Authenticating FortiClient Dialup Clients

Technical Note

Authenticating FortiClient Dialup Clients Technical Note	
Document Version:	Version 4
Publication Date:	27 October 2005
Description:	This technical note explains how to configure VPN settings and FortiClient dialup clients using preshared keys, local IDs, and user groups as authentication components. Multiple dialup VPN clients having different authentication settings can connect to the same FortiGate IPSec VPN tunnel.
Product:	FortiGate v2.80 MR11 and FortiClient v1.2 MR3
Document Number:	01-28011-0064-20051027

Fortinet Inc.

Authenticating FortiClient Dialup Clients Technical Note
FortiGate v2.80 and FortiClient v1.2 MR3
27 October 2005
01-28011-0064-20051027

Table of Contents

This technical note explains how to configure VPN settings and FortiClient dialup clients using preshared keys, local IDs, and user groups as authentication components. Multiple dialup VPN clients having different authentication settings can connect to the same FortiGate IPSec VPN tunnel.

The following topics are included:

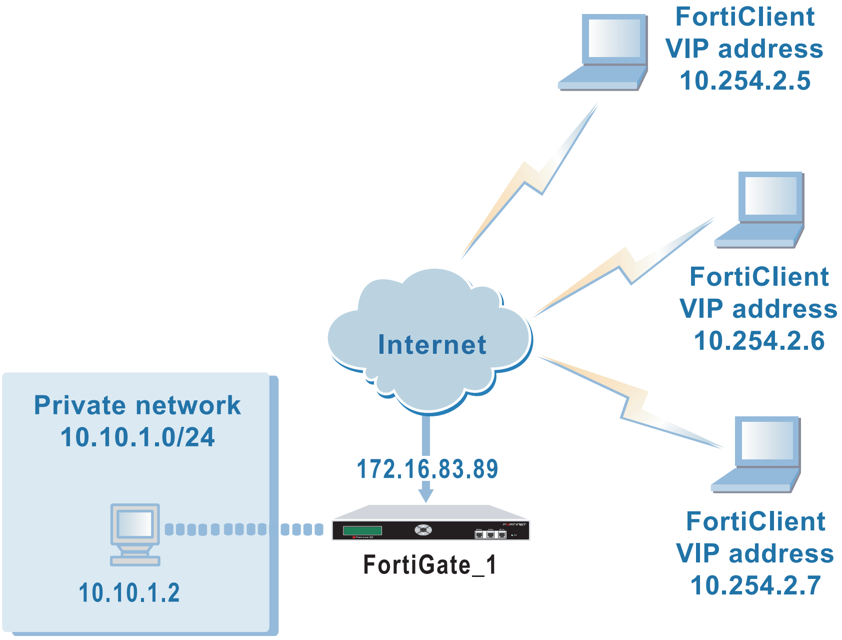
Configuration options

Multiple remote clients that use VPN client software such as the FortiClient Host Security application can connect to the same FortiGate IPSec VPN tunnel. A variety of configurations are possible for authenticating remote clients using preshared keys, including some that include local IDs and user groups as authentication components:

- Dialup clients share a preshared key (the simplest configuration). This configuration can be implemented in either aggressive or main mode. See "Dialup clients share the same preshared key" on page 7.
- Dialup clients share the same preshared key and local ID. This configuration must be implemented in aggressive mode. See "Dialup clients share the same preshared key and local ID" on page 10.
- Each dialup client uses a unique local ID and preshared key, and the clients are associated with a FortiGate user group. The FortiClient local ID is compared to the FortiGate user name, and the FortiClient preshared key is compared to the FortiGate password. This configuration can be implemented in either aggressive or main mode. See "Dialup clients use unique local IDs and preshared keys" on page 11.
- Each dialup client uses a unique preshared key, and the clients are associated with a FortiGate user group. The FortiClient preshared key is compared to the result of combining the FortiGate user name and password. This configuration must be implemented in main mode. See "Dialup clients use unique preshared keys" on page 12.
- Dialup clients share a preshared key but authenticate individually using Extended Authentication (XAuth). This configuration can be implemented in either aggressive or main mode. See "Dialup clients authenticate individually through XAuth" on page 14.

Figure 1 shows an example network configuration.

Figure 1: Example FortiClient dialup-client configuration



General FortiGate dialup-server configuration steps

For detailed information about how to configure a FortiGate dialup server, see the "FortiClient dialup-client configurations" section of the *FortiGate VPN Guide*.

