FortiOS™ Handbook

IPsec VPN for FortiOS 5.0

IPsec VPN for FortiOS 5.0

19 February 2014

01-504-112804-20140219

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of contents

Chapter 1 IPsec VPN for FortiOS 5.0

This FortiOS Handbook chapter contains the following sections:

IPsec VPN concepts explains the basic concepts that you need to understand about virtual private networks (VPNs).

IPsec VPN Overview provides a brief overview of IPsec technology and includes general information about how to configure IPsec VPNs using this guide.

IPsec VPN in the web-based manager describes the IPsec VPN menu of the web-based manager interface.

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 configuration 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 dynamic IP address and a domain name.

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 Endpoint 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 with a dynamic IP address initiates a VPN tunnel with the FortiGate dialup server.

Supporting IKE Mode config clients explains how to set up a FortiGate unit as either an IKE Mode Config server or client. IKE Mode Config is an alternative to DHCP over IPsec.

Internet-browsing configuration explains how to support secure web browsing performed by dialup VPN clients, and 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 security 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 two FortiGate units that create a VPN tunnel between two separate private networks transparently. In transparent mode, all FortiGate unit interfaces 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 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. IPv6 IPsec VPNs are available in FortiOS 3.0 MR5 and later.

L2TP and IPsec (Microsoft VPN) explains how to support Microsoft Windows native VPN clients.

GRE over IPsec (Cisco VPN) explains how to interoperate with Cisco VPNs that use Generic Routing Encapsulation (GRE) protocol with IPsec.

Protecting OSPF with IPsec provides an example of protecting OSPF links with IPsec.

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 methods such as extended authentication (XAuth).

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 VPN security policies explains how to specify the source and destination IP addresses of traffic transmitted through an IPsec VPN tunnel, and how to define a security encryption policy. Security policies control all IP traffic passing between a source address and a destination address.

Hardware offloading and acceleration explains how to make use of FortiASIC network processor IPsec accelerated processing capabilities.

Monitoring and troubleshooting provides VPN monitoring and testing procedures

IPsec VPN concepts

Virtual Private Network (VPN) technology enables remote users to connect to private computer networks to gain access to their resources in a secure way. For example, an employee traveling or working from home can use a VPN to securely access the office network through the Internet.

Instead of remotely logging on to a private network using an unencrypted and unsecure Internet connection, the use of a VPN ensures that unauthorized parties cannot access the office network and cannot intercept any of the information that is exchanged between the employee and the office. It is also common to use a VPN to connect the private networks of two or more offices.

Fortinet offers VPN capabilities in the FortiGate Unified Threat Management (UTM) appliance and in the FortiClient Endpoint Security suite of applications. A FortiGate unit can be installed on a private network, and FortiClient software can be installed on the user's computer. It is also possible to use a FortiGate unit to connect to the private network instead of using FortiClient software.

This chapter discusses VPN terms and concepts including:

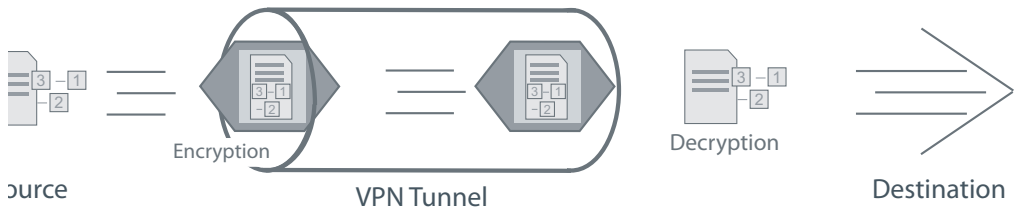
- VPN tunnels
- VPN gateways
- Clients, servers, and peers
- Encryption
- Authentication
- Phase 1 and Phase 2 settings
- Security Association

VPN tunnels

The data path between a user's computer and a private network through a VPN is referred to as a tunnel. Like a physical tunnel, the data path is accessible only at both ends. In the telecommuting scenario, the tunnel runs between the FortiClient application on the user's PC, or a FortiGate unit or other network device and the FortiGate unit on the office private network.

Encapsulation makes this possible. IPsec packets pass from one end of the tunnel to the other and contain data packets that are exchanged between the local user and the remote private network. Encryption of the data packets ensures that any third-party who intercepts the IPsec packets can not access the data.

Figure 1: Encoded data going through a VPN tunnel



You can create a VPN tunnel between:

- a PC equipped with the FortiClient application and a FortiGate unit
- two FortiGate units
- third-party VPN software and a FortiGate unit

Third-party VPN software is not covered in this document. Refer to the Fortinet Knowledge Base for more information on this topic.

VPN gateways

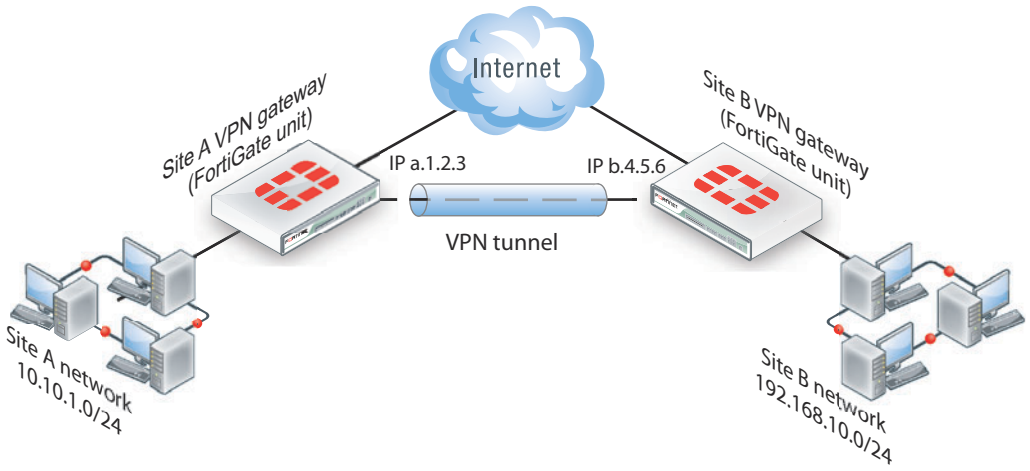
A gateway is a router that connects the local network to other networks. The default gateway setting in your computer's TCP/IP properties specifies the gateway for your local network.

A VPN gateway functions as one end of a VPN tunnel. It receives incoming IPsec packets, decrypts the encapsulated data packets and passes the data packets to the local network. Also, it encrypts data packets destined for the other end of the VPN tunnel, encapsulates them, and sends the IPsec packets to the other VPN gateway. The VPN gateway is a FortiGate unit because the private network behind it is protected, ensuring the security of the unencrypted VPN data. The gateway can also be FortiClient software running on a PC since the unencrypted data is secure on the PC.

The IP address of a VPN gateway is usually the IP address of the network interface that connects to the Internet. Optionally, you can define a secondary IP address for the interface and use that address as the local VPN gateway address. The benefit of doing this is that your existing setup is not affected by the VPN settings.

The following diagram shows a VPN connection between two private networks with FortiGate units acting as the VPN gateways. This configuration is commonly referred to as Gateway-to-Gateway IPsec VPN.

Figure 2: VPN tunnel between two private networks



Although the IPsec traffic may actually pass through many Internet routers, you can visualize the VPN tunnel as a simple secure connection between the two FortiGate units.

Users on the two private networks do not need to be aware of the VPN tunnel. The applications on their computers generate packets with the appropriate source and destination addresses, as they normally do. The FortiGate units manage all the details of encrypting, encapsulating and sending the packets to the remote VPN gateway.

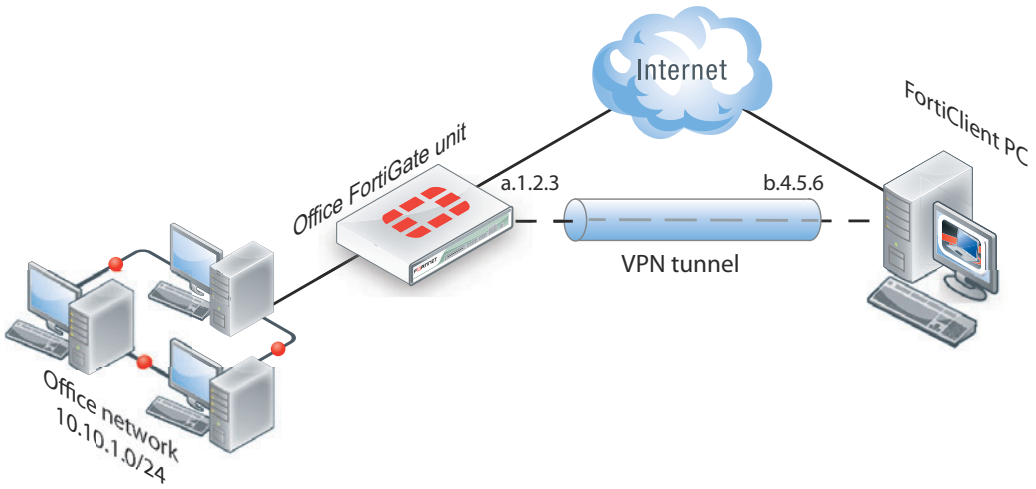
The data is encapsulated in IPsec packets only in the VPN tunnel between the two VPN gateways. Between the user's computer and the gateway, the data is on the secure private network and it is in regular IP packets.

For example User1 on the Site A network, at IP address 10.10.1.7, sends packets with destination IP address 192.168.10.8, the address of User2 on the Site B network. The Site A FortiGate unit is configured to send packets with destinations on the 192.168.10.0 network through the VPN, encrypted and encapsulated. Similarly, the Site B FortiGate unit is configured to send packets with destinations on the 10.10.1.0 network through the VPN tunnel to the Site A VPN gateway.

In the site-to-site, or gateway-to-gateway VPN shown in Figure 2, the FortiGate units have static (fixed) IP addresses and either unit can initiate communication.

You can also create a VPN tunnel between an individual PC running FortiClient and a FortiGate unit, as shown below. This is commonly referred to as Client-to-Gateway IPsec VPN.

Figure 3: VPN tunnel between a FortiClient PC and a FortiGate unit



On the PC, the FortiClient application acts as the local VPN gateway. Packets destined for the office network are encrypted, encapsulated into IPsec packets, and sent through the VPN tunnel to the FortiGate unit. Packets for other destinations are routed to the Internet as usual. IPsec packets arriving through the tunnel are decrypted to recover the original IP packets.

Clients, servers, and peers

A FortiGate unit in a VPN can have one of the following roles:

- ***server*** — responds to a request to establish a VPN tunnel.
- ***client*** — contacts a remote VPN gateway and requests a VPN tunnel.
- ***peer*** — brings up a VPN tunnel or responds to a request to do so.

The site-to-site VPN shown in Figure 2 is a peer-to-peer relationship. Either FortiGate unit VPN gateway can establish the tunnel and initiate communications. The FortiClient-to-FortiGate VPN shown in Figure 3 is a client-server relationship. The FortiGate unit establishes a tunnel when the FortiClient PC requests one.

A FortiGate unit cannot be a VPN server if it has a dynamically-assigned IP address. VPN clients need to be configured with a static IP address for the server. A FortiGate unit acts as a server only when the remote VPN gateway has a dynamic IP address or is a client-only device or application, such as FortiClient.

As a VPN server, a FortiGate unit can also offer automatic configuration for FortiClient PCs. The user needs to know only the IP address of the FortiGate VPN server and a valid user name/password. FortiClient downloads the VPN configuration settings from the FortiGate VPN server. For information about configuring a FortiGate unit as a VPN server, see the *FortiClient Administration Guide*.

Encryption

Encryption mathematically transforms data to appear as meaningless random numbers. The original data is called plaintext and the encrypted data is called ciphertext. The opposite process, called decryption, performs the inverse operation to recover the original plaintext from the ciphertext.

The process by which the plaintext is transformed to ciphertext and back again is called an algorithm. All algorithms use a small piece of information, a key, in the arithmetic process of converted plaintext to ciphertext, or vice-versa. IPsec uses symmetrical algorithms, in which the same key is used to both encrypt and decrypt the data.

The security of an encryption algorithm is determined by the length of the key that it uses. FortiGate IPsec VPNs offer the following encryption algorithms, in descending order of security:

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

The default encryption algorithms provided on FortiGate units make recovery of encrypted data almost impossible without the proper encryption keys

There is a human factor in the security of encryption. The key must be kept secret, known only to the sender and receiver of the messages. Also, the key must not be something that unauthorized parties might easily guess, such as the sender's name, birthday or simple sequence such as `123456`.

Authentication

In addition to protecting data through encryption, a VPN must ensure that only authorized users can access the private network. You must use either a preshared key on both VPN gateways or RSA X.509 security certificates. The examples in this guide use only preshared key authentication. Refer to the Fortinet Knowledge Base for articles on RSA X.509 security certificates.

Preshared keys

A preshared key contains at least six random alphanumeric characters. Users of the VPN must obtain the preshared key from the person who manages the VPN server and add the preshared key to their VPN client configuration.

Although it looks like a password, the preshared key, also known as a shared secret, is never sent by either gateway. The preshared key is used in the calculations at each end that generate

the encryption keys. As soon as the VPN peers attempt to exchange encrypted data, preshared keys that do not match will cause the process to fail.

Additional authentication

To increase security, you can require additional means of authentication from users:

- an identifier, called a peer ID or a local ID
- extended authentication (XAUTH) which imposes an additional user name/password requirement

A Local ID is an alphanumeric value assigned in the Phase 1 configuration. The Local ID of a peer is called a Peer ID.

Phase 1 and Phase 2 settings

A VPN tunnel is established in two phases: Phase 1 and Phase 2. Several parameters determine how this is done. Except for IP addresses, the settings simply need to match at both VPN gateways. There are defaults that are appropriate for most cases.

FortiClient distinguishes between Phase 1 and Phase 2 only in the VPN Advanced settings and uses different terms. Phase 1 is called the IKE Policy. Phase 2 is called the IPsec Policy.

Phase 1

In Phase 1, the two VPN gateways exchange information about the encryption algorithms that they support and then establish a temporary secure connection to exchange authentication information.

When you configure your FortiGate unit or FortiClient application, you must specify the following settings for Phase 1:

Remote Gateway	The remote VPN gateway's address. FortiGate units also have the option of operating only as a server by selecting the "Dialup User" option.
Preshared key	This must be the same at both ends. It is used to encrypt phase 1 authentication information.
Local interface	The network interface that connects to the other VPN gateway. This applies on a FortiGate unit only.

All other Phase 1 settings have default values. These settings mainly configure the types of encryption to be used. The default settings on FortiGate units and in the FortiClient application are compatible. The examples in this guide use these defaults.

For more detailed information about Phase 1 settings, see the "Auto Key phase 1 parameters" on page 36.

Phase 2

Similar to the Phase 1 process, the two VPN gateways exchange information about the encryption algorithms that they support for Phase 2. You may choose different encryption for Phase 1 and Phase 2. If both gateways have at least one encryption algorithm in common, a VPN tunnel can be established. Keep in mind that more algorithms each phase does not share

with the other gateway, the longer negotiations will take. In extreme cases this may cause timeouts during negotiations.

To configure default Phase 2 settings on a FortiGate unit, you need only select the name of the corresponding Phase 1 configuration. In FortiClient, no action is required to enable default Phase 2 settings.

For more detailed information about Phase 2 settings, see “Phase 2 parameters” on page 52.

Security Association

The establishment of a Security Association (SA) is the successful outcome of Phase 1 negotiations. Each peer maintains a database of information about VPN connections. The information in each SA can include cryptographic algorithms and keys, keylife, and the current packet sequence number. This information is kept synchronized as the VPN operates. Each SA has a Security Parameter Index (SPI) that is provided to the remote peer at the time the SA is established. Subsequent IPsec packets from the peer always reference the relevant SPI. It is possible for peers to have multiple VPNs active simultaneously, and correspondingly multiple SPIs.

IPsec VPN Overview

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:

- Types of VPNs
- Planning your VPN
- General preparation steps
- How to use this guide to configure an IPsec VPN

VPN configurations interact with the firewall component of the FortiGate unit. There must be a security policy in place to permit traffic to pass between the private network and the VPN tunnel.

Security policies for VPNs specify:

- the FortiGate interface that provides the physical connection to the remote VPN gateway, usually an interface connected to the Internet
- the FortiGate interface that connects to the private network
- IP addresses associated with data that has to be encrypted and decrypted
- optionally, a schedule that restricts when the VPN can operate
- optionally, the services (types of data) that can be sent

When the first packet of data that meets all of the conditions of the security policy arrives at the FortiGate unit, a VPN tunnel may be initiated and the encryption or decryption of data is performed automatically afterward. For more information, see “Defining VPN security policies” on page 58.

Types of VPNs

FortiGate unit VPNs can be policy-based or route-based. There is little difference between the two types. In both cases, you specify phase 1 and phase 2 settings. However there is a difference in implementation. A route-based VPN creates a virtual IPsec network interface that applies encryption or decryption as needed to any traffic that it carries. That is why route-based VPNs are also known as interface-based VPNs. A policy-based VPN is implemented through a special security policy that applies the encryption you specified in the phase 1 and phase 2 settings.

Route-based VPNs

For a route-based VPN, you create two security policies between the virtual IPsec interface and the interface that connects to the private network. In one policy the virtual interface is the source. In the other policy the virtual interface is the destination. The Action for both policies is Accept. This creates bidirectional policies that ensure traffic will flow in both directions over the VPN.

Policy-based VPNs

For a policy-based VPN, one security policy enables communication in both directions. You must select IPSEC as the Action and then select the VPN tunnel you defined in the phase 1 settings. You can then enable inbound and outbound traffic as needed within that policy, or create multiple policies of this type to handle different types of traffic differently. For example HTTPS traffic may not require the same level of scanning as FTP traffic.

Comparing policy-based or route-based VPNs

For both VPN types you create phase 1 and phase 2 configurations. Both types are handled in the stateful inspection security layer, assuming there is no IPS or AV. For more information on the three security layers, see the FortiOS Troubleshooting guide.

The main difference is in the security policy.

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

You create a route-based VPN by enabling IPsec interface mode in the VPN phase 1 configuration. This creates a virtual IPsec interface. You then define a regular ACCEPT security policy to permit traffic to flow between the virtual IPsec interface and another network interface. And lastly, configure a static route to allow traffic over the VPN.

Where possible, you should create route-based VPNs. Generally, route-based VPNs are more flexible and easier to configure than policy-based VPNs — by default they are treated as interfaces. However, these two VPN types have different requirements that limit where they can be used.

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

Features	Policy-based	Route-based
• Both NAT and transparent modes available	• Yes	• NAT mode only
• L2TP-over-IPsec supported	• Yes	• No
• GRE-over-IPsec supported	• No	• Yes
• security policy requirements	• Requires a security policy with IPSEC action that specifies the VPN tunnel	• Requires only a simple security policy with ACCEPT action
• Number of policies per VPN	• One policy controls connections in both directions	• A separate policy is required for connections in each direction

Planning your VPN

It is a good idea to plan the VPN configuration ahead of time. This will save time later and be help you configure your VPN correctly.

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.

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.

Table 2: VPN network topologies and brief descriptions

Topology	Description
Gateway-to-gateway configurations	Standard one-to-one VPN between two FortiGate units. See "Gateway-to-gateway configurations" on page 64.
Hub-and-spoke configurations	One central FortiGate unit has multiple VPNs to other remote FortiGate units. See "Hub-and-spoke configurations" on page 78.
Dynamic DNS configuration	One end of the VPN tunnel has a changing IP address and the other end must go to a dynamic DNS server for the current IP address before establishing a tunnel. See "Dynamic DNS configuration" on page 94.
FortiClient dialup-client configurations	Typically remote FortiClient dialup-clients use dynamic IP addresses through NAT devices. The FortiGate unit acts as a dialup server allowing dialup VPN connections from multiple sources. See "FortiClient dialup-client configurations" on page 108.
FortiGate dialup-client configurations	Similar to FortiClient dialup-client configurations but with more gateway-to-gateway settings such as unique user authentication for multiple users on a single VPN tunnel. See "FortiGate dialup-client configurations" on page 123.
Internet-browsing configuration	Secure web browsing performed by dialup VPN clients, and/or hosts behind a remote VPN peer. See "Internet-browsing configuration" on page 136.
Redundant VPN configurations	Options for supporting redundant and partially redundant IPsec VPNs, using route-based approaches. See "Redundant VPN configurations" on page 140.
Transparent mode VPNs	In transparent mode, the FortiGate acts as a bridge with all incoming traffic being broadcast back out on all other interfaces. Routing and NAT must be performed on external routers. See "Transparent mode VPNs" on page 165.

Table 2: VPN network topologies and brief descriptions

Topology	Description
Manual-key configurations	Manually define cryptographic keys to establish an IPsec VPN, either policy-based or route-based. See "Manual-key configurations" on page 171.
L2TP and IPsec (Microsoft VPN)	Configure VPN for Microsoft Windows dialup clients using the built in L2TP software. Users do not have to install any See "L2TP and IPsec (Microsoft VPN)" on page 188.

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.

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.

- **The private IP addresses of 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.
- **The public IP addresses of the VPN end-point interfaces.** The VPN devices establish tunnels with each other through these interfaces.
- **The private IP addresses associated with the VPN-device interfaces to the private networks.** Computers on the private networks 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 36.
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 52.
3. Specify the source and destination addresses of IP packets that are to be transported through the VPN tunnel. See "Defining policy addresses" on page 58.

4. Create an IPsec security policy to define the scope of permitted services between the IP source and destination addresses. See “Defining VPN security policies” on page 59.

These steps assume you configure the FortiGate unit to generate unique IPsec encryption and authentication keys automatically. In situations where a remote VPN peer or client requires a specific IPsec encryption and 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 171.

IPsec VPN in the web-based manager

The IPsec VPN menu in FortiOS provides settings to configure an IPsec VPN. IPsec VPNs that are configured by using the general procedure below. With these steps, your FortiGate unit will automatically generate unique IPsec encryption and authentication keys. If a remote VPN peer or client requires a specific IPsec encryption or authentication key, you must configure your FortiGate unit to use manual keys instead. See “Manual Key” on page 32.

1. Define phase 1 parameters to authenticate remote peers and clients for a secure connection. See “Phase 1 configuration” on page 24.
2. Define phase 2 parameters to create a VPN tunnel with a remote peer or dialup client. See “Phase 2 configuration” on page 28.
3. Create a security policy to permit communication between your private network and the VPN. Policy-based VPNs have an action of IPSEC, where for interface-based VPNs the security policy action is ACCEPT. See “Defining VPN security policies” on page 58.

The FortiGate unit implements the Encapsulated Security Payload (ESP) protocol. Internet Key Exchange (IKE) is performed automatically based on pre-shared keys or X.509 digital certificates. As an option, you can specify manual keys. Interface mode, supported in NAT mode only, creates a virtual interface for the local end of a VPN tunnel.

This topic contains the following:

Auto Key (IKE)

You can configure VPN peers (or a FortiGate dialup server and a VPN client) to generate unique Internet Key Exchange (IKE) keys automatically during the IPsec phase 1 and phase 2 exchanges.

When you define phase 2 parameters, you can choose any set of phase 1 parameters to set up a secure connection for the tunnel and authenticate the remote peer. Auto Key configuration applies to both tunnel-mode and interface-mode VPNs.

To configure VPN peers go to *VPN* > *IPsec* > *Auto Key (IKE)*.

Create Phase 1	Creates a new phase 1 tunnel configuration. For more information, see “Phase 1 configuration” on page 24.
Create Phase 2	Creates a new phase 2 configuration. For more information, see “Phase 2 configuration” on page 28.
Create FortiClient VPN	Creates a new FortiClient VPN. For more information, see “FortiClient VPN” on page 31.

If you want to control how the IKE negotiation process controls traffic when there is no traffic, as well as the length of time the FortiGate unit waits for negotiations to occur, use the `negotiation-timeout` and `auto-negotiation` commands in the CLI.

Phase 1 configuration

The basic phase 1 settings associate IPsec phase 1 parameters with a remote gateway, if a pre-shared key or digital certificate will be used, and if a special identifier will be used to identify the remote VPN peer or client.

Name	Type a name for the phase 1 definition. The maximum name length is 15 characters for an interface mode VPN, 35 characters for a policy-based VPN. If *Remote Gateway* is *Dialup User*, the maximum name length is further reduced depending on the number of dialup tunnels that can be established: by 2 for up to 9 tunnels, by 3 for up to 99 tunnels, 4 for up to 999 tunnels, and so on. For a tunnel mode VPN, the name normally reflects where the remote connection originates. For a route-based tunnel, the FortiGate unit also uses the name for the virtual IPsec interface that it creates automatically.
Remote Gateway	Select the category of the remote connection: • *Static IP Address* — If the remote peer has a static IP address. • *Dialup User* — If one or more FortiClient or FortiGate dialup clients with dynamic IP addresses will connect to the FortiGate unit. • *Dynamic DNS* — If a remote peer that has a domain name and subscribes to a dynamic DNS service will connect to the FortiGate unit.
IP Address	If you selected *Static IP Address*, enter the IP address of the remote peer.
Dynamic DNS	If you selected *Dynamic DNS*, enter the domain name of the remote peer.
Local Interface	This option is available in NAT mode only. Select the name of the interface through which remote peers or dialup clients connect to the FortiGate unit. By default, the local VPN gateway IP address is the IP address of the interface that you selected. Optionally, you can specify a unique IP address for the VPN gateway in the *Advanced* settings.
Mode	• *Main mode* — the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • *Aggressive mode* — the phase 1 parameters are exchanged in single message with authentication information that is not encrypted. When the remote VPN peer has a dynamic IP address and is authenticated by a pre-shared key, you must select Aggressive mode if there is more than one dialup phase1 configuration for the interface IP address. When the remote VPN peer has a dynamic IP address and is authenticated by a certificate, you must select Aggressive mode if there is more than one phase 1 configuration for the interface IP address and these phase 1 configurations use different proposals.
Authentication Method	Select *Preshared Key* or *RSA Signature*.

Pre-shared Key	If you selected *Pre-shared Key*, enter the pre-shared 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 key at the remote peer or client. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters.
Certificate Name	If you selected *RSA Signature*, 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. For information about obtaining and loading the required server certificate, see the *FortiOS User Authentication guide*.
Peer Options	Peer options are available to authenticate VPN peers or clients, depending on the *Remote Gateway* and *Authentication Method* settings.
Accept any peer ID	Accept the local ID of any remote VPN peer or client. The FortiGate unit does not check identifiers (local IDs). You can set *Mode* to *Aggressive* or *Main*. You can use this option with RSA Signature authentication. But, for highest security, configure a PKI user/group for the peer and set *Peer Options* to *Accept this peer certificate only*.
Accept this peer ID	This option is available when *Aggressive Mode* is enabled. Enter the identifier that is used to authenticate the remote peer. This identifier must match the Local ID that the remote peer's administrator has configured. If the remote peer is a FortiGate unit, the identifier is specified in the *Local ID* field of the Advanced phase 1 configuration. If the remote peer is a FortiClient user, the identifier is specified in the *Local ID* field, accessed by selecting *Config* in the *Policy* section of the VPN connection's *Advanced Settings*.
Accept peer ID in dialup group	Authenticate multiple FortiGate or FortiClient dialup clients that use unique identifiers and unique pre-shared keys (or unique pre-shared keys only) through the same VPN tunnel. You must create a dialup user group for authentication purposes. Select the group from the list next to the *Accept peer ID in dialup group* option. You must set *Mode* to *Aggressive* when the dialup clients use unique identifiers and unique pre-shared keys. If the dialup clients use unique pre-shared keys only, you can set *Mode* to *Main* if there is only one dialup phase 1 configuration for this interface IP address.
Advanced	Defines advanced phase 1 parameters. For more information, see Phase 1 advanced configuration settings.

Phase 1 advanced configuration settings

You use the advanced parameters to select the encryption and authentication algorithms that the FortiGate unit uses to generate keys for the IKE exchange. You can also select these advanced settings to ensure the smooth operation of phase 1 negotiations.

To configure Phase 1settings, go to *VPN* > *Auto Key (IKE)* and select *Create Phase 1*.

Enable IPsec Interface Mode	This is available in NAT mode only. Create a virtual interface for the local end of the VPN tunnel. Select this option to create a route-based VPN, clear it to create a policy-based VPN.
IKE Version	Select the version of IKE to use. This is available only if *IPsec Interface Mode* is enabled. For more information about IKE v2, refer to RFC 4306. IKE v2 is not available if *Mode* is *Aggressive*. When *IKE Version* is *2*, *Mode* and *XAUTH* are not available.
IPv6 Version	Select if you want to use IPv6 addresses for the remote gateway and interface IP addresses. This is available only when *Enable IPsec Interface Mode* is selected and IPv6 Support is enabled in the administrative settings (*System* > *Admin* > *Settings*).
Local Gateway IP	If you selected *Enable IPsec Interface Mode*, specify an IP address for the local end of the VPN tunnel. Select one of the following: • *Main Interface IP* — The FortiGate unit obtains the IP address of the interface from the network interface settings. • *Specify* — Enter a secondary address of the interface selected in the phase 1 *Local Interface* field. You cannot configure Interface mode in a transparent mode VDOM.
P1 Proposal	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of three combinations. The remote peer or client must be configured to use at least one of the proposals that you define. 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 Cipher Block Chaining (CBC) algorithm that uses a 128-bit key. • *AES192* — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key. • *AES256* — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.

	Select either of the following authentication 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. • *SHA256* — Secure Hash Algorithm 2, which produces a 256-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, 5 and 14. At least one of the *DH Group* settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.
Keylife	Enter the time (in seconds) that must 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 172 800 seconds.
Local ID	If the FortiGate unit will act as a VPN client and you are using peer IDs for authentication purposes, enter the identifier that the FortiGate unit will supply to the VPN server during the phase 1 exchange. If the FortiGate unit will act as a VPN client, and you are using security certificates for authentication, select the distinguished name (DN) of the local server certificate that the FortiGate unit will use for authentication purposes. If the FortiGate unit is a dialup client and will not be sharing a tunnel with other dialup clients (that is, the tunnel will be dedicated to this Fortinet dialup client), set *Mode* to *Aggressive*. Note that this Local ID value must match the peer ID value given for the remote VPN peer's Peer Options.
XAuth	This option supports the authentication of dialup clients. It is available for IKE v1 only. • *Disable* — Select if you do not use XAuth. • *Enable as Client* — If the FortiGate unit is a dialup client, enter the user name and password that the FortiGate unit will need to authenticate itself to the remote XAuth server. • *Enable as Server* — This is available only if *Remote Gateway* is set to *Dialup User*. Dialup clients authenticate as members of a dialup user group. You must first create a user group for the dialup clients that need access to the network behind the FortiGate unit. You must also configure the FortiGate unit to forward authentication requests to an external RADIUS or LDAP authentication server. Select a *Server Type* setting to determine the type of encryption method to use between the FortiGate unit, the XAuth client and the external authentication server, and then select the user group from the User Group list.
Username	Enter the user name that is used for authentication.

Password	Enter the password that is used for authentication.
NAT Traversal	Select the check box 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) to connect reliably.
Keepalive Frequency	If you enabled *NAT-traversal*, enter a keepalive frequency setting.
Dead Peer Detection	Select this check box to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. You can use this option to receive notification whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, in scenarios where a dialup client or dynamic DNS peer connects from an IP address that changes periodically, traffic may be suspended while the IP address changes. With *Dead Peer Detection* selected, you can use the `config vpn ipsec phase1` (tunnel mode) or `config vpn ipsec phase1-interface` (interface mode) CLI command to optionally specify a retry count and a retry interval.

Phase 2 configuration

After IPsec phase 1 negotiations end successfully, you begin phase 2. You configure the phase 2 parameters to define the algorithms that the FortiGate unit may use to encrypt and transfer data for the remainder of the session. During phase 2, you select specific IPsec security associations needed to implement security services and establish a tunnel.

The basic phase 2 settings associate IPsec phase 2 parameters with the phase 1 configuration that specifies the remote end point of the VPN tunnel. In most cases, you need to configure only basic phase 2 settings.

To configure Phase 2 settings, go to *VPN* > *Auto Key (IKE)* and select *Create Phase 2*.

Name	Type a name to identify the phase 2 configuration.
Phase 1	Select the phase 1 tunnel configuration. For more information on configuring phase 1, see “Phase 1 configuration” on page 24. The phase 1 configuration describes how remote VPN peers or clients will be authenticated on this tunnel, and how the connection to the remote peer or client will be secured.
Advanced	Define advanced phase 2 parameters. For more information, see “Phase 2 advanced configuration settings” on page 28.

Phase 2 advanced configuration settings

In phase 2, the FortiGate unit and the VPN peer or client exchange keys again to establish a secure communication channel between them. You select the encryption and authentication algorithms needed to generate keys for protecting the implementation details of Security Associations (SAs). These are called P2 Proposal parameters. The keys are generated automatically using a Diffie-Hellman algorithm.

You can use a number of additional advanced phase 2 settings to enhance the operation of the tunnel.

P2 Proposal	Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. You can specify up to three proposals. To establish a VPN connection, at least one of the proposals that you specify must match configuration on the remote peer. Initially there are two proposals. *Add* and *Delete* icons are next to the second *Authentication* field. It is invalid to set both *Encryption* and *Authentication* to NULL.
Encryption	Select one 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 Cipher Block Chaining (CBC) algorithm that uses a 128-bit key. • *AES192* — a 128-bit block CBC algorithm that uses a 192-bit key. • *AES256* — a 128-bit block CBC algorithm that uses a 256-bit key.
Authentication	Select one 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. • *SHA256* — Secure Hash Algorithm 2, which produces a 256-bit message digest. • *SHA384* — Secure Hash Algorithm 2, which produces a 384-bit message digest. • *SHA512* — Secure Hash Algorithm 2, which produces a 512-bit message digest.
Enable 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)	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, 5 or 14). This must match the DH Group that the remote peer or dialup client uses.
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.
Autokey Keep Alive	Select the check box if you want the tunnel to remain active when no data is being processed.

