

# **Linux FreeS/WAN**

## **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.</b> | <b>Linux FreeS/WAN .....</b>          | <b>3</b> |
| 1.1.      | Important notice .....                | 3        |
| 1.2.      | Brief step-by-step instructions ..... | 3        |
| 1.3.      | Configuring Linux FreeS/WAN .....     | 3        |
| 1.4.      | Configuring the InJoy side .....      | 4        |
| 1.5.      | Connecting to the FreeS/WAN.....      | 4        |
| 1.6.      | Road Warriors.....                    | 5        |

# 1. *Linux FreeS/WAN*

---

## 1.1. *Important notice*

The connections in the following tests were conducted over a LAN, using 192.168.x.x IP addresses for the IPsec endpoints. When modifying these samples for Internet use, replace the 192.168.x.x addresses with the external IP address of the IPsec endpoints.

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

**To create a VPN using the InJoy IPsec and Linux FreeS/WAN, the following steps must be completed:**

- 1 Install an InJoy product with IPsec ("**Remote Gateway**").
- 2 Install the Pluto IKE server on the InJoy PC.
- 3 Configure the FreeS/WAN ("**Local Host**").
  - 3.1 Install the FreeS/WAN package as described in its documentation
  - 3.2 Edit the FreeS/WAN configuration files: define the IPsec security association and the pre-shared secret
  - 3.3 Update FreeS/WAN with the updated configuration
- 4 Configure the InJoy IPsec side.
- 5 Restart the InJoy IPsec product and the IKE server.

## 1.3. *Configuring Linux FreeS/WAN*

- 1 Install Linux FreeS/WAN according to the "Installation Guide" section of the official FreeS/WAN documentation
- 2 Edit the `/etc/ipsec.secrets` file as follows:
  - 2.1 `192.168.0.1` is the address of Local Gateway (the Linux FreeS/WAN side)
  - 2.2 `192.168.0.2` is the address of Remote Gateway (the InJoy side)
  - 2.3 `supersecret` is the pre-shared secret of both sides
  - 2.4 `PSK` signifies pre-shared key for FreeS/WAN
- 3 Add a connection description to the `/etc/ipsec.conf` file:

```
# Connection to InJoy
conn injoy
    left=192.168.0.2
    leftsubnet=192.168.0.0/24
    right=192.168.0.1
    rightsubnet=192.162.0.0/24
    auto=add
```

```
pfs=no
```

- 3.1 If you need immediate negotiation after Linux reboots, specify **start** as the value of the **auto** configuration attribute
  - 3.2 If you need delayed negotiation, specify **add** as the value of the **auto** configuration attribute
  - 3.3 More information about the syntax of keys, especially **leftsubnet** and **rightsubnet** keys can be found in the FreeS/WAN documentation and the **man** pages
- 4 Update FreeS/WAN with the new connection definition:
    - 4.1 Update the Pluto IKE Server (a component of FreeS/WAN):

```
[root@libresse etc] # ipsec auto add injoy
```

- 4.2 Re-read the secrets file:

```
[root@libresse etc] # ipsec whack -listen
002 listening for IKE messages
002 forgetting secrets
002 loading secrets from "/etc/ipsec.secrets"
```

- 5 The Linux FreeS/WAN side is ready to negotiate.

## 1.4. *Configuring the InJoy side*

**On the Remote Gateway, add the following section to the file ipsec.cnf:**

```
freeswan
Description = "Linux FreeS/WAN",
Mode = Tunnel,
Local-IP = "192.168.0.1",      # local gateway IP address
Local-Net = "192.162.0.0",
Local-Mask = "255.255.255.0",
Remote-IP = "192.162.0.2",    # remote host IP address
Remote-Net = "192.168.0.0",
Remote-Mask = "255.255.255.0",
AH = No,
ESP = DES,
Reinit = No,
Preshared-Secret = "supersecret",
```

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

## 1.5. *Connecting to the FreeS/WAN*

In case you need the FreeS/WAN to initiate negotiations, use **start** as the value of the **auto** configuration attribute in the connection definition, and **No** as the value of the **Reinit** attribute in the ipsec.cnf (on the InJoy side). To force the InJoy side to trigger negotiations, use **Yes** as the value of the **Reinit** attribute (in ipsec.cnf on the InJoy side), and specify **add** as the value of the **auto** key configuration attribute (on the FreeS/WAN side).

