FortiClient Internet-browsing IPSec VPN Example

Technical Note

FortiClient Internet-browsing IPSec VPN Example Technical Note	
Document Version:	Version 1
Publication Date:	20 June 2005
Description:	This technical note features a detailed configuration example that 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 Virtual IP (VIP) address through FortiGate DHCP relay.
Product:	FortiGate v2.80 MR10 and FortiClient 1.2 MR3
Document Number:	01-28010-0135-20050620

Fortinet Inc.

FortiClient Internet-browsing IPSec VPN Example Technical Note
FortiGate v2.80 MR10 and FortiClient 1.2 MR3
20 June 2005
01-28010-0135-20050620

Table of Contents

FortiClient Internet-browsing IPSec VPN Example

This technical note features a detailed configuration example that 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 Virtual IP (VIP) address through FortiGate DHCP relay. The following sections are included:

- Network topology
- Configuring FortiGate_1
- Configuring the FortiClient Host Security application

Network topology

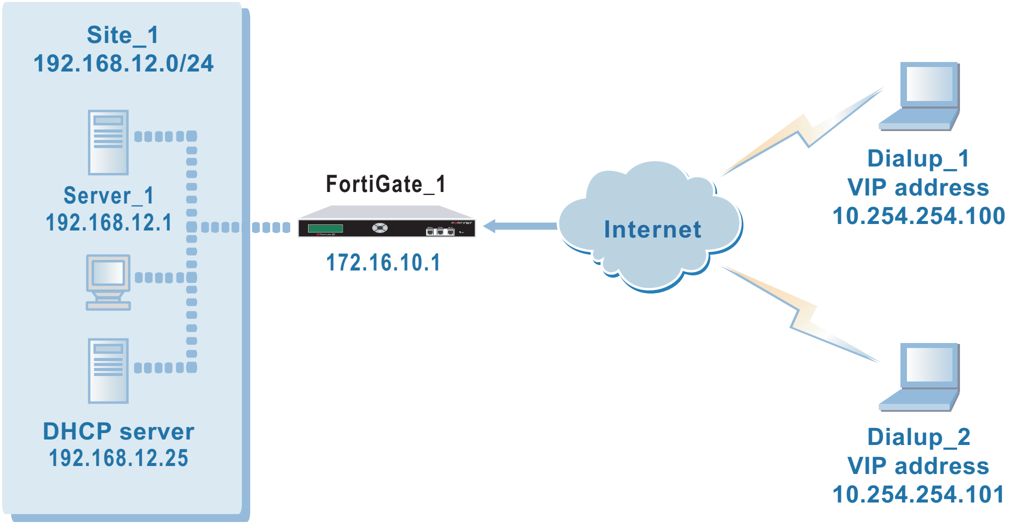
Internet-browsing configurations are based on dialup-client configurations. In a dialup-client configuration, remote hosts running VPN client software such as the FortiClient Host Security application are assigned dynamic IP addresses through an ISP before the VPN client initiates a connection to a FortiGate dialup server.

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. For more information, see the *FortiGate VPN Guide*.

As a precaution to prevent IP-address overlap between the remote host and the private network behind the FortiGate unit, FortiClient dialup clients may be configured to acquire uncommonly used VIP addresses through the FortiGate DHCP relay feature: the FortiClient Host Security application is configured to broadcast a DHCP request to the FortiGate unit, and the FortiGate unit is configured to relay the DHCP request to a DHCP server behind the FortiGate unit. The DHCP server is configured to respond with a VIP address for the dialup client.

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 1.

Figure 1: Example FortiClient Internet-browsing configuration



When Internet browsing is enabled on the FortiGate unit, dialup clients can access the private network behind the FortiGate unit and browse the Internet as if they were part of the private network behind the FortiGate unit. Packets from dialup clients are decrypted, subjected to the firewall policy for the private network, and sent back out the FortiGate interface that has Internet access. The VIP address of the FortiClient dialup client is used as the source address for all traffic generated by the dialup client inside the tunnel.

In the example configuration:

- Private IP addresses are used for both private and public IP addresses.
- VIP addresses that are not commonly used (in this case, 10.254.254.0/24) are assigned to the FortiClient dialup clients.
- The dialup clients are provided access to Server_1 at IP address 192.168.12.1 behind FortiGate_1.
- The other network devices are assigned IP addresses as shown in Figure 1.
- Inbound NAT is enabled in the firewall encryption policy on the FortiGate unit. Inbound NAT translates the source IP addresses of inbound decrypted packets into the IP address of the FortiGate internal interface.
- A DHCP server (192.168.12.25/32) is available on the network behind the FortiGate unit. The DHCP server has been configured to supply VIP addresses to the dialup clients.

Before you begin

Before you begin, determine which VIP addresses to use and add them to the DHCP server that resides on the network behind the FortiGate unit (follow the software supplier’s documentation).

