

SafeNet/ Soft-PK

Interoperability Guide

Copyright © 2004, F/X Communications. All Rights Reserved. The use and copying of this product is subject to a license agreement. Any other use is strictly prohibited. No part of this publication may be reproduced, transcribed, or translated into any language, in any form by any means without the prior written consent of F/X Communications. Information in this document is subject to change without notice and does not constitute any commitment on the part of F/X Communications.

F/X Communications, Brolaeggerstraede 12, DK-4300 Holbaek, Denmark.

Contents

1. SafeNet/Soft-PK for Win 9x/NT	3
1.1. Important notice	3
1.2. Brief step-by-step instructions	3
1.3. Host to Host Case	3
Adding the Remote Host	3
Configuring the InJoy side	4
Connecting to the InJoy side	5
1.4. Host to Gateway case	5
Adding Remote Gateway	5
Configuring the InJoy side	7
Connecting to InJoy side	7

1. SafeNet/Soft-PK for Win 9x/NT

1.1. Important notice

The connections in the following tests were conducted over a LAN, using 192.162.x.x IP addresses for the IPSec endpoints. 192.168.x.x addresses were used to illustrate internal networks (behind IPSec endpoints). When modifying these samples for Internet use, replace the 192.162.x.x addresses with the external IP addresses of the IPSec endpoints.

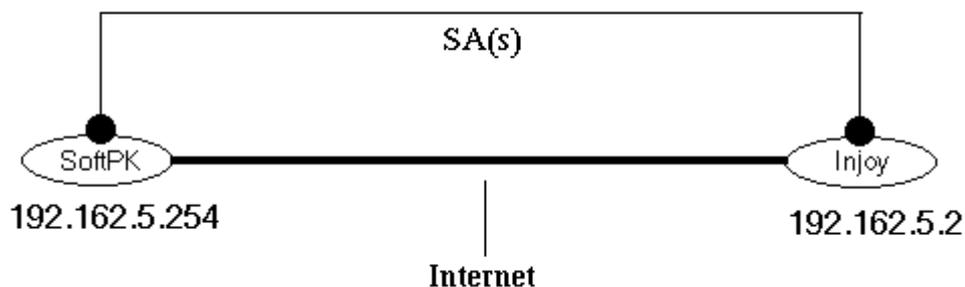
1.2. Brief step-by-step instructions

In order to create a Virtual Private Network using the InJoy IPSec Plugin and soft-PK client, the following steps must be completed:

- 1 Install the SafeNet/Soft-PK client on a Windows PC (Local Host).
- 2 Install an InJoy product with IPSec ("**Remote Host**").
- 3 Install the Pluto IKE server on the InJoy PC.
- 4 Configure the SafeNet/Soft-PK client.
 - 4.1 Define whether the Remote Host is a stand-alone or a secure gateway for the corporate network.
 - 4.2 Start the SafeNet/Soft-PK Security Policy Editor.
 - 4.3 Add the SA description (refer to the sections [Host to Host](#) case and [Host to Gateway](#) case accordingly)
- 5 Configure the InJoy IPSec side.
- 6 Restart the InJoy IPSec product and the IKE server.
- 7 Trigger the SafeNet/Soft-PK client to establish SA. (note: any traffic between IPSec endpoints will force this).

