



# IPSec VPN Quick Start Guide

|  |  |
|--|--|
| <i>Fortinet™ IPSec VPN Quick Start Guide</i> |  |
| <b>Document Version:</b>                     | Version 1.1  |
| <b>Publication Date:</b>                     | 09 November 2005   |
| <b>Description:</b>                          | This quick start guide explains how to configure the FortiClient™ Host Security application or a FortiGate™ unit to connect to a remote network. |
| <b>Product:</b>                              | FortiGate v2.80 MR10 and FortiClient v2.0  |
| <b>Document Number:</b>                      | 01-28010-0238-20051109   |

**Fortinet Inc.**

© 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.

*Fortinet™ IPsec VPN Quick Start Guide*  
FortiGate v2.80 MR10 and FortiClient v2.0  
09 November 2005  
01-28010-0238-20051109

#### Trademarks

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

## Revision history

| Version | Description  |
|---------|--|
| 1.0     | First edition  |
| 1.1     | In "Configuring your FortiGate unit to connect to the remote network", the step that said to clear Allow Inbound in the firewall policy was removed. In the field, clearing this default option had caused VPNs to not work. |

---

# Table of Contents

|  |    |
|--|----|
| Basic VPN concepts .....   | 6  |
| How IP addresses are used to send data through a VPN tunnel.....       | 7  |
| Additional settings used to create secure connections .....            | 9  |
| Preshared keys.....  | 10 |
| VPN client identifiers .....   | 10 |
| IPSec settings.....  | 10 |
| Schedule and service settings for FortiGate VPN clients .....          | 11 |
| Example VPNs.....  | 11 |
| Computer-to-private-network VPN .....                                  | 12 |
| Network-to-network VPN .....   | 12 |
| Connecting to a remote network using FortiClient software .....        | 13 |
| Before you begin .....   | 13 |
| Starting the FortiClient Host Security application.....                | 14 |
| Configuring FortiClient software to connect to a FortiGate unit .....  | 14 |
| Connecting to a remote network through a FortiGate unit .....          | 21 |
| Before you begin .....   | 21 |
| Configuring your FortiGate unit to connect to the remote network ..... | 22 |
| For more information.....  | 31 |



# FORTINET™

## Fortinet™ IPsec VPN Quick Start Guide

Virtual Private Network (VPN) technology allows users to connect to remote networks in a secure way. Someone could be traveling to a business conference or working at home, but thanks to VPNs, accessing a remote network from anywhere in the world is possible.

To enable authorized users to connect to a remote network from anywhere, Fortinet™ offers the FortiGate™ Antivirus Firewall and the FortiClient™ Host Security application. A FortiGate unit must be installed on the remote network, and FortiClient software is installed on the user's computer. A FortiGate unit may be used to connect to the remote network instead of FortiClient software.

This quick start guide explains how to configure the FortiClient Host Security application or a FortiGate unit to connect to a remote network. The following topics are included:

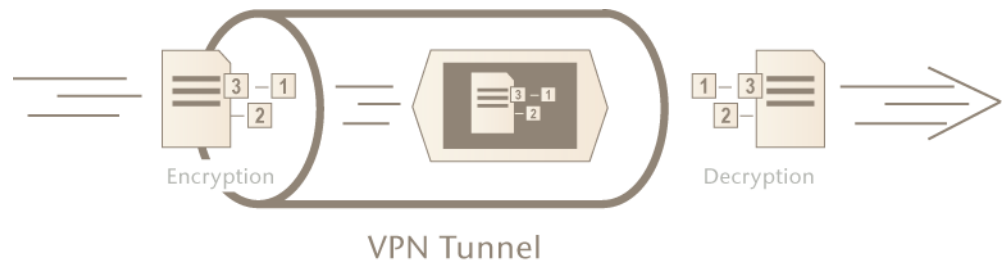
- To learn about VPN concepts, VPN technology, and the basic settings needed to create a Fortinet IPsec VPN, see [“Basic VPN concepts” on page 6](#). If you need more information as you go through the procedures in this document, refer to [“Basic VPN concepts”](#) for details.
- [“Example VPNs”](#) describes two of the most common ways to connect computers securely through the Internet using Fortinet IPsec VPN technology. To determine which one of these solutions applies to your situation, see [“Example VPNs” on page 11](#).
- If you would like to know how to connect your home computer to a remote network using FortiClient software, see [“Connecting to a remote network using FortiClient software” on page 13](#).
- If you have a FortiGate unit and would like to know how to connect your local private network to a remote network through a VPN, see [“Connecting to a remote network through a FortiGate unit” on page 21](#).
- The complete set of Fortinet product documentation and trouble-shooting information can be obtained from the Fortinet Technical Documentation web site and Fortinet Knowledge Center. Hyperlinks to these additional sources of information are provided in [“For more information” on page 31](#).

## Basic VPN concepts

A VPN is 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. VPNs also ensure that data transmitted between computers cannot be intercepted by unauthorized users.

Internet Protocol Security (IPSec) is used often to create VPNs. Using IPSec, the information transmitted between two computers cannot be seen by other computers. In general, the data is encoded so that it cannot be understood, and the data has to be decrypted before it can be used. When data is encoded and transmitted over the Internet, the data is said to be sent through a “VPN tunnel”. This idea is shown conceptually in [Figure 1](#).

**Figure 1: Encoded data going through a VPN tunnel**



To create a VPN tunnel, the computer that sends the information (a VPN client) and the computer that receives the information (a VPN server) must be equipped with data encryption and decryption software such as the FortiClient Host Security Application or the Fortinet FortiOS™ operating system, which is present on all FortiGate units.

A VPN tunnel can be established between:

- a FortiClient VPN client and a FortiGate VPN server
- a FortiGate VPN client and a FortiGate VPN server

Because the FortiClient Host Security application is a VPN client, it is responsible for initiating VPN tunnels with FortiGate VPN servers. FortiGate units themselves can perform both VPN client and/or VPN server functions. After a tunnel is established, the client computer can send and receive encoded data through the VPN tunnel and exchange data with remote computers securely.

Here's how it works:

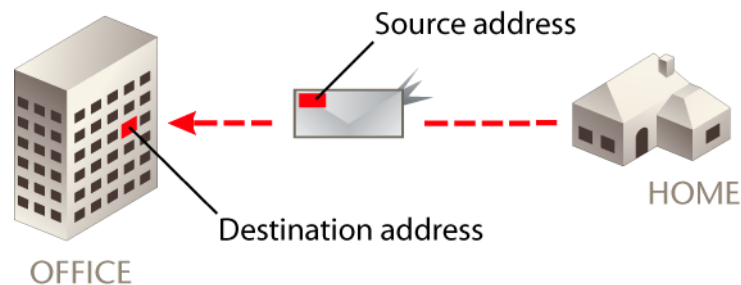
- 1 First, the FortiClient VPN client contacts the FortiGate VPN server with a request to create a tunnel—the client would contact the server whenever encoded data has to be sent to a remote computer.
- 2 Next, the FortiGate VPN server authenticates the FortiClient VPN client. Authentication is a process by which the server determines whether it is allowed to accept data from the client. If the server has been configured to accept data from the client, the server establishes a connection with the client.
- 3 With a secure connection in place, the FortiClient VPN client encrypts the data and sends it through the tunnel. The FortiGate VPN server accepts the encrypted data, decrypts the data, and forwards the data to the remote computer.

- 4 If the remote computer is required to send data back to the client computer, the remote computer sends its response to the FortiGate VPN server, which encrypts the data and forwards it to the FortiClient VPN client through the VPN tunnel.
- 5 The FortiClient VPN client accepts the data and decrypts it so that it can be used by the client computer.

