Quick Note

Configure an IPSec VPN tunnel between a TransPort LR router and a TransPort WR router.

Digi Technical Support

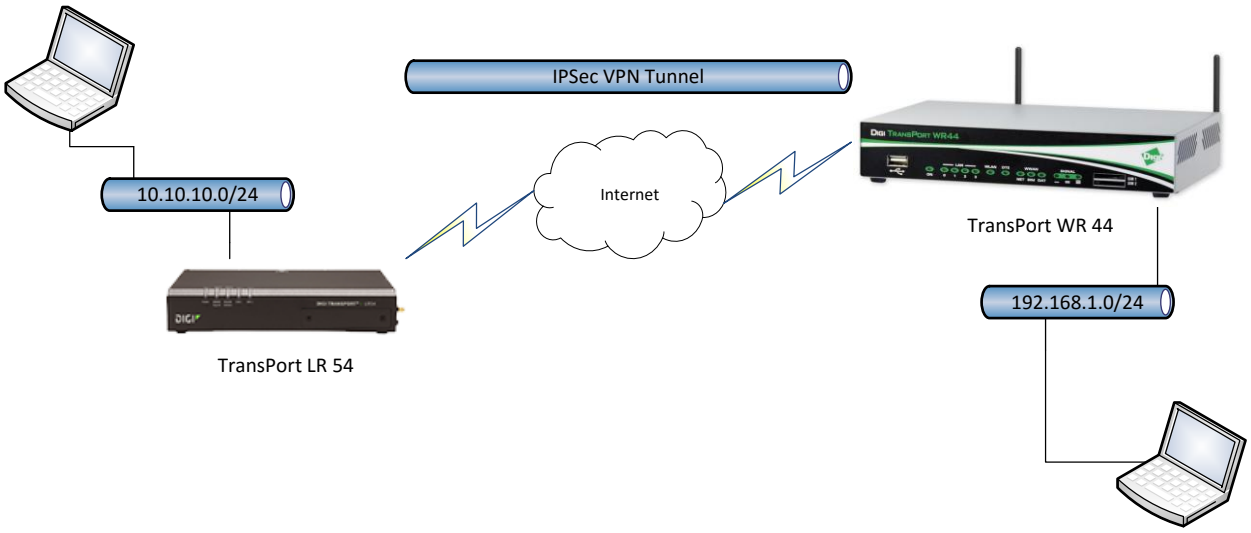
8 June 2017

Contents

1 INTRODUCTION

1.1 Outline

This document will describe how to configure an IPSec VPN tunnel between a TransPort LR54 as the INITIATOR and a TransPort WR router as the RESPONDER. The document will assume that WAN connectivity is configured and available on both units.



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 to:

Model: Digi TransPort LR54 and Digi TransPort WR44

Firmware versions:
LR54: 1.1.0.6 and later
WR44: 2.17.10 and later

Configuration: This document assumes that the devices are set to their factory default configurations. Most configuration commands are shown only if they differ from the factory default.

Please note: This application note has been specifically rewritten for the specified firmware versions and later but will work on earlier versions of firmware. Please contact tech.support@digi.com if your require assistance in upgrading the firmware of the TransPort LR or TransPort WR routers.

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.

2 VERSION

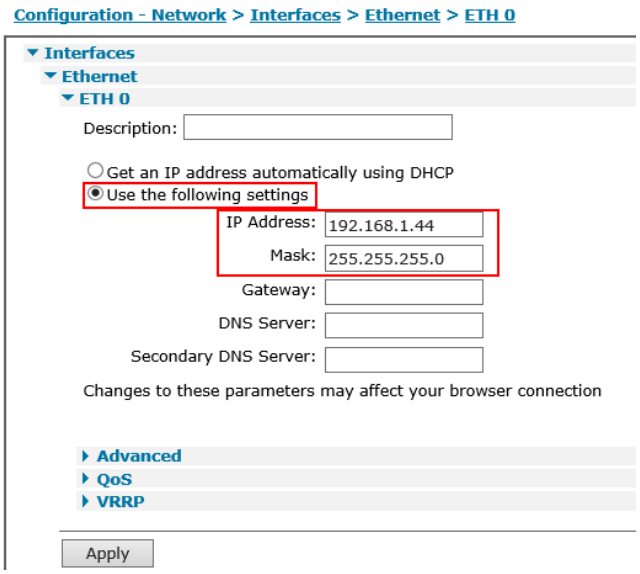
Version Number	Status
1.0	published
1.1	Added notes and firewall rules for MAIN mode and RESPONDER

