FortiClient to FortiGate IPSec VPN Configuration

Technical Note

FortiClient to FortiGate IPSec VPN Configuration Technical Note	
Document Version:	Version 1
Publication Date:	June 29, 2004
Description:	Describes the setup of IPSec VPN tunnels between a FortiClient dialup user and a FortiGate dialup server.
Product:	FortiClient Host Security 1.0 and 1.2 FortiGate Antivirus Firewall v2.50

Fortinet Inc.

FortiClient to FortiGate IPSec VPN Configuration Technical Note
Version 1
June 29, 2004

Regulatory Compliance
FCC Class A Part 15 CSA/CUS

Table of Contents

FortiClient to FortiGate IPSec VPN Configuration Technical Note

This technical note contains example procedures and configurations for IPSec AutoIKE key VPN tunnels between a client PC running the FortiClient software and a FortiGate Antivirus Firewall running FortiOS v2.50.

This technical note contains the following sections:

- Network topologies
- FortiClient to FortiGate VPN with pre-shared keys
- FortiClient to FortiGate VPN with certificates
- Configuring eXtended Authentication

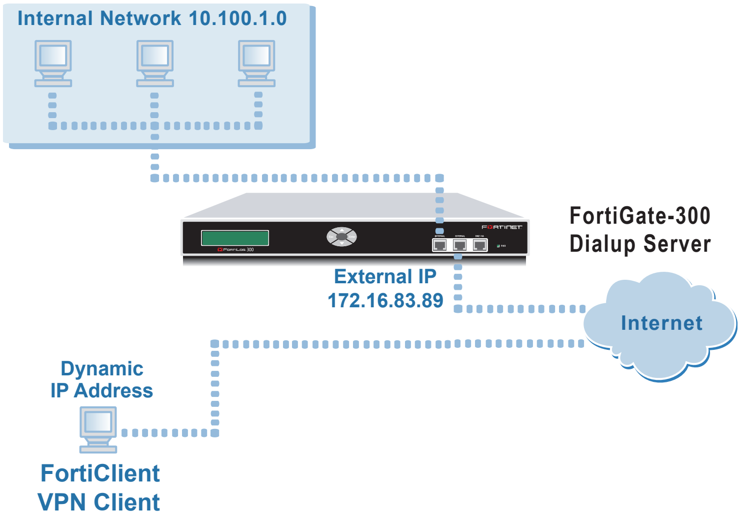
Network topologies

The configurations described in this technical note are for the following firmware and client software versions:

- FortiClient Host Security v1.0 and 1.2
- Any FortiGate unit with firmware v2.50

Figure 1 shows the FortiClient to FortiGate IPSec network topology used for the examples in "FortiClient to FortiGate VPN with pre-shared keys" on page 6 and "FortiClient to FortiGate VPN with certificates" on page 13. The diagram shows a FortiGate-300 unit, but the procedures and configurations could be applied to any FortiGate unit.

Figure 1: FortiClient to FortiGate-300 network topology



FortiClient to FortiGate VPN with pre-shared keys

This section describes how to configure and test a dialup VPN in main mode, for a network topology similar to that shown in Figure 1. In this case, the FortiGate unit is the dialup server and the FortiClient user is the dialup client. Both ends use pre-shared keys.

General configuration steps

1 Configure the FortiGate unit as a dialup server.

- Add a remote gateway.
- Add an AutoIKE key VPN tunnel.
- Add a source address to the internal interface to specify the address or address range on the FortiGate internal network that is part of the VPN.
- Add a destination address to the external interface.
- Add an internal to external encrypt policy that includes the source address, the destination address, and the dialup VPN tunnel.
- Place the encrypt policy above the non-encrypt policies in the policy list.

2 Configure the FortiClient software as a dialup VPN client.

To add a FortiClient to FortiGate VPN, you need:

- a descriptive name for the connection,
- the remote gateway IP address for the FortiGate gateway,
- the remote network IP address and netmask,
- the pre-shared key.

Configuring the FortiGate unit

The following procedures describes the detailed configuation information. Because the default FortiGate VPN settings are compatible with the FortiClient ones, in most cases, you do not have to modify the default settings.

For detailed configuration information, see *FortiGate VPN Guide*.

