Quick Note 65

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

Digi Technical Support

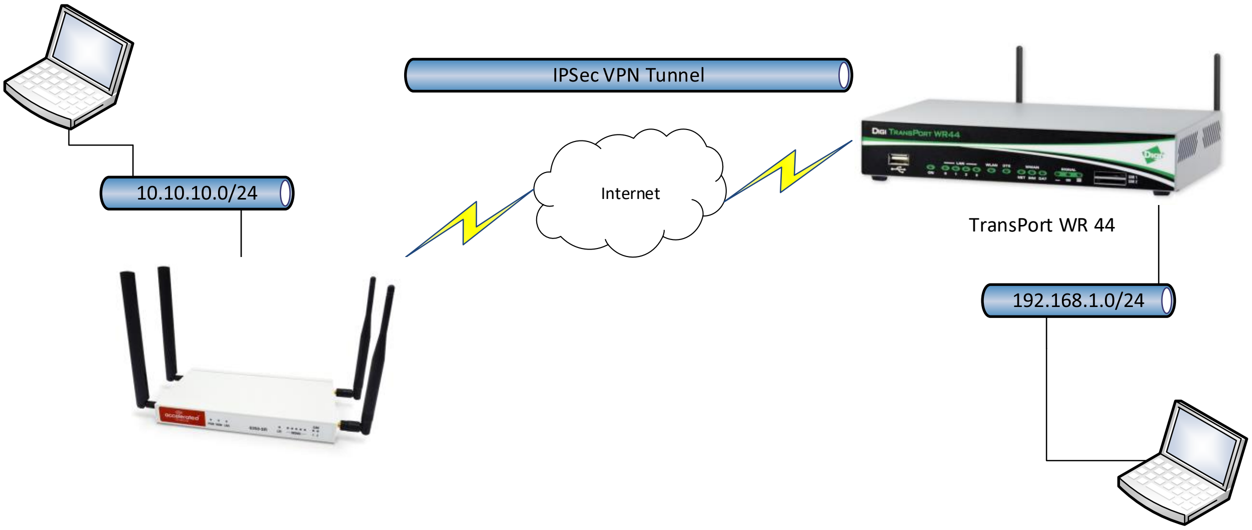
10 November 2020

Contents

1 INTRODUCTION

1.1 Outline

This document will describe how to configure an IPSec VPN tunnel between 6350 SR 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: Accelerated 6350-SR and Digi TransPort WR44

Firmware versions:
6350-SR: 18.1.29.41 and later
WR44: 6.1.2.2 and later
Other Compatible Models: Digi TransPort WR11,WR21,WR31, Digi IX Family, Digi EX Family, Digi TX Family, Digi 63xx Family.

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 6530 SR 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

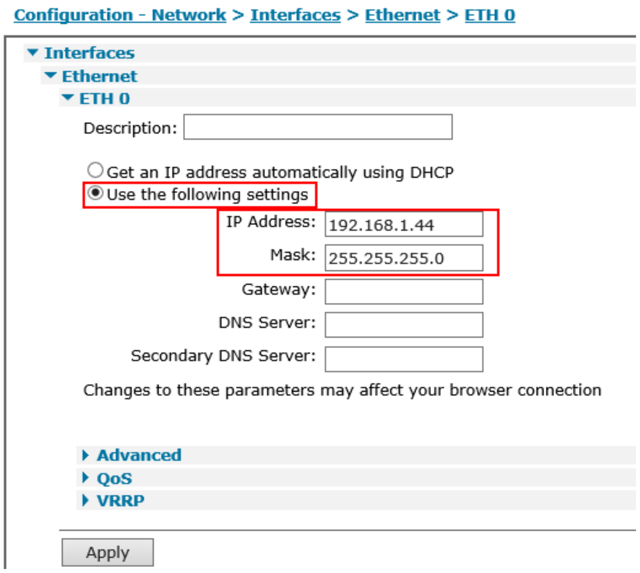
Version Number	Status
1.0	Published
1.1	Clarified supported saros/dal devices

3 TRANSPORT WR44 CONFIGURATION (RESPONDER)

3.1 Local Ethernet Interface configuration

Navigate to:

Configuration – Network > Interfaces > Ethernet > ETH 0



Configuration - Network > Interfaces > Ethernet > ETH 0

▾ Interfaces
▾ Ethernet
▾ ETH 0

Description:

○ Get an IP address automatically using DHCP
● Use the following settings

IP Address: 192.168.1.44
Mask: 255.255.255.0
Gateway:
DNS Server:
Secondary DNS Server:

Changes to these parameters may affect your browser connection

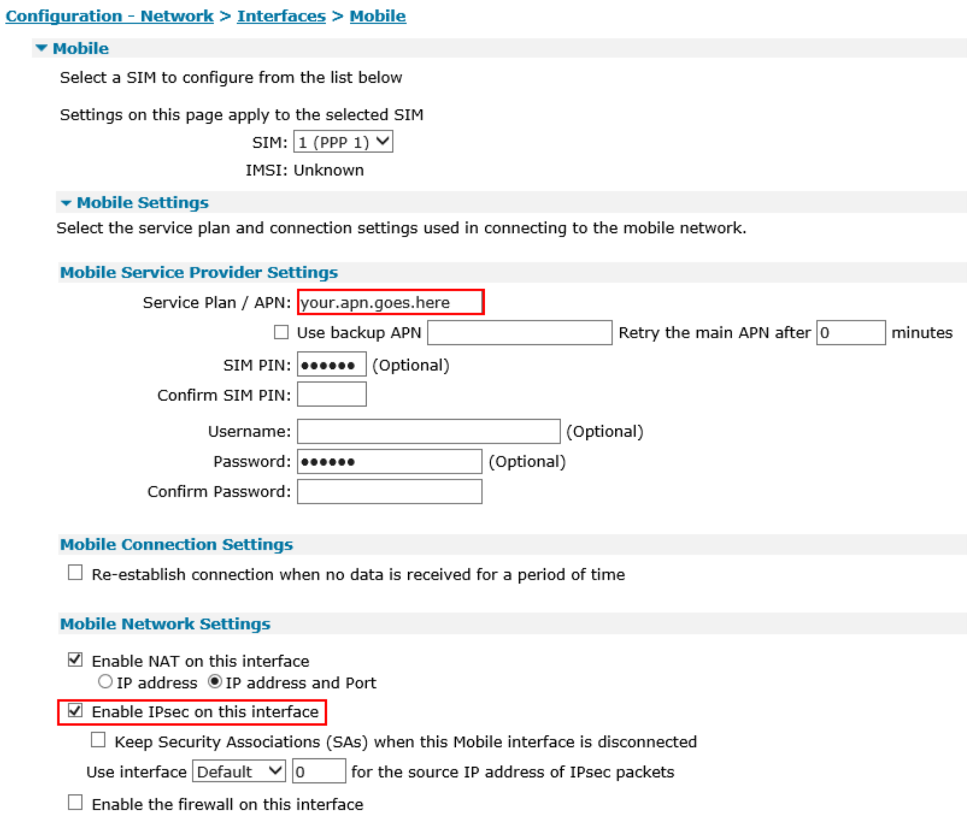
Parameter	Setting	Description
Use the following settings	Checked	A static IP Address will be used in this example
IP Address	192.168.1.44	IP Address of the TransPort WR44 Ethernet Interface. In this example, this IP Address is in the subnet range used for the Tunnel (useful for testing)
Mask	255.255.255.0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



Configuration - Network > Interfaces > Mobile

▼ 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 0 minutes

SIM PIN: •••••• (Optional)

Confirm SIM PIN:

Username: (Optional)

Password: •••••• (Optional)

Confirm Password:

Mobile Connection Settings

□ Re-establish connection when no data is received for a period of time

Mobile Network Settings

☑ Enable NAT on this interface

○ IP address ● IP address and Port

☑ Enable IPsec on this interface

□ Keep Security Associations (SAs) when this Mobile interface is disconnected

Use interface Default 0 for the source IP address of IPsec packets

□ Enable the firewall on this interface

Parameter	Setting	Description
Service Plan / APN	Your.APN.goes.here	Enter 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.

