Application Note 10

IPSec Over Cellular using Digi Transport Routers

With Pre-shared key authentication

September 2020

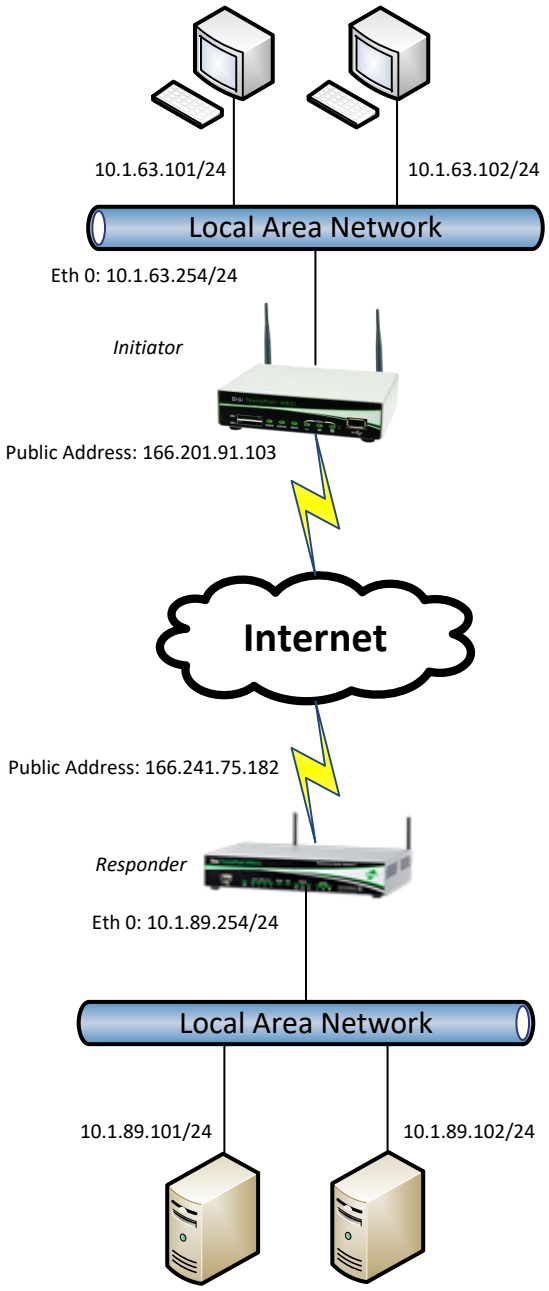
Contents

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@digi.com

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

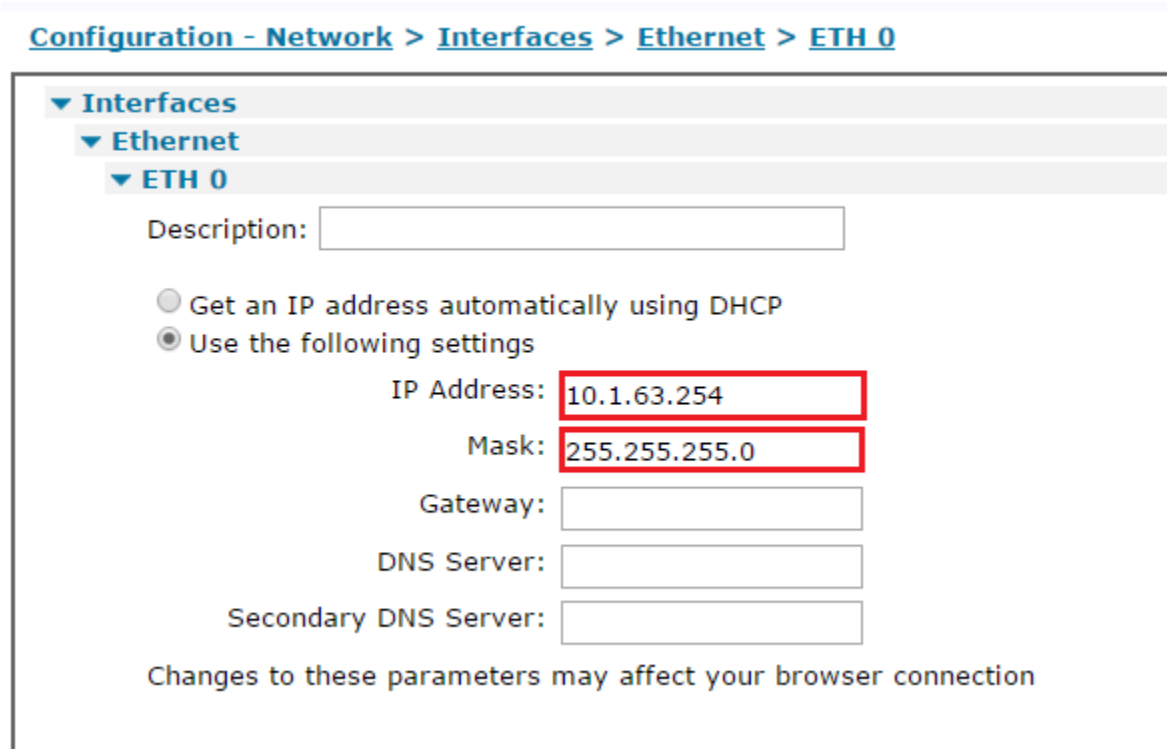
This procedure includes setting up the initial Ethernet interface.

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



Click **Apply**.

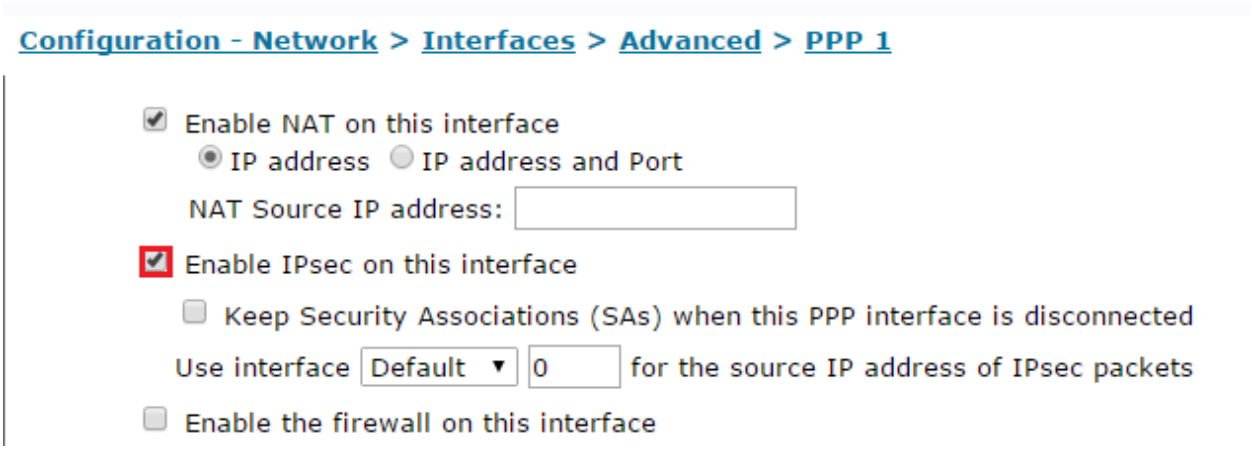
2.2 VPN Initiator (WR21) Cellular PPP Interface

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

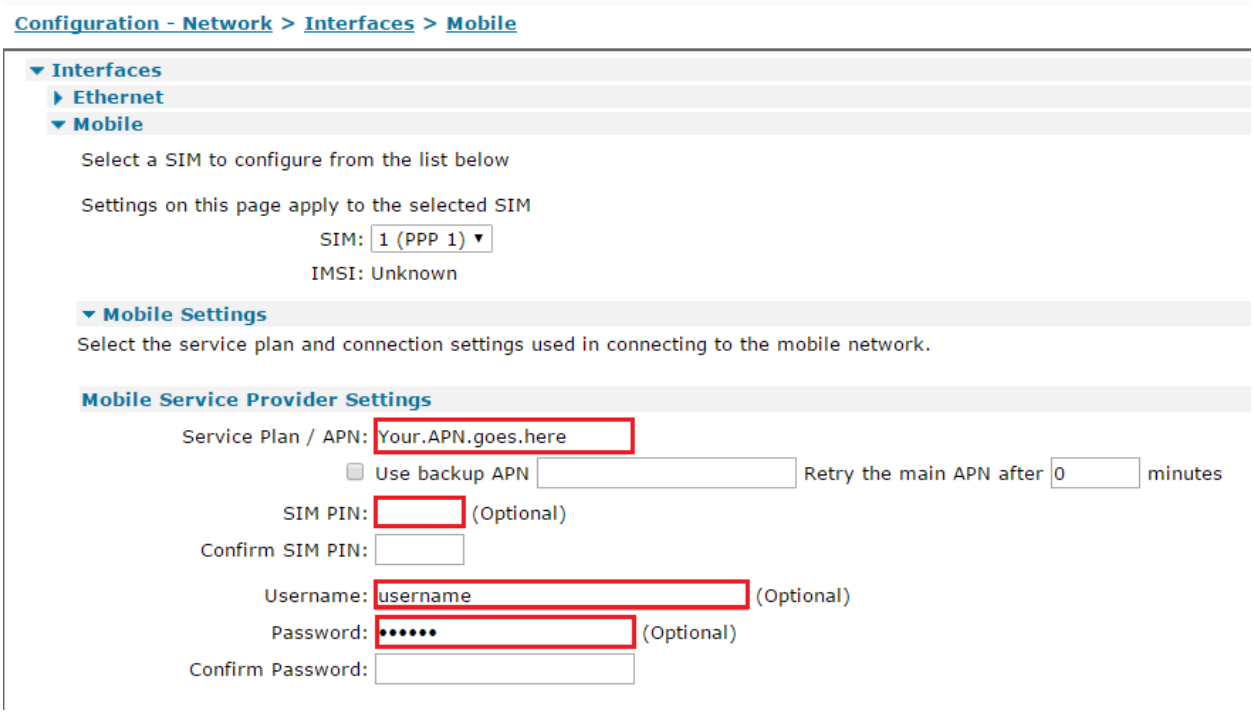


Click **Apply**.