To add the remote gateway

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

2 Select New.

3 Enter the following information, then select OK.

Gateway Name	Dialup_Client
Remote Gateway	Dialup User
Mode	Main (ID Protection)
P1 Proposal	1-Encryption 3DES, Authentication SHA1
DH Group	5
Keylife	28800 (seconds)
Authentication Method	Preshared key
Pre-shared key	Enter the pre-shared key. The FortiClient user must use the same pre-shared 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.
Local ID	

To add the VPN tunnel

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

2 Select New.

3 Enter the following information, then select OK.

Tunnel Name	Client_IKE
Remote Gateway	Dialup_Client
P2 Proposal	1-Encryption 3DES, Authentication SHA1
Enable replay detection	Enable
Enable perfect forward frequency	Enable
DH Group	5
Keylife	3600 (seconds)
Autokey Keep Alive	Enable
Concentrator	None
Quick Mode Identities	Use selectors from policy

To add the source address

1 Go to **Firewall > Address > Internal.**

2 Select New.

3 Enter the following information, then select OK.

Address Name	FortiGate_network
IP Address	10.100.1.0
Netmask	255.255.255.0

To add the destination address

1 Go to **Firewall > Address > External.**

2 Select New.

3 Enter the following information, then select OK.

Address Name	FortiClient_users
IP Address	10.100.2.0 This subnet should be different from the local FortiGate subnet and will be used as the virtual IP addresses for the remote FortiClient PCs. See "To configure the FortiClient VPN settings" on page 10.
Netmask	255.255.255.0

To add the firewall policy

1 Go to **Firewall > Policy > Int->Ext.**

2 Select New.

3 Enter the following information, then select OK.

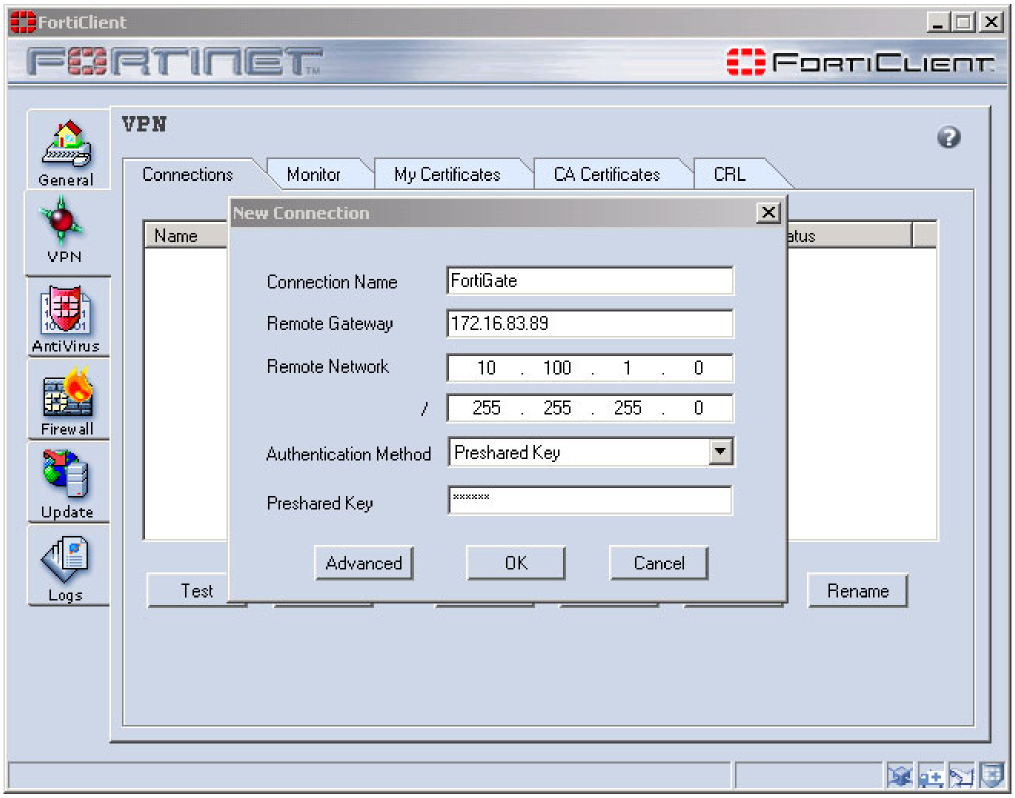
Source	FortiGate_network
Destination	FortiClient_users
Schedule	Always
Service	Any
Action	ENCRYPT
VPN Tunnel	Client_IKE
Allow Inbound	Check Allow Inbound to enable inbound users to connect to the source address.
Allow Outbound	Check Allow Outbound to enable outbound users to connect to the destination address.
Inbound NAT	Check Inbound NAT.
Outbound NAT	Check Outbound NAT.
Traffic Shaping	Configure settings as required for this policy.
Anti-Virus & Web filter	Configure settings as required for this policy.
Log Traffic	Check Log Traffic if you want messages written to the traffic log whenever the policy processes a connection.
Comments	Optionally enter a short description of the firewall policy.

4 Place the policy in the policy list above non-encrypt policies. If there are more than one encrypt policies in the list, place the more specific ones above the more general ones with similar source and destination addresses.

Configuring the FortiClient software for pre-shared key VPN

The FortiClient default settings are compatible with those of the FortiGate unit. You can just enter the following basic required information.

