPSec Interface) you configured in Step 1.
Source Address Name	Select All.
Destination Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address Name	Select All.
Action	Select ACCEPT.
NAT	Disable.

If you want to allow hosts on the private network to initiate communications with the FortiClient users after the tunnel is established, you need to define a firewall policy for communication in that direction. Enter these settings in particular:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select All.
Destination Interface/Zone	Select the VPN Tunnel (IPSec Interface) you configured in Step 1.
Destination Address Name	Select All.
Action	Select ACCEPT.
NAT	Disable.

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

Configuring the FortiGate unit as a VPN policy server

When a FortiClient application set to automatic configuration connects to the FortiGate unit, the FortiGate unit requests a user name and password. If the user supplies valid credentials, the FortiGate unit downloads the VPN settings to the FortiClient application.

You must do the following to configure the FortiGate unit to work as a VPN policy server for FortiClient automatic configuration:

1. Create user accounts for FortiClient users.
2. Create a user group for FortiClient users and the user accounts that you created in step 1.

   For more information about user accounts and user groups, refer to the *FortiGate User Authentication Guide* or to the User chapter of the *FortiGate Administration Guide*.
3. Connect to the FortiGate unit CLI and configure VPN policy distribution as follows:

```
config vpn ipsec forticlient
  edit <policy_name>
    set phase2name <tunnel_name>
    set usergroupname <group_name>
    set status enable
  end
```

`<tunnel_name>` must be the Name you specified in the step 2 of “Configure the FortiGate unit” on page 59. `<group_name>` must be the name of the user group your created for FortiClient users.

Configuring DHCP service on the FortiGate unit

If the FortiClient dialup clients are configured to obtain a VIP address using DHCP, configure the FortiGate dialup server to either:

- relay DHCP requests to a DHCP server behind the FortiGate unit (see “To configure DHCP relay on the FortiGate unit” below).
- act as a DHCP server (see “To configure a DHCP server on the FortiGate unit” on page 63).

To configure DHCP relay on the FortiGate unit

1. Go to **System > DHCP > Service**.
2. Expand the row that corresponds to the interface to the Internet (for example, external or wan1).
3. In the Relay row beneath the interface name, select the Edit icon.
4. Select DHCP Relay Agent Enable
5. For Type select IPSEC.
6. In the DHCP Server IP field, type the IP address of the DHCP server.
7. Select OK.
8. If a router is installed between the FortiGate unit and the DHCP server, define a static route to the DHCP server. See the “Router Static” chapter of the *FortiGate Administration Guide*.

To configure a DHCP server on the FortiGate unit

1. Go to **System > DHCP > Service**.
2. Expand the row that corresponds to the interface to the Internet (for example, external or wan1).
3. In the Servers row beneath the interface name, select the Add DHCP Server icon (+).
4. In the Name field, type a name for the FortiGate DHCP server configuration.
5. Select IPSec, enter the following information and select OK:

IP Range

Enter the range of VIP addresses that the DHCP server can dynamically assign to dialup clients when they connect. As a precaution, do not assign VIP addresses that match the private network behind the FortiGate unit (for example, if the dialup clients need to access a host on local subnet 192.168.12.0/24, you could configure the DHCP server to assign any VIP address in the `10.254.254.100` to `10.254.254.125` range). If you need to exclude specific IP addresses from the range, you can define an exclusion range (see Advanced below).

Network Mask

Enter the network mask of the IP addresses that you specified in the IP Range fields (for example, `255.255.255.0` for a class C network).

Default Gateway

Enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.

Domain

If you want the FortiGate unit to assign a domain name to dialup clients when they connect, enter the registered domain name.

Lease Time

Specify a lease time:

- Select Unlimited to allow the dialup client to use the assigned IP address for an unlimited amount of time (that is, until the client disconnects).
- Enter the amount of time (in days, hours, and minutes) that the dialup client may use the assigned IP address, after which the dialup client must request new settings from the DHCP server. The range is from 5 minutes to 100 days.

Advanced

Set these Advanced options as applicable:

- In the DNS Server 1 field, type the IP address of the DNS server that dialup clients can access after the tunnel has been established. You can specify up to three DNS servers.
- In the WINS Server 1 field, type the IP address of the Windows Internet Service (WINS) server that dialup clients can access after the tunnel has been established. You can specify a second WINS server if required.
- If you want to send DHCP options to the dialup client, type the option code in the Code field, and if applicable, type any associated data in the Option field (for more information, see RFC 2132, *DHCP Options and BOOTP Vendor Extensions*).
- To specify any VIP addresses that must be excluded from the VIP address range, select Add, and then type the starting and ending IP addresses. You can add more than one range to exclude.

Configure the FortiClient Host Security application

The following procedure explains how to configure the FortiClient Host Security application to communicate with a remote FortiGate dialup server using the VIP address that you specify manually.

Configuring FortiClient to work with VPN policy distribution

If the remote FortiGate gateway is configured as a VPN policy server, you can configure the FortiClient software to download the VPN settings from the FortiGate gateway.

Note: For VPNs with automatic configuration, only preshared keys are supported. Certificates are not supported.

To add a VPN with automatic configuration on the FortiClient PC

1 Go to **VPN > Connections**.

2 Select Advanced and then select Add.

3 In the New Connection dialog box, enter a connection name.

4 For Configuration, select Automatic.

5 For Policy Server, enter the IP address or FQDN of the FortiGate gateway.

6 Select OK.

Configuring FortiClient manually

This procedure explains how to configure the FortiClient application manually using the default IKE and IPSec settings. For more information, refer to the *FortiClient Host Security User Guide*.

This procedure includes instructions for configuring a virtual IP for the FortiClient application, either manually or using DHCP over IPSec.

To create a FortiClient VPN configuration

1 Go to **VPN > Connections**.

2 Select Advanced and then select Add.

3 Enter the following information:

Connection Name	Enter a descriptive name for the connection.
Configuration	Select Manual
Remote Gateway	Enter the IP address or the fully qualified domain name (FQDN) of the remote gateway.
Remote Network	Enter the IP address and netmask of the network behind the FortiGate unit.
Authentication Method	Select Pre-shared Key.
Pre-shared Key	Enter the pre-shared key.

4 Follow the remaining steps only if you want to configure a VIP. Otherwise, select OK.

5 Select Advanced.

6 Enable Acquire a virtual IP address and then select the adjacent Config button.

7 Enter the following information and select OK.

Options	Select one of these options:
DHCP	Obtain virtual IP address from the FortiGate unit using DHCP over IPSec.
Manually Set	Assign the virtual IP address manually using the settings in the Manual VIP section.
Manual VIP	These settings are available only if you select Manually Set in the Options section.
IP	Enter the IP address that the FortiClient dialup client uses. This address must not conflict with any IP address at either end of the VPN tunnel.
Subnet Mask	Enter the subnet for the private network.
DNS Server **WINS Server**	Optionally, enter the addresses of the DNS and WINS servers that the FortiClient user can access through the VPN.

8 Select OK twice to close the dialog boxes.

9 Repeat this procedure for each FortiClient dialup client.

Adding XAuth authentication

Extended Authentication (XAuth) increases security by requiring additional user authentication in a separate exchange at the end of the VPN phase 1 negotiation. The FortiGate unit challenges the user for a user name and password. It then forwards the user’s credentials to an external RADIUS or LDAP server for verification.

Implementation of XAuth requires configuration at both the FortiGate unit and the FortiClient application. For information about configuring a FortiGate unit as an XAuth server, see “Using the FortiGate unit as an XAuth server” on page 141. The following procedure explains how to configure the FortiClient application.

To configure the FortiClient Host Security application

In the FortiClient Host Security application, make the following changes to the VPN configuration to enable XAuth authentication to the FortiGate unit.

1 Go to **VPN > Connections**, select the VPN connection you want to modify, and then select Advanced > Edit.

2 Select Advanced.

3 Select the eXtended Authentication check box and then select the Config button to the right of it.

4 In the Extended Authentication (XAuth) dialog box, either:

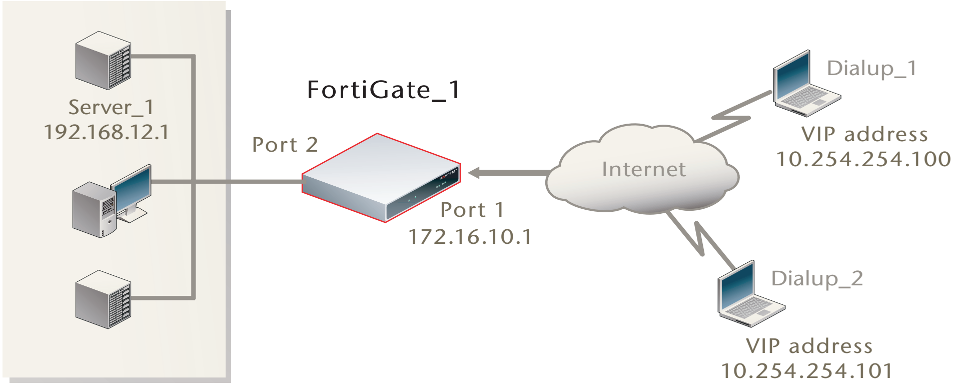
- Select Prompt to login. The FortiClient Host Security application prompts the user for a user name and password when it receives the XAuth challenge. This is the default.
- Clear the Prompt to login check box and enter the user name and password values into the User Name and Password fields. The FortiClient Host Security application automatically responds to the XAuth challenge with these values.

5 Select OK to close all dialog boxes.

FortiClient dialup-client configuration example

This example demonstrates how to set up a FortiClient dialup-client IPSec VPN that uses preshared keys for authentication purposes. In the example configuration, the DHCP over IPSec feature is enabled in the FortiClient Host Security application so that the FortiClient Host Security application can acquire a VIP address through FortiGate DHCP relay.

Figure 12: Example FortiClient dialup-client configuration



In the example configuration:

- VIP addresses that are not commonly used (in this case, 10.254.254.0/24) are assigned to the FortiClient dialup clients using a DHCP server.
- The dialup clients are provided access to Server_1 at IP address 192.168.12.1 behind FortiGate_1.
- The other network devices are assigned IP addresses as shown in Figure 12.
- NAT is enabled in the firewall policy to translate the source IP addresses of the decrypted inbound packets to the IP address of the FortiGate interface to the private network.

Configuring FortiGate_1

When a FortiGate unit receives a connection request from a dialup client, it uses IPSec phase 1 parameters to establish a secure connection and authenticate the client. Then, if the firewall policy permits the connection, the FortiGate unit establishes the tunnel using IPSec phase 2 parameters and applies the IPSec firewall 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 dialup clients and establish a secure connection. See “Define the phase 1 parameters” on page 67.
- Define the phase 2 parameters that the FortiGate unit needs to create a VPN tunnel and enable all dialup clients having VIP addresses on the 10.254.254.0/24 network to connect using the same tunnel definition. See “Define the phase 2 parameters” on page 67.

- Create an IPSec firewall policy to control the permitted services and permitted direction of traffic between the IP source address and the dialup clients. A single policy controls both inbound and outbound IP traffic through the VPN tunnel. See “Define the IPSec firewall policy” on page 68.
- Configure the FortiGate unit to relay DHCP requests from dialup clients to the DHCP server. See “Configure FortiGate_1 to assign VIPs” on page 69.

Define the phase 1 parameters

The phase 1 configuration defines the parameters that FortiGate_1 will use to authenticate dialup clients and establish a secure connection. For the purposes of this example, a preshared key will be used to authenticate dialup clients. The same preshared key must be specified when you configure the FortiClient Host Security application on each remote host.

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.

To define the phase 1 parameters

1 Go to **VPN > IPSEC > Auto Key**.

2 Select Create Phase 1, enter the following information, and select OK:

Name	Enter a name to identify the VPN tunnel (for example, `FG1toDialupClients`).
Remote Gateway	Dialup User
Local Interface	Port 1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Disable

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 > Auto Key** and select Create Phase 2.

2 Select Advanced, enter the following information, and select OK:

Name	Enter a name for the phase 2 configuration (for example, `FG1toDialupP2`).
Phase 1	Select the gateway that you defined previously (for example, `FG1toDialupClients`).
Advanced	Select DHCP-IPsec Enable.

Define the IPSec firewall policy

Firewall policies control all IP traffic passing between a source address and a destination address. An IPSec firewall 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 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 address. The IP source address corresponds to the private IP address of Server_1 behind the FortiGate unit (for example, 192.168.12.1/32).

Because VIP addresses are assigned through FortiGate DHCP relay, you do not need to define a specific destination address. Instead, you will select the predefined destination address “all” in the IPSec firewall policy to refer to dialup clients.

To define the private IP address of Server_1 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, `Server_1`).
Subnet/IP Range	Enter the private IP address of the server (for example `192.168.12.1/32`).

To define the firewall policy

1 Go to **Firewall > Policy**.

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

Source Interface/Zone	Port 2.
Source Address Name	`Server_1`
Destination Interface/Zone	Port 1
Destination Address Name	`all`
Schedule	As required.
Service	As required.
Action	IPSEC
VPN Tunnel	`FG1toDialupClients`.
Allow Inbound	Enable
Allow Outbound	Enable if you want to allow hosts on the private network behind the FortiGate unit to initiate communications with the FortiClient users after the tunnel is established.
Inbound NAT	Enable

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

Configure FortiGate_1 to assign VIPs

In the example configuration, dialup clients obtain VIP addresses through a FortiGate DHCP server.

Note: You may optionally configure the FortiGate unit to act as a DHCP relay instead. See "To configure DHCP relay on the FortiGate unit" on page 62.

To configure a DHCP server on the FortiGate unit

1. Go to **System > DHCP > Service**.
2. Expand the row that corresponds to Port 1.
3. In the Servers row beneath the interface name, select the Add DHCP Server icon.
4. Select IPSec, enter the following information and select OK:

Name	Enter a name for the DHCP server, `ClientVIPs` for example.
Enable	Select
Type	Select IPSEC.
IP Range	`10.254.254.1 - 10.254.254.100`
Network Mask	`255.255.255.0`
Default Gateway	Enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.

Configuring the FortiClient Host Security application

The following procedure explains how to configure the FortiClient Host Security application to connect to FortiGate_1 and broadcast a DHCP request. The dialup client uses the VIP address acquired through FortiGate DHCP relay as its IP source address for the duration of the connection.

To configure FortiClient

1. At the remote host, start FortiClient.
2. Go to **VPN > Connections** and select Add.
3. In the Connection Name field, type a descriptive name for the connection.
4. In the Remote Gateway field, type the public static IP address of the FortiGate unit.
5. In the Remote Network fields, type the private IP address and netmask of the server that FortiClient needs to access behind the FortiGate unit (for example, `192.168.12.1/255.255.255.255`).
6. From the Authentication Method list, select Preshared Key.
7. In the Preshared Key field, type the preshared key. The value must be identical to the preshared key that you specified previously in the FortiGate_1 configuration.
8. Select Advanced.
9. In the Advanced Settings dialog box, select Acquire virtual IP address and then select Config.
10. Verify that the Dynamic Host Configuration Protocol (DHCP) over IPSec option is selected, and then select OK.
11. Select OK twice to close the dialog boxes.

12 Exit FortiClient and repeat this procedure at all other remote hosts.

FortiGate dialup-client configurations

This section explains how to set up a FortiGate dialup-client IPSec VPN. In a FortiGate dialup-client configuration, a FortiGate unit with a static IP address acts as a dialup server and a FortiGate unit having a dynamic IP address initiates a VPN tunnel with the FortiGate dialup server.

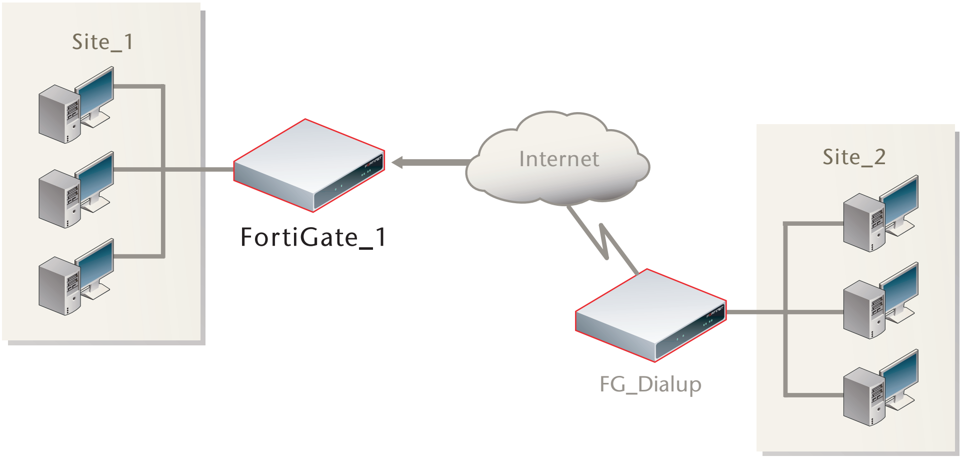
The following topics are included in this section:

- Configuration overview
- FortiGate dialup-client configuration steps
- Configure the server to accept FortiGate dialup-client connections
- Configure the FortiGate dialup client

Configuration overview

A dialup client can be a FortiGate unit—the FortiGate dialup client typically obtains a dynamic IP address from an ISP through the Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol over Ethernet (PPPoE) before initiating a connection to a FortiGate dialup server.

Figure 13: Example FortiGate dialup-client configuration



In a dialup-client configuration, the FortiGate dialup server does not rely on a phase 1 remote gateway address to establish an IPSec VPN connection with dialup clients. As long as authentication is successful and the IPSec firewall policy associated with the tunnel permits access, the tunnel is established.

Several different ways to authenticate dialup clients and restrict access to private networks based on client credentials are available. To authenticate FortiGate dialup clients and help to distinguish them from FortiClient dialup clients when multiple clients will be connecting to the VPN through the same tunnel, we recommend that you assign a unique identifier (local ID) to each FortiGate dialup client. For more information, see "Authenticating remote peers and clients" on page 131.

Note: Whenever you add a unique identifier (local ID) to a FortiGate dialup client for identification purposes, you must select Aggressive mode on the FortiGate dialup server and also specify the identifier as a peer ID on the FortiGate dialup server. For more information, see "Enabling VPN access using user accounts and pre-shared keys" on page 135.

Users behind the FortiGate dialup server cannot initiate the tunnel because the FortiGate dialup client does not have a static IP address. After the tunnel is initiated by users behind the FortiGate dialup client, traffic from the private network behind the FortiGate dialup server can be sent to the private network behind the FortiGate dialup client.

Encrypted packets from the FortiGate dialup client are addressed to the public interface of the dialup server. Encrypted packets from the dialup server are addressed either to the public IP address of the FortiGate dialup client (if the dialup client connects to the Internet directly), or if the FortiGate dialup client is behind a NAT device, encrypted packets from the dialup server are addressed to the public IP address of the NAT device.

Note: If a router with NAT capabilities is in front of the FortiGate dialup client, the router must be NAT-T compatible for encrypted traffic to pass through the NAT device. For more information, see "NAT traversal" on page 140.

When the FortiGate dialup server decrypts a packet from the FortiGate dialup client, the source address in the IP header may be one of the following values, depending on the configuration of the network at the far end of the tunnel:

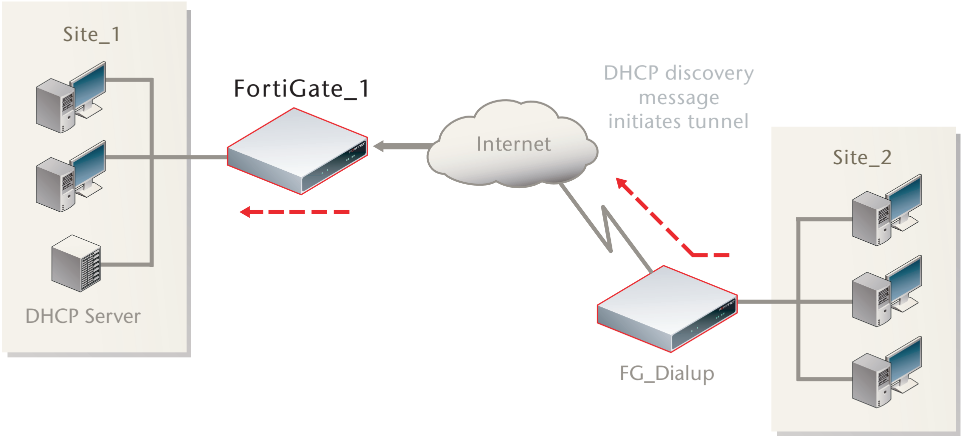
- If the FortiGate dialup client connects to the Internet directly, the source address will be the private IP address of a host or server on the network behind the FortiGate dialup client.
- If the FortiGate dialup client is behind a NAT device, the source address will be the public IP address of the NAT device.

In some cases, computers on the private network behind the FortiGate dialup client may (by co-incidence) have IP addresses that are already used by computers on the network behind the FortiGate dialup server. In this type of situation (ambiguous routing), conflicts may occur in one or both of the FortiGate routing tables and traffic destined for the remote network through the tunnel may not be sent.

In many cases, computers on the private network behind the FortiGate dialup client will most likely obtain IP addresses from a local DHCP server behind the FortiGate dialup client. However, unless the local and remote networks use different private network address spaces, unintended ambiguous routing and/or IP-address overlap issues may arise.

