



Application Note 10

**IPSec Over Cellular using Digi Transport Routers
With Pre-shared key authentication**

September 2020

Contents

1	Introduction	4
1.1	Outline	4
1.2	Assumptions	5
1.3	Corrections	5
1.4	Version	5
2	VPN INITIATOR (WR21) Configuration	6
2.1	VPN Initiator (WR21) Inside Ethernet Interface	6
2.2	VPN Initiator (WR21) Cellular PPP Interface	7
2.3	VPN Initiator (WR21) Wireless WAN (W-WAN) Module	7
2.4	VPN Initiator (WR21) Phase 1-IKE	8
2.5	VPN Initiator (WR21) Phase 2 – IPSec	11
2.6	VPN Initiator (WR21) Pre-shared Key	13
2.7	VPN Initiator (WR21) Configure Packet Analyser for Debugging	14
3	VPN RESPONDER (WR44) CONFIGURATION	16
3.1	VPN Responder (WR44) Inside LAN Ethernet Interface	16
3.2	VPN Responder (WR44) Cellular PPP Interface	17
3.3	VPN Responder (WR44) Wireless WAN (W-WAN) Module	17
3.4	VPN Responder (WR44) Phase 1-IKE	18
3.5	VPN Responder (WR44) Phase 2 – IPSEC	21
3.6	VPN Responder (WR44) Pre-shared Key	23
3.7	VPN Responder (WR44) Analayser.	24
4	TESTING	26
4.1	Successful connection:	26
4.1.1	Initiator (WR21) Log:	26
4.1.2	Responder (WR44) Log:	26
4.1.3	IPSEC Security Associations	27

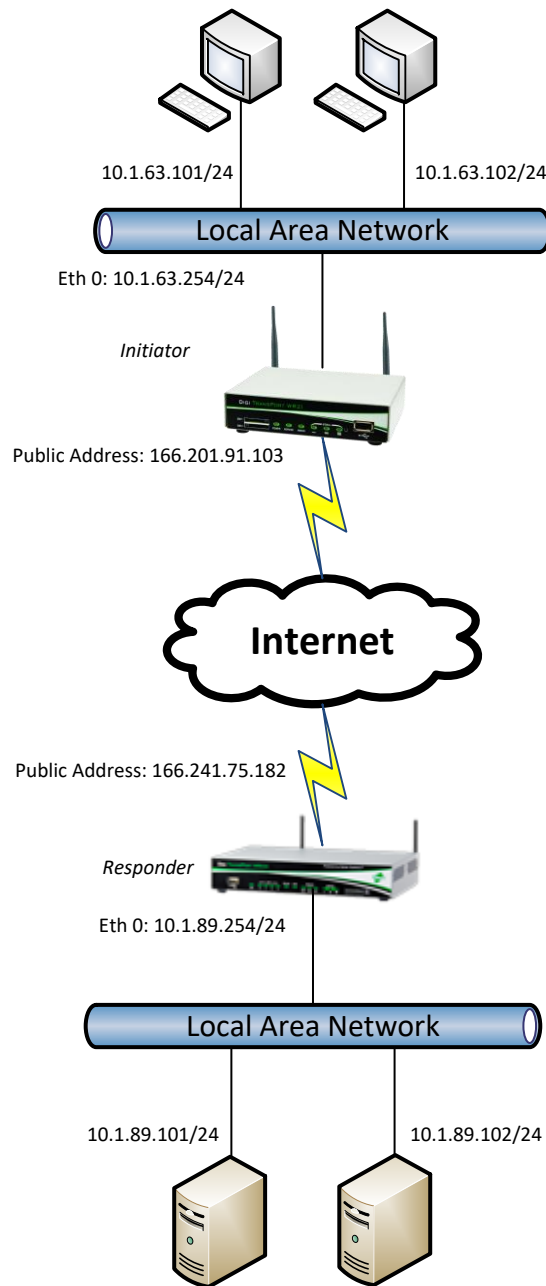
4.1.4	IPsec Peers.....	28
4.1.5	IKE SAs	29
5	CONFIGURATION & Firmware FILES	30
5.1	Digi Transport WR21 (Initiator) Configuration	30
5.2	Digi Transport WR44 (Responder) Configuration.....	31
5.3	Digi Transport WR21 (Initiator) Firmware	32
5.4	Digi Transport WR44 (Responder) Firmware.....	33
6	Various Comments/Tips.....	34
7	VPN INITIATOR (DSL Connection) Configuration	34
7.1	VPN Initiator (WR44) with DSL Setup.....	34
7.2	VPN Initiator (WR44) ADSL PPP Interface	35
7.3	Successful Connection.....	37
7.3.1	Initiator Log	37
7.3.2	IPSEC Security Associations.....	38
7.3.3	IPSec Peers	38
7.3.4	IKE SAs	39

1 INTRODUCTION

1.1 Outline

This application note aims to enable the reader to easily configure a VPN tunnel between two local area networks using a Digi Transport router at both ends of the tunnel.

The diagram below details the IP number scheme and architecture of this example configuration.



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.

Configuration: This application note assumes that the WR21 will be connecting to a cellular network (i.e. GPRS, EDGE, 3G, HSDPA, HSUPA, LTE). Routers connecting to cellular networks are usually allocated a private IP address which would translate to a routable internet external IP at the border of the mobile internet network. In this case, the mode of IPSec needs to be “aggressive mode” with NAT-Traversal.

The IPSec responder’s IP address needs to be in the public address range and is either fixed or dynamic. In the case of the latter, a type of dynamic DNS hostname will be required because the IPSec initiator always needs to know where to connect.

