

# PGPNet

## 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

---

<b>1. PGP 6.5.2a for Win 9x/NT/2000</b> .....	<b>3</b>
1.1. Important notice .....	3
1.2. Brief step-by-step instructions .....	3
1.3. Configuring PGP Options .....	3
1.4. Host to Host Case .....	5
Adding Remote Host .....	5
Configuring the InJoy side .....	7
Connecting to the InJoy side .....	8
1.5. Host to Gateway case .....	9
Adding Remote Gateway .....	9
Configuring the InJoy side .....	11
Connecting to the InJoy side .....	11

# ***1. PGP 6.5.2a for Win 9x/NT/2000***

---

## ***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.

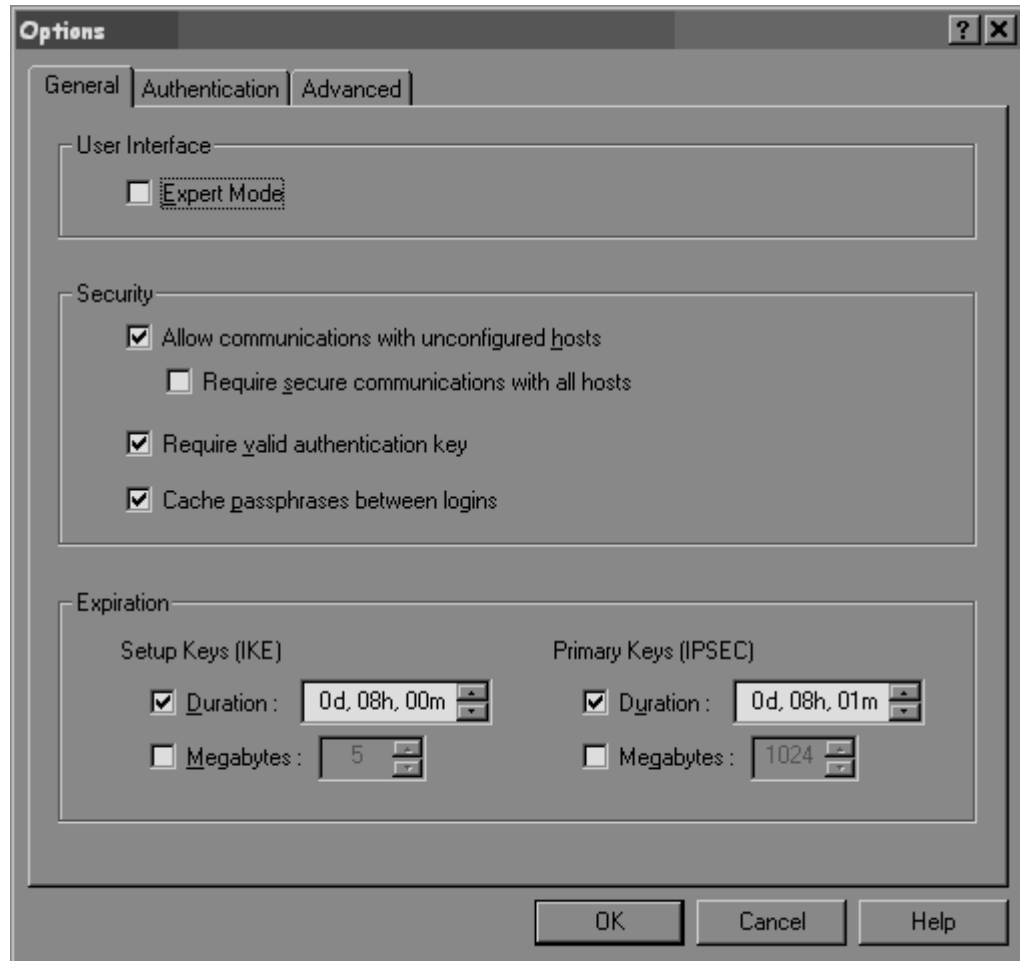
## ***1.2. Brief step-by-step instructions***