To avoid these issues, you can configure FortiGate DHCP relay on the dialup client instead of using a DHCP server on the network behind the dialup client. The FortiGate dialup client can be configured to relay DHCP requests from the local private network to a DHCP server that resides on the network behind the FortiGate dialup server (see Figure 14 on page 73). You configure the FortiGate dialup client to pass traffic from the local private network to the remote network by enabling FortiGate DHCP relay on the FortiGate dialup client interface that is connected to the local private network.

Figure 14: Preventing network overlap in a FortiGate dialup-client configuration



Afterward, when a computer on the network behind the dialup client broadcasts a DHCP request, the dialup client relays the message through the tunnel to the remote DHCP server. The remote DHCP server responds with a private IP address for the computer. To avoid ambiguous routing and network overlap issues, the IP addresses assigned to computers behind the dialup client cannot match the network address space used by the private network behind the FortiGate dialup server.

When the DHCP server resides on the private network behind the FortiGate dialup server as shown in Figure 14, the IP destination address specified in the IPSec firewall policy on the FortiGate dialup client must refer to that network.

Note: If the DHCP server is not directly connected to the private network behind the FortiGate dialup server (that is, its IP address does not match the IP address of the private network), you must add (to the FortiGate dialup client's routing table) a static route to the DHCP server, and the IP destination address specified in the IPSec firewall policy on the FortiGate dialup client must refer to the DHCP server address. In this case, the DHCP server must be configured to assign IP addresses that do not belong to the network on which the DHCP server resides. In addition, the IP addresses cannot match the network address space used by the private network behind the FortiGate dialup server.

FortiGate dialup-client infrastructure requirements

- To support a policy-based VPN, the FortiGate dialup server may operate in either NAT/Route mode or Transparent mode. NAT/Route mode is required if you want to create a route-based VPN.
- The FortiGate dialup server has a static public IP address.

- Computers on the private network behind the FortiGate dialup client can obtain IP addresses either from a DHCP server behind the FortiGate dialup client, or a DHCP server behind the FortiGate dialup server.
  - If the DHCP server resides on the network behind the dialup client, the DHCP server must be configured to assign IP addresses that do not match the private network behind the FortiGate dialup server.
  - If the DHCP server resides on the network behind the FortiGate dialup server, the DHCP server must be configured to assign IP addresses that do not match the private network behind the FortiGate dialup client. In addition, the FortiGate dialup client routing table must contain a static route to the DHCP server (see the “Router Static” chapter of the *FortiGate Administration Guide*).

FortiGate dialup-client configuration steps

The procedures in this section assume that computers on the private network behind the FortiGate dialup client obtain IP addresses from a local DHCP server. The assigned IP addresses do not match the private network behind the FortiGate dialup server.

Note: In situations where IP-address overlap between the local and remote private networks is likely to occur, FortiGate DHCP relay can be configured on the FortiGate dialup client to relay DHCP requests to a DHCP server behind the FortiGate dialup server. For more information, see “To configure DHCP relay on the FortiGate unit” on page 62.

Configuring dialup client capability for FortiGate dialup clients involves the following general configuration steps:

- Determine which IP addresses to assign to the private network behind the FortiGate dialup client, and add the IP addresses to the DHCP server behind the FortiGate dialup client. Refer to the software supplier’s documentation to configure the DHCP server.
- Configure the FortiGate dialup server. See “Configure the server to accept FortiGate dialup-client connections” on page 75.
- Configure the FortiGate dialup client. See “Configure the FortiGate dialup client” on page 76.

Configure the server to accept FortiGate dialup-client connections

Before you begin, optionally reserve a unique identifier (peer ID) for the FortiGate dialup client. The dialup client will supply this value to the FortiGate dialup server for authentication purposes during the IPSec phase 1 exchange. In addition, the value will enable you to distinguish FortiGate dialup-client connections from FortiClient dialup-client connections. The same value must be specified on the dialup server and on the dialup client.

1. At the FortiGate dialup server, define the phase 1 parameters needed to authenticate the FortiGate dialup client and establish a secure connection. See "Auto Key phase 1 parameters" on page 127. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel. This name appears in phase 2 configurations, firewall policies and the VPN monitor.
Remote Gateway	Select Dialup User.
Local Interface	Select the interface through which clients connect to the FortiGate unit.
Mode	If you will be assigning an ID to the FortiGate dialup client, select Aggressive.
Peer Options	If you will be assigning an ID to the FortiGate dialup client, select Accept this peer ID and type the identifier that you reserved for the FortiGate dialup client into the adjacent field.
Enable IPSec Interface Mode	You must select Advanced to see this setting. If IPSec Interface Mode is enabled, the FortiGate unit creates a virtual IPSec interface for a route-based VPN. Disable this option if you want to create a policy-based VPN. After you select OK to create the phase 1 configuration, you cannot change this setting.

2. Define the phase 2 parameters needed to create a VPN tunnel with the FortiGate dialup client. See "Phase 2 parameters" on page 143. Enter these settings in particular:

Name	Enter a name to identify this phase 2 configuration.
Phase 1	Select the name of the phase 1 configuration that you defined.

3. Define names for the addresses or address ranges of the private networks that the VPN links. See "Defining firewall addresses" on page 149. Enter these settings in particular:
   - Define an address name for the server, host, or network behind the FortiGate dialup server.
   - Define an address name for the private network behind the FortiGate dialup client.
4. Define the firewall policies to permit communications between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different firewall policies. For detailed information about creating firewall policies, see "Defining firewall policies" on page 150.

Policy-based VPN firewall policy

Define an IPSec firewall policy. Enter these settings in particular:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Destination Interface/Zone	Select the FortiGate unit's public interface.
Destination Address Name	Select the address name that you defined in Step 3.
Action	Select IPSEC.
VPN Tunnel	Select the name of the phase 1 configuration that you created in Step 1. 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.

Route-based VPN firewall policy

Define an ACCEPT firewall policy to permit communications between hosts on the private network behind the FortiGate dialup client and the private network behind this FortiGate dialup server. Because communication cannot be initiated in the opposite direction, there is only one policy. Enter these settings in particular:

Source Interface/Zone	Select the VPN tunnel (IPSec interface) created in Step 1.
Source Address Name	Select All.
Destination Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address Name	Select All.
Action	Select ACCEPT.
NAT	Disable

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

Configure the FortiGate dialup client

Configure the FortiGate dialup client as follows:

1 At the FortiGate dialup client, define the phase 1 parameters needed to authenticate the dialup server and establish a secure connection. See "Auto Key phase 1 parameters" on page 127. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel. This name appears in phase 2 configurations, firewall policies and the VPN monitor.
Remote Gateway	Select Static IP Address.
IP Address	Type the IP address of the dialup server's public interface.
Local Interface	Select the interface that connects to the public network.
Mode	Because the FortiGate dialup client has a dynamic IP address, select Aggressive.
Advanced	Select to view the following options.

Local ID	If you defined a peer ID for the dialup client in the FortiGate dialup server configuration, enter the identifier of the dialup client. The value must be identical to the peer ID that you specified previously in the FortiGate dialup server configuration.
Enable IPSec Interface Mode	If IPSec Interface Mode is enabled, the FortiGate unit creates a virtual IPSec interface for a route-based VPN. Disable this option if you want to create a policy-based VPN. After you select OK to create the phase 1 configuration, you cannot change this setting.

2 Define the phase 2 parameters needed to create a VPN tunnel with the dialup server. See “Phase 2 parameters” on page 143. Enter these settings in particular:

Name	Enter a name to identify this phase 2 configuration.
Phase 1	Select the set of phase 1 parameters that you defined in step 1.

3 Define names for the addresses or address ranges of the private networks that the VPN links. See “Defining firewall addresses” on page 149. Enter these settings in particular:

- Define an address name for the server, host, or network behind the FortiGate dialup server.
- Define an address name for the private network behind the FortiGate dialup client.

4 Define firewall policies to permit communication between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different firewall policies. For detailed information about creating firewall policies, see “Defining firewall policies” on page 150.

Policy-based VPN firewall policy

Define an IPSec firewall policy to permit communications between the source and destination addresses. Enter these settings in particular:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Destination Interface/Zone	Select the FortiGate unit’s public interface.
Destination Address Name	Select the address name that you defined in Step 3 for the private network behind the dialup server.
Action	Select IPSEC.
VPN Tunnel	Select the name of the phase 1 configuration that you created in Step 1. 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.

Route-based VPN firewall policy

Define an ACCEPT firewall policy to permit communications between hosts on the private network behind this FortiGate dialup client and the private network behind the FortiGate dialup server. Because communication cannot be initiated in the opposite direction, there is only one policy. Enter these settings in particular:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select All.
Destination Interface/Zone	Select the VPN tunnel (IPSec interface) created in Step 1.
Destination Address Name	Select All.
Action	Select ACCEPT.
NAT	Disable

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

Internet-browsing configuration

This section explains how to support secure web browsing performed by dialup VPN clients, and/or hosts behind a remote VPN peer. Remote users can access the private network behind the local FortiGate unit and browse the Internet securely. All traffic generated remotely is subject to the firewall policy that controls traffic on the private network behind the local FortiGate unit.

The following topics are included in this section:

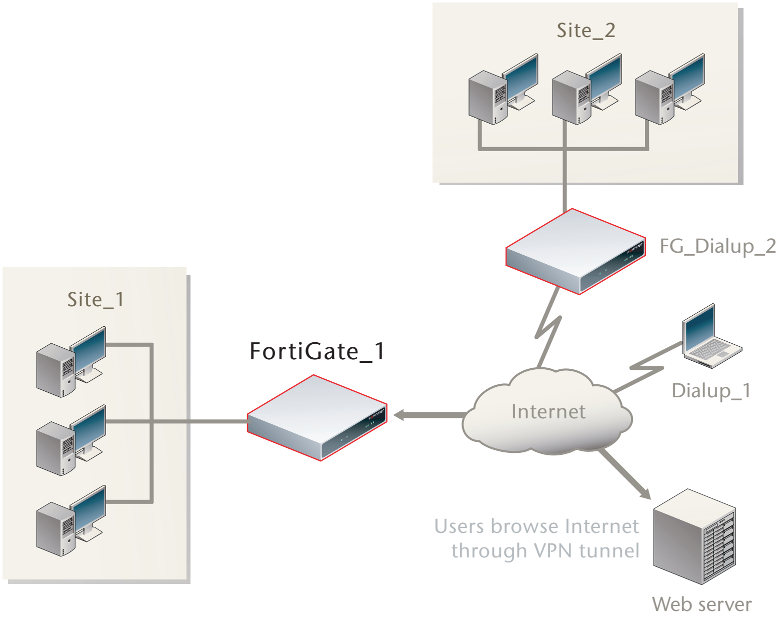
- Configuration overview
- Creating an Internet browsing firewall policy
- Routing all remote traffic through the VPN tunnel

Configuration overview

A VPN provides secure access to a private network behind the FortiGate unit. You can also enable VPN clients to access the Internet securely. The FortiGate unit inspects and processes all traffic between the VPN clients and hosts on the Internet according to the Internet browsing policy. This is accomplished even though the same FortiGate interface is used for both encrypted VPN client traffic and unencrypted Internet traffic.

In Figure 15, FortiGate_1 enables secure Internet browsing for FortiClient Host Security users such as Dialup_1 and users on the Site_2 network behind FortiGate_2, which could be a VPN peer or a dialup client.

Figure 15: Example Internet-browsing configuration



You can adapt any of the following configurations to provide secure Internet browsing:

- a gateway-to-gateway configuration (see "Gateway-to-gateway configurations" on page 19)
- a FortiClient dialup-client configuration (see "FortiClient dialup-client configurations" on page 55)
- a FortiGate dialup-client configuration (see "FortiGate dialup-client configurations" on page 71)

The procedures in this section assume that one of these configurations is in place, and that it is operating properly.

To create an internet-browsing configuration based on an existing gateway-to-gateway configuration, you must edit the gateway-to-gateway configuration as follows:

- On the FortiGate unit that will provide Internet access, create an Internet browsing firewall policy. See "Creating an Internet browsing firewall policy", below.
- Configure the remote peer or client to route all traffic through the VPN tunnel. You can do this on a FortiGate unit or on a FortiClient Host Security application. See "Routing all remote traffic through the VPN tunnel" on page 81.

Creating an Internet browsing firewall policy

On the FortiGate unit that acts as a VPN server and will provide secure access to the Internet, you must create an Internet browsing firewall policy. This policy differs depending on whether your gateway-to-gateway configuration is policy-based or route-based.

To create an Internet browsing policy - policy-based VPN

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

Source Interface	The interface to which the VPN tunnel is bound.
Source Address Name	The address of the remote FortiGate gateway.
Destination Interface	The interface to which the VPN tunnel is bound. (Same as Source Address).
Destination Address Name	All
Schedule	As required.
Service	As required.
Action	IPSEC
VPN Tunnel	Select the tunnel that provides access to the private network behind the FortiGate unit.
Protection Profile	Select the protection profile that you want to apply to Internet access.
Allow Inbound	Enable
Allow Outbound	Enable

Inbound NAT	Enable

Configure other settings as needed.

To create an Internet browsing policy - route-based VPN

1 Go to **Firewall > Policy**.

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

Source Interface	The IPSec VPN interface.
Source Address Name	All
Destination Interface	The interface that connects to the Internet. The virtual IPSec interface is configured on this physical interface.
Destination Address Name	All
Schedule	As required.
Service	As required.
Action	ACCEPT
NAT	Enable
Protection Profile	Select the protection profile that you want to apply to Internet access.

Configure other settings as needed.

The VPN clients must be configured to route all Internet traffic through the VPN tunnel.

Routing all remote traffic through the VPN tunnel

To make use of the Internet browsing configuration on the VPN server, the VPN peer or client must route all traffic through the VPN tunnel. Usually, only the traffic destined for the private network behind the FortiGate VPN server is sent through the tunnel.

The remote end of the VPN can be a FortiGate unit that acts as a peer in a gateway-to-gateway configuration or a FortiClient Host Security application that protects an individual client such as a notebook PC.

- To configure a remote peer FortiGate unit for Internet browsing via VPN, see “Configuring a FortiGate remote peer to support Internet browsing”.
- To configure a FortiClient Host Security application for Internet browsing via VPN, see “Configuring a FortiClient application to support Internet browsing” on page 82.

These procedures assume that your VPN connection to the protected private network is working and that you have configured the FortiGate VPN server for Internet browsing as described in “Creating an Internet browsing firewall policy” on page 80.

Configuring a FortiGate remote peer to support Internet browsing

The configuration changes to send all traffic through the VPN differ for policy-based and route-based VPNs.

To route all traffic through a policy-based VPN

1. At the FortiGate dialup client, go to **Firewall > Policy**.
2. Select the Edit icon in the row that corresponds to the IPSec firewall policy.
3. From the Address Name list under Destination, select all.
4. Select OK.

   All packets are routed through the VPN tunnel, not just packets destined for the protected private network.

To route all traffic through a route-based VPN

1. At the FortiGate dialup client, go to **Router > Static**.
2. Select the Edit icon for the default route (destination IP 0.0.0.0). If there is no default route, select Create New. Enter the following information and select OK:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	Select the IPSec virtual interface.
Gateway	Enter the remote gateway IP address for the VPN.
Distance	Leave at default.

All packets are routed through the VPN tunnel, not just packets destined for the protected private network.

Configuring a FortiClient application to support Internet browsing

By default, the FortiClient application configures the PC so that traffic destined for the remote protected network passes through the VPN tunnel but all other traffic is sent to the default gateway. You need to modify the FortiClient settings so that it configures the PC to route all outbound traffic through the VPN.

To route all traffic through VPN - FortiClient application

1. At the remote host, start FortiClient.
2. Go to **VPN > Connections**.
3. Select the definition that connects FortiClient to the FortiGate dialup server.
4. Select Advanced and then select Edit.
5. In the Edit Connection dialog box, select Advanced.
6. In the Remote Network group, select Add.
7. In the IP and Subnet Mask fields, type `0.0.0.0/0.0.0.0` and select OK.

   The address is added to the Remote Network list. The first destination IP address in the list establishes a VPN tunnel. The second destination address (`0.0.0.0/0.0.0.0` in this case) forces all other traffic through the VPN tunnel.
8. Select OK twice to close the dialog boxes.

Redundant VPN configurations

This section discusses the options for supporting redundant and partially redundant IPSec VPNs, using route-based approaches.

The following topics are included in this section:

- Configuration overview
- General configuration steps
- Configure the VPN peers - route-based VPN
- Redundant route-based VPN configuration example
- Partially-redundant route-based VPN example
- Creating a backup IPSec interface

Configuration overview

A FortiGate unit with two interfaces to the Internet can be configured to support redundant VPNs to the same remote peer. If the primary connection fails, the FortiGate unit can establish a VPN using the other connection.

A fully-redundant configuration requires redundant connections to the Internet on both peers. Figure 16 on page 84 shows an example of this. This is useful to create a reliable connection between two FortiGate units with static IP addresses.

When only one peer has redundant connections, the configuration is partially-redundant. For an example of this, see "Partially-redundant route-based VPN example" on page 98. This is useful for to provide reliable service from a FortiGate unit with static IP addresses that accepts connections from dialup IPSec VPN clients.

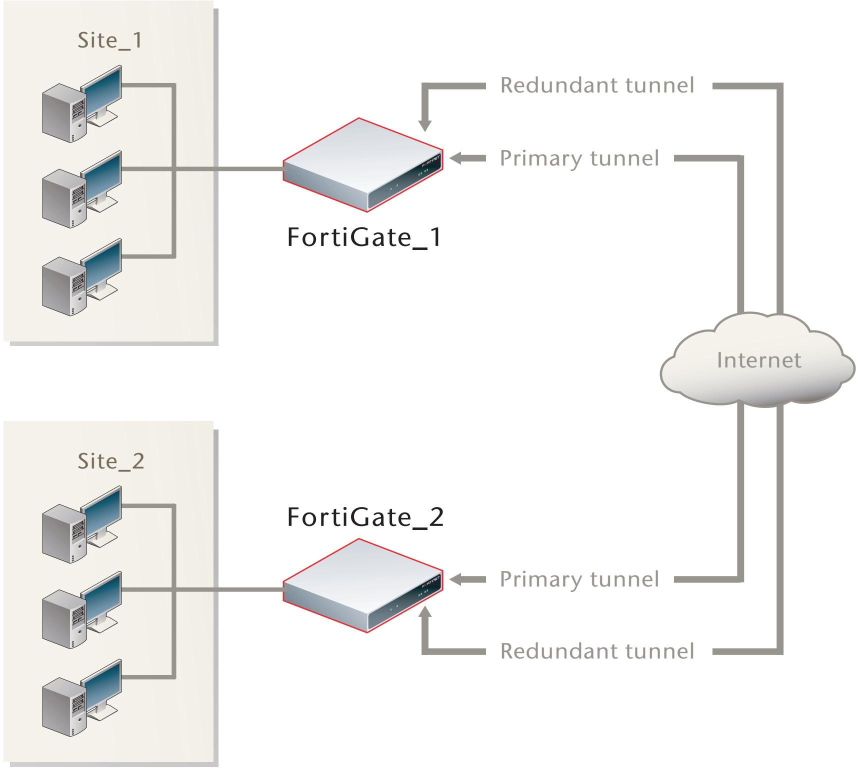
In a fully-redundant VPN configuration with two interfaces on each peer, four distinct paths are possible for VPN traffic from end to end. Each interface on a peer can communicate with both interfaces on the other peer. This ensures that a VPN will be available as long as each peer has one working connection to the Internet.

You configure a VPN and an entry in the routing table for each of the four paths. All of these VPNs are ready to carry data. You set different routing distances for each route and only the shortest distance route is used. If this route fails, the route with the next shortest distance is used.

The redundant configurations described in this chapter use route-based VPNs, otherwise known as virtual IPSec interfaces. This means that the FortiGate unit must operate in NAT/Route mode. You must use auto-keying. A VPN that is created using manual keys (see "Manual-key configurations" on page 111) cannot be included in a redundant-tunnel configuration.

The configuration described here assumes that your redundant VPNs are essentially equal in cost and capability. When the original VPN returns to service, traffic continues to use the replacement VPN until the replacement VPN fails. If your redundant VPN uses more expensive facilities, you want to use it only as a backup while the main VPN is down. For information on how to do this, see "Creating a backup IPSec interface" on page 104.

Figure 16: Example redundant-tunnel configuration



Note: A VPN that is created using manual keys (see "Manual-key configurations" on page 111) cannot be included in a redundant-tunnel configuration.

General configuration steps

A redundant configuration at each VPN peer includes:

- one phase 1 configuration (virtual IPSec interface) for each path between the two peers. In a fully-meshed redundant configuration, each network interface on one peer can communicate with each network interface on the remote peer. If both peers have two public interfaces, this means that each peer has four paths, for example.
- one phase 2 definition for each phase 1 configuration
- one static route for each IPSec interface, with different distance values to prioritize the routes
- two Accept firewall policies per IPSec interface, one for each direction of traffic
- dead peer detection enabled in each phase 1 definition

The procedures in this section assume that two separate interfaces to the Internet are available on each VPN peer.

Configure the VPN peers - route-based VPN

Configure each VPN peer as follows:

1 Ensure that the interfaces used in the VPN have static IP addresses.

2 Create a phase 1 configuration for each of the paths between the peers. Enable IPSec Interface mode so that this creates a virtual IPSec interface. Enable dead peer detection so that one of the other paths is activated if this path fails.

Enter these settings in particular:

Path 1

Remote Gateway	Select Static IP Address.
IP Address	Type the IP address of the primary interface of the remote peer.
Local Interface	Select the primary public interface of this peer.
Enable IPSec Interface Mode	Enable
Dead Peer Detection	Enable

Other settings as required by VPN.