This application note applies to:

Models shown: Digi Transport WR21, as the Initiator, and WR21, as the responder.

Other Compatible Models: Digi Transport WR11, WR31. WR44

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. For the purpose of this application note the following applies:

- The IPSec responder router’s IP address must be in the public address range and fully routable.

As with all Digi Transport routers you have the option of configuring the IPSec parameters either via the web interface or by writing a new configuration file. We will show the web configuration in this application note. Only the parts of the configuration files that specifically relate to the configuration of this example will be explained in detail. (The configuration files used for this application note can be found in their entirety at the end of this document).

The key to VPNs: Make sure that the settings match on both ends of the connection.

1.3 Corrections

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

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

1.4 Version

Status	
1	Published
1.1	Revision for new W-WAN usage in the web GUI post release 5.036.
2	Updated and rebranded
2.1	Fixed errors and updated
2.2	Updated screenshots and instructions for new web interface and rebranding (Sep 2016)
2.3	Updated screenshots and instructions (Sep 2020)

2 VPN INITIATOR (WR21) CONFIGURATION

The WR21, in this example, will act as the initiator for the IPsec tunnel. This means that it is responsible for starting the VPN connection. Please reference the drawing on page 4. It does have a cellular connection. An example of an initiator for an IPsec tunnel, with a DSL connection, may be found under section 7.

2.1 VPN Initiator (WR21) Inside Ethernet Interface

This procedure includes setting up the initial Ethernet interface.

Using the TransPort's web interface browse to:

Configuration - Network > Interfaces > Ethernet > ETH 0

The following is how the WR21 was set up for this network:

Parameter	Setting	Description
IP Address	10.1.63.254	Enter the IP address of the LAN interface for the router
Mask	255.255.255.0	Enter the subnet mask

[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

Click **Apply**.

2.2 VPN Initiator (WR21) Cellular PPP Interface

IPSec is enabled on the outside interface; in this example the outside interface is the cellular interface PPP 1.

Using the TransPort's web interface browse to:

Configuration - Network > Interfaces > Advanced > PPP 1

Parameter	Setting	Description
Enable IPSec on this interface	✓	Enable IPSec on PPP 1 interface

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

☒ Enable NAT on this interface
 ☒ IP address ☐ IP address and Port
 NAT Source IP address:

☒ Enable IPsec on this interface
 ☐ Keep Security Associations (SAs) when this PPP interface is disconnected
 Use interface for the source IP address of IPsec packets

☐ Enable the firewall on this interface

Click **Apply**.

2.3 VPN Initiator (WR21) Wireless WAN (W-WAN) Module

Browse to **Configuration - Network > Interfaces > Mobile**

Parameter	Setting	Description
Service Plan/APN	internet	Enter the APN of your mobile provider
SIM PIN/Confirm Pin	0123	Enter SIM PIN if required
Username	username	Enter Username if required
Password/Confirm Password	password	Enter Password if required

▼ Interfaces

► Ethernet

▼ Mobile

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: 1 (PPP 1) ▼

IMSI: Unknown

▼ 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 minutes

SIM PIN: (Optional)

Confirm SIM PIN:

Username: (Optional)

Password: (Optional)

Confirm Password:

Click **Apply**.

2.4 VPN Initiator (WR21) Phase 1-IKE

IKE is the first stage in establishing a secure link between two endpoints and has to be configured to match the settings on the VPN host Digi Transport. In this example 3DES and MD5 are used to encrypt and authenticate. Aggressive mode is enabled. MODP group 2 is used, meaning a 1024 bit key for the IKE Diffie-Hellman exchange. Set the IKE SAs to be removed when the IPSec SAs are removed. Set debug to very high as this will help diagnose any problems if the two units fail to build the VPN tunnel.

This first step configures the WR44 Packet Analyser for Debugging

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

Parameter	Setting	Description
Enable IKE Debug	✓	Turn on IKE Debugging
Debug Level	Very High	This will allow for detailed debugging and can be turned off once you are happy that this is working

[Configuration - Network](#) > [Virtual Private Networking \(VPN\)](#) > [IPsec](#) > [IKE](#) > [IKE Debug](#)

▼ IPsec

▶ IPsec Tunnels

▶ IPsec Default Action

▶ Dead Peer Detection (DPD)

▼ IKE

▼ IKE Debug

☒ Enable IKE Debug

Debug Level: **Very High ▼**

Debug IP Address Filter:

☐ Forward debug to port

Click **Apply**.

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

And make the following changes:

Parameter	Setting	Description
Encryption	3DES	The encryption algorithm to be used for IKE exchanges over the IP connection
Authentication	MD5	The algorithm used to authenticate the IKE session
Mode	Aggressive	Aggressive mode is used in this example
MODP Group for Phase 1	2 (1024)	The key length used in the IKE Diffie-Hellman exchange
MODP Group for Phase 2	2 (1024)	The minimum width of the numeric field used in the calculations for phase 2 of the security exchange.

[Configuration - Network](#) > [Virtual Private Networking \(VPN\)](#) > [IPsec](#) > [IKE](#) > [IKE 0](#)

▼ Virtual Private Networking (VPN)

▼ IPsec

▶ IPsec Tunnels

▶ IPsec Default Action

▶ Dead Peer Detection (DPD)

▼ IKE

▶ IKE Debug

▼ 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: 2 (1024) ▼

Renegotiate after 8 hrs 0 mins 0 secs

▶ Advanced

Click **Apply**.

