



Application Note

How to Configure an IKEv2 VPN Tunnel
Between Two Digi Transport Routers

14 March 2017

Contents

1	INTRODUCTION	5
1.1	Outline	5
1.2	Assumptions	5
1.3	Corrections	6
1.4	Version	6
2	DIGI CONFIGURATION – INITIATOR.....	7
2.1	LAN Settings	7
2.2	WAN Settings	8
2.2.1	ETH 1 configuration.....	8
2.2.2	Default Route configuration	10
2.3	IKEv2 Configuration	10
2.4	IPsec tunnel Configuration	12
2.5	Preshared Key Configuration.....	14
3	DIGI CONFIGURATION - RESPONDER	16
3.1	LAN Settings	16
3.2	WAN Settings	17
3.2.1	Cellular module configuration.....	17
3.2.2	WAN Interface Configuration (PPP1)	19
3.2.3	Default Route Configuration.....	20
3.3	IKEv2 Configuration	21
3.4	IPsec Tunnel Configuration	22
3.5	Preshared Key Configuration.....	24
4	TESTING.....	26
4.1	Analyser Settings.....	26
4.2	Setting the tunnel UP.....	29
4.3	Testing Traffic on the tunnel.....	31
5	CONFIGURATION FILES	36

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

5.1	Initiator Configuration	36
5.2	Responder Configuration.....	39

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

Figures

Figure 1-1-1: Overview Diagram	5
Figure 2-1: LAN Settings	7
Figure 2-2 ETH 1 Configuration.....	8
Figure 2-3 ETH 1 Configuration – Advanced.....	9
Figure 2-4 Default Route	10
Figure 2-5 IKE v2 configuration.....	11
Figure 2-6 IPsec Tunnel Configuration	12
Figure 2-7 Preshared Key Configuration - Initiator user	14
Figure 2-8 Preshared Key Configuration - Responder user	15
Figure 3-1 LAN Settings	16
Figure 3-2: Mobile settings.....	17
Figure 3-3 PPP 1 settings	19
Figure 3-4 Default Route	20
Figure 3-5 IKEv2 Configuration	21
Figure 3-6 IPsec Tunnel Configuration	22
Figure 3-7 Preshared Key Configuration - Initiator user	24
Figure 3-8 Preshared Key Configuration - Responder user	25
Figure 4-1 Analyser Settings - Initiator	26
Figure 4-2 Analyser Settings – Responder.....	27

1 INTRODUCTION

1.1 Outline

This application note will consider the following scenario:

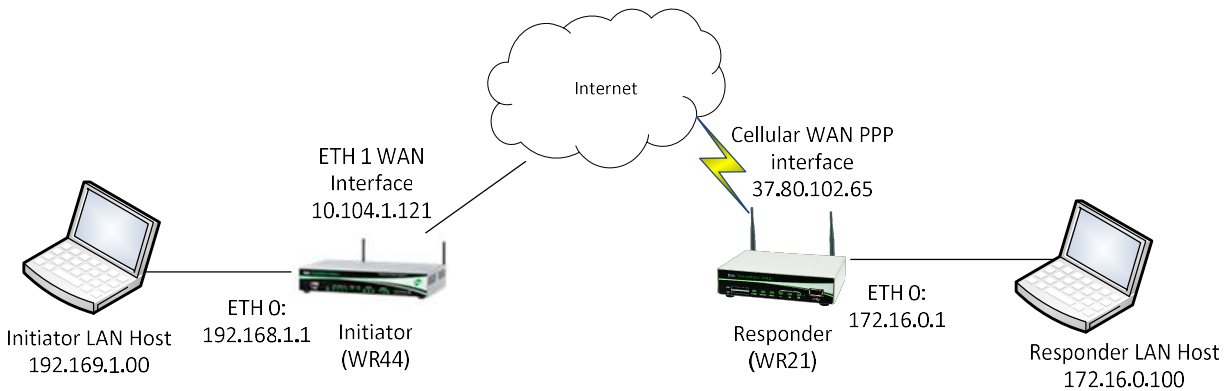


Figure 1-1-1: Overview Diagram

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 two TransPort routers.

1.2 Assumptions

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

This application note applies only to:

Model: Digi Transport WR44

Other Compatible Models: Digi Transport VC7400 VPN Concentrator, WR, SR or DR.

Firmware versions: 5.077 and 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.

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

For the purpose of this application note the following applies:

- Preconditions: This guide assumes that two Digi TransPort are reachable to each other via an Internet connection.

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	January 2017 – Updated WEB UI, brand, tests

2 DIGI CONFIGURATION – INITIATOR

2.1 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:

CONFIGURATION – NETWORK > INTERFACES > ETHERNET > ETH 0

Figure 2-1: LAN Settings

Parameter	Setting	Description
IP Address	192.168.1.1	This parameter specifies the IP address of this Ethernet port on your LAN
Mask	255.255.255.0	The subnet mask of the IP subnet to which the router is attached via this Ethernet port

2.2 WAN Settings

First of all, the Digi TransPort acting as Initiator must have an Internet connection, in this Application note we will configure the ETH WAN in the WR44 as follows.

