



VPN Installation Procedures

Cisco 827/837 ADSL Router

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 827/837 ADSL Router

© 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: 3/10/08

1	Introduction	1
2	System Requirements	2
3	Installing the Router	3
3.1	Authentication	3
3.2	Configuration	3
4	Testing Tunnel Access.....	4
5	Testing your Sunrise™ Exchange Connection.....	5
6	Troubleshooting.....	7
6.1	Turn debug on	7
6.2	Incorrect Pre Shared Key	7
Appendix A	8
Sample PPPoE Configuration	8
Appendix B	12
Sample Bridge Configuration	12
Appendix C	15
Sample Debug output when VPN is established normally	15

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 access 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 System Requirements

The Cisco 827/837 router must have the following minimum configurations:

- RAM:
 - 24MB DRAM (32MB Recommended)
 - 16MB Flash
- IOS:
 - IOS Version 12.2 IP Firewall Plus IPSec 3DES or later
- ADSL Connection:
 - Static IP Address from ISP
 - PPPoE or Bridge configuration

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 & B*

Substitute the EbixExchange VPN static IP address for **172.29.xx.yy**.

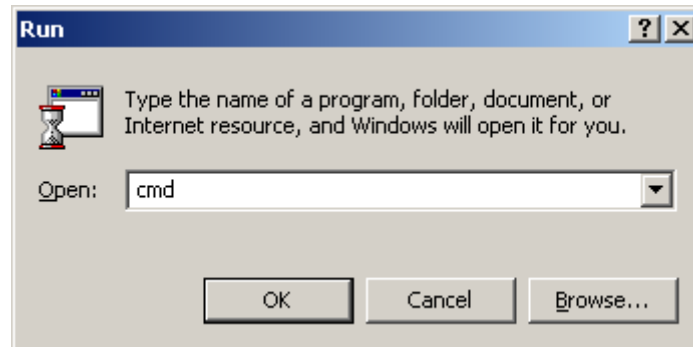
Substitute the static public IP address for **aaa.bbb.ccc.ddd**.

Substitute **192.168.0.0** and **192.168.0.1** for your local LAN addresses.

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
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

Z:\>ping 172.27.1.91

Pinging 172.27.1.91 with 32 bytes of data:

Reply from 172.27.1.91: bytes=32 time=3ms TTL=254
Reply from 172.27.1.91: bytes=32 time=1ms TTL=254
Reply from 172.27.1.91: bytes=32 time=2ms TTL=254
Reply from 172.27.1.91: bytes=32 time=1ms TTL=254

Ping statistics for 172.27.1.91:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

