Application Note 27

Configure an IPsec VPN between a Digi TransPort and Cisco PIX

November 2015

Contents

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.

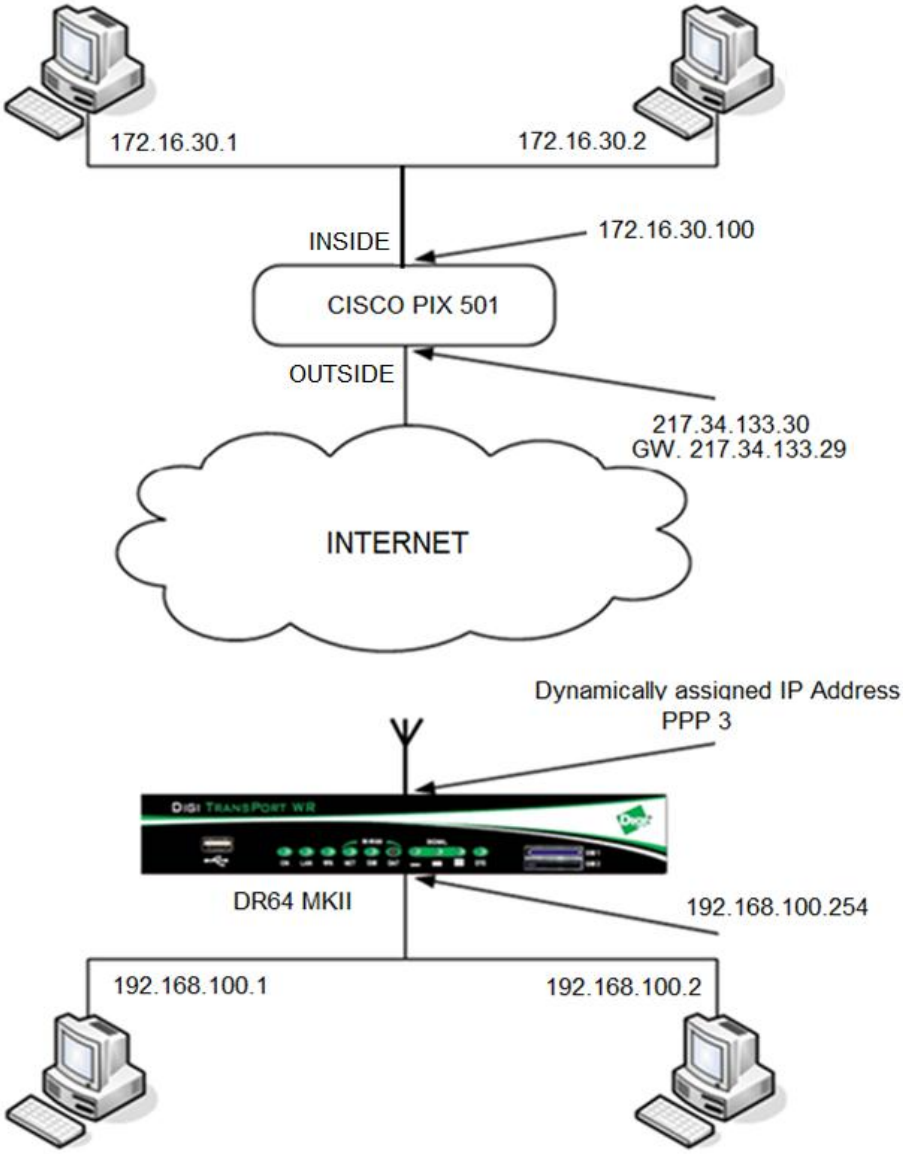


Figure 1-1: Overview Diagram

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

Version Number	Status
1.0	Published
2.0	Rebranded and updated to 5156 firmware

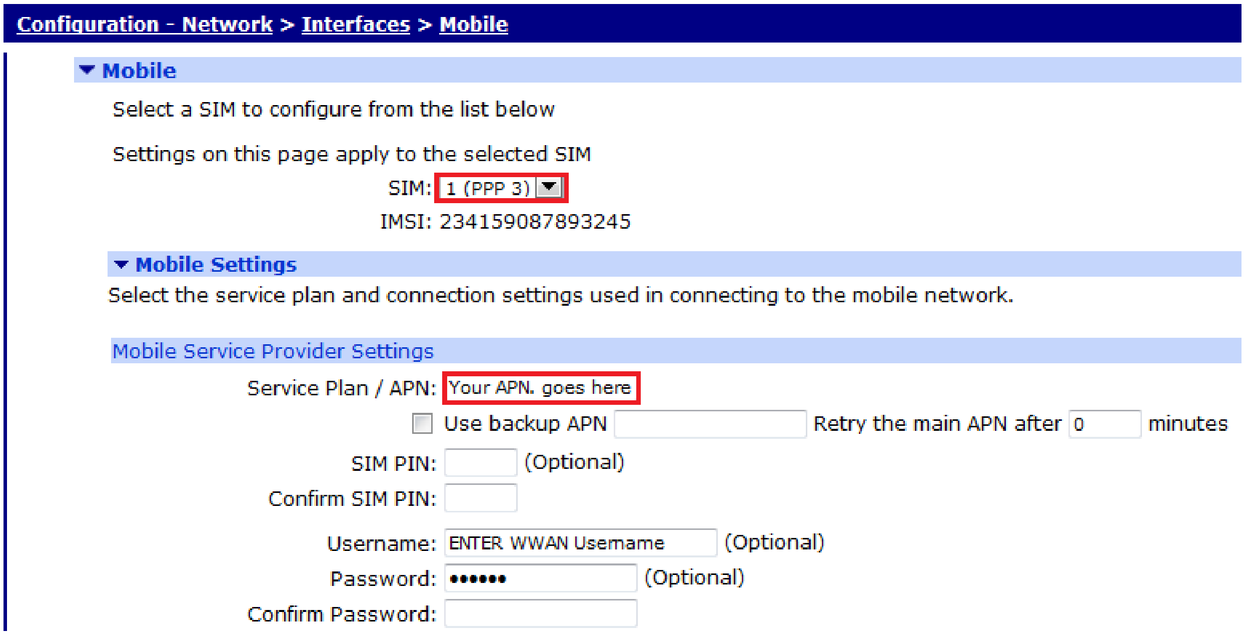
2 DIGI TRANSPORT CONFIGURATION

2.1 Configure the cellular module.

Browse to

Configuration - Network > Interfaces > Mobile

Parameter	Setting	Description
SIM	1	Select SIM 1 for the PPP 3 interface
Service Plan/APN	*APN*	The Access Point Name for the network



Configuration - Network > Interfaces > Mobile

▼ Mobile

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: 1 (PPP 3)

IMSI: 234159087893245

▼ Mobile Settings

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

Mobile Service Provider Settings

Service Plan / APN: Your APN. goes here

□ Use backup APN Retry the main APN after 0 minutes

SIM PIN: (Optional)

Confirm SIM PIN:

Username: ENTER WWAN Username (Optional)

Password: •••••• (Optional)