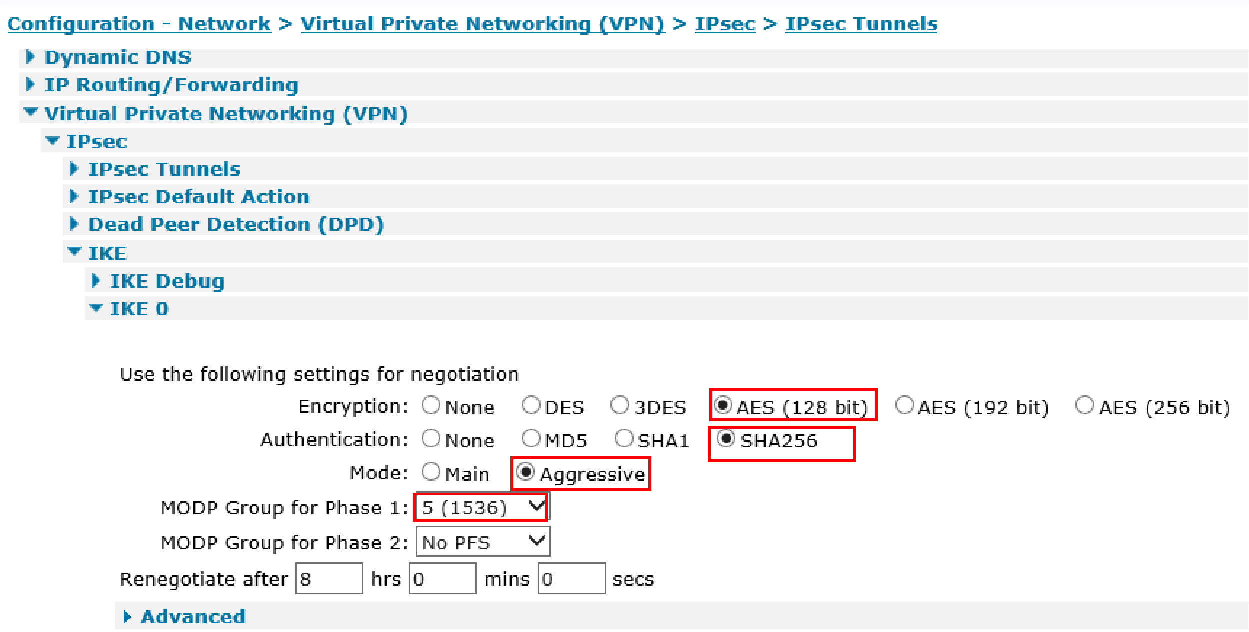
3.3 Tunnel Configuration

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


Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels
Dynamic DNS
IP Routing/Forwarding
Virtual Private Networking (VPN)
IPsec
IPsec Tunnels
IPsec Default Action
Dead Peer Detection (DPD)
IKE
IKE Debug
IKE 0
Advanced

Use the following settings for negotiation

Encryption: ○ None ○ DES ○ 3DES ● AES (128 bit) ○ AES (192 bit) ○ AES (256 bit)

Authentication: ○ None ○ MD5 ○ SHA1 ● SHA256

Mode: ○ Main ● Aggressive

MODP Group for Phase 1: 5 (1536)

MODP Group for Phase 2: No PFS

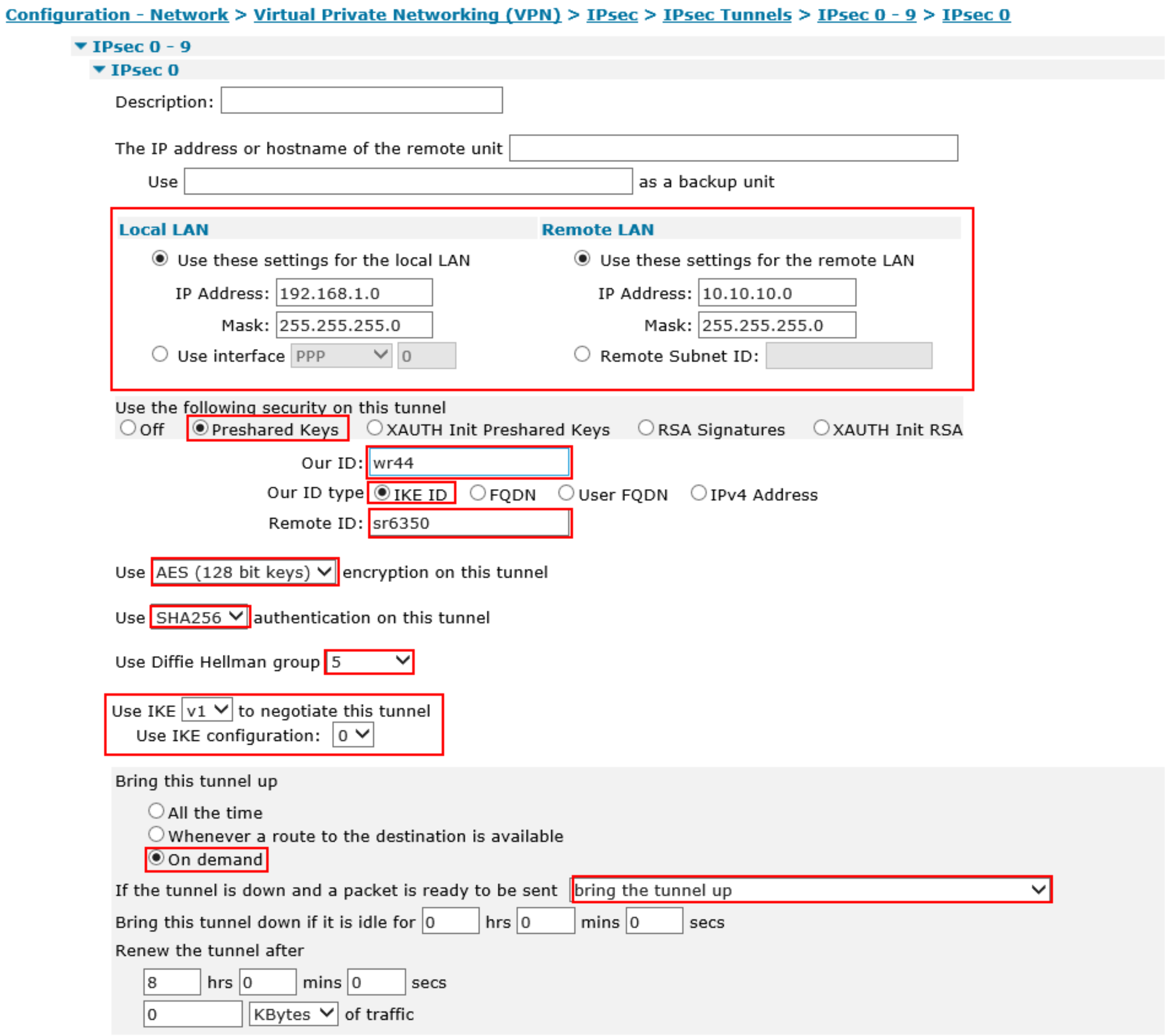
Renegotiate after 8 hrs 0 mins 0 secs

Parameter	Setting	Description
Encryption	AES (128 bit)	Encryption algorithm used in this tunnel
Authentication	SHA256	Authentication algorithm used in this tunnel
Mode	Aggressive	IKE Mode used in this tunnel
MODP Group for Phase 1	5 (1536)	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



