Connecting to a Remote Network

Technical Note

Connecting to a Remote Network Technical Note	
Document Version:	Version 1
Publication Date:	6 September 2005
Description:	This technical note describes how to connect to a remote network through a VPN using the FortiClient Host Security application. It also describes how to configure a FortiGate unit to create a VPN to a remote network.
Product:	FortiGate v2.80 MR10 and FortiClient v2.0
Document Number:	01-28010-0235-20050906

Fortinet Inc.

Connecting to a Remote Network Technical Note
FortiGate v2.80 MR10 and FortiClient v2.0
6 September 2005
01-28010-0235-20050906

Table of Contents

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.

- If you want to connect to the remote network using FortiClient software, see "How to connect to the remote network using FortiClient software" below.
- If you need to connect to the remote network through a FortiGate unit instead, see "How to connect to the remote network through a FortiGate unit" on page 7.

How to connect to the remote network using FortiClient software

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

The following procedure assumes that:

- You have used the web browser on your 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 unit. As long as the settings correspond, you will be able to access the remote network using FortiClient software. To ensure that the settings correspond, confirm the following information with the person who manages the FortiGate unit:

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

Note: By default, the phase 1 and phase 2 encryption and authentication algorithms used by FortiClient are DES-MD5. The person who manages the FortiGate unit should be made aware that the phase 1 and phase 2 settings on the FortiGate unit have to be configured to accept your FortiClient settings. If you will not be using the recommended settings, refer to the "FortiClient dialup-client configurations" section of the *FortiGate VPN Guide* for more information and detailed configuration instructions.

When you talk to the person who manages the FortiGate unit, ask for the following information:

- What is the public IP address of the FortiGate unit?
- 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?

You will need this information to complete the following procedure. The person who manages the FortiGate unit may also give you some additional information.

To configure FortiClient software to connect to a FortiGate unit

1. Start the FortiClient Host Security application.
2. Go to **VPN > Connections** and select Add.
3. In the Connection Name field, type a name for the connection.
4. Select Manual.
5. In the Remote Gateway field, type the public IP address of the FortiGate unit. Do not include a network mask.
6. In the Remote Network fields, type the private IP address and network mask of the network that you want to access (for example, `192.168.12.0/255.255.255.0`).
7. From the Authentication Method list, select Preshared key.
8. In the Preshared Key field, type the preshared key that the FortiClient software is to use.
9. Select Advanced.
10. Under Advanced in the Advanced Settings dialog box, select Acquire virtual IP address and then select Config.
11. Under Options in the Virtual IP Acquisition dialog box, select Manually Set.
12. In the IP and Subnet Mask fields, enter the VIP address and netmask that has to be assigned to the FortiClient software.
13. Select OK, and then select OK twice more to close the dialog boxes.
14. Test the connection. See "To test the connection" on page 7.

To test the connection

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” below.

1. In the list of connections, 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 unit indefinitely. If a connection cannot be made, the most common problems are caused by mismatched IPSec phase 1 and phase 2 settings. Check all of the FortiClient settings carefully, and if you are unable to resolve the problem yourself, contact the FortiGate administrator at the remote site.

To connect to the remote network

1. With the FortiClient Host Security application running, go to **VPN > Connections** and select Connect.

   The FortiClient software negotiates a connection with the FortiGate unit. When a connection is established, a “Negotiation Succeeded!" message is displayed. If you encounter problems, contact the FortiGate administrator at the remote site.
2. Select OK.

   You now have direct 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 administrator at the remote site.

When you no longer need to access the remote network, disconnect from the FortiGate unit as follows: with the FortiClient Host Security application running, go to **VPN > Connections** and select Disconnect.

How to connect to the remote network through a FortiGate unit

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

This procedure assumes that:

- Your FortiGate unit is installed and working correctly. 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 through a VPN. 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).
- An identifier will be assigned to your FortiGate unit to help the remote administrator monitor VPN connections (recommended).
- 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 address space used by the private network behind the remote FortiGate unit (mandatory).

Note: If your situation does not conform to the constraints listed above, refer to the "FortiGate dialup-client configurations" section of the *FortiGate VPN Guide* for more information and detailed configuration instructions.

When you talk to the person who manages the remote FortiGate unit, ask for the following information and keep the information confidential:

- What is the public IP address of the remote FortiGate unit?
- What is the preshared key that your FortiGate unit is to use?
- What identifier is your FortiGate unit to use?
- What is the private IP address and network mask of the network behind the remote FortiGate unit?

In addition, both you and the remote administrator will need to know the IP address and network mask of the private network behind your FortiGate unit.

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 instructs you to modify a setting.

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

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

Gateway Name	Type a name that represents the remote FortiGate unit (for example, `FG_Site1`).
Remote Gateway	Static IP Address
IP Address	Type the public IP address of the remote FortiGate unit.
Mode	Aggressive
Authentication Method	Preshared Key
Pre-shared Key	Type the preshared key.
Advanced	In the Local ID field, type the identifier that belongs to your FortiGate unit.

3 Go to **VPN > IPSEC > Phase 2**.

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

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 2 (for example, `FG_Site1`).

5 Go to **Firewall > Address**.

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

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 remote FortiGate unit (for example, `10.10.1.0/24`).

7 Go to **Firewall > Address**.

8 Select Create New, enter the following information, and 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, `192.168.10.0/24`).

9 Go to **Firewall > Policy**.

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

Interface/Zone	Source Select the interface that connects your FortiGate unit to the local private network (for example, `internal`). Destination Select the interface that connects your FortiGate unit to the Internet (for example, `external` or `wan1`).

Address Name	Source
	`Local_network`
	Destination
	`Remote_network`

Action	ENCRYPT
VPN Tunnel	`Tunnel_to_FG_Site1` Clear Allow inbound.

11 Place the policy in the policy list above all other policies that apply to the same source and destination interfaces.

To test the connection

The remote FortiGate unit must be configured and running properly.

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

2 Select Enable.

3 In the Source IP 1 field, type the IP address of any computer that resides on the private network behind your FortiGate unit (for example, `192.168.10.1`).

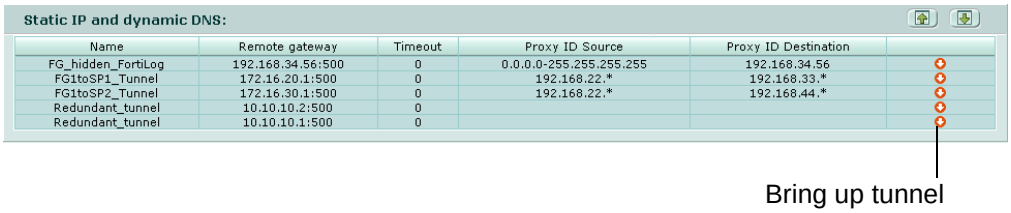
4 In the Destination IP 1 field, type the IP address of any computer that resides on the private network behind the remote FortiGate unit (for example, `10.10.1.1`).

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 1: Example tunnel status information



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.