Quick Note

Configure an IPSec VPN tunnel in Aggressive mode between a TransPort LR router and a Cisco router.

Digi Technical Support

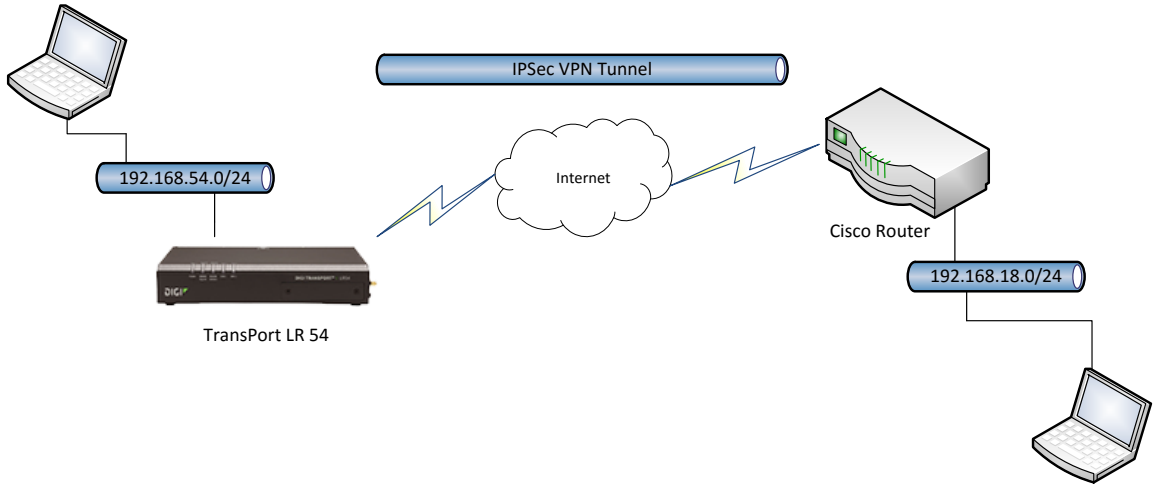
7 October 2016

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 Cisco 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 Cisco Router
Firmware versions: LR54: 1.1.0.6 and later **Cisco:** 15.1(4)M1

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.

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 CISCO ROUTER CONFIGURATION (RESPONDER)

3.1 Network configuration

3.1.1 WAN Interface

The WAN interface in this instance is an Ethernet connection with a fixed public address. This address will be used by the TransPort to build the VPN

```
interface FastEthernet0/1
ip address 12.34.56.789 255.255.255.248
no shutdown
```

3.1.2 Default Route

This tells the Cisco Router where to find the next hope router in this case a cable modem with a fixed IP.

```
ip route 0.0.0.0 0.0.0.0 12.34.56.788
```

3.1.3 LAN Interface

This is the network that will be secured by the IPSec VPN

```
interface FastEthernet0/0
ip address 192.168.18.1 255.255.255.0
no shutdown
```

3.2 Tunnel Configuration

3.2.1 VPN Access Rules

This access rule is used by the Cisco router to match interesting traffic to be passed onto the VPN from the Local network to the remote network

```
ip access-list extended LR54-VPN
permit ip 192.168.18.0 0.0.0.255 192.168.54.0 0.0.0.255
```

3.2.2 IKE / ISAKMP

This configures the authentication / encryption and hash method for the IKE session
AES256, SHA1 , group 5, Pre-shared key. The Hash is default so does not show in configuration

```
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 5
```

3.2.3 Preshared Key

This is the password linked to the IKE ID passed during negotiation from the TransPort. The password in this case being “digidigi”

```
crypto isakmp key digidigi hostname LR54.digi.com no-xauth
```

3.2.4 DPD Configuration

Configure Dead Peer Detection

```
crypto isakmp keepalive 10 3 periodic
```

3.2.5 IPSec Transform

Configure IPSec encryption

```
crypto ipsec transform-set LR54 esp-aes 256 esp-sha-hmac
```

