



# VPN Installation Procedures Cisco ASA 5500 Series

## **EbixExchange Confidential and Proprietary**

This document and the information contained therein are confidential to and the property of EbixExchange Australia Pty Ltd. This information is made available to Sunrise customers for the sole purpose of conducting the company's business and is not to be disclosed without prior written consent. All rights reserved.

---

# VPN Installation Procedures

## Cisco ASA 5500 Series

**Document Number Sr-1054**

**Version 1.00**

© EbixExchange Australia Pty Ltd 2008

**Disclaimer:**

Every effort has been made to provide accurate and complete information. However, EbixExchange Australia Pty Ltd assumes no responsibility for any direct, indirect, incidental or consequential damages arising from the use of the information in this document. Data and case-study examples are intended to be fictional.

**Copyright:**

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means electronic, mechanical photocopying, recording, or otherwise without written permission from EbixExchange Australia Pty Ltd.

This manual was produced using Windows XP Professional and Microsoft Word 2003

Last Updated: 28/10/08

1	Introduction .....	1
2	Minimum Configuration Requirements .....	1
3	Installing the Router .....	2
3.1	Authentication .....	2
3.2	Configuration .....	2
3.3	VPN Technical Details.....	2
3.4	Command Line (CLI) access.....	2
4	Testing Tunnel Access .....	4
5	Testing your Sunrise™ Exchange Connection.....	5
	Appendix A .....	7
	ASA Configuration .....	7
	Appendix B .....	9
	Troubleshooting Commands.....	9

# 1 Introduction

EbixExchange's use of Sunrise™ Exchange uses a Virtual Private Network (VPN). Connecting to a remote corporate server, using a routing infrastructure such as the Internet, the VPN allows connection between insurers and intermediaries to operate in a secure manner.

Other options open to insurers who operate Sunrise™ Exchange independently of EbixExchange include IP-based intranets and extranets, as well as the public Internet.

The Sunrise™ Exchange VPN is based on the IPSec protocol and takes advantage of the broad availability of the Internet.

IPSec encrypts everything between two computers. Using a VPN connection, data is carried over the public network, but is unreadable to unauthorised clients. It also provides audit records to show accessed information.

**Note:**

**IP addresses, user names and user passwords used throughout this document are not valid and are displayed for demonstration purposes only. EbixExchange will supply valid IP addresses and user details upon connection to Sunrise™ Exchange.**

## 2 Minimum Configuration Requirements

To create a VPN, the following minimum configurations are required:

**Cisco Hardware:**

- Cisco ASA 5505 or higher model

**Internet Connection:**

- Static IP Address from ISP

## 3 Installing the Router

### 3.1 Authentication

The customer must inform the EbixExchange VPN Team of the static IP address that has been assigned to them by their ISP.

EbixExchange will provide the following details:

- Preshared key
- IP address for VPN tunnel (This is a EbixExchange allocated private address)

### 3.2 Configuration

Configuration is a two-step process:

- Connect the ADSL Router to Internet:  
Ensure the network can access the Internet before proceeding.
- Connect the VPN to Sunrise Exchange:  
using the sample configurations shown in *Appendices A*  
substitute the EbixExchange VPN static IP address for **172.29.xx.yy**.  
substitute **192.168.xx.yy** for your local LAN addresses.

### 3.3 VPN Technical Details

The IKE VPN tunnel establishes 2 IPSEC tunnels.

Tunnel-1 is between EbixExchange provided 172.29.xx.yy/32 and 172.27.1.0/24

Tunnel-2 is between EbixExchange provided 172.29.xx.yy/32 and 10.125.0.0/16

All customers LAN traffic is NATed to the 172.29.xx.yy/32 address to reach EbixExchange. Therefore EbixExchange does not need to be aware of customer's local LAN addressing details.

### 3.4 Command Line (CLI) access

To configure the Cisco ASA 5500 device you need Command Line (CLI) access

The commands given below may need to be given for SSH access, if you do not have access to direct console access (via Hyperterm etc).