Path 2

Remote Gateway	Select Static IP Address.
IP Address	Type the IP address of the secondary interface of the remote peer.
Local Interface	Select the primary public interface of this peer.
Enable IPSec Interface Mode	Enable
Dead Peer Detection	Enable

Other settings as required by VPN.

Path 3

Remote Gateway	Select Static IP Address.
IP Address	Type the IP address of the primary interface of the remote peer.
Local Interface	Select the secondary public interface of this peer.
Enable IPSec Interface Mode	Enable
Dead Peer Detection	Enable

Other settings as required by VPN.

Path 4

Remote Gateway	Select Static IP Address.
IP Address	Type the IP address of the secondary interface of the remote peer.
Local Interface	Select the secondary public interface of this peer.
Enable IPSec Interface Mode	Enable
Dead Peer Detection	Enable

Other settings as required by VPN.

For more information, see "Auto Key phase 1 parameters" on page 127.

3 Create a phase 2 definition for each path. See "Phase 2 parameters" on page 143. Enter these settings in particular:

Phase 1	Select the phase 1 configuration (virtual IPSec interface) that you defined for this path. You can select the name from the Static IP Address part of the list.

4 Create a route for each path to the other peer. If there are two ports on each peer, there are four possible paths between the peer devices.

Destination IP/Mask	The IP address and netmask of the private network behind the remote peer.
Device	One of the virtual IPSec interfaces on the local peer.
Distance	For each path, enter a different value to prioritize the paths.

5 Define the firewall policy for the local primary interface. See "Defining firewall policies" on page 150. You need to create two policies for each path to enable communication in both directions. Enter these settings in particular:

Source Interface/Zone	Select the local interface to the internal (private) network
Source Address Name	All
Destination Interface/Zone	Select one of the virtual IPSec interfaces you created in Step 2.
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

Source Interface/Zone	Select one of the virtual IPSec interfaces you created in Step 2.
Source Address Name	All
Destination Interface/Zone	Select the local interface to the internal (private) network.
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

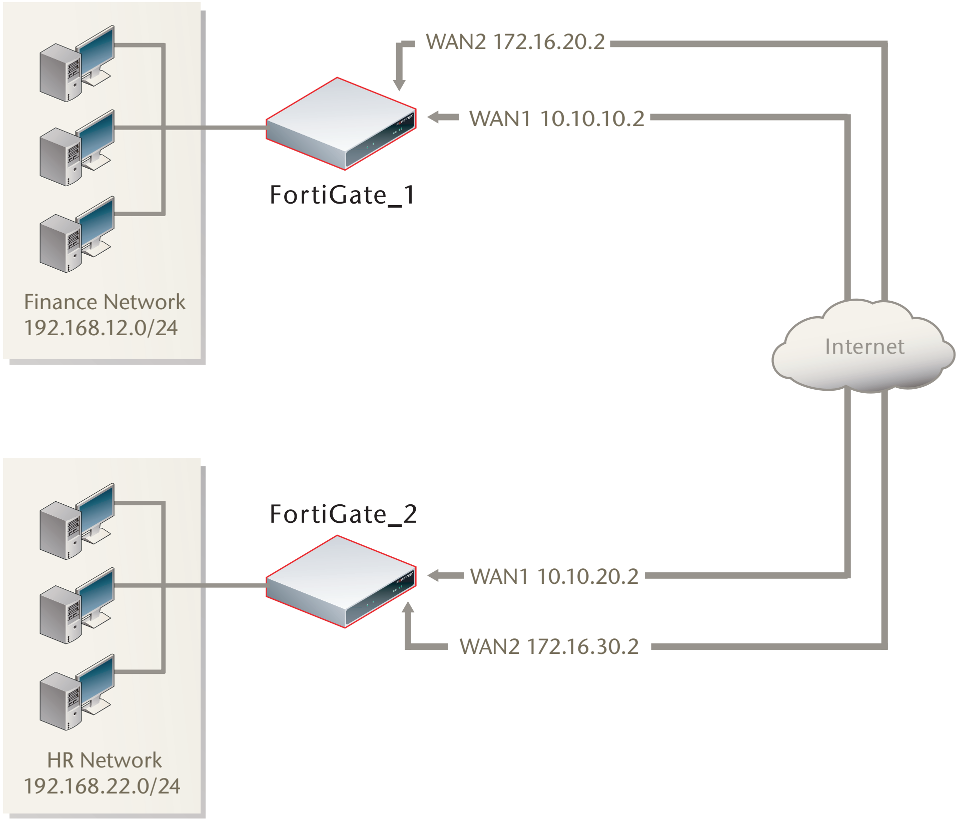
7 Repeat this procedure at the remote FortiGate unit.

Redundant route-based VPN configuration example

This example demonstrates a fully redundant site-to-site VPN configuration using route-based VPNs. At each site, the FortiGate unit has two interfaces connected to the Internet through different ISPs. This means that there are four possible paths for communication between the two units. In this example, these paths, listed in descending priority, are:

- FortiGate_1 WAN 1 to FortiGate_2 WAN 1
- FortiGate_1 WAN 1 to FortiGate_2 WAN 2
- FortiGate_1 WAN 2 to FortiGate_2 WAN 1
- FortiGate_1 WAN 2 to FortiGate_2 WAN 2

Figure 17: Example redundant route-based VPN configuration



For each path, VPN configuration, firewall policies and routing are defined. By specifying a different routing distance for each path, the paths are prioritized. A VPN tunnel is established on each path, but only the highest priority one is used. If the highest priority path goes down, the traffic is automatically routed over the next highest priority path. You could use dynamic routing, but to keep this example simple, static routing is used.

Configuring FortiGate_1

You must

- configure the interfaces involved in the VPN
- define the phase 1 configuration for each of the four possible paths, creating a virtual IPSec interface for each one

- define the phase 2 configuration for each of the four possible paths
- configure routes for the four IPSec interfaces, assigning the appropriate priorities
- configure incoming and outgoing firewall policies between the internal interface and each of the virtual IPSec interfaces

To configure the network interfaces

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

2 Select the Edit icon for the Internal interface, enter the following information and then select OK:

Addressing mode	Manual
IP/Netmask	`192.168.12.0/255.255.255.0`

3 Select the Edit icon for the WAN1 interface, enter the following information and then select OK:

Addressing mode	Manual
IP/Netmask	`10.10.10.2/255.255.255.0`

4 Select the Edit icon for the WAN2 interface, enter the following information and then select OK:

Addressing mode	Manual
IP/Netmask	`172.16.20.2/255.255.255.0`

To configure the IPSec interfaces (phase 1 configurations)

1 Go to **VPN > IPSEC > Auto Key**.

2 Select Create Phase 1, enter the following information, and select OK:

Name	`Site_1_A`
Remote Gateway	Static IP Address
IP Address	`10.10.20.2`
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Select
Dead Peer Detection	Select

3 Select Create Phase 1, enter the following information, and select OK:

Name	`Site_1_B`
Remote Gateway	Static IP Address
IP Address	`172.16.30.2`
Local Interface	WAN1

Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Select
Dead Peer Detection	Select

4 Select Create Phase 1, enter the following information, and select OK:

Name	`Site_1_C`
Remote Gateway	Static IP Address
IP Address	`10.10.20.2`
Local Interface	WAN2
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Select
Dead Peer Detection	Select

5 Select Create Phase 1, enter the following information, and select OK:

Name	`Site_1_D`
Remote Gateway	Static IP Address
IP Address	`172.16.30.2`
Local Interface	WAN2
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Select
Dead Peer Detection	Select

To define the phase 2 configurations for the four VPNs

1 Go to **VPN > IPSEC > Auto Key**.

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

Name	`Route_A`.
Phase 1	`Site_1_A`

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

Name	`Route_B`.
Phase 1	`Site_1_B`

4. Select Create Phase 2, enter the following information and select OK:

Name	`Route_C`.
Phase 1	`Site_1_C`

5. Select Create Phase 2, enter the following information and select OK:

Name	`Route_D`.
Phase 1	`Site_1_D`

To configure routes

1. Go to **Router > Static**.
2. Select Create New, enter the following default gateway information and then select OK:

Destination IP/Mask	`0.0.0.0/0.0.0.0`
Device	WAN1
Gateway	`10.10.10.1`
Distance	`10`

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

Destination IP/Mask	`192.168.22.0/255.255.255.0`
Device	Site_1_A
Distance	`1`

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

Destination IP/Mask	`192.168.22.0/255.255.255.0`
Device	Site_1_B
Distance	`2`

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

Destination IP/Mask	`192.168.22.0/255.255.255.0`
Device	Site_1_C
Distance	`3`

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

Destination IP/Mask	`192.168.22.0/255.255.255.0`
Device	Site_1_D
Distance	`4`

To configure firewall policies

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

Source Interface/Zone	Internal
Source Address Name	All
Destination Interface/Zone	Site_1_A
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Site_1_A
Source Address Name	All
Destination Interface/Zone	Internal
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Internal
Source Address Name	All
Destination Interface/Zone	Site_1_B
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Site_1_B
Source Address Name	All
Destination Interface/Zone	Internal
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Internal
Source Address Name	All
Destination Interface/Zone	Site_1_C
Destination Address Name	All
Schedule	Always

Service	Any
Action	ACCEPT

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

Source Interface/Zone	Site_1_C
Source Address Name	All
Destination Interface/Zone	Internal
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Internal
Source Address Name	All
Destination Interface/Zone	Site_1_D
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Site_1_D
Source Address Name	All
Destination Interface/Zone	Internal
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

Configuring FortiGate_2

The configuration for FortiGate_2 is very similar that of FortiGate_1. You must

- configure the interfaces involved in the VPN
- define the phase 1 configuration for each of the four possible paths, creating a virtual IPSec interface for each one
- define the phase 2 configuration for each of the four possible paths
- configure routes for the four IPSec interfaces, assigning the appropriate priorities
- configure incoming and outgoing firewall policies between the internal interface and each of the virtual IPSec interfaces

To configure the network interfaces

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

2 Select the Edit icon for the Internal interface, enter the following information and then select OK:

Addressing mode	Manual
IP/Netmask	`192.168.22.0/255.255.255.0`

3 Select the Edit icon for the WAN1 interface, enter the following information and then select OK:

Addressing mode	Manual
IP/Netmask	`10.10.20.2/255.255.255.0`

4 Select the Edit icon for the WAN2 interface, enter the following information and then select OK:

Addressing mode	Manual
IP/Netmask	`172.16.30.2/255.255.255.0`

To configure the IPSec interfaces (phase 1 configurations)

1 Go to **VPN > IPSEC > Auto Key**.

2 Select Create Phase 1, enter the following information, and select OK:

Name	`Site_2_A`
Remote Gateway	Static IP Address
IP Address	`10.10.10.2`
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Select
Dead Peer Detection	Select

3 Select Create Phase 1, enter the following information, and select OK:

Name	`Site_2_B`
Remote Gateway	Static IP Address
IP Address	`172.16.20.2`
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Select
Dead Peer Detection	Select

4 Select Create Phase 1, enter the following information, and select OK:

Name	`Site_2_C`
Remote Gateway	Static IP Address
IP Address	`10.10.10.2`
Local Interface	WAN2
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Select
Dead Peer Detection	Select

5 Select Create Phase 1, enter the following information, and select OK:

Name	`Site_2_D`
Remote Gateway	Static IP Address
IP Address	`172.16.20.2`
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Select
Dead Peer Detection	Select

To define the phase 2 configurations for the four VPNs

1 Go to **VPN > IPSEC > Auto Key**.

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

Name	`Route_A`.
Phase 1	`Site_2_A`

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

Name	`Route_B`.
Phase 1	`Site_2_B`

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

Name	`Route_C`.
Phase 1	`Site_2_C`

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

Name	`Route_D`.
Phase 1	`Site_2_D`

To configure routes

1. Go to **Router > Static**.
2. Select Create New, enter the following default gateway information and then select OK:

Destination IP/Mask	`0.0.0.0/0.0.0.0`
Device	WAN1
Gateway	`10.10.10.1`
Distance	`10`

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

Destination IP/Mask	`192.168.12.0/255.255.255.0`
Device	Site_2_A
Distance	`1`

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

Destination IP/Mask	`192.168.12.0/255.255.255.0`
Device	Site_2_B
Distance	`2`

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

Destination IP/Mask	`192.168.12.0/255.255.255.0`
Device	Site_2_C
Distance	`3`

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

Destination IP/Mask	`192.168.12.0/255.255.255.0`
Device	Site_2_D
Distance	`4`

To configure firewall policies

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

Source Interface/Zone	Internal
Source Address Name	All
Destination Interface/Zone	Site_2_A
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Site_2_A
Source Address Name	All
Destination Interface/Zone	Internal
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Internal
Source Address Name	All
Destination Interface/Zone	Site_2_B
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Site_2_B
Source Address Name	All
Destination Interface/Zone	Internal
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Internal
Source Address Name	All
Destination Interface/Zone	Site_2_C
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Site_2_C
Source Address Name	All
Destination Interface/Zone	Internal
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Internal
Source Address Name	All
Destination Interface/Zone	Site_2_D
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Site_2_D
Source Address Name	All
Destination Interface/Zone	Internal
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

Partially-redundant route-based VPN example

This example demonstrates how to set up a partially redundant IPSec VPN between a local FortiGate unit and a remote VPN peer that receives a dynamic IP address from an ISP before it connects to the FortiGate unit. For more information about FortiGate dialup-client configurations, see "FortiGate dialup-client configurations" on page 71.

When a FortiGate unit has more than one interface to the Internet (see FortiGate_1 in Figure 18), you can configure redundant routes—if the primary connection fails, the FortiGate unit can establish a VPN using the redundant connection.

In this case, FortiGate_2 has 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.

In the configuration example:

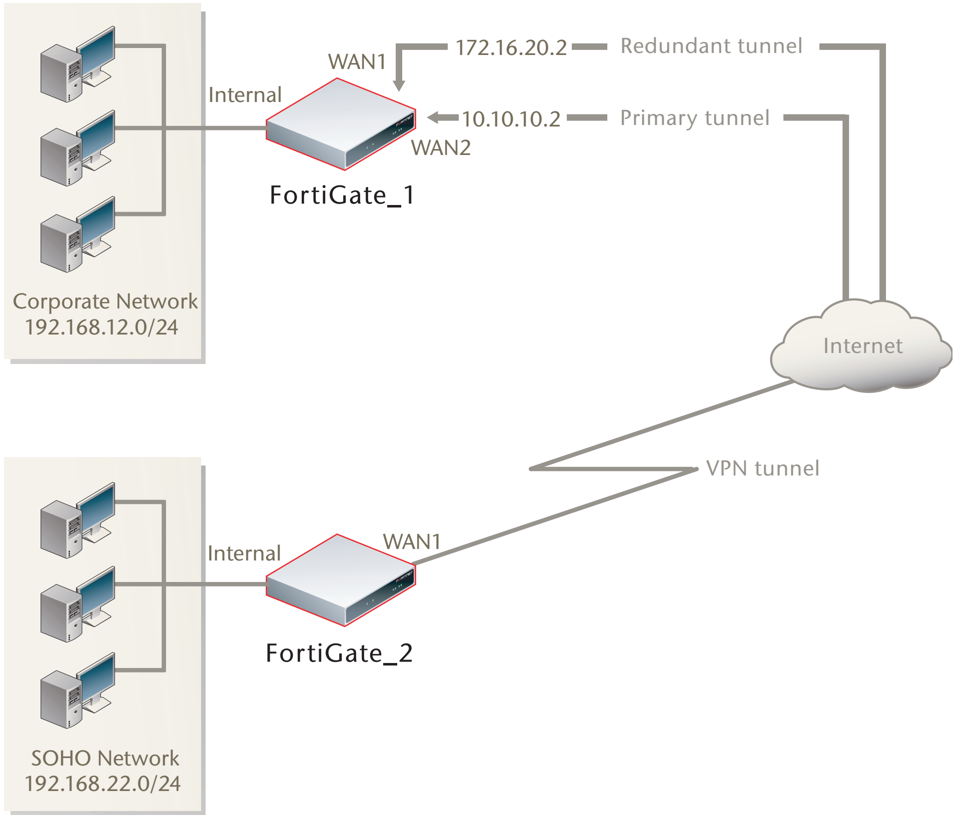
- Both FortiGate units operate in NAT/Route mode.
- Two separate interfaces to the Internet (10.10.10.2 and 172.16.20.2) are available on FortiGate_1. Each interface has a static public IP address.
- FortiGate_2 has a single connection to the Internet and obtains a dynamic public IP address (for example, 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. Encrypted packets from FortiGate_2 are addressed to the public interface of FortiGate_1. Encrypted packets from FortiGate_1 are addressed to the public IP address of FortiGate_2.

There are two possible paths for communication between the two units. In this example, these paths, listed in descending priority, are:

- FortiGate_1 WAN 1 to FortiGate_2 WAN 1
- FortiGate_1 WAN 2 to FortiGate_2 WAN 1

For each path, VPN configuration, firewall policies and routing are defined. By specifying a different routing distance for each path, the paths are prioritized. A VPN tunnel is established on each path, but only the highest priority one is used. If the highest priority path goes down, the traffic is automatically routed over the next highest priority path. You could use dynamic routing, but to keep this example simple, static routing is used.

Figure 18: Example partially redundant route-based configuration



Configuring FortiGate_1

You must

- configure the interfaces involved in the VPN
- define the phase 1 configuration for each of the two possible paths, creating a virtual IPSec interface for each one
- define the phase 2 configuration for each of the two possible paths
- configure incoming and outgoing firewall policies between the internal interface and each of the virtual IPSec interfaces

To configure the network interfaces

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

2 Select the Edit icon for the Internal interface, enter the following information and then select OK:

Addressing mode	Manual
IP/Netmask	`192.168.12.2/255.255.255.0`

3 Select the Edit icon for the WAN1 interface, enter the following information and then select OK:

Addressing mode	Manual
IP/Netmask	`10.10.10.2/255.255.255.0`

4 Select the Edit icon for the WAN2 interface, enter the following information and then select OK:

Addressing mode	Manual
IP/Netmask	`172.16.20.2/255.255.255.0`

To configure the IPSec interfaces (phase 1 configurations)

1 Go to **VPN > IPSEC > Auto Key**.

2 Select Create Phase 1, enter the following information, and select OK:

Name	`Site_1_A`
Remote Gateway	Dialup User
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Select
Dead Peer Detection	Select

3 Select Create Phase 1, enter the following information, and select OK:

Name	`Site_1_B`
Remote Gateway	Dialup User
Local Interface	WAN2
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Select
Dead Peer Detection	Select

To define the phase 2 configurations for the two VPNs

1 Go to **VPN > IPSEC > Auto Key**.

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

Name	`Route_A`.
Phase 1	`Site_1_A`

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

Name	`Route_B`.
Phase 1	`Site_1_B`

To configure routes

1 Go to **Router > Static**.

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

Destination IP/Mask	`0.0.0.0/0.0.0.0`
Device	WAN1
Gateway	`10.10.10.1`
Distance	`10`

To configure firewall policies

1 Go to **Firewall > Policy**.

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

Source Interface/Zone	Internal
Source Address Name	All
Destination Interface/Zone	Site_1_A
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Internal
Source Address Name	All
Destination Interface/Zone	Site_1_B
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

Configuring FortiGate_2

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

- configure the interface involved in the VPN
- define the phase 1 configuration for the primary and redundant paths, creating a virtual IPSec interface for each one
- define the phase 2 configurations for the primary and redundant paths, defining the internal network as the source address so that FortiGate_1 can automatically configure routing
- configure the routes for the two IPSec interfaces, assigning the appropriate priorities
- configure firewall policies between the internal interface and each of the virtual IPSec interfaces

To configure the network interfaces

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

2 Select the Edit icon for the Internal interface, enter the following information and then select OK:

Addressing mode	Manual
IP/Netmask	`192.168.22.2/255.255.255.0`

3 Select the Edit icon for the WAN1 interface, enter the following information and then select OK:

Addressing mode	DHCP

To configure the two IPSec interfaces (phase 1 configurations)

1 Go to **VPN > IPSEC > Auto Key**.

2 Select Create Phase 1, enter the following information, and select OK:

Name	`Site_2_A`
Remote Gateway	Static IP Address
IP Address	`10.10.10.2`
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Select
Dead Peer Detection	Select

3 Select Create Phase 1, enter the following information, and select OK:

Name	`Site_2_B`
Remote Gateway	Static IP Address
IP Address	`172.16.20.2`
Local Interface	WAN1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
Advanced	
Enable IPSec Interface Mode	Select
Dead Peer Detection	Select

To define the phase 2 configurations for the two VPNs

1 Go to **VPN > IPSEC > Auto Key**.

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

Name	`Route_A`.
Phase 1	`Site_2_A`
Advanced	
Source Address	192.168.22.0/24

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

Name	`Route_B`.
Phase 1	`Site_2_B`
Advanced	
Source Address	192.168.22.0/24

To configure routes

1 Go to **Router > Static**.

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

Destination IP/Mask	`192.168.12.0/255.255.255.0`
Device	Site_2_A
Distance	`1`

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

Destination IP/Mask	`192.168.12.0/255.255.255.0`
Device	Site_2_B
Distance	`2`

To configure firewall policies

1 Go to **Firewall > Policy**.

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

Source Interface/Zone	Internal
Source Address Name	All
Destination Interface/Zone	Site_2_A
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

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

Source Interface/Zone	Internal
Source Address Name	All
Destination Interface/Zone	Site_2_B
Destination Address Name	All
Schedule	Always
Service	Any
Action	ACCEPT

Creating a backup IPSec interface

Starting in FortiOS 3.0 MR4, you can configure a route-based VPN that acts as a backup facility to another VPN. It is used only while your main VPN is out of service. This is desirable when the redundant VPN uses a more expensive facility.