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



Click **Apply**.

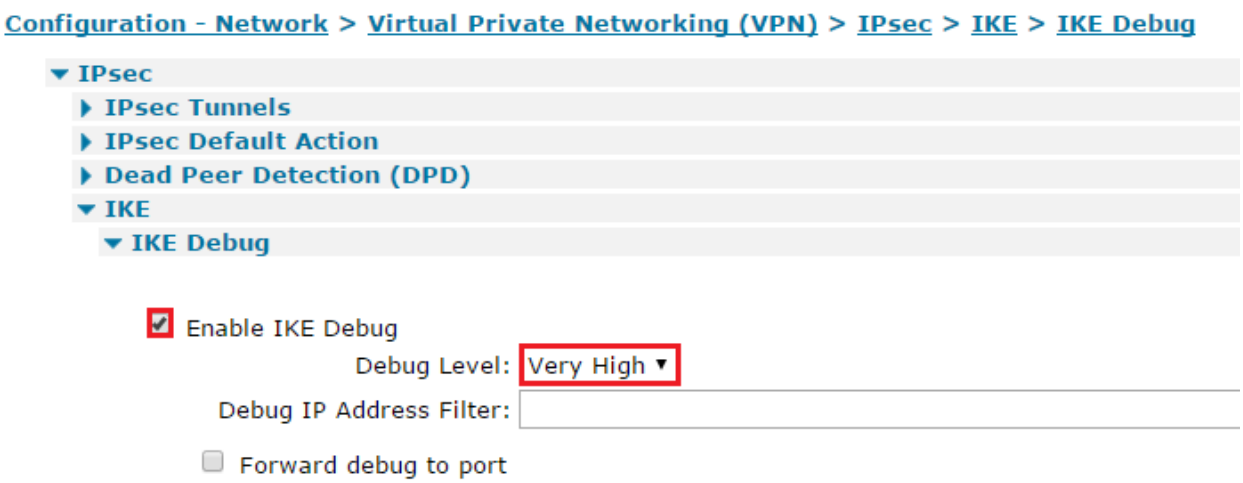
2.4 VPN Initiator (WR21) Phase 1-IKE

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

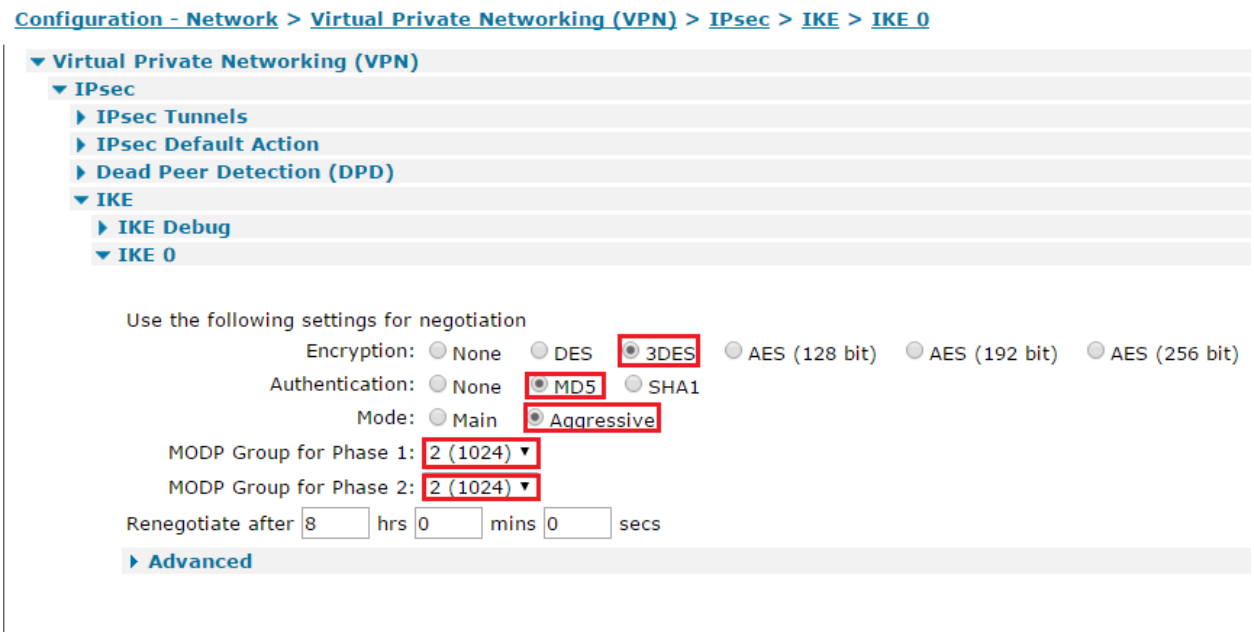


Click **Apply**.

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

And make the following changes:

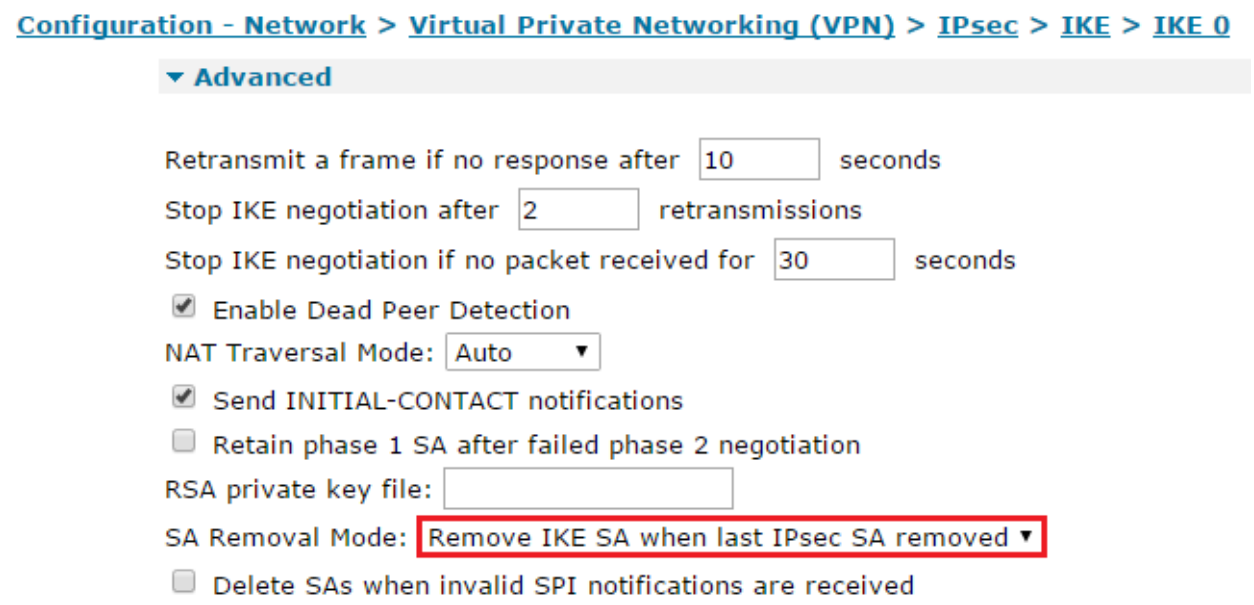
Parameter	Setting	Description
Encryption	3DES	The encryption algorithm to be used for IKE exchanges over the IP connection
Authentication	MD5	The algorithm used to authenticate the IKE session
Mode	Aggressive	Aggressive mode is used in this example
MODP Group for Phase 1	2 (1024)	The key length used 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.