Figure 2: Creating a new VPN connection



New Connection

Connection Name: FortiGate

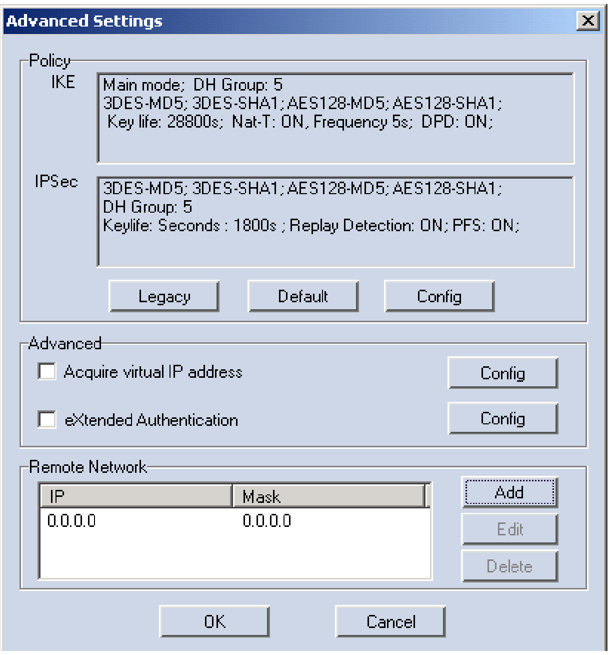
Remote Gateway: 172.16.83.89

Remote Network: 10 . 100 . 1 . 0 / 255 . 255 . 255 . 0

Authentication Method: Preshared Key

Preshared Key: ******

Figure 3: Configuring advanced settings


Advanced Settings

Policy

IKE: Main mode; DH Group: 5
3DES-MD5; 3DES-SHA1; AES128-MD5; AES128-SHA1;
Key life: 28800s; Nat-T: ON, Frequency 5s; DPD: ON;

IPSec: 3DES-MD5; 3DES-SHA1; AES128-MD5; AES128-SHA1;
DH Group: 5
Keylife: Seconds : 1800s ; Replay Detection: ON; PFS: ON;

Advanced

□ Acquire virtual IP address

□ eXtended Authentication

Remote Network

IP	Mask
0.0.0.0	0.0.0.0

To configure the FortiClient VPN settings

1 Go to **VPN > Connections**.

2 Click Add.

3 For Connection Name, enter FortiGate.

4 For Remote Gateway, enter 172.16.83.89.

5 For Remote Network, enter 10.100.1.0/255.255.255.0.

6 Enter the Pre-shared key.

The pre-shared key must be the same as the one used by the FortiGate VPN configuration.

7 Click Advanced.

8 In the Advanved Settings dialog box, select Acquire Virtual IP Address and click Config.

9 In the Virtual IP Acquisition dialog box, select Manually Set. Then enter the IP address and subnet that you want to use for the FortiClient user. The virtual IP must be within the destination subnet you specified in "To add the destination address" on page 7.

10 Click OK.

Testing the connection

You can test the VPN connection between the FortiClient software and the remote FortiGate unit.

To test the connection

1 Go to **VPN > Connections**.

2 Select the connection you want to test.

3 Click Test.

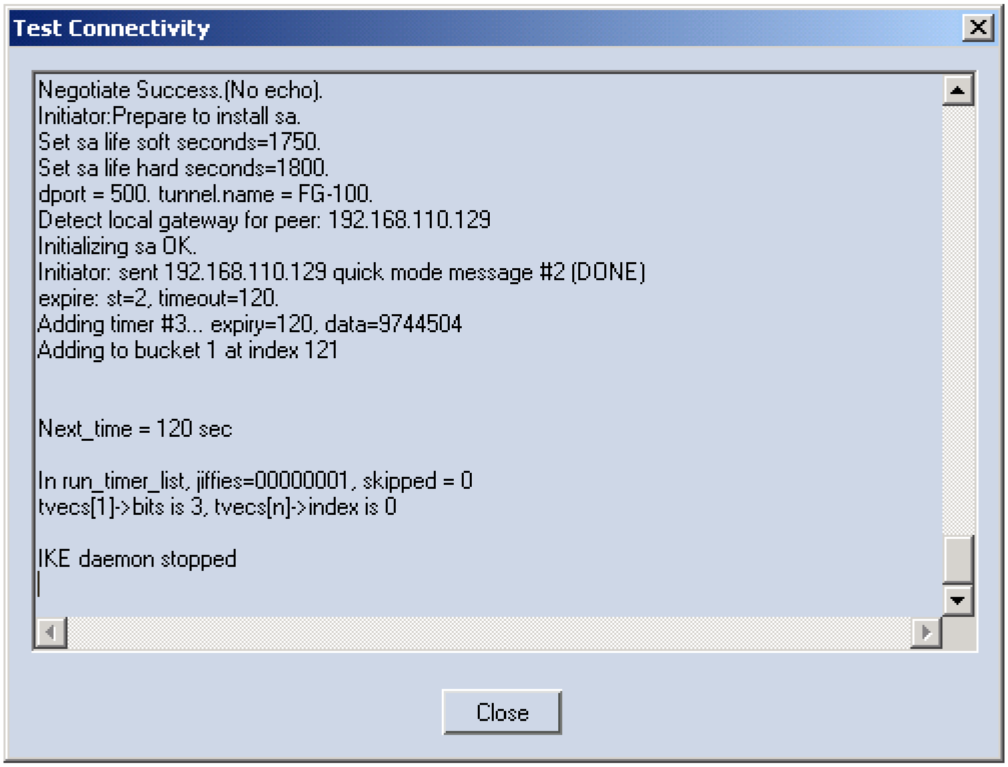
A log window opens and begins to negotiate the VPN connection with the remote FortiGate unit. If the test is successful, the last line of the log will read "IKE daemon stopped".