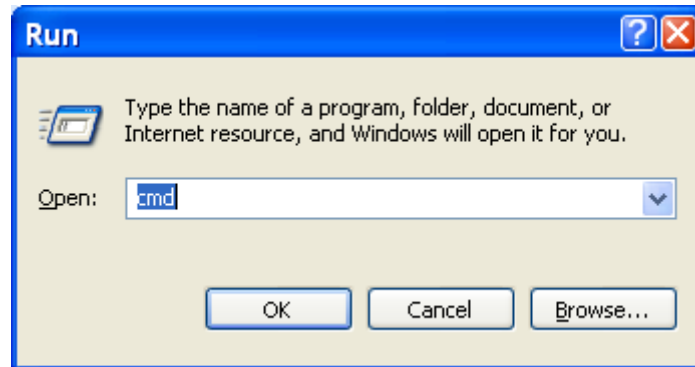
- `aaa authentication ssh console LOCAL`
- `ssh 192.168.xx.yyy .0 255.255.255.0 inside`

- enable password (your enable password)

## 4 Testing Tunnel Access

From one of the PCs:

Click **S**tart and **R**un.



Type **cmd** and click **O**K.

```
C:\WINNT\system32\cmd.exe
C:\>
C:\>
C:\>ping 172.27.1.91
Pinging 172.27.1.91 with 32 bytes of data:
Reply from 172.27.1.91: bytes=32 time<10ms TTL=255
Reply from 172.27.1.91: bytes=32 time<10ms TTL=255
Reply from 172.27.1.91: bytes=32 time<10ms TTL=255
Ping statistics for 172.27.1.91:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.125.80.50
Pinging 10.125.80.50 with 32 bytes of data:
Reply from 10.125.80.50: bytes=32 time=11ms TTL=252
Reply from 10.125.80.50: bytes=32 time=11ms TTL=252
Reply from 10.125.80.50: bytes=32 time=10ms TTL=252
Reply from 10.125.80.50: bytes=32 time=11ms TTL=252
```

Type **ping 172.27.1.91**

If you see more than one line beginning with **Reply from...** appear on the screen, this indicates the vpn is responding and the test has been successful.

To perform a basic test to check access to web-based insurer products, perform the same test above, typing **ping 10.125.80.50**

Again, if you see more than one line beginning with **Reply from...** appear on the screen, this indicates access to web-based insurer products may be possible.

If there are any problems, please contact the EbixExchange CSC support team via e-mail at [csc@ebix.com.au](mailto:csc@ebix.com.au) or via phone on 1800 331 018 to test and confirm successful VPN installation.

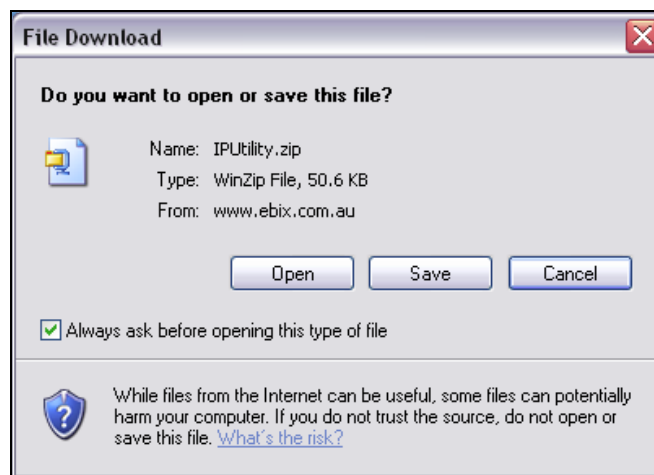
## 5 Testing your Sunrise™ Exchange Connection

Whilst the tests run in 4 prove that your VPN Connection is responding correctly, they do not necessarily prove that your PC can load the Sunrise™ Exchange insurer products.

To test that the products will load successfully, you will need to download a program called **IPUtility**.