DHCP-IPSec	Provide IP addresses dynamically to VPN clients. This is available for phase 2 configurations associated with a dialup phase 1 configuration. You also need configure a DHCP server or relay on the private network interface. You must configure the DHCP parameters separately. If you configure the DHCP server to assign IP addresses based on RADIUS user group attributes, you must also set the Phase 1 *Peer Options* to *Accept peer ID in dialup group* and select the appropriate user group. See "Phase 1 configuration" on page 24. If the FortiGate unit acts as a dialup server and you manually assigned FortiClient dialup clients VIP addresses that match the network behind the dialup server, selecting the check box will cause the FortiGate unit to act as a proxy for the dialup clients.
Quick Mode Selector	Specify the source and destination IP addresses to be used as selectors for IKE negotiations. If the FortiGate unit is a dialup server, keep the default value of 0.0.0.0/0 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 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.
Source address	If the FortiGate unit is a dialup server, enter the source IP address that corresponds to the local senders 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 Fortinet dialup client.
Source port	Enter the port number that the local VPN peer uses to transport traffic related to the specified service (protocol number). The range is from 0 to 65535. To specify all ports, type `0`.
Destination address	Enter the destination IP address that corresponds to the recipients 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	Enter the port number that the remote VPN peer uses to transport traffic related to the specified service (protocol number). To specify all ports, enter `0`.
Protocol	Enter the IP protocol number of the service. To specify all services, enter `0`.

FortiClient VPN

Use the FortiClient VPN configuration settings when configuring an IPsec VPN for remote users to connect to the VPN tunnel using FortiClient.

To create a FortiClient VPN tunnel, go to *VPN* > *IPsec* > *Auto Key (IKE)* and select *Create FortiClient VPN* at the top of the screen.

When configuring a FortiClient VPN connection, the settings for phase 1 and phase 2 settings are automatically configured by the FortiGate unit. They are set to:

- Remote Gateway — Dialup User
- Mode — Aggressive
- IPSec Interface Mode — Enabled
- Default settings for P1 and P2 Proposal
- XAUTH Enable as Server (Auto)
- IKE mode-config will be enabled
- Peer Option — “Accept any peer ID”

The remainder of the settings use the current FortiGate defaults. Note that FortiClient settings need to match these FortiGate defaults. If you need to configure advanced settings for the FortiClient VPN, select *Edit* on the Auto Key (IKE) page (Go to *VPN* > *IPsec* > *Auto Key (IKE)*) and configure the peer options or advanced options.

Name	Enter a name for the FortiClient VPN.
Local Outgoing Interface	Select the local outgoing interface for the VPN.
Authentication Method	Select the type of authentication used when logging in to the VPN.
Preshared Key	If *Pre-shared Key* was selected in *Authentication Method*, enter the pre-shared key in the field provided.
User Group	Select a user group. You can also create a user group from the drop-down list by selecting *Create New*.
Address Range Start IP	Enter the start IP address for the DHCP address range for the client.
Address Range End IP	Enter the end IP address for the address range.
Subnet Mask	Enter the subnet mask.
Enable IPv4 Split Tunnel	Enabled by default, this option enables the FortiClient user to use the VPN to access internal resources while other Internet access is not sent over the VPN, alleviating potential traffic bottlenecks in the VPN connection. Disable this option to have all traffic sent through the VPN tunnel.
Accessible Networks	Select from a list of internal networks that the FortiClient user can access.

Client Options	These options affect how the FortiClient application behaves when connected to the FortiGate VPN tunnel. When enabled, a check box for the corresponding option appears on the VPN login screen in FortiClient, and is not enabled by default. **Save Password** - When enabled, if the user selects this option, their password is stored on the user's computer and will automatically populate each time they connect to the VPN. **Auto Connect** - When enabled, if the user selects this option, when the FortiClient application is launched, for example after a reboot or system startup, FortiClient will automatically attempt to connect to the VPN tunnel. **Always Up (Keep Alive)** - When enabled, if the user selects this option, the FortiClient connection will not shut down. When not selected, during periods of inactivity, FortiClient will attempt to stay connected every three minutes for a maximum of 10 minutes.
Endpoint Registration	When selected, the FortiGate unit requests a registration key from FortiClient before a connection can be established. A registration key is defined by going to *System* > *Config* > *Advanced*. For more information on FortiClient VPN connections to a FortiGate unit, see the *FortiClient Administration Guide*.
DNS Server	Select which DNS server to use for this VPN: • *Use System DNS* — Use the same DNS servers as the FortiGate unit. These are configured at *System* > *Interface* > *DNS*. This is the default option. • *Specify* — Specify the IP address of a different DNS server.

Manual Key

Use manual keys only if it is unavoidable. There are potential difficulties in keeping keys confidential and in propagating changed keys to remote VPN peers securely.

If required, you can manually define cryptographic keys for establishing an IPsec VPN tunnel. You would define manual keys in situations where:

- you require prior knowledge of the encryption or authentication key (that is, one of the VPN peers requires a specific IPsec encryption or authentication key).
- you need to disable encryption and authentication.

In both cases, you do not specify IPsec phase 1 and phase 2 parameters; you define manual keys by going to *VPN* > *IPsec* > *Manual Key* instead.

To use manual keys, you must first enable the feature. To do this, go to *System* > *Admin* > *Settings* and select *IPSec Manual Key* from the *Display Options on GUI* section.

Manual key configuration settings

If one of the VPN devices is manually keyed, the other VPN device must also be manually keyed with the identical authentication and encryption keys. In addition, it is essential that both VPN devices be configured with complementary Security Parameter Index (SPI) settings. The administrators of the devices need to cooperate to achieve this.

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

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. You must manually specify an SPI for each SA. There is an SA for each direction, so for each VPN you must specify two SPIs, a local SPI and a remote SPI, to cover bidirectional communications between two VPN devices.

To add a manual key, go to *VPN* > *IPsec* > *Manual Key* and select *Create New*.

Name	Type a name for the VPN tunnel. The maximum name length is 15 characters for an interface mode VPN, 35 characters for a policy-based VPN.
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	Enter the IP address of the public interface to the remote peer. The address identifies the recipient of ESP datagrams.
Local Interface	This option is available in NAT mode only. Select the name of the interface to which the IPsec tunnel will be bound. The FortiGate unit obtains the IP address of the interface from the network interface settings.
Encryption Algorithm	Select one of the following symmetric-key encryption 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, where plain text is encrypted three times by three keys. • *AES128* — a 128-bit block Cipher Block Chaining algorithm that uses a 128-bit key. • *AES192* — a 128-bit block Cipher Block Chaining) algorithm that uses a 192-bit key. • *AES256* — a 128-bit block Cipher Block Chaining algorithm that uses a 256-bit key. **Note:** The algorithms for encryption and authentication cannot both be NULL.

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	Enter the IP address of the public interface to the remote peer. The address identifies the recipient of ESP datagrams.
Local Interface	This option is available in NAT mode only. Select the name of the interface to which the IPsec tunnel will be bound. The FortiGate unit obtains the IP address of the interface from the network interface settings.
Encryption Algorithm	Select one of the following symmetric-key encryption 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, where plain text is encrypted three times by three keys. • *AES128* — a 128-bit block Cipher Block Chaining algorithm that uses a 128-bit key. • *AES192* — a 128-bit block Cipher Block Chaining) algorithm that uses a 192-bit key. • *AES256* — a 128-bit block Cipher Block Chaining algorithm that uses a 256-bit key. **Note:** The algorithms for encryption and authentication cannot both be NULL.

Concentrator

In a hub-and-spoke configuration, policy-based VPN connections to a number of remote peers radiate from a single, central FortiGate unit. Site-to-site connections between the remote peers do not exist; however, you can establish VPN tunnels between any two of the remote peers through the FortiGate unit's "hub".

In a hub-and-spoke network, all VPN tunnels terminate at the hub. The peers that connect to the hub are known as "spokes". The hub functions as a concentrator on the network, managing all VPN connections between the spokes. VPN traffic passes from one tunnel to the other through the hub.

You define a concentrator to include spokes in the hub-and-spoke configuration. You create the concentrator in *VPN* > *IPSec* > *Concentrator* and select *Create New*. A concentrator configuration specifies which spokes to include in an IPsec hub-and-spoke configuration.

Concentrator Name	Type a name for the concentrator.
Available Tunnels	A list of defined IPsec VPN tunnels. Select a tunnel from the list and then select the right arrow.
Members	A list of tunnels that are members of the concentrator. To remove a tunnel from the concentrator, select the tunnel and select the left arrow.

IPsec Monitor

You can use the IPsec 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, including tunnel mode and route-based (interface mode) tunnels.

To view the IPsec monitor, go to *VPN* > *Monitor* > *IPsec Monitor*.

For dialup VPNs, the list provides status information about the VPN tunnels established by dialup clients, and their IP addresses.

For static IP or dynamic DNS VPNs, the list provides status and IP addressing information about VPN tunnels, active or not, to remote peers that have static IP addresses or domain names. You can also start and stop individual tunnels from the list.

Auto Key phase 1 parameters

This chapter 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.

For more information on phase 1 parameters in the web-based manager, see "Phase 1 configuration" on page 24.

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 171 instead.

The following topics are included in this section:

Overview

To configure IPsec phase 1 settings, go to *VPN* > *IPsec* > *Auto Key (IKE)* and select *Create Phase 1*. IPsec phase 1 settings define:

- the remote and local ends of the IPsec tunnel
- if 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)
- if a preshared key or digital certificates will be used to authenticate the FortiGate unit to the VPN peer or dialup client
- if 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.

For all the phase 1 web-based manager fields, see "Phase 1 configuration" on page 24.

If you want to control how the IKE negotiation process controls traffic when there is no traffic, as well as the length of time the unit waits for negotiations to occur, use the `negotiation-timeout` and `auto-negotiation` commands in the CLI.

Defining the tunnel ends

To begin defining the phase 1 configuration, go to *VPN* > *IPsec* > *Auto Key (IKE)* 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 the FortiGate interface that sends and receives IPsec packets.

The remote gateway can be:

- 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 security 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 security 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 Endpoint 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 (typically the WAN1 port). Packets from this interface pass to the private network through a security policy.

By default, the local VPN gateway is the IP address of the selected Local Interface. If you are configuring an interface mode VPN, you can optionally use a secondary IP address of the Local Interface as the local gateway.

Choosing main mode or aggressive mode

The FortiGate unit and the remote peer or dialup client exchange phase 1 parameters in either Main mode or Aggressive mode. This choice does not apply if you use IKE version 2, which is available only for route-based configurations.

- 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.

Although Main mode is more secure, 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 whether Main or Aggressive mode is required.

Choosing the IKE version

If you create a route-based VPN, you have the option of selecting IKE version 2. Otherwise, IKE version 1 is used.

IKEv2, defined in RFC 4306, simplifies the negotiation process that creates the security association (SA).

If you select IKEv2:

- There is no choice in Phase 1 of Aggressive or Main mode.
- FortiOS does not support Peer Options or Local ID.
- Extended Authentication (XAUTH) is not available.
- You can select only one DH Group.

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 *FortiOS User Authentication guide*.

To authenticate the FortiGate unit using digital certificates

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)*.
2. Create a new phase 1 configuration or edit an existing phase 1 configuration.
3. Include appropriate entries as follows:

Name	Enter a name that reflects the origination of the remote connection. For interface mode, the name can be up to 15 characters long.
Remote Gateway	Select the nature of the remote connection. Each option changes the available fields you must configure. For more information, see “Defining the tunnel ends” on page 37.
Local Interface	Select the interface that is the local end of the IPsec tunnel. For more information, see “Defining the tunnel ends” on page 37. The local interface is typically the WAN1 port.

Mode	Select a mode. It is easier to use aggressive mode. • In Main mode, parameters are exchanged in multiple encrypted rounds. • In Aggressive mode, parameters are exchanged in a single unencrypted message. Aggressive mode must be used 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). For more information, see "Choosing main mode or aggressive mode" on page 37.
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. You must obtain and load the required server certificate before this selection. See the *FortiOS User Authentication guide.* If you have not loaded any certificates, use the certificate named *Fortinet_Factory*.
Peer Options	Peer options define the authentication requirements for remote peers or dialup clients. They are not for your FortiGate unit itself. See "Authenticating remote peers and clients" on page 41.
Advanced	You can use the default settings for most phase 1 configurations. Changes are required only if your network requires them. These settings includes IKE version, DNS server, P1 proposal encryption and authentication settings, and XAuth settings. See "Defining IKE negotiation parameters" on page 45.

4. If you are configuring authentication parameters for a dialup user group, optionally define extended authentication (XAuth) parameters in the Advanced section. See "Using the FortiGate unit as an XAuth server" on page 50.
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 is 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 with user accounts and pre-shared keys" on page 44.

The pre-shared key must contain at least 6 printable characters and best practices dictate that it be known only to network administrators. For optimum protection against currently known attacks, the key must 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 (IKE)*.
2. Create a new phase 1 configuration or edit 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. For more information, see "Defining the tunnel ends" on page 37.
Local Interface	Select the interface that is the local end of the IPsec tunnel. For more information, see "Defining the tunnel ends" on page 37. The local interface is typically the WAN1 port.
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 37.
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 best practices dictate that it only be known by network administrators. For optimum protection against currently known attacks, the key must 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 41.
Advanced	You can retain the default settings unless changes are needed to meet your specific requirements. See "Defining IKE negotiation parameters" on page 45.

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 50.
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:

Table 3: Methods of authenticating remote VPN peers

Certificates or Pre-shared key	Local ID	User account pre-shared keys	Reference
Certificates			See "Enabling VPN access for specific certificate holders" on page 41
Either	X		See "Enabling VPN access by peer identifier" on page 43
Pre-shared key		X	See "Enabling VPN access with user accounts and pre-shared keys" on page 44
Pre-shared key	X	X	See "Enabling VPN access with user accounts and pre-shared keys" on page 44

For authentication of users of the remote peer or dialup client device, see "Using XAuth authentication" on page 49.

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 38). 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 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 42.

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 *System* > *Certificates* > *Local Certificates*.
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 *System* > *Certificates* > *CA Certificates*.
2. Note the value in the *Name* column (for example, `CA_Cert_1`).

Configuring certificate authentication for a VPN

With peer certificates loaded, peer users and peer groups defined, you can configure your VPN to authenticate users by certificate.

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 (IKE)*.
2. In the list of defined configurations, select the phase 1 configuration and edit it.
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 41.
   - 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 41.
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.

A peer ID, also called local ID, can be up to 63 characters long containing standard regular expression characters. Local ID is set in phase1 Aggressive Mode configuration.

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 a phase 1 configuration and 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 a phase 1 configuration and 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 application

Follow this procedure to add a peer ID to an existing FortiClient configuration:

1. Start the FortiClient application.
2. Go to *VPN* > *Connections*, select the existing configuration.
3. Select *Advanced* > *Edit* > *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 with 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 38). 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 Endpoint 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 43.

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 Authentication Guide*.

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. For more information, see the *User Authentication 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.

To authenticate dialup clients using unique preshared keys and/or peer IDs

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 user account password will be used as the preshared key.

5 Select *Accept peer ID in dialup group* and then select the group name from the list of user groups.
6 Select *OK*.

Follow this procedure to add a unique pre-shared key and unique peer ID to an existing FortiClient configuration.

To configure FortiClient - pre-shared key and peer ID

1. Start the FortiClient Endpoint Security application.
2. Go to *VPN* > *Connections*, select the existing configuration.
3. Select *Advanced* > *Edit*.

4. In the *Preshared Key* field, type the FortiGate password that belongs to the dialup client (for example, `1234546`).

   The user account password will be used as the preshared key.
5. Select *Advanced*.
6. Under *Policy*, select *Config*.
7. In the *Local ID* field, type the FortiGate user name that you assigned previously to the dialup client (for example, `FortiClient1`).
8. Select *OK* to close all dialog boxes.

Configure all FortiClient dialup clients this way using unique preshared keys and local IDs.

Follow this procedure to add a unique pre-shared key to an existing FortiClient configuration.

To configure FortiClient - preshared key only

1. Start the FortiClient Endpoint Security application.
2. Go to *VPN* > *Connections*, select the existing configuration
3. Select *Advanced* > *Edit*.
4. 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`)
5. 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 and negotiate a way to encrypt further communications for the duration of the session. For more information see "Authenticating remote peers and clients" on page 41. 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 (DH 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. These algorithms are defined in RFC 2409. 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 49.

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 in FIPS-CC mode, the FortiGate unit requires DH key exchange to use values at least 3072 bits long. However most browsers need the key size set to 1024. You can set the minimum size of the DH keys in the CLI.

```
config system global
  set dh-params 3072
end
```

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, HMAC-SHA-1, or HMAC-SHA-256). Hash-based Message Authentication Code (HMAC) is a method for calculating an authentication code using a hash function plus a secret key, and is defined in RFC 2104. Each party signs a different combination of inputs and the other party verifies that the same result can be computed.

SHA-256, SHA-384 and SHA-512 are not accelerated by some FortiASIC processors (including FortiASIC network processors and security processors). As a result, using SHA-256, SHA-384 and SHA-512 may reduce the performance of the FortiGate unit more significantly than SHA-1 which is accelerated by all FortiASIC processors.

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 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 with user accounts and pre-shared keys" on page 44 and "Using the FortiGate unit as an XAuth server" on page 50. 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 and select *OK*:

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 these 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 one 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. • SHA-256 Secure Hash Algorithm 256, which produces a 256-bit message digest • SHA-384 Secure Hash Algorithm 384, which produces a 384-bit message digest • SHA-512 Secure Hash Algorithm 512, which produces a 512-bit message digest To specify a third combination, use the add button beside the fields for the second combination. SHA-256, SHA-384 and SHA-512 are not accelerated by some FortiASIC processors (including FortiASIC network processors and security processors). As a result, using SHA-256, SHA-384 and SHA-512 may reduce the performance of the FortiGate unit more significantly than SHA-1 which is accelerated by all FortiASIC processors.

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). When in doubt, enable NAT-traversal. See “NAT traversal” on page 48.
Keepalive Frequency	If you enabled NAT traversal, enter a keepalive frequency setting. The value represents an interval from 0 to 900 seconds where the connection will be maintained with no activity. For additional security this value must be as low as possible. See “NAT keepalive frequency” on page 49.
Dead Peer Detection	Enable this option to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. This feature minimizes the traffic required to check if a VPN peer is available or unavailable (dead). See “Dead peer detection” on page 49.

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, 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, when you enable NAT traversal specify how often the FortiGate unit sends 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. To be effective, the keepalive interval must be smaller than the session lifetime value used by the NAT device.

The keepalive packet is a 138-byte ISAKMP exchange.

Dead peer detection

Sometimes, due to routing issues 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, sometimes referred to as gateway detection or ping server, 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, Dead Peer Detection sends probe messages every five seconds by default (see `dpd-retryinterval` in the *FortiGate CLI Reference*). If you are experiencing high network traffic, you can experiment with increasing the ping interval. However longer intervals will require more traffic to detect dead peers which will result in more traffic.

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 commands and the related `config router gwdetect` CLI command, see the *FortiGate CLI Reference*.

For example, enter the following CLI commands to configure dead peer detection on the existing IPsec Phase1 configuration called `test` to use 15 second intervals and to wait for 3 missed attempts before declaring the peer dead and taking action.

```
config vpn ipsec phase1
  edit test
    set dpd enable
    set dpd-retryinveral 15
    set dpd-retrycount 3
  next
end
```

Using XAuth authentication

Extended authentication (XAuth) increases security by requiring the remote dialup client user to authenticate 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.If the server or client is attempting a connection using XAuth and the other end is not using XAuth, the failed connection attempts that are logged will not specify XAuth as the reason.

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.

If the user records on the RADIUS server have suitably configured Framed-IP-Address fields, you can assign client virtual IP addresses by XAuth instead of from a DHCP address range. See "Assigning VIPs by RADIUS user group" on page 112.

The authentication protocol to use for XAuth depends on the capabilities of the authentication server and the XAuth client:

- Select PAP whenever possible.
- You must select PAP for all implementations of LDAP and some implementations of Microsoft RADIUS.
- Select AUTO 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.

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 *FortiGate User Authentication Guide*.

To authenticate a dialup user group using XAuth settings

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.
   - *AUTO*—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*.

Using the FortiGate unit as an XAuth client

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 a phase 1 configuration and select *Edit*.
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

After IPsec VPN phase 1 negotiations complete successfully, phase 2 negotiation begins. 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 defining phase 2 parameters, you can choose any set of phase 1 parameters to set up a secure connection and authenticate the remote peer.

For more information on phase 2 settings in the web-based manager, see “Phase 2 configuration” on page 28

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 171 instead.

Advanced phase 2 settings

The following additional advanced phase 2 settings are available to enhance the operation of the tunnel:

- P2 Proposals
- Replay detection
- Perfect forward secrecy (PFS)
- Keylife
- Quick mode selectors

P2 Proposals

In phase 2, the VPN peer or client and the FortiGate unit exchange keys again to establish a secure communication channel. 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 (PFS)

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. The default units are seconds. 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 for 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 goes down, the auto-negotiate feature will attempt to re-establish it. However, the Autokey Keep Alive feature is a better method to ensure your VPN remains up.

Autokey Keep Alive

The phase 2 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 without interruption. If there is no traffic, the SA expires and the VPN tunnel goes down. A new SA will not be generated until there is traffic.

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.

With the DHCP-IPsec option, the FortiGate dialup server acts 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 (when a remote server sends an ARP to the local FortiClient dialup client), 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.

This feature prevents the VIP address assigned to the FortiClient dialup client from causing possible arp broadcast problems — the normal and VIP addresses can confuse some network switches by two addresses having the same MAC address.

Quick mode selectors

Quick Mode selectors determine which IP addresses can perform IKE negotiations to establish a tunnel. By only allowing authorized IP addresses access to the VPN tunnel, the network is more secure.

The default settings are as broad as possible: any IP address or configured address object, using any protocol, on any port.

While the drop down menus for specifying an address also show address groups, the use of address groups is not supported.

To made it easy to determine if one of the choices in the drop down menu is an address or an address group the two types of objects have been broken into sections with the address groups at the bottom of the list.

When configuring Quick Mode selector *Source Address* and *Destination address*, valid options include IPv4 and IPv6 single addresses, IPv4 subnet, or IPv6 subnet. For more information on IPv6 IPsec VPN, see “Overview of IPv6 IPsec support” on page 174.

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

With FortiOS VPNs, your network has multiple layers of security, with quick mode selectors being an important line of defence.

- Routes guide traffic from one IP address to another.
- Phase 1 and phase 2 connection settings ensure there is a valid remote end point for the VPN tunnel that agrees on the encryption and parameters.
- Quick mode selectors allow IKE negotiations only for allowed peers.
- Security policies control which IP addresses can connect to the VPN.
- Security policies also control what protocols are allowed over the VPN along with any bandwidth limiting.

Configure the phase 2 parameters

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*.
3. Enter a *Name* for the phase 2 configuration, and select a *Phase 1* configuration from the drop-down list.

4 Select *Advanced*.

5 Include appropriate entries and select *OK*:

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	Select a 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; 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. • **SHA1** — Secure Hash Algorithm 1 - 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, 5, or 14). 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 address to be used as selectors for IKE negotiations. If the FortiGate unit is a dialup server, keep the default value 0.0.0.0/0 unless you need to circumvent problems caused by ambiguous IP addresses between one or more of the private networks making up the VPN. Note that IKEv1 does not support the use of multiple addresses in selectors. Instead, use the default 0.0.0.0/0 subnet selector and rely on the firewall policy to limit destination addresses. Only use the Addressing objects if they are carried over from earlier versions of FortiOS. 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`.

Defining VPN security 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 security policies.

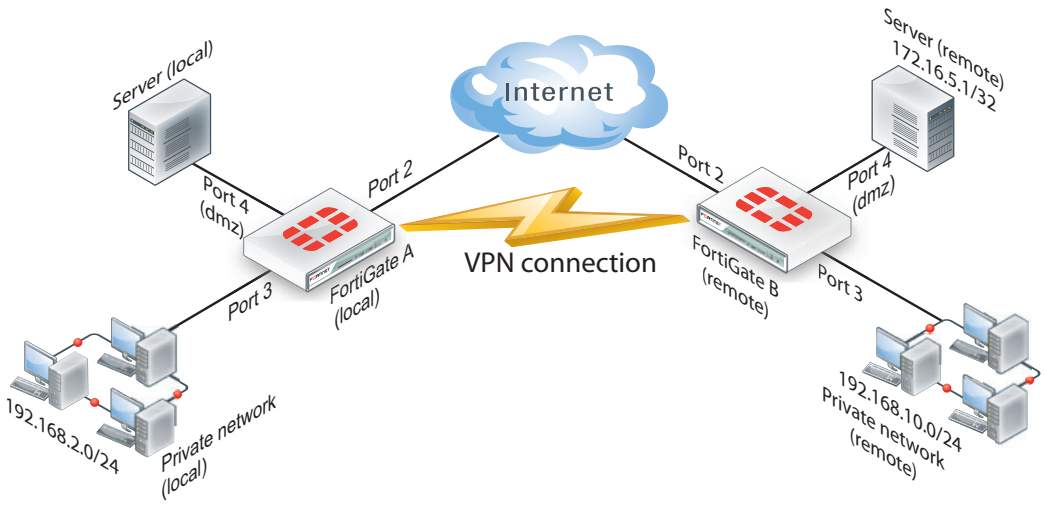
The following topics are included in this section:

Defining policy 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 security policy.

Figure 4: Example topology for the following policies



In general:

- In a gateway-to-gateway, hub-and-spoke, dynamic DNS, redundant-tunnel, or transparent configuration, you need to define a policy 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 policy 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 security policy to refer to the dialup clients.
- If you assign VIP addresses to FortiClient dialup clients manually, you need to define a policy 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 policy address for the private IP address of a host, server, or network behind the FortiGate dialup server.

To define a security IP address

1. Go to *Firewall Objects* > *Address* > *Addresses* and select *Create New*.
2. In the *Name* field, type a descriptive name that represents the network, server(s), or host(s).
3. In *Type*, select *Subnet*.
4. In the *Subnet/IP Range* field, type the corresponding IP address and subnet mask.

   For a subnet you could use the format `172.16.5.0/24` or its equivalent `172.16.5.0/255.255.255.0`. For a server or host it would likely be `172.16.5.1/32`. Alternately you can use an IP address range such as `192.168.10.[80-100]` or `192.168.10.80-192.168.10.100`.
5. Select *OK*.

Defining VPN security policies

Security 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. Then only traffic from those addresses will be allowed.

Policy-based and route-based VPNs require different security policies.

- A policy-based VPN requires an IPsec security 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 security 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. One security policy must be configured for each direction of each VPN interface.

There are examples of security policies for both policy-based and route-based VPNs throughout this guide. See “Route-based or policy-based VPN” on page 96.

If the security policy, which grants the VPN Connection is limited to certain services, DHCP must be included, otherwise the client won’t be able to retrieve a lease from the FortiGate’s (IPSec) DHCP server, because the DHCP Request (coming out of the tunnel) will be blocked.

Defining an IPsec security policy for a policy-based VPN

An IPsec security 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.

Allow traffic to be initiated from the remote site

In addition to these operations, security policies specify which IP addresses can initiate a tunnel. by default, traffic from the local private network initiates the tunnel. When the *Allow traffic to be initiated form the remote site* option is selected, traffic from a dialup client or computers on the remote network initiates the tunnel. Both can be enabled at the same time for bi-directional initiation of the tunnel.

Outbound and inbound NAT

When a FortiGate unit operates in NAT 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. By default, these options are not selected in security 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. .

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.

Source and destination addresses

Most security policies control outbound IP traffic. A VPN 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 security 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 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.

Enabling other policy features

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.

As an option, differentiated services (diffserv or DSCP) can be enabled in the security policy through CLI commands. For more information on this feature, see Traffic Shaping guide or 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 security 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 security 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. To follow this negotiation in the web-based manager, go to *VPN* > *Monitor* > *IPsec Monitor*. There you will find a list of the VPN tunnels, their status, and the data flow both incoming and outgoing.

Before you begin

Before you define the IPsec policy, you must:

- Define the IP source and destination addresses. See "Defining policy addresses" on page 58.
- Specify the phase 1 authentication parameters. See "Auto Key phase 1 parameters" on page 36.
- Specify the phase 2 parameters. See "Phase 2 parameters" on page 52.

To define an IPsec security policy

1. Go to *Policy* > *Policy* > *Policy.*
2. Select *Create New* and select *VPN*.
3. Complete the options:

Local Interface	Select the local interface to the internal (private) network.
Local Protected Subnet	Select the name that corresponds to the local network, server(s), or host(s) from which IP packets may originate.
Outgoing VPN Interface	Select the local interface to the external (public) network.
Remote Protected Subnet	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.
VPN Tunnel	Select *Use Existing* and select the tunnel from the drop-down list.
Allow traffic to be initiated from the remote site	Select if traffic from the remote network will be allowed to initiate the tunnel.

4. You may enable UTM features, and/or event logging, or select advanced settings to authenticate a user group, or shape traffic. For more information, see the *Firewall Guide*.
5. Select *OK*.
6. 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 security 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.

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 security 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 security 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 security policies.

To define security policies for a route-based VPN

1. Go to *Policy* > *Policy* > *Policy*.
2. Select *Create New* and leave the *Policy Type* as *Firewall*, and the *Policy Subtype* as *Address*.
3. Define an ACCEPT security policy to permit communications between the local private network and the private network behind the remote peer. Enter these settings in particular:

Incoming Interface	Select the interface that connects to the private network behind this FortiGate unit.
Source Address	Select the address name that you defined for the private network behind this FortiGate unit.
Outgoing Interface	Select the IPsec Interface you configured.
Destination Address	Select the address name that you defined for the private network behind the remote peer.
Action	Select *ACCEPT*.
Enable NAT	Disable.

To permit the remote client to initiate communication, you need to define a security policy for communication in that direction.

4. Select *Create New* and leave the *Policy Type* as *Firewall*, and the *Policy Subtype* as *Address*
5. Enter these settings in particular:

Incoming Interface	Select the IPsec Interface you configured.
Source Address	Select the address name that you defined for the private network behind the remote peer.
Outgoing Interface	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address	Select the address name that you defined for the private network behind this FortiGate unit.
Action	Select *ACCEPT*.
Enable NAT	Disable.

Gateway-to-gateway configurations

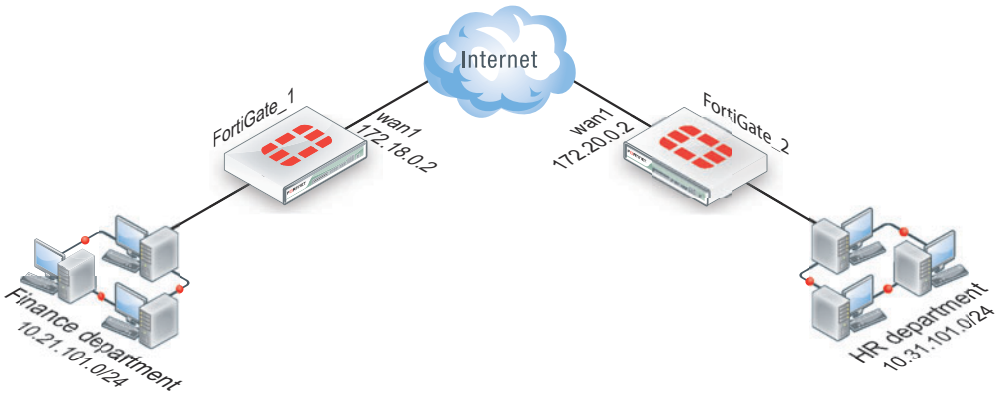
This section explains how to set up a basic gateway-to-gateway (site-to-site) IPsec VPN.

The following topics are included in this section:

Configuration overview

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 security policies.

Figure 5: Example gateway-to-gateway configuration

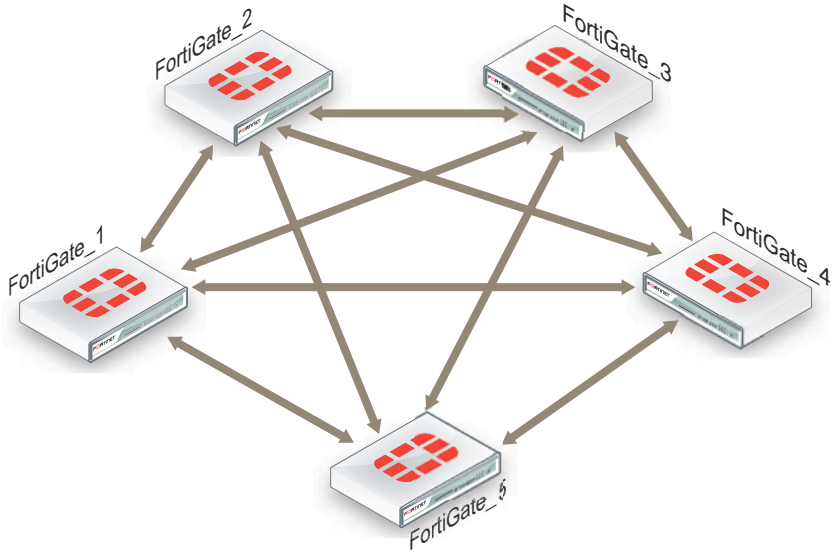


In some cases, computers on the private network behind one VPN peer may (by co-incidence) have IP addresses that are already used by computers on the network behind the other VPN peer. In this type of situation (ambiguous routing), conflicts may occur in one or both of the FortiGate routing tables and 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 71.

