



Application Note

Configure a VPN Tunnel Between a Digi Transport
and Cisco Adaptive Security Appliance

Patrick W Brannelly

June 10, 2009

Contents

1	Introduction	5
1.1	Outline.....	5
1.2	Assumptions.....	5
1.3	Corrections.....	6
1.4	Version	6
2	Cisco Configuration	7
2.1	Put the Cisco ASA into configure mode	7
2.2	Configure the login passwords.....	7
2.3	Configure the Cisco ASA for basic routing to the internet.....	7
2.3.1	Configure LAN and WAN VLAN interfaces	7
2.3.2	Configure VLAN access.....	8
2.3.3	Configure the default route, which in this case points to the ADSL Router via the “Outside” interface.	8
2.4	Configure IKE.....	9
2.5	Configure IPSEC.....	9
3	Digi Transport Configuration	11
3.1	Configure the mobile interface and associated PPP interface	11
3.1.1	Configuration Parameters for SIM 1	11
3.1.2	PPP 3 Interface Configuration for SIM 1	12
3.1.3	PPP 3 Standard Page	12
3.2	Configure IKE.....	14
3.3	Configure the IPSEC Eroute.....	16
3.4	Configure the default eroute	19
3.5	Configure the pre-shared key	20
4	TESTING.....	22
4.1	View the IPsec Peers.....	22
4.2	View the IKE Security Associations	22
4.3	View the IPsec Eroute.....	23

Transport to Cisco ASA VPN Application Note

4.4	Cisco ASA Results	24
4.5	Ping test	24

Transport to Cisco ASA VPN Application Note

Figures

Figure 3-1: SIM 1 Configuration	12
Figure 3-2: PPP 3 - Standard Configuration	14
Figure 3-3: IKE 0 Configuration	16
Figure 3-4: IPSec Eroute (part 1)	18
Figure 3-5: IPSec Eroute (part 2)	19
Figure 3-6: Default Eroute.....	20
Figure 3-7: Pre-shared key/User configuration	21
Figure 4-1: IPSec Peers.....	22
Figure 4-2: IKE SAs.....	23
Figure 4-3: IPSec Eroute 0	23
Figure 4-4: Ping Results.....	24

Tables

Table 3-1: SIM 1 Parameters.....	11
Table 3-2: PPP 3 Standard Parameters	13

1 INTRODUCTION

1.1 Outline

It is often required to configure a Digi Transport router as one end of a VPN tunnel where the other end is a Cisco device such as a Cisco ASA. This Application Note aims to enable the reader to easily configure the Cisco device to accept incoming VPN requests from a remote Digi Transport router with a dynamic public IP address. The diagram below details the IP number scheme and architecture of this example configuration.

NOTE: *If the Transport's WAN IP address is translated from private to public, the head-end device must support NAT-Traversal version draft 3 (draft-ietf-ipsecnat-t-ike-03). Any version less than draft three is not useable in practice.*

1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a Digi Transport router and Cisco Adaptive Security Appliance and to configure them with basic routing functions.

This application note applies only to:

Model: Digi Transport WR, SR or DR and Cisco Adaptive Security Appliance

Firmware versions: All firmware and Cisco Adaptive Security Appliance Software versions

Configuration: This Application Note assumes the Transport router and Cisco ASA are set to the factory default configuration. Most configuration commands are only shown if they differ from the factory default.

For the purpose of this application note the following applies:

- The Transport's IP address is dynamic
- IPSEC is to be used in "aggressive mode"

If required, NAT-Traversal on the Transport can be activated via the web interface by browsing to Configuration - VPN > IPsec > IKE > IKE X (where "X" is the IKE instance) and setting the NAT-Traversal enabled: to YES.

Activating NAT-Traversal on the CISCO PIX can be done by entering the command:

isakmp nat-traversal

Transport to Cisco ASA VPN Application Note

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: support@digicom.com

Requests for new application notes can be sent to the same address.

1.4 Version

Version Number:	0.1
Status:	RELEASED

2 CISCO CONFIGURATION

The following Cisco Adaptive Security Appliance configuration was created using software version 7.2(3).