3.2.6 IPSec Crypto Map

Configure the Crypto Map used for this tunnel

```
crypto dynamic-map SDM_DYNMAP_1 1
 set transform-set LR54
 match address LR54-VPN

crypto map SDM_CMAP_1 65535 ipsec-isakmp dynamic SDM_DYNMAP_1
```

3.2.7 Map Crypto to the WAN interface

Assigned the Crypto Map to the WAN interface

```
interface FastEthernet0/1
crypto map SDM_CMAP_1
```

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 the **IKE** and **IPSec** configuration is done within the **ipsec** command.
The following command will show all available options:

```
ipsec 1 <Tab Key>
```

4.1 Configure Phase 1 settings

Configure the IKE Phase 1 settings to match the settings of the Cisco Router.

- IKE version 1
- SHA 1
- Group 5
- 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 group5
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<Tab Key>
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              aggressive            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 Cisco Router.

- Pre-shared key
- SHA 1
- Group 5
- 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 group5
digi.router> ipsec 1 esp-encryption aes256
digi.router> ipsec 1 lifetime 3600
digi.router> ipsec 1 psk digidigi
```

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

```
digi.router> ipsec 1 es<Tab Key>

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        aes256              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 Cisco Router.

- Local ID : LR54.digi.com
- Remote ID : **12.34.56.789**
- Local network : 192.168.54.0
- Local mask : 255.255.255.0
- Remote network : 192.168.18.0
- Remote mask : 255.255.255.0

Enter the parameters as follow:

```
digi.router> ipsec 1 local-id LR54.digi.com
digi.router> ipsec 1 remote-id 12.34.56.789
digi.router> ipsec 1 local-mask 255.255.255.0
digi.router> ipsec 1 local-network 192.168.54.0
digi.router> ipsec 1 remote-mask 255.255.255.0
digi.router> ipsec 1 remote-network 192.168.18.0
```

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

```
digi.router> ipsec 1 loc<Tab Key>

Configures an IPsec tunnel

Syntax:
ipsec 1 <parameter> <value>

Available Parameters:
 Parameter             Current Value       Description
-------------------------------------------------------------------------------
 local-id              LR54.digi.com       Local ID used for this IPsec tunnel
 local-mask            255.255.255.0       Local network mask for this IPsec tunnel
 local-network         192.168.54.0        Local network for this IPsec tunnel

digi.router> ipsec 1 rem<Tab Key>

Configures an IPsec tunnel

Syntax:
ipsec 1 <parameter> <value>

Available Parameters:
 Parameter             Current Value       Description
-------------------------------------------------------------------------------
 remote-id             12.34.56.789       Remote ID used for this IPsec tunnel
 remote-mask           255.255.255.0       Remote network mask for this tunnel
 remote-network        192.168.18.0        Remote network for this IPsec tunnel
```

4.3 Configure Peer address

To configure the Peer address, in this example, the WAN IP address of the Cisco 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      12.34.56.789     192.168.54.0/24     192.168.18.0/24     10 seconds
```

5 TESTING

Verify that data is going through the tunnel by issuing a ping from the Cisco router to the local Ethernet interface of the LR54. From command line issue the ping command with the source address of the local LAN interface

```
Router#ping 192.168.54.1 source fastEthernet 0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.54.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.18.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Router#
```

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 192.168.54.0/24 -d 192.168.18.0/24 -j ACCEPT
```

To check the firewall and view the rule:

```
digi.router> firewall -t nat -L -v

Chain PREROUTING (policy ACCEPT 1322 packets, 172K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 171 packets, 14562 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 176 packets, 13440 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 168 packets, 39850 bytes)
 pkts bytes target     prot opt in     out     source               destination
    8   600 ACCEPT     all  --  any    any     192.168.54.0/24      192.168.18.0/24
  494 29679 MASQUERADE  all  --  any    eth1    anywhere             anywhere
    0     0 MASQUERADE  all  --  any    cellular1  anywhere             anywhere
    0     0 MASQUERADE  all  --  any    cellular2  anywhere             anywhere
```

