

Windows 2000

Windows XP

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. Windows	3
1.1. Important notice	3
1.2. Brief step-by-step instructions	3
1.3. Configuring Windows	4
1.4. Configuring the InJoy side.....	9
1.5. Connecting to Windows.....	9
2. Making Windows Road Warrior	10
2.1. Configuring the InJoy side.....	10
2.2. Configuring Windows	10

1. Windows

1.1. Important notice

The information in this interoperability guide applies to both Windows 2000 and Windows XP.

The connections in the following tests were conducted over a LAN, using 192.168.0.x IP addresses for the IPSec endpoints. The internal network behind the IPSec end-point was also in the 192.168.0.x range, yet any network (like 192.162.1.x) can be used (however – pay strict attention to the wide-ranging limitations below).

The guiding rules/limitations for creating the VPN connection between Windows and InJoy IPSec are:

- **Only one of the two IPSec endpoints can have a network behind it;**
- The Windows XP IPSec does NOT support X-Authentication;
- If the designated IPSec end-point (**with a subnet behind it**) does not belong to the network behind it, it will be inaccessible (e.g. having: 192.162.5.254 as IPSec gateway address and 192.168.1.0 / 255.255.255.0 as internal network – won't work);
- If the endpoint belongs to the network behind it, it will be accessible for both endpoints (example; 192.162.5.254 and 192.162.5.0 / 255.255.255.0);
- If it's the InJoy side that has the subnet behind it and the public IP address (of the InJoy Gateway) doesn't fix the internal network address space, it is suggested to use the Inner-IP feature to remap the public IP address (to an internal address that fits with the internal network behind the InJoy product). **Note that this type of setup has not yet been approved by F/X Communications.**

When modifying these samples for Internet use, replace the internal addresses (such as 192.162.x.x and 192.168.x.x) with the external IP addresses of the IPSec endpoints.

1.2. Brief step-by-step instructions

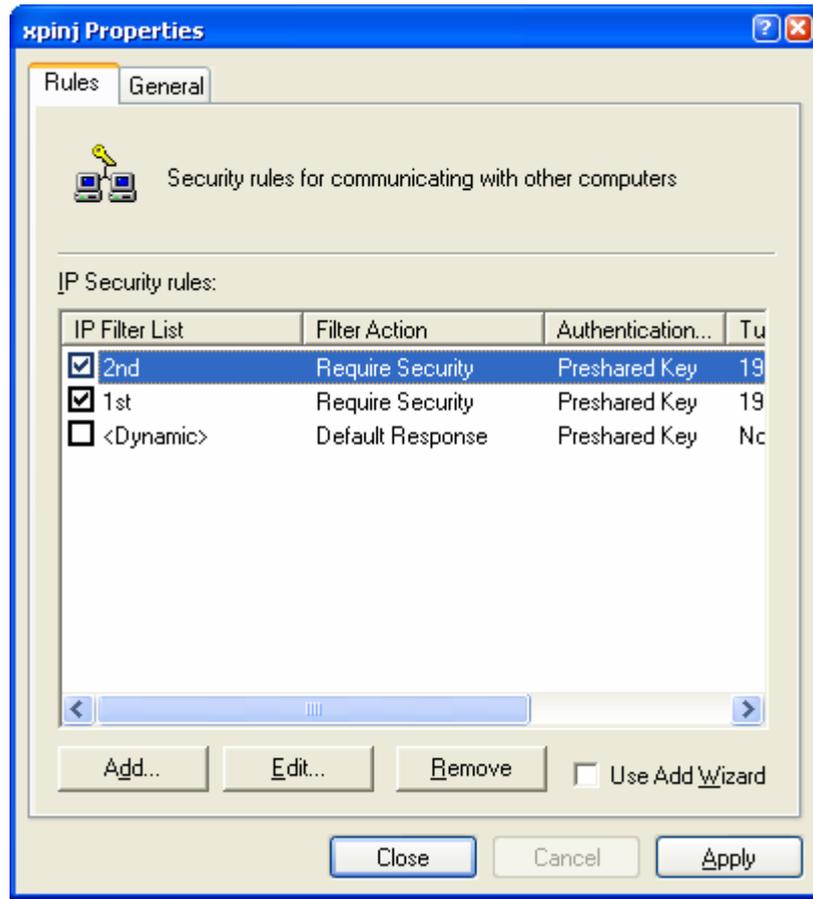
To create a VPN using the InJoy IPSec and Windows, the following steps must be completed:

- 1 Install an InJoy product with IPSec ("**Remote Gateway**").
- 2 Install the Pluto IKE server on the InJoy PC.
- 3 Configure the Windows ("**Local Host**").