Configuring FortiGate_1

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

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

- Define the phase 1 parameters that the FortiGate unit needs to authenticate the dialup clients and establish a secure connection. See "Define the phase 1 parameters" on page 7.
- Define the phase 2 parameters that the FortiGate unit needs to create a VPN tunnel and enable all dialup clients having VIP addresses on the 10.254.254.0/24 network to connect using the same tunnel definition. See "Define the phase 2 parameters" on page 8.
- Create a firewall encryption policy to control the permitted services and permitted direction of traffic between the IP source address and the dialup clients. A single encryption policy controls both inbound and outbound IP traffic through the VPN tunnel. See "Define the firewall encryption policy" on page 8.
- Configure the FortiGate unit to relay DHCP requests from dialup clients to the DHCP server. See "Configure FortiGate_1 to relay DHCP requests" on page 9.

Define the phase 1 parameters

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

Before you define the phase 1 parameters, you need to:

- Reserve a name for the phase 1 configuration.
- Reserve a unique value for the preshared key.

The key must contain at least 6 printable characters and should only be known by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.

To define the phase 1 parameters

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

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

Gateway Name	Type a name for the remote gateway (for example, `Dialup_clients`).
Remote Gateway	Dialup User
Mode	Main

Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID

Define the phase 2 parameters

The basic phase 2 settings associate IPSec phase 2 parameters with the phase 1 configuration and specify the remote end point of the VPN tunnel. Before you define the phase 2 parameters, you need to reserve a name for the tunnel.

To define the phase 2 parameters

1 Go to **VPN > IPSEC > Phase 2** and select Create New.

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

Tunnel Name	Enter a name for the tunnel (for example, `FG1toDialupClients`).
Remote Gateway	Select the gateway that you defined previously (for example, `Dialup_clients`).
Advanced	Select DHCP-IPsec Enable, and then from the Internet browsing list, select the interface that connects the FortiGate unit to the local private network.

3 Enter the following CLI command to enable all dialup clients having VIP addresses on the 10.254.254.0/24 network to connect using the same phase 2 tunnel definition:

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

Define the 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. A single encryption policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

Before you define the policy, you must first specify the IP source address. The IP source address corresponds to the private IP address of Server_1 behind the FortiGate unit (for example, 192.168.12.1/32).

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

To define the private IP address of Server_1 behind FortiGate_1

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

Address Name	Enter an address name (for example, `Server_1`).
IP Range/Subnet	Enter the private IP address of the server (for example `192.168.12.1/32`).

To define the firewall encryption policy

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

Interface/Zone	Source Select the interface to the internal (private) network. Destination Select the interface to the external (public) network.

Address Name	Source
	`Server_1`
	Destination
	`all`

Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	Select `FG1toDialupClients`, and then select Inbound NAT to translate the IP source addresses of inbound decrypted packets into the IP address of the FortiGate interface to the private network.

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

Configure FortiGate_1 to relay DHCP requests

In the example configuration, dialup clients obtain VIP addresses through FortiGate DHCP relay. To provide dialup clients with VIP addresses, you configure the FortiGate unit to relay client DHCP requests to a DHCP server on the network behind the FortiGate unit.

To configure the FortiGate unit to relay DHCP requests

1. Go to **System > DHCP > Service**.
2. In the list of interfaces, select the Edit button that corresponds to the interface to the Internet.
3. Select DHCP Relay Agent, and then select IPSEC.
4. In the DHCP Server IP field, type the IP address of the DHCP server that resides on the network behind the FortiGate unit (for example, `192.168.12.25`).
5. Select OK.

Configuring the FortiClient Host Security application

The following procedure explains how to configure the FortiClient Host Security application to connect to FortiGate_1 and broadcast a DHCP request. The dialup client uses the acquired VIP address as its IP source address for the duration of the connection. To complete the Internet-browsing configuration, you configure FortiClient to force all IP traffic through the VPN tunnel.

To configure FortiClient

1. At the remote host, start FortiClient.
2. Go to **VPN > Connections** and select Add.
3. In the Connection Name field, type a descriptive name for the connection.
4. In the Remote Gateway field, type the public static IP address of the FortiGate unit.
5. In the Remote Network fields, type the private IP address and netmask of the server that FortiClient needs to access behind the FortiGate unit (for example, `192.168.12.1/255.255.255.255`).
6. From the Authentication Method list, select Preshared Key.
7. In the Preshared Key field, type the preshared key. The value must be identical to the preshared key that you specified previously in the FortiGate_1 configuration.
8. Select Advanced.
9. In the Advanced Settings dialog box, select Acquire virtual IP address and then select Config.
10. Verify that the Dynamic Host Configuration Protocol (DHCP) over IPSec option is selected, and then select OK.
11. In the Remote Network group, select Add.
12. 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.
13. Select OK twice to close the dialog boxes.
14. Exit FortiClient and repeat this procedure at all other remote hosts.