3 TRANSPORT WR44 CONFIGURATION (RESPONDER)

3.1 Local Ethernet Interface configuration

Navigate to:

Configuration – Network > Interfaces > Ethernet > ETH 0



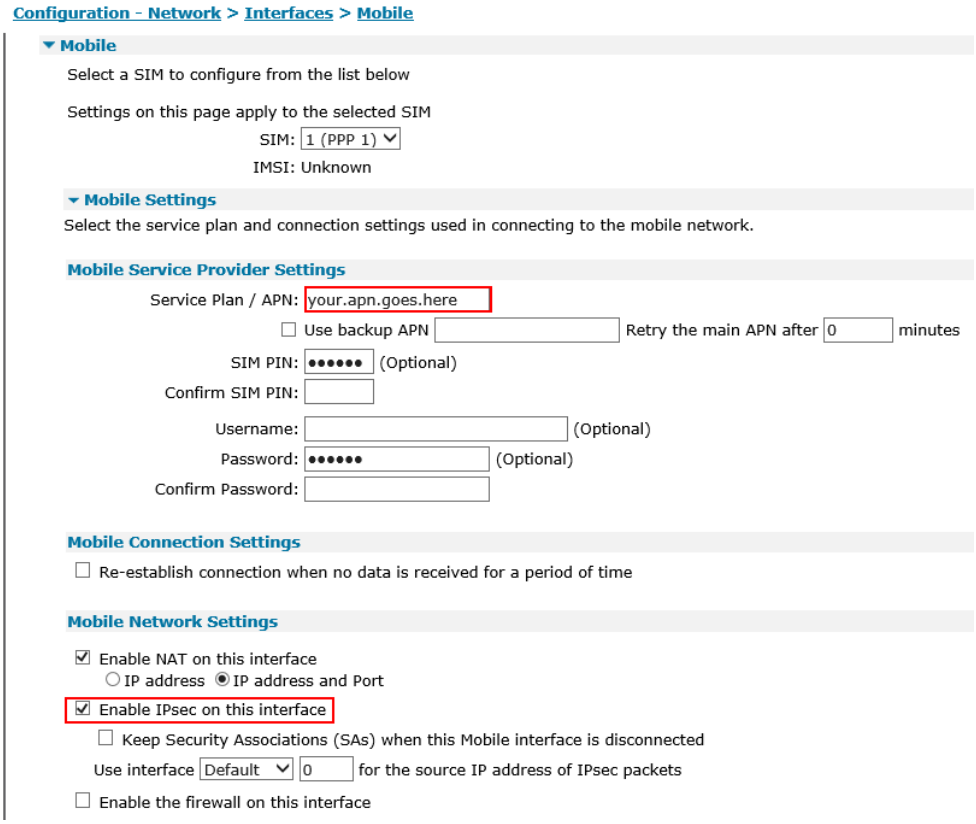
Parameter	Setting	Description
Use the following settings	Checked	A static IP Address will be used in this example
IP Address	192.168.1.44	IP Address of the TransPort WR44 Ethernet Interface. In this example, this IP Address is in the subnet range used for the Tunnel (useful for testing)
Mask	255.255.255.0	Subnet mask

3.2 WAN interface configuration

In this example, the mobile interface will be used as the WAN interface on which the IPsec tunnel will be established.