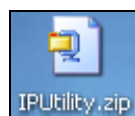
Click on the following link:

<http://www.ebix.com.au/files/zip/IPUtility.zip>

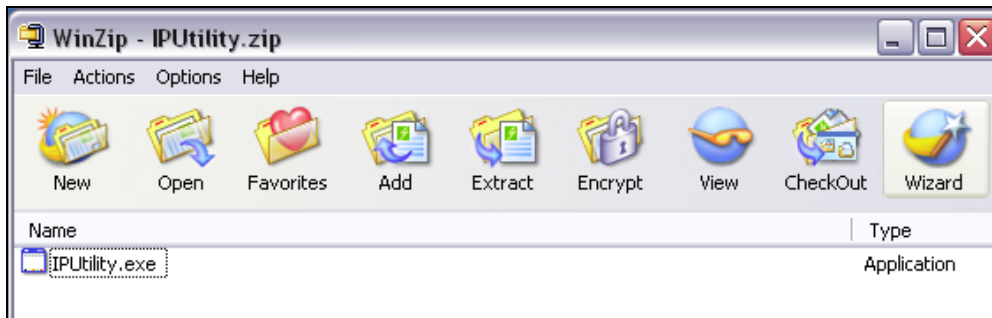


Click **Save** and save **IPUtility.zip** to a folder on your Desktop.

Double-click on **IPUtility.zip**.



WinZip will display



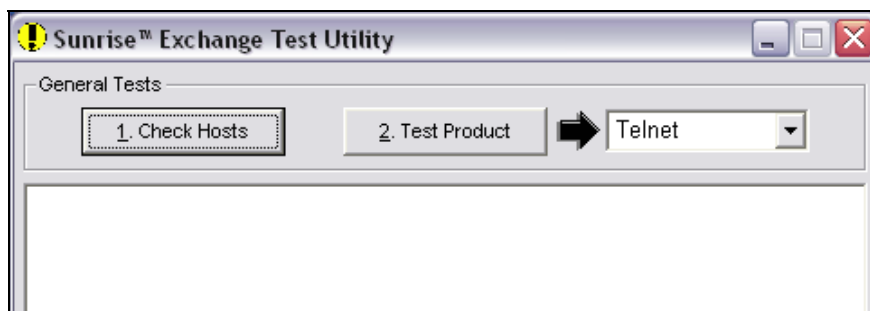
Highlight **IPUtility.exe** and click **Extract**.

Select Desktop and click **Extract**.

Double-click on **IPUtility.exe**.



The Sunrise™ Exchange Test Utility window will display



Please refer to the **Sunrise Exchange VPN Tests.pdf** for further instructions to run the Web Product Test.

A **No JVM Error** message indicates you will need to download and install Java. This download is available from <http://java.com/en/download/manual.jsp>.

Download and install the "Windows" file.

Re-run the **IPUtility** again and make sure it can now load the test product.

**Note:**

**Please contact our Client Service Centre (CSC) on 1800 331 018 to run the Web Product Test and advise them of the successful completion of the installation of your VPN.**

# Appendix A

## ASA Configuration

```
access-list acl-sunrise-vpn permit ip host 172.29.xx.yy 172.27.1.0  
255.255.255.0 <<== Change to Sunrise VPN Address
```

```
access-list acl-sunrise-vpn permit ip host 172.29.xx.yy 10.125.0.0 255.255.0.0  
<<== Change to Sunrise VPN Address
```

```
access-list acl-lan-sunrise-nat permit ip 192.168.xx.yy 255.255.255.0  
172.27.1.0 255.255.255.0
```

```
access-list acl-lan-sunrise-nat permit ip 192.168.xx.yy 255.255.255.0  
10.125.0.0 255.255.0.0
```

```
crypto isakmp policy 5
```

```
authentication pre-share
```

```
encryption 3des
```

```
hash md5
```

```
group 2
```

```
lifetime 86400
```

```
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
```

```
crypto map tosunrise 30 ipsec-isakmp
```

```
crypto map tosunrise 30 match address acl-sunrise-vpn
```

```
crypto map tosunrise 30 set peer 202.12.184.137
```

```
crypto map tosunrise 30 set transform-set ESP-3DES-MD5
```

```
crypto map tosunrise interface outside
```

```
crypto isakmp enable outside
```

```
tunnel-group 202.12.184.137 type ipsec-l2l
```

**tunnel-group 202.12.184.138 ipsec-attributes**

**pre-shared-key *preshared-key***

**global (outside) 2 172.29.xx.yy**

**nat (inside) 2 access-list acl-lan-sunrise-nat 0 0**

# Appendix B

## Troubleshooting Commands

- show 192h crypto isakmp sa
- Debug crypto isakmp
- Ter mon

**END**