2.1 Put the Cisco ASA into configure mode

The ASA is put into configuration mode by using the command “configure terminal”. In Cisco devices, the commands can be shortened, so the command would be:

```
conf t
```

2.2 Configure the login passwords

Set the password and enable password using the commands *passwd* and *enable password*, as shown below where the password is “myloginpassword” and the enable password is “mysecret”:

```
passwd myloginpassword
enable password mysecret
```

2.3 Configure the Cisco ASA for basic routing to the internet.

To configure the ASA for basic routing, four steps are required:

1. Configure the local area network (LAN) and wide area network (WAN) VLAN interfaces
2. Configure VLAN access for the applicable Ethernet ports
3. Configure a default route
4. Configure Network Address Translation (NAT)

2.3.1 Configure LAN and WAN VLAN interfaces

The interfaces must be named and a security level applied. The security levels are set to default with the interface names, so “inside” has a default setting of 100 (the highest) and “outside” is 0 (the lowest).

In this example, VLAN 1 and 2 were used, but new VLANs can be created. In fact, it is typical not to use VLAN 1 in a normal setting. \\

The IP address of the LAN interface is 192.168.100.1/24 and the WAN interface is 70.57.159.140/27. Here are the commands needed and can only be applied in configuration mode:

```
interface Vlan1
  nameif inside
  security-level 100
```

Transport to Cisco ASA VPN Application Note

```
ip address 192.168.100.1 255.255.255.0
!
interface Vlan2
  nameif outside
  security-level 0
  ip address 70.57.159.140 255.255.255.224
```

2.3.2 Configure VLAN access

Now that the VLANs are created, the next step is to apply those VLANs to physical Ethernet ports. In this case, Ethernet ports 0/0 and 0/1 were used. Since VLAN 1 was used, and it is the default VLAN for all ports, it was not necessary to assign Ethernet 0/1 a VLAN. But in order to separate Ethernet 0/0 from VLAN 1 and be added to VLAN 2, the following commands were used:

```
interface Ethernet0/0
  switchport access vlan 2
```

2.3.3 Configure the default route, which in this case points to the ADSL Router via the “Outside” interface.

The default route is configured with the “catch-all” route of 0.0.0.0 0.0.0.0 and the gateway for the ADSL router, which in this case is 70.57.159.158.

```
route outside 0.0.0.0 0.0.0.0 70.57.159.158
```

2.3.3.1 Configure NAT

Normally, network address translation needs to be on for members of the LAN behind the gateway to reach the Internet. In the case of the VPN however, it is necessary to remove NAT functions between the two LANs connected by the tunnel. This is accomplished by creating a NAT instance that disables NAT and is associated with an access list. The access list is called “NONAT”. Next a NAT instance is created for the LAN to provide Internet access.

```
nat (inside) 0 access-list NONAT
nat (inside) 1 192.168.100.0 255.255.255.0 0 0
```

The access list “NONAT” creates a route between the two LANs: 192.168.100.0/24 and 192.168.1.0/24.

```
access-list NONAT extended permit ip 192.168.100.0 255.255.255.0
192.168.1.0 255.255.255.0
```


Transport to Cisco ASA VPN Application Note

The Cisco ASA's global outside address is used for outgoing NAT communications. In reality, the type of NAT is Port Address Translation (PAT), allowing all LAN users to use the same IP with a different TCP port. The command to bind NAT/PAT to the interface is:

```
global (outside) 1 interface
```

2.4 Configure IKE

IKE is configured by first enabling isakmp, and then creating a policy. The policy number is arbitrary. In this example, the authentication is a pre-shared key, the encryption is AES, the authentication algorithm is SHA-1 and the Diffie-Helman group is 2. The commands are as follows:

```
crypto isakmp enable outside
crypto isakmp policy 65535
  authentication pre-share
  encryption aes
  hash sha
  group 2
```

The pre-shared key is created by configuring a tunnel group and then the key. The tunnel group is the public IP address of the Transport router. The key in this example is "transport". Once configured, the configuration will show the key as an asterisk (*).

```
tunnel-group 67.177.44.106 ipsec-attributes
  pre-shared-key transport
```

2.5 Configure IPSEC

On the Cisco ASA, IPsec is created in two steps:

1. Create an IPsec Transform Set
2. Create a Crypto Map

The transform set defines the encryption and authentication methods of the tunnel. The command for the transform set is as follows:

```
crypto ipsec transform-set transport esp-aes esp-sha-hmac
```