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



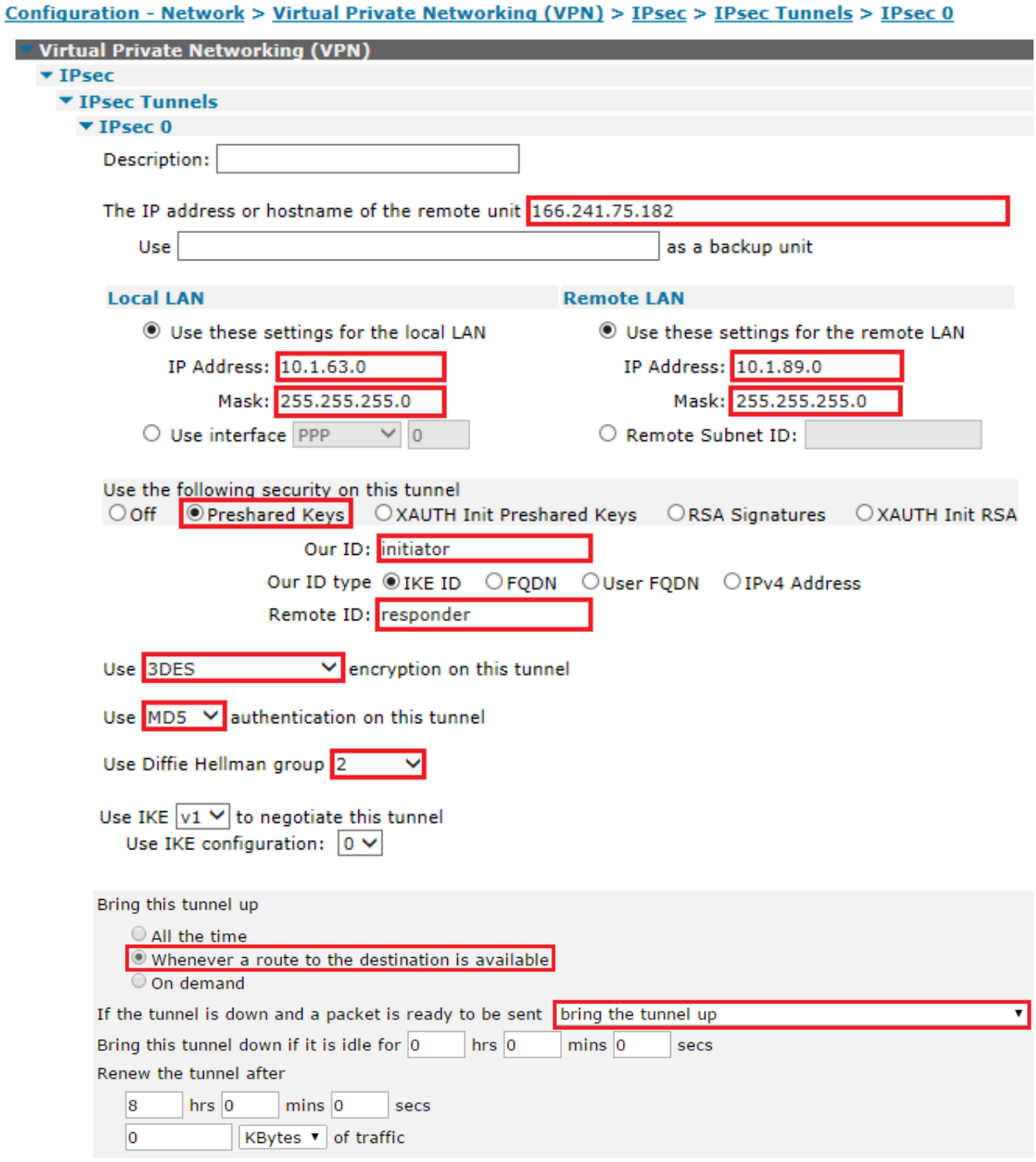
Click **Apply**.

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	


Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0
Virtual Private Networking (VPN)
IPsec
IPsec Tunnels
IPsec 0
Description:
The IP address or hostname of the remote unit 166.241.75.182
Use as a backup unit
Local LAN
Use these settings for the local LAN
IP Address: 10.1.63.0
Mask: 255.255.255.0
Use interface PPP 0
Remote LAN
Use these settings for the remote LAN
IP Address: 10.1.89.0
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: initiator
Our ID type IKE ID FQDN User FQDN IPv4 Address
Remote ID: responder
Use 3DES encryption on this tunnel
Use MD5 authentication on this tunnel
Use Diffie Hellman group 2
Use IKE v1 to negotiate this tunnel
Use IKE configuration: 0
Bring this tunnel up
All the time
Whenever a route to the destination is available
On demand
If the tunnel is down and a packet is ready to be sent bring the tunnel up
Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs
Renew the tunnel after
8 hrs 0 mins 0 secs
0 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

Click **Apply**.

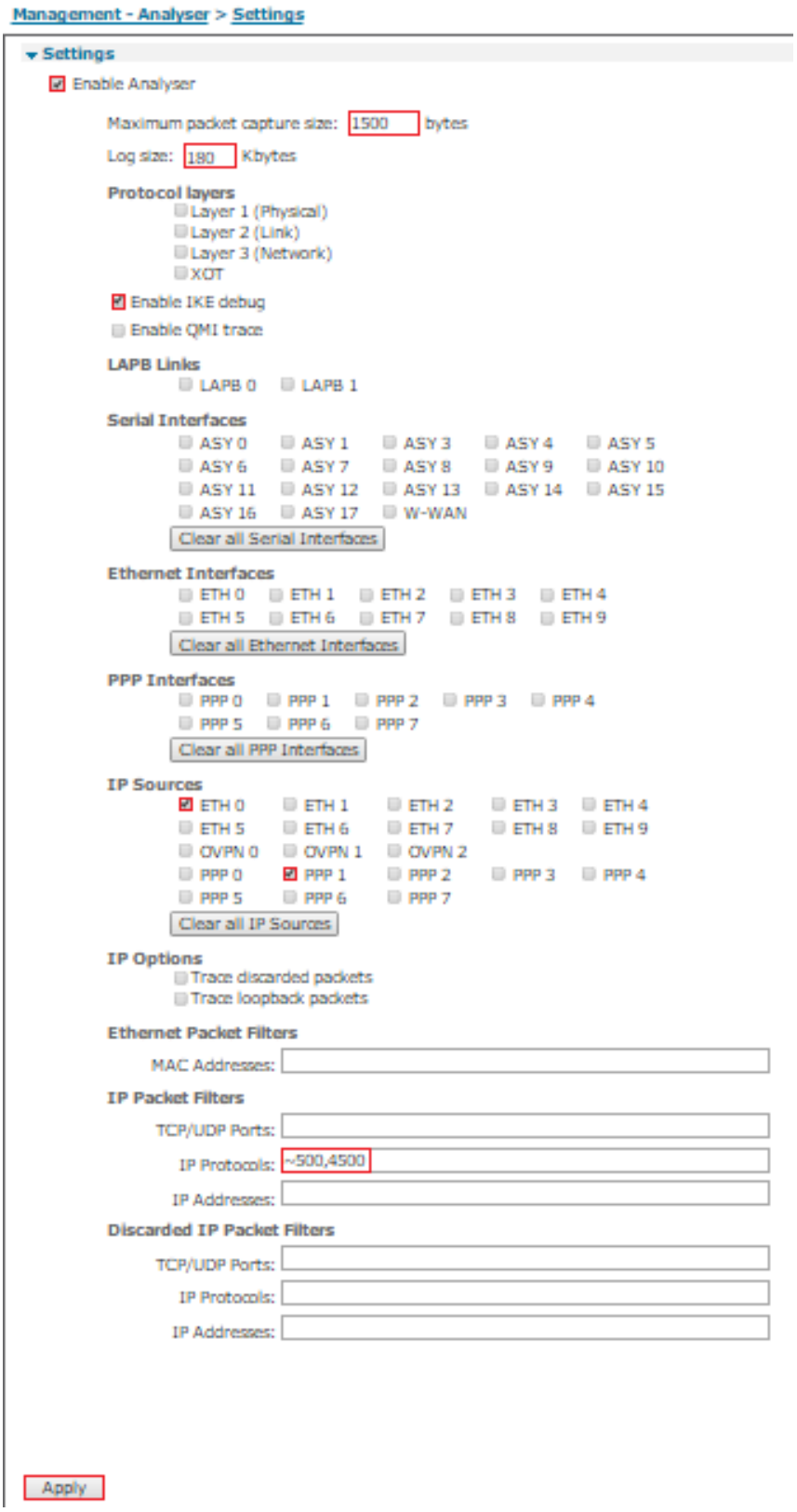
2.7 VPN Initiator (WR21) Configure Packet Analyser for Debugging