Navigate to:

Configuration – Network > Interfaces > Mobile



Parameter	Setting	Description
Service Plan / APN	Your.APN.goes.here	Enther the APN of your mobile provider
Enable IPsec on this interface	Checked	Enable IPsec to be built on this WAN interface

Please note: If required, enter a SIM PIN and Username/Password for this SIM card and APN.

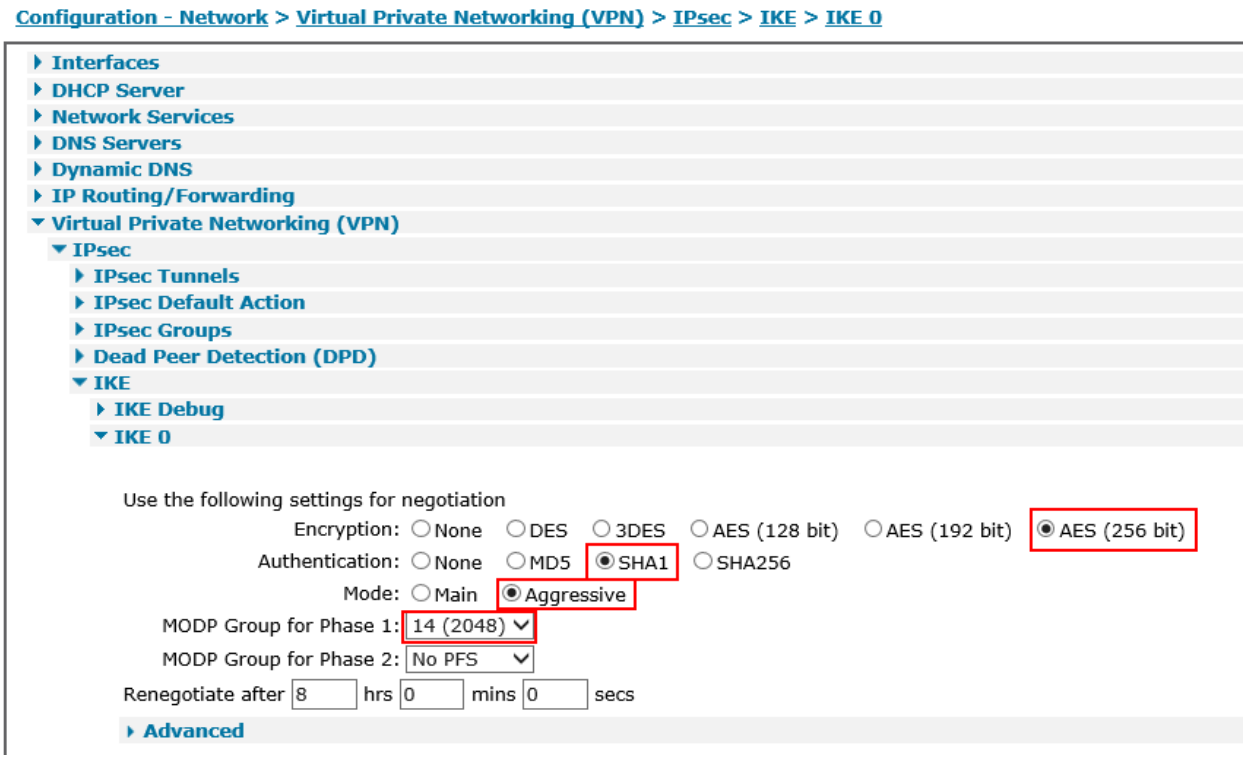
3.3 Tunnel Configuration

Open a web browser to the IP address of the TransPort WR44 router.

