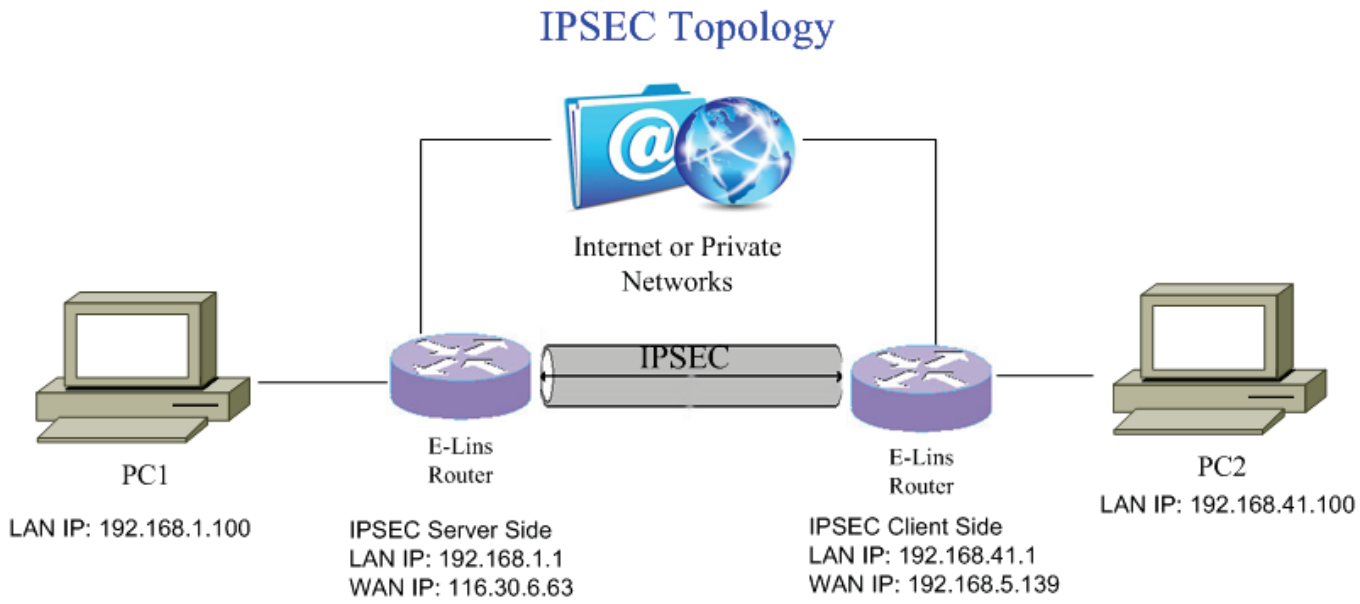
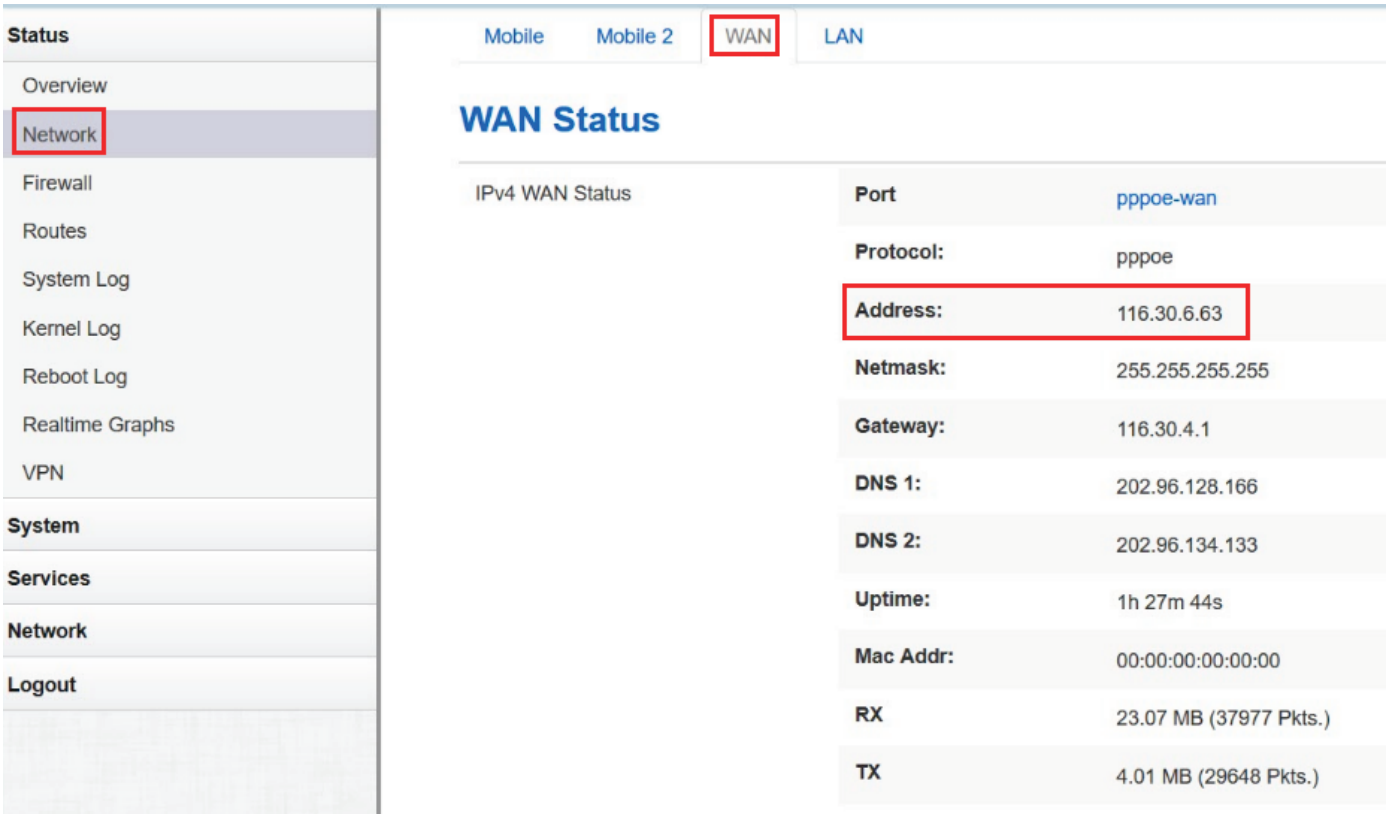
VPN Setting Example - IPSEC