The crypto map matches the outside address to the tunnel, the peer (which is the IP address of the Transport), the authentication and encryption and assigns the interface (outside). The commands are as follows:

```
crypto map outside_map 1 match address outside_1_cryptomap
crypto map outside_map 1 set peer 67.177.44.106
```

Transport to Cisco ASA VPN Application Note

```
crypto map outside_map 1 set transform-set ESP-AES-128-SHA  
crypto map outside_map interface outside
```

3 DIGI TRANSPORT CONFIGURATION

The Digi Transport can be configured using the web user interface or writing a new configuration file. Only the parts of the configuration file that specifically relate to the configuration of this example will be explained in detail. (The entire configuration file can be found at the end of this document.)

3.1 Configure the mobile interface and associated PPP interface

The mobile (W-WAN) interface and associated PPP instance need to be configured for WAN/Internet access. The following sections demonstrate the configuration of SIM 1 and PPP 3.

3.1.1 Configuration Parameters for SIM 1

The configuration page is located under **Configuration - Interfaces>Mobile>W-WAN Module>SIM 1**

Enter the APN (Access Point Name) and PIN number (if required) for SIM card 1. (Usually these will be provided by your mobile operator.) In the figure 2-1, the APN example is wap.cingular and there is no pin number. These settings will vary depending on the mobile operator.

Table 3-1: SIM 1 Parameters

Parameter	Setting	Description
APN	wap.cingular	Enter the correct APN for your network
PIN	1234	Enter the PIN number for your SIM card (if required)

Configuration - Interfaces > Mobile > W-WAN Module > SIM 1

Configure: W-WAN Module SIM 1

APN:	<input type="text" value="wap.cingular"/>
Static IP address:	<input type="text"/>
Use back-up APN:	<input type="button" value="Off"/> ▼
Back-up APN:	<input type="text"/>
Backup static IP address:	<input type="text"/>
Retry APN time (mins):	<input type="text" value="0"/>
PIN (Empty):	<input type="text"/>
Confirm PIN:	<input type="text"/>
PUK(Empty):	<input type="text"/>
Confirm PUK:	<input type="text"/>
Initialisation string 1:	<input type="text" value="+CGQREQ=1"/>
Initialisation string 2:	<input type="text" value="+CGQMIN=1"/>
Initialisation string 3:	<input type="text"/>
Network preference/locking string:	<input type="text"/>
Hang-up string:	<input type="text"/>
Post hang-up string:	<input type="text"/>
Intercall idle time (s):	<input type="text" value="0"/>
Link retries:	<input type="text" value="10"/>
Status retries:	<input type="text" value="30"/>
Signal strength event interval (mins):	<input type="text" value="0"/>
Minimum attach interval (secs):	<input type="text" value="0"/>
Power cycle on loss of registration:	<input type="button" value="W-WAN only"/> ▼
SMS message centre:	<input type="text"/>

Figure 3-1: SIM 1 Configuration

3.1.2 PPP 3 Interface Configuration for SIM 1

3.1.3 PPP 3 Standard Page

The configuration page is located under **Configuration - Interfaces > PPP > PPP 0 - 4 > PPP 3 > Standard.**

Transport to Cisco ASA VPN Application Note

PPP 3 is configured for W-WAN SIM 1 by default, but there are a few more parameters to configure to support failover. The following table and figures show these parameters and their settings:

Table 3-2: PPP 3 Standard Parameters

Parameter	Setting	Description
Dial-out number:	*98*1#	Dial string to attach to the GSM network
Use W-WAN/external modem:	Any W-WAN channel	Configures the router to use any W-WAN channel
W-WAN SIM:	SIM 1	Configures the W-WAN link on PPP 1 to use SIM card 1
Username:	Username	Username provided by the mobile carrier
Password:		Password provided by the mobile carrier
Confirm Password:		Same as above
Always On Mode:	ON	Auto activates PPP 3 and keeps the link up

Transport to Cisco ASA VPN Application Note

Configuration - Interfaces > PPP > PPP 0 - 4 > PPP 3 > Standard

Configure: PPP 3 (Standard)