Then in the **Advanced** section:

Parameter	Setting	Description
SA Removal Mode	Remove IKE SA when last IPsec SA removed	Remove IKE SA when last IPSEC SA removed

[Configuration - Network](#) > [Virtual Private Networking \(VPN\)](#) > [IPsec](#) > [IKE](#) > [IKE 0](#)

▼ Advanced

Retransmit a frame if no response after 10 seconds

Stop IKE negotiation after 2 retransmissions

Stop IKE negotiation if no packet received for 30 seconds

☒ Enable Dead Peer Detection

NAT Traversal Mode: Auto ▼

☒ Send INITIAL-CONTACT notifications

☐ Retain phase 1 SA after failed phase 2 negotiation

RSA private key file:

SA Removal Mode: Remove IKE SA when last IPsec SA removed ▼

☐ Delete SAs when invalid SPI notifications are received

Click **Apply**.

2.5 VPN Initiator (WR21) Phase 2 – IPsec

Browse to **Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0**
We will next configure the Eroute (encrypted route).

This will determine what traffic is routed to the remote network over the VPN.

Note: In Aggressive mode the Peer ID and the Our ID can be any alpha-numeric value as long as they correspond with the remote VPN router, they are also case sensitive. In Main Mode, the outside interface addresses are expected to be used.

Parameter	Setting	Description
IP Address or Hostname of the remote unit	213.152.58.85	IP address of the VPN host machine
Local LAN IP Address	10.1.63.0	Packets will be directed through this tunnel if the source and destination IP matches
Local LAN Mask	255.255.255.0	Subnet mask for the network
Remote LAN IP Address	10.1.89.0	Packets will be directed through this tunnel if the source and destination IP matches:
Remote LAN Mask	255.255.255.0	Subnet mask for the network
Use the following security on this tunnel	Pre-shared Keys	Pre-shared keys will be used for authentication
Our ID	initiator	The ID of the VPN initiator router (this router)
Remote ID	responder	The ID of the VPN responder router (remote router)
Use () encryption on this tunnel	3DES	The IPSEC encryption algorithm to use is 3DES
Use () Authentication on this tunnel	MD5	The IPSEC ESP authentication algorithm is MD5:
Use Diffie Hellman group ()	2	The Diffie Hellman (DH) group to use when negotiating new IPsec SAs.
Bring this tunnel up	Whenever a route to the destination is available	
If this tunnel is down and a packet is ready to be sent	Bring the tunnel up	

Virtual Private Networking (VPN)

IPsec

IPsec Tunnels

IPsec 0

Description:

The IP address or hostname of the remote unit

Use as a backup unit

Local LAN

☒ Use these settings for the local LAN

IP Address:

Mask:

☐ Use interface

Remote LAN

☒ Use these settings for the remote LAN

IP Address:

Mask:

☐ 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

Click **Apply**

2.6 VPN Initiator (WR21) Pre-shared Key

In this section the pre-shared key is set up. The pre-shared key is enabled by creating a username with the name of the remote peer (Peer ID from the Eroute) and the password is the pre-shared key

Browse to **Configuration - Security > Users > User 10 - 14 > User 10**

Parameter	Setting	Description
Username	responder	Name should match the Peer ID: value from Eroute 0
Password	password	Enter a password
Confirm Password	password	Re-enter the password
Access Level	None	This user will not be granted any admin access as only used as a pre-shared key

[Configuration - Security > Users > User 10 - 14 > User 10](#)

▶ System

▼ Users

▶ User 0 - 9

▼ User 10 - 14

▼ User 10

Username:

responder

Password:

••••

Confirm Password:

••••

Access Level:

None ▼

Click **Apply**.

2.7 VPN Initiator (WR21) Configure Packet Analyser for Debugging

IP analysis is also enabled on this interface for use during the testing phase.

Browse to **Management - Analyser > Settings**

Configure the following settings

Parameter	Setting	Description
Enable Analyser	✓	Turn on the Analyser
Max packet capture size	1500	Capture any packet up to 1500 Bytes
Log Size	180	The maximum size of the log file in kilobytes
Enable IKE Debug	✓	When this is ticked we will see IKE debug in the trace
IP Source	Eth 0	Enable logging for this interface
IP Source	PPP 1	Enable logging for this interface
IP Packet filter ports	500, 4500	Restrict the ports logged to show only IKE and IPSec

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 3 ☐ ASY 4 ☐ 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

IP Options

☐ Trace discarded packets

☐ Trace loopback packets

Ethernet Packet Filters

MAC Addresses:

IP Packet Filters

TCP/UDP Ports:

IP Protocols: ~500,4500

IP Addresses:

Discarded IP Packet Filters

TCP/UDP Ports:

IP Protocols:

IP Addresses:

Apply

Click **Apply** and then **Save**.

3 VPN RESPONDER (WR44) CONFIGURATION

The WR44, in this example, will act as the responder for the IPsec tunnel. Please reference the drawing on page 4.

3.1 VPN Responder (WR44) Inside LAN Ethernet Interface

Using the TransPort's web interface browse to:

Configuration - Network > Interfaces > Ethernet > ETH 0

Parameter	Setting	Description
IP Address	10.1.89.254	Enter the IP address of the LAN interface for the router
Mask	255.255.255.0	Enter the subnet mask

[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

Click **Apply**

3.2 VPN Responder (WR44) Cellular PPP Interface

IPSec is enabled on the outside interface; in this example the outside interface is the cellular interface PPP 1. IP analysis is also enabled on this interface for use during the testing phase.