3.3.1 Phase 1 Settings

Navigate to:

Configuration – Network > Virtual Private Network (VPN) >IKE > IKE 0

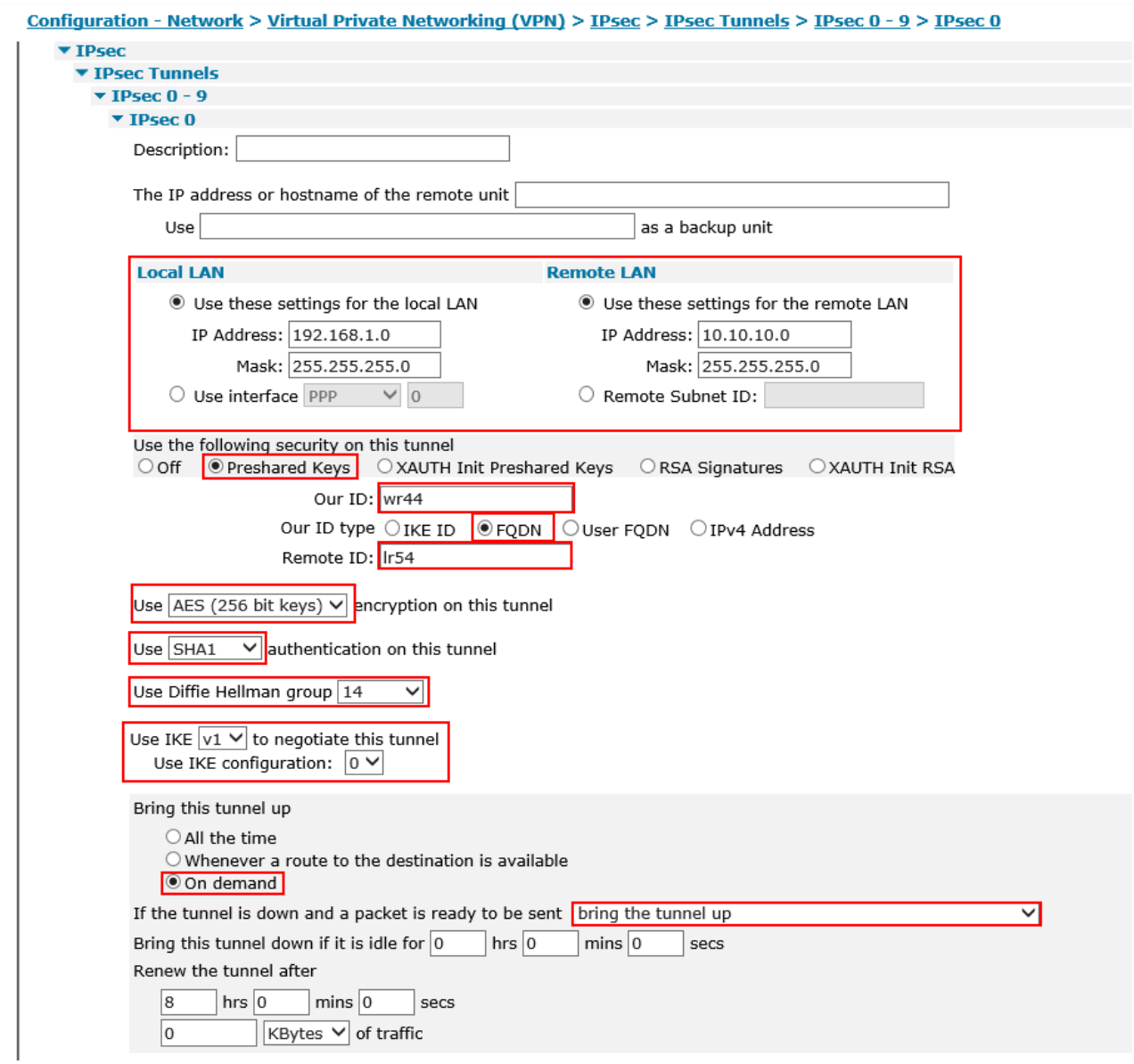


Parameter	Setting	Description
Encryption	AES (256 bit)	Encryption algorithm used in this tunnel
Authentication	SHA1	Authentication algorithm used in this tunnel
Mode	Aggressive	IKE Mode used in this tunnel
MODP Group for Phase 1	14 (2048)	Key length used in the IKE Diffie-Hellman exchange
MODP Group for Phase 2	No PFS	Key length used in the ESP Diffie-Hellman exchange

