# VPN between Ingate Firewall and PGP Desktop Security

Tested versions: Ingate Firewall 2.6.0 with Ingate VPN
PGP Desktop Security 7.0 (called PGP in this document)

## 1. Create an X.509 certificate

This can be done in various ways, depending on what CA is used. Below is a description of how to do it with OpenSSL. We do not recommend any special CA. If you use one of the bigger CA:s on the market, the PGP client will support them to a certain extent, which could make administration easier in a network with a lot of clients.

- Create a PKCS-12 file (.p12) using some CA. Note that this file contains the public as well as the private part of the key, which means that you should handle it carefully.
- Run PGPkeys, select **Keys** -> **Import** and import the .p12 file.
- Sign the certificate by selecting **Keys** -> **Sign**.

## 2. Export the client’s public key

Your Ingate Firewall must have the public part of the client’s X.509 certificate. You can get this directly from the Ca or export it from the PGP client like this:

- Select the client’s X.509 certificate.
- Select **Keys** -> **Export**. The public key will be saved to a text file which you can paste in the Ingate Firewall GUI..

## 3. Import the Ingate Firewall certificate into PGP

- Export the public X.509 certificate from the firewall as a .pem file.
- Run PGPkeys.
- Select **Keys** -> **Import** and import the .pem file from the firewall.
- Select the X.509 certificate you just imported, and select **Keys** -> **Sign**, to verify that you trust this certificate..

## 4. Configure the VPN tunnel

You configure the VPN tunnel itself with the PGPnet tool.

- Select the **VPN** tab and click **Add**. The client must be active when you add a network. You start the client by clicking on the shield in the upper right corner.
- Enter a name for the firewall at the other end of the tunnel. It doesn’t matter what name you enter.
- Enter the IP address that was selected as **Local side** under the **VPN Peers** tab
- Select **Secure Gateway** and click on X.**509 Certificate**. You will get a list of imported certificates. Select the certificate from Ingate Firewall.
- Select **Ok**, which will end the configuration of a secure gateway in PGPnet. Select the gateway you just created and select **Add**.
- Now it’s time to configure the network behind the firewall. Start with entering a name of the network.
- Select **Insecure Subnet** and enter the IP address and the netmask for the network behind the firewall. This information should be the same as was entered as **Local side of network** under the **Tunneled networks** tab in Ingate Firewall.
- Select **Ok**, which will end the configuration of the tunneled network.

# 5. PGP Options

Some configuration is needed under Options.

- Enter the client’s own X.509 certificate under the **VPN Authentication** tab. Select **Select Certificate** and select the client’s private key.

Some encryption parameters are needed under the **VPN Advanced** tab.

- Nothing needs to be changed under **Allowed remote Proposals**. You can allow most things.
- Under **Proposals** -> **IKE** there should be an option containing ’RSA Signature’, ’SHA’, TripleDES’, ’1536’.
- Under **Proposals** -> **IPSec** there should be an option containing ’None, MD5, TripleDES’, ’None’.
- Select ’1536’ for **Perfect Forward Secrecy**.
- Finally you should give a value for the key renegotiation time, under the **VPN** tab.
- Go to **IKE** -> **Duration** and enter the same time as for ISAKMP key lifetime under the **VPN peers** tab in the Ingate Firewall.
- Go to **IPSec** -> **Duration** and enter the same time as for IPSec key lifetime under the **Tunneled Networks** tab in the Ingate Firewall. Do not select ’Megabytes’.