Using the TransPort's web interface browse to:

Configuration - Network > Interfaces > Advanced > PPP 1

Parameter	Setting	Description
Enable IPSec on this interface	✓	Enable IPSec on PPP 1 interface

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

☒ Enable NAT on this interface

☒ IP address ☐ IP address and Port

NAT Source IP address:

☒ Enable IPsec on this interface

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

Use interface for the source IP address of IPsec packets

☐ Enable the firewall on this interface

Click **Apply**

3.3 VPN Responder (WR44) Wireless WAN (W-WAN) Module

Browse to **Configuration - Network > Interfaces > Mobile**

Parameter	Setting	Description
Service Plan/APN	internet	Enter the APN of your mobile provider
SIM PIN/Confirm Pin	0123	Enter SIM PIN if required
Username	username	Enter Username if required
Password/Confirm Password	password	Enter Password if required

▼ Interfaces

► Ethernet

▼ Mobile

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: 1 (PPP 1) ▼

IMSI: Unknown

▼ 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 minutes

SIM PIN: (Optional)

Confirm SIM PIN:

Username: (Optional)

Password: (Optional)

Confirm Password:

Click **Apply**

3.4 VPN Responder (WR44) Phase 1-IKE

IKE is the first stage in establishing a secure link between two endpoints and has to be configured to match the settings on the VPN host Digi Transport. In this example 3DES and MD5 are used to encrypt and authenticate. Aggressive mode is enabled. MODP group 2 is used, meaning a 1024 bit key for the IKE Diffie-Hellman exchange. Set the IKE SAs to be removed when the IPSec SAs are removed. Set debug to very high as this will help diagnose any problems if the two units fail to build the VPN tunnel.

This first step configures the WR44 Packet Analyser for Debugging

Browse to **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	Sets the level of IKE debugging

[Configuration - Network](#) > [Virtual Private Networking \(VPN\)](#) > [IPsec](#) > [IKE](#) > [IKE Debug](#)

▼ IPsec

▶ IPsec Tunnels

▶ IPsec Default Action

▶ Dead Peer Detection (DPD)

▼ IKE

▼ IKE Debug

☒ Enable IKE Debug

Debug Level: **Very High ▼**

Debug IP Address Filter:

☐ Forward debug to port

Click **Apply**

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

And make the following changes:

Parameter	Setting	Description
Encryption	3DES	The encryption algorithm to be used for IKE exchanges over the IP connection
Authentication	MD5	The algorithm used to authenticate the IKE session
Mode	Aggressive	Aggressive mode is used in this example
MODP Group for Phase 1	2 (1024)	The key length used in the IKE Diffie-Hellman exchange
MODP Group for Phase 2	2 (1024)	The minimum width of the numeric field used in the calculations for phase 2 of the security exchange.

[Configuration - Network](#) > [Virtual Private Networking \(VPN\)](#) > [IPsec](#) > [IKE](#) > [IKE 0](#)

▼ Virtual Private Networking (VPN)

▼ IPsec

▶ IPsec Tunnels

▶ IPsec Default Action

▶ Dead Peer Detection (DPD)

▼ IKE

▶ IKE Debug

▼ 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: 2 (1024) ▼

Renegotiate after 8 hrs 0 mins 0 secs

▶ Advanced

Click **Apply**.

Then in the **Advanced** section:

Parameter	Setting	Description
SA Removal Mode	Remove IKE SA when last IPsec SA removed	Remove IKE SA when last IPSEC SA removed

[Configuration - Network](#) > [Virtual Private Networking \(VPN\)](#) > [IPsec](#) > [IKE](#) > [IKE 0](#)

▼ Advanced

Retransmit a frame if no response after 10 seconds

Stop IKE negotiation after 2 retransmissions

Stop IKE negotiation if no packet received for 30 seconds

☒ Enable Dead Peer Detection

NAT Traversal Mode: Auto ▼

☒ Send INITIAL-CONTACT notifications

☐ Retain phase 1 SA after failed phase 2 negotiation

RSA private key file:

SA Removal Mode: Remove IKE SA when last IPsec SA removed ▼

☐ Delete SAs when invalid SPI notifications are received

This will delete the IKE SA when all the IPsec SAs that it created to a particular peer are removed.

Click **Apply**.

3.5 VPN Responder (WR44) Phase 2 – IPSEC

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

Parameter	Setting	Description
Local LAN IP Address	10.1.89.0	Packets will be directed through this tunnel if the source and destination IP matches
Local LAN Mask	255.255.255.0	Subnet mask for the network
Remote LAN IP Address	10.1.63.0	Packets will be directed through this tunnel if the source and destination IP matches:
Remote LAN Mask	255.255.255.0	Subnet mask for the network
Use the following security on this tunnel	Pre-shared Keys	Pre-shared keys will be used for authentication
Our ID	Responder	The ID of the VPN initiator router (this router)
Remote ID	Initiator	The ID of the VPN responder router (remote router)
Use () encryption on this tunnel	3DES	The IPSEC encryption algorithm to use is 3DES
Use () Authentication on this tunnel	MD5	The IPSEC ESP authentication algorithm is MD5:
Use Diffie Hellman group ()	2	The Diffie Hellman (DH) group to use when negotiating new IPsec SAs.
Bring this tunnel up	Whenever a route to the destination is available	
If this tunnel is down and a packet is ready to be sent	Bring the tunnel up	

▼ IPsec

▼ IPsec Tunnels

▼ IPsec 0

Description:

The IP address or hostname of the remote unit

Use as a backup unit

Local LAN

☒ Use these settings for the local LAN
IP Address:
Mask:
☐ Use interface

Remote LAN

☒ Use these settings for the remote LAN
IP Address:
Mask:
☐ 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

Click **Apply**.