## How IP addresses are used to send data through a VPN tunnel

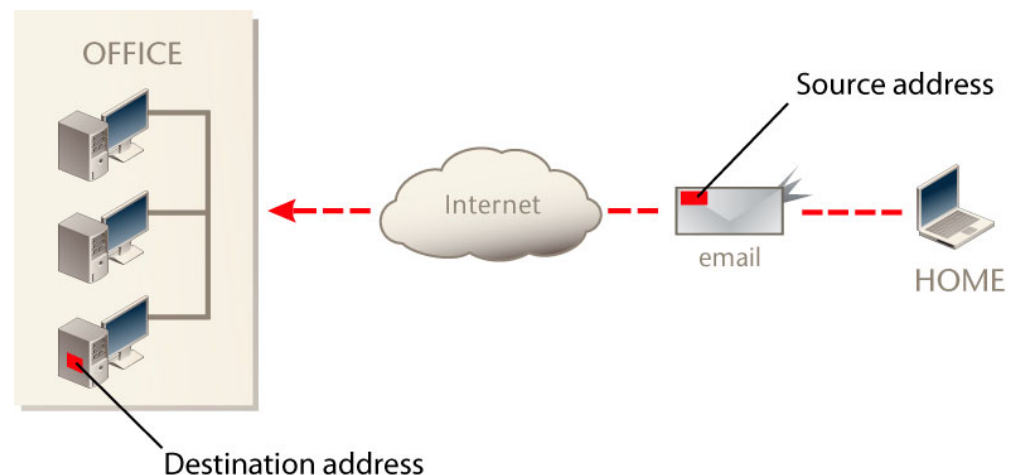
In network terminology, data is sent in something called an “IP packet.” An IP packet contains the data, a source address, and a destination address. Conceptually, source and destination addresses can be compared to street and/or apartment addresses (see [Figure 2](#)). When a letter is mailed, it is delivered to a street and/or apartment address (destination address). The return address (source address) is printed on the envelope.

**Figure 2: IP addresses can be compared to street addresses**



The source address corresponds to the computer that sent the data, and the destination address corresponds to the computer that will use the data. Computers use source and destination addresses to determine where a packet came from and where it is going. [Figure 3](#) shows a computerized version of the street-address analogy.

**Figure 3: Computerized version of street-address analogy**



In reality, an IP address identifies the physical place where a computer is attached to a network. The first part of an IP address contains four numbers separated by periods (for example, 192.168.10.5). These numbers refer to a specific computer. A complete IP address ends with something called a network mask (or “subnet mask”). The mask starts with a forward-slash, followed by four numbers separated by periods. These numbers identify a specific network. An example of a complete IP address is 192.168.10.0/255.255.255.0.

IP addresses can only be used to deliver packets on networks that use TCP/IP protocols to deliver packets. The Internet is an example of a public TCP/IP network. The networks commonly found in business offices are examples of private TCP/IP networks.

All computers on TCP/IP networks require IP addresses. Internet Service Providers (ISPs) are responsible for assigning IP addresses to computers that connect to the Internet. A computer can have a permanent IP address called a “static” IP address, or a temporary IP address called a “dynamic” IP address.

A FortiClient VPN client cannot establish a tunnel with a FortiGate VPN server unless the IP address of the VPN server is known ahead of time. Because VPN servers such as FortiGate units must be accessible to VPN clients constantly and without interruptions to service, VPN servers are typically assigned static IP addresses. Because a static IP address does not change, a VPN client can always use the same IP address to contact a VPN server that has a static IP address.

Dynamic IP addresses expire after a certain period of time. As a result, computers that have dynamic IP addresses may receive a different IP address at any time. A computer may be assigned a dynamic IP address for numerous reasons—the main reason being that dynamic IP addresses are less expensive compared to static IP addresses for accessing the Internet. Because home computers usually need to access the Internet intermittently for relatively short periods of time, having an IP address that changes periodically does not usually cause problems.

However, because dynamic IP addresses are temporary, a VPN server cannot use a dynamic IP address to communicate with a VPN client. Instead, FortiGate VPN servers use “virtual IP addresses” to deliver packets to FortiClient VPN clients, and identifiers (called “local IDs”) to identify FortiGate VPN clients. A virtual IP address is an IP address that a FortiGate VPN server assigns to a FortiClient VPN client. A local ID is simply a name for a FortiGate VPN client.



**Note:** Because a FortiGate unit may act as a VPN client, a FortiGate unit may be assigned a dynamic IP address. If you have a FortiGate unit, you can contact your ISP if required to find out if a static or dynamic IP address is associated with your Internet account.

Figure 4 shows some example IP addresses for configuring a FortiClient VPN client.

**Figure 4: Example FortiClient VPN client configuration**

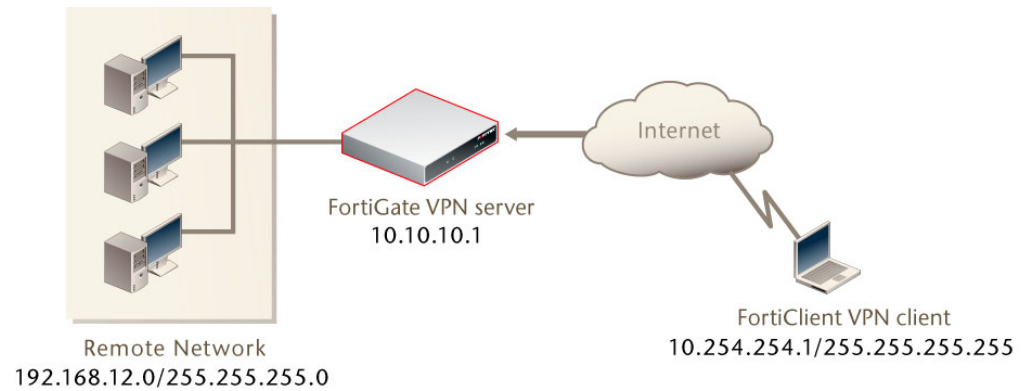
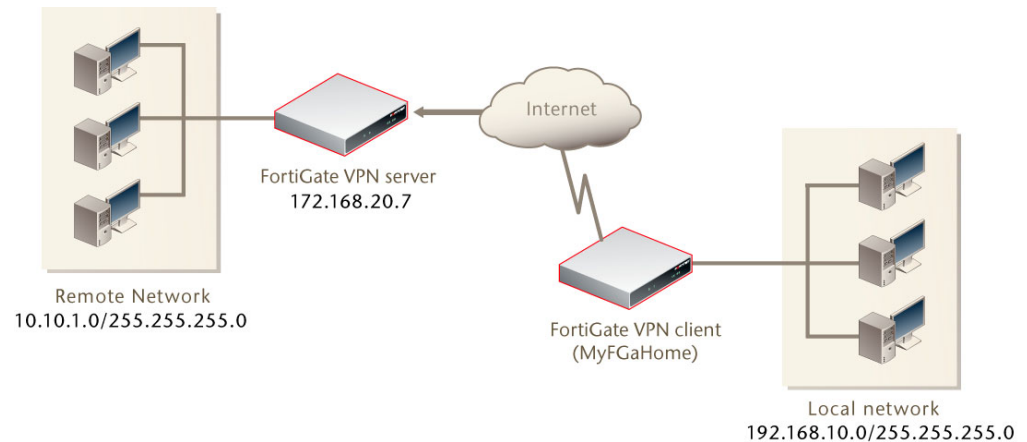


Figure 5 shows some example IP addresses for configuring a FortiGate VPN client.

**Figure 5: Example FortiGate VPN client configuration**



## Additional settings used to create secure connections

Several important settings are needed to create secure connections. To make sure that none of the required settings are missed, the FortiClient Host Security application and all FortiGate units come with most of the required settings ready—in other words, you do not have to change the majority of these settings. The following sections provide detailed information about the few settings that you have to adjust.

## Preshared keys

FortiGate VPN servers ensure that only authorized users gain access to private networks. One of the ways that a FortiGate VPN server controls access is by forcing VPN clients to supply a specific password before a tunnel can be established. In VPN terminology, the password is known as a “preshared key.” A preshared key contains at least 6 randomly chosen alphanumeric characters. You will need to add a preshared key to your VPN client configuration. You can get the preshared key from the person who manages the VPN server.

The same preshared key has to be added to the VPN client configuration and the VPN server configuration. When the client contacts the server to establish a tunnel, the client supplies its preshared key to the server. If the preshared key supplied by the client is identical to the preshared key in the server configuration, the server accepts the connection and access is permitted. If the preshared key supplied by the client is not identical to the preshared key in the server configuration, the server refuses the connection and access is denied.

