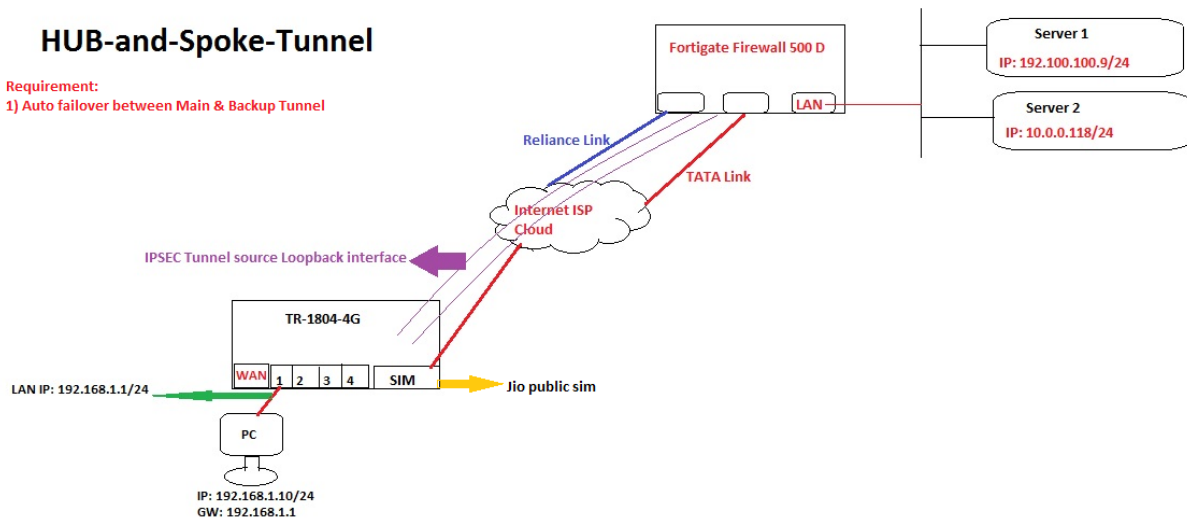


## Topology

### HUB-and-Spoke-Tunnel

Requirement:


1) Auto failover between Main & Backup Tunnel



## Cell Status

The screenshot shows the Techroutes TR-1804-4G Wireless Cellular Router/Modem status page. The page is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with the following items: Status, Overview, Network, Firewall, Routes, System Log, Kernel Log, Reboot Log, Realtime Graphs, VPN, System, Services, Network, and Logout. The main content area displays the following information:

- Status** (with an AUTO REFRESH ON button)
- System**
  - Hostname: TR-1815-LTE
  - SN: 860400153A000545
  - Firmware Version: 3.2.173
  - Kernel Version: 3.18.29
  - Local Time: Mon Jul 30 13:55:17 2018
  - Uptime: 0h 10m 29s
  - Load Average: 1.73, 1.97, 1.23
  - Port Status: LAN1, LAN2, LAN3, LAN4, WAN (indicated by icons)
- Mobile 1**
  - Cellular Status: Up
  - IP Address: 10.90.86.72/255.255.255.255

Cellular Status	Up
IP Address	10.90.86.72/255.255.255.255
DNS 1	49.45.0.1
DNS 2	
Cell Modem	SLM730_SLM750 (05C6_F601)
IMEI/ESN	868621029221243
Sim Status	SIM Ready
Strength	 25 / 31, dBm : -63
Selected Network	4G (LTE) only
Registered Network	Registered on Home network "JIO 4G", 7,
Sub Network Type	TDD LTE
Location Area Code	16
Cell ID	16F118
Band	40,38800
ICCID	89918740400031581709
RSRP	-96 dBm
RSRQ	-12 dB
SINR	9.0 dB
MSISDN/MSI	/405874003635168

## NAT Enable

Status

System

Services

Network

Operation Mode

Mobile

LAN

Wired WAN

WAN IPv6

Interfaces

Wi-Fi

Firewall

Switch

### Operation mode configuration

You may configure the operation mode suitable for you environment.

Operation mode

Bridge mode  
All ethernet and wireless interfaces are bridged into a single bridge interface.

Gateway mode  
The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

AP client mode  
The wireless ap client interface is treated as WAN port

Wired-WAN port role

Wired-WAN port acts as WAN

Wired-WAN port acts as LAN


NAT enable

Save & Apply Save Reset

## Cell Configuration

Status	General	Operator Selection	Data Limitation
System	<b>Mobile Configuration</b>		
Services	SIM 1		
Network	Enable <input checked="" type="checkbox"/>		
Operation Mode	Mobile connection: pppd mode		
Mobile	PIN code: <input type="text"/>		
LAN	Dialing number: *99#		
Wired WAN	APN: ltonet		
WAN IPv6	Authentication method: None		
Interfaces	Dual APN support: <input type="checkbox"/>		
Wi-Fi	Network Type: 4G (LTE) only		
Firewall	MTU: 1500		
Switch	Online mode: Keep Alive		
DHCP and DNS	Metric: 0		
Diagnostics			
Loopback Interface			
Hostnames			
Dynamic Routing			
Guest LAN(Guest WiFi)			
Static Routes			
QoS			

## LAN Configuration

		TR-1804-4G Wireless Cellular Router/Modem	
		<a href="#">UNSAVED CHANGES: 2</a> <a href="#">AUTO REFRESH ON</a>	
Status	<b>Interfaces - LAN</b>		
System	On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE.VLANID (e.g.: eth0.1).		
Services	<b>Common Configuration</b>		
Network	General Setup   <b>Advanced Settings</b>   Physical Settings   Firewall Settings		
Logout	Status:  br-lan   Uptime: 0h 10m 47s   MAC-Address: 90:22:06:00:08:37   RX: 634.72 KB (8701 Pkts.)   TX: 1.84 MB (8050 Pkts.)   IPv4: 192.168.1.1/24   IPv6: fdcd:06e0:bd35::1/60		
	Protocol: Static address		
	Really switch protocol? <input checked="" type="checkbox"/> Switch protocol		
	IPv4 address: 192.168.1.1		
	IPv4 netmask: 255.255.255.0		

## Loopback Configuration

**Techroutes** TR-1804-4G Wireless Cellular Router/Modem

**Loopback Interface Configuration**

IP address:

Netmask:

[Save & Apply](#) [Save](#) [Reset](#)

**Navigation Sidebar:** Status, System, Services, Network, Operation Mode, Mobile, LAN, Wired WAN, WAN IPv6, Interfaces, Wi-Fi, Firewall, Switch, DHCP and DNS, Diagnostics, Loopback Interface.