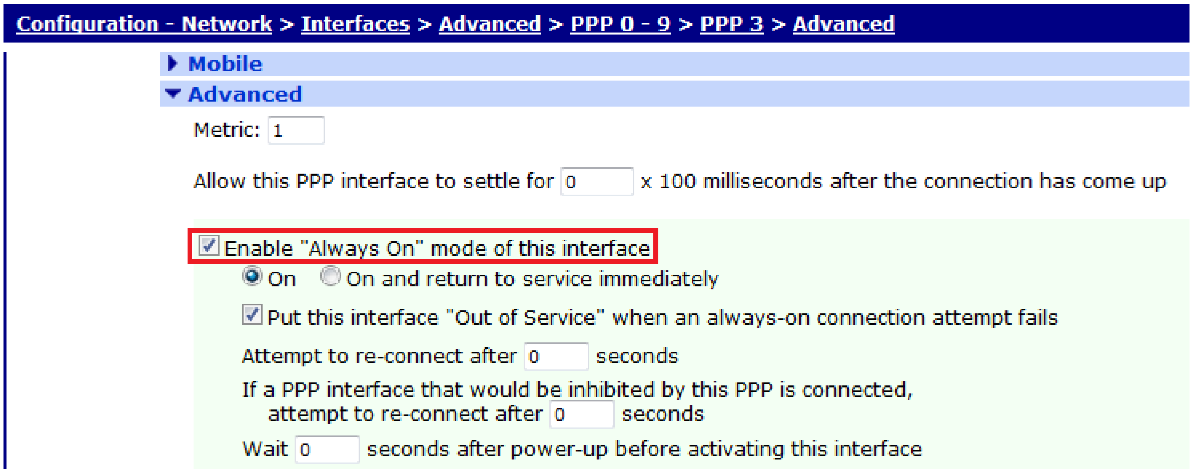
Confirm Password:

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

Parameter	Setting	Description
"Always On" mode	✓	Sets this interface as 'Always on' (This is the default setting for PPP 3)



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

Metric: 1

Allow this PPP interface to settle for 0 x 100 milliseconds after the connection has come up

☑ Enable "Always On" mode of this interface

● On ○ On and return to service immediately

☑ Put this interface "Out of Service" when an always-on connection attempt fails

Attempt to re-connect after 0 seconds

If a PPP interface that would be inhibited by this PPP is connected, attempt to re-connect after 0 seconds

Wait 0 seconds after power-up before activating this interface

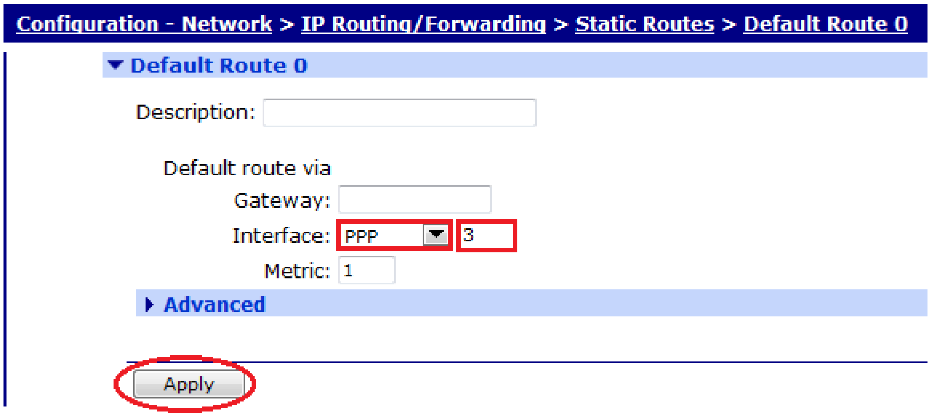
Click Apply

2.2 Configure the Default IP route

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

And make the following settings

Parameter	Setting	Description
Interface	PPP	Enter PPP as the default route interface type
Interface #	PPP 3	Enter 3 as the PPP interface number



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

Description:

Default route via

Gateway:

Interface: PPP 3

Metric: 1

Click Apply

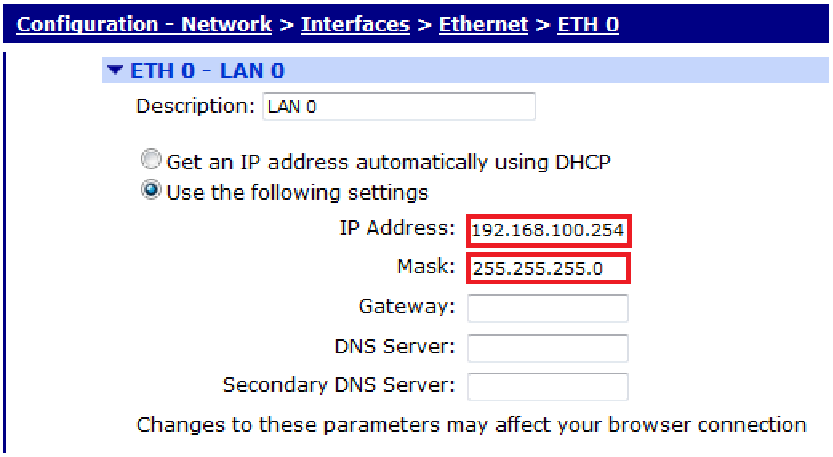
2.3 Configure the Private Network Interface (Ethernet 0)

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

Configuration - Network > Interfaces > Ethernet > ETH 0

And make the following settings

Parameter	Setting	Description
IP Address	192.168.100.254	Enter the TransPort's Ethernet IP address
Mask	255.255.255.0	Enter the TransPort's Ethernet subnet mask


Configuration - Network > Interfaces > Ethernet > ETH 0

ETH 0 - LAN 0

Description: LAN 0

○ Get an IP address automatically using DHCP
● Use the following settings

IP Address: 192.168.100.254
Mask: 255.255.255.0
Gateway:
DNS Server:
Secondary DNS Server:

Changes to these parameters may affect your browser connection

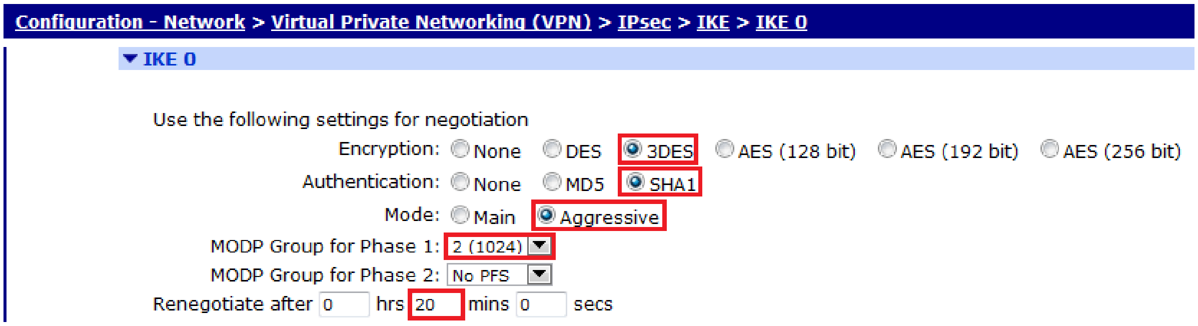
Click Apply

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

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



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

▼ IKE 0

Use the following settings for negotiation

Encryption: ○ None ○ DES ● 3DES ○ AES (128 bit) ○ AES (192 bit) ○ AES (256 bit)