3.3.2 Phase 2 settings

Navigate to:

Configuration – Network > Virtual Private Network (VPN) > IPsec > IPsec 0 – 9 > IPsec 0



Parameter	Setting	Description
Local LAN settings		
Use these settings for the local LAN	Checked	Local LAN subnet
IP Address	192.168.1.0	Local LAN subnet IP Address
Mask	255.255.255.0	Local LAN subnet mask
Remote LAN settings		
Use these settings for the local LAN	Checked	Remote LAN subnet
IP Address	10.10.10.0	Remote LAN subnet IP Address
Mask	255.255.255.0	Remote LAN subnet mask
Tunnel Security		
Preshared Keys	Checked	Use preshared keys for authentication on this tunnel
Our ID	wr44	The ID of the VPN responder router (this router)
Remote ID	lr54	The ID of the VPN initiator router (remote router)
Our ID type	FQDN	Use Fully Qualified Domain Name type ID
Use () encryption on this tunnel	AES (256 bit keys)	The IPsec encryption algorithm to use is AES
Use () authentication on this tunnel	SHA1	The IPsec ESP authentication to use is SHA1
Tunnel creation		
Bring this tunnel up	On demand	
If the tunnel is down and a packet is ready to be sent	Bring the tunnel up	

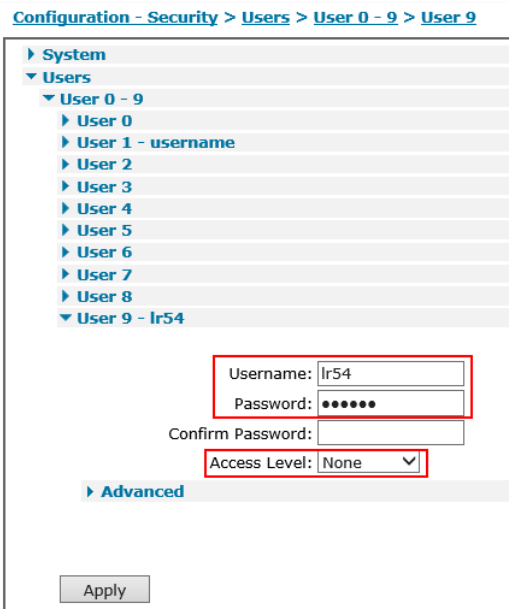
Click **Apply**

3.3.3 Preshared key settings

The pre-shared key is enabled by creating a username with the name of the remote peer (Remote ID from the Phase 2 settings) and the password is the preshared key.

Navigate to:

Configuration – Security > Users > Users 0 - 9 > User 9



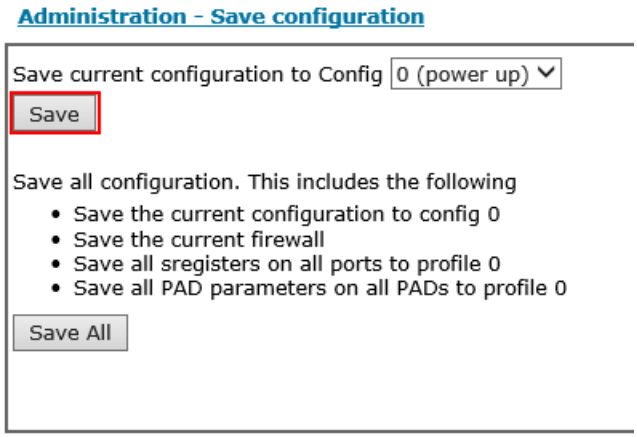
Parameter	Setting	Description
Username	lr54	Name should match the Remote ID value from Phase 2 settings
Password	digitestvpn123	Enter the password which will be used as the preshared key. This has to match the value on the Remote router.
Confirm password	digitestvpn123	Re-enter the password
Access Level	None	This user will not be granted any admin access as it is only used as a preshared key.