- 3.1 Run the IPSec policy configuration
- 3.2 Create an IPSec security policy
- 3.3 Add 2 security rules
- 3.4 Edit created rules
- 3.5 Assign the Policy
- 3.6 Activate the Policy in Network and Dial-up Connection properties
- 4 Configure the InJoy IPSec side.
- 5 Restart the InJoy IPSec product and the IKE server.
- 6 Trigger Windows to establish the SA. (Note: any traffic between IPSec endpoints will force this).

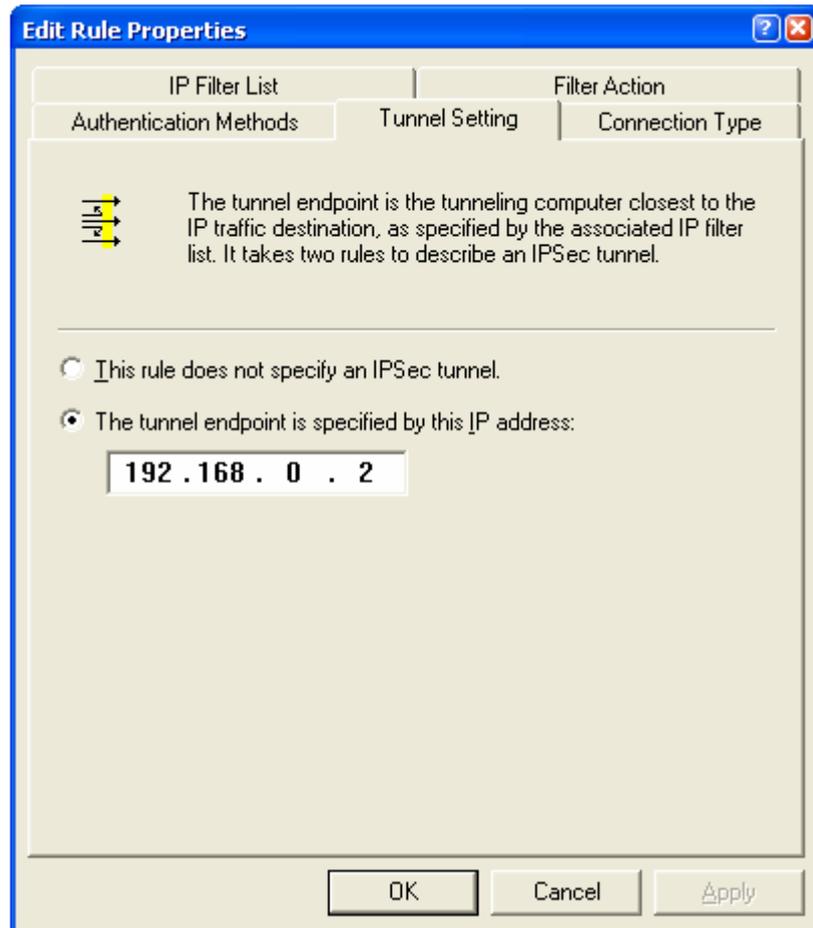
1.3. Configuring Windows

- 1 Run Microsoft Management Console - Click **Start**, click **Run**, type **mmc**, and then click **Ok**.
- 2 On the Console menu, click Add/Remove Snap-in.
- 3 Click **Add**, and then double-click **IP Security Management**.
- 4 Create IP Security Policy, un-assign all existing Policies except the new one.
- 5 Click right mouse button on the created Policy, click **Properties**
- 6 Remove or deactivate all existing IP Security Rules - Remove check sign at the beginning of Rule line.
- 7 Create 2 new IP Security Rules (for example **1st** and **2nd**).