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 123.

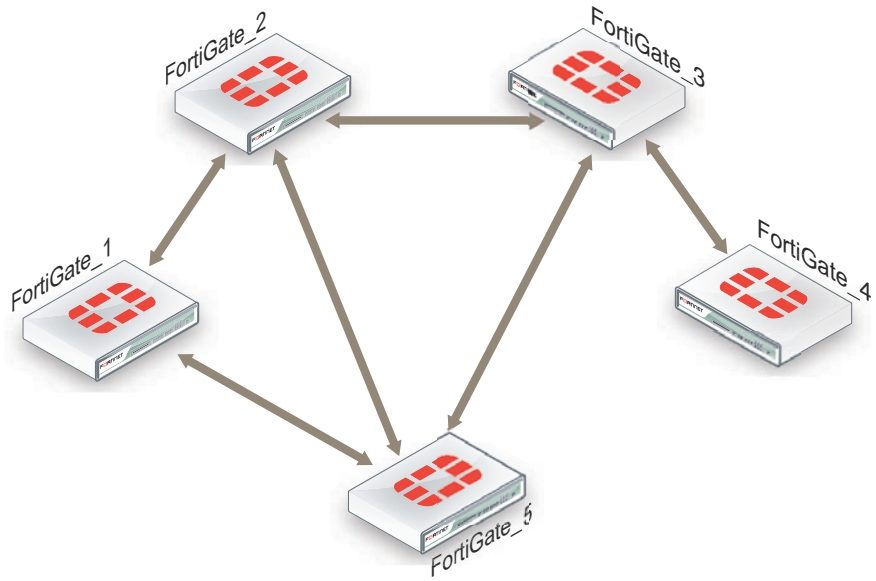
You can set up a fully meshed or partially meshed configuration (see Figure 6 and Figure 7).

Figure 6: 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. Best practices dictates a hub-and-spoke configuration instead (see "Hub-and-spoke configurations" on page 78).

Figure 7: 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.

General configuration steps

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

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 that VPN peer. Then, if the security policy permits the connection, the FortiGate unit establishes the tunnel using IPsec phase 2 parameters and applies the IPsec security 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 by 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 security policies to control the permitted services and permitted direction of traffic between the IP source and destination addresses.

Using auto-ipsec

In some cases, it may be easier to use the `auto-ipsec` CLI command to notify and push the IPsec configuration to the branch offices. Fore more information, refer to the FortiGate CLI Reference.

Configuring the two VPN peers

Configure the VPN peers as follows. Each step is required, but these are general steps. For more detailed information on each step follow the cross references. See “Auto Key phase 1 parameters” on page 36. All steps are required. Cross references point to required information that is repeated. No steps are optional.

Configuring Phase 1 and Phase 2 for both peers

This procedure applies to both peers. Repeat the procedure on each FortiGate unit, using the correct IP address for each. You may wish to vary the Phase 1 names but this is optional. Otherwise all steps are the same for each peer.

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 best practices dictate that it only be known by network administrators. For optimum protection against currently known attacks, the key must have a minimum of 16 randomly chosen alphanumeric characters.

At the local FortiGate unit, define the phase 1 configuration needed to establish a secure connection with the remote peer. See “Phase 1 configuration” on page 24.

To create phase 1 to establish a secure connection with the remote peer

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)*.
2. Select *Create Phase 1*.
3. Enter the following information, and select *OK*.

Name	Enter `peer_1`. A name to identify the VPN tunnel. This name appears in phase 2 configurations, security policies and the VPN monitor.
Remote Gateway	Select *Static IP Address*.
IP Address	Enter `172.20.0.2` when configuring FortiGate_1. Enter `172.18.0.2` when configuring FortiGate_2. The IP address of the remote peer public interface.
Local Interface	Select *wan1*.
Enable IPsec Interface Mode	Select *Advanced* to see this setting. Enable *IPsec Interface Mode* to have the FortiGate unit create a virtual IPsec interface for a route-based VPN. Disable this option to create a policy-based VPN. For more information, see "Comparing policy-based or route-based VPNs" on page 19. After selecting *OK*, you cannot change this setting.

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. See "Phase 2 configuration" on page 28.

To configure phase 2 settings

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)*.
2. Select *Create Phase 2*.
3. Enter a *Name* of `peer_1_p2`.
4. Select *peer_1* from the *Phase 1* drop-down menu.

Creating security policies

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

An IPsec security 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 security 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.

When you are creating security policies, choose one of either route-based or policy-based methods and follow it for both VPN peers. DO NOT configure both route-based and policy-based policies on the same FortiGate unit for the same VPN tunnel.

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 security policy and define the scope of permitted services between the IP source and destination addresses.

When creating security policies it is good practice to include a comment describing what the policy does.

When creating security policies you need to be

- Creating firewall addresses
- Creating route-based VPN security policies
- Configuring a default route for VPN interface

or

- Creating firewall addresses
- Creating policy-based VPN security policy

Creating firewall addresses

Define names for the addresses or address ranges of the private networks that the VPN links. These addresses are used in the security policies that permit communication between the networks.

To define the IP address of the network behind FortiGate_1

1. Go to *Firewall Objects* > *Address* > *Addresses* and select *Create New*.
2. Enter the *Name* of `Finance_network`.
3. Select a *Type* of *Subnet*.
4. Enter the *Subnet* of `10.21.101.0/24`.
5. Select *OK*.

To specify the address of the network behind FortiGate_2

1. Go to *Firewall Objects* > *Address* > *Addresses* and select *Create New*.
2. Enter the *Name* of `HR_network`.
3. Select a *Type* of *Subnet*.
4. Enter the *Subnet/IP Range* of `10.31.101.0/24`.
5. Select *OK*.

Creating route-based VPN security policies

Define an ACCEPT security policy to permit communications between the source and destination addresses.

To create route-based VPN security policies

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following, and select *OK*.

Incoming Interface	Select *internal*. The interface that connects to the private network behind this FortiGate unit.
Source Address	Select *Finance_network* when configuring FortiGate_1. Select *HR_network* when configuring FortiGate_2. The address name for the private network behind this FortiGate unit.
Outgoing Interface	Select *peer_1*. The VPN Tunnel (IPsec Interface) you configured earlier.
Destination Address	Select *HR_network* when configuring FortiGate_1. Select *Finance_network* when configuring FortiGate_2. The address name that you defined for the private network behind the remote peer.
Action	Select *ACCEPT*.
Enable NAT	Disable.
Comments	Allow Internal to remote VPN network traffic.

4. Configure any additional features such as UTM or traffic shaping you may want. (optional).
5. Select *Create New* to create another policy for the other direction.
6. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
7. Enter the following information, and select *OK*.

Incoming Interface	Select *peer_1*. The VPN Tunnel (IPsec Interface) you configured.
Source Address	Select *HR_network* when configuring FortiGate_1. Select *Finance_Network* when configuring FortiGate_2. The address name defined for the private network behind the remote peer.
Outgoing Interface	Select *internal*. The interface that connects to the private network behind this FortiGate unit.
Destination Address	Select *Finance_Network* when configuring FortiGate_1. Select *HR_network* when configuring FortiGate_2. The address name defined for the private network behind this FortiGate unit.

Action	Select *ACCEPT*.
Enable NAT	Disable.
Comments	Allow remote VPN network traffic to Internal.

8. Configure any additional features such as UTM or traffic shaping you may want. (optional).

Configuring a default route for VPN interface

All network traffic must have a static route to direct its traffic to the proper destination. Without a route, traffic will not flow even if the security policies are configured properly. You may need to create a static route entry for both directions of VPN traffic if your security policies allow bi-directional tunnel initiation.

To configure the route for a route-based VPN

1. On FortiGate_2, go to *Router* > *Static* > *Static Routes* and select *Create New*.

   For low-end FortiGate units, go to *System* > *Network* > *Routing* and select *Create New*.
2. Enter the following information, and then select *OK*:

Destination IP / Mask	10.21.101.0/24
Device	FGT2_to_FGT1_Tunnel
Gateway	Leave as default: 0.0.0.0.
Distance (Advanced)	Leave this at its default. If there are other routes on this FortiGate unit, you may need to set the distance on this route so the VPN traffic will use it as the default route. However, this normally happens by default because this route is typically a better match than the generic default route.

Creating policy-based VPN security policy

Define an IPsec security policy to permit communications between the source and destination addresses.

1. Go to *Policy* > *Policy* > *Policy*.
2. Select the *Policy Type* as *VPN* and leave the *Policy Subtype* as *IPsec*.
3. Complete the following:

Local Interface	Select *internal*. The interface that connects to the private network behind this FortiGate unit.
Local Protected Subnet	Select *Finance_network* when configuring FortiGate_1. Select *HR_network* when configuring FortiGate_2. The address name defined for the private network behind this FortiGate unit.
Outgoing VPN Interface	Select *wan1*. The FortiGate unit's public interface.

Remote Protected Subnet	Select *HR_network* when configuring FortiGate_1. Select *Finance_network* when configuring FortiGate_2. The address name that you defined in Step for the private network behind the remote peer.
VPN Tunnel	Select *Use Existing* and select *peer_1* from the *VPN Tunnel* drop-down list. Select *Allow traffic to be initiated from the remote site* to enable traffic from the remote network to initiate the tunnel.
Comments	Bidirectional policy-based VPN policy.

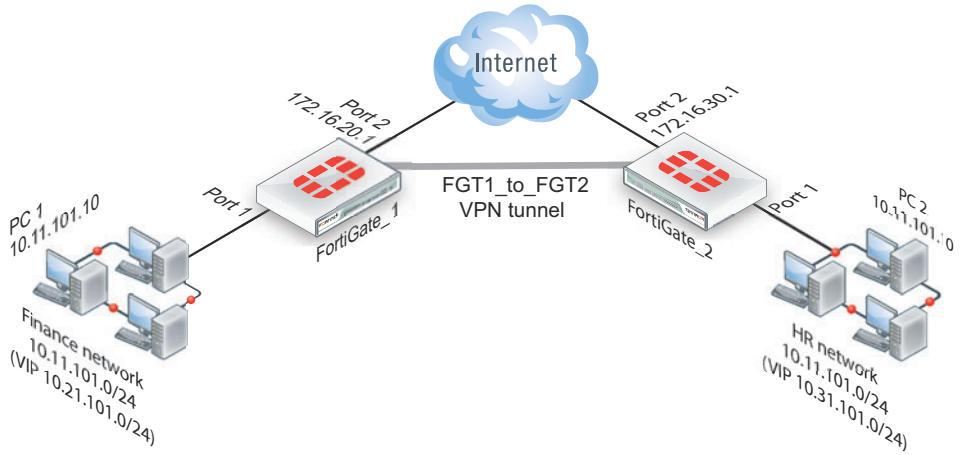
Place VPN policies in the policy list above any other policies having similar source and destination addresses.

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).

VIPs allow computers on those overlapping private subnets to each have another set of IP addresses that can be used without confusion. The FortiGate unit maps the VIP addresses to the original addresses. This means if PC1 starts a session with PC2 at 10.31.101.10, FortiGate_2 directs that session to 10.11.101.10 — the actual IP address of PC2. Figure 8 shows this — Finance network VIP is 10.21.101.0/24 and the HR network is 10.31.101.0/24.

Figure 8: Overlapped subnets example



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 `FGT1_to_FGT2`.
- Configure virtual IP (VIP) mapping:
  - the 10.21.101.0/24 network mapped to the 10.11.101.0/24 network on FortiGate_1
  - the 10.31.101.0/24 network mapped to the 10.11.101.0/24 network on FortiGate_2
- Configure an outgoing security policy with ordinary source NAT on both FortiGates.
- Configure an incoming security policy with the VIP as the destination on both FortiGates.
- Configure a route to the remote private network over the IPsec interface on both FortiGates.

To configure VIP mapping on both FortiGates

1. Go to *Firewall Objects* > *Virtual IPs* > *Virtual IPs* and select *Create New*.
2. Enter the following information, and select *OK*:

Name	Enter a name, for example, `my_vip`.
External Interface	Select `FGT1_to_FGT2`. The IPsec interface.
Type	Static NAT
External IP Address/Range	For the external IP address field enter: • `10.21.101.1` when configuring FortiGate_1, or • `10.31.101.1` when configuring FortiGate_2.
Mapped IP Address/Range	For the Mapped IP Address enter `10.11.101.1`. For the Range enter `10.11.101.254`.
Port Forwarding	Disable

Repeat this procedure on both FortiGate_1 and FortiGate_2.

To configure the outbound security policy on both FortiGates

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information, and select *OK*:

Incoming Interface	Select *Port 1*.
Source Address	Select *all*.
Outgoing Interface	Select *FGT1_to_FGT2*. The IPsec interface.
Destination Address	Select *all*.
Action	Select *ACCEPT*
Enable NAT	Enable

Repeat this procedure on both FortiGate_1 and FortiGate_2.

To configure the inbound security policy on both FortiGates

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information, and then select *OK*:

Incoming Interface	Select *FGT1_to_FGT2*.
Source Address	Select *all*.
Outgoing Interface	Select *Port 1*. The IPsec interface.
Destination Address	Select *my-vip*.
Action	Select *ACCEPT*
Enable NAT	Disable

Repeat this procedure on both FortiGate_1 and FortiGate_2.

To configure the static route for both FortiGates

1. Go to *Router* > *Static* > *Static Routes* and select *Create New*.
   For low-end FortiGate units, go to *System* > *Network* > *Routing* and select *Create New*.
2. Enter the following information, and then select *OK*:

Destination IP / Mask	Enter `10.31.101.0/24` when configuring FortiGate_1. Enter `10.21.101.0/24` when configuring FortiGate_2.
Device	Select *FGT1_to_FGT2*.
Gateway	Leave as default: 0.0.0.0.
Distance (Advanced)	Leave at default. If you have advanced routing on your network, you may have to change this value

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 10.31.101.10, and PC2 communicates with PC1 using IP address 10.21.101.10.

In this solution however, outbound NAT is used to translate the source address of packets from the 10.11.101.0/24 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 10.11.101.0/24 network.

For example, PC1 uses the destination address 10.31.101.10 to contact PC2. Outbound NAT on FortiGate_1 translates the PC1 source address to 10.21.101.10. At the FortiGate_2 end of the tunnel, the outbound NAT configuration translates the destination address to the actual PC2 address of 10.11.101.10. Similarly, PC2 replies to PC1 using destination address 10.21.101.10,

with the PC2 source address translated to 10.31.101.10. 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, 10.11.101.0/24.
- Define a firewall address for the remote private network:
  - define a firewall address for 10.31.101.0/24 on FortiGate_1
  - define a firewall address for 10.21.101.0/24 on FortiGate_2
- Configure an outgoing IPsec security policy with outbound NAT to map 10.11.101.0/24 source addresses:
  - to the 10.21.101.0/24 network on FortiGate_1
  - to the 10.31.101.0/24 network on FortiGate_2

To configure IPsec Phase 2 - CLI

```
config vpn ipsec phase2
  edit "FGT1_FGT2_p2"
    set keepalive enable
    set pfs enable
    set phase1name FGT1_to_FGT2
    set proposal 3des-sha1 3des-md5
    set replay enable
    set use-natip disable
  end
```

In this example, your phase 1 definition is named FGT1_to_FGT2. `use-natip` is set to `disable`, so 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`.

The `pfs` keyword ensures that perfect forward secrecy (PFS) is used. This ensures that each Phase 2 key created is unrelated to any other keys in use.

To define the local private network firewall address

1. Go to *Firewall Objects* > *Address* > *Addresses* and select *Create New*.
2. Enter the following information and select *OK*.

Name	Enter `vpn-local`. A meaningful name for the local private network.
Type	Subnet
Subnet / IP Range	10.11.101.0 255.255.255.0
Interface	Any

To define the remote private network firewall address

1. Go to *Firewall Objects* > *Address* > *Addresses* and select *Create New*.

2. Enter the following information, and select *OK*:

Name	Enter `vpn-remote`. A meaningful name for the remote private network.
Type	Subnet
Subnet / IP Range	`10.31.101.0 255.255.255.0` on FortiGate_1. `10.21.101.0 255.255.255.0` on FortiGate_2.
Interface	Any

To configure the IPsec security policy

In the CLI on FortiGate_1, enter the 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 "FGT1_to_FGT2"
    set natoutbound enable
    set natip 10.31.101.0 255.255.255.0
  end
```

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

Enter the same commands on FortiGate_2, but set natip be `10.21.101.0 255.255.255.0`.

Testing

The best testing is to look at the packets both as the VPN tunnel is negotiated, and when the tunnel is up.

To determine what the other end of the VPN tunnel is proposing

1. Start a terminal program such as puTTY and set it to log all output.

   When necessary refer to the logs to locate information when output is verbose.
2. Logon to the FortiGate unit using a super_admin account.
3. Enter the following CLI commands.
4. Display all the possible IKE error types and the number of times they have occurred:

   ```
   diag vpn ike errors
   ```

5. Check for existing debug sessions:
   ```
   diag debug info
   ```
   If a debug session is running, to halt it enter:
   ```
   diag debug disable
   ```
6. Confirm your proposal settings:
   ```
   diag vpn ike config list
   ```
7. If your proposal settings do not match what you expect, make a change to it and save it to force an update in memory. If that fixes the problem, stop here.
8. List the current vpn filter:
   ```
   diag vpn ike filter
   ```
9. If all fields are set to any, there are no filters set and all VPN ike packets will be displayed in the debug output. If your system has only a few VPNs, skip setting the filter.

   If your system has many VPN connections this will result in very verbose output and make it very difficult to locate the correct connection attempt.
10. Set the VPN filter to display only information from the destination IP address for example 10.10.10.10:
    ```
    diag vpn ike log-filter dst-addr4 10.10.10.10
    ```
    To add more filter options, enter them one per line as above. Other filter options are:

clear	**erase the current filter**
dst-addr6	the IPv6 destination address range to filter by
dst-port	the destination port range to filter by
interface	interface that IKE connection is negotiated over
list	display the current filter
name	the phase1 name to filter by
negate	negate the specified filter parameter
src-addr4	the IPv4 source address range to filter by
src-addr6	the IPv6 source address range to filter by
src-port	the source port range to filter by
vd	index of virtual domain. 0 matches all

11. Start debugging:
    ```
    diag debug app ike 255
    diag debug enable
    ```
12. Have the remote end attempt a VPN connection.

    If the remote end attempts the connection they become the initiator. This situation makes it easier to debug VPN tunnels because then you have the remote information and all of your local information. by initiate the connection, you will not see the other end's information.
13. If possible go to the web-based manager on your FortiGate unit, go to the VPN monitor and try to bring the tunnel up.
14. Stop the debug output:
    ```
    diag debug disable
    ```

15. Go back through the output to determine what proposal information the initiator is using, and how it is different from your VPN P1 proposal settings.

Things to look for in the debug output of attempted VPN connections are shown below.

Table 4: Important terms to look for in VPN debug output

`initiator`	Starts the VPN attempt, in the above procedure that is the remote end
`responder`	Answers the initiator's request
`local ID`	In aggressive mode, this is not encrypted
`error no SA proposal chosen`	There was no proposal match — there was no encryption-authentication pair in common, usually occurs after a long list of proposal attempts
`R U THERE and` `R U THERE ack`	dead peer detection (dpd), also known as dead gateway detection — after three failed attempts to contact the remote end it will be declared dead, no farther attempts will be made to contact it
`negotiation result`	lists the proposal settings that were agreed on
`SA_life_soft and SA_life_hard`	negotiating a new key, and the key life
`R U THERE`	If you see this, it means Phase 1 was successful
`tunnel up`	the negotiation was successful, the VPN tunnel is operational

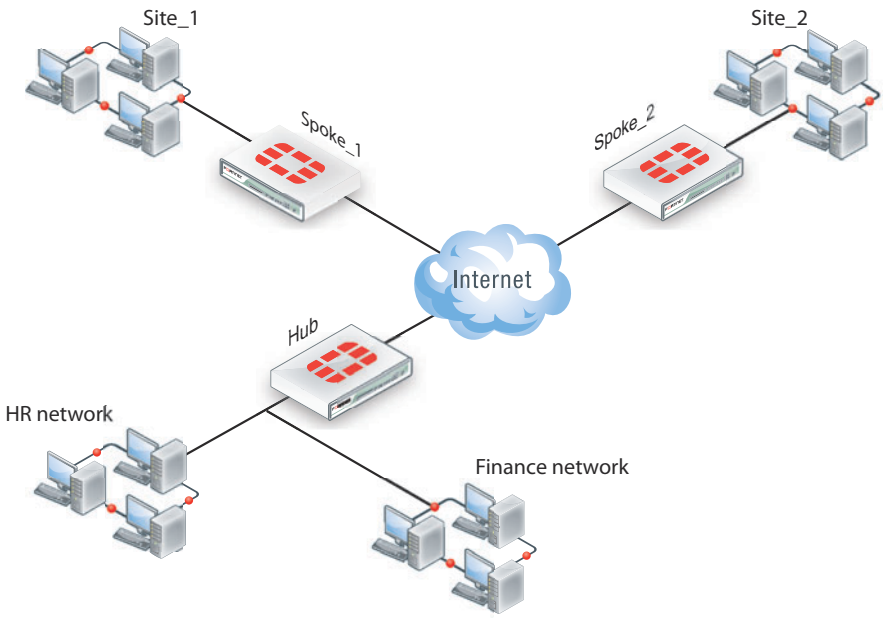
Hub-and-spoke configurations

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

Configuration overview

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 9: 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 mode and have a static public IP address.
- Spokes may have static IP addresses, dynamic IP addresses (see “FortiGate dialup-client configurations” on page 123), or static domain names and dynamic IP addresses (see “Dynamic DNS configuration” on page 94).

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 88 for an example of this configuration.

Protected networks addressing

The addresses of the protected networks are needed to configure destination selectors and sometimes for security 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

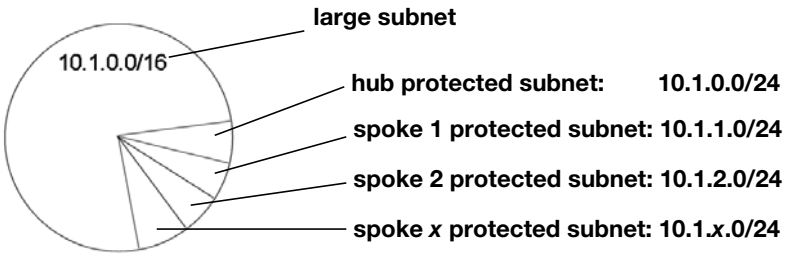
  or

- 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 10: Aggregated subnets



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

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

Each spoke uses the address of its own protected subnet as the IPsec source selector and as the source address in its VPN security 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 security policy.

For a route-based VPN, the destination of the VPN security 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 security 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 Endpoint 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 36. Enter these settings in particular:

Name	Enter a name to identify the VPN in phase 2 configurations, security 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 *Dynamic DNS* domain name. Either the hub or the spoke can establish the VPN connection. For more information, see "Dynamic DNS configuration" on page 94.
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 "Comparing policy-based or route-based VPNs" on page 19. 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 52. 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 security policies

1. Define a name for the address of the private network behind the hub. For more information, see "Defining policy addresses" on page 58.
2. Define names for the addresses or address ranges of the private networks behind the spokes. For more information, see "Defining policy addresses" on page 58.
3. Define the VPN concentrator. See "To define the VPN concentrator" on page 83.
4. Define security policies to permit communication between the hub and the spokes. For more information, see "Defining VPN security policies" on page 59.

Route-based VPN security policies

Define ACCEPT security policies to permit communications between the hub and the spoke. You need one policy for each direction.

To add policies

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.

3. Enter these settings in particular:

Incoming Interface	Select the VPN Tunnel (IPsec Interface) you configured in Step 1.
Source Address	Select the address name you defined in Step 2 for the private network behind the spoke FortiGate unit.
Outgoing Interface	Select the hub's interface to the internal (private) network.
Destination Address	Select the source address that you defined in Step 1.
Action	Select *ACCEPT*.
Enable NAT	Enable.

Incoming Interface	Select the VPN Tunnel (IPsec Interface) you configured in Step 1.
Source Address	Select the address name you defined in Step 2 for the private network behind the spoke FortiGate units.
Outgoing Interface	Select the source address that you defined in Step 1.
Destination Address	Select the hub's interface to the internal (private) network.

Action	Select *ACCEPT*.
Enable NAT	Enable.

Policy-based VPN security policy

Define an IPsec security policy to permit communications between the hub and the spoke.

To add policies

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Select the *Policy Type* as *VPN* and leave the *Policy Subtype* as *IPsec*.
3. Enter these settings in particular:

Local Interface	Select the hub's interface to the internal (private) network.
Local Protected Subnet	Select the source address that you defined in Step 1.
Outgoing VPN Interface	Select the hub's public network interface.
Remote Protected Subnet	Select the address name you defined in Step 2 for the private network behind the spoke FortiGate unit.
VPN Tunnel	Select *Use Existing* and select the name of the phase 1 configuration that you created for the spoke in Step 1. Select *Allow traffic to be initiated from the remote site* to enable traffic from the remote network to initiate the tunnel.

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 security 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.
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 security policy for the VPN, but you cannot apply UTM features to scan the traffic for security threats.
- put all of the IPsec interfaces into a zone and create a single zone-to-zone security policy
- create a security 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 UTM features using this method.

1. Go to *System* > *Network* > *Interfaces.*
2. Select the down-arrow on the *Create New* button and select *Zone*.
3. In the *Zone Name* field, enter a name, such as `Our_VPN_zone`.
4. Clear *Block intra-zone traffic*.
5. In the *Interface Members* list, select the IPsec interfaces that are part of your VPN.
6. 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 UTM features with just one security policy.

To create a zone for the VPN

1. Go to *System* > *Network* > *Interfaces.*
2. Select the down-arrow on the *Create New* button and select *Zone*.
3. In the *Zone Name* field, enter a name, such as `Our_VPN_zone`.
4. Select *Block intra-zone traffic*.

5. In the *Interface Members* list, select the IPsec interfaces that are part of your VPN.
6. Select *OK*.

To create a security policy for the zone

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the settings: and select *OK*.

Incoming Interface	Select the zone you created for your VPN.
Source Address	Select *All*.
Outgoing Interface	Select the zone you created for your VPN.
Destination Address	Select *All*.
Action	Select *ACCEPT*.
Enable NAT	Enable.

Using security policies as a concentrator

To enable communication between two spokes, you need to define an ACCEPT security policy for them. To allow either spoke to initiate communication, you must create a policy for each direction. This procedure describes a security 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 policy addresses" on page 58.
2. Go to *Policy* > *Policy* > *Policy* and select *Create New.*
3. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
4. Enter the settings and select *OK*.

Incoming Interface	Select the IPsec interface that connects to Spoke 1.
Source Address	Select the address of the private network behind Spoke 1.
Outgoing Interface	Select the IPsec interface that connects to Spoke 2.
Destination Address	Select the address of the private network behind Spoke 2.
Action	Select *ACCEPT*.
Enable NAT	Enable.

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 Endpoint Security.

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

To create the phase 1 and phase_2 configurations

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 36. Enter these settings:

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 52. 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 security policies for hub-to-spoke communication

1. Create an address for this spoke. See "Defining policy addresses" on page 58. Enter the IP address and netmask of the private network behind the spoke.
2. Create an address to represent the hub. See "Defining policy addresses" on page 58. Enter the IP address and netmask of the private network behind the hub.
3. Define the security policy to enable communication with the hub.

Route-based VPN security policy

Define two security policies to permit communications to and from the hub.

1. Go to *Policy* > *Policy* > *Policy* and select *Create New.*
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter these settings:

Incoming Interface	Select the virtual IPsec interface you created.
Source Address	Select the hub address you defined in Step 1.
Outgoing Interface	Select the spoke's interface to the internal (private) network.
Destination Address	Select the spoke addresses you defined in Step 2.
Action	Select *ACCEPT*.
Enable NAT	Enable

Incoming Interface	Select the spoke's interface to the internal (private) network.
Source Address	Select the spoke address you defined in Step 1.
Outgoing Interface	Select the virtual IPsec interface you created.
Destination Address	Select the hub destination addresses you defined in Step 2.

Action	Select *ACCEPT*.
Enable NAT	Enable

Policy-based VPN security policy

Define an IPsec security policy to permit communications with the hub. See "Defining VPN security policies" on page 59.

1. Go to *Policy* > *Policy* > *Policy* and select *Create New.*
2. Select the *Policy Type* as *VPN* and leave the *Policy Subtype* as *IPsec*.
3. Enter these settings in particular:

Local Interface	Select the spoke's interface to the internal (private) network.
Local Protected Subnet	Select the spoke address you defined in Step 1.
Outgoing VPN Interface	Select the spoke's interface to the external (public) network.
Remote Protected Subnet	Select the hub address you defined in Step 2.
VPN Tunnel	Select *Use Existing* and select the name of the phase 1 configuration you defined. Select *Allow traffic to be initiated from the remote site* to enable traffic from the remote network to initiate the tunnel.

Configuring security policies for spoke-to-spoke communication

Each spoke requires security policies to enable communication with the other spokes. Instead of creating separate security policies for each spoke, you can create an address group that contains the addresses of the networks behind the other spokes. The security 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.
2. Define the security policy to enable communication between this spoke and the spokes in the address group you created.

   Policy-based VPN security policy

   Define an IPsec security policy to permit communications with the other spokes. See "Defining VPN security policies" on page 59. Enter these settings in particular:

Route-based VPN security policy

Define two security policies to permit communications to and from the other spokes.

1. Go to *Policy* > *Policy* > *Policy* and select *Create New.*
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter these settings in particular:

Incoming Interface	Select the virtual IPsec interface you created.
Source Address	Select the spoke address group you defined in Step 1.
Outgoing Interface	Select the spoke's interface to the internal (private) network.

Destination Address	Select this spoke's address name.
Action	Select *ACCEPT.*
Enable NAT	Enable

4. Select *Create New*, leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*, and enter these settings:

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

Policy-based VPN security policy

1. Go to *Policy* > *Policy* > *Policy* and select *Create New.*
2. Select the *Policy Type* as *VPN* and leave the *Policy Subtype* as *IPsec*.
3. Enter the following:

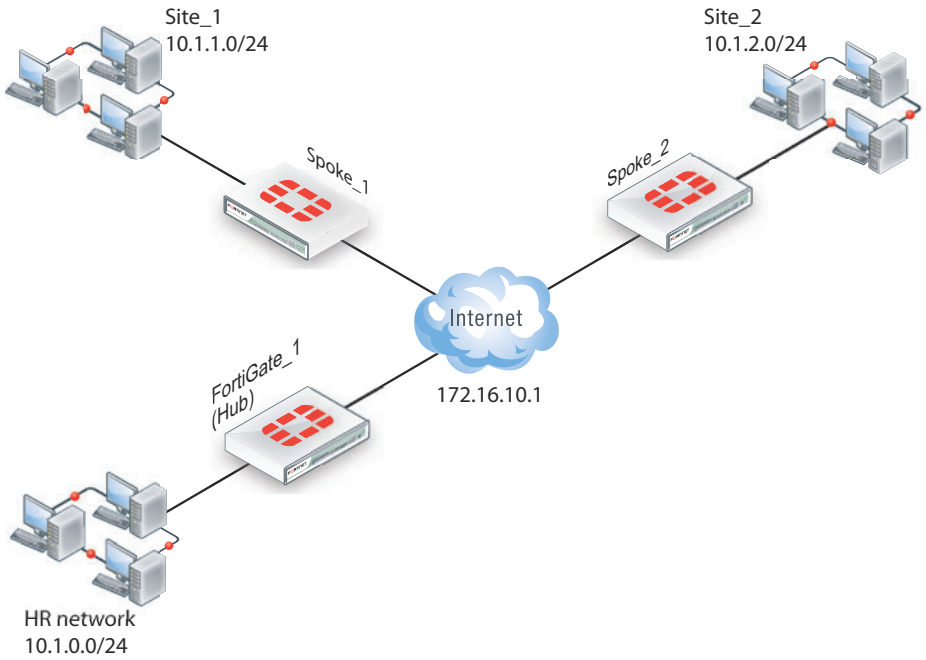
Local Interface	Select this spoke's internal (private) network interface.
Local Protected Subnet	Select this spoke's source address.
Outgoing VPN Interface	Select the spoke's interface to the external (public) network.
Remote Protected Subnet	Select the spoke address group you defined in Step 1.
VPN Tunnel	Select *Use Existing* and select the name of the phase 1 configuration you defined. Select *Allow traffic to be initiated from the remote site* to enable traffic from the remote network to initiate the tunnel.

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 11: 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 best practices dictates that it only be known by network administrators. For optimum protection against currently known attacks, each key must 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 (IKE)*.
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	Enter 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 (IKE)*.
2. 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 security policies

security 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 security 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 Objects* > *Address* > *Addresses*.
2. Select *Create New*, enter the following information, and select *OK*:

Name	Enter an address name (for example, `HR_Network`).

Type	Subnet
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 Objects* > *Address* > *Addresses*.
2. Select *Create New*, enter the following information, and select *OK*:

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

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

1. Go to *Policy* > *Policy* > *Policy*. and select *Create New*,
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information, and select *OK*:

Incoming Interface	Select the interface to the HR network, *port 1*.
Source Address	Select *HR_Network*.
Outgoing Interface	Select the virtual IPsec interface that connects to the spokes, `toSpokes`.
Destination Address	Select *Spoke_net*.
Action	Select *ACCEPT*.

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 security policy.

To create a zone for the VPN

1. Go to *System* > *Network* > *Interfaces.*
2. Select the down-arrow on the *Create New* button and select *Zone*.
3. In the *Zone Name* field, enter a name, such as `Our_VPN_zone`.
4. Select *Block intra-zone traffic*.

   You could enable intra-zone traffic and then you would not need to create a security policy. But, you would not be able to apply UTM features.
5. In *Interface Members*, select the virtual IPsec interface, `toSpokes`.
6. Select *OK*.

To create a security policy for the zone

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter these settings:

Incoming Interface	Select `Our_VPN_zone`.
Source Address	Select *All*.
Outgoing Interface	Select `Our_VPN_zone`.
Destination Address	Select *All*.
Action	Select *ACCEPT*.
Enable NAT	Enable.

4. 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 security 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 (IKE)*.
2. Select *Create Phase 1*, enter the following information, and select *OK*:

Name	Type a name, for example, `toHub`.
Remote Gateway	Select *Static IP Address*.
IP Address	Enter `172.16.10.1`.
Local Interface	Select *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	Select *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 (IKE)*.
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 security policies

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

To define the IP address of the network behind the spoke

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

Address Name	Enter an address name, for example `LocalNet`.
Type	Subnet
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 Objects* > *Address* > *Addresses*.
2. Select *Create New*, enter the following information, and select *OK*:

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

To define the security policy

1. Go to *Policy* > *Policy* > *Policy* and select *Create New.*

2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following and select *OK*:

Incoming Interface	Select the virtual IPsec interface, `toHub`.
Source Address	Select the aggregate protected network address `Spoke_net`.
Outgoing Interface	Select the interface to the internal (private) network, `port1`.
Destination Address	Select the address for this spoke's protected network `LocalNet`.
Action	Select *ACCEPT*.

4. Select *Create New*.
5. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
6. Enter the following information, and select *OK*:

Incoming Interface	Select the interface to the internal private network, `port1`.
Source Address	Select the address for this spoke's protected network, `LocalNet`.
Outgoing Interface	Select the virtual IPsec interface, `toHub`.
Destination Address	Select the aggregate protected network address, `Spoke_net`.
Action	Select *ACCEPT*.

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

Dynamic DNS configuration

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 domain name and a dynamic IP address.

The following topics are included in this section:

Dynamic DNS over VPN concepts

A typical computer has a static IP address and one or more DNS servers to resolve fully qualified domain names (FQDN) into IP addresses. A domain name assigned to this computer is resolved by any DNS server having an entry for the domain name and its static IP address. The IP address never changes or changes only rarely so the DNS server can reliably say it has the correct address for that domain all the time.

Dynamic DNS (DDNS)

It is different when a computer has a dynamic IP address, such as an IP address assigned dynamically by a DHCP server, and a domain name. Computers that want to contact this computer do not know what its current IP address is. To solve this problem there are dynamic DNS servers. These are public servers that store a DNS entry for your computer that includes its current IP address and associated domain name. These entries are kept up to date by your computer sending its current IP address to the dynamic DNS (DDNS) server to ensure its entry is always up to date. When other computers want to contact your domain, their DNS gets your IP address from your DDNS server. To use DDNS servers, you must subscribe to them and usually pay for their services.

When configuring DDNS on your FortiGate unit, go to *System* > *Network* > *DNS* and enable *Enable FortiGuard DDNS*. Then select the interface with the dynamic connection, which DDNS server you have an account with, your domain name, and account information. If your DDNS server is not on the list, there is a generic option where you can provide your DDNS server information.

Routing

When an interface has some form of changing IP address (DDNS, PPPoE, or DHCP assigned address), routing needs special attention. The standard static route cannot handle the changing IP address. The solution is to use the dynamic-gateway command in the CLI. Say for example you already have four static routes, and you have a PPPoE connection over the wan2 interface and you want to use that as your default route.

The route is configured on the dynamic address VPN peer trying to access the static address FortiGate unit.

To configure dynamic gateway routing - CLI