Authentication: ○ None ○ MD5 ● SHA1

Mode: ○ Main ● Aggressive

MODP Group for Phase 1: 2 (1024)

MODP Group for Phase 2: No PFS

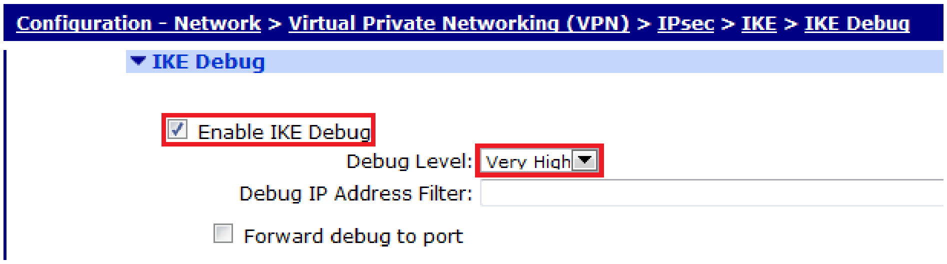
Renegotiate after 0 hrs 20 mins 0 secs

Click Apply

2.5 Turn on IKE debug

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

Parameter	Setting	Description
Enable IKE Debug	✓	Enables IKE debugging to be displayed on the debug port
Debug Level	Very High	Full IKE debug will be recorded



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

▼ IKE Debug

☑ Enable IKE Debug

Debug Level: Very High

Debug IP Address Filter:

□ Forward debug to port

Click Apply

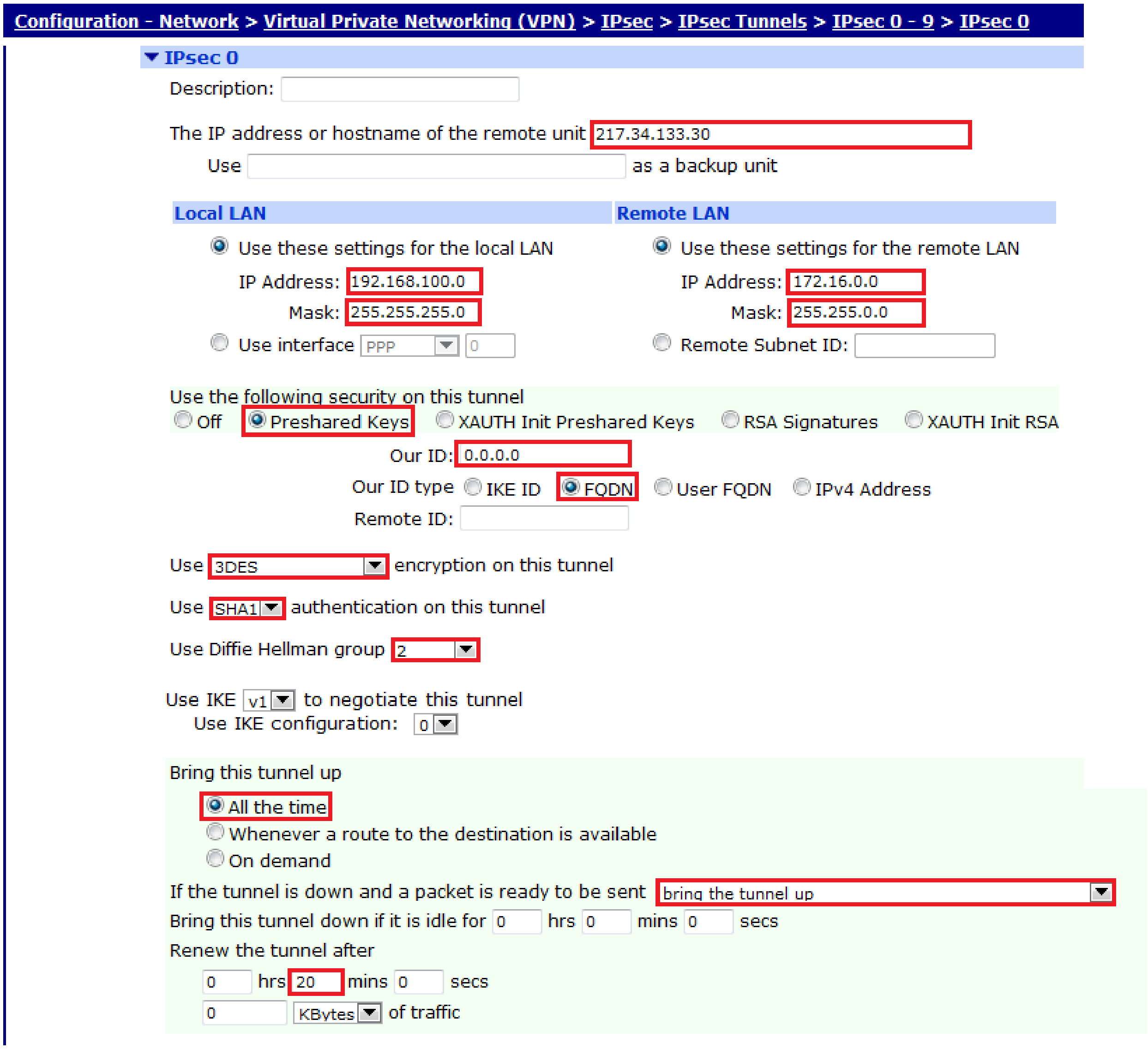
2.6 Configure the IPSEC Eroute

Browse to:

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

And make the following settings

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



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

▼ IPsec 0

Description:

The IP address or hostname of the remote unit 217.34.133.30

Use as a backup unit

Local LAN

● Use these settings for the local LAN

IP Address: 192.168.100.0

Mask: 255.255.255.0

○ Use interface PPP 0

Remote LAN

● Use these settings for the remote LAN

IP Address: 172.16.0.0

Mask: 255.255.0.0

○ Remote Subnet ID:

Use the following security on this tunnel

○ Off ● Preshared Keys ○ XAUTH Init Preshared Keys ○ RSA Signatures ○ XAUTH Init RSA

Our ID: 0.0.0.0

Our ID type ○ IKE ID ● FQDN ○ User FQDN ○ IPv4 Address

Remote ID:

Use 3DES encryption on this tunnel

Use SHA1 authentication on this tunnel

Use Diffie Hellman group 2

Use IKE v1 to negotiate this tunnel

Use IKE configuration: 0

Bring this tunnel up

● All the time

○ Whenever a route to the destination is available

○ On demand

If the tunnel is down and a packet is ready to be sent bring the tunnel up

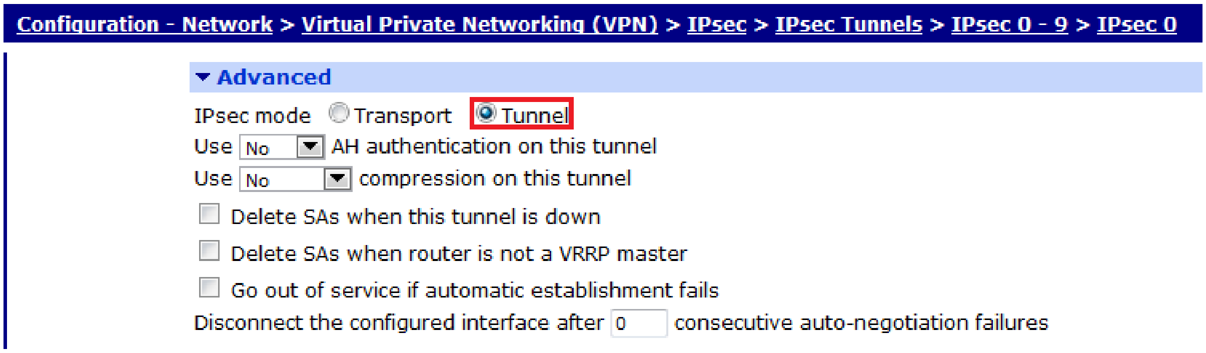
Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs

Renew the tunnel after

0 hrs 20 mins 0 secs

0 KBytes of traffic

And under “Advanced” make sure that IPsec mode is set to “Tunnel”



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

▼ Advanced

IPsec mode ○ Transport ● Tunnel

Use No AH authentication on this tunnel

Use No compression on this tunnel

☐ Delete SAs when this tunnel is down

☐ Delete SAs when router is not a VRRP master

☐ Go out of service if automatic establishment fails

Disconnect the configured interface after 0 consecutive auto-negotiation failures

Click Apply

2.7 Configure the pre-shared key

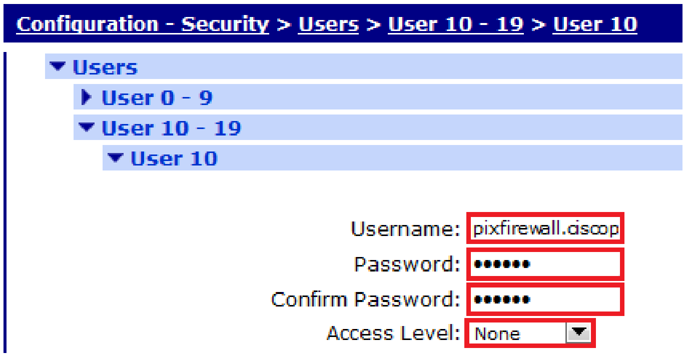
Browse to:

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

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

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.


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

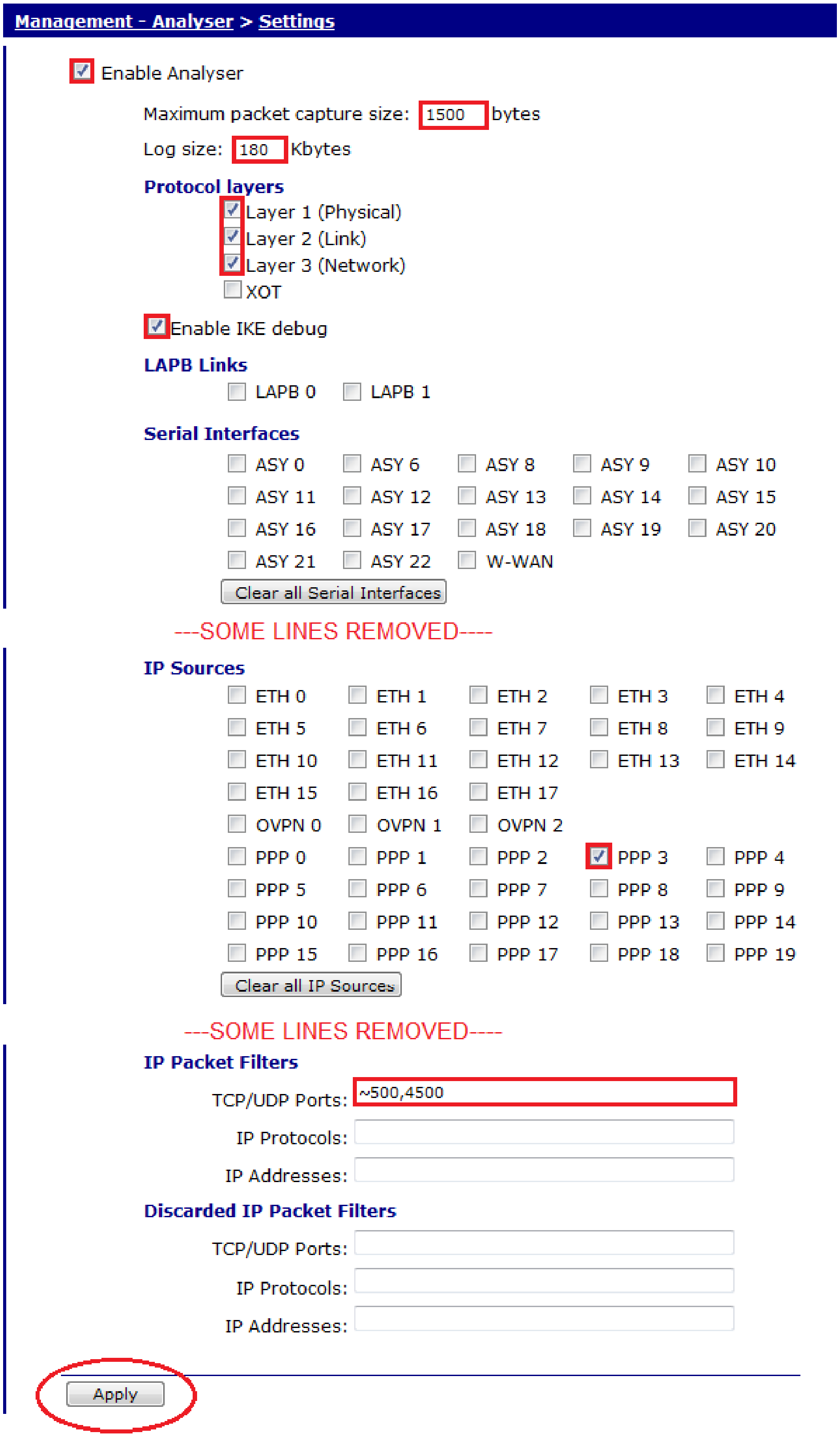
Username: pixfirewall.ciscop
Password: ••••••
Confirm Password: ••••••
Access Level: None

Click Apply

2.8 Set up the analyser trace

Configure the Analyser to assist with any troubleshooting that may be required.
Management - Analyser > Settings

Parameter	Setting	Description
Enable Analyser	✓	Enables analysis
Maximum packet capture size	1500	Captures the full packet
Log size	180	180 is the maximum log size in Kb
Protocol Layers	1,2 and 3	Enable debug on these layers
Enable IKE Debug	✓	IKE debugging information is recorded
IP Sources	PPP 3	PPP 3 IP data is recorded
IP Packet Filters: TCP/UDP Ports	~500, 4500	IKE & NAT-T traffic is recorded



Management - Analyser > Settings

☑ Enable Analyser

Maximum packet capture size: 1500 bytes

Log size: 180 Kbytes

Protocol layers

☑ Layer 1 (Physical)
☑ Layer 2 (Link)
☑ Layer 3 (Network)
☐ XOT

☑ Enable IKE debug

LAPB Links

☐ LAPB 0 ☐ LAPB 1

Serial Interfaces

☐ ASY 0 ☐ ASY 6 ☐ ASY 8 ☐ ASY 9 ☐ ASY 10
☐ ASY 11 ☐ ASY 12 ☐ ASY 13 ☐ ASY 14 ☐ ASY 15
☐ ASY 16 ☐ ASY 17 ☐ ASY 18 ☐ ASY 19 ☐ ASY 20
☐ ASY 21 ☐ ASY 22 ☐ W-WAN