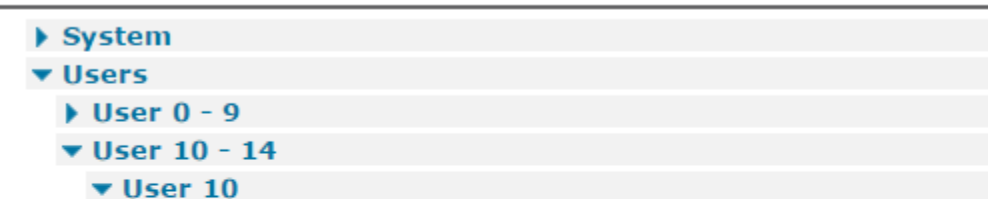
3.6 VPN Responder (WR44) Pre-shared Key

In this section the pre-shared key is set up, the pre-shared key is set up by creating a username with the name of the remote peer (initiator) VPN id and the password is the pre-shared key.

Browse to **Configuration - Security > Users > User 10 - 14 > User 10**

Parameter	Setting	Description
Username	initiator	Name should match the Peer ID: value from Eroute 0
Password	password	Enter the password
Confirm Password	password	Re-enter the password
Access Level	None	This user will not be granted any admin access as only used as a pre-shared key

[Configuration - Security > Users > User 10 - 14 > User 10](#)



Username:	<input type="text" value="initiator"/>
Password:	<input type="password" value="password"/>
Confirm Password:	<input type="password" value="password"/>
Access Level:	<input type="text" value="None"/>

Click **Apply**.

3.7 VPN Responder (WR44) Analayser.

Browse to **Management - Analyser > Settings**

Configure the following settings -

Parameter	Setting	Description
Enable Analyser	✓	Turn on the analyser
Max packet capture size	1500	Capture any packet up to 1500 Bytes
Log Size	180	The maximum size of the log file in kilobytes
Enable IKE Debug	✓	When this is ticked we will see IKE debug in the trace
IP Source	Eth 0	Enable logging for this interface
IP Source	PPP 1	Enable logging for this interface
IP Packet filter ports	500, 4500	Restrict the ports logged to show only IKE and IPSec

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 3
 ☐ ASY 4
 ☐ 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

IP Options

☐ Trace discarded packets
 ☐ Trace loopback packets

Ethernet Packet Filters

MAC Addresses:

IP Packet Filters

TCP/UDP Ports:
 IP Protocols: ~500,4500
 IP Addresses:

Discarded IP Packet Filters

TCP/UDP Ports:
 IP Protocols:
 IP Addresses:

Apply

Click **Apply** and then **Save**.

4 TESTING

4.1 Successful connection:

4.1.1 Initiator (WR21) Log:

The Event Log may be found under **Management – Event Log**.

The event log shows the events occurring within the operating system. Here is a successful IPsec connection from the Initiator point of view.

Management - Event Log

```
19:37:29, 08 Jan 2000, (3) IKE SA Removed. Peer: responder, Successful Negotiation
19:37:00, 08 Jan 2000, Eroute 0 VPN up peer: responder
19:37:00, 08 Jan 2000, New IPsec SA created by responder
19:37:00, 08 Jan 2000, (3) IKE Notification: Initial Contact, RX
19:37:00, 08 Jan 2000, (4) IKE Notification: Responder Lifetime, RX
19:36:59, 08 Jan 2000, (3) New Phase 2 IKE Session 166.241.75.182, Initiator
19:36:59, 08 Jan 2000, (2) IKE Keys Negotiated. Peer: responder
19:36:59, 08 Jan 2000, IKE Request Received From Eroute 0
19:36:49, 08 Jan 2000, (2) New Phase 1 IKE Session 166.241.75.182, Initiator
19:36:49, 08 Jan 2000, IKE Request Received From Eroute 0
19:36:49, 08 Jan 2000, (1) IKE SA Removed. Peer: , Negotiation Failure
19:36:49, 08 Jan 2000, (1) IKE Negotiation Failed. Peer: , Retries Exceeded
19:36:39, 08 Jan 2000, IKE Request Received From Eroute 0
19:36:29, 08 Jan 2000, IKE Request Received From Eroute 0
19:36:25, 08 Jan 2000, Network technology changed to LTE
19:36:24, 08 Jan 2000, WEB Login OK by username lvl 0
19:36:24, 08 Jan 2000, DNS Query Failed on [time.etherios.com]
19:36:19, 08 Jan 2000, (1) New Phase 1 IKE Session 166.241.75.182, Initiator
19:36:19, 08 Jan 2000, IKE Request Received From Eroute 0
19:36:19, 08 Jan 2000, Default Route 0 Available, Activation
```

4.1.2 Responder (WR44) Log:

Here is a successful IPsec connection from the Responder point of view.

Management - Event Log

```
14:05:15, 08 Sep 2016, (3) IKE SA Removed. Peer: initiator, Successful Negotiation
14:05:15, 08 Sep 2016, Network technology changed to LTE
14:05:13, 08 Sep 2016, Eroute 0 VPN up peer: initiator
14:05:13, 08 Sep 2016, New IPsec SA created by initiator
14:05:12, 08 Sep 2016, (3) IKE Notification: Initial Contact, RX
14:05:12, 08 Sep 2016, (3) New Phase 2 IKE Session 166.201.91.63, Responder
14:05:11, 08 Sep 2016, (1) IKE Keys Negotiated. Peer: initiator
14:05:11, 08 Sep 2016, (1) New Phase 1 IKE Session 166.201.91.63, Responder
14:05:08, 08 Sep 2016, Default Route 0 Available, Activation
```

4.1.3 IPSEC Security Associations

The IPsec SAs may be found under **Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels**.