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



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

3 VPN RESPONDER (WR44) CONFIGURATION

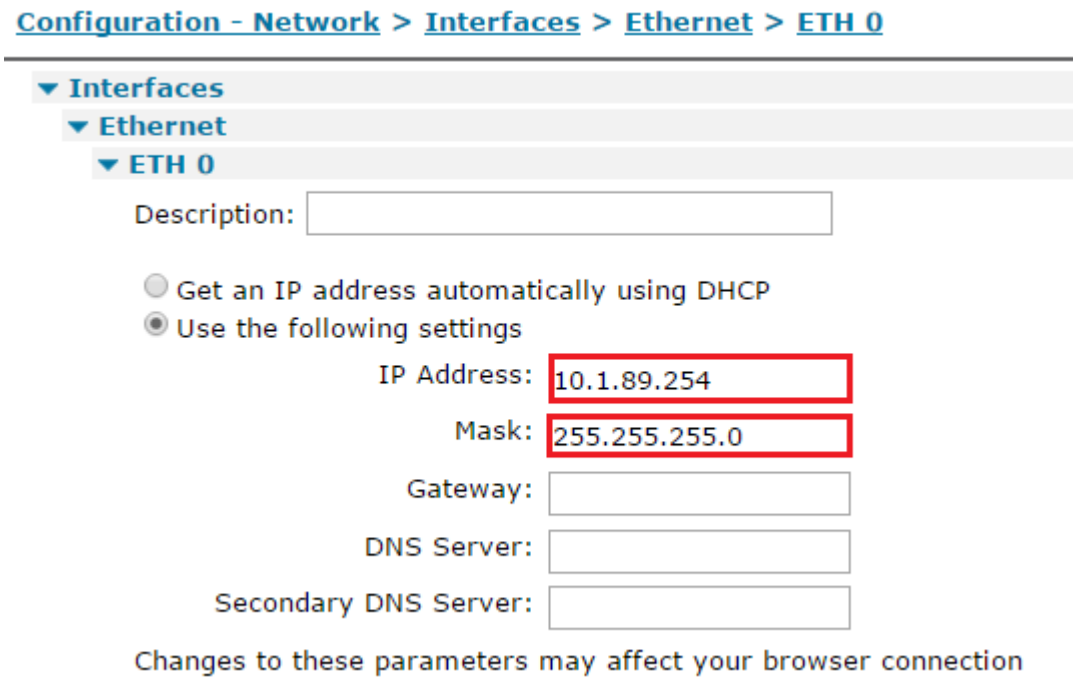
The WR44, in this example, will act as the responder for the IPsec tunnel. Please reference the drawing on page 4.

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



Click **Apply**

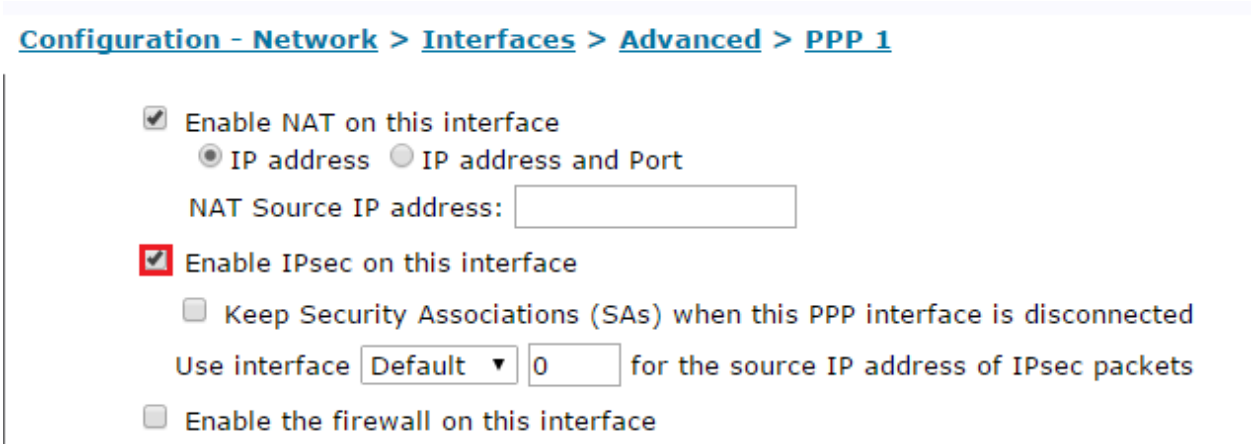
3.2 VPN Responder (WR44) Cellular PPP Interface