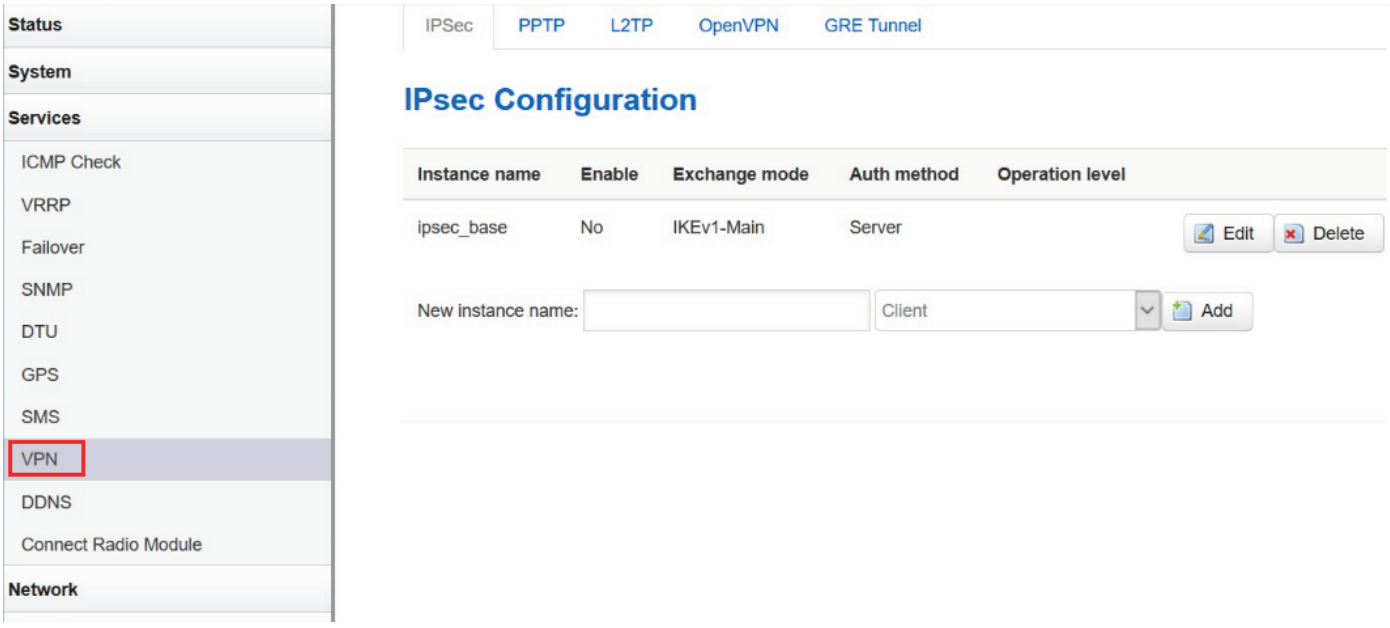


IPSEC Server Side

1. Make sure the IPSEC Server Router is online.



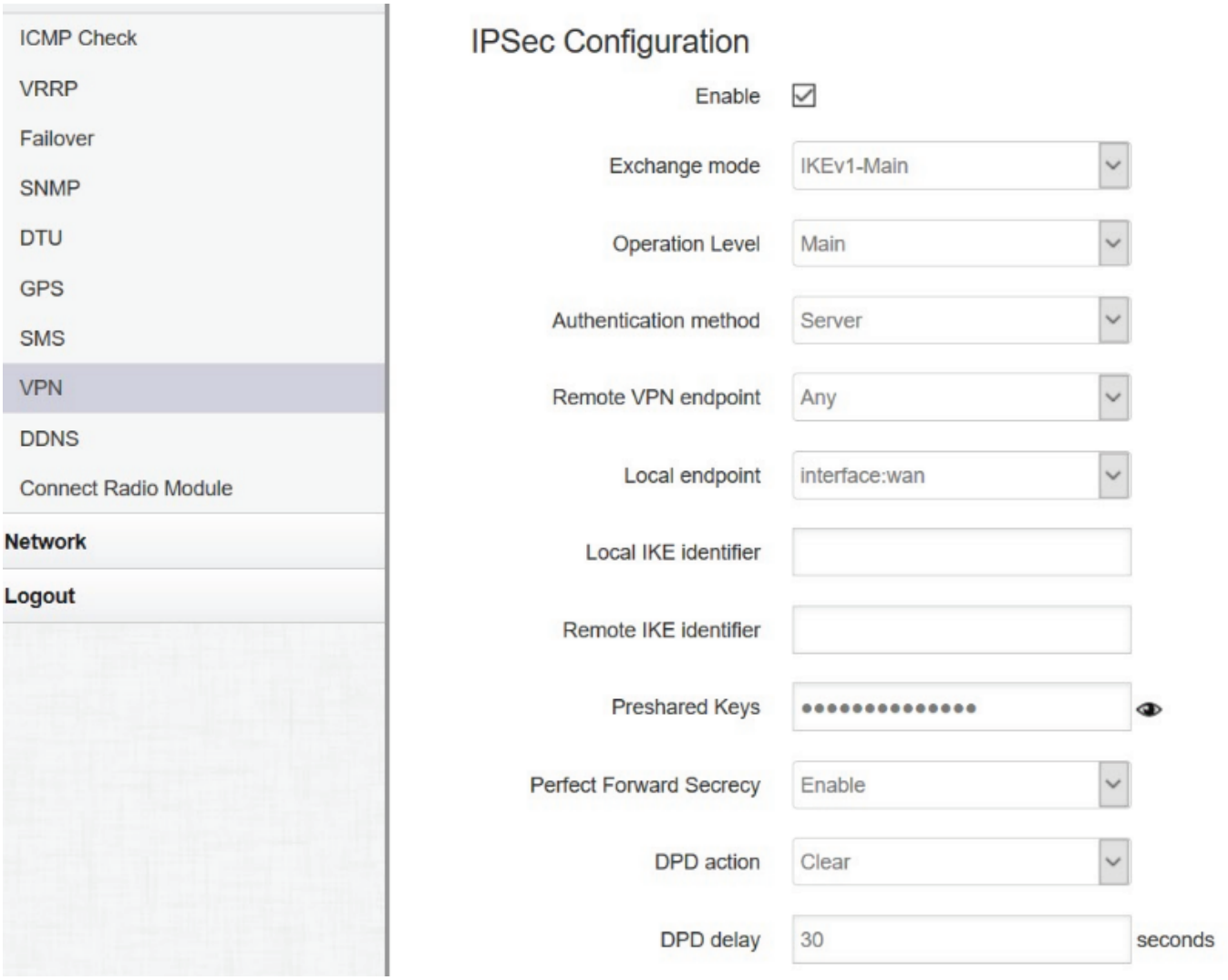
2. Open web management page, click “Services”-→”VPN” at the left navigation bar, then click “IPSEC” to open IPSEC Configuration page.