In FortiOS releases prior to 3.0 MR4, a backup VPN configuration is possible only if the backup connection is a modem in a Redundant mode configuration.

You can configure a backup IPSec interface only in the CLI. The backup feature works only on interfaces with static addresses that have dead peer detection enabled. The monitor-phase1 option creates a backup VPN for the specified phase 1 configuration.

In the following example, backup_vpn is a backup for main_vpn.

```
config vpn ipsec phase1-interface
  edit main_vpn
    set dpd on
    set interface port1
    set nattraversal enable
    set psksecret "hard-to-guess"
    set remote-gw 10.10.10.8
    set type static
  end
  edit backup_vpn
    set dpd on
    set interface port2
    set monitor-phase1 main_vpn
    set nattraversal enable
    set psksecret "hard-to-guess"
    set remote-gw 10.10.10.8
    set type static
  end
```

Transparent mode VPNs

This section describes transparent VPN configurations, in which two FortiGate units create a VPN tunnel between two separate private networks transparently.

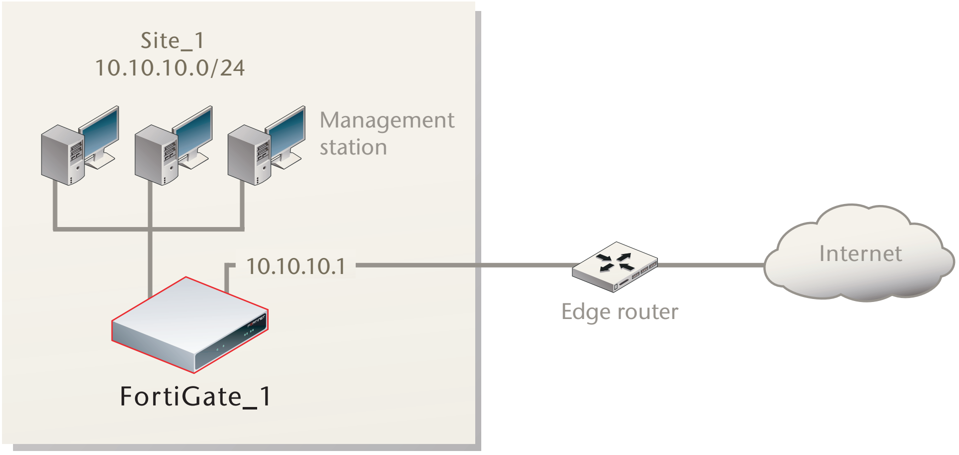
The following topics are included in this section:

- Configuration overview
- Configure the VPN peers

Configuration overview

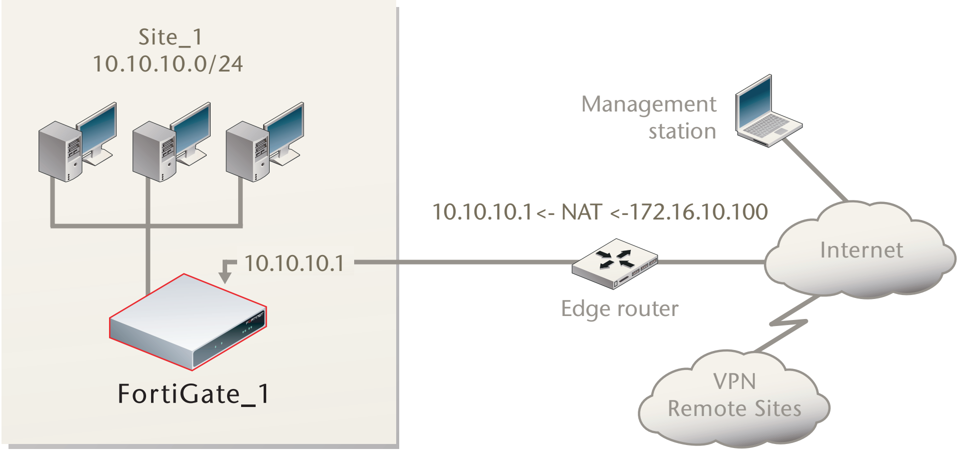
In Transparent mode, all interfaces of the FortiGate unit except the management interface (which by default is assigned IP address 10.10.10.1/255.255.255.0) are invisible at the network layer. Typically, when a FortiGate unit runs in Transparent mode, different network segments are connected to the FortiGate interfaces. Figure 19 shows the management station on the same subnet. The management station can connect to the FortiGate unit directly through the web-based manager.

Figure 19: Management station on internal network



An edge router typically provides a public connection to the Internet and one interface of the FortiGate unit is connected to the router. If the FortiGate unit is managed from an external address (see Figure 20 on page 106), the router must translate (NAT) a routable address to direct management traffic to the FortiGate management interface.

Figure 20: Management station on external network



In a transparent VPN configuration, two FortiGate units create a VPN tunnel between two separate private networks transparently. All traffic between the two networks is encrypted and protected by FortiGate firewall policies.

Both FortiGate units may be running in Transparent mode, or one could be running in Transparent mode and the other running in NAT/Route mode. If the remote peer is running in NAT/Route mode, it must have a static public IP address.

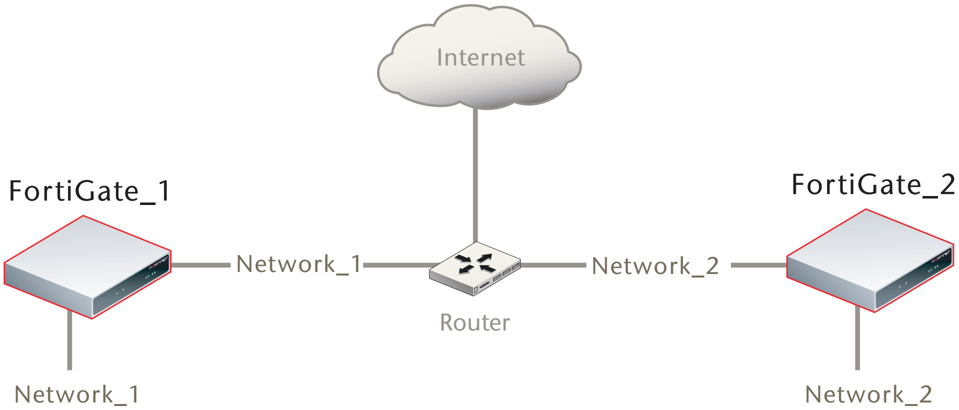
Note: VPNs between two FortiGate units running in Transparent mode do not support inbound/outbound NAT (supported through CLI commands) within the tunnel. In addition, a FortiGate unit running in Transparent mode cannot be used in a hub-and-spoke configuration.

Encrypted packets from the remote VPN peer are addressed to the management interface of the local FortiGate unit. If the local FortiGate unit can reach the VPN peer locally, a static route to the VPN peer must be added to the routing table on the local FortiGate unit. If the VPN peer connects through the Internet, encrypted packets from the local FortiGate unit must be routed to the edge router instead. For information about how to add a static route to the FortiGate routing table, see the “Router Static” chapter of the *FortiGate Administration Guide*.

In the example configuration shown in Figure 20, Network Address Translation (NAT) is enabled on the router. When an encrypted packet from the remote VPN peer arrives at the router through the Internet, the router performs inbound NAT and forwards the packet to the FortiGate unit. Refer to the software supplier’s documentation to configure the router.

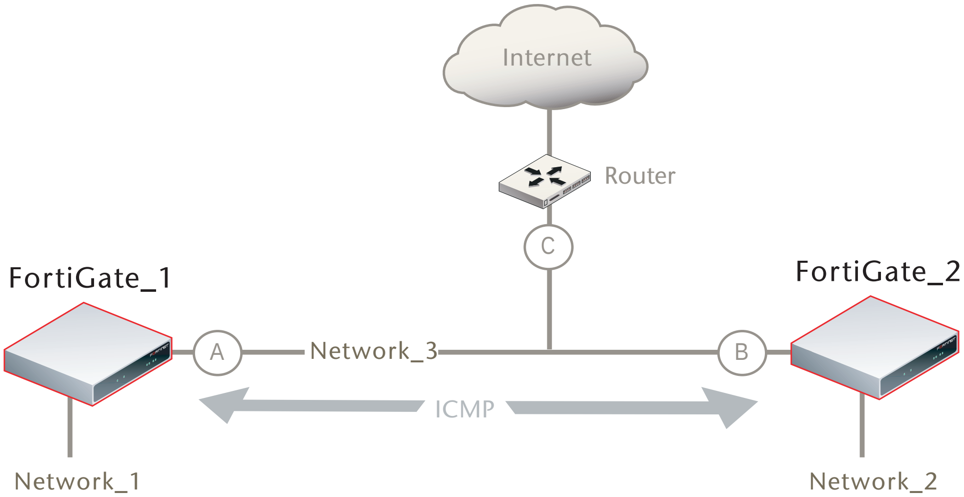
If you want to configure a VPN between two FortiGate units running in Transparent mode, each unit must have an independent connection to a router that acts as a gateway to the Internet, and both units must be on separate networks that have a different address space. When the two networks linked by the VPN tunnel have different address spaces (see Figure 21 on page 107), at least one router must separate the two FortiGate units, unless the packets can be redirected using ICMP (see Figure 22 on page 107).

Figure 21: Link between two FortiGate units running in Transparent mode



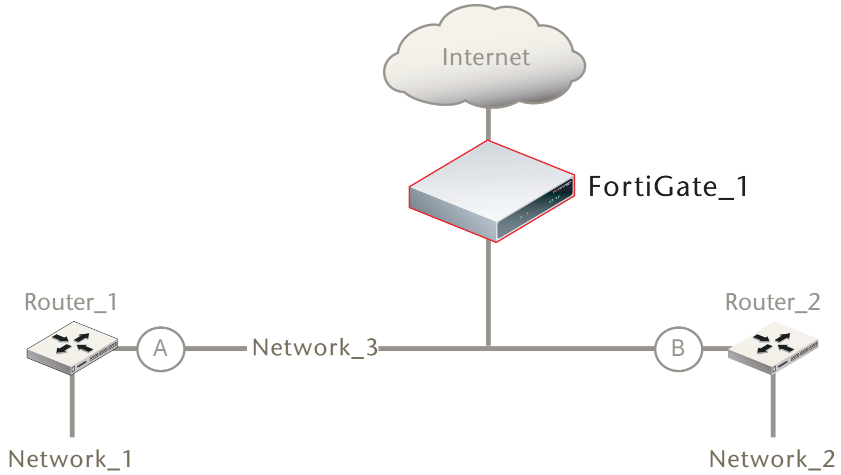
In Figure 22, interface C behind the router is the default gateway for both FortiGate units. Packets that cannot be delivered on Network_1 are routed to interface C by default. Similarly, packets that cannot be delivered on Network_2 are routed to interface C. In this case, the router must be configured to redirect packets destined for Network_1 to interface A and redirect packets destined for Network_2 to interface B.

Figure 22: ICMP redirecting packets to two FortiGate units running in Transparent mode



If there are additional routers behind the FortiGate unit (see Figure 23 on page 108) and the destination IP address of an inbound packet is on a network behind one of those routers, the FortiGate routing table must include routes to those networks. For example, in Figure 23, the FortiGate unit must be configured with static routes to interfaces A and B in order to forward packets to Network_1 and Network_2 respectively.

Figure 23: Destinations on remote networks behind internal routers



Transparent VPN infrastructure requirements

- The local FortiGate unit must be operating in Transparent mode.
- The management IP address of the local FortiGate unit specifies the local VPN gateway. The management IP address is considered a static IP address for the local VPN peer.
- If the local FortiGate unit is managed through the Internet, or if the VPN peer connects through the Internet, the edge router must be configured to perform inbound NAT and forward management traffic and/or encrypted packets to the FortiGate unit.
- If the remote peer is operating in NAT/Route mode, it must have a static public IP address.

A FortiGate unit operating in Transparent mode requires the following basic configuration to operate as a node on the IP network:

- The unit must have sufficient routing information to reach the management station.
- For any traffic to reach external destinations, a default static route to the edge router must be present in the FortiGate routing table. The router forwards packets to the Internet.
- When all of the destinations are located on the external network, the FortiGate unit may route packets using a single default static route. If the network topology is more complex, one or more static routes in addition to the default static route may be required in the FortiGate routing table.

Before you begin

An IPSec VPN definition links a gateway with a tunnel and an IPSec policy. If your network topology includes more than one virtual domain, you must choose components that were created in the same virtual domain. Therefore, before you define a transparent VPN configuration, choose an appropriate virtual domain in which to create the required interfaces, firewall policies, and VPN components. For more information, see the “Using virtual domains” chapter of the *FortiGate Administration Guide*.

Configure the VPN peers

The following procedure assumes that the local VPN peer operates in Transparent mode. The remote VPN peer may operate in NAT/Route mode or Transparent mode.

1 At the local FortiGate unit, define the phase 1 parameters needed to establish a secure connection with the remote peer. See “Auto Key phase 1 parameters” on page 127. Select Advanced and enter these settings in particular:

Remote Gateway	Select Static IP Address.
IP Address	Type the IP address of the public interface to the remote peer. If the remote peer is a FortiGate unit running in Transparent mode, type the IP address of the remote management interface.
Advanced	Select Nat-traversal, and type a value into the Keepalive Frequency field. These settings protect the headers of encrypted packets from being altered by external NAT devices and ensure that NAT address mappings do not change while the VPN tunnel is open. For more information, see “NAT traversal” on page 140 and “NAT keepalive frequency” on page 140.

2 Define the phase 2 parameters needed to create a VPN tunnel with the remote peer. See “Phase 2 parameters” on page 143. Enter these settings in particular:

Phase 1	Select the set of phase 1 parameters that you defined for the remote peer. The name of the remote peer can be selected from the Static IP Address list.

3 Define the source and destination addresses of the IP packets that are to be transported through the VPN tunnel. See “Defining firewall addresses” on page 149. Enter these settings in particular:

- For the originating address (source address), enter the IP address of the local management interface (for example, `10.10.10.1/32`).
- For the remote address (destination address), enter the IP address and netmask of the private network behind the remote peer (for example, `192.168.10.0/24`). If the remote peer is a FortiGate unit running in Transparent mode, enter the IP address of the remote management interface instead.

4 Define an IPSec firewall policy to permit communications between the source and destination addresses. See “Defining firewall policies” on page 150. Enter these settings in particular:

Source Interface/Zone	Select the local interface to the internal (private) network.
Source Address Name	Select the source address that you defined in Step 3.
Destination Interface/Zone	Select the interface to the edge router. When you configure the IPSec firewall policy on a remote peer that operates in NAT/Route mode, you select the public interface to the external (public) network instead.
Destination Address Name	Select the destination address that you defined in Step 3.
Action	IPSEC
VPN Tunnel	Select the name of the phase 2 tunnel configuration that you created in Step 2. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow outbound to enable traffic from the local network to initiate the tunnel.

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

6 Repeat this procedure at the remote FortiGate unit.

Manual-key configurations

This section explains how to manually define cryptographic keys to establish an IPSec VPN, either policy-based or route-based.

The following topics are included in this section:

- Configuration overview
- Specify the manual keys for creating a tunnel

Configuration overview

You can manually define cryptographic keys for the FortiGate unit to establish an IPSec VPN.

You define manual keys where prior knowledge of the encryption and/or authentication key is required (that is, one of the VPN peers requires a specific IPSec encryption and/or authentication key). In this case, you do not specify IPSec phase 1 and phase 2 parameters; you define manual keys on the **VPN > IPSEC > Manual Key** tab instead.

If one VPN peer uses specific authentication and encryption keys to establish a tunnel, both VPN peers must be configured to use the same encryption and authentication algorithms and keys.

Note: It may not be safe or practical to define manual keys because network administrators must be trusted to keep the keys confidential, and propagating changes to remote VPN peers in a secure manner may be difficult.

It is essential that both VPN peers be configured with matching encryption and authentication algorithms, matching authentication and encryption keys, and complementary Security Parameter Index (SPI) settings.

You can define either the encryption or the authentication as NULL (disabled), but not both.

Each SPI identifies a Security Association (SA). The value is placed in ESP datagrams to link the datagrams to the SA. When an ESP datagram is received, the recipient refers to the SPI to determine which SA applies to the datagram. An SPI must be specified manually for each SA. Because an SA applies to communication in one direction only, you must specify two SPIs per configuration (a local SPI and a remote SPI) to cover bidirectional communications between two VPN peers.

Caution: If you are not familiar with the security policies, SAs, selectors, and SA databases for your particular installation, do not attempt the following procedure without qualified assistance.

Specify the manual keys for creating a tunnel

Specify the manual keys for creating a tunnel as follows:

1 Go to **VPN > IPSEC > Manual Key** and select Create New.

2 Include appropriate entries as follows:

Name
Type a name for the VPN tunnel.

Local SPI
Type a hexadecimal number (up to 8 characters, 0-9, a-f) that represents the SA that handles outbound traffic on the local FortiGate unit. The valid range is from `0x100` to `0xffffffff`. This value must match the Remote SPI value in the manual key configuration at the remote peer.

Remote SPI
Type a hexadecimal number (up to 8 characters, 0-9, a-f) that represents the SA that handles inbound traffic on the local FortiGate unit. The valid range is from `0x100` to `0xffffffff`. This value must match the Local SPI value in the manual key configuration at the remote peer.

Remote Gateway
Type the IP address of the public interface to the remote peer. The address identifies the recipient of ESP datagrams.

Local Interface
Select the name of the physical, aggregate, or VLAN interface to which the IPSec tunnel will be bound. The FortiGate unit obtains the IP address of the interface from **System > Network > Interface** settings. This is available in NAT/Route mode only.

Encryption Algorithm
Select one of the following symmetric-key encryption algorithms:

- DES-Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- 3DES-Triple-DES, in which plain text is encrypted three times by three keys.
- AES128-A 128-bit block algorithm that uses a 128-bit key.
- AES192-A 128-bit block algorithm that uses a 192-bit key.
- AES256-A 128-bit block algorithm that uses a 256-bit key.

Encryption Key
If you selected:

- DES, type a 16-character hexadecimal number (0-9, a-f).
- 3DES, type a 48-character hexadecimal number (0-9, a-f) separated into three segments of 16 characters.
- AES128, type a 32-character hexadecimal number (0-9, a-f) separated into two segments of 16 characters.
- AES192, type a 48-character hexadecimal number (0-9, a-f) separated into three segments of 16 characters.
- AES256, type a 64-character hexadecimal number (0-9, a-f) separated into four segments of 16 characters.

Authentication Algorithm	Select one of the following message digests: • MD5-Message Digest 5 algorithm, which produces a 128-bit message digest. • SHA1-Secure Hash Algorithm 1, which produces a 160-bit message digest.
Authentication Key	If you selected: • MD5, type a 32-character hexadecimal number (0-9, a-f) separated into two segments of 16 characters. • SHA1, type 40-character hexadecimal number (0-9, a-f) separated into one segment of 16 characters and a second segment of 24 characters.
IPSec Interface Mode	Select to create a route-based VPN. A virtual IPSec interface is created on the Local Interface that you selected. This option is available only in NAT/Route mode.

3 Select OK.

IPv6 IPSec VPNs

This chapter describes how to configure your FortiGate unit’s IPv6 IPSec VPN functionality.

IPv6 configuration is not supported in the web-based manager. You must use the Command Line Interface (CLI). This section outlines the relevant CLI commands. For detailed information about the CLI, see the *FortiGate CLI Reference*.

The following topics are included in this section:

- Overview of IPv6 IPSec support
- Configuring IPv6 IPSec VPNs
- Site-to-site IPv6 over IPv6 VPN example
- Site-to-site IPv4 over IPv6 VPN example
- Site-to-site IPv6 over IPv4 VPN example

Overview of IPv6 IPSec support

The FortiGate unit supports interface-based IPv6 IPSec, but not policy-based. This section describes only how IPv6 IPSec support differs from IPv4 IPSec support.

FortiOS 3.0 supports IPv6 VPNs, but only in the CLI. The web-based manager does not display the configurations or status of any IPv6 VPN.

Where both the gateways and the protected networks use IPv6 addresses, sometimes called IPv6 over IPv6, you can create either an auto-keyed or manually-keyed VPN. You can combine IPv6 and IPv4 addressing in an auto-keyed VPN in the following ways:

IPv4 over IPv6 The VPN gateways have IPv6 addresses.
The protected networks have IPv4 addresses. The phase 2 configurations at either end use IPv4 selectors.

IPv6 over IPv4 The VPN gateways have IPv4 addresses.
The protected networks use IPv6 addresses. The phase 2 configurations at either end use IPv6 selectors.

Compared with IPv4 IPSec VPN functionality, there are some limitations:

- Except for IPv6 over IPv4, remote gateways with Dynamic DNS are not supported. This is because FortiOS 3.0 does not support IPv6 DNS.
- You cannot use RSA certificates in which the common name (cn) is a domain name that resolves to an IPv6 address. This is because FortiOS 3.0 does not support IPv6 DNS.
- DHCP over IPSec is not supported, because FortiOS 3.0 does not support IPv6 DHCP.
- Selectors cannot be firewall address names. Only IP address, address range and subnet are supported.
- Redundant IPv6 tunnels are not supported.