Note: To test the VPN connection, the FortiClient software attempts to negotiate the VPN connection but does not actually open a VPN connection.

If the last line of the log reads "Next_time = x sec", where x is an integer, the test was not successful. The FortiClient software is continuing to try to negotiate the connection.

4 Click Close.

Figure 4: A successful connection test



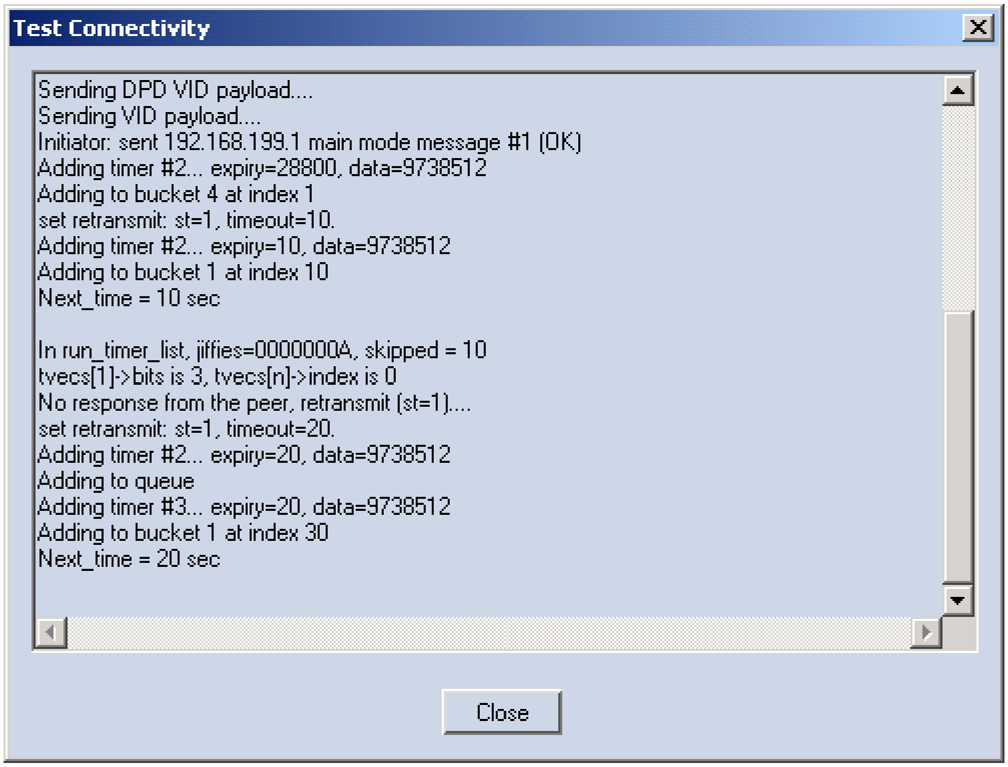
```
Negotiate Success.(No echo).
Initiator:Prepare to install sa.
Set sa life soft seconds=1750.
Set sa life hard seconds=1800.
dport = 500. tunnel.name = FG-100.
Detect local gateway for peer: 192.168.110.129
Initializing sa OK.
Initiator: sent 192.168.110.129 quick mode message #2 (DONE)
expire: st=2, timeout=120.
Adding timer #3... expiry=120, data=9744504
Adding to bucket 1 at index 121


Next_time = 120 sec

In run_timer_list, jiffies=00000001, skipped = 0
tvecs[1]->bits is 3, tvecs[n]->index is 0

IKE daemon stopped
```

Figure 5: A failed connection test



```
Sending DPD VID payload....
Sending VID payload....
Initiator: sent 192.168.199.1 main mode message #1 (OK)
Adding timer #2... expiry=28800, data=9738512
Adding to bucket 4 at index 1
set retransmit: st=1, timeout=10.
Adding timer #2... expiry=10, data=9738512
Adding to bucket 1 at index 10
Next_time = 10 sec

In run_timer_list, jiffies=0000000A, skipped = 10
tvecs[1]->bits is 3, tvecs[n]->index is 0
No response from the peer, retransmit (st=1)....
set retransmit: st=1, timeout=20.
Adding timer #2... expiry=20, data=9738512
Adding to queue
Adding timer #3... expiry=20, data=9738512
Adding to bucket 1 at index 30
Next_time = 20 sec
```

Connecting to the remote FortiGate network

After you set up a VPN connection, you can start or stop the connection as required.