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

▾ IPsec 0 - 9

▾ 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: 192.168.1.0

Mask: 255.255.255.0

○ Use interface PPP 0

Remote LAN

● Use these settings for the remote LAN

IP Address: 10.10.10.0

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: wr44

Our ID type ● IKE ID ○ FQDN ○ User FQDN ○ IPv4 Address

Remote ID: sr6350

Use AES (128 bit keys) encryption on this tunnel

Use SHA256 authentication on this tunnel

Use Diffie Hellman group 5

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

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	Sr6350	The ID of the VPN initiator router (remote router)
Our ID type	IKE ID	Use Fully Qualified Domain Name type ID
Use () encryption on this tunnel	AES (128 bit keys)	The IPsec encryption algorithm to use is AES
Use () authentication on this tunnel	SHA256	The IPsec ESP authentication to use is SHA1
Use Diffie Hellman group	5	The Diffie Hellman group to use for Phase 2
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	

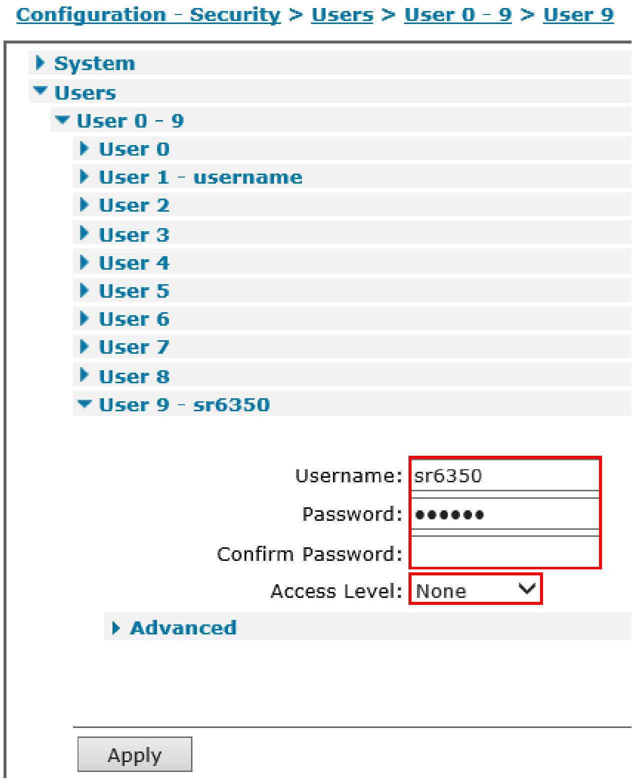
Click **Apply**

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



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

Username: sr6350

Password: ••••••

Confirm Password:

Access Level: None

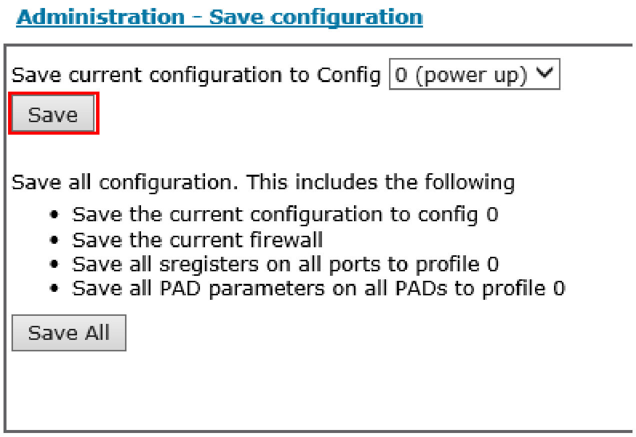
Parameter	Setting	Description
Username	Sr6350	Name should match the Remote ID value from Phase 2 settings
Password	digitestvpn123	Enter the password which will be used as the preshared key. This has to match the value on the Remote router.
Confirm password	digitestvpn123	Re-enter the password
Access 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



Administration - Save configuration

Save current configuration to Config 0 (power up)

Save all configuration. This includes the following

- Save the current configuration to config 0
- Save the current firewall
- Save all sregisters on all ports to profile 0
- Save all PAD parameters on all PADs to profile 0