In summary, to configure a FortiGate unit as a dialup server:

1. Add the phase 1 gateway definition.
2. Add the phase 2 tunnel definition.
3. Create the IP source address to define the host, server, or network behind the FortiGate dialup server.
4. Create an IP destination address that refers to the Virtual IP (VIP) addresses used by FortiClient dialup clients.
5. Add a firewall encryption policy that includes the IP source address, the IP destination address, and the phase 2 tunnel definition.
6. Place the firewall encryption policy above all regular (non-encryption) policies in the policy list.

General FortiClient dialup-client configuration steps

If there are multiple networks behind the FortiGate dialup server to which the FortiClient dialup clients need access, those networks must be defined through the FortiClient **VPN > Connections** tab (when you add or edit a connection, select Advanced, and then define the network in the Remote Network field).

To configure the FortiClient Host Security application as a dialup client, you need:

- a descriptive name for the connection
- the IP address of the external (public) interface to the FortiGate dialup server
- the IP address of the host, server, or network that dialup users will be allowed to access behind the FortiGate unit
- a preshared key

For more information, see the “FortiClient dialup-client configurations” section of the *FortiGate VPN Guide*.

In the examples throughout this technical bulletin, the FortiClient dialup clients are assigned VIP addresses from the 10.254.2.0/24 network. The VIP addresses are assigned manually. You may choose VIP addresses that meet the requirements of your situation. As a precaution to avoid ambiguous routing and IP-address overlap, remember to choose VIP addresses that do not match the private network address space behind the FortiGate dialup server.

Dialup clients share the same preshared key

In this scenario, all FortiClient dialup clients are assigned the same preshared key. To begin, start the web-based manager on the FortiGate unit.

To configure the phase 1 settings on the FortiGate unit

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 phase 1 gateway (for example, `Dialup_Client`).
Remote Gateway	Dialup User
Mode	Aggressive or Main
Authentication Method	Preshared Key
Pre-shared Key	Enter 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.
Peer Options	Accept any peer ID
Advanced	As required.

To configure the phase 2 settings on the FortiGate unit

1. Go to **VPN > IPSEC > Phase 2**.
2. Select Create New, and then select Advanced.
3. Enter the following information, and then select OK:

Tunnel Name	Enter a name for the phase 2 tunnel (for example, `Dialup_Tunnel`).
Remote Gateway	Select the phase 1 gateway that you defined for dialup clients (for example, `Dialup_Client`).
Autokey Keep Alive	Select Autokey Keep Alive. Set the other options as required.

4. Enter the following CLI command to enable all FortiClient dialup clients having VIP addresses from the 10.254.2.0/24 network to connect using the same phase 2 tunnel definition:

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

Defining the firewall encryption policy

Firewall policies control all VPN traffic passing through the FortiGate unit. A policy is needed to allow encrypted packets, specify the permitted direction of VPN traffic, and select the VPN tunnel that will be subject to the policy.

Before you define the policy, you must first specify the IP source and destination addresses. In the example dialup-client configuration:

- The IP source address corresponds to the private IP address of the server behind the FortiGate dialup server (`10.10.1.2/32`).
- The IP destination address refers to the VIP addresses that dialup clients will be using (`10.254.2.0/24`).

To define the source address

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

Address Name	Enter an address name (for example, `Network_1`).
IP Range/Subnet	Enter the private IP address and subnet mask of the server behind the FortiGate unit (for example, `10.10.1.2/32`).

To define the destination address

1 Go to **Firewall > Address**.

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

Address Name	Enter an address name (for example, `Dialup_VIPs`).
IP Range/Subnet	Enter the VIP address used by dialup clients (for example, `10.254.2.0/24`).

To define the firewall encryption policy

1 Go to **Firewall > Policy**.

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

Source	Interface/Zone Select the interface to the internal (private) network. Address Name `Network_1`
Destination	Interface/Zone Select the interface to the external (public) network. Address Name `Dialup_VIPs`
Schedule	As required.
Service	As required.
Action	ENCRYPT
VPN Tunnel	`Dialup_Tunnel` Select the Allow inbound option to allow traffic from the dialup client to enter the internal network. Select the Allow outbound option to allow traffic from the internal network to be routed to the dialup client.
Advanced	As required.

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

To configure FortiClient

Configure all dialup clients as follows using the same preshared key:

1 Start FortiClient.

2 Go to **VPN > Connections** and select Add.

3 In the Connection Name field, type a descriptive name for the connection (for example, `FortiGate_1`.

4 In the Remote Gateway field, type the public IP address of the FortiGate unit (for example, `172.16.83.89`).

5 In the Remote Network fields, type the private IP address and subnet mask of the server behind the FortiGate unit (for example, `10.10.1.2/255.255.255.255`).