```
config router static
  edit 5
    set dst 0.0.0.0 0.0.0.0
    set dynamic-gateway enable
    set device wan2
  next
end
```

For more information on DDNS, see the *System Administration guide*.

Dynamic DNS over VPN

IPsec VPN expects an IP address for each end of the VPN tunnel. All configuration and communication with that tunnel depends on the IP addresses as reference points. However, when the interface the tunnel is on has DDNS enabled there is no set IP address. The remote end of the VPN tunnel now needs another way to reference your end of the VPN tunnel. This is accomplished using Local ID.

A FortiGate unit that has a domain name and a dynamic IP address can initiate VPN connections anytime. The remote peer can reply to the local FortiGate unit using the source IP address that was sent in the packet header because it is current. Without doing a DNS lookup first, the remote peer runs the risk of the dynamic IP changing before it attempts to connect. To avoid this, the remote peer must perform a DNS lookup for the domain name of to be sure of the dynamic IP address before initiating the connection.

Remote Gateway

When configuring the Phase 1 entry for a VPN tunnel, the Remote Gateway determines the addressing method the remote end of the tunnel uses as one of Static IP Address, Dialup User, or Dynamic DNS. There are different fields for each option.

When you select the Dynamic DNS VPN type there is a related field called Dynamic DNS. The Dynamic DNS field is asking for the FQDN of the remote end of the tunnel. It uses this information to look up the IP address of the remote end of the tunnel through the DDNS server associated with that domain name.

Local ID (peer ID)

The Local ID or peer ID can be used to uniquely identify one end of a VPN tunnel. This enables a more secure connection. Also if you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect. When you configure it on your end, it is your Local ID. When the remote end connects to you, they see it as your peer ID.

If you are debugging a VPN connection, the Local ID is part of the VPN negotiations. You can use it to help troubleshoot connection problems.

To configure your Local ID

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)*.
2. Select *Create New Phase 1* or edit an existing Phase 1 entry.
3. Select *Advanced*.
4. In the *P1 Proposal* section, enter your Local ID.
5. Select *OK*.

The default configuration is to accept all local IDs (peer IDs). If you have the Local ID set, the remote end of the tunnel must be configured to accept your Local ID.

To accept a specific Peer ID

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)*.
2. Select *Create New Phase 1.*
3. Select *Aggressive mode*.
4. For *Peer Options*, select *Accept this peer ID*. This option becomes visible only when Aggressive mode is selected.
5. Enter the string the other end of the tunnel used for its Local ID.
6. Configure the rest of the Phase 1 entry as required.
7. Select *OK*.

Route-based or policy-based VPN

VPN over dynamic DNS can be configured with either route-based or policy-based VPN settings. Both are valid, but have differences in configuration. Choose the best method based on your requirements. For more information on route-based and policy-based, see "Types of VPNs" on page 18.

Route-based VPN configuration requires two security policies to be configured (one for each direction of traffic) to permit traffic over the VPN virtual interface, and you must also add a static route entry for that VPN interface or the VPN traffic will not reach its destination. See "Creating branch_2 route-based security policies" on page 101 and "Creating branch_1 route-based security policies" on page 105.

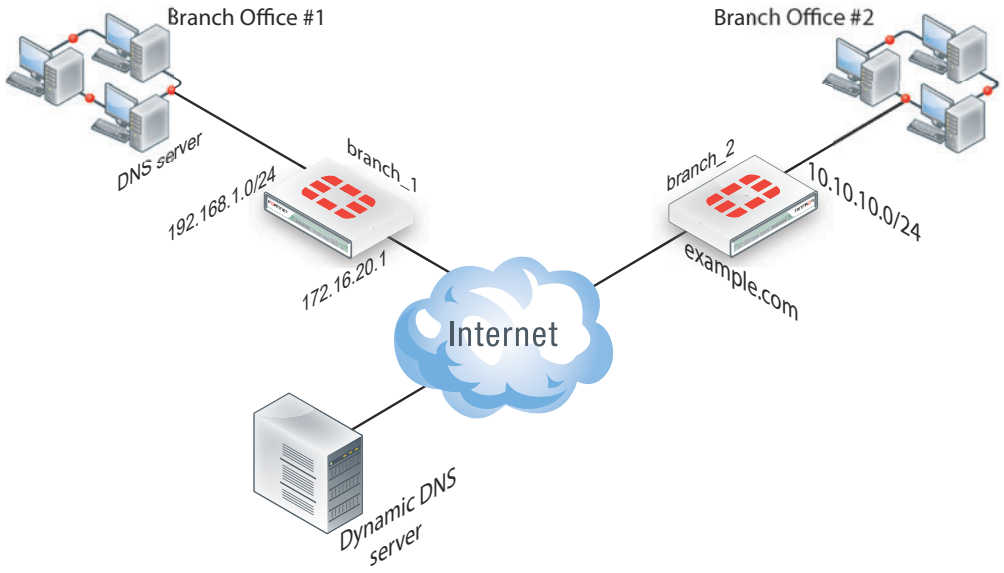
Policy-based VPN configuration uses more complex and often more IPsec security policies, but does not require a static route entry. It has the benefit of being able to configure multiple policies for handling multiple protocols in different ways, such as more scanning of less secure protocols or guaranteeing a minimum bandwidth for protocols such as VoIP. See "Creating branch_2 policy-based security policies" on page 102 and "Creating branch_1 policy-based security policies" on page 106

Dynamic DNS topology

In this scenario, two branch offices each have a FortiGate unit and are connected in a gateway-to-gateway VPN configuration. One FortiGate unit has a domain name (example.com) with a dynamic IP address. See `branch_2` in Figure 12.

Whenever the `branch_2` 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. The unit has its domain name registered with a dynamic DNS service. The `branch_2` unit checks in with the DDNS server on a regular basis, and that server provides the DNS information for the domain name, updating the IP address from time to time. Remote peers have to locate the `branch_2` FortiGate unit through a DNS lookup each time to ensure the address they get is current and correct.

Figure 12: Example dynamic DNS configuration



When a remote peer (such as the `branch_1` FortiGate unit in Figure 12) initiates a connection to `example.com`, the local DNS server looks up and returns the IP address that matches the domain name `example.com`. The remote peer uses the retrieved IP address to establish a VPN connection with the `branch_2` FortiGate unit.

Assumptions

- You have administrator access to both FortiGate units.
- Both FortiGate units have interfaces named wan1 and internal. (If not, you can use the alias feature to assign these labels as “nicknames” to other interfaces to follow this example.)
- Both FortiGate units have the most recent firmware installed, have been configured for their networks, and are currently passing normal network traffic.
- The `branch_2` FortiGate unit has its `wan1` interface defined as a dynamic DNS interface with the domain name of *example.com*.
- A basic gateway-to-gateway configuration is in place (see “Gateway-to-gateway configurations” on page 64) except one of the FortiGate units has a static domain name and a dynamic IP address instead of a static IP address.
- The FortiGate unit with the domain name is subscribed 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 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 security policy permits the connection, the FortiGate unit establishes the tunnel using IPsec phase 2 parameters and applies the security policy. Key management, authentication, and security services are negotiated dynamically through the IKE protocol.

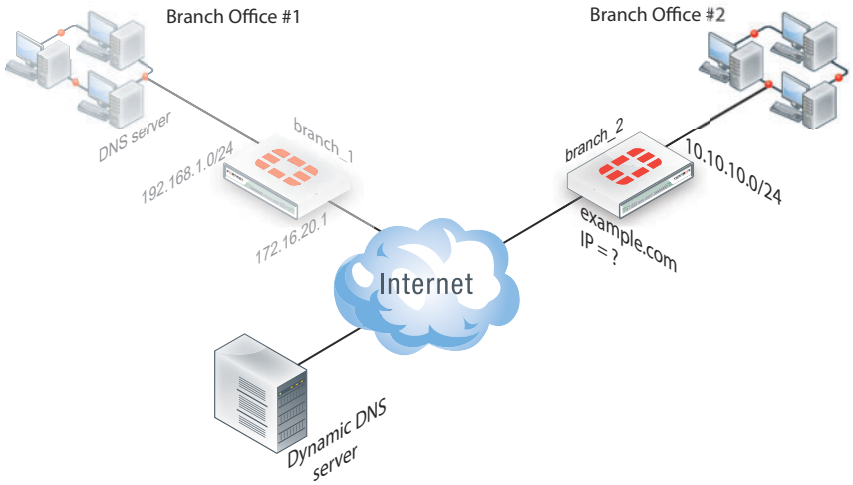
To support these functions, the following general configuration steps must be performed:

- Configure the branch_2 FortiGate unit with the dynamic IP address. This unit uses a Local ID string instead of an IP address to identify itself to the remote peer. See "Configure the dynamically-addressed VPN peer" on page 98.
  - Configuring branch_2 VPN tunnel settings
  - Configuring branch_2 security policies
- Configure the fixed-address VPN peer. To initiate a VPN tunnel with the dynamically-addressed peer, this unit must first retrieve the IP address for the domain from the dynamic DNS service. See "Configure the fixed-address VPN peer" on page 103.
  - Configuring branch_1 VPN tunnel settings
  - Configuring branch_1 security policies

Configure the dynamically-addressed VPN peer

It is assumed that this FortiGate unit (`branch_2`) has already had its public facing interface, for example the `wan1`, configured with the proper dynamic DNS configuration.

Figure 13: Configure branch_2, the dynamic address side



Configuring the dynamically-addressed VPN peer includes:

- Configuring branch_2 VPN tunnel settings
- Configuring branch_2 security policies

Configuring branch_2 VPN tunnel settings

Define the phase 1 parameters needed to establish a secure connection with the remote peer. See "Auto Key phase 1 parameters" on page 36. During this procedure you need to choose if you will be using route-based or policy-based VPNs.

To configure branch_2 VPN tunnel settings

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)*.
2. Select *Create New Phase 1*.

3. Enter the following information.

Name	Enter `branch_2`, a name to identify the VPN tunnel. This name appears in phase 2 configurations, security policies, and the VPN monitor.
Remote Gateway	Select *Static IP Address*. The remote peer this FortiGate is connecting to has a static IP public address. If the remote interface is PPPoE do not select *Retrieve default gateway from server*.
IP Address	Enter `172.16.20.1`. The IP address of the public interface to the remote peer.
Enter 172.16.20.1 The IP address of the public interface to the remote peer.	Select *Aggressive*.

4. Select *Advanced* and complete the following:

Enable IPsec Interface Mode	Enable for a route-based VPN and when configuring policies, go to "Creating branch_2 route-based security policies" on page 101. Disable for a policy-based VPN and when configuring policies, go to "Creating branch_2 policy-based security policies" on page 102. If enabled, default settings are used.
Local ID	Enter `example.com`. A character string used by the `branch_2` FortiGate unit to identify itself to the remote peer. This value must be identical to the value in the *Accept this peer ID* field of the phase 1 remote gateway configuration on the branch_1 remote peer. See "Configuring branch_1 VPN tunnel settings" on page 103.

5. Select *Create Phase 2*.

   Define the phase 2 parameters needed to create a VPN tunnel with the remote peer. For details on phase 2, see "Phase 2 parameters" on page 52.

6. Enter the following information and select *OK*.

Name	Enter `branch_2_phase2`. A name to identify this phase 2 configuration.
Phase 1	Select `branch_2`. The name of the phase 1 configuration that you defined earlier.

Configuring branch_2 security policies

Define security policies to permit communications between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different security policies. For detailed information about creating security policies, see “Defining VPN security policies” on page 59.

After defining the two address ranges, select one of “Creating branch_2 route-based security policies” on page 101 or “Creating branch_2 policy-based security policies” on page 102 to configure the appropriate VPN policies.

Define address ranges for branch_2 security policies

Define VPN connection names for the address ranges of the private networks. These addresses are used in the security policies that permit communication between the networks. For more information, see “Defining policy addresses” on page 58.

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

To define branch_2 address ranges

1. Go to *Firewall Objects* > *Address* > *Addresses*.
2. Select *Create New*.
3. Enter the following information, and select *OK*.

Name	Enter `branch_2_internal`. Enter a meaningful name.
Type	Select *Subnet*.
Subnet / IP Range	Enter `10.10.10.0/24`. Include the netmask or specify a specific range.
Interface	Select *internal*. The interface that will be handling the traffic from the internal network.

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

4. Select *Create New*.
5. Enter the following information, and select *OK*.

Name	Enter `branch_1_internal`. A meaningful name for the private network at the remote end of the VPN tunnel.
Type	Select *Subnet*.
Subnet / IP Range	Enter `192.168.1.0/24`. Include the netmask. Optionally you can specify a range
Interface	Select *any*. The interface that will be handling the remote VPN traffic on this FortiGate unit. If you are unsure, or multiple interfaces may be handling this traffic use `any`.

Creating branch_2 route-based security policies

Define ACCEPT security policies to permit communication between the branch_2 and branch_1 private networks. Once the route-based policy is configured a routing entry must be configured to route traffic over the VPN interface.

Define a policy to permit the branch_2 local FortiGate unit to initiate a VPN session with the branch_1 VPN peer.

To create route-based security policies

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information, and select *OK*.

Incoming Interface	Select *internal*. The interface that connects to the private network behind this FortiGate unit.
Source Address	Select *branch_2_internal*. Select the address name for the private network behind this FortiGate unit.
Outgoing Interface	Select *branch_2*. The VPN Tunnel (IPsec Interface).
Destination Address	Select *branch_1_internal*. The address name the private network behind the remote peer.
Action	Select *ACCEPT*.
Enable NAT	Disable.
Comments	Route-based: Initiate a branch_2 to branch_1 VPN tunnel.

Define a policy to permit the branch_1 remote VPN peer to initiate VPN sessions.

1. Select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information, and select *OK*.

Incoming Interface	Select *branch_2*. The VPN Tunnel (IPsec Interface).
Source Address	Select *branch_1_internal*. The address name for the private network behind the remote peer.
Outgoing Interface	Select *internal*. The interface connecting the private network behind this FortiGate unit.
Destination Address	Select *branch_2_internal*. The address name for the private network behind this FortiGate unit.
Action	Select *ACCEPT*.
Enable NAT	Disable.
Comments	Route-based: Initiate a branch_1 to branch_2 internal VPN tunnel.

4. Optionally configure any other security policy settings you require such as UTM or traffic shaping for this policy.
5. Place these policies in the policy list above any other policies having similar source and destination addresses. This will ensure VPN traffic is matched against the VPN policies before any other policies.

To create routing entry for VPN interface - CLI

