



Application Note 58

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

10 November 2020

Contents

1	Introduction	4
1.1	Outline	4
1.2	Assumptions	4
1.3	Corrections	4
1.4	Version	4
2	Scenario.....	5
3	Digi TransPort router configuration - Initiator.....	6
3.1	LAN Settings	6
3.2	WAN Settings	7
3.3	Default Route.....	9
3.4	IKEv2 Configuration	10
3.5	IPsec Tunnel configuration	11
3.6	Preshared Key configuration	13
4	Cisco router configuration - Responder	15
4.1	LAN Settings	15
4.2	WAN Settings	15
4.3	Default Route.....	15
4.4	IKEv2 Configuration and Preshared Key	16
4.5	IPsec Tunnel configuration	18
4.6	Access List configuration	18
4.7	Crypto Map configuration	18
5	Testing.....	20
5.1	Debug settings on TransPort	20
5.2	Debug settings on Cisco.....	24
5.3	Setting the tunnel UP.....	24
5.4	IPsev SAs status.....	25
5.5	Testing traffic on the tunnel	26

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

6	Configuration file.....	30
6.1	Initiator (TransPort) Configuration File.....	30
6.2	Responder (Cisco) Configuration File.....	33

Figures

Figure 3.1-1: Initiator LAN settings	6
Figure 3.2-1: Initiator WAN settings	7
Figure 3.2-2: Enabling IPsec on WAN	8
Figure 3.3-1: Default route	9
Figure 3.4-1: Initiator IKEv2 settings.....	10
Figure 3.5-1: Initiator IPsec settings	11
Figure 3.6-1: Remote peer Preshared Key	13
Figure 3.6-2: Local peer Preshared Key	14
Figure 5.1-1: Analyser settings - 1	20
Figure 5.1-2:Analyser settings – 2	21
Figure 5.1-3: Enabling IKE debug.....	23

1 INTRODUCTION

1.1 Outline

Internet Protocol Security (IPsec) is a set of protocols providing cryptographic security services and allows creation of encrypted tunnel between two private networks (VPN). In order to set up and maintain the IPsec VPN, Internet Key Exchange Protocol (IKE) is used. In the last few years, a new version has been designed for IKE protocol (IKEv2), that has the basic outcome as IKEv1 but introduces many improvements as decreased latency (only 4 messages need to be exchanged for set up the VPN) and reliability (all messages are acknowledge and sequenced).

This Application Note gives a guide on configuring an IPsec VPN with IKEv2 between a TransPort router that acts as Initiator and a Cisco router acting as the responder.

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.

Preconditions: This guide assumes that two Digi TransPort are reachable to each other via an Ethernet connection passing through another router. Other kind of WAN technology can be used.

Models shown: Digi TransPort WR44

Other Compatible Models: All other Digi TransPort WR products with IPsec enabled.

Firmware versions: All Versions

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.

1.3 Corrections

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

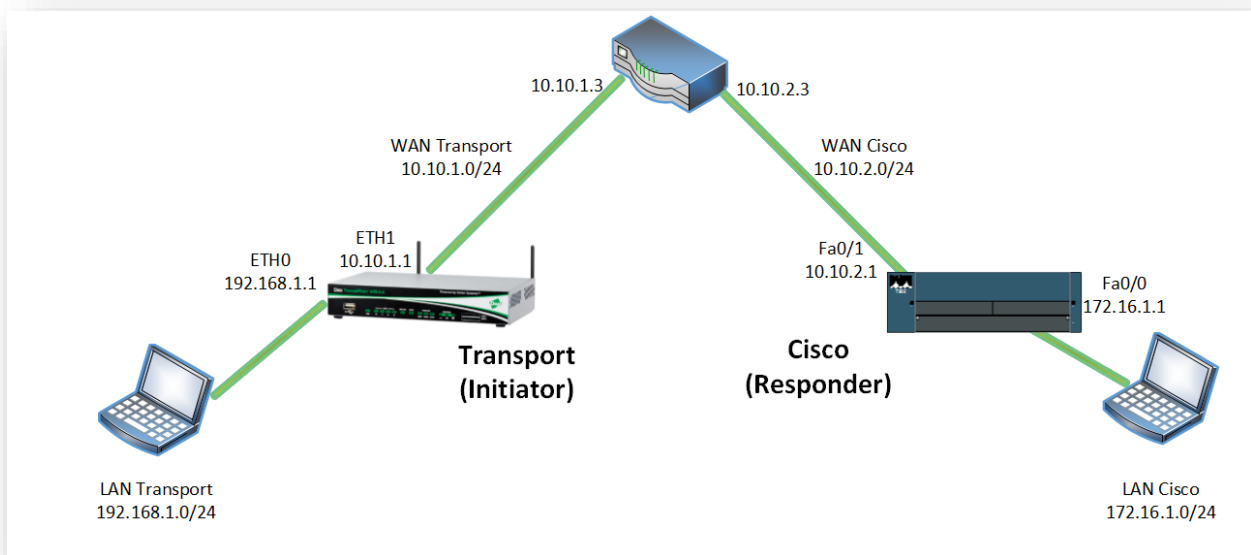
Requests for new application notes can be sent to the same address.

1.4 Version

Version Number	Status
0.1	Draft
1.0	Published, typos and link fixes.

2 SCENARIO

This application note will consider the following scenario:



The TransPort device acts as Initiator and the Cisco as responder. An IPsec tunnel will be set up between the peers using IKEv2 negotiation. The tunnel will protect the LAN to LAN traffic between them (192.168.1.0/24 <-> 172.16.1.0/24).

3 DIGI TRANSPORT ROUTER CONFIGURATION - INITIATOR

In order to configure the Digi TransPort, connect a PC to the ETH0 of the TransPort and log into the Web User Interface (WebUI) with a browser at the default address 192.168.1.1. Then follow the sections below.