## VPN client identifiers

In addition to checking preshared keys, a FortiGate VPN server may be configured to accept connections from:

- a FortiClient VPN client based on its virtual IP address
- a FortiGate VPN client based on its local ID

If your ISP account provides a dynamic IP address, you will need to add a virtual IP address or local ID to your VPN client configuration. Contact the person who manages the FortiGate VPN server to get a virtual IP address or local ID.

## IPsec settings

When a VPN server receives a connection request from VPN client, a secure connection is established in two distinct phases:

- in phase 1, the server authenticates the client
- in phase 2, the server establishes a VPN tunnel with the client

During both phases, the client and server exchange and compare a number of different IPsec settings to determine the best way to encode data. This process of negotiation is needed for the server to authenticate the client and determine whether the client is capable of creating a tunnel and encrypting/decrypting data in a way that complements the capabilities of the server.

The client must be capable of matching one of the methods used by the server to authenticate clients during phase 1 of the exchange. The client must also be capable of matching one of the methods used by the server to establish tunnels during phase 2 of the exchange. To ensure that a VPN server will be able to authenticate a VPN client and establish a tunnel, we assume that the person who manages the server will configure the phase 1 and phase 2 settings of the server to accept the phase 1 and phase 2 settings of the client. As long as the server administrator changes the settings in the server configuration, you will not have to make any changes to the client configuration.



**Note:** The default phase 1 and phase 2 encryption and authentication algorithms used by the FortiClient Host Security application are DES-MD5. The default phase 1 and phase 2 encryption and authentication algorithms used by FortiGate VPN clients and servers are 3DES-SHA1 and 3DES-MD5. To accept connections from FortiClient VPN clients, at least one of the settings on the FortiGate VPN server (for both phase 1 and phase 2) must be DES-MD5. For more information about FortiGate IPsec phase 1 and phase 2 settings, see the “Configuring IPsec VPNs” chapter of the [FortiGate Administration Guide](#).

A FortiGate VPN server uses its IPsec phase 1 settings to authenticate a VPN client. Then, if the connection is permitted, the FortiGate VPN server establishes a tunnel with the VPN client using its IPsec phase 2 settings.

### Schedule and service settings for FortiGate VPN clients

If you do not change any of the remaining settings, any type of data could be exchanged through an established tunnel at any time of the day or night. If needed, rules can be added to allow data to go into the tunnel according to a schedule, or permit the data associated with a particular service or services only through the tunnel. Rules like this can be added to a FortiGate VPN client’s firewall encryption policy.



**Note:** For detailed information about scheduling rules and how to allow/prevent certain types of data through a VPN tunnel, see the “Firewall Policy” chapter of the [FortiGate Administration Guide](#).

The basic firewall encryption policy settings on a FortiGate unit specify:

- on which FortiGate interface will data destined for the tunnel be received
- through which FortiGate interface will encrypted data be sent for delivery
- which IP addresses are associated with data that has to be encrypted and decrypted
- if the rules are applied according to a schedule
- if the rules are applied to certain types of data only

When the first packet of data meeting all of the conditions of the policy arrives at the FortiGate unit, a VPN tunnel may be initiated and the encryption/decryption of data is performed automatically afterward.

## Example VPNs

A VPN provides a secure way to transmit data over the Internet. Fortinet IPsec VPNs can be used to encrypt most Internet-based traffic. You can use an IPsec VPN to create a connection between a FortiClient client computer and the remote network behind a FortiGate unit (see “[Computer-to-private-network VPN](#)” on page 12). If you have a FortiGate unit, you can connect a local private network to a remote private network through a VPN (see “[Network-to-network VPN](#)” on page 12). FortiGate units provide enhanced security technology for private networks.

## Computer-to-private-network VPN

Let's say you want to work at home using your home computer, and you need to download a file from the private network at the office. The FortiClient Host Security application has been installed on your home computer, and the application has been configured with appropriate VPN settings, including a virtual IP address, the static public IP address of the FortiGate VPN server, and the static private IP address of the remote network behind the FortiGate VPN server.

Before you can access the remote network, you must first connect to the Internet through your ISP. Afterward, as long as the FortiClient Host Security application is running, the FortiClient software initiates a VPN tunnel with the FortiGate VPN server automatically. That is, as soon as you try to open a file on the remote network, the FortiGate VPN server authenticates the FortiClient VPN client and establishes a tunnel.

After the tunnel has been established, you can access the remote network and download the file as if your computer were connected to the remote network directly. The VPN configuration ensures that all data sent by your computer or retrieved from the remote network is processed securely.

To set up and use a VPN like the one described above, see [“Connecting to a remote network using FortiClient software” on page 13](#).

## Network-to-network VPN

Let's say you have a small business, and as part of that business, your employees frequently contact suppliers to order materials. You already have a FortiGate unit filtering and processing traffic (for example, email) on your private network.

For convenience, one of your suppliers has offered to provide your employees with direct access to the ordering system, as long as your employees place the orders through a VPN. The supplier will give you a special software application to install on your computers so that your employees can place the orders themselves. You can use the FortiGate unit that you already have to create the VPN.

Your FortiGate unit has been configured with appropriate VPN settings, including a local ID, the static public IP address of the supplier's VPN server, and the static private IP address of the remote network where the ordering system is located. Similarly, the supplier's VPN server has been configured with appropriate VPN settings, including the information it needs to authenticate your FortiGate unit.

To access the supplier's ordering system, all you have to do is start the supplier's ordering application. As soon as an order begins, your FortiGate unit intercepts the data and initiates a tunnel with the supplier's VPN server automatically. The VPN server authenticates your FortiGate unit and establishes a tunnel.

After the tunnel has been established, data can be exchanged between your computer and the remote ordering system as if your computer were connected to the supplier's network directly. The VPN configuration ensures that all ordering data transmitted between the two networks is filtered and processed securely.

To set up and use a VPN like the one described above, see [“Connecting to a remote network through a FortiGate unit” on page 21](#).

## Connecting to a remote network using FortiClient software

Using FortiClient software, you can connect your home computer to a remote network through a VPN.

The following procedure assumes that:

- You have used the web browser on your home computer to access public Internet sites.
- You already have the FortiClient Host Security application installed on your computer. If you need to install the software, see the “Installation” chapter of the [FortiClient User Guide](#).

### Before you begin

The settings in the FortiClient software have to correspond to the settings on the FortiGate VPN server. As long as the settings correspond, you will be able to access the remote network. To ensure that the settings correspond, confirm the following information with the person who manages the FortiGate VPN server:

- A preshared key will be assigned to the FortiClient software for authentication purposes (recommended).
- A virtual IP address will be assigned to the FortiClient software manually (recommended).
- The default FortiClient IPsec VPN settings will be used (recommended).



**Note:** If you will not be using the recommended settings, refer to the “FortiClient dialup-client configurations” section of the [FortiGate VPN Guide](#) if required for more information and detailed configuration instructions.

When you talk to the person who manages the FortiGate VPN server, ask for and write down the following information:

- What is the public IP address of the FortiGate VPN server?
- What is the private IP address and network mask of the remote network?
- What is the preshared key that the FortiClient software is to use?
- What is the virtual IP address and network mask to assign to the FortiClient software?

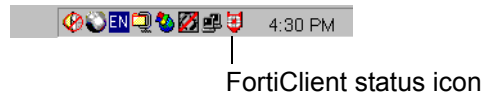
Keep this information confidential. You will need this information to complete the configuration procedure (see “[Configuring FortiClient software to connect to a FortiGate unit](#)” on page 14).

The person who manages the FortiGate unit may also give you the IP addresses of the Domain Name Service (DNS) server and/or Windows Internet Name Service (WINS) server on the remote network. DNS and WINS servers are computers that find the IP addresses of other computers whenever you send an email message or surf the Internet. You may need these settings to complete the FortiClient configuration.

## Starting the FortiClient Host Security application

After you install the FortiClient Host Security application, it continuously monitors activity on your computer. Normally, the application runs whenever your computer is powered on, and a FortiClient icon is displayed in the status bar (see [Figure 6](#)).