Name:	<input type="text"/>
IP Analysis:	Off <input type="button" value="v"/>
PPP Analysis:	Off <input type="button" value="v"/>
Answering:	Off <input type="button" value="v"/>
Metric:	<input type="text" value="1"/>
Calling number:	<input type="text"/>
MSN:	<input type="text"/>
Sub-address:	<input type="text"/>
CLI:	<input type="text"/>
Remote access options:	No restrictions <input type="button" value="v"/>
Dial-out prefix:	<input type="text"/>
Dial-out number:	*98*1#
Dial-out number #2:	<input type="text"/>
Dial-out number #3:	<input type="text"/>
Dial-out number #4:	<input type="text"/>
Use W-WAN/external modem:	Any W-WAN channel <input type="button" value="v"/>
Detach W-WAN on link failure:	No <input type="button" value="v"/>
Detach W-WAN between connection attempts:	No <input type="button" value="v"/>
W-WAN SIM:	Any <input type="button" value="v"/>
Username:	ENTER WWAN Username
Password (Assigned):	<input type="text"/>
Confirm password:	<input type="text"/>
AODI NUA:	<input type="text"/>
Always on mode:	On <input type="button" value="v"/>
AODI delay (s):	<input type="text" value="0"/>
AODI delay when other PPPs inhibited by this one are connected (s):	<input type="text" value="0"/>
Power up AODI delay (s):	<input type="text" value="0"/>
Go out of service if first AODI connections fail:	Yes <input type="button" value="v"/>

Figure 3-2: PPP 3 - Standard Configuration

3.2 Configure IKE

IKE is the first stage in establishing a secure link between two endpoints. The Transport router will act as the IKE 'initiator' and as such will make first contact with the ASA's VPN server. This is because the

Transport to Cisco ASA VPN Application Note

Transport is using a dynamic IP address from the ISP which will change over time. This therefore makes it impossible for the ASA to know the Transport's IP address unless the Transport initiates the VPN connection. The Transport's current IP address will be included each time IKE is negotiated.

The IKE configuration is located at **Configuration - VPN > IPsec > IKE > IKE 0**. In this example, IKE 0 was used, but the Transport supports more than one IKE instance. The steps to configuration are the:

1. Encryption algorithm
2. Encryption key
3. Authentication algorithm
4. Duration
5. Aggressive mode (because of the dynamic IP address of the mobile interface)
6. Dead Peer Detection is also on by default
7. IKE MODP group
8. NAT Traversal is on by default, and can be left alone because it works only when needed
9. SA removal mode

Figure 3-3 shows the configuration page:

Configuration - VPN > IPsec > IKE > IKE 0	
Configure: IKE 0 (Initiator)	
Encryption algorithm:	AES
Encryption key bits (AES only):	128
Authentication algorithm:	SHA1
Duration (s):	1200
Aggressive mode:	On
Dead Peer Detection:	On
IKE MODP group:	2 (1024)
Minimum IPsec MODP group:	No PFS
RSA private key file:	
Maximum re-transmits:	2
Re-transmit interval (s):	10
Inactivity timeout (s):	30
Send INITIAL-CONTACT notifications:	Yes
Retain phase 1 SA after phase 2 negotiation failure:	No
NAT traversal enabled:	Yes
NAT traversal keep-alive interval (s):	20
SA removal mode:	Remove IPsec SAs when IKE SA removed
Use debug port:	Yes
Debug level:	Very High
Debug IP address filter:	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 3-3: IKE 0 Configuration

3.3 Configure the IPSEC Eroute

On the Digi Transport, the eroute is the VPN tunnel. The essential parameters are:

1. Peer IP/Hostname (the public IP address of the Cisco ASA)
2. Peer ID (also the public IP address of the Cisco ASA)
3. Our ID (0.0.0.0)
4. Send our ID as FQDN (send Our ID as a Fully Qualified Domain Name)

Transport to Cisco ASA VPN Application Note

5. Local subnet IP address (the Transport's LAN subnet)
6. Local subnet mask (the Transport's LAN subnet mask)
7. Remote subnet IP address (the Cisco ASA's LAN subnet)
8. Remote subnet mask (the Cisco ASA's LAN subnet mask)
9. Mode (Tunnel, not Transport)
10. ESP authentication algorithm (SHA1)
11. ESP encryption algorithm (AES)
12. No SA Action (Use IKE)
13. Create SA's automatically (YES)
14. Authentication method (Preshared Key)

Figure 3-4 and 3-5 demonstrate the configuration.

