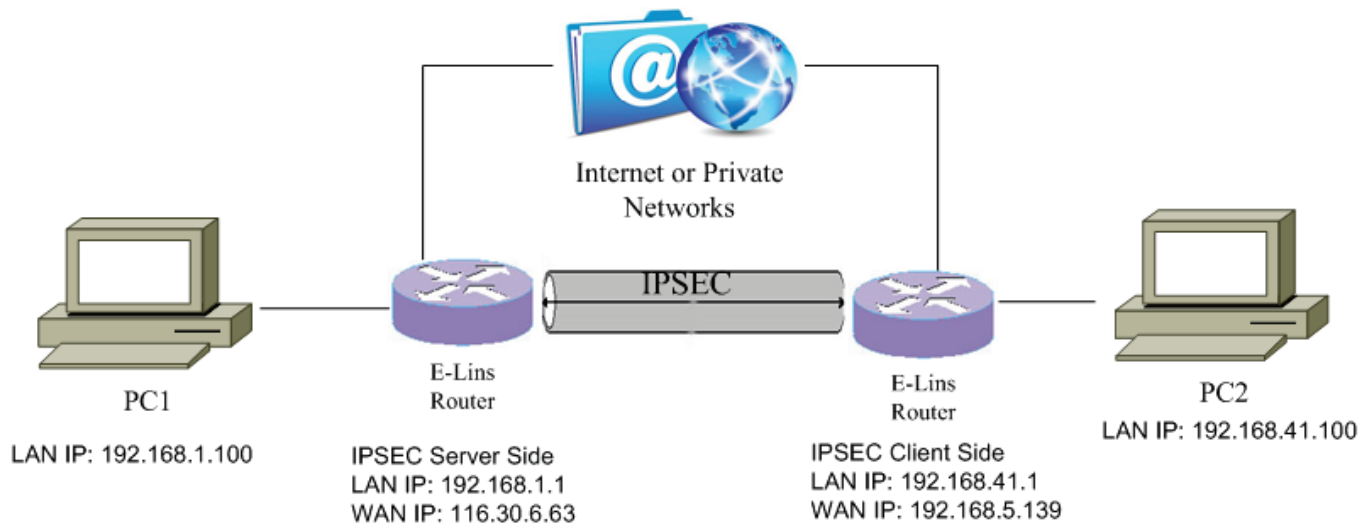


VPN Setting Example - IPSEC

IPSEC Topology



IPSEC Server Side

1. Make sure the IPSEC Server Router is online.



The screenshot shows the WAN Status page. On the left is a navigation menu with 'Network' highlighted. The main content area has tabs for 'Mobile', 'Mobile 2', 'WAN', and 'LAN', with 'WAN' selected. The title is 'WAN Status'. Below it, there's a table for 'IPv4 WAN Status' with the following data:

Port	pppoe-wan
Protocol:	pppoe
Address:	116.30.6.63
Netmask:	255.255.255.255
Gateway:	116.30.4.1
DNS 1:	202.96.128.166
DNS 2:	202.96.134.133
Uptime:	1h 27m 44s
Mac Addr:	00:00:00:00:00:00
RX	23.07 MB (37977 Pkts.)
TX	4.01 MB (29648 Pkts.)

- Open web management page, click "Services" -> "VPN" at the left navigation bar, then click "IPSEC" to open IPSEC Configuration page.

The screenshot shows the IPsec Configuration page. On the left is a navigation menu with 'VPN' highlighted. The main content area has tabs for 'IPSec', 'PPTP', 'L2TP', 'OpenVPN', and 'GRE Tunnel', with 'IPSec' selected. The title is 'IPsec Configuration'. Below it is a table with the following data:

Instance name	Enable	Exchange mode	Auth method	Operation level	
ipsec_base	No	IKEv1-Main	Server		Edit Delete

Below the table, there is a form for adding a new instance:


New instance name: Client

If there is no IPSEC server instance in the list, input new instance name, select "Server" as role, and then click button "Add New".

Click button "Edit" in the list to configure IPSEC server.

3. Checked "Enable", set parameters as below,

ICMP Check	
VRRP	
Failover	
SNMP	
DTU	
GPS	
SMS	
VPN	
DDNS	
Connect Radio Module	
Network	
Logout	

IPSec Configuration	
Enable	<input checked="" type="checkbox"/>
Exchange mode	IKEv1-Main
Operation Level	Main
Authentication method	Server
Remote VPN endpoint	Any
Local endpoint	interface:wlan
Local IKE identifier	
Remote IKE identifier	
Preshared Keys 
Perfect Forward Secrecy	Enable
DPD action	Clear
DPD delay	30 seconds

Click button  behind password can show/hide password.

Select "Clear" for "DPD action".