## IPSEC Main & Backup Configuration

**Techroutes** TR-1804-4G Wireless Cellular Router/Modem

IPSec | PPTP | L2TP | OpenVPN | GRE Tunnel

**IPsec Configuration**

Instance name	Enable	Exchange mode	Auth method	Operation level	
Reliance_Link	Yes	IKEv1-Aggressive	PSK Client	Main	<a href="#">Edit</a> <a href="#">Delete</a>
TATA_Link	Yes	IKEv1-Main	PSK Client	backup ( Reliance_Link )	<a href="#">Edit</a> <a href="#">Delete</a>

New instance name:  Client [Add](#)

**Navigation Sidebar:** Status, System, Services, ICMP Check, VRRP, Failover, DTU, SNMP, GPS, SMS, VPN.

## IPSEC Main Reliance Link Configuration

**Techroutes** TR-1804-4G Wireless Cellular Router/Modem

IPSec | PPTP | L2TP | OpenVPN | GRE Tunnel

**IPsec Instance: Reliance\_Link**

[Switch to advanced configuration >](#)

Enable

Exchange mode:

Operation Level:

Authentication method:

Remote VPN endpoint:

Local endpoint:

Local IKE Identifier:

Remote IKE Identifier:

Preshared Keys:

Perfect Forward Secrecy:

**Navigation Sidebar:** Status, System, Services, ICMP Check, VRRP, Failover, DTU, SNMP, GPS, SMS, VPN, DDNS, Connect Radio Module, NMS, Network, Logout.

Perfect Forward Secrecy

DPD action

DPD delay  seconds

DPD timeout  seconds

NAT Traversal

Local LAN bypass

Local subnet

Remote subnet

Local source ip

Remote source ip

**Phase 1 Proposal**

Enable

Encryption algorithm

Hash algorithm

DH group

Life time  seconds

**Phase 2 Proposal**

Enable


Encryption algorithm

PFS group

Authentication

Life time  seconds

[Save & Apply](#) [Save](#) [Reset](#)


TR-1804-4G Wireless Cellular Router/Modem

**Status**

---

**System**

---

**Services**

ICMP Check

VRRP

Failover

DTU

SNMP

GPS

SMS

VPN

DDNS

Connect Radio Module

NMS

---

**Network**

---

Logout

IPSec
PPTP
L2TP
OpenVPN
GRE Tunnel

**IPSec Instance: Reliance\_Link**

we can only enable IPSec ICMP check on Main tunnel, not on Backup tunnel

[Switch to basic configuration](#)

Enable ICMP check

ICMP Check type

Main Remote endpoint IP address


switch from backup to Main instance if ping succeed

Check interval

Check retries

[Save & Apply](#) [Save](#) [Reset](#)

# IPSec Backup Tata Link Configuration

TR-1804-4G Wireless Cellular Router/Modem

IPSec PPTP L2TP OpenVPN GRE Tunnel

### IPSec Instance: TATA\_Link

[Switch to advanced configuration »](#)

Enable

Exchange mode IKEv1-Main

Operation Level Backup

Backup for instance Reliance\_Link

Authentication method PSK Client

Remote VPN endpoint 14.141.165.149

Local endpoint interface:loopback

Local IKE identifier

Remote IKE identifier

Preshared Keys \*\*\*\*\*

Perfect Forward Secrecy Enable

Perfect Forward Secrecy Enable

DPD action Clear

DPD delay 30 seconds

DPD timeout 60 seconds

NAT Traversal Enable

Local LAN bypass

Local subnet 192.168.1.0/24

Remote subnet 192.100.100.0/24  
10.0.0.0/24

Local source ip

Remote source ip

### Phase 1 Proposal

Enable

Encryption algorithm: AES 128

Hash algorithm: HMAC\_MD5

DH group: MODP1024/2

Life time: 86400 seconds

### Phase 2 Proposal

Enable

Encryption algorithm: AES 128

PFS group: MODP1024/2

Authentication: HMAC\_SHA1

Life time: 43201 seconds

TR-1804-4G Wireless Cellular Router/Modem

**Status**

---

**System**

---

**Services**

- ICMP Check
- VRRRP
- Failover
- DTU
- SNMP
- GPS
- SMS
- VPN
- DDNS
- Connect Radio Module
- NMS

---

**Network**

---

**Logout**

IPSec   PPTP   L2TP   OpenVPN   GRE Tunnel

### IPSec Instance: TATA\_Link

we can only enable IPSec ICMP check on Main tunnel, not on Backup tunnel

« Switch to basic configuration

Enable ICMP check

ICMP Check type: Check remote VPN endpoint

Main Remote endpoint IP address: 115.254.59.45

switch from backup to Main instance if ping succeed

Check interval: 10

Check retries: 3

# Main tunnel up (Reliance link) IPSEC Status

The screenshot shows a web interface for IPsec status. At the top, there are tabs for 'IPSec', 'IPSec Log', 'OpenVPN', 'PPTP tunnel', and 'L2TP tunnel'. The 'IPSec' tab is selected. Below the tabs, there is a 'Refresh' button. The main content area displays the status of the IKE charon daemon (weakSwan 5.3.3, Linux 3.18.29, mips):

- uptime: 64 seconds, since Jul 30 13:58:22 2018
- malloc: sbrk 122880, mmap 0, used 108624, free 14256
- worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 6
- loaded plugins: charon random nonce aes des sha1 sha2 md5 pem pkcs1 gmp x509 revocation hmac stroke kernel-netlink socket-default updown xauth-generic
- Listening IP addresses:
  - 192.168.1.1
  - fd0d:66e6:bd35::1
  - 10.90.86.72

Connections:

- Reliance\_Link: %any, 115.254.59.45 IKEv1 Aggressive, dpddelay=30s
- Reliance\_Link: local: [10.90.86.72] uses pre-shared key authentication
- Reliance\_Link: remote: [115.254.59.45] uses pre-shared key authentication
- Reliance\_Link: child: 172.16.103.92/32 === 192.100.100.0/24 TUNNEL, dpdaction=clear
- Reliance\_Link\_1: %any, 115.254.59.45 IKEv1 Aggressive, dpddelay=30s
- Reliance\_Link\_1: local: [10.90.86.72] uses pre-shared key authentication
- Reliance\_Link\_1: remote: [115.254.59.45] uses pre-shared key authentication
- Reliance\_Link\_1: child: 172.16.103.92/32 === 10.0.0.0/24 TUNNEL, dpdaction=clear