2.2.1 ETH 1 configuration

In this Application note we will configure the ETH 1 as DHCP Client:

CONFIGURATION – NETWORK > INTERFACES > ETHERNET > ETH 1

The screenshot shows the configuration page for the ETH 1 interface. The breadcrumb trail at the top is "Configuration - Network > Interfaces > Ethernet > ETH 1". The left sidebar shows a tree view with "Interfaces" expanded, then "Ethernet", then "ETH 0", and finally "ETH 1" selected. The main content area for ETH 1 includes a "Description:" field, a radio button selected for "Get an IP address automatically using DHCP", and a section for "Override these DHCP server values:" with fields for "Mask:" (containing "255.255.255.0"), "Gateway:", "DNS Server:", and "Secondary DNS Server:". There are also checkboxes for "Use the MAC address as the client ID" and "Use the following settings". A warning message states "Changes to these parameters may affect your browser connection". At the bottom, there are expandable sections for "Advanced", "QoS", and "VRRP", and an "Apply" button.

Figure 2-2 ETH 1 Configuration

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

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

[Configuration - Network > Interfaces > Ethernet > ETH 1 > Advanced](#)

☐ Use the MAC address as the client ID
☐ Use the following settings

Changes to these parameters may affect your browser connection

Advanced

This device is currently in Port Isolate mode [Switch to Hub mode](#)

Metric:

MTU:

☒ Enable auto-negotiation

Speed (currently 100Base-T): ☒ Auto ☐ 10Base-T ☐ 100Base-T

Duplex: ☒ Auto ☐ Full Duplex ☐ Half Duplex

Max Rx rate: kbps

Max Tx rate: kbps

TCP transmit buffer size: bytes

Take this interface out of service after seconds when the link is lost (e.g. cable removed or broken)

☐ Enable NAT on this interface

☒ Enable IPsec on this interface

☐ Keep Security Associations (SAs) when this ETH interface is disconnected

Use interface for the source IP address of IPsec packets

☐ Enable the firewall on this interface

☐ Enable DNS inbound blocking

☐ Enable DMNR advertisement from this subnet

Remote management access:

Multihome additional consecutive addresses:

☐ Respond to ARP requests only if the requestor is of this network

☐ Enable IGMP on this interface

☐ Enable Bridge on this interface

☐ Generate Heartbeats on this interface

☐ Generate Ping packets on this interface

[QoS](#)

[VRRP](#)

[Apply](#)

Figure 2-3 ETH 1 Configuration – Advanced

Parameter	Setting	Description
Get an IP address automatically using DHCP	Ticked	When selected, enable the DHCP client on the ETH interface so it will get an IP address automatically using DHCP
Enable IPsec on this interface	Enabled	Enable IPsec security features for this interface

2.2.2 Default Route configuration

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:

CONFIGURATION - NETWORK > IP ROUTING/FORWARDING > STATIC ROUTES > DEFAULT ROUTE 0:

Figure 2-4 Default Route

Parameter	Setting	Description
Interface	Ethernet 1	The interface used to route the packets is selected from the drop-down list and its instance number is entered into the adjacent text box.

2.3 IKEv2 Configuration

In order to configure the IKEv2 part for the initiator, set the parameters as indicated below:

CONFIGURATION – NETWORK > VPN > IPSEC > IKE > IKEV2 > IKEV2 0

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKEv2 > IKEv2 0

- 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
 - 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: 2 (1024) ▼

Renegotiate after 8 hrs 0 mins 0 secs

Rekey after 0 hrs 0 mins 0 secs

[Advanced](#)

Figure 2-5 IKE v2 configuration

Parameter	Setting	Description
Encryption	AES (128 bit)	Defines the encryption algorithm used
Authentication	SHA1	Defines the authentication algorithm used.
PRF Algorithm	SHA1	Defines the PRF (Pseudo Random Function) algorithm used
MODP Group for Phase 1	2 (1024)	Sets the key length used in the IKE Diffie-Hellman exchange

Click apply to temporarily save the changes.

2.4 IPsec tunnel Configuration

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

Refer to the following picture and table for the settings of parameters:

CONFIGURATION – NETWORK > VPN > IPSEC > IPSEC TUNNELS > IPSEC 0

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

- Interfaces
- DHCP Server
- Network Services
- DNS Servers
- Dynamic DNS
- IP Routing/Forwarding
- Virtual Private Networking (VPN)
 - IPsec
 - IPsec Tunnels
 - IPsec 0 - 9
 - IPsec 0 - IKEv2 IPsec Tunnel

Description:

The IP address or hostname of the remote unit

Use as a backup unit

Local LAN	Remote LAN
☒ Use these settings for the local LAN IP Address: 192.168.1.0 Mask: 255.255.255.0 ☐ Use interface PPP 0	☒ Use these settings for the remote LAN IP Address: 172.16.0.0 Mask: 255.255.255.0 ☐ Remote Subnet ID:

Use the following security on this tunnel

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

Our ID:

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 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](#)
[Advanced](#)

Figure 2-6 IPsec Tunnel Configuration

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

Parameter	Setting	Description
The IP address or hostname of the remote unit	37.80.37.21	The IP address or hostname of the remote IPsec peer that a VPN will be initiated to.
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
Remote LAN > Use these settings for the Remote LAN	IP address: 172.16.0.0 Mask: 255.255.255.0	The subnet LAN of the other peer
Use the following security on this tunnel	Preshared Keys (Selected)	Choose the security type for the connection. In this AN, Preshared Keys are used
Our ID	initiator	The ID that the initiator will use. This AN will use “transport” as the local ID.
Our ID type	IKE ID	Choose the type of ID used, IKE ID allows the use of descriptive text strings (friendly names)
Remote ID	responder	Set the ID that responder will use. In this AN we will use the id “transport2” as the Remote ID for this tunnel.
Use <> encryption on this tunnel	AES (128 bit keys)	This is the encryption type to use for the tunnel. This AN uses 3DES
Use <> authentication on this tunnel	SHA1	This is the authentication type to use for the tunnel. This AN uses SHA1.
Use Diffie Hellman group <>	2	This is the Diffie Hellman (DH) group to use. This AN uses group 2.
Use IKE <> to negotiate this tunnel	v2	Set The IKE version to use to negotiate this IPsec tunnel, for this AN select “v2”
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
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

2.5 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'.