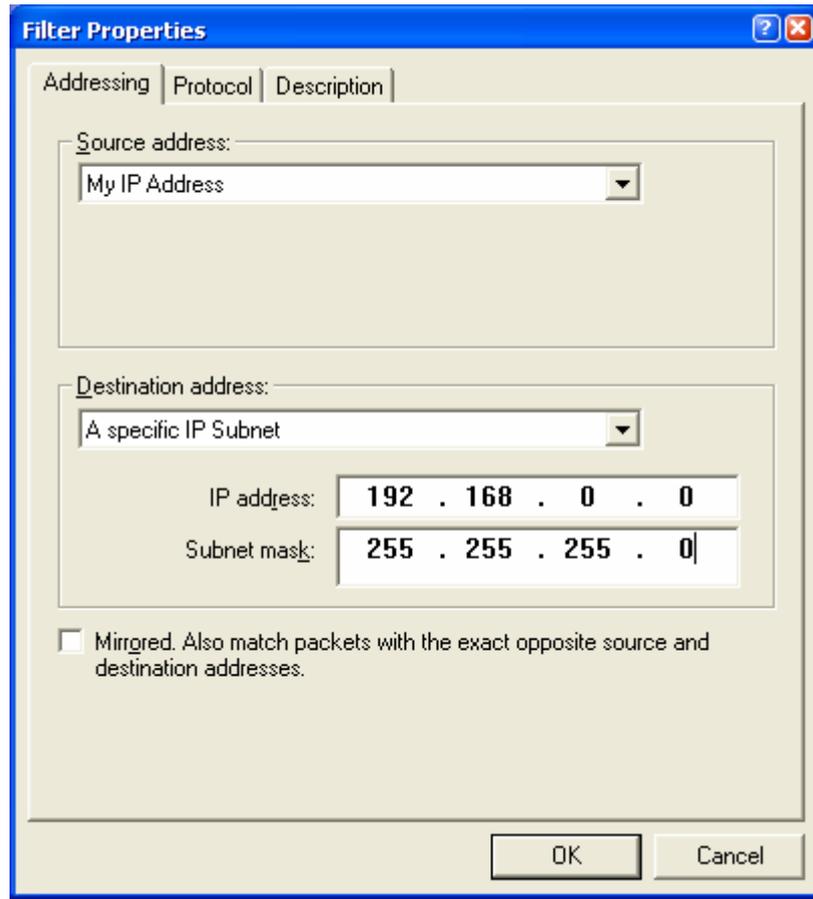


8 Edit 1st Rule:

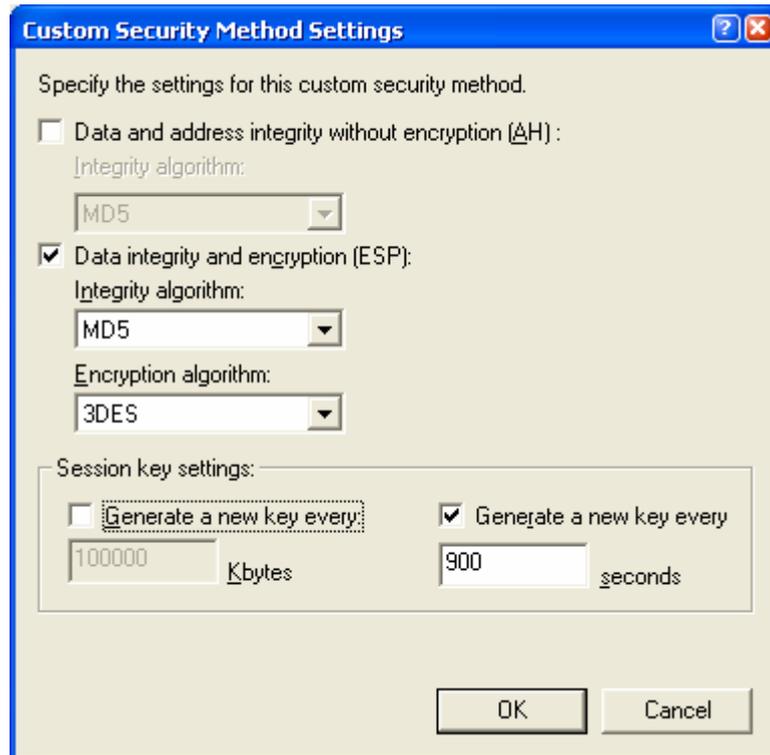
- 8.1 On the **Connection Type** notebook page choose **All network connections**
- 8.2 On the **Tunnel Setting** notebook page specify the IP address of the Remote Gateway (192.168.0.2)