Figure 6: FortiClient status icon



If you do not see the FortiClient status icon in the lower-right corner of your computer monitor, you can start the application in either of the following ways:

- On the Windows Start menu, select **Programs > FortiClient > FortiClient**.
- On your desktop, double-click the FortiClient application icon (see [Figure 7](#)).

Figure 7: FortiClient application icon

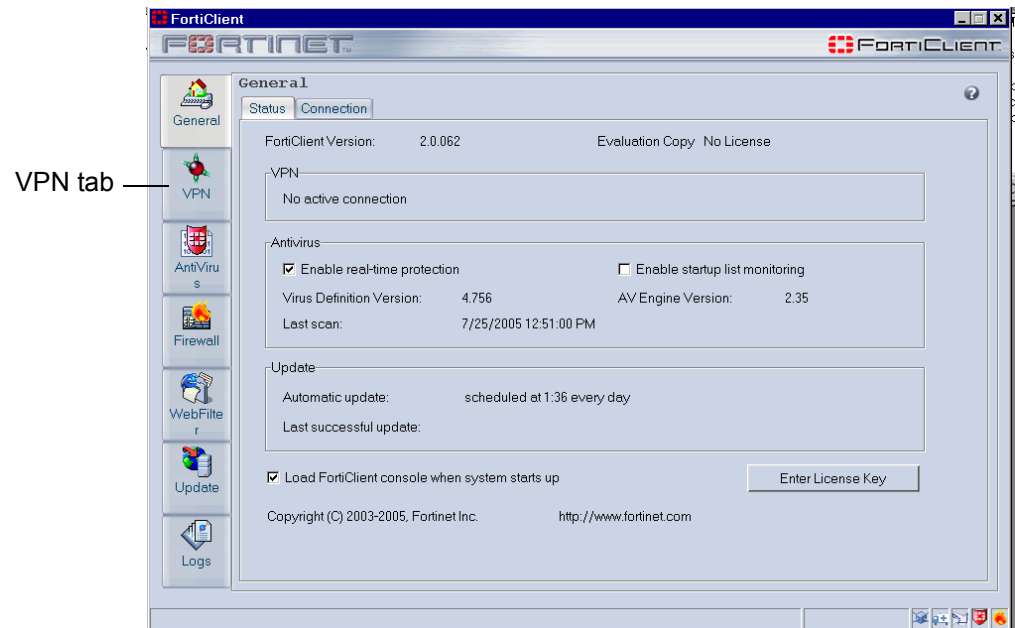


## Configuring FortiClient software to connect to a FortiGate unit

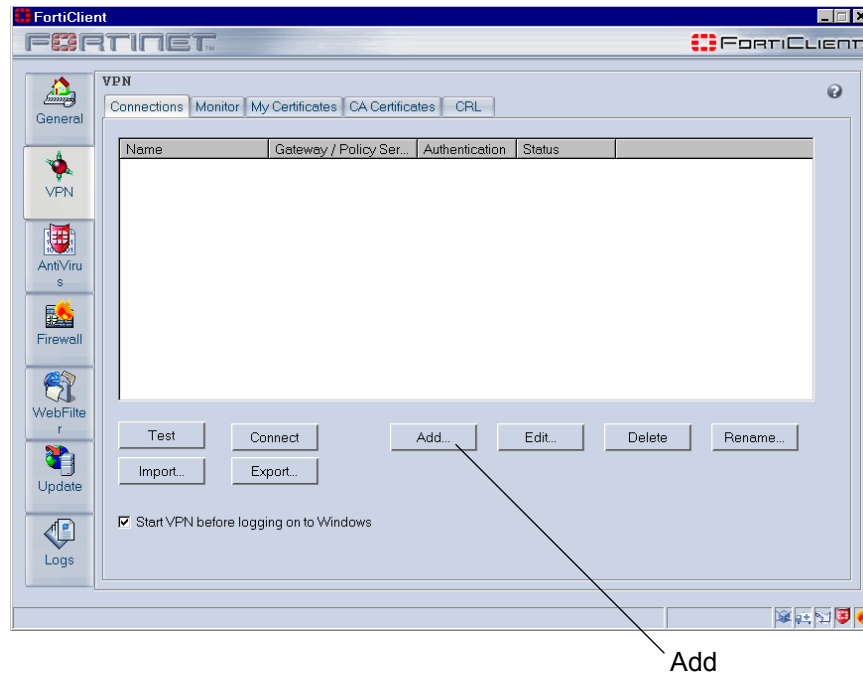
Follow these steps to configure the FortiClient Host Security application:

- 1 Open the FortiClient window: on your desktop, double-click the FortiClient icon in the status bar.

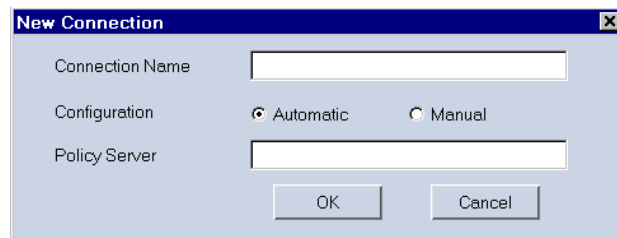
The FortiClient window is displayed.



- 2 Select the VPN tab.  
The Connections page is displayed.

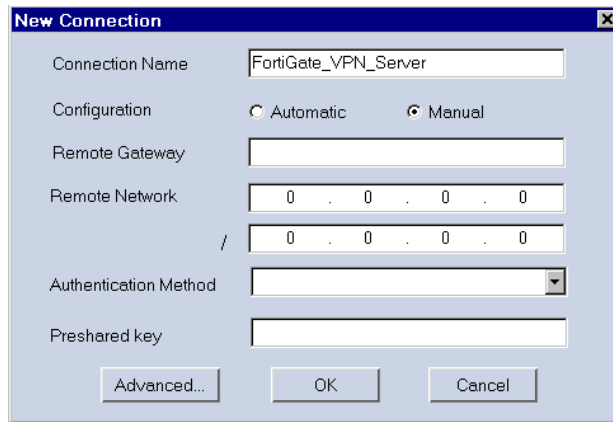


- 3 On the Connections page, select Add.  
The New Connection dialog is displayed.



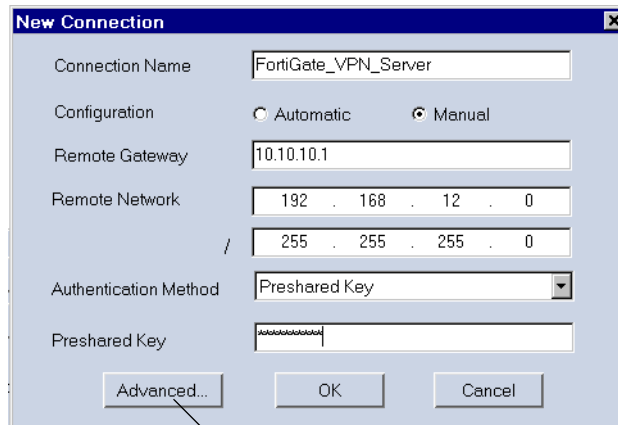
- 4 In the Connection Name field, type a name for the connection (for example, FortiGate\_VPN\_Server).

- 5 Select Manual.  
Additional options are displayed.