Transport to Cisco ASA VPN Application Note

Configuration - VPN > IPsec > IPsec Eroutes > Eroute 0 - 9 > Eroute 0	
Configure: IPsec EROUTE 0	
Description:	Digi ASA
Peer IP/hostname:	70.57.159.140
Backup peer IP:	
Peer ID:	70.57.159.140
Our ID:	0.0.0.0
XAUTH ID:	
RSA private key file:	
Send our ID as FQDN:	Yes
Interface to use for local subnet IP address:	None
Interface # to use for local subnet IP address:	0
Local subnet IP address:	192.168.1.0
Local subnet mask:	255.255.255.0
Local subnet IP address to negotiate (if different from above):	
Local subnet mask to negotiate (if different from above):	
Negotiate virtual local IP address using MODECFG (initiators only):	No
Remote subnet IP address:	192.168.100.0
Remote subnet mask:	255.255.255.0
Remote subnet ID:	
Local port:	0
Remote port:	0
TX packets with these TOS values through this eroute:	
First local port (IKEv2 only):	0
Last local port (IKEv2 only):	65535
First remote port (IKEv2 only):	0
Last remote port (IKEv2 only):	65535
Mode:	Tunnel
AH authentication algorithm:	Off
ESP authentication algorithm:	SHA1

Figure 3-4: IPsec Eroute (part 1)

Transport to Cisco ASA VPN Application Note

Configuration - VPN > IPSec > IPSec Eroutes > Eroute 0 - 9 > Eroute 0	
ESP authentication algorithm:	SHA1
ESP encryption algorithm:	AES
ESP encrypt key length (bits):	Default
IPCOMP algorithm:	Off
IPSec MODP group:	No PFS
IP protocol:	Off
Duration (s):	1200
Duration (kb):	1000
Inactivity Timeout (s):	0
No SA action:	Use IKE
Create SA's automatically:	Yes
Go out of service if automatic establishment fails:	No
Authentication method:	Preshared Keys
This eroute is tunnelled within another eroute:	No
NAT traversal keep-alive interval (s):	20
Link eroute with interface:	Any
Link eroute with interface #:	0
IKE config to use when initiator:	0
IKE version:	1
Check APN usage:	No
Interface must use this APN:	Main APN
Use Secondary IP address as source address:	No
Get source address from this interface:	N/A
Get source address from this interface #:	0
Delete SAs when eroute goes out of service:	No
Inhibit this eroute when these eroutes are not OOS:	
Inhibit unless this eroute is UP:	
Delete SAs if not VRRP Master:	No
Display IKE lookup debug info:	No

OK Cancel

Figure 3-5: IPSec Eroute (part 2)

3.4 Configure the default eroute

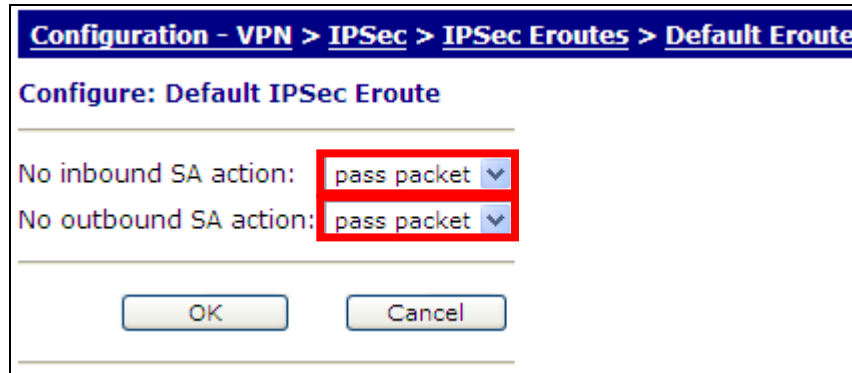
IPSec eroutes have a default configuration that is applied if no specific route can be found.

The configuration page is **Configuration - VPN > IPSec Eroutes > Default Eroute**. The parameters are as follows:

Transport to Cisco ASA VPN Application Note

Both “No inbound SA action” and “No outbound SA action” are set to “Pass Packet”. It is selected when data matching an Eroute definition will be decrypted and authenticated (depending on the eroute options selected) but data that does not match will also be allowed to pass.