3.1 LAN Settings

In this AN the LAN interface of the Transport that acts as Initiator is configured on ETH 0 and left as default (192.168.1.1). The configuration can be checked going to the WEB UI at the section Configuration – Network > Interfaces > Ethernet > ETH 0:

Configuration - Network > Interfaces > Ethernet > ETH 0

Interfaces

Ethernet

ETH 0 - Transport LAN

Description: Transport LAN

☐ Get an IP address automatically using DHCP
☒ Use the following settings

IP Address: 192.168.1.1

Mask: 255.255.255.0

Gateway:

DNS Server:

Secondary DNS Server:

Changes to these parameters may affect your browser connection

Figure 3.1-1: Initiator LAN settings

Parameter	Setting	Description	CLI command
IP Address	192.168.1.1	Specifies the IP address of this Ethernet port	<i>eth 0 ipaddr 192.168.1.1</i>
Mask	255.255.255.0	Specifies the subnet mask of the IP subnet to which the unit is attached via this Ethernet port	<i>eth 0 mask 255.255.255.0</i>

3.2 WAN Settings

In this Application note, we will configure the ETH 1 as WAN connection as follows:

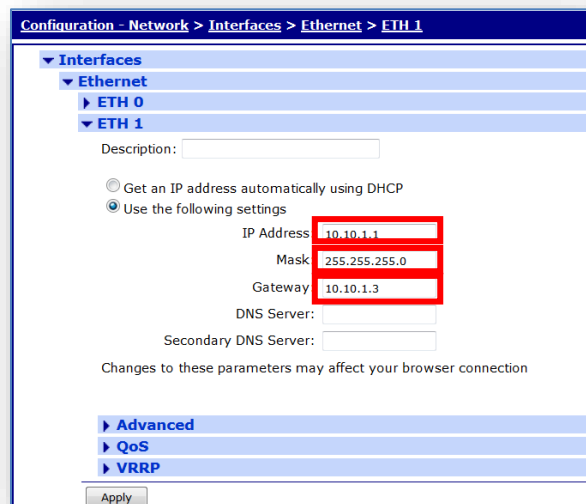


Figure 3.2-1: Initiator WAN settings

Then, IPsec must be enabled under the interface, going into the advance section:

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

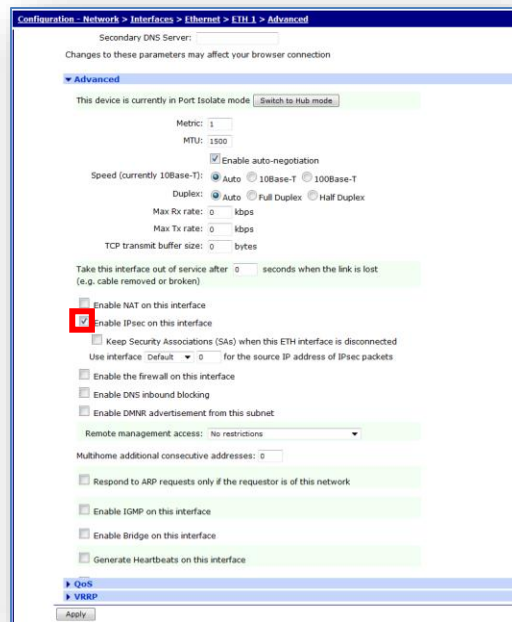


Figure 3.2-2: Enabling IPsec on WAN

Parameter	Setting	Description	CLI command
IP Address	10.10.1.1	Specifies the IP address of this Ethernet port	<i>eth 1 ipaddr 10.10.1.1</i>
Mask	255.255.255.0	Specifies the subnet mask of the IP subnet to which the unit is attached via this Ethernet port	<i>eth 0 mask 255.255.255.0</i>
Gateway	10.10.1.3	Specifies the IP address of a gateway to be used by the unit	<i>eth 1 gateway 10.10.1.3</i>
Enable IPsec on this interface	Enabled	Enable IPsec security features for this interface	<i>eth 1 ipsec 1</i>

3.3 Default Route

In the scenario considered in this AN, the default gateway for the TransPort that acts as Initiator is 10.10.1.3, so a default route need to be configured going in **Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0:**

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

- Interfaces
- DHCP Server
- Network Services
- DNS Servers
- Dynamic DNS
- IP Routing/Forwarding
 - IP Routing
 - Static Routes
 - Routes 0 - 9
 - Routes 10 - 19
 - Routes 20 - 29
 - Routes 30 - 39
 - Routes 40 - 49
 - Default Route 0

Description:

Default route via

Gateway:

Interface:

Use PPP sub-configuration:

Metric:

Advanced

Apply

Figure 3.3-1: Default route

Parameter	Setting	Description	CLI command
Gateway	10.10.1.3	Set the IP address of the default gateway	<i>def_route 0 gateway 10.10.1.3</i>
Interface	Ethernet 1	Set the interface used to default route the packets, is selected from the drop-down list and the interface instance number is entered into the adjacent text box	<i>def_route 0 ll_ent "eth"</i> <i>def_route 0 ll_add 1</i>

3.4 IKEv2 Configuration

In order to configure the IKEv2 part for the initiator, go to the section **Configuration – Network > VPN > IPsec > IKE > IKEv2 > IKEv2 0** and set the parameters as indicated below:

Virtual Private Networking (VPN)

- IPsec
 - IPsec Tunnels
 - IPsec Default Action
 - IPsec Groups
 - Dead Peer Detection (DPD)
 - IKE
 - IKEv2
 - IKEv2 0

Use the following settings for negotiation

Encryption: ☐ None ☐ DES ☐ 3DES ☒ AES (128 bit) ☐ AES (192 bit) ☐ AES (256 bit)

Authentication: ☐ None ☐ MD5 ☒ SHA1

PRF Algorithm: ☐ None ☐ MD5 ☒ SHA1

MODP Group for Phase 1:

Renegotiate after 8 hrs 0 mins 0 secs

Rekey after 0 hrs 0 mins 0 secs

[Advanced](#)

Figure 3.4-1: Initiator IKEv2 settings

Parameter	Setting	Description	CLI command
Encryption	AES (128 bit)	Defines the encryption algorithm used	<i>ike2 0 iencalg "AES"</i> <i>ike2 0 ienckeybits 128</i>
Authentication	SHA1	Defines the authentication algorithm used.	<i>ike2 0 iauthalg sha1</i>
PRF Algorithm	SHA1	Defines the PRF (Pseudo Random Function) algorithm used	<i>ike2 0 iprfalg sha1</i>
MODP Group for Phase 1	2 (1024)	Sets the key length used in the IKE Diffie-Hellman exchange	<i>ike2 0 idhgroup 2</i>

Table 3.4-1: Initiator IKEv2 settings

Click **apply** to confirm the changes.