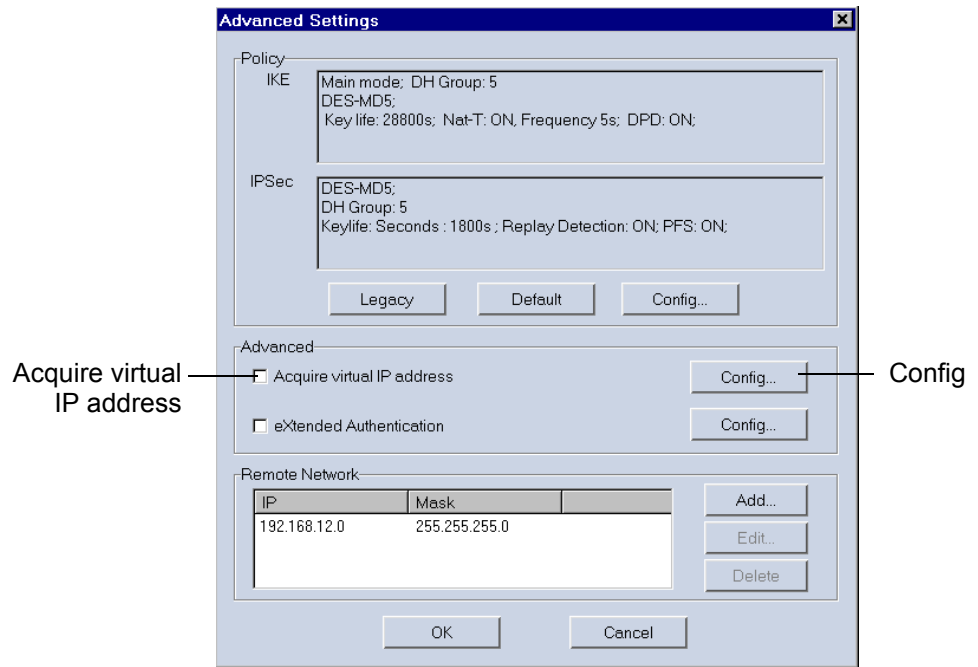
- 6 In the Remote Gateway field, type the public IP address of the FortiGate VPN server (for example, 10 . 10 . 10 . 1). Do not include a network mask.
- 7 In the Remote Network fields, type the private IP address and network mask of the network behind the FortiGate unit (for example, 192 . 168 . 12 . 0 / 255 . 255 . 255 . 0).
- 8 From the Authentication Method list, select Preshared key.
- 9 In the Preshared Key field, type the preshared key that the FortiClient software will use for authentication purposes.

At this point, your settings should look similar to the ones shown below:



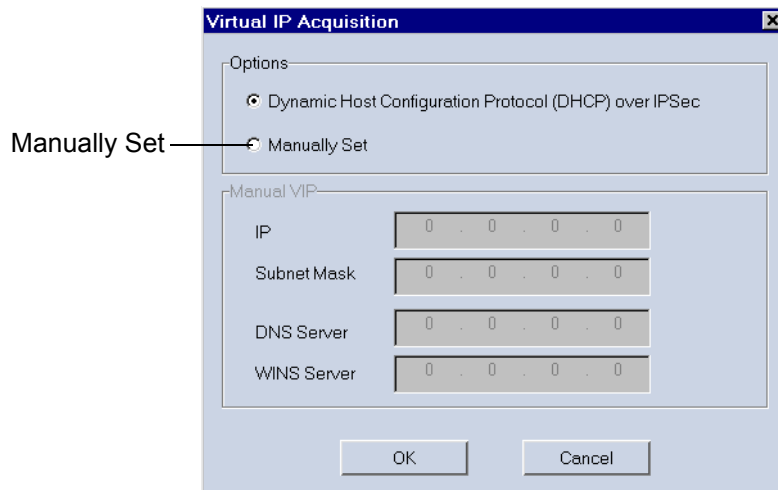
- 10 Select Advanced.

- 11 The Advanced Settings dialog is displayed.



- 12 Select Acquire virtual IP address and then select Config.

- 13 The Virtual IP Acquisition dialog is displayed.



- 14 Select Manually Set.

- 15** In the IP and Subnet Mask fields, enter the virtual IP address and network mask that has to be assigned to the FortiClient software (for example 10.254.254.1/255.255.255.255).

At this point, your settings should look similar to the ones shown below:

The screenshot shows a dialog box titled "Virtual IP Acquisition". It has two main sections: "Options" and "Manual VIP". In the "Options" section, there are two radio buttons: "Dynamic Host Configuration Protocol (DHCP) over IPsec" (which is unselected) and "Manually Set" (which is selected). The "Manual VIP" section contains four input fields: "IP" with the value "10 . 254 . 254 . 1", "Subnet Mask" with "255 . 255 . 255 . 255", "DNS Server" with "0 . 0 . 0 . 0", and "WINS Server" with "0 . 0 . 0 . 0". At the bottom of the dialog box are "OK" and "Cancel" buttons.

- 16** If the person who manages the FortiGate unit gave you an IP address for the DNS server and/or WINS server on the remote network, type the information into the DNS Server and/or WINS Server fields. You do not have to enter a network mask.
- 17** Select OK, and then select OK twice more to close the dialog boxes.
- 18** Test the connection. See [“To test the connection” on page 19](#).

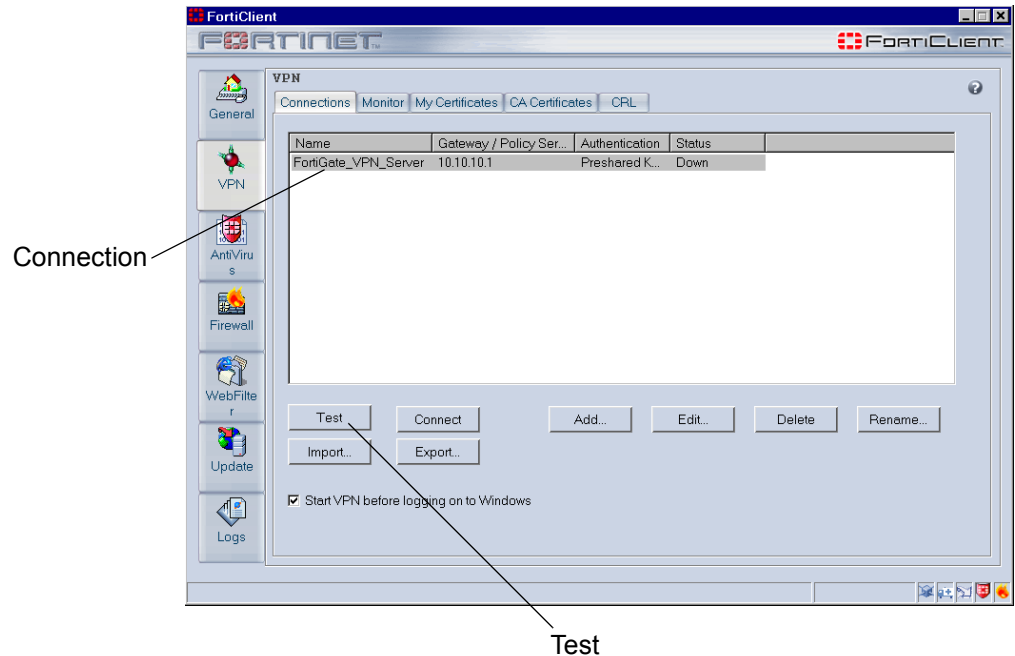


**Note:** Testing the connection does not establish a connection to the remote network. To connect to the remote network, see [“To connect to the remote network” on page 20](#).

### To test the connection

The following procedure assumes that the FortiGate VPN server is running and has been configured properly.

- 1 In the list of connections on the FortiClient Connections page, select the connection that you created:



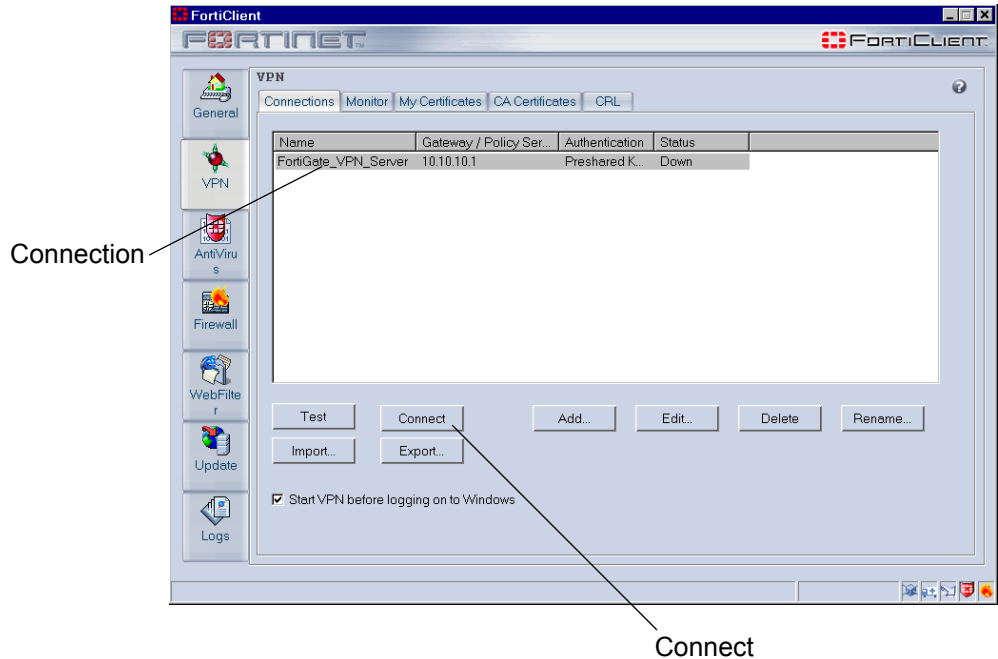
- 2 Select Test.

