

The Fortinet logo is displayed in white, uppercase letters. The letter 'O' is replaced by a red square containing a white grid pattern. A small 'TM' trademark symbol is located at the end of the word.

FORTINETTM

FortiGate VPN Guide

FortiGate VPN Guide

Version 2.80 MR11

4 October 2005

01-28011-0065-20051004

© Copyright 2005 Fortinet Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

FortiGate VPN Guide
Version 2.80 MR11
4 October 2005
01-28011-0065-20051004

Trademarks

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

Regulatory Compliance

FCC Class A Part 15 CSA/CUS

For technical support, please visit <http://www.fortinet.com>.

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

Version	Date	Description of changes
MR8	Jan. 28, 2005	Extensively rewritten and reissued.
MR10 v1	Jun. 30, 2005	Added documentation to differentiate FortiGate dialup-client configurations from FortiClient dialup-client configurations. Added information about how to avoid ambiguous routing. Added information about how to apply the FortiGate DHCP relay feature. Additional minor changes and corrections.
MR10 v2	Jul. 20, 2005	Added steps for enabling internet browsing in a FortiGate dialup-client configuration to "Internet-browsing configurations" section. Corrected descriptions of phase 1 Local ID, Dynamic DNS, and Accept this peer ID fields in "Dynamic DNS configuration steps" section. Added descriptions of two new technical notes to "Related technical notes" section. Added hyperlink to information about how to disable Microsoft L2TP with IPsec to "Overview" section of "Configuring L2TP VPNs" chapter.
MR10 v3	Aug. 30, 2005	Moved descriptions of outbound NAT option (IPsec encryption policy) to "Defining a firewall encryption policy" section. Refined descriptions of IPsec phase 1 Peer ID options and procedure for configuring phase 1 peer IDs. Added description of new technical note to "Related technical notes" section. Simplified Table 3, IPsec VPN trouble-shooting tips. Enabled hyperlinks to Fortinet Technical Documentation web site and Fortinet Knowledge Center throughout document.
MR11	Oct. 4, 2005	Refer to the <i>FortiGate Administration Guide Addendum</i> .

Table of Contents

Introduction	9
About FortiGate VPNs	9
Supported VPN protocols	9
Using the web-based manager and CLI to configure VPNs	10
About this document	10
Fortinet documentation	11
Fortinet Knowledge Center	12
Comments on Fortinet technical documentation	12
Customer service and technical support	12
Configuring IPSec VPNs	13
Overview	13
IPSec VPN configuration overview	14
How to use this guide to configure an IPSec VPN	14
Network topologies	15
Gateway-to-gateway configurations	15
Gateway-to-gateway infrastructure requirements	16
Gateway-to-gateway configuration steps	17
Hub-and-spoke configurations	18
Hub-and-spoke infrastructure requirements	18
Hub-and-spoke configuration steps	18
Configure the hub	19
To configure the VPN hub	19
To define the VPN concentrator	20
Configure the spokes	20
To configure a VPN spoke	20
Dynamic DNS configurations	22
Dynamic DNS infrastructure requirements	23
Dynamic DNS configuration steps	23
To configure a FortiGate unit that has a domain name	23
To configure the remote VPN peer	24
FortiClient dialup-client configurations	25
FortiClient dialup-client infrastructure requirements	28
FortiClient dialup-client configuration steps	28
Configuring the dialup server to accept FortiClient connections	29
Configuring the FortiClient Host Security application	30
To manually specify a VIP address for FortiClient	31
FortiGate dialup-client configurations	31
FortiGate dialup-client infrastructure requirements	34
FortiGate dialup-client configuration steps	34
Configuring the dialup server to accept FortiGate dialup client connections	35

Configuring a FortiGate dialup client	36
Internet-browsing configurations	37
Internet-browsing infrastructure requirements	38
Internet-browsing configuration steps	39
Enabling Internet browsing in a gateway-to-gateway configuration	39
To enable Internet browsing in a gateway-to-gateway configuration	39
Enabling Internet browsing in a FortiClient dialup-client configuration	40
To select the Internet-browsing interface on the FortiGate dialup server	40
To configure FortiClient to force all IP traffic through the VPN tunnel	40
Enabling Internet browsing in a FortiGate dialup-client configuration	41
To enable Internet browsing in a FortiGate dialup-client configuration	41
Redundant-tunnel configurations	41
Redundant-tunnel infrastructure requirements	42
Redundant-tunnel configuration steps	43
Transparent VPN configurations	44
Transparent VPN infrastructure requirements	47
Before you begin	48
Transparent VPN configuration steps	48
Manual-key configurations	49
To specify manual keys for creating a tunnel	50
Defining Phase 1 IKE and authentication parameters	51
Authenticating remote peers and clients	52
To authenticate a remote peer or dialup client using digital certificates	52
To authenticate a remote peer using a preshared key	53
Managing digital certificates.....	54
To generate a certificate request	55
To install a signed personal or site certificate	56
To install a CA root certificate	56
Peer and user authentication options	57
Enabling VPN access for specific certificate holders	57
To view server certificate information and obtain the local DN	58
To view CA root certificate information and obtain the CA certificate name	58
To enable access for a specific certificate holder or a group of certificate holders ...	58
Enabling VPN peer identification	59
To assign an identifier (local ID) to a FortiGate unit	61
To authenticate a FortiGate DDNS peer or dialup client(s) using one ID	62
To authenticate dialup clients that use unique identifiers and preshared keys	62
To authenticate dialup clients that use unique preshared keys	62
Enabling XAuth on the FortiGate unit	63
To authenticate a dialup user group using XAuth settings	63
To configure a FortiGate dialup client act as an XAuth client	64
Defining IKE negotiation parameters	64
Generating keys to authenticate an exchange	65
Defining the remaining phase 1 options.....	66

NAT traversal	66
NAT keepalive frequency	66
Dead peer detection	67
Configuring the phase 1 IKE exchange	67
To define IKE negotiation parameters.....	67
To define additional dead peer detection parameters	68
Command syntax pattern	68
Example.....	70
Defining Phase 2 tunnel creation parameters	71
Exchanging keys to implement security associations	71
Defining the remaining tunnel creation options.....	72
Replay detection	72
Perfect forward secrecy	72
DHCP-IPsec	72
Internet browsing	73
Quick mode identities	73
Configuring the phase 2 tunnel creation parameters	73
To specify phase 2 parameters for creating a tunnel	73
Using the ping generator to keep a tunnel open	75
To configure the ping generator.....	76
Defining IP source and destination addresses	76
To define an IP source address	77
To define an IP destination address.....	77
Defining a firewall encryption policy	78
Defining multiple encryption policies for the same tunnel	79
To define a firewall encryption policy	80
Related technical notes	81
Configuring PPTP VPNs.....	83
Overview	83
Network topology	85
PPTP infrastructure requirements	85
PPTP server configuration overview	85
PPTP pass through configuration overview	86
Authenticating PPTP clients	86
Enabling PPTP and specifying an address range	86
To enable PPTP and specify the PPTP address range	87
Configuring a FortiGate PPTP server	87
Defining firewall source and destination addresses	87
To define the firewall source address	87
To define the firewall destination address.....	88
Add the firewall policy	88
To define the traffic and services permitted inside the PPTP tunnel	88
Configuring PPTP pass through	88

To define a virtual port-forwarding address for PPTP pass through	89
To create a port-forwarding firewall policy for PPTP pass through	89
Configuring a Windows client	90
To set up an PPTP dialup connection on a Windows 2000 client.....	90
To set up a PPTP dialup connection on a Windows XP client.....	91
To connect to the FortiGate PPTP server.....	91
Configuring a Linux client	91
Configuring L2TP VPNs	93
Overview	93
Network topology	95
L2TP infrastructure requirements	95
L2TP configuration overview	96
Authenticating L2TP clients	96
Enabling L2TP and specifying an address range	96
To enable L2TP and specify the L2TP address range.....	97
Defining firewall source and destination addresses	97
To define the firewall source address	97
To define the firewall destination address.....	97
Adding the firewall policy	98
To define the traffic and services permitted inside the L2TP tunnel	98
Configuring a Linux client	98
Monitoring and Testing VPN Tunnels	101
Viewing IPsec VPN tunnel status	101
Monitoring VPN connections.....	102
Monitoring connections to remote peers.....	102
To establish or take down a VPN tunnel.....	102
Monitoring dialup IPsec connections.....	102
Monitoring IKE, PPTP, and L2TP sessions	104
Testing VPN connections.....	104
Logging VPN events	104
To log VPN events	105
To filter VPN events	105
To view event logs	105
IPsec VPN troubleshooting tips.....	106
A word about NAT devices	107
Glossary	109
Index	113

Introduction

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

- [About FortiGate VPNs](#)
- [About this document](#)
- [Fortinet documentation](#)
- [Customer service and technical support](#)

About FortiGate VPNs

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

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

Supported VPN protocols

FortiGate units support the following protocols to authenticate and encrypt traffic:

- Internet Protocol Security (IPSec), a framework for the secure exchange of packets at the IP layer. FortiGate units implement the Encapsulated Security Payload (ESP) protocol in tunnel mode. The encrypted packets look like ordinary packets that can be routed through any IP network. Internet Key Exchange (IKE) is performed automatically based on preshared keys or X.509 digital certificates. As an option, you can specify manual keys.
- Point-to-Point Tunneling Protocol (PPTP), which enables interoperability between FortiGate units and Windows or Linux PPTP clients. PPTP uses PPP authentication protocols so that standard PPP software can operate on tunneled PPP links.
- Layer Two Tunneling Protocol (L2TP), which combines the features of PPTP and Layer 2 Forwarding (L2F). The FortiGate implementation of L2TP enables a remote dialup client to establish an L2TP tunnel with the FortiGate unit directly.

Because FortiGate units support industry standard VPN technologies, you can configure a VPN between a FortiGate unit and most third-party VPN peers. For more information about FortiGate VPN interoperability, contact Fortinet Technical Support.

Using the web-based manager and CLI to configure VPNs

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

In the web-based manager:

- IPsec VPN operating parameters are located on the following tabs:
 - **VPN > IPSEC > Phase 1**
 - **VPN > IPSEC > Phase 2**
 - **VPN > IPSEC > Manual Key**
 - **VPN > IPSEC > Concentrator**
 - **VPN > IPSEC > Ping Generator**
 - **VPN > Certificates**
- PPTP settings are located on the **VPN > PPTP** tab.
- L2TP settings are located on the **VPN > L2TP** tab.

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

- `config vpn ipsec phase1`
- `config vpn ipsec phase2`
- `config vpn ipsec manualkey`
- `config vpn ipsec concentrator`
- `config vpn pinggen`
- `execute vpn certificate`
- `config vpn pptp`
- `config vpn l2tp`

For detailed information about these CLI commands, refer to the “config vpn” and “execute vpn” chapters of the [FortiGate CLI Reference Guide](#).

About this document

This document explains how to configure VPNs using the web-based manager. To define comparable parameters through the CLI, see the [FortiGate CLI Reference Guide](#).

This document contains the following chapters:

- [Configuring IPsec VPNs](#) describes how to set up various IPsec VPN configurations.
- [Configuring PPTP VPNs](#) describes how to configure a PPTP tunnel between a FortiGate unit and a PPTP client.

- [Configuring L2TP VPNs](#) describes how to configure the FortiGate unit to operate as an L2TP network server.
- [Monitoring and Testing VPN Tunnels](#) outlines some general monitoring and testing procedures for VPNs.

Fortinet documentation

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

The following [FortiGate product documentation](#) is available:

- *FortiGate QuickStart Guide*
Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Installation Guide*
Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*
Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*
Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference Guide*
Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference Guide*
Describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability Guide*
Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS Guide*
Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate VPN Guide*
Explains how to configure VPNs using the web-based manager.
- *FortiGate VLANs and VDOMs Guide*
Describes how to configure VLANs and VDOMs in both NAT/Route and Transparent mode. Includes detailed examples.

Fortinet Knowledge Center

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

Comments on Fortinet technical documentation

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

Customer service and technical support

For antivirus and attack definition updates, firmware updates, updated product documentation, technical support information, and other resources, please visit the Fortinet Technical Support web site at <http://support.fortinet.com>.

You can also register Fortinet products and service contracts from <http://support.fortinet.com> and change your registration information at any time.

Technical support is available through email from any of the following addresses. Choose the email address for your region:

amer_support@fortinet.com	For customers in the United States, Canada, Mexico, Latin America and South America.
apac_support@fortinet.com	For customers in Japan, Korea, China, Hong Kong, Singapore, Malaysia, all other Asian countries, and Australia.
eu_support@fortinet.com	For customers in the United Kingdom, Scandinavia, Mainland Europe, Africa, and the Middle East.

For information about our priority support hotline (live support), see <http://support.fortinet.com>.

When requesting technical support, please provide the following information:

- your name
- your company's name and location
- your email address
- your telephone number
- your support contract number (if applicable)
- the product name and model number
- the product serial number (if applicable)
- the software or firmware version number
- a detailed description of the problem

Configuring IPsec VPNs

This chapter provides step-by-step instructions for configuring IPsec VPNs and includes the following topics:

- [Overview](#)
- [IPsec VPN configuration overview](#)
- [Network topologies](#)
- [Defining Phase 1 IKE and authentication parameters](#)
- [Defining Phase 2 tunnel creation parameters](#)
- [Defining IP source and destination addresses](#)
- [Defining a firewall encryption policy](#)
- [Related technical notes](#)

Overview

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

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

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

When a FortiGate unit receives a connection request from a remote peer, it uses phase 1 parameters to establish a secure connection and authenticate the VPN peer. Then, if the firewall policy permits the connection, the FortiGate unit establishes the VPN tunnel using phase 2 parameters and applies the firewall encryption policy. Key management, authentication, and security services are negotiated dynamically through the IKE protocol.

IPSec VPN configuration overview

This guide uses a task-based approach to provide all of the procedures needed to create different types of VPN configurations. In this chapter, you can read about various network topologies and find the procedures needed to configure IPSec VPNs. The [“Network topologies”](#) section explains what you have to do based on the network topology that you choose.

How to use this guide to configure an IPSec VPN

First, identify the network topology that you want to configure (see [“Network topologies” on page 15](#)). Afterward, follow the step-by-step configuration procedures to set up the VPN.

The highest-level procedures are presented in the [“Network topologies”](#) section. 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 in the [“Network topologies”](#) section to complete the procedure.

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 and establish a secure a connection. See [“Authenticating remote peers and clients” on page 52](#).
- 2 Define the phase 2 parameters that the FortiGate unit needs to create a VPN tunnel with a remote peer or dialup client. See [“Defining Phase 2 tunnel creation parameters” on page 71](#).
- 3 Define source and destination addresses for the IP packets that are to be transported through the VPN tunnel. See [“Defining IP source and destination addresses” on page 76](#).
- 4 Create the firewall encryption policy and define the scope of permitted services between the IP source and destination addresses. See [“Defining a firewall encryption policy” on page 78](#).



Note: The procedures throughout this chapter assume that you will perform Steps 1 and 2 to have the FortiGate unit generate unique IPSec encryption and authentication keys automatically. In situations where a remote VPN peer requires a specific IPSec encryption and/or authentication key, you must configure the FortiGate unit to use manual keys instead of performing Steps 1 and 2. For more information, see [“Manual-key configurations” on page 49](#).

Network topologies

The topology of your network will determine how remote peers and clients connect to the VPN and how VPN traffic is routed. The configurations listed below are discussed in this section:

- [Gateway-to-gateway configurations](#)
- [Hub-and-spoke configurations](#)
- [Dynamic DNS configurations](#)
- [FortiClient dialup-client configurations](#)
- [FortiGate dialup-client configurations](#)
- [Internet-browsing configurations](#)
- [Redundant-tunnel configurations](#)
- [Transparent VPN configurations](#)
- [Manual-key configurations](#)

These sections contain high-level configuration guidelines with cross-references to detailed configuration procedures.

Gateway-to-gateway configurations

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

Figure 1: Example gateway-to-gateway configuration

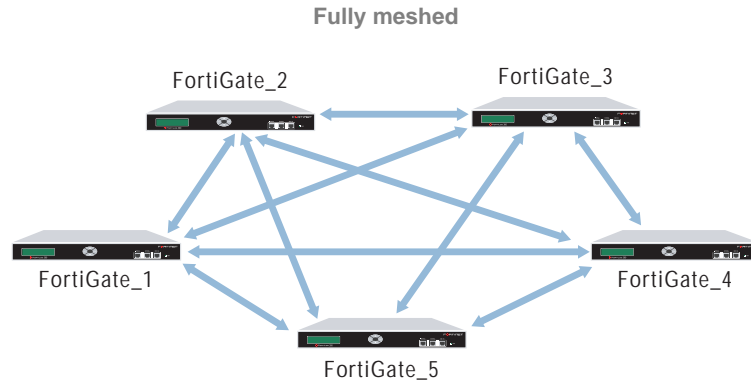


Note: In some cases, computers on the private network behind one VPN peer may (by coincidence) have IP addresses that are already used by computers on the network behind the other VPN peer. In this type of situation (ambiguous routing), conflicts may occur in one or both of the FortiGate routing tables and traffic destined for the remote network through the tunnel may not be sent. To resolve issues related to ambiguous routing, refer to the [Outbound NAT for IPSec VIP Technical Note](#).

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 31](#).

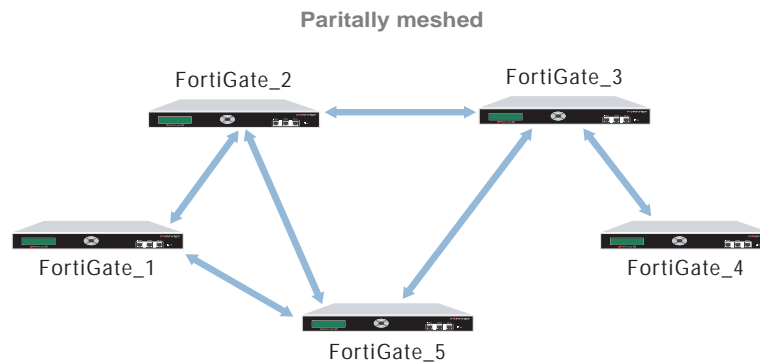
You can set up a fully meshed configuration or partially meshed configuration (see [Figure 2](#) and [Figure 3](#)).

Figure 2: Fully meshed configuration



In a fully meshed network, all VPN peers are connected to each other, with one hop between peers. This topology is the most fault-tolerant: if one peer goes down, the rest of the network is not affected. This topology is difficult to scale because it requires connections between all peers. In addition, unnecessary communication can occur between peers. We recommend a hub-and-spoke configuration instead (see [“Hub-and-spoke configurations”](#) on page 18).

Figure 3: Partially meshed configuration



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

Gateway-to-gateway infrastructure requirements

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

Gateway-to-gateway configuration steps

- 1 At the local FortiGate unit, define the phase 1 parameters needed to establish a secure connection with the remote peer. See [“Defining Phase 1 IKE and authentication parameters” on page 51](#). 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.

- 2 Define the phase 2 parameters needed to create a VPN tunnel with the remote peer. See [“Defining Phase 2 tunnel creation parameters” on page 71](#). Enter these settings in particular:

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

- 3 Define the source and destination addresses of the IP packets that are to be transported through the VPN tunnel. See [“Defining IP source and destination addresses” on page 76](#). Enter these settings in particular:

- For the originating address (source address), enter the IP address and netmask of the private network behind the local FortiGate unit.
- For the remote address (destination address), enter the IP address and netmask of the private network behind the remote peer.

- 4 Define a firewall encryption policy to permit communications between the source and destination addresses. See [“Defining a firewall encryption policy” on page 78](#). Enter these settings in particular:

Source Interface/Zone
 Select the local interface to the internal (private) network.
Address Name
 Select the source address that you defined in Step 3.

Destination Interface/Zone
 Select the local interface to the external (public) network.
Address Name
 Select the destination address that you defined in Step 3.

Action Select ENCRYPT.

VPN Tunnel Select the name of the phase 2 tunnel configuration that you created in Step 2.
 Select Allow inbound to enable traffic from the remote network to initiate the tunnel.
 Select Allow outbound to enable traffic from the local network to initiate the tunnel.

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

Hub-and-spoke configurations

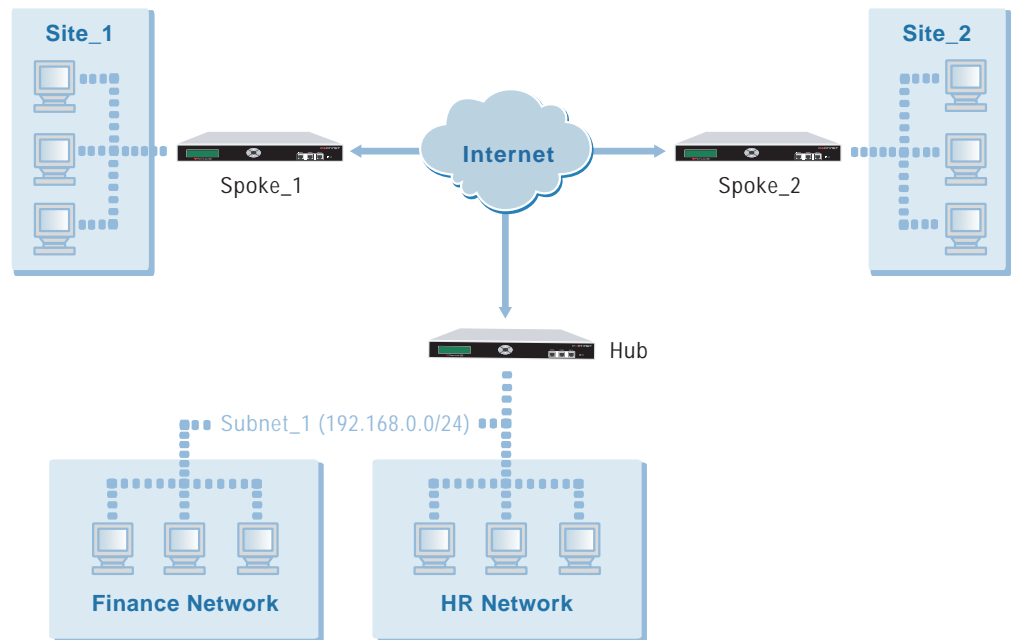
In a hub-and-spoke configuration, connections to a number of remote peers radiate from a single, central FortiGate unit. Site-to-site connections between the remote peers do not exist; however, VPN tunnels between any two of the remote peers can be established through the FortiGate unit “hub”.

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.



Note: The hub does not log information related to VPN sessions between two spokes.

Figure 4: Example hub-and-spoke configuration



Hub-and-spoke infrastructure requirements

- All FortiGate units must be operating in NAT/Route mode and have static public IP addresses.



Note: Many hub-and-spoke configurations require static IP addresses. However, a spoke may have a dynamic IP address (see “[FortiClient dialup-client configurations](#)” on page 25) or a static domain name and dynamic IP address (see “[Dynamic DNS configurations](#)” on page 22). For more information, contact Fortinet Technical Support.

Hub-and-spoke configuration steps

- 1 Configure the hub. See “[Configure the hub](#)” below.
- 2 Configure each spoke. See “[Configure the spokes](#)” on page 20.

Configure the hub

Perform these steps at the FortiGate unit that will act as the hub.

To configure the VPN hub

- 1 At the hub, define a set of phase 1 parameters for each spoke. See [“Defining Phase 1 IKE and authentication parameters” on page 51](#). Enter these settings in particular:

Remote Gateway Select Static IP Address.
IP Address Type the IP address of the public interface to the spoke.

- 2 Create a source address for the hub. See [“Defining IP source and destination addresses” on page 76](#). Enter the IP address and netmask of the private network behind the hub.

- 3 Create a phase 2 tunnel definition for each spoke. See [“Defining Phase 2 tunnel creation parameters” on page 71](#). Enter these settings in particular:

Remote Gateway Select the set of phase 1 parameters that you defined for the spoke.
 The name of the spoke can be selected from the Static IP Address list.

- 4 Create a destination address for each spoke. See [“Defining IP source and destination addresses” on page 76](#). Enter the IP address and netmask of the private network behind each spoke.
- 5 Define the VPN concentrator. See [“To define the VPN concentrator” on page 20](#).
- 6 Create a firewall encryption policy for each spoke. See [“Defining a firewall encryption policy” on page 78](#). Enter these settings in particular:

Source Interface/Zone
 Select the hub's interface to the internal (private) network.
 Address Name
 Select the source address that you defined in Step 2.

Destination Interface/Zone
 Select the hub's interface to the external (public) network.
 Address Name
 Select the destination address that you defined for the spoke in Step 4.

Action Select ENCRYPT.

VPN Tunnel Select the name of the phase 2 tunnel configuration that you created for the spoke.
 Select Allow inbound to enable traffic from the remote network to initiate the tunnel.
 Select Allow outbound to enable traffic from the local network to initiate the tunnel.

- 7 In the policy list, arrange the policies in the following order:
 - encryption policies that control traffic between the hub and the spokes first
 - the default firewall policy last

To define the VPN concentrator

You define a concentrator to include spokes in the hub-and-spoke configuration.

- 1 At the hub, go to **VPN > IPSEC > Concentrator** and select **Create New**.
- 2 In the **Concentrator Name** field, type a name to identify the concentrator.
- 3 From the **Available Tunnels** list, select a VPN tunnel and then select the right-pointing arrow.



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

- 4 Repeat Step 3 until all of the tunnels associated with the spokes are included in the concentrator.
- 5 Select **OK**.