Below, an example of a successfully established tunnel:

Linux side:

```
[root@libresse root] # ipsec whack --initiate --name injoy
002 "injoy"          #30: initiating Main Mode
104 "injoy"          #30: STATE_MAIN_I1: initiate
106 "injoy"          #30: STATE_MAIN_I2: sent MI2, expecting MR2
108 "injoy"          #30: STATE_MAIN_I3: sent MI3, expecting MR3
002 "injoy"          #30: ISAKMP SA established
004 "injoy"          #30: STATE_MAIN_I4: ISAKMP SA established
002 "injoy"          #31: initiating Quick Mode PSK+ENCRYPT+TUNNEL
112 "injoy"          #31: STATE_QUICK_I1: initiate
002 "injoy"          #31: sent QI2, IPsec SA established
004 "injoy"          #31: STATE_QUICK_I2: sent QI2, IPsec SA established
```

InJoy side:

```
18082002 14580500 Install SA :freeswan.
18082002 14580500 SA Name.....: freeswan
18082002 14580500 Authentication.....: IP Address/Preshared Secret.
18082002 14580500 Local IP address.....: 192.168.0.1
18082002 14580500 Local Net.....: 192.162.0.0
18082002 14580500 Local Netmask.....: 255.255.255.0
18082002 14580500 Remote IP address.....: 192.168.0.2
18082002 14580500 Remote Net.....: 192.168.0.0
18082002 14580500 Remote Netmask.....: 255.255.255.0
18082002 14580500 ISAKMP SA lifetime.....: 120 seconds
18082002 14580500 IPSEC SA lifetime.....: 90 seconds
18082002 14580500 ESP encr/auth/keylen.....: 3DES/MD5/40
18082002 14580500 AH method/keylen.....: None/0
18082002 14580500 IPCOMP.....: None
18082002 14580500 Road Warrior.....: No
18082002 14580500 Remote Road Warrior.....: No
```

## 1.6. Road Warriors

It is possible to make any of the sides involved a Road Warrior. Road Warrior is a technique that allows the remote side to use a dynamic IP address (such as with dial-up connections).

### 1 Making InJoy side Road Warrior:

#### 1.1 Edit the connection description as follows:

```
conn injoy
    left=192.168.0.2
    leftsubnet=192.168.0.0/24
    right=%any
    auto=add
    pfs=no
```

#### 1.2 Edit the pre-shared secret definition as follows:

```
192.168.0.2 %any: PSK "supersecret"
```

#### 1.3 Edit the SA on the InJoy side as follows:

```
freeswan
    Description = "Linux FreeS/WAN",
    Mode = Tunnel,
    Local-IP = "0.0.0.0",
    Local-Net = "192.162.0.0",
    Local-Mask = "255.255.255.0",
    Remote-IP = "192.162.0.2",
```

```
Remote-Net = "192.168.0.0",
Remote-Mask = "255.255.255.0",
AH = No,
ESP = 3DES,
Reinit = No,
Preshared-Secret = "supersecret",
```

## 2 Making the FreeS/WAN side Road Warrior:

### 2.1 Edit the connection description as follows:

```
conn injoy
left=%defaultroute
leftsubnet=192.168.0.0/24
right=192.168.0.2
rightsubnet=192.162.0.0/24
auto=add
pfs=no
```

### 2.2 Modify the secrets file exactly as in the previous case

### 2.3 Edit the SA on the InJoy side as follows:

```
freeswan
Description = "Linux FreeS/WAN",
Mode = Tunnel,
Local-IP = "192.168.0.1",
Local-Net = "192.162.0.0",
Local-Mask = "255.255.255.0",
Remote-IP = "0.0.0.0",
AH = No,
ESP = 3DES,
Reinit = No,
Preshared-Secret = "supersecret",
```