Application Note 27

Configure an IPsec VPN between a Digi TransPort and Cisco PIX

November 2015
### Contents

1. Introduction .............................................................................................................................................. 4  
   1.1 Assumptions ......................................................................................................................................... 5  
   1.2 Corrections ........................................................................................................................................ 5  
   1.3 Version ................................................................................................................................................ 5  

2. Digi transport Configuration .................................................................................................................. 6  
   2.1 Configure the cellular module .............................................................................................................. 6  
   2.2 Configure the Default IP route .......................................................................................................... 7  
   2.3 Configure the Private Network Interface (Ethernet 0) ....................................................................... 8  
   2.4 Configure IKE ...................................................................................................................................... 9  
   2.5 Turn on IKE debug ............................................................................................................................. 9  
   2.6 Configure the IPSEC Eroute .............................................................................................................. 10  
   2.7 Configure the pre-shared key .......................................................................................................... 12  
   2.8 Set up the analyser trace .................................................................................................................. 12  

3. Cisco PIX Configuration ....................................................................................................................... 14  
   3.1 Put the CISCO PIX into Global configuration mode ......................................................................... 14  
   3.2 Enter a Hostname for the Cisco PIX ................................................................................................ 14  
   3.3 Configure the login passwords ......................................................................................................... 14  
   3.4 Configure the Cisco PIX for basic routing to the internet. ................................................................ 14  
   3.5 Name the interfaces and assign a security level ............................................................................. 14  
   3.6 Assign an IP address to the Ethernet interfaces .............................................................................. 14  
   3.7 Configure an Access List permitting access to and from the protected private networks .......... 15  
   3.8 Configure the default route, which in this case points to the ADSL Router via the “Outside” interface ......................................................................................................................... 15  
   3.9 Configure NAT .................................................................................................................................. 15  
   3.10 Configure IKE ................................................................................................................................... 15  
      3.10.1 Enable IKE on the outside interface ......................................................................................... 15  
      3.10.2 Specify the authentication method (pre-shared keys) ............................................................. 16  
   3.11 Enter a domain name for the Cisco PIX .......................................................................................... 16
3.12 Configure a pre-shared key ........................................................................................................ 16
3.13 Specify an encryption method for the IKE negotiations .............................................................. 16
3.14 Specify an ESP authentication algorithm for the IKE negotiations ............................................... 16
3.15 Specify a MODP Diffie-Hellman group for the IKE negotiations .................................................. 16
3.16 Specify a key lifetime before the key is renewed ......................................................................... 16
3.17 Enable NAT traversal .................................................................................................................. 17
3.18 Configure IPSEC .......................................................................................................................... 17
    3.18.1 Create IPSec security associations, security association global lifetime values, and global
    transform sets .............................................................................................................................. 17
    3.18.2 Create a dynamic crypto map entry ...................................................................................... 17
    3.18.3 Create a crypto map entry .................................................................................................... 17
    3.18.4 Specify the identifying interface to be used by the PIX Firewall to identify itself to peers .... 18
    3.18.5 Permit all inbound IPSec authenticated cipher sessions. This allows IPSec traffic to pass
    through the PIX Firewall .............................................................................................................. 18
3.19 Save the configuration .................................................................................................................. 18
4  TESTING ........................................................................................................................................ 19
    4.1 Confirm that the W-WAN interface (PPP 3) is up ...................................................................... 19
    4.2 Check the Eventlog .................................................................................................................... 19
        4.2.1 IPSec Security Associations ............................................................................................... 20
    4.3 Ping test ..................................................................................................................................... 21
    4.4 Cisco PIX show output ............................................................................................................... 23
5  CONFIGURATION FILEs ................................................................................................................ 26
    5.1 Digi Transport DR6410 (Initiator) ............................................................................................. 26
        5.1.1 Digi Transport Firmware Versions ..................................................................................... 29
    5.2 Cisco PIX 501 (Responder) ....................................................................................................... 30
1 INTRODUCTION

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

NB: If the TransPort is a cellular router and the WAN IP address is “natted” it can still work but the head-end device must support NAT traversal version draft 3 (draft-ietf-ipsec-nat-t-ike-03). Any version less than draft three is not useable in practice.

Figure 1-1: Overview Diagram
1.1 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.

This application note applies to;
**Model shown:** Digi Transport DR64 router with W-WAN running firmware version 5156.

**Other Compatible Models:** All Digi Transport routers with a WAN or W-WAN interface.
**Firmware versions:** 4905 or later.

