Instructions for configuring a SafeNet/Soft-PK client for use with an Ingate Firewall

Tested versions: Ingate Firewall 2.6.1, Ingate Firewall 3.0.2
SafeNet/Soft-PK, Secure VPN Client Version 5.0.2 (Build 2), 6.1.0 (Build 10)

1. Install the software on the client machine according to instructions

Note that the client must support the 3DES encryption algorithm, product number PI-IPSECNT at MBG Electronics.

2. Start the Certificate Manager

- Click **Request Certificate** under **My Certificates**. Answer **Yes** when asked if you want to make a file based request.
- Fill in the form
- Click **Browse** and enter a name and location for the file.
- Click **OK**. Now a certificate request file is created at the location of your choice.
- Sign the certificate request at a Certifying Authority, CA. (See separate documentation on how to set up a CA.)
- Copy the signed certificate and the public certificate of the CA to the client machine.
- Some CA software gives more information in the certificate file than the SafeNet client needs. If the client isn't able to import the certificate, you can load it into a text editor (for example, Notepad under Windows) and delete any text before the '-----BEGIN CERTIFICATE-----' and after the '-----END CERTIFICATE-----' lines.
- Import the CA certificate like this: Click **Import Certificate** under **CA Certificates** and select the file. Check in the new dialogue window that it is the right certificate, and click **yes** when you are sure everything is OK. You will be asked to type a password.
- Import the client certificate like this: Click **Import Certificate** under **My Certificates**. Make sure that the **Import Private Key** option isn't selected. Click **Browse** in the **Certificate** box and select the file. Check in the new dialogue window that it is the right certificate, and click **yes** when you are sure everything is OK.

3. Log on to Ingate Firewall

This is a short guide. For more details, consult chapter 10 in the Ingate Firewall User Manual.

- Go to the **Local X.509 certificate** page. Create a local X.509 certificate for the firewall, if you haven't already done this. Do not enter any e-mail address; the SafeNet client might react funny.
- Go to the **VPN peers** page. Create a new row for the client. Import the client certificate under **Authentication info**. Enter '*' in the **Remote side** field.
- Go to the **Tunneled networks** page. Create a new network with the computers that should be reachable through the VPN tunnel. Make a separate row in the network for the firewall's Authentication server if you use RADIUS authentication. Enter '*' in the **Remote side of network: Network number** field and leave the **Remote side of network: Netmask** field empty. You must enter a value in the **IPSec key lifetime** field if you use SafeNet version 8.
- Go to the **Networks and Computers** page under **Firewall rules** and create a new network, which contains at least all IP addresses that the client will be able to use. Select '−' as the **Interface**.
- Go to the **Rules** page and create new rules for the VPN traffic. If the rule concerns traffic from the VPN client to the local network, select the client as VPN peer under **From VPN**. If the rule concerns traffic from the local network to the VPN client, select the client as VPN peer under **To VPN**. The rest of the settings work just as with ordinary firewall rules.
- Apply the configuration on the **Save/Load configuration** page under **Administration**.

- Download the firewall certificate and transfer it to the SafeNet client.
- Import the certificate under **CA Certificates** as described above.

4. Start the Security Policy Editor

4.1. Create a New Connection

Give the connection a name of your choice.

In the **Connection Security** box:

- Select **Secure**.

In the **Remote Party Identity and Addressing** box:

- **ID Type** = IP subnet
- **Subnet** = The network address for the network behind the firewall, the same as in **Tunneled networks - Local side of network**.
- **Mask** = The network mask for the network above.
- **Protocol** = We suggest you select **All** and do any filtering in the firewall itself.
- Select **Connect using Secure Gateway Tunnel**
- **ID type** = Distinguished Name
- Enter the IP address of the interface used on the firewall (see **VPN peers** - **Local side**).
- Click **Edit Name** and enter the **Distinguished Name** (the same as was entered when the firewall certificate was created).

4.2. Under Security Policy

- Select **Main mode**
- Select **Enable Perfect Forward Secrecy (PFS)**
- **PFS Key Group** = 2 or 5. The firewall will accept any of those two.
- Select **Enable Replay Detection**

4.3. Under My Identity

- Select the previously imported certificate (under **My Certificates**) at **Select Certificate**.
- Check that the **ID Type** is **Distinguished Name**.

4.4. Under Security Policy - Authentication (Phase 1) - Proposal 1

- **Encrypt Alg** = Triple DES
- **Hash Alg** = SHA-1 or MD-5
- **SA Life** = Seconds. Set the same time as the firewall’s **ISAKMP key lifetime** (the **VPN peers** tab).
- **Key Group** = 2 or 5. The firewall will accept any of those two.

4.5. Under Security Policy - Key Exchange (Phase 2) - Proposal 1

- **SA-Life** = Seconds. Set the same time as the firewall’s **IPSec key lifetime** (the **Tunneled Networks** tab).
- Select Enc**apsulation Protocol (ESP)**
- **Encrypt Alg** = Triple DES
- **Hash Alg** = SHA-1 or MD-5
- **Encapsulation** = Tunnel

5. Activate the tunnel

- Save the changes.
- Right-click on the SafeNet icon in the bottom list and select **Deactivate Security Policy**.
- Right-click again and select **Activate Security Policy**.

When you try to connect to a network behind the VPN tunnel, the VPN connection is automatically established.

6. Tunnling more than one network through the same VPN tunnel

Several networks can easily be tunneled using the same VPN tunnel.

6.1. The firewall side

On the **Tunneled Networks** page (refer to paragraph 3), create a **Peer** and enter the first pair of networks (a pair consists of one remote network and one local network). Then, press the plus sign in the **Name** column for this peer. This creates a new row, where next network can be entered.

6.2. The client side

Create one **New Connection** for each pair of tunneled networks (a pair consists of one remote network and one local network/computer).

7. Troubleshooting

7.1. The client certificate can’t be imported to the firewall

Check the certificate in a text editor (Notepad or similar) and ensure that there is no other information in the file except for the certificate itself, which starts with `-----BEGIN CERTIFICATE-----` and ends with `-----END CERTIFICATE-----`.

7.2. The firewall certificate ends up in My Certificates in the client

This happens when the firewall certificate was signed by an external CA (as opposed to a self-signed firewall certificate). In this case, you don’t have to import the firewall certificate, but instead the external CA certificate.

8. Miscellaneous

When you test the client, start the **Log Viewer** by clicking the icon in the lower right corner. The log info will be shown in a small window. If **Log Viewer** is turned off, the log information will not be stored anywhere.

If you use RADIUS authentication, you must begin a VPN session with contacting the authentication server using https.