Configure the spokes

You must configure each remote peer that will function as a spoke. Each spoke requires:

- 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
- a destination address that represents the network behind the hub
- several destination addresses to represent the networks behind each of the other spokes
- a firewall encryption policy to enable communications between the spoke and the hub
- several firewall encryption policies, to enable communications between the spoke and each of the other spokes



Note: To avoid creating a large number of destination addresses and firewall encryption policies at each spoke, you may define a destination address group at each spoke to represent the networks behind the other spokes. You could then define a single firewall encryption policy to enable communications between the spoke and the group of addresses associated with the other spokes. For information about how to create an address group, see the “Firewall” chapter of the [FortiGate Administration Guide](#).

To configure a VPN spoke

- 1 At the spoke, define the phase 1 parameters that the spoke will use to establish a secure connection with the hub. See [“Defining Phase 1 IKE and authentication parameters” on page 51](#). Enter these settings in particular:

Remote Gateway	Select Static IP Address.
IP Address	Type the IP address of the public interface to the hub.

- 2 Create the phase 2 tunnel definition. See [“Defining Phase 2 tunnel creation parameters” on page 71](#). Enter these settings in particular:

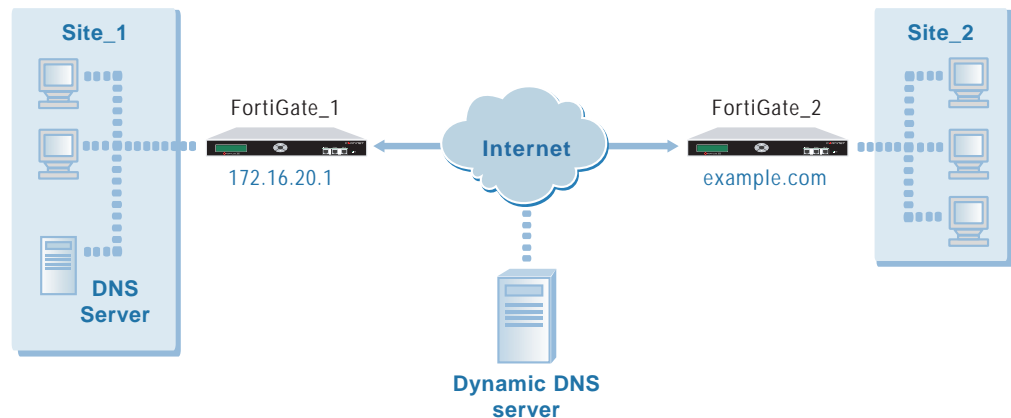
Remote Gateway	Select the set of phase 1 parameters that you defined for the hub. The name of the hub can be selected from the Static IP Address list.
-----------------------	---
- 3 Create a source address for the spoke. See [“Defining IP source and destination addresses” on page 76](#). Enter the IP address and netmask of the private network behind the spoke.
- 4 Create a destination address to represent the hub. See [“Defining IP source and destination addresses” on page 76](#). Enter the IP address and netmask of the private network behind the hub.
- 5 Define a firewall encryption policy to permit communications with the hub. See [“Defining a firewall encryption policy” on page 78](#). Enter these settings in particular:

Source	Interface/Zone Select the spoke's interface to the internal (private) network. Address Name Select the source address that you defined for the spoke in Step 3.
Destination	Interface/Zone Select the spoke's interface to the external (public) network. Address Name Select the destination addresses that you defined for the hub in Step 4.
Action	Select ENCRYPT.
VPN Tunnel	Select the name of the phase 2 tunnel configuration that you created in Step 2. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow outbound to enable traffic from the local network to initiate the tunnel.
- 6 Define several destination addresses to represent the networks behind each of the other spokes.
- 7 Define one firewall encryption policy for each of the destination addresses that you defined in Step 6.
- 8 Place the encryption policies in the policy list above any other policies having similar source and destination addresses.
- 9 Repeat this procedure at each of the remaining spokes.

Dynamic DNS configurations

In this type of scenario, one of the FortiGate units in a gateway-to-gateway configuration has a static domain name (for example, example.com) and a dynamic IP address. See FortiGate_2 in Figure 5. Whenever that FortiGate unit connects to the Internet (and possibly also at predefined intervals of time set by the ISP), the ISP may assign a different IP address to the FortiGate unit. Therefore, remote peers have to locate the FortiGate unit through DNS lookup.

Figure 5: Example dynamic DNS configuration



In Figure 5, FortiGate_1 requests a DNS lookup before initiating a connection to FortiGate_2. FortiGate_2 pushes its dynamic IP address to a dynamic DNS server whenever its address changes to ensure that all DNS servers are updated.

When a remote peer (such as FortiGate_1 in Figure 5) initiates a connection to the domain name, a DNS server looks up and returns the IP address that matches the domain name. The remote peer uses the retrieved IP address to establish a connection with the FortiGate unit.

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

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

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

Dynamic DNS infrastructure requirements

- A basic gateway-to-gateway configuration must be in place (see [“Gateway-to-gateway configurations” on page 15](#)) except one of the FortiGate units has a static domain name and a dynamic IP address instead of a static IP address.
- A DNS server must be available to VPN peers that initiate connections to the domain name. For instructions about how to configure FortiGate units to look up the IP address of a domain name, see the “System Network DNS” section of the [FortiGate Administration Guide](#).
- The FortiGate unit with the domain name must subscribe to one of the supported dynamic DNS services. Contact one of the services to set up an account. For more information and instructions about how to configure the FortiGate unit to push its dynamic IP address to a dynamic DNS server, see the “System Network Interface” section of the [FortiGate Administration Guide](#).

Dynamic DNS configuration steps

- 1 Configure the FortiGate unit that has a static domain name and a dynamic IP address. See [“To configure a FortiGate unit that has a domain name” on page 23](#).
- 2 Configure the remote VPN peer. See [“To configure the remote VPN peer” on page 24](#).

To configure a FortiGate unit that has a domain name

- 1 At the FortiGate unit that has a domain name, define the phase 1 parameters needed to establish a secure connection with the remote peer. See [“Defining Phase 1 IKE and authentication parameters” on page 51](#). 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.
Mode	Select Aggressive.
Local ID	Type a character string that the local FortiGate unit can use to identify itself to the remote peer (for example, you could type the fully qualified domain name of the FortiGate unit, <code>example.com</code>). This value must be identical to the value in the Accept this peer ID field of the phase 1 remote gateway configuration on the remote peer.

- 2 Define the phase 2 parameters needed to create a VPN tunnel with the remote peer. See [“Defining Phase 2 tunnel creation parameters” on page 71](#). Enter these settings in particular:

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

- 3 Define the source and destination addresses of the IP packets that are to be transported through the VPN tunnel. See [“Defining IP source and destination addresses” on page 76](#). Enter these settings in particular:
 - For the originating address (source address), enter the IP address and netmask of the private network behind the local FortiGate unit.
 - For the remote address (destination address), enter the IP address and netmask of the private network behind the remote peer.

- 4 Define a firewall encryption policy to permit communications between the source and destination addresses. See [“Defining a firewall encryption policy” on page 78](#). Enter these settings in particular:

Source	Interface/Zone Select the local interface to the internal (private) network. Address Name Select the source address that you defined in Step 3.
Destination	Interface/Zone Select the local interface to the external (public) network. Address Name Select the destination address that you defined in Step 3.
Action	Select ENCRYPT.
VPN Tunnel	Select the name of the phase 2 tunnel configuration that you created in Step 2. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow outbound to enable traffic from the local network to initiate the tunnel.

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

To configure the remote VPN peer

- 1 At the VPN peer that has a static IP address, define the phase 1 parameters needed to establish a secure connection with the remote peer. See [“Defining Phase 1 IKE and authentication parameters” on page 51](#). Enter these settings in particular:

Remote Gateway	Select Dynamic DNS.
Dynamic DNS	Type the fully qualified domain name of the remote peer (for example, <code>example.net</code>).
Mode	Select Aggressive.
Peer Options	Select Accept this peer ID, and type the identifier of the FortiGate unit that has a dynamic IP address (for example, <code>example.com</code>). This value must be identical to the value in the Local ID field of the phase 1 remote gateway configuration on the remote peer.

- 2 Define the phase 2 parameters needed to create a VPN tunnel with the remote peer. See [“Defining Phase 2 tunnel creation parameters” on page 71](#). Enter these settings in particular:

Remote Gateway	Select the set of phase 1 parameters that you defined for the remote peer. The name of the remote gateway can be selected from the Dynamic DNS list.
-----------------------	--

- 3 Define the source and destination addresses of the IP packets that are to be transported through the VPN. See [“Defining IP source and destination addresses” on page 76](#). Enter these settings in particular:

- For the originating address (source address), enter the IP address and netmask of the private network behind the local FortiGate unit.
- For the remote address (destination address), enter the IP address and netmask of the private network behind the remote peer.

- 4 Define a firewall encryption policy to permit communications between the source and destination addresses. See [“Defining a firewall encryption policy” on page 78](#). Enter these settings in particular:

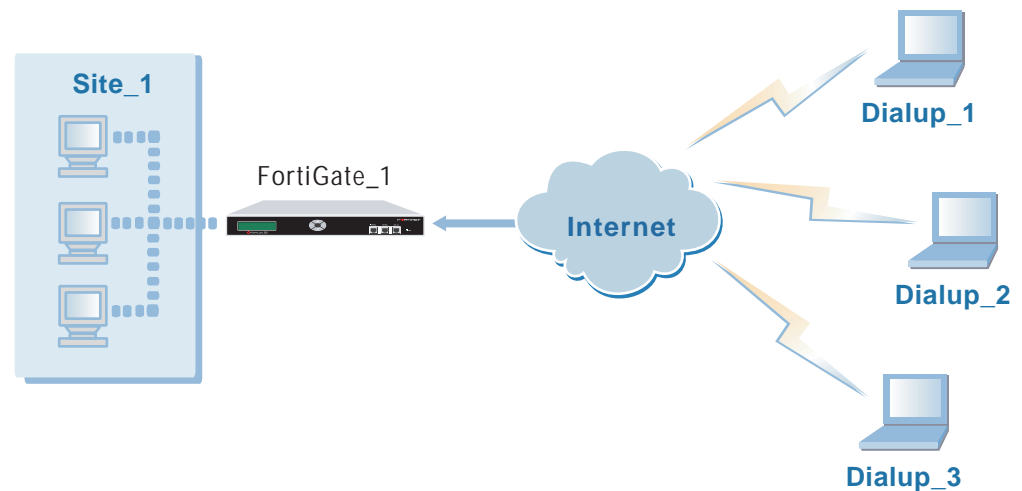
Source	Interface/Zone Select the local interface to the internal (private) network. Address Name Select the source address that you defined in Step 3.
Destination	Interface/Zone Select the local interface to the external (public) network. Address Name Select the destination address that you defined in Step 3.
Action	Select ENCRYPT.
VPN Tunnel	Select the name of the phase 2 tunnel configuration that you created in Step 2. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow outbound to enable traffic from the local network to initiate the tunnel.

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

FortiClient dialup-client configurations

In a FortiClient dialup-client configuration, remote hosts running VPN client software such as the FortiClient Host Security application are assigned dynamic IP addresses before the VPN client initiates a connection to a FortiGate dialup server. The remote hosts typically obtain dynamic IP addresses from an ISP through the Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol over Ethernet (PPPoE).

Figure 6: Example FortiClient dialup-client configuration



FortiClient dialup clients can establish an IPsec tunnel with a FortiGate unit that has been configured to act as a dialup server. When the FortiGate unit acts as a dialup server, it does not rely on a phase 1 remote gateway address to establish an IPsec VPN connection with the dialup client. As long as authentication is successful and the firewall encryption 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. For more information, see [“Peer and user authentication options” on page 57](#).

By default, the FortiClient Host Security application encrypts IP traffic and addresses the encrypted packets to the public interface of the FortiGate unit. Encrypted packets from the FortiGate unit may be addressed either to the public IP address of the remote host (if the remote host connects to the Internet directly), or if the host computer is behind a NAT device, encrypted packets from the FortiGate unit are addressed to the remote host’s IP address on the private network behind the NAT device.



Note: If a router with NAT capabilities is in front of the FortiClient host (for example, when the FortiClient host is located in a remote office or hotel LAN), the router must be NAT_T compatible (see [“NAT traversal” on page 66](#)) for encrypted packets to pass through the NAT device.

When the FortiGate unit decrypts a packet from the FortiClient 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 host device connects to the Internet directly, the source address will be the public IP address of the FortiClient host.
- If the host device is behind a NAT device, the source address will be the private IP address of the FortiClient host.

When the remote host is located behind a NAT device, unintended IP-address overlap issues may arise between the remote private network and the private network behind the FortiGate unit. For example, the remote host may receive a private IP address from a DHCP server on the remote network. If the private IP address assigned to the remote host is (by co-incidence) the same as a private IP address on the network behind the FortiGate unit, a conflict will occur in the host’s routing table and the FortiClient Host Security application will be unable to send traffic through the tunnel.

In situations where IP-address overlap is likely to occur, a Virtual IP (VIP) configuration is recommended. A VIP configuration enables you to assign uncommonly used IP addresses (for example, 10.254.254.0/24 or 192.168.254.0/24) to FortiClient dialup clients. When a VIP address is assigned, the FortiClient VPN client software and the FortiGate unit both use the VIP address as the IP address of the FortiClient dialup client for the duration of the connection. As a result, when the FortiGate unit decrypts a packet from a FortiClient dialup client that has a VIP address, the source address in the IP header will be the VIP address used by the FortiClient dialup client.



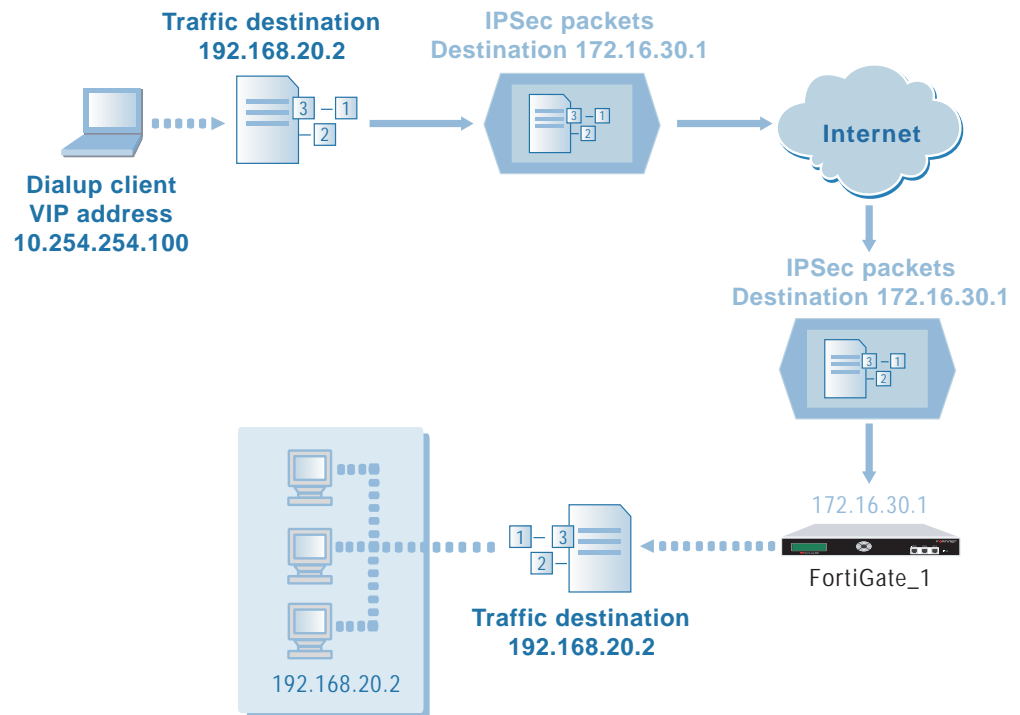
Note: To determine which VIP address the FortiClient Host Security application is using, type `ipconfig /all` at the Windows Command Prompt on the FortiClient host. The output will also show the IP address that has been assigned to the host Network Interface Card (NIC).

You can choose whether to assign a VIP address to the FortiClient Host Security application manually or through the FortiGate dialup server (via DHCP relay):

- To assign a VIP address to the FortiClient Host Security application manually, you must first start the application on the remote host. The settings can be enabled through the VPN tab. For more information, see [“Configuring the FortiClient Host Security application” on page 30](#).
- To assign a VIP address through FortiGate DHCP relay, you configure the FortiClient Host Security application to broadcast a DHCP request to the FortiGate unit (see the [FortiClient Dialup-client IPsec VPN Example Technical Note](#)). You must also configure the FortiGate unit to relay the DHCP request to a DHCP server behind the FortiGate unit (see [“Configuring the dialup server to accept FortiClient connections” on page 29](#)). The DHCP server will respond with a VIP address for the dialup client.

In both cases, the FortiClient dialup client uses the acquired VIP address as its source address for IP packets for the duration of the connection. IP packets from the FortiClient dialup client are addressed to a computer on the private network behind the FortiGate unit. IP packets from the network behind the FortiGate unit are addressed to the client VIP address. See [Figure 7](#).

Figure 7: IP address assignments in a FortiClient dialup-client configuration



In summary, if you do not assign VIP addresses to FortiClient dialup clients, the FortiGate unit must be configured to accept connections from any dialup VPN client. In this case, if the FortiClient host connects to the Internet directly, the source address of encrypted packets from the dialup client and the source address of decrypted IP packets will be the same (the public IP address of the FortiClient host). If the FortiClient host is behind a NAT device, the source address of encrypted packets will correspond to the public IP address of the NAT device, and the source IP address of traffic sent through the tunnel will correspond to the private IP address of the FortiClient host.

When you assign VIP addresses to FortiGate dialup clients manually, you can control which clients are allowed to connect to the FortiGate unit by creating a firewall encryption policy that allows connections from a specific VIP address or a subnet address comprising VIP addresses. However, take care to prevent overlapping IP addresses. As a precaution, consider using VIP addresses that are not commonly used.

FortiClient dialup-client infrastructure requirements

- The FortiGate dialup server may operate in NAT/Route mode or Transparent mode and has a static public IP address.
- 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 firewall encryption 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 dialup-client configuration steps

- 1 If you will be using VIP addresses to identify dialup clients, determine which VIP addresses to use. You can choose whether to assign VIP addresses manually or through FortiGate DHCP relay. As a precaution, consider using VIP addresses that are not commonly used.
- 2 If the dialup clients will be configured to obtain VIP addresses through DHCP relay, add the VIP addresses to the DHCP server behind the FortiGate dialup server. Refer to the software supplier's documentation to configure the DHCP server.
- 3 Configure the FortiGate unit to act as a dialup server. See [“Configuring the dialup server to accept FortiClient connections” on page 29](#).
- 4 Configure the dialup clients. See [“Configuring the FortiClient Host Security application” on page 30](#).

Configuring the dialup server to accept FortiClient connections

- 1 At the FortiGate dialup server, define the phase 1 parameters needed to authenticate dialup clients and establish a secure connection. See [“Defining Phase 1 IKE and authentication parameters” on page 51](#). Enter this setting in particular:

Remote Gateway Select Dialup User.

- 2 Define the phase 2 parameters needed to create a VPN tunnel with dialup clients. See [“Defining Phase 2 tunnel creation parameters” on page 71](#). Enter these settings in particular:

Remote Gateway Select the set of phase 1 parameters that you defined for dialup clients. The name of the gateway can be selected from the Dialup User list.

- 3 Enter the following CLI command to enable FortiClient dialup clients to connect using the same phase 2 tunnel definition:

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

For more information about CLI commands, see the [FortiGate CLI Reference Guide](#).

- 4 Define the source and destination addresses of the IP packets that are to be transported through the VPN tunnel. See [“Defining IP source and destination addresses” on page 76](#). Enter these settings in particular:
 - For the originating address (source address), enter the IP address of the server, host, or network that dialup clients need to access behind the FortiGate dialup server.
 - If you are not using VIP addresses (the FortiClient Acquire virtual IP address option is clear), you do not need to define a specific destination address. Instead, you will select the predefined destination address “all” in the firewall encryption policy to refer to dialup clients.
 - If VIP addresses are assigned through FortiGate DHCP relay (the FortiClient Acquire virtual IP address option is selected and the FortiClient Dynamic Host Configuration Protocol (DHCP) over IPsec option is selected), you do not need to define a specific destination address. Instead, you will select the predefined destination address “all” in the firewall encryption policy to refer to dialup clients.
 - If VIP addresses are configured manually (the FortiClient Acquire virtual IP address option is selected and the FortiClient Manually Set option is selected), create an IP destination address that references the exact VIP address or the subnet address comprising VIP addresses.

- 5 Define the firewall encryption policy to permit communications between the source and destination addresses. See [“Defining a firewall encryption policy” on page 78](#). Enter these settings in particular:

Source	Interface/Zone Select the local interface to the internal (private) network. Address Name Select the source address that you defined in Step 4.
Destination	Interface/Zone Select the local interface to the external (public) network. Address Name If you are not using VIP addresses, or if VIP addresses are assigned through FortiGate DHCP relay, keep the default setting (all). If VIP addresses are assigned manually, select the destination address that you defined in Step 4.
Action	Select ENCRYPT.
VPN Tunnel	Select the name of the phase 2 tunnel configuration that you created in Step 2. Select Allow inbound to enable dialup clients to initiate the tunnel. Clear Allow outbound to prevent traffic from the local network from initiating the tunnel after the tunnel has been established. If you want the FortiGate unit to perform inbound NAT on IP packets from dialup clients, select Inbound NAT.

- 6 Place the policy in the policy list above any other policies having similar source and destination addresses.
- 7 If the dialup clients are configured to obtain a VIP address through FortiGate DHCP relay, configure the FortiGate dialup server to relay DHCP requests as follows:
- Go to **VPN > IPSEC > Phase 2**.
 - Select the Edit icon in the row beside the existing phase 2 configuration.
 - Select Advanced, and then select DHCP-IPsec Enable.
 - Go to **System > DHCP > Service**.
 - In the list of interfaces, select the Edit button that corresponds to the interface to the Internet.
 - Select DHCP Relay Agent, and then select IPSEC.
 - In the DHCP Server IP field, type the IP address of the DHCP server that resides on the network behind the FortiGate dialup server.
 - Select OK.
 - If a router is installed between the FortiGate unit and the DHCP server, define a static route to the DHCP server. See the “Router” chapter of the [FortiGate Administration Guide](#).


Configuring the FortiClient Host Security application

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



Note: As an alternative, you can configure the FortiClient Host Security application to broadcast a DHCP request and obtain a VIP through FortiGate DHCP relay. For information about how to configure the FortiClient Host Security application to obtain a VIP address through DHCP relay, see the [FortiClient Dialup-client IPsec VPN Example Technical Note](#).

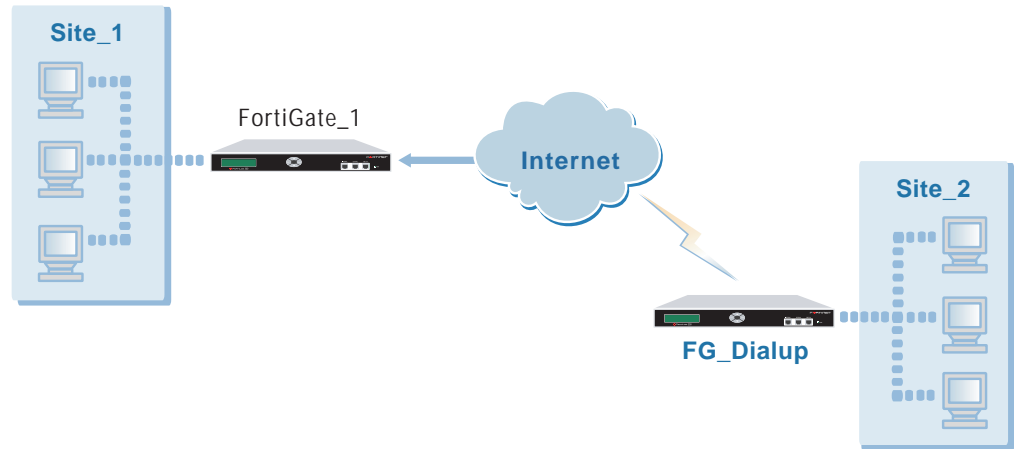
To manually specify a VIP address for FortiClient

- 1 At the remote host, start FortiClient.
 - 2 Go to **VPN > Connections** and select Add.
 - 3 In the Connection Name field, type a descriptive name for the connection.
 - 4 In the Remote Gateway field, type the public static IP address of the FortiGate unit.
 - 5 In the Remote Network fields, type the IP address and netmask of the server or host that FortiClient needs to access on the private network behind the FortiGate unit (for example, 192.168.12.1/255.255.255.255). If FortiClient needs to access a subnet behind the FortiGate unit, enter the subnet address (for example, 192.168.12.0/255.255.255.0).
 - 6 From the Authentication Method list, select an authentication method. The settings that you choose must correspond to the phase 1 authentication settings on the FortiGate unit.
 - 7 Select Advanced.
 - 8 In the Advanced Settings dialog box, select Acquire virtual IP address and then select Config.
 - 9 In the Virtual IP Acquisition dialog box, select Manually Set.
 - 10 In the IP and Subnet Mask fields, enter the VIP address and netmask that the dialup client will use as its source address for transmitting IP packets through the tunnel.
 - 11 Select OK.
 - 12 Retain the default advanced settings unless changes are needed to make the IKE and IPSec proposals match the phase 1 and 2 settings on the FortiGate unit.
-  **Note:** FortiClient settings determine which DNS server and Windows Internet Service (WINS) server the client can access after the tunnel has been established. For more information, see *FortiClient online Help*.
- 13 Select OK twice to close the dialog boxes.
 - 14 Exit FortiClient and repeat this procedure at all other remote hosts.