Certificates

On a VPN with IPv6 phase 1 configuration, you can authenticate using VPN certificates in which the common name (cn) is an IPv6 address. The `cn-type` keyword of the `user peer` command has an option, `ipv6`, to support this.

Configuring IPv6 IPSec VPNs

Configuration of an IPv6 IPSec VPN follows the same sequence as for an IPv4 interface-based VPN: phase 1 settings, phase 2 settings, firewall policies and routing.

Phase 1 configuration

You define an IPSec phase 1 configuration as IPv6 by setting `ip-version` to 6. Its default value is 4. Then, the `local-gw` and `remote-gw` keywords are hidden and the corresponding `local-gw6` and `remote-gw6` keywords are available. The values for `local-gw6` and `remote-gw6` must be IPv6 addresses.

To configure IPv6 IPSec VPN phase 1

```
config vpn ipsec phase1-interface
  edit tunnel6
    set ip-version 6
    set remote-gw6 0:123:4567::1234
    set interface port3
    set proposal 3des-md5
  end
```

Phase 2 configuration

An IPv6 IPSec phase 2 configuration has IPv6 address selectors. The `src-addr-type` and `dst-addr-type` options `ip6`, `range6` and `subnet6` require IPv6 addresses, but are otherwise the same as the similarly-named IPv4 options. The `name` option, referring to a firewall address or address group name, applies only to IPv4 configurations.

To configure IPv6 IPSec VPN phase 2

```
config vpn ipsec phase2-interface
  edit tunnel6_p2
    set src-addr-type subnet6
    set dst-addr-type subnet6
    set dst-subnet6 1200:2345::3456/64
    set interface port3
    set proposal 3des-md5
  end
```

Firewall policies

To complete the VPN configuration, you need a firewall policy in each direction to permit traffic between the protected network’s port and the IPSec interface. You need IPv6 policies unless the VPN is IPv4 over IPv6.

Routing

Appropriate routing is needed for both the IPSec packets and the encapsulated traffic within them. You need a route, which could be the default route, to the remote VPN gateway via the appropriate interface. You also need a route to the remote protected network via the IPSec interface. For example, where the remote network is fec0:0000:0000:0004::/64 and the IPSec interface is `toB`:

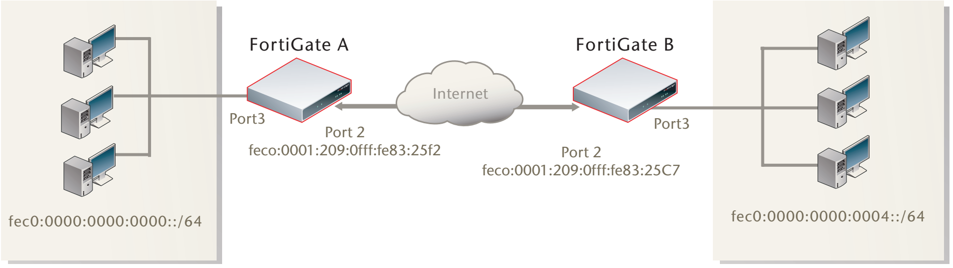
```
config router static6
  edit 1
    set device port2
    set dst 0::/0
  next
  edit 2
    set device toB
    set dst fec0:0000:0000:0004::/64
  next
end
```

If the VPN is IPV4 over IPv6, the route to the remote protected network is an IPv4 route. If the VPN is IPv6 over IPv4, the route to the remote VPN gateway is an IPv4 route.

Site-to-site IPv6 over IPv6 VPN example

In this example, computers on IPv6-addressed private networks communicate securely over public IPv6 infrastructure.

Figure 24: Example IPv6-over-IPv6 VPN topology



Configure FortiGate A interfaces

Port 2 connects to the public network and port 3 connects to the local network.

```
config system interface
  edit port2
    config ipv6
      set ip6-address fec0::0001:209:0fff:fe83:25f2/64
    end
  next
  edit port3
    config ipv6
      set ip6-address fec0::0000:209:0fff:fe83:25f3/64
    end
  next
end
```

Configure FortiGate A IPSec settings

The phase 1 configuration creates a virtual IPSec interface on port 2 and sets the remote gateway to the public IP address FortiGate B. This configuration is the same as for an IPv4 interface-based VPN, except that `ip-version` is set to 6 and the `remote-gw6` keyword is used to specify an IPv6 remote gateway address.

```
config vpn ipsec phase1-interface
  edit toB
    set ip-version 6
    set interface port2
    set remote-gw6 fec0:0000:0000:0003:209:0fff:fe83:25c7
    set dpd enable
    set psksecret maryhadalittlelamb
    set proposal 3des-md5 3des-sha1
  end
```

By default, phase 2 selectors are set to accept all subnet addresses for source and destination. The default setting for `src-addr-type` and `dst-addr-type` is `subnet`. The IPv6 equivalent is `subnet6`. The default subnet addresses are 0.0.0.0/0 for IPv4, `::/0` for IPv6.

```
config vpn ipsec phase2-interface
  edit toB2
    set phase1name toB
    set proposal 3des-md5 3des-sha1
    set pfs enable
    set replay enable
    set src-addr-type subnet6
    set dst-addr-type subnet6
  end
```

Configure FortiGate A firewall policies

Firewall policies are required to allow traffic between port3 and the IPsec interface toB in each direction. The address `all6` must be defined using the `firewall address6` command as `::/0`.

```
config firewall policy6
  edit 1
    set srcintf port3
    set dstintf toB
    set srcaddr all6
    set dstaddr all6
    set action accept
    set service ANY
    set schedule always
  next
  edit 2
    set srcintf toB
    set dstintf port3
    set srcaddr all6
    set dstaddr all6
    set action accept
    set service ANY
    set schedule always
  end
```

Configure FortiGate A routing

This simple example requires just two static routes. Traffic to the protected network behind FortiGate B is routed via the virtual IPSec interface toB. A default route sends all IPv6 traffic out on port2.

```
config router static6
  edit 1
    set device port2
    set dst 0::/0
  next
  edit 2
    set device toB
    set dst fec0:0000:0000:0004::/64
  end
```

Configure FortiGate B

The configuration of FortiGate B is very similar to that of FortiGate A. A virtual IPSec interface toA is configured on port2 and its remote gateway is the public IP address of FortiGate A. Firewall policies enable traffic to pass between the private network and the IPSec interface. Routing ensures traffic for the private network behind FortiGate A goes through the VPN and that all IPv6 packets are routed to the public network.

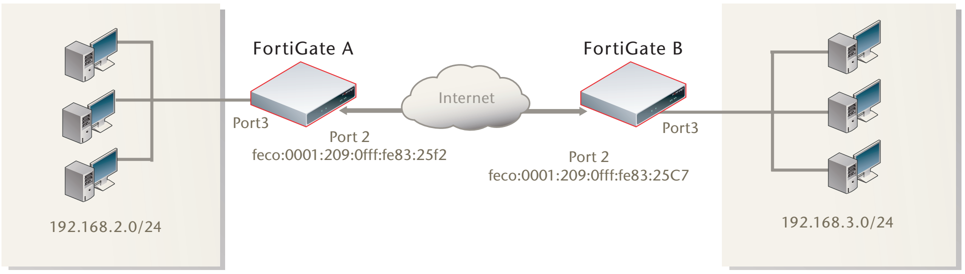
```
config system interface
  edit port2
    config ipv6
      set ip6-address fec0::0003:209:0fff:fe83:25c7/64
    end
  next
  edit port3
    config ipv6
      set ip6-address fec0::0004:209:0fff:fe83:2569/64
    end
  end
config vpn ipsec phase1-interface
  edit toA
    set ip-version 6
    set interface port2
    set remote-gw6 fec0:0000:0000:0001:209:0fff:fe83:25f2
    set dpd enable
    set psksecret maryhadalittlelamb
    set proposal 3des-md5 3des-sha1
  end
config vpn ipsec phase2-interface
  edit toA2
    set phase1name toA
    set proposal 3des-md5 3des-sha1
    set pfs enable
    set replay enable
    set src-addr-type subnet6
    set dst-addr-type subnet6
  end
```

```
config firewall policy6
  edit 1
    set srcintf port3
    set dstintf toA
    set srcaddr all6
    set dstaddr all6
    set action accept
    set service ANY
    set schedule always
  next
  edit 2
    set srcintf toA
    set dstintf port3
    set srcaddr all6
    set dstaddr all6
    set action accept
    set service ANY
    set schedule always
  end
config router static6
  edit 1
    set device port2
    set dst 0::/0
  next
  edit 2
    set device toA
    set dst fec0:0000:0000:0000::/64
  end
```

Site-to-site IPv4 over IPv6 VPN example

In this example, two private networks with IPv4 addressing communicate securely over IPv6 infrastructure.

Figure 25: Example IPv4-over-IPv6 VPN topology



Configure FortiGate A interfaces

Port 2 connects to the IPv6 public network and port 3 connects to the IPv4 LAN.

```
config system interface
  edit port2
    config ipv6
      set ip6-address fec0::0001:209:0fff:fe83:25f2/64
    end
  next
  edit port3
    set 192.168.2.1/24
  end
```

Configure FortiGate A IPSec settings

The phase 1 configuration is the same as in the IPv6 over IPv6 example.

```
config vpn ipsec phase1-interface
  edit toB
    set ip-version 6
    set interface port2
    set remote-gw6 fec0:0000:0000:0003:209:0fff:fe83:25c7
    set dpd enable
    set psksecret maryhadalittlelamb
    set proposal 3des-md5 3des-sha1
  end
```

The phase 2 configuration is the same as you would use for an IPv4 VPN. By default, phase 2 selectors are set to accept all subnet addresses for source and destination.

```
config vpn ipsec phase2-interface
  edit toB2
    set phase1name toB
    set proposal 3des-md5 3des-sha1
    set pfs enable
    set replay enable
  end
```

Configure FortiGate A firewall policies

Firewall policies are required to allow traffic between port3 and the IPsec interface toB in each direction. These are IPv4 firewall policies.

```
config firewall policy
  edit 1
    set srcintf port3
    set dstintf toB
    set srcaddr all
    set dstaddr all
    set action accept
    set service ANY
    set schedule always
  next
  edit 2
    set srcintf toB
    set dstintf port3
    set srcaddr all
    set dstaddr all
    set action accept
    set service ANY
    set schedule always
  end
```

Configure FortiGate A routing

This simple example requires just two static routes. Traffic to the protected network behind FortiGate B is routed via the virtual IPSec interface toB using an IPv4 static route. A default route sends all IPv6 traffic, including the IPv6 IPSec packets, out on port2.

```
config router static6
  edit 1
    set device port2
    set dst 0::/0
  next
  edit 2
    set device toB
    set dst 192.168.3.0/24
  end
```

Configure FortiGate B

The configuration of FortiGate B is very similar to that of FortiGate A. A virtual IPSec interface toA is configured on port2 and its remote gateway is the public IP address of FortiGate A. The IPSec phase 2 configuration has IPv4 selectors.

IPv4 firewall policies enable traffic to pass between the private network and the IPSec interface. An IPv4 static route ensures traffic for the private network behind FortiGate A goes through the VPN and an IPv6 static route ensures that all IPv6 packets are routed to the public network.

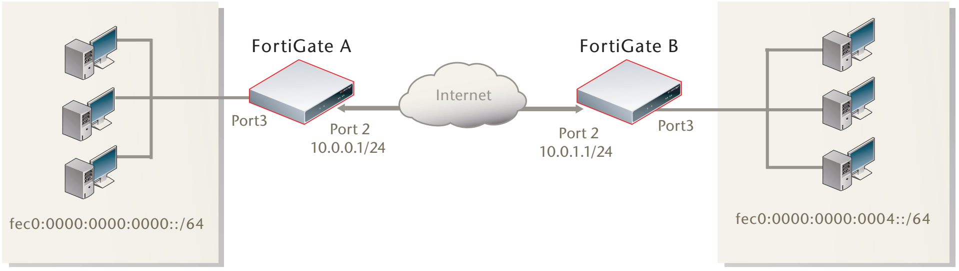
```
config system interface
  edit port2
    config ipv6
      set ip6-address fec0::0003:fe83:25c7/64
    end
  next
  edit port3
    set 192.168.3.1/24
  end
config vpn ipsec phase1-interface
  edit toA
    set ip-version 6
    set interface port2
    set remote-gw6 fec0:0000:0000:0001:209:0fff:fe83:25f2
    set dpd enable
    set psksecret maryhadalittlelamb
    set proposal 3des-md5 3des-sha1
  end
config vpn ipsec phase2-interface
  edit toA2
    set phase1name toA
    set proposal 3des-md5 3des-sha1
    set pfs enable
    set replay enable
  end
```

```
config firewall policy
  edit 1
    set srcintf port3
    set dstintf toA
    set srcaddr all
    set dstaddr all
    set action accept
    set service ANY
    set schedule always
  next
  edit 2
    set srcintf toA
    set dstintf port3
    set srcaddr all
    set dstaddr all
    set action accept
    set service ANY
    set schedule always
  end
config router static6
  edit 1
    set device port2
    set dst 0::/0
  next
  edit 2
    set device toA
    set dst 192.168.2.0/24
  end
```

Site-to-site IPv6 over IPv4 VPN example

In this example, IPv6-addressed private networks communicate securely over IPv4 public infrastructure.

Figure 26: Example IPv6-over-IPv4 VPN topology



Configure FortiGate A interfaces

Port 2 connects to the IPv4 public network and port 3 connects to the IPv6 LAN.

```
config system interface
  edit port2
    set 10.0.0.1/24
  next
  edit port3
    config ipv6
      set ip6-address fec0::0001:209:0fff:fe83:25f3/64
    end
```

Configure FortiGate A IPSec settings

The phase 1 configuration uses IPv4 addressing.

```
config vpn ipsec phase1-interface
  edit toB
    set interface port2
    set remote-gw 10.0.1.1
    set dpd enable
    set psksecret maryhadalittlelamb
    set proposal 3des-md5 3des-sha1
  end
```

The phase 2 configuration uses IPv6 selectors. By default, phase 2 selectors are set to accept all subnet addresses for source and destination. The default setting for `src-addr-type` and `dst-addr-type` is `subnet`. The IPv6 equivalent is `subnet6`. The default subnet addresses are 0.0.0.0/0 for IPv4, `::/0` for IPv6.

```
config vpn ipsec phase2-interface
  edit toB2
    set phase1name toB
    set proposal 3des-md5 3des-sha1
    set pfs enable
    set replay enable
    set src-addr-type subnet6
    set dst-addr-type subnet6
  end
```

Configure FortiGate A firewall policies

IPv6 firewall policies are required to allow traffic between port3 and the IPsec interface toB in each direction. The address `all6` must be defined using the `firewall address6` command as `::/0`.

```
config firewall policy6
  edit 1
    set srcintf port3
    set dstintf toB
    set srcaddr all6
    set dstaddr all6
    set action accept
    set service ANY
    set schedule always
  next
  edit 2
    set srcintf toB
    set dstintf port3
    set srcaddr all6
    set dstaddr all6
    set action accept
    set service ANY
    set schedule always
  end
```

Configure FortiGate A routing

This simple example requires just two static routes. Traffic to the protected network behind FortiGate B is routed via the virtual IPSec interface toB using an IPv6 static route. A default route sends all IPv4 traffic, including the IPv4 IPSec packets, out on port2.

```
config router static6
  edit 1
    set device toB
    set dst fec0:0000:0000:0004::/64
  end
config router static
  edit 1
    set device port2
    set dst 0.0.0.0/0
    set gateway 10.0.0.254
  end
```

Configure FortiGate B

The configuration of FortiGate B is very similar to that of FortiGate A. A virtual IPSec interface toA is configured on port2 and its remote gateway is the IPv4 public IP address of FortiGate A. The IPSec phase 2 configuration has IPv6 selectors.

IPv6 firewall policies enable traffic to pass between the private network and the IPSec interface. An IPv6 static route ensures traffic for the private network behind FortiGate A goes through the VPN and an IPv4 static route ensures that all IPv4 packets are routed to the public network.

```
config system interface
  edit port2
    set 10.0.1.1/24
  next
  edit port3
    config ipv6
      set ip6-address fec0::0004:209:0fff:fe83:2569/64
    end
config vpn ipsec phase1-interface
  edit toA
    set interface port2
    set remote-gw 10.0.0.1
    set dpd enable
    set psksecret maryhadalittlelamb
    set proposal 3des-md5 3des-sha1
  end
config vpn ipsec phase2-interface
  edit toA2
    set phase1name toA
    set proposal 3des-md5 3des-sha1
    set pfs enable
    set replay enable
    set src-addr-type subnet6
    set dst-addr-type subnet6
  end
config firewall policy6
  edit 1
    set srcintf port3
    set dstintf toA
    set srcaddr all6
    set dstaddr all6
    set action accept
    set service ANY
    set schedule always
  next
  edit 2
    set srcintf toA
    set dstintf port3
    set srcaddr all6
    set dstaddr all6
    set action accept
    set service ANY
    set schedule always
  end
config router static6
  edit 1
    set device toA
    set dst fec0:0000:0000:0000::/64
  end
config router static
  edit 1
    set device port2
    set gateway 10.0.1.254
  end
```

Auto Key phase 1 parameters

This section provides detailed step-by-step procedures for configuring a FortiGate unit to accept a connection from a remote peer or dialup client. The phase 1 parameters identify the remote peer or clients and support authentication through preshared keys or digital certificates. You can increase access security further using peer identifiers, certificate distinguished names, group names, or the FortiGate extended authentication (XAuth) option for authentication purposes.

Note: The information and procedures in this section do not apply to VPN peers that perform negotiations using manual keys. Refer to "Manual-key configurations" on page 111 instead.

The following topics are included in this section:

- Overview
- Defining the tunnel ends
- Choosing main mode or aggressive mode
- Authenticating the FortiGate unit
- Authenticating remote peers and clients
- Defining IKE negotiation parameters
- Defining the remaining phase 1 options
- Using XAuth authentication

Overview

IPSec phase 1 settings define:

- the ends of the IPSec tunnel, remote and local
- whether the various phase 1 parameters are exchanged in multiple rounds with encrypted authentication information (main mode) or in a single message with authentication information that is not encrypted (aggressive mode)
- whether a preshared key or digital certificates will be used to authenticate the FortiGate unit to the VPN peer or dialup client
- whether the VPN peer or dialup client is required to authenticate to the FortiGate unit. A remote peer or dialup client can authenticate by peer ID or, if the FortiGate unit authenticates by certificate, it can authenticate by peer certificate.
- the IKE negotiation proposals for encryption and authentication
- optional XAuth authentication, which requires the remote user to enter a user name and password. A FortiGate VPN server can act as an XAuth server to authenticate dialup users. A FortiGate unit that is a dialup client can also be configured as an XAuth client to authenticate itself to the VPN server.

Defining the tunnel ends

To begin defining the phase 1 configuration, you go to **VPN > IPSEC > Auto Key** and select Create Phase 1. Enter a descriptive name for the VPN tunnel. This is particularly important if you will create several tunnels.

The phase 1 configuration mainly defines the ends of the IPSec tunnel. The remote end is the remote gateway with which the FortiGate unit exchanges IPSec packets. The local end is FortiGate interface that sends and receives IPSec packets.

The remote gateway can be any of the following:

- a static IP address
- a domain name with a dynamic IP address
- a dialup client

A statically addressed remote gateway is the simplest to configure. You specify the IP address. Unless restricted in the firewall policy, either the remote peer or a peer on the network behind the FortiGate unit can bring up the tunnel.

If the remote peer has a domain name and subscribes to a dynamic DNS service, you need to specify only the domain name. The FortiGate unit performs a DNS query to determine the appropriate IP address. Unless restricted in the firewall policy, either the remote peer or a peer on the network behind the FortiGate unit can bring up the tunnel.

If the remote peer is a dialup client, only the dialup client can bring up the tunnel. The IP address of the client is not known until it connects to the FortiGate unit. This configuration is a typical way to provide a VPN for client PCs running VPN client software such as the FortiClient Host Security application.

The local end of the VPN tunnel, the Local Interface, is the FortiGate interface that sends and receives the IPSec packets. This is usually the public interface of the FortiGate unit that is connected to the Internet. Packets from this interface pass to the private network through a firewall policy. If you are configuring an interface mode VPN, in the Advanced phase 1 settings you can optionally specify a unique address for the FortiGate end of the tunnel. By default, the FortiGate unit uses the IP address of the selected Local Interface taken from the System > Network > Interface settings.

Choosing main mode or aggressive mode

The FortiGate unit and the remote peer or dialup client exchange phase 1 parameter in either Main mode or Aggressive mode.

- In Main mode, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information
- In Aggressive mode, the phase 1 parameters are exchanged in single message with authentication information that is not encrypted.

Main mode is more secure, but you must select Aggressive mode if there is more than one dialup phase 1 configuration for the interface IP address and the remote VPN peer or client is authenticated using an identifier (local ID). Descriptions of the peer options in this guide indicate if either Main or Aggressive mode is required.

Authenticating the FortiGate unit

The FortiGate unit can authenticate itself to remote peers or dialup clients using either a pre-shared key or an RSA Signature (certificate).

Authenticating the FortiGate unit with digital certificates

To authenticate the FortiGate unit using digital certificates, you must have the required certificates installed on the remote peer and on the FortiGate unit. The signed server certificate on one peer is validated by the presence of the root certificate installed on the other peer. If you use certificates to authenticate the FortiGate unit, you can also require the remote peers or dialup clients to authenticate using certificates.