**Configuration:** This Application Note assumes the devices are set to their factory default configurations. Most configuration commands are only shown if they differ from the factory default.

1.2 Corrections

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

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

1.3 Version

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Published</td>
</tr>
<tr>
<td>2.0</td>
<td>Rebranded and updated to 5156 firmware</td>
</tr>
</tbody>
</table>
2 DIGI TRANSPORT CONFIGURATION

2.1 Configure the cellular module.

Browse to

**Configuration - Network > Interfaces > Mobile**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIM</td>
<td>1</td>
<td>Select SIM 1 for the PPP 3 interface</td>
</tr>
<tr>
<td>Service Plan/APN</td>
<td>APN</td>
<td>The Access Point Name for the network</td>
</tr>
</tbody>
</table>

![Configuration - Network > Interfaces > Mobile](image)

Select a SIM to configure from the list below.

Settings on this page apply to the selected SIM.

SIM: 1 (PPP 3)

IMS: 234159087893245

Select the service plan and connection settings used in connecting to the mobile network.

**Mobile Settings**

- **Service Plan / APN**: Choose the APN for the service plan.
- **Use backup APN**: Check this if you want to use a backup APN.
- **SIM PIN**: Enter the SIM PIN (Optional).
- **Confirm SIM PIN**: Re-enter the SIM PIN for confirmation.
- **Username**: Enter the WWAN username (Optional).
- **Password**: Enter the WWAN password (Optional).
- **Confirm Password**: Enter the WWAN password again (Optional).
Next browse to:

**Configuration - Network > Interfaces > Advanced > PPP 0 - 9 > PPP 3 > Advanced**

And make sure that "Always On" mode is enabled on this interface

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Always On” mode</td>
<td>✓</td>
<td>Sets this interface as ‘Always on’</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(This is the default setting for PPP 3)</td>
</tr>
</tbody>
</table>

**Configuration - Network > Interfaces > Advanced > PPP 0 - 9 > PPP 3 > Advanced**

Click Apply

### 2.2 Configure the Default IP route

**Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0**

And make the following settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>PPP</td>
<td>Enter PPP as the default route interface type</td>
</tr>
<tr>
<td>Interface #</td>
<td>PPP 3</td>
<td>Enter 3 as the PPP interface number</td>
</tr>
</tbody>
</table>

**Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0**

Click Apply
2.3 Configure the Private Network Interface (Ethernet 0)

This will be the gateway address of any devices on the LAN.

**Configuration - Network > Interfaces > Ethernet > ETH 0**

And make the following settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.100.254</td>
<td>Enter the TransPort’s Ethernet IP address</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>Enter the TransPort’s Ethernet subnet mask</td>
</tr>
</tbody>
</table>

Click Apply
2.4 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 VPN server. This is because the TransPort router is issued with a dynamic IP address from the ISP which will change over time. This therefore makes it impossible for the Cisco PIX 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.

**Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Algorithm:</td>
<td>3DES</td>
<td>Set the Encryption Algorithm to 3DES</td>
</tr>
<tr>
<td>Authentication Algorithm:</td>
<td>SHA1</td>
<td>Set the Authentication Algorithm to SHA1</td>
</tr>
<tr>
<td>Renegotiate after</td>
<td>1200</td>
<td>Set the IKE lifetime to 1200 seconds (20 mins)</td>
</tr>
<tr>
<td>Mode</td>
<td>Aggressive</td>
<td>Enable Aggressive Mode</td>
</tr>
<tr>
<td>MODP Group for Phase 1</td>
<td>2(1024)</td>
<td>Configure Diffie-Hellman group 2</td>
</tr>
</tbody>
</table>

Click Apply

2.5 Turn on IKE debug

**Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Debug**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IKE Debug</td>
<td>✔</td>
<td>Enables IKE debugging to be displayed on the debug port</td>
</tr>
<tr>
<td>Debug Level</td>
<td>Very High</td>
<td>Full IKE debug will be recorded</td>
</tr>
</tbody>
</table>

Click Apply
## 2.6 Configure the IPSEC Eroute

Browse to:

**Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 0**

And make the following settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address or hostname of the remote unit</td>
<td>217.34.133.30</td>
<td>Enter the WAN IP address of the Cisco PIX</td>
</tr>
<tr>
<td>local LAN IP Address</td>
<td>192.168.100.0</td>
<td>Enter the local subnet IP address</td>
</tr>
<tr>
<td>local LAN Mask</td>
<td>255.255.255.0</td>
<td>Enter the local subnet mask</td>
</tr>
<tr>
<td>Remote LAN IP Address</td>
<td>172.16.0.0</td>
<td>Enter the remote subnet IP address</td>
</tr>
<tr>
<td>Remote LAN Mask</td>
<td>255.255.0.0</td>
<td>Enter the remote subnet mask</td>
</tr>
<tr>
<td>Use the following security on this tunnel</td>
<td>Preshared Keys</td>
<td>Select Pre-shared keys for the authentication method</td>
</tr>
<tr>
<td>Our ID</td>
<td>0.0.0.0</td>
<td>PIX expects to see 0.0.0.0</td>
</tr>
<tr>
<td>Our ID type</td>
<td>FQDN</td>
<td>PIX expects to see ID as a fully qualified Domain name</td>
</tr>
<tr>
<td>Use the following encryption on this tunnel</td>
<td>3DES</td>
<td>Select 3DES as the encryption algorithm</td>
</tr>
<tr>
<td>Use the following authentication on this tunnel</td>
<td>SHA1</td>
<td>Select SHA 1 as the authentication algorithm</td>
</tr>
<tr>
<td>Use Diffie Hellman group</td>
<td>2</td>
<td>Configure Diffie-Hellman group 2</td>
</tr>
<tr>
<td>Bring this tunnel up</td>
<td>All the time</td>
<td>This controls how the IPsec tunnel is brought up</td>
</tr>
<tr>
<td>If the tunnel is down and a packet is ready to be sent</td>
<td>Bring the tunnel up</td>
<td>Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent.</td>
</tr>
<tr>
<td>Renew the tunnel after</td>
<td>1200</td>
<td>Enter 1200 (20 mins) seconds for the IPSEC lifetime</td>
</tr>
<tr>
<td>IPsec mode</td>
<td>Tunnel</td>
<td>Set IPsec mode as tunnel</td>
</tr>
</tbody>
</table>
And under “Advanced” make sure that IPsec mode is set to “Tunnel”

Click Apply
2.7 Configure the pre-shared key

Browse to:

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>pixfirewall.ciscopix.com</td>
<td>This is what the Cisco PIX sends to the TransPort</td>
</tr>
<tr>
<td>Password</td>
<td>secret</td>
<td>Preshared secret key</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>secret</td>
<td>Preshared secret key</td>
</tr>
<tr>
<td>Access Level</td>
<td>None</td>
<td>This user will not be granted any admin access as only used as a Preshared key</td>
</tr>
</tbody>
</table>

The user ID in the user table is a combination of the PIX’s configured “hostname” and “domain-name” fields. So in this instance the user ID is pixfirewall.ciscopix.com

The password field is the preshared key. This must match the preshared key on the PIX.

**Click Apply**

2.8 Set up the analyser trace

Configure the Analyser to assist with any troubleshooting that may be required.

**Management - Analyser > Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Analyser</td>
<td>✓</td>
<td>Enables analysis</td>
</tr>
<tr>
<td>Maximum packet capture size</td>
<td>1500</td>
<td>Captures the full packet</td>
</tr>
<tr>
<td>Log size</td>
<td>180</td>
<td>180 is the maximum log size in Kb</td>
</tr>
<tr>
<td>Protocol Layers</td>
<td>1,2 and 3</td>
<td>Enable debug on these layers</td>
</tr>
<tr>
<td>Enable IKE Debug</td>
<td>✓</td>
<td>IKE debugging information is recorded</td>
</tr>
<tr>
<td>IP Sources</td>
<td>PPP 3</td>
<td>PPP 3 IP data is recorded</td>
</tr>
<tr>
<td>IP Packet Filters: TCP/UDP Ports</td>
<td>~500, 4500</td>
<td>IKE &amp; NAT-T traffic is recorded</td>
</tr>
</tbody>
</table>
Click Apply
The following Cisco PIX configuration was used on a PIX 501 running software version 6.3(3).