To connect to a remote FortiGate gateway

1. Go to **VPN > Connections**.
2. Select the connection you want to start.
3. Click Connect.

   The FortiClient software opens a log window and begins to negotiate a VPN connection with the remote FortiGate firewall. If the negotiation is successful and the connection is established, the last line of the log will read “Negotiation Succeeded!”
4. Click OK or wait for the log window to close automatically.

   If the last line of the log is “Negotiation failed! Please check log” and the log window does not close automatically, then the connection attempt failed. Test the connection to verify the configuration. See “Testing the connection” on page 10.
5. To stop the connection, click Disconnect.

FortiClient to FortiGate VPN with certificates

This section describes how to configure and test a FortiClient to FortiGate dialup VPN in main mode, for a network topology similar to that shown in Figure 1. The FortiGate unit is the dialup server and the FortiClient user is the dialup client with a dynamically assigned IP address. In this case, the VPN participants uses certificates, instead of the pre-shared keys.

General steps for certificate management on a FortiGate unit

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, before an encrypted VPN tunnel is set up between the participants.

You need both a signed local certificate and a CA certificate. The local certificate is the digital certificate that the FortiGate unit uses to authenticate itself to other devices.The CA certificate is the certificate that the FortiGate unit uses to validate digital certificates received from other devices.

General configuration steps to obtain a signed local certificate

To obtain a signed local certificate, complete these steps:

1. Generate the certificate request.

   This procedure creates a private and public key pair for the local FortiGate unit. The public key accompanies the certificate request. The private key remains confidential.

   See “Generating the certificate request” on page 14.
2. Download the certificate request to the management computer.

   See Downloading the certificate request.
3. Submit the certificate request to the CA.

   Copy the certificate request from the downloaded text file and paste it into a web page form controlled by the CA. The CA will notify you after it has signed the request. You must then go to the web server operated by the CA, copy the signed certificate and save it to your local computer.

   See “Requesting the signed local certificate” on page 15.
4. Import the signed certificate to the FortiGate unit.

   See “Importing the signed local certificate” on page 15.

General configuration steps to obtain a CA certificate

To obtain a CA certificate, complete these steps:

1. Retrieve the CA certificate.

   Connect to the web page controlled by the CA, copy the CA certificate and save it to your local computer. The CA certificate includes a certificate path which grants legitimacy to all certificates issued by the CA.

   See “Downloading a CA certificate” on page 16.
2. Import the CA certificate to the Fortigate unit.

   See “Importing a CA certificate” on page 16.

Obtaining a signed local certificate for the FortiGate unit

The signed local certificate provides the FortiGate unit with a means to authenticate itself to other devices.

Note: The VPN peers must use digital certificates that adhere to the X.509 standard.

Generating the certificate request

To generate the certificate request

1. Go to **VPN > Local Certificates**.
2. Select Generate.
3. Enter a Certificate Name.

   Typically, this is the name of the FortiGate unit being certified.

   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
4. Configure the Subject Information that identifies the FortiGate unit being certified.

   Preferably use an IP address or domain name. If this is impossible (such as with a dialup client), use an email address.

   Host IP For Host IP, enter the IP address of the FortiGate unit being certified.

   Domain Name For Domain name, enter the fully qualified domain name of the FortiGate unit being certified. Do not include the protocol specification (http://) or any port number or path names.

   E-Mail For E-mail, enter the email address of the owner of the FortiGate unit being certified. Typically, email addresses are entered only for clients, not gateways.

Note: If you specify a host IP or domain name, use the IP address or domain name associated with the interface on which IKE negotiations will take place (e.g. the external interface of the local FortiGate unit). If the IP address in the certificate does not match the IP address of the local interface (or if the domain name in the certificate does not match a DNS query of the FortiGate unit's IP), then some implementations of IKE may reject the connection. Enforcement of this rule varies for different IPSec products.

5. Configure the Optional Information to further identify the object being certified.

   Organization Unit Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiGate unit.

   Organization Enter the name of the organization that is requesting the certificate for the FortiGate unit.

   Locality (City) Enter the name of the city, or town, where the person or organization certifying the FortiGate unit resides.

   State/Province Enter the name of the state or province where the FortiGate unit is located.

   Country Select the country where the FortiGate unit is located.

   e-mail Enter a contact e-mail address for the FortiGate unit.

6 Configure the key.

Key Type	Select RSA as the key encryption type. No other key type is supported.
Key Size	Select one of 1024 Bit, 1536 Bit or 2048 Bit. If you do not specify a key size, 1024 Bit will be used. Larger keys are slower to generate but more secure.

7 Select OK to generate the private and public key pair and the certificate request.

The certificate request will be displayed on the Local Certificates list with a status of Pending.