1.3. Host to Host Case

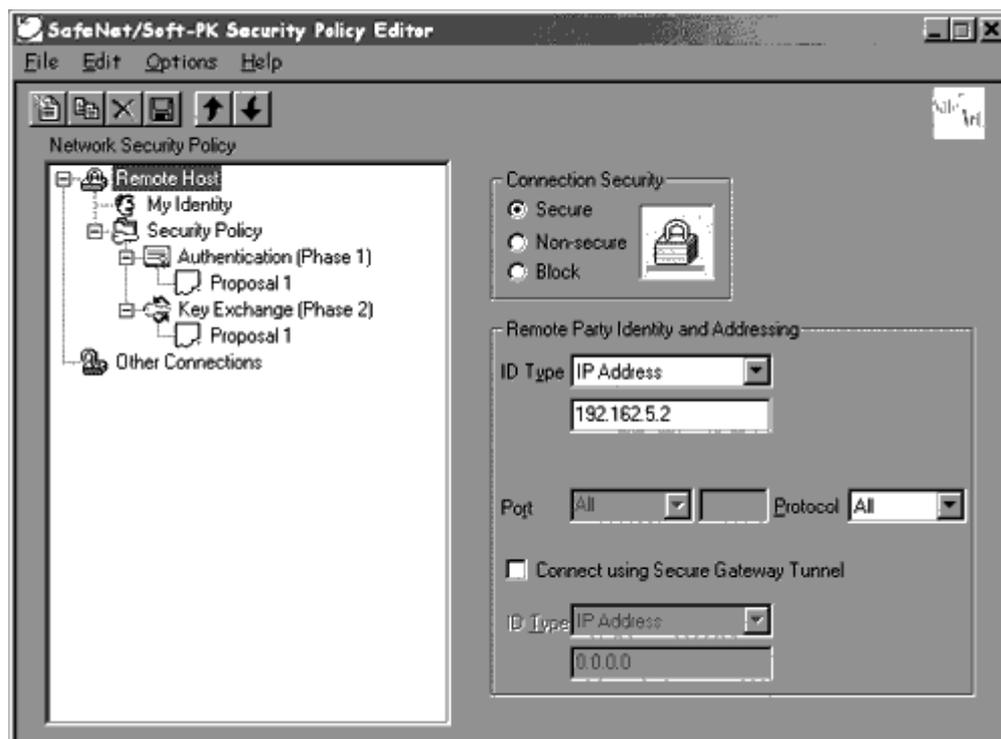
Adding the Remote Host



To configure a Host to Host connection with the Remote Host, complete the following steps:

- 1 Start the SafeNet/Soft-PK Security Policy Editor and press the New button.
- 2 Enter an appropriate description for the Remote Host entry.
- 3 Choose Secure in Connection Security Box.
- 4 Choose IP Address as ID Type.
- 5 Enter IP Address of the Remote Host.
- 6 Select My Identity in the Network Security Policy Window and press the Pre-Shared Key button.
- 7 Enter the preshared secret. The same secret will be used on the Remote Host.
- 8 If necessary, add/change Proposals on the Authentication and Key Exchange Pages. At present, default values are compatible with the InJoy side.
- 9 Save changes.

Adding a Remote Host and Entering Host Parameters:



Configuring the InJoy side

On the Remote Host (InJoy side), add the following section to ipsec.conf. It describes the SA to use with the spkNet client:

```
spk-end
    Description = "SafeNet / SoftPK",
```

```

Mode = Tunnel,
Local-IP = "192.162.5.2",      # local host IP address
Remote-IP = "192.162.5.254", # remote host IP address
AH = Yes,
ESP = Yes,
Reinit = Yes,
Preshared-Secret = "secret_phrase",

```

Restart the InJoy IPsec side for changes to take effect.

Connecting to the InJoy side

Any traffic to the Remote Subnet behind the Gateway will trigger IKE negotiations. When the SA is established, it can be seen in the Log Viewer Window.

On the Remote Host, the ipsec.log will contain the following lines:

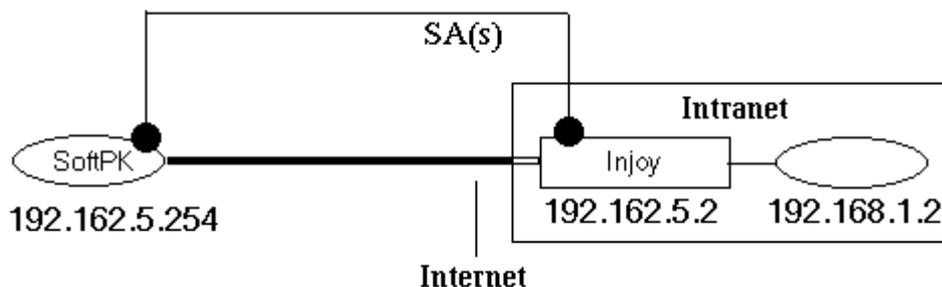
```

Mar 1 05:14:01 : IPSEC Init -----
Mar 1 05:14:01 : PlugIn version: 1.41
Mar 1 05:14:07 : Dll caller inited us with ip: 192.162.5.2
Mar 1 05:14:07 : adding to pluto: softpk-end
Mar 1 05:14:08 : routing for pluto: softpk-end
Mar 1 05:14:36 : ipsec: install sa [softpk-end]
Mar 1 05:14:36 : SA name = [softpk-end]
Mar 1 05:14:36 : Local gateway (host) ip address = [192.162.5.2]
Mar 1 05:14:36 : Local net = [192.162.5.2]
Mar 1 05:14:36 : Local net mask = [255.255.255.255]
Mar 1 05:14:36 : Remote gateway (host) ip address = [192.162.5.254]
Mar 1 05:14:36 : Remote net = [192.162.5.254]
Mar 1 05:14:36 : Remote net mask = [255.255.255.255]
Mar 1 05:14:36 : SA lifetime = [3600] seconds
Mar 1 05:14:36 : ESP encr/auth/keylen=[ESP_ALG_CBC_DES/AH_ALG_SHA1/28]
Mar 1 05:14:36 : AH method/keylen = [unknown/0]
Mar 1 05:14:36 : Road Warrior = [no]

```

1.4. Host to Gateway case

Adding Remote Gateway

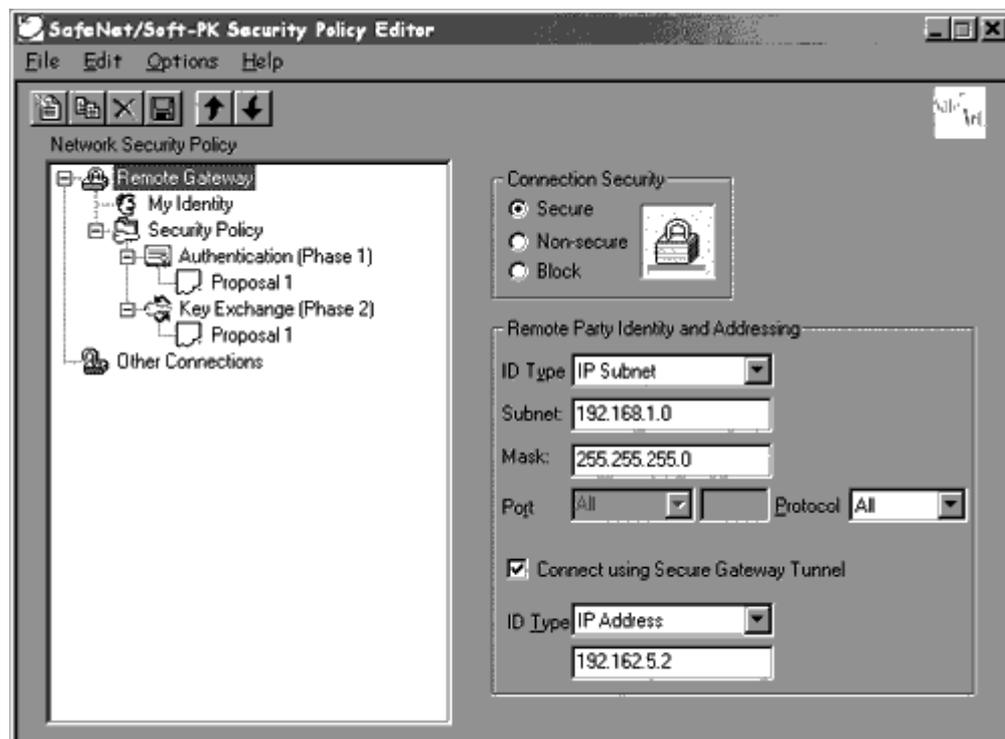


To configure the Host to Gateway connection with the Remote Gateway (InJoy side), complete the following steps:

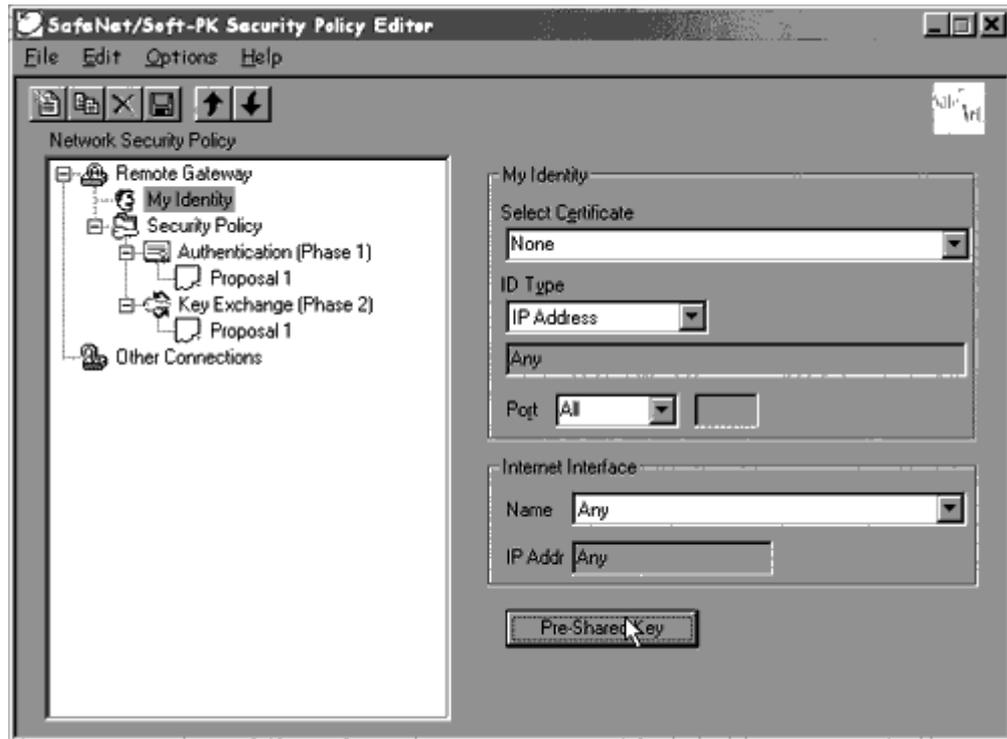
- 1 Start the SafeNet/Soft-PK Security Policy Editor and press the New button.
- 2 Enter an appropriate description for the Remote Gateway entry.

- 3 Choose Secure in the Connection Security Box.
- 4 Choose IP Subnet as ID Type.
- 5 Enter Subnet and Mask.
- 6 Check Connect Using Secure Gateway box and enter Remote Gateway IP address.
- 7 Select My Identity in the Network Security Policy Window and select Pre-Shared Key.
- 8 Enter the preshared secret. The same secret will be used on the Remote Host.
- 9 If necessary add/change Proposals on the Authentication and the Key Exchange Pages. At present, the default values are compatible with InJoy.
- 10 Save changes.

Adding the Remote Gateway and entering Gateway Parameters:



Adding the Remote Gateway. Selecting preshared secret:



Configuring the InJoy side

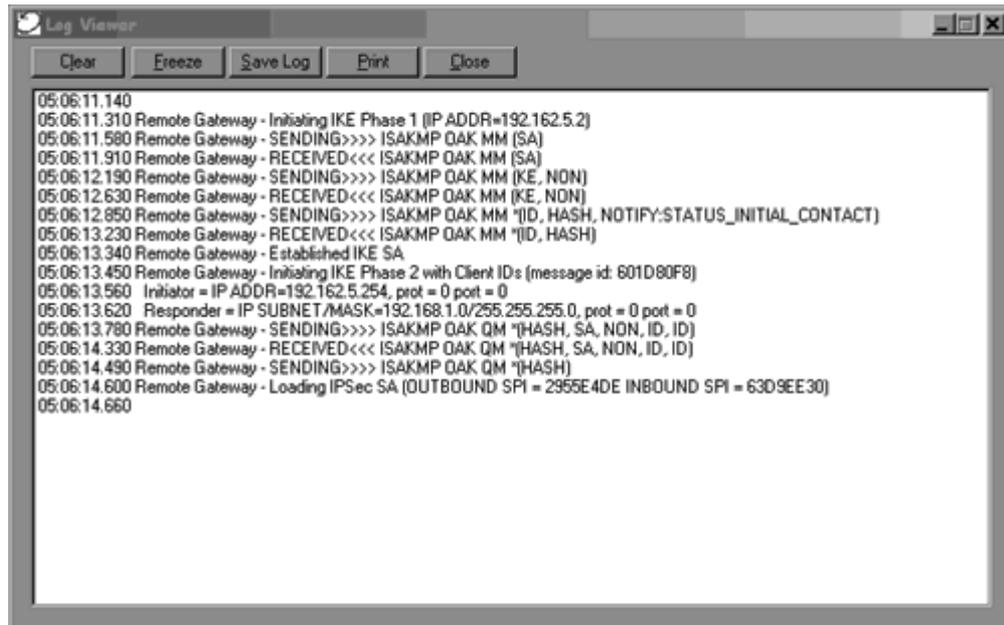
On the Remote Host (InJoy side), add the following section to the ipsec.cnf file. The section defines the SA to be used with the spkNet client:

```
softpk-client
    Description = "SoftPK client",
    Mode = Tunnel,
    Local-IP = "192.162.5.2",      # local host IP address
    Local-Net = "192.168.1.0",
    Local-Mask = "255.255.255.0",
    Remote-IP = "192.162.5.254", # remote host IP address
    Exclude_Local_IP = Yes,      # gateway is not part of SA bundle
    AH = Yes,
    ESP = Yes,
    Reinit = Yes,
    Preshared-Secret = "secret_phrase",
```

Restart InJoy IPsec side for changes to take effect.

Connecting to InJoy side

Any traffic to the Remote Subnet behind the Gateway will trigger IKE negotiations. When the SA is established, it can be seen in the Log Viewer Window:



On the Remote Host, the ipsec.log will contain the following lines:

```

Mar 1 05:09:25 : IPSEC Init -----
Mar 1 05:09:25 : PlugIn version: 1.41
Mar 1 05:09:28 : Dll caller inited us with ip: 192.162.5.2
Mar 1 05:09:28 : adding to pluto: softpk-client
Mar 1 05:09:28 : routing for pluto: softpk-client
Mar 1 05:09:35 : ipsec: install sa [softpk-client]
Mar 1 05:09:35 : SA name = [softpk-client]
Mar 1 05:09:35 : Local gateway (host) ip address = [192.162.5.2]
Mar 1 05:09:35 : Local net = [192.168.1.0]
Mar 1 05:09:35 : Local net mask = [255.255.255.0]
Mar 1 05:09:35 : Remote gateway (host) ip address = [192.162.5.254]
Mar 1 05:09:35 : Remote net = [192.162.5.254]
Mar 1 05:09:35 : Remote net mask = [255.255.255.255]
Mar 1 05:09:35 : SA lifetime = [3600] seconds
Mar 1 05:09:35 : ESP encr/auth/keylen=[ESP_ALG_CBC_DES/AH_ALG_SHA1/28]
Mar 1 05:09:35 : AH method/keylen = [unknown/0]
Mar 1 05:09:35 : Road Warrior = [no]

```

When the SA is established, you will be able to communicate with hosts in the subnet associated with the Remote Gateway. The SafeNet/Soft-PK client does not count the Remote Gateway as part of the SA bundle, leaving all traffic that is destined to the Remote Gateway itself (not subnet behind) unprocessed. The same applies to traffic from the Remote Gateway, which is NOT considered IPsec traffic. The InJoy IPsec implementation does NOT discriminate traffic from the gateway in any way. To redefine the default behavior of the InJoy IPsec and achieve compatibility with SafeNet/Soft-PK client, you must use the **Exclude_Local_IP = Yes** setting.

An alternative approach is to define an alias IP address for the Gateway, which belongs to the subnet address space and communicate with the Gateway using that address. When the internal address of the Remote Gateway (e.g. 192.168.1.1) is used, IPsec processing is applied.