Z:\>
```

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.

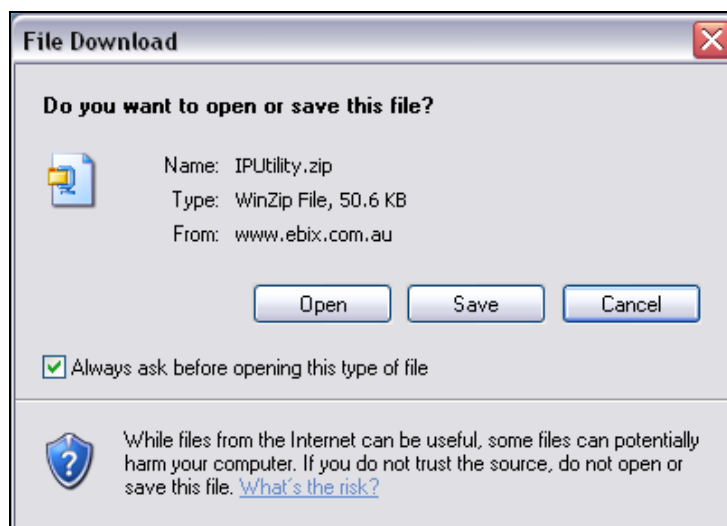
5 Testing your Sunrise™ Exchange Connection

Whilst the tests run in 4 prove that your VPN Connections 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**.

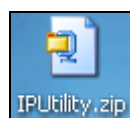
Click on the following link:

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

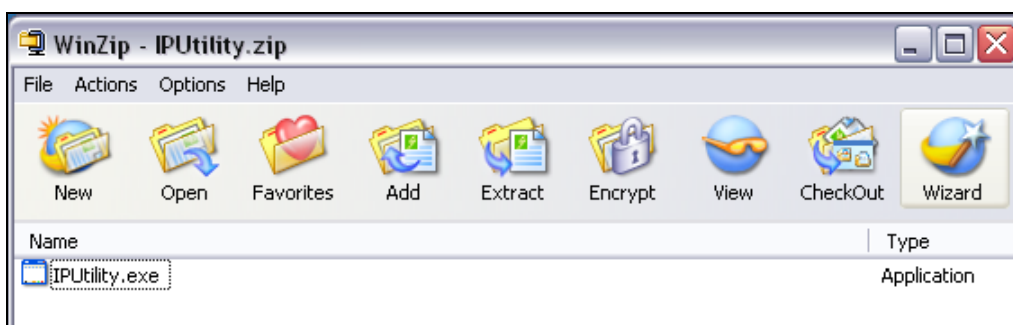


Click **Save** and save IPUtility.zip to a folder on your Desktop.

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



WinZip will display



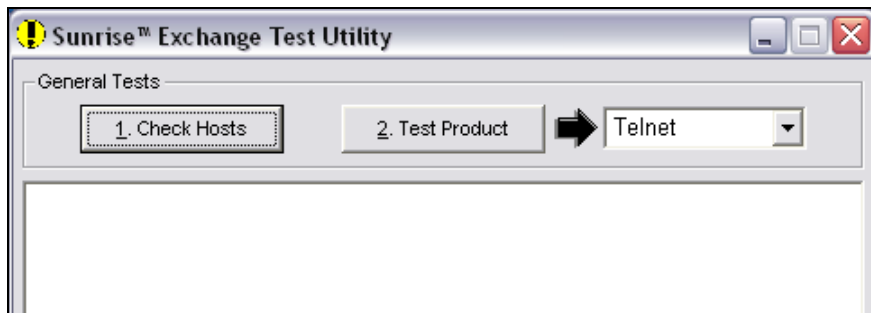
Highlight **IPUtility.exe** and click **E**xtract.

Select Desktop and click **E**xtract.

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.

6 Troubleshooting

6.1 Turn debug on

```
Debug crypto isakmp
Ter mon
Show crypto isakmp sa
```

This command should show **QM_Idle** if VPN is established, as shown below:

dst	src	state	conn-id	slot
61.95.25.26	203.44.206.217	QM_IDLE	1	0

6.2 Incorrect Pre Shared Key

Debug output of `Debug crypto isakmp` will have the following error message if the preshared key is incorrect:

```
%CRYPTO-6-IKMP_NOT_ENCRYPTED: IKE packet from %15i was not encrypted and it should've been.
```

Refer *Appendix C* for a sample debug output when the VPN is established normally.

Recommended Action: Check the preshared key. If this is correct, please contact EbixExchange for further investigation.

Appendix A

Sample PPPoE Configuration

```
version 12.2
no service pad
service tcp-keepalives-in
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname <your host name here>
!
!
ip subnet-zero
no ip domain-lookup
ip name-server 139.130.4.4 < Change to your ISP's DNS server address >
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 10
hash md5
authentication pre-share
group 2
crypto isakmp key <insert your pre shared key here> address 202.12.184.137
!
crypto ipsec transform-set insnettrans esp-3des esp-md5-hmac
!
crypto map insnetvpn 10 ipsec-isakmp
set peer 202.12.184.137
set transform-set insnettrans
match address 101
!
interface Loopback1
ip address 172.29.xxx.yyy 255.255.255.255 <== Change to Sunrise VPN
Address
!
interface Ethernet0
```

```
description FNN16100XXXXC LAN
ip address 192.168.0.1 255.255.255.0 <<== Change to Local LAN
no ip proxy-arp
ip nat inside
no ip route-cache
no ip mroute-cache
no keepalive
no cdp enable
hold-queue 100 out
!
interface ATM0
no ip address
no ip route-cache
no ip mroute-cache
no atm ilmi-keepalive
bundle-enable
dsl operating-mode auto
hold-queue 224 in
!
interface ATM0.1 point-to-point
description Internet Network
no ip route-cache
no ip mroute-cache
pvc 8/35
ubr 128
encapsulation aal5mux ppp dialer
dialer pool-member 1
!
!
interface Dialer1
description Internet Network
ip address aaa.bbb.ccc.ddd 255.255.255.xxx <<== Change to Internet Static Address and Mask provided by ISP ##
ip nat outside
encapsulation ppp
no ip route-cache
no ip mroute-cache
dialer pool 1
dialer-group 1
no cdp enable
```