---SOME LINES REMOVED----

IP Sources

☐ ETH 0 ☐ ETH 1 ☐ ETH 2 ☐ ETH 3 ☐ ETH 4
☐ ETH 5 ☐ ETH 6 ☐ ETH 7 ☐ ETH 8 ☐ ETH 9
☐ ETH 10 ☐ ETH 11 ☐ ETH 12 ☐ ETH 13 ☐ ETH 14
☐ ETH 15 ☐ ETH 16 ☐ ETH 17
☐ OVPN 0 ☐ OVPN 1 ☐ OVPN 2
☐ PPP 0 ☐ PPP 1 ☐ PPP 2 ☑ PPP 3 ☐ PPP 4
☐ PPP 5 ☐ PPP 6 ☐ PPP 7 ☐ PPP 8 ☐ PPP 9
☐ PPP 10 ☐ PPP 11 ☐ PPP 12 ☐ PPP 13 ☐ PPP 14
☐ PPP 15 ☐ PPP 16 ☐ PPP 17 ☐ PPP 18 ☐ PPP 19

---SOME LINES REMOVED----

IP Packet Filters

TCP/UDP Ports: ~500,4500

IP Protocols:

IP Addresses:

Discarded IP Packet Filters

TCP/UDP Ports:

IP Protocols:

IP Addresses:

Click Apply

3 CISCO PIX CONFIGURATION

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.

```
route 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.

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

```
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.

```
domain-name domain name
```

```
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.

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

```
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

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

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

3.14 Specify an ESP authentication algorithm for the IKE negotiations

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

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

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

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

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

3.16 Specify a key lifetime before the key is renewed

```
isakmp policy priority lifetime lifetime
```

```
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
```

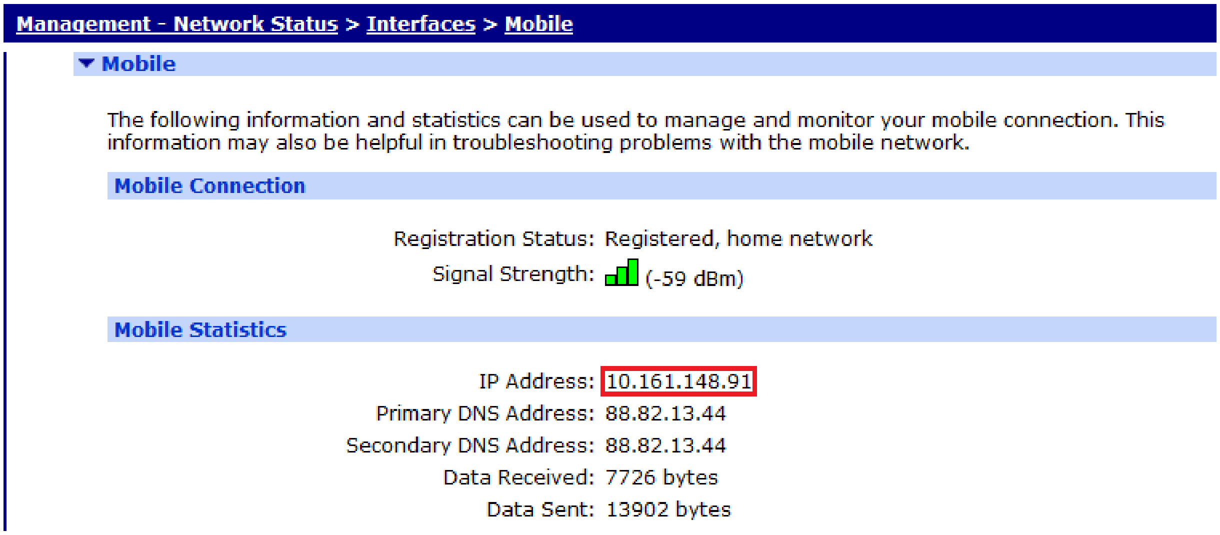
3.19 Save the configuration

```
pixfirewall(config)#write mem
```

4 TESTING

4.1 Confirm that the W-WAN interface (PPP 3) is up

Management - Network Status > Interfaces > Mobile



Management - Network Status > Interfaces > Mobile

▼ Mobile

The following information and statistics can be used to manage and monitor your mobile connection. This information may also be helpful in troubleshooting problems with the mobile network.

Mobile Connection

Registration Status: Registered, home network

Signal Strength: (-59 dBm)