3.1  Put the CISCO PIX into Global configuration mode

```
Config t
Pix#Config t
```

3.2  Enter a Hostname for the Cisco PIX

```
hostname hostname
Pix(config)#hostname pixfirewall
```

3.3  Configure the login passwords

Set the password and enable password

```
passwd password
enable password secret
```

```
pixfirewall(config)# passwd myloginpassword
pixfirewall(config)# enable password mysecret
```

3.4  Configure the Cisco PIX for basic routing to the internet.

Set the interface speed to each interface.

```
interface <hardware_id> [<hw_speed> auto|100full]
pixfirewall(config)#interface ethernet0 auto
pixfirewall(config)#interface ethernet1 100full
```

3.5  Name the interfaces and assign a security level

```
nameif hardware_id if_name security_level
pixfirewall(config)#nameif ethernet0 outside security0
pixfirewall(config)#nameif ethernet1 inside security100
```

3.6  Assign an IP address to the Ethernet interfaces.

In this example, Ethernet 0 (Outside interface) is assigned a fixed public IP address and Ethernet 1 (Inside interface) is assigned a private IP address.

```
ip address if_name ip_address [netmask]
pixfirewall(config)#ip address outside 217.34.133.30 255.255.255.240
pixfirewall(config)#ip address inside 172.16.30.100 255.255.0.0
```
3.7 Configure an Access List permitting access to and from the protected private networks

The access list shown below permits traffic to be sent from the 172.16.x.x network via the IPSec tunnel, to the 192.168.100.x network. The Remote/Local subnets in the TransPort’s Eroute configuration will mirror this access list. The access list can also serve to determine which traffic will initiate the IKE and IPSec negotiations. However, as the TransPort in this example has a dynamic IP address the TransPort will be the initiator.

```
access-list acl_ID [deny | permit] protocol {source_addr | local_addr} {source_mask | local_mask} operator port {destination_addr | remote_addr} {destination_mask | remote_mask} operator port
```

```
pixfirewall(config)#access-list NONAT permit ip 172.16.0.0 255.255.0.0 192.168.100.0 255.255.255.0
pixfirewall(config)#access-list NONAT permit icmp 172.16.0.0 255.255.0.0 192.168.100.0 255.255.255.0
```

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

```
routef if_name ip_address netmask gateway_ip
```

```
pixfirewall(config)#route outside 0.0.0.0 0.0.0.0 217.34.133.29 1
```

3.9 Configure NAT

Turn on NAT and associate networks where NAT is to be applied on outgoing connections. The NAT_id is an arbitrary positive number. If the number was to be ‘0’ then this would specify that traffic is to be exempt from using NAT

```
nat [(if_name)] nat_id local_ip netmask
```

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

Bind the Global address to the outside interface

```
global [(if_name)] nat_id {global_ip [-global_ip] [netmask global_mask]} | interface
```

```
pixfirewall(config)#global (outside) 1 interface
```

3.10 Configure IKE

3.10.1 Enable IKE on the outside interface.

```
isakmp enable interface-name
```

```
pixfirewall(config)#isakmp enable outside
```
### 3.10.2 Specify the authentication method (pre-shared keys)

The policy [priority] uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

```bash
isakmp policy priority authentication pre-share | rsa-sig
```

```bash
pixfirewall(config)#isakmp policy 10 authentication pre-share
```

### 3.11 Enter a domain name for the Cisco PIX

If you do not have a registered domain name for the Cisco’s IP address then this parameter can be anything you like. This is important as this will be the host id transmitted to the TransPort during the IKE negotiations and is linked to the pre-shared keys.

```bash
domain-name domain name
```

```bash
pixfirewall(config)#domain-name ciscopix.com
```

### 3.12 Configure a pre-shared key

Specify a pre-shared key (which in this example is the word “secret”) linking it to a remote peer. In this example the remote peer will have a dynamic public IP address therefore all 0’s for the peer IP and subnet mask.

```bash
isakmp key keystring address peer-address [netmask mask]
```

```bash
pixfirewall(config)#isakmp key secret address 0.0.0.0 netmask 0.0.0.0
```

### 3.13 Specify an encryption method for the IKE negotiations

```bash
isakmp policy priority encryption encryption algorithm
```

```bash
pixfirewall(config)#isakmp policy 10 encryption 3des
```

### 3.14 Specify an ESP authentication algorithm for the IKE negotiations

```bash
isakmp policy priority hash authentication algorithm
```

```bash
pixfirewall(config)#isakmp policy 10 hash sha
```

### 3.15 Specify a MODP Diffie-Hellman group for the IKE negotiations

```bash
isakmp policy priority group diffie-hellman group
```

```bash
pixfirewall(config)#isakmp policy 10 group 2
```

### 3.16 Specify a key lifetime before the key is renewed

```bash
isakmp policy priority lifetime lifetime
```

```bash
pixfirewall(config)#isakmp policy 10 lifetime 1200
```
### 3.17 Enable NAT traversal

```
isakmp nat-traversal [natkeepalive]
pixfirewall(config)#isakmp nat-traversal 20
``` 