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

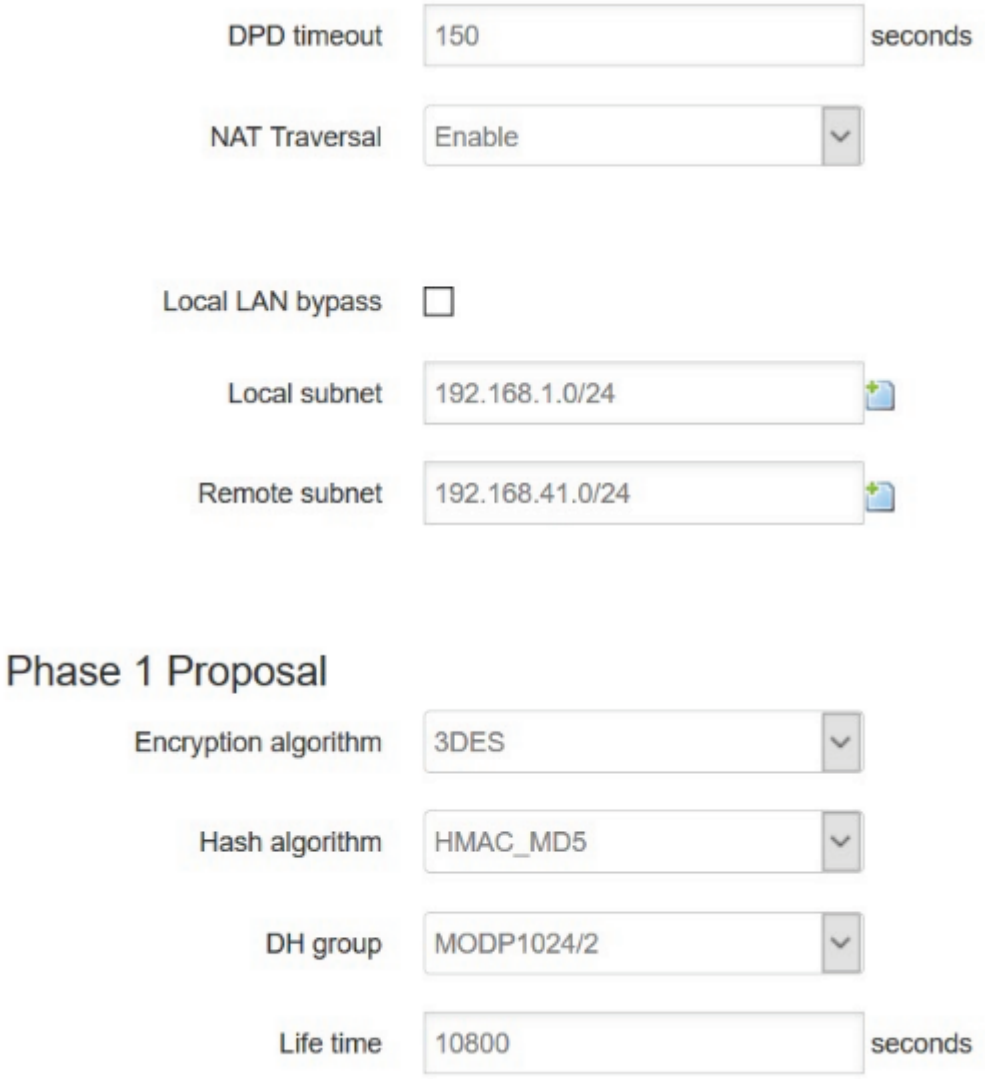
Click button “Edit” in the list to configure IPSEC server.