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

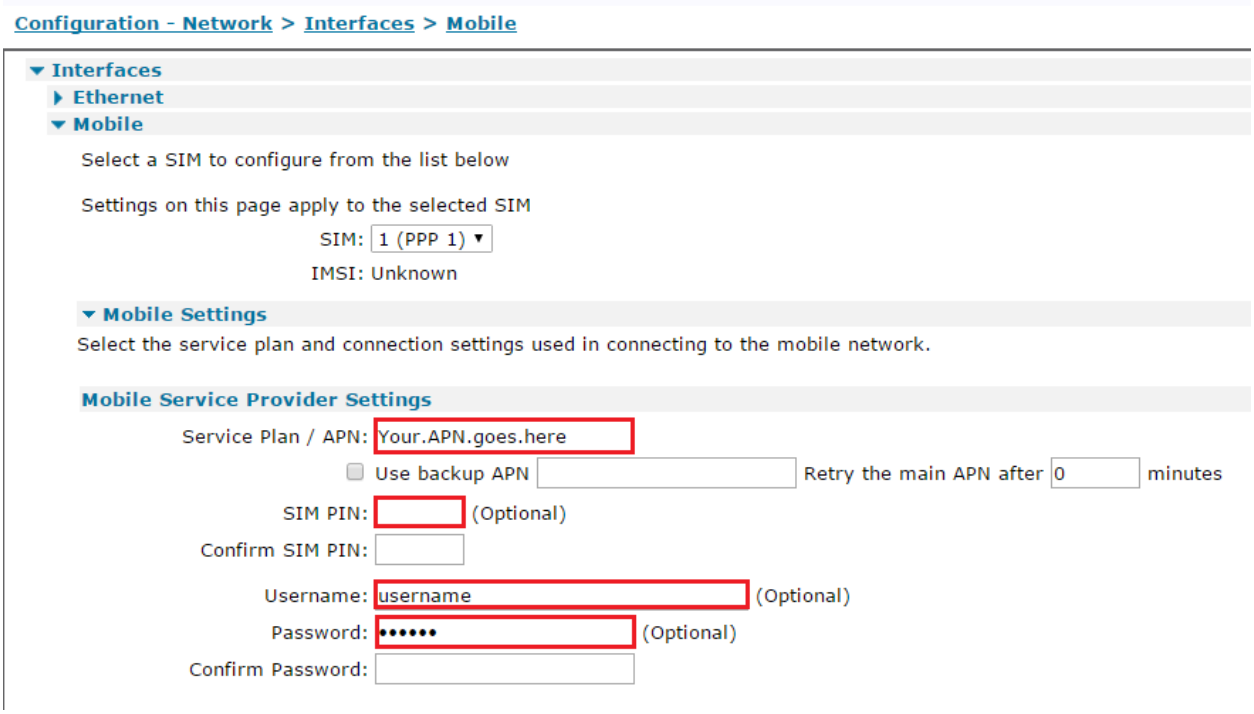


Click **Apply**

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



Click **Apply**

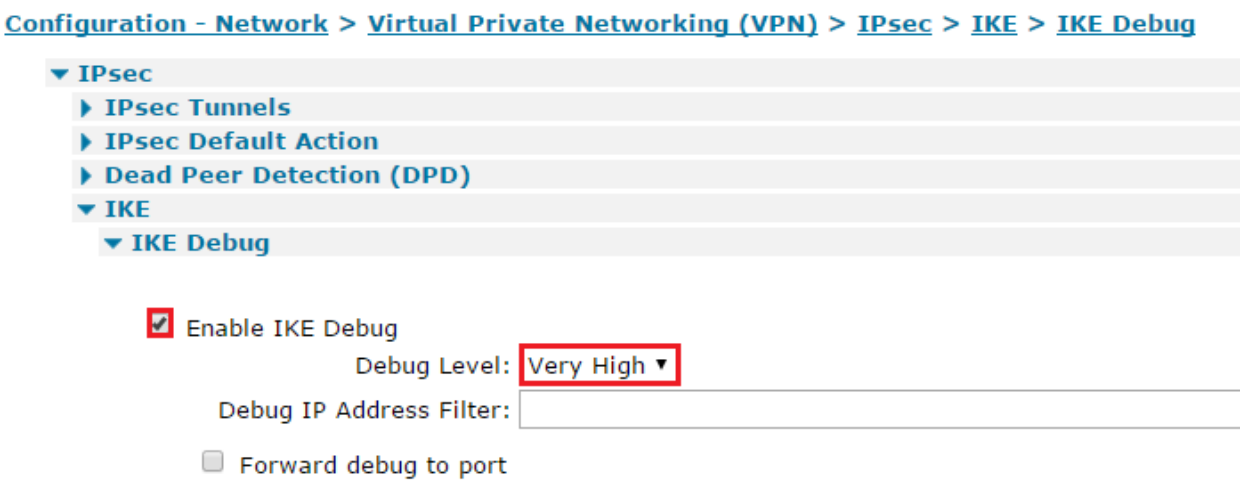
3.4 VPN Responder (WR44) Phase 1-IKE

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

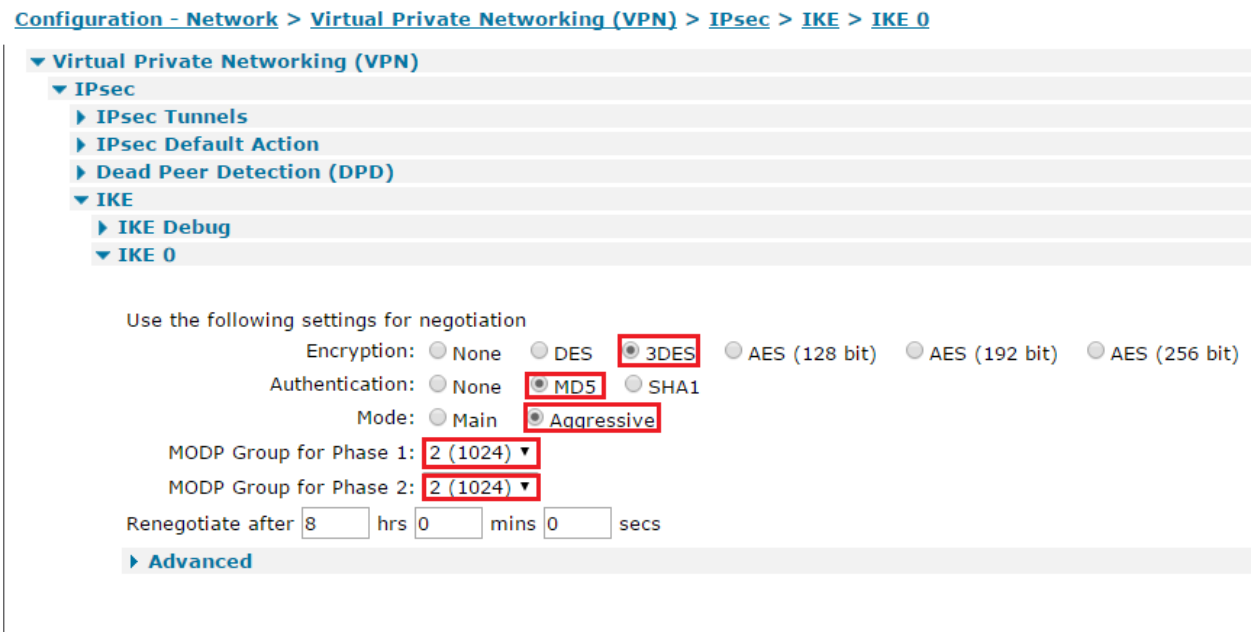


Click **Apply**

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

And make the following changes:

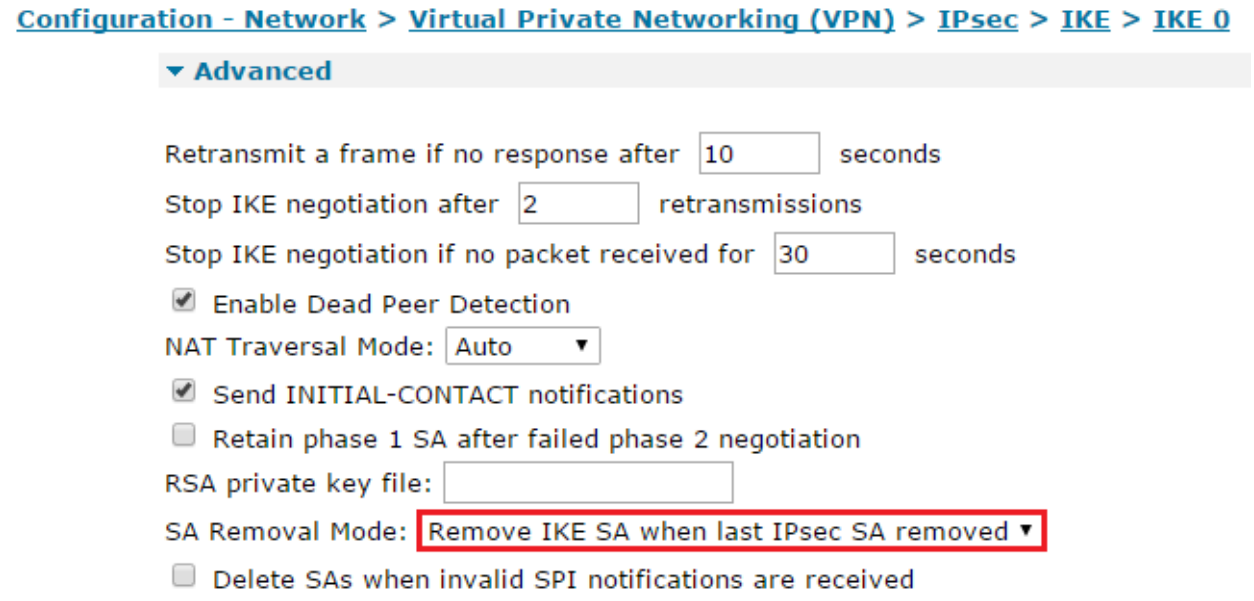
Parameter	Setting	Description
Encryption	3DES	The encryption algorithm to be used for IKE exchanges over the IP connection
Authentication	MD5	The algorithm used to authenticate the IKE session
Mode	Aggressive	Aggressive mode is used in this example
MODP Group for Phase 1	2 (1024)	The key length used 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.



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



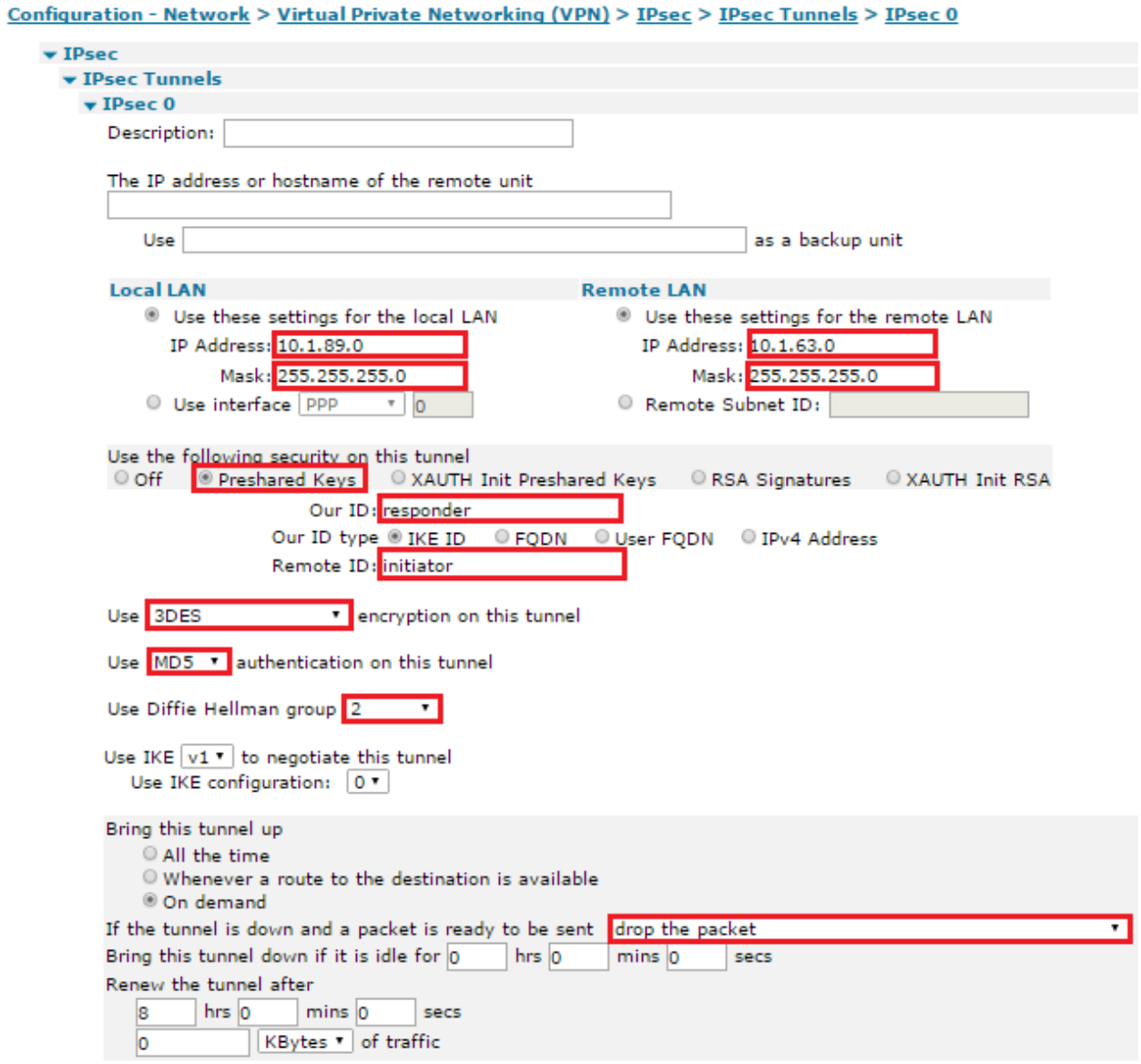
This will delete the IKE SA when all the IPsec SAs that it created to a particular peer are removed.