When a VPN is successful, the IPsec SAs can be viewed on both the Initiator and the Responder IPsec SAs list. This shows the peer IP, the remote and local networks, the authentication algorithm and time left until keys are again exchanged.

Here is the Initiator (WR21)

[Management - Connections > Virtual Private Networking \(VPN\) > IPsec > IPsec Tunnels](#)

▼ **Virtual Private Networking (VPN)**

▼ **IPsec**

▼ **IPsec Tunnels**

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	VIP	
0	166.241.75.182	10.1.63.0/24	10.1.89.0/24	N/A	MD5	3DES	N/A	0	0	25574	PPP 1	N/A	Remove

[Remove All](#)

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	VIP	
0	166.241.75.182	10.1.63.0/24	10.1.89.0/24	N/A	MD5	3DES	N/A	0	0	25574	PPP 1	N/A	Remove

[Remove All](#)

Outbound V2 SAs
No Tunnels

Inbound V2 SAs
No Tunnels

[Refresh](#)

Here is the Responder (WR44)

[Management - Connections > Virtual Private Networking \(VPN\) > IPsec > IPsec Tunnels](#)

► **IP Connections**

► **PPP Connections**

▼ **Virtual Private Networking (VPN)**

▼ **IPsec**

▼ **IPsec Tunnels**

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	VIP	
0	166.201.91.63	10.1.89.0/24	10.1.63.0/24	N/A	MD5	3DES	N/A	0	0	25316	PPP 1	N/A	Remove

[Remove All](#)

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	VIP	
0	166.201.91.63	10.1.89.0/24	10.1.63.0/24	N/A	MD5	3DES	N/A	0	0	25316	PPP 1	N/A	Remove

[Remove All](#)

Outbound V2 SAs
No Tunnels

Inbound V2 SAs
No Tunnels

[Refresh](#)

4.1.4 IPsec Peers

The IPsec Peers may be found under **Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Peers**.

This is the list of remote devices that have successfully negotiated an IPsec tunnel with the router.

Here is the Initiator (WR21)

[Management - Connections](#) > [Virtual Private Networking \(VPN\)](#) > [IPsec](#) > [IPsec Peers](#)

▶ IP Connections						
▶ PPP Connections						
▼ Virtual Private Networking (VPN)						
▼ IPsec						
▶ IPsec Tunnels						
▼ IPsec Peers						
Peer IP Address	Our ID	Peer ID	Dead Peer Detection (DPD)	NATT Local Port	NATT Remote Port	
166.241.75.182	initiator	responder	Inactive. Next REQ in 25 secs	N/A	N/A	
Remove all unused						

Here is the Responder (WR44)

[Management - Connections](#) > [Virtual Private Networking \(VPN\)](#) > [IPsec](#) > [IPsec Peers](#)

▶ IP Connections						
▶ PPP Connections						
▼ Virtual Private Networking (VPN)						
▼ IPsec						
▶ IPsec Tunnels						
▶ Dynamic IPsec tunnels						
▼ IPsec Peers						
Peer IP Address	Our ID	Peer ID	Dead Peer Detection (DPD)	NATT Local Port	NATT Remote Port	
166.201.91.63	responder	initiator	Inactive. Next REQ in 67 secs	N/A	N/A	
Remove all unused						

4.1.5 IKE SAs

The IKE SAs may be found under **Management - Connections > Virtual Private Networking (VPN) > IPsec > IKE SAs**.

This displays the current status of the IKE Security Associations (SA).

Here is the Initiator (WR21)

[Management - Connections](#) > [Virtual Private Networking \(VPN\)](#) > [IPsec](#) > [IKE SAs](#)

▶ IP Connections

▶ PPP Connections

▼ Virtual Private Networking (VPN)

▼ IPsec

▶ IPsec Tunnels

▶ IPsec Peers

▼ IKE SAs

IKEv1 SAs

Our ID	Peer ID	Peer IP Address	Our IP Address	Time Left (secs)	Session ID	Internal ID	
initiator	responder	166.241.75.182	166.201.91.63	25424	0x0	2	Remove

Refresh

Remove All V1 SAs

IKEv2 SAs

No SAs

Here is the Responder (WR44)

[Management - Connections](#) > [Virtual Private Networking \(VPN\)](#) > [IPsec](#) > [IKE SAs](#)

▶ IP Connections
▶ PPP Connections
▼ Virtual Private Networking (VPN)

▼ IPsec

▶ IPsec Tunnels
▶ Dynamic IPsec tunnels
▶ IPsec Peers
▼ IKE SAs

IKEv1 SAs

Our ID	Peer ID	Peer IP Address	Our IP Address	Time Left (secs)	Session ID	Internal ID	
responder	initiator	166.201.91.63	166.241.75.182	25218	0x0	1	Remove

Refresh
Remove All V1 SAs

IKEv2 SAs

No SAs

5 CONFIGURATION & FIRMWARE FILES

This section shows the configuration files on each side of our example.