**To create a VPN using the InJoy IPSec and the PGPNet client, the following steps must be completed:**

- 1 Install the PGPNet client on a Windows PC ("Local Host").
- 2 Install an InJoy product with IPSec ("Remote Host").
- 3 Install the Pluto IKE server on InJoy PC.
- 4 Configure the PGPNet client.
  - 4.1 Configure the General and the Advanced Options.
  - 4.2 Define whether Remote Host is stand-alone or secure gateway for a corporate subnet.
  - 4.3 Add SA description (refer to 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 PGPNet to establish SA. (note: any traffic between IPSec endpoints will force this).

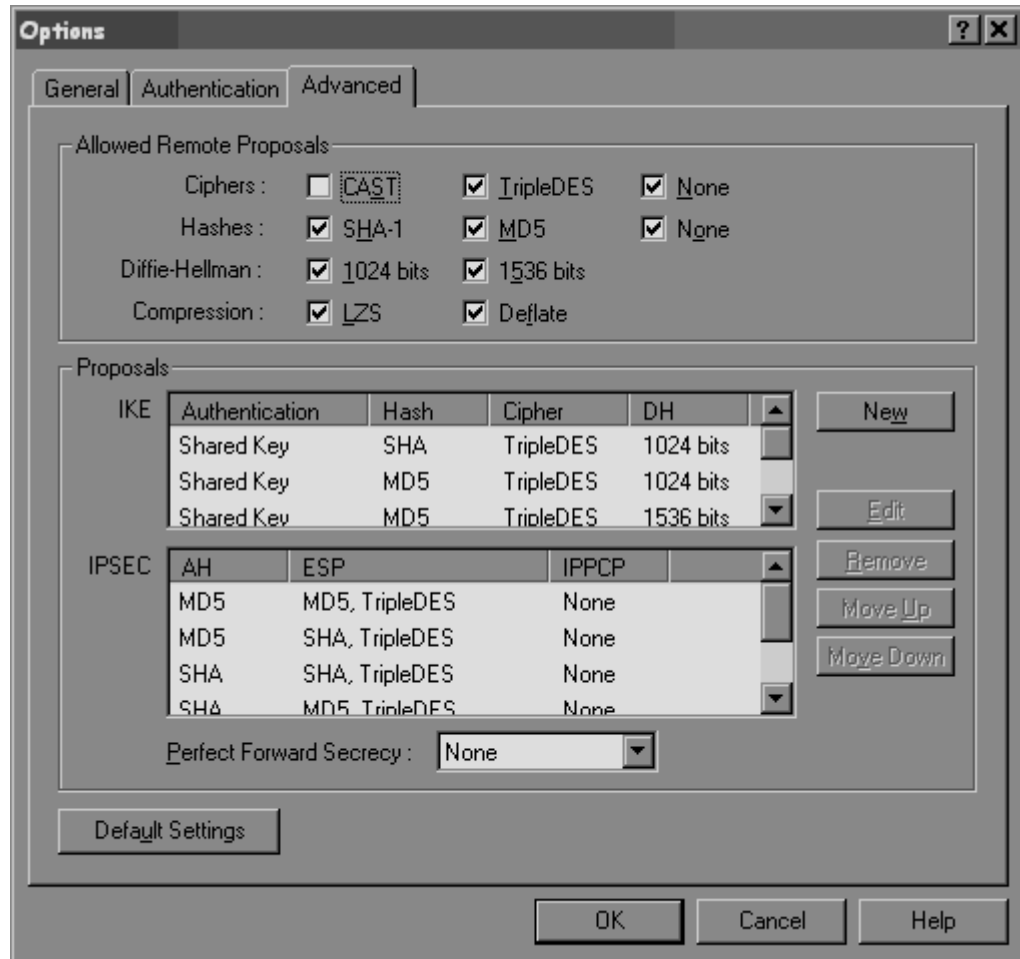
## ***1.3. Configuring PGP Options***

Select View->Options from the PGPNet menu. You will see the Options notebook. Check the "Allow communications with unconfigured hosts" box. Also the Duration of IKE keys renegotiations must be 8 hours or less, as greater values are insecure and the Pluto IKE server rejects them.