Refer to the following pictures and tables for the configuration of the users:

CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 10

Figure 2-7 Preshared Key Configuration - Initiator user

Parameter	Setting	Description
Username	initiator	This is the username for the local peer and should match the Local ID configured in the IPsec tunnel
Password/Confirm	****	Fill this field with the Preshared Key for the Local peer ID in the VPN tunnel
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

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 10

The screenshot shows the configuration page for User 11. The breadcrumb trail at the top is 'Configuration - Security > Users > User 10 - 19 > User 11'. On the left, a tree view shows the navigation path: System, Users, User 0 - 9, User 10 - 19, User 10, and User 11. The main area contains the following fields: Username (responder), Password (masked with dots), Confirm Password (masked with dots), and Access Level (None). There is an 'Advanced' link and an 'Apply' button at the bottom.

Figure 2-8 Preshared Key Configuration - Responder user

Parameter	Setting	Description
Username	responder	This is the username for the remote peer and should match the Remote ID configured in the IPsec tunnel
Password/Confirm	****	Fill this field with the Preshared Key for the Remote peer ID in the VPN tunnel.
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

3 DIGI CONFIGURATION - RESPONDER

As done for the 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 Responder is configured on ETH 0, so that need to be changed from the default settings, going to the WEB UI at the section

CONFIGURATION – NETWORK > INTERFACES > ETHERNET > ETH 0:

Configuration - Network > Interfaces > Ethernet > ETH 0

Interfaces

▼ Ethernet

▼ ETH 0

Description:

☐ Get an IP address automatically using DHCP

☒ Use the following settings

IP Address:

Mask:

Gateway:

DNS Server:

Secondary DNS Server:

Changes to these parameters may affect your browser connection

▶ Advanced

▶ QoS

▶ VRRP

Figure 3-1 LAN Settings

Parameter	Setting	Description
IP Address	172.16.0.1	Specifies the IP address of this Ethernet port
Mask	255.255.255.0	Specifies the subnet mask of the IP subnet to which the unit is attached via this Ethernet port

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

Please note that having changed the LAN address, you will need to connect again to the router with the browser pointing at the new address 172.16.0.1 (this implies a change also in the IP address of your laptop).

3.2 WAN Settings

First of all, the Digi TransPort acting as responder must have an Internet connection, in this Application note we will configure the Cellular WAN in the WR44 as follows.

3.2.1 Cellular module configuration

Refer to the following picture and table for the settings of parameters. Note that the SIM PIN, username and password fields may or may not be required.

CONFIGURATION → INTERFACES → MOBILE → MOBILE SETTINGS

The screenshot shows the 'Configuration - Network > Interfaces > Mobile' page. Under the 'Mobile' section, it prompts to 'Select a SIM to configure from the list below'. The selected SIM is '1 (PPP 1)' with IMSI '262010050359784'. Below this is the 'Mobile Settings' section, which says 'Select the service plan and connection settings used in connecting to the mobile network.' The 'Mobile Service Provider Settings' section includes fields for 'Service Plan / APN' (set to 'internet.t-d1.de'), a checkbox for 'Use backup APN' (unchecked), a field for 'Retry the main APN after' (set to '0' minutes), 'SIM PIN' (Optional), 'Confirm SIM PIN', 'Username' (Optional), 'Password' (Optional), and 'Confirm Password'.

Figure 3-2: Mobile settings

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

Parameter	Setting	Description
SIM	1	Select SIM 1 for the PPP 1 interface
Service Plan/APN	internet.t-d1.de	The Access Point Name for the network
SIM PIN / Confirm SIM PIN	<PIN> (optional)	Insert/Confirm the SIM PIN if required by the SIM
Username	W-WAN username	Enter the username given by your wireless operator (If required)
Password/ Confirm Password	W-WAN Password	Enter the password given by your wireless operator (If required)

Click Apply.

Note: The APN is dependent on the mobile operator, check with the service provider to obtain the correct APN.

3.2.2 WAN Interface Configuration (PPP1)

The following section configures the Digi TransPort to use PPP 1 for the cellular interface. Leave all the default settings, except for what is indicated in the following. The username and password fields may or may not be required by the SIM

CONFIGURATION → INTERFACES → ADVANCED → PPP1

The screenshot shows the 'Configuration - Network > Interfaces > Advanced > PPP 1' page. The left sidebar lists navigation options: Mobile, GRE, Serial, Advanced (selected), External Modems, PPP Mappings, PPP 0, and PPP 1 - W-WAN. The main area contains the following settings:

- Description:** W-WAN
- This PPP interface will use:** W-WAN (dropdown)
- Dial out using numbers:** *98*1#
- Prefix:** (empty) to the dial out number
- Username:** (empty)
- Password:** (empty)
- Confirm password:** (empty)
- IP Addressing:**
 - ☒ Allow the remote device to assign a local IP address to this router
 - ☐ Try to negotiate to use 0.0.0.0 as the local IP address for this router
 - ☐ Use 0.0.0.0 as the local IP address for this router (i.e. not negotiable)
- Use mask:** 255.255.255.255 for this interface
- DNS Settings:**
 - ☐ Use the following DNS servers if not negotiated
 - Primary DNS server:** (empty)
 - Secondary DNS server:** (empty)
 - DNS Port:** 53
- ☐ Attempt to assign the following IP configuration to remote devices
- ☒ Request packet data connection
- ☐ Allow this PPP interface to answer incoming calls
- Close the PPP connection:**
 - after 0 seconds
 - if it has been up for 0 minutes in a day
 - if it has been idle for 0 hrs 0 mins 0 secs
 - Alternative idle timer for static routes 0 seconds
 - if the link has not received any packets for 0 seconds
 - if the negotiation is not complete in 80 seconds
- ☒ Enable NAT on this interface
 - ☒ IP address ☐ IP address and Port
 - NAT Source IP address:** (empty)
- ☒ Enable IPsec on this interface
 - ☐ Keep Security Associations (SAs) when this PPP interface is disconnected
 - Use interface:** Default 0 for the source IP address of IPsec packets
- ☐ Enable the firewall on this interface
- Remote management access:** No restrictions (dropdown)

At the bottom, there are links for Mobile, Advanced (selected), PPP Negotiation, and QoS, followed by an 'Apply' button.

Figure 3-3 PPP 1 settings

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

Parameter	Setting	Description
Username	<Username> (optional)	The username to use when authenticating with the mobile operator
Password / Confirm Password	<Password> (optional)	The password to use when authenticating with the mobile operator
Enable IPsec on this interface	Ticked	Enables IPsec on PPP 1 interface.

Click apply, then go to **ADMINISTRATION → SAVE CONFIGURATION** and save.

3.2.3 Default Route Configuration

In the scenario considered in this AN the default gateway for the TransPort that acts as Responder is 10.10.2.3, so a default route need to be configured:

CONFIGURATION - NETWORK > IP ROUTING/FORWARDING > STATIC ROUTES > DEFAULT ROUTE 0:

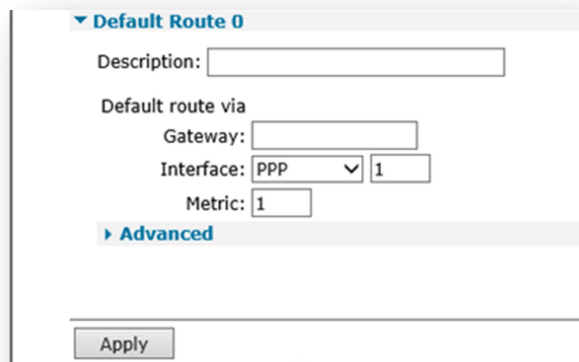


Figure 3-4 Default Route

Parameter	Setting	Description
Interface	PPP 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

3.3 IKEv2 Configuration

In order to configure the IKEv2 part for the responder, set the parameters as indicated below.

In order to have the TransPort to be able to respond to IKE request for every authentication/encryption/PRF/group algorithm, check all the options as shown below (by default may not be all already selected). Leave the rest of the settings as default.

CONFIGURATION – NETWORK > VPN > IPSEC > IKE > IKEV2 > IKEV2 RESPONDER

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKEv2 > IKEv2 Responder

- Interfaces
- DHCP Server
- Network Services
- DNS Servers
- Dynamic DNS
- IP Routing/Forwarding
- Virtual Private Networking (VPN)
 - IPsec
 - IPsec Tunnels
 - IPsec Default Action
 - Dead Peer Detection (DPD)
 - IKE
 - IKEv2
 - IKEv2 0
 - IKEv2 1
 - IKEv2 2
 - IKEv2 3
 - IKEv2 4
 - IKEv2 Responder
 - ☒ Enable IKEv2 Responder
 - Accept IKEv2 Requests with
 - Encryption: ☒ DES (256 bit) ☒ 3DES ☒ AES (128 bit) ☒ AES (192 bit) ☒ AES
 - Authentication: ☒ MD5 ☒ SHA1
 - PRF Algorithm: ☒ MD5 ☒ SHA1
 - MODP Group between: 1 (768) and 2 (1024)
 - Renegotiate after 8 hrs 0 mins 0 secs
 - Rekey after 0 hrs 0 mins 0 secs

[Advanced](#)

Apply

Figure 3-5 IKEv2 Configuration

Parameter	Setting	Description
Encryption	ALL selected	Set the acceptable encryption algorithms and minimum AES key length
Authentication	ALL selected	Set the acceptable authentication algorithms.
PRF Algorithm	ALL selected	Set the acceptable PRF (Pseudo Random Function) algorithms

3.4 IPsec Tunnel Configuration

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

Refer to the following picture and table for the settings of parameters:

CONFIGURATION – NETWORK > VPN > IPSEC > IPSEC TUNNELS > IPSEC 0

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

IPsec Tunnels

IPsec 0

Description:

The IP address or hostname of the remote unit

Use as a backup unit

Local LAN	Remote LAN
☒ Use these settings for the local LAN IP Address: 172.16.0.0 Mask: 255.255.255.0 ☐ Use interface PPP 0	☒ Use these settings for the remote LAN IP Address: 192.168.1.0 Mask: 255.255.255.0 ☐ Remote Subnet ID:

Use the following security on this tunnel

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

Our ID:

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 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

Advanced

Figure 3-6 IPsec Tunnel Configuration

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

Parameter	Setting	Description
Local LAN > Use these settings for the Local LAN	IP address: 172.16.1.0 Mask: 255.255.255.0	The subnet LAN of the local peer
Remote LAN > Use these settings for the Remote LAN	IP address: 192.168.1.0 Mask: 255.255.255.0	The subnet LAN of the other peer
Use the following security on this tunnel	Preshared Keys (Selected)	Choose the security type for the connection. In this AN, Preshared Keys are used
Our ID	Transport2	The ID that the responder will use. This AN will use “transport2” as the local ID.
Our ID type	IKE ID	Choose the type of ID used, IKE ID allows the use of descriptive text strings (friendly names)
Remote ID	transport	Set the ID that initiator will use. In this AN we will use the id “transport” as the Remote ID for this tunnel.
Use <> encryption on this tunnel	3DES	This is the encryption type to use for the tunnel. This AN uses 3DES
Use <> authentication on this tunnel	SHA1	This is the authentication type to use for the tunnel. This AN uses SHA1.
Use Diffie Hellman group <>	2	This is the Diffie Hellman (DH) group to use. This AN uses group 2.
Use IKE <> to negotiate this tunnel	v2	Set The IKE version to use to negotiate this IPsec tunnel, for this AN select “v2”
Bring this tunnel up	On demand	This controls how the IPsec tunnel is brought up, for the responder “On demand” option is chosen
If the tunnel is down and a packet is ready to be sent	Drop the packet	Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent. For the responder is chosen “drop packet” option
Local LAN > Use these settings for the Local LAN	IP address: 172.16.1.0 Mask: 255.255.255.0	The subnet LAN of the local peer
Remote LAN > Use these settings for the Remote LAN	IP address: 192.168.1.0 Mask: 255.255.255.0	The subnet LAN of the other peer
Use the following security on this tunnel	Preshared Keys (Selected)	Choose the security type for the connection. In this AN, Preshared Keys are used

3.5 Preshared Key Configuration

As done for the initiator, also in the responder two users need to be configured for the two peers.

Refer to the following pictures and tables for the configuration of the users:

CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 10

The screenshot shows the configuration page for 'User 10 - initiator' under the path 'Configuration - Security > Users > User 10 - 14 > User 10'. The left sidebar shows a tree structure with 'System' expanded, 'Users' selected, and 'User 10 - 14' expanded, with 'User 10 - initiator' selected. The main area contains the following fields:

- Username:
- Password:
- Confirm Password:
- Access Level: (dropdown menu)
-
-

Figure 3-7 Preshared Key Configuration - Initiator user

Parameter	Setting	Description
Username	initiator	This is the username for the local peer and should match the Local ID configured in the IPsec tunnel
Password/Confirm	****	Fill this field with the Preshared Key for the Local peer ID in the VPN tunnel
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

CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 11

Configuration - Security > Users > User 10 - 14 > User 11

- System
- Users
 - User 0 - 9
 - User 10 - 14
 - User 10 - initiator
 - User 11 - responder

Username: responder

Password: ••••••

Confirm Password:

Access Level: None

Advanced

Apply

Figure 3-8 Preshared Key Configuration - Responder user

Parameter	Setting	Description
Username	responder	This is the username for the remote peer and should match the Remote ID configured in the IPsec tunnel
Password/Confirm	****	Fill this field with the Preshared Key for the Remote peer ID in the VPN tunnel.
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

4 TESTING

4.1 Analyser Settings

In many cases is very useful configure the analyser 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 both initiator and responder change the settings of the Analyser as shown below (uncheck everything else):

MANAGEMENT - ANALYSER > SETTINGS

Initiator (WR44):

The screenshot shows the 'Management - Analyser > Settings' configuration page. The settings are as follows:

- Enable Analyser:** ☒ 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:** ☒ Enable IKE debug
- Enable QMI trace:** ☐ Enable QMI trace
- LAPB Links:**
 - ☐ LAPB 0
 - ☐ LAPB 1
- Serial Interfaces:**
 - ☐ ASY 0 ☐ ASY 1 ☐ ASY 2 ☐ ASY 3 ☐ ASY 4
 - ☐ ASY 6 ☐ ASY 7 ☐ ASY 8 ☐ ASY 9 ☐ ASY 10
 - ☐ ASY 11 ☐ ASY 12 ☐ ASY 13 ☐ ASY 14 ☐ ASY 15
 - ☐ ASY 16 ☐ ASY 17 ☐ ASY 18 ☐ W-WAN
- Ethernet Interfaces:**
 - ☐ 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 ☐ ETH 24
 - ☐ ETH 25 ☐ ETH 26 ☐ ETH 27
- DSL PVC Sources:**
 - ☐ PVC 0 ☐ PVC 1 ☐ PVC 2 ☐ PVC 3 ☐ PVC 4
 - ☐ PVC 5 ☐ PVC 6 ☐ PVC 7
- PPP Interfaces:**
 - ☐ 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
- IP Sources:**
 - ☒ ETH 0 ☒ ETH 1 ☐ ETH 2 ☐ ETH 3 ☐ ETH 4

Figure 4-1 Analyser Settings - Initiator

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

Responder (WR21):