5.1 Digi Transport WR21 (Initiator) Configuration

```
eth 0 IPAddr "10.1.63.254"
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 peerip "166.241.75.182"
eroute 0 peerid "responder"
eroute 0 ourid "initiator"
eroute 0 locip "10.1.63.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "10.1.89.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "MD5"
eroute 0 ESPenc "3DES"
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"
eroute 0 autosa 1
eroute 0 dhgroup 2
dhcp 0 IPmin "10.1.63.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "10.1.63.254"
dhcp 0 DNS "10.1.63.254"
sntp 0 server "time.etherios.com"
ppp 0 timeout 300
ppp 1 name "W-WAN"
ppp 1 phonenum "*98*3#"
ppp 1 username "username"
ppp 1 epassword "KDSISVJDVVg="
ppp 1 IPAddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 ipsec 1
ppp 1 firewall ON
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
```

5.2 Digi Transport WR44 (Responder) Configuration

```
eth 0 IPAddr "10.1.89.254"
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
gps 0 asy_add 1
gps 0 gpson ON
ip 0 cidr ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 peerid "initiator"
eroute 0 ourid "responder"
eroute 0 locip "10.1.89.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "10.1.63.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "MD5"
eroute 0 ESPenc "3DES"
eroute 0 authmeth "PRESHARED"
eroute 0 dhgroup 2
dhcp 0 IPmin "10.1.89.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "10.1.89.254"
dhcp 0 DNS "10.1.89.254"
dhcpcli 0 idismac ON
sntp 0 server "time.digi.com"
ppp 0 timeout 300
ppp 1 name "W-WAN"
ppp 1 phonenum "*98*3#"
ppp 1 username "username"
ppp 1 epassword "KD5ISVJDVVg="
ppp 1 IPAddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 ipsec 1
ppp 1 firewall ON
ppp 1 use_modem 1
ppp 1 cdma_backoff ON
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 pwr_dly 40
ppp 1 ipanon ON
ppp 1 r_chap OFF
```

5.3 Digi Transport WR21 (Initiator) Firmware

```
Digi TransPort WR21-L52A-DE1-XX Ser#:293824 HW Revision: 1201a
Software Build Ver5.2.15.4. Jun 22 2016 12:23:54 WW
ARM Bios Ver 7.56u v43 454MHZ B987-M995-F80-00,0 MAC:00042d047bc0
Power Up Profile: 0
Async Driver Revision: 1.19 Int clk
Ethernet Port Isolate Driver Revision: 1.11
Firewall Revision: 1.0
EventEdit Revision: 1.0
Timer Module Revision: 1.1
(B)USBHOST Revision: 1.0
L2TP Revision: 1.10
PPTP Revision: 1.00
TACPLUS Revision: 1.00
MODBUS Revision: 0.00
RealPort Revision: 0.00
MultiTX Revision: 1.00
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
GPS Revision: 1.0
TELITUPD Revision: 1.0
SCRIBATSK Revision: 1.0
BASTSK Revision: 1.0
PYTHON Revision: 1.0
CLOUDSMS Revision: 1.0
TCP (HASH mode) Revision: 1.14
TCP Utils Revision: 1.13
PPP Revision: 5.2
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 (SIERRA LTE) Revision: 5.2
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
PWRCTRL Revision: 1.0
RADIUS client Revision: 1.0
SSH Server Revision: 1.0
SCP Revision: 1.0
SSH client Revision: 1.0
CERT Revision: 1.0
LowPrio Revision: 1.0
Tunnel Revision: 1.2
OVPN Revision: 1.2
TEMPLOG Revision: 1.0
QDL Revision: 1.0
OK
```


5.4 Digi Transport WR44 (Responder) Firmware

```
Digi TransPort WR44-L5G1-NE1-SU Ser#:387507 HW Revision: 2202a
Software Build Ver5.2.15.4. Jun 22 2016 12:24:12 LW
ARM Bios Ver 7.56u v45 800MHZ B995-M1003-F80-00,0 MAC:00042d05e9b3
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
(B)USBHOST Revision: 1.0
L2TP Revision: 1.10
PPTP Revision: 1.00
TACPLUS Revision: 1.00
MODBUS Revision: 0.00
MySQL Revision: 0.01
RealPort Revision: 0.00
MultitX Revision: 1.00
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
GPS Revision: 1.0
TELITUPD Revision: 1.0
SCRIBATSK Revision: 1.0
BASTSK Revision: 1.0
PYTHON Revision: 1.0
CLOUDSMS Revision: 1.0
ARM sync Driver Revision: 1.18
TCP (HASH mode) Revision: 1.14
TCP Utils Revision: 1.13
PPP Revision: 5.2
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 (SIERRA LTE) Revision: 5.2
FLASH Write Revision: 1.2
Command Interpreter Revision: 1.38
SSCLI Revision: 1.0
OSPF Revision: 1.0
BGP Revision: 1.0
QOS Revision: 1.0
PWRCTRL Revision: 1.0
RADIUS Client Revision: 1.0
SSH Server Revision: 1.0
SCP Revision: 1.0
SSH Client Revision: 1.0
CERT Revision: 1.0
LowPrio Revision: 1.0
Tunnel Revision: 1.2
OVPN Revision: 1.2
TEMPLOG Revision: 1.0
QDL Revision: 1.0
OK
```

6 VARIOUS COMMENTS/TIPS

The key to VPNs: Make sure that the settings match on both ends of the connection.

If you are using pre-shared keys, be sure to add a user, with the ID of the remote side and the PSK as described in sections 2.6 (initiator) and 3.6 (responder) of this document. Again, the PSK must match on both ends.

NAT Traversal (NAT-T) is required for plans with private IP addresses which are NAT'd by the provider, this necessitates that the remote TransPort sends keep-alive data on a regular basis.

Aggressive Mode must be used for your IKE settings if the wireless plan can only provide dynamic addresses as it is not possible to know the IP address of the interface when creating the configuration.

Note that there is an IPsec Tunnel Wizard available that will create simple Aggressive Mode IPsec Tunnels.

NAT-Traversal, within the advanced settings of IKE, may need to be enabled if one end of the IPsec tunnel is behind a NAT box in order for the tunnel to pass packets.