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

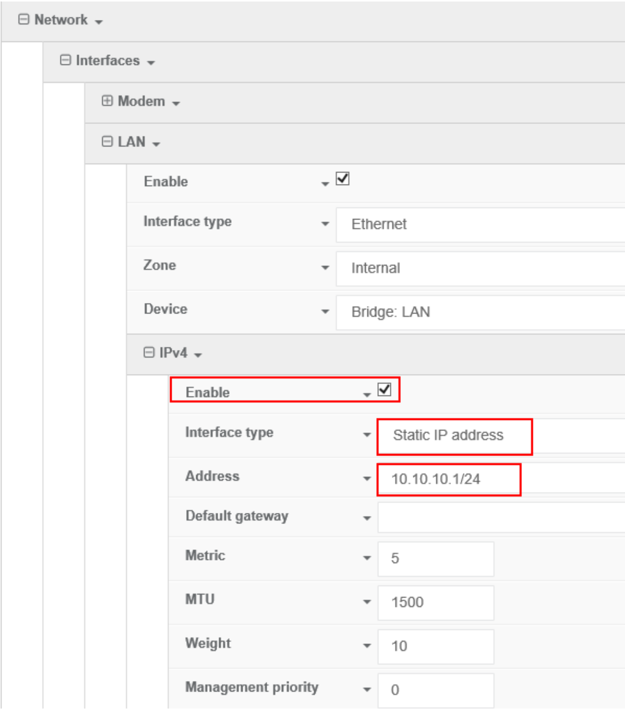
4 6350-SR CONFIGURATION

Please note: The configuration examples in this document are shown with Central Management **disabled.**

4.1 Local Ethernet configuration

Navigate to:

Configuration > Network > Interfaces > LAN > IPV4



⊟ Network

⊟ Interfaces

⊞ Modem

⊟ LAN

Enable	☑
Interface type	Ethernet
Zone	Internal
Device	Bridge: LAN

⊟ IPv4

Enable	☑
Interface type	Static IP address
Address	10.10.10.1/24
Default gateway	
Metric	5
MTU	1500
Weight	10
Management priority	0

Parameter	Setting	Description
Use the following settings	Checked	Enable
Interface type	Static IP address	Use a static ip address for the LAN interface
Address	10.10.10.1/24	IP Address used for the lan interface (this will be used for testing the tunnel)

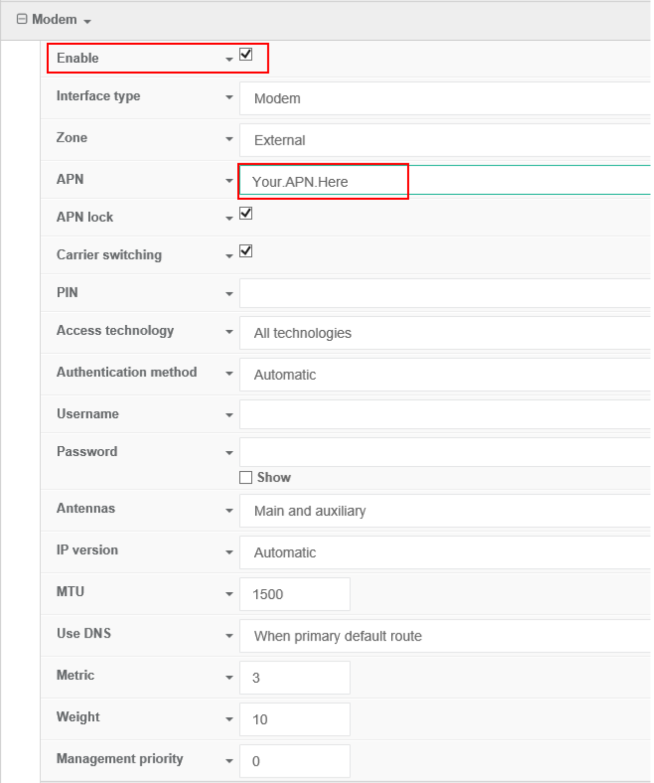
Click **Save**

4.2 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 > Modem



⊟ Modem

Enable ☑

Interface type: Modem

Zone: External

APN: Your.APN.Here

APN lock ☑

Carrier switching ☑

PIN

Access technology: All technologies

Authentication method: Automatic

Username

Password

□ Show

Antennas: Main and auxiliary

IP version: Automatic

MTU: 1500

Use DNS: When primary default route

Metric: 3

Weight: 10

Management priority: 0

Parameter	Setting	Description
Enable	Checked	Enable Cellular interface
APN	xxxx	Enther the APN of your mobile provider

If your APN requires a USERNAME / PASSWORD enter them on this page.

If your SIM card requires a PIN code, enter it on this page.

Click **Save**

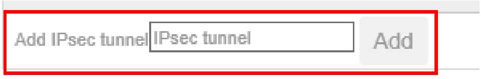
4.3 Tunnel Configuration

Open a web browser to the IP address of the 6350-SR router.