DPD timeout seconds

NAT Traversal

Local LAN bypass

Local subnet

Remote subnet

Phase 1 Proposal

Encryption algorithm

Hash algorithm

DH group

Life time seconds



Phase 2 Proposal

Encryption algorithm	AES 128	▼
PFS group	MODP1024/2	▼
Authentication	HMAC_SHA1	▼
Life time	3600	seconds

Save & Apply

Save

Reset

Click button "Save & Apply" if everything is done.

IPSEC Client Side

1. Make sure the IPSEC Client Router is online.

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

Mobile	WAN	LAN
--------	-----	-----

Mobile Status

Mobile 1

Cellular Status	Up
Cell Modem	TRICHEER_LM92XX (1C9E_9B07)
IMEI/ESN	862234024935001
Sim Status	SIM Ready
Strength	31 / 31, dBm : -79
Selected Network	Automatic
Registered Network	Registered on Home network: "CHN-CT ?????", 7,
Sub Network Type	LTE FDD

2. Check if IPSEC Client Router can visit IPSEC Server Router without IPSEC. If cannot visit, the IPSEC will not be connected.

The screenshot shows the router's web management interface. On the left is a navigation menu with 'Diagnostics' highlighted. The main content area is titled 'Diagnostics' and 'Network Utilities'. It features a form with a text input containing '116.30.6.63', a dropdown menu set to 'IPv4', and a 'Ping' button. Below the form, the results of the ping test are displayed, showing 5 successful pings with round-trip times between 41.178 ms and 42.497 ms, and 0% packet loss.

3. Open web management page, click "Services" -> "VPN" at the left navigation bar, then click "IPSEC" to open IPSEC Configuration page.

The screenshot shows the router's web management interface for IPsec configuration. The left navigation menu has 'VPN' highlighted. The main content area is titled 'IPsec Configuration' and has 'IPSec' selected in the top tabs. A table lists the existing IPsec instances:

Instance name	Enable	Exchange mode	Auth method	Operation level
ipsec_base	Yes	IKEv1-Main	Client	Main

Below the table, there is a form to add a new instance with a 'New instance name:' field and a dropdown menu set to 'Client'. The 'Add' button is visible. The 'ipsec_base' row in the table has 'Edit' and 'Delete' buttons.

Input new instance name, the example we input "ipsec_base", and then select "Client" as role, finally Click Button "Add".

Click button "Edit" in the row of "ipsec_base" instance.



IPSec Configuration

Enable	<input checked="" type="checkbox"/>
Exchange mode	<input type="text" value="IKEv1-Main"/>
Operation Level	<input type="text" value="Main"/>
Authentication method	<input type="text" value="Client"/>
Remote VPN endpoint	<input type="text" value="116.30.6.63"/>
Local endpoint	<input type="text" value="interface:ifmobile"/>
Local IKE identifier	<input type="text"/>
Remote IKE identifier	<input type="text"/>
Preshared Keys	<input type="text" value="....."/>
Perfect Forward Secrecy	<input type="text" value="Enable"/>
DPD action	<input type="text" value="Restart"/>
DPD delay	<input type="text" value="30"/> seconds
DPD timeout	<input type="text" value="150"/> seconds
NAT Traversal	<input type="text" value="Enable"/>



Local LAN bypass

Local subnet

Remote subnet

Phase 1 Proposal

Encryption algorithm

Hash algorithm

DH group

Life time seconds

Phase 2 Proposal

Encryption algorithm

PFS group

Authentication

Life time seconds

Checked "Enable", fill in value of "Remote VPN endpoint" as IPSEC Server WAN IP address. Here our IPSEC Server Router has WAN IP address 116.30.6.63 and LAN IP address 192.168.1.1;