### 3.18 Configure IPSEC

#### 3.18.1 Create IPsec security associations, security association global lifetime values, and global transform sets.
- A **transform-set** represents a certain combination of security protocols and algorithms. During the IPsec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow.
- A **transform-set-name** specifies a name for your transform set.
- **Transform (1, 2 and 3)** Specifies up to three transforms. Transforms define the IPsec security protocol(s) and algorithm(s). Each transform represents an IPsec security protocol (ESP, AH, or both) plus the algorithm you want to use. In our example we specify just one.

```
crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]
pixfirewall(config)#crypto ipsec transform-set myset esp-3des esp-sha-hmac
``` 

#### 3.18.2 Create a dynamic crypto map entry
- A **dynamic-map-name** specifies a name for your dynamic crypto map set.
- A **dynamic-seq-num** specifies the sequence number that corresponds to the dynamic crypto map entry.

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set transform-set transform-set-name
pixfirewall(config)#crypto dynamic-map cisco 1 set transform-set myset
``` 

#### 3.18.3 Create a crypto map entry
- **map-name** specifies the name of the dynamic crypto map set to be used as the policy template.
- **dynamic-seq-num** is the number you assign to the crypto map entry.
- **seq-num** The number you assign to the crypto map entry.
- **ipsec-isakmp** indicates that IKE will be used to establish the IPsec security associations for protecting the traffic specified by this crypto map entry.
- **dynamic-map-name** specifies the name of the dynamic crypto map set to be used as the policy template.

```
crypto map map-name seq-num ipsec-isakmp dynamic [dynamic-map-name]
pixfirewall(config)#crypto map vpn-map 10 ipsec-isakmp dynamic cisco
```
3.18.4 Specify the identifying interface to be used by the PIX Firewall to identify itself to peers

crypto map map-name interface interface-name

pixfirewall(config)#crypto map vpn-map interface outside

3.18.5 Permit all inbound IPSec authenticated cipher sessions. This allows IPSec traffic to pass through the PIX Firewall

sysopt connection { permit-ipsec | permit-l2tp | permit-pptp | timewait | {tcpmss [minimum] <bytes>} }

pixfirewall(config)#sysopt connection permit-ipsec

3.19 Save the configuration

pixfirewall(config)#write mem
4.1 Confirm that the W-WAN interface (PPP 3) is up

Management - Network Status > Interfaces > Mobile

4.2 Check the Eventlog

Management - Event Log

The eventlog shows the events occurring within the operating system. Here you can see the W-WAN interface (PPP 3) comes up and the VPN is established.
4.2.1 IPsec Security Associations

On successful connection you will see the IPSec SAs in both the Initiator and the Responder IPSec SAs list. The following outputs display the IPsec tunnel, the IPsec peers and IKE Security Associations.

Here you can see the peer IP the remote and local networks, the authentication algorithm and time left until keys are again exchanged.

Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec Tunnels 0 - 9 > IPsec Tunnel 0

<table>
<thead>
<tr>
<th>#</th>
<th>Peer IP Addr</th>
<th>Local Network</th>
<th>Remote Network</th>
<th>AH</th>
<th>ESP Auth</th>
<th>ESP Enc</th>
<th>IP Comp</th>
<th>KBys Delivered</th>
<th>KBytes Left</th>
<th>Time Left (secs)</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>217.34.133.30</td>
<td>192.168.100.0/24</td>
<td>172.16.0.0/16</td>
<td>N/A</td>
<td>SHA1</td>
<td>3DES</td>
<td>N/A</td>
<td>0</td>
<td>4608000</td>
<td>1116</td>
<td>PPP 3</td>
</tr>
</tbody>
</table>

Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Peers

<table>
<thead>
<tr>
<th>Peer IP Address</th>
<th>Our ID</th>
<th>Peer ID</th>
<th>Dead Peer Detection (DPD)</th>
<th>NATT Local Port</th>
<th>NATT Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>217.34.133.30</td>
<td>0.0.0.0</td>
<td>pixfirewall.ciscopix.com</td>
<td>Active (40), Next REQ in 103 secs</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Management - Connections > Virtual Private Networking (VPN) > IPsec > IKE SAs
4.3 Ping test

Ping across the VPN tunnel from the host PC at each end.

From the Cisco PIX LAN a successful ping from 172.16.30.2 across the tunnel
From the Digi Transport DR64 LAN a Successful ping from 192.168.100.2 across the tunnel
4.4  Cisco PIX show output

pixfirewall# sh crypto isakmp sa
Total : 1
Embryonic : 0

<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>pending</th>
<th>created</th>
</tr>
</thead>
<tbody>
<tr>
<td>217.34.133.30</td>
<td>212.183.128.77</td>
<td>QM_IDLE</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

IKE phase one is established

pixfirewall# show crypto ipsec sa

interface: outside
  Crypto map tag: vpn-map, local addr. 217.34.133.30

  local  ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
  current_peer: 212.183.128.77:44937
  dynamic allocated peer ip: 0.0.0.0

    PERMIT, flags={transport_parent,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 217.34.133.30, remote crypto endpt.: 212.183.128.77
    path mtu 1500, ipsec overhead 64, media mtu 1500
    current outbound spi: 264789d

inbound esp sas:
  spi: 0xfea24b5a(4272048986)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel UDP-Encaps, }
    slot: 0, conn id: 1, crypto map: vpn-map
    sa timing: remaining key lifetime (k/sec): (4608000/832)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x264789d(40138909)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel UDP-Encaps, }
    slot: 0, conn id: 2, crypto map: vpn-map
sa timing: remaining key lifetime (k/sec): (4608000/823)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

IPsec tunnel is created successfully....

pixfirewall# sh crypto ipsec sa

interface: outside
   Crypto map tag: vpn-map, local addr. 217.34.133.30

local ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
current_peer: 212.183.128.27:15984
dynamic allocated peer ip: 0.0.0.0

PERMIT, flags={transport_parent,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 217.34.133.30, remote crypto endpt.: 212.183.128.27
path mtu 1500, ipsec overhead 64, media mtu 1500
current outbound spi: abafd410

inbound esp sas:
spi: 0x208aa9b2(545958322)
   transform: esp-3des esp-sha-hmac,
in use settings ={Tunnel UDP-Encaps,}
   slot: 0, conn id: 4, crypto map: vpn-map
sa timing: remaining key lifetime (k/sec): (4607999/1035)
IV size: 8 bytes
   replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xabafd410(2880427024)
   transform: esp-3des esp-sha-hmac,
And after the pings are sent we can see the packets are encrypted