Status messages are displayed in the Test Connectivity window.

The FortiClient software will try to establish a connection with the FortiGate VPN server indefinitely. If a connection cannot be made, the most common problems are caused by mismatched IPsec phase 1 and phase 2 settings (see [“Additional settings used to create secure connections” on page 9](#)). Check all of the FortiClient settings carefully, and if you are unable to resolve the problem yourself, contact the FortiGate VPN server administrator at the remote site.

### To connect to the remote network

- 1 On the FortiClient Connections page, select the connection to the FortiGate VPN server.



- 2 Select Connect.  
The FortiClient software negotiates a connection with the FortiGate VPN server. When a connection is established, a "Negotiation Succeeded!" message is displayed. If you encounter problems, contact the FortiGate VPN server administrator at the remote site.
- 3 Select OK.  
You now have secure access to the remote network and can start working normally. For example, using a client application on your computer, you could connect to a server application on the remote network and download information.



**Note:** The resources that you are allowed to access using FortiClient software could be different compared to what you would be allowed to access if your computer were connected to the remote network directly. For details, contact the FortiGate VPN server administrator at the remote site.

When you no longer need to access the remote network, disconnect from the FortiGate VPN server as follows: on the FortiClient Connections page, select Disconnect.

## Connecting to a remote network through a FortiGate unit

If you have a FortiGate unit, you can connect your local private network to a remote private network through a VPN.

This procedure assumes that:

- Your FortiGate unit is installed and working properly. If you need to install the unit, see the [FortiGate Installation Guide](#).
- When the FortiGate unit is running, you can use any web browser on your local private network to access public Internet sites.

### Before you begin

The settings on your FortiGate unit and the settings on the remote FortiGate unit have to agree. As long as the settings agree, you will be able to access the remote network. To ensure that the settings correspond, confirm the following information with the person who manages the remote FortiGate unit:

- A preshared key will be assigned to your FortiGate unit for authentication purposes (recommended).
- A local ID will be assigned to your FortiGate unit (required if your ISP account provides a dynamic IP address).
- The default FortiGate IPsec VPN settings will be used (recommended).
- The IP addresses used by the computers on your private network do not match the IP addresses used by the computers on the private network behind the FortiGate VPN server (required).



**Note:** If your situation does not conform to the constraints listed above and your ISP account provides a dynamic IP address, refer to the “FortiGate dialup-client configurations” section of the [FortiGate VPN Guide](#) for more information and detailed configuration instructions. If your situation does not conform to the constraints listed above and your ISP account provides a static IP address, refer to the “Gateway-to-gateway configurations” section of the [FortiGate VPN Guide](#) instead.

When you talk to the person who manages the FortiGate VPN server, ask for and write down the following information:

- What is the public IP address of the remote FortiGate VPN server?
- What is the preshared key that your FortiGate unit is to use?
- What local ID is your FortiGate unit to use?
- What is the private IP address and network mask of the remote network?

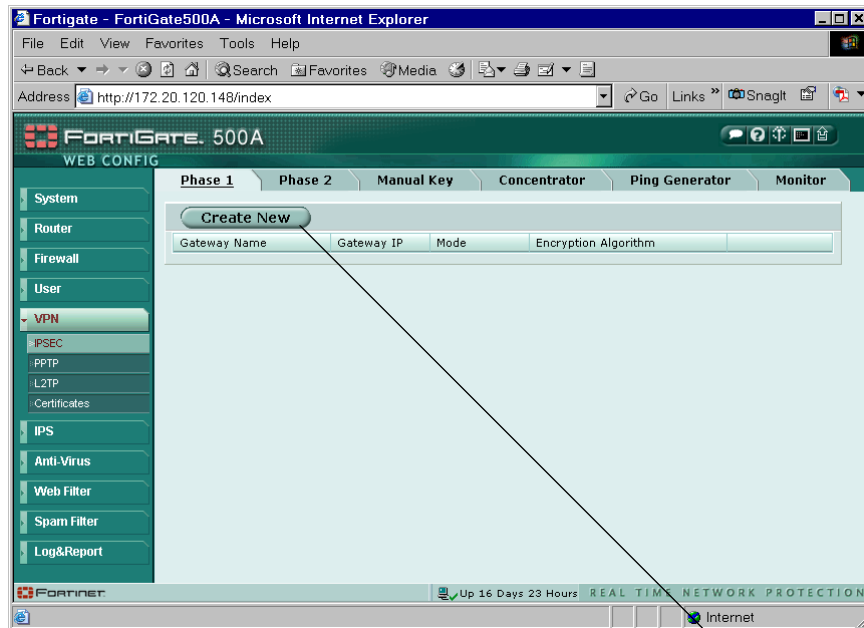
Keep this information confidential.

In addition, both you and the remote administrator will need to know the private IP address and network mask of the network behind your FortiGate unit. In addition, if your ISP account provides a static IP address for your FortiGate unit, tell the remote administrator what the IP address is. If you do not know the IP address, you can get the address from your ISP.

## Configuring your FortiGate unit to connect to the remote network

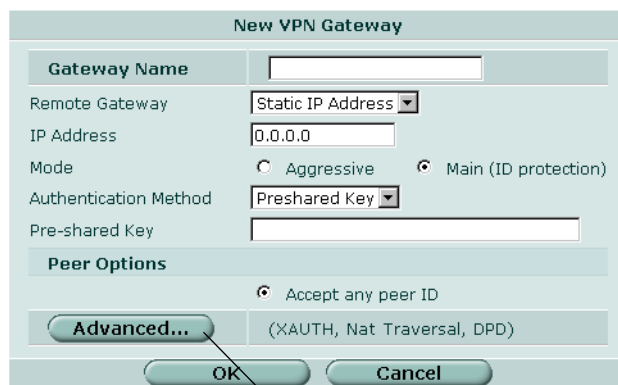
Use the web-based manager to configure your FortiGate unit. Keep the default settings unless the following procedure specifically instructs you to modify a setting. You can use this procedure to configure FortiGate VPN clients that have static or dynamic IP addresses.

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



Create New

- 2 On the Phase 1 page, select Create New.  
The New VPN Gateway dialog is displayed.



Advanced

**3** Select Advanced.

Advanced options are displayed. The only advanced option that you need to set is the Local ID field. Do not change any of the other advanced option settings.