FortiGate dialup-client configurations

A dialup client may 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 8: 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 firewall encryption policy associated with the tunnel permits access, the tunnel is established.

Several different ways to authenticate dialup clients and restrict access to private networks based on client credentials are available. To authenticate FortiGate dialup clients and help to distinguish them from FortiClient dialup clients when multiple clients will be connecting to the VPN through the same tunnel, we recommend that you assign a unique identifier (local ID) to each FortiGate dialup client. For more information, see [“Peer and user authentication options” on page 57](#).



Note: Whenever you add a unique identifier (local ID) to a FortiGate dialup client for identification purposes, you must select Aggressive mode on the FortiGate dialup server and also specify the identifier as a peer ID on the FortiGate dialup server. For more information, see [“Enabling VPN peer identification” on page 59](#).

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 private IP address of the FortiGate dialup client.



Note: If a router with NAT capabilities is in front of the FortiGate dialup client, the router must be NAT_T compatible for encrypted traffic to pass through the NAT device. For more information, see [“NAT traversal” on page 66](#).

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:

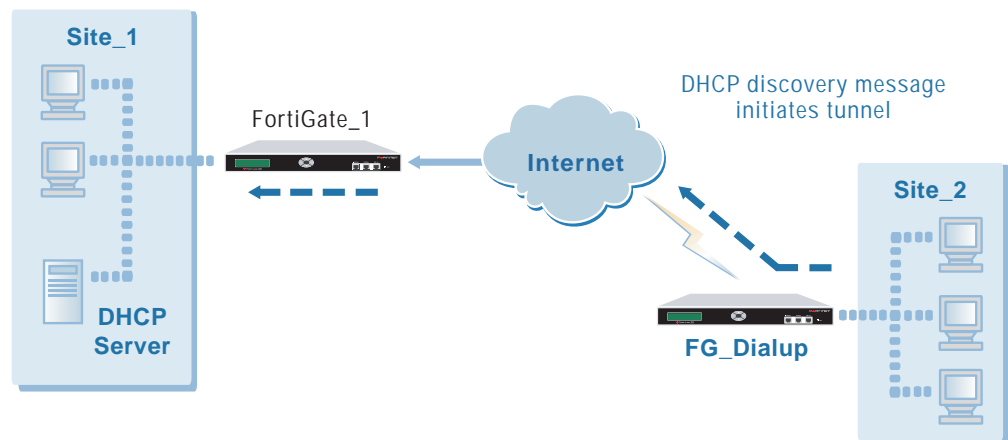
- If the FortiGate dialup client connects to the Internet directly, the source address will be the private IP address of a host or server on the network behind the FortiGate dialup client.
- If the FortiGate dialup client is behind a NAT device, the source address will be the private IP address of the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

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. To resolve issues related to ambiguous routing, refer to the [Outbound NAT for IPsec VIP Technical Note](#).

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

To avoid these issues, you can configure FortiGate DHCP relay on the dialup client instead of using a DHCP server on the network behind the dialup client. The FortiGate dialup client can be configured to relay DHCP requests from the local private network to a DHCP server that resides on the network behind the FortiGate dialup server (see [Figure 9 on page 33](#)). You configure the FortiGate dialup client to pass traffic from the local private network to the remote network by enabling FortiGate DHCP relay on the FortiGate dialup client interface that is connected to the local private network.

Figure 9: Preventing network overlap in a FortiGate dialup-client configuration



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

When the DHCP server resides on the private network behind the FortiGate dialup server as shown in [Figure 9](#), the IP destination address specified in the firewall encryption policy on the FortiGate dialup client must refer to that network.



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

FortiGate dialup-client infrastructure requirements

- The FortiGate dialup client and the FortiGate dialup server may operate in NAT/Route mode or Transparent mode.
- The FortiGate dialup server has a static public IP address.
- Computers on the private network behind the FortiGate dialup client may obtain IP addresses either from a local DHCP server behind the FortiGate dialup client, or a remote DHCP server behind the FortiGate dialup server:
 - If the DHCP server resides on the network behind the FortiGate dialup client, the DHCP server must be configured to assign IP addresses that do not match the private network behind the FortiGate dialup server.
 - If the DHCP server resides on the network behind the FortiGate dialup server, the DHCP server must be configured to assign IP addresses that do not match the private network behind the FortiGate dialup client. In addition, the FortiGate dialup client routing table must contain a static route to the DHCP server (see the “Router” chapter of the [FortiGate Administration Guide](#)).

FortiGate dialup-client configuration steps

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

- 1 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.
- 2 Configure the FortiGate dialup server. See [“Configuring the dialup server to accept FortiGate dialup client connections” on page 35](#).
- 3 Configure the FortiGate dialup client. See [“Configuring a FortiGate dialup client” on page 36](#).

Configuring the dialup 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 [“Defining Phase 1 IKE and authentication parameters” on page 51](#). Enter these settings in particular:

Remote Gateway	Select Dialup User.
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.

- 2 Define the phase 2 parameters needed to create a VPN tunnel with the FortiGate dialup client. See [“Defining Phase 2 tunnel creation parameters” on page 71](#). Enter these settings in particular:

Remote Gateway	Select the set of phase 1 parameters that you defined for the FortiGate dialup client. The name of the gateway can be selected from the Dialup User list.
-----------------------	---

- 3 Define the source and destination addresses of the IP packets that are to be transported through the VPN tunnel. See [“Defining IP source and destination addresses” on page 76](#). Enter these settings in particular:
 - For the originating address (source address), enter the IP address of the server, host, or network behind the FortiGate dialup server.
 - For the remote address (destination address), enter the IP address and netmask of the private network behind the FortiGate dialup client.
- 4 Define the firewall encryption policy to permit communications between the source and destination addresses. See [“Defining a firewall encryption policy” on page 78](#). Enter these settings in particular:

Source	Interface/Zone Select the local interface to the internal (private) network. Address Name Select the source address that you defined in Step 3.
Destination	Interface/Zone Select the local interface to the external (public) network. Address Name Select the destination address that you defined in Step 3.

Action	Select ENCRYPT.
VPN Tunnel	Select the name of the phase 2 tunnel configuration that you created in Step 2. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Clear Allow outbound to prevent traffic from the local 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.

Configuring a FortiGate dialup client

- At the FortiGate dialup client, define the phase 1 parameters needed to authenticate the dialup server and establish a secure connection. See [“Defining Phase 1 IKE and authentication parameters” on page 51](#). Enter these settings in particular:

Remote Gateway	Select Static IP Address.
IP Address	Type the IP address of the dialup server's public interface.
Mode	Because the FortiGate dialup client has a dynamic IP address, select Aggressive.
Advanced	If you defined a peer ID for the dialup client in the FortiGate dialup server configuration, in the Local ID field, type 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.

- Define the phase 2 parameters needed to create a VPN tunnel with the dialup server. See [“Defining Phase 2 tunnel creation parameters” on page 71](#). Enter these settings in particular:

Remote Gateway	Select the set of phase 1 parameters that you defined for the dialup server. The name of the dialup server can be selected from the Static IP Address list.
-----------------------	---

- Define the source and destination addresses of the IP packets that are to be transported through the VPN tunnel. See [“Defining IP source and destination addresses” on page 76](#). Enter these settings in particular:
 - For the originating address (source address), enter the IP address and netmask of the private network behind the FortiGate dialup client.
 - For the remote address (destination address), enter the IP address of the host, server, or network behind the FortiGate dialup server.
- Define a firewall encryption policy to permit communications between the source and destination addresses. See [“Defining a firewall encryption policy” on page 78](#). Enter these settings in particular:

Source	Interface/Zone Select the local interface to the internal (private) network. Address Name Select the source address that you defined in Step 3.
Destination	Interface/Zone Select the local interface to the external (public) network. Address Name Select the destination address that you defined in Step 3.

- | | |
|-------------------|---|
| Action | Select ENCRYPT. |
| VPN Tunnel | Select the name of the phase 2 tunnel configuration that you created in Step 2.
Clear Allow inbound to prevent traffic from the remote network from initiating the tunnel after the tunnel has been established.
Select Allow outbound to enable traffic from the local network to initiate the tunnel. |
- 5 Place the policy in the policy list above any other policies having similar source and destination addresses.

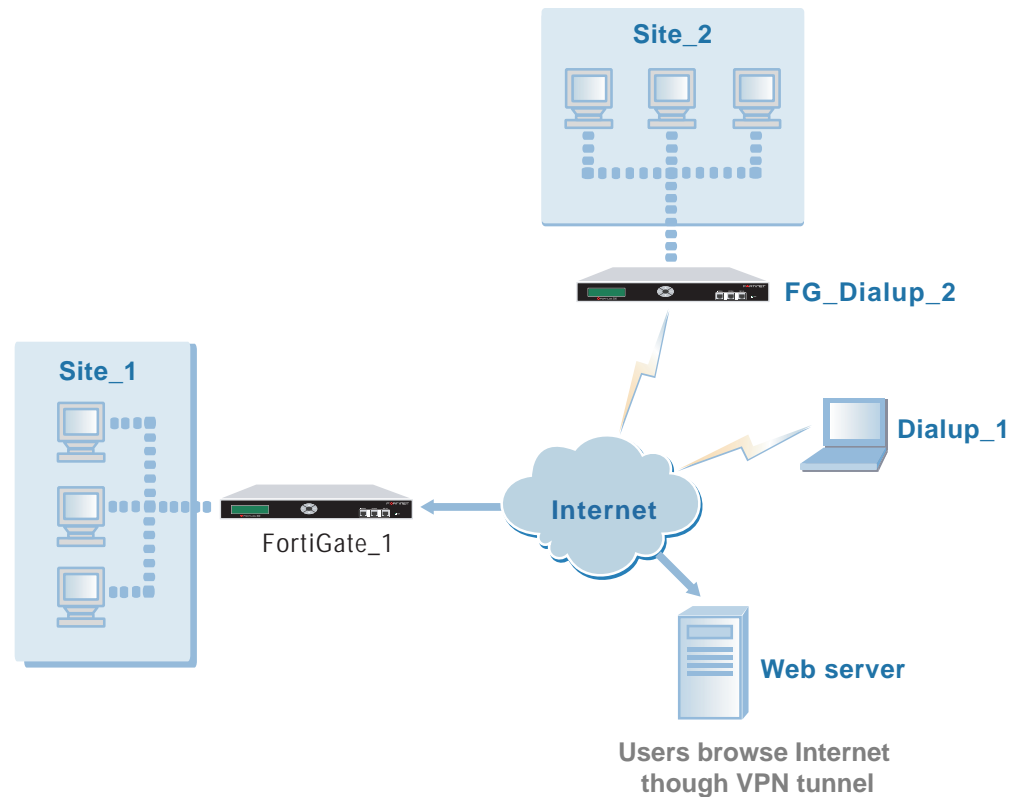
Internet-browsing configurations

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

The FortiGate unit enables FortiClient dialup clients and computers behind a remote FortiGate VPN peer or FortiGate dialup client to access private local networks through VPN tunnels.

When Internet browsing is enabled on the FortiGate unit (for example, see FortiGate_1 in [Figure 10](#)), remote users can access the private network behind FortiGate_1 and browse the Internet securely—all traffic generated remotely is inspected and processed by FortiGate_1 to ensure that the content is safe. Packets from remote VPN clients and/or peers are decrypted, subjected to the firewall policy for the private network behind FortiGate_1, and sent back out the FortiGate_1 interface that has Internet access.

Figure 10: Example Internet-browsing configuration



In Figure 10, FG_Dialup_2 may be a VPN peer or a dialup client.

Internet-browsing infrastructure requirements

Any of the following configurations may be in place:

- a gateway-to-gateway configuration (see [“Gateway-to-gateway configurations” on page 15](#))
- a FortiClient dialup-client configuration (see [“FortiClient dialup-client configurations” on page 25](#))
- a FortiGate dialup-client configuration (see [“FortiGate dialup-client configurations” on page 31](#))

Internet-browsing configuration steps

To enable Internet browsing in a gateway-to-gateway configuration, see [“Enabling Internet browsing in a gateway-to-gateway configuration” on page 39](#).

To enable Internet browsing in a FortiClient dialup-client configuration, see [“Enabling Internet browsing in a FortiClient dialup-client configuration” on page 40](#).

To enable Internet browsing in a FortiGate dialup-client configuration, see [“Enabling Internet browsing in a FortiGate dialup-client configuration” on page 41](#).

Enabling Internet browsing in a gateway-to-gateway configuration

The procedure in this section assumes that a gateway-to-gateway configuration 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:

- Enable Internet browsing on the FortiGate unit whose firewall policy is to apply to both local and remote traffic. When the Internet browsing option is enabled on a FortiGate unit, all IP traffic generated remotely is screened and processed according to the firewall policy that applies to the local private network.
- Configure the remote peer to force all traffic through the VPN tunnel by changing the IP destination address in its firewall encryption policy to “all”.

To enable Internet browsing in a gateway-to-gateway configuration

- 1 On the FortiGate unit whose firewall policy is to apply to both local and remote traffic, go to **VPN > IPSec > Phase 2**.
- 2 Select the Edit icon in the row beside the phase 2 definition that creates a VPN tunnel with the remote peer.
- 3 Select Advanced.
- 4 From the Internet browsing list, select the interface that connects the FortiGate unit to the local private network.
- 5 Select OK.
- 6 At the remote peer, go to Firewall > Policy.
- 7 Select the Edit icon in the row that corresponds to the firewall encryption policy.
- 8 From the Address Name list under Destination, select all.
- 9 Select OK.

Enabling Internet browsing in a FortiClient dialup-client configuration

The procedures in this section assume that a FortiClient dialup-client configuration is in place, and that it is operating properly. All you have to do to create an internet-browsing configuration based on an existing FortiClient dialup-configuration is edit the dialup-client configuration as follows:

- Enable Internet browsing in the IPsec phase 2 settings on the FortiGate dialup server. See [“To select the Internet-browsing interface on the FortiGate dialup server”](#) below.
- Configure the FortiClient Host Security application to force all IP traffic through the VPN tunnel. See [“To configure FortiClient to force all IP traffic through the VPN tunnel”](#) below.

To select the Internet-browsing interface on the FortiGate dialup server

- 1 At the FortiGate dialup server, go to **VPN > IPsec > Phase 2**.
- 2 Select the Edit icon in the row beside the phase 2 tunnel definition that you defined for FortiClient dialup clients.
- 3 Select Advanced.
- 4 From the Internet browsing list, select the interface that connects the FortiGate dialup server to the local private network.
- 5 Select OK.

To configure FortiClient to force all IP traffic through the VPN tunnel

- 1 At the remote host, start FortiClient.
- 2 Go to **VPN > Connections**.
- 3 Select the definition that connects FortiClient to the FortiGate dialup server, and then select Edit.
- 4 In the Edit Connection dialog box, select Advanced.
- 5 In the Remote Network group, select Add.
- 6 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.
- 7 Select OK twice to close the dialog boxes.

Enabling Internet browsing in a FortiGate dialup-client configuration

The procedure in this section assumes that a FortiGate dialup-client configuration is in place, and that it is operating properly. To create an internet-browsing configuration based on an existing FortiGate dialup-client configuration, you must edit the FortiGate dialup-client configuration as follows:

- Enable Internet browsing on the FortiGate dialup server. When the Internet browsing option is enabled on the dialup server, all IP traffic generated remotely is screened and processed according to the firewall policy that applies to the private network behind the dialup server.
- Configure the remote peer to force all traffic through the VPN tunnel by changing the IP destination address in its firewall encryption policy to “all”.

To enable Internet browsing in a FortiGate dialup-client configuration

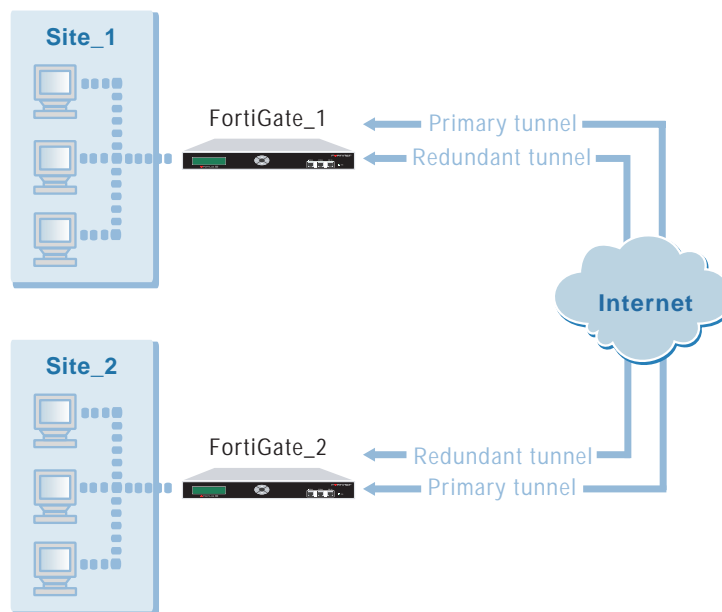
- 1 At the FortiGate dialup server, go to **VPN > IPSec > Phase 2**.
- 2 Select the Edit icon in the row beside the phase 2 definition that creates a VPN tunnel with the FortiGate dialup client.
- 3 Select Advanced.
- 4 From the Internet browsing list, select the interface that connects the FortiGate dialup server to the local private network.
- 5 Select OK.
- 6 At the FortiGate dialup client, go to **Firewall > Policy**.
- 7 Select the Edit icon in the row that corresponds to the firewall encryption policy.
- 8 From the Address Name list under Destination, select all.
- 9 Select OK.

Redundant-tunnel configurations

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

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

Figure 11: Example redundant-tunnel configuration



In [Figure 11](#), two separate interfaces to the Internet are available on both VPN peers.



Note: A tunnel that is created using manual keys (see [“Manual-key configurations”](#) on page 49) cannot be included in a redundant-tunnel configuration.

A redundant-tunnel configuration at each VPN peer includes:

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

The procedures in this section assume that two separate interfaces to the Internet are available on each VPN peer. The source addresses specified in both firewall encryption policies on the same VPN peer must be identical. Similarly, the destination addresses specified in both firewall encryption policies on the same VPN peer must be identical.

Redundant-tunnel infrastructure requirements

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

Redundant-tunnel configuration steps

- 1 At the local FortiGate unit, configure phase 1 parameters for the primary interface of the remote peer. See [“Defining Phase 1 IKE and authentication parameters” on page 51](#). Enter these settings in particular:

Remote Gateway Select Static IP Address.
IP Address Type the IP address of the primary interface of the remote peer.

- 2 Repeat Step 1 for the redundant interface of the remote peer.
- 3 Create a phase 2 definition for the primary tunnel. See [“Defining Phase 2 tunnel creation parameters” on page 71](#). Enter these settings in particular:

Remote Gateway Select the phase 1 gateway that you defined for the primary interface of the remote peer. The name of the gateway can be selected from the Static IP Address list.

- 4 Enter the following CLI command to bind the tunnel to the FortiGate interface to the internal network:

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

For more information about CLI commands, see the [FortiGate CLI Reference Guide](#).

- 5 Repeat Steps 3 and 4 for the redundant tunnel.
- 6 Define the source and destination addresses of the IP packets that are to be transported through the primary and redundant tunnels. See [“Defining IP source and destination addresses” on page 76](#). Enter these settings in particular:
 - For the originating address (source address), enter the IP address and netmask of the private network behind the local FortiGate unit.
 - For the remote address (destination address), enter the IP address and netmask of the private network behind the remote peer.
- 7 Define the firewall encryption policy for the local primary interface. See [“Defining a firewall encryption policy” on page 78](#). Enter these settings in particular:

Source Interface/Zone
 Select the local interface to the internal (private) network.
 Address Name
 Select the source address that you defined in Step 6.

Destination Interface/Zone
 Select the local primary interface to the Internet.
 Address Name
 Select the destination address that you defined in Step 6.

Action Select ENCRYPT.

VPN Tunnel Select the name of the phase 2 tunnel configuration that you created in Step 3.
 Select Allow inbound to enable traffic from the remote network to initiate the tunnel.
 Select Allow outbound to enable traffic from the local network to initiate the tunnel.

- 8 Place the policy in the policy list above any other policies having similar source and destination addresses.
- 9 Define a firewall encryption policy for the local redundant interface. See [“Defining a firewall encryption policy” on page 78](#). Enter these settings in particular:

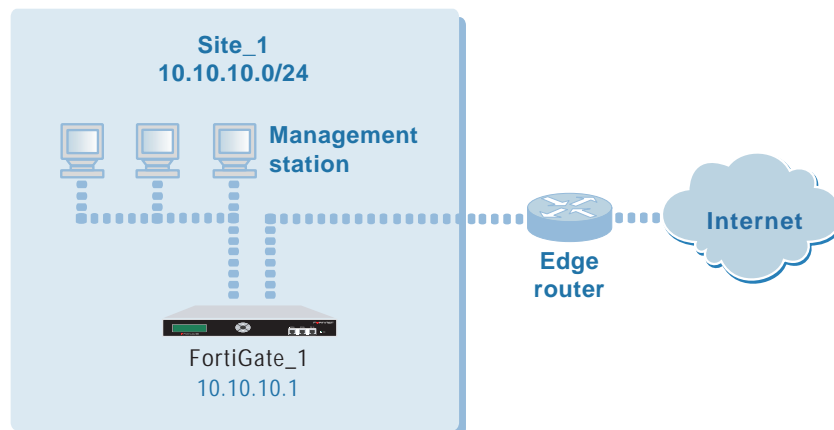
Source	Interface/Zone Select the local interface to the internal (private) network. Address Name Select the source address that you defined in Step 6.
Destination	Interface/Zone Select the local redundant interface to the Internet. Address Name Select the destination address that you defined in Step 6.
Action	Select ENCRYPT.
VPN Tunnel	Select the name of the phase 2 configuration that you created in Step 5. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow outbound to enable traffic from the local network to initiate the tunnel.

- 10 Place the policy in the policy list directly beneath the policy for the primary interface.
- 11 Configure ping servers on the local primary and redundant interfaces. See [“To add a ping server to an interface”](#) in the [“System network”](#) chapter of the [FortiGate Administration Guide](#).
- 12 Repeat this procedure at the remote FortiGate unit.

Transparent VPN configurations

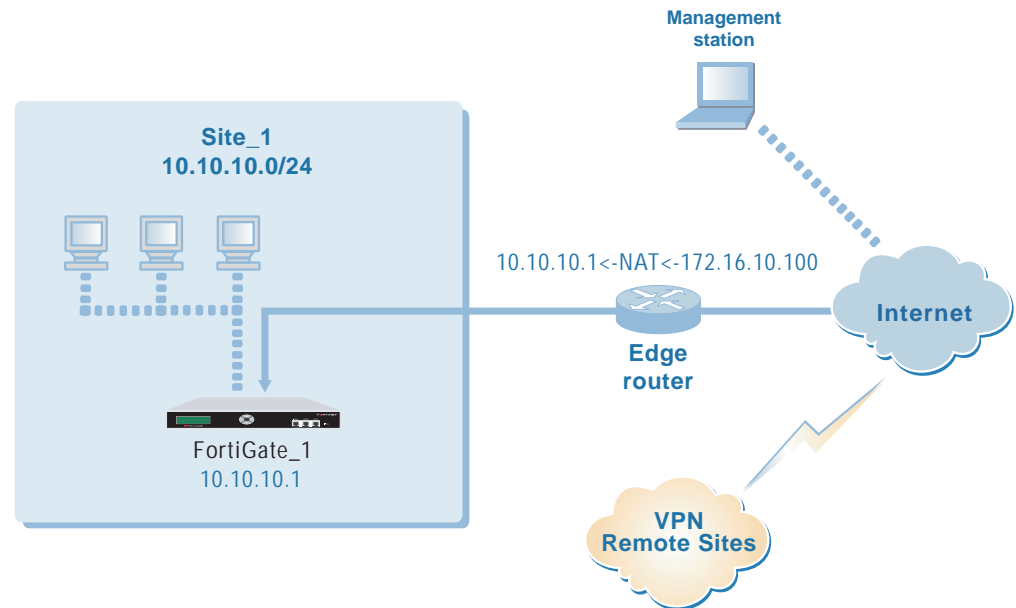
In Transparent mode, all interfaces of the FortiGate unit except the management interface (which by default is assigned IP address 10.10.10.1/255.255.255.0) are invisible at the network layer. Typically, when a FortiGate unit runs in Transparent mode, different network segments are connected to the FortiGate interfaces. [Figure 12](#) shows the management station on the same subnet. The management station can connect to the FortiGate unit directly through the web-based manager.

Figure 12: 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 13](#)), the router must translate (NAT) a routable address to direct management traffic to the FortiGate management interface.

Figure 13: Management station on external network



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

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



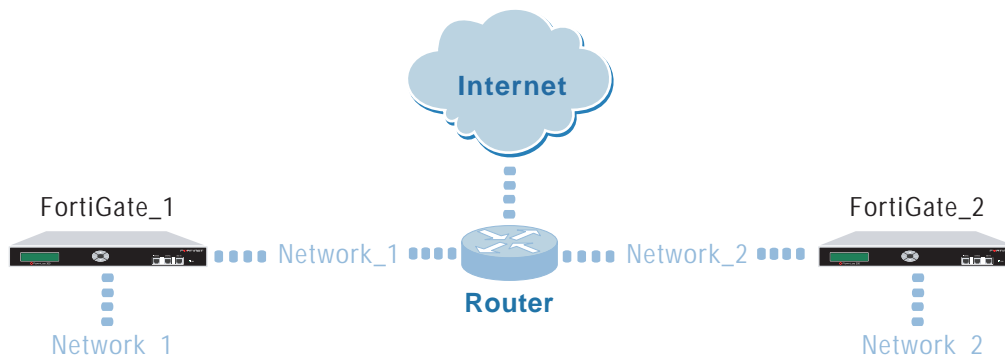
Note: VPNs between two FortiGate units running in Transparent mode do not support inbound/outbound NAT within the tunnel. In addition, a FortiGate unit running in Transparent mode cannot be used in a hub-and-spoke configuration.