Downloading the certificate request

To download the certificate request

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

2 Select Download to download the local certificate to the management computer.

The File Download dialog will display.

3 Select Save.

4 Name the file and save it on the management computer.

Requesting the signed local certificate

To request the signed local certificate

1 On the management computer, open the certificate request file in a text editor.

2 Copy the certificate request.

3 Connect to the CA web server.

4 Request the signed local certificate.

Follow the CA web server instructions to:

- add a base64 encoded PKCS#10 certificate request to the CA web server,
- paste the certificate request to the CA web server,
- submit the certificate request to the CA web server.

The certificate request is submitted to the CA for it to sign.

5 After the certificate is signed, select Base 64 encoded, then select Download CA certificate. The File Download dialog will display.

6 Select Save.

7 Name the file and save it on the management computer.

Importing the signed local certificate

To import the signed local certificate

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

2 Select Import.

3 Enter the path or browse to locate the file containing the signed local certificate.

4. Select OK.
   The signed local certificate will be displayed on the Local Certificates list with a status of OK.

Obtaining a CA certificate

For the VPN peers to authenticate themselves to each other, they must both obtain a CA certificate from the same certificate authority.

Note: The CA certificate must adhere to the X.509 standard.

Downloading a CA certificate

To download the CA certificate

1. Connect to the CA web server.
2. Follow the CA web server instructions to download the CA certificate.
   The File Download dialog will display.
3. Select Save.
4. Name the file and save it on the management computer.

Importing a CA certificate

To import the CA certificate

1. Go to **VPN > CA Certificates**.
2. Select Import.
3. Enter the path or browse to locate the file containing the CA certificate.
4. Select OK.
   The CA certificate appears on the CA Certificates list.

Configuring the FortiGate unit for dialup VPN

General configuration steps

- Add a remote gateway with Dialup User. Select the certificate as the authentication method.
- Add an AutoIKE key VPN tunnel.
- Add a source address to specify the address or address range on the FortiGate internal network that is part of the VPN.
- Add a destination address.
- Add an internal to external encrypt policy that includes the source address, the destination address, and the dialup VPN tunnel.
- Place the encrypt policy above the non-encrypt policies in the policy list.

For detailed configuration procedures, see “Configuring the FortiGate unit” on page 6 and the *FortiGate VPN Guide*.

Digital certificate management on a FortiClient PC

To use digital certificates, you need a signed local certificate, the certificate authority (CA) certificates for any CAs you are using, and any applicable certificate revocation lists (CRLs). The FortiClient software can use a manual, file based enrollment method or the simple certificate enrollment protocol (SCEP) to get certificates. SCEP is simpler, but can only be used if the CA supports SCEP.

File based enrollment requires copying and pasting text files from the local computer to the CA, and from the CA to the local computer. SCEP automates this process but CRLs must still be manually copied and pasted between the CA and the local computer.

Getting a signed local certificate

The FortiClient software uses the signed local certificate to authenticate itself to a FortiGate gateway or other devices.

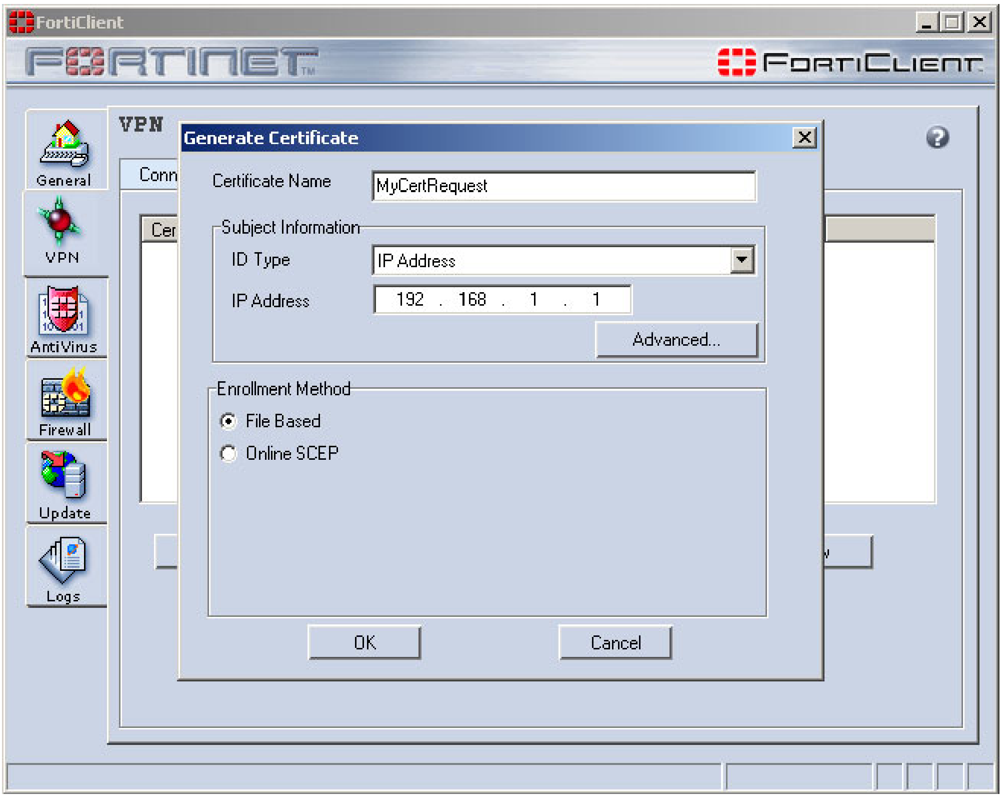
Note: The digital certificates must comply with the X.509 standard.