Ping should now be going through:

```
digi.router> ping 192.168.18.1

PING 192.168.18.1 (192.168.18.1) 56(84) bytes of data.
64 bytes from 192.168.18.1: icmp_seq=1 ttl=255 time=3.86 ms
64 bytes from 192.168.18.1: icmp_seq=2 ttl=255 time=0.483 ms
64 bytes from 192.168.18.1: icmp_seq=3 ttl=255 time=0.492 ms
64 bytes from 192.168.18.1: icmp_seq=4 ttl=255 time=0.522 ms
64 bytes from 192.168.18.1: icmp_seq=5 ttl=255 time=0.518 ms

--- 192.168.18.1 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
```

6 CONFIGURATION FILES

6.1 LR54 Configuration

```
system 1 timeout 3600
lan 1 description "Ethernet and Wi-Fi LAN network"
lan 1 interfaces "eth2,eth3,eth4"
lan 1 state "on"
lan 1 ip-address "192.168.54.1"
user 1 name "admin"
user 1 password
"$6$bN/3kMvPNYfiN4.G$9W4nFpcnDbUthqcgvUAT0p8Ieps4mQRBUOlBS4h85YnT1SUah63Ztmv1E7X0eC9i/Xl6uC/pe
VhvREiQUAVK2/"
ipsec 1 esp-diffie-hellman "group5"
ipsec 1 ike-diffie-hellman "group5"
ipsec 1 esp-encryption "aes256"
ipsec 1 ike-encryption "aes256"
ipsec 1 ike-mode "aggressive"
ipsec 1 local-mask "255.255.255.0"
ipsec 1 local-network "192.168.54.0"
ipsec 1 remote-mask "255.255.255.0"
ipsec 1 remote-network "192.168.18.0"
ipsec 1 peer "12.34.56.789"
ipsec 1 dpd "on"
ipsec 1 psk "$00$U2FsdGVkX189883PNPMNF+lxqVbtDRhB1rtcnfNQFMc="
ipsec 1 local-id "LR54.digi.com"
ipsec 1 remote-id "12.34.56.789"
ipsec 1 dpddelay 10
ipsec 1 dpdtimeout 30
ipsec 1 state "on"
dhcp-server 1 state "on"
dhcp-server 1 ip-address-start "192.168.54.100"
dhcp-server 1 ip-address-end "192.168.54.199"
dhcp-server 1 mask "255.255.255.0"
dhcp-server 1 gateway "192.168.54.1"
dhcp-server 1 dns1 "192.168.54.1"
wan 1 ip-address "192.168.9.54"
wan 1 gateway "192.168.9.253"
wan 1 dns1 "192.168.9.253"
wan 1 dhcp "off"
wan 1 interface "eth1"
wan 2 interface "cellular1"
wan 3 interface "cellular2"
 [FIREWALL]
*nat
-A POSTROUTING -s 192.168.54.0/24 -d 192.168.18.0/24 -j ACCEPT
COMMIT
[FIREWALL_END]
```

6.2 Cisco Configuration

```
Building configuration...

Current configuration : 1566 bytes
!
! Last configuration change at 13:17:00 UTC Thu Oct 6 2016
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
memory-size iomem 5
dot11 syslog
ip source-route
!
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
!
!
!
license udi pid CISCO1841 sn FCZ102822EM
!
redundancy
!
!
!
!
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 5
crypto isakmp key digidigi hostname LR54.digi.com no-xauth
crypto isakmp keepalive 10 3 periodic
!
!
crypto ipsec transform-set LR54 esp-aes 256 esp-sha-hmac
!
crypto dynamic-map SDM_DYNMAP_1 1
 set transform-set LR54
 match address LR54-VPN
!
!
```

```
crypto map SDM_CMAP_1 65535 ipsec-isakmp dynamic SDM_DYNMAP_1
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.18.1 255.255.255.0
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 12.34.56.789 255.255.255.248
 ip virtual-reassembly in
 duplex auto
 speed auto
 crypto map SDM_CMAP_1
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 12.34.56.788
!
ip access-list extended LR54-VPN
 permit ip 192.168.18.0 0.0.0.255 192.168.54.0 0.0.0.255
!
!
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
end
```