Mobile Statistics

IP Address: 10.161.148.91

Primary DNS Address: 88.82.13.44

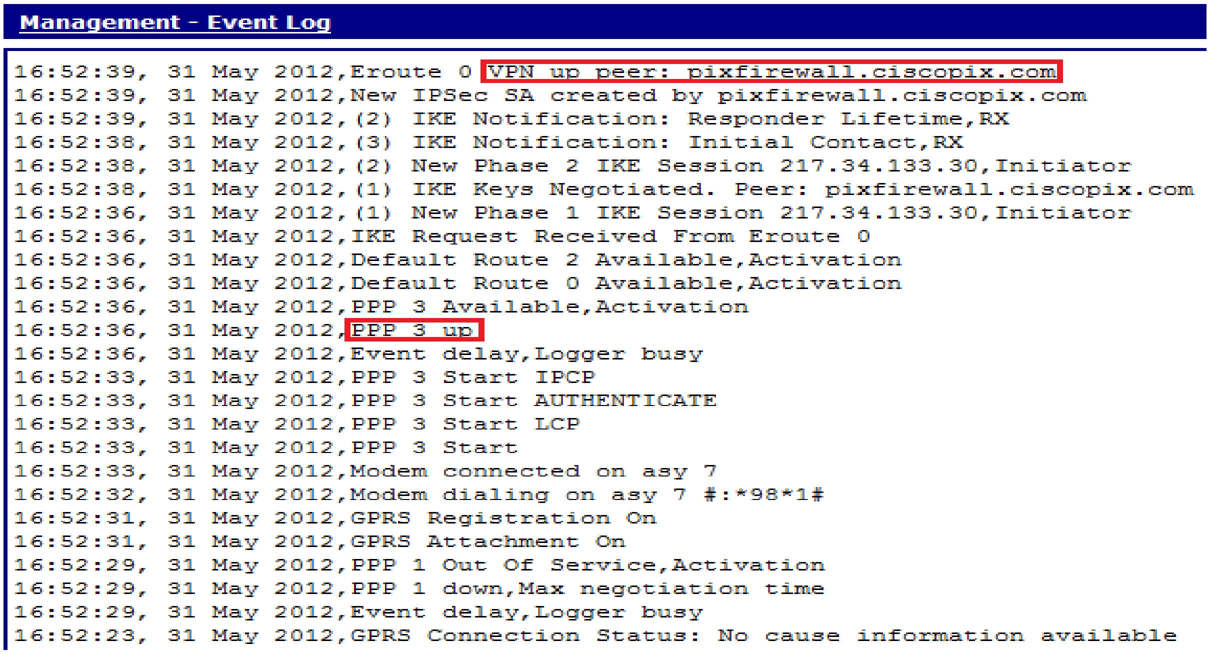
Secondary DNS Address: 88.82.13.44

Data Received: 7726 bytes

Data Sent: 13902 bytes

4.2 Check the Eventlog

Management - Event Log



Management - Event Log

```
16:52:39, 31 May 2012,Eroute 0 VPN up peer: pixfirewall.ciscopix.com
16:52:39, 31 May 2012,New IPSec SA created by pixfirewall.ciscopix.com
16:52:39, 31 May 2012,(2) IKE Notification: Responder Lifetime,RX
16:52:38, 31 May 2012,(3) IKE Notification: Initial Contact,RX
16:52:38, 31 May 2012,(2) New Phase 2 IKE Session 217.34.133.30,Initiator
16:52:38, 31 May 2012,(1) IKE Keys Negotiated. Peer: pixfirewall.ciscopix.com
16:52:36, 31 May 2012,(1) New Phase 1 IKE Session 217.34.133.30,Initiator
16:52:36, 31 May 2012,IKE Request Received From Eroute 0
16:52:36, 31 May 2012,Default Route 2 Available,Activation
16:52:36, 31 May 2012,Default Route 0 Available,Activation
16:52:36, 31 May 2012,PPP 3 Available,Activation
16:52:36, 31 May 2012,PPP 3 up
16:52:36, 31 May 2012,Event delay,Logger busy
16:52:33, 31 May 2012,PPP 3 Start IPCP
16:52:33, 31 May 2012,PPP 3 Start AUTHENTICATE
16:52:33, 31 May 2012,PPP 3 Start LCP
16:52:33, 31 May 2012,PPP 3 Start
16:52:33, 31 May 2012,Modem connected on asy 7
16:52:32, 31 May 2012,Modem dialing on asy 7 #:*98*1#
16:52:31, 31 May 2012,GPRS Registration On
16:52:31, 31 May 2012,GPRS Attachment On
16:52:29, 31 May 2012,PPP 1 Out Of Service,Activation
16:52:29, 31 May 2012,PPP 1 down,Max negotiation time
16:52:29, 31 May 2012,Event delay,Logger busy
16:52:23, 31 May 2012,GPRS Connection Status: No cause information available
```

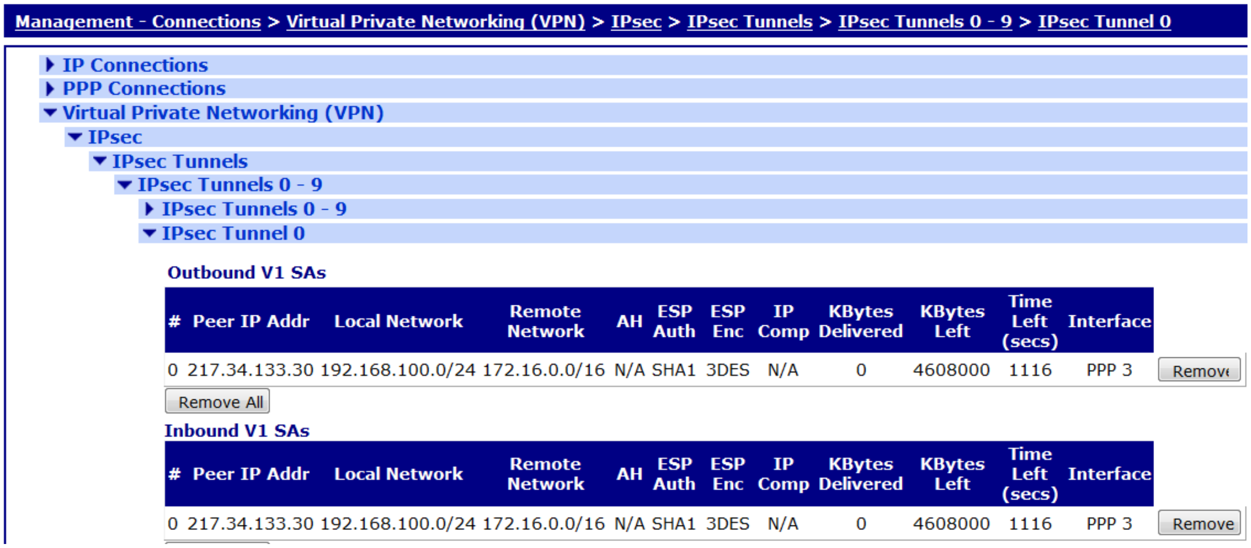
The eventlog shows the events occurring within the operating system. Here you can see the W-WAN interface (PPP 3) comes up and the VPN is established.

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


Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec Tunnels 0 - 9 > IPsec Tunnel 0
IP Connections
PPP Connections
Virtual Private Networking (VPN)
IPsec
IPsec Tunnels
IPsec Tunnels 0 - 9
IPsec Tunnels 0 - 9
IPsec Tunnel 0
Remove All

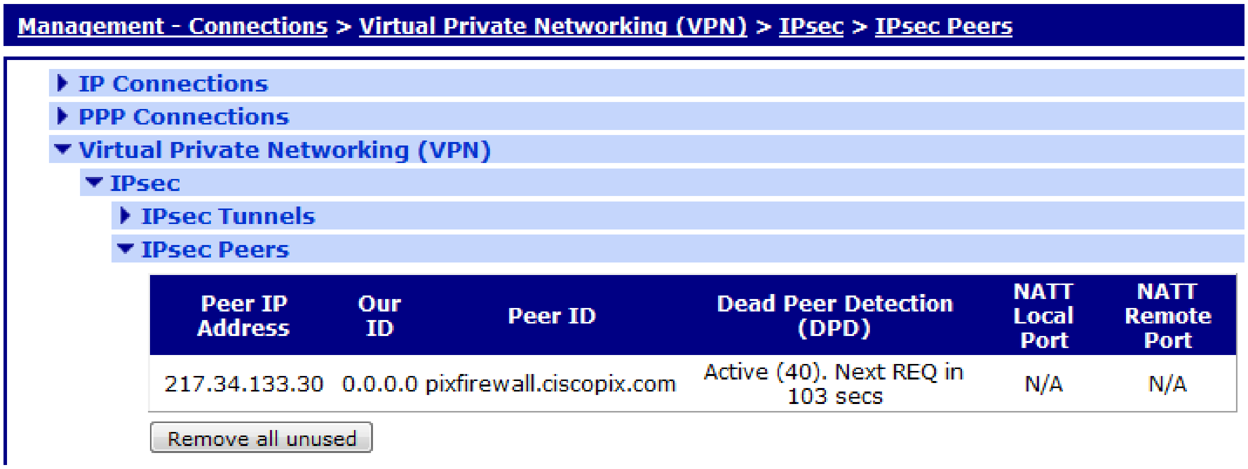
Outbound V1 SAs

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	
0	217.34.133.30	192.168.100.0/24	172.16.0.0/16	N/A	SHA1	3DES	N/A	0	4608000	1116	PPP 3	Remove