3.5 IPsec Tunnel configuration

The following section describes how to configure the Digi TransPort's IPsec Tunnel settings on the initiator.

Browse to **Configuration – Network > VPN > IPsec > IPsec Tunnels > IPsec 0** and refer to the following picture and table for the settings of parameters:

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

IPsec

IPsec Tunnels

IPsec 0 - VPN to Cisco

Description: VPN to Cisco

The IP address or hostname of the remote unit

 Use as a backup unit

Local LAN	Remote LAN
<input checked="" type="radio"/> Use these settings for the local LAN IP Address <input type="text" value="192.168.1.0"/> Mask <input type="text" value="255.255.255.0"/> <input type="radio"/> Use interface <input type="text" value="PPP"/> <input type="text" value="0"/>	<input checked="" type="radio"/> Use these settings for the remote LAN IP Address <input type="text" value="172.16.1.0"/> Mask <input type="text" value="255.255.255.0"/> <input type="radio"/> Remote Subnet ID: <input type="text"/>

Use the following security on this tunnel

☐ Off
 ☒ Preshared Keys
 ☐ XAUTH Init Preshared Keys
 ☐ RSA Signatures
 ☐ XAUTH Init RSA

Our ID

Our ID type ☒ IKE ID ☐ FQDN ☐ User FQDN ☐ IPv4 Address

Remote ID

Use encryption on this tunnel

Use authentication on this tunnel

Use Diffie Hellman group

Use ☒ IKE v2 to negotiate this tunnel

Use IKE configuration:

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 this tunnel down if it is idle for hrs mins secs

Renew the tunnel after

hrs mins secs
 KBytes of traffic

Tunnel Negotiation

Figure 3.5-1: Initiator IPsec settings

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

Parameter	Setting	Description	CLI command
The IP address or hostname of the remote unit	10.10.2.1	The IP address or hostname of the remote IPsec peer that a VPN will be initiated to.	<i>eroute 0 peerip "10.10.2.1"</i>
Local LAN > Use these settings for the Local LAN	IP address: 192.168.1.0 Mask: 255.255.255.0	The subnet LAN of the local peer	<i>eroute 0 locip "192.168.1.0"</i> <i>eroute 0 locmsk "255.255.255.0"</i>
Remote LAN > Use these settings for the Remote LAN	IP address: 172.16.1.0 Mask: 255.255.255.0	The subnet LAN of the other peer	<i>eroute 0 remip "172.16.1.0"</i> <i>eroute 0 remmsk "255.255.255.0"</i>
Use the following security on this tunnel	Preshared Keys (Selected)	Choose the security type for the connection. In this AN, Preshared Keys are used	<i>eroute 0 authmeth "PRESHARED"</i>
Our ID	transport	The ID that the initiator will use. This AN will use “transport” as the local ID.	<i>eroute 0 ourid "transport"</i>
Our ID type	IKE ID	Choose the type of ID used, IKE ID allows the use of descriptive text strings (friendly names)	<i>eroute 0 ouridtype 0</i>
Remote ID	cisco1	Set the ID that responder will use. In this AN we will use the id “transport2” as the Remote ID for this tunnel.	<i>eroute 0 peerid "cisco1"</i>
Use <> encryption on this tunnel	3DES	This is the encryption type to use for the tunnel. This AN uses 3DES	<i>eroute 0 ESPenc "3DES"</i>
Use <> authentication on this tunnel	SHA1	This is the authentication type to use for the tunnel. This AN uses SHA1.	<i>eroute 0 ESPauth "SHA1"</i>
Use Diffie Hellman group <>	2	This is the Diffie Hellman (DH) group to use. This AN uses group 2.	<i>eroute 0 dhgroup 2</i>
Use IKE <> to negotiate this tunnel	v2	Set The IKE version to use to negotiate this IPsec tunnel, for this AN select “v2”	<i>eroute 0 ikever 2</i>
Bring this tunnel up	All the time	This controls how the IPsec tunnel is brought up, for the initiator “All the time” option is chosen	<i>eroute 0 autosa 2</i>
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. For the initiator in this AN the “bring the tunnel up” option is chosen	<i>eroute 0 nosa "try"</i>

Table 3.5-1: Initiator IPsec settings

3.6 Preshared Key configuration

In IKEv2 for the configuration of Preshared Key, two users need to be configured, one for the local peer and one for the remote. The key for the two users can be different (but each has to match the one configured on the other peer for the same user).

Note that any user can be used as the user for the Preshared Key, but best practice recommends using a user in the upper range of users because these users have the (router management) Access Level already set to 'None'. If a lower User number is configured, the Access Level should be changed to be 'None'.

Browse to **Configuration – Security > Users > User 10-14 > User 10** & **> User 11** and refer to the following pictures and tables for the configuration of the users:

Remote peer:

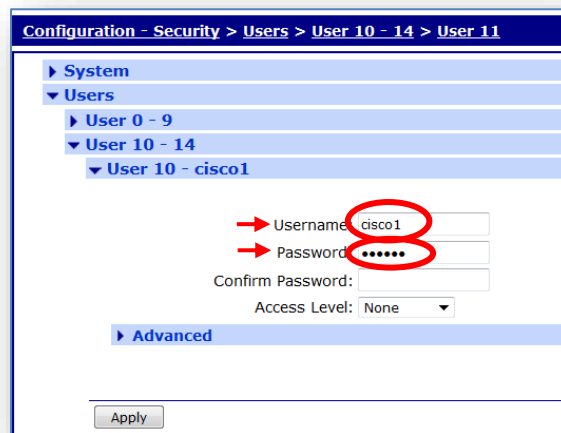
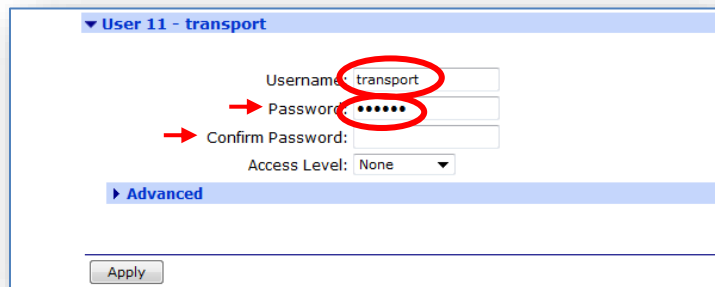