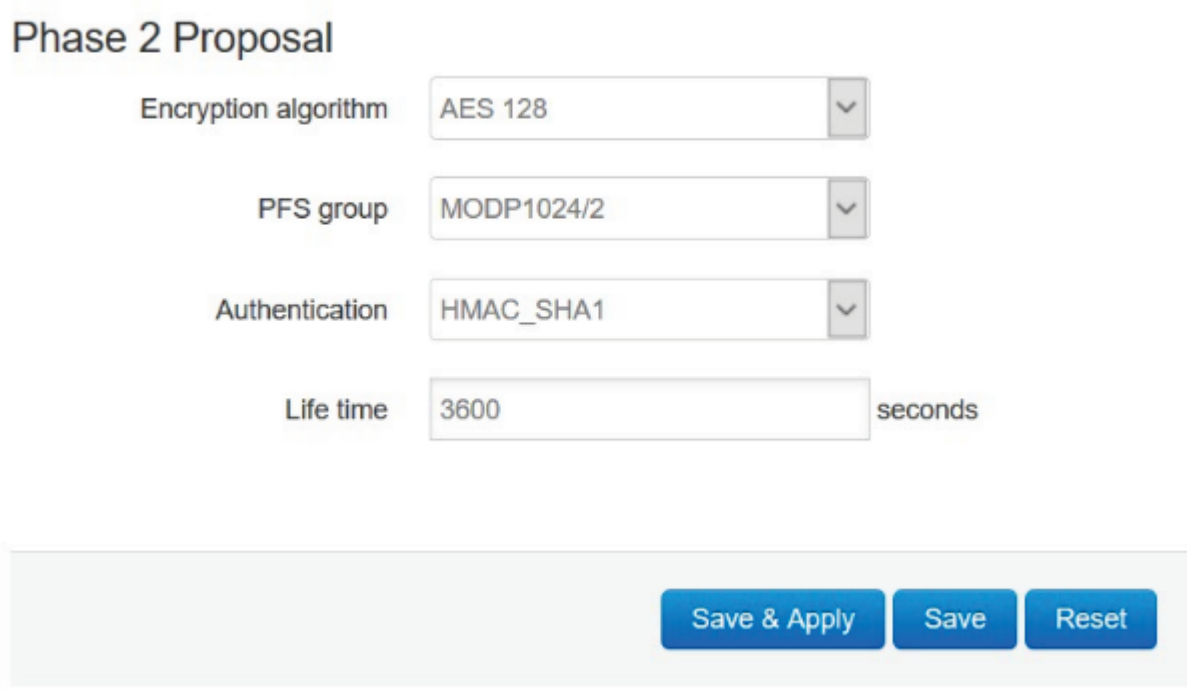
3. Checked “Enable”, set parameters as below,



Click button behind password can show/hide password.

Select “Clear” for “DPD action”.

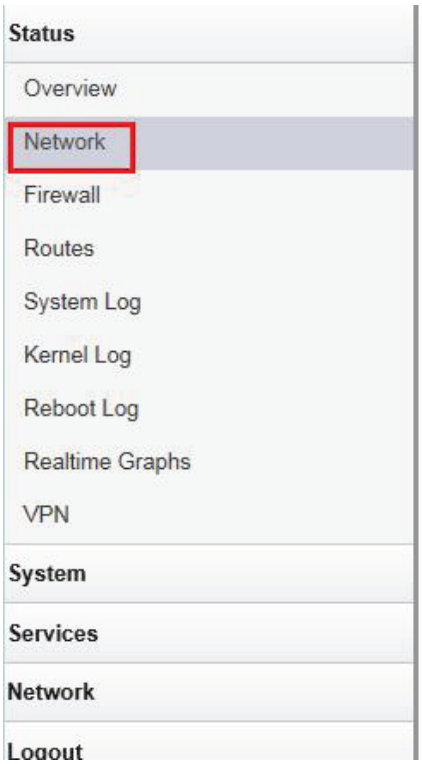

DPD timeout
150
seconds
NAT Traversal
Enable
Local LAN bypass
Local subnet
192.168.1.0/24
Remote subnet
192.168.41.0/24
Phase 1 Proposal
Encryption algorithm
3DES
Hash algorithm
HMAC_MD5
DH group
MODP1024/2
Life time
10800
seconds