Security Associations (1 up, 0 connecting):

- Reliance\_Link\_1[2]: ESTABLISHED 63 seconds ago, 10.90.86.72[10.90.86.72]\_115.254.59.45[115.254.59.45]
- Reliance\_Link\_1[2]: IKEv1 SPIs: 541c8e9ddcd0750a\_r1 a02db0dce899898a\_r, pre-shared key reauthentication in 7 hours
- Reliance\_Link\_1[2]: IKE proposal: 3DES\_CBC/HMAC\_MD5\_96/PRF\_HMAC\_MD5/MODP\_1024
- Reliance\_Link\_1[1]: INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: cdc91947\_i c857da51\_o
- Reliance\_Link\_1[1]: 3DES\_CBC/HMAC\_SHA1\_96, 6960 bytes\_i (116 pkts, 1s ago), 3480 bytes\_o (58 pkts, 1s ago), rekeying in 45 minutes
- Reliance\_Link\_1[1]: 172.16.103.92/32 === 192.100.100.0/24
- Reliance\_Link\_1[2]: INSTALLED, TUNNEL, reqid 2, ESP in UDP SPIs: c6dca084\_i c857da52\_o
- Reliance\_Link\_1[2]: 3DES\_CBC/HMAC\_SHA1\_96, 18959 bytes\_i (164 pkts, 1s ago), 63270 bytes\_o (249 pkts, 1s ago), rekeying in 41 minutes
- Reliance\_Link\_1[2]: 172.16.103.92/32 === 10.0.0.0/24

The first screenshot shows a Windows command prompt window with the command `ping 192.100.100.9`. The output shows 15 successful replies from 192.100.100.9, each with a TTL of 60 and varying response times between 54ms and 97ms.

```
Reply from 192.100.100.9: bytes=32 time=97ms TTL=60
Reply from 192.100.100.9: bytes=32 time=51ms TTL=60
Reply from 192.100.100.9: bytes=32 time=53ms TTL=60
Reply from 192.100.100.9: bytes=32 time=47ms TTL=60
Reply from 192.100.100.9: bytes=32 time=52ms TTL=60
Reply from 192.100.100.9: bytes=32 time=71ms TTL=60
Reply from 192.100.100.9: bytes=32 time=77ms TTL=60
Reply from 192.100.100.9: bytes=32 time=58ms TTL=60
Reply from 192.100.100.9: bytes=32 time=38ms TTL=60
Reply from 192.100.100.9: bytes=32 time=70ms TTL=60
Reply from 192.100.100.9: bytes=32 time=73ms TTL=60
Reply from 192.100.100.9: bytes=32 time=182ms TTL=60
Reply from 192.100.100.9: bytes=32 time=48ms TTL=60
Reply from 192.100.100.9: bytes=32 time=46ms TTL=60
Reply from 192.100.100.9: bytes=32 time=36ms TTL=60
Reply from 192.100.100.9: bytes=32 time=75ms TTL=60
Reply from 192.100.100.9: bytes=32 time=89ms TTL=60
Reply from 192.100.100.9: bytes=32 time=49ms TTL=60
Reply from 192.100.100.9: bytes=32 time=57ms TTL=60
Reply from 192.100.100.9: bytes=32 time=59ms TTL=60
Reply from 192.100.100.9: bytes=32 time=37ms TTL=60
Reply from 192.100.100.9: bytes=32 time=93ms TTL=60
Reply from 192.100.100.9: bytes=32 time=95ms TTL=60
Reply from 192.100.100.9: bytes=32 time=54ms TTL=60
```

The second screenshot shows a Windows command prompt window with the command `ping 10.0.0.118 -t`. The output shows 20 successful replies from 192.100.100.9, each with a TTL of 60 and varying response times between 44ms and 78ms.

```
Reply from 192.100.100.9: bytes=32 time=78ms TTL=60
Reply from 192.100.100.9: bytes=32 time=64ms TTL=60
Reply from 192.100.100.9: bytes=32 time=41ms TTL=60
Reply from 192.100.100.9: bytes=32 time=27ms TTL=60
Reply from 192.100.100.9: bytes=32 time=51ms TTL=60
Reply from 192.100.100.9: bytes=32 time=92ms TTL=60
Reply from 192.100.100.9: bytes=32 time=37ms TTL=60
Reply from 192.100.100.9: bytes=32 time=34ms TTL=60
Reply from 192.100.100.9: bytes=32 time=56ms TTL=60
Reply from 192.100.100.9: bytes=32 time=49ms TTL=60
Reply from 192.100.100.9: bytes=32 time=47ms TTL=60
Reply from 192.100.100.9: bytes=32 time=47ms TTL=60
Reply from 192.100.100.9: bytes=32 time=85ms TTL=60
Reply from 192.100.100.9: bytes=32 time=58ms TTL=60
Reply from 192.100.100.9: bytes=32 time=97ms TTL=60
Reply from 192.100.100.9: bytes=32 time=88ms TTL=60
Reply from 192.100.100.9: bytes=32 time=62ms TTL=60
Reply from 192.100.100.9: bytes=32 time=156ms TTL=60
Reply from 192.100.100.9: bytes=32 time=47ms TTL=60
Reply from 192.100.100.9: bytes=32 time=81ms TTL=60
Reply from 192.100.100.9: bytes=32 time=95ms TTL=60
Reply from 192.100.100.9: bytes=32 time=47ms TTL=60
Reply from 192.100.100.9: bytes=32 time=44ms TTL=60
```



Status Overview Network Firewall Routes System Log Kernel Log Reboot Log Realtime Graphs VPN System Services Network Logout

IPSec IPSec Log OpenVPN PPTP tunnel L2TP tunnel

### IPSec Status

Refresh

Status of IKE charon daemon (weakSwan 5.3.3, Linux 3.18.29, mips):  
 uptime: 108 seconds, since Jul 30 13:58:22 2018  
 malloc: sbrk 122880, mmap 0, used 108624, free 14256  
 worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 6  
 loaded plugins: charon random nonce aes des sha1 sha2 md5 pem pkcs1 gmp x509 revocation hmac stroke kernel-netlink socket-default updown xauth-generic  
 Listening IP addresses:  
 192.168.1.1  
 fd:d66e:bd35:1  
 10.90.86.72