Figure 3.6-1: Remote peer Preshared Key

Parameter	Setting	Description	CLI command
Username	cisco1	This is the username for the remote peer and should match the Remote ID configured in the IPsec tunnel	<i>user 10 name "cisco1"</i>
Password/Confirm	****	Fill this field with the Preshared Key for the VPN tunnel.	<i>user 10 epassword ****</i>
Access Level	None	This is the access level for the user, in the case of preshared key user, it will not be granted any admin access	<i>user 10 access 4</i>

Table 3.6-1: Remote peer Preshared Key

Local peer:



▼ User 11 - transport

Username: transport

→ Password: *****

→ Confirm Password: *****

Access Level: None

► Advanced

Apply

Figure 3.6-2: Local peer Preshared Key

Parameter	Setting	Description	CLI command
Username	transport	This is the username for the local peer and should match the Our ID configured in the IPsec tunnel	user 11 name "transport"
Password/Confirm password	*****	Fill this field with the Preshared Key for the VPN tunnel.	user 11 epassword *****
Access Level	None	This is the access level for the user, in the case of preshared key user, it will not be granted any admin access	user 11 access 4

Table 3.6-2: Local peer Preshared Key

Click **Apply** and **Save** to save the settings.

4 CISCO ROUTER CONFIGURATION - RESPONDER

The first step is to obtain a command prompt at the Cisco router and establish that the IPsec option has been installed and if IKEv2 is supported. If IPsec option is not installed has not, you will not be able to enter the keyword “crypto” without getting an error. If IKEv2 is not supported by the firmware, you will not be able to enter the keywords “crypto ikev2” without getting an error.

Remember as well that you need to be in Enable mode and have entered configuration mode (e.g. by typing “configure terminal”) to enter configuration commands.

4.1 LAN Settings

For the LAN settings on the cisco, type the following commands:

```
interface FastEthernet0/0
ip address 172.16.1.1 255.255.255.0
speed auto
duplex auto
```

4.2 WAN Settings

For the WAN settings on the cisco, type the following commands:

```
interface FastEthernet0/1
ip address 10.10.2.1 255.255.255.0
speed auto
duplex auto
```

4.3 Default Route

In the scenario considered in this AN, the default gateway for the Cisco that acts as Responder is 10.10.2.3, so a default route needs to be configured typing the following command:

```
ip route 0.0.0.0 0.0.0.0 10.10.2.3
```

4.4 IKEv2 Configuration and Preshared Key

In order to configure the IKEv2 part for the responder, type the following commands (details are reported on each part)

Proposal:

```
crypto ikev2 proposal proposal1
encryption aes-cbc-128
integrity sha1
group 2
```

Command	Setting	Description
<i>crypto ikev2 proposal</i>	proposal1	Create the proposal and set a name for it
<i>encryption</i>	aes-cbc-128	Set the acceptable encryption algorithm
<i>integrity</i>	sha1	Set the acceptable authentication algorithm
<i>group</i>	2	Set the acceptable DH group

Policy:

```
crypto ikev2 policy policy1
proposal proposal1
```

Parameter	Setting	Description
<i>crypto ikev2 policy</i>	policy1	Create the policy and set a name for it
<i>proposal</i>	proposal1	Apply the proposal already created to the policy

Keyring:

```
crypto ikev2 keyring kyr1
peer transport
identity key-id transport
pre-shared-key digidigi
!
```

Parameter	Setting	Description
<i>crypto ikev2 keyring</i>	kyr1	Create a keyring and set a name for it
<i>peer</i>	transport	Create a peer under the keyring and set a name for it
<i>identity key-id</i>	transport	Set the ID for the remote peer (and the type)
<i>pre-shared-key</i>	digidigi	Set the preshared key for the remote peer

Profile:

```
crypto ikev2 profile prof
match identity remote key-id transport
identity local key-id cisco1
authentication remote pre-share
authentication local pre-share
keyring local kyr1
```

Parameter	Setting	Description
<i>crypto ikev2 profile</i>	prof	Create an IKEv2 profile and set a name for it
<i>match identity remote key-id</i>	transport	match this profile with the remote peer ID and ID type
<i>identity local key-id</i>	cisco1	define local ID and ID type
<i>authentication remote</i>	pre-share	define authentication method for remote peer ID
<i>authentication local</i>	pre-share	define authentication method for local peer ID
<i>keyring local</i>	kyr1	apply the keyring created in the step before to the profile

4.5 IPsec Tunnel configuration

In order to configure the IPsec part for the responder, type the following commands:

```
crypto ipsec transform-set trans esp-3des esp-sha-hmac
mode tunnel
```

Parameter	Setting	Description
<i>crypto ipsec transform-set</i>	trans esp-3des esp-sha-hmac	Create an IPsec transform set with a name and encryption/authentication algorithms

4.6 Access List configuration

In order to define which kind of traffic has to be tunnelled, an Access List needs to be configured, typing the following commands:

```
ip access-list extended ikev2list
permit ip 172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255
```

As configured on the TransPort router (IPsec Tunnel section), with this ACL, we define that LAN-to-LAN traffic needs to be protected and sent through the tunnel.

4.7 Crypto Map configuration

In Cisco devices, a Crypto Map needs to be configured in order to combine together the settings for IKEv2, IPsec, and traffic that need to be tunneled.