Management - Analyser > Settings

▼ 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

☐ Enable QMI trace

LAPB Links

- ☐ LAPB 0 ☐ LAPB 1

Serial Interfaces

- ☐ ASY 0 ☐ ASY 1 ☐ ASY 2 ☐ ASY 3 ☐ ASY 5
- ☐ ASY 6 ☐ ASY 7 ☐ ASY 8 ☐ ASY 9 ☐ ASY 10
- ☐ ASY 11 ☐ ASY 12 ☐ ASY 13 ☐ ASY 14 ☐ ASY 15
- ☐ ASY 16 ☐ ASY 17 ☐ W-WAN

Clear all Serial Interfaces

Ethernet Interfaces

- ☐ ETH 0 ☐ ETH 1 ☐ ETH 2 ☐ ETH 3 ☐ ETH 4
- ☐ ETH 5 ☐ ETH 6 ☐ ETH 7 ☐ ETH 8 ☐ ETH 9

Clear all Ethernet Interfaces

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
- ☐ 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

Figure 4-2 Analyser Settings – Responder

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

Parameter	Setting	Description
Enable Analyser	Selected	This checkbox is used to enable or disable the analyser.
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
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 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
Enable IKE debug	Selected	Used to enable/disable the inclusion of IKE packets in the analyser trace when using IPsec
IP Sources	ETH 0 & ETH 1 ETH 0 & PPP 1	Select the IP sources over which packets will be captured and included in the analyser trace

4.2 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 in the eventlog of the devices:

MANAGEMENT - EVENT LOG

Initiator:

```
10:55:41, 03 Jan 2017,(69) IKEv2 Negotiation completed pe,Initiator
10:55:41, 03 Jan 2017,Erout 0 VPN up peer: responder
10:55:41, 03 Jan 2017,New IPSec SA created by responder
10:55:41, 03 Jan 2017,(69) New IKEv2 Negotiation peer 37.80.102.65,Initiator (Create Child)
10:55:41, 03 Jan 2017,IKE Request Received From Erout 0
10:55:41, 03 Jan 2017,Par change by username, erout 0 autosa to 2
10:55:38, 03 Jan 2017,(69) IKEv2 Negotiation completed pe,Initiator
10:55:38, 03 Jan 2017,PPP 1 down,LL disconnect
10:55:37, 03 Jan 2017,(69) New IKEv2 Negotiation peer 37.80.102.65,Initiator (Info)
```

Responder:

```
10:50:51, 03 Jan 2017,(154) IKEv2 Negotiation completed pe,Responder
10:50:51, 03 Jan 2017,Erout 0 VPN up peer: initiator
10:50:51, 03 Jan 2017,New IPSec SA created by initiator
10:50:51, 03 Jan 2017,(154) New IKEv2 Negotiation peer 217.151.242.15,Responder (Create Child)
10:50:49, 03 Jan 2017,Telnet session closed
10:50:48, 03 Jan 2017,(154) IKEv2 Negotiation completed pe,Responder
10:50:48, 03 Jan 2017,(154) New IKEv2 Negotiation peer 217.151.242.15,Responder (Info)
```

The status of the IPsec and IKEv2 SAs can also be seen in the WEB UI:

MANAGEMENT - CONNECTIONS > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC

Initiator:

▼ IPsec Tunnels 0 - 9

Outbound V1 SAs
No Tunnels

Inbound V1 SAs
No Tunnels

Outbound V2 SAs

#	Peer IP	First Rem. IP	Last Rem. IP	First Loc. IP	Last Loc. IP	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left	Interface	
0	37.80.102.65	172.16.0.0	172.16.0.255	192.168.1.0	192.168.1.255	N/A	SHA1	AES(128)	N/A	0	0	17320	ETH 1	Remove

Remove All

Inbound V2 SAs

#	Peer IP	First Rem. IP	Last Rem. IP	First Loc. IP	Last Loc. IP	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left	Interface	
0	37.80.102.65	172.16.0.0	172.16.0.255	192.168.1.0	192.168.1.255	N/A	SHA1	AES(128)	N/A	0	0	17320	ETH 1	Remove

Remove All Refresh

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

Responder:

▼ IPsec Tunnels

Outbound V1 SAs
No Tunnels

Inbound V1 SAs
No Tunnels

Outbound V2 SAs

#	Peer IP	First Rem. IP	Last Rem. IP	First Loc. IP	Last Loc. IP	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left	Interface	
0	217.151.242.15	192.168.1.0	192.168.1.255	172.16.0.0	172.16.0.255	N/A	SHA1	AES(128)	N/A	0	0	17294	PPP 1	Remove

[Remove All](#)

Inbound V2 SAs

#	Peer IP	First Rem. IP	Last Rem. IP	First Loc. IP	Last Loc. IP	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left	Interface	
0	217.151.242.15	192.168.1.0	192.168.1.255	172.16.0.0	172.16.0.255	N/A	SHA1	AES(128)	N/A	0	0	17294	PPP 1	Remove

[Remove All](#) [Refresh](#)

4.3 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 a host on initiator LAN to a host in responder LAN. In this AN the two hosts have 192.168.1.100 and 172.16.1.100 as ip addresses.