6 From the Authentication Method list, select Preshared Key.

7 In the Preshared Key field, type the preshared key that was specified previously in the phase 1 gateway configuration on the FortiGate unit.

8 Select Advanced.

9 Select Acquire virtual IP address and then select Config.

10 Select Manually Set, and in the IP and Subnet Mask fields, type the VIP address and subnet mask that the client will use as its source address for transmitting IP packets through the tunnel (for example, `10.254.2.5/255.255.255.0`). This value will be compared to the firewall destination address that you specified previously on the FortiGate unit (see "To define the destination address" on page 9).

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 VPN settings on the FortiGate unit.

13 Select OK to close all dialog boxes.

Dialup clients share the same preshared key and local ID

Choose a preshared key and identifier that can be used by all dialup clients.

To configure the phase 1 settings on the FortiGate unit

Use the same steps from the general FortiGate configuration (see "Dialup clients share the same preshared key" on page 7) with the following differences:

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 phase 1 gateway (for example, `Dialup_Client`).
Remote Gateway	Dialup User
Mode	Aggressive
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Select Accept this peer ID and type the identifier that the FortiGate unit will use to recognize dialup clients.
Advanced	As required.

To configure FortiClient

Make the following addition to the general FortiClient configuration (see "To configure FortiClient" on page 9) to specify the same preshared key and local ID for all dialup clients:

1 Start FortiClient.

2 Go to **VPN > Connections**, select the existing configuration, and then select Edit.

3 Select Advanced.

4 Under Policy, select Config.

5 In the Local ID field, type the identifier that will be shared by all dialup clients. This value must match the Accept this peer ID value that you specified previously in the phase 1 gateway configuration on the FortiGate unit.

6 Select OK to close all dialog boxes.

7 Configure all dialup clients the same way using the same preshared key and local ID.

Dialup clients use unique local IDs and preshared keys

In this scenario, user accounts are created for each dialup client and the dialup clients are placed in a user group. Choose a unique local ID and a unique preshared key for each dialup client. The FortiGate unit will compare the local ID that you specify for FortiClient dialup clients to the FortiGate account user name, and the FortiClient preshared key will be compared to the FortiGate account password.

To assign a user name and password to dialup clients

1 At the FortiGate unit, go to **User > Local**.

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

User Name	Type a unique user name for a dialup client (for example, `FortiClient1`).
Password	Type a unique password to go with the user name (for example, `123456`). The value must be least six characters long.

3 Repeat this procedure for all dialup clients.

To create a user group of dialup clients

1 At the FortiGate unit, go to **User > User Group**.

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

Group Name	Type a name for the user group (for example, `Dialup_Group1`).
Available Users	One at a time, select the user name of each dialup client and then select the right-arrow button to move each user name into the Members box.
Protection Profile	Select a protection profile for the group. If you do not want to assign a protection profile to the group, select unfiltered.

To configure the phase 1 settings on the FortiGate unit

Use the same steps from the general FortiGate configuration (see “Dialup clients share the same preshared key” on page 7) with the following differences:

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 phase 1 gateway (for example, `Dialup_Client`).
Remote Gateway	Dialup User
Mode	Aggressive

Authentication Method	Preshared Key
Pre-shared Key	Leave this field empty. The FortiGate unit will compare the FortiClient preshared key to the user account password value instead.
Peer Options	Select Accept peer ID in dialup group and then select the group name (for example, `Dialup_Group1`) from the list of user groups.
Advanced	As required.

To configure FortiClient

Make the following changes to the general FortiClient configuration (see "To configure FortiClient" on page 9) to specify a unique preshared key and local ID for each dialup client:

1. Start FortiClient.
2. Go to **VPN > Connections**, select the existing configuration, and then select Edit.
3. In the Preshared Key field, type the FortiGate password that belongs to this dialup client (for example, `1234546`).
4. Select Advanced.
5. Under Policy, select Config.
6. In the Local ID field, type the FortiGate user name that you assigned previously to this dialup client (for example, `FortiClient1`).
7. Select OK to close all dialog boxes.
8. Configure all dialup clients the same way using unique preshared keys and local IDs.

Dialup clients use unique preshared keys

In this scenario, user accounts are created for each dialup client and the dialup clients are placed in a user group. Choose a unique preshared key for each dialup client. In this case, the unique values that you specify for FortiClient preshared keys are compared to the combined values of the user name and password specified on the FortiGate dialup server.