Connections:  
 Reliance\_Link: %any, 115.254.59.45 IKEv1 Aggressive, dpddelay=30s  
 Reliance\_Link: local: [10.90.86.72] uses pre-shared key authentication  
 Reliance\_Link: remote: [115.254.59.45] uses pre-shared key authentication  
 Reliance\_Link: child: 172.16.103.92/32 === 192.100.100.0/24 TUNNEL, dpdaction=clear  
 Reliance\_Link\_1: %any, 115.254.59.45 IKEv1 Aggressive, dpddelay=30s  
 Reliance\_Link\_1: local: [10.90.86.72] uses pre-shared key authentication  
 Reliance\_Link\_1: remote: [115.254.59.45] uses pre-shared key authentication  
 Reliance\_Link\_1: child: 172.16.103.92/32 === 10.0.0.0/24 TUNNEL, dpdaction=clear  
 Security Associations (1 up, 0 connecting):  
 Reliance\_Link\_1[2]: ESTABLISHED 107 seconds ago, 10.90.86.72[10.90.86.72]...115.254.59.45[115.254.59.45]  
 Reliance\_Link\_1[2]: IKEv1 SPIs: 541cbe9ddc0750a\_1 a02db0dce899898a\_r, pre-shared key reauthentication in 7 hours  
 Reliance\_Link\_1[2]: IKE proposal: 3DES\_CBC/HMAC\_MD5\_96/PRF\_HMAC\_MD5/MODP\_1024  
 Reliance\_Link\_1[1]: INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: cdc094f\_1 c857da51\_o  
 Reliance\_Link\_1[1]: 3DES\_CBC/HMAC\_SHA1\_96, 11760 bytes\_i (196 pkts, 1s ago), 5940 bytes\_o (99 pkts, 1s ago), rekeying in 44 minutes  
 Reliance\_Link\_1[1]: 172.16.103.92/32 === 192.100.100.0/24  
 Reliance\_Link\_1[2]: INSTALLED, TUNNEL, reqid 2, ESP in UDP SPIs: c6dca084\_i c857da52\_o  
 Reliance\_Link\_1[2]: 3DES\_CBC/HMAC\_SHA1\_96, 35533 bytes\_i (298 pkts, 1s ago), 114621 bytes\_o (451 pkts, 1s ago), rekeying in 40 minutes  
 Reliance\_Link\_1[2]: 172.16.103.92/32 === 10.0.0.0/24

## Main tunnel down (Reliance link) then automatically Backup tunnel up (Tata link)

```

C:\Windows\system32\cmd.exe - ping 192.100.100.9 -t
Reply from 192.100.100.9: bytes=32 ttime=63ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=54ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=54ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=54ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=56ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=60ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=59ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=44ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=56ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=45ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=60ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=49ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=57ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=59ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=60ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=60ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=63ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=55ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=55ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=65ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=45ms TTL=60
Request timed out.
Request timed out.
Request timed out.
Request timed out.

C:\Windows\system32\cmd.exe - ping 10.0.0.118 -t
Reply from 192.100.100.9: bytes=32 ttime=45ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=49ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=57ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=57ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=38ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=36ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=41ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=40ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=43ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=31ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=50ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=46ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=36ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=49ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=45ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=37ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=38ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=37ms TTL=60
Reply from 192.100.100.9: bytes=32 ttime=47ms TTL=60
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

```

```

C:\Windows\system32\cmd.exe - ping 192.100.100.9 -t
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.100.100.9: bytes=32 time=91ms TTL=252
Reply from 192.100.100.9: bytes=32 time=97ms TTL=60
Reply from 192.100.100.9: bytes=32 time=85ms TTL=60
Reply from 192.100.100.9: bytes=32 time=40ms TTL=60
Reply from 192.100.100.9: bytes=32 time=40ms TTL=60
Reply from 192.100.100.9: bytes=32 time=59ms TTL=60

C:\Windows\system32\cmd.exe - ping 10.0.0.118 -t
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.100.100.9: bytes=32 time=91ms TTL=60
Reply from 192.100.100.9: bytes=32 time=91ms TTL=60
Reply from 192.100.100.9: bytes=32 time=47ms TTL=60
Reply from 192.100.100.9: bytes=32 time=47ms TTL=60
Reply from 192.100.100.9: bytes=32 time=66ms TTL=60

```

**Techroutes**  
NETWORK
TR-1804-4G Wireless Cellular Router/Modem

---

Status

IPSec
IPSec Log
OpenVPN
PPTP tunnel
L2TP tunnel

- Overview
- Network
- Firewall
- Routes
- System Log
- Kernel Log
- Reboot Log
- Realtime Graphs
- VPN
- System
- Services
- Network
- Logout