The screenshot shows the 'New VPN Gateway' configuration window. The 'Advanced...' button is highlighted, and the 'Advanced' section is expanded, showing options for P1 Proposal, DH Group, Keylife, Local ID, XAuth, Nat-traversal, Keepalive Frequency, and Dead Peer Detection.

| New VPN Gateway                                     |  |
|---|--|
| Gateway Name  | <input type="text"/>   |
| Remote Gateway                                      | Static IP Address  |
| IP Address  | <input type="text" value="0.0.0.0"/>   |
| Mode  | <input type="radio"/> Aggressive <input checked="" type="radio"/> Main (ID protection)                                 |
| Authentication Method                               | Preshared Key  |
| Pre-shared Key                                      | <input type="text"/>   |
| <b>Peer Options</b>                                 |  |
| <input checked="" type="radio"/> Accept any peer ID |  |
| <b>Advanced...</b> (XAUTH, Nat Traversal, DPD)      |  |
| <b>P1 Proposal</b>                                  |  |
| 1 - Encryption                                      | 3DES Authentication SHA1   |
| 2 - Encryption                                      | 3DES Authentication MD5  |
| DH Group  | 1 <input type="checkbox"/> 2 <input type="checkbox"/> 5 <input checked="" type="checkbox"/>                            |
| Keylife   | <input type="text" value="28800"/> (120-172800 seconds)  |
| Local ID  | <input type="text"/> (optional)  |
| XAuth   | <input checked="" type="radio"/> Disable <input type="radio"/> Enable as Client <input type="radio"/> Enable as Server |
| Nat-traversal                                       | <input checked="" type="checkbox"/> Enable   |
| Keepalive Frequency                                 | <input type="text" value="5"/> (0-900 seconds)   |
| Dead Peer Detection                                 | <input checked="" type="checkbox"/> Enable   |
| OK Cancel   |  |

**4** Enter the following information:

|                              |   |
|------------------------------|---|
| <b>Gateway Name</b>          | Type a name that represents the remote FortiGate unit (for example, FG_Site1).  |
| <b>Remote Gateway</b>        | Static IP Address   |
| <b>IP Address</b>            | Type the public IP address of the remote FortiGate unit (for example, 172.168.20.7).  |
| <b>Mode</b>                  | Aggressive  |
| <b>Authentication Method</b> | Preshared Key   |
| <b>Pre-shared Key</b>        | Type the preshared key. The same characters must be recorded in the remote VPN server configuration. The key must contain at least 6 printable characters. For optimum protection, the key should consist of a minimum of 16 randomly chosen alphanumeric characters. |
| <b>Local ID</b>              | Type the identifier that belongs to your FortiGate unit (for example, MyFGaHome).   |

Your settings should look similar to the settings shown below:

**New VPN Gateway**

**Gateway Name** FG\_Site1

Remote Gateway Static IP Address

IP Address 172.168.20.7

Mode  Aggressive  Main (ID protection)

Authentication Method Preshared Key

Pre-shared Key \*\*\*\*\*

**Peer Options**

Accept any peer ID

**Advanced...** (XAUTH, Nat Traversal, DPD)

**P1 Proposal**

1 - Encryption 3DES Authentication SHA1

2 - Encryption 3DES Authentication MD5

DH Group 1  2  5

Keylife 28800 (120-172800 seconds)

Local ID MyFGaHome (optional)

XAuth  Disable  Enable as Client  Enable as Server

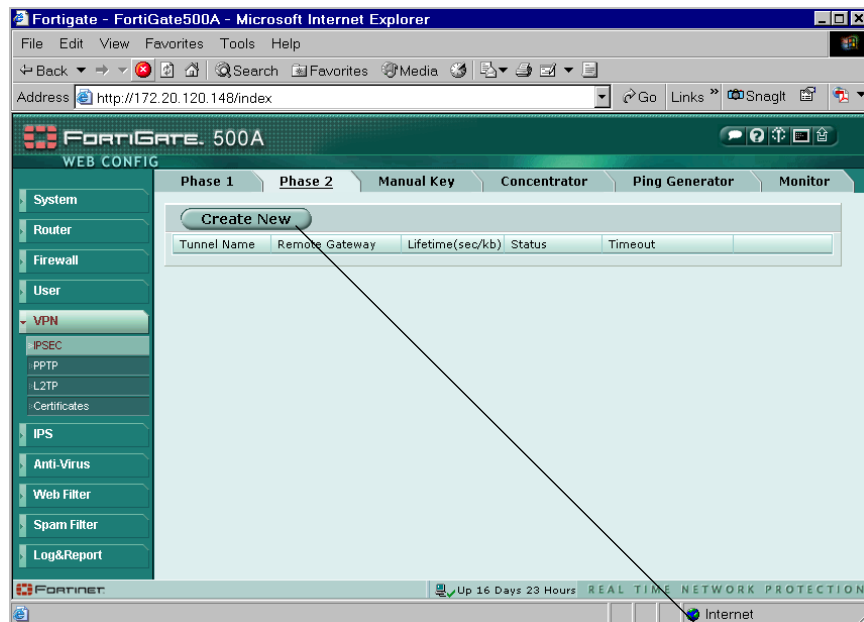
Nat-traversal  Enable

Keepalive Frequency 5 (0-900 seconds)

Dead Peer Detection  Enable

OK Cancel

- 5 Select OK.
- 6 Go to **VPN > IPSEC > Phase 2**.



Create New

- 7 On the Phase 2 page, select Create New.  
The New VPN Tunnel dialog is displayed.

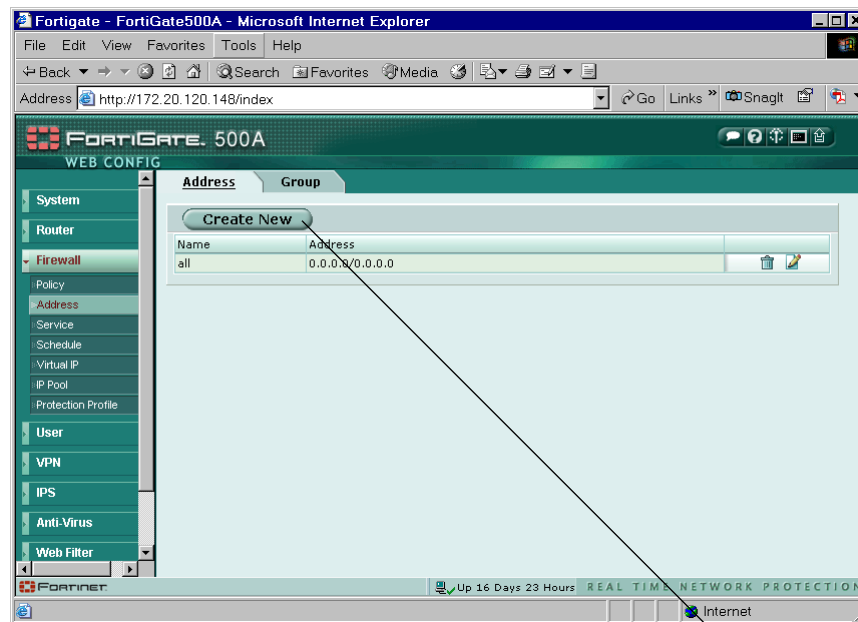
- 8 Enter the following information:

**Tunnel Name** Enter a name for the phase 2 tunnel (for example, Tunnel\_to\_FG\_Site1).

**Remote Gateway** Select the name of the phase 1 gateway that you defined in Step 4 (for example, FG\_Site1).

Your settings should look similar to the settings shown below:

- 9 Select OK.
- 10 Go to **Firewall > Address**.



Create New

- 11 On the Address page, select Create New.  
The New Address dialog is displayed. You will enter information that corresponds to the private network behind the FortiGate VPN server.

- 12 Enter the following information:

**Address Name** Enter an address name (for example, Remote\_network).

**IP Range/Subnet** Enter the private IP address and network mask of the network behind the FortiGate VPN server (for example, 10.10.1.0/255.255.255.0).