```
config router static
  edit 5
    set dst 0.0.0.0 0.0.0.0
    set dynamic-dateway enable
    set device wan1
  next
end
```

This routing entry must be added in the CLI because the dynamic-gateway option is not available in the web-based manager.

Creating branch_2 policy-based security policies

Define an IPsec policy to permit VPN sessions between the private networks. Define an IPsec policy to permit the VPN sessions between the local branch_2 unit and the remote branch_1 unit.

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Select the *Policy Type* as *VPN* and leave the *Policy Subtype* as *IPsec*.
3. Enter the following information, and select *OK*.

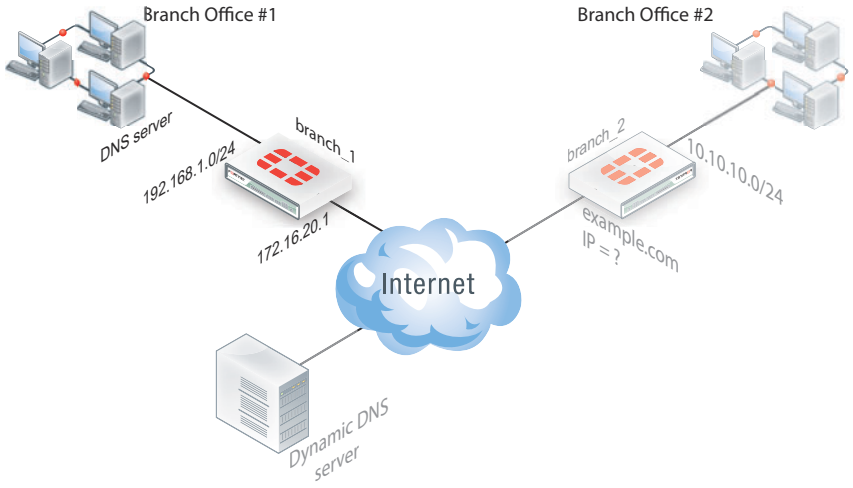
Local Interface	Select *internal*. The interface connecting the private network behind this FortiGate unit.
Local Protected Subnet	Select *branch_2_internal*. The address name for the private network behind this local FortiGate unit.
Outgoing VPN Interface	Select *wan1*. The FortiGate unit's public interface.
Remote Protected Subnet	Select *branch_1_internal*. The address name for the private network behind branch_1, the remote peer.
VPN Tunnel	Select *Use Existing* and select *branch_2* from the drop-down list. The name of the phase 1 tunnel.
	Select *Allow traffic to be initiated from the remote site*.
Comments	Policy-based: allows traffic in either direction to initiate the VPN tunnel.

4. Optionally configure any other security policy settings you require such as UTM or traffic shaping for this policy.
5. Place these policies in the policy list above any other policies having similar source and destination addresses. This will ensure VPN traffic is matched against the VPN policies before any other policies.

Configure the fixed-address VPN peer

The fixed-address VPN peer, branch_1, needs to retrieve the IP address from the dynamic DNS service to initiate communication with the dynamically-addressed peer, branch_2. It also depends on the peer ID (local ID) to initiate the VPN tunnel with branch_2.

Figure 14: Configure branch_1, the fixed address side



Configuring the fixed-address VPN peer includes:

- Configuring branch_1 VPN tunnel settings
- Configuring branch_1 security policies

Configuring branch_1 VPN tunnel settings

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 36.

To configure branch_1 phase 1 VPN settings

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)*.
2. Select *Create New Phase 1*.
3. Enter the following information and select *OK*.

Name	Enter `branch_1`. A name to identify the VPN tunnel. This name appears in phase 2 configurations, security policies and the VPN monitor.
Remote Gateway	Select *Dynamic DNS*. The remote peer this FortiGate is connecting to has a dynamic IP address.
Dynamic DNS	Type the fully qualified domain name of the remote peer (for example, `example.com`).
Interface	Select *wan1*. The public facing interface on the fixed-address FortiGate unit.
Mode	Select *Aggressive*.

Peer Options	Select *Accept this peer ID*, and enter `example.com`. This option only appears when the mode is set to Aggressive. The identifier of the FortiGate unit with the dynamic address.
Enable IPsec Interface Mode	Enable for a route-based VPN and when configuring policies, go to "Creating branch_1 route-based security policies" on page 105. Disable for a policy-based VPN and when configuring policies, go to "Creating branch_1 policy-based security policies" on page 106. If Interface mode is enabled, default settings are used.

4. Define the phase 2 parameters needed to create a VPN tunnel with the remote peer. See "Phase 2 parameters" on page 52. Enter these settings in particular:

Name	Enter `branch_1_p2`. A name to identify this phase 2 configuration.
Phase 1	Select *branch_1*. 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.

Configuring branch_1 security policies

The `branch_1` FortiGate unit has a fixed IP address and will be connecting to the `branch_2` FortiGate unit that has a dynamic IP address and a domain name of `example.com`. Remember if you are using route-based security policies that you must add a route for the VPN traffic.

Defining address ranges for branch_1 security policies

As with `branch_2` previously, `branch_1` needs address ranges defined as well. See "Defining policy addresses" on page 58.

1. Go to *Firewall Objects* > *Address* > *Addresses*.
2. Select *Create New*.
3. Enter the following information, and select *OK*.

Name	Enter `branch_2_internal`. A meaningful name for the private network behind the `branch_2` FortiGate unit.
Type	Select *Subnet*.
Subnet / IP Range	Enter `10.10.10.0/24`. Include the netmask or specify a specific range.
Interface	Select *internal*. This is the interface on this FortiGate unit that will be handling with this traffic.

4. Define an address name for the IP address and netmask of the private network behind the remote peer.
5. Select *Create New*.

6. Enter the following information, and select *OK*.

Name	Enter `branch_1_internal`. A meaningful name for the private network behind the `branch_1` peer.
Type	Select *Subnet*.
Subnet / IP Range	Enter `192.168.1.0/24`. Include the netmask or specify a specific range.
Interface	Select *any*. The interface on this FortiGate unit that will be handling with this traffic. If you are unsure, or multiple interfaces may be handling this traffic use `any`.

Creating branch_1 route-based security policies

Define an ACCEPT security policy to permit communications between the source and destination addresses. See "Defining VPN security policies" on page 59.

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information, and select *OK*.

Incoming Interface	Select *internal*. The interface that connects to the private network behind the `branch_1` FortiGate unit.
Source Address	Select *branch_1_internal*. The address name that you defined for the private network behind this FortiGate unit.
Outgoing Interface	Select *branch_1*. The VPN Tunnel (IPsec Interface) you configured earlier.
Destination Address	Select *branch_2_internal*. The address name that you defined for the private network behind the `branch_2` peer.
Action	Select *ACCEPT*.
Enable NAT	Disable
Comments	Internal -> branch2

To permit the remote client to initiate communication, you need to define a security policy for communication in that direction.

4. Select *Create New*.
5. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
6. Enter the following information, and select *OK*.

Incoming Interface	Select *branch_1*. The VPN Tunnel (IPsec Interface) you configured earlier.
Source Address	Select *branch_2_internal*. The address name that you defined for the private network behind the `branch_2` remote peer.
Outgoing Interface	Select *internal*. The interface that connects to the private network behind this FortiGate unit.

Destination Address	Select *branch_1_internal*. The address name that you defined for the private network behind this FortiGate unit.
Action	Select *ACCEPT*.
Enable NAT	Disable
Comments	branch_2 -> Internal

Creating branch_1 policy-based security policies

A policy-based security policy allows you the flexibility to allow inbound or outbound traffic or both through this single policy.

This policy-based IPsec VPN security policy allows both inbound and outbound traffic

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Select the *Policy Type* as *VPN* and leave the *Policy Subtype* as *IPsec*.
3. Enter the following information, and select *OK*.

Local Interface	Select *internal*. The interface that connects to the private network behind this FortiGate unit.
Local Protected Subnet	Select *branch_1_internal*. The address name that you defined for the private network behind this FortiGate unit.
Outgoing VPN Interface	Select *wan1*. The FortiGate unit's public interface.
Remote Protected Subnet	Select *branch_2_internal*. The address name that you defined for the private network behind the remote peer.
VPN Tunnel	Select *Use Existing* and select *branch_1* from the drop-down list. Select *Allow traffic to be initiated from the remote site* to enable traffic from the remote network to initiate the tunnel.

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

Testing

Once both ends are configured, you can test the VPN tunnel.

To test the VPN initiated by branch_2

1. On branch_2, go to *VPN* > *Monitor* > *IPsec Monitor*.

   All IPsec VPN tunnels will be listed on this page, no matter if they are connected or disconnected.
2. Select the tunnel listed for branch_2, and select the status column for that entry.

   The status will say *Bring Up* and remote port, incoming and outgoing data will all be zero. This indicates an inactive tunnel. When you select *Bring Up*, the FortiGate will try to set up a VPN session over this tunnel. If it is successful, Bring Up will change to Active, and the arrow icon will change to a green up arrow icon.
3. If this does not create a VPN tunnel with increasing values for incoming and outgoing data, you need to start troubleshooting:

To test the VPN initiated by branch_1

1. On branch_1, go to *VPN* > *Monitor* > *IPsec Monitor*.
2. Select the tunnel listed for branch_1, and select the status column.

   The difference between branch_2 and branch_1 at this point is that the tunnel entry for branch-1 will not have a remote gateway IP address. It will be resolved when the VPN tunnel is started.
3. If this does not create a VPN tunnel with increasing values for incoming and outgoing data, you need to start troubleshooting.

Some troubleshooting ideas include:

- If there was no entry for the tunnel on the monitor page, check the Auto Key (IKE) page to verify the phase 1 and phase 2 entries exist.
- Check the security policy or policies, and ensure there is an outgoing policy as a minimum.
- Check that you entered a local ID in the phase 1 configuration, and that branch_1 has the same local ID.
- Ensure the local DNS server has an up-to-date DNS entry for exmaple.com.

For more information on VPN troubleshooting and testing, see “VPN troubleshooting tips” on page 228.

FortiClient dialup-client configurations

The FortiClient Endpoint Security application is an IPsec 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 Endpoint 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.

The following topics are included in this section:

Configuration overview

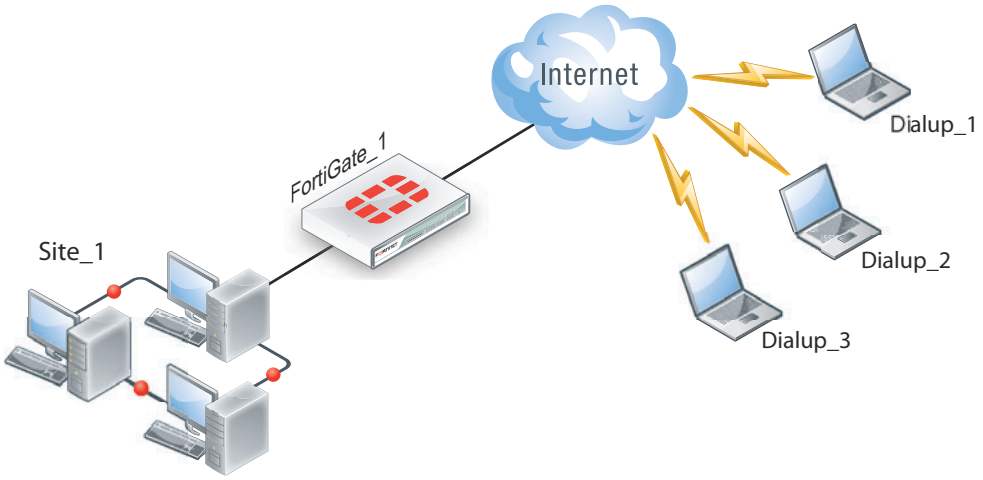
Dialup users typically obtain dynamic IP addresses from an ISP through Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol over Ethernet (PPPoE). Then, the FortiClient Endpoint Security application initiates a connection to a FortiGate dialup server.

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 traversal (NAT-T) compatible to pass encrypted packets (see “NAT traversal” on page 48). 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.

For a faster and easier method of configuring a FortiGate - to - FortiClient VPN, see “One button FortiGate - to - FortiClient Phase1 VPN” on page 110.

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 interface to download VPN settings from the FortiGate unit. See “Automatic configuration of FortiClient dialup clients” on page 109.

Figure 15: Example FortiClient dialup-client configuration



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 security policy associated with the tunnel permits access. If configured, the FortiGate unit could also require FortiClient registration, that is, the remote user would be required to have FortiClient installed before connection is completed.

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 41.

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.

One button FortiGate - to - FortiClient Phase1 VPN

On the FortiOS VPN IKE page there is a method to create a Phase1 portion of a VPN tunnel between the FortiGate and FortiClient. Very little information is required for this configuration. No encryption or authentication method is required. This feature is ideal for setting up quick VPN connections with basic settings.

On the Phase 1 screen (*VPN* > *IPsec* > *Phase 1*) is the option *Create a FortiClient VPN.* When selected, the FortiGate uint requires a few basic VPN configuration related questions. Once all the information is added, select *OK*. This will create a new dial-up IPsec-interface mode tunnel. Phase 1 and Phase 2 will be added using the default ike settings.

The following Settings will be used when creating a one-button FortiClient VPN Phase1 object:

- Remote Gateway: Dialup User
- Mode: Aggressive
- Enable IPSec Interface Mode
- Default setting for P1 and P2 Proposal
- XAUTH Enable as Server (Auto)
- IKE mode-config will be enabled
- Peer Option set to “Accept any peer ID”
- Rest of the setting use the current defaults (Default value needs to be the same on FCT side)

Once the completed, you need tocreate a default Phase2 configuration. This only requires a name for the Phase2 object, and select the FortiClient connection Phase1 name.

How the FortiGate unit determines which settings to apply

The FortiGate unit follows these steps to determine the configuration information to send to the FortiClient application:

1. Check the virtual domain associated with the connection to determine which VPN policies might apply.
2. Select the VPN policy that matches the dialup client’s user group and determine which tunnel (phase 1 configuration) is involved.
3. Check all IPsec security policies that use the specified tunnel to determine which private networks the dialup clients may access.
4. Retrieve the rest of the VPN policy information 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 Endpoint 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 security policies that allow access only to that source address range. If you do not use VIPs, the security 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*.

On the host computer, you can find out the VIP address that the FortiClient Endpoint Security application is using. For example, in Windows command prompt, type `ipconfig /all`

On Linux or Mac OS X, type `ifconfig` in a terminal window. The output will also show the IP address that has been assigned to the host Network Interface Card (NIC).

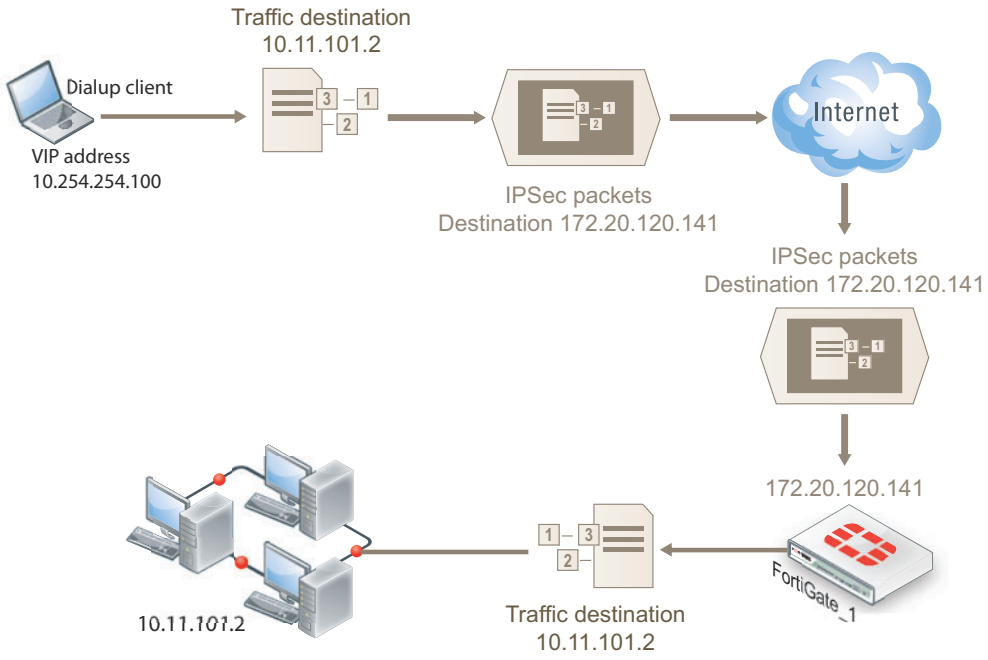
It is best to assign VIPs using DHCP over IPsec. The FortiGate dialup server can act as a DHCP server or relay requests to an external DHCP server. You can also configure VIPs manually on FortiClient applications, but it is more difficult to ensure that all clients use unique addresses.

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 54

FortiGate units fully support RFC 3456. The FortiGate DHCP over IPsec feature can be enabled to allocate VIP addresses to FortiClient dialup clients using a FortiGate DHCP server.

Figure 16 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 16:IP address assignments in a FortiClient dialup-client configuration



Assigning VIPs by RADIUS user group

If you use XAuth authentication, you can assign users the virtual IP address stored in the Framed-IP-Address field of their record on the RADIUS server. (See RFC 2865 and RFC 2866 for more information about RADIUS fields.) To do this:

- Set the DHCP server *IP Assignment Mode* to *User-group defined method*. This is an Advanced setting. See "To configure a DHCP server on a FortiGate interface" on page 116.
- Create a new firewall user group and add the RADIUS server to it.
- In your phase 1 settings, configure the FortiGate unit as an XAuth server and select from *User Group* the new user group that you created. For more information, see "Using the FortiGate unit as an XAuth server" on page 50.
- Configure the FortiClient application to use XAuth. See "Adding XAuth authentication" on page 117.

FortiClient dialup-client infrastructure requirements

- To support policy-based VPNs, the FortiGate dialup server may operate in either NAT mode or transparent mode. NAT 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 security 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:

1. 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.
2. Configure the FortiGate unit to act as a dialup server. See "Configure the FortiGate unit" on page 113.
3. 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.
4. Configure the dialup clients. See "Configure the FortiClient Endpoint Security application" on page 117.

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 FortiClient dialup clients automatically. For more information, see "Configuring the FortiGate unit as a VPN policy server" on page 116.

Configure the FortiGate unit

Configuring the FortiGate unit to establish VPN connections with FortiClient Endpoint 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 VIP addresses by DHCP over IPsec, configure an IPsec DHCP server or relay

The procedures in this section cover basic setup of policy-based and route-based VPNs compatible with FortiClient Endpoint Security. A route-based VPN is simpler to configure.

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 security policy

1. On 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 36. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel. This name appears in phase 2 configurations, security 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.

2. Define the phase 2 parameters needed to create a VPN tunnel with the FortiClient peer. See "Phase 2 parameters" on page 52. 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 security policies that permit communication between the networks. For more information, see "Defining policy addresses" on page 58.

   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 VIP addresses, define an address name for the subnet to which these VIPs belong.

4. Define security policies to permit communication between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different security policies. For detailed information about creating security policies, see "Defining VPN security policies" on page 59.

If the security policy, which grants the VPN Connection is limited to certain services, DHCP must be included, otherwise the client won't be able to retrieve a lease from the FortiGate's (IPSec) DHCP server, because the DHCP Request (coming out of the tunnel) will be blocked.

Route-based VPN security policies

Define an ACCEPT security policy to permit communications between the source and destination addresses.

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter these settings in particular:

Incoming Interface	Select the VPN Tunnel (IPsec Interface) you configured in Step 1.
Source Address	Select *All*.

Outgoing Interface	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address	Select *All*.
Action	Select *ACCEPT*.
Enable 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 security policy for communication in that direction.

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter these settings in particular:

Incoming Interface	Select the interface that connects to the private network behind this FortiGate unit.
Source Address	Select *All*.
Outgoing Interface	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address	Select *All*.
Action	Select *ACCEPT*.
Enable NAT	Disable.

Policy-based VPN security policy

Define an IPsec security policy to permit communications between the source and destination addresses.

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Select the *Policy Type* of *VPN* and leave the *Policy Subtype* as *IPsec*.
3. Enter these settings in particular:

Local Interface	Select the interface that connects to the private network behind this FortiGate unit.
Local Protected Subnet	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Outgoing VPN Interface	Select the FortiGate unit's public interface.
Remote Protected Subnet	If FortiClient users are assigned VIPs, select the address name that you defined in Step 3 for the VIP subnet. Otherwise, select *All*.
VPN Tunnel	Select *Use Existing* and select the name of the phase 1 configuration that you created in Step 1. Select *Allow traffic to be initiated from the remote site* to enable traffic from the remote network to initiate the tunnel.

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.
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 113. `<group_name>` must be the name of the user group your created for FortiClient users.

Configuring DHCP services on a FortiGate interface

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 a FortiGate interface" below).
- act as a DHCP server (see "To configure a DHCP server on a FortiGate interface" on page 116).

Note that DHCP services are typically configured during the interface creation stage, but you can return to an interface to modify DHCP settings if need be.

To configure DHCP relay on a FortiGate interface

1. Go to *System* > *Network* > *Interfaces* and select the interface that you want to relay DHCP.
2. Under *DHCP Server*, select *Enable* and create a new DHCP *Address Range* and *Netmask*.
3. Open the *Advanced...* menu and select *Relay* for the *Mode* option.
4. For the *Type*, select *IPsec*.
5. Select *OK*.

To configure a DHCP server on a FortiGate interface

1. Go to *System* > *Network* > *Interfaces* and select the interface that you want to act as a DHCP server.
2. Under *DHCP Server*, select *Enable* and create a new DHCP *Address Range* and *Netmask*.
3. For *Default Gateway*, enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
4. For *DNS Server*, select *Same as System DNS*. If you want to use a different DNS server for VPN clients, select *Specify* and enter an IP address in the available field.

5. Open the *Advanced...* menu and select *Server* for the *Mode* option.
6. For the *Type*, select *IPsec*.
7. Select *OK*.

Configure the FortiClient Endpoint Security application

The following procedure explains how to configure the FortiClient Endpoint Security application to communicate with a remote FortiGate dialup server using the VIP address that you specify manually. These procedures are based on FortiClient 5.0.

Configuring FortiClient

This procedure explains how to configure the FortiClient application manually using the default IKE and IPsec settings. For more information, refer to the *FortiClient Administration 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 *Remote Access* and select the down-arrow for the VPN connection.
2. Select *Add new connection* and complete following information:

VPN Type	Select *IPsec VPN.*
Connection Name	Enter a descriptive name for the connection.
Remote Gateway	Enter the IP address or the fully qualified domain name (FQDN) of the remote gateway.
Authentication Method	Select *Pre-shared Key*.
Pre-shared Key	Enter the pre-shared key.
User Name	Enter the user name to connect to the tunnel.

3. Select *OK*.

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 50. The following procedure explains how to configure the FortiClient application.

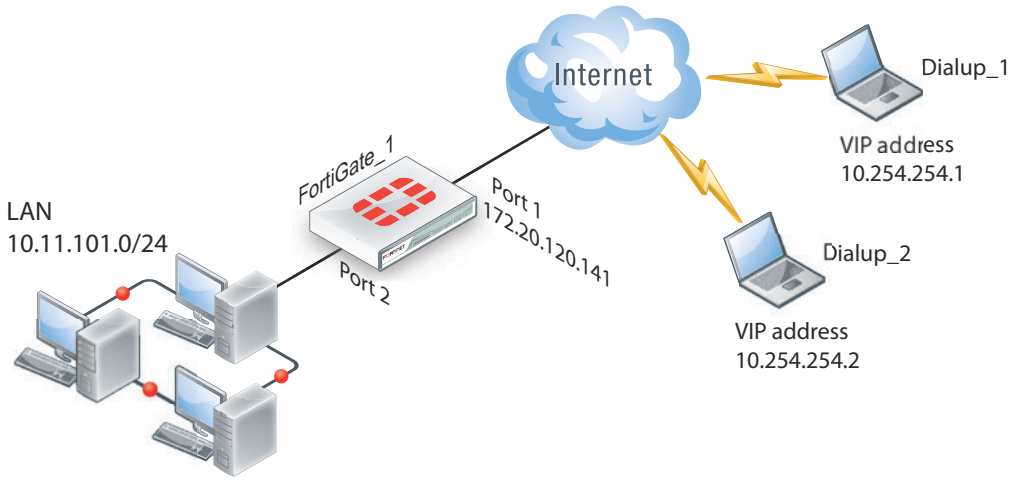
Note that XAuth is not compatible with IKE version 2.

For more information on configuring XAuth authentication, see the *FortiClient Administration Guide*.

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 Endpoint Security application so that the FortiClient Endpoint Security application can acquire a VIP address through the FortiGate DHCP server. Both route-based and policy-based solutions are covered.

Figure 17: 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 have access to the LAN behind FortiGate_1.
- The other network devices are assigned IP addresses as shown in Figure 17.

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 security policy permits the connection, the FortiGate unit establishes the tunnel using IPsec phase 2 parameters and applies the IPsec security 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 "To define the phase 1 parameters" on page 119.
- 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 "To define the phase 2 parameters" on page 119.
- Create security policy to control the permitted services and permitted direction of traffic between the IP source address and the dialup clients. See "To define the firewall addresses" on page 120.
- Configure the FortiGate unit to service DHCP requests from dialup clients. See "Configuring the FortiClient Endpoint Security application" on page 121.

To define the phase 1 parameters

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)*.
2. Select *Create Phase 1*, enter the following information, and select *OK*:

Name	todialups
Remote Gateway	Dialup User
Local Interface	Port 1
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	hardtoguess
Peer Options	Accept any peer ID
Advanced	Select
Enable IPsec Interface Mode	Enable for route-based VPN. Disable for policy-based VPN.

To define the phase 2 parameters

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)* and select *Create Phase 2*.
2. Select *Advanced*, enter the following information, and select *OK*:

Name	td_2
Phase 1	todialups
Advanced	DHCP-IPsec

To define the firewall addresses

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

Name	internal_net
Type	Subnet
Subnet/IP Range	10.11.101.0/24
Interface	Port 2

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

Name	dialups
Type	IP Range
Subnet/IP Range	10.254.254.1-10.254.254.10
Interface	Route-based VPN: todialups Policy-based VPN: Any

The security policies for route-based and policy-based VPNs are described in separate sections below.

To define security policies - route-based VPN

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information, and select *OK*:

Incoming Interface	todialups
Source Address	dialups
Outgoing Interface	Port 2
Destination Address	internal_net
Action	ACCEPT
Enable NAT	Disable

4. Select *Create New*.
5. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
6. Enter the following information, and select *OK*:

Incoming Interface	Port 2
Source Address	internal_net
Outgoing Interface	todialups
Destination Address	dialups

Action	ACCEPT
Enable NAT	Disable

7. Select *Create New*.
8. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
9. Enter the following information, and select *OK*:

Incoming Interface	Port 2
Source Address	internal_net
Outgoing Interface	todialups
Destination Address	all
Service	DHCP
Action	ACCEPT
Enable NAT	Disable

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

The policy in step 7 is required for DHCP to function properly for policy-based VPNs. You can omit this policy if you change the *Destination Address Name* to `all` in the step before. Route-based policies are not affected by this.

To define the security policy - policy-based VPN

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Select the *Policy Type* of *VPN* and leave the Policy Subtype as *IPsec*.
3. Enter the following information, and select *OK*:

Local Interface	Port 2
Local Protected Subnet	internal_net
Outgoing VPN Interface	Port 1
Remote Protected Subnet	dialups
VPN Tunnel	Select *Use Existing* and select *todialups* from the drop-down list.
Allow traffic to be initiated from the remote site	Enable

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

Configuring the FortiClient Endpoint Security application

The following procedure explains how to configure the FortiClient Endpoint 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. Go to *Remote Access* and select the down-arrow for the VPN connection.
2. Select *Add new connection* and complete following information:

VPN Type	Select *IPsec VPN.*
Connection Name	Headquarters.
Remote Gateway	The port1 IP address.
Authentication Method	Select *Pre-shared Key*.
Pre-shared Key	hardtoguess
User Name	Enter the user name to connect to the tunnel.

3. Select *OK*.

FortiGate dialup-client configurations

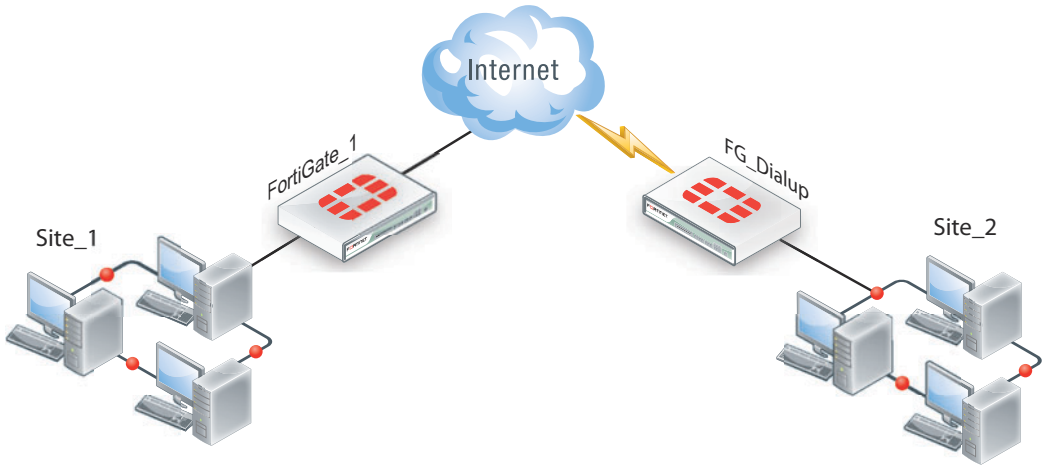
This section explains how to set up a FortiGate dialup-client IPsec VPN. In a FortiGate dialup-client configuration, a FortiGate unit with a static IP address acts as a dialup server and a FortiGate unit having a dynamic IP address initiates a VPN tunnel with the FortiGate dialup server.

The following topics are included in this section:

Configuration overview

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 18: 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 security 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, best practices dictate that you assign a unique identifier (local ID

or peer ID) to each FortiGate dialup client. For more information, see “Authenticating remote peers and clients” on page 41.

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 with user accounts and pre-shared keys” on page 44.

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.

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 48.

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.

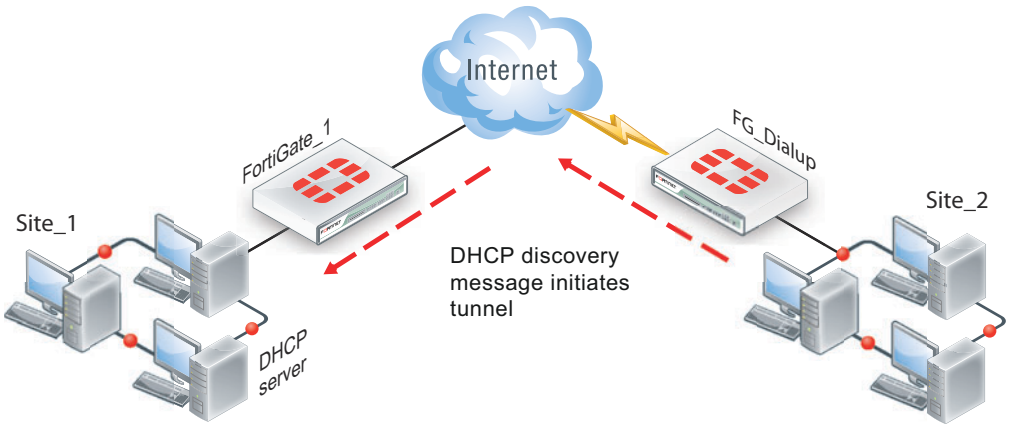
In some cases, computers on the private network behind the FortiGate dialup client may (by co-incidence) have IP addresses that are already used by computers on the network behind the FortiGate dialup server. In this type of situation (ambiguous routing), conflicts may occur in one or both of the FortiGate 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 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 19 on page 125). 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.

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.

Figure 19: Preventing network overlap in a FortiGate dialup-client configuration



When the DHCP server resides on the private network behind the FortiGate dialup server, the IP destination address specified in the IPsec security policy on the FortiGate dialup client must refer to that network.

You must add a static route to the DHCP server FortiGate unit if it is not directly connected to the private network behind the FortiGate dialup server; its IP address does not match the IP address of the private network. Also, the destination address in the IPsec security policy on the FortiGate dialup client must refer to the DHCP server address. The DHCP server must be configured to assign a range of IP addresses different from the DHCP server's local network, and also different from the private network addresses behind the FortiGate dialup server. See “Routing” on page 94.

FortiGate dialup-client infrastructure requirements

The requirements are:

- The FortiGate dialup server must have a static public IP address.
- NAT mode is required if you want to create a route-based VPN.
- The FortiGate dialup server may operate in either NAT mode or transparent mode to support a policy-based VPN.
- 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.

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.

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 a FortiGate interface" on page 116.

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 126.
- Configure the FortiGate dialup client. See "Configure the FortiGate dialup client" on page 128.

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 36. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel. This name appears in phase 2 configurations, security 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 52. 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 policy addresses" on page 58. 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 security policies to permit communications between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different security policies. For detailed information about creating security policies, see "Defining VPN security policies" on page 59.

Route-based VPN security policy

Define an ACCEPT security 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.

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter these settings in particular:

Incoming Interface	Select the VPN tunnel (IPsec interface) created in Step 1.
Source Address	Select *All*.
Outgoing Interface	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address	Select *All*.
Action	Select *ACCEPT*.
Enable NAT	Disable

Policy-based VPN security policy

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Select the *Policy Type* of *VPN* and leave the *Policy Subtype* as *IPsec*.
3. Enter these settings in particular:

Local Interface	Select the interface that connects to the private network behind this FortiGate unit.
Local Protected Subnet	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Outgoing VPN Interface	Select the FortiGate unit's public interface.
Remote Protected Subnet	Select the address name that you defined in Step 3.
VPN Tunnel	Select *Use Existing* and select the name of the phase 1 configuration that you created in Step 1. from the drop-down list. Select *Allow traffic to be initiated from the remote site* 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.

4. To prevent traffic from the local network from initiating the tunnel after the tunnel has been established, you need to disable the outbound VPN traffic in the CLI

```
config firewall policy
   edit <policy_number>
      set outbound disable
end
```

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

If configuring a route-based policy, configure a default route for VPN traffic on this interface.

Configure the FortiGate dialup client

Configure the FortiGate dialup client.

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 36. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel.
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	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 52. 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 policy addresses" on page 58. 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 security policies to permit communication between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different security policies. For detailed information about creating security policies, see "Defining VPN security policies" on page 59.

Route-based VPN security policy

Define an ACCEPT security 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.

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* of *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter these settings in particular:

Incoming Interface	Select the interface that connects to the private network behind this FortiGate unit.
Source Address	Select *All*.
Outgoing Interface	Select the VPN tunnel (IPsec interface) created in Step 1.
Destination Address	Select *All*.

Action	Select *ACCEPT*.
Enable NAT	Disable

Policy-based VPN security policy

Define an IPsec security policy to permit communications between the source and destination addresses.

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Select the *Policy Type* of *VPN* and leave the *Policy Subtype* as *IPsec*.
3. Enter these settings in particular:

Local Interface	Select the interface that connects to the private network behind this FortiGate unit.
Local Protected Subnet	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Outgoing Interface	Select the FortiGate unit's public interface.
Remote Protected Subnet	Select the address name that you defined in Step 3 for the private network behind the dialup server.
VPN Tunnel	Select *Use Existing* and select the name of the phase 1 configuration that you created in Step 1 from the drop-down list. Clear *Allow traffic to be initiated from the remote site* to prevent traffic from the remote network from initiating the tunnel after the tunnel has been established.

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

Supporting IKE Mode config clients

IKE Mode Config is an alternative to DHCP over IPsec. A FortiGate unit can be configured as either an IKE Mode Config server or client. This chapter contains the following sections:

Automatic configuration overview

VPN configuration for remote clients is simpler if it is automated. Several protocols support automatic configuration:

- The Fortinet FortiClient Endpoint Security application can completely configure a VPN connection with a suitably configured FortiGate unit given only the FortiGate unit's address. This protocol is exclusive to Fortinet. For more information, see the "FortiClient dialup-client configurations" chapter.
- DHCP over IPsec can assign an IP address, Domain, DNS and WINS addresses. The user must first configure IPsec parameters such as gateway address, encryption and authentication algorithms.
- IKE Mode Config can configure host IP address, Domain, DNS and WINS addresses. The user must first configure IPsec parameters such as gateway address, encryption and authentication algorithms. Several network equipment vendors support IKE Mode Config, which is described in the ISAKMP Configuration Method document *draft-dukes-ike-mode-cfg-02.txt*.

This chapter describes how to configure a FortiGate unit as either an IKE Mode Config server or client.

IKE Mode Config overview

Dialup VPN clients connect to a FortiGate unit that acts as a VPN server, providing the client the necessary configuration information to establish a VPN tunnel. The configuration information typically includes a virtual IP address, netmask, and DNS server address.

IKE Mode Config is available only for VPNs that are route-based, also known as interface-based. A FortiGate unit can function as either an IKE Configuration Method server or client. IKE Mode Config is configurable only in the CLI.

Configuring IKE Mode Config

IKE Mode Config is configured with the CLI command `config vpn ipsec phase1-interface`. The `mode-cfg` variable enables IKE Mode Config. The `type` field determines whether you are creating an IKE Mode Config server or a client. Setting `type` to `dynamic` creates a server configuration, otherwise the configuration is a client.

Configuring an IKE Mode Config client

If the FortiGate unit will connect as a dialup client to a remote gateway that supports IKE Mode Config, the relevant `vpn ipsec phase1-interface` variables are as follows:

Variable	Description
`ike-version 1`	IKE v1 is the default for FortiGate IPsec VPNs. IKE Mode Config is also compatible with IKE v2 (RFC 4306).
`mode-cfg enable`	Enable IKE Mode Config.
`type {ddns | static}`	If you set `type` to `dynamic`, an IKE Mode Config server is created.
`assign-ip {enable | disable}`	Enable to request an IP address from the server.
`interface <interface_name>`	This is a regular IPsec VPN field. Specify the physical, aggregate, or VLAN interface to which the IPsec tunnel will be bound.
`proposal <encryption_combination>`	This is a regular IPsec VPN field that determines the encryption and authentication settings that the client will accept. For more information, see "Defining IKE negotiation parameters" on page 45.
`mode-cfg-ip-version {4|6}`	Select if the Method client receives an IPv4 or IPv6 IP address. The default is `4`. the `ip-version` setting matches this variable's value.
`ip-version <4 | 6>`	This is a regular IPsec VPN field. By default, IPsec VPNs use IPv4 addressing. You can set `ip-version` to `6` to create a VPN with IPv6 addressing.

For a complete list of available variables, see the *CLI Reference*.

Configuring an IKE Mode Config server

If the FortiGate unit will accept connection requests from dialup clients that support IKE Mode Config, the following `vpn ipsec phase1-interface` settings are required before any other configuration is attempted:

Variable	Description
`ike-version 1`	IKE v1 is the default for FortiGate IPsec VPNs. IKE Mode Config is also compatible with IKE v2 (RFC 4306).
`mode-cfg enable`	Enable IKE Mode Config.
`type dynamic`	Any other setting creates an IKE Mode Config client.
`interface <interface_name>`	This is a regular IPsec VPN field. Specify the physical, aggregate, or VLAN interface to which the IPsec tunnel will be bound.

Variable	Description
`proposal <encryption_combination>`	This is a regular IPsec VPN field that determines the encryption and authentication settings that the server will accept. For more information, see "Defining IKE negotiation parameters" on page 45.
`ip-version <4 | 6>`	This is a regular IPsec VPN field. By default, IPsec VPNs use IPv4 addressing. You can set `ip-version` to `6` to create a VPN with IPv6 addressing.

For a complete list of available variables, see the *CLI Reference*.

After you have enabled the basic configuration, you can configure:

- IP address assignment for clients
- DNS and WINS server assignment

IP address assignment

Usually you will want to assign IP addresses to clients. The simplest method is to assign addresses from a specific range, similar to a DHCP server.

If your clients are authenticated by a RADIUS server, you can obtain the user's IP address assignment from the Framed-IP-Address attribute. The user must be authenticated using XAuth.

To assign IP addresses from an address range

If your VPN uses IPv4 addresses,

```
config vpn ipsec phase1-interface
  edit vpn1
    set mode-cfg-ipversion 4
    set assign-ip enable
    set assign-ip-type ip
    set assign-ip-from range
    set ipv4-start-ip <range_start>
    set ipv4-end-ip <range_end>
    set ipv4-netmask <netmask>
  end
```

If your VPN uses IPv6 addresses,

```
config vpn ipsec phase1-interface
  edit vpn1
    set mode-cfg-ipversion 6
    set assign-ip enable
    set assign-ip-type ip
    set assign-ip-from range
    set ipv6-start-ip <range_start>
    set ipv6-end-ip <range_end>
  end
```

To assign IP addresses from a RADIUS server

The users must be authenticated by a RADIUS server and assigned to the FortiGate user group `<grpname>`. Since the IP address will not be static, `type` is set to dynamic, and `mode-cfg` is enabled. This is IKE Configuration Method so that compatible clients can configure themselves with settings that the FortiGate unit provides.

```
config vpn ipsec phase1-interface
  edit vpn1
    set type dynamic
      set mode-cfg enable
      set assign-ip enable
      set assign-ip-from usrgrp
      set xauthtype auto
      set authusrgrp <grpname>
  end
```

Example: FortiGate unit as IKE Mode Config server

In this example, the FortiGate unit assigns IKE Mode Config clients addresses in the range of 10.11.101.160 through 10.11.101.180. DNS and WINS server addresses are also provided. The public interface of the FortiGate unit is Port 1.

The `ipv4-split-include` variable specifies a firewall address that represents the networks to which the clients will have access. This destination IP address information is sent to the clients.

Only the CLI fields required for IKE Mode Config are shown here. For detailed information about these variables, see the *FortiGate CLI Reference*.

```
config vpn ipsec phase1-interface
  edit vpn1
    set ip-version 4
    set type dynamic
    set interface port1
    set proposal 3des-sha1 aes128-sha1
    set mode-cfg enable
    set mode-cfg-ipversion 4
    set assign-ip enable
    set assign-ip-type ip
    set assign-ip-from range
    set ipv4-start-ip 10.11.101.160
    set ipv4-end-ip 10.11.101.180
    set ipv4-netmask 255.255.255.0
    set dns-server1 10.11.101.199
    set dns-server2 66.11.168.195
    set wins-server1 10.11.101.191
    set domain example
    set ipv4-split-include OfficeLAN
  end
```

Example: FortiGate unit as IKE Mode Config client

In this example, the FortiGate unit connects to a VPN gateway with a static IP address that can be reached through Port 1. Only the port, gateway and proposal information needs to be configured. All other configuration information will come from the IKE Mode Config server.

```
config vpn ipsec phase1-interface
  edit vpn1
    set ip-version 4
    set type static
    set remote-gw <gw_address>
    set interface port 1
    set proposal 3des-sha1 aes128-sha1
    set mode-cfg enable
    set mode-cfg-ipversion 4
    set assign-ip enable
  end
```

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 security policy that controls traffic on the private network behind the local FortiGate unit.

The following topics are included in this section:

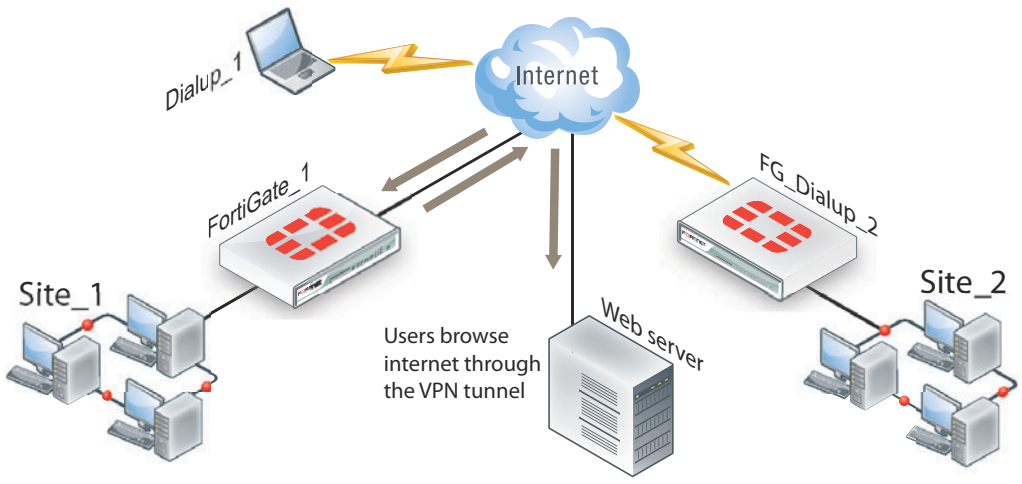
- Configuration overview
- Creating an Internet browsing security policy
- Routing all remote traffic through the VPN tunnel

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 20, FortiGate_1 enables secure Internet browsing for FortiClient Endpoint 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 20: 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 64)
- a FortiClient dialup-client configuration (see “FortiClient dialup-client configurations” on page 108)
- a FortiGate dialup-client configuration (see “FortiGate dialup-client configurations” on page 123)

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 security policy. See "Creating an Internet browsing security 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 Endpoint Security application. See "Routing all remote traffic through the VPN tunnel" on page 138.

Creating an Internet browsing security 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 security 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 *Policy* > *Policy* > *Policy* and select *Create New*.
2. Select the *Policy Type* as *VPN* and leave the *Policy Subtype* as *IPsec*.
3. Enter the following information and then select *OK*:

Local Interface	The interface to which the VPN tunnel is bound.
Local Protected Subnet	All
Outgoing VPN Interface	The interface to which the VPN tunnel is bound.
Remote Protected Subnet	The internal range of address of the remote spoke site.
VPN Tunnel	Select *Use Existing* and select the tunnel that provides access to the private network behind the FortiGate unit.
Allow traffic to be initiated from the remote site	Enable
Inbound NAT	Enable

4. Enable inbound NAT in the CLI.