Generating a local certificate request

This procedure generates a private and public key pair. The public key is the base component of the certificate request.

Note: The FortiClient software generates 1024bit keys.

Figure 6: Generating a local certificate request



Certificate Name: MyCertRequest

Subject Information

ID Type: IP Address

IP Address: 192 . 168 . 1 . 1

Enrollment Method

● File Based

○ Online SCEP

To generate the local certificate request

1 Go to **VPN > My Certificates**.

2 Click Generate.

3 Enter a Certificate Name.

4 Under subject information, select the ID Type for the subject.
You can select from domain name, email address or IP address.

5 Enter the information for the ID type that you selected.

Domain name If you selected domain name, enter the fully qualified domain name of the FortiClient computer being certified.

Email address If you selected email address, enter the email address of the owner of the FortiClient computer being certified.

IP address If you selected IP address, enter the IP address of the FortiClient computer being certified.

6 Optionally click Advanced and enter the advanced setting information.

Email Enter a contact email address for the FortiClient computer user.

Department Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiClient computer (such as Manufacturing or MF).

Company	Enter the legal name of the organization that is requesting the certificate for the FortiClient computer.
City	Enter the name of the city or town where the FortiClient Computer is located.
State/Province	Enter the name of the state or province where the FortiClient computer is located.
Country	Enter the name of the country where the FortiClient computer is located.

7 Click OK.

8 Select either File Based or Online SCEP as the enrollment method.

9 If you select file based enrollment, the private/public key pair is generated and the certificate request is displayed in the My Certificates list with the type of Request.

Continue with “Exporting the local certificate request”.

10 If you select Online SCEP as the enrollment method, select an issuer CA from the list provided or enter the URL of the CA server.

11 Click OK to generate the private and public key pair and the certificate request.

The FortiClient software:

- submits the local certificate request,
- retrieves and imports the signed local certificate,
- retrieves and imports the CA certificate.

The signed local certificate is displayed on the Local Certificates list with the type of Certificate. The CA certificate is displayed on the CA Certificates list. The expiration dates of the certificates are listed in the Valid To column of each list.

Continue with “Getting a CRL” on page 21.

Exporting the local certificate request

Use the following procedure to export the local certificate request from the FortiClient software to a .csr file.

To export the local certificate request

1 Go to **VPN > My Certificates**.

2 From the certificate list, select the local certificate to export.

3 Click Export.

4 Name the file and save it in a directory on the FortiClient computer.

After exporting the certificate request, you can submit it to the CA so that the CA can sign the certificate.

Requesting the signed local certificate

Use the following procedure to copy and paste the certificate request from the FortiClient computer to the CA web server.

To request the signed local certificate

1 On the FortiClient computer, open the local certificate request using a text editor.

2 Connect to the CA web server.

3 Follow the CA web server instructions to:

- add a base64 encoded PKCS#10 certificate request to the CA web server,
- paste the certificate request to the CA web server,
- submit the certificate request to the CA web server.

Retrieving the signed local certificate

After you receive notification from the CA that it has signed the certificate request, connect to the CA web server and download the signed local certificate to the FortiClient computer.

Importing the signed local certificate

Use this procedure to import the signed local certificate to the FortiClient software.

To import the certificate

1 Go to **VPN > My Certificates**.

2 Click Import.

3 Enter the path or browse to locate the signed local certificate on the FortiClient computer.

4 Click OK.

The signed local certificate is displayed on the Local Certificates list with the type of Certificate showing in the certificate list. The expiration date of the certificate is listed in the Valid To column.

Exporting the signed local certificate

You can back up the certificate by saving it into a PKCS7 (Public-Key Cryptography Standards) or PKCS12 file to your local or network computer.

To export the certificate

1 Go to **VPN > My Certificates**.

2 Select the certificate and click Export.

3 In the Save As dialog box, select the folder where you want to save the file.

4 Enter a file name.

5 Select either PKCS7 or PKCS12. If you select PKCS12, you must enter a password.

6 Click Save.

Getting a CA certificate

For the FortiClient software and the FortiGate gateway to authenticate themselves to each other, they must both have a CA certificate from the same CA.