```
ppp authentication chap callin
ppp chap hostname xxxxxxxxxxxx
ppp chap password xxxxxxxxxxxx
crypto map insnetvpn
!
ip nat inside source route-map insnetnat interface Loopback1 overload
ip nat inside source route-map internetnat interface Dialer1 overload
ip classless
ip forward-protocol udp netbios-ss
ip route 0.0.0.0 0.0.0.0 Dialer1
ip route 172.27.1.0 255.255.255.0 202.12.184.137
ip route 10.125.0.0 255.255.0.0 202.12.184.137
no ip http server
no ip pim bidir-enable
!
access-list 101 permit ip 192.168.0.0 0.0.0.255 172.27.1.0
0.0.0.255
access-list 101 permit ip host 172.29.xx.yy 172.27.1.0 0.0.0.255
access-list 101 permit ip 192.168.0.0 0.0.0.255 10.125.0.0
0.0.255.255
access-list 101 permit ip host 172.29.xx.yy 10.125.0.0 0.0.255.255
access-list 102 deny ip 192.168.0.0 0.0.0.255 172.27.1.0 0.0.0.255
access-list 102 deny ip 192.168.0.0 0.0.0.255 10.125.0.0
0.0.255.255
access-list 102 permit ip 192.168.0.0 0.0.0.255 any
dialer-list 1 protocol ip permit
no cdp run
route-map internetnat permit 1
match ip address 102
!
route-map insnetnat permit 1
match ip address 101
!
!
line con 0
exec-timeout 30 0
logging synchronous
login
topbits 1
line vty 0 4
```

```
access-class 21 in
exec-timeout 30 0
password xxxxxxxxxx
login
!
scheduler max-task-time 5000
end
```

Appendix B

Sample Bridge Configuration

```
!  
version 12.2  
no service pad  
service tcp-keepalives-in  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname <your host name here>  
!  
enable secret 5 xxyyzz  
enable password XXXYYYZZZ  
!  
username admin password 0 XXXYYYZZZ  
ip subnet-zero  
!  
!  
crypto isakmp policy 10  
hash md5  
authentication pre-share  
group 2  
crypto isakmp key <insert your pre shared key here> address 202.12.184.137  
!  
crypto ipsec transform-set insnettrans esp-3des esp-md5-hmac  
!  
crypto map insnetvpn 10 ipsec-isakmp  
set peer 202.12.184.137  
set transform-set insnettrans  
match address 101  
!  
bridge irb  
!  
interface Loopback1  
ip address 172.29.xxx.yyy 255.255.255.255 <== Change to Sunrise VPN  
Address
```

```
!  
interface Ethernet0  
ip address 192.168.0.1 255.255.255.0  
no ip proxy-arp  
ip nat inside  
no ip route-cache  
no ip mroute-cache  
no keepalive  
no cdp enable  
hold-queue 100 out  
!  
interface ATM0  
no ip address  
no ip route-cache  
no ip mroute-cache  
no atm ilmi-keepalive  
pvc 8/35  
encapsulation aal5snap  
!  
bundle-enable  
dsl operating-mode auto  
bridge-group 1  
hold-queue 224 in  
!  
interface BVI1  
ip address aaa.bbb.ccc.ddd 255.255.255.xxx <== Change to Internet  
Static Address and Mask provided by ISP ##  
ip nat outside  
no ip route-cache  
no ip mroute-cache  
crypto map insnetvpn  
!  
ip nat inside source route-map insnetnat interface Loopback1 overload  
ip nat inside source route-map internetnat interface BVI1 overload  
ip classless  
ip forward-protocol udp netbios-ss  
ip route 0.0.0.0 0.0.0.0 ISP_ROUTER ADDRESS  
ip route 172.27.1.0 255.255.255.0 202.12.184.137  
ip route 10.125.0.0 255.255.0.0 202.12.184.137  
no ip http server
```

```
no ip pim bidir-enable
!
!