Figure 3-6 shows the configuration page:



Configuration - VPN > IPsec > IPsec Eroutes > Default Eroute

Configure: Default IPsec Eroute

No inbound SA action: pass packet ▼

No outbound SA action: pass packet ▼

OK Cancel

Figure 3-6: Default Eroute

3.5 Configure the pre-shared key

The pre-shared key is configured under the User section located at **Configuration - Security > Users > User 10 - 19 > User 10.**

It is recommended User 10 or higher should be used to avoid accidentally configuring over another user, configured by default.

The username is the public IP address of the Cisco ASA and the password is the pre-shared key already configured on the Cisco ASA. In this example, it is “transport”. Figure 3-7 demonstrates this configuration:

Transport to Cisco ASA VPN Application Note

Configuration - Security > Users > User 10 - 19 > User 10

Configure: User 10

Name:	<input type="text" value="70.57.159.140"/>
Password:	<input type="password" value="••••••••"/>
Confirm Password:	<input type="password" value="••••••••"/>
New Password:	<input type="text"/>
Confirm New Password:	<input type="text"/>
Access Level:	<input type="text" value="None"/> ▾
Remote peer address:	<input type="text"/>
Remote subnet address:	<input type="text"/>
Remote subnet mask:	<input type="text"/>
Dialback number:	<input type="text"/>
Public Key file:	<input type="text"/> ▾
DUN access enabled:	<input type="text" value="Yes"/> ▾
Web page display mode:	<input type="text" value="Auto"/> ▾

Figure 3-7: Pre-shared key/User configuration

4 TESTING

The VPN tunnel can be tested by viewing the IPsec peers, the IKE and IPsec security associations and the Eroute under **Diagnostics - Status > IPsec > IPsec SAs** on the Transport, and by pinging a device on the Cisco ASA's LAN from a device on the Transport's LAN.

4.1 View the IPsec Peers

Figure 4-1 shows the peer, which is the Cisco ASA's public IP address.

Peer IP	Our ID	Peer ID	DPD	NATT local port	NATT remote port
70.57.159.140	0.0.0.0	70.57.159.140	Inactive. Next REQ in 109 secs	N/A	N/A

Remove all unused

Figure 4-1: IPsec Peers

4.2 View the IKE Security Associations

Figure 4-2 shows the IKE version 1 security associations, consisting of the Cisco ASA's and Transport's ID and IP.

Diagnostics - Status > IPsec > IKE SAs

IKE Status

V1 SAs

Our ID	Peer ID	Peer IP	Our IP	Session ID	Time Left	Internal ID	
0.0.0.0	70.57.159.140	70.57.159.140	67.177.44.106	0x0	1073	2894	Remove

[Remove All V1 SAs](#)

V2 SAs

[List Empty](#)

Figure 4-2: IKE SAs

4.3 View the IPsec Eroute

Figure 4-3 shows the IPsec Eroute which displays the peer IP address (Cisco ASA public IP), the remote and local selectors (the local subnets for each device), the ESP authentication and encryption, and the outbound interface.

Diagnostics - Status > IPsec > IPsec SAs > Eroute 0 - 9 > Eroute 0

IPsec Status: Eroutes 0 -> 0

Outbound V1 SAs

SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
1560fd53	0	70.57.159.140	192.168.100.0/24	192.168.1.0/24	N/A	SHA1	AES(128)	N/A	0	1000	924	PPP 3	Remove

[Remove All](#)

Inbound V1 SAs

SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
4ad059b8	0	70.57.159.140	192.168.100.0/24	192.168.1.0/24	N/A	SHA1	AES(128)	N/A	0	1000	924	PPP 3	Remove

[Remove All](#)

Outbound V2 SAs

[List Empty](#)

Inbound V2 SAs

[List Empty](#)

[Refresh](#)