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	


Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0
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: 10.1.89.0
Mask: 255.255.255.0
Use interface PPP 0
Remote LAN
Use these settings for the remote LAN
IP Address: 10.1.63.0
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: responder
Our ID type IKE ID FQDN User FQDN IPv4 Address
Remote ID: initiator
Use 3DES encryption on this tunnel
Use MD5 authentication on this tunnel
Use Diffie Hellman group 2
Use IKE v1 to negotiate this tunnel
Use IKE configuration: 0
Bring this tunnel up
All the time
Whenever a route to the destination is available
On demand
If the tunnel is down and a packet is ready to be sent drop the packet
Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs
Renew the tunnel after
8 hrs 0 mins 0 secs
0 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

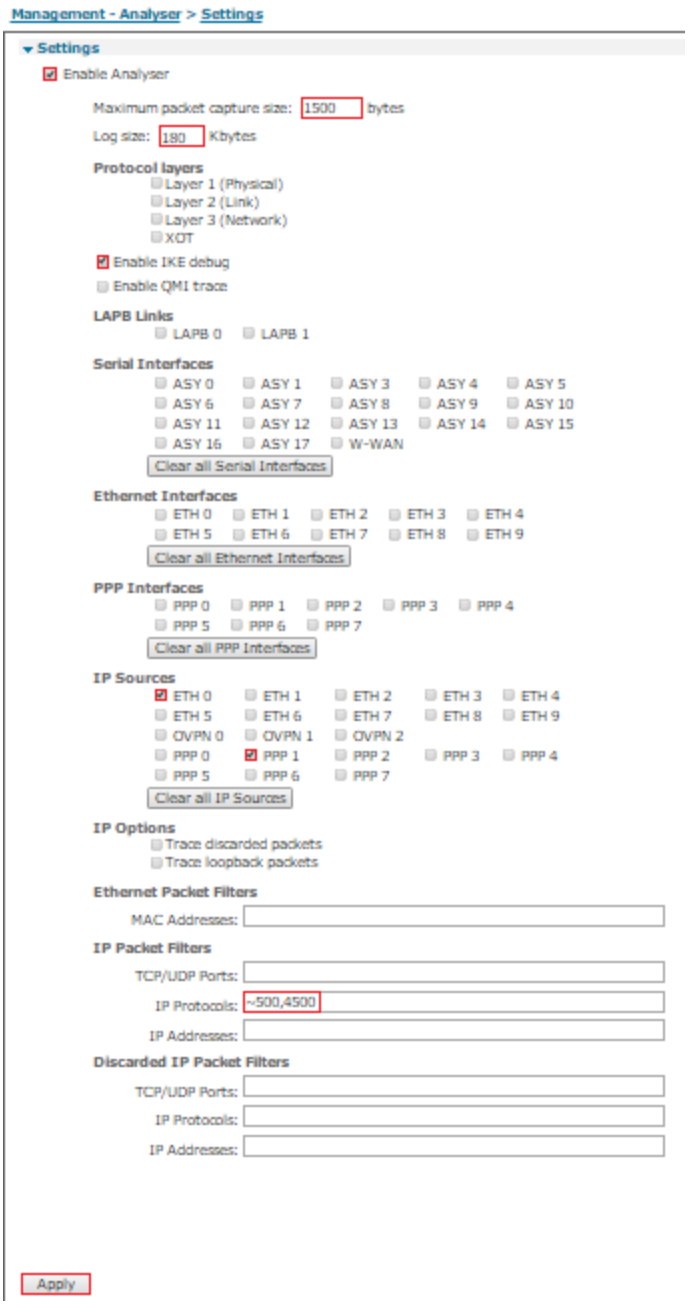
Click **Apply**.