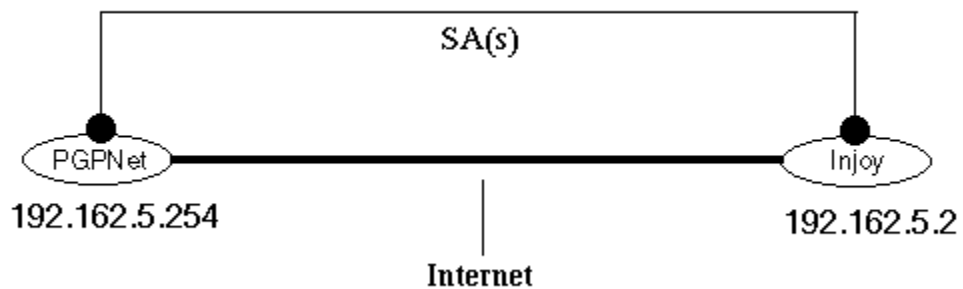
Go to the **Advanced** page of the **Option** notebook and configure proposals compatible with the InJoy IPsec implementation. Disable CAST cipher and all proposals based on it. Valid combinations must be based on DES or TripleDES as Cipher, and MD5 and SHA as authentication hashes.

**Example below shows a working configuration:**



## 1.4. Host to Host Case

### *Adding Remote Host*

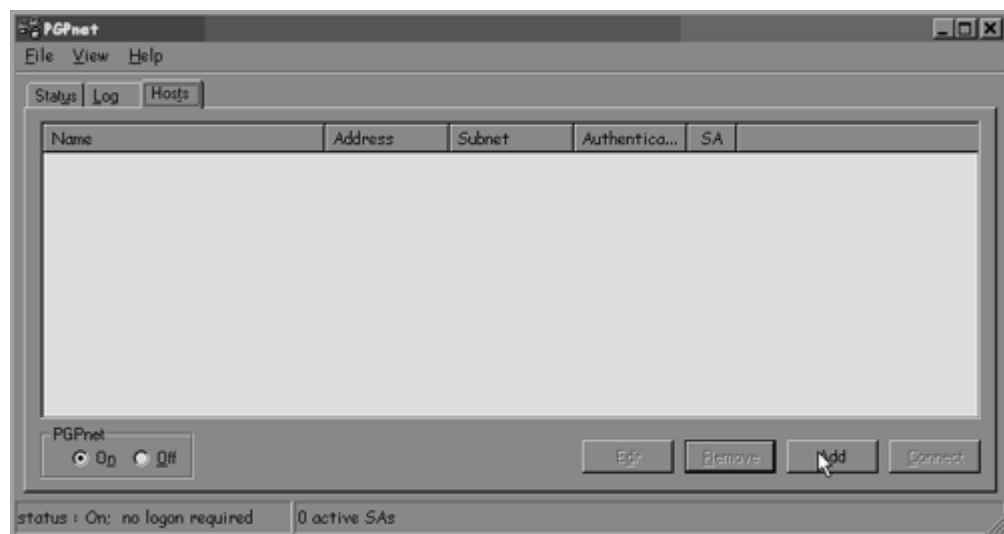


**To configure a Host to Host connection with the Remote Host, complete the following actions:**

- 1 Go to the Hosts page and press the **Add** button.
- 1 When the Connection Wizard dialog appears, select the **Host** item.
- 2 Click Next button and choose "**Enforce secure communications**".
- 3 Click **Next** button and fill in an appropriate description of the Remote Host.