Click **Apply**

3.4 Save configuration

Navigate to:

Administration – Save Configuration



Click **Save**. The configuration will now be saved to the unit.

4 TRANSPORT LR54 CONFIGURATION

Please Note: At the time of this document, the configuration of the TransPort LR54 is exclusively done via CLI (Command Line Interface)

4.1 Configure a local interface

In this example, we will use the 10.10.10.0/24 subnet on LAN 1. To configure this:

```
lan 1 ip-address 10.10.10.1
lan 1 mask 255.255.255.0
```

All **IKE** and **IPSec** configuration is done within the **ipsec** command.

The following command will show all available options:

```
ipsec 1 ?
```

4.2 Configure Phase 1 settings

Configure the IKE Phase 1 settings to match the settings of the Connect WAN Router.

- IKE version 1
- SHA 1
- Group 14
- AES 256
- 4800 lifetime
- AGGRESSIVE mode

Enter the parameters as follow:

```
digi.router> ipsec 1 ike 1
digi.router> ipsec 1 ike-authentication sha1
digi.router> ipsec 1 ike-diffie-hellman group14
digi.router> ipsec 1 ike-encryption aes256
digi.router> ipsec 1 ike-lifetime 4800
digi.router> ipsec 1 ike-mode aggressive
```

Type the following to verify the IKE Phase 1 settings:

```
ipsec 1 ik?
digi.router> ipsec 1 ik?

Configures an IPsec tunnel

Syntax:
ipsec 1 <parameter> <value>

Available Parameters:
 Parameter             Current Value       Description
-------------------------------------------------------------------------------
 ike                   1                   IKE version to use for this IPsec tunnel
 ike-authentication    sha1                IKE authentication type for IPsec tunnel
 ike-diffie-hellman    group14             IKE Diffie-Hellman group for IPsec
 ike-encryption        aes256              IKE encryption type
 ike-lifetime          4800                Key lifetime in seconds
 ike-mode              aggressive          IKEv1 mode to use for this IPsec tunnel
 ike-tries             3                   Number of attempts to negotiate
```

4.3 Configure Phase 2 settings

4.3.1 Authentication and encryption settings

Configure the Phase 2 authentication and encryption settings to match the settings of the Connect WAN Router.

- Pre-shared key
- SHA 1
- Group 14
- AES 256
- 3600 lifetime
- psk

Enter the parameters as follow:

```
digi.router> ipsec 1 auth-by psk
digi.router> ipsec 1 esp-authentication sha1
digi.router> ipsec 1 esp-diffie-hellman group14
digi.router> ipsec 1 esp-encryption aes256
digi.router> ipsec 1 lifetime 3600
digi.router> ipsec 1 psk digitestvpn123
```

Type the following to verify the Phase 2 authentication and encryption settings:

```
digi.router> ipsec 1 es?

Configures an IPsec tunnel

Syntax:
ipsec 1 <parameter> <value>

Available Parameters:
 Parameter             Current Value       Description
-------------------------------------------------------------------------------
 esp-authentication    sha1                ESP authentication type for IPsec tunnel
 esp-diffie-hellman    group5              ESP Diffie-Hellman group for IPsec
 esp-encryption        aes128              ESP encryption type for IPsec tunnel
```

4.3.2 Local and Remote traffic selector settings

Configure the Phase 2 local and remote traffic selector settings to match the settings of the Connect WAN Router.