```
pixfirewall# sh crypto map

Crypto Map: "vpn-map" interfaces: { outside }

Crypto Map "vpn-map" 10 ipsec-isakmp
  Dynamic map template tag: cisco

Crypto Map "vpn-map" 20 ipsec-isakmp
  Peer = 212.183.128.77
  access-list dynacl13; 1 elements
    access-list dynacl13 line 1 permit ip 172.16.0.0 255.255.0.0 192.168.100.0 255.255.255.0 (hitcnt=0)
  dynamic (created from dynamic map cisco/1)
  Current peer: 212.183.128.77
  Security association lifetime: 4608000 kilobytes/1200 seconds
  PFS (Y/N): Y
  DH group: group2
  Transform sets={ myset, }```
5 CONFIGURATION FILES

5.1 Digi Transport DR6410 (Initiator)

This is the config.dao file used for the purpose of this Application Note

```
config c show
wifinode 0 enabled OFF
wifinode 0 ssid "digi.router.SN:%s"
eth 0 descr "LAN 0"
et 0 IPaddr "192.168.100.254"
et 0 bridge ON
et 1 descr "LAN 1"
et 2 descr "LAN 2"
et 3 descr "LAN 3"
et 4 descr "ATM PVC 0"
et 4 do_nat 2
et 5 descr "ATM PVC 1"
et 5 do_nat 2
et 6 descr "ATM PVC 2"
et 6 do_nat 2
et 7 descr "ATM PVC 3"
et 7 do_nat 2
et 8 descr "ATM PVC 4"
et 8 do_nat 2
et 9 descr "ATM PVC 5"
et 9 do_nat 2
et 10 descr "ATM PVC 6"
et 10 do_nat 2
et 11 descr "ATM PVC 7"
et 11 do_nat 2
et 12 descr "Logical"
et 13 descr "Logical"
et 14 descr "Logical"
et 15 descr "Logical"
et 16 descr "Logical"
addp 0 enable ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
ip 0 cidr ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
def_route 1 ll_ent "eth"
def_route 1 ll_add 4
def_route 2 ll_ent "PPP"
def_route 2 ll_add 3
eroute 0 peerip "217.34.133.30"
eroute 0 ourid "0.0.0.0"
eroute 0 ouridtype 1
eroute 0 locip "192.168.100.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "172.16.0.0"
eroute 0 remmsk "255.255.0.0"
```
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "3DES"
eroute 0 ltime 1200
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"
eroute 0 autosa 2
eroute 0 dhgroup 2
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
dyndns 0 epassword "MjZ7WEodFg8="
ppp 0 timeout 300
  pp 1 name "ADSL"
  pp 1 liface "AAL"
  pp 1 IPaddr "0.0.0.0"
  pp 1 timeout 0
  pp 1 aodion 1
  pp 1 autoassert 1
  pp 1 immos ON
  pp 1 echo 10
  pp 1 echodropcnt 5
  pp 3 name "W-wAN (HSPA 3G)"
  pp 3 phonenum "*98*1#"
  pp 3 username "ENTER WwAN Username"
  pp 3 epassword "KD51SVJDVVg="
  pp 3 r_addr OFF
  pp 3 IPaddr "0.0.0.0"
  pp 3 l_addr ON
  pp 3 timeout 0
  pp 3 ipsec 1
  pp 3 use_modem 1
  pp 3 aodion 1
  pp 3 autoassert 1
  pp 3 immos ON
  pp 3 l_pap OFF
  pp 3 l_chap OFF
  pp 3 r_chap OFF
  pp 3 defpak 16
  pp 4 defpak 16
ike 0 encalg "3DES"
ike 0 authalg "SHA1"
ie 0 ltime 1200
ike 0 aggressive ON
ike 0 ikegroup 2
modemcc 0 info_asy_add 8
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "internet"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.Goes.Here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_interval_2 1
ana 0 anon ON
ana 0 lion ON
ana 0 lapdon 0
ana 0 asyon 1
ana 0 logsize 45
cmd 0 unitid "ss%>
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 tremto 1200
cmd 0 web_suffix ".wb2"
user 1 name "username"
user 1 epassword "KDS1SVJDVVg=
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
user 10 name "pixfirewall.ciscopix.com"
user 10 epassword "Kzp1SEBY"
user 10 access 4
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
idigi 0 sms_optin ON
### 5.1.1 Digi Transport Firmware Versions