### IPSec Status

Refresh


Status of IKE charon daemon (weakSwan 5.3.3, Linux 3.18.29, mips):  
 uptime: 25 seconds, since Jul 30 14:03:11 2018  
 malloc: sbrk 114688, mmap 0, used 106656, free 8032  
 worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4  
 loaded plugins: charon random nonce aes des sha1 sha2 md5 pem pkcs1 gmp x509 revocation hmac stroke kernel-netlink socket-default updown xauth-generic  
 Listening IP addresses:  
 192.168.1.1  
 ffd:666:bd35:1  
 10.90.86.72  
 Connections:  
 TATA\_Link %any\_14.141.165.149 IKEv1, dpddelay=30s  
 TATA\_Link local: [10.90.86.72] uses pre-shared key authentication  
 TATA\_Link remote: [14.141.165.149] uses pre-shared key authentication  
 TATA\_Link child: 172.16.103.92/32 === 192.100.100.0/24 TUNNEL, dpdaction=clear  
 TATA\_Link\_1: child: 172.16.103.92/32 === 10.0.0.0/24 TUNNEL, dpdaction=clear  
 Security Associations (1 up, 0 connecting):  
 TATA\_Link[1]: ESTABLISHED 24 seconds ago, 10.90.86.72[10.90.86.72]\_14.141.165.149[14.141.165.149]  
 TATA\_Link[1]: IKEv1 SPIs: 2fe7928a11c724fa\_\*7e509faede3bf9ec\_0, pre-shared key reauthentication in 23 hours  
 TATA\_Link[1]: IKE proposal: AES\_CBC\_128/HMAC\_MD5\_96/PRF\_HMAC\_MD5/MODP\_1024  
 TATA\_Link[1]: INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c3392098\_j c857dabf\_o  
 TATA\_Link[1]: AES\_CBC\_128/HMAC\_SHA1\_96, 2400 bytes\_j (40 pkts, 1s ago), 1200 bytes\_o (20 pkts, 1s ago), rekeying in 11 hours  
 TATA\_Link[1]: 172.16.103.92/32 === 192.100.100.0/24  
 TATA\_Link\_1[2]: INSTALLED, TUNNEL, reqid 2, ESP in UDP SPIs: c206d3d5\_j c857dac0\_o  
 TATA\_Link\_1[2]: AES\_CBC\_128/HMAC\_SHA1\_96, 2500 bytes\_j (21 pkts, 6s ago), 9118 bytes\_o (43 pkts, 1s ago), rekeying in 11 hours  
 TATA\_Link\_1[2]: 172.16.103.92/32 === 10.0.0.0/24

```

C:\Windows\system32\cmd.exe - ping 192.100.100.9 -t
Reply From 192.100.100.9: bytes=32 time=84ms TTL=60
Reply From 192.100.100.9: bytes=32 time=36ms TTL=60
Reply From 192.100.100.9: bytes=32 time=39ms TTL=60
Reply From 192.100.100.9: bytes=32 time=66ms TTL=60
Reply From 192.100.100.9: bytes=32 time=40ms TTL=60
Reply From 192.100.100.9: bytes=32 time=93ms TTL=60
Reply From 192.100.100.9: bytes=32 time=93ms TTL=60
Reply From 192.100.100.9: bytes=32 time=85ms TTL=60
Reply From 192.100.100.9: bytes=32 time=36ms TTL=60
Reply From 192.100.100.9: bytes=32 time=62ms TTL=60
Reply From 192.100.100.9: bytes=32 time=93ms TTL=60
Reply From 192.100.100.9: bytes=32 time=87ms TTL=60
Reply From 192.100.100.9: bytes=32 time=48ms TTL=60
Reply From 192.100.100.9: bytes=32 time=41ms TTL=60
Reply From 192.100.100.9: bytes=32 time=80ms TTL=60
Reply From 192.100.100.9: bytes=32 time=52ms TTL=60
Reply From 192.100.100.9: bytes=32 time=54ms TTL=60
Reply From 192.100.100.9: bytes=32 time=76ms TTL=60
Reply From 192.100.100.9: bytes=32 time=75ms TTL=60
Reply From 192.100.100.9: bytes=32 time=38ms TTL=60
Reply From 192.100.100.9: bytes=32 time=60ms TTL=60
Reply From 192.100.100.9: bytes=32 time=72ms TTL=60
Reply From 192.100.100.9: bytes=32 time=37ms TTL=60
Reply From 192.100.100.9: bytes=32 time=46ms TTL=60

C:\Windows\system32\cmd.exe - ping 10.0.0.118 -t
Reply From 192.100.100.9: bytes=32 time=90ms TTL=60
Reply From 192.100.100.9: bytes=32 time=37ms TTL=60
Reply From 192.100.100.9: bytes=32 time=70ms TTL=60
Reply From 192.100.100.9: bytes=32 time=38ms TTL=60
Reply From 192.100.100.9: bytes=32 time=86ms TTL=60
Reply From 192.100.100.9: bytes=32 time=92ms TTL=60
Reply From 192.100.100.9: bytes=32 time=93ms TTL=60
Reply From 192.100.100.9: bytes=32 time=42ms TTL=60
Reply From 192.100.100.9: bytes=32 time=62ms TTL=60
Reply From 192.100.100.9: bytes=32 time=101ms TTL=60
Reply From 192.100.100.9: bytes=32 time=95ms TTL=60
Reply From 192.100.100.9: bytes=32 time=48ms TTL=60
Reply From 192.100.100.9: bytes=32 time=47ms TTL=60
Reply From 192.100.100.9: bytes=32 time=80ms TTL=60
Reply From 192.100.100.9: bytes=32 time=70ms TTL=60
Reply From 192.100.100.9: bytes=32 time=58ms TTL=60
Reply From 192.100.100.9: bytes=32 time=91ms TTL=60
Reply From 192.100.100.9: bytes=32 time=89ms TTL=60
Reply From 192.100.100.9: bytes=32 time=51ms TTL=60
Reply From 192.100.100.9: bytes=32 time=89ms TTL=60
Reply From 192.100.100.9: bytes=32 time=109ms TTL=60
Reply From 192.100.100.9: bytes=32 time=58ms TTL=60
Reply From 192.100.100.9: bytes=32 time=45ms TTL=60