For more information about obtaining and installing certificates, see the *FortiGate Certificate Management User Guide.*

To authenticate the FortiGate unit using digital certificates

1 Go to **VPN > IPSEC > Auto Key**.

2 Select Create Phase 1 to add a new phase 1 configuration or select the Edit button beside an existing Phase 1 configuration.

3 Include appropriate entries as follows:

Name
Enter a name that reflects the origination of the remote connection.

Remote Gateway
Select the nature of the remote connection:

- Static IP Address.
- Dialup User.
- Dynamic DNS.

For more information, see “Defining the tunnel ends” on page 128.

Local Interface
Select the interface that is the local end of the IPSec tunnel. For more information, see “Defining the tunnel ends” on page 128.

Mode
Select Main or Aggressive mode.

- In Main mode, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information.
- In Aggressive mode, the phase 1 parameters are exchanged in single message with authentication information that is not encrypted.

When the remote VPN peer or client has a dynamic IP address, or the remote VPN peer or client will be authenticated using an identifier (local ID), you must select Aggressive mode if there is more than one dialup phase 1 configuration for the interface IP address.

For more information, see “Choosing main mode or aggressive mode” on page 128.

Authentication Method
Select RSA Signature.

Certificate Name
Select the name of the server certificate that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. To obtain and load the required server certificate, see the *FortiGate Certificate Management User Guide*.

Peer Options	Peer options define the authentication requirements for remote peers or dialup clients, not for the FortiGate unit itself. For more information, see “Authenticating remote peers and clients” on page 131.
Advanced	You can retain the default settings unless changes are needed to meet your specific requirements. See “Defining IKE negotiation parameters” on page 137.

4 If you are configuring authentication parameters for a dialup user group, optionally define extended authentication (XAuth) parameters. See “Using the FortiGate unit as an XAuth server” on page 141.

5 Select OK.

Authenticating the FortiGate unit with a pre-shared key

The simplest way to authenticate a FortiGate unit to its remote peers or dialup clients is by means of a pre-shared key. This is less secure than using certificates, especially if it used alone, without requiring peer IDs or extended authentication (XAuth). Also, you need to have a secure way to distribute the pre-shared key to the peers.

If you use pre-shared key authentication alone, all remote peers and dialup clients must be configured with the same pre-shared key. Optionally, you can configure remote peers and dialup clients with unique pre-shared keys. On the FortiGate unit, these are configured in user accounts, not in the phase_1 settings. For more information, see “Enabling VPN access using user accounts and pre-shared keys” on page 135.

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

If you authenticate the FortiGate unit using a pre-shared key, you can require remote peers or dialup clients to authenticate using peer IDs, but not client certificates.

To authenticate the FortiGate unit with a pre-shared key

1 Go to **VPN > IPSEC > Auto Key**.

2 Select Create Phase 1 to add a new phase 1 configuration or select the Edit button beside an existing configuration.

3 Include appropriate entries as follows:

Name	Enter a name that reflects the origination of the remote connection.
Remote Gateway	Select the nature of the remote connection: • Static IP Address. • Dialup User. • Dynamic DNS. For more information, see “Defining the tunnel ends” on page 128.
Local Interface	Select the interface that is the local end of the IPSec tunnel. For more information, see “Defining the tunnel ends” on page 128.

Mode

Select Main or Aggressive mode.

- In Main mode, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information.
- In Aggressive mode, the phase 1 parameters are exchanged in single message with authentication information that is not encrypted.

When the remote VPN peer or client has a dynamic IP address, or the remote VPN peer or client will be authenticated using an identifier (local ID), you must select Aggressive mode if there is more than one dialup phase 1 configuration for the interface IP address.

For more information, see “Choosing main mode or aggressive mode” on page 128.

Authentication Method

Select Pre-shared Key.

Pre-shared Key

Enter the preshared key that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. You must define the same value at the remote peer or client. 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.

Peer options

Peer options define the authentication requirements for remote peers or dialup clients, not for the FortiGate unit itself. You can require the use of peer IDs, but not client certificates. For more information, see “Authenticating remote peers and clients” on page 131.

Advanced

You can retain the default settings unless changes are needed to meet your specific requirements. See “Defining IKE negotiation parameters” on page 137.

4 If you are configuring authentication parameters for a dialup user group, optionally define extended authentication (XAuth) parameters. See “Using the FortiGate unit as an XAuth server” on page 141.

5 Select OK.

Authenticating remote peers and clients

Certificates or pre-shared keys restrict who can access the VPN tunnel, but they do not identify or authenticate the remote peers or dialup clients. You have the following options for authentication:

- You can permit access only for remote peers or clients who use certificates that you recognize. This is available only if the FortiGate unit authenticates using certificates. See “Enabling VPN access for specific certificate holders” on page 132.
- You can permit access only for remote peers or clients that have certain peer identifier (local ID) value configured. This is available with both certificate and preshared key authentication. See “Enabling VPN access by peer identifier” on page 134.
- You can permit access to remote peers or dialup clients who each have a unique preshared key. Each peer or client must have a user account on the FortiGate unit. See “Enabling VPN access using user accounts and pre-shared keys” on page 135.

- You can permit access to remote peers or dialup clients who each have a unique peer ID and a unique preshared key. Each peer or client must have a user account on the FortiGate unit. See “Enabling VPN access using user accounts and pre-shared keys” on page 135.

For authentication of users of the remote peer or dialup client device, see “Using XAuth authentication” on page 141.

Enabling VPN access for specific certificate holders

When a VPN peer or dialup client is configured to authenticate using digital certificates, it sends the DN of its certificate to the FortiGate unit. This DN can be used to allow VPN access for the certificate holder. That is, a FortiGate unit can be configured to deny connections to all remote peers and dialup clients except the one having the specified DN.

Before you begin

The following procedures assume that you already have an existing phase 1 configuration (see “Authenticating the FortiGate unit with digital certificates” on page 129). Follow the procedures below to add certificate-based authentication parameters to the existing configuration.

Before you begin, you must obtain the certificate DN of the remote peer or dialup client. If you are using the FortiClient Host Security application as a dialup client, refer to *FortiClient online Help* for information about how to view the certificate DN. To view the certificate DN of a FortiGate unit, see “To view server certificate information and obtain the local DN” on page 133.

Afterward, use the config user peer CLI command to load the DN value into the FortiGate configuration. For example, if a remote VPN peer uses server certificates issued by your own organization, you would enter information similar to the following:

```
config user peer
  edit DN_FG1000
    set cn 192.168.2.160
    set cn-type ipv4
  end
```

The value that you specify to identify the entry (for example, DN_FG1000) is displayed in the Accept this peer certificate only list in the IPSec phase 1 configuration when you return to the web-based manager.

If the remote VPN peer has a CA-issued certificate to support a higher level of credibility, you would enter information similar to the following:

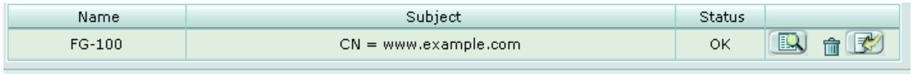
```
config user peer
  edit CA_FG1000
    set ca CA_Cert_1
    set subject FG1000_at_site1
  end
```

The value that you specify to identify the entry (for example, CA_FG1000) is displayed in the Accept this peer certificate only list in the IPSec phase 1 configuration when you return to the web-based manager. For more information about these CLI commands, see the “user” chapter of the *FortiGate CLI Reference*.

A group of certificate holders can be created based on existing user accounts for dialup clients. To create the user accounts for dialup clients, see the “User” chapter of the *FortiGate Administration Guide*. To create the certificate group afterward, use the `config user peergrp` CLI command. See the “user” chapter of the *FortiGate CLI Reference*.

To view server certificate information and obtain the local DN

1 Go to **VPN > Certificates > Local Certificates**.

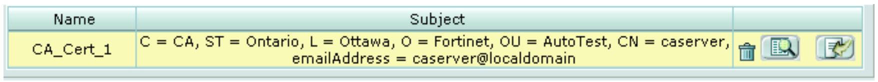


Name	Subject	Status	
FG-100	CN = www.example.com	OK	

2 Note the CN value in the Subject field (for example, `CN = 172.16.10.125`, `CN = info@fortinet.com`, or `CN = www.example.com`).

To view CA root certificate information and obtain the CA certificate name

1 Go to **VPN > Certificates > CA Certificates**.



Name	Subject	
CA_Cert_1	C = CA, ST = Ontario, L = Ottawa, O = Fortinet, OU = AutoTest, CN = caserver, emailAddress = caserver@localdomain	

2 Note the value in the Name column (for example, `CA_Cert_1`).

To enable access for a specific certificate holder or a group of certificate holders

1. At the FortiGate VPN server, go to **VPN > IPSEC > Auto Key**.
2. In the list of defined configurations, select the Edit button to edit the existing phase 1 configuration.
3. From the Authentication Method list, select RSA Signature.
4. From the Certificate Name list, select the name of the server certificate that the FortiGate unit will use to authenticate itself to the remote peer or dialup client
5. Under Peer Options, select one of these options:
   - To accept a specific certificate holder, select Accept this peer certificate only and select the name of the certificate that belongs to the remote peer or dialup client. The certificate DN must be added to the FortiGate configuration through CLI commands before it can be selected here. See “Before you begin” on page 132.
   - To accept dialup clients who are members of a certificate group, select Accept this peer certificate group only and select the name of the group. The group must be added to the FortiGate configuration through CLI commands before it can be selected here. See “Before you begin” on page 132.
6. If you want the FortiGate VPN server to supply the DN of a local server certificate for authentication purposes, select Advanced and then from the Local ID list, select the DN of the certificate that the FortiGate VPN server is to use.
7. Select OK.

Enabling VPN access by peer identifier

Whether you use certificates or pre-shared keys to authenticate the FortiGate unit, you can require that remote peers or clients have a particular peer ID. This adds another piece of information that is required to gain access to the VPN. More than one FortiGate/FortiClient dialup client may connect through the same VPN tunnel when the dialup clients share a preshared key and assume the same identifier.

You cannot require a peer ID for a remote peer or client that uses a pre-shared key and has a static IP address.

To authenticate remote peers or dialup clients using one peer ID

1. At the FortiGate VPN server, go to **VPN > IPSEC > Auto Key (IKE)**.
2. In the list, select the Edit icon of a phase 1 configuration to edit its parameters.
3. Select Aggressive mode in any of the following cases:
   - the FortiGate VPN server authenticates a FortiGate dialup client that uses a dedicated tunnel
   - a FortiGate unit has a dynamic IP address and subscribes to a dynamic DNS service
   - FortiGate/FortiClient dialup clients sharing the same preshared key and local ID connect through the same VPN tunnel
4. Select Accept this peer ID and type the identifier into the corresponding field.
5. Select OK.

To assign an identifier (local ID) to a FortiGate unit

Use this procedure to assign a peer ID to a FortiGate unit that acts as a remote peer or dialup client.

1 Go to **VPN > IPSEC > Auto Key (IKE)**.

2 In the list, select the Edit icon of a phase 1 configuration to edit its parameters.

3 Select Advanced.

4 In the Local ID field, type the identifier that the FortiGate unit will use to identify itself.

5 Set Mode to Aggressive if any of the following conditions apply:

- The FortiGate unit is a dialup client that will use a unique ID to connect to a FortiGate dialup server through a dedicated tunnel.
- The FortiGate unit has a dynamic IP address, subscribes to a dynamic DNS service, and will use a unique ID to connect to the remote VPN peer through a dedicated tunnel.
- The FortiGate unit is a dialup client that shares the specified ID with multiple dialup clients to connect to a FortiGate dialup server through the same tunnel.

6 Select OK.

To configure the FortiClient Host Security application

Follow this procedure to add a peer ID to an existing FortiClient configuration:

1 Start the FortiClient Host Security application.

2 Go to **VPN > Connections**, select the existing configuration, and then select Advanced > Edit.

3 Select Advanced.

4 Under Policy, select Config.

5 In the Local ID field, type the identifier that will be shared by all dialup clients. This value must match the Accept this peer ID value that you specified previously in the phase 1 gateway configuration on the FortiGate unit.

6 Select OK to close all dialog boxes.

7 Configure all dialup clients the same way using the same preshared key and local ID.

Enabling VPN access using user accounts and pre-shared keys

You can permit access only to remote peers or dialup clients that have pre-shared keys and/or peer IDs configured in user accounts on the FortiGate unit.

If you want two VPN peers (or a FortiGate unit and a dialup client) to accept reciprocal connections based on peer IDs, you must enable the exchange of their identifiers when you define the phase 1 parameters.

The following procedures assume that you already have an existing phase 1 configuration (see “Authenticating the FortiGate unit with digital certificates” on page 129). Follow the procedures below to add ID checking to the existing configuration.

Before you begin, you must obtain the identifier (local ID) of the remote peer or dialup client. If you are using the FortiClient Host Security application as a dialup client, refer to the *Authenticating FortiClient Dialup Clients Technical Note* to view or assign an identifier. To assign an identifier to a FortiGate dialup client or a FortiGate unit that has a dynamic IP address and subscribes to a dynamic DNS service, see "To assign an identifier (local ID) to a FortiGate unit" on page 135.

If required, a dialup user group can be created from existing user accounts for dialup clients. To create the user accounts and user groups, see the "User" chapter of the *FortiGate Administration Guide*.

To authenticate dialup clients using unique preshared keys and/or peer IDs

The following procedure supports FortiGate/FortiClient dialup clients that use unique preshared keys and/or peer IDs. The client must have an account on the FortiGate unit and be a member of the dialup user group.

The dialup user group must be added to the FortiGate configuration before it can be selected (see the "User" chapter of the *FortiGate Administration Guide*).

The FortiGate dialup server compares the local ID that you specify at each dialup client to the FortiGate user-account user name. The dialup-client preshared key is compared to a FortiGate user-account password.

1. At the FortiGate VPN server, go to **VPN > IPSEC > Auto Key (IKE)**.
2. In the list, select the Edit icon of a phase 1 configuration to edit its parameters.
3. If the clients have unique peer IDs, set Mode to Aggressive.
4. Clear the Pre-shared Key field (the field should be empty).
5. Select Accept peer ID in dialup group and then select the group name from the list of user groups.
6. Select OK.

To configure FortiClient dialup clients - pre-shared key and peer ID

Follow this procedure to add a unique pre-shared key and unique peer ID to an existing FortiClient configuration:

1. Start the FortiClient Host Security application.
2. Go to **VPN > Connections**, select the existing configuration, and then select Advanced > Edit.
3. In the Preshared Key field, type the FortiGate password that belongs to the dialup client (for example, `1234546`).
4. Select Advanced.
5. Under Policy, select Config.
6. In the Local ID field, type the FortiGate user name that you assigned previously to the dialup client (for example, `FortiC1ient1`).
7. Select OK to close all dialog boxes.

Configure all FortiClient dialup clients this way using unique preshared keys and local IDs.

To configure FortiClient dialup clients - preshared key only

Follow this procedure to add a unique pre-shared key to an existing FortiClient configuration:

1. Start the FortiClient Host Security application.
2. Go to **VPN > Connections**, select the existing configuration, and then select Advanced > Edit.
3. In the Preshared Key field, type the user name, followed by a "+" sign, followed by the password that you specified previously in the user account settings on the FortiGate unit (for example, `FC2+1FG6LK`)
4. Select OK to close all dialog boxes.

Configure all the FortiClient dialup clients this way using their unique peer ID and pre-shared key values.

Defining IKE negotiation parameters

In phase 1, the two peers exchange keys to establish a secure communication channel between them. As part of the phase 1 process, the two peers authenticate each other (see "Authenticating remote peers and clients" on page 131) and negotiate a way to encrypt further communications for the duration of the session. The P1 Proposal parameters select the encryption and authentication algorithms that are used to generate keys for protecting negotiations.

The IKE negotiation parameters determine:

- which encryption algorithms may be applied for converting messages into a form that only the intended recipient can read
- which authentication hash may be used for creating a keyed hash from a preshared or private key
- which Diffie-Hellman group will be used to generate a secret session key

Phase 1 negotiations (in main mode or aggressive mode) begin as soon as a remote VPN peer or client attempts to establish a connection with the FortiGate unit. Initially, the remote peer or dialup client sends the FortiGate unit a list of potential cryptographic parameters along with a session ID. The FortiGate unit compares those parameters to its own list of advanced phase 1 parameters and responds with its choice of matching parameters to use for authenticating and encrypting packets. The two peers handle the exchange of encryption keys between them, and authenticate the exchange through a preshared key or a digital signature.

Generating keys to authenticate an exchange

The FortiGate unit supports the generation of secret session keys automatically using a Diffie-Hellman algorithm. The Keylife setting in the P1 Proposal area determines the amount of time before the phase 1 key expires. Phase 1 negotiations are rekeyed automatically when there is an active security association. See "Dead peer detection" on page 141.

Note: You can enable or disable automatic rekeying between IKE peers through the `phase1-rekey` attribute of the `config system global` CLI command. For more information, see the “system” chapter of the *FortiGate CLI Reference*.

When you use a preshared key (shared secret) to set up two-party authentication, the remote VPN peer or client and the FortiGate unit must both be configured with the same preshared key. Each party uses a session key derived from the Diffie-Hellman exchange to create an authentication key, which is used to sign a known combination of inputs using an authentication algorithm (such as HMAC-MD5 or HMAC-SHA-1). Each party signs a different combination of inputs and the other party verifies that the same result can be computed.

Note: When you use preshared keys to authenticate VPN peers or clients, you must distribute matching information to all VPN peers and/or clients whenever the preshared key changes.

As an alternative, the remote peer or dialup client and FortiGate unit can exchange digital signatures to validate each other’s identity with respect to their public keys. In this case, the required digital certificates (see the *FortiGate Certificate Management User Guide*) must be installed on the remote peer and on the FortiGate unit. By exchanging certificate DNs, the signed server certificate on one peer is validated by the presence of the root certificate installed on the other peer.

The following procedure assumes that you already have a phase 1 definition that describes how remote VPN peers and clients will be authenticated when they attempt to connect to a local FortiGate unit. For information about the Local ID and XAuth options, see “Enabling VPN access using user accounts and pre-shared keys” on page 135 and “Using the FortiGate unit as an XAuth server” on page 141. Follow this procedure to add IKE negotiation parameters to the existing definition.

Defining IKE negotiation parameters

1. Go to **VPN > IPSEC > Auto Key (IKE)**.
2. In the list, select the Edit button to edit the phase 1 parameters for a particular remote gateway.

3 Select Advanced and include appropriate entries as follows:

P1 Proposal

Select the encryption and authentication algorithms that will be used to generate keys for protecting negotiations.

Add or delete encryption and authentication algorithms as required. Select a minimum of one and a maximum of three combinations. The remote peer must be configured to use at least one of the proposals that you define.

You can select any of the following symmetric-key algorithms:

- DES-Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- 3DES-Triple-DES, in which plain text is encrypted three times by three keys.
- AES128-A 128-bit block algorithm that uses a 128-bit key.
- AES192-A 128-bit block algorithm that uses a 192-bit key.
- AES256-A 128-bit block algorithm that uses a 256-bit key.

You can select either of the following message digests to check the authenticity of messages during phase 1 negotiations:

- MD5-Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA1-Secure Hash Algorithm 1, which produces a 160-bit message digest.

To specify a third combination, use the add button beside the fields for the second combination.

DH Group

Select one or more Diffie-Hellman groups from DH group 1, 2, and 5. When using aggressive mode, DH groups cannot be negotiated.

- If both VPN peers (or a VPN server and its client) have static IP addresses and use aggressive mode, select a single DH group. The setting on the FortiGate unit must be identical to the setting on the remote peer or dialup client.
- When the remote VPN peer or client has a dynamic IP address and uses aggressive mode, select up to three DH groups on the FortiGate unit and one DH group on the remote peer or dialup client. The setting on the remote peer or dialup client must be identical to one of the selections on the FortiGate unit.
- If the VPN peer or client employs main mode, you can select multiple DH groups. At least one of the settings on the remote peer or dialup client must be identical to the selections on the FortiGate unit.

Keylife

Type the amount of time (in seconds) that will be allowed to pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172800 seconds.

Nat-traversal

Enable this option if a NAT device exists between the local FortiGate unit and the VPN peer or client. The local FortiGate unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared).

Keepalive Frequency

If you enabled NAT traversal, enter a keepalive frequency setting. The value represents an interval from 0 to 900 seconds.

Dead Peer Detection

Enable this option to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required.

4 Select OK.

Defining the remaining phase 1 options

Additional advanced phase 1 settings are available to ensure the smooth operation of phase 1 negotiations:

- Nat-traversal—If outbound encrypted packets will be subjected to NAT, this option determines whether the packet will be wrapped in a UDP IP header to protect the encrypted packet from modification. See "NAT traversal" below.
- Keepalive Frequency—If outbound encrypted packets will be subjected to NAT, this option determines how frequently empty UDP packets will be sent through the NAT device to prevent NAT address mapping from changing before the lifetime of a session expires. See "NAT keepalive frequency" below.
- Dead Peer Detection—This option determines whether the FortiGate unit will detect dead IKE peers and terminate a session between the time when a VPN connection becomes idle and the phase 1 encryption key expires. See "Dead peer detection" on page 141.

NAT traversal

Network Address Translation (NAT) is a way to convert private IP addresses to publicly routable Internet addresses and vise versa. When an IP packet passes through a NAT device, the source or destination address in the IP header is modified. FortiGate units support NAT version 1 (encapsulate on port 500 with non-IKE marker), version 3 (encapsulate on port 4500 with non-ESP marker), and compatible versions.