Please note that IOS supports two different types of CMs: static and dynamic. Static CMs are used to define remote peering relationships when all of the variables needed to establish an IPsec peering relationship are known prior to any negotiation between the VPN gateway and the remote peer taking place. Dynamic CMs are used when only some of the remote peer parameters are known prior to negotiation with the VPN gateway. In the case described in this AN, as the Cisco acts as responder, so maybe it doesn't know the other peer IP address, a dynamic map is a good choice.

Also, Dynamic CMs are anchored to a static CM; they are not directly applied to a router interface. The dynamic CM is created with the command: "crypto dynamic-map {dynamic map name} {1-65535}".

Once created, it is added to the static CM using some options on the static CM command: "crypto map {static map name} {1-65535} {ipsec-isakmp} {dynamic} {dynamic map name}". A dynamic CM must be created before it can be anchored to the static CM.

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

In order to configure the Crypto Map, type the following commands:

```
crypto dynamic-map dmap 1
  set transform-set trans
  set ikev2-profile prof
  match address ikev2list
!
!
crypto map cmap 1 ipsec-isakmp dynamic dmap
!
interface FastEthernet0/1
  crypto map cmap
```

Parameter	Setting	Description
<i>crypto dynamic-map</i>	<i>dmap 1</i>	Create the Dynamic Crypto Map and a name
<i>set transform-set</i>	trans	Apply the IPsec transform set already created
<i>set ikev2-profile prof</i>	prof	Apply the IKEv2 profile already created
<i>match address ikev2list</i>	ikev2list	Apply the access list already created
<i>crypto map</i>	<i>cmap 1 ipsec-isakmp dynamic dmap</i>	Create a CM to which is applied the DM already created and set it to an IPsec-ISAKMP type
<i>interface FastEthernet0/1</i>	-	Enter in the WAN Interface Configuration mode
<i>crypto map</i>	cmap	Apply the Crypto Map to the WAN Interface

5 TESTING

5.1 Debug settings on TransPort

In many cases is very useful configure the device in order to have a debug trace for the IKE negotiation in case of issues of setting up the VPN and for check that the traffic is correctly tunnelled.

On the TransPort, go to **Management - Analyser > Settings** and change the settings as shown below (uncheck everything else):

The screenshot shows the 'Management - Analyser > Settings' window. The 'Settings' tab is selected. The 'Enable Analyser' checkbox is checked. The 'Maximum packet capture size' is set to 1500 bytes and the 'Log size' is 180 Kbytes. Under 'Protocol layers', 'Layer 3 (Network)' is checked. Under 'Enable IKE debug', the checkbox is checked. Under 'LAPB Links', 'LAPB 0' and 'LAPB 1' are unchecked. Under 'Serial Interfaces', all checkboxes from ASY 0 to W-WAN are unchecked. Under 'Wi-Fi Analyser Configuration', 'Wi-Fi Analysis' is unchecked, and both 'Wi-Fi Management Packet Analysis' and 'Wi-Fi Data Packet Analysis' are set to 'None'. Under 'Ethernet Interfaces', all checkboxes from ETH 0 to ETH 23 are unchecked. There are 'Clear all Serial Interfaces' and 'Clear all Ethernet Interfaces' buttons at the bottom of their respective sections.

Figure 5.1-1: Analyser settings - 1

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

Management - Analyser > Settings

PPP Interfaces

☐ PPP 0 ☐ PPP 1 ☐ PPP 2 ☐ PPP 3 ☐ PPP 4
☐ PPP 5 ☐ PPP 6 ☐ PPP 7

Clear all PPP Interfaces

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 ☐ ETH 18 ☐ ETH 19
☐ ETH 20 ☐ ETH 21 ☐ ETH 22 ☐ ETH 23
☐ OVPN 0 ☐ OVPN 1 ☐ OVPN 2
☐ PPP 0 ☒ PPP 1 ☐ PPP 2 ☐ PPP 3 ☐ PPP 4
☐ PPP 5 ☐ PPP 6 ☐ PPP 7

Clear all IP Sources

IP Options

☐ Trace discarded packets
☐ Trace loopback packets

Ethernet Packet Filters

MAC Addresses:

IP Packet Filters

TCP/UDP Ports:
IP Protocols:
IP Addresses:

Discarded IP Packet Filters

TCP/UDP Ports:
IP Protocols:
IP Addresses:

Apply

Figure 5.1-2:Analyser settings – 2

Parameter	Setting	Description	CLI command
Enable Analyser	Selected	This checkbox is used to enable or disable the analyser.	ana 0 anon ON
Maximum packet capture size	1500	The number of bytes that are captured and stored for each packet. If the packet is bigger than the configured size, the packet is truncated. Common practice is to set it to 1500	ana 0 maxdata 1500
Log Size	180	The maximum size of the pseudo file “ana.txt” that is used to store the captured data packets. Common practice is to	ana 0 logsize 180

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

Parameter	Setting	Description	CLI command
		set at this maximum (180). Notice that the data is compressed so more than 180Kb of trace data will be captured.	
Protocol layers	Layer 3 (Network)	Specify which protocol layers are captured and included in the analyser trace. For the purpose of this AN the Network Layer (Layer 3) is chosen	ana 0 l3on
Enable IKE debug	Selected	Used to enable/disable the inclusion of IKE packets in the analyser trace when using IPsec	ana 0 ikeon ON
IP Sources	ETH 0 ETH 1	Select the IP sources over which packets will be captured and included in the analyser trace	eth 0 ipanon on eth 1 ipanon on
IP Packet Filters / TCP/UDP Ports	~500,4500	This parameter is used to filter out TCP or UDP packets with particular source or destination port numbers. In order to filter the IKE negotiation phases, set to 500 and 4500. In order to capture data traffic, leave the field empty	ana 0 ipfilt "~500,4500"

It is also needed to enable the IKE debug under IKE settings (**Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Debug**):

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

The screenshot shows a web-based configuration interface. At the top, a breadcrumb trail reads: Configuration > Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Debug. Below this, a tree view on the left lists various configuration categories: Interfaces, DHCP Server, Network Services, DNS Servers, Dynamic DNS, IP Routing/Forwarding, Virtual Private Networking (VPN), IPsec, IPsec Tunnels, IPsec Default Action, IPsec Groups, Dead Peer Detection (DPD), IKE, and IKE Debug. The 'IKE Debug' item is selected and expanded. The main content area contains the following settings: a checked checkbox for 'Enable IKE Debug', a 'Debug Level' dropdown menu set to 'Very High', a 'Debug IP Address Filter' text input field, and an unchecked checkbox for 'Forward debug to port'. An 'Apply' button is located at the bottom left of the configuration area.