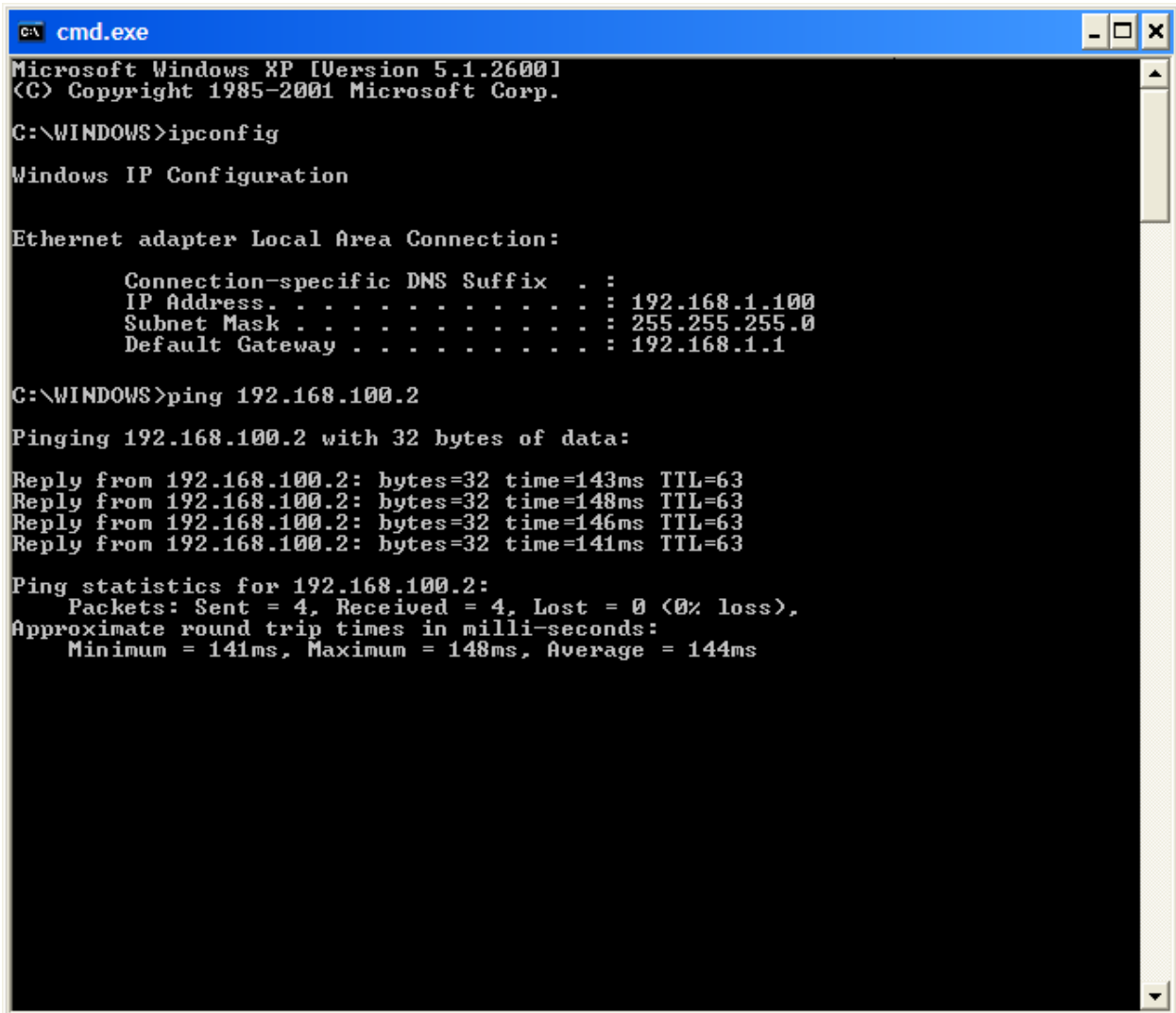
Figure 4-3: IPsec Eroute 0

4.4 Cisco ASA Results

4.5 Ping test

If in the above sections the SA's can be seen then the tunnel is up, the next step is to confirm the connectivity by sending a ping via the tunnel.

Figure 4-4 shows the IP configuration and ping results from a laptop on the Transport LAN to a device on the Cisco ASA with the IP address of 192.168.100.2.



```
cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\WINDOWS>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:

Reply from 192.168.100.2: bytes=32 time=143ms TTL=63
Reply from 192.168.100.2: bytes=32 time=148ms TTL=63
Reply from 192.168.100.2: bytes=32 time=146ms TTL=63
Reply from 192.168.100.2: bytes=32 time=141ms TTL=63

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 141ms, Maximum = 148ms, Average = 144ms
```

Figure 4-4: Ping Results