Navigate to:

Configuration > VPN > IPsec

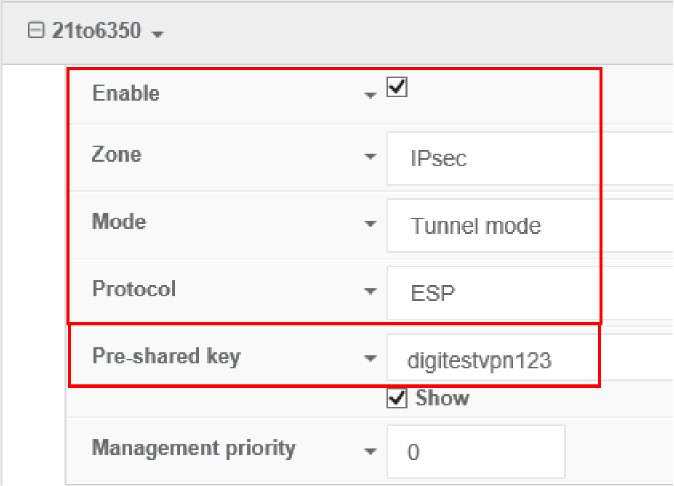
Enter a desired IPsec tunnel name and click **Add**



Add IPsec tunnel: IPsec tunnel

4.3.1 IPsec Settings

Configure the Main IPsec settings.



21to6350

Enable: ☑

Zone: IPsec

Mode: Tunnel mode

Protocol: ESP

Pre-shared key: digitestvpn123

☑ Show

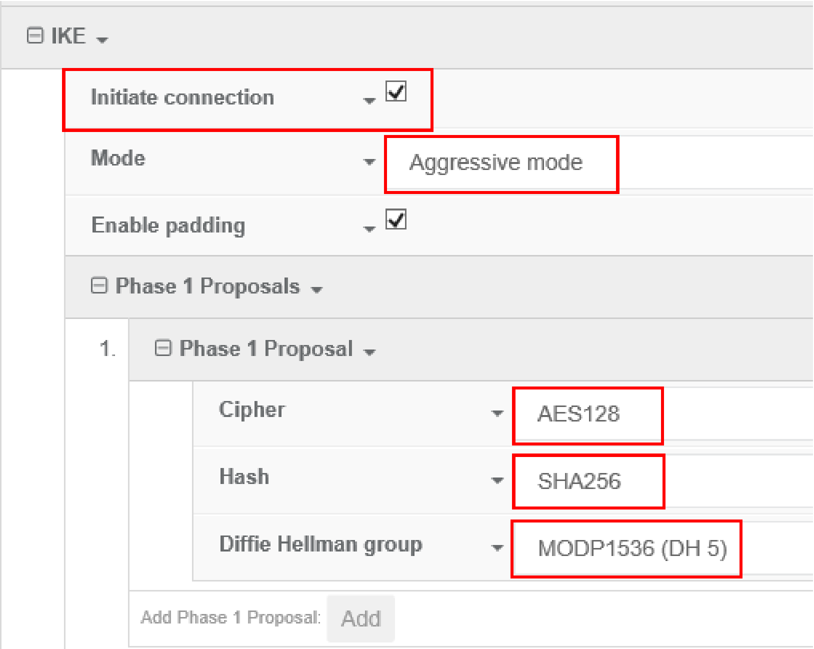
Management priority: 0

Parameter	Setting	Description
Enable	Checked	Enable this IPsec tunnel
Zone	IPsec	Firewall Zone assigned to this tunnel
Mode	Tunnel Mode	Mode used for this IPsec tunnel
Protocol	ESP	Protocol used for this IPsec tunnel
Pre-shared key	digitestvpn123	Enter the password which will be used as the preshared key. This has to match the value on the Remote router.

4.3.2 Phase 1 settings

Expand the **IKE** menu.

Configure Phase 1 settings.



⊟ IKE

Initiate connection ☑

Mode: Aggressive mode

Enable padding ☑

⊟ Phase 1 Proposals

1. ⊟ Phase 1 Proposal

Cipher: AES128

Hash: SHA256

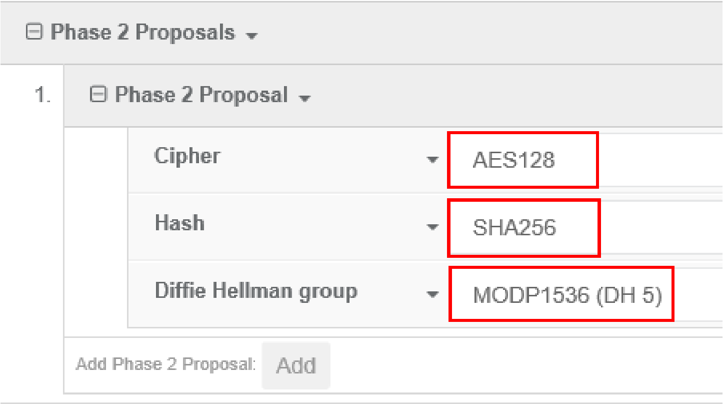
Diffie Hellman group: MODP1536 (DH 5)

Parameter	Setting	Description
Initiate connection	Checked	The SR router will be the INITIATOR.
Mode	Aggressive	IKE Mode used in this tunnel
Cipher	AES (128 bit)	Encryption algorithm used in this tunnel
Hash	SHA256	Authentication algorithm used in this tunnel
Diffie Hellman group	5 (1536)	Key length used in the IKE Diffie-Hellman exchange

4.3.3 Phase 2 settings

Configure Phase 2 settings

Expand the **Phase 2 Proposals** menu.