- Local ID
- Remote ID
- Local network : 10.10.10.0
- Local mask : 255.255.255.0
- Remote network: 192.168.1.0
- Remote mask : 255.255.255.0

Enter the parameters as follow:

```
digi.router> ipsec 1 local-id lr54
digi.router> ipsec 1 remote-id wr44
digi.router> ipsec 1 local-mask 255.255.255.0
digi.router> ipsec 1 local-network 10.10.10.0
digi.router> ipsec 1 remote-mask 255.255.255.0
digi.router> ipsec 1 remote-network 192.168.1.0
```

Type the following to verify the Phase 2 local and remote traffic selector settings:

```
digi.router> ipsec 1 loc?

Configures an IPsec tunnel

Syntax:
ipsec 1 <parameter> <value>

Available Parameters:
 Parameter             Current Value       Description
-------------------------------------------------------------------------------
 local-id              lr54                Local ID used for this IPsec tunnel
 local-mask            255.255.255.0       Local network mask for this IPsec tunnel
 local-network         10.10.10.0          Local network for this IPsec tunnel

digi.router> ipsec 1 rem?

Configures an IPsec tunnel

Syntax:
ipsec 1 <parameter> <value>

Available Parameters:
 Parameter             Current Value       Description
-------------------------------------------------------------------------------
 remote-id             wr44                Remote ID used for this IPsec tunnel
 remote-mask           255.255.255.0       Remote network mask for this tunnel
 remote-network        192.168.1.0         Remote network for this IPsec tunnel
```

4.4 Configure Peer address

To configure the Peer address, in this example, the IP address of the Mobile interface of the Connect WAN router do the following:

```
digi.router> ipsec 1 peer x.x.x.x
```

x.x.x.x being an IP address reachable via the WAN interface of the LR54.

4.5 Turn IPSec on

To enable the configured IPSec VPN tunnel, do the following:

```
digi.router> ipsec 1 state on
```

The configuration is complete and the tunnel should now be built.

4.6 Configure the Firewall

Please note: By default, no traffic will be allowed inside the tunnel. It is necessary to add the following firewall rule to bypass the MASQUERADE (NAT) rules in place:

firewall -t nat -I POSTROUTING 1 -s 10.10.0.0/16 -d 192.168.1.0/24 -j ACCEPT

4.6.1 Firewall rules needed for MAIN mode VPN.

The example used in this document uses an Aggressive mode VPN. If a MAIN mode VPN is used, the following rule will be required to allow ESP packets inbound:

```
firewall -A INPUT -p 50 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

4.6.2 Firewall rules needed for RESPONDER configuration

The example used in this document uses the LR 54 as the INITIATOR.

If the LR 54 is used as the RESPONDER, the following rules will be required to allow inbound VPN connections:

```
firewall -A INPUT -p udp -m multiport --dports 500,4500 -m conntrack --
ctstate NEW,ESTABLISHED -j ACCEPT

firewall -A OUTPUT -p udp -m multiport --dports 500,4500 -m conntrack --
ctstate NEW,ESTABLISHED -j ACCEPT