7 VPN INITIATOR (DSL CONNECTION) CONFIGURATION

In this example a DSL link is used, this link provided a static IP for the host Digi Transport. IPsec is enabled on this interface. It is using a WR44 and is the initiator to the same responder as under section 3

For the Responder (WR44) setup, it should be the same as section 3.

7.1 VPN Initiator (WR44) with DSL Setup

For the Initiator (WR44) setup, for this DSL link, please use the following sections:

2.1 VPN Initiator (WR21) Inside Ethernet Interface

2.4 VPN Initiator (WR21) Phase 1-IKE

2.5 VPN Initiator (WR21) Phase 2 – IPsec

2.6 VPN Initiator (WR21) Pre-shared Key

2.7 VPN Initiator (WR21) Configure Packet Analyser for Debugging – Please note, use PPP 3 rather than PPP 1 under the IP Source.

7.2 VPN Initiator (WR44) ADSL PPP Interface

In addition, for the Initiator (WR44), please do the following:

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

Parameter	Setting	Description
Username	Your username goes here	ADSL access username
Password	password	ADSL access password
Confirm Password	password	Confirm ADSL access password
Enable IPsec	✓	Enable IPsec on PPP 1 interface
Keep (SAs) when this PPP interface is disconnected	✓	Keep the SAs when PPP 1 interface becomes disconnected

Description:

This PPP interface will use

Dial out using

numbers:

Prefix: to the dial out number

Username:

Password:

Confirm password:

☒ Allow the remote device to assign a local IP address to this router

☐ Try to negotiate to use as the local IP address for this router

☐ Use as the local IP address for this router (i.e. not negotiable)

Use mask for this interface

Use the following DNS servers if not negotiated

Primary DNS server:

Secondary DNS server:

DNS Port:

☐ 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 seconds

if it has been up for minutes in a day

if it has been idle for hrs mins secs

Alternative idle timer for static routes seconds

if the link has not received any packets for seconds

if the negotiation is not complete in seconds

☒ Enable NAT on this interface

☐ IP address ☒ IP address and Port

NAT Source IP address:

☒ Enable IPsec on this interface

☒ Keep Security Associations (SAs) when this PPP interface is disconnected

Use interface for the source IP address of IPsec packets

☒ Enable the firewall on this interface

Remote management access:

Click **Apply** and then **Save**.

7.3 Successful Connection

7.3.1 Initiator Log

The Event Log may be found under **Management – Event Log**.

Here is a successful IPsec connection from the Initiator point of view. You can see the DSL interface (PPP 3) establishing followed by the VPN.

Management - Event Log

```
07:07:38, 21 Sep 2016, (2) IKE SA Removed. Peer: responder, Successful Negotiation
07:07:09, 21 Sep 2016, Eroute 0 VPN up peer: responder
07:07:09, 21 Sep 2016, New IPsec SA created by responder
07:07:08, 21 Sep 2016, (2) IKE Notification: Initial Contact, RX
07:07:08, 21 Sep 2016, IKE Request Received From Eroute 0
07:06:58, 21 Sep 2016, (2) New Phase 2 IKE Session 166.241.75.182, Initiator
07:06:58, 21 Sep 2016, (1) IKE Keys Negotiated. Peer: responder
07:06:58, 21 Sep 2016, IKE Request Received From Eroute 0
07:06:48, 21 Sep 2016, (1) New Phase 1 IKE Session 166.241.75.182, Initiator
07:06:48, 21 Sep 2016, IKE Request Received From Eroute 0
07:06:48, 21 Sep 2016, Default Route 0 Available, Activation
07:06:48, 21 Sep 2016, PPP 3 Available, Activation
07:06:48, 21 Sep 2016, PPP 3 up
07:06:48, 21 Sep 2016, PPP 3 Start IPCP
07:06:48, 21 Sep 2016, PPP 3 Start AUTHENTICATE
07:06:45, 21 Sep 2016, PPP 3 Start LCP
07:06:45, 21 Sep 2016, PPP 3 Start
07:06:40, 21 Sep 2016, ATM PVC 0 up
07:06:40, 21 Sep 2016, DSL 0 up
07:06:40, 21 Sep 2016, DSL line: Showtime (1024 kbps down | 544 kbps up)
07:06:37, 21 Sep 2016, PPP 3 down, Max negotiation time
07:06:31, 21 Sep 2016, DSL line: Training
07:06:27, 21 Sep 2016, DNS Query Failed on [time.devicecloud.com]
07:06:24, 21 Sep 2016, DNS Query Failed on [time.devicecloud.com]
07:06:21, 21 Sep 2016, DNS Query Failed on [time.devicecloud.com]
07:06:20, 21 Sep 2016, DSL line: Activating
07:06:18, 21 Sep 2016, DSL line: Idle
```

[Refresh](#)[Clear Log](#)[Open in New Window](#)

7.3.4 IKE SAs

The IKE SAs may be found under **Management - Connections > Virtual Private Networking (VPN) > IPsec > IKE SAs**.

This displays the current status of the IKE Security Associations (SA).

[Management - Connections](#) > [Virtual Private Networking \(VPN\)](#) > [IPsec](#) > [IKE SAs](#)

▶ IP Connections

▶ PPP Connections

▼ Virtual Private Networking (VPN)

▼ IPsec

▶ IPsec Tunnels

▶ Dynamic IPsec tunnels

▶ IPsec Peers

▼ IKE SAs

IKEv1 SAs

Our ID	Peer ID	Peer IP Address	Our IP Address	Time Left (secs)	Session ID	Internal ID	
initiator	responder	166.241.75.182	216.160.3.110	28665	0x0	1	<button>Remove</button>

RefreshRemove All V1 SAs

IKEv2 SAs

No SAs