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

In the example configuration shown in [Figure 13](#), 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.

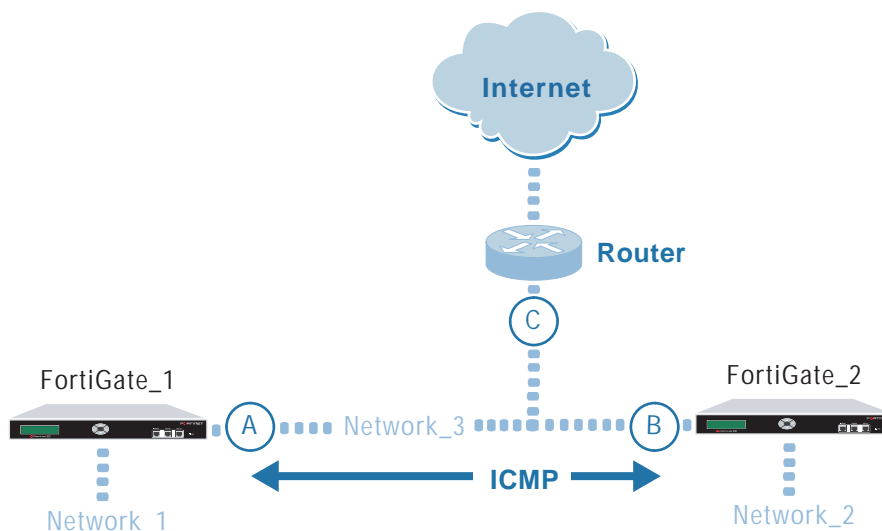
If you want to configure a VPN between two FortiGate units running in Transparent mode, each unit must have an independent connection to a router that acts as a gateway to the Internet, and both units must be on separate networks that have a different address space. When the two networks linked by the VPN tunnel have different address spaces (see Figure 14), at least one router must separate the two FortiGate units, unless the packets can be redirected using Internet Control Message Protocol (ICMP) (see Figure 15).

Figure 14: Link between two FortiGate units running in Transparent mode



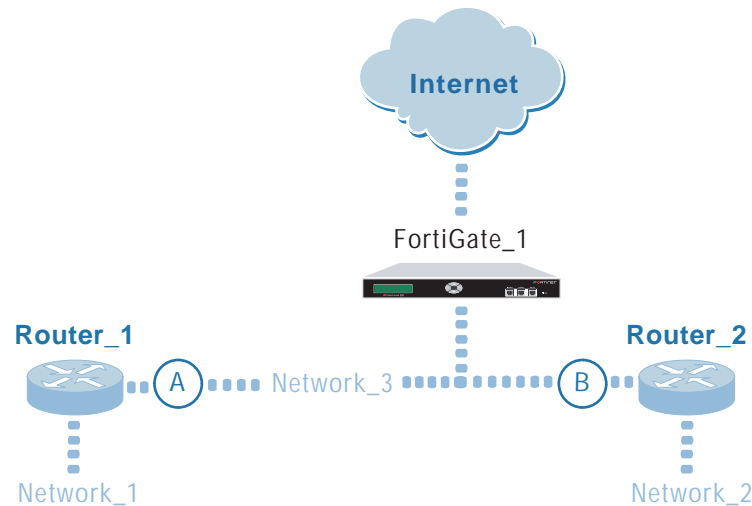
In Figure 15, interface C behind the router is the default gateway for both FortiGate units. Packets that cannot be delivered on Network_1 are routed to interface C by default. Similarly, packets that cannot be delivered on Network_2 are routed to interface C. In this case, the router must be configured to redirect packets destined for Network_1 to interface A and redirect packets destined for Network_2 to interface B.

Figure 15: ICMP redirecting packets to two FortiGate units running in Transparent mode



If there are additional routers behind the FortiGate unit (see [Figure 16](#)) 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 16](#), 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 16: Destinations on remote networks behind internal routers



Transparent VPN infrastructure requirements

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

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

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

Before you begin

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

Transparent VPN configuration steps

- 1 At the local FortiGate unit, define the phase 1 parameters needed to establish a secure connection with the remote peer. See [“Defining Phase 1 IKE and authentication parameters” on page 51](#). 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 66 and “NAT keepalive frequency” on page 66 .

- 2 Define the phase 2 parameters needed to create a VPN tunnel with the remote peer. See [“Defining Phase 2 tunnel creation parameters” on page 71](#). Enter these settings in particular:

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

- 3 Define the source and destination addresses of the IP packets that are to be transported through the VPN tunnel. See [“Defining IP source and destination addresses” on page 76](#). Enter these settings in particular:
 - For the originating address (source address), enter the IP address of the local management interface (for example, 10.10.10.1/32).
 - For the remote address (destination address), enter the IP address and netmask of the private network behind the remote peer (for example, 192.168.10.0/24). If the remote peer is a FortiGate unit running in Transparent mode, enter the IP address of the remote management interface instead.
- 4 Define a firewall encryption policy to permit communications between the source and destination addresses. See [“Defining a firewall encryption policy” on page 78](#). Enter these settings in particular:

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

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

Manual-key configurations

If required, you can manually define cryptographic keys for establishing an IPsec VPN tunnel. You would define manual keys in situations 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).
- Encryption and authentication needs to be disabled.

In both cases, you do not specify IPsec phase 1 and phase 2 parameters; you define manual keys on the **VPN > IPSEC > Manual Key** tab instead.

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



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

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

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



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

To specify manual keys for creating a tunnel

- 1 Go to **VPN > IPSEC > Manual Key** and select **Create New**.
- 2 Include appropriate entries as follows:

VPN Tunnel 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 0xbb8 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 0xbb8 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.
Encryption Algorithm	Select one of the following symmetric-key encryption algorithms: <ul style="list-style-type: none"> • DES-Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 3DES-Triple-DES, in which plain text is encrypted three times by three keys. • AES128-A 128-bit block algorithm that uses a 128-bit key. • AES192-A 128-bit block algorithm that uses a 192-bit key. • AES256-A 128-bit block algorithm that uses a 256-bit key.
Encryption Key	If you selected: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • MD5-Message Digest 5 algorithm, which produces a 128-bit message digest. • SHA1-Secure Hash Algorithm 1, which produces a 160-bit message digest.

Authentication Key If you selected:

- MD5, type a 32-character hexadecimal number (0-9, a-f) separated into two segments of 16 characters.
- SHA1, type 40-character hexadecimal number (0-9, a-f) separated into one segment of 16 characters and a second segment of 24 characters.

Concentrator

If the tunnel will be included in a hub-and-spoke configuration, you may select the concentrator from the list. The hub must be added to the FortiGate configuration before it can be selected here. See [“Hub-and-spoke configurations”](#) on page 18.

- 3 Select OK.

Defining Phase 1 IKE and authentication parameters

The basic phase 1 settings associate IPsec phase 1 parameters with a remote peer or dialup client(s) and determine:

- whether the various phase 1 parameters will be exchanged in multiple rounds with encrypted authentication information (main mode) or in a single message with authentication information that is not encrypted (aggressive mode)
- whether a preshared key or digital certificates will be used to authenticate the identities of two VPN peers (or a VPN server and its client)
- whether a special identifier, certificate distinguished name, or group name will be used to identify the remote peer or dialup client when a connection attempt is made

Figure 17: Basic Phase 1 settings (VPN > IPSEC > Phase 1 > Create New)

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 49 instead.

Authenticating remote peers and clients

A phase 1 configuration defines the parameters that a FortiGate unit will use to authenticate remote VPN peers and dialup clients. You can authenticate remote peers and dialup clients using digital certificates if you have the required personal/site certificates and root certificates from the issuing CA (see [“To authenticate a remote peer or dialup client using digital certificates” on page 52](#)). Otherwise, you can authenticate remote peers and dialup clients using a preshared key (see [“To authenticate a remote peer using a preshared key” on page 53](#)).

Additional options are available to authenticate remote peers and clients based on:

- peer ID
- certificate distinguished name
- extended authentication (XAuth), which provides password-based authentication for dialup user groups through technologies such as PAP, CHAP, RADIUS, and LDAP

For more information about these options, see [“Peer and user authentication options” on page 57](#).

To authenticate a remote peer or dialup client using digital certificates

- 1 Go to **VPN > IPSEC > Phase 1**.
- 2 Select Create New to add a new phase 1 configuration or select the Edit button beside an existing configuration.
- 3 Include appropriate entries as follows:

Gateway Name	Enter a name that reflects the origination of the remote connection.
Remote Gateway	Select the nature of the remote connection: <ul style="list-style-type: none"> • If a remote peer with a static IP address will be connecting to the FortiGate unit, select Static IP Address. • If one or more FortiGate/FortiClient dialup clients with dynamic IP addresses will be connecting to the FortiGate unit, select Dialup User. • If a remote peer that has a domain name and subscribes to a dynamic DNS service will be connecting to the FortiGate unit, select Dynamic DNS.
IP Address	If you set Remote Gateway to Static IP Address, type the IP address of the remote peer.
Dynamic DNS	If you set Remote Gateway to Dynamic DNS, type the domain name of the remote peer.
Mode	Select Main or Aggressive, depending on the Peer Options setting. <ul style="list-style-type: none"> • 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. You must select Aggressive when the remote FortiGate unit has a dynamic IP address.
Authentication Method	Select RSA Signature.

Certificate Name	Select the name of the server certificate that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. To obtain and load the required server certificate, see “Managing digital certificates” on page 54 .
Peer Options	To authenticate one (or more) remote peers or dialup clients based on a particular (or shared) security certificate, select Accept this peer certificate only and select the name of the certificate from the list. For details, see “Enabling VPN access for specific certificate holders” on page 57 . The certificate must be added to the FortiGate configuration through the <code>config user peer</code> CLI command before it can be selected here. For more information, see the “config user” chapter of the FortiGate CLI Reference Guide . If the remote VPN peer or client has a dynamic IP address, set Mode to Aggressive. Select Accept this peer certificate group only to use a certificate group to authenticate remote peers and dialup clients that have dynamic IP addresses and use unique certificates. Select the name of the group from the list. For details, see “Enabling VPN access for specific certificate holders” on page 57 . The group must be added to the FortiGate configuration through the <code>config user peer</code> and <code>config user peergrp</code> CLI commands before it can be selected here. For more information, see the “config user” chapter of the FortiGate CLI Reference Guide . When the remote peers and clients have dynamic IP addresses, you must set Mode to Aggressive.
Advanced	You may retain the default settings unless changes are needed to meet your specific requirements. See “Defining IKE negotiation parameters” on page 64 and “Configuring the phase 1 IKE exchange” on page 67 .

4 If you are configuring authentication parameters for a dialup user group, optionally define extended authentication (XAuth) parameters. See [“Enabling XAuth on the FortiGate unit” on page 63](#).

5 Select OK.

To authenticate a remote peer using a preshared key

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

2 Select Create New to add a new phase 1 configuration or select the Edit button beside an existing configuration.

3 Include appropriate entries as follows:

Gateway Name	Enter a name that reflects the origination of the remote connection.
Remote Gateway	Select the nature of the remote connection: <ul style="list-style-type: none"> • If a remote peer with a static IP address will be connecting to the FortiGate unit, select Static IP Address. • If one or more FortiGate/FortiClient dialup clients with dynamic IP addresses will be connecting to the FortiGate unit, select Dialup User. • If a remote peer that has a domain name and subscribes to a dynamic DNS service will be connecting to the FortiGate unit, select Dynamic DNS.
IP Address	If you set Remote Gateway to Static IP Address, type the IP address of the remote peer.

- | | |
|------------------------------|---|
| Dynamic DNS | If you set Remote Gateway to Dynamic DNS, type the domain name of the remote peer. |
| Mode | Select Main or Aggressive, depending on the Peer Options setting. <ul style="list-style-type: none"> • 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. You must select Aggressive when the remote FortiGate unit has a dynamic IP address. |
| Authentication Method | Select Pre-shared Key. |
| Pre-shared Key | Enter the preshared key that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. You must define the same value at the remote peer or client. The key must contain at least 6 printable characters and should only be known by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters. |
| Peer options | To accept connections without checking peer IDs, select Accept any peer ID.
To grant access to one or more remote peers or FortiGate dialup clients based on a peer ID, select Accept this peer ID and type the identifier. This value must be identical to the value in the Local ID field of the phase 1 remote gateway configuration on the remote peer or FortiGate dialup client. For details, see “Enabling VPN peer identification” on page 59 . If you are configuring authentication parameters for FortiClient dialup clients, refer to the Authenticating FortiClient Dialup Clients Technical Note .
To grant access to dialup users based on the name of a dialup group, select Accept peer ID in dialup group and select the name of the group from the list. You must create the user group before it can be selected here. See the “User” chapter of the FortiGate Administration Guide . For more information about using peer IDs to authenticate dialup users, see “Enabling VPN peer identification” on page 59 . |
| Advanced | You may retain the default settings unless changes are needed to meet your specific requirements. See “Defining IKE negotiation parameters” on page 64 and “Configuring the phase 1 IKE exchange” on page 67 . |
- 4 If you are configuring authentication parameters for a dialup user group, optionally define extended authentication (XAuth) parameters. See [“Enabling XAuth on the FortiGate unit” on page 63](#).
 - 5 Select OK.

Managing digital certificates

Digital certificates are downloadable files that you can install on FortiGate units and VPN peers or clients. Digital certificates are used to authenticate VPN peers and clients. An X.509 digital certificate consists of a public key and some identifying information that has been digitally signed by a trusted third party known as a certificate authority (CA). Because CAs can be trusted, the certificates issued by a CA are deemed to be trustworthy.

To obtain a personal or site certificate, you must send a request to a CA that provides digital certificates that adhere to the X.509 standard. The FortiGate unit provides a way for you to generate the request. The generated request includes information such as the FortiGate unit's public static IP address, domain name, or email address.

In return, the CA will verify the information and register the contact information on a digital certificate that contains a serial number, an expiration date, and a public key. The CA will then send the digital certificate to you to install on the FortiGate unit. You must also obtain and install the CA's root certificate on the FortiGate unit.

After the required personal or site certificates and root certificates have been installed on the VPN peers and clients, the peers and clients identify themselves during phase 1 negotiations using certificates. The FortiGate unit provides its public key to the remote peer or client so that the remote peer or client can send encrypted messages to the FortiGate unit. Conversely, the remote peer or client provides its public key to the FortiGate unit, which uses the key to encrypt messages destined for the remote peer or client.

To generate a certificate request

- 1 Go to **VPN > Certificates > Local Certificates**.
- 2 Select **Generate**.
- 3 In the **Certification Name** field, type a name for the certificate request. Typically, this would be the name of the FortiGate unit.
- 4 Enter values in the **Subject Information** area to identify the FortiGate unit. If the FortiGate unit does not have a public IP address, use an email address (or domain name if available).
 - If you select **Host IP**, enter the public IP address of the FortiGate unit.
 - If you select **Domain Name**, enter the fully qualified domain name of the FortiGate unit. Do not include the protocol specification (`http://`) or any port number or path names.
 - If you select **E-mail**, enter the email address of the owner of the FortiGate unit.
- 5 Enter values in the **Optional Information** area to further identify the FortiGate unit.

Organization Unit	Name of your department.
Organization	Legal name of your company or organization.
Locality (City)	Name of the city or town where the FortiGate unit is installed.
State/Province	Name of the state or province where the FortiGate unit is installed.
Country	Select the country where the FortiGate unit is installed.
e-mail	Contact email address.
- 6 From the **Key Size** list, select **1024 Bit**, **1536 Bit** or **2048 Bit**. Larger keys are slower to generate but more secure. Not all FortiGate units support all three key sizes.
- 7 Select **OK**.

The request is generated and displayed in the **Local Certificates** list with a status of **Pending**.
- 8 Select the **Download** button to download the request to a PC on the local network.
- 9 In the **File Download** dialog box, select **Save**.

- 10 Name the file and save it on the local file system.
- 11 Submit the request to your CA as follows:
 - Using the web browser on the local PC, browse to the CA web site.
 - Follow the CA instructions to place a base-64 encoded PKCS#10 certificate request and upload your certificate request.
 - Follow the CA instructions to download their root certificate, and then install the root certificate on the FortiGate unit. See [“To install a CA root certificate” on page 56](#).
- 12 When you receive a signed certificate from the CA, install the certificate on the FortiGate unit. See [“To install a signed personal or site certificate” on page 56](#).

To install a signed personal or site certificate

- 1 When you receive a signed certificate from the CA, save the certificate on a PC that has management access to the FortiGate unit.
- 2 On the FortiGate unit, go to **VPN > Certificates > Local Certificates**.
- 3 Select Import.
- 4 Browse to the location on the management PC where the certificate has been saved, select the certificate, and then select OK.
- 5 Select OK.



Note: Consider backing up the certificate. The backup file is saved as a password-protected PKCS12 (Public Key Cryptography Standard 12) file. You can use the backup file if you need to restore the original certificate. For more information, see the “System maint” chapter of the [FortiGate Administration Guide](#).

To install a CA root certificate

- 1 After you download the root certificate of the CA, save the certificate on a PC that has management access to the FortiGate unit.
- 2 On the FortiGate unit, go to **VPN > Certificates > CA Certificates**.
- 3 Select Import.
- 4 Browse to the location on the management PC where the certificate has been saved, select the certificate, and then select OK.
- 5 Select OK.

The system assigns a unique name to each CA certificate. The names are numbered consecutively (CA_Cert_1, CA_Cert_2, CA_Cert_3, and so on).

Peer and user authentication options

In addition to preshared keys and RSA signatures, FortiGate units also support the following options to authenticate remote peers and dialup clients:

- If you are using certificates, certificate distinguished names can be used to permit access to recognized peers or dialup clients only. If required to authenticate a number of peers or clients that use unique Distinguished Names (DNs), you can create a certificate group. See [“Enabling VPN access for specific certificate holders” on page 57](#).
- If you are using preshared keys, you can enable the recognition of identifiers for FortiGate/FortiClient dialup clients or FortiGate units that have dynamic IP addresses and subscribe to a dynamic DNS service. When the preshared key and identifier belonging to the remote peer or dialup client matches the values specified on the FortiGate unit, access is granted. See [“Enabling VPN peer identification” on page 59](#).
- If you are using preshared keys, you can enable the recognition of a dialup user group for a number of FortiGate/FortiClient dialup clients that use unique identifiers and preshared keys. When a dialup client authenticates as a member of the user group, access is granted. See [“Enabling VPN peer identification” on page 59](#).
- Extended authentication (XAuth) can be enabled in conjunction with PAP, CHAP, RADIUS, or LDAP services to challenge dialup clients for a user name and password. See [“Enabling XAuth on the FortiGate unit” on page 63](#).

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.

If you want two VPN peers (or a FortiGate unit and a dialup client) to accept reciprocal connections using certificates, you must enable a DN exchange when you define the phase 1 parameters.

Before you begin

The following procedures assume that you already have an existing phase 1 configuration (see [“To authenticate a remote peer or dialup client using digital certificates” on page 52](#)). Follow the procedures below to add certificate-based authentication parameters to the existing configuration.

Before you begin, you must obtain the certificate DN of the remote peer or dialup client. If you are using the FortiClient Host Security application as a dialup client, refer to *FortiClient online Help* for information about how to view the certificate DN. To view the certificate DN of a FortiGate unit, see [“To view server certificate information and obtain the local DN”](#) below.

Afterward, use the `config user peer` CLI command to load the DN value into the local 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 “config user” chapter of the [FortiGate CLI Reference Guide](#).

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 “Users and authentication” chapter of the [FortiGate Administration Guide](#). To create the certificate group afterward, use the `config user peergrp` CLI command. See the “config user” chapter of the [FortiGate CLI Reference Guide](#).

To view server certificate information and obtain the local DN

- 1 Go to **VPN > Certificates > Local Certificates**.

Name	Subject	Status	
FortiGate-500A	CN = info@fortinet.com	OK	  

- 2 Note the CN value in the Subject field (for example, CN = 172.16.10.125 or CN = info@fortinet.com).

To view CA root certificate information and obtain the CA certificate name

- 1 Go to **VPN > Certificates > CA Certificates**.
- 2 Note the value in the Name column (for example, CA_Cert_1).

To enable access for a specific certificate holder or a group of certificate holders

- 1 At the FortiGate VPN server, go to **VPN > IPSEC > Phase 1**.
- 2 In the list of defined phase 1 configurations, select the Edit button to edit the existing phase 1 configuration.

- 3 Under Peer Options, select one of these options:
 - To accept a specific certificate holder, select Accept this peer certificate only and select the DN 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.
 - 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.
- 4 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.
- 5 Select OK.

Enabling VPN peer identification

If you are using preshared keys to authenticate remote peers and clients, you can use peer IDs to enhance access security. To enable peer identification, you assign IDs to remote peers and/or dialup clients. Afterward, when a remote peer or dialup client attempts to establish a VPN connection with the local FortiGate unit, the unit can accept the connection based on the ID of the remote peer or dialup client.

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 phase 1 Remote Gateway and Mode settings determine which Peer Options settings may be used for authentication purposes (see [Table 1](#)). The Mode setting offers identifier confidentiality as follows:

- When main mode is selected, the identifier is hidden. Main mode is typically used when both VPN peers have static IP addresses.
- When aggressive mode is selected, the VPN peers exchange identifiers in the clear. Aggressive mode is typically used when a remote peer or dialup client has a dynamic IP address. More than one remote peer or dialup client can share the same identifier (local ID) for authentication purposes when aggressive mode is selected.



Note: If you want to dedicate a tunnel to a FortiGate dialup client or a FortiGate unit that has a dynamic IP address and subscribes to a dynamic DNS service, you must assign a unique identifier (local ID) to that FortiGate unit. Afterward select Aggressive mode on the FortiGate VPN server and specify the identifier as a peer ID value on the FortiGate VPN server.

Table 1: Phase 1 Peer Options settings

Remote Gateway and Mode	Accept any peer ID	Accept this peer ID	Accept peer ID in dialup group
Dialup User			
Main mode	•		•
Aggressive mode	•	•	•
Static IP address			
Main mode	•		
Aggressive mode	•		
Dynamic DNS			
Main mode	•		
Aggressive mode	•	•	

Accept any peer ID is always available. It is the default choice and when selected, the FortiGate unit accepts connections without checking peer IDs for authentication purposes (the remote peer or dialup client authenticates using a preshared key or certificate only).

Accept this peer ID is available to support remote VPN peers and clients that have dynamic IP addresses, including FortiGate units that subscribe to a dynamic DNS service. To authenticate FortiGate VPN peers or dialup clients, the value specified on the FortiGate dialup server must be identical to the value in the Local ID field in the phase 1 settings on the remote peer or dialup client. If you are configuring authentication parameters for FortiClient dialup clients, refer to the [Authenticating FortiClient Dialup Clients Technical Note](#).

The Accept this peer ID option also permits ID sharing when more than one FortiGate/FortiClient dialup client connects to the same IPsec VPN tunnel—the FortiGate dialup server will accept connections from any FortiGate/FortiClient dialup client that uses the same preshared key and the specified ID, as long as Mode is set to Aggressive. For more information, see one or more of the following sections:

- [“To assign an identifier \(local ID\) to a FortiGate unit” on page 61](#)
- [“To authenticate a FortiGate DDNS peer or dialup client\(s\) using one ID” on page 62.](#)
- [“To authenticate dialup clients that use unique identifiers and preshared keys” on page 62](#)
- [“To authenticate dialup clients that use unique preshared keys” on page 62](#)

Accept peer ID in dialup group is available to support connections from multiple FortiGate/FortiClient dialup clients that use unique IDs and preshared keys to connect to the VPN through the same VPN tunnel. To use this option, you must first include the dialup clients in a user group for authentication purposes. The FortiGate dialup server will accept connections from any FortiGate/FortiClient dialup client in the user group. Mode may be set to Main or Aggressive, depending on the dialup-client configuration.

For more information, see one or more of the following sections:

- [“To assign an identifier \(local ID\) to a FortiGate unit” on page 61](#)
- [“To authenticate dialup clients that use unique identifiers and preshared keys” on page 62](#)
- [“To authenticate dialup clients that use unique preshared keys” on page 62](#)

See the [Authenticating FortiClient Dialup Clients Technical Note](#) to configure FortiClient dialup clients.

Before you begin

The following procedures assume that you already have an existing phase 1 configuration (see [“To authenticate a remote peer using a preshared key” on page 53](#)). Follow the procedures below to add ID checking to the existing configuration.

Before you begin, you must obtain the identifier (local ID) of the remote peer or dialup client. If you are using the FortiClient Host Security application as a dialup client, refer to the [Authenticating FortiClient Dialup Clients Technical Note](#) to view or assign an identifier. To assign an identifier to a FortiGate dialup client or a FortiGate unit that has a dynamic IP address and subscribes to a dynamic DNS service, see [“To assign an identifier \(local ID\) to a FortiGate unit” on page 61](#).

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 “Users and authentication” chapter of the [FortiGate Administration Guide](#).

To assign an identifier (local ID) to a FortiGate unit

- 1 Go to **VPN > IPSEC > Phase 1**.
- 2 In the list of defined phase 1 configurations, select the Edit button to edit the phase 1 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 authenticate a FortiGate DDNS peer or dialup client(s) using one ID

The following procedure supports FortiGate/FortiClient dialup clients and FortiGate units that have dynamic IP addresses and subscribe to a DDNS (dynamic DNS) service. A FortiGate DDNS peer or dialup client may use a unique identifier and preshared key to connect using a dedicated tunnel. 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.