This is the firmware version used for the purpose of this Application Note

<table>
<thead>
<tr>
<th>Component</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>ati5</td>
<td></td>
</tr>
<tr>
<td>Digi Transport DR64-HXA1-WE2-XX(MkII) Ser#:155285 HW Revision: 7503a</td>
<td></td>
</tr>
<tr>
<td>Software Build Ver5156.</td>
<td></td>
</tr>
<tr>
<td>ARM Bio Ver 6.67 v35 197MHz B128-M128-F300-0100000,0 MAC:00042d025e95</td>
<td></td>
</tr>
<tr>
<td>Power Up Profile:</td>
<td></td>
</tr>
<tr>
<td>Async Driver</td>
<td>1.19</td>
</tr>
<tr>
<td>Int clk</td>
<td></td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>2.0</td>
</tr>
<tr>
<td>Ethernet Port Isolate Driver</td>
<td>1.11</td>
</tr>
<tr>
<td>Firewall</td>
<td>1.0</td>
</tr>
<tr>
<td>EventEdit</td>
<td>1.0</td>
</tr>
<tr>
<td>Timer Module</td>
<td>1.1</td>
</tr>
<tr>
<td>AAL</td>
<td>1.0</td>
</tr>
<tr>
<td>ADSL</td>
<td>1.0</td>
</tr>
<tr>
<td>(B)USBHOST</td>
<td>1.0</td>
</tr>
<tr>
<td>L2TP</td>
<td>1.10</td>
</tr>
<tr>
<td>PPTP</td>
<td>1.00</td>
</tr>
<tr>
<td>TACPLUS</td>
<td>1.00</td>
</tr>
<tr>
<td>MySQL</td>
<td>0.01</td>
</tr>
<tr>
<td>LAPB</td>
<td>1.12</td>
</tr>
<tr>
<td>X25 Layer</td>
<td>1.19</td>
</tr>
<tr>
<td>MACRO</td>
<td>1.0</td>
</tr>
<tr>
<td>PAD</td>
<td>1.4</td>
</tr>
<tr>
<td>X25 Switch</td>
<td>1.7</td>
</tr>
<tr>
<td>V120</td>
<td>1.16</td>
</tr>
<tr>
<td>TPAD Interface</td>
<td>1.12</td>
</tr>
<tr>
<td>SCRIBATS6K</td>
<td>1.0</td>
</tr>
<tr>
<td>BASTSK</td>
<td>1.0</td>
</tr>
<tr>
<td>ARM Sync Driver</td>
<td>1.18</td>
</tr>
<tr>
<td>TCP (HASH mode)</td>
<td>1.14</td>
</tr>
<tr>
<td>TCP Utilities</td>
<td>1.13</td>
</tr>
<tr>
<td>PPP</td>
<td>1.19</td>
</tr>
<tr>
<td>WEB</td>
<td>1.5</td>
</tr>
<tr>
<td>SMTP</td>
<td>1.1</td>
</tr>
<tr>
<td>FTP Client</td>
<td>1.5</td>
</tr>
<tr>
<td>FTP</td>
<td>1.4</td>
</tr>
<tr>
<td>IKE</td>
<td>1.0</td>
</tr>
<tr>
<td>PollANS</td>
<td>1.2</td>
</tr>
<tr>
<td>PPPOE</td>
<td>1.0</td>
</tr>
<tr>
<td>BRIDGE</td>
<td>1.1</td>
</tr>
<tr>
<td>MODEM CC (Option 3G)</td>
<td>1.4</td>
</tr>
<tr>
<td>FLASH Write</td>
<td>1.2</td>
</tr>
<tr>
<td>Command Interpreter</td>
<td>1.38</td>
</tr>
<tr>
<td>SSLCLI</td>
<td>1.0</td>
</tr>
<tr>
<td>OSPF</td>
<td>1.0</td>
</tr>