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



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

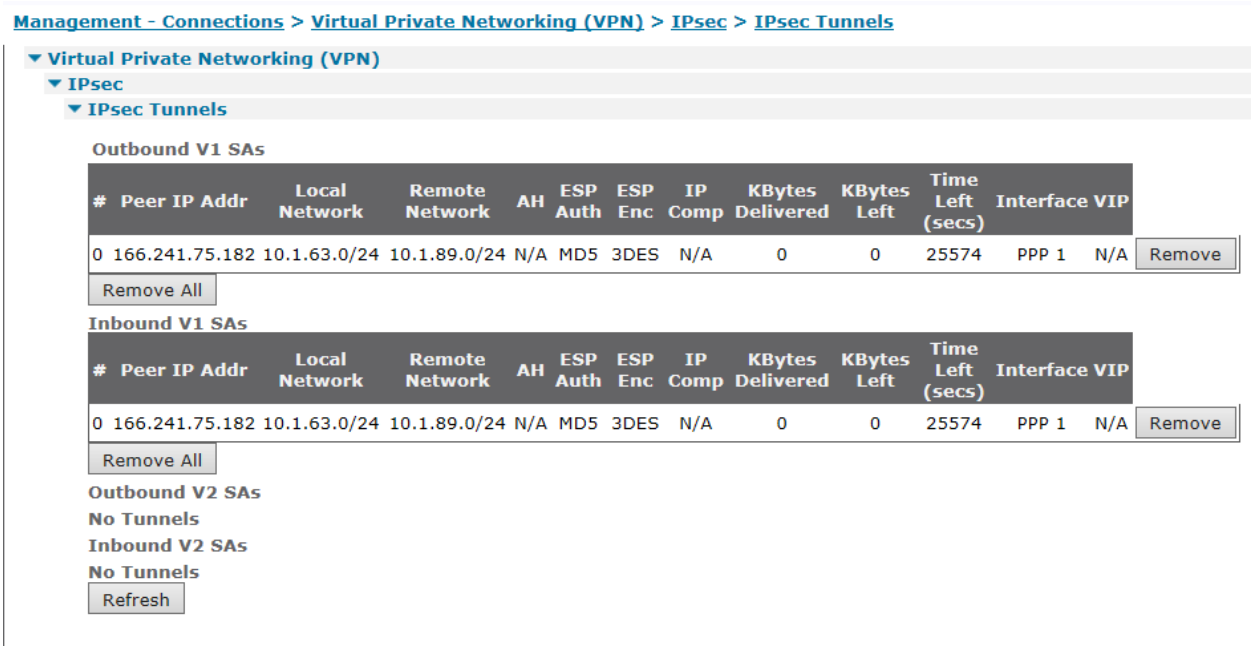
```
14:05:15, 08 Sep 2016,(3) IKE SA Removed. Peer: initiator,Successful Negotiation
14:05:15, 08 Sep 2016,Network technology changed to LTE
14:05:13, 08 Sep 2016,Eroute 0 VPN up peer: initiator
14:05:13, 08 Sep 2016,New IPSec SA created by initiator
14:05:12, 08 Sep 2016,(3) IKE Notification: Initial 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

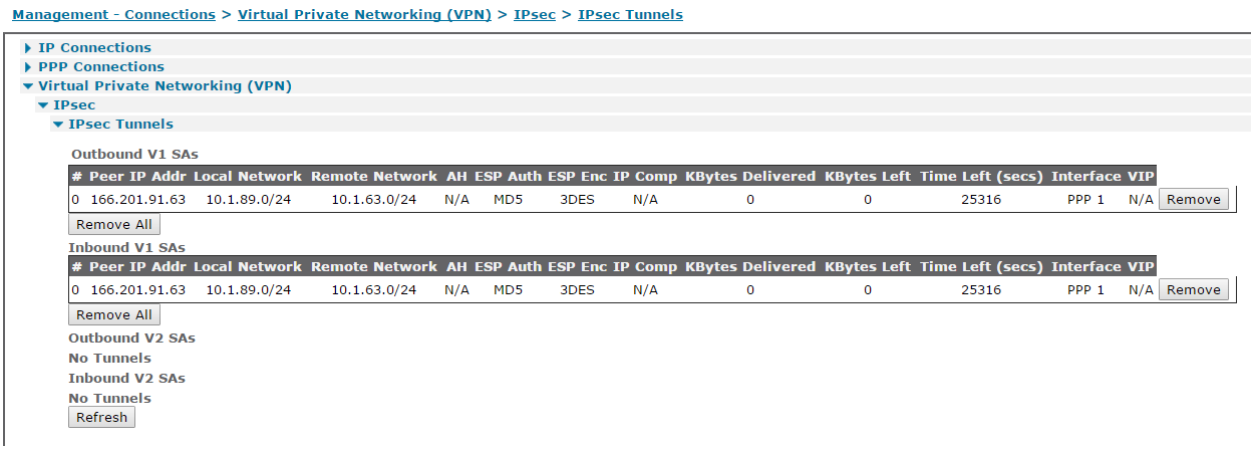
The IPSec SAs may be found under **Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels**.

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)



Here is the Responder (WR44)

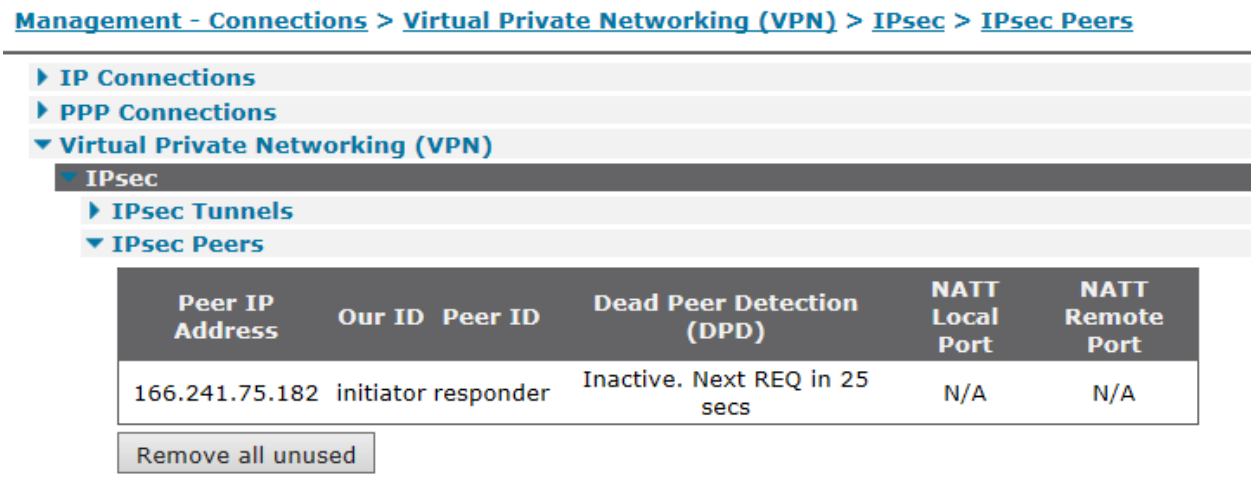


4.1.4 IPsec Peers

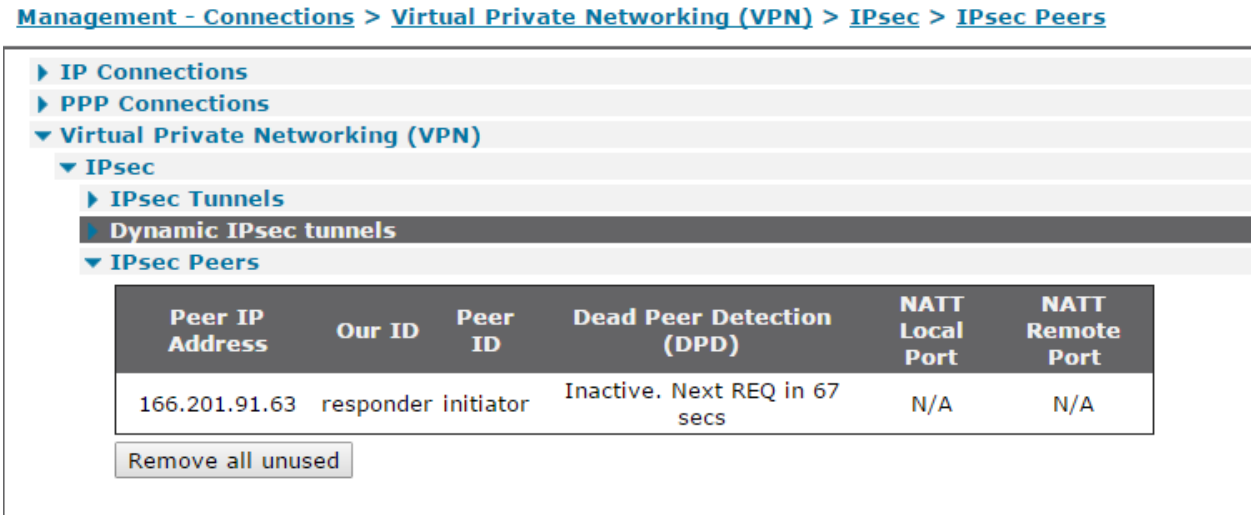
The IPSec Peers may be found under **Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Peers**.

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

Here is the Initiator (WR21)



Here is the Responder (WR44)

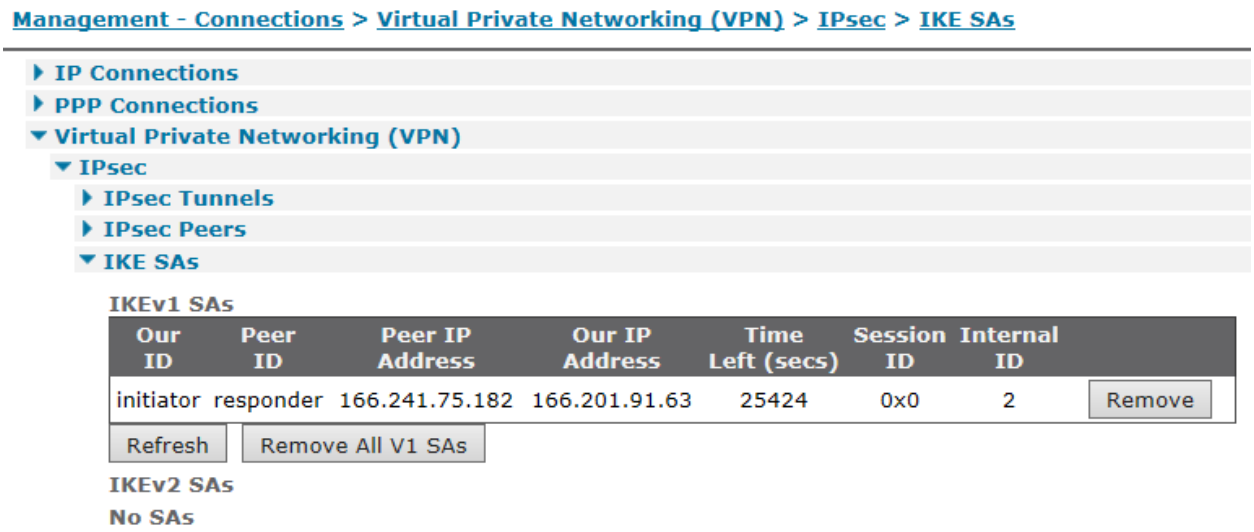


4.1.5 IKE SAs

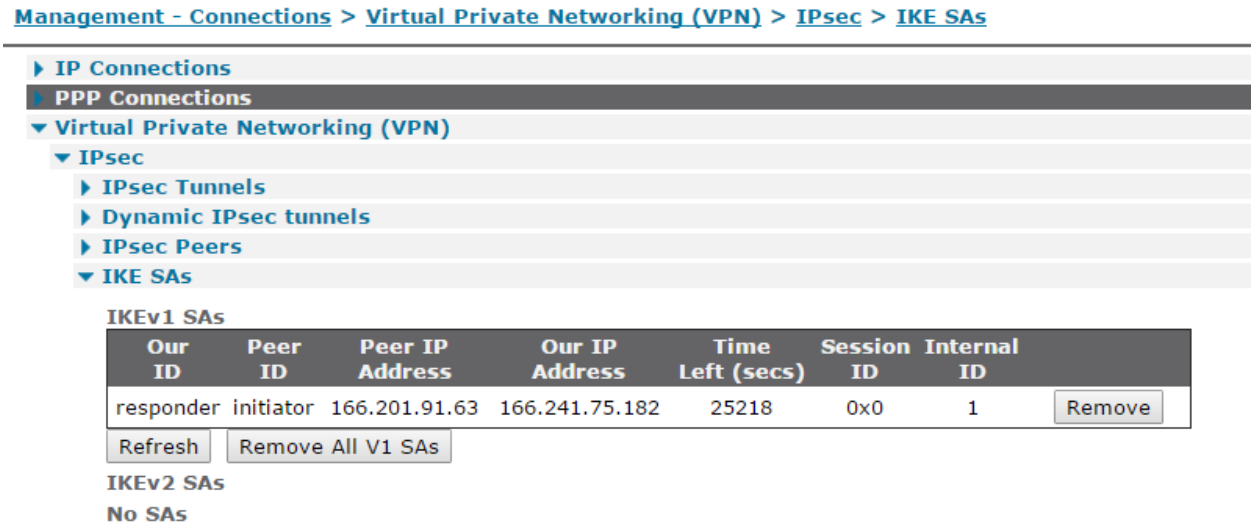
The IKE SAs may be found under **Management - Connections > Virtual Private Networking (VPN) > IPsec > IKE SAs**.

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

Here is the Initiator (WR21)



Here is the Responder (WR44)



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 "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 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
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
```