```



## TR-1804-4G Wireless Cellular Router/Modem

---

**Status**

Overview

Network

Firewall

Routes

System Log

Kernel Log

Reboot Log

Realtime Graphs

**VPN**

System

Services

Network

Logout

IPSec   **IPSec Log**   OpenVPN   PPTP tunnel   L2TP tunnel

### IPSec Status

Refresh

Status of IKE charon daemon (weakSwan 5.3.3, Linux 3.18.29, mips):  
 uptime: 53 seconds, since Jul 30 14:03:11 2018  
 malloc: sbrk 114688, mmap 0, used 106856, free 8032  
 worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0, scheduled: 4  
 loaded plugins: charon random nonce aes des sha1 sha2 md5 pem pkcs1 gmp x509 revocation hmac stroke kernel-netlink socket-default updown xauth-generic  
 Listening IP addresses:  
 192.168.1.1  
 fd:d:66e6:bd35::1  
 10.90.86.72  
 Connections:  
 TATA\_Link %any..14.141.165.149 IKEv1, dpddelay=30s  
 TATA\_Link local: [10.90.86.72] uses pre-shared key authentication  
 TATA\_Link remote: [14.141.165.149] uses pre-shared key authentication  
 TATA\_Link child: 172.16.103.92/32 === 192.100.100.0/24 TUNNEL, dpdaction=clear  
 TATA\_Link\_1: child: 172.16.103.92/32 === 10.0.0.0/24 TUNNEL, dpdaction=clear  
 Security Associations (1 up, 0 connecting):  
 TATA\_Link[1]: ESTABLISHED 52 seconds ago, 10.90.86.72[10.90.86.72]..14.141.165.149[14.141.165.149]  
 TATA\_Link[1]: IKEv1 SPIs: 2fe7928a11c724fa\_\*7e509faede3bf9ec\_r, pre-shared key reauthentication in 23 hours  
 TATA\_Link[1]: IKE proposal: AES\_CBC\_128/HMAC\_MD5\_96/PRF\_HMAC\_MD5/MODP\_1024  
 TATA\_Link[1]: INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c3392098\_j c857dabf\_o  
 TATA\_Link[1]: AES\_CBC\_128/HMAC\_SHA1\_96, 5760 bytes\_j (96 pkts, 18446744073709551615s ago), 2880 bytes\_o (48 pkts, 18446744073709551615s ago), rekeying in 11 hours  
 TATA\_Link[1]: 172.16.103.92/32 === 192.100.100.0/24  
 TATA\_Link[1(2): INSTALLED, TUNNEL, reqid 2, ESP in UDP SPIs: c206d3d5\_j c857dac0\_o  
 TATA\_Link[1(2): AES\_CBC\_128/HMAC\_SHA1\_96, 2500 bytes\_j (21 pkts, 35s ago), 10798 bytes\_o (71 pkts, 1s ago), rekeying in 11 hours  
 TATA\_Link[1(2): 172.16.103.92/32 === 10.0.0.0/24

```

Jul 30 14:03:11 [IKEv1] received stroke, initiate TATA_Link_1
Jul 30 14:03:11 [NET] <TATA_Link1> received packet: from 14.141.165.149[500] to 10.90.86.72[500] (148 bytes)
Jul 30 14:03:11 [ENC] <TATA_Link1> parsed ID_PROT response 0 [ SA V V V ]
Jul 30 14:03:11 [IKE] <TATA_Link1> received NAT-T (RFC 3947) vendor ID
Jul 30 14:03:11 [IKE] <TATA_Link1> received DPD vendor ID
Jul 30 14:03:11 [ENC] <TATA_Link1> received unknown vendor ID: 82:99:03:17:57:a3:60:82:c5:a6:21:de:00:00:00:00
Jul 30 14:03:11 [NET] <TATA_Link1> generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
Jul 30 14:03:11 [NET] <TATA_Link1> sending packet: from 10.90.86.72[500] to 14.141.165.149[500] (236 bytes)
Jul 30 14:03:11 [NET] <TATA_Link1> received packet: from 14.141.165.149[500] to 10.90.86.72[500] (220 bytes)
Jul 30 14:03:11 [ENC] <TATA_Link1> parsed ID_PROT response 0 [ KE No NAT-D NAT-D ]
Jul 30 14:03:11 [IKE] <TATA_Link1> local host is behind NAT, sending keep alive
Jul 30 14:03:11 [NET] <TATA_Link1> generating ID_PROT request 0 [ ID HASH N(INITIAL_CONTACT) ]
Jul 30 14:03:11 [NET] <TATA_Link1> sending packet: from 10.90.86.72[4500] to 14.141.165.149[4500] (92 bytes)
Jul 30 14:03:12 [NET] <TATA_Link1> received packet: from 14.141.165.149[4500] to 10.90.86.72[4500] (76 bytes)
Jul 30 14:03:12 [ENC] <TATA_Link1> parsed ID_PROT response 0 [ ID HASH ]
Jul 30 14:03:12 [IKE] <TATA_Link1> IKE_SA TATA_Link1 established between 10.90.86.72[10.90.86.72]...14.141.165.149[14.141.165.149]
Jul 30 14:03:12 [IKE] <TATA_Link1> scheduling reauthentication in 85788s
Jul 30 14:03:12 [IKE] <TATA_Link1> maximum IKE_SA lifetime 86328s
Jul 30 14:03:12 [ENC] <TATA_Link1> generating QUICK_MODE request 3797477768 [ HASH SA No KE ID ID ]
Jul 30 14:03:12 [NET] <TATA_Link1> sending packet: from 10.90.86.72[4500] to 14.141.165.149[4500] (316 bytes)
Jul 30 14:03:12 [NET] <TATA_Link1> received packet: from 14.141.165.149[4500] to 10.90.86.72[4500] (300 bytes)
Jul 30 14:03:12 [ENC] <TATA_Link1> parsed QUICK_MODE response 3797477768 [ HASH SA No KE ID ID ]
Jul 30 14:03:12 [0] <TATA_Link1> policy already exists, try to update it
Jul 30 14:03:12 [0] <TATA_Link1> policy already exists, try to update it
Jul 30 14:03:12 [0] <TATA_Link1> policy already exists, try to update it
Jul 30 14:03:12 [0] <TATA_Link1> CHILD_SA TATA_Link1 established with SPIs c3392098_i c857dabf_o and TS 172.16.103.92/32 === 192.100.100.0/24
Jul 30 14:03:13 [0] <TATA_Link1> generating QUICK_MODE request 3797477768 [ HASH ]
Jul 30 14:03:13 [NET] <TATA_Link1> sending packet: from 10.90.86.72[4500] to 14.141.165.149[4500] (60 bytes)
Jul 30 14:03:13 [0] <TATA_Link1> generating QUICK_MODE request 4275136958 [ HASH SA No KE ID ID ]
Jul 30 14:03:13 [NET] <TATA_Link1> sending packet: from 10.90.86.72[4500] to 14.141.165.149[4500] (316 bytes)
Jul 30 14:03:13 [0] <TATA_Link1> received packet: from 14.141.165.149[4500] to 10.90.86.72[4500] (300 bytes)
Jul 30 14:03:13 [0] <TATA_Link1> parsed QUICK_MODE response 4275136958 [ HASH SA No KE ID ID ]
Jul 30 14:03:14 [0] <TATA_Link1> policy already exists, try to update it
Jul 30 14:03:14 [0] <TATA_Link1> policy already exists, try to update it
Jul 30 14:03:14 [0] <TATA_Link1> policy already exists, try to update it
Jul 30 14:03:14 [0] <TATA_Link1> CHILD_SA TATA_Link_12 established with SPIs c206d3d5_i c857dac0_o and TS 172.16.103.92/32 === 10.0.0.0/24
Jul 30 14:03:14 [0] <TATA_Link1> updown: uci: invalid argument
Jul 30 14:03:14 [0] <TATA_Link1> updown: uci: invalid argument
Jul 30 14:03:14 [0] <TATA_Link1> generating QUICK_MODE request 4275136958 [ HASH ]
Jul 30 14:03:14 [NET] <TATA_Link1> sending packet: from 10.90.86.72[4500] to 14.141.165.149[4500] (60 bytes)