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

- ▶ Interfaces
- ▶ DHCP Server
- ▶ Network Services
- ▶ DNS Servers
- ▶ Dynamic DNS
- ▶ IP Routing/Forwarding
- ▼ Virtual Private Networking (VPN)
 - ▼ IPsec
 - ▶ IPsec Tunnels
 - ▶ IPsec Default Action
 - ▶ IPsec Groups
 - ▶ Dead Peer Detection (DPD)
 - ▼ IKE
 - ▼ IKE Debug

☒ Enable IKE Debug

Debug Level: Very High ▼

Debug IP Address Filter:

☐ Forward debug to port

Apply

Figure 5.1-3: Enabling IKE debug

5.2 Debug settings on Cisco

To double check what is going on during testing, it would be good, if possible, to enable some debugs also on Cisco device. In order to do that, please type the following commands:

```
terminal monitor
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 internal
```

Please note that the first command “Terminal Monitor” is only needed if you connect to the Cisco with Telnet or SSH as, by default, Cisco IOS does not send log messages to a terminal session over IP. Instead, console connections on a serial cable do have logging enabled by default.

5.3 Setting the tunnel UP

As soon as the initiator is configured to set up a VPN, it will try to connect to the responder. For a successful negotiation we should see the following logs

Initiator (TransPort):

Going in the eventlog (WEB UI: **Management - Event Log**) of the device:

```
22:22:30, 05 Mar 2000, (5) IKEv2 Negotiation completed pe, Initiator
22:22:30, 05 Mar 2000, Route 0 VPN up peer: cisco1
22:22:30, 05 Mar 2000, New IPSec SA created by cisco1
22:22:30, 05 Mar 2000, (5) IKE Notification: 16395, RX
22:22:30, 05 Mar 2000, (5) IKE Notification: 16394, RX
22:22:30, 05 Mar 2000, (5) IKE Notification: Set window size, RX
22:22:30, 05 Mar 2000, (5) IKE Keys Negotiated. Peer:
22:22:30, 05 Mar 2000, (5) IKE Notification: NATD dest. IP, RX
22:22:30, 05 Mar 2000, (5) IKE Notification: NATD source IP, RX
22:22:29, 05 Mar 2000, (5) New IKEv2 Negotiation peer 10.10.2.1, Initiator (Init)
22:22:29, 05 Mar 2000, IKE Request Received From Route 0
```

Responder (Cisco):

On the terminal monitor should appear the debug, at the end of the negotiation should show the following:

```
*Jul 1 11:05:47.211: IKEv2:(SA ID = 1):IKEV2 SA created; inserting SA into database. SA lifetime timer (86400 sec) started
*Jul 1 11:05:47.215: IKEv2:(SA ID = 1):Session with IKE ID PAIR (transport, cisco1) is UP
*Jul 1 11:05:47.219: IKEv2:IKEv2 MIB tunnel started, tunnel index 1
*Jul 1 11:05:47.223: IKEv2:(SA ID = 1):Load IPSEC key material
*Jul 1 11:05:47.223: IKEv2:(SA ID = 1):[IKEv2 -> IPsec] Create IPsec SA into IPsec database
*Jul 1 11:05:47.227: IKEv2:(SA ID = 1):Asynchronous request queued
*Jul 1 11:05:47.227: IKEv2:(SA ID = 1):
*Jul 1 11:05:47.263: IKEv2:(SA ID = 1):[IPsec -> IKEv2] Creation of IPsec SA into IPsec database PASSED
*Jul 1 11:05:47.275: IKEv2:(SA ID = 1):Checking for duplicate IKEv2 SA
*Jul 1 11:05:47.279: IKEv2:(SA ID = 1):No duplicate IKEv2 SA found
*Jul 1 11:05:47.283: IKEv2:(SA ID = 1):Starting timer (8 sec) to delete negotiation context
```


5.4 IPsev SAs status

The status of the IPsec SAs can be verified on the CLI or going to the WEB UI at **Administration - Execute a command and type: "sastat"**. The result shows that the IPsec SAs (IKEv2 tyoe) are correctly UP:

IPsec SAs (total:1). Eroute 0 -> 4

Outbound V1 SAs

List Empty

Inbound V1 SAs

List Empty

Outbound V2 SAs

SPI	Eroute	Peer IP	First Rem. IP	Last Rem. IP	First Loc. IP	Last Loc. IP	TTL	KBytes Left	VIP
e0889ce1	0	10.10.2.1	172.16.1.0	172.16.1.255	192.168.1.0	192.168.1.255	28664	0	N/A

Inbound V2 SAs

SPI	Eroute	Peer IP	First Rem. IP	Last Rem. IP	First Loc. IP	Last Loc. IP	TTL	KBytes Left	VIP
c9049431	0	10.10.2.1	172.16.1.0	172.16.1.255	192.168.1.0	192.168.1.255	28664	0	N/A

OK

Also in the Cisco device it is possible to check the status of the VON with the following command:

Cisco1#sh cry se de

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

X - IKE Extended Authentication, F - IKE Fragmentation

Interface: FastEthernet0/1

Uptime: 00:02:41

Session status: UP-ACTIVE

Peer: 10.10.1.1 port 500 fvr: (none) ivrf: (none)

Phase1_id: transport

Desc: (none)

IKEv2 SA: local 10.10.2.1/500 remote 10.10.1.1/500 Active

Capabilities:(none) connid:1 lifetime:23:57:19

IPSEC FLOW: permit ip 172.16.1.0/255.255.255.0 192.168.1.0/255.255.255.0

Active SAs: 2, origin: dynamic crypto map

Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4608000/3438

Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4608000/3438

5.5 Testing traffic on the tunnel

Once the VPN is UP, in order to test if LAN to LAN traffic is tunnelled as configured, do a ping from an address in the Initiator LAN and an address in the responder LAN.