- 4 Click **Next** button and **enter** the IP address of the Remote Host.
- 5 Click **Next** button and choose the shared secret field.
- 6 You now need to enter the shared secret that will be used to authenticate IKE negotiations with the Remote Host. The same secret must be used on the Remote Host. **Do not use "secret\_phrase" as in the example below!**
- 7 Click **Next** button and Select the IP address as identification method for authentication.
- 8 Click **Next** button and when the "Congratulations!" screen appears, click on the **Finish** button.

**Adding Remote Host. Adding entry on Host page:**



**Adding Remote Host. Selecting Host entry:**



```

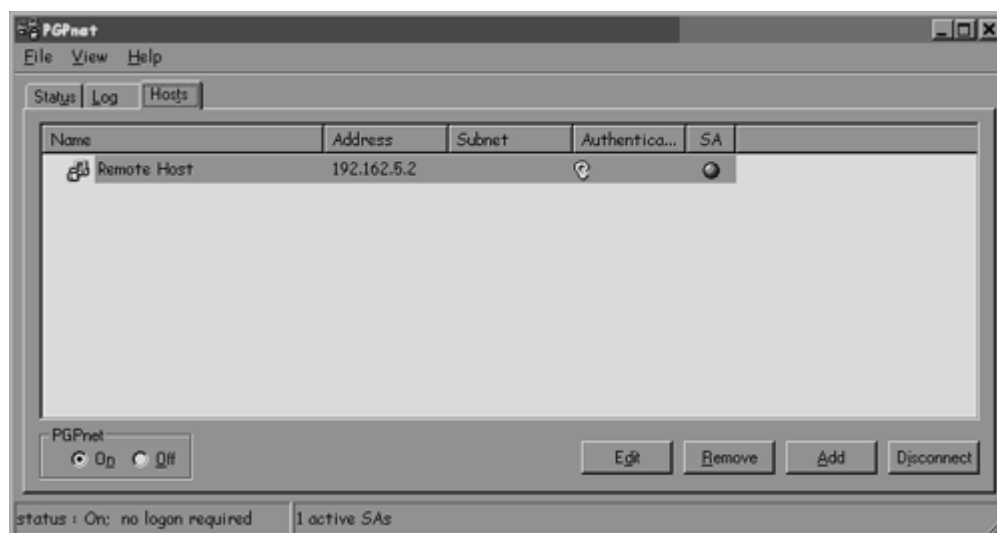
pgp-end
Description = "PGP link",
Mode = Transport,
Local-IP = "192.162.5.2", # local host IP address
Remote-IP = "192.162.5.254", # remote host IP address
AH = Yes,
ESP = Yes,
Reinit = Yes,
Preshared-Secret = "secret_phrase",

```

Restart the InJoy IPsec product and the Pluto IKE server for changes to take effect.

### *Connecting to the InJoy side*

To establish the IPsec connection to the Remote Host, select it from the Hosts Page and press the Connect button. When the SA will be established, a green dot appears at the right side of the Remote Host entry.



You can check the SA parameters on the Status page.