- 8.3 On the **Authentication Methods** notebook page choose **Preshared Key** and enter an appropriate key (superkey)
- 8.4 On the **IP Filter List** notebook page choose **1st Rule**, click **Edit**
- 8.5 Add IP Filter.
- 8.6 On the **Addressing** notebook page of the **Filter Properties** choose **My IP Address** as **Source Address** and **A Specific IP Subnet** as **Destination Address**. Specify the IP Address of the subnet (192.168.0.0) and the subnet mask (255.255.255.0). Uncheck the **Mirrored** checkbox.



- 8.7 On the **Protocol** notebook page select **Any** in the protocol field
- 8.8 Press **OK** on the **Filter Properties** page.
- 8.9 Press **OK** on the **IP Filter List** page.
- 8.10 On the Filter Action notebook page select **Require Security**, click **Edit**
- 8.11 Select **Negotiate Security**, check **Accept unsecured communications, but always respond using IPSec**, checkboxes for **Allow unsecured communications with non IPSec-aware computer** and **Session key Perfect Forward Secrecy** must be cleared.
- 8.12 Choose the upper Security Method and click **Edit**
- 8.13 Select **Custom**, click **Settings**
- 8.14 Select **Data integrity and encryption(ESP)**, choose algorithms (NOTE: you should select **3DES only** if you installed 3DES support for Windows, otherwise select DES)



- 8.15 Press **OK** on the **Custom Security Method Settings** page.
- 8.16 Press **OK** on the **Modify Security Method** page.
- 8.17 Press **OK** on the **Security Method** page.
- 8.18 Press **OK** on the **Edit Rule Properties** page.
- 9 Edit **2nd** Rule: make all settings the same as for the **1st** rule with 2 exceptions:
 - 9.1 On the Tunnel Settings notebook page specify Local Host address as the tunnel endpoint (192.168.0.1)
 - 9.2 On the Addressing notebook page of Filter Properties specify the subnet parameters (192.168.0.0/255.255.255.0) as the Source address and My IP Address as the Destination Address
- 10 Switch to the **General** notebook page, click **Advanced**, disable **Master key Perfect Forward Secrecy**, click **Methods**, edit the upper Security Method in list, specify algorithms (NOTE: you should select 3DES **only** if you installed 3DES support for Windows, otherwise select DES)
- 11 Save all settings and close Microsoft Management Console
- 12 Click **Start**, click **Network and Dial-up Connections**, choose appropriate connection, right click on it, click **Properties**, choose TCP/IP, click **Properties**, and click **Advanced**. On **Options** notebook page choose **IP Security**, click **Properties**, click **Use this IP Security Policy** and choose the name of the policy you just created

1.4. *Configuring the InJoy side*

On the Remote Gateway add the following section to ipsec.cnf, to describe the SA to the Windows:

```
winxp
Description = "Microsoft Windows 2000/XP",
Mode = Tunnel,
Local-IP = "192.168.0.2",           # local gateway IP address
Local-Net = "192.168.5.0",
Local-Mask = "255.255.255.0",
Remote-IP = "192.168.0.1",       # remote host IP address
AH = No,
ESP = DES,
Reinit = No,
Preshared-Secret = "superkey",
```

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

1.5. *Connecting to Windows*

Any traffic between IPsec endpoints will trigger IKE negotiations. For example if you ping 192.168.0.2 from the Windows PC, you will see:

```
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
```

After these messages, the IPsec link will be established.