- 1 At the FortiGate VPN server, go to **VPN > IPSEC > Phase 1**.
- 2 In the list of phase 1 configurations, select the Edit button to edit the phase 1 parameters.
- 3 If the FortiGate VPN server is to authenticate a FortiGate dialup client that uses a dedicated tunnel, a FortiGate unit that has a dynamic IP address and subscribes to a dynamic DNS service, or FortiGate/FortiClient dialup clients that share the same preshared key and local ID to connect through the same VPN tunnel, select Aggressive.
- 4 Select Accept this peer ID and type the identifier into the corresponding field.
- 5 Select OK.

To authenticate dialup clients that use unique identifiers and preshared keys

The following procedure supports FortiGate/FortiClient dialup clients that use unique identifiers and preshared keys and are members of a dialup user group. Each dialup client must have a unique local ID and a unique preshared key. The dialup user group must be added to the FortiGate configuration before it can be selected (see the “User” chapter of the [FortiGate Administration Guide](#)).

The FortiGate dialup server compares the local ID that you specify at each dialup client to the FortiGate user-account user name. The dialup-client preshared key is compared to a FortiGate user-account password.

- 1 At the FortiGate VPN server, go to **VPN > IPSEC > Phase 1**.
- 2 In the list of phase 1 configurations, select the Edit button to edit the phase 1 parameters.
- 3 Verify that Mode is set to Aggressive.
- 4 Clear the Pre-shared Key field (the field should be empty). The FortiGate dialup server will compare the dialup-client preshared key value to the user account password value instead.
- 5 Select Accept peer ID in dialup group and then select the group name from the list of user groups.
- 6 Select OK.

To authenticate dialup clients that use unique preshared keys

The following procedure supports FortiGate/FortiClient dialup clients that use unique preshared keys and are members of a dialup user group. Each dialup client must have a unique preshared key. The dialup user group must be added to the FortiGate configuration before it can be selected (see the “User” chapter of the [FortiGate Administration Guide](#)).

The FortiGate dialup server compares the unique preshared key that you specify at each dialup client to the combined values of the user name and password specified in the corresponding FortiGate user account.

- 1 At the FortiGate VPN server, go to **VPN > IPSEC > Phase 1**.
- 2 In the list of phase 1 configurations, select the Edit button to edit the phase 1 parameters.
- 3 Select Main.
- 4 Clear the Pre-shared Key field (the field should be empty). The FortiGate dialup server will compare the dialup-client preshared key value to the user-account user name and password values instead.
- 5 Select Accept peer ID in dialup group and then select the group name from the list of user groups.
- 6 Select OK.

Enabling XAuth on the FortiGate unit

Extended authentication (XAuth) increases security by enabling remote dialup clients to be authenticated 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. A FortiGate unit can be configured to function either as an XAuth server or an XAuth client.

As an XAuth server, the FortiGate unit uses PAP or CHAP to forward authentication requests to an external RADIUS or LDAP server. In all cases, dialup clients are challenged to provide a user name and password when they attempt to connect to the FortiGate unit.

When choosing the type of encryption method to use between the FortiGate unit, the authentication server, and an XAuth client:

- Select PAP whenever possible. Select CHAP instead if applicable.
- You must select PAP for all implementations of LDAP and some implementations of Microsoft RADIUS.
- Select MIXED when the authentication server supports CHAP but the XAuth client does not. The FortiGate unit will use PAP to communicate with the XAuth client and CHAP to communicate with the authentication server.

As an XAuth client, the FortiGate unit is configured with its own user name and password, which it provides when challenged.

To authenticate a dialup user group using XAuth settings

Before you begin, create user accounts and user groups to identify the dialup clients that need to access the network behind the FortiGate dialup server. If password protection will be provided through an external RADIUS or LDAP server, you must configure the FortiGate dialup server to forward authentication requests to the authentication server. For information about these topics, see the “Users and Authentication” chapter of the [FortiGate Administration Guide](#).

- 1 At the FortiGate dialup server, go to **VPN > IPSEC > Phase 1**.

- 2 In the list of defined phase 1 configurations, select the Edit button to edit the phase 1 parameters for a particular remote gateway.
- 3 Select Advanced.
- 4 Under XAuth, select Enable as Server.
- 5 The Server Type setting determines the type of encryption method to use between the XAuth client, the FortiGate unit and the authentication server. Select one of the following options:
 - PAP—Password Authentication Protocol.
 - CHAP— Challenge-Handshake Authentication Protocol.
 - MIXED—Use PAP between the XAuth client and the FortiGate unit, and CHAP between the FortiGate unit and the authentication server.
- 6 From the User Group list, select the user group that needs to access the private network behind the FortiGate unit. The group must be added to the FortiGate configuration before it can be selected here.
- 7 Select OK.

To configure a FortiGate dialup client act as an XAuth client

- 1 At the FortiGate dialup client, go to **VPN > IPSEC > Phase 1**.
- 2 In the list of defined phase 1 configurations, select the Edit button to edit the phase 1 parameters for a particular remote gateway.
- 3 Select Advanced.
- 4 Under XAuth, select Enable as Client.
- 5 In the Username field, type the FortiGate PAP, CHAP, RADIUS, or LDAP user name that the FortiGate XAuth server will compare to its records when the FortiGate XAuth client attempts to connect.
- 6 In the Password field, type the password to associate with the user name.
- 7 Select OK.

Defining IKE negotiation parameters

In phase 1, the two peers exchange keys to establish a secure communication channel between them. As part of the phase 1 process, the two peers authenticate each other (see [“Authenticating remote peers and clients” on page 52](#)) and negotiate a way to encrypt further communications for the duration of the session. The P1 Proposal parameters select the encryption and authentication algorithms that are used to generate keys for protecting negotiations.

The IKE negotiation parameters determine:

- which encryption algorithms may be applied for converting messages into a form that the intended recipient only can read
- which authentication hash may be used for creating a keyed hash from a preshared or private key
- which Diffie-Hellman group will be used to generate a secret session key

Phase 1 negotiations (in main mode or aggressive mode) begin as soon as a remote VPN peer or client attempts to establish a connection with the FortiGate unit. Initially, the remote peer or dialup client sends the FortiGate unit a list of potential cryptographic parameters along with a session ID. The FortiGate unit compares those parameters to its own list of advanced phase 1 parameters and responds with its choice of matching parameters to use for authenticating and encrypting packets. The two peers handle the exchange of encryption keys between them, and authenticate the exchange through a preshared key or a digital signature.

Generating keys to authenticate an exchange

The FortiGate unit supports the generation of secret session keys automatically using a Diffie-Hellman algorithm. The Keylife setting in the P1 Proposal area determines the amount of time before the phase 1 key expires. Phase 1 negotiations are rekeyed automatically when there is an active security association. See [“Dead peer detection” on page 67](#).



Note: You can enable or disable automatic rekeying between IKE peers through the `phase1-rekey` attribute of the `config system global` CLI command. For more information, see the “config system” chapter of the [FortiGate CLI Reference Guide](#).

When you use a preshared key (shared secret) to set up two-party authentication, the remote VPN peer or client and the FortiGate unit must both be configured with the same preshared key. Each party uses a session key derived from the Diffie-Hellman exchange to create an authentication key, which is used to sign a known combination of inputs using an authentication algorithm (such as HMAC-MD5 or HMAC-SHA-1). Each party signs a different combination of inputs and the other party verifies that the same result can be computed.



Note: When you use preshared keys to authenticate VPN peers or clients, you must distribute matching information to all VPN peers and/or clients whenever the preshared key changes.

As an alternative, the remote peer or dialup client and FortiGate unit can exchange digital signatures to validate each other's identity with respect to their public keys. In this case, the required digital certificates (personal or site certificate and a root certificate from the CA) must be installed on the remote peer and on the FortiGate unit. By exchanging certificate DNs, the signed digital certificate on one peer is validated by the presence of the root certificate installed on the other peer.

Defining the remaining phase 1 options

Additional advanced phase 1 settings are available to ensure the smooth operation of phase 1 negotiations:

- **Nat-traversal**—If outbound encrypted packets will be subjected to NAT, this option determines whether the packet will be wrapped in a UDP IP header to protect the encrypted packet from modification. See [“NAT traversal”](#) below.
- **Keepalive Frequency**—If outbound encrypted packets will be subjected to NAT, this option determines how frequently empty UDP packets will be sent through the NAT device to prevent NAT address mapping from changing before the lifetime of a session expires. See [“NAT keepalive frequency”](#) below.
- **Dead Peer Detection**—This option determines whether the FortiGate unit will detect dead IKE peers and terminate a session between the time when a VPN connection becomes idle and the phase 1 encryption key expires. See [“Dead peer detection”](#) on page 67.

NAT traversal

Network Address Translation (NAT) is a way to convert private IP addresses to publicly routable Internet addresses and vice versa. When an IP packet passes through a NAT device, the source or destination address in the IP header is modified. FortiGate units support NAT version 1 (encapsulate on port 500 with non-IKE marker), version 3 (encapsulate on port 4500 with non-ESP marker), and compatible versions.

NAT cannot be performed on IPsec packets in ESP tunnel mode because the packets do not contain a port number. As a result, the packets cannot be demultiplexed. To work around this problem, the FortiGate unit provides a way to protect IPsec packet headers from NAT modifications. When the Nat-traversal option is enabled, outbound encrypted packets are wrapped inside a UDP IP header that contains a port number. This extra encapsulation allows NAT devices to change the port number without modifying the IPsec packet directly.

To provide the extra layer of encapsulation on IPsec packets, the Nat-traversal option must be enabled whenever a NAT device exists between two FortiGate VPN peers or a FortiGate unit and a dialup client such as FortiClient. On the receiving end, the FortiGate unit or FortiClient removes the extra layer of encapsulation before decrypting the packet.

NAT keepalive frequency

When a NAT device performs network address translation on a flow of packets, the NAT device determines how long the new address will remain valid if the flow of traffic stops (for example, the connected VPN peer may be idle). The device may reclaim and reuse a NAT address when a connection remains idle for too long. To work around this problem, when you enable NAT traversal, you can specify how often the FortiGate unit should send periodic keepalive packets through the NAT device in order to ensure that the NAT address mapping does not change during the lifetime of a session. The keepalive interval should be smaller than the session lifetime value used by the NAT device.

Dead peer detection

Sometimes, due to routing problems or other difficulties, the communication link between a FortiGate unit and a VPN peer or client may go down—packets could be lost if the connection is left to time out on its own. The FortiGate unit provides a mechanism called Dead Peer Detection (DPD) to prevent this situation and reestablish IKE negotiations automatically before a connection times out: the active phase 1 security associations are caught and renegotiated (rekeyed) before the phase 1 encryption key expires. DPD does not send probe messages on a regular basis. If configured (see the `dpd-idleworry` keyword under [“To define additional dead peer detection parameters” on page 68](#)), DPD sends probe messages when a connection has been idle, or when the local peer sends traffic to the remote peer.

Configuring the phase 1 IKE exchange

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 peer identification” on page 59](#) and [“Enabling XAuth on the FortiGate unit” on page 63](#). Follow this procedure to add IKE negotiation parameters to the existing definition.

To define IKE negotiation parameters

- 1 Go to **VPN > IPSEC > Phase 1**.
- 2 In the list of defined phase1 configurations, select the Edit button to edit the phase 1 parameters for a particular remote gateway.
- 3 Select Advanced and include appropriate entries as follows:

- P1 Proposal** Select the encryption and authentication algorithms that will be used to generate keys for protecting negotiations. Add or delete encryption and authentication algorithms as required. Select a minimum of one and a maximum of three combinations. The remote peer must be configured to use at least one of the proposals that you define. You can select any of the following symmetric-key algorithms:
- DES-Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
 - 3DES-Triple-DES, in which plain text is encrypted three times by three keys.
 - AES128-A 128-bit block algorithm that uses a 128-bit key.
 - AES192-A 128-bit block algorithm that uses a 192-bit key.
 - AES256-A 128-bit block algorithm that uses a 256-bit key.
- You can select either of the following message digests to check the authenticity of messages during phase 1 negotiations:
- MD5-Message Digest 5, the hash algorithm developed by RSA Data Security.
 - SHA1-Secure Hash Algorithm 1, which produces a 160-bit message digest.
- To specify a third combination, use the add button beside the fields for the second combination.

DH Group	Select one or more Diffie-Hellman groups from DH group 1, 2, and 5. When using aggressive mode, DH groups cannot be negotiated. <ul style="list-style-type: none"> If both VPN peers (or a VPN server and its client) have static IP addresses and use aggressive mode, select a single DH group. The setting on the FortiGate unit must be identical to the setting on the remote peer or dialup client. When the remote VPN peer or client has a dynamic IP address and uses aggressive mode, select up to three DH groups on the FortiGate unit and one DH group on the remote peer or dialup client. The setting on the remote peer or dialup client must be identical to one of the selections on the FortiGate unit. If the VPN peer or client employs main mode, you can select multiple DH groups. At least one of the settings on the remote peer or dialup client must be identical to the selections on the FortiGate unit.
Keylife	Type the amount of time (in seconds) that will be allowed to pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172800 seconds.
Nat-traversal	Enable this option if a NAT device exists between the local FortiGate unit and the VPN peer or client. The local FortiGate unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared).
Keepalive Frequency	If you enabled NAT traversal, enter a keepalive frequency setting. The value represents an interval from 0 to 900 seconds.
Dead Peer Detection	Enable this option to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required.

4 Select OK.

To define additional dead peer detection parameters

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 long and short idle time, a retry count, and a retry interval.

For more information about CLI commands, see the [FortiGate CLI Reference Guide](#).

Command syntax pattern

```
config vpn ipsec phase1
  edit <name_str>
    set <keyword> <variable>
  end

config vpn ipsec phase1
  edit <name_str>
    unset <keyword>
  end
```

config vpn ipsec phase1 command keywords and variables

Keywords and variables	Description	Default	Availability
<code>dpd-idlecleanup</code> <seconds_integer>	The DPD long idle setting when <code>dpd</code> is set to enable. Set the time, in seconds, that a link must remain unused before the local VPN peer pro-actively probes its state. After this period of time expires, the local peer will send a DPD probe to determine the status of the link even if there is no traffic between the local peer and the remote peer. The <code>dpd-idlecleanup</code> range is 100 to 28 800 and must be greater than the <code>dpd-idleworry</code> setting.	300 seconds	All models. dpd must be set to enable.
<code>dpd-idleworry</code> <seconds_integer>	The DPD short idle setting when <code>dpd</code> is set to enable. Set the time, in seconds, that a link must remain unused before the local VPN peer considers it to be idle. After this period of time expires, whenever the local peer sends traffic to the remote VPN peer it will also send a DPD probe to determine the status of the link. The <code>dpd-idleworry</code> range is 1 to 300. To control the length of time that the FortiGate unit takes to detect a dead peer with DPD probes, use the <code>dpdretrycount</code> and <code>dpd-retryinterval</code> keywords.	10 seconds	All models. dpd must be set to enable.
<code>dpd-retrycount</code> <retry_integer>	The DPD retry count when <code>dpd</code> is set to enable. Set the number of times that the local VPN peer sends a DPD probe before it considers the link to be dead and tears down the security association (SA). The <code>dpd-retrycount</code> range is 0 to 10. To avoid false negatives due to congestion or other transient failures, set the retry count to a sufficiently high value for your network.	3	All models. dpd must be set to enable.
<code>dpd-retryinterval</code> <seconds_integer>	The DPD retry interval when <code>dpd</code> is set to enable. Set the time, in seconds, that the local VPN peer waits between sending DPD probes. The <code>dpd-retryinterval</code> range is 1 to 60.	5 seconds	All models. dpd must be set to enable.

Example

Use the following command to edit an IPsec VPN phase 1 configuration with the following characteristics:

- Phase 1 configuration name: `Example_Gateway`
- Remote peer address type: `Dynamic`
- Encryption and authentication proposal: `des-md5`
- Authentication method: `psk`
- Pre-shared key: `Qf2p3093jIj2bz7E`
- Mode: `aggressive`
- Dead Peer Detection: `enable`
- Long idle: `1000`
- Short idle: `150`
- Retry count: `5`
- Retry interval: `30`

```
config vpn ipsec phase1
    edit Example_Gateway
        set Type dynamic
        set proposal des-md5
        set authmethod psk
        set psksecret Qf2p3093jIj2bz7E
        set mode aggressive
        set dpd enable
        set dpd-idlecleanup 1000
        set dpd-idleworry 150
        set dpd-retrycount 5
        set dpd-retryinterval 30
    end
```

Defining Phase 2 tunnel creation parameters

After phase 1 negotiations complete successfully, phase 2 begins. The phase 2 parameters define the algorithms that the FortiGate unit may use to encrypt and transfer data for the remainder of the session. During phase 2, the specific IPsec security associations needed to implement security services are selected and a tunnel is established.

The basic phase 2 settings associate IPsec phase 2 parameters with a phase 1 configuration and specify the remote end point of the VPN tunnel. When you define phase 2 tunnel creation parameters, you can choose any set of phase 1 parameters to set up a secure connection for the tunnel and authenticate the remote peer. The same remote peer can be associated with more than one phase 2 tunnel definition.

Figure 18: Basic Phase 2 settings (VPN > IPSEC > Phase 2 > Create New)

If the tunnel will join a spoke and a concentrator (see [“Hub-and-spoke configurations” on page 18](#)), the name of the concentrator can be specified as part of the basic phase 2 configuration.

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 49](#) instead.

Exchanging keys to implement security associations

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

The Keylife setting sets a limit on the length of time that a phase 2 key can be used. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when either the time has passed or the number of KB have been processed. When the phase 2 key expires, a new key is generated without interrupting service.

Autokey Keep Alive setting is used to rekey phase 2 SA negotiations when the key life expires so that the tunnel will not shut down. Enable the option to ensure that the tunnel remains active when no data is being processed. As an alternative, you can generate traffic artificially using the FortiGate ping generator (see [“Using the ping generator to keep a tunnel open” on page 75](#)).

Defining the remaining tunnel creation options

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

- Enable replay detection
- Enable perfect forward secrecy (PFS)
- Internet browsing
- DHCP-IPsec
- Quick Mode Identities

Figure 19: Advanced phase 2 settings

The screenshot shows the 'P2 Proposal' configuration window. It includes the following settings:

- 1-Encryption:** 3DES
- Authentication:** SHA1
- 2-Encryption:** 3DES
- Authentication:** MD5
- Enable replay detection
- Enable perfect forward secrecy(PFS).
- DH Group:** 1 (selected), 2, 5
- Keylife:** Seconds: 1800 (Seconds), 4608000 (KBytes)
- Autokey Keep Alive:** Enable
- DHCP-IPsec:** Enable
- Internet browsing:** None
- Quick Mode Identities:**
 - Use selectors from policy
 - Use wildcard selectors
 - Specify a selector

Replay detection

IPsec tunnels can be vulnerable to replay attacks. Replay detection enables the FortiGate unit to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the FortiGate unit discards them.

Perfect forward secrecy

By default, phase 2 keys are derived from the session key created in phase 1. Perfect forward secrecy forces a new Diffie-Hellman exchange when the tunnel starts and whenever the phase 2 keylife expires, causing a new key to be generated each time. This exchange ensures that the keys created in phase 2 are unrelated to the phase 1 keys or any other keys generated automatically in phase 2.

DHCP-IPsec

If a FortiGate dialup server will assign VIP addresses to FortiClient dialup clients through FortiGate DHCP relay, select DHCP-IPsec Enable. Do not select this option on FortiGate units that act as dialup clients. The DHCP relay parameters must be configured separately. For more information, see [“FortiClient dialup-client configurations” on page 25](#).

Internet browsing

If the tunnel will support an Internet-browsing configuration (see “[Internet-browsing configurations](#)” on page 37), you can select the browsing interface from the Internet browsing list. The browsing interface is the FortiGate interface to the local private network. Do not select this option on FortiGate units that act as dialup clients.

Quick mode identities

The Quick Mode Identities setting determines the method that will be used to choose selectors for IKE negotiations. You can:

- Choose a selector from a firewall encryption policy. In this case, the VPN tunnel specified in the firewall encryption policy is referenced.
- Disable selector negotiation for a tunnel to avoid negotiation errors. For example, invalid ID information may result when the set of policies between the peers is not symmetric.
- Specify the firewall encryption policy source and destination IP addresses, ports, and IP protocol to use for selector negotiations. When this option is set, VPN clients cannot propose selectors.

Configuring the phase 2 tunnel creation parameters

Follow this procedure to create an IPsec phase 2 tunnel definition.



Note: If you are creating a hub-and-spoke configuration or an Internet-browsing configuration, you may have already started defining some of the required phase 2 parameters. If so, edit the existing definition to complete the configuration.

To specify phase 2 parameters for creating a tunnel

- 1 Go to **VPN > IPSEC > Phase 2**.
- 2 Select Create New to add a new phase 2 configuration or select the Edit button beside an existing configuration.
- 3 Include appropriate entries as follows:

Tunnel Name	Enter a name to identify the tunnel configuration.
Remote Gateway	Select the phase 1 configuration that describes how remote peers or dialup clients will be authenticated on this tunnel, and how the connection to the remote peer or dialup client will be secured.
- 4 Select Advanced.

5 Include appropriate entries as follows:

P2 Proposal

Select the encryption and authentication algorithms that will be used to change data into encrypted code.

Add or delete encryption and authentication algorithms as required. Select a minimum of one and a maximum of three combinations. The remote peer must be configured to use at least one of the proposals that you define.

You can select any of the following symmetric-key algorithms:

- NULL-Do not use an encryption algorithm.
- DES-Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- 3DES-Triple-DES, in which plain text is encrypted three times by three keys.
- AES128-A 128-bit block algorithm that uses a 128-bit key.
- AES192-A 128-bit block algorithm that uses a 192-bit key.
- AES256-A 128-bit block algorithm that uses a 256-bit key.

You can select either of the following message digests to check the authenticity of messages during an encrypted session:

- NULL-Do not use a message digest.
- MD5-Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA1-Secure Hash Algorithm 1, which produces a 160-bit message digest.

To specify one combination only, set the Encryption and Authentication options of the second combination to NULL. To specify a third combination, use the add button beside the fields for the second combination.

Enable replay detection

Enable or disable replay detection.

Enable perfect forward secrecy (PFS)

Enable or disable PFS.

DH Group

Select one Diffie-Hellman group (1, 2, or 5). The remote peer or dialup client must be configured to use the same group.

Keylife

Select Seconds, KBytes, or Both for the units of measurement. The keylife range can be from 120 to 172800 seconds or from 5120 to 99999 KBytes.

Autokey Keep Alive

Enable this option if you want to keep the VPN connection open when no data is being processed.

DHCP-IPsec

Select Enable if the FortiGate unit acts as a dialup server and FortiGate DHCP relay will be used to assign VIP addresses to FortiClient dialup clients. Do not select this option on FortiGate units that act as dialup clients. The DHCP relay parameters must be configured separately. For more information, see ["FortiClient dialup-client configurations"](#) on page 25.

Internet browsing

Select the FortiGate interface to the local private network if the FortiGate unit has to support an Internet-browsing configuration (see “Internet-browsing configurations” on page 37). Do not select this option on FortiGate units that act as dialup clients.

Quick Mode Identities

Enter the method for choosing selectors for IKE negotiations:

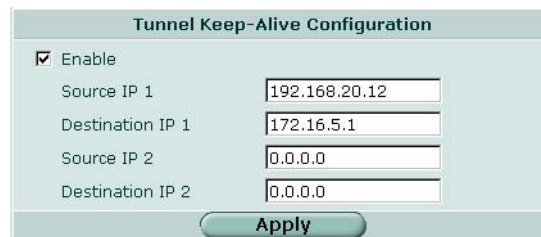
- To choose a selector from a firewall encryption policy, select Use selectors from policy.
- To disable selector negotiation, select Use wildcard selectors.
- To specify the firewall encryption policy source and destination IP addresses, select Specify a selector and then select the names of the source and destination addresses from the Source address and Dest address lists. You may optionally specify source and destination port numbers and/or a protocol number.

6 Select OK.

Using the ping generator to keep a tunnel open

The ping generator generates traffic in an IPsec VPN tunnel to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, the ping generator is useful 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. You may also use the ping generator to troubleshoot network connectivity inside a VPN tunnel.

Figure 20: Ping generator settings for one tunnel



You can configure settings to generate traffic through two tunnels simultaneously. The ping interval is fixed at 40 seconds.

The source and destination IP addresses refer to the source and destination addresses of IP packets that are to be transported through the VPN tunnel. When source and destination addresses of 0 . 0 . 0 . 0 are entered, no ping traffic is generated between the source and destination.

To configure the ping generator

- 1** Go to **VPN > IPSEC > Ping Generator**.
- 2** Select **Enable**.
- 3** In the **Source IP 1** field, type the private IP address or subnet address from which traffic may originate locally (for example, 192.168.20.12 or 192.168.20.0 respectively).
- 4** In the **Destination IP 1** field, enter the IP address of a remote computer:
 - For a peer-to-peer configuration, the destination address is the private IP address of a server or host behind the remote VPN peer (for example, 172.16.5.1).
 - For a dialup-client or Internet-browsing configuration where the remote VPN client is configured to acquire a virtual IP address, the destination address must correspond to the virtual IP address that can be acquired.
- 5** If you want to enable a second ping generator, repeat Steps 3 and 4 for the **Source IP 2** and **Destination IP 2** settings.
- 6** Select **Apply**.

Defining IP source and destination 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.

A source address defines the originating IP address of a packet and the destination address defines the IP address of the intended remote recipient or network. The source and destination addresses typically correspond to networks behind the VPN end points.