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

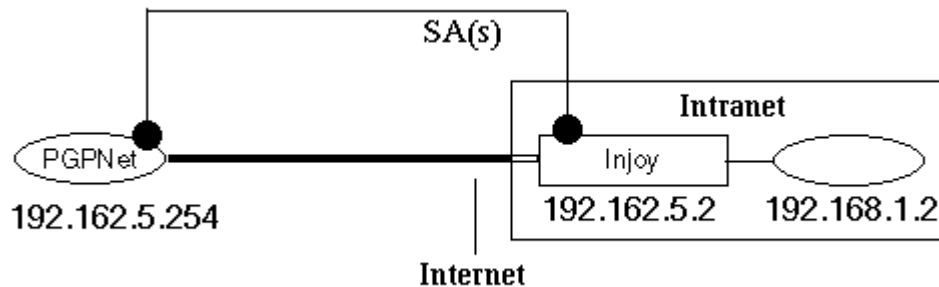
```

Feb 23 07:00:23 : IPSEC Init -----
Feb 23 07:00:23 : PlugIn version: 1.40
Feb 23 07:00:27 : Dll caller inited us with ip: 192.162.5.2
Feb 23 07:00:27 : adding to pluto: pgp-end
Feb 23 07:00:27 : routing for pluto: pgp-end
Feb 23 07:02:29 : ipsec: install sa [pgp-end]
Feb 23 07:02:29 : SA name = [pgp-end]
Feb 23 07:02:29 : Local gateway (host) ip address = [192.162.5.2]
Feb 23 07:02:29 : Local net = [0.0.0.0]
Feb 23 07:02:29 : Local net mask = [255.255.255.255]
Feb 23 07:02:29 : Remote gateway (host) ip address = [192.162.5.254]
Feb 23 07:02:29 : Remote net = [0.0.0.0]
Feb 23 07:02:29 : Remote net mask = [255.255.255.255]
Feb 23 07:02:29 : SA lifetime = [28800] seconds
Feb 23 07:02:29 : ESP encr/auth/keylen=[ESP_ALG_CBC_3DES/AH_ALG_MD5/40]
Feb 23 07:02:29 : AH method/keylen = [AH_ALG_MD5/16]
Feb 23 07:02:29 : Road Warrior = [no]

```

## 1.5. Host to Gateway case

### Adding Remote Gateway



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

- 1 Go to the **Hosts** page and press the **Add** button.
- 2 When the **Connection Wizard** dialog appears, select **Gateway**.
- 3 Click **Next** button and fill in an appropriate description of the Remote Host.
- 4 Click **Next** button and enter the IP address of the Remote Host.
- 5 Click **Next** button and choose the shared secret field. You now need to enter the shared secret that will be used to authenticate the IKE negotiations. The same secret must be used on the Remote Host. **Don't use "secret\_phrase" as in the example below!**
- 6 Click **Next** button and Select the IP address as identification method for authentication.
- 7 Click **Next** button and Select **Yes** to create host or subnet associated with gateway.
- 8 Click **Next** button and Select Subnet.
- 9 Click **Next** button and Select **"Allow insecure communications"**. It doesn't mean that the communication is "insecure". It means that the Gateway will work as IPsec endpoint and traffic from the PGPNet client to the host behind the gateway will be decrypted and detunneled on the Gateway PC. The data is secured when traversing the Internet.

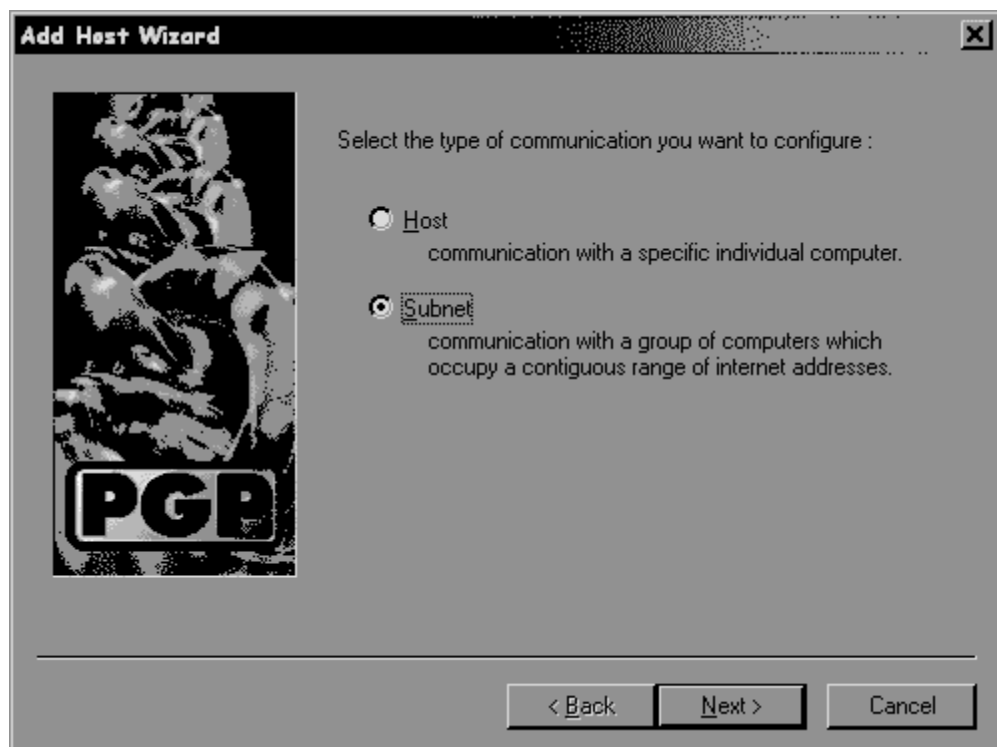
10 Click **Next** button and fill in an appropriate description for the subnet behind the Remote Gateway.