Inbound V1 SAs

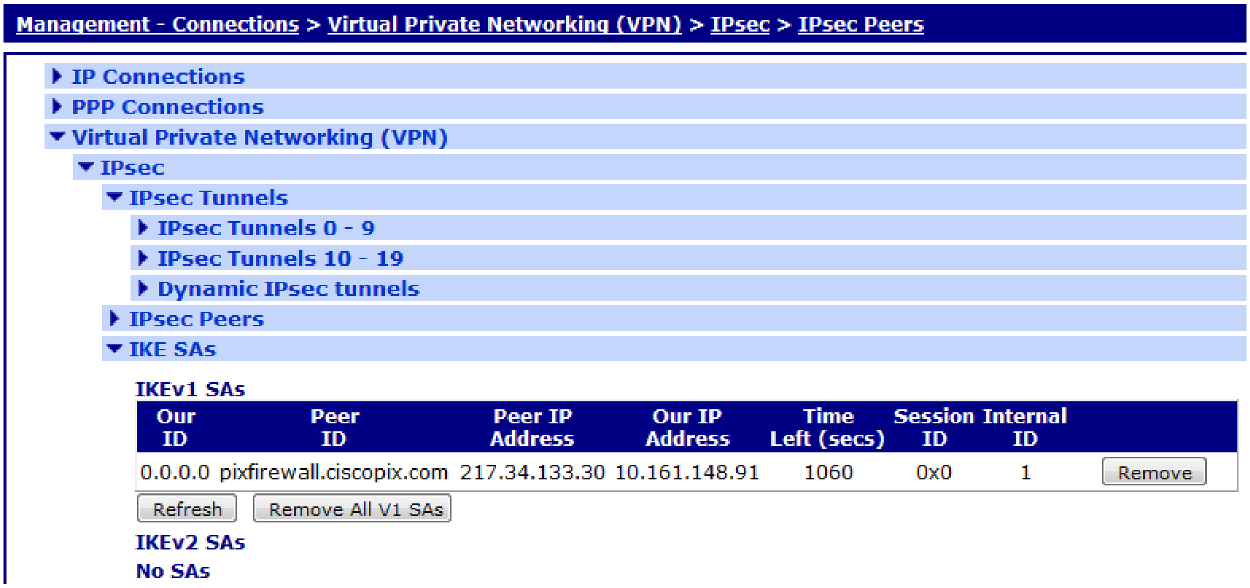
#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	
0	217.34.133.30	192.168.100.0/24	172.16.0.0/16	N/A	SHA1	3DES	N/A	0	4608000	1116	PPP 3	Remove

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


Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Peers
IP Connections
PPP Connections
Virtual Private Networking (VPN)
IPsec
IPsec Tunnels
IPsec Peers
Remove all unused

Peer IP Address	Our ID	Peer ID	Dead Peer Detection (DPD)	NATT Local Port	NATT Remote Port
217.34.133.30	0.0.0.0	pixfirewall.ciscopix.com	Active (40). Next REQ in 103 secs	N/A	N/A

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



IKEv1 SAs

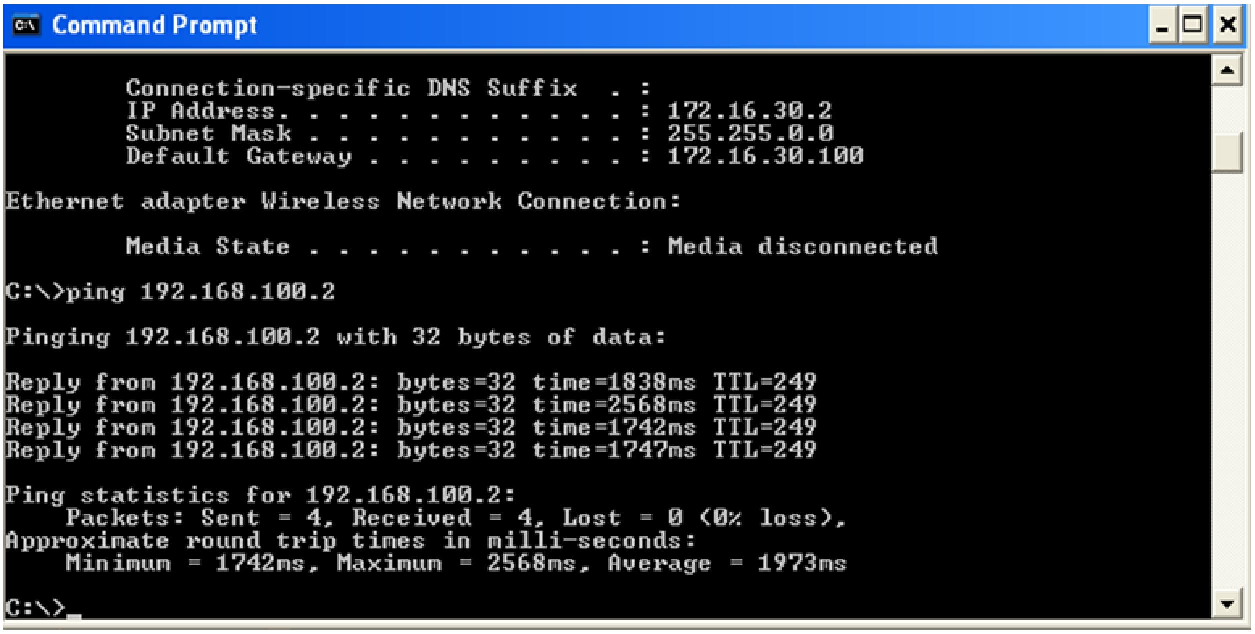
Our ID	Peer ID	Peer IP Address	Our IP Address	Time Left (secs)	Session ID	Internal ID	
0.0.0.0	pixfirewall.ciscopix.com	217.34.133.30	10.161.148.91	1060	0x0	1	Remove