In a simple case (for example, in a gateway-to-gateway configuration), the source IP address would correspond to the private network behind the local FortiGate unit and the destination IP address would correspond to the private network behind the remote FortiGate unit. In another case, the source IP address could be the private IP address of an email server behind the local FortiGate gateway, and the destination address could be the VIP address that a FortiClient dialup client may acquire.

In general:

- In a gateway-to-gateway, hub-and-spoke, dynamic DNS, redundant-tunnel, or transparent configuration, the destination address refers to the private IP address of the network behind the remote VPN peer (for example, 192.168.10.0/255.255.255.0).
- In a peer-to-peer configuration, the destination address is the private IP address of a server or host behind the remote VPN peer (for example, 172.16.5.1/255.255.255.255).
- For a FortiGate dialup server in a dialup-client or Internet-browsing configuration:
 - If you are not using VIP addresses, or if the FortiGate dialup server assigns VIP addresses to FortiClient dialup clients through FortiGate DHCP relay, select the predefined destination address “all” in the firewall encryption policy to refer to the dialup clients.
 - If you assign VIP addresses to FortiClient dialup clients manually, the destination address may be the VIP address assigned to the dialup client, or a subnet address comprising VIP addresses (for example, 10.254.254.1/32 for a single dialup client, or 10.254.254.0/24 for a subnet address from which the VIP addresses are assigned).
- For a FortiGate dialup client in a dialup-client or Internet-browsing configuration, the destination address refers to the private IP address of a host, server, or network behind the FortiGate dialup server.

To define an IP source address

- 1 Go to **Firewall > Address** and select Create New.
- 2 In the Address Name field, type a name that represents the local network, server(s), or host(s) from which IP packets may originate on the private network behind the local FortiGate unit.
- 3 In the IP Range/Subnet field, type the corresponding IP address and subnet mask (for example, 172.16.5.0/24 for a subnet, or 172.16.5.1/32 for a server or host) or IP address range (for example, 192.168.10.[80-100]).
- 4 Select OK.

To define an IP destination address

- 1 Go to **Firewall > Address** and select Create New.
- 2 In the Address Name field, type a name that represents the remote network, server(s), or host(s) to which IP packets may be delivered.
- 3 In the IP Range/Subnet field, type the corresponding IP address and subnet mask (for example, 192.168.20.0/24 for a subnet, or 192.168.20.2/32 for a server or host), or IP address range (for example, 192.168.20.[10-25]).
- 4 Select OK.

Defining a firewall encryption policy

Firewall policies control all IP traffic passing between a source address and a destination address. A firewall encryption policy is needed to allow the transmission of encrypted packets, specify the permitted direction of VPN traffic, and select the VPN tunnel that will be subject to the policy. In most cases, a single encryption policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

In addition to these operations, firewall encryption policies specify which IP addresses can initiate a tunnel. Traffic from computers on the local private network initiates the tunnel when the Allow outbound option is selected. Traffic from a dialup client or computers on the remote network initiates the tunnel when the Allow inbound option is selected.

When a FortiGate unit runs in NAT/Route mode, you can also enable inbound or outbound NAT. Outbound NAT may be performed on outbound encrypted packets, or on IP packets before they are sent through the tunnel. Inbound NAT is performed on IP packets emerging from the tunnel. These options are not selected by default in firewall encryption policies.

When used in conjunction with the `nat ip` CLI attribute (see the “config firewall” chapter of the [FortiGate CLI Reference Guide](#)), outbound NAT enables you to change the source addresses of IP packets before they go into the tunnel. This feature is often used to resolve ambiguous routing when two or more of the private networks making up a VPN have the same or overlapping IP addresses. For examples of how to use these two features together, see the [FortiGate Outbound NAT for IPsec VIP Technical Note](#), the [FortiGate IPsec VPN Subnet-address Translation Technical Note](#) and the [Circumventing Ambiguous Routing in a Hub-and-spoke IPsec VPN Technical Note](#).

When inbound NAT is enabled, inbound encrypted packets are intercepted and decrypted, and the source IP addresses of the decrypted packets are translated into the IP address of the FortiGate interface to the local private network before they are routed to the private network. If the computers on the local private network can communicate only with devices on the local private network (that is, the FortiGate interface to the private network is not the default gateway) and the remote client (or remote private network) does not have an IP address in the same network address space as the local private network, enable inbound NAT.

Most firewall encryption policies control outbound IP traffic. An outbound policy usually has a source address originating on the private network behind the local FortiGate unit, and a destination address belonging to a dialup VPN client or a network behind the remote VPN peer. The source address that you choose for the firewall encryption policy identifies from where outbound cleartext IP packets may originate, and also defines the local IP address or addresses that a remote server or client will be allowed to access through the VPN tunnel. The destination address that you choose for the firewall encryption policy identifies where IP packets must be forwarded after they are decrypted at the far end of the tunnel, and determines the IP address or addresses that the local network will be able to access at the far end of the tunnel.

You can fine-tune an encryption policy for services such as HTTP, FTP, and POP3; enable logging, traffic shaping, differentiated services, antivirus protection, web filtering, email filtering, file transfer, and email services throughout the VPN; and optionally allow connections according to a predefined schedule. For more information, see the “Firewall” chapter of the *FortiGate Administration Guide*.

When a remote server or client attempts to connect to the private network behind a FortiGate gateway, the firewall encryption policy intercepts the connection attempt and starts the VPN tunnel. The FortiGate unit uses the remote gateway specified in its phase 2 tunnel configuration to reply to the remote peer. When the remote peer receives a reply, it checks its own encryption 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.

Defining multiple encryption policies for the same tunnel

You must define at least one encryption 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 encryption policy for each network. Multiple encryption 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 ENCRYPT policies before ACCEPT and DENY firewall policies. Because the FortiGate unit reads policies starting at the top of the list, you must move all encryption policies to the top of the list. When you define multiple encryption policies for the same tunnel, you must reorder the encryption policies that apply to the tunnel so that specific constraints can be evaluated before general constraints.



Note: Adding multiple encryption 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 encryption policy or the tunnel may fail.

For example, if you create two equivalent encryption policies for two different tunnels, it does not matter which one comes first in the list of encryption policies—the system will select the correct policy based on the specified source and destination addresses. If you create two different encryption 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 encryption policies to ensure that the system selects the correct encryption 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 encryption policy having the most specific constraints at the top of the list so that it can be evaluated first.

Before you begin

Before you define the encryption policy, you must:

- Define the IP source and destination addresses. See [“Defining IP source and destination addresses” on page 76](#).
- Specify the phase 1 authentication parameters. See [“Defining Phase 1 IKE and authentication parameters” on page 51](#).
- Specify the phase 2 tunnel creation parameters. See [“Defining Phase 2 tunnel creation parameters” on page 71](#).

To define a firewall encryption policy

- 1 Go to **Firewall > Policy** and select Create New.
- 2 Include appropriate entries as follows:

Source	Interface/Zone Select the local interface to the internal (private) network. Address Name Select the name that corresponds to the local network, server(s), or host(s) from which IP packets may originate.
Destination	Interface/Zone Select the local interface to the external (public) network. Address Name Select the name that corresponds to the remote network, server(s), or host(s) to which IP packets may be delivered.
Schedule	Keep the default setting (always) unless changes are needed to meet specific requirements.
Service	Keep the default setting (ANY) unless changes are needed to meet your specific requirements.
Action	Select ENCRYPT.
VPN Tunnel	Select the name of the phase 2 tunnel configuration to which this policy will apply. Select Allow inbound if traffic from the remote network will be allowed to initiate the tunnel. Select Allow outbound if traffic from the local network will be allowed to initiate the tunnel. If you want to translate the source IP addresses of inbound decrypted packets into the IP address of the FortiGate interface to the local private network, select Inbound NAT. If you want to translate the source IP addresses of outbound cleartext packets into the IP address that you specify, select Outbound NAT. Outbound NAT should not be selected unless you specify a <code>natip</code> value through the CLI. Outbound NAT, when used in combination with the <code>natip</code> value, translates the source addresses of IP packets sent through the tunnel into the substitution address that you provide through the <code>natip</code> value. To specify a <code>natip</code> value, see the “config firewall” chapter of the FortiGate CLI Reference Guide .

- 3 You may enable a protection profile, and/or event logging, or select advanced settings to shape traffic or differentiate services. See the “Firewall” chapter of the [FortiGate Administration Guide](#).
- 4 Select OK.
- 5 Place the policy in the policy list above any other policies having similar source and destination addresses.

Related technical notes

For detailed step-by-step procedures on the following topics, refer to one of these technical notes. These technical notes are available from the [Fortinet Knowledge Center](#).

Table 2: IPsec VPN configuration examples

Gateway-to-gateway IPsec VPN Example	Demonstrates how to set up a basic gateway-to-gateway IPsec VPN that uses preshared keys to authenticate the two VPN peers.
Hub-and-spoke IPsec VPN Example	Demonstrates how to set up a basic hub-and-spoke IPsec VPN that uses preshared keys to authenticate VPN peers.
FortiClient in Hub-and-spoke IPsec VPN Example	Demonstrates how to include FortiClient dialup clients in a basic hub-and-spoke IPsec VPN. The VPN peers and clients use preshared keys for authentication purposes.
Circumventing Ambiguous Routing in a Hub-and-spoke IPsec VPN	Provides guidelines for circumventing ambiguous routing in a hub-and-spoke IPsec VPN. Ambiguous routing may become problematic when two or more of the private networks behind FortiGate spokes unintentionally use the same IP address space or have overlapping IP addresses.
FortiClient Dialup-client IPsec VPN Example	Demonstrates how to set up a FortiClient dialup-client IPsec VPN that uses preshared keys for authentication purposes. In the example configuration, the FortiClient Host Security application acquires a VIP address through FortiGate DHCP relay.
FortiClient Internet-browsing IPsec VPN Example	Demonstrates how to set up a FortiClient Internet-browsing IPsec VPN that uses preshared keys for authentication purposes. In the example configuration, the FortiClient Host Security application acquires a VIP address through FortiGate DHCP relay.
Authenticating FortiClient Dialup Clients	Explains how to configure VPN settings and FortiClient dialup clients using preshared keys, local IDs, and user groups as authentication components. Multiple dialup clients having different authentication settings can connect to the same FortiGate IPsec VPN tunnel.
Redundant-tunnel IPsec VPN Example	Demonstrates how to set up a redundant-tunnel IPsec VPN that uses preshared keys for authentication purposes. In the example configuration, two separate interfaces to the Internet are available on both VPN peers.
Partially Redundant IPsec VPN Tunnel Example	Demonstrates how to set up a partially redundant IPsec VPN tunnel 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. In the example configuration, both VPN peers use preshared keys for authentication purposes, and the remote VPN peer identifies itself using a peer ID.
Outbound Nat for IPsec VIP	Explains how to use the outbound NAT and IPsec virtual IP (VIP) features to circumvent ambiguous routing caused by combining two networks that use the same private address space.
FortiGate IPsec VPN Subnet-address Translation	Provides a detailed configuration example that enables bidirectional subnet-address translation inside an IPsec VPN tunnel. The CLI <code>nat ip</code> attribute, when used with the outbound NAT feature, enables one-to-one subnet-address translation inside the tunnel.

Configuring PPTP VPNs

This chapter describes how to configure a FortiGate unit to act as a PPTP server. It also describes how to configure the FortiGate unit to forward PPTP packets to an external PPTP server. The chapter contains the following sections:

- [Overview](#)
- [Network topology](#)
- [PPTP server configuration overview](#)
- [PPTP pass through configuration overview](#)
- [Authenticating PPTP clients](#)
- [Enabling PPTP and specifying an address range](#)
- [Configuring a FortiGate PPTP server](#)
- [Configuring PPTP pass through](#)
- [Configuring a Windows client](#)
- [Configuring a Linux client](#)

Overview

FortiGate units support PPTP to tunnel PPP traffic between two VPN peers. Windows or Linux PPTP clients can establish a PPTP tunnel with a FortiGate unit that has been configured to act as a PPTP server. As an alternative, you can configure the FortiGate unit to forward PPTP packets to a PPTP server on the network behind the FortiGate unit.

When the FortiGate unit acts as a PPTP server, a PPTP session and tunnel is created as soon as the PPTP client connects to the FortiGate unit. More than one PPTP session can be supported on the same tunnel. FortiGate units support PAP, CHAP, and plain text authentication. PPTP clients are authenticated as members of a user group.

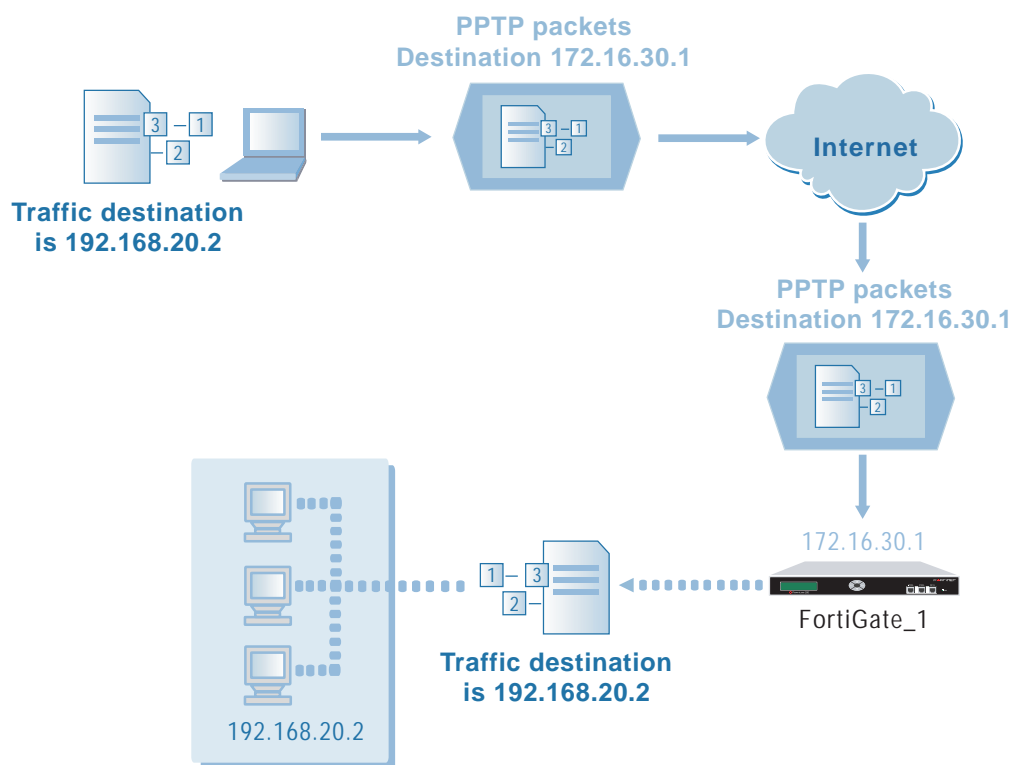
Traffic from one PPTP peer is encrypted using PPP before it is encapsulated using Generic Routing Encapsulation (GRE) and routed to the other PPTP peer through an ISP network. PPP packets from the remote client are addressed to a computer on the private network behind the FortiGate unit. PPTP packets from the remote client are addressed to the public interface of the FortiGate unit. See [Figure 21 on page 84](#).



Caution: PPTP control channel messages are not authenticated, and their integrity is not protected. Furthermore, encapsulated PPP packets are not cryptographically protected and may be read or modified unless appropriate encryption software such as Secure Shell (SSH) or Secure File Transfer Protocol (SFTP) is used to transfer data after the tunnel has been established.

As an alternative, you can use encryption software such as Microsoft Point-to-Point Encryption (MPPE) to secure the channel. MPPE is built into Windows clients and can be installed on Linux clients. FortiGate units support MPPE.

Figure 21: Packet encapsulation



In Figure 21, traffic from the remote client is addressed to a computer on the network behind the FortiGate unit. When the PPTP tunnel is established, packets from the remote client are encapsulated and addressed to the FortiGate unit. The FortiGate unit forwards disassembled packets to the computer on the internal network.

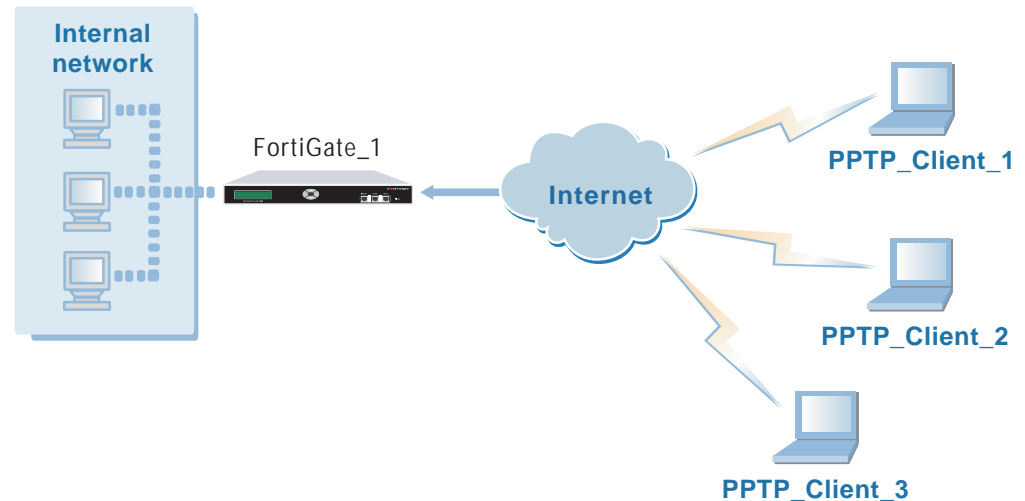
When the remote PPTP client connects, the FortiGate unit assigns an IP address from a reserved range of IP addresses to the client PPTP interface. The PPTP client uses the assigned IP address as its source address for the duration of the connection.

When the FortiGate unit receives a PPTP packet, the unit disassembles the PPTP packet and forwards the packet to the correct computer on the internal network. The firewall policy and protection profiles on the FortiGate unit ensure that inbound traffic is screened and processed securely.

Network topology

In the most common Internet scenario, the PPTP client connects to an ISP that offers PPP connections with dynamically assigned IP addresses. The ISP forwards PPTP packets to the Internet, where they are routed to the FortiGate unit.

Figure 22: Example PPTP configuration



PPTP infrastructure requirements

- The FortiGate unit may operate in NAT/Route mode or Transparent mode and have a static or dynamic public IP address.
- The dialup client ISP account supports PPP connections with dynamically assigned IP addresses and if the ISP runs a PPTP server, the server must be configured to forward PPTP packets to the FortiGate unit.
- The PPTP client includes PPP support (with MPPE if encryption is required).

PPTP server configuration overview

If the FortiGate unit will act as a PPTP server, perform the following tasks in the order given:

- Create a PPTP user group containing one user for each PPTP client. See [“Authenticating PPTP clients” on page 86](#).
- Enable PPTP on the FortiGate unit and specify the range of addresses that can be assigned to PPTP clients when they connect. See [“Enabling PPTP and specifying an address range” on page 86](#).
- Configure the PPTP server. See [“Configuring a FortiGate PPTP server” on page 87](#).
- Configure the PPTP clients. For general guidelines, refer to these sections:
 - [“Configuring a Windows client” on page 90](#).
 - [“Configuring a Linux client” on page 91](#).

PPTP pass through configuration overview

To arrange for PPTP packets to pass through the FortiGate unit to an external PPTP server, perform the following tasks in the order given:

- Create a PPTP user group containing one user for each PPTP client. See [“Authenticating PPTP clients” on page 86](#).
- Enable PPTP on the FortiGate unit and specify the range of addresses that can be assigned to PPTP clients when they connect. See [“Enabling PPTP and specifying an address range” on page 86](#).
- Configure PPTP pass through on the FortiGate unit. See [“Configuring PPTP pass through” on page 88](#).
- Configure the PPTP clients. For general guidelines, refer to these sections:
 - [“Configuring a Windows client” on page 90](#).
 - [“Configuring a Linux client” on page 91](#).

Authenticating PPTP clients

PPTP clients must be authenticated before a tunnel is established. The authentication process relies on FortiGate user group definitions, which can optionally use established authentication mechanisms such as RADIUS or LDAP to authenticate PPTP clients. All PPTP clients are challenged when a connection attempt is made.

To enable authentication, you must create user accounts and a user group to identify the PPTP clients that need access to the network behind the FortiGate unit. Within the user group, add a user for each PPTP client. For more information, see the “Users and Authentication” chapter of the [FortiGate Administration Guide](#).

You can choose to use a plain text password for authentication or forward authentication requests to an external RADIUS or LDAP server. If password protection will be provided through a RADIUS or LDAP server, you must configure the FortiGate unit to forward authentication requests to the authentication server. For more information, see the “Users and Authentication” chapter of the [FortiGate Administration Guide](#).

Enabling PPTP and specifying an address range

The PPTP address range specifies the range of addresses reserved for remote PPTP clients. When a PPTP client connects to the FortiGate unit, the client is assigned an IP address from this range. Afterward, the FortiGate unit uses the assigned address to communicate with the PPTP client.

The address range that you reserve can be associated with private or routable IP addresses. If you specify a private address range that matches a network behind the FortiGate unit, the assigned address will make the PPTP client appear to be part of the internal network.

To enable PPTP and specify the PPTP address range

- 1 Go to **VPN > PPTP > PPTP Range**.
- 2 Select **Enable PPTP**.

- 3 In the Starting IP field, type the starting address in the range of reserved IP addresses.
- 4 In the Ending IP field, type the ending address in the range of reserved IP addresses.
- 5 From the User Group list, select the name of the PPTP user group that you defined previously. See [“Authenticating PPTP clients” on page 86](#).
- 6 Select **Apply**.

Configuring a FortiGate PPTP server

To configure a FortiGate unit to act as a PPTP server, you perform the following configuration tasks on the FortiGate unit:

- Define firewall source and destination addresses to indicate where packets transported through the PPTP tunnel will originate and be delivered. See [“Defining firewall source and destination addresses”](#) below.
- Create the firewall policy and define the scope of permitted services between the source and destination addresses. [“Add the firewall policy” on page 88](#).

Defining firewall source and destination addresses

Before you define the firewall policy, you must define the source and destination addresses of packets that are to be transported through the PPTP tunnel:

- For the source address, enter the range of addresses that you reserved for PPTP clients (for example `192.168.10.[80-100]`).
- For the destination address, enter the IP addresses of the computers that the PPTP clients need to access on the private network behind the FortiGate unit (for example, `172.16.5.0/24` for a subnet, or `172.16.5.1/32` for a server or host, or `192.168.10.[10-15]` for an IP address range).

To define the firewall source address

- 1 Go to **Firewall > Address** and select **Create New**.
- 2 In the Address Name field, type a name that represents the range of addresses that you reserved for PPTP clients (for example, `Ext_PPTPrange`).
- 3 In the IP Range/Subnet field, type the corresponding IP address range.
- 4 Select **OK**.

To define the firewall destination address

- 1 Go to **Firewall > Address** and select Create New.
- 2 In the Address Name field, type a name that represents a range of IP addresses on the private network behind the FortiGate unit (for example, `Int_PPTPaccess`).
- 3 In the IP Range/Subnet field, type the corresponding IP address range.
- 4 Select OK.

Add the firewall policy

The firewall policy specifies the source and destination addresses that can generate traffic inside the PPTP tunnel and defines the scope of services permitted through the tunnel. If a selection of services are required, define a service group. For more information, see the “Firewall” chapter of the [FortiGate Administration Guide](#).

To define the traffic and services permitted inside the PPTP tunnel

- 1 Go to **Firewall > Policy** and select Create New.
- 2 Enter these settings in particular:

Interface/Zone	Source Select the FortiGate interface to the Internet. Destination Select the FortiGate interface to the internal (private) network.
Address Name	Source Select the name that corresponds to the range of addresses that you reserved for PPTP clients (for example, <code>Ext_PPTPrange</code>). Destination Select the name that corresponds to the IP addresses behind the FortiGate unit (for example, <code>Int_PPTPaccess</code>).
Service	Select ANY, or if selected services are required instead, select the service group that you defined previously.
Action	Select ACCEPT.

- 3 You may enable NAT, a protection profile, and/or event logging, or select advanced settings to shape traffic or differentiate services. See the “Firewall” chapter of the [FortiGate Administration Guide](#).
- 4 Select OK.

Configuring PPTP pass through

To forward PPTP packets to a PPTP server on the network behind the FortiGate unit, you perform the following configuration tasks on the FortiGate unit:

- Define a virtual port-forwarding IP address that uses TCP port 1723 (the PPTP port). See [“To define a virtual port-forwarding address for PPTP pass through” on page 89](#). The FortiGate unit will forward PPTP packets to the address you specify.
- Create a firewall policy that allows incoming PPTP packets to pass through to the PPTP server. See [“To create a port-forwarding firewall policy for PPTP pass through” on page 89](#).

To define a virtual port-forwarding address for PPTP pass through

- 1 Go to **Firewall > Virtual IP** and select Create New.
- 2 In the Name field, type a name for the virtual IP address (for example, `PPTP_pass`).
- 3 From the External Interface list, choose the FortiGate interface on which packets destined for the PPTP server arrive. For example, in [Figure 23](#), the value is `external`. Your FortiGate unit may have a different set of interface names.
- 4 Select Port Forwarding.

Figure 23: Defining a port-forwarding address

The screenshot shows the 'Add New Virtual IP Mapping' configuration window. The fields are as follows:

- Name: PPTP_pass
- External Interface: external
- Type: Port Forwarding (selected)
- External IP Address: (empty)
- External Service Port: (empty)
- Map to IP: (empty)
- Map to Port: (empty)
- Protocol: TCP (selected)

- 5 In the External IP Address field, type the IP address of the FortiGate interface to the Internet.
- 6 In the External Service Port field, type 1723.
- 7 In the Map to IP field, type the IP address of the PPTP server.
- 8 In the Map to Port field, type 1723.
- 9 Select TCP, and then select OK.