Looking at the trace on the initiator (**MANAGEMENT - ANALYSER > TRACE**):

- 1) An ICMP ECHO REQUEST arrives on ETH 0 from 192.168.1.100, with destination address the host at Responder LAN side (172.16.0.100):

```

----- 3-1-2017 13:06:43.230 -----
 45 00 00 3C 11 8B 00 00 80 01 BA B5 C0 A8 01 64    E.<.....d
AC 10 00 64 08 00 4D 4C 00 01 00 0F 61 62 63 64    ...d..ML....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 (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
11 8B            ID:          4491
00 00            Frag Offset:  0
                  Congestion:  Normal
                  May Fragment
                  Last Fragment

80                TTL:        128
01                Proto:      ICMP
BA B5            Checksum:    47797
C0 A8 01 64      Src IP:      192.168.1.100
AC 10 00 64      Dst IP:      172.16.0.100
ICMP:
08                Type:       ECHO REQ
00                Code:       0
4D 4C            Checksum:    19533
-----

```

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

- 2) The packet matches the eroute 0 and is encrypted and sent through the tunnel with source 10.104.1.121 (initiator WAN address) and destination 37.80.102.65 (responder WAN address)

```

----- 3-1-2017 13:06:43.230 -----
45 00 00 3C 11 8B 00 00 7F 01 BB B5 C0 A8 01 64      E.<.....d
AC 10 00 64 08 00 4D 4C 00 01 00 0F 61 62 63 64      ...d..ML....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

ER 0-responder From LOC TO REMIFACE: ETH 1
45          IP Ver:          4
          Hdr Len:          20
00          TOS:             Routine
          Delay:             Normal
          Throughput:        Normal
          Reliability:        Normal
00 3C       Length:          60
11 8B       ID:              4491
00 00       Frag Offset:     0
          Congestion:        Normal
          May Fragment
          Last Fragment
7F          TTL:             127
01          Proto:           ICMP
BB B5       Checksum:        48053
C0 A8 01 64 Src IP:          192.168.1.100
AC 10 00 64 Dst IP:          172.16.0.100
ICMP:
08          Type:            ECHO REQ
00          Code:            0
4D 4C       Checksum:        19533
-----
----- 3-1-2017 13:06:43.230 -----
45 00 00 80 00 0C 00 00 FA 11 28 EF 0A 68 01 79      E.....(..h.y
25 50 66 41 11 94 11 94 00 6C 00 00 83 82 E0 3A      %PfA.....l.....:
00 00 00 07 C1 D6 9B 1F E3 49 48 40 7C 9B 3F 51      .....IH@|. ?Q
B8 B9 14 05 1B 04 E4 0C C6 BB AF 6A 1A CB 12 E7      .....j....
6F 42 2E CB 8F AA 7D A7 3F 51 48 84 ED 1B 9B 13      oB....}. ?QH.....
A0 1B DF E1 67 31 1E 8F 3B 91 0E 27 CB 16 C8 7E      ....g1...;..'....~
9C 27 D2 FC 56 E6 68 1E E2 F1 9F 92 34 8F 9C DB      ..'.V.h.....4...
8B 50 CC CF 19 6E FF 76 16 85 2B B3 91 FC B4 79      .P...n.v...+....y

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 80       Length:          128

```


How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

```

00 0C          ID:          12
00 00          Frag Offset: 0
                  Congestion: Normal
                        May Fragment
                        Last Fragment
FA            TTL:          250
11            Proto:        UDP
28 EF          Checksum:    10479
0A 68 01 79    Src IP:      10.104.1.121
25 50 66 41    Dst IP:      37.80.102.65
UDP:
11 94          SRC Port:    IKE FLOAT (4500)
11 94          DST Port:    IKE FLOAT (4500)
00 6C          Length:      108
00 00          Checksum:    0
-----

```

3) The reply arrives on ETH1 through the tunnel:

```

----- 3-1-2017 13:06:44.480 -----
45 00 00 80 00 0B 00 00 E9 11 39 F0 25 50 66 41  E.....9.%PfA
0A 68 01 79 11 94 11 94 00 6C 00 00 76 41 2D C2  .h.y.....l..vA-.
00 00 00 07 6A DA 9C E0 8A E4 81 8F B7 03 BB 76  ....j.....v
46 A1 2A EB D1 52 98 6F 42 89 83 83 13 AE 0F 6E  F.*..R.oB.....n
77 3F 2E 7C BC 94 D7 15 88 57 BE B3 8F 8C 55 37  w?..|.....W....U7
67 41 A2 5C 9B 11 5E 62 E8 AF 51 8C BF 2B A5 C1  gA.\..^b..Q..+..
CD 48 5A BE E4 90 74 7E 2B 9D 68 86 10 C5 CA 63  .HZ...t~+.h....c
57 FD 33 1C 7E 86 E5 1D 1B 40 EE 98 1F 98 AA DF  W.3.~.....@.....

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 80        Length:         128
00 0B        ID:             11
00 00        Frag Offset:    0
          Congestion:        Normal
                        May Fragment
                        Last Fragment
E9          TTL:             233
11          Proto:           UDP
39 F0        Checksum:       14832
25 50 66 41  Src IP:         37.80.102.65
0A 68 01 79  Dst IP:         10.104.1.121
UDP:
11 94        SRC Port:       IKE FLOAT (4500)
11 94        DST Port:       IKE FLOAT (4500)
00 6C        Length:         108

```

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

```
00 00          Checksum:      0
-----
```