```
config firewall policy
  edit <policy_number>
    set natinbound enable
end
```

To create an Internet browsing policy - route-based VPN

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information and then select *OK*:

Incoming Interface	The IPsec VPN interface.
Source Address	All

Outgoing Interface	The interface that connects to the Internet. The virtual IPsec interface is configured on this physical interface.
Destination Address	The internal range of address of the remote spoke site.
Action	ACCEPT
Enable NAT	Enable

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 application that protects an individual client 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 Endpoint Security application for Internet browsing via VPN, see "Configuring a FortiClient application to support Internet browsing" on page 139.

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 security policy" on page 137.

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 *Policy* > *Policy* > *Policy*.
2. Select the IPsec security policy and then select *Edit*.
3. From the *Remote Protected Subnet* list, select *all*.
4. Select *OK*.

Packets are routed through the VPN tunnel, not just those 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* > *Static Route*s.
2. On a low-end FortiGate unit, go to *System* > *Network* > *Routing*.
3. Select the default route (destination IP 0.0.0.0) and then select *Edit*. 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.
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*.

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

A FortiGate unit with two interfaces connected 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.

Redundant tunnels do not support Tunnel Mode or Manual Keys. You must use Interface Mode.

A fully-redundant configuration requires redundant connections to the Internet on both peers. Figure 21 on page 141 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 157. This is useful to provide reliable service from a FortiGate unit with static IP addresses that accepts connections from dialup IPsec VPN clients.

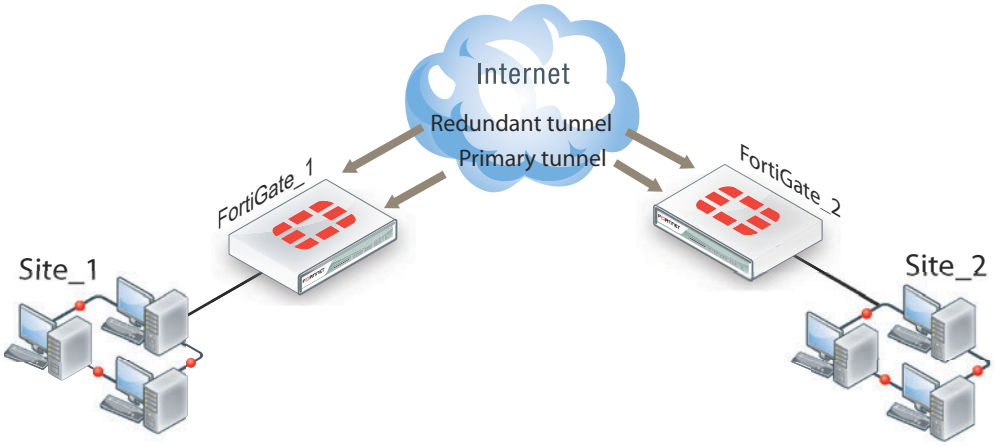
In a fully-redundant VPN configuration with two interfaces on each peer, four distinct paths are possible for VPN traffic from end to end. Each interface on a peer can communicate with both interfaces on the other peer. This ensures that a VPN will be available as long as each peer has one working connection 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 mode. You must use auto-keying. A VPN that is created using manual keys (see "Manual-key configurations" on page 171) 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 164.

Figure 21: Example redundant-tunnel configuration



A VPN that is created using manual keys (see "Manual-key configurations" on page 171) 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 security 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

VPN peers are configured using Interface Mode for redundant tunnels.

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, and any other VPN settings as required:

   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

   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

   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

   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

   For more information, see “Auto Key phase 1 parameters” on page 36.

3. Create a phase 2 definition for each path. See "Phase 2 parameters" on page 52. 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 security policy for the local primary interface. See "Defining VPN security policies" on page 59. You need to create two policies for each path to enable communication in both directions. Enter these settings in particular:

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

6. Select *Create New*, leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*, and enter these settings:

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

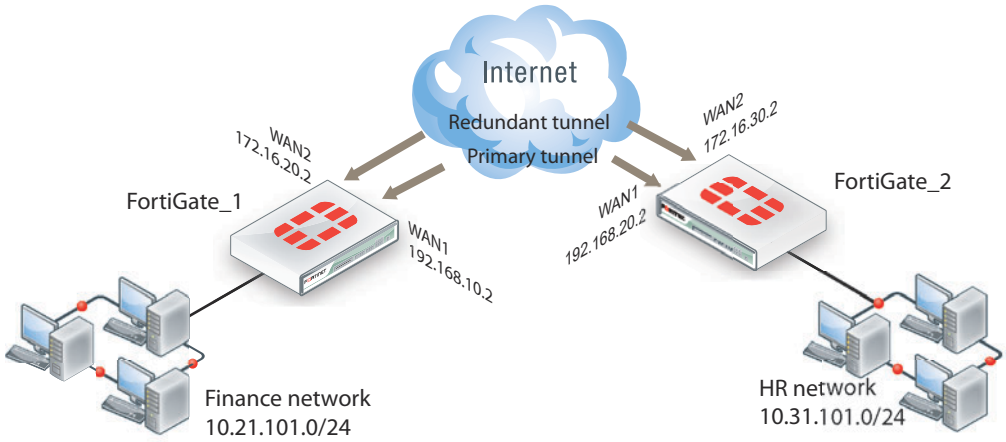
7. Place the policy in the policy list above any other policies having similar source and destination addresses.
8. Repeat this procedure at the remote FortiGate unit.

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 22: Example redundant route-based VPN configuration



For each path, VPN configuration, security 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 security policies between the internal interface and each of the virtual IPsec interfaces

To configure the network interfaces

1. Go to *System* > *Network* > *Interfaces*.
2. Select the Internal interface and select *Edit*.

3. Enter the following information and then select *OK*:

Addressing mode	Manual
IP/Netmask	10.21.101.0/255.255.255.0

4. Select the WAN1 interface and select *Edit*, enter the following information and then select *OK*:

Addressing mode	Manual
IP/Netmask	192.168.10.2/255.255.255.0

5. Select the WAN2 interface and select *Edit*, 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 (IKE)*.
2. Select *Create Phase 1*, enter the following information, and select *OK*:

Name	Site_1_A
Remote Gateway	Static IP Address
IP Address	192.168.20.2
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	192.168.20.2
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 (IKE)*.
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* > *Static Routes*.
   For low-end FortiGate units, go to *System* > *Network* > *Routing*.
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	192.168.10.1
Distance (Advanced)	10

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

Destination IP/Mask	10.31.101.0/255.255.255.0
Device	Site_1_A
Distance (Advanced)	1

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

Destination IP/Mask	10.31.101.0/255.255.255.0
Device	Site_1_B
Distance (Advanced)	2

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

Destination IP/Mask	10.31.101.0/255.255.255.0
Device	Site_1_C
Distance (Advanced)	3

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

Destination IP/Mask	10.31.101.0/255.255.255.0
Device	Site_1_D
Distance (Advanced)	4

To configure security policies

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information, and then select *OK*:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_1_A
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

4. Select *Create New*.
5. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
6. Enter the following information, and select *OK*:

Incoming Interface	Site_1_A
Source Address	All
Outgoing Interface	Internal
Destination Address	All

Schedule	Always
Service	Any
Action	ACCEPT

7. Select *Create New*.
8. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
9. Enter the following information, and select *OK*:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_1_B
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

10. Select *Create New*.
11. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
12. Enter the following information, and select *OK*:

Incoming Interface	Site_1_B
Source Address	All
Outgoing Interface	Internal
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

13. Select *Create New*.
14. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
15. Enter the following information, and select *OK*:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_1_C
Destination Address	All
Schedule	Always

Service	Any
Action	ACCEPT

16. Select *Create New*.
17. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
18. Enter the following information, and select *OK*:

Incoming Interface	Site_1_C
Source Address	All
Outgoing Interface	Internal
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

19. Select *Create New*.
20. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
21. Enter the following information, and select *OK*:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_1_D
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

22. Select *Create New*.
23. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
24. Enter the following information, and select *OK*:

Incoming Interface	Site_1_D
Source Address	All
Outgoing Interface	Internal
Destination Address	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 security policies between the internal interface and each of the virtual IPsec interfaces

To configure the network interfaces

1. Go to *System* > *Network* > *Interfaces*.
2. Select the Internal interface and then select *Edit*. Enter the following information and then select *OK*:

Addressing mode	Manual
IP/Netmask	10.31.101.0/255.255.255.0

3. Select the WAN1 interface and then select *Edit*. Enter the following information and then select *OK*:

Addressing mode	Manual
IP/Netmask	192.168.20.2/255.255.255.0

4. Select the WAN2 interface and then select *Edit*. 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 (IKE)*.
2. Select *Create Phase 1*, enter the following information, and select *OK*:

Name	Site_2_A
Remote Gateway	Static IP Address
IP Address	192.168.10.2
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	192.168.10.2
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

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 (IKE)*.
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* > *Static Route*s.

   For low-end FortiGate units, go to *System* > *Network* > *Routing*.

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	192.168.10.1
Distance (Advanced)	10

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

Destination IP/Mask	10.21.101.0/255.255.255.0
Device	Site_2_A
Distance (Advanced)	1

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

Destination IP/Mask	10.21.101.0/255.255.255.0
Device	Site_2_B
Distance (Advanced)	2

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

Destination IP/Mask	10.21.101.0/255.255.255.0
Device	Site_2_C
Distance (Advanced)	3

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

Destination IP/Mask	10.21.101.0/255.255.255.0
Device	Site_2_D
Distance (Advanced)	4

To configure security policies

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information, and select *OK*:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_2_A
Destination Address	All

Schedule	Always
Service	Any
Action	ACCEPT

4. Select *Create New*.
5. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
6. Enter the following information, and select *OK*:

Incoming Interface	Site_2_A
Source Address	All
Outgoing Interface	Internal
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

7. Select *Create New*.
8. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
9. Enter the following information, and select *OK*:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_2_B
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

10. Select *Create New*.
11. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
12. Enter the following information, and select *OK*:

Incoming Interface	Site_2_B
Source Address	All
Outgoing Interface	Internal
Destination Address Name	All
Schedule	Always

Service	Any
Action	ACCEPT

13. Select *Create New*.
14. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
15. Enter the following information, and select *OK*:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_2_C
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

16. Select *Create New*.
17. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
18. Enter the following information, and select *OK*:

Incoming Interface	Site_2_C
Source Address	All
Outgoing Interface	Internal
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

19. Select *Create New*.
20. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
21. Enter the following information, and select *OK*:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_2_D
Destination Address	All
Schedule	Always

Service	Any
Action	ACCEPT

22. Select *Create New*.
23. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
24. Enter the following information, and select *OK*:

Incoming Interface	Site_2_D
Source Address	All
Outgoing Interface	Internal
Destination Address	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 123.

When a FortiGate unit has more than one interface to the Internet (see FortiGate_1 in Figure 23), 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:

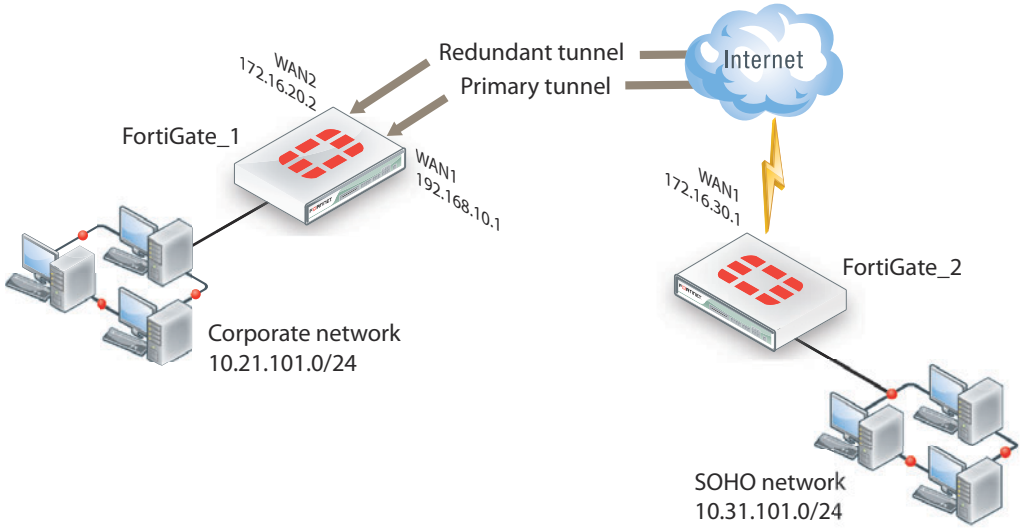
- Both FortiGate units operate in NAT mode.
- Two separate interfaces to the Internet (192.168.10.2 and 172.16.20.2) are available on FortiGate_1. Each interface has a static public IP address.
- FortiGate_2 has a single connection to the Internet and obtains a dynamic public IP address (for example, 172.16.30.1) when it connects to the Internet.
- FortiGate_2 forwards IP packets from the SOHO network (10.31.101.0/24) to the corporate network (10.21.101.0/24) 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, security 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 23: 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 security policies between the internal interface and each of the virtual IPsec interfaces

To configure the network interfaces

1. Go to *System* > *Network* > *Interfaces*.
2. Select the Internal interface and select *Edit*. Enter the following information and select *OK*:

Addressing mode	Manual
IP/Netmask	10.21.101.2/255.255.255.0

3. Select the WAN1 interface and select *Edit*. Enter the following information and select *OK*:

Addressing mode	Manual
IP/Netmask	192.168.10.2/255.255.255.0

4. Select the WAN2 interface and select *Edit*. Enter the following information and 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 (IKE)*.
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 (IKE)*.
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* > *Static Routes*.
   For low-end FortiGate units, go to *System* > *Network* > *Routing*.
2. Select *Create New*, enter the following default gateway information and select *OK*:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	WAN1
Gateway	192.168.10.1
Distance (Advanced)	10

To configure security policies

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information, and select *OK*:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_1_A
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

4. Select *Create New*.
5. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
6. Enter the following information, and select *OK*:

Incoming Interface	Internal
Source Address	All

Outgoing Interface	Site_1_B
Destination Address	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 security policies between the internal interface and each of the virtual IPsec interfaces

To configure the network interfaces

1. Go to *System* > *Network* > *Interfaces*.
2. Select the Internal interface and select *Edit*. Enter the following information and select *OK*:

Addressing mode	Manual
IP/Netmask	10.31.101.2/255.255.255.0

3. Select the WAN1 interface and select *Edit*. Set the *Addressing mode* to *DHCP*.

To configure the two IPsec interfaces (phase 1 configurations)

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)*.
2. Select *Create Phase 1*, enter the following information, and select *OK*:

Name	Site_2_A
Remote Gateway	Static IP Address
IP Address	192.168.10.2
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 (IKE)*.
2. Select *Create Phase 2*, enter the following information and select *OK*:

Name	`Route_A`
Phase 1	Site_2_A
Advanced	
Source Address	10.31.101.0/24

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

Name	`Route_B`
Phase 1	Site_2_B
Advanced	
Source Address	10.31.101.0/24

To configure routes

1. Go to *Router* > *Static* > *Static Route*s.
   For low-end FortiGate units, go to *System* > *Network* > *Routing*.

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

Destination IP/Mask	10.21.101.0/255.255.255.0
Device	Site_2_A
Distance (Advanced)	1

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

Destination IP/Mask	10.21.101.0/255.255.255.0
Device	Site_2_B
Distance (Advanced)	2

To configure security policies

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information, and select *OK*:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_2_A
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

4. Select *Create New*.
5. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
6. Enter the following information, and select *OK*:

Incoming Interface	Internal
Source Address	All
Outgoing Interface	Site_2_B
Destination Address	All
Schedule	Always
Service	Any
Action	ACCEPT

Creating a backup IPsec interface

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.

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` 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 192.168.10.8
    set type static
  end
  edit backup_vpn
    set dpd on
    set interface port2
    set monitor main_vpn
    set nattraversal enable
    set psksecret "hard-to-guess"
    set remote-gw 192.168.10.8
    set type static
  end
```

Transparent mode VPNs

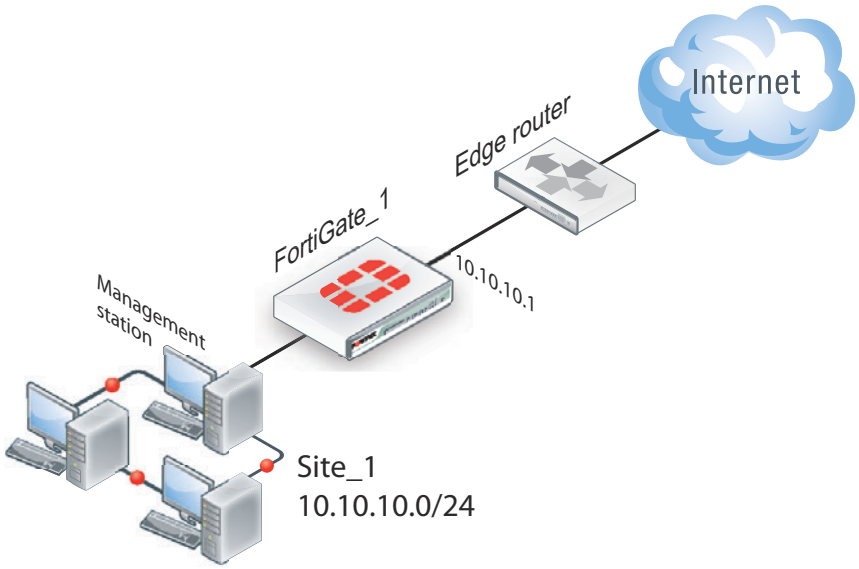
This section describes transparent VPN configurations, in which two FortiGate units create a VPN tunnel between two separate private networks transparently.

The following topics are included in this section:

Configuration overview

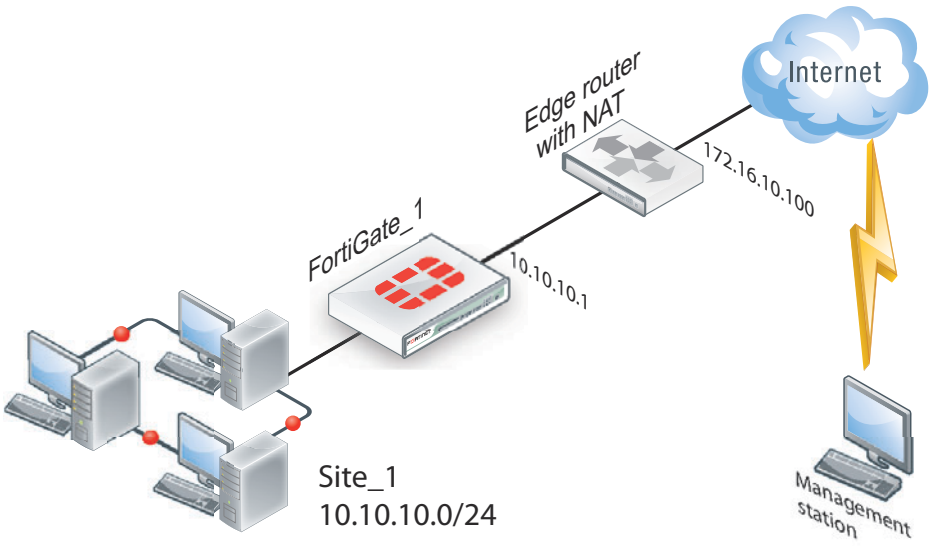
In transparent mode, all interfaces of the FortiGate unit except the management interface (which by default is assigned IP address 10.10.10.1/255.255.255.0) are invisible at the network layer. Typically, when a FortiGate unit runs in transparent mode, different network segments are connected to the FortiGate interfaces. Figure 24 shows the management station on the same subnet. The management station can connect to the FortiGate unit directly through the web-based manager.

Figure 24: 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 25 on page 166), the router must translate (NAT) a routable address to direct management traffic to the FortiGate management interface.

Figure 25: 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 security policies.

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

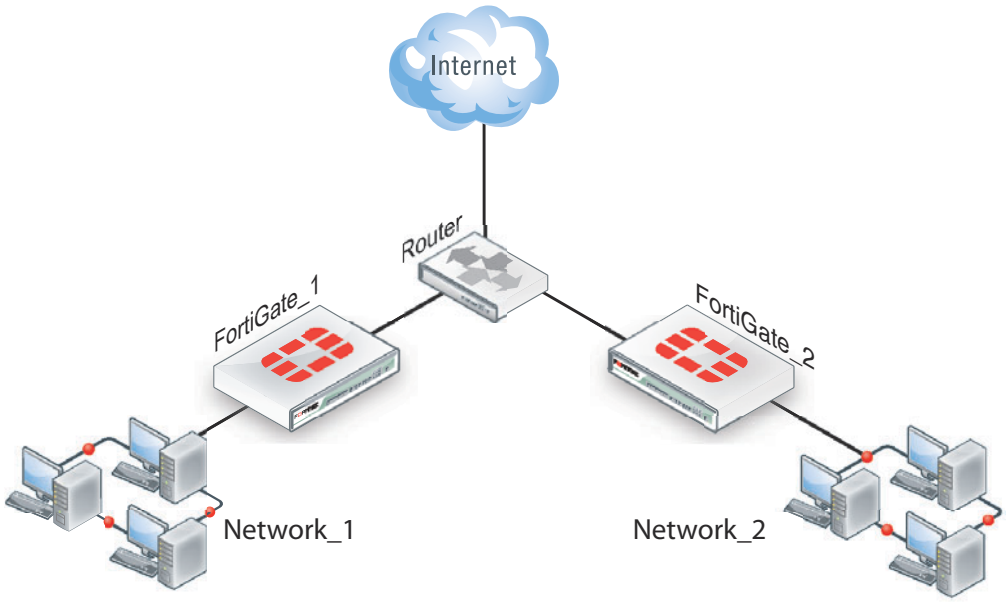
VPNs between two FortiGate units running in transparent mode do not support inbound/outbound NAT (supported through CLI commands) within the tunnel. In addition, a FortiGate unit running in transparent mode cannot be used in a hub-and-spoke configuration.

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 *Advanced Routing Guide*.

In the example configuration shown in Figure 25, 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.

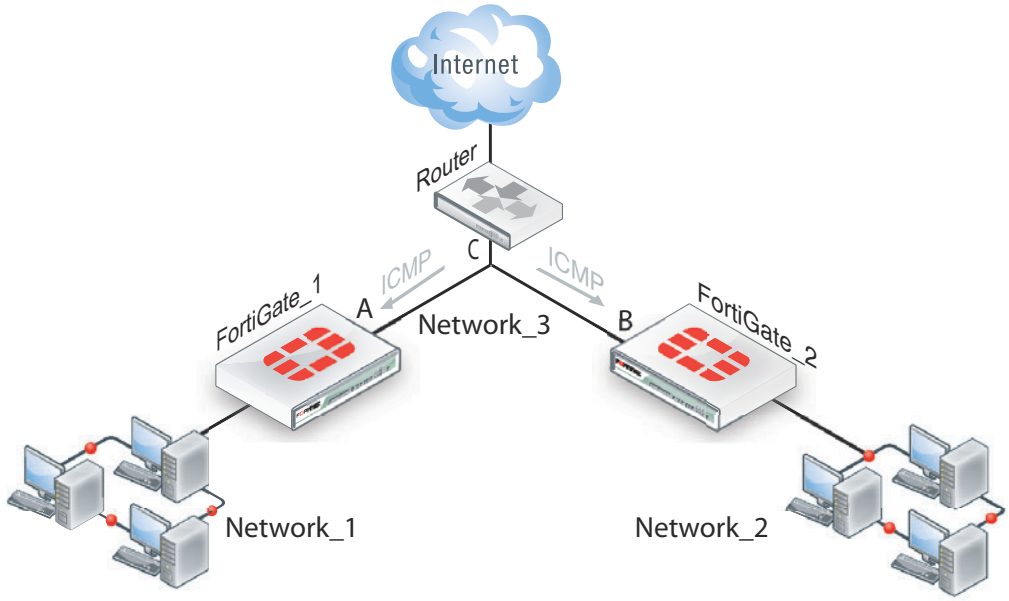
If you want to configure a VPN between two FortiGate units running in transparent mode, each unit must have an independent connection to a router that acts as a gateway to the Internet, and both units must be on separate networks that have a different address space. When the two networks linked by the VPN tunnel have different address spaces (see Figure 26 on page 167), at least one router must separate the two FortiGate units, unless the packets can be redirected using ICMP (see Figure 27 on page 167).

Figure 26: Link between two FortiGate units in transparent mode



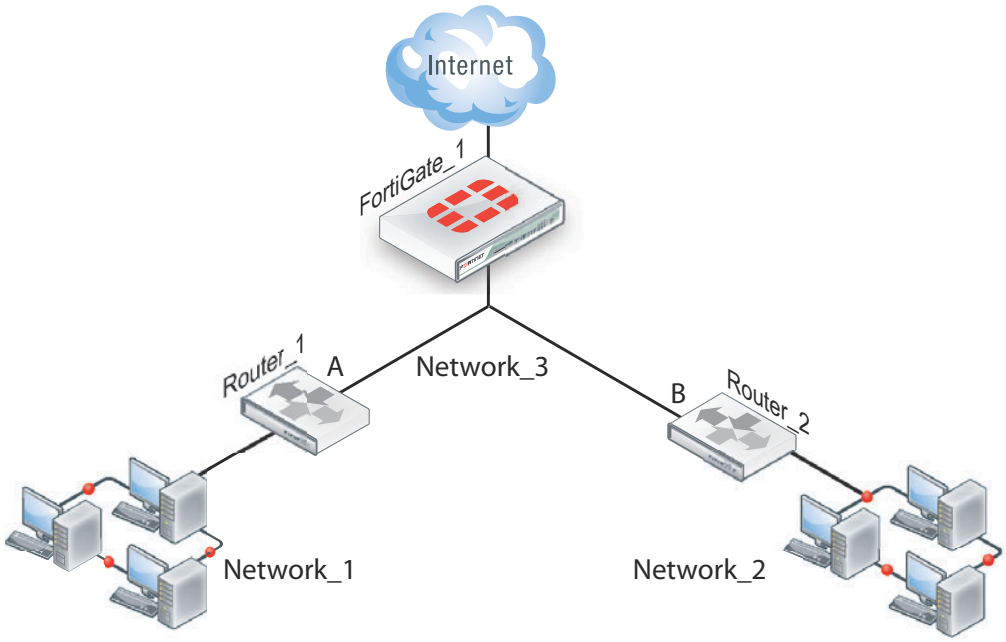
In Figure 27, interface C behind the router is the default gateway for both FortiGate units. Packets that cannot be delivered on Network_1 are routed to interface C by default. Similarly, packets that cannot be delivered on Network_2 are routed to interface C. In this case, the router must be configured to redirect packets destined for Network_1 to interface A and redirect packets destined for Network_2 to interface B.

Figure 27:ICMP redirecting packets to two FortiGate units in transparent mode



If there are additional routers behind the FortiGate unit (see Figure 28 on page 168) 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 28, 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 28: 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 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 an edge router that forwards packets to the Internet must be present in the FortiGate routing table.
- 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.

Only policy-based VPN configurations are possible in transparent mode.

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, security policies, and VPN components. For more information, see the *Virtual Domains Guide*.

Configure the VPN peers

1. The local VPN peer need to operate in transparent mode.

   To determine if your FortiGate unit is in transparent mode, go to *System* > *Dashboard* > *Status* to *the System Information* widget. Select *[change].* Select transparent for the *Operation Mode*. Two new fields will appear to enter the *Management IP/Netmask*, and the *Default Gateway*.

   In transparent mode, the FortiGate unit is invisible to the network. All of its interfaces are on the same subnet and share the same IP address. You only have to configure a management IP address so that you can make configuration changes.

The remote VPN peer may operate in NAT mode or transparent mode.

2. 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 36. 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 48 and "NAT keepalive frequency" on page 49.

3. Define the phase 2 parameters needed to create a VPN tunnel with the remote peer. See "Phase 2 parameters" on page 52. 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.
4. Define the source and destination addresses of the IP packets that are to be transported through the VPN tunnel. See "Defining policy addresses" on page 58. Enter these settings in particular:
   - For the originating address (source address), enter the IP address and netmask of the private network behind the local peer network. for the management interface, for example, `10.10.10.0/24`. This address needs to be a range to allow traffic from your network through the tunnel. Optionally select `any` for this address.
   - 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.
5. Define an IPsec security policy to permit communications between the source and destination addresses. See "Defining VPN security policies" on page 59. Enter these settings in particular:

Local Interface	Select the local interface to the internal (private) network.
Local Protected Subnet	Select the source address that you defined in Step 4.

Outgoing VPN Interface	Select the interface to the edge router. When you configure the IPsec security policy on a remote peer that operates in NAT mode, you select the public interface to the external (public) network instead.
Remote Protected Subnet	Select the destination address that you defined in Step 4.
VPN Tunnel	Select *Use Existing* and select the name of the phase 2 tunnel configuration that you created in Step 3 from the drop-down list. Select *Allow traffic to be initiated from the remote site* to enable traffic from the remote network to initiate the tunnel.

6. Place the policy in the policy list above any other policies having similar source and destination addresses.
7. Define another IPsec security policy to permit communications between the source and destination addresses in the opposite direction. This security policy and the previous one form a bi-directional policy pair. See "Defining VPN security policies" on page 59. Enter these settings in particular:

Local Interface	Select the interface to the edge router. When you configure the IPsec security policy on a remote peer that operates in NAT mode, you select the public interface to the external (public) network instead.
Local Protected Subnet	Select the destination address that you defined in Step 4.
Outgoing VPN Interface	Select the local interface to the internal (private) network.
Remote Protected Subnet	Select the source address that you defined in Step 4.
VPN Tunnel	Select *Use Existing* and select the name of the phase 2 tunnel configuration that you created in Step 3 from the drop-down list. Select *Allow traffic to be initiated from the remote site* to enable traffic from the remote network to initiate the tunnel.

8. Repeat this procedure at the remote FortiGate unit to create bidirectional security policies. Use the local interface and address information local to the remote FortiGate unit.

For more information on transparent mode, see the System Administration Guide.

Manual-key configurations

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

For more information on web-based manual key configuration, see “Manual Key” on page 32.

The following topics are included in this section:

By default Manual key configurations to not appear on the Web-based Manager. You need to enable the feature first.

To enable manual key configurations

1. Go to *System* > *Admin* > *Settings*.
2. In the *Display Options on GUI* section, select *IPsec Manual Key*.
3. Select *Apply*.

Configuration overview

You manual define cryptographic 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 by going to *VPN* > *IPsec* > *Manual Key*.

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.

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.

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 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 (Hex)	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 (Hex)	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 mode.

3. Select *OK*.

IPv6 IPsec VPNs

This chapter describes how to configure your FortiGate unit's IPv6 IPsec VPN functionality.

By default IPv6 configurations to not appear on the Web-based Manager. You need to enable the feature first.

To enable IPv6

1. Go to *System* > *Admin* > *Settings*.
2. In the *Display Options on GUI* section, select *IPv6*.
3. Select *Apply*.

The following topics are included in this section:

Overview of IPv6 IPsec support

FortiOS supports route-based IPv6 IPsec, but not policy-based. This section describes how IPv6 IPsec support differs from IPv4 IPsec support. FortiOS 4.0 MR3 is IPv6 Ready Logo Program Phase 2 certified.

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.
- 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 route-based VPN: phase 1 settings, phase 2 settings, security policies and routing.

By default IPv6 configurations to not appear on the Web-based Manager. You need to enable the feature first.

To enable IPv6

1. Go to *System* > *Admin* > *Settings*.
2. In the *Display Options on GUI* section, select *IPv6*.
3. Select *Apply*.

Phase 1 configuration

In the web-based manager, you define the Phase 1 as IPv6 in the Advanced settings. Enable the IPv6 Version check box. You can then enter an IPv6 address for the remote gateway.

In the CLI, 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. For example:

```
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

To create an IPv6 IPsec phase 2 configuration in the web-based manager, you need to define IPv6 selectors in the Advanced settings. Change the default “0.0.0.0/0” address for Source address and Destination address to the IPv6 value “::/0”. If needed, enter specific IPv6 addresses, address ranges or subnet addresses in these fields.

In the CLI, set `src-addr-type` and `dst-addr-type` to `ip6`, `range6` or `subnet6` to specify IPv6 selectors. By default, zero selectors are entered, "::/0" for the `subnet6` address type, for example. The simplest IPv6 phase 2 configuration looks like this:

```
config vpn ipsec phase2-interface
  edit tunnel6_p2
    set phase1name tunnel6
    set proposal 3des-md5
    set src-addr-type subnet6
    set dst-addr-type subnet6
  end
```

Security policies

To complete the VPN configuration, you need a security 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.

To create a static route in the web-based manager

1. Go to *Router* > *Static* > *Static Routes*.

   On low-end FortiGate units, go to *System* > *Network* > *Routing*.
2. Select the drop-down arrow on the *Create New* button and select *IPv6 Route*.
3. Enter the information and select *OK*.

In the CLI, use the `router static6` command. 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
```

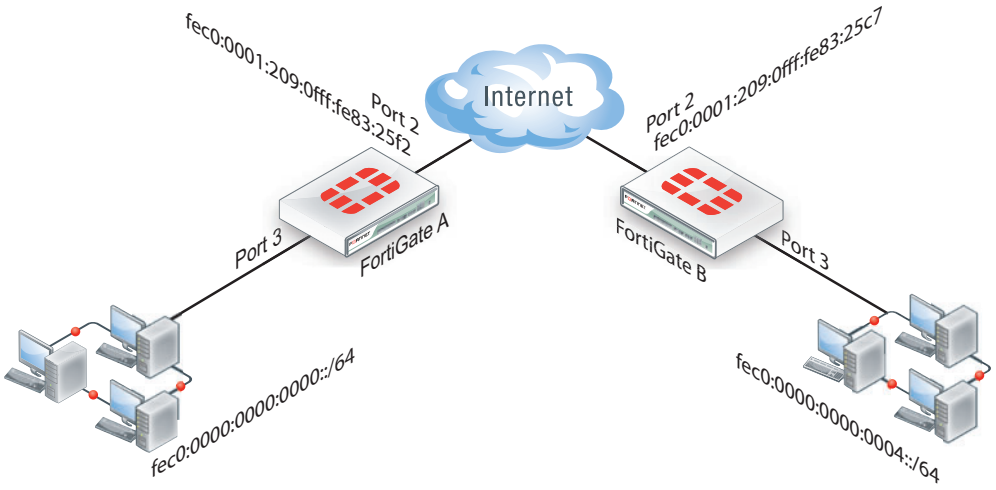
If the VPN is IPV4 over IPv6, the route to the remote protected network is an IPv4 route. If the VPN is IPv6 over IPv4, the route to the remote VPN gateway is an IPv4 route.

Site-to-site IPv6 over IPv6 VPN example

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

To access IPv6 functionality through the web-based manager, go to *System Admin* > *Settings* and enable *IPv6* in the section, *Display Options on GUI*.

Figure 29: 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

route-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 security policies

Security 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. Security 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.