11 Click **Next** button and **enter the IP address and netmask** of the subnet behind the Remote Gateway.

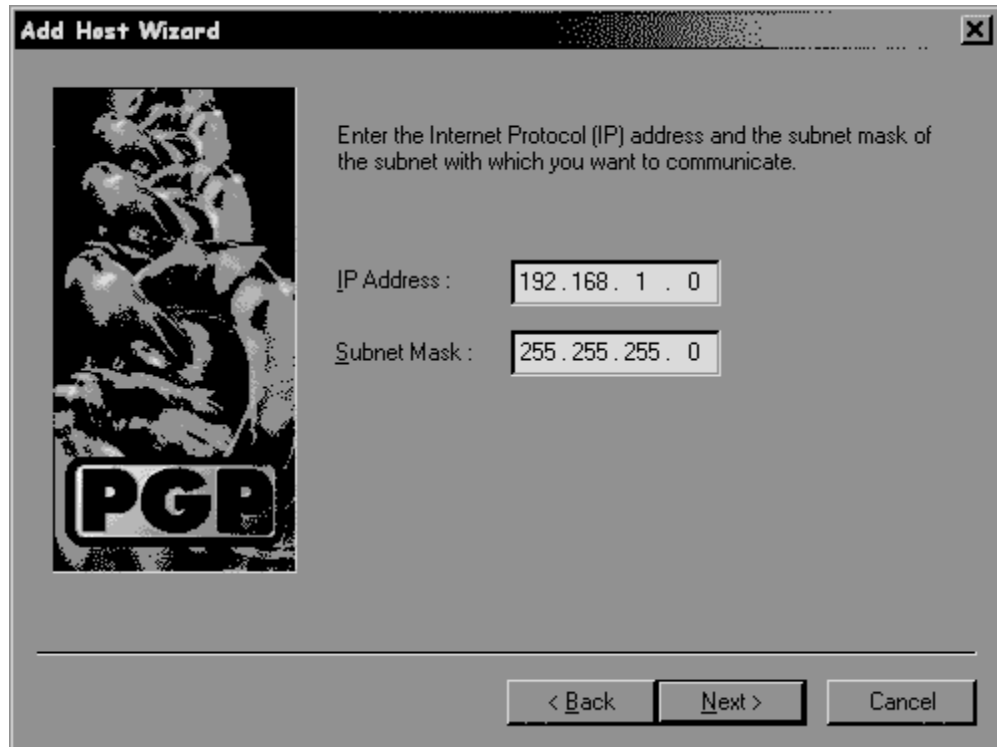
12 Click **Next** button and select **NOT** to add more hosts/subnets associated with gateway.