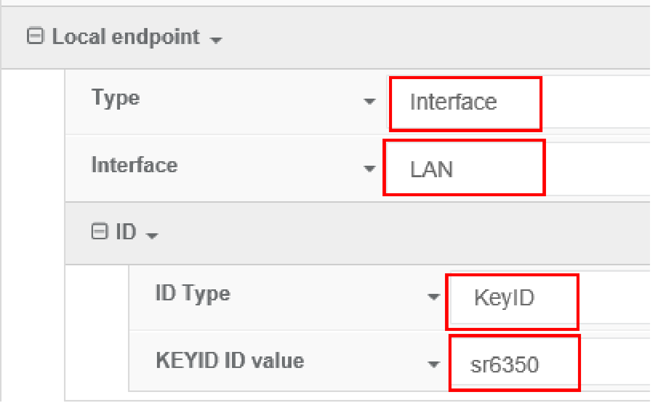
⊟ Phase 2 Proposals

1. ⊟ Phase 2 Proposal

Cipher	AES128
Hash	SHA256
Diffie Hellman group	MODP1536 (DH 5)

Add Phase 2 Proposal: Add

Expand the **Local endpoint** menu.



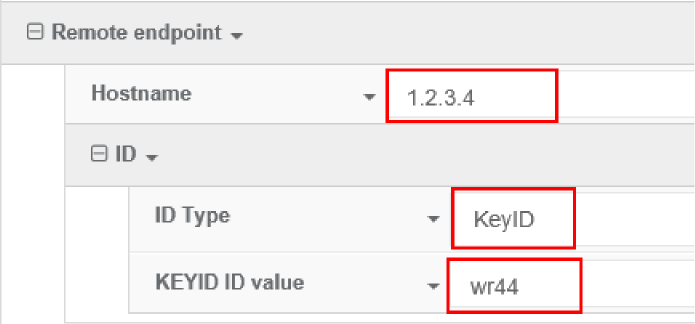
⊟ Local endpoint

Type	Interface
Interface	LAN

⊟ ID

ID Type	KeyID
KEYID ID value	sr6350

Expand the **Remote endpoint** menu.



⊟ Remote endpoint

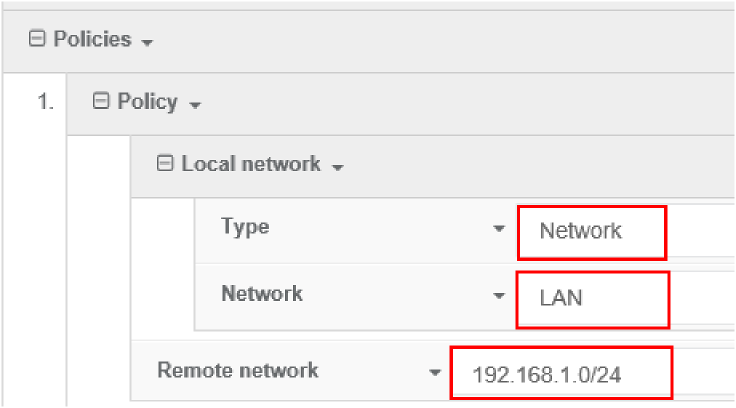
Hostname	1.2.3.4

⊟ ID

ID Type	KeyID
KEYID ID value	wr44

Expand the **Policies** menu.

Click **Add** to add a new policy



Type: Network

Network: LAN

Remote network: 192.168.1.0/24

Click **Save**

Parameter	Setting	Description
Local endpoint		
Type	Interface	Local LAN subnet
Interface	LAN	Local LAN interface
ID Type	KeyID	Use IKE ID as the ID type
KEYID ID value	sr6350	IKE ID of the router. Has to match the value of the remote site
Remote endpoint		
Hostname	1.2.3.4	WAN IP address of the Responder router (WR44)
ID Type	KeyID	Use IKE ID as the ID type
KEYID ID value	Wr44	IKE ID of the remote router. Has to match the value of the remote site
Phase 2 proposals		
Cipher	AES (128 bit keys)	The IPsec encryption algorithm to use is AES
Hash	SHA256	The IPsec ESP authentication to use is SHA1
Diffie Hellman group	5	The Diffie Hellman group to use for Phase 2
Policy		
Type	Network	Type of local network to use
Network	LAN	Use a LAN interface for the Local network
Remote network	192.168.1.0/24	Remote network subnet

