Quick Note

Configure an IPSec VPN tunnel between a Digi TransPort LR router and a Digi Connect gateway.

Digi Technical Support

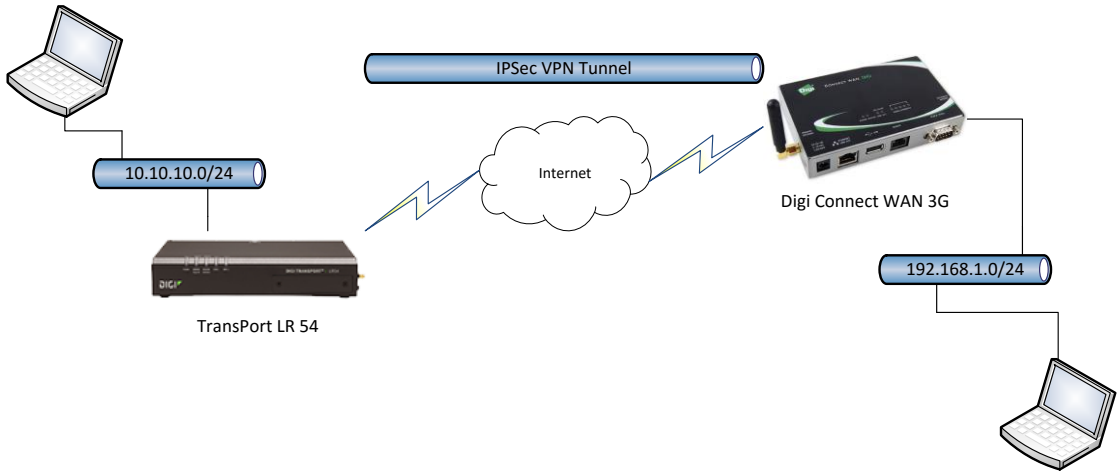
20 September 2016

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 Connect WAN 3G 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 Connect WAN 3G

Firmware versions: LR54: 1.1.0.6 and later **DCWAN:** 2.17.6.1

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 or Connect WAN router.

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

3 CONNECT WAN CONFIGURATION (RESPONDER)

3.1 Tunnel Configuration

Open a web browser to the IP address of the Connect WAN router.

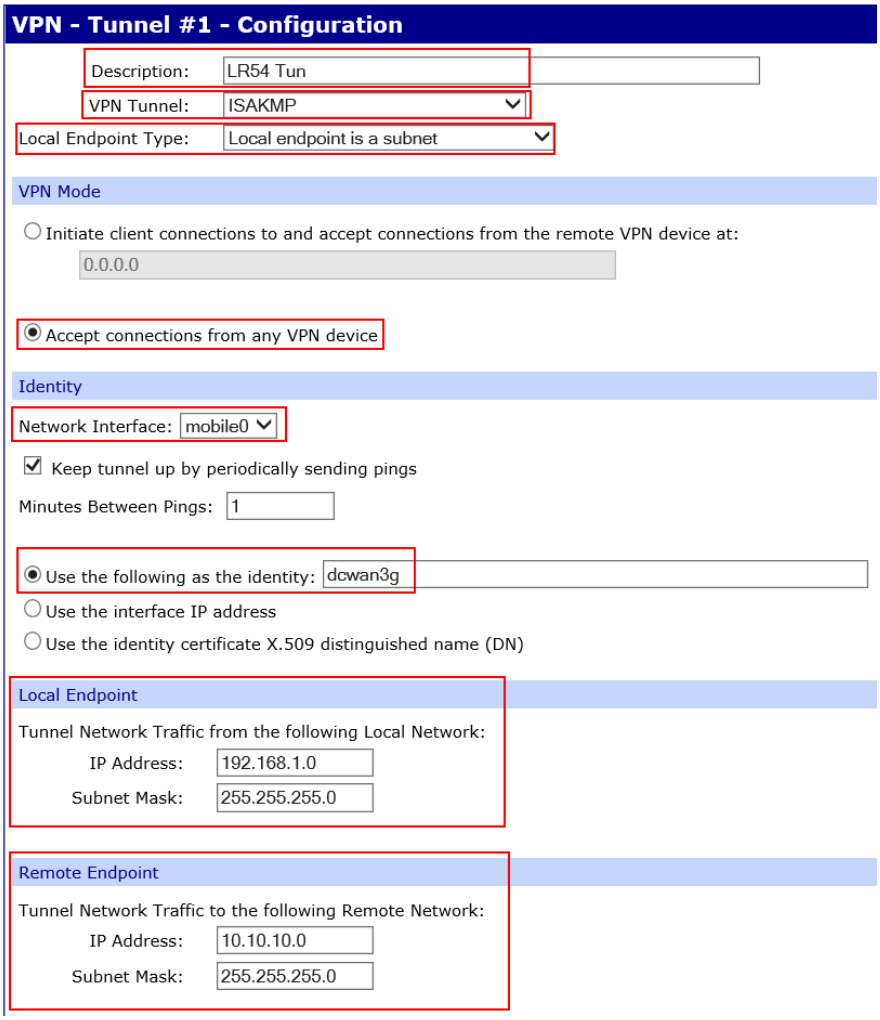
Navigate to:

Configuration – Network > Virtual Private Network (VPN) Settings > VPN Policy Settings

Click **Add**

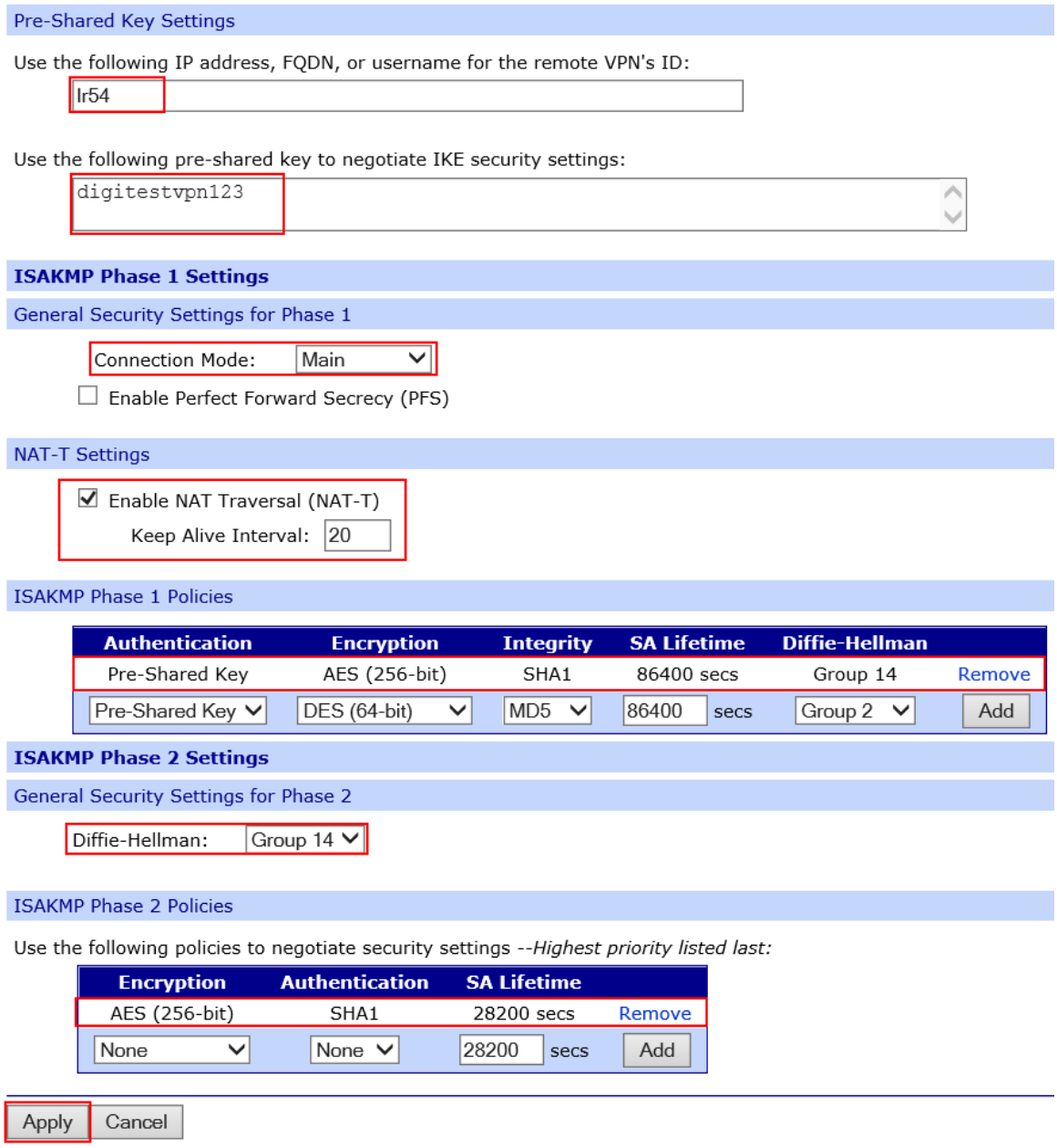
3.1.1 Tunnel Settings

Configure the VPN mode for incoming and set the remaining settings as required or like in the below example:



Parameter	Setting	Description
Description	LR54 Tun	This is the description of the Tunnel
VPN Tunnel	ISAKMP	Tunnel mode used. IPSec with IKE and Preshared key
Local Endpoint Type	Local endpoint is a subnet	Lan to Lan type VPN connecting 2 subnets.
VPN Mode	Accept connections from any VPN device	Responder mode
Network Interface	Mobile0	Interface used to build the IPSec VPN Tunnel
Use the following as the identity	dcwan3g	Local ID
Local Endpoint IP Address	192.168.1.0	Local subnet IP Address on the Connect WAN side
Local Endpoint Subnet Mask	255.255.255.0	Local subnet Mask on the Connect WAN side
Remote Endpoint IP Address	10.10.10.0	Remote subnet IP Address on the TransPort LR side
Remote Enpoint Subnet Mask	255.255.255.0	Remote subnet Mask on the TransPort LR side

3.1.2 Phase 1, Phase 2 & Pre-shared key settings



Parameter	Setting	Description
Remote VPN ID	lr54	Remote VPN ID used on the TransPort LR54
Pre-shared key	digitestvpn123	Pre-shared key used for the tunnel
Connection Mode	Main	Use Main mode as the connection mode.
NAT Traversal	Checked	Enable NAT Traversal
ISAKMP Phase 1 policies		
Authentication	Pre-Shared Key	PSK Authentication
Encyprtion	AES (256-bit)	Encryption Type
Integrity	SHA1	Integrity algorithm
SA Lifetime	86400 secs	Security Association lifetime
Diffie Hellman	Group 14	DH Group
ISAKMP Phase 2 Settings		
Diffie-Hellman	Group 14	DH Group
ISAKMP Phase 2 Policies		
Encryption	AES (256-bit)	Encryption Type
Authentication	SHA1	Authentication algorithm
SA Lifetime	28200	Security Association lifetime

Click **Apply** to save and apply the changes.

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)

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

The following command will show all available options:

```
ipsec 1 ?
```

4.1 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 5
- AES 256
- 4800 lifetime
- MAIN 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 group5
digi.router> ipsec 1 ike-encryption aes256
digi.router> ipsec 1 ike-lifetime 4800
digi.router> ipsec 1 ike-mode main
```

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    group5              IKE Diffie-Hellman group for IPsec
 ike-encryption        aes256              IKE encryption type
 ike-lifetime          4800                Key lifetime in seconds
```

```
 ike-mode              main                 IKEv1 mode to use for this IPsec
tunnel
 ike-tries             3                    Number of attempts to negotiate
```

4.2 Configure Phase 2 settings

4.2.1 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 5
- AES 128
- 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 group5
digi.router> ipsec 1 esp-encryption aes128
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
```

4.2.2 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 dcwan3g
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              dcwan3g             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
```

4.3 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.

4.4 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.

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

```
digi.router> show ipsec

 #   Status  Peer             Local               Remote              Uptime
 ------------------------------------------------------------------------------
 1   Up      90.122.0.189       10.10.10.0/24      192.168.1.0/24     10
seconds
```

5 TESTING

Verify that data is going through the tunnel by issueing a ping from the Connect WAN router to the local Ethernet interface of the LR54. From the web interface, this can be done from **Administration > System Information > Diagnostic**

```
PING 10.10.10.1: 64 data bytes

64 bytes from 10.10.10.1: icmp_seq=0 time=41 ms
64 bytes from 10.10.10.1: icmp_seq=1 time=65 ms
64 bytes from 10.10.10.1: icmp_seq=2 time=87 ms

--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss
```

To test the VPN tunnel from the LR54 command line, it is needed to add a firewall rule in order to bypass the MASQUERADE (NAT) rules in place.

Add the following rule:

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

To check the firewall and view the rule:

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

Ping should now be going through:

```
digi.router> ping 192.168.1.50

PING 192.168.1.50 (192.168.1.50) 56(84) bytes of data.
64 bytes from 192.168.1.50: icmp_seq=1 ttl=255 time=3.86 ms
64 bytes from 192.168.1.50: icmp_seq=2 ttl=255 time=0.483 ms
64 bytes from 192.168.1.50: icmp_seq=3 ttl=255 time=0.492 ms
64 bytes from 192.168.1.50: icmp_seq=4 ttl=255 time=0.522 ms
64 bytes from 192.168.1.50: icmp_seq=5 ttl=255 time=0.518 ms

--- 192.168.1.50 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.483/1.176/3.865/1.344 ms
```