13 Click **Next** button and when the "Congratulations!" screen appears, click on the **Finish** button.

**Adding Remote Gateway. Selecting Subnet entry:**



**Adding Remote Gateway. Entering Subnet parameters:**



### *Configuring the InJoy side*

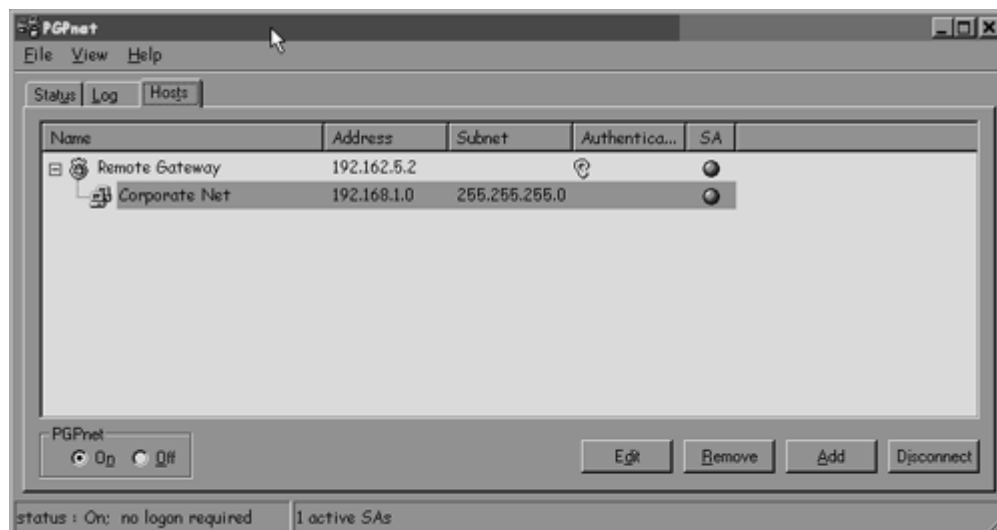
**On the Remote Host (InJoy side), add the following section to ipsec.conf, describing the SA to the PGPNet client:**

```
pgp-client
Description = "PGP 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
AH = Yes,
ESP = Yes,
Reinit = Yes,
Preshared-Secret = "secret_phrase",
```

Restart InJoy IPsec side for changes to take effect.

### *Connecting to the InJoy side*

To establish the IPsec connection, select the Remote Subnet from the Hosts Page and press Connect. When the SA is established, you will see a green dot at the right side of the Remote Gateway and Subnet entries.



You can check SA parameters on the Status page.

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

```
Feb 23 06:41:56 : IPSEC Init -----
Feb 23 06:41:56 : PlugIn version: 1.40
Feb 23 06:41:59 : Dll caller inited us with ip: 192.162.5.2
Feb 23 06:41:59 : adding to pluto: pgp-client
Feb 23 06:41:59 : routing for pluto: pgp-client
Feb 23 06:42:03 : ipsec: install sa [pgp-client]
Feb 23 06:42:03 : SA name = [pgp-client]
Feb 23 06:42:03 : Local gateway (host) ip address = [192.162.5.2]
Feb 23 06:42:03 : Local net = [192.168.1.0]
Feb 23 06:42:03 : Local net mask = [255.255.255.0]
Feb 23 06:42:03 : Remote gateway (host) ip address = [192.162.5.254]
Feb 23 06:42:03 : Remote net = [192.162.5.254]
Feb 23 06:42:03 : Remote net mask = [255.255.255.255]
Feb 23 06:42:03 : SA lifetime = [28800] seconds
Feb 23 06:42:03 : ESP encr/auth/keylen=[ESP_ALG_CBC_3DES/AH_ALG_MD5/40]
Feb 23 06:42:03 : AH method/keylen = [AH_ALG_MD5/16]
Feb 23 06:42:03 : Road Warrior = [no]
```

When the SA is established, you will be able to communicate to hosts in the subnet associated with the Remote Gateway. Due to specifics of PGPNet, you cannot communicate directly with the IPsec Gateway itself. You can however define an alias IP address for the Gateway PC (e.g. 192.168.0.1) which belongs to the subnet address space and communicate "to" (not from) the Gateway using that address.