<tr>
<td>BGP</td>
<td>1.0</td>
</tr>
<tr>
<td>QOS</td>
<td>1.0</td>
</tr>
<tr>
<td>RADIUS Client</td>
<td>1.0</td>
</tr>
<tr>
<td>SSH Server</td>
<td>1.0</td>
</tr>
<tr>
<td>SCP</td>
<td>1.0</td>
</tr>
<tr>
<td>CERT</td>
<td>1.0</td>
</tr>
<tr>
<td>LowPrlo</td>
<td>1.0</td>
</tr>
<tr>
<td>Tunnel</td>
<td>1.2</td>
</tr>
<tr>
<td>OVPN</td>
<td>1.2</td>
</tr>
<tr>
<td>TEMLOG</td>
<td>1.0</td>
</tr>
<tr>
<td>TEMPLOG</td>
<td>2.0</td>
</tr>
<tr>
<td>iDigi</td>
<td></td>
</tr>
</tbody>
</table>
5.2 Cisco PIX 501 (Responder)

This is the running configuration used for the purpose of this Application Note

```
pixfirewall# sh run
: Saved :
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name ciscopix.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list NONAT permit icmp 172.16.0.0 255.255.0.0 192.168.100.0 255.255.255.0
access-list NONAT permit ip 172.16.0.0 255.255.0.0 192.168.100.0 255.255.255.0
access-list acl-outside permit icmp any any
access-list acl-inside permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 217.34.133.30 255.255.255.240
ip address inside 172.16.30.100 255.255.0.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list NONAT
nat (inside) 1 192.168.100.0 255.255.255.0
access-group acl-outside in interface outside
route outside 0.0.0.0 0.0.0.0 217.34.133.29 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
```
This is the Cisco PIX 501 firmware used in this application note

```
pixfirewall# sh ver
Cisco PIX Firewall Version 6.3(3)
Cisco PIX Device Manager Version 1.1(2)

Compiled on Wed 13-Aug-03 13:55 by morlee

pixfirewall up 1 day 2 hours

Hardware: PIX-501, 16 MB RAM, CPU Am5x86 133 MHz
Flash E28F640J3 @ 0x3000000, 8MB
BIOS Flash E28F640J3 @ 0xffffd000, 128KB
0: ethernet0: address is 000a.417e.5a3a, irq 9
1: ethernet1: address is 000a.417e.5a3b, irq 10

Licensed Features:
Failover: Disabled
VPN-DES: Enabled
VPN-3DES-AES: Enabled
Maximum Physical Interfaces: 2
Maximum Interfaces: 2
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled
Inside Hosts: 10
Throughput: Unlimited
IKE peers: 10

This PIX has a Restricted (R) license.

Serial Number: 806272549 (0x300ebe25)
Running Activation Key: 0x27c5b4ee 0x3dcfa70f 0xe7b55669 0x9adf8976
```