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

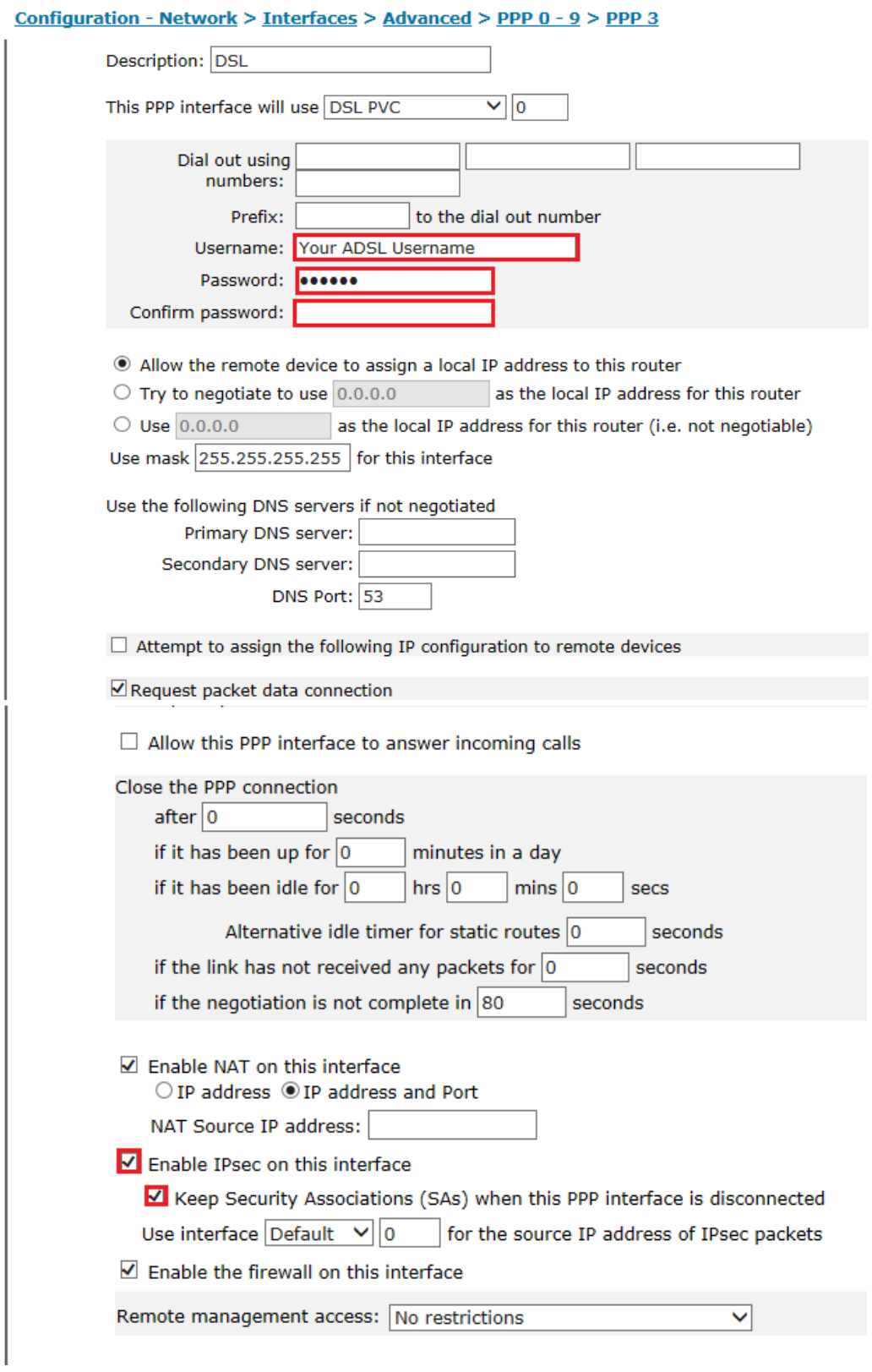
2.7 VPN Initiator (WR21) Configure Packet Analyser for Debugging – Please note, use **PPP 3** rather than **PPP 1** under the **IP Source**.

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



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

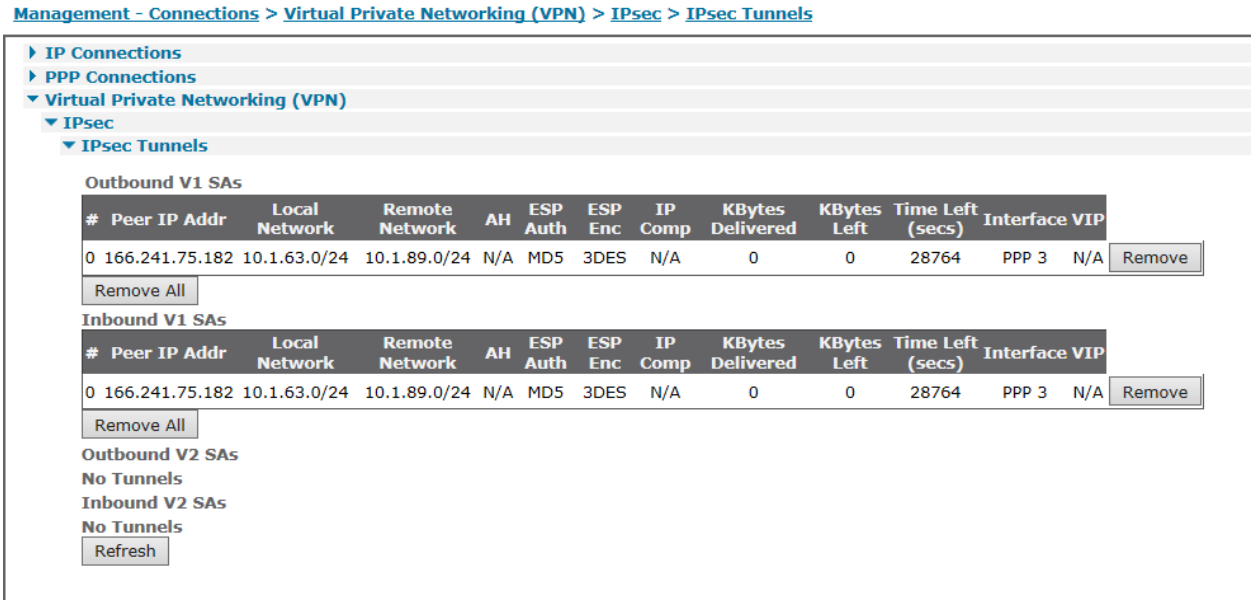
```
07:07:38, 21 Sep 2016,(2) IKE SA Removed. Peer: responder,Successful Negotiation
07:07:09, 21 Sep 2016,Eroute 0 VPN up peer: responder
07:07:09, 21 Sep 2016,New IPSec SA created by responder
07:07:08, 21 Sep 2016,(2) IKE Notification: Initial Contact,RX
07:07:08, 21 Sep 2016,IKE Request Received 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
```

Refresh | Clear Log | Open in New Window

7.3.2 IPSEC Security Associations

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

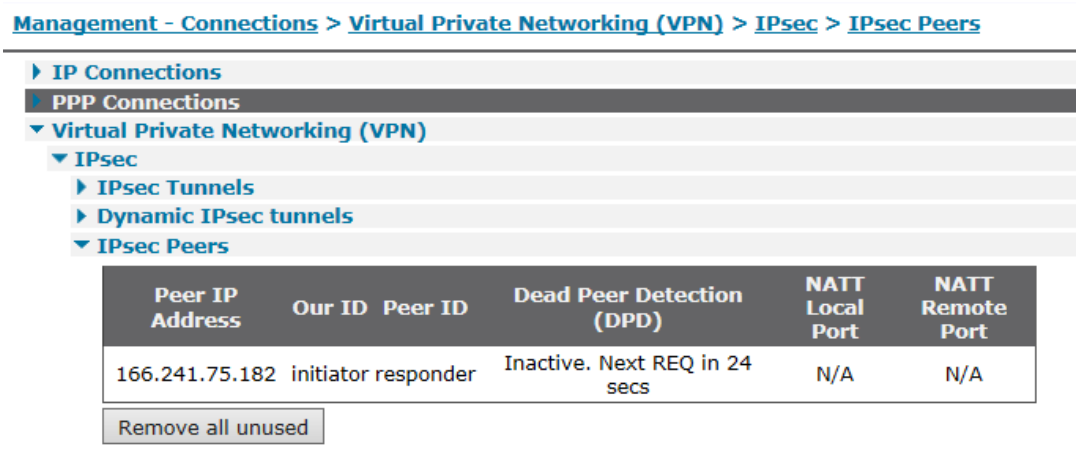
This shows the peer IP, the remote and local networks, the authentication algorithm and time left until keys are again exchanged.



7.3.3 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.



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).