```

Again Main tunnel up (Reliance link) automatically Backup tunnel down (Tata link)

```

C:\Windows\system32\cmd.exe - ping 192.100.100.9
Reply from 192.100.100.9: bytes=32 time=49ms TTL=60
Reply from 192.100.100.9: bytes=32 time=48ms TTL=60
Reply from 192.100.100.9: bytes=32 time=67ms TTL=60
Reply from 192.100.100.9: bytes=32 time=51ms TTL=60
Reply from 192.100.100.9: bytes=32 time=64ms TTL=60
Reply from 192.100.100.9: bytes=32 time=46ms TTL=60
Reply from 192.100.100.9: bytes=32 time=46ms TTL=60
Reply from 192.100.100.9: bytes=32 time=47ms TTL=60
Reply from 192.100.100.9: bytes=32 time=48ms TTL=60
Reply from 192.100.100.9: bytes=32 time=46ms TTL=60
Reply from 192.100.100.9: bytes=32 time=48ms TTL=60
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.100.100.9: bytes=32 time=71ms TTL=252
Reply from 192.100.100.9: bytes=32 time=66ms TTL=252
Reply from 192.100.100.9: bytes=32 time=240ms TTL=252
Reply from 192.100.100.9: bytes=32 time=89ms TTL=252
Reply from 192.100.100.9: bytes=32 time=70ms TTL=252
Reply from 192.100.100.9: bytes=32 time=74ms TTL=60
Reply from 192.100.100.9: bytes=32 time=75ms TTL=60
Reply from 192.100.100.9: bytes=32 time=40ms TTL=60

C:\Windows\system32\cmd.exe - ping 10.0.0.118
Reply from 192.100.100.9: bytes=32 time=79ms TTL=60
Reply from 192.100.100.9: bytes=32 time=50ms TTL=60
Reply from 192.100.100.9: bytes=32 time=45ms TTL=60
Reply from 192.100.100.9: bytes=32 time=86ms TTL=60
Reply from 192.100.100.9: bytes=32 time=65ms TTL=60
Reply from 192.100.100.9: bytes=32 time=46ms TTL=60
Reply from 192.100.100.9: bytes=32 time=88ms TTL=60
Reply from 192.100.100.9: bytes=32 time=52ms TTL=60
Reply from 192.100.100.9: bytes=32 time=60ms TTL=60
Reply from 192.100.100.9: bytes=32 time=73ms TTL=60
Reply from 192.100.100.9: bytes=32 time=82ms TTL=60
Reply from 192.100.100.9: bytes=32 time=84ms TTL=60
Reply from 192.100.100.9: bytes=32 time=86ms TTL=60
Reply from 192.100.100.9: bytes=32 time=87ms TTL=60
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.100.100.9: bytes=32 time=86ms TTL=60
Reply from 192.100.100.9: bytes=32 time=89ms TTL=60
Reply from 192.100.100.9: bytes=32 time=85ms TTL=60
Reply from 192.100.100.9: bytes=32 time=47ms TTL=60

```

Overview
Network
Firewall
Routes
System Log
Kernel Log
Reboot Log
Realtime Graphs
VPN
System
Services
Network
Logout

## IPSec Status

 Refresh

```
Status of IKE charon daemon (weakSwan 5.3.3, Linux 3.18.29, mips):
uptime: 20 seconds, since Jul 30 14:10:17 2018
malloc: sbrk 122880, mmap 0, used 108792, free 14088
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 7
loaded plugins: charon random nonce aes des sha1 sha2 md5 pem pkcs1 gmp x509 revocation hmac stroke kernel-netlink socket-default updown xauth-generic
Listening IP addresses:
192.168.1.1
fdfd:66e6:bd35::1
10.90.86.72
Connections:
Reliance_Link: %any..115.254.59.45 IKEv1 Aggressive, dpddelay=30s
Reliance_Link: local: [10.90.86.72] uses pre-shared key authentication
Reliance_Link: remote: [115.254.59.45] uses pre-shared key authentication
Reliance_Link: child: 172.16.103.92/32 === 192.100.100.0/24 TUNNEL, dpdaction=clear
Reliance_Link_1: %any..115.254.59.45 IKEv1 Aggressive, dpddelay=30s
Reliance_Link_1: local: [10.90.86.72] uses pre-shared key authentication
Reliance_Link_1: remote: [115.254.59.45] uses pre-shared key authentication
Reliance_Link_1: child: 172.16.103.92/32 === 10.0.0.0/24 TUNNEL, dpdaction=clear
Security Associations (1 up, 0 connecting):
Reliance_Link_1[2]: ESTABLISHED 17 seconds ago, 10.90.86.72[10.90.86.72]..115.254.59.45[115.254.59.45]
Reliance_Link_1[2]: IKEv1 SPIs: a3f6fab7703330e..1*6b286a73bed64ab1_r, pre-shared key reauthentication in 7 hours
Reliance_Link_1[2]: IKE proposal: 3DES_CBC_HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
Reliance_Link(1): INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: cd566bbc_j c857db62_o
Reliance_Link(1): 3DES_CBC_HMAC_SHA1_96, 1680 bytes_j (28 pkts, 1s ago), 1020 bytes_o (17 pkts, 0s ago), rekeying in 44 minutes
Reliance_Link(1): 172.16.103.92/32 === 192.100.100.0/24
Reliance_Link_1[2]: INSTALLED, TUNNEL, reqid 2, ESP in UDP SPIs: c48466bb_j c857db63_o
Reliance_Link_1[2]: 3DES_CBC_HMAC_SHA1_96, 360 bytes_j (6 pkts, 6s ago), 1140 bytes_o (19 pkts, 0s ago), rekeying in 42 minutes
Reliance_Link_1[2]: 172.16.103.92/32 === 10.0.0.0/24
```