5 CHECK TUNNEL STATUS

5.1 TransPort WR44

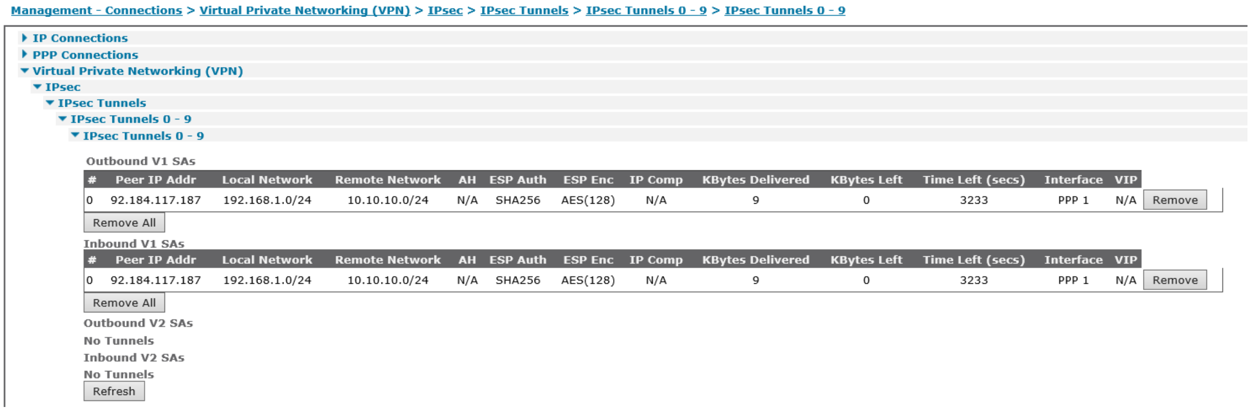
Navigate to **Management – Event Log**

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

```
09:09:36, 07 Jun 2018,(2) IKE SA Removed. Peer: sr6350,Successful Negotiation
09:09:33, 07 Jun 2018,Eroute 0 VPN up peer: sr6350
09:09:33, 07 Jun 2018,New IPSec SA created by sr6350
09:09:33, 07 Jun 2018,(2) New Phase 2 IKE Session 92.184.117.187,Responder
09:09:32, 07 Jun 2018,(1) IKE Keys Negotiated. Peer: sr6350
09:09:31, 07 Jun 2018,(1) New Phase 1 IKE Session 92.184.117.187,Responder
```

Navigate to

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



Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec Tunnels 0 - 9 > IPsec Tunnels 0 - 9
IP Connections
PPP Connections
Virtual Private Networking (VPN)
IPsec
IPsec Tunnels
IPsec Tunnels 0 - 9
IPsec Tunnels 0 - 9

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	92.184.117.187	192.168.1.0/24	10.10.10.0/24	N/A	SHA256	AES(128)	N/A	9	0	3233	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	92.184.117.187	192.168.1.0/24	10.10.10.0/24	N/A	SHA256	AES(128)	N/A	9	0	3233	PPP 1	N/A	Remove

Remove All

Outbound V2 SAs

No Tunnels

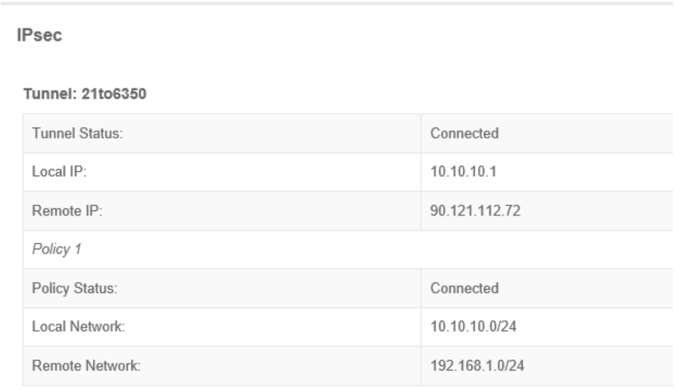
Inbound V2 SAs

No Tunnels

Refresh

5.2 6350-SR

Navigate to **Status > Tunnels**



IPsec

Tunnel: 21to6350

Tunnel Status:	Connected
Local IP:	10.10.10.1
Remote IP:	90.121.112.72
Policy 1	
Policy Status:	Connected
Local Network:	10.10.10.0/24
Remote Network:	192.168.1.0/24

Navigate to **Terminal** and issue:

```
# ipsec status
Security Associations (1 up):
21to6350_1of1[4]: ESTABLISHED 16 minutes ago,
10.10.10.1[sr6350]...90.121.112.72[wr44]
21to6350_1of1{1}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: cc262ae7_i
d627e1b1_o
21to6350_1of1{1}:   10.10.10.0/24 === 192.168.1.0/24

.10.10.0/24 === 192.168.1.0/24
```

6 TESTING

Verify that data is going through the tunnel by issuing a ping from each side of the tunnel. In this example the local interface of each router is used.

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 0.63 seconds
Iface: PPP 1
Ping Statistics
Sent         : 1
Received     : 1
Success      : 100 %
Average RTT  : 0.63 seconds

OK
```

6.2 6350-SR

From the web interface (similar to CLI), this can be done from **Terminal**

```
# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=250 time=668 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=250 time=609 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=250 time=779 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 2999ms
rtt min/avg/max/mdev = 609.999/686.033/779.459/70.272 ms
```