firewall -A INPUT -p 50 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

firewall -A OUTPUT -p 50 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

4.7 Save Configuration

To save configuration, do the following:

```
digi.router> save config
```

5 CHECK TUNNEL STATUS

5.1 TransPort WR44

Navigate to

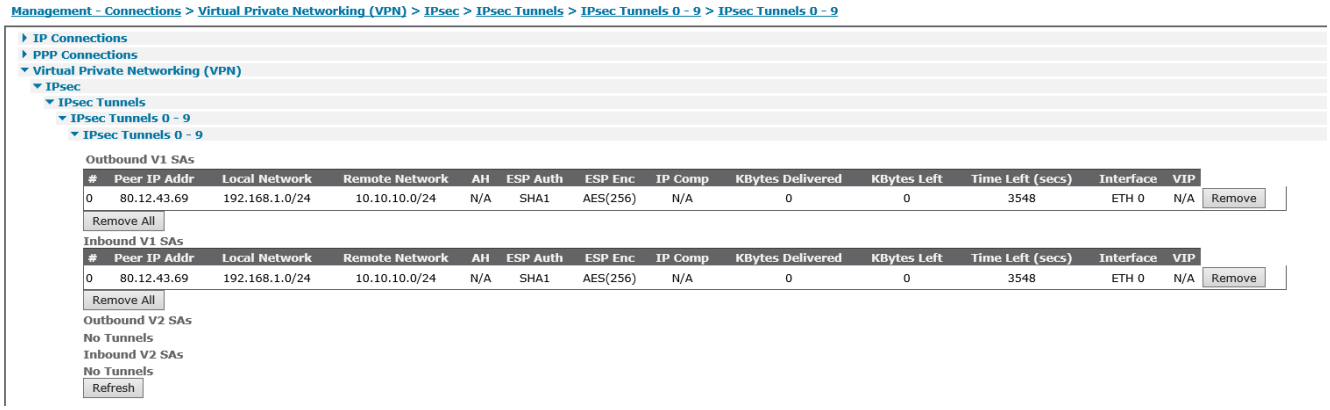
Management – Event Log

The following line should show that the tunnel was built successfully:

```
11:05:56, 22 Feb 2017,(287) IKE SA Removed. Peer: lr54,Successful Negotiation
11:05:53, 22 Feb 2017,Eroute 0 VPN up peer: lr54
11:05:53, 22 Feb 2017,New IPSec SA created by lr54
11:05:53, 22 Feb 2017,(287) New Phase 2 IKE Session 80.12.43.69,Responder
11:05:52, 22 Feb 2017,(286) IKE Keys Negotiated. Peer: lr54
11:05:52, 22 Feb 2017,(286) New Phase 1 IKE Session 80.12.43.69,Responder
```

Navigate to

Management – Virtual Private Networking (VPN) > IPsec > IPsec Tunnels 0 – 9 > IPsec Tunnels 0 – 9



5.2 TransPort LR54

To verify if the tunnel is up, do the following:

```
digi.router> show ipsec 1

 IPsec 1 Status and Statistics
 -----------------------------
 Description      :
 Admin Status     : Up
 Oper Status      : Up
 Uptime           : 7 seconds

 Peer             : 86.200.150.100
 Local Network    : 10.10.10.0/24
 Remote Network   : 192.168.1.0/24

 IKE Information
 ---------------
 Key Negotiation  : IKEv1, aes256, sha1, modp2048
 SPIs             : 2b5b3cf0b24e2d30_i* ae4f7a47b6e7b81d_r

 Tunnel Information
 ------------------
 Rekeying In      : 69 minutes
 AH Cipher Suite  : Not Used
 ESP Cipher Suite : aes256, sha1, modp2048
 Renegotiating In : 43 minutes
 Outbound ESP SAs : 0dbd35cf
 Inbound ESP SAs  : cf29fbb7

 Dead Peer Detection is on

 Bytes In         : 0
 Bytes Out        : 0
```

6 TESTING

Verify that data is going through the tunnel by issuing a ping from each side of the tunnel.

6.1 TransPort WR44

From the web interface (similar to CLI), this can be done from **Administration – Execute a command**

Make sure to specify the interface used to generate this ping (in this example, we use ETH 0)

```
Ping 10.10.10.1 -e0

Pinging Addr [10.10.10.1]

sent PING # 1
PING receipt # 1 : response time 1.18 seconds
Iface: ETH 0
Ping Statistics
Sent         : 1
Received     : 1
Success      : 100 %
Average RTT : 1.18 seconds

OK
```

6.2 TransPort LR54

From the web interface (similar to CLI), this can be done from **System > Device Console**

```
digi.router> ping 192.168.1.44

PING 192.168.1.44 (192.168.1.44) 56(84) bytes of data.
64 bytes from 192.168.1.44: icmp_seq=1 ttl=251 time=57.5 ms
64 bytes from 192.168.1.44: icmp_seq=2 ttl=251 time=55.2 ms
64 bytes from 192.168.1.44: icmp_seq=3 ttl=251 time=60.3 ms

--- 192.168.1.44 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3011ms
rtt min/avg/max/mdev = 55.270/57.708/60.306/2.077 ms
```

If no traffic is going through, make sure that the firewall rule has been added properly, see section 4.6

You can view firewall rules by using the following:

```
firewall -t nat -L -v
```