access-list 101 permit ip 192.168.0.0 0.0.0.255 172.27.1.0
0.0.0.255
access-list 101 permit ip host 172.29.xx.yy 172.27.1.0 0.0.0.255
access-list 101 permit ip 192.168.0.0 0.0.0.255 10.125.0.0
0.0.255.255
access-list 101 permit ip host 172.29.xx.yy 10.125.0.0 0.0.255.255
access-list 102 deny ip 192.168.0.0 0.0.0.255 172.27.1.0 0.0.0.255
access-list 102 deny ip 192.168.0.0 0.0.0.255 10.125.0.0
0.0.255.255
access-list 102 permit ip 192.168.0.0 0.0.0.255 any
no cdp run
!
route-map internetnat permit 1
match ip address 102
!
route-map insnetnat permit 1
match ip address 101
!
bridge 1 protocol ieee
bridge 1 route ip
!
line con 0
stopbits 1
line vty 0 4
password XXXYYYZZZ
login local
```

Appendix C

Sample Debug output when VPN is established normally

```
clear crypto isakmp sa      (Clear any established ISAKMP SA)
Do an extended ping from the Ethernet interface.
Please note that the 1st ping is not replied as it is lost during isakmp sa
establishment.
ping
Protocol [ip]:
Target IP address: 172.27.1.91
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.0.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.27.1.91, timeout is 2 seconds:
23:10:43: ISAKMP: received ke message (1/1)
23:10:43: ISAKMP: local port 500, remote port 500
23:10:43: ISAKMP: set new node 0 to QM_IDLE
23:10:43: ISAKMP (0:5): Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_MM
Old State = IKE_READY  New State = IKE_I_MM1
23:10:43: ISAKMP (0:5): beginning Main Mode exchange
23:10:43: ISAKMP (0:5): sending packet to 202.12.184.137 (I) MM_NO_STATE
23:10:43: ISAKMP (0:5): received packet from 202.12.184.137 (I) MM_NO_STATE
23:10:43: ISAKMP (0:5): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_I_MM1  New State = IKE_I_MM2
23:10:43: ISAKMP (0:5): processing SA payload. message ID = 0
23:10:43: ISAKMP (0:5): processing vendor id payload
23:10:43: ISAKMP (0:5): vendor ID seems Unity/DPD but bad major
23:10:43: ISAKMP (0:5): found peer pre-shared key matching 202.12.184.137
```

```
23:10:43: ISAKMP (0:5) local preshared key found
23:10:43: ISAKMP (0:5): Checking ISAKMP transform 1 against priority 10
policy
23:10:43: ISAKMP:      encryption DES-CBC
23:10:43: ISAKMP:      hash MD5
23:10:43: ISAKMP:      default group 2
23:10:43: ISAKMP:      auth pre-share
23:10:43: ISAKMP:      life type in seconds
23:10:43: ISAKMP:      life duration (VPI) of 0x0 0x1 0x51 0x80
23:10:43: ISAKMP (0:5): atts are acceptable. Next payload is 0.!
23:10:43: ISAKMP (0:5): processing vendor id payload
23:10:43: ISAKMP (0:5): vendor ID seems Unity/DPD but bad major
23:10:43: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_I_MM2 New State = IKE_I_MM2
23:10:43: ISAKMP (0:5): sending packet to 202.12.184.137 (I) MM_SA_SETUP
23:10:43: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_I_MM2 New State = IKE_I_MM3
23:10:43: ISAKMP (0:5): received packet from 202.12.184.137 (I) MM_SA_SETUP
23:10:43: ISAKMP (0:5): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_I_MM3 New State = IKE_I_MM4
23:10:43: ISAKMP (0:5): processing KE payload. message ID = 0
23:10:44: ISAKMP (0:5): processing NONCE payload. message ID = 0
23:10:44: ISAKMP (0:5): found peer pre-shared key matching 202.12.184.137
23:10:44: ISAKMP (0:5): SKEYID state generated
23:10:44: ISAKMP (0:5): processing vendor id payload
23:10:44: ISAKMP (0:5): vendor ID is Unity
23:10:44: ISAKMP (0:5): processing vendor id payload
23:10:44: ISAKMP (0:5): vendor ID seems Unity/DPD but bad major
23:10:44: ISAKMP (0:5): vendor ID is XAUTH
23:10:44: ISAKMP (0:5): processing vendor id payload
23:10:44: ISAKMP (0:5): speaking to another IOS box!
23:10:44: ISAKMP (0:5): processing vendor id payload
23:10:44: ISAKMP (0:5): vendor ID seems Unity/DPD but bad major
23:10:44: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_I_MM4 New State = IKE_I_MM4
23:10:44: ISAKMP (0:5): SA is doing pre-shared key authentication using id
type ID_IPV4_ADDR
23:10:44: ISAKMP (5): ID payload
    next-payload : 8
    type          : 1
```