Looking at the trace on the initiator (**Management - Analyser > Trace**):

1) An ICMP ECHO REQUEST arrives on ETH 0 from 192.168.1.100:

```
----- 5-3-2000 22:26:02.370 -----
45 00 00 3C 01 D3 00 00 80 01 C9 D0 C0 A8 01 64  E..&lt;.....d
AC 10 01 01 08 00 4D 51 00 01 00 0A 61 62 63 64  .....MQ....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74  efg hijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69          uvw abcdefghi
```

IP (In) From REM TO LOC IFACE: ETH 0

```
45      IP Ver:    4
      Hdr Len:    20
00      TOS:      Routine
      Delay:     Normal
      Throughput: Normal
      Reliability: Normal
00 3C    Length:   60
01 D3    ID:      467
00 00    Frag Offset: 0
      Congestion: Normal
      May Fragment
      Last Fragment
80      TTL:     128
01      Proto:   ICMP
C9 D0    Checksum: 51664
C0 A8 01 64  Src IP: 192.168.1.100
AC 10 01 01  Dst IP: 172.16.1.1
ICMP:
08      Type:    ECHO REQ
00      Code:    0
4D 51    Checksum: 19793
-----
```

2) The packet matches the IPsec tunnel 0:

```
----- 5-3-2000 22:26:02.370 -----
45 00 00 3C 01 D3 00 00 7F 01 CA D0 C0 A8 01 64  E..&lt;.....d
AC 10 01 01 08 00 4D 51 00 01 00 0A 61 62 63 64  .....MQ....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74  efg hijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69          uvw abcdefghi
```

ER 0-cisco1 From LOC TO REM IFACE: ETH 1

```
45      IP Ver:    4
      Hdr Len:    20
00      TOS:      Routine
      Delay:     Normal
      Throughput: Normal
```

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

```
Reliability: Normal
00 3C   Length:   60
01 D3   ID:      467
00 00   Frag Offset: 0
        Congestion: Normal
            May Fragment
            Last Fragment
7F      TTL:     127
01      Proto:   ICMP
CA D0   Checksum: 51920
C0 A8 01 64 Src IP: 192.168.1.100
AC 10 01 01 Dst IP: 172.16.1.1
ICMP:
08      Type:    ECHO REQ
00      Code:    0
4D 51   Checksum: 19793
-----
```

- 3) The packet is then encrypted and sent through the tunnel with source 10.10.1.1 (initiator WAN address) and destination 10.10.2.1 (responder WAN address)

```
----- 5-3-2000 22:26:02.370 -----
45 00 00 70 00 0F 00 00 FA 32 A9 37 0A 0A 01 01  E..p.....2.7....
0A 0A 02 01 E0 88 9C E1 00 00 00 02 B8 6C 35 FC  .....l5.
AC 88 93 D0 FD 74 FD 16 A7 18 3D A7 23 8C 49 EB  ....t....=.#.l.
09 49 D9 7D BA D4 57 67 13 C4 78 1B 32 91 98 72  .l.}.Wg..x.2..r
24 FF 29 40 AB DD 5A 18 49 8B DC 89 60 FC 3A 59  $.)@..Z.l...`.:Y
06 7D D0 C3 81 B3 DB BB 30 BD 9A AC BB 69 AA 47  .j.....0....i.G
AF D3 35 AD 94 FC F8 D9 36 1C F1 74 CC 0C 4E 36  ..5.....6..t..N6
```

IP (Final) From LOC TO REM IFACE: ETH 1

```
45      IP Ver:    4
        Hdr Len:   20
00      TOS:      Routine
        Delay:     Normal
        Throughput: Normal
        Reliability: Normal
00 70   Length:   112
00 0F   ID:       15
00 00   Frag Offset: 0
        Congestion: Normal
            May Fragment
            Last Fragment
FA      TTL:     250
32      Proto:    ESP
A9 37   Checksum: 43319
0A 0A 01 01 Src IP: 10.10.1.1
0A 0A 02 01 Dst IP: 10.10.2.1
-----
```

- 4) An ESP packet arrives on interface ETH 1 from 10.10.2.1 directed to 10.10.1.1:

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

```
----- 5-3-2000 22:26:02.440 -----
45 00 00 70 00 0D 00 00 FE 32 A5 39 0A 0A 02 01  E..p.....2.9....
0A 0A 01 01 C9 04 94 31 00 00 00 02 54 16 73 89  ....1....T.s.
57 1E 0A 62 6F A9 42 89 4F 6D F6 78 D9 85 30 FC  W..bo.B.Om.x..0.
3E 6A DF 17 8E 61 25 31 AD AD DE 1F BE 01 18 93  &gt;j...a%1.....
E8 6C 4C A9 05 87 BD 68 3F BE 16 32 A8 5A A4 CE  .l....h?...2.Z..
58 75 99 ED 50 1A 33 4D FF 75 88 6B AD 5B 22 96  Xu..P.3M.u.k.[".
ED 99 8C 91 D5 8A 51 8D 3D CF 02 36 94 F8 70 13  ....Q.=..6..p.
```

IP (In) From REM TO LOC IFACE: ETH 1

```
45      IP Ver:    4
      Hdr Len:    20
00      TOS:      Routine
      Delay:      Normal
      Throughput: Normal
      Reliability: Normal
00 70    Length:   112
00 0D    ID:       13
00 00    Frag Offset: 0
      Congestion: Normal
      May Fragment
      Last Fragment
FE      TTL:      254
32      Proto:    ESP
A5 39    Checksum: 42297
0A 0A 02 01 Src IP: 10.10.2.1
0A 0A 01 01 Dst IP: 10.10.1.1
-----
```

5) The packet is decrypted, revealing the ICMP ECHO REPLY from 172.16.1.1 to 192.168.1.100:

```
----- 5-3-2000 22:26:02.440 -----
45 00 00 3C 01 D3 00 00 FF 01 4A D0 AC 10 01 01  E..&lt;.....J....
C0 A8 01 64 00 00 55 51 00 01 00 0A 61 62 63 64  ...d..UQ....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74  efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69             uvwabcdefghi
```