To create a port-forwarding firewall policy for PPTP pass through

- 1 Go to **Firewall > Address** and select Create New.
- 2 In the Address Name field, type a name that represents the range of addresses that you reserved for PPTP clients (for example, `Ext_PPTPrange`).
- 3 In the IP Range/Subnet field, type the corresponding IP address range (for example `192.168.10.[80-100]`).
- 4 Select OK.
- 5 Go to **Firewall > Policy** and select Create New.

- 6 Enter these settings in particular:

Interface/Zone	Source Select the FortiGate interface to the Internet. Destination Select the FortiGate interface to the PPTP server.
Address Name	Source Select the name that corresponds to the range of addresses that you reserved for PPTP clients (for example, <code>Ext_PPTPrange</code>). Destination Select the name that corresponds to the port-forwarding IP address that you defined for PPTP services (for example, <code>PPTP_pass</code>).
Service	Select PPTP.
Action	Select ACCEPT.
- 7 You may enable NAT, a protection profile, and/or event logging, or select advanced settings to shape traffic or differentiate services. See the “Firewall” chapter of the [FortiGate Administration Guide](#).
- 8 Select OK.

Configuring a Windows client

The following procedures outline how to configure a Windows 2000 client and a Windows XP client to access resources behind a FortiGate unit that has been set up to accept PPTP connections. For details, refer to the software supplier’s documentation.

To configure the client, you need to know the public IP address of the FortiGate unit. Contact the FortiGate administrator if required to obtain the IP address.

To set up an PPTP dialup connection on a Windows 2000 client

- 1 Go to **Start > Settings > Network and Dial-up Connections > Make New Connection**, and then select Next.
- 2 Select Connect to a private network through the Internet, and then select Next.
- 3 Select Do not dial the initial connection, and then select Next.
- 4 In the Host name or IP address field, type the public IP address of the FortiGate unit and then select Next.
- 5 Select Only for myself, and then select Next.
- 6 Type a name for the connection.
- 7 Select Add a shortcut to this connection to your desktop, and select Finish.
- 8 When you are prompted to connect to the FortiGate unit, select Cancel.

To set up a PPTP dialup connection on a Windows XP client

- 1 Go to **Start > Settings > Network Connections > New Connection Wizard**, and then select Next.
- 2 Select Connect to the network at my workplace, and then select Next.
- 3 Select Virtual Private Network Connection, and then select Next.
- 4 In the Company Name field, type a name for the connection, and then select Next.
- 5 In the Host name or IP address field, type the public IP address of the FortiGate unit and then select Next.
- 6 Select Add a shortcut to this connection to your desktop, and select Finish.
- 7 When you are prompted to connect to the FortiGate unit, select Cancel.

To connect to the FortiGate PPTP server

Before you can connect to the FortiGate PPTP server, you need to know the user name and password that has been set up on the FortiGate unit to authenticate PPTP clients. Contact the FortiGate PPTP server administrator if required to obtain the user name and password.

- 1 Connect to the Internet.
- 2 On your desktop, double-click the PPTP connection shortcut.
- 3 In the User name field, type the PPTP user name.
- 4 In the Password field, type the PPTP password.
- 5 Select Connect.

After the connection is established, the PPTP client computer is visible on the network behind the FortiGate unit and can be accessed using the IP address of the client PPP interface. Only the servers and hosts that the PPTP client has access to will be visible to the PPTP client.

To disconnect, right-click the icon in the taskbar and then select Disconnect.

Configuring a Linux client

The following procedure outlines how to install PPTP Client software and run a PPTP tunnel on a Linux computer. Obtain a copy of PPTP Client that meets your requirements (for example, `pptp-linux`). If needed to encrypt traffic, obtain a copy that supports encryption using MPPE.

To establish a PPTP tunnel with a FortiGate unit that has been set up to accept PPTP connections, you can obtain and install the client software following these general guidelines:

- 1 If encryption is required but MPPE support is not already present in the kernel, download and install an MPPE kernel module and reboot your computer.
- 2 If required, download and install a PPP package that contains compatible MPPE support.
- 3 Download and install the PPTP Client package.

- 4 Configure a PPP connection to run the PPTP program.
- 5 Configure routes to determine whether all or some of your network traffic will be sent through the tunnel. You must define a route to the remote network over the PPTP link and a host route to the FortiGate unit.
- 6 Run `pppd` to start the tunnel.

Follow the software supplier's documentation to complete the steps.

To configure the system, you need to know the public IP address of the FortiGate unit, and the user name and password that has been set up on the FortiGate unit to authenticate PPTP clients. Contact the FortiGate PPTP server administrator if required to obtain this information.

Configuring L2TP VPNs

This chapter describes how to configure a FortiGate unit to establish an L2TP tunnel with a remote dialup client and includes the following topics:

- [Overview](#)
- [Network topology](#)
- [L2TP configuration overview](#)
- [Authenticating L2TP clients](#)
- [Enabling L2TP and specifying an address range](#)
- [Defining firewall source and destination addresses](#)
- [Adding the firewall policy](#)
- [Configuring a Linux client](#)

Overview

According to RFC 2661, an Access Concentrator (LAC) can establish an L2TP tunnel with an L2TP Network Server (LNS). In a typical scenario, the LAC is managed by an ISP and located on the ISP premises; the LNS is the gateway to a private network. When a remote dialup client connects to the Internet through the ISP, the ISP uses a local database to establish the identity of the caller and determine whether the caller needs access to an LNS through an L2TP tunnel. If the services registered to the caller indicate that an L2TP connection to the LNS is required, the ISP LAC attempts to establish an L2TP tunnel with the LNS.

A FortiGate unit can be configured to act as an LNS. The FortiGate implementation of L2TP enables a remote dialup client to establish an L2TP tunnel with the FortiGate unit directly, bypassing any LAC managed by an ISP. The ISP must configure its network access server to forward L2TP traffic from the remote client to the FortiGate unit directly whenever the remote client requires an L2TP connection to the FortiGate unit.

When the FortiGate unit acts as an LNS, an L2TP session and tunnel is created as soon as the remote client connects to the FortiGate unit. The FortiGate unit assigns an IP address to the client from a reserved range of IP addresses. The remote client uses the assigned IP address as its source address for the duration of the connection.

More than one L2TP session can be supported on the same tunnel. FortiGate units can be configured to authenticate remote clients using a plain text user name and password, or authentication can be forwarded to an external RADIUS or LDAP server. L2TP clients are authenticated as members of a user group.

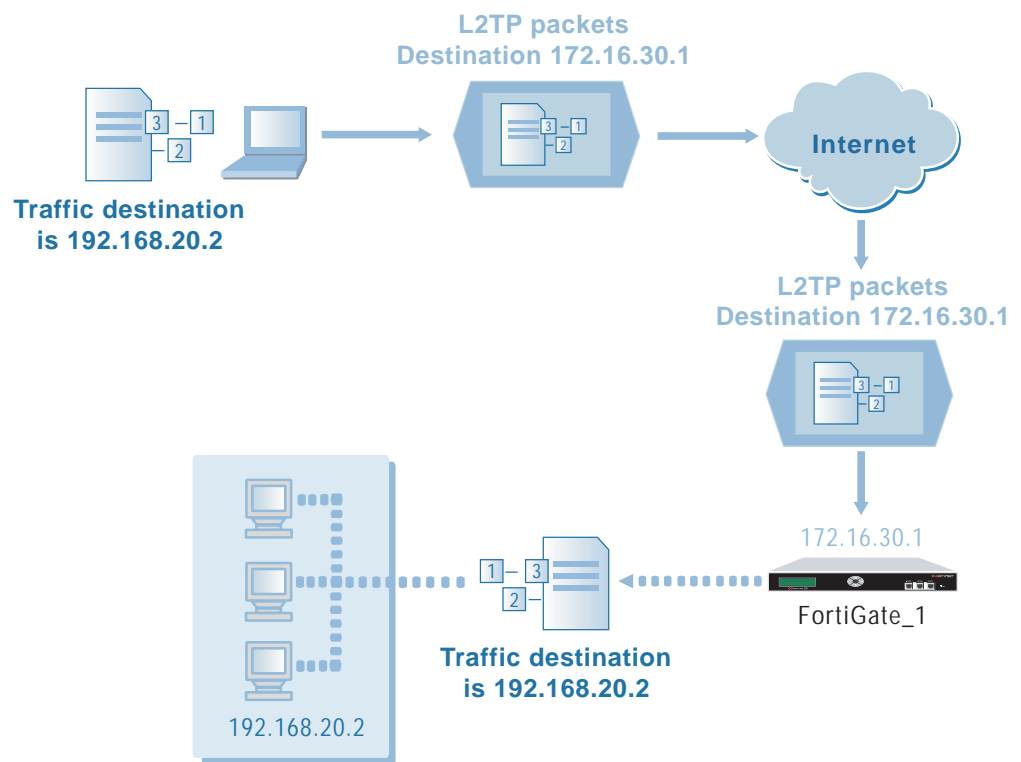


Caution: FortiGate units support L2TP with Microsoft Point-to-Point Encryption (MPPE) encryption only. Later implementations of Microsoft L2TP for Windows use IPsec and require certificates for authentication and encryption. If you want to use Microsoft L2TP with IPsec to connect to a FortiGate unit, the IPsec and certificate elements must be disabled on the remote client. For more information, see the [Disabling Microsoft L2TP for IPsec](#) article in the Fortinet Knowledge Center.

Traffic from the remote client must be encrypted using MPPE before it is encapsulated and routed to the FortiGate unit. Packets originating at the remote client are addressed to a computer on the private network behind the FortiGate unit. Encapsulated packets are addressed to the public interface of the FortiGate unit. See [Figure 24 on page 94](#).

When the FortiGate unit receives an L2TP packet, the unit disassembles the packet and forwards the packet to the correct computer on the internal network. The firewall policy and protection profiles on the FortiGate unit ensure that inbound traffic is screened and processed securely.

Figure 24: L2TP encapsulation



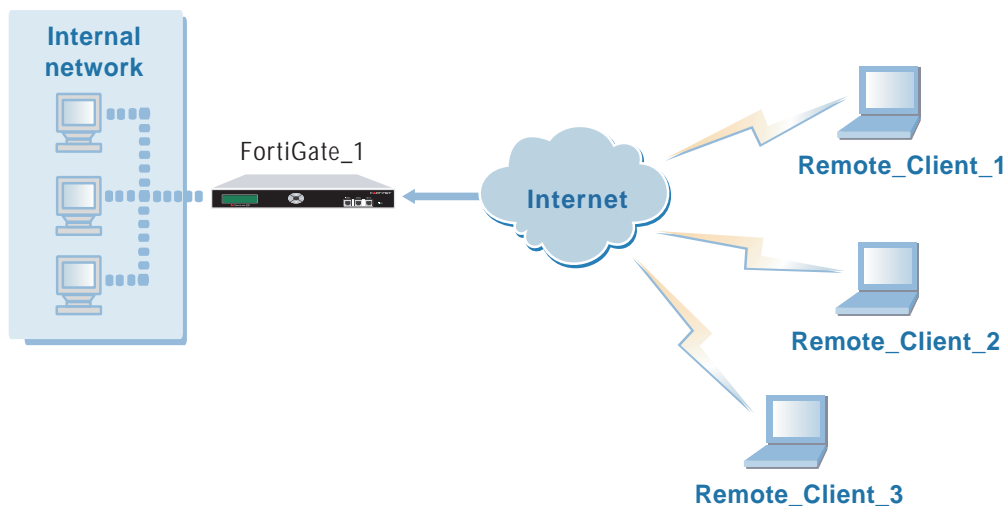


Note: Fortinet units cannot deliver non-IP traffic such as Frame Relay or ATM frames encapsulated in L2TP packets — FortiGate units support the IPv4 and IPv6 addressing schemes only.

Network topology

The remote client connects to an ISP that determines whether the client requires an L2TP connection to the FortiGate unit. If an L2TP connection is required, the connection request is forwarded to the FortiGate unit directly.

Figure 25: Example L2TP configuration



L2TP infrastructure requirements

- The FortiGate unit must be operating in NAT/Route mode and have a static public IP address.
- The ISP must configure its network access server to forward L2TP traffic from remote clients to the FortiGate unit directly.
- The remote client must not generate non-IP traffic (Frame Relay or ATM frames).
- The remote client includes L2TP support with MPPE encryption. If the remote client includes Microsoft L2TP with IPsec, the IPsec and certificate components must be disabled.

L2TP configuration overview

To configure a FortiGate unit to act as an LNS, you perform the following tasks on the FortiGate unit:

- Create an L2TP user group containing one user for each remote client. See [“Authenticating L2TP clients” on page 96](#).
- Enable L2TP on the FortiGate unit and specify the range of addresses that can be assigned to remote clients when they connect. See [“Enabling L2TP and specifying an address range” on page 96](#).
- Define firewall source and destination addresses to indicate where packets transported through the L2TP tunnel will originate and be delivered. See [“Defining firewall source and destination addresses” on page 97](#).
- Create the firewall policy and define the scope of permitted services between the source and destination addresses. [“Adding the firewall policy” on page 98](#).
- Configure the remote clients. For example, see [“Configuring a Linux client” on page 98](#).

Authenticating L2TP clients

L2TP clients must be authenticated before a tunnel is established. The authentication process relies on FortiGate user group definitions, which can optionally use established authentication mechanisms such as RADIUS or LDAP to authenticate L2TP clients. All L2TP clients are challenged when a connection attempt is made.

To enable authentication, you must create user accounts and a user group to identify the L2TP clients that need access to the network behind the FortiGate unit. Within the user group, add a user for each remote client. For more information, see the “Users and Authentication” chapter of the [FortiGate Administration Guide](#).

You can choose to use a plain text password for authentication or forward authentication requests to an external RADIUS or LDAP server. If password protection will be provided through a RADIUS or LDAP server, you must configure the FortiGate unit to forward authentication requests to the authentication server. For more information, see the “Users and Authentication” chapter of the [FortiGate Administration Guide](#).

Enabling L2TP and specifying an address range

The L2TP address range specifies the range of addresses reserved for remote clients. When a remote client connects to the FortiGate unit, the client is assigned an IP address from this range. Afterward, the FortiGate unit uses the assigned address to communicate with the remote client.

The address range that you reserve can be associated with private or routable IP addresses. If you specify a private address range that matches a network behind the FortiGate unit, the assigned address will make the remote client appear to be part of the internal network.

To enable L2TP and specify the L2TP address range

- 1 Go to **VPN > L2TP > L2TP Range**.
- 2 Select Enable L2TP.

- 3 In the Starting IP field, type the starting address in the range of reserved IP addresses.
- 4 In the Ending IP field, type the ending address in the range of reserved IP addresses.
- 5 From the User Group list, select the name of the L2TP user group that you defined previously. See [“Authenticating L2TP clients” on page 96](#).
- 6 Select Apply.

Defining firewall source and destination addresses

Before you define the firewall policy, you must define the source and destination addresses of packets that are to be transported through the L2TP tunnel:

- For the source address, enter the range of addresses that you reserved for remote L2TP clients (for example 192.168.10.[80-100]).
- For the destination address, enter the IP addresses of the computers that the L2TP clients need to access on the private network behind the FortiGate unit (for example, 172.16.5.0/24 for a subnet, or 172.16.5.1/32 for a server or host, or 192.168.10.[10-15] for an IP address range).

To define the firewall source address

- 1 Go to **Firewall > Address** and select Create New.
- 2 In the Address Name field, type a name that represents the range of addresses that you reserved for remote clients (for example, Ext_L2TPrange).
- 3 In the IP Range/Subnet field, type the corresponding IP address range.
- 4 Select OK.

To define the firewall destination address

- 1 Go to **Firewall > Address** and select Create New.
- 2 In the Address Name field, type a name that represents a range of IP addresses on the network behind the FortiGate unit (for example, Int_L2TPaccess).
- 3 In the IP Range/Subnet field, type the corresponding IP address range.
- 4 Select OK.

Adding the firewall policy

The firewall policy specifies the source and destination addresses that can generate traffic inside the L2TP tunnel and defines the scope of services permitted through the tunnel. If a selection of services are required, define a service group. For more information, see the “Firewall” chapter of the [FortiGate Administration Guide](#).

To define the traffic and services permitted inside the L2TP tunnel

- 1 Go to **Firewall > Policy** and select Create New.
- 2 Enter these settings in particular:

Interface/Zone	Source Select the FortiGate interface to the Internet. Destination Select the FortiGate interface to the internal (private) network.
Address Name	Source Select the name that corresponds to the range of addresses that you reserved for L2TP clients (for example, <code>Ext_L2TPrange</code>). Destination Select the name that corresponds to the IP addresses behind the FortiGate unit (for example, <code>Int_L2TPaccess</code>).
Service	Select ANY, or if selected services are required instead, select the service group that you defined previously.
Action	Select ACCEPT.
- 3 You may enable NAT, a protection profile, and/or event logging, or select advanced settings to shape traffic or differentiate services. See the “Firewall” chapter of the [FortiGate Administration Guide](#).
- 4 Select OK.

Configuring a Linux client

The following procedure outlines how to install L2TP client software and run an L2TP tunnel on a Linux computer. Obtain an L2TP client package that meets your requirements (for example, `rp-l2tp`). If needed to encrypt traffic, obtain L2TP client software that supports encryption using MPPE.

To establish an L2TP tunnel with a FortiGate unit that has been set up to accept L2TP connections, you can obtain and install the client software following these general guidelines:

- 1 If encryption is required but MPPE support is not already present in the kernel, download and install an MPPE kernel module and reboot your computer.
- 2 Download and install the L2TP client package.
- 3 Configure an L2TP connection to run the L2TP program.
- 4 Configure routes to determine whether all or some of your network traffic will be sent through the tunnel. You must define a route to the remote network over the L2TP link and a host route to the FortiGate unit.
- 5 Run `l2tpd` to start the tunnel.

Follow the software supplier's documentation to complete the steps.

To configure the system, you need to know the public IP address of the FortiGate unit, and the user name and password that has been set up on the FortiGate unit to authenticate L2TP clients. Contact the FortiGate administrator if required to obtain this information.

Monitoring and Testing VPN Tunnels

This chapter outlines some general maintenance and monitoring procedures for VPNs and includes the following topics:

- [Viewing IPsec VPN tunnel status](#)
- [Monitoring VPN connections](#)
- [Monitoring IKE, PPTP, and L2TP sessions](#)
- [Testing VPN connections](#)
- [Logging VPN events](#)
- [IPsec VPN troubleshooting tips](#)

Viewing IPsec VPN tunnel status

You can display the IPsec VPN tunnel list to view the status of all IPsec VPN tunnels. The list shows the status of all active tunnels as well as the tunnel time out values.

To view IPsec VPN tunnel status, go to **VPN > IPSEC > Phase 2**.

Figure 26: IPsec tunnel status

Tunnel Name	Remote Gateway	Lifetime(sec/kb)	Status	Timeout	
Static_Tunnel_1	65.34.56.78	1800/NA	Down	0	
Dialup_tunnel	Dialup	1800/NA	Unknown	0	
Dyn_DNS_tunnel	mydomain.com	1800/NA	Down	0	

The Status column displays the status of each tunnel. If Status is Up, the tunnel is active. If Status is Down, the tunnel is not active. Unknown is displayed for dialup tunnels.

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.

Monitoring VPN connections

You can use the monitor to view activity on IPsec VPN tunnels and start or stop those tunnels. The display provides a list of addresses, proxy IDs, and timeout information for all active tunnels.

Monitoring connections to remote peers

The list of tunnels provides information about VPN connections to remote peers that have static IP addresses or domain names. You can use this list to view status and IP addressing information for each tunnel configuration. You can also start and stop individual tunnels from the list.

To view the list of static-IP and dynamic-DNS tunnels, go to **VPN > IPSEC > Monitor**.

Figure 27: List of static-IP and dynamic-DNS tunnels

Static IP and dynamic DNS:					
Name	Remote gateway	Timeout	Proxy ID Source	Proxy ID Destination	
FG_hidden_FortiLog	192.168.34.56:500	0	0.0.0.0-255.255.255.255	192.168.34.56	⊕
FG1toSP1_Tunnel	172.16.20.1:500	0	192.168.22.*	192.168.33.*	⊕
FG1toSP2_Tunnel	172.16.30.1:500	0	192.168.22.*	192.168.44.*	⊕
Redundant_tunnel	10.10.10.2:500	0			⊕
Redundant_tunnel	10.10.10.1:500	0			⊕

Bring up tunnel

To establish or take down a VPN tunnel

- 1 Go to **VPN > IPSEC > Monitor**.
- 2 In the list of tunnels, select the Bring down tunnel or Bring up tunnel button in the row that corresponds to the tunnel that you want to bring down or up.

Monitoring dialup IPsec connections

The list of dialup tunnels provides information about the status of tunnels that have been established for dialup clients. The list displays the IP addresses of dialup clients and the names of all active tunnels. The number of tunnels shown in the list can change as dialup clients connect and disconnect.

To view the list of dialup tunnels, go to **VPN > IPSEC > Monitor**.

Figure 28: List of dialup tunnels

Dialup:						
Name	Remote gateway	Username	Timeout	Proxy ID Source	Proxy ID Destination	
Dialup_tunnel_3	172.20.120.20:500		1746	10.0.0.2	172.20.120.20	⊕



Note: If you take down an active tunnel while a dialup client such as FortiClient is still connected, FortiClient will continue to show the tunnel connected and idle. The dialup client must disconnect before another tunnel can be initiated.

The list of dialup tunnels displays the following statistics:

- The Name column displays the name of the tunnel.
- The meaning of the value in the Remote gateway column changes, depending on the configuration of the network at the far end:
 - When a FortiClient dialup client establishes a tunnel, the Remote gateway column displays either the public IP address and UDP port of the remote host device (on which the FortiClient Host Security application is installed), or if a NAT device exists in front of the remote host, the Remote gateway column displays the public IP address and UDP port of the remote host.
 - When a FortiGate dialup client establishes a tunnel, the Remote gateway column displays the public IP address and UDP port of the FortiGate dialup client.
- The Username column displays the peer ID, certificate name, or XAuth user name of the dialup client (if a peer ID, certificate name, or XAuth user name was assigned to the dialup client for authentication purposes).
- The Timeout column displays the time before the next key exchange. The time is calculated by subtracting the time elapsed since the last key exchange from the keylife.
- The Proxy ID Source column displays the IP addresses of the hosts, servers, or private networks behind the FortiGate unit. A network range may be displayed if the source address in the firewall encryption policy was expressed as a range of IP addresses.
- The meaning of the value in the Proxy ID Destination column changes, depending on the configuration of the network at the far end:
 - When a FortiClient dialup client establishes a tunnel:
 - If VIP addresses are not used and the remote host connects to the Internet directly, the Proxy ID Destination field displays the public IP address of the Network Interface Card (NIC) in the remote host.
 - If VIP addresses are not used and the remote host is behind a NAT device, the Proxy ID Destination field displays the private IP address of the NIC in the remote host.
 - If VIP addresses were configured (manually or through FortiGate DHCP relay), the Proxy ID Destination field displays either the VIP address belonging to a FortiClient dialup client, or a subnet address from which VIP addresses were assigned.
 - When a FortiGate dialup client establishes a tunnel, the Proxy ID Destination field displays the IP address of the remote private network.

Monitoring IKE, PPTP, and L2TP sessions

You can display a list of all active sessions and view activity by port number. By default, the following ports are used for VPN-related communications:

- port numbers 500 and 4500 for IPsec IKE activity
- port number 4500 for NAT traversal activity
- port number 1723 for PPTP activity
- port number 1701 for L2TP activity

If required, active sessions can be stopped from this view. For more information, see the “System status” chapter of the [FortiGate Administration Guide](#).

To view the list of active sessions, go to **System > Status > Session**.

Figure 29: Session list

Protocol	From IP	From Port	To IP	To Port	Expire(secs)	Policy ID
udp	10.0.0.1	520	224.0.0.9	520	0	
tcp	172.20.120.20	3935	172.20.120.125	443	3599	
udp	127.0.0.1	1024	127.0.0.1	53	24	
udp	172.20.120.125	520	224.0.0.9	520	0	

Testing VPN connections

To confirm whether a VPN has been configured correctly, issue a ping command on the network behind the FortiGate unit to test the connection to a computer on the remote network. See also “[Using the ping generator to keep a tunnel open](#)” on [page 75](#). A VPN tunnel will be established automatically when the first data packet destined for the remote network is intercepted by the FortiGate unit.

To confirm that a VPN between a local network and a dialup client has been configured correctly, at the dialup client, issue a ping command to test the connection to the local network. The VPN tunnel initializes when the dialup client attempts to connect.

Logging VPN events

You can configure the FortiGate unit to log VPN events. For IPsec VPNs, phase 1 and phase 2 authentication and encryption events are logged. For PPTP and L2TP VPNs, connection events and tunnel status (up/down) are logged. For information about how to interpret log messages, see the [FortiGate Log Message Reference Guide](#).

To log VPN events

- 1 Go to **Log&Report > Log Config > Log Setting**.
- 2 Enable the storage of log messages to one or more of the following locations:
 - a FortiLog unit
 - the FortiGate hard disk (if available, depending on the model)
 - the FortiGate system memory
 - a remote computer running a syslog server
 - a remote computer running a WebTrends firewall reporting server
- 3 Select the blue arrow beside each option to reveal and configure associated settings.

If logs will be written to disk:

 - From the Level list, select Information.
 - Select Log file upload settings, and verify that Event Log is selected.