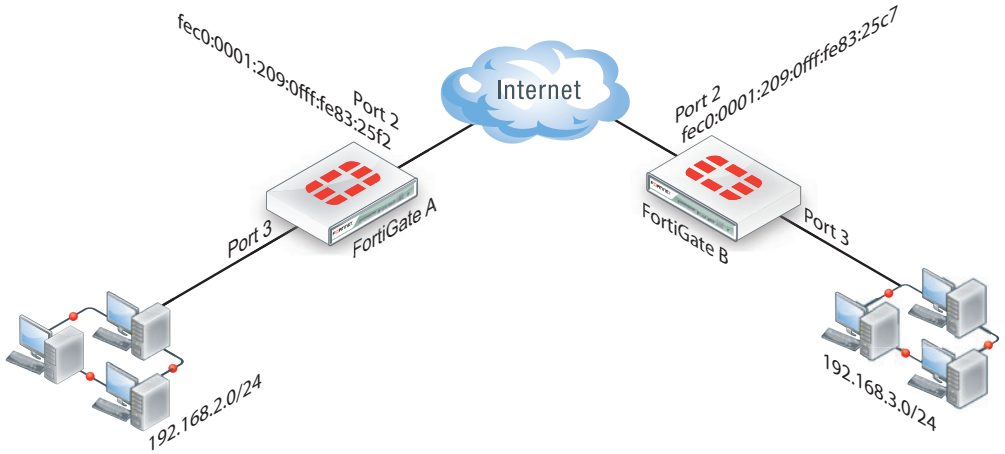
```
config system interface
  edit port2
    config ipv6
      set ip6-address fec0::0003:209:0fff:fe83:25c7/64
    end
  next
  edit port3
    config ipv6
      set ip6-address fec0::0004:209:0fff:fe83:2569/64
    end
  end
config vpn ipsec phase1-interface
  edit toA
    set ip-version 6
    set interface 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 30: 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 security policies

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

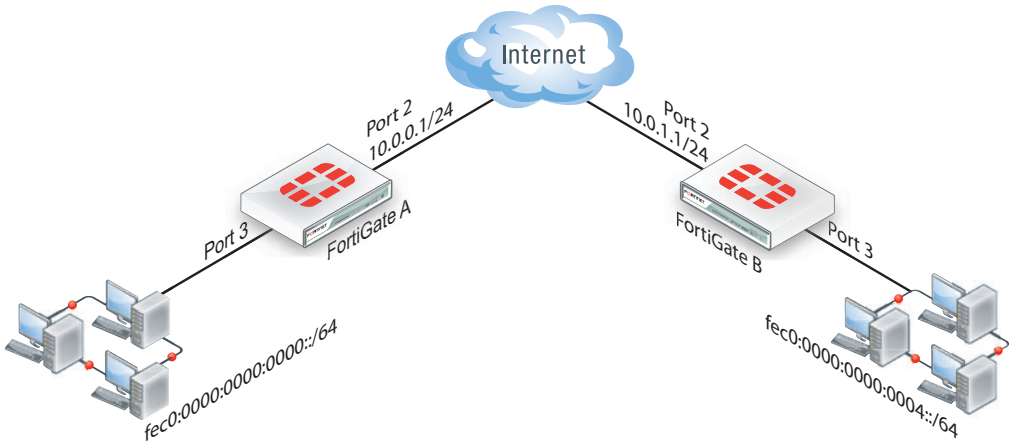
```
config system interface
  edit port2
    config ipv6
      set ip6-address fec0::0003:fe83:25c7/64
    end
  next
  edit port3
    set 192.168.3.1/24
  end
config vpn ipsec phase1-interface
  edit toA
    set ip-version 6
    set interface port2
    set remote-gw6 fec0:0000:0000:0001:209:0fff:fe83:25f2
    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 31: 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 security policies

IPv6 security policies are required to allow traffic between port3 and the IPsec interface toB in each direction. Define the address `all6` 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 security 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
```

L2TP and IPsec (Microsoft VPN)

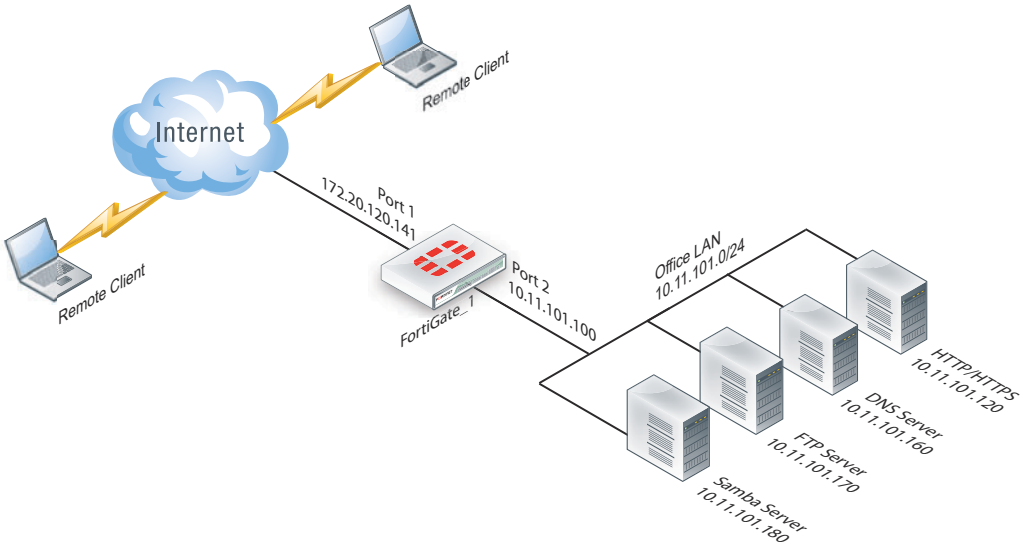
This section describes how to set up a VPN that is compatible with the Microsoft Windows native VPN, which is Layer 2 Tunneling Protocol (L2TP) with IPsec encryption.

The following topics are included in this section:

Overview

The topology of a VPN for Microsoft Windows dialup clients is very similar to the topology for FortiClient Endpoint Security clients.

Figure 32: Example FortiGate VPN configuration with Microsoft clients



For users, the difference is that instead of installing and using the FortiClient application, they configure a network connection using the software built into the Microsoft Windows operating system. Starting in FortiOS 4.0 MR2, you can configure a FortiGate unit to work with unmodified Microsoft VPN client software.

Layer 2 Tunneling Protocol (L2TP)

L2TP is a tunneling protocol published in 1999 that is used with VPNs, as the name suggests. Microsoft Windows operating system has a built-in L2TP client starting since Windows 2000. Mac OS X 10.3 system and higher also have a built-in client.

L2TP provides no encryption and used UDP port 1701. IPsec is used to secure L2TP packets. The initiator of the L2TP tunnel is called the L2TP Access Concentrator (LAC).

L2TP and IPSec is supported for native Windows XP, Windows Vista and Mac OSX native VPN clients. However, in Mac OSX (OSX 10.6.3, including patch releases) the L2TP feature does not work properly on the Mac OS side.

Assumptions

The following assumptions have been made for this example:

- L2TP protocol traffic is allowed through network firewalls (TCP and UDP port 1701)
- User has Microsoft Windows 2000 or higher — a Windows version that supports L2TP

Configuring the FortiGate unit

To configure the FortiGate unit, you need to:

- configure LT2P users and firewall user group;
- configure the L2TP VPN, including the IP address range it assigns to clients;
- configure an IPsec VPN with encryption and authentication settings that match the Microsoft VPN client;
- configure security policies.

Configuring LT2P users and firewall user group

Remote users must be authenticated before they can request services and/or access network resources through the VPN. The authentication process can use a password defined on the FortiGate unit or an established external authentication mechanism such as RADIUS or LDAP.

Creating user accounts

You need to create user accounts and then add these users to a firewall user group to be used for L2TP authentication. The Microsoft VPN client can automatically send the user's Window network logon credentials. You might want to use these for their L2TP user name and password.

To create a user account - web-based manager

1. Go to *User & Device* > *User* > *User Definition* and select *Create New*.
2. Enter the *User Name*.
3. Do one of the following:
   - Select *Password* and enter the user's assigned password.
   - Select *Match user on LDAP server*, *Match user on RADIUS server*, or *Match user on TACACS+ server* and select the authentication server from the list. The authentication server must be already configured on the FortiGate unit.
4. Select *OK*.

To create a user account - CLI

To create a user account called `user1` with the password `123_user`, enter:

```
config user local
  edit user1
    set type password
    set passwd "123_user"
    set status enable
  end
```

Creating a user group

When clients connect using the L2TP-over-IPsec VPN, the FortiGate unit checks their credentials against the user group you specify for L2TP authentication. You need to create a firewall user group to use for this purpose.

To create a user group - web-based manager

1. Go to *User & Device* > *User* > *User Groups*, select *Create New*, and enter the following:

Name	Type or edit the user group name (for example, `L2TP_group`).
Type	Select *Firewall*.
Available Users/Groups	The list of Local users, RADIUS servers, LDAP servers, TACACS+ servers, or PKI users that can be added to the user group. To add a member to this list, select the name and then select the right arrow button.
Members	The list of Local users, RADIUS servers, LDAP servers, TACACS+ servers, or PKI users that belong to the user group. To remove a member, select the name and then select the left arrow button.

2. Select *OK*.

To create a user group - CLI

To create the user group L2TP_group and add members User_1, User_2, and User_3, enter:

```
config user group
  edit L2TP_group
    set group-type firewall
    set member User_1 User_2 User_3
  end
```

Configuring L2TP

You can only configure L2TP settings in the CLI. As well as enabling L2TP, you set the range of IP address values that are assigned to L2TP clients and specify the user group that can access the VPN. For example, to allow access to users in the L2TP_group and assign them addresses in the range 192.168.0.50 to 192.168.0.59, enter:

```
config vpn l2tp
  set sip 192.168.0.50
  set eip 192.168.0.59
  set status enable
  set usrgrp "L2TP_group"
end
```

One of the security policies for the L2TP over IPsec VPN uses the client address range, so you need also need to create a firewall address for that range. For example,

```
config firewall address
  edit L2TPclients
    set type iprange
    set start-ip 192.168.0.50
    set end-ip 192.168.0.59
end
```

Alternatively, you could define this range in the web-based manager.

Configuring IPsec

The Microsoft VPN client uses IPsec for encryption. The configuration needed on the FortiGate unit is the same as for any other IPsec VPN with the following exceptions.

- Transport mode is used instead of tunnel mode.
- The encryption and authentication proposals must be compatible with the Microsoft client.

L2TP over IPsec is supported on the FortiGate unit using policy-based, not route-based configurations.

Configuring phase 1 - web-based manager

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)* and select *Create Phase 1*.
2. Enter the following information and then select *OK*.

Name	Enter a name for this VPN, dialup_p1 for example.
Remote Gateway	Dialup User
Local Interface	Select the network interface that connects to the Internet. For example, port1.
Mode	Main (ID protection)
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key. This key must also be entered in the Microsoft VPN client.
Advanced	Select *Advanced* to enter the following information.
Enable IPsec Interface Mode	This must ***not*** be selected.
P1 Proposal	Enter the following Encryption/Authentication pairs: AES256-MD5, 3DES-SHA1, AES192-SHA1
DH Group	2

NAT Traversal	Enable
Dead Peer Detection	Enable

Configuring phase 1 - CLI

To create a phase 1 configuration called dialup_p1 on a FortiGate unit that has port1 connected to the Internet, you would enter:

```
config vpn ipsec phase1
  edit dialup_p1
    set type dynamic
    set interface port1
    set mode main
    set psksecret ********
    set proposal aes256-md5 3des-sha1 aes192-sha1
    set dhgrp 2
    set nattraversal enable
    set dpd enable
end
```

Configuring phase 2 - web-based manager

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)* and select *Create Phase 2*.
2. Enter the following information and then select *OK*.

Name	Enter a name for this phase 2 configuration.
Phase 1	Select the name of the phase 1 configuration.
Advanced	Select *Advanced* to enter the following information.
P2 Proposal	Enter the following Encryption/Authentication pairs: AES256-MD5, 3DES-SHA1, AES192-SHA1
Enable replay detection	Enable
Enable perfect forward secrecy (PFS)	Disable
Keylife	3600 seconds

3. Make this a transport-mode VPN. You must use the CLI to do this. If your phase 2 name is dialup_p2, you would enter:

```
config vpn ipsec phase2
  edit dialup_p2
    set encapsulation transport-mode
  end
```

Configuring phase 2 - CLI

To configure a phase 2 to work with your phase_1 configuration, you would enter:

```
config vpn ipsec phase2
  edit dialup_p2
    set phase1name dialup_p1
    set proposal aes256-md5 3des-sha1 aes192-sha1
    set replay enable
    set pfs disable
    set keylifeseconds 3600
    set encapsulation transport-mode
  end
```

Configuring security policies

The security policies required for L2TP over IPsec VPN are:

- an IPSEC policy, as you would create for any policy-based IPsec VPN
- a regular ACCEPT policy to allow traffic from the L2TP clients to access the protected network

Configuring the IPSEC security policy - web-based manager

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Select the *Policy Type* as *VPN* and leave the *Policy Subtype* as *IPsec*.
3. Enter the following information and select *OK*:

Local Interface	Select the interface that connects to the private network behind this FortiGate unit.
Local Protected Subnet	All
Outgoing VPN Interface	Select the FortiGate unit's public interface.
Remote Protected Subnet	All
VPN Tunnel	Select *Use Existing* and select the name of the phase 1 configuration that you created. For example, dialup_p1. See "Configuring IPsec" on page 191.
Allow traffic to be initiated from the remote site	enable

Configuring the IPSEC security policy - CLI

If your VPN tunnel (phase 1) is called dialup_p1, your protected network is on port2, and your public interface is port1, you would enter:

```
config firewall policy
  edit 0
    set srcintf port2
    set dstintf port1
    set srcaddr all
    set dstaddr all
    set action ipsec
    set schedule always
    set service ANY
    set inbound enable
    set vpntunnel dialup_p1
  end
```

Configuring the ACCEPT security policy - web-based manager

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and leave the *Policy Subtype* as *Address*.
3. Enter the following information and select *OK*:

Incoming Interface	Select the FortiGate unit's public interface.
Source Address	Select the firewall address that you defined for the L2TP clients.
Outgoing Interface	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address	All
Action	ACCEPT

Configuring the ACCEPT security policy - CLI

If your public interface is port1, your protected network is on port2, and L2TPclients is the address range that L2TP clients use, you would enter:

```
config firewall policy
  edit 0
    set srcintf port1
    set dstintf port2
    set srcaddr L2TPclients
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
  end
```

Configuring the Windows PC

Configuration of the Windows PC for a VPN connection to the FortiGate unit consists of the following:

- In Network Connections, configure a Virtual Private Network connection to the FortiGate unit.
- Ensure that the IPSEC service is running.
- Ensure that IPsec has not been disabled for the VPN client. It may have been disabled to make the Microsoft VPN compatible with an earlier version of FortiOS.

The instructions in this section are based on Windows XP SP3. Other versions of Windows may vary slightly.

To configure the network connection

1. Open *Network Connections*.

   This is available through the Control Panel.
2. Double-click *New Connection Wizard* and *Select Next*.
3. Select *Connect to the network at my workplace*.
4. Select *Next*.
5. Select *Virtual Private Network connection* and select *Next*.
6. In the *Company Name* field, enter a name for the connection and select *Next*.
7. Select *Do not dial the initial connection* and then select *Next*.
8. Enter the public IP address or FQDN of the FortiGate unit and select *Next*.
9. Optionally, select *Add a shortcut to this connection to my desktop*.
10. Select *Finish*.

    The *Connect* dialog opens on the desktop.
11. Select *Properties* and then select the *Security* tab.
12. Select *IPSec Settings*.
13. Select *Use pre-shared key for authentication*, enter the preshared key that you configured for your VPN, and select *OK*.
14. Select *OK*.

To check that the IPSEC service is running

1. Open *Administrative Tools* through the Control Panel.
2. Double-click *Services*.
3. Look for IPSEC Services. Confirm that the *Startup Type* is *Automatic* and *Status* is set to *Started*. If needed, double-click *IPSEC Services* to change these settings.

To check that IPsec has not been disabled

1. Select *Start* > *Run*.
2. Enter regedit and select *OK*.
3. Find the Registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters
4. If there is a ProhibitIPSec value, it must be set to 0.

Troubleshooting

This section describes some checks and tools you can use to resolve issues with L2TP-over-IPsec VPNs.

This section includes:

Quick checks

The table below is a list of common L2TP over IPsec VPN problems and the possible solutions.

Problem	What to check
IPsec tunnel does not come up.	Check the logs to determine whether the failure is in Phase 1 or Phase 2. Check the settings, including encapsulation setting, which must be transport-mode. Check the user password. Confirm that the user is a member of the user group assigned to L2TP. On the Windows PC, check that the IPsec service is running and has not been disabled. See "Configuring the Windows PC" on page 195.
Tunnel connects, but there is no communication.	Did you create an ACCEPT security policy from the public network to the protected network for the L2TP clients? See "Configuring security policies" on page 193.

Mac OS X and L2TP

FortiOS allows L2TP connections with empty AVP host names and therefore Mac OS X L2TP connections can connect to the FortiGate.

Prior to FortiOS 4.0 MR3, FortiOS refused L2TP connections with empty AVP host names in compliance with RFC 2661 and RFC 3931.

Setting up logging

L2TP logging must be enabled to record L2TP events. Alert email can be configured to report L2TP errors.

To configure FortiGate logging for L2TP over IPsec

1. Go to *Log & Report* > *Log Config* > *Log Settings*.
2. Select *Event Log*.
3. Select the *VPN activity event* check box.
4. Select *Apply*.

To view FortiGate logs

1. Go to *Log & Report* > *Event Log* > *VPN*.
2. Select the *Log location* if required.
3. After each attempt to start the L2TP over IPsec VPN, select *Refresh* to view logged events.

Using the FortiGate unit debug commands

To view debug output for IKE and L2TP

1. Start an SSH or Telnet session to your FortiGate unit.
2. Enter the following CLI commands

```
diagnose debug application ike -1
diagnose debug application l2tp -1
diagnose debug enable
```

3. Attempt to use the VPN and note the debug output in the SSH or Telnet session.
4. Enter the following command to reset debug settings to default:

```
diagnose debug reset
```

To use the packet sniffer

1. Start an SSH or Telnet session to your FortiGate unit.
2. Enter the following CLI command

```
diagnose sniffer packet any icmp 4
```

3. Attempt to use the VPN and note the debug output.
4. Enter `Ctrl-C` to end sniffer operation.

Typical L2TP over IPsec session startup log entries - raw format

```
2010-01-11 16:39:58 log_id=0101037127 type=event subtype=ipsec
pri=notice vd="root" msg="progress IPsec phase 1" action="negotiate"
rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500
out_intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A"
group="N/A" xauth_user="N/A" xauth_group="N/A" vpn_tunnel="dialup_p1"
status=success init=remote mode=main dir=outbound stage=1
role=responder result=OK

2010-01-11 16:39:58 log_id=0101037127 type=event subtype=ipsec
pri=notice vd="root" msg="progress IPsec phase 1" action="negotiate"
rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500
out_intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A"
group="N/A" xauth_user="N/A" xauth_group="N/A" vpn_tunnel="dialup_p1"
status=success init=remote mode=main dir=outbound stage=2
role=responder result=OK

2010-01-11 16:39:58 log_id=0101037127 type=event subtype=ipsec
pri=notice vd="root" msg="progress IPsec phase 1" action="negotiate"
rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500
out_intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A"
group="N/A" xauth_user="N/A" xauth_group="N/A" vpn_tunnel="dialup_p1"
status=success init=remote mode=main dir=inbound stage=3 role=responder
result=DONE

2010-01-11 16:39:58 log_id=0101037127 type=event subtype=ipsec
pri=notice vd="root" msg="progress IPsec phase 1" action="negotiate"
rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500
out_intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A"
```

```
group="N/A" xauth_user="N/A" xauth_group="N/A" vpn_tunnel="dialup_p1_0"
status=success init=remote mode=main dir=outbound stage=3
role=responder result=DONE

2010-01-11 16:39:58 log_id=0101037129 type=event subtype=ipsec
pri=notice vd="root" msg="progress IPsec phase 2" action="negotiate"
rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500
out_intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A"
group="N/A" xauth_user="N/A" xauth_group="N/A" vpn_tunnel="dialup_p1_0"
status=success init=remote mode=quick dir=outbound stage=1
role=responder result=OK

2010-01-11 16:39:58 log_id=0101037133 type=event subtype=ipsec
pri=notice vd="root" msg="install IPsec SA" action="install_sa"
rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500
out_intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A"
group="N/A" xauth_user="N/A" xauth_group="N/A" vpn_tunnel="dialup_p1_0"
role=responder in_spi=61100fe2 out_spi=bd70fca1

2010-01-11 16:39:58 log_id=0101037139 type=event subtype=ipsec
pri=notice vd="root" msg="IPsec phase 2 status change"
action="phase2-up" rem_ip=172.20.120.151 loc_ip=172.20.120.141
rem_port=500 loc_port=500 out_intf="port1"
cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A" group="N/A"
xauth_user="N/A" xauth_group="N/A" vpn_tunnel="dialup_p1_0"
phase2_name=dialup_p2

2010-01-11 16:39:58 log_id=0101037138 type=event subtype=ipsec
pri=notice vd="root" msg="IPsec connection status change"
action="tunnel-up" rem_ip=172.20.120.151 loc_ip=172.20.120.141
rem_port=500 loc_port=500 out_intf="port1"
cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A" group="N/A"
xauth_user="N/A" xauth_group="N/A" vpn_tunnel="dialup_p1_0"
tunnel_ip=172.20.120.151 tunnel_id=1552003005 tunnel_type=ipsec
duration=0 sent=0 rcvd=0 next_stat=0 tunnel=dialup_p1_0

2010-01-11 16:39:58 log_id=0101037129 type=event subtype=ipsec
pri=notice vd="root" msg="progress IPsec phase 2" action="negotiate"
rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500
out_intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A"
group="N/A" xauth_user="N/A" xauth_group="N/A" vpn_tunnel="dialup_p1_0"
status=success init=remote mode=quick dir=inbound stage=2
role=responder result=DONE

2010-01-11 16:39:58 log_id=0101037122 type=event subtype=ipsec
pri=notice vd="root" msg="negotiate IPsec phase 2" action="negotiate"
rem_ip=172.20.120.151 loc_ip=172.20.120.141 rem_port=500 loc_port=500
out_intf="port1" cookies="5f6da1c0e4bbf680/d6a1009eb1dde780" user="N/A"
group="N/A" xauth_user="N/A" xauth_group="N/A" vpn_tunnel="dialup_p1_0"
status=success role=responder esp_transform=ESP_3DES esp_auth=HMAC_SHA1

2010-01-11 16:39:58 log_id=0103031008 type=event subtype=ppp vd=root
pri=information action=connect status=success msg="Client
172.20.120.151 control connection started (id 805), assigned ip
192.168.0.50"

2010-01-11 16:39:58 log_id=0103029013 type=event subtype=ppp vd=root
pri=notice pppd is started

2010-01-11 16:39:58 log_id=0103029002 type=event subtype=ppp vd=root
pri=notice user="user1" local=172.20.120.141 remote=172.20.120.151
```

```
assigned=192.168.0.50 action=auth_success msg="User 'user1' using l2tp
with authentication protocol MSCHAP_V2, succeeded"

2010-01-11 16:39:58 log_id=0103031101 type=event subtype=ppp vd=root
pri=information action=tunnel-up tunnel_id=1645784497 tunnel_type=l2tp
remote_ip=172.20.120.151 tunnel_ip=192.168.0.50 user="user1"
group="L2TPusers" msg="L2TP tunnel established"
```

GRE over IPsec (Cisco VPN)

This section describes how to configure a FortiGate VPN that is compatible with Cisco-style VPNs that use GRE in an IPsec tunnel.

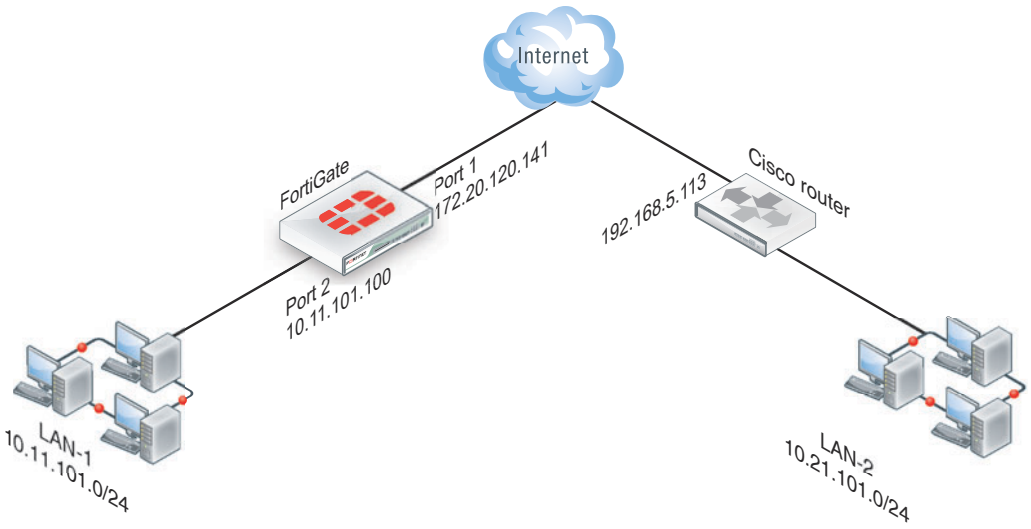
The following topics are included in this section:

Overview

Cisco products that include VPN support often use Generic Routing Encapsulation (GRE) protocol tunnel over IPsec encryption. This chapter describes how to configure a FortiGate unit to work with this type of Cisco VPN.

Cisco VPNs can use either transport mode or tunnel mode IPsec. Before FortiOS 4.0 MR2, the FortiGate unit was compatible only with tunnel mode IPsec.

Figure 33: Example FortiGate to Cisco GRE-over-IPsec VPN



In this example, users on LAN-1 are provided access to LAN-2.

Configuring the FortiGate unit

There are several steps to the GRE-over-IPsec configuration:

- Enable overlapping subnets. This is needed because the IPsec and GRE tunnels will use the same addresses.
- Configure a route-based IPsec VPN on the external interface.
- Configure a GRE tunnel on the virtual IPsec interface. Set its local gateway and remote gateway addresses to match the local and remote gateways of the IPsec tunnel.
- Configure security policies to allow traffic to pass in both directions between the GRE virtual interface and the IPsec virtual interface.
- Configure security policies to allow traffic to pass in both directions between the protected network interface and the GRE virtual interface.
- Configure a static route to direct traffic destined for the network behind the Cisco router into the GRE-over-IPsec tunnel.

Enabling overlapping subnets

By default, each FortiGate unit network interface must be on a separate network. The configuration described in this chapter assigns an IPsec tunnel end point and the external interface to the same network. Enable subnet overlap as follows:

```
config system settings
  set allow-subnet-overlap enable
end
```

Configuring the IPsec VPN

A route-based VPN is required. It must use encryption and authentication algorithms compatible with the Cisco equipment to which it connects. In this chapter, preshared key authentication is shown.

To configure the IPsec VPN - web-based manager

1. Define the phase 1 configuration needed to establish a secure connection with the remote Cisco device. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel, tocisco for example. This is the name of the virtual IPsec interface. It appears in phase 2 configurations, security policies and the VPN monitor.
Remote Gateway	Select *Static IP Address*.
IP Address	Enter the IP address of the Cisco device public interface. For example, 192.168.5.113.
Local Interface	Select the FortiGate unit's public interface. For example, 172.20.120.141.
Mode	Select *Main (ID Protection)*.
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key. It must match the preshared key on the Cisco device.

Advanced	Select the Advanced button to see the following settings.
Enable IPsec Interface Mode	Enable.
P1 Proposal	3DES-MD5 At least one proposal must match the settings on the Cisco unit.

For more information about these settings, see "Auto Key phase 1 parameters" on page 36.

2. Define the phase 2 parameters needed to create a VPN tunnel with the remote peer. For compatibility with the Cisco router, Quick Mode Selectors must be entered, which includes specifying protocol 47, the GRE protocol. 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 in Step 1.
Advanced	Select *Advanced* to view the following fields.
P2 Proposal	*3DES-MD5* At least one proposal must match the settings on the Cisco unit.
Quick Mode Selector	
Source Address	Enter the GRE local tunnel end IP address. For example 172.20.120.141.
Source Port	0
Destination Address	Enter the GRE remote tunnel end IP address. For example 192.168.5.113.
Destination Port	0
Protocol	47

For more information about these settings, see "Phase 2 parameters" on page 52.

3. If the Cisco device is configured to use transport mode IPsec, you need to use transport mode on the FortiGate VPN. You can configure this only in the CLI. In your phase 2 configuration, set `encapsulation` to `transport-mode` as follows:

```
config vpn phase2-interface
  edit to_cisco_p2
    set encapsulation transport-mode
  end
```

To configure the IPsec VPN - CLI

```
config vpn ipsec phase1-interface
  edit tocisco
    set interface port1
    set proposal 3des-sha1 aes128-sha1
    set remote-gw 192.168.5.113
    set psksecret xxxxxxxxxxxxxxx
  end
config vpn ipsec phase2-interface
  edit tocisco_p2
    set phase1name "tocisco"
    set proposal 3des-md5
    set encapsulation tunnel-mode      // if tunnel mode
    set encapsulation transport-mode   // if transport mode
    set protocol 47
    set src-addr-type ip
    set dst-start-ip 192.168.5.113
    set src-start-ip 172.20.120.141
  end
```

Adding IPsec tunnel end addresses

The Cisco configuration requires an address for its end of the IPsec tunnel. The addresses are set to match the GRE gateway addresses. Use the CLI to set the addresses, like this:

```
config system interface
  edit tocisco
    set ip 172.20.120.141 255.255.255.255
    set remote-ip 192.168.5.113
  end
```

Configuring the GRE tunnel

The GRE tunnel runs between the virtual IPsec public interface on the FortiGate unit and the Cisco router. You must use the CLI to configure a GRE tunnel. In the example, you would enter:

```
config system gre-tunnel
  edit gre1
    set interface tocisco
    set local-gw 172.20.120.141
    set remote-gw 192.168.5.113
end
```

`interface` is the virtual IPsec interface, `local-gw` is the FortiGate unit public IP address, and `remote-gw` is the remote Cisco device public IP address

Adding GRE tunnel end addresses

You will also need to add tunnel end addresses. The Cisco router configuration requires an address for its end of the GRE tunnel. Using the CLI, enter tunnel end addresses that are not used elsewhere on the FortiGate unit, like this:

```
config system interface
  edit gre1
    set ip 10.0.1.1 255.255.255.255
    set remote-ip 10.0.1.2
  end
```

Configuring security policies

Two sets of security policies are required:

- policies to allow traffic to pass in both directions between the GRE virtual interface and the IPsec virtual interface.
- policies to allow traffic to pass in both directions between the protected network interface and the GRE virtual interface.

To configure security policies - web-based manager

1. Define an ACCEPT firewall security policy to permit communications between the protected network and the GRE tunnel:

Incoming Interface	Select the interface that connects to the private network behind this FortiGate unit.
Source Address	All
Outgoing Interface	Select the GRE tunnel virtual interface you configured.
Destination Address	All
Action	ACCEPT
Enable NAT	Disable

2. To permit the remote client to initiate communication, you need to define a firewall address security policy for communication in that direction:

Incoming Interface	Select the GRE tunnel virtual interface you configured.
Source Address	All
Outgoing Interface	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address	All
Action	ACCEPT
Enable NAT	Disable

3. Define a pair of ACCEPT firewall address security policies to permit traffic to flow between the GRE virtual interface and the IPsec virtual interface:

Incoming Interface	Select the GRE virtual interface. See "Configuring the GRE tunnel" on page 203.
Source Address	All
Outgoing Interface	Select the virtual IPsec interface you created. See "Configuring the IPsec VPN" on page 201.
Destination Address	All
Action	ACCEPT
Enable NAT	Disable

Incoming Interface	Select the virtual IPsec interface you created. See "Configuring the IPsec VPN" on page 201.
Source Address	All
Outgoing Interface	Select the GRE virtual interface. See "Configuring the GRE tunnel" on page 203.
Destination Address	All
Action	ACCEPT
Enable NAT	Disable

To configure security policies - CLI

```
config firewall policy
  edit 1                    // LAN to GRE tunnel
    set srcintf port2
    set dstintf gre1
    set srcaddr all
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
  next
  edit 2                    // GRE tunnel to LAN
    set srcintf gre1
    set dstintf port2
    set srcaddr all
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
  next
```

```
edit 3                    // GRE tunnel to IPsec interface
   set srcintf "gre1"
   set dstintf "tocisco"
   set srcaddr "all"
   set dstaddr "all"
   set action accept
   set schedule "always"
   set service "ANY"
next
edit 4                    // IPsec interface to GRE tunnel
   set srcintf "tocisco"
   set dstintf "gre1"
   set srcaddr "all"
   set dstaddr "all"
   set action accept
   set schedule "always"
   set service "ANY"
end
```

Configuring routing

Traffic destined for the network behind the Cisco router must be routed to the GRE tunnel. To do this, create a static route

1. Go to *Router* > *Static* > *Static Routes* and select *Create New*.

   For low-end FortiGate units, go to *System* > *Network* > *Routing* and select *Create New*.
2. Enter the following information and select OK.

Destination IP/Mask	Enter the IP address and netmask for the network behind the Cisco router. For example 10.21.101.0 255.255.255.0.
Device	Select the GRE virtual interface.
Distance (Advanced)	Leave setting at default value.

In the CLI, using the example values, you would enter

```
config router static
  edit 0
    set device gre1
    set dst 10.21.101.0 255.255.255.0
  end
```

Configuring the Cisco router

Using Cisco IOS, you would configure the Cisco router as follows, using the addresses from the example:

```
config ter
crypto ipsec transform-set myset esp-3des esp-md5-hmac
no mode
exit
no ip access-list extended tunnel
ip access-list extended tunnel
permit gre host 192.168.5.113 host 172.20.120.141
exit
interface Tunnel1
ip address 10.0.1.2 255.255.255.0
tunnel source 192.168.5.113
tunnel destination 172.20.120.141
!
ip route 10.11.101.0 255.255.255.0 Tunnel1
end
clea crypto sa
clea crypto isakmp
```

For transport mode, change `no mode` to `mode transport`.

This is only the portion of the Cisco router configuration that applies to the GRE-over-IPsec tunnel. For more information, refer to the Cisco documentation.

Troubleshooting

This section describes some checks and tools you can use to resolve issues with the GRE-over-IPsec VPN.

Quick checks

Here is a list of common problems and what to verify.

Problem	What to check
No communication with remote network.	Use the `execute ping` command to ping the Cisco device public interface. Use the FortiGate VPN Monitor page to see whether the IPsec tunnel is up or can be brought up.

IPsec tunnel does not come up.	Check the logs to determine whether the failure is in Phase 1 or Phase 2. Check that the encryption and authentication settings match those on the Cisco device. Check the encapsulation setting: tunnel-mode or transport-mode. Both devices must use the same mode.
Tunnel connects, but there is no communication.	Check the security policies. See "Configuring security policies" on page 204. Check routing. See "Configuring routing" on page 206.

Setting up logging

To configure FortiGate logging for IPsec

1. Go to *Log & Report* > *Log Config* > *Log Settings*.
2. Select the *Event Logging*.
3. Select *VPN activity event*.
4. Select *Apply*.

To view FortiGate logs

1. Go to *Log & Report* > *Event Log* > *VPN*.
2. Select the log storage type.
3. Select *Refresh* to view any logged events.

Using diagnostic commands

There are some diagnostic commands that can provide useful information. When using diagnostic commands, it is best practice that you connect to the CLI using a terminal program, such as puTTY, that allows you to save output to a file. This will allow you to review the data later on at your own speed without worry about missed data as the diag output scrolls by.

To use the packet sniffer

1. Enter the following CLI command:
   ```
   diag sniff packet any icmp 4
   ```
2. Ping an address on the network behind the FortiGate unit from the network behind the Cisco router.

The output will show packets coming in from the GRE interface going out of the interface that connects to the protected network (LAN) and vice versa. For example:

```
114.124303 gre1 in 10.0.1.2 -> 10.11.101.10: icmp: echo request
114.124367 port2 out 10.0.1.2 -> 10.11.101.10: icmp: echo request
114.124466 port2 in 10.11.101.10 -> 10.0.1.2: icmp: echo reply
114.124476 gre1 out 10.11.101.10 -> 10.0.1.2: icmp: echo reply
```

3. Enter `CTRL-C` to stop the sniffer.

To view debug output for IKE

1. Enter the following CLI commands
   ```
   diagnose debug application ike -1
   diagnose debug enable
   ```

2. Attempt to use the VPN or set up the VPN tunnel and note the debug output.
3. Enter CTRL-C to stop the debug output.
4. Enter the following command to reset debug settings to default:

```
diagnose debug reset
```

Protecting OSPF with IPsec

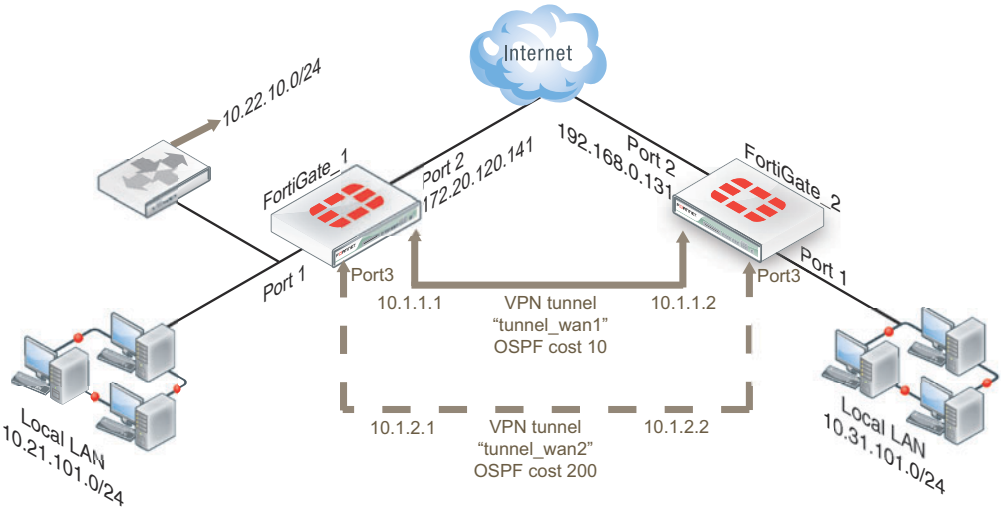
For enhanced security, OSPF dynamic routing can be carried over IPsec VPN links.

The following topics are included in this section:

Overview

This chapter shows an example of OSPF routing conducted over an IPsec tunnel between two FortiGate units. The network shown in Figure 34 is a single OSPF area. FortiGate_1 is an Area border router that advertises a static route to 10.22.10.0/24 in OSPF. FortiGate_2 advertises its local LAN as an OSPF internal route.

Figure 34:OSPF over an IPsec VPN tunnel



The section "OSPF over IPsec configuration" describes the configuration with only one IPsec VPN tunnel, tunnel_wan1. Then, the section "Creating a redundant configuration" on page 216 describes how you can add a second tunnel to provide a redundant backup path. This is shown in Figure 34 as VPN tunnel "tunnel_wan2".

Only the parts of the configuration concerned with creating the IPsec tunnel and integrating it into the OSPF network are described. It is assumed that security policies are already in place to allow traffic to flow between the interfaces on each FortiGate unit.

OSPF over IPsec configuration

There are several steps to the OSPF-over-IPsec configuration:

- Configure a route-based IPsec VPN on an external interface. It will connect to a corresponding interface on the other FortiGate unit. Define the two tunnel-end addresses.
- Configure a static route to the other FortiGate unit.
- Configure the tunnel network as part of the OSPF network and define the virtual IPsec interface as an OSPF interface.

This section describes the configuration with only one VPN, tunnel_wan1. The other VPN is added in the section "Creating a redundant configuration" on page 216.

Configuring the IPsec VPN

A route-based VPN is required. In this chapter, preshared key authentication is shown. Certificate authentication is also possible. Both FortiGate units need this configuration.

To configure Phase 1

1 Define the phase 1 configuration needed to establish a secure connection with the other FortiGate unit. For more information, see "Auto Key phase 1 parameters" on page 36. Enter these settings in particular:

Name	Enter a name to identify the VPN tunnel, tunnel_wan1 for example. This becomes the name of the virtual IPsec interface.
Remote Gateway	Select *Static IP Address*.
IP Address	Enter the IP address of the other FortiGate unit's public (Port 2) interface.
Local Interface	Select this FortiGate unit's public (Port 2) interface.
Mode	Select *Main (ID Protection)*.
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key. It must match the preshared key on the other FortiGate unit.
Advanced	Select *Advanced*.
Enable IPsec Interface Mode	Enable

To assign the tunnel end IP addresses

1. Go to *System* > *Network* > *Interfaces,* select the virtual IPsec interface that you just created on Port 2 and select *Edit*.
2. In the *IP* and *Remote IP* fields, enter the following tunnel end addresses:

	FortiGate_1	FortiGate_2
IP	10.1.1.1	10.1.1.2
Remote_IP	10.1.1.2	10.1.1.1

These addresses are from a network that is not used for anything else.

To configure Phase 2

1. Enter a name to identify this phase 2 configuration, twan1_p2, for example.
2. Select the name of the phase 1 configuration that you defined in Step 1, tunnel_wan1 for example.

Configuring static routing

You need to define the route for traffic leaving the external interface.

1. Go to *Router* > *Static* > *Static Route*s, select *Create New*.
2. For low-end FortiGate units, go to *System* > *Network* > *Routing* and select *Create New*.
3. Enter the following information.

Destination IP/Mask	Leave as 0.0.0.0 0.0.0.0.
Device	Select the external interface.
Gateway	Enter the IP address of the next hop router.

Configuring OSPF

This section does not attempt to explain OSPF router configuration. It focusses on the integration of the IPsec tunnel into the OSPF network. This is accomplished by assigning the tunnel as an OSPF interface, creating an OSPF route to the other FortiGate unit.

This configuration uses loopback interfaces to ease OSPF troubleshooting. The OSPF router ID is set to the loopback interface address.The loopback interface ensures the router is always up. Even though technically the router ID doesn't have to match a valid IP address on the FortiGate unit, having an IP that matches the router ID makes troubleshooting a lot easier.

The two FortiGate units have slightly different configurations. FortiGate_1 is an AS border router that advertises its static default route. FortiGate_2 advertises its local LAN as an OSPF internal route.

Setting the router ID for each FortiGate unit to the lowest possible value is useful if you want the FortiGate units to be the designated router (DR) for their respective ASes. This is the router that broadcasts the updates for the AS.

Leaving the IP address on the OSPF interface at 0.0.0.0 indicates that all potential routes will be advertised, and it will not be limited to any specific subnet. For example if this IP address was 10.1.0.0, then only routes that match that subnet will be advertised through this interface in OSPF.

FortiGate_1 OSPF configuration

When configuring FortiGate_1 for OSPF, the loopback interface is created, and then you configure OSPF area networks and interfaces.

With the exception of creating the loopback interface, OSPF for this example can all be configured in either the web-based manager or CLI.

To create the loopback interface

A loopback interface can be configured in the CLI only. For example, if the interface will have an IP address of 10.0.0.1, you would enter:

```
config system interface
  edit lback1
   set vdom root
    set ip 10.0.0.1 255.255.255.255
    set type loopback
  end
```

The loopback addresses and corresponding router IDs on the two FortiGate units must be different. For example, set the FortiGate 1 loopback to 10.0.0.1 and the FortiGate 2 loopback to 10.0.0.2.

To configure OSPF area, networks, and interfaces - web-based manager

1. On FortiGate_1, go to *Router* > *Dynamic* > *OSPF*.

   For low end FortiGate units, you first need to enable *Dynamic Routing* by going to *System* > *Admin* > *Settings*.
2. Enter the following information to define the router, area, and interface information.

Router ID	Enter `10.0.0.1`. Select *Apply* before entering the remaining information.
Advanced Options	
Redistribute	Select the *Connected* and *Static* check boxes. Use their default metric values.
Areas	Select *Create New*, enter the *Area* and *Type* and then select *OK*.
Area	0.0.0.0
Type	Regular
Interfaces	Enter a name for the OSPF interface, ospf_wan1 for example.
Name	
Interface	Select the virtual IPsec interface, tunnel_wan1.
IP	0.0.0.0

3. For *Networks*, select *Create New*.
4. Enter the *IP/Netmask* of `10.1.1.0/255.255.255.0` and an *Area* of `0.0.0.0`.
5. For *Networks*, select *Create New*.
6. Enter the *IP/Netmask* of `10.0.0.1/255.255.255.0` and an *Area* of `0.0.0.0`.
7. Select *Apply*.

To configure OSPF area and interfaces - CLI

Your loopback interface is 10.0.0.1, your tunnel ends are on the 10.1.1.0/24 network, and your virtual IPsec interface is named `tunnel_wan1`. Enter the following CLI commands:

```
config router ospf
  set router-id 10.0.0.1
  config area
    edit 0.0.0.0
  end
  config network
    edit 4
      set prefix 10.1.1.0 255.255.255.0
    next
    edit 2
      set prefix 10.0.0.1 255.255.255.255
    end
  config ospf-interface
    edit ospf_wan1
      set cost 10
      set interface tunnel_wan1
      set network-type point-to-point
    end
  config redistribute connected
    set status enable
  end
  config redistribute static
    set status enable
  end
end
```

FortiGate_2 OSPF configuration

When configuring FortiGate_2 for OSPF, the loopback interface is created, and then you configure OSPF area networks and interfaces.

Configuring FortiGate_2 differs from FortiGate_1 in that three interfaces are defined instead of two. The third interface is the local LAN that will be advertised into OSPF.

With the exception of creating the loopback interface, OSPF for this example can all be configured in either the web-based manager or CLI.

To create the loopback interface

A loopback interface can be configured in the CLI only. For example, if the interface will have an IP address of 10.0.0.2, you would enter:

```
config system interface
  edit lback1
    set vdom root
    set ip 10.0.0.2 255.255.255.255
    set type loopback
  end
```

The loopback addresses on the two FortiGate units must be different. For example, set the FortiGate 1 loopback to 10.0.0.1 and the FortiGate 2 loopback to 10.0.0.2.

To configure OSPF area and interfaces - web-based manager

1. On FortiGate_2, go to *Router* > *Dynamic* > *OSPF*.

   For low end FortiGate units, you first need to enable *Dynamic Routing* by going to *System* > *Admin* > *Settings*.

2. Complete the following.

Router ID	10.0.0.2
Areas	Select *Create New*, enter the *Area* and *Type* and then select *OK*.
Area	0.0.0.0
Type	Regular
Interfaces	
Name	Enter a name for the OSPF interface, ospf_wan1 for example.
Interface	Select the virtual IPsec interface, tunnel_wan1.
IP	0.0.0.0

3. For *Networks*, select *Create New*.
4. Enter the following information for the loopback interface:

IP/Netmask	10.0.0.2/255.255.255.255
Area	0.0.0.0

5. For *Networks*, select *Create New*.
6. Enter the following information for the tunnel interface:

IP/Netmask	10.1.1.0/255.255.255.255
Area	0.0.0.0

7. For *Networks*, select *Create New*.
8. Enter the following information for the local LAN interface:

IP/Netmask	10.31.101.0/255.255.255.255
Area	0.0.0.0

9. Select *Apply*.

To configure OSPF area and interfaces - CLI

If for example, your loopback interface is 10.0.0.2, your tunnel ends are on the 10.1.1.0/24 network, your local LAN is 10.31.101.0/24, and your virtual IPsec interface is named tunnel_wan1, you would enter:

```
config router ospf
  set router-id 10.0.0.2
  config area
    edit 0.0.0.0
  end
  config network
    edit 1
      set prefix 10.1.1.0 255.255.255.0
    next
    edit 2
      set prefix 10.31.101.0 255.255.255.0
    next
    edit 2
      set prefix 10.0.0.2 255.255.255.255
    end
  config ospf-interface
    edit ospf_wan1
      set interface tunnel_wan1
      set network-type point-to-point
    end
end
```

Creating a redundant configuration

You can improve the reliability of the OSPF over IPsec configuration described in the previous section by adding a second IPsec tunnel to use if the default one goes down. Redundancy in this case is not controlled by the IPsec VPN configuration but by the OSPF routing protocol.

To do this you:

- Create a second route-based IPsec tunnel on a different interface and define tunnel end addresses for it.
- Add the tunnel network as part of the OSPF network and define the virtual IPsec interface as an additional OSPF interface.
- Set the OSPF cost for the added OSPF interface to be significantly higher than the cost of the default route.

Adding the second IPsec tunnel

The configuration is the same as in “Configuring the IPsec VPN” on page 211, but the interface and addresses will be different. Ideally, the network interface you use is connected to a different Internet service provider for added redundancy.

When adding the second tunnel to the OSPF network, choose another unused subnet for the tunnel ends, 10.1.2.1 and 10.1.2.2 for example.

Adding the OSPF interface

OSPF uses the metric called cost when determining the best route, with lower costs being preferred. Up to now in this example, only the default cost of 10 has been used. Cost can be set only in the CLI.

The new IPsec tunnel will have its OSPF cost set higher than that of the default tunnel to ensure that it is only used if the first tunnel goes down. The new tunnel could be set to a cost of 200 compared to the default cost is 10. Such a large difference in cost will ensure this new tunnel will only be used as a last resort.

If the new tunnel is called tunnel_wan2, you would enter the following on both FortiGate units:

```
config router ospf
  config ospf-interface
    edit ospf_wan2
      set cost 200
      set interface tunnel_wan2
      set network-type point-to-point
    end
  end
```

Hardware offloading and acceleration

FortiGate units incorporate proprietary FortiASIC NPx network processors that can provide accelerated processing for IPsec VPN traffic. This section describes how to configure offloading and acceleration.

The following topics are included in this section:

Overview

Fortinet's NPx network processors contain features to improve IPsec tunnel performance. For example, network processors can encrypt and decrypt packets, offloading cryptographic work from the FortiGate unit's main processing resources.

On FortiGate units with the appropriate hardware, you can configure offloading of both IPsec sessions and HMAC checking.

IPsec session offloading requirements

Sessions must be fast path ready. Fast path ready session requirements are:

- Layer 2 type/length must be 0x0800 (IEEE 802.1q VLAN specification is supported); link aggregation between any network interfaces sharing the same network processor(s) may be used (IEEE 802.3ad specification is supported)
- Layer 3 protocol must be IPv4
- Layer 4 protocol must be UDP, TCP or ICMP
- Layer 3 / Layer 4 header or content modification must not require a session helper (for example, SNAT, DNAT, and TTL reduction are supported, but application layer content modification is not supported)
- FortiGate unit security policy must not require antivirus or IPS inspection, although hardware accelerated anomaly checks are acceptable.
- The session must not use an aggregated link or require QoS, including rate limits and bandwidth guarantees (NP1 processor only).
- Ingress and egress network interfaces are both attached to the same network processor(s)
- In Phase I configuration, Local Gateway IP must be specified as an IP address of a network interface attached to a network processor
- In Phase II configuration:
  - encryption algorithm must be DES, 3DES, AES-128, AES-192, AES-256, or null (for NP1 processor, only 3DES is supported)
  - authentication must be MD5, SHA1, or null (for NP1 processor, only MD5 is supported)
  - if replay detection is enabled, encryption and decryption options must be enabled in the CLI (see "IPsec encryption offloading", below)

  If the IPsec session meets the above requirements, the FortiGate unit sends the IPsec security association (SA) and configured processing actions to the network processors.

Packet offloading requirements

In addition to the session requirements, the packets themselves must meet fast-path requirements:

- Incoming packets must not be fragmented.
- Outgoing packets must be 385 bytes or larger after any fragmentation. This means the configured MTU (Maximum Transmission Unit) for the network processors' interfaces must have an MTU of 385 bytes or larger.

If packet offloading requirements are not met, an individual packet will use the FortiGate unit main processing resources, regardless of whether other packets in the session are offloaded to the specialized network processors.

IPsec encryption offloading

Network processing unit (NPU) settings configure offloading behavior for IPsec VPNs. Configured behavior applies to all network processors contained by the FortiGate unit itself or any installed AMC modules.

If replay detection is not enabled (IPsec Phase 2 settings), encryption is always offloaded. NPU offloading is supported when the local gateway is a loopback interface.

To enable offloading of encryption even when replay detection is enabled

```
config system npu
  set enc-offload-antireplay enable
  set offload-ipsec-host enable
end
```

To enable offloading of decryption even when replay detection is enabled

```
config system npu
  set dec-offload-antireplay enable
end
```

HMAC check offloading

The Hash-based Message Authentication Code (HMAC) check can also be offloaded to hardware. SHA-256, SHA-384, or SHA-512 cannot be off-loaded to hardware, and must be processed using only software resources.

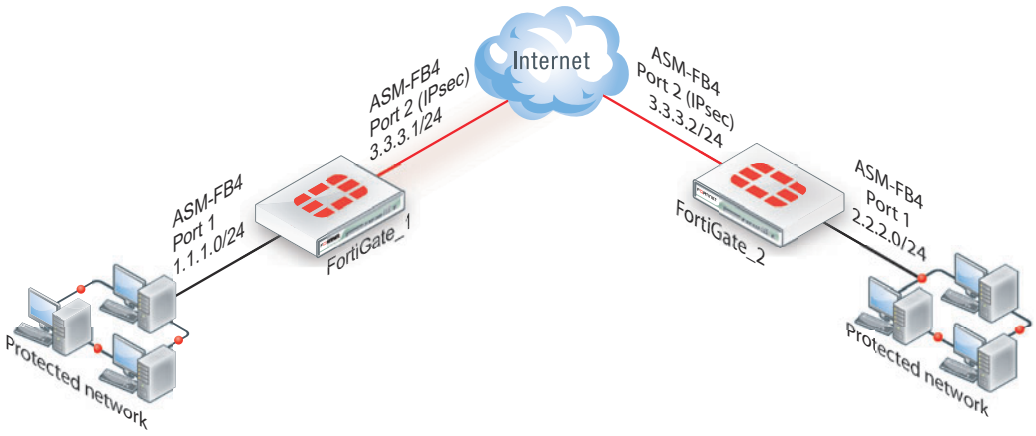
To enable HMAC check offloading

```
configure system global
  set ipsec-hmac-offload (enable|disable)
end
```

IPsec offloading configuration examples

The following examples configure two FortiASIC NPx network processor accelerated VPNs, one route-based, the other policy based. In both cases, the network topology is as shown in Figure 35.

Figure 35: Hardware accelerated IPsec VPN topology



Accelerated route-based VPN configuration

This example uses the accelerated ports on FortiGate-ASM-FB4 modules in each FortiGate unit. These accelerated ports on the modules are paired interfaces that have their own network processor (NPU) to offload work from the FortiGate unit CPU. Beyond this fact, the example is normal VPN example.

Configuring the FortiGate units require the same basic steps:

- Configure VPN Phase 1
- Configure VPN Phase 2
- Create security policies to allow traffic to flow
- Create a static route to allow traffic to flow

When both FortiGates are have the VPN tunnel configured, test to ensure it is working properly.

To configure FortiGate_1

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)* and select *Create Phase 1*.
2. Configure Phase 1 settings (name FGT_1_IPsec), plus
   - Select *Advanced*.
   - Select *Enable IPsec Interface Mode*.
   - In *Local Gateway IP*, select *Specify* and enter the VPN IP address 3.3.3.1, which is the IP address of FortiGate_1's FortiGate-ASM-FB4 module on port 2.
3. Select *OK*.
4. Select *Create Phase 2* and configure Phase 2 settings, including
   - Select *Enable replay detection*.
   - set `enc-offload-antireplay` to `enable` using the `config system npu` CLI command.
5. Go to *Policy* > *Policy* > *Policy*.
6. Configure two firewall address policies (one for each direction) to apply the Phase 1 IPsec configuration you configured in step 2 to traffic leaving from or arriving on FortiGate-ASM-FB4 module port 1.
7. Go to *Router* > *Static* > *Static Routes*.

   For low-end FortiGate units, go to *System* > *Network* > *Routing*.

8. Configure a static route to route traffic destined for FortiGate_2's protected network to the virtual IPsec interface, FGT_1_IPsec.

To add the static route from the CLI:

```
config router static
  edit 2
    set device "FGT_1_IPsec"
    set dst 2.2.2.0 255.255.255.0
end
```

To configure FortiGate_2

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)* and select *Create Phase 1*.
2. Configure Phase 1 settings (name FGT_2_IPsec), plus
   - Select *Advanced*.
   - Select *Enable IPsec Interface Mode*.
   - In *Local Gateway IP*, select *Specify* and enter the VPN IP address 3.3.3.2, which is the IP address of FortiGate_2's FortiGate-ASM-FB4 module on port 2.
3. Select *OK*.
4. Select *Create Phase 2* and configure Phase 2 settings, including
   - Select *Enable replay detection*.
   - set `enc-offload-antireplay` to `enable` using the `config system npu` CLI command.
5. Go to *Policy* > *Policy* > *Policy*.
6. Configure two firewall address policies (one for each direction) to apply the Phase 1 IPsec configuration you configured in step 2 to traffic leaving from or arriving on FortiGate-ASM-FB4 module port 1.
7. Go to *Router* > *Static* > *Static Route*s.
8. Configure a static route to route traffic destined for FortiGate_1's protected network to the virtual IPsec interface, FGT_2_IPsec.

To add the static route from the CLI:

```
config router static
  edit 2
    set device "FGT_2_IPsec"
    set dst 1.1.1.0 255.255.255.0
  end
```

To test the VPN

1. Activate the IPsec tunnel by sending traffic between the two protected networks.
2. To verify tunnel activation, go to *VPN* > *Monitor* > *IPsec Monitor*.

Accelerated policy-based VPN configuration

To configure FortiGate_1

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)* and select *Create Phase 1*.
2. Configure Phase 1 settings (name FGT_1_IPsec), plus
   - Select *Advanced*.
   - Ensure that the *Enable IPsec Interface Mode* check box is not selected.
   - In *Local Gateway IP*, select *Specify* and enter the VPN IP address 3.3.3.1, which is the IP address of FortiGate_1's FortiGate-ASM-FB4 module on port 2.
3. Select *OK*.
4. Select Create *Phase 2* and configure Phase 2 settings, including
   - Select *Enable replay detection*.
   - set `enc-offload-antireplay` to `enable` using the `config system npu` CLI command.
5. Go to *Policy* > *Policy* > *Policy*.
6. Configure an IPsec VPN policy to apply the Phase 1 IPsec tunnel you configured in step 2 to traffic between FortiGate-ASM-FB4 module ports 1 and 2.
7. Go to *Router* > *Static* > *Static Routes*.

   For low-end FortiGate units, go to *System* > *Network* > *Routing*.
8. Configure a static route to route traffic destined for FortiGate_2's protected network to FortiGate_2's VPN gateway, 3.3.3.2, through the FortiGate-ASM-FB4 module's port 2 (device).

To add the static route from the CLI:

```
config router static
  edit 0
    set device "AMC-SW1/2"
    set dst 2.2.2.0 255.255.255.0
    set gateway 3.3.3.1
  end
```

To configure FortiGate_2

1. Go to *VPN* > *IPsec* > *Auto Key (IKE)* and select *Create Phase 1*.
2. Configure Phase 1 settings (name FGT_2_IPsec), plus
   - Select *Advanced*.
   - Select *Enable IPsec Interface Mode*.
   - In *Local Gateway IP*, select *Specify* and enter the VPN IP address 3.3.3.2, which is the IP address of FortiGate_2's FortiGate-ASM-FB4 module on port 2.
3. Select *OK*.
4. Select *Create Phase 2* and configure Phase 2 settings, including
   - Select *Enable replay detection*.
   - set `enc-offload-antireplay` to `enable` using the `config system npu` CLI command.
5. Go to *Policy* > *Policy* > *Policy*.
6. Configure an IPsec VPN policy to apply the Phase 1 IPsec tunnel you configured in step 2 to traffic between FortiGate-ASM-FB4 module ports 1 and 2.

7. Go to *Router* > *Static* > *Static Route*s.

   For low-end FortiGate units, go to *System* > *Network* > *Routing*.

8. Configure a static route to route traffic destined for FortiGate_1's protected network to FortiGate_2's VPN gateway, 3.3.3.2, through the FortiGate-ASM-FB4 module's port 2 (device).

To add the static route from the CLI:

```
config router static
  edit 0
    set device "AMC-SW1/2"
    set dst 1.1.1.0 255.255.255.0
    set gateway 3.3.3.2
  end
```

To test the VPN

1. Activate the IPsec tunnel by sending traffic between the two protected networks.
2. To verify tunnel activation, go to *VPN* > *Monitor* > *IPsec Monitor*.

Monitoring and troubleshooting

This section provides some general maintenance and monitoring procedures for VPNs.

The following topics are included in this section:

Monitoring VPN connections

You can use the monitor to view activity on IPsec VPN tunnels and to 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 go to *VPN* > *Monitor* > *IPsec Monitor*.

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 go to *VPN* > *Monitor* > *IPsec Monitor*.

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 Endpoint 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 security 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.

Testing VPN connections

A VPN connection has multiple stages that can be confirmed to ensure the connection is working properly. It is easiest to see if the final stage is successful first since if it is successful the other stages will be working properly. Otherwise, you will need to work back through the stages to see where the problem is located.

When a VPN connection is properly established, traffic will flow from one end to the other as if both ends were physically in the same place. If you can determine the connection is working properly then any problems are likely problems with your applications.

If the connection is not working properly, you can move on to "Troubleshooting VPN connections" on page 226 to determine the exact problem.

LAN interface connection

To confirm whether a VPN connection over LAN interfaces has been configured correctly, issue a ping or traceroute command on the network behind the FortiGate unit to test the connection to a computer on the remote network. If the connection is properly configured, a VPN tunnel will be established automatically when the first data packet destined for the remote network is intercepted by the FortiGate unit.

If the ping or traceroute fail, it indicates a connection problem between the two ends of the tunnel. This may or may not indicate problems with the VPN tunnel. You can confirm this by going to *VPN* > *Monitor* > *IPsec Monitor* where you will be able to see your connection. A green arrow means the tunnel is up and currently processing traffic. A red arrow means the tunnel is not processing traffic, and this VPN connection has a problem.

If the connection has problems, see "Troubleshooting VPN connections" on page 226.

Dialup connection

A dialup VPN connection has additional steps. 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.

If the ping or traceroute fail, it indicates a connection problem between the two ends of the tunnel. This may or may not indicate problems with the VPN tunnel, or dialup client. As with the LAN connection, confirm the VPN tunnel is established by checking *VPN* > *Monitor* > *IPsec Monitor*.

Troubleshooting VPN connections

If you have determined that your VPN connection is not working properly through "Testing VPN connections" on page 225, the next step is to verify that you have a phase2 connection.

If traffic is not passing through the FortiGate unit as you expect, ensure the traffic does not contain IPcomp packets (IP protocol 108, RFC 3173). FortiGate units do not allow IPcomp packets, they compress packet payload, preventing it from being scanned.

Testing phase 1 and 2 connections is a bit more difficult than testing the working VPN. This is because they require diagnose CLI commands. These commands are typically used by Fortinet customer support to discover more information about your FortiGate unit and its current configuration.

Before you start troubleshooting you need to:

- configure FortiGate units on both ends for interface VPN
- record the information in your VPN phase 1 and phase 2 configurations - for our example here the remote IP address is 10.11.101.10 and the names of the phases are Phase1 and Phase2
- install a telnet or SSH client such as putty that allows logging of output
- ensure that the admin interface supports your chosen connection protocol so you can connect to your FortiGate unit admin interface.
- For this example, default values were used unless stated otherwise.

To get diagnose information for the VPN connection - CLI

1. Log into the CLI as admin with the output being logged to a file.
2. Stop any diagnose debug sessions that are currently running with the CLI command
   ```
   diagnose debug disable
   ```
3. Clear any existing log-filters by running
   ```
   diagnose vpn ike log-filter clear
   ```
4. Set the log-filter to the IP address of the remote computer (10.11.101.10). This filters out all VPN connections except ones to the IP address we are concerned with. The command is
   ```
   diagnose vpn ike log-filter dst-addr4 10.11.101.10.
   ```
5. Set up the commands to output the VPN handshaking. The commands are:
   ```
   diagnose debug app ike 255
   diagnose debug enable
   ```

6. Have the remote FortiGate initiate the VPN connection in the web-based manager by going to *VPN* > *Monitor* and selecting *Bring up*.

   This makes the remote FortiGate the initiator and the local FortiGate becomes the responder. Establishing the connection in this manner means the local FortiGate will have its configuration information as well as the information the remote computer sends. Having both sets of information locally makes it easier to troubleshoot your VPN connection.
7. Watch the screen for output, and after roughly 15 seconds enter the following CLI command to stop the output.

   ```
   diagnose debug disable
   ```
8. If needed, save the log file of this output to a file on your local computer. Saving the output to a file can make it easier to search for a particular phrase, and is useful for comparisons.

To troubleshoot a phase1 VPN connection

Using the output from "To get diagnose information for the VPN connection - CLI" on page 226, search for the word `proposal` in the output. It may occur once indicating a successful connection, or it will occur two or more times for an unsuccessful connection — there will be one proposal listed for each end of the tunnel and each possible combination in their settings. For example if 10.11.101.10 selected both DH Group 1 and 5, that would be at least 2 proposals set.

A successful negotiation proposal will look similar to

```
IPsec SA connect 26 10.12.101.10->10.11.101.10:500
config found
created connection: 0x2f55860 26 10.12.101.10->10.11.101.10:500
IPsec SA connect 26 10.12.101.10->10.11.101.10:500 negotiating
no suitable ISAKMP SA, queuing quick-mode request and initiating
     ISAKMP SA negotiation
initiator: main mode is sending 1st message...
cookie 3db6afe559e3df0f/0000000000000000
out [encyrption]
sent IKE msg (ident-i1send): 10.12.101.10:500->10.11.101.10:500,
     len=264, id=3db6afe559e3df0f/0000000000000000
diaike 0: comes 10.12.101.1:500->10.11.101.1:500,ifindex=26....
```

Note the phrase "`initiator: main mode is sending 1st message...`" which shows you the handshake between the ends of the tunnel is in progress. Initiator shows the remote unit is sending the first message.

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 Settings*.
2. Verify that the *VPN activity event* option is selected.
3. Select *Apply*.

To view event logs

1. Go to *Log & Report* > *Event Log* > *VPN*.
2. Select the *Log location*.

VPN troubleshooting tips

More in-depth VPN troubleshooting can be found in the *Troubleshooting guide*.

The VPN proposal is not connecting

One side may attempt to initiate the VPN tunnel unsuccessful. There are a number of potential reasons for this problem.

Attempting hardware offloading beyond SHA1

If you are trying to off-load VPN processing to a network processing unit (NPU), remember that only SHA1 authentication is supported. For high levels of authentication such as SHA256, SHA384, and SHA512 hardware offloading is not an option — all VPN processing must be done in software.

Check Phase 1 proposal settings

Ensure that both sides have at least one Phase 1 proposal in common. Otherwise they will not connect. If there are many proposals in the list, this will slow down the negotiating of Phase 1. If its too slow, the connection may timeout before completing. If this happens, try removing some of the unused proposals.

NPU offloading is supported when the local gateway is a loopback interface.

Check your routing

If routing is not properly configured with an entry for the remote end of the VPN tunnel, traffic will not flow properly. You may need static routes on both ends of the tunnel. If routing is the problem, the proposal will likely setup properly but no traffic will flow.

Try enabling XAuth

If one end of an attempted VPN tunnel is using XAuth and the other end is not, the connection attempt will fail. The log messages for the attempted connection will not mention XAuth is the reason, but when connections are failing it is a good idea to ensure both ends have the same XAuth settings. If you do not know the other end's settings enable or disable XAuth on your end to see if that is the problem.

General 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 225.
2. Traceroute the remote network or client. If DNS is working, you can use domain names. Otherwise use IP addresses.
3. Check the routing behind the dialup client. Routing problems may be affecting DHCP. If this appears to be the case, configure a DHCP relay service to enable DHCP requests to be relayed to a DHCP server on or behind the FortiGate server.

4. 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.
5. To correct the problem, see the following table.

Table 5: 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 37.
Peer ID or certificate name of the remote peer or dialup client is not recognized by FortiGate VPN server.	Check Phase 1 configuration. 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 41). 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 41.
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 45 and “Configure the phase 2 parameters” on page 55.
NAT traversal settings are mismatched.	Select or clear both options as required. See “NAT traversal” on page 48 and “NAT keepalive frequency” on page 49.
SPI settings for manual key tunnels are mismatched.	Enter complementary SPI settings. See “Manual-key configurations” on page 171.

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, that device must be NAT traversal (NAT-T) compatible for encrypted traffic to pass through the NAT device. For more information, see “NAT traversal” on page 48.

Index

E

F

G

H

I

K

L

M

N

S

T

V

W

X

Z