IP (Cont) From REM TO LOC IFACE: ETH 1

```
45      IP Ver:    4
      Hdr Len:    20
00      TOS:      Routine
      Delay:      Normal
      Throughput: Normal
      Reliability: Normal
00 3C    Length:   60
01 D3    ID:       467
00 00    Frag Offset: 0
      Congestion: Normal
      May Fragment
      Last Fragment
FF      TTL:      255
01      Proto:    ICMP
4A D0    Checksum: 19152
AC 10 01 01 Src IP: 172.16.1.1
```

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

C0 A8 01 64 Dst IP: 192.168.1.100

ICMP:

00 Type: ECHO REPLY

00 Code: 0

55 51 Checksum: 21841

6) The ECHO REPLY is then sent out through the ETH 0 interface to the destination host:

----- 5-3-2000 22:26:02.440 -----

45 00 00 3C 01 D3 00 00 FE 01 4B D0 AC 10 01 01 E..<.....K....

C0 A8 01 64 00 00 55 51 00 01 00 0A 61 62 63 64 ...d..UQ....abcd

65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 efghijklmnopqrst

75 76 77 61 62 63 64 65 66 67 68 69 uvwabcdefghi

IP (Final) From LOC TO REM IFACE: ETH 0

45 IP Ver: 4

Hdr Len: 20

00 TOS: Routine

Delay: Normal

Throughput: Normal

Reliability: Normal

00 3C Length: 60

01 D3 ID: 467

00 00 Frag Offset: 0

Congestion: Normal

May Fragment

Last Fragment

FE TTL: 254

01 Proto: ICMP

4B D0 Checksum: 19408

AC 10 01 01 Src IP: 172.16.1.1

C0 A8 01 64 Dst IP: 192.168.1.100

ICMP:

00 Type: ECHO REPLY

00 Code: 0

55 51 Checksum: 21841

6 CONFIGURATION FILE

6.1 Initiator (TransPort) Configuration File

This is the configuration used on the Initiator (TransPort) in this Application Note:

```
'config c show'

eth 0 descr "Transport LAN"
eth 0 IPaddr "192.168.1.1"
eth 0 ipanon ON
eth 1 descr "Transport WAN"
eth 1 IPaddr "10.10.1.1"
eth 1 ipsec 1
eth 1 ipanon ON
eth 4 mask ""
eth 5 mask ""
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
route 0 mask ""
route 1 mask ""
route 2 mask ""
route 10 mask ""
route 11 mask ""
def_route 0 gateway "10.10.1.3"
def_route 0 ll_ent "eth"
def_route 0 ll_add 1
eroute 0 descr "VPN to Cisco"
eroute 0 peerip "10.10.2.1"
eroute 0 peerid "cisco1"
eroute 0 ourid "transport"
eroute 0 locip "192.168.1.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "172.16.1.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "3DES"
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "try"
eroute 0 autosa 2
eroute 0 ikever 2
eroute 0 dhgroup 2
eroute 0 debug ON
eroute 1 autosa 2
dhcp 0 IPmin "192.168.1.100"
```

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

```
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"
ppp 0 timeout 300
ppp 1 name "W-WAN (HSPA 3G)"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
ike 0 deblevel 4
ike2 0 iencalg "AES"
ike2 0 ienckeybits 128
ike2 0 idhgroup 2
ike2 0 rencalgs "DES,3DES,AES"
ike2 0 renckeybits 128
ike2 0 rauthalgs "MD5,SHA1"
ike2 0 rprfalgs "MD5,SHA1"
modemcc 0 info_asy_add 7
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Your.APN.goes.here"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
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
ana 0 anon ON
ana 0 l2on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 ipfilt "~500,4500"
ana 0 ikeon ON
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "wr44"
cmd 0 asyled_mode 1
cmd 0 anonftp ON
cmd 0 asy_listen 8002
cmd 0 tremto 1200
cmd 0 rcihhttp ON
user 0 access 0
user 1 name "username"
```

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

```
user 1 epassword "KD51SVJDVg="
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 "cisco1"
user 10 epassword "PDZxU0FFQFU="
user 10 access 4
user 11 name "transport"
user 11 epassword "PDZxU0FFQFU="
user 11 access 4
user 12 epassword "PDZxU0FFQFU="
user 12 access 4
local 0 transaccess 2
sslsrv 0 certfile "cert01.pem"
sslsrv 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
tun 0 mask ""
cloud 0 ssl ON
```

OK

6.2 Responder (Cisco) Configuration File

This is the configuration used on the Responder (Cisco) in this Application Note:

```
Cisco1# sh run
Building configuration...

Current configuration : 1669 bytes
!
! Last configuration change at 11:00:08 UTC Tue Jul 1 2014
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname Cisco1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
crypto ikev2 proposal proposal1
  encryption aes-cbc-128
  integrity sha1
  group 2
!
crypto ikev2 policy policy1
  proposal proposal1
!
crypto ikev2 keyring kyr1
  peer transport
```

```

identity key-id transport
pre-shared-key digidigi
!
!
!
crypto ikev2 profile prof
match identity remote key-id transport
identity local key-id cisco1
authentication remote pre-share
authentication local pre-share
keyring local kyr1
!
!
!
ip tcp synwait-time 5
!
!
!
crypto ipsec transform-set trans esp-3des esp-sha-hmac
mode tunnel
!
!
!
crypto dynamic-map dmap 1
set transform-set trans
set ikev2-profile prof
match address ikev2list
!
!
crypto map cmap 1 ipsec-isakmp dynamic dmap
!
!
!
!
interface FastEthernet0/0
ip address 172.16.1.1 255.255.255.0
speed auto
duplex auto
!
interface FastEthernet0/1
ip address 10.10.2.1 255.255.255.0
speed auto
duplex auto
crypto map cmap
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.10.2.3
!
ip access-list extended ikev2list

```

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

```
permit ip 172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255
!
!
!
!
control-plane
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  login
!
!
end
```