The FortiClient computer obtains the CA certificate to validate the digital certificate that it receives from the remote VPN peer. The remote VPN peer obtains the CA certificate to validate the digital certificate that it receives from the FortiClient computer.

Note: The CA certificate must comply with the X.509 standard.

To retrieve the CA certificate

1. Connect to the CA web server.
2. Follow the CA web server instructions to download the CA certificate.

To import the CA certificate

1. Go to **VPN > CA Certificates**.
2. Click Import.
3. Enter the path or browse to locate the CA certificate on the FortiClient computer.
4. Click OK.
   The CA certificate is displayed on the CA Certificates list. The expiration date of the certificate is listed in the Valid To column.

Getting a CRL

A CRL is a list of CA certificate subscribers paired with digital certificate status. The list contains the revoked certificates and the reason(s) for revocation. It also records the certificate issue dates and the CAs that issued them.

The FortiClient software uses the CRL to ensure that the certificates belonging to the CA and the remote VPN peer are valid.

To retrieve the CRL

1. Connect to the CA web server.
2. Follow the CA web server instructions to download the CRL.

To import the CRL

1. Go to **VPN > CRL**.
2. Click Import.
3. Enter the path or browse to locate the CRL on the FortiClient computer.
4. Click OK.
   The CRL is displayed on the CRL list.

Configuring the FortiClient software

The FortiClient default settings are compatible with those of the FortiGate unit. You can just enter the following basic required information.

To configure the FortiClient VPN settings

1. Go to **VPN > Connections**.
2. Click Add.
3. For Connection Name, enter FortiGate.
4. For Remote Gateway, enter 172.16.83.89.

5 For Remote Network, enter 10.100.1.0/255.255.255.0.

6 For Authentication Method, select X509 Certificate.

7 Select the certificate.

8 Click OK.

For other configuration options, see "To configure the FortiClient VPN settings" on page 10.

Configuring eXtended Authentication

Extended Authentication (XAuth) is an enhancement to the existing IKE protocol. It allows users to be authenticated in a separate exchange held between Phases 1 and 2.

When setting up the FortiClient to FortiGate VPN, you can use XAuth for extra security. The FortiGate unit is configured as the XAuth server and the FortiClient user is the XAuth client.

Configuring the FortiGate unit

If the FortiGate unit is configured as an XAuth server, it will authenticate remote FortiClient user by referring to a user group. The users contained in the user group can be configured locally on the FortiGate unit or on remotely located LDAP or RADIUS servers.

To configure the FortiGate unit as an XAuth server

1 Go to **User > Local** to add the FortiClient user. The FortiGate XAuth server will use the user name and password to challenge the FortiClient user at the beginning of VPN negotiations. You can also add the FortiClient users the Radius or LDAP servers then go to **User > RADIUS** or **User > LDAP** to add the servers.

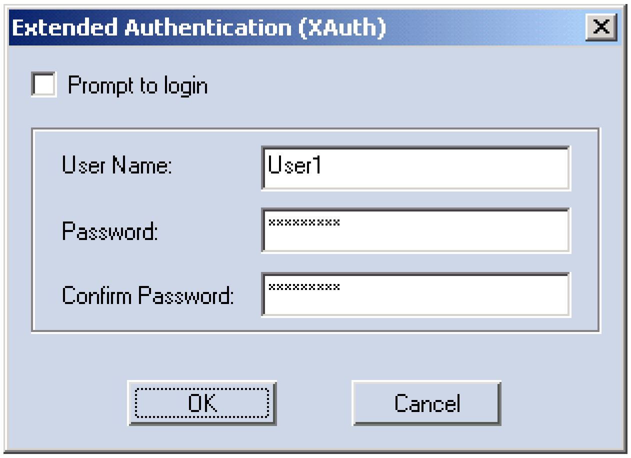
2 Go to **User > User Group** to create a group and add the FortiClient user, the Radius Server, or the PDAP server to the group.

3 When configuring the IPSec VPN Phase 1 settings, select Enable as Server under XAuth and select the user group which contains the FortiClient user.

Configuring the FortiClient software

If the remote FortiGate unit is configured as an XAuth server, it will require the FortiClient software to provide a user name and password when a VPN connection is attempted. The user name and password are defined by the XAuth server. They can be saved as part of an advanced VPN configuration, or they can be manually entered every time a connection is attempted.

Figure 7: Configuring eXtended authentication



□ Prompt to login

User Name: User1

Password: *********

Confirm Password: *********

To configure XAuth

1. Go to **VPN > Connections**.
2. Click Add to add a new connection, or click Edit to edit an existing connection.
3. Click Advanced.
4. In the Advanced Settings dialog box, click Config for eXtended Authentication.
5. In the Extended Authentication dialog box, do one of the following:
   - If you want to enter the login user name and password for each VPN connection, select Prompt to login. When prompted to log in, you can select the password saving option so that you do not have to enter the password the next time you are prompted to log in.
   - If you want to save the login user name and password, clear Prompt to login and enter the user name and password.
6. Click OK.