On the InJoy Gateway, the ipsec.log will contain the following lines:

```
10052002 04360700 Install SA :winxp.
10052002 04360700 SA Name.....: winxp
10052002 04360700 Authentication.....: IP Address/Preshared Secret.
10052002 04360700 Local IP address.....: 192.168.0.2
10052002 04360700 Local Net.....: 192.168.0.0
10052002 04360700 Local Netmask.....: 255.255.255.0
10052002 04360700 Remote IP address.....: 192.168.0.1
10052002 04360700 Remote Net.....: 192.168.0.1
10052002 04360700 Remote Netmask.....: 255.255.255.255
10052002 04360700 ISAKMP SA lifetime.....: 3600 seconds
10052002 04360700 IPSEC SA lifetime.....: 28800 seconds
10052002 04360700 ESP encr/auth/keylen.....: 3DES/MD5/40
10052002 04360700 AH method/keylen.....: None/0
10052002 04360700 IPCOMP.....: None
10052002 04360700 Road Warrior.....: No
10052002 04360700 Remote Road Warrior.....: No
```

2. Making Windows Road Warrior

2.1. Configuring the InJoy side

On the Remote Gateway add the following section to the file `ipsec.conf`. The section describes the SA to Windows:

```
win2k
Description = "Microsoft Windows 2000/XP (RW)",
Mode = Tunnel,
Local-IP = "192.168.0.1", # local gateway IP address
Local-Net = "192.168.0.0",
Local-Mask = "255.255.255.0",
Remote-IP = "0.0.0.0", # remote host IP address
AH = No,
ESP = DES,
Reinit = No,
Preshared-Secret = "superkey",
```

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

2.2. Configuring Windows

Windows 2000 prerequisites:

- Windows 2000 Service Pack 2:
<http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/sp2lang.asp>
- Windows 2000 IPSEC POL Tool version 1.22, which can be found in the Resource Kit or at the following location:
<http://agent.microsoft.com/windows2000/techinfo/reskit/tools/existing/ipsecpol-o.asp>
- Windows 2000 VPN tool by Marcus Müller:
<http://vpn.ebootis.de/package.zip>

Windows XP prerequisites:

- IPSECCMD tool from Windows XP Support Tools, which can be installed by running `setup.exe` in the `\SUPPORT\TOOLS` folder on your Windows XP installation CD.
- Windows XP VPN tool by Marcus Müller:
<http://vpn.ebootis.de/package.zip>

To configure Windows for being Road Warrior, the following steps must be completed:

- 1 Edit the `ipsec.conf` file from the VPN tool distribution as follows:

```

conn %default
    dial=astranet

conn injoy
    left=192.168.0.1
    leftsubnet=192.168.0.0/24
    right=%any
    network=ras
    auto=start
    pfs=no
    presharedkey=superkey

```

- 1.1 astranet is the RAS connection name to be dialed;
 - 1.2 192.168.0.1 is the remote system address;
 - 1.3 192.168.0.0/24 is the remote system net and net mask;
 - 1.4 superkey is the pre-shared secret
- 2 Run the VPN tool:

```

IPSec Version 2.1.4 (c) 2001,2002 Marcus Mueller
Getting running Config ...
Microsoft's Windows 2000 identified
Host name is: libra
Dialing astranet ... OK
1 RAS connection(s) found!
RAS IP Address: 213.80.136.136
LAN IP address: 192.168.0.33
Setting up IPSec ...
    Deactivating old policy...
    Removing old policy...
Connection injoy:
MyTunnel : 213.80.136.136
MyNet : 213.80.136.136/255.255.255.255
PartnerTunnel: 192.168.0.1
PartnerNet : 192.168.0.0/255.255.255.0
CA (ID) : Preshared Key *****
PFS : n
Auto : start
Auth.Mode : MD5
Rekeying : 3600S/50000K
Activating policy...

```

- 3 Establish the tunnel by e.g. pinging the remote system (refer to section 1.5).
- 4 For more information on using Marcus Muller's VPN Tool, refer to his home page at <http://vpn.ebootis.de/>.