Overview
Network
Firewall
Routes
System Log
Kernel Log
Reboot Log
Realtime Graphs
VPN
System
Services
Network
Logout

```
Jul 30 14:10:18 01[NET] <Reliance_Link_1[2]> received packet from 115.254.59.45[500] to 10.90.86.72[500] (264 bytes)
Jul 30 14:10:18 01[ENC] <Reliance_Link_1[2]> parsed AGGRESSIVE response 0 [SA KE No ID HASH V NAT-D NAT-D V V]
Jul 30 14:10:18 01[KE] <Reliance_Link_1[2]> received NAT-T (RFC 3947) vendor ID
Jul 30 14:10:18 01[KE] <Reliance_Link_1[2]> received DPD vendor ID
Jul 30 14:10:18 01[ENC] <Reliance_Link_1[2]> received unknown vendor ID: 82:99:03:17:57:a3:60:82:c6:a6:21:de:00:00:00:00
Jul 30 14:10:18 02[ENC] <Reliance_Link_1[2]> generating QUICK_MODE request 2000509438 [HASH SA No KE ID ID]
Jul 30 14:10:18 02[NET] <Reliance_Link_1[2]> sending packet from 10.90.86.72[4500] to 115.254.59.45[4500] (300 bytes)
Jul 30 14:10:18 13[NET] <Reliance_Link_1[2]> received packet from 115.254.59.45[4500] to 10.90.86.72[4500] (284 bytes)
Jul 30 14:10:18 13[ENC] <Reliance_Link_1[2]> parsed QUICK_MODE response 2000509438 [HASH SA No KE ID ID]
Jul 30 14:10:19 01[KE] <Reliance_Link_1[2]> local host is behind NAT, sending keep alives
Jul 30 14:10:19 13[KE] <Reliance_Link_1[2]> CHILD_SA Reliance_Link_1[2] established with SPIs cd566bbc_j c857db62_o and TS 172.16.103.92/32 === 192.100.100.0/24
Jul 30 14:10:20 13[ENC] <Reliance_Link_1[2]> generating QUICK_MODE request 2000509438 [HASH ]
Jul 30 14:10:20 13[NET] <Reliance_Link_1[2]> sending packet from 10.90.86.72[4500] to 115.254.59.45[4500] (52 bytes)
Jul 30 14:10:20 01[KE] <Reliance_Link_1[2]> detected reauth of existing IKE_SA, adopting 1 children and 0 virtual IPs
Jul 30 14:10:20 01[KE] <Reliance_Link_1[2]> IKE_SA Reliance_Link_1[2] established between 10.90.86.72[10.90.86.72]..115.254.59.45[115.254.59.45]
Jul 30 14:10:20 01[KE] <Reliance_Link_1[2]> scheduling reauthentication in 28051s
Jul 30 14:10:20 01[KE] <Reliance_Link_1[2]> maximum IKE_SA lifetime 28591s
Jul 30 14:10:20 01[ENC] <Reliance_Link_1[2]> generating AGGRESSIVE request 0 [HASH NAT-D NAT-D]
Jul 30 14:10:20 01[NET] <Reliance_Link_1[2]> sending packet from 10.90.86.72[4500] to 115.254.59.45[4500] (92 bytes)
Jul 30 14:10:20 01[ENC] <Reliance_Link_1[2]> generating QUICK_MODE request 2121225840 [HASH SA No KE ID ID]
Jul 30 14:10:20 01[NET] <Reliance_Link_1[2]> sending packet from 10.90.86.72[4500] to 115.254.59.45[4500] (300 bytes)
Jul 30 14:10:20 14[NET] <Reliance_Link_1[2]> received packet from 115.254.59.45[4500] to 10.90.86.72[4500] (284 bytes)
Jul 30 14:10:20 14[ENC] <Reliance_Link_1[2]> parsed QUICK_MODE response 2121225840 [HASH SA No KE ID ID]
Jul 30 14:10:21 14[KE] <Reliance_Link_1[2]> CHILD_SA Reliance_Link_1[2] established with SPIs c48466bb_j c857db63_o and TS 172.16.103.92/32 === 10.0.0.0/24
Jul 30 14:10:21 14[CHD] <Reliance_Link_1[2]> updown: uci: invalid argument
Jul 30 14:10:21 14[CHD] <Reliance_Link_1[2]> updown: uci: invalid argument
Jul 30 14:10:22 14[ENC] <Reliance_Link_1[2]> generating QUICK_MODE request 2121225840 [HASH ]
Jul 30 14:10:22 14[NET] <Reliance_Link_1[2]> sending packet from 10.90.86.72[4500] to 115.254.59.45[4500] (52 bytes)
Jul 30 14:10:30 04[KE] <Reliance_Link_1[2]> deleting IKE_SA Reliance_Link_1[2] between 10.90.86.72[10.90.86.72]..115.254.59.45[115.254.59.45]
Jul 30 14:10:30 04[KE] <Reliance_Link_1[2]> generating DELETE for IKE_SA Reliance_Link_1[2]
Jul 30 14:10:30 04[ENC] <Reliance_Link_1[2]> generating INFORMATIONAL_V1 request 1470048019 [HASH D]
Jul 30 14:10:30 04[NET] <Reliance_Link_1[2]> sending packet from 10.90.86.72[4500] to 115.254.59.45[4500] (84 bytes)
```

Overview
Network
Firewall
Routes
System Log
Kernel Log
Reboot Log
Realtime Graphs
VPN
System
Services
Network
Logout

## IPSec Status

 Refresh

```
Status of IKE charon daemon (weakSwan 5.3.3, Linux 3.18.29, mips):
uptime: 108 seconds, since Jul 30 14:10:17 2018
malloc: sbrk 122880, mmap 0, used 108640, free 14240
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 6
loaded plugins: charon random nonce aes des sha1 sha2 md5 pem pkcs1 gmp x509 revocation hmac stroke kernel-netlink socket-default updown xauth-generic
Listening IP addresses:
192.168.1.1
fdfd:66e6:bd35::1
10.90.86.72
Connections:
Reliance_Link: %any..115.254.59.45 IKEv1 Aggressive, dpddelay=30s
Reliance_Link: local: [10.90.86.72] uses pre-shared key authentication
Reliance_Link: remote: [115.254.59.45] uses pre-shared key authentication
Reliance_Link: child: 172.16.103.92/32 === 192.100.100.0/24 TUNNEL, dpdaction=clear
Reliance_Link_1: %any..115.254.59.45 IKEv1 Aggressive, dpddelay=30s
Reliance_Link_1: local: [10.90.86.72] uses pre-shared key authentication
Reliance_Link_1: remote: [115.254.59.45] uses pre-shared key authentication
Reliance_Link_1: child: 172.16.103.92/32 === 10.0.0.0/24 TUNNEL, dpdaction=clear
Security Associations (1 up, 0 connecting):
Reliance_Link_1[2]: ESTABLISHED 105 seconds ago, 10.90.86.72[10.90.86.72]..115.254.59.45[115.254.59.45]
Reliance_Link_1[2]: IKEv1 SPIs: a3f6fab7703330e..1*6b286a73bed64ab1_r, pre-shared key reauthentication in 7 hours
Reliance_Link_1[2]: IKE proposal: 3DES_CBC_HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
Reliance_Link(1): INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: cd566bbc_j c857db62_o
Reliance_Link(1): 3DES_CBC_HMAC_SHA1_96, 12240 bytes_j (204 pkts, 1s ago), 6240 bytes_o (104 pkts, 1s ago), rekeying in 43 minutes
Reliance_Link(1): 172.16.103.92/32 === 192.100.100.0/24
Reliance_Link_1[2]: INSTALLED, TUNNEL, reqid 2, ESP in UDP SPIs: c48466bb_j c857db63_o
Reliance_Link_1[2]: 3DES_CBC_HMAC_SHA1_96, 17663 bytes_j (260 pkts, 1s ago), 34198 bytes_o (363 pkts, 1s ago), rekeying in 40 minutes
Reliance_Link_1[2]: 172.16.103.92/32 === 10.0.0.0/24
```