If logs will be written to system memory:

 - From the Level list, select Information.

For more information, see the “Log & Report” chapter of the [FortiGate Administration Guide](#).
- 4 Select Apply.

To filter VPN events

- 1 Go to **Log&Report > Log Config > Log Filter**.
- 2 In the top row, depending on whether logs will be written to disk or memory, select Disk or Memory.
- 3 Under Event Log, in the Disk or Memory column (whichever format you are using to save log messages), verify that one or both of the following options are selected, depending on your requirements:
 - IPSec negotiation event
 - L2TP/PPTP/PPPoE service event
- 4 Select Apply.

To view event logs

- 1 Go to **Log&Report > Log Access > Event**.
- 2 If the option is available from the Type list, select the log file from disk or memory.

Entries similar to the following indicate that a tunnel has been established.

```

1 2004-10-26 16:57:33 notice negotiate Initiator: tunnel 172.16.20.143, transform=ESP_3DES, HMAC_SHA1
2 2004-10-26 16:57:33 notice negotiate Initiator: sent 172.16.20.14 quick mode message #2 (DONE)
3 2004-10-26 16:57:33 notice install_sa Initiator: tunnel 10.10.10.3/172.16.20.143 install ipsec sa
4 2004-10-26 16:57:33 notice negotiate Initiator: sent 172.16.20.14 quick mode message #1 (OK)
5 2004-10-26 16:57:33 notice negotiate Initiator: parsed 172.16.20.14 main mode message #3 (DONE)
6 2004-10-26 16:57:33 notice negotiate Responder: sent 172.16.20.14 main mode message #3 (OK)

```

```

7 2004-10-26 16:57:33 notice negotiate Initiator: sent 172.16.20.14 main mode message #2 (OK)
8 2004-10-26 16:57:33 notice negotiate Initiator: sent 172.16.20.14 main mode message #1 (OK)

```

Entries similar to the following indicate that a tunnel has been taken down.

```

1 2004-10-26 18:11:30 notice delete_phase1_sa delete phase1 sa
2 2004-10-26 18:11:30 notice negotiate Responder: sent 172.16.20.14 quick mode message #1 (OK)
3 2004-10-26 18:11:30 notice delete_ipsec_sa delete ipsec sa

```

Entries similar to the following indicate that phase 1 negotiations broke down because the preshared keys belonging to the VPN peers were not identical. A tunnel was not established.

```

1 2004-10-26 18:12:22 notice delete_phase1_sa delete phase1 sa

3 2004-10-26 18:12:22 notice negotiate Responder: sent 172.16.20.14 main mode message #3 (OK)
4 2004-10-26 18:12:22 notice negotiate Initiator: sent 172.16.20.14 main mode message #2 (OK)
5 2004-10-26 18:12:22 notice negotiate Initiator: sent 172.16.20.14 main mode message #1 (OK)

```

IPSec VPN troubleshooting tips

Most connection failures are due to a configuration mismatch between the FortiGate unit and the remote peer. In general, begin troubleshooting an IPSec VPN connection failure as follows:

- 1 Ping the remote network or client to verify whether the connection is up. See [“Testing VPN connections” on page 104](#).
- 2 Verify the configuration of the FortiGate unit and the remote peer. The following IPSec parameters must agree:
 - 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 vice versa.
- 3 Refer to [Table 3 on page 107](#) to correct the problem.

Table 3: VPN trouble-shooting tips

Configuration problem	Correction
Mode settings do not match.	Select complementary mode settings. See “Configuring the phase 1 IKE exchange” on page 67 .
Peer ID or certificate name of the remote peer or dialup client is not recognized by FortiGate VPN server.	Go to VPN > Phase 1 . Depending on the Remote Gateway and Authentication Method settings, you have a choice of options to authenticate remote dialup clients or VPN peers by ID or certificate name (see “Peer and user authentication options” on page 57). 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 52 .
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 “Configuring the phase 1 IKE exchange” on page 67 and “Configuring the phase 2 tunnel creation parameters” on page 73 .
NAT traversal settings are mismatched.	Select or clear both options as required. See “NAT traversal” on page 66 and “NAT keepalive frequency” on page 66 .
SPI settings for manual key tunnels are mismatched.	Enter complementary SPI settings. See “Manual-key configurations” on page 49 .

A word about NAT devices

When a device with NAT capabilities is located between two VPN peers or a VPN peer and a dialup client, the device must be NAT_T compatible for encrypted traffic to pass through the NAT device. For more information, see [“NAT traversal” on page 66](#).

Glossary

address: An IP address (logical address) or the address of a physical interface (hardware address). An Ethernet address is sometimes called a MAC address. See also *IP address*.

aggressive mode: A way to establish a secure channel during IPSec phase 1 negotiations when the VPN peer uses its identity as part of the authentication process. See also *main mode*.

AH, Authentication Header: An IPSec security protocol. Fortinet IPSec uses ESP in tunnel mode, not AH. See *ESP*.

ARP, Address Resolution Protocol: A protocol that resolves a logical IP address to a physical Ethernet address.

authentication: A process whereby a server determines whether a client may establish a connection and access private resources.

CA, Certificate Authority: A company that issues digital certificates to validate the identity of a person or entity in an online exchange.

CHAP, Challenge Handshake Authentication Protocol: An authentication protocol supported by PPP. See also *PPP*.

client: An application that requires and requests services from a server.

cluster: A group of servers configured to act as a single fault-tolerant unit.

connection: A link between computers, applications, or processes that can be logical, physical, or both.

decryption: A method of decoding an encrypted file into its original state.

DHCP, Dynamic Host Configuration Protocol: An Internet protocol that assigns IP addresses to network clients, usually when the client connects to the Internet.

Diffie-Hellman: An algorithm for establishing a shared secret key over an insecure medium. See *Diffie-Hellman group*.

Diffie-Hellman group: FortiGate units support Diffie-Hellman groups 1, 2 and 5. The size of the modulus used to calculate the key varies according to the group:

- Group 1: 768-bit modulus
- Group 2: 1024-bit modulus
- Group 5: 1536-bit modulus

digital certificate: A digital document that guarantees the identity of a person or entity and is issued by a CA.

DMZ, Demilitarized Zone: An untrusted area of a private network, usually used to host Internet services without allowing unauthorized access to an internal (private) network. Typically, the DMZ contains servers accessible to Internet traffic, such as Web, FTP, SMTP, and DNS servers.

DMZ interface: The FortiGate interface that connects to a DMZ network.

DNS, Domain Name System: A service that converts symbolic node names to IP addresses. A domain name server (DNS server) implements the protocol.

DoS, Denial-of-Service: An attempt to disrupt a service by flooding the network with fake requests that consume network resources.

DSL, Digital Subscriber Line: A way to access the Internet at higher speeds using existing copper telephone lines. Users can maintain a continuous connection to the Internet and use the phone simultaneously.

encapsulate: Add a header to a packet to create a unit of transmission that matches the unit of transmission on a different network layer.

encryption: A method of encoding a file so that it cannot be understood. The information must be decrypted before it can be used.

endpoint: The IP address or port number that defines one end of a connection.

ESP, Encapsulated Security Protocol: An IPSec security protocol that provides encapsulation of encrypted data—IP packets are embedded in other IP packets so that the originating source and destination IP addresses cannot be seen on the Internet.

Ethernet: Can refer to the IEEE 802.3 signaling protocol, or an Ethernet controller (also known as a Media Access Controller or MAC).

external interface: The FortiGate interface that connects to the Internet.

FTP, File Transfer Protocol: A protocol used to transfer files between computers that have different operating systems.

gateway: A combination of hardware and layer-3 (network-layer) software that relays packets from one network to another.

hash algorithm: A procedure that renders a text message as a unique number.

header: The part of a packet that includes the source and destination address of the associated data. This addressing information is used to route packets.

hop: The segment of packet transmission that occurs between two routers. A packet may make several hops as it travels to its destination.

host: A network entity that has an IP address.

HTTP, Hypertext Transmission Protocol: The protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

HTTPS: The secure HTML protocol for transmitting encrypted information to web servers using SSL. See also *SSL*.

hub: A device where communication links are brought together to exchange data between several computers.

ICMP, Internet Control Message Protocol: An IP message control protocol that supports error messages, test packets, and information messages related to IP. This protocol is used by the ping generator to send ICMP echo requests to a host.

IKE, Internet Key Exchange: A method of automatically exchanging IPsec authentication and encryption keys between two secure servers.

IMAP, Internet Message Access Protocol: An Internet email protocol that allows access to an email server from any IMAP-compatible browser.

internal interface: The FortiGate interface that connects to an internal (private) network.

Internet: The network that encompasses the world. As a generic term, it refers to any collection of interdependent networks.

IP, Internet Protocol: The component of TCP/IP that handles routing.

IP address: The point of attachment to a TCP/IP network. An IP address is a 32-bit quantity written in dotted decimal notation (four numbers separated by periods). See also *netmask*.

IPSec, Internet Protocol Security: A set of protocols that support secure exchange of packets at the IP layer. IPSec is most often used to support VPNs. See *VPN*.

ISP, Internet Service Provider: A company that provides customers with access to the Internet.

KB, kilobyte: A unit of storage (1 024 bytes).

L2TP, Layer 2 Tunneling Protocol: A security protocol that enables ISPs to establish VPN tunnels on behalf of dialup clients.

LAN, Local Area Network: A computer network that spans a relatively small area.

Layer 2: The data-link layer of the OSI model. Layer 2 is responsible for transmission, framing, and error control over a single link.

Layer 3: The network layer of the OSI model. Layer 3 is responsible for examining each network packet and sending them to the proper destination over the Internet.

local: The near end point (an IP address or port number) of a connection.

MAC address, Media Access Control address: A layer-2 hardware address that uniquely identifies a network node.

main mode: A way to hide the identities of VPN peers from passive eavesdroppers during IPsec phase 1 negotiations. See also *aggressive mode*.

MB, Megabyte: A unit of storage (1 048 576 bytes).

MIB, Management Information Base: A database of objects that can be monitored by an SNMP network manager.

modem: A device that converts digital signals into analog signals and back again for transmission over telephone lines.

MTU, Maximum Transmission Unit: The largest physical packet size, measured in bytes, that a network can transmit. Any packets larger than the MTU are divided into smaller packets before they are sent.

NAT, Network Address Translation: A way of routing IPv4 packets transparently. Using NAT, a router or FortiGate unit between a private and public network translates private IP addresses to public addresses and the other way around.

netmask, network mask: Also sometimes called subnet mask. A 32-bit quantity that indicates which bits of an IP address refer to the network portion.

NTP, Network Time Protocol: Used to synchronize the time of a computer to an NTP server. NTP provides accuracies to within tens of milliseconds across the Internet relative to coordinated universal time.

OSI, Open Systems Interconnection: A standard that defines network communication protocols using a seven-layer model.

packet: A piece of data transmitted over a packet-switched network. A packet contains a payload, the source and destination addresses, and a checksum. In IP networks, packets are often called datagrams. Packets are passed between the OSI data-link and network layers.

PAP, Password Authentication Protocol: An authentication protocol supported by PPP. See also *PPP*.

ping, packet Internet grouper: A utility for determining whether the device at a specific IP address is accessible. The utility sends a packet to the specified address and waits for a reply.

POP3, Post Office Protocol: A protocol used to transfer email from a mail server to a mail client across the Internet. Most email clients use POP.

port: The part of an interface on which application traffic is carried. By convention, the port number identifies the type of traffic. For example, port 80 is used for HTTP traffic.

PPP, Point-to-Point Protocol: A protocol for transmitting IP packets over serial point-to-point links (that is, across any DTE/DCE interface).

PPPoE, PPP over Ethernet: A protocol that specifies how to encapsulate PPP packets over Ethernet.

PPTP, Point-to-Point Tunneling Protocol: A security protocol that creates a VPN by encapsulating PPP packets.

protocol: A standard format for transmitting data. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device indicates that it has finished sending a message, and how the receiving device indicates that it has received a message.

RADIUS, Remote Authentication Dial-In User Service: A user authentication and network-usage accounting system. When users dial into an ISP they enter a user name and password. This information is passed to a RADIUS server, which authenticates the user and authorizes access to the network.

remote: The far end point (an IP address or port number) of a connection.

replay detection: A way to determine whether a replay attack is underway in an IPsec tunnel. A replay attack occurs when an unauthorized party intercepts a series of IPsec packets and changes them in an attempt to flood a tunnel or access a VPN.

RFC, Request for Comments: Internet Standards Committee documentation.

RIP, Routing Information Protocol: An Internet protocol for sharing routing information within an autonomous system.

router: A hardware device that connects computers on the Internet together and routes traffic between them. A router may connect a LAN and/or DMZ to the Internet.

routing: The process of determining which path to use for sending packets to a destination.

routing table: A list of possible paths that a packet can take to reach a destination.

SA, Security Association: SAs protect tunneled packets. They contain the information needed to create an IPsec VPN tunnel. An SA is uniquely identified by a security parameter index, an IP destination address, and a security protocol identifier. The Internet Security Association and Key Management Protocol (ISAKMP) is used to manage SAs.

server: An application that answers requests from clients. Used as a generic term for any device that provides services to the rest of the network such as printing, storage, and network access.

SMTP, Simple Mail Transfer Protocol: A protocol that supports email delivery services.

SNMP, Simple Network Management Protocol: A set of protocols for managing networks. SNMP agents store and return data about themselves to SNMP requesters.

spam: Unsolicited email.

SSH, Secure Shell: An application that enables users to log into a remote computer and run commands securely.

SSL, Secure Sockets Layer: An Internet security protocol that uses private and public encryption keys and certificates to keep transactions private.

subnet, subnetwork: A logical network comprising devices whose IP addresses have the same network prefix. For example, all devices having IP addresses in the 192.168.10.0/24 range can be accessed on the same subnet. See also *netmask*.

TCP, Transmission Control Protocol: One of the main protocols in TCP/IP networks. TCP guarantees delivery of data and also guarantees that packets are delivered in the same order sent.

trojan horse: A harmful program that disguises itself as another program.

UDP, User Datagram Protocol: A connectionless protocol that runs on IP networks and is used primarily for broadcasting messages throughout the network.

virus: A computer program that replicates and spreads itself through computers or networks, usually with harmful intent.

VPN, Virtual Private Network: A secure logical network created from physically separate networks. VPNs use encryption and other security mechanisms to ensure that only authorized users can access the network and that data transmitted between VPN devices cannot be intercepted.

worm: A harmful program that replicates itself until it fills a computer or network, which can shut the system down.

Index

A

- Accept any peer ID 60
- Accept peer ID in dialup group 60, 62, 63
- Accept this peer certificate group only 59
- Accept this peer certificate only 59
- Accept this peer ID 60, 62
- Action, Policy 80
- aggressive mode 59
- Allow inbound, encryption policy 78
- Allow outbound, encryption policy 78
- ambiguous routing
 - resolving in FortiClient dialup-client configuration 26
 - resolving in FortiGate dialup-client configuration 33
 - resolving in gateway-to-gateway configuration 15
- authenticating
 - based on peer IDs 62
 - IPsec VPN peers and clients 52
 - L2TP clients 96
 - PPTP clients 86
 - through IPsec certificate 52
 - through IPsec preshared key 53
 - through XAuth settings 63
- Authentication Algorithm, Manual Key 50
- Authentication Key, Manual Key 51
- authentication server, external
 - for L2TP 96
 - for PPTP 86
 - for XAuth 63
- Autokey Keep Alive, Phase 2 71, 74

B

- backup, IPsec certificate 56

C

- CA Certificates 56
- Certificate Name, Phase 1 53
- certificate, IPsec 52
 - generating request 55
 - group 58
 - installing CA 56
 - installing signed 56
 - Local ID setting 59
 - managing 54
 - Subject Information 55
 - using DN to establish access 57
 - viewing local DN 58
- CLI 10
 - dead peer detection options 68
- comments, documentation 12
- concentrator, defining 20

- Concentrator, Manual Key 51
- Concentrator, New VPN Tunnel 71
- configuring
 - dynamic DNS IPsec VPN 23
 - FortiClient dialup-client VPN 28
 - FortiClient in dialup-client IPsec VPN 30
 - FortiClient in Internet-browsing IPsec VPN 40
 - FortiGate dialup-client VPN 34
 - FortiGate in dialup-client IPsec VPN 36
 - FortiGate in Internet-browsing IPsec VPN 41
 - gateway-to-gateway IPsec VPN 17
 - hub-and-spoke IPsec VPN 18
 - IPsec VPNs 14
 - manual key IPsec VPN 50
 - redundant-tunnel IPsec VPN 43
 - transparent IPsec VPN 48
- customer support, contacting 12

D

- DDNS services, subscribing to 23
- dead peer detection, CLI commands 68
- Dead Peer Detection, Phase 1 66, 67, 68
- destination IP address 76
 - example 77
- DH Group, Phase 1 65, 68
- DH Group, Phase 2 71, 74
- DHCP relay
 - in FortiClient dialup-client configuration 30
 - in FortiGate dialup-client configuration 33
- DHCP-IPsec, phase 2 72, 74
- dialup server, FortiGate unit as 26, 32
- dialup-client IPsec configuration
 - configuration steps for FortiClient dialup clients 28
 - configuration steps for FortiGate dialup clients 34
 - DHCP relay for FortiClient VIP 30
 - dialup server for FortiClient dialup clients 29
 - dialup server for FortiGate dialup clients 35
 - FortiClient configuration 30
 - FortiGate client configuration 36
 - infrastructure requirements for FortiClient access 28
 - infrastructure requirements for FortiGate client access 34
- Diffie-Hellman algorithm 65, 71
- DNS server, dynamic DNS configuration 22, 23
- documentation
 - commenting on 12
 - FortiGate 11
 - IPsec technical notes 81
- domain name, dynamic DNS configuration 22, 23
- dpd-idlecleanup 69
- dpd-idleworry 69
- dpd-retrycount 69
- dpd-retryinterval 69

- dynamic DNS IPsec configuration
 - configuration steps 23
 - domain name configuration 23
 - infrastructure requirements 23
 - overview 22
 - remote VPN peer configuration 24
 - supported DDNS services 23
- dynamic IP address
 - FortiClient dialup client 25
 - FortiGate dialup client 31
 - FortiGate VPN peer 22

E

- Enable perfect forward secrecy (PFS), Phase 2 72, 74
- Enable replay detection, Phase 2 72, 74
- Encryption Algorithm, Manual Key 50
- Encryption Key, Manual Key 50
- encryption policy
 - allow outbound and inbound 78
 - defining IP addresses 76
 - defining IPsec 78, 80
 - defining multiple for same IPsec tunnel 79
 - enabling specific services 79
 - evaluating multiple 79
 - outbound and inbound NAT 78
 - traffic direction 78
- examples, IPsec VPN configurations 81
- exporting, certificate backup 56
- extended authentication (XAuth) 63

F

- firewall IP addresses
 - defining IPsec 76
 - defining L2TP 97
 - defining PPTP 87
- firewall policy
 - defining IPsec 78
 - defining L2TP 97, 98
 - defining PPTP 88
- FortiClient
 - manually assigning a VIP address 31
- FortiClient dialup-client IPsec configuration
 - FortiClient overview 25
 - using DHCP relay in 27
 - VIP address assignment 27
- FortiGate dialup-client IPsec configuration
 - FortiGate acting as client 31
 - using DHCP relay in 33
- FortiGate documentation 11
 - commenting on 12
 - contacting technical support 12
- Fortinet Knowledge Center 12
- Fortinet products, registering 12

G

- gateway-to-gateway IPsec configuration
 - configuration steps 17
 - infrastructure requirements 16
 - overview 15
- generating
 - IPsec certificate request 55
 - IPsec phase 1 keys 65
 - IPsec phase 2 keys 71

H

- hub-and-spoke IPsec configuration
 - concentrator, defining 20
 - configuration steps 18
 - hub configuration 19
 - infrastructure requirements 18
 - overview 18
 - spoke configuration 20

I

- IKE negotiation
 - configuring 67
 - parameters 64
- importing
 - CA certificate 56
 - signed certificate 56
- Inbound NAT, encryption policy 78
- Internet browsing, Phase 2 73, 75
- Internet-browsing IPsec configuration
 - FortiClient dialup-client configuration 40
 - FortiGate dialup-client configuration 41
 - gateway-to-gateway configuration 39
 - infrastructure requirements 38
 - overview 37
- introduction
 - FortiGate documentation 11
 - FortiGate VPNs 9
 - VPN Guide 10
- IP Range/Subnet, Address 77
- IPsec VPN
 - authentication methods 52
 - authentication options 57
 - certificates 57
 - extended authentication (XAuth) 63
 - firewall encryption policy 78
 - firewall IP addresses, defining 76
 - FortiGate implementation 9
 - keeping tunnel open 71, 75
 - overview 13
 - peer identification 59
 - phase 1 parameters 51
 - phase 2 parameters 71
 - role of encryption policy 79

K

- Keepalive Frequency, Phase 1 66, 68
- Keylife, Phase 1 65, 68

Keylife, Phase 2 71, 74

L

L2TP network server, FortiGate unit as 93

L2TP VPN

- authentication method 96
- configuration steps 96
- enabling 96
- firewall IP addresses, defining 97
- firewall policy, defining 98
- FortiGate implementation 9
- infrastructure requirements 95
- network configuration 95
- overview 93
- restrictions 93, 95
- VIP address range 96

LDAP server, external

- for L2TP 96
- for PPTP 86
- for XAuth 63

Local Certificates 55, 56

Local ID

- for certificates 59
- for peer IDs 61

Local ID, to identify FortiGate dialup clients 32

Local SPI, Manual Key 50

M

main mode 59

manual key IPsec configuration

- configuration steps 50
- overview 49

meshed VPN 16

Mode, Phase 1 52, 54, 59

N

NAT

- keepalive frequency 66
- traversal 66

Nat-traversal, Phase 1 66, 68

negotiating

- IPsec phase 1 parameters 65
- IPsec phase 2 parameters 71

network topology

- fully meshed network 16
- IPsec dynamic DNS 22
- IPsec FortiClient dialup-client 25
- IPsec FortiGate dialup-client 31
- IPsec gateway-to-gateway 15
- IPsec hub-and-spoke 18
- IPsec Internet-browsing 37
- IPsec manual key 49
- IPsec redundant-tunnel 41
- IPsec transparent VPN 44
- IPsec VPNs 15
- L2TP VPN 95
- partially meshed network 16
- PPTP VPN 85

O

Outbound NAT, encryption policy 78

overlap

- resolving IP address 15, 33
- resolving through FortiGate DHCP relay 33

P

P1 Proposal, Phase 1 64, 67

P2 Proposal, Phase 2 71, 74

partially meshed VPN 16

peer ID

- assigning to FortiGate unit 61
- enabling 59
- Local ID setting 61
- Peer Options settings 60

perfect forward secrecy, enabling 72

phase 1 parameters

- authentication method 52
- authentication options 57
- defining 51
- negotiating 65
- overview 51
- Peer Options 60

phase 2 parameters

- configuring 73
- defining 71
- negotiating 71

ping generator, configuring 75

PPTP server

- configuring FortiGate unit as 87
- external 88

PPTP VPN

- authentication method 86
- configuration steps 85
- configuring pass through 86, 88
- enabling 86
- firewall IP addresses, defining 87
- firewall policy, defining 88
- FortiGate implementation 9
- infrastructure requirements 85
- network configuration 85
- overview 83
- VIP address range 86

preshared key, for IPsec authentication 52

Pre-shared Key, Phase 1 54

product registration 12

protocols, supported VPN 9

Q

Quick mode identities, Phase 2 73, 75

R

RADIUS server, external

- for L2TP 96
- for PPTP 86
- for XAuth 63

redundant-tunnel IPsec configuration

- configuration steps 43
- infrastructure requirements 42
- overview 41

remote client

- authenticating with certificates 52
- authenticating with preshared key 53
- FortiClient dialup-client 25
- FortiClient Host Security application 25
- FortiGate acting as 31
- FortiGate dialup-client 31
- Internet-browsing IPsec configuration 37
- L2TP VPN 98
- PPTP VPN 90, 91

Remote Gateway

- Dialup User 60
- Dynamic DNS 60
- Static IP address 60

Remote Gateway, Phase 1 52, 53, 59

Remote Gateway, Phase 2 73

remote peer

- authenticating with certificates 52
- authenticating with preshared key 53
- dynamic DNS IPsec configuration 24
- gateway-to-gateway IPsec configuration 17
- internet-browsing IPsec configuration 39
- manual key IPsec configuration 49
- redundant-tunnel IPsec configuration 43
- transparent IPsec VPN configuration 45

Remote SPI, Manual Key 50

replay detection, enabling 72

routing, transparent VPN IPsec configuration 47

S

Schedule, Policy 80

Service, Policy 80

source IP address 76

example 77

subscribing to DDNS service 23

T

technical notes, IPsec 81

technical support, contacting 12

Transparent mode 44

transparent VPN IPsec configuration

- configuration steps 48
- infrastructure requirements 47
- overview 44
- prerequisites to configuration 48

Tunnel Name, Phase 2 73

V

VIP address

- assigning to FortiClient 31
- FortiClient dialup clients 27
- L2TP clients 96
- PPTP clients 86

VIP address, assigning to FortiClient 26

virtual domain, transparent VPN IPsec configuration 48

VPN

- general steps for configuring IPsec 14
- general steps for configuring L2TP 96
- general steps for configuring PPTP 85
- interoperability 10
- supported protocols 9

VPN Tunnel, Policy 80

W

web-based manager 10

X

XAuth client, FortiGate unit as 64

XAuth Enable as Client, Phase 1 64

XAuth Enable as Server, Phase 1 64

XAuth server, FortiGate unit as 63

XAuth, enabling 63