Your settings should look similar to the settings shown below:

- 13 Select OK.
- 14 Select Create New again to create a second address. You will enter information that corresponds to your local private network.
- 15 In the New Address dialog, enter the following information, and then select OK:

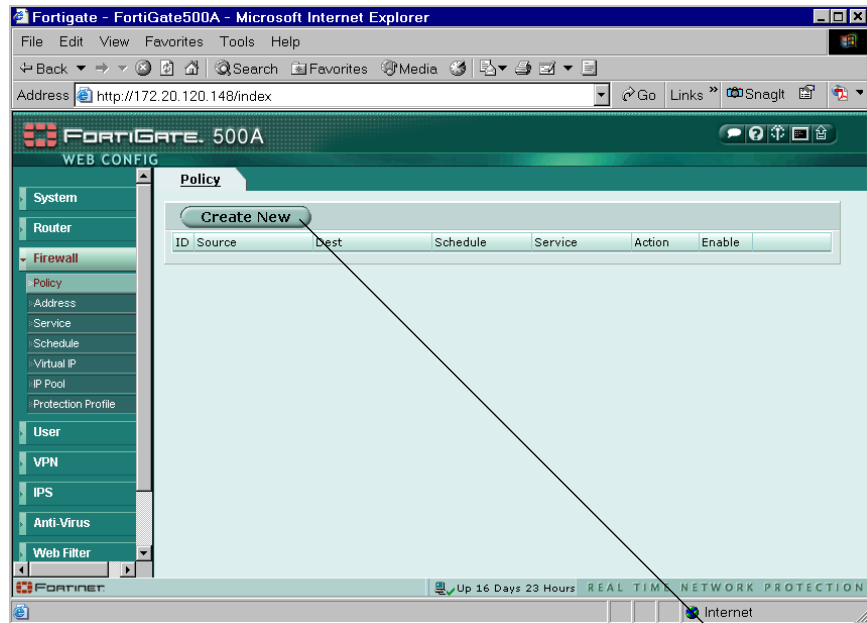
**Address Name** Enter an address name (for example, Local\_network).

**IP Range/Subnet** Enter the private IP address and network mask of the network behind your FortiGate unit (for example, 192.168.10.0/255.255.255.0).

At this point, the settings in the Address list should look similar to the settings shown below:

| Create New     |                            |  |
|----------------|----------------------------|--|
| Name           | Address                    |  |
| all            | 0.0.0.0/0.0.0.0            |  |
| Remote_network | 10.10.1.0/255.255.255.0    |  |
| Local_network  | 192.168.10.0/255.255.255.0 |  |

## 16 Go to Firewall &gt; Policy.



Create New

## 17 Select Create New.

- 18 The New Policy dialog is displayed. In the image shown below, the names of the options in the Interface/Zone fields correspond to a FortiGate-500A unit. If you have a different FortiGate model, your interface names may be different.

 The 'New Policy' dialog box is displayed with the following configuration:
 

- Source:** Interface/Zone: lan; Address Name: ----- Address -----
- Destination:** Interface/Zone: port1; Address Name: ----- Address -----
- Schedule:** always
- Service:** ANY
- Action:** ACCEPT
- NAT
- Dynamic IP Pool
- Fixed Port
- Protection Profile: strict
- Log Traffic
- Advanced...** (Authentication, Traffic Shaping, Differentiated Services)

 At the bottom of the dialog are 'OK' and 'Cancel' buttons.

**19** Enter the following information:

- Source**
  - Interface/Zone Select the interface that connects your FortiGate unit to the local private network (for example, `internal` or `port1`).
  - Address Name Select `Local_network`.
- Destination**
  - Interface/Zone Select the interface that connects your FortiGate unit to the Internet (for example, `external`, `wan1`, or `port2`).
  - Address Name Select `Remote_network`.
- Schedule** As required.
- Service** As required.
- Action** Select `ENCRYPT`.
- VPN Tunnel** `Tunnel_to_FG_Site1`

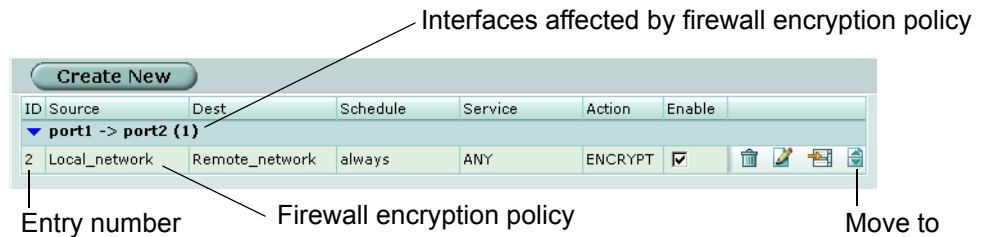
The settings in the New Policy dialog should look similar to the settings shown below:

The screenshot shows the 'New Policy' dialog box with the following settings:

- Source**
  - Interface/Zone: port1
  - Address Name: Local\_network
- Destination**
  - Interface/Zone: port2
  - Address Name: Remote\_network
- Schedule**: always
- Service**: ANY
- Action**: ENCRYPT
- VPN Tunnel**: Tunnel\_to\_FG\_Site1
- Allow inbound,  Inbound NAT
- Allow outbound,  Outbound NAT
- Protection Profile: strict
- Log Traffic
- (Traffic Shaping, Differentiated Services)

**20** Select OK.

- 21 In the Policy list, locate the firewall encryption policy that you just created. Clicking the blue arrows in the Policy list displays the firewall policies that have been assigned to FortiGate interfaces. In the example list shown below, one firewall encryption policy similar to the one defined in the preceding steps is shown.



- 22 In your situation, if more than one policy has been created for the same interfaces affected by the firewall encryption policy, you must move the firewall encryption policy to the top of the list. To move the firewall encryption policy to the top of the list:

- Note the entry number of the top-most entry in the list.
- In the row that corresponds to the firewall encryption policy, select the Move to icon.

The Move Policy dialog is displayed.

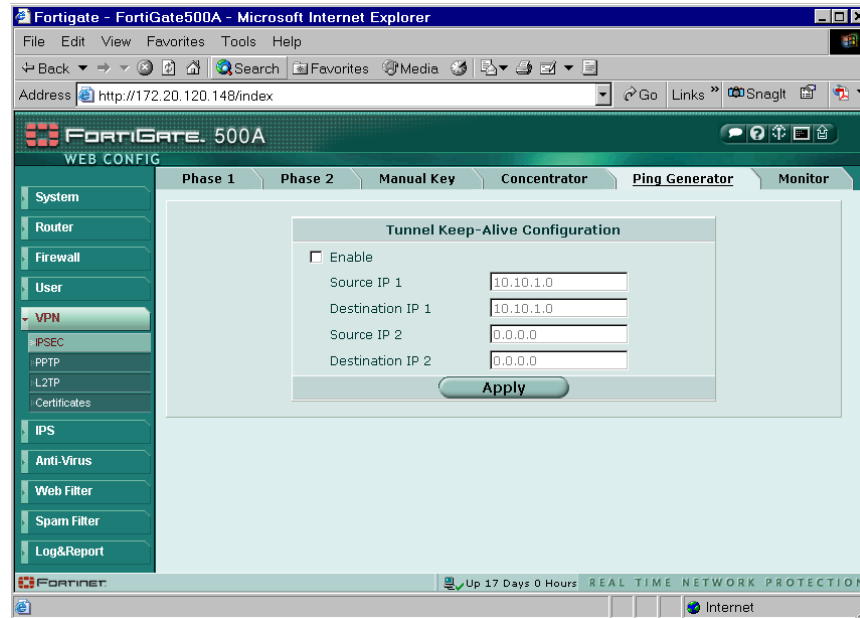


- In the Move to field, type the number of the top-most entry in the list.
- Select OK.
- Verify that the entry corresponding to the firewall encryption policy is now the top-most entry in the list.

**To test the connection**

The following procedure assumes that the FortiGate VPN server is running and has been configured properly.

- 1 Go to **VPN > IPSEC > Ping Generator**.



- 2 In the Tunnel Keep-Alive Configuration dialog, select Enable.
- 3 In the Source IP 1 field, type the IP address of any computer that is located on the private network behind your FortiGate unit (for example, 192.168.10.1).
- 4 In the Destination IP 1 field, type the IP address of any computer that is located on the private network behind the remote FortiGate unit (for example, 10.10.1.1).
- 5 Select Apply.
- 6 Go to **VPN > IPSEC > Monitor**.

When a VPN has been established, the display shows you information about the VPN connection between your FortiGate unit and the remote FortiGate unit. In the figure shown below, all connections are down. To initiate a connection, select the red Bring up tunnel icon that applies to your configuration.

**Figure 8: Example tunnel status information**

| 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

If you encounter problems, refer to the “Monitoring and Testing VPN Tunnels” chapter in the *FortiGate VPN Guide*. Enabling and viewing log messages may help you to resolve the problem. If you are unable to resolve the problem yourself, contact the administrator of the remote FortiGate unit for help.

## For more information

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>.

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>.