NAT cannot be performed on IPSec packets in ESP tunnel mode because the packets do not contain a port number. As a result, the packets cannot be demultiplexed. To work around this problem, the FortiGate unit provides a way to protect IPSec packet headers from NAT modifications. When the Nat-traversal option is enabled, outbound encrypted packets are wrapped inside a UDP IP header that contains a port number. This extra encapsulation allows NAT devices to change the port number without modifying the IPsec packet directly.

To provide the extra layer of encapsulation on IPSec packets, the Nat-traversal option must be enabled whenever a NAT device exists between two FortiGate VPN peers or a FortiGate unit and a dialup client such as FortiClient. On the receiving end, the FortiGate unit or FortiClient removes the extra layer of encapsulation before decrypting the packet.

NAT keepalive frequency

When a NAT device performs network address translation on a flow of packets, the NAT device determines how long the new address will remain valid if the flow of traffic stops (for example, the connected VPN peer may be idle). The device may reclaim and reuse a NAT address when a connection remains idle for too long. To work around this problem, when you enable NAT traversal, you can specify how often the FortiGate unit should send periodic keepalive packets through the NAT device in order to ensure that the NAT address mapping does not change during the lifetime of a session. The keepalive interval should be smaller than the session lifetime value used by the NAT device.

Dead peer detection

Sometimes, due to routing problems or other difficulties, the communication link between a FortiGate unit and a VPN peer or client may go down—packets could be lost if the connection is left to time out on its own. The FortiGate unit provides a mechanism called Dead Peer Detection (DPD) to prevent this situation and reestablish IKE negotiations automatically before a connection times out: the active phase 1 security associations are caught and renegotiated (rekeyed) before the phase 1 encryption key expires. By default, DPD send probe messages every five seconds (see `dpd-retryinterval` in the *FortiGate CLI Reference*).

In the web-based manager, the Dead Peer Detection option can be enabled when you define advanced phase 1 options. The `config vpn ipsec phase1` CLI command supports additional options for specifying a retry count and a retry interval. For more information about these CLI commands, see the *FortiGate CLI Reference*.

Using XAuth authentication

Extended authentication (XAuth) increases security by requiring authentication of the user of the remote dialup client in a separate exchange at the end of phase 1. XAuth draws on existing FortiGate user group definitions and uses established authentication mechanisms such as PAP, CHAP, RADIUS and LDAP to authenticate dialup clients. You can configure a FortiGate unit to function either as an XAuth server or an XAuth client.

Using the FortiGate unit as an XAuth server

A FortiGate unit can act as an XAuth server for dialup clients. When the phase 1 negotiation completes, the FortiGate unit challenges the user for a user name and password. It then forwards the user’s credentials to an external RADIUS or LDAP server for verification.

The authentication protocol to use for XAuth depends on the capabilities of the authentication server and the XAuth client:

- Select PAP whenever possible. Select CHAP instead if applicable.
- You must select PAP for all implementations of LDAP and some implementations of Microsoft RADIUS.
- Select MIXED when the authentication server supports CHAP but the XAuth client does not. The FortiGate unit will use PAP to communicate with the XAuth client and CHAP to communicate with the authentication server.

To authenticate a dialup user group using XAuth settings

Before you begin, create user accounts and user groups to identify the dialup clients that need to access the network behind the FortiGate dialup server. If password protection will be provided through an external RADIUS or LDAP server, you must configure the FortiGate dialup server to forward authentication requests to the authentication server. For information about these topics, see the “User” chapter of the *FortiGate Administration Guide*.

1. At the FortiGate dialup server, go to **VPN > IPSEC > Auto Key (IKE)**.
2. In the list, select the Edit icon of a phase 1 configuration to edit its parameters for a particular remote gateway.

3 Select Advanced.

4 Under XAuth, select Enable as Server.

5 The Server Type setting determines the type of encryption method to use between the XAuth client, the FortiGate unit and the authentication server. Select one of the following options:

- PAP—Password Authentication Protocol.
- CHAP— Challenge-Handshake Authentication Protocol.
- MIXED—Use PAP between the XAuth client and the FortiGate unit, and CHAP between the FortiGate unit and the authentication server.

6 From the User Group list, select the user group that needs to access the private network behind the FortiGate unit. The group must be added to the FortiGate configuration before it can be selected here.

7 Select OK.

Authenticating the FortiGate unit as a client with XAuth

If the FortiGate unit acts as a dialup client, the remote peer, acting as an XAuth server, might require a user name and password. You can configure the FortiGate unit as an XAuth client, with its own user name and password, which it provides when challenged.

To configure the FortiGate dialup client as an XAuth client

1 At the FortiGate dialup client, go to **VPN > IPSEC > Auto Key (IKE)**.

2 In the list, select the Edit icon of a phase 1 configuration to edit its parameters for a particular remote gateway.

3 Select Advanced.

4 Under XAuth, select Enable as Client.

5 In the Username field, type the FortiGate PAP, CHAP, RADIUS, or LDAP user name that the FortiGate XAuth server will compare to its records when the FortiGate XAuth client attempts to connect.

6 In the Password field, type the password to associate with the user name.

7 Select OK.

Phase 2 parameters

This section describes the phase 2 parameters that are required to establish communication through a VPN.

The following topics are included in this section:

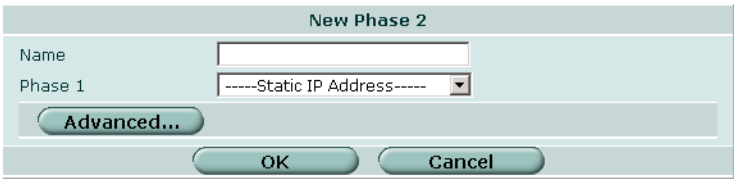
- Basic phase 2 settings
- Advanced phase 2 settings
- Configure the phase 2 parameters

Basic phase 2 settings

After phase 1 negotiations complete successfully, phase 2 begins. The phase 2 parameters define the algorithms that the FortiGate unit can use to encrypt and transfer data for the remainder of the session. The basic phase 2 settings associate IPSec phase 2 parameters with a phase 1 configuration.

When you define phase 2 parameters, you can choose any set of phase 1 parameters to set up a secure connection and authenticate the remote peer.

Figure 27: Basic Phase 2 settings (VPN > IPSEC > Auto Key (IKE) > Create Phase 2



New Phase 2

Name	
Phase 1	-----Static IP Address-----

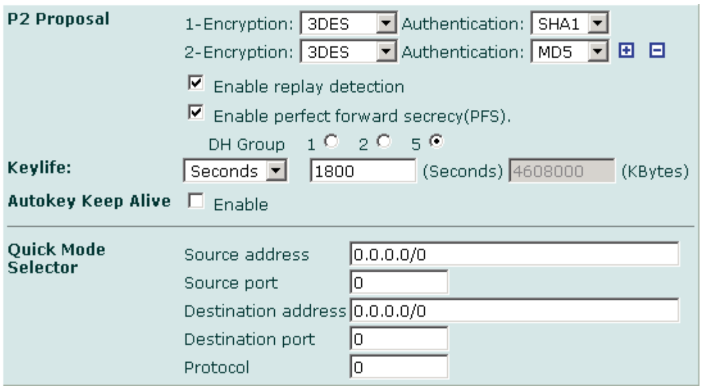
The information and procedures in this section do not apply to VPN peers that perform negotiations using manual keys. Refer to “Manual-key configurations” on page 111 instead.

Advanced phase 2 settings

The following additional advanced phase 2 settings are available to enhance the operation of the tunnel:

- P2 proposal
- Enable replay detection
- Enable perfect forward secrecy (PFS)
- Quick Mode Identities

Figure 28: Advanced phase 2 settings



P2 Proposal
1-Encryption: 3DES Authentication: SHA1
2-Encryption: 3DES Authentication: MD5
☑ Enable replay detection
☑ Enable perfect forward secrecy(PFS).
DH Group 1 ○ 2 ○ 5 ●

Keylife: Seconds 1800 (Seconds) 4608000 (KBytes)

Autokey Keep Alive □ Enable

Quick Mode Selector
Source address 0.0.0.0/0
Source port 0
Destination address 0.0.0.0/0
Destination port 0
Protocol 0

P2 Proposal

In phase 2, the FortiGate unit and the VPN peer or client exchange keys again to establish a secure communication channel between them. The P2 Proposal parameters select the encryption and authentication algorithms needed to generate keys for protecting the implementation details of Security Associations (SAs). The keys are generated automatically using a Diffie-Hellman algorithm.

Replay detection

IPSec tunnels can be vulnerable to replay attacks. Replay detection enables the FortiGate unit to check all IPSec packets to see if they have been received before. If any encrypted packets arrive out of order, the FortiGate unit discards them.

Perfect forward secrecy

By default, phase 2 keys are derived from the session key created in phase 1. Perfect forward secrecy forces a new Diffie-Hellman exchange when the tunnel starts and whenever the phase 2 keylife expires, causing a new key to be generated each time. This exchange ensures that the keys created in phase 2 are unrelated to the phase 1 keys or any other keys generated automatically in phase 2.

Keylife

The Keylife setting sets a limit on the length of time that a phase 2 key can be used. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when either the time has passed or the number of KB have been processed. When the phase 2 key expires, a new key is generated without interrupting service.

Auto-negotiate

By default, the phase 2 security association (SA) is not negotiated until a peer attempts to send data. The triggering packet and some subsequent packets are dropped until the SA is established. Applications normally resend this data, so there is no loss, but there might be a noticeable delay in response to the user.

Automatically establishing the SA can also be important on a dialup peer. This ensures that the VPN tunnel is available for peers at the server end to initiate traffic to the dialup peer. Otherwise, the VPN tunnel does not exist until the dialup peer initiates traffic.

When enabled, auto-negotiate initiates the phase 2 SA negotiation automatically, repeating every five seconds until the SA is established.

The auto-negotiate feature is available only through the Command Line Interface (CLI). Use the following commands to enable it.

```
config vpn ipsec phase2
  edit <phase2_name>
    set auto-negotiate enable
  end
```

If the tunnel ever goes down, the auto-negotiate feature will try to re-establish it. However, the Autokey Keep Alive feature is a better way to keep your VPN up.

Autokey Keep Alive

The phase 2 security association (SA) has a fixed duration. If there is traffic on the VPN as the SA nears expiry, a new SA is negotiated and the VPN switches to the new SA with no interruption. If there is no traffic, the SA expires and the VPN tunnel goes down.

The Autokey Keep Alive option ensures that a new SA is negotiated even if there is no traffic so that the VPN tunnel stays up.

DHCP-IPSec

Select this option if the FortiGate unit assigns VIP addresses to FortiClient dialup clients through a DHCP server or relay. This option is available only if the Remote Gateway in the phase 1 configuration is set to Dialup User and it works only on policy-based VPNs.

The DHCP-IPSec option causes the FortiGate dialup server to act as a proxy for FortiClient dialup clients that have VIP addresses on the subnet of the private network behind the FortiGate unit. In this case, the FortiGate dialup server acts as a proxy on the local private network for the FortiClient dialup client. When a host on the network behind the dialup server issues an ARP request that corresponds to the device MAC address of the FortiClient host, the FortiGate unit answers the ARP request on behalf of the FortiClient host and forwards the associated traffic to the FortiClient host through the tunnel.

Quick mode selectors

The Quick Mode selectors determine who (which IP addresses) can perform IKE negotiations to establish a tunnel. The default settings are as broad as possible: any IP address, using any protocol, on any port. This enables configurations in which multiple subnets at each end of the tunnel can communicate, limited only by the firewall policies at each end.

There are some configurations that require specific selectors:

- the VPN peer is a third-party device that uses specific phase2 selectors
- the FortiGate unit connects as a dialup client to another FortiGate unit, in which case you must specify a source IP address, IP address range or subnet

The quick mode selectors allow IKE negotiations only for peers that match the specified configuration. This does not control traffic on the VPN. Access to IPSec VPN tunnels is controlled through firewall policies.

Configure the phase 2 parameters

Follow this procedure to create an IPSec phase 2 definition.

Note: If you are creating a hub-and-spoke configuration or an Internet-browsing configuration, you may have already started defining some of the required phase 2 parameters. If so, edit the existing definition to complete the configuration.

Specifying the phase 2 parameters

1. Go to **VPN > IPSEC > Auto Key (IKE)**.
2. Select Create Phase 2 to add a new phase 2 configuration or select the Edit button beside an existing phase 2 configuration.
3. Include appropriate entries as follows:

Name	Enter a name to identify the phase 2 configuration.
Phase 1	Select the phase 1 configuration that describes how remote peers or dialup clients will be authenticated on this tunnel, and how the connection to the remote peer or dialup client will be secured.

4. Select Advanced.

5 Include appropriate entries as follows:

P2 Proposal Select the encryption and authentication algorithms that will be used to change data into encrypted code.

Add or delete encryption and authentication algorithms as required. Select a minimum of one and a maximum of three combinations. The remote peer must be configured to use at least one of the proposals that you define.

It is invalid to set both Encryption and Authentication to null.

Encryption You can select any of the following symmetric-key algorithms:

- NULL-Do not use an encryption algorithm.
- DES-Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- 3DES-Triple-DES, in which plain text is encrypted three times by three keys.
- AES128-A 128-bit block algorithm that uses a 128-bit key.
- AES192-A 128-bit block algorithm that uses a 192-bit key.
- AES256-A 128-bit block algorithm that uses a 256-bit key.

Authentication You can select either of the following message digests to check the authenticity of messages during an encrypted session:

- NULL-Do not use a message digest.
- MD5-Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA1-Secure Hash Algorithm 1, which produces a 160-bit message digest.

To specify one combination only, set the Encryption and Authentication options of the second combination to NULL. To specify a third combination, use the Add button beside the fields for the second combination.

Enable replay detection Optionally enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPSec packets and replays them back into the tunnel.

Enable perfect forward secrecy (PFS) Enable or disable PFS. Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.

DH Group Select one Diffie-Hellman group (1, 2, or 5). The remote peer or dialup client must be configured to use the same group.

Keylife Select the method for determining when the phase 2 key expires: Seconds, KBytes, or Both. If you select both, the key expires when either the time has passed or the number of KB have been processed. The range is from 120 to 172800 seconds, or from 5120 to 2147483648 KB.

Autokey Keep Alive Enable the option if you want the tunnel to remain active when no data is being processed.

DHCP-IPSec Select Enable if the FortiGate unit acts as a dialup server and FortiGate DHCP server or relay will be used to assign VIP addresses to FortiClient dialup clients. The DHCP server or relay parameters must be configured separately.

If the FortiGate unit acts as a dialup server and the FortiClient dialup client VIP addresses match the network behind the dialup server, select Enable to cause the FortiGate unit to act as a proxy for the dialup clients.

This is available only for phase 2 configurations associated with a dialup phase 1 configuration. It works only on policy-based VPNs.

Quick Mode Selector

Optionally specify the source and destination IP addresses to be used as selectors for IKE negotiations. If the FortiGate unit is a dialup server, the default value 0.0.0.0/0 should be kept unless you need to circumvent problems caused by ambiguous IP addresses between one or more of the private networks making up the VPN. You can specify a single host IP address, an IP address range, or a network address. You may optionally specify source and destination port numbers and/or a protocol number.

If you are editing an existing phase 2 configuration, the Source address and Destination address fields are unavailable if the tunnel has been configured to use firewall addresses as selectors. This option exists only in the CLI. See the `dst-addr-type`, `dst-name`, `src-addr-type` and `src-name` keywords for the `vpn ipsec phase2` command in the *FortiGate CLI Reference*.

Source address

If the FortiGate unit is a dialup server, type the source IP address that corresponds to the local sender(s) or network behind the local VPN peer (for example, `172.16.5.0/24` or `172.16.5.0/255.255.255.0` for a subnet, or `172.16.5.1/32` or `172.16.5.1/255.255.255.255` for a server or host, or `192.168.10.[80-100]` or `192.168.10.80-192.168.10.100` for an address range). A value of `0.0.0.0/0` means all IP addresses behind the local VPN peer.

If the FortiGate unit is a dialup client, source address must refer to the private network behind the FortiGate dialup client.

Source port

Type the port number that the local VPN peer uses to transport traffic related to the specified service (protocol number). The range is 0 to 65535. To specify all ports, type `0`.

Destination address

Type the destination IP address that corresponds to the recipient(s) or network behind the remote VPN peer (for example, `192.168.20.0/24` for a subnet, or `172.16.5.1/32` for a server or host, or `192.168.10.[80-100]` for an address range). A value of `0.0.0.0/0` means all IP addresses behind the remote VPN peer.

Destination port

Type the port number that the remote VPN peer uses to transport traffic related to the specified service (protocol number). The range is 0 to 65535. To specify all ports, type `0`.

Protocol

Type the IP protocol number of the service. The range is `1` to `255`. To specify all services, type `0`.

6 Select OK.

Defining firewall policies

This section explains how to specify the source and destination IP addresses of traffic transmitted through an IPSec VPN, and how to define appropriate firewall policies.

The following topics are included in this section:

- Defining firewall addresses
- Defining firewall policies

Defining firewall addresses

A VPN tunnel has two end points. These end points may be VPN peers such as two FortiGate gateways. Encrypted packets are transmitted between the end points. At each end of the VPN tunnel, a VPN peer intercepts encrypted packets, decrypts the packets, and forwards the decrypted IP packets to the intended destination.

You need to define firewall addresses for the private networks behind each peer. You will use these addresses as the source or destination address depending on the firewall policy.

In general:

- In a gateway-to-gateway, hub-and-spoke, dynamic DNS, redundant-tunnel, or transparent configuration, you need to define a firewall address for the private IP address of the network behind the remote VPN peer (for example, `192.168.10.0/255.255.255.0` or `192.168.10.0/24`).
- In a peer-to-peer configuration, you need to define a firewall address for the private IP address of a server or host behind the remote VPN peer (for example, `172.16.5.1/255.255.255.255` or `172.16.5.1/32` or `172.16.5.1`).
- For a FortiGate dialup server in a dialup-client or Internet-browsing configuration:
  - If you are not using VIP addresses, or if the FortiGate dialup server assigns VIP addresses to FortiClient dialup clients through FortiGate DHCP relay, select the predefined destination address “all” in the firewall policy to refer to the dialup clients.
  - If you assign VIP addresses to FortiClient dialup clients manually, you need to define a firewall address for the VIP address assigned to the dialup client (for example, `10.254.254.1/32`), or a subnet address from which the VIP addresses are assigned (for example, `10.254.254.0/24` or `10.254.254.0/255.255.255.0`).
- For a FortiGate dialup client in a dialup-client or Internet-browsing configuration, you need to define a firewall address for the private IP address of a host, server, or network behind the FortiGate dialup server.

To define an IP address

1 Go to **Firewall > Address** and select Create New.

2 In the Address Name field, type a descriptive name that represents the network, server(s), or host(s).

3 In the Subnet/IP Range field, type the corresponding IP address and subnet mask (for example, `172.16.5.0/24` or `172.16.5.0/255.255.255.0` for a subnet, or `172.16.5.1/32` for a server or host) or IP address range (for example, `192.168.10.[80-100]` or `192.168.10.80-192.168.10.100`).

4 Select OK.

Defining firewall policies

Firewall policies allow IP traffic to pass between interfaces on a FortiGate unit. You can limit communication to particular traffic by specifying source address and destination addresses.

Policy-based and route-based VPNs require different firewall policies.

- A policy-based VPN requires an IPSec firewall policy. You specify the interface to the private network, the interface to the remote peer and the VPN tunnel. A single policy can enable traffic inbound, outbound, or in both directions.
- A route-based VPN requires an Accept firewall policy for each direction. As source and destination interfaces, you specify the interface to the private network and the virtual IPSec interface (phase 1 configuration) of the VPN. The IPSec interface is the destination interface for the outbound policy and the source interface for the inbound policy.

There are examples of firewall policies for both policy-based and route-based VPNs throughout this guide.

Defining an IPSec firewall policy for a policy-based VPN

An IPSec firewall policy enables the transmission and reception of encrypted packets, specifies the permitted direction of VPN traffic, and selects the VPN tunnel. In most cases, a single policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

In addition to these operations, firewall policies specify which IP addresses can initiate a tunnel. Traffic from computers on the local private network initiates the tunnel when the Allow outbound option is selected. Traffic from a dialup client or computers on the remote network initiates the tunnel when the Allow inbound option is selected.

When a FortiGate unit runs in NAT/Route mode, you can also enable inbound or outbound NAT. Outbound NAT may be performed on outbound encrypted packets, or on IP packets before they are sent through the tunnel. Inbound NAT is performed on IP packets emerging from the tunnel. These options are not selected by default in firewall policies.

When used in conjunction with the `natip` CLI attribute (see the “config firewall” chapter of the *FortiGate CLI Reference*), outbound NAT enables you to change the source addresses of IP packets before they go into the tunnel. This feature is often used to resolve ambiguous routing when two or more of the private networks making up a VPN have the same or overlapping IP addresses. For examples of how to use these two features together, see the *FortiGate Outbound NAT for IPSec VIP Technical Note* and the *FortiGate IPSec VPN Subnet-address Translation Technical Note*.

When inbound NAT is enabled, inbound encrypted packets are intercepted and decrypted, and the source IP addresses of the decrypted packets are translated into the IP address of the FortiGate interface to the local private network before they are routed to the private network. If the computers on the local private network can communicate only with devices on the local private network (that is, the FortiGate interface to the private network is not the default gateway) and the remote client (or remote private network) does not have an IP address in the same network address space as the local private network, enable inbound NAT.