- 4) The packet is decrypted and the ICMP ECHO REPLY is revealed and sent to the destination host via ETH 0:

```
----- 3-1-2017 13:06:44.480 -----
45 00 00 3C 54 BC 00 00 7F 01 78 84 AC 10 00 64   E..<T.....x....d
C0 A8 01 64 00 00 55 4C 00 01 00 0F 61 62 63 64   ...d..UL....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              uvwabcdeghi

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
54 BC                      ID:           21692
00 00                      Frag Offset:  0
                          Congestion:   Normal
                          May Fragment
                          Last Fragment

7F                          TTL:         127
01                          Proto:        ICMP
78 84                      Checksum:     30852
AC 10 00 64                Src IP:       172.16.0.100
C0 A8 01 64                Dst IP:       192.168.1.100
ICMP:
00                          Type:         ECHO REPLY
00                          Code:         0
55 4C                      Checksum:     19541
-----

----- 3-1-2017 13:06:44.480 -----
45 00 00 3C 54 BC 00 00 7E 01 79 84 AC 10 00 64   E..<T...~.y....d
C0 A8 01 64 00 00 55 4C 00 01 00 0F 61 62 63 64   ...d..UL....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              uvwabcdeghi

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
54 BC                      ID:           21692
```

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

```
00 00      Frag Offset:  0
           Congestion:  Normal
           May Fragment
           Last Fragment
7E         TTL:         126
01         Proto:       ICMP
79 84      Checksum:    31108
AC 10 00 64 Src IP:     172.16.0.100
C0 A8 01 64 Dst IP:     192.168.1.100
ICMP:
00         Type:        ECHO REPLY
00         Code:        0
55 4C      Checksum:    19541
-----
```

5 CONFIGURATION FILES

5.1 Initiator Configuration

This is the config.da0 file used for the purpose of this Application Note on the Initiator side:

```
eth 0 IPaddr "192.168.1.1"
eth 0 ipanon ON
eth 1 dhcpcli ON
eth 1 ipsec 1
eth 1 ipanon 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 "ETH"
def_route 0 ll_add 1
eroute 0 descr "IKEv2 IPsec Tunnel"
eroute 0 peerip "37.80.102.65"
eroute 0 peerid "responder"
eroute 0 ourid "initiator"
eroute 0 locip "192.168.1.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "172.16.0.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"
eroute 0 autosa 2
eroute 0 ikever 2
eroute 0 dhgroup 2
eroute 0 enckeybits 128
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"
sntp 0 server "time.devicecloud.com"
dyndns 0 ifent "default"
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 aodion 1
ppp 1 autoassert 1
```

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

```
ppp 1 r_chap OFF
ppp 3 name "DSL"
ppp 3 l1iface "AAL"
ppp 3 username "Enter ADSL Username"
ppp 3 r_addr OFF
ppp 3 IPaddr "0.0.0.0"
ppp 3 l_addr ON
ppp 3 timeout 0
ppp 3 do_nat 2
ppp 3 aodion 1
ppp 3 autoassert 1
ppp 3 immoos ON
ppp 3 echo 10
ppp 3 echodropcnt 5
ppp 3 l_pap OFF
ppp 3 l_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
ftpccli 0 hostname "ftp1.digi.com"
ftpccli 0 directory "support/firmware/transport/radio_module_firmware/he910d"
ike2 0 iencalg "AES"
ike2 0 ienckeybits 128
ike2 0 idhgroup 2
modemcc 0 info_asy_add 6
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
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 anon ON
ana 0 l2on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 ikeon ON
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 anonftp ON
cmd 0 tremto 1200
```

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

```
cmd 0 rcihhttp ON
cmd 4 cmd_processor OFF
user 0 access 0
user 1 name "username"
user 1 epassword "KD51SVJDVVg="
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 "initiator"
user 10 epassword "PDZxU0FFQFU="
user 10 access 4
user 11 name "responder"
user 11 epassword "PDZxU0FFQFU="
user 11 access 4
local 0 transaccess 2
sslcli 0 verify 10
sslsrv 0 certfile "cert01.pem"
sslsrv 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
templog 0 mb_autooff ON
templog 0 mo_autooff ON
cloud 0 ssl ON
```

5.2 Responder Configuration

This is the config.da0 file used for the purpose of this Application Note on the Responder side:

```
eth 0 IPaddr "172.16.0.1"
eth 0 ipanon ON
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
eroute 0 descr "IKEv2 IPsec Tunnel"
eroute 0 peerid "initiator"
eroute 0 ourid "responder"
eroute 0 locip "172.16.0.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "192.168.1.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "PRESHARED"
eroute 0 ikever 2
eroute 0 dhgroup 2
eroute 0 enckeybits 128
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"
snmp 0 server "time.etherios.com"
snmpuser 0 eCommunity "KCp0VxkP"
ppp 0 timeout 300
ppp 1 name "W-WAN"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 ipsec 1
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipanon ON
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
ike 0 deblevel 4
ike2 0 rencalgs "DES,3DES,AES"
ike2 0 renckeybits 128
```

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

```
ike2 0 rauthalgs "MD5,SHA1"
ike2 0 rprfalgs "MD5,SHA1"
modemcc 0 asy_add 4
modemcc 0 info_asy_add 2
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Internet.t-d1.de"
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
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 anon ON
ana 0 l2on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 ikeon ON
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
cmd 0 rcihttp ON
user 0 access 0
user 1 name "username"
user 1 epassword "KD51SVJDVVg="
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 "initiator"
user 10 epassword "PDZxU0FFQFU="
user 10 access 4
user 11 name "responder"
user 11 epassword "PDZxU0FFQFU="
user 11 access 4
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
```


How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

```
ssh 0 hostkey1 "privSSH.pem"  
ssh 0 nb_listen 5  
ssh 0 v1 OFF  
templog 0 mo_autooff ON  
cloud 0 ssl ON
```