```
protocol      : 17
port          : 500
length       : 8
23:10:44: ISAKMP (5): Total payload length: 12
23:10:44: ISAKMP (0:5): sending packet to 202.12.184.137 (I) MM_KEY_EXCH
23:10:44: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_I_MM4 New State = IKE_I_MM5
23:10:44: IPSec: Key engine got KEYENG_IKMP_MORE_SAS message
23:10:44: ISAKMP: received ke message (6/1)
23:10:44: ISAKMP: received KEYENG_IKMP_MORE_SAS message
23:10:44: ISAKMP: set new node 1078392488 to QM_IDLE
23:10:44: ISAKMP (0:5): sending packet to 202.12.184.137 (I) MM_KEY_EXCH
23:10:44: ISAKMP (0:5): purging node 1078392488
23:10:44: ISAKMP (0:5): Sending initial contact.
23:10:44: ISAKMP (0:5): Unknown Input: state = IKE_I_MM5, major, minor =
IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
23:10:44: ISAKMP (0:5): received packet from 202.12.184.137 (I) MM_KEY_EXCH
23:10:44: ISAKMP (0:5): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_I_MM5 New State = IKE_I_MM6
23:10:44: ISAKMP (0:5): processing ID payload. message ID = 0
23:10:44: ISAKMP (0:5): processing HASH payload. message ID = 0
23:10:44: ISAKMP:received payload type 14
23:10:44: ISAKMP (0:5): processing vendor id payload
23:10:44: ISAKMP (0:5): vendor ID is DPD
23:10:44: ISAKMP (0:5): SA has been authenticated with 202.12.184.137
23:10:44: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_I_MM6 New State = IKE_I_MM6
23:10:44: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_I_MM6 New State = IKE_P1_COMPLETE
23:10:44: ISAKMP (0:5): beginning Quick Mode exchange, M-ID of -1957392785
23:10:44: ISAKMP (0:5): sending packet to 202.12.184.137 (I) QM_IDLE
23:10:44: ISAKMP (0:5): Node -1957392785, Input = IKE_MESG_INTERNAL,
IKE_INIT_QM
Old State = IKE_QM_READY New State = IKE_QM_I_QM1
23:10:44: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
23:10:44: ISAKMP (0:5): received packet from 202.12.184.137 (I) QM_IDLE
23:10:44: ISAKMP (0:5): processing HASH payload. message ID = -1957392785
23:10:44: ISAKMP (0:5): processing SA payload. message ID = -1957392785
23:10:44: ISAKMP (0:5): Checking IPSec proposal 1
```

```
23:10:44: ISAKMP: transform 1, ESP_DES
23:10:44: ISAKMP:   attributes in transform:
23:10:44: ISAKMP:     SA life type in seconds
23:10:44: ISAKMP:     SA life duration (basic) of 3600
23:10:44: ISAKMP:     SA life type in kilobytes
23:10:44: ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
23:10:44: ISAKMP:     encaps is 1
23:10:44: ISAKMP:     authenticator is HMAC-MD5
23:10:44: ISAKMP (0:5): atts are acceptable.
23:10:44: ISAKMP (0:5): processing NONCE payload. message ID = -1957392785
23:10:44: ISAKMP (0:5): processing ID payload. message ID = -1957392785
23:10:44: ISAKMP (0:5): processing ID payload. message ID = -1957392785
23:10:44: ISAKMP (0:5): Creating IPsec SAs
23:10:44:     inbound SA from 202.12.184.137 to 203.44.206.217
        (proxy 172.27.1.0 to 172.29.20.61)
23:10:44:     has spi 0x783CD2E9 and conn_id 2000 and flags 4
23:10:44:     lifetime of 3600 seconds
23:10:44:     lifetime of 4608000 kilobytes
23:10:44:     outbound SA from 203.44.206.217  to 202.12.184.137 (proxy
172.29.20.61  to 172.27.1.0      )
23:10:44:     has spi 87633422 and conn_id 2001 and flags C
23:10:44:     lifetime of 3600 seconds
23:10:44:     lifetime of 4608000 kilobytes
23:10:44: ISAKMP (0:5): sending packet to 202.12.184.137 (I) QM_IDLE
23:10:44: ISAKMP (0:5): deleting node -1957392785 error FALSE reason ""
23:10:44: ISAKMP (0:5): Node -1957392785, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 68/185/340 ms
web-827-0#Old State = IKE_QM_I_QM1  New State = IKE_QM_PHASE2_COMPLETE
```