Most firewall policies control outbound IP traffic. An outbound policy usually has a source address originating on the private network behind the local FortiGate unit, and a destination address belonging to a dialup VPN client or a network behind the remote VPN peer. The source address that you choose for the firewall policy identifies from where outbound cleartext IP packets may originate, and also defines the local IP address or addresses that a remote server or client will be allowed to access through the VPN tunnel. The destination address that you choose for the firewall policy identifies where IP packets must be forwarded after they are decrypted at the far end of the tunnel, and determines the IP address or addresses that the local network will be able to access at the far end of the tunnel.

You can fine-tune a policy for services such as HTTP, FTP, and POP3; enable logging, traffic shaping, antivirus protection, web filtering, email filtering, file transfer, and email services throughout the VPN; and optionally allow connections according to a predefined schedule. For more information, see the “Firewall Policy” chapter of the *FortiGate Administration Guide*.

Note: As an option, differentiated services can be enabled in the firewall policy through CLI commands. For more information, see the “firewall” chapter of the *FortiGate CLI Reference*.

When a remote server or client attempts to connect to the private network behind a FortiGate gateway, the firewall policy intercepts the connection attempt and starts the VPN tunnel. The FortiGate unit uses the remote gateway specified in its phase 1 tunnel configuration to reply to the remote peer. When the remote peer receives a reply, it checks its own firewall policy, including the tunnel configuration, to determine which communications are permitted. As long as one or more services are allowed through the VPN tunnel, the two peers begin to negotiate the tunnel.

Before you begin

Before you define the IPSec policy, you must:

- Define the IP source and destination addresses. See “Defining firewall addresses” on page 149.
- Specify the phase 1 authentication parameters. See “Auto Key phase 1 parameters” on page 127.
- Specify the phase 2 parameters. See “Phase 2 parameters” on page 143.

To define an IPSec firewall policy

1 Go to **Firewall > Policy** and select Create New.

2 Include appropriate entries as follows:

Source Interface/Zone	Select the local interface to the internal (private) network.
Source Address Name	Select the name that corresponds to the local network, server(s), or host(s) from which IP packets may originate.
Destination Interface/Zone	Select the local interface to the external (public) network.
Destination Address Name	Select the name that corresponds to the remote network, server(s), or host(s) to which IP packets may be delivered.
Schedule	Keep the default setting (always) unless changes are needed to meet specific requirements.
Service	Keep the default setting (ANY) unless changes are needed to meet your specific requirements.
Action	Select IPSEC.
VPN Tunnel	Select the name of the phase 1 tunnel configuration to which this policy will apply.
Allow Inbound	Select if traffic from the remote network will be allowed to initiate the tunnel.
Allow Outbound	Select if traffic from the local network will be allowed to initiate the tunnel.
Inbound NAT	Select if you want to translate the source IP addresses of inbound decrypted packets into the IP address of the FortiGate interface to the local private network.
Outbound NAT	Select in combination with a `natip` CLI value to translate the source addresses of outbound cleartext packets into the IP address that you specify. Do not select Outbound NAT unless you specify a `natip` value through the CLI. When a `natip` value is specified, the source addresses of outbound IP packets are replaced before the packets are sent through the tunnel. For more information, see the “firewall” chapter of the *FortiGate CLI Reference*.

3 You may enable a protection profile, and/or event logging, or select advanced settings to authenticate a user group, or shape traffic. For more information, see the “Firewall Policy” chapter of the *FortiGate Administration Guide*.

4 Select OK.

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

Defining multiple IPSec policies for the same tunnel

You must define at least one IPSec policy for each VPN tunnel. If the same remote server or client requires access to more than one network behind a local FortiGate unit, the FortiGate unit must be configured with an IPSec policy for each network. Multiple policies may be required to configure redundant connections to a remote destination or control access to different services at different times.

To ensure a secure connection, the FortiGate unit must evaluate IPSEC policies before ACCEPT and DENY firewall policies. Because the FortiGate unit reads policies starting at the top of the list, you must move all IPSec policies to the top of the list. When you define multiple IPSec policies for the same tunnel, you must reorder the IPSec policies that apply to the tunnel so that specific constraints can be evaluated before general constraints.

Note: Adding multiple IPSec policies for the same VPN tunnel can cause conflicts if the policies specify similar source and destination addresses but have different settings for the same service. When policies overlap in this manner, the system may apply the wrong IPSec policy or the tunnel may fail.

For example, if you create two equivalent IPSec policies for two different tunnels, it does not matter which one comes first in the list of IPSec policies—the system will select the correct policy based on the specified source and destination addresses. If you create two different IPSec policies for the same tunnel (that is, the two policies treat traffic differently depending on the nature of the connection request), you might have to reorder the IPSec policies to ensure that the system selects the correct IPSec policy. Reordering is especially important when the source and destination addresses in both policies are similar (for example, if one policy specifies a subset of the IP addresses in another policy). In this case, place the IPSec policy having the most specific constraints at the top of the list so that it can be evaluated first.

Defining firewall policies for a route-based VPN

When you define a route-based VPN, you create a virtual IPSec interface on the physical interface that connects to the remote peer. You create ordinary Accept firewall policies to enable traffic between the IPSec interface and the interface that connects to the private network. This makes configuration simpler than for policy-based VPNs, which require IPSec firewall policies.

To define firewall policies for a route-based VPN

Define an ACCEPT firewall policy to permit communications between the local private network and the private network behind the remote peer. Enter these settings in particular:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select the address name that you defined for the private network behind this FortiGate unit.
Destination Interface/Zone	Select the IPSec Interface you configured.
Destination Address Name	Select the address name that you defined for the private network behind the remote peer.
Action	Select ACCEPT.
NAT	Disable.

To permit the remote client to initiate communication, you need to define a firewall policy for communication in that direction. Enter these settings in particular:

Source Interface/Zone	Select the IPSec Interface you configured.
Source Address Name	Select the address name that you defined for the private network behind the remote peer.
Destination Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.

Destination Address Name	Select the address name that you defined for the private network behind this FortiGate unit.
Action	Select ACCEPT.
NAT	Disable.

Monitoring and testing VPNs

This section provides some general maintenance and monitoring procedures for VPNs.

The following topics are included in this section:

- Monitoring VPN connections
- Monitoring IKE sessions
- Testing VPN connections
- Logging VPN events
- VPN troubleshooting tips

Monitoring VPN connections

You can use the monitor to view activity on IPSec VPN tunnels and start or stop those tunnels. The display provides a list of addresses, proxy IDs, and timeout information for all active tunnels.

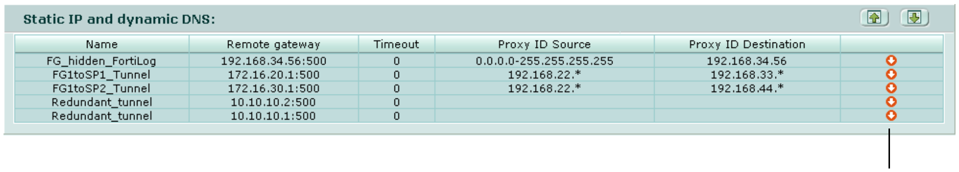
Monitoring connections to remote peers

The list of tunnels provides information about VPN connections to remote peers that have static IP addresses or domain names. You can use this list to view status and IP addressing information for each tunnel configuration. You can also start and stop individual tunnels from the list.

To view the list of static-IP and dynamic-DNS tunnels

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

Figure 29: List of static-IP and dynamic-DNS tunnels



Static IP and dynamic DNS:

Name	Remote gateway	Timeout	Proxy ID Source	Proxy ID Destination	
FG_hidden_FortiLog	192.168.34.56:500	0	0.0.0.0-255.255.255.255	192.168.34.56	⬇
FG1toSP1_Tunnel	172.16.20.1:500	0	192.168.22.*	192.168.33.*	⬇
FG1toSP2_Tunnel	172.16.30.1:500	0	192.168.22.*	192.168.44.*	⬇
Redundant_tunnel	10.10.10.2:500	0			⬇
Redundant_tunnel	10.10.10.1:500	0			⬇

Bring up tunnel

To establish or take down a VPN tunnel

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

2 In the list of tunnels, select the Bring down tunnel or Bring up tunnel button in the row that corresponds to the tunnel that you want to bring down or up.

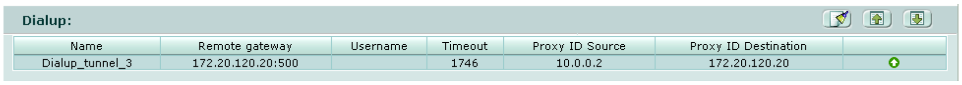
Monitoring dialup IPSec connections

The list of dialup tunnels provides information about the status of tunnels that have been established for dialup clients. The list displays the IP addresses of dialup clients and the names of all active tunnels. The number of tunnels shown in the list can change as dialup clients connect and disconnect.

To view the list of dialup tunnels

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

Figure 30: List of dialup tunnels



Dialup:

Name	Remote gateway	Username	Timeout	Proxy ID Source	Proxy ID Destination	
Dialup_tunnel_3	172.20.120.20:500		1746	10.0.0.2	172.20.120.20	●

Note: If you take down an active tunnel while a dialup client such as FortiClient is still connected, FortiClient will continue to show the tunnel connected and idle. The dialup client must disconnect before another tunnel can be initiated.

The list of dialup tunnels displays the following statistics:

- The Name column displays the name of the tunnel.
- The meaning of the value in the Remote gateway column changes, depending on the configuration of the network at the far end:
  - When a FortiClient dialup client establishes a tunnel, the Remote gateway column displays either the public IP address and UDP port of the remote host device (on which the FortiClient Host Security application is installed), or if a NAT device exists in front of the remote host, the Remote gateway column displays the public IP address and UDP port of the remote host.
  - When a FortiGate dialup client establishes a tunnel, the Remote gateway column displays the public IP address and UDP port of the FortiGate dialup client.
- The Username column displays the peer ID, certificate name, or XAuth user name of the dialup client (if a peer ID, certificate name, or XAuth user name was assigned to the dialup client for authentication purposes).
- The Timeout column displays the time before the next key exchange. The time is calculated by subtracting the time elapsed since the last key exchange from the keylife.
- The Proxy ID Source column displays the IP addresses of the hosts, servers, or private networks behind the FortiGate unit. A network range may be displayed if the source address in the firewall encryption policy was expressed as a range of IP addresses.
- The meaning of the value in the Proxy ID Destination column changes, depending on the configuration of the network at the far end:
  - When a FortiClient dialup client establishes a tunnel:

    If VIP addresses are not used and the remote host connects to the Internet directly, the Proxy ID Destination field displays the public IP address of the Network Interface Card (NIC) in the remote host.

    If VIP addresses are not used and the remote host is behind a NAT device, the Proxy ID Destination field displays the private IP address of the NIC in the remote host.

If VIP addresses were configured (manually or through FortiGate DHCP relay), the Proxy ID Destination field displays either the VIP address belonging to a FortiClient dialup client, or a subnet address from which VIP addresses were assigned.

- When a FortiGate dialup client establishes a tunnel, the Proxy ID Destination field displays the IP address of the remote private network.

Monitoring IKE sessions

You can display a list of all active sessions and view activity by port number. By default, the following ports are used for IPSec VPN-related communications:

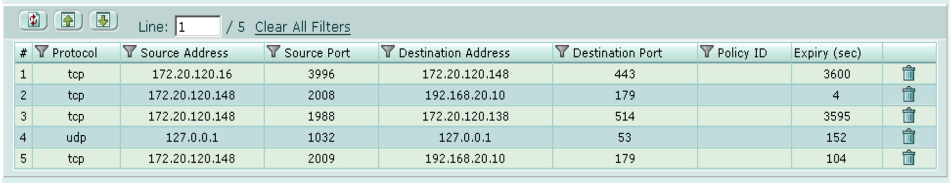
- port numbers 500 and 4500 for IPSec IKE activity
- port number 4500 for NAT traversal activity

If required, active sessions can be stopped from this view. For more information, see the “System Status” chapter of the *FortiGate Administration Guide*.

To view the list of active sessions

1. Go to **System > Status**.
2. In the Statistics section, select Details on the Sessions line.

Figure 31: Session list



Line: 1 / 5 Clear All Filters

#	Protocol	Source Address	Source Port	Destination Address	Destination Port	Policy ID	Expiry (sec)	
1	tcp	172.20.120.16	3996	172.20.120.148	443		3600	🗑
2	tcp	172.20.120.148	2008	192.168.20.10	179		4	🗑
3	tcp	172.20.120.148	1988	172.20.120.138	514		3595	🗑
4	udp	127.0.0.1	1032	127.0.0.1	53		152	🗑
5	tcp	172.20.120.148	2009	192.168.20.10	179		104	🗑

Testing VPN connections

To confirm whether a VPN has been configured correctly, issue a ping command on the network behind the FortiGate unit to test the connection to a computer on the remote network. A VPN tunnel will be established automatically when the first data packet destined for the remote network is intercepted by the FortiGate unit.

To confirm that a VPN between a local network and a dialup client has been configured correctly, at the dialup client, issue a ping command to test the connection to the local network. The VPN tunnel initializes when the dialup client attempts to connect.

Logging VPN events

You can configure the FortiGate unit to log VPN events. For IPSec VPNs, phase 1 and phase 2 authentication and encryption events are logged. For information about how to interpret log messages, see the *FortiGate Log Message Reference*.

To log VPN events

1. Go to **Log&Report > Log Config > Log Setting**.
2. Enable the storage of log messages to one or more of the following locations:
   - a FortiLog unit
   - the FortiGate system memory
   - a remote computer running a syslog server

Note: If available on your FortiGate unit, you can enable the storage of log messages to a system hard disk. In addition, as an alternative to the options listed above, you may choose to forward log messages to a remote computer running a WebTrends firewall reporting server. For more information about enabling either of these options through CLI commands, see the “log” chapter of the *FortiGate CLI Reference*.

3. If the options are concealed, select the blue arrow beside each option to reveal and configure associated settings.
4. If logs will be written to system memory, from the Log Level list, select Information. For more information, see the “Log&Report” chapter of the *FortiGate Administration Guide*.
5. Select Apply.

To filter VPN events

1. Go to **Log&Report > Log Config > Event Log**.
2. Verify that the IPSec negotiation event option is selected.
3. Select Apply.

To view event logs

1. Go to **Log&Report > Log Access > Event**.
2. If the option is available from the Type list, select the log file from disk or memory.

   Entries similar to the following indicate that a tunnel has been established.

```
2005-03-31 15:38:29 log_id=0101023004 type=event subtype=ipsec pri=notice vd=root
loc_ip=172.16.62.10 loc_port=500 rem_ip=172.16.62.11 rem_port=500 out_if=port2
vpn_tunnel=asdf cookies=151c3a5c6dd93c54/0000000000000000 action=negotiate init=local
mode=main stage=1 dir=outbound status=success msg="Initiator: sent 172.16.62.11 main
mode message #1 (OK)"
2005-03-31 15:38:29 log_id=0101023004 type=event subtype=ipsec pri=notice vd=root
loc_ip=172.16.62.10 loc_port=500 rem_ip=172.16.62.11 rem_port=500 out_if=port2
vpn_tunnel=asdf cookies=151c3a5c6dd93c54/5ed26a81fb7a2d0c action=negotiate init=local
mode=main stage=2 dir=outbound status=success msg="Initiator: sent 172.16.62.11 main
mode message #2 (OK)"
2005-03-31 15:38:29 log_id=0101023004 type=event subtype=ipsec pri=notice vd=root
loc_ip=172.16.62.10 loc_port=500 rem_ip=172.16.62.11 rem_port=500 out_if=port2
vpn_tunnel=asdf cookies=151c3a5c6dd93c54/5ed26a81fb7a2d0c action=negotiate init=local
mode=main stage=3 dir=outbound status=success msg="Initiator: sent 172.16.62.11 main
mode message #3 (OK)"
2005-03-31 15:38:29 log_id=0101023004 type=event subtype=ipsec pri=notice vd=root
loc_ip=172.16.62.10 loc_port=500 rem_ip=172.16.62.11 rem_port=500 out_if=port2
vpn_tunnel=asdf cookies=151c3a5c6dd93c54/5ed26a81fb7a2d0c action=negotiate init=local
mode=main stage=3 dir=inbound status=success msg="Initiator: parsed 172.16.62.11 main
mode message #3 (DONE)"
```

```
2005-03-31 15:38:29 log_id=0101023004 type=event subtype=ipsec pri=notice vd=root
loc_ip=172.16.62.10 loc_port=500 rem_ip=172.16.62.11 rem_port=500 out_if=port2
vpn_tunnel=asdf cookies=151c3a5c6dd93c54/5ed26a81fb7a2d0c action=negotiate init=local
mode=quick stage=1 dir=outbound status=success msg="Initiator: sent 172.16.62.11 quick
mode message #1 (OK)"
2005-03-31 15:38:29 log_id=0101023006 type=event subtype=ipsec pri=notice vd=root
loc_ip=172.16.62.10 loc_port=500 rem_ip=172.16.62.11 rem_port=500 out_if=port2
vpn_tunnel=asdf cookies=151c3a5c6dd93c54/5ed26a81fb7a2d0c action=install_sa
in_spi=66867f2b out_spi=e22de275 msg="Initiator: tunnel 172.16.62.10/172.16.62.11
install ipsec sa"
2005-03-31 15:38:29 log_id=0101023004 type=event subtype=ipsec pri=notice vd=root
loc_ip=172.16.62.10 loc_port=500 rem_ip=172.16.62.11 rem_port=500 out_if=port2
vpn_tunnel=asdf cookies=151c3a5c6dd93c54/5ed26a81fb7a2d0c action=negotiate init=local
mode=quick stage=2 dir=outbound status=success msg="Initiator: sent 172.16.62.11 quick
mode message #2 (DONE)"
2005-03-31 15:38:29 log_id=0101023002 type=event subtype=ipsec pri=notice vd=root
loc_ip=172.16.62.10 loc_port=500 rem_ip=172.16.62.11 rem_port=500 out_if=port2
vpn_tunnel=asdf cookies=151c3a5c6dd93c54/5ed26a81fb7a2d0c action=negotiate
status=success msg="Initiator: tunnel 172.16.62.11, transform=ESP_3DES, HMAC_SHA1"
```

Entries similar to the following indicate that phase 1 negotiations broke down because the preshared keys belonging to the VPN peers were not identical. A tunnel was not established.

```
2005-03-31 16:06:39 log_id=0101023003 type=event subtype=ipsec pri=error vd=root
loc_ip=192.168.70.2 loc_port=500 rem_ip=192.168.80.2 rem_port=500 out_if=port2
vpn_tunnel=s cookies=3896343ae575f210/0a7ba199149e31e9 action=negotiate
status=negotiate_error msg="Negotiate SA Error: probable pre-shared secret mismatch"
```

For more information about how to interpret error log messages, see the *FortiGate Log Message Reference*.

VPN troubleshooting tips

Most connection failures are due to a configuration mismatch between the FortiGate unit and the remote peer. In general, begin troubleshooting an IPSec VPN connection failure as follows:

1. Ping the remote network or client to verify whether the connection is up. See “Testing VPN connections” on page 157.
2. Verify the configuration of the FortiGate unit and the remote peer. Check the following IPSec parameters:
   - The mode setting for ID protection (main or aggressive) on both VPN peers must be identical.
   - The authentication method (preshared keys or certificates) used by the client must be supported on the FortiGate unit and configured properly.
   - If preshared keys are being used for authentication purposes, both VPN peers must have identical preshared keys.
   - The remote client must have at least one set of phase 1 encryption, authentication, and Diffie-Hellman settings that match corresponding settings on the FortiGate unit.
   - Both VPN peers must have the same NAT traversal setting (enabled or disabled).
   - The remote client must have at least one set of phase 2 encryption and authentication algorithm settings that match the corresponding settings on the FortiGate unit.
   - If you are using manual keys to establish a tunnel, the Remote SPI setting on the FortiGate unit must be identical to the Local SPI setting on the remote peer, and vise versa.

3 Refer to Table 2 on page 160 to correct the problem.

Table 2: VPN trouble-shooting tips

Configuration problem	Correction
Mode settings do not match.	Select complementary mode settings. See "Choosing main mode or aggressive mode" on page 128.
Peer ID or certificate name of the remote peer or dialup client is not recognized by FortiGate VPN server.	Go to **VPN > Phase 1**. Depending on the Remote Gateway and Authentication Method settings, you have a choice of options to authenticate FortiGate dialup clients or VPN peers by ID or certificate name (see "Authenticating remote peers and clients" on page 131). If you are configuring authentication parameters for FortiClient dialup clients, refer to the *Authenticating FortiClient Dialup Clients Technical Note*.
Preshared keys do not match.	Reenter the preshared key. See "Authenticating remote peers and clients" on page 131.
Phase 1 or phase 2 key exchange proposals are mismatched.	Make sure that both VPN peers have at least one set of proposals in common for each phase. See "Defining IKE negotiation parameters" on page 137 and "Configure the phase 2 parameters" on page 146.
NAT traversal settings are mismatched.	Select or clear both options as required. See "NAT traversal" on page 140 and "NAT keepalive frequency" on page 140.
SPI settings for manual key tunnels are mismatched.	Enter complementary SPI settings. See "Manual-key configurations" on page 111.

A word about NAT devices

When a device with NAT capabilities is located between two VPN peers or a VPN peer and a dialup client, the device must be NAT-T compatible for encrypted traffic to pass through the NAT device. For more information, see "NAT traversal" on page 140.

Index

www.fortinet.com

FORTINET™

www.fortinet.com