To assign a user name and password to dialup clients

1. At the FortiGate unit, go to **User > Local**.
2. Select Create New, enter the following information, and select OK:

User Name	Type a unique user name for a dialup client (for example, `FC2`).
Password	Type a unique password to go with the user name (for example `1FG6LK`). The value must be least six characters long.

3. Repeat this procedure for all dialup clients.

To create a user group of dialup clients

1. At the FortiGate unit, go to **User > User Group**.
2. Select Create New, enter the following information, and select OK:

Group Name	Type a name for the user group (for example, `Dialup_Group2`).
Available Users	One at a time, select the user name of each dialup client and then select the right-arrow button to move each user name into the Members box.
Protection Profile	Select a protection profile for the group. If you do not want to assign a protection profile to the group, select unfiltered.

To configure the phase 1 settings on the FortiGate unit

Use the same steps from the general FortiGate configuration (see “Dialup clients share the same preshared key” on page 7) with the following differences:

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 phase 1 gateway (for example, `Dialup_Client`).
Remote Gateway	Dialup User
Mode	Main
Authentication Method	Preshared Key
Pre-shared Key	Leave this field empty. The FortiGate unit will compare FortiClient preshared key values to user-account user name and password values instead.
Peer Options	Select Accept peer ID in dialup group and then select the group name (for example, `Dialup_Group2`) from the list of user groups.
Advanced	Retain the default settings unless changes are needed to meet your specific requirements.

To configure FortiClient

Make the following changes to the general FortiClient configuration (see “To configure FortiClient” on page 9) to specify a unique preshared key and password for each dialup client:

1. Start FortiClient.
2. Go to **VPN > Connections**, select the existing configuration, and then select Edit.
3. In the Preshared Key field, type the user name, followed by a “+” sign, followed by the password that you specified previously in the user account settings on the FortiGate unit (for example, `FC2+1FG6LK`).
4. Select OK.
5. Configure all dialup clients the same way using unique preshared keys.

Dialup clients authenticate individually through XAuth

If it is necessary to have dialup clients authenticate against a RADIUS or LDAP server, enable extended authentication (XAuth). XAuth is enabled in conjunction with RADIUS or LDAP services to challenge a dialup client for a RADIUS or LDAP user name and password. When the FortiGate unit is configured to operate as an XAuth server, the dialup client must authenticate using the user name and password defined in the RADIUS or LDAP server. The FortiGate unit derives the user account information from the RADIUS or LDAP server.

To configure the RADIUS or LDAP server

Add a RADIUS or LDAP server to the FortiGate unit. Refer to the “User” chapter of the *FortiGate Administration Guide*.

To add a group of RADIUS or LDAP clients

1 At the FortiGate unit, go to **User > User Group**.

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

Group Name	Type a name for the user group (for example, `RADIUS_Group`).
Available Users	One at a time, select the user name of each dialup client that requires RADIUS or LDAP authentication and then select the right-arrow button to move the user name into the Members box.

To configure the phase 1 settings on the FortiGate unit

Use the same steps from the general FortiGate configuration (see “Dialup clients share the same preshared key” on page 7) with the following differences:

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

2 Select Create New, and then select Advanced.

3 Enter the following information, and then select OK:

Gateway Name	Type a name for the phase 1 gateway (for example, `Dialup_Client`).
Remote Gateway	Dialup User
Mode	Aggressive or Main
Authentication Method	Preshared Key
Pre-shared Key	Enter the preshared key.
Peer Options	Accept any peer ID
XAuth	Enable as Server

Server Type

Choose the correct communication protocol for your RADIUS or LDAP server. In general:

- 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.

User Group

Select the RADIUS or LDAP group name (for example, `RADIUS_Group`) from the list of user groups.

To configure FortiClient

At each dialup client, make the following changes to the general FortiClient configuration (see "To configure FortiClient" on page 9) to specify the user name and password response to a RADIUS or LDAP server:

1. Start FortiClient.
2. Go to **VPN > Connections**, select the existing configuration, and then select Edit.
3. Select Advanced.
4. Select eXtended Authentication, and then select Config.
5. In the Extended Authentication (XAuth) dialog box, either:
   - Select Prompt to login, which makes the FortiClient user responsible for typing a RADIUS or LDAP user name and password when challenged.
   - Type the user name and password values into the User Name and Password fields. When challenged, FortiClient will automatically supply the values for the FortiGate dialup server to forward to the RADIUS or LDAP server.
6. Select OK to close all dialog boxes.
7. Configure all dialup clients the same way using unique RADIUS or LDAP user names and passwords for each dialup client.