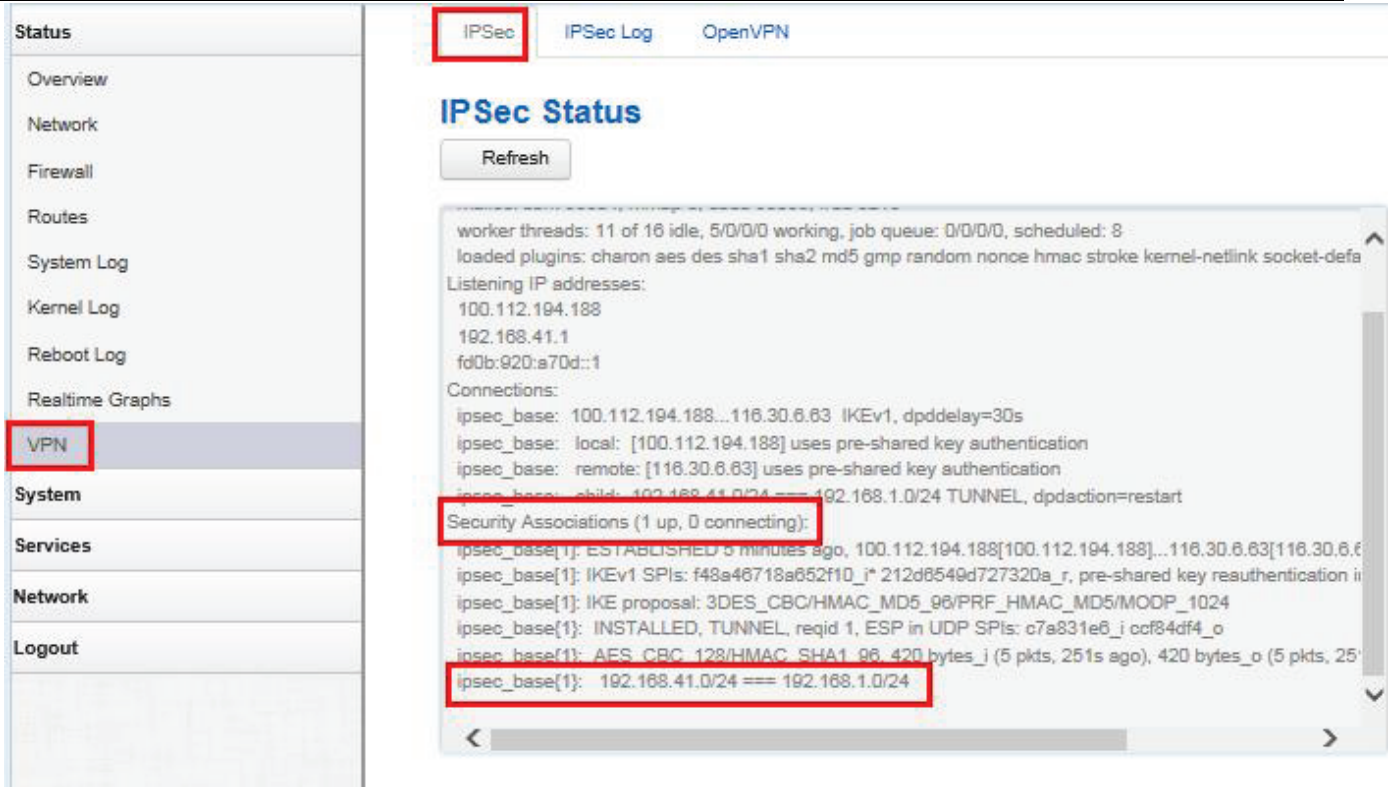
Local endpoint: select the correct WAN for IPSEC Client Router. In this example, the Client Router goes with mobile.

Preshared Keys: set password we configured on IPSEC server;

DPD action: select "Restart".

Click button "Save & Apply" if everything is done.

4. Wait some seconds until the IPSEC Client Router connects to IPSEC Server Router via IPSEC. Check the link status of IPSEC Client Router.



The screenshot displays the IPsec configuration interface. On the left, a navigation menu has 'VPN' highlighted. The main panel shows 'IPSec Status' with a 'Refresh' button. Below is a log window showing the following text:

```
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 8
loaded plugins: charon aes des sha1 sha2 md5 gmp random nonce hmac stroke kernel-netlink socket-defa
Listening IP addresses:
100.112.194.188
192.168.41.1
fd0b:920:a70d::1
Connections:
ipsec_base: 100.112.194.188...116.30.6.63 IKEv1, dpddelay=30s
ipsec_base: local: [100.112.194.188] uses pre-shared key authentication
ipsec_base: remote: [116.30.6.63] uses pre-shared key authentication
ipsec_base: child: 192.168.41.0/24 === 192.168.1.0/24 TUNNEL, dpdaction=restart
Security Associations (1 up, 0 connecting):
ipsec_base(1): ESTABLISHED 5 minutes ago, 100.112.194.188[100.112.194.188]...116.30.6.63[116.30.6.63]
ipsec_base(1): IKEv1 SPIs: f48a46718a652f10_i* 212d6549d727320a_r, pre-shared key reauthentication i
ipsec_base(1): IKE proposal: 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
ipsec_base(1): INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c7a831e6_i ccf84df4_o
ipsec_base(1): AES_CBC_128/HMAC_SHA1_96_420 bytes_j (5 pkts, 251s ago), 420 bytes_o (5 pkts, 25
ipsec_base(1): 192.168.41.0/24 === 192.168.1.0/24
```

Once the IPSEC connection is up, the IPSEC Client Router will display IPSEC IP address at “Status—VPN--IPSec”.

5. Ping from IPSEC Client Router to IPSEC Server Router (with LAN IP 192.168.1.1)



Status
System
Services
Network
Operation Mode
Mobile
LAN
Wired WAN
WAN IPv6
Interfaces
Wi-Fi
Firewall
Static Routes
Switch
DHCP and DNS
Diagnostics
Loopback Interface
Hostnames

Diagnostics

Network Utilities

192.168.1.1	www.google.com	www.google.com
IPv4 <input type="button" value="v"/>	<input type="button" value="Ping"/>	<input type="button" value="Traceroute"/>
		<input type="button" value="Nslookup"/>

```
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=55.095 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=46.356 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=46.856 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=47.915 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=45.856 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 45.856/48.415/55.095 ms
```