IKEv2 SAs

No SAs

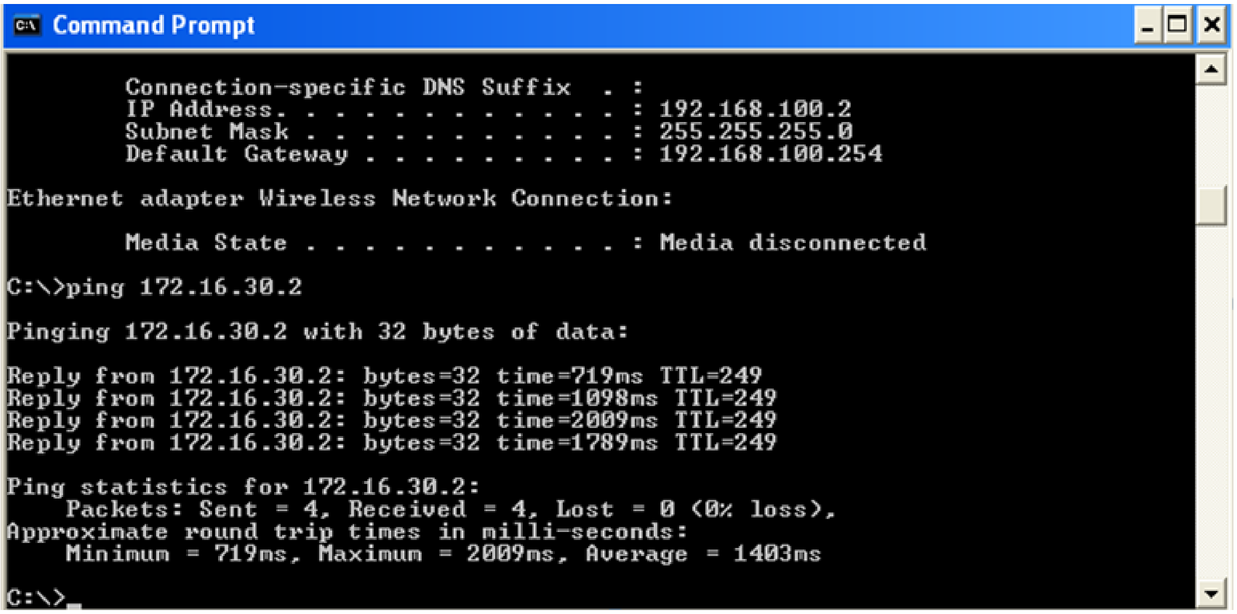
4.3 Ping test

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



```
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.16.30.2
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.30.100

Ethernet adapter Wireless Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:

Reply from 192.168.100.2: bytes=32 time=1838ms TTL=249
Reply from 192.168.100.2: bytes=32 time=2568ms TTL=249
Reply from 192.168.100.2: bytes=32 time=1742ms TTL=249
Reply from 192.168.100.2: bytes=32 time=1747ms TTL=249

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1742ms, Maximum = 2568ms, Average = 1973ms

C:\>_
```

From the Cisco PIX LAN a successful ping from 172.16.30.2 across the tunnel



```
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.100.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.100.254

Ethernet adapter Wireless Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\>ping 172.16.30.2

Pinging 172.16.30.2 with 32 bytes of data:

Reply from 172.16.30.2: bytes=32 time=719ms TTL=249
Reply from 172.16.30.2: bytes=32 time=1098ms TTL=249
Reply from 172.16.30.2: bytes=32 time=2009ms TTL=249
Reply from 172.16.30.2: bytes=32 time=1789ms TTL=249

Ping statistics for 172.16.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 719ms, Maximum = 2009ms, Average = 1403ms

C:\>_
```

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
        dst               src        state     pending     created
   217.34.133.30   212.183.128.77    QM_IDLE         0           1
```

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 ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 3, crypto map: vpn-map
        sa timing: remaining key lifetime (k/sec): (4607999/945)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:


     outbound pcp sas:
```

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"
eth 0 IPaddr "192.168.100.254"
eth 0 bridge ON
eth 1 descr "LAN 1"
eth 2 descr "LAN 2"
eth 3 descr "LAN 3"
eth 4 descr "ATM PVC 0"
eth 4 do_nat 2
eth 5 descr "ATM PVC 1"
eth 5 do_nat 2
eth 6 descr "ATM PVC 2"
eth 6 do_nat 2
eth 7 descr "ATM PVC 3"
eth 7 do_nat 2
eth 8 descr "ATM PVC 4"
eth 8 do_nat 2
eth 9 descr "ATM PVC 5"
eth 9 do_nat 2
eth 10 descr "ATM PVC 6"
eth 10 do_nat 2
eth 11 descr "ATM PVC 7"
eth 11 do_nat 2
eth 12 descr "Logical"
eth 13 descr "Logical"
eth 14 descr "Logical"
eth 15 descr "Logical"
eth 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
ppp 1 name "ADSL"
ppp 1 l1iface "AAL"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 immoos ON
ppp 1 echo 10
ppp 1 echodropcnt 5
ppp 3 name "W-WAN (HSPA 3G)"
ppp 3 phonenum "*98*1#"
ppp 3 username "ENTER WWAN Username"
ppp 3 epassword "KD5lSVJDVVg="
ppp 3 r_addr OFF
ppp 3 IPaddr "0.0.0.0"
ppp 3 l_addr ON
ppp 3 timeout 0
ppp 3 ipsec 1
ppp 3 use_modem 1
ppp 3 aodion 1
ppp 3 autoassert 1
ppp 3 immoos ON
ppp 3 l_pap OFF
ppp 3 l_chap OFF
ppp 3 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
ike 0 encalg "3DES"
ike 0 authalg "SHA1"
ike 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 l1on ON
ana 0 lapdon 0
ana 0 asyon 1
ana 0 logsize 45
cmd 0 unitid "ss%s>"
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 "KD5lSVJDVVg="
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

```
ati5
Digi TransPort DR64-HXA1-WE2-XX(MkII) Ser#:155285 HW Revision: 7503a
Software Build Ver5156.  May 17 2012 21:06:15  9W
ARM Bios Ver 6.67 v35 197MHz B128-M128-F300-O100000,0 MAC:00042d025e95
Power Up Profile: 0
Async Driver              Revision: 1.19  Int clk
Wi-Fi                     Revision: 2.0
Ethernet Port Isolate Driver Revision: 1.11
Firewall                  Revision: 1.0
EventEdit                 Revision: 1.0
Timer Module              Revision: 1.1
AAL                       Revision: 1.0
ADSL                      Revision: 1.0
(B)USBHOST                Revision: 1.0
L2TP                      Revision: 1.10
PPTP                      Revision: 1.00
TACPLUS                   Revision: 1.00
MySQL                     Revision: 0.01
LAPB                      Revision: 1.12
X25 Layer                 Revision: 1.19
MACRO                     Revision: 1.0
PAD                       Revision: 1.4
X25 Switch                Revision: 1.7
V120                      Revision: 1.16
TPAD Interface            Revision: 1.12
SCRIBATSK                 Revision: 1.0
BASTSK                    Revision: 1.0
ARM Sync Driver           Revision: 1.18
TCP (HASH mode)           Revision: 1.14
TCP Utils                 Revision: 1.13
PPP                       Revision: 1.19
WEB                       Revision: 1.5
SMTP                      Revision: 1.1
FTP Client                Revision: 1.5
FTP                       Revision: 1.4
IKE                       Revision: 1.0
PollANS                   Revision: 1.2
PPPOE                     Revision: 1.0
BRIDGE                    Revision: 1.1
MODEM CC (Option 3G)      Revision: 1.4
FLASH Write               Revision: 1.2
Command Interpreter       Revision: 1.38
SSLCLI                    Revision: 1.0
OSPF                      Revision: 1.0
BGP                       Revision: 1.0
QOS                       Revision: 1.0
RADIUS Client             Revision: 1.0
SSH Server                Revision: 1.0
SCP                       Revision: 1.0
CERT                      Revision: 1.0
LowPrio                   Revision: 1.0
Tunnel                    Revision: 1.2
OVPN                      Revision: 1.2
TEMPLOG                   Revision: 1.0
iDigi                     Revision: 2.0
```

```
OK
```

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 skinny 2000
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
```

```
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-3des esp-sha-hmac
crypto dynamic-map cisco 1 set transform-set myset
crypto map vpn-map 10 ipsec-isakmp dynamic cisco
crypto map vpn-map interface outside
isakmp enable outside
isakmp key ******** address 0.0.0.0 netmask 0.0.0.0
isakmp nat-traversal 20
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d0d6cbc6090b71580fda766ec2158b15
: end
```

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 @ 0xfffd8000, 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
```

```
Configuration last modified by enable_15 at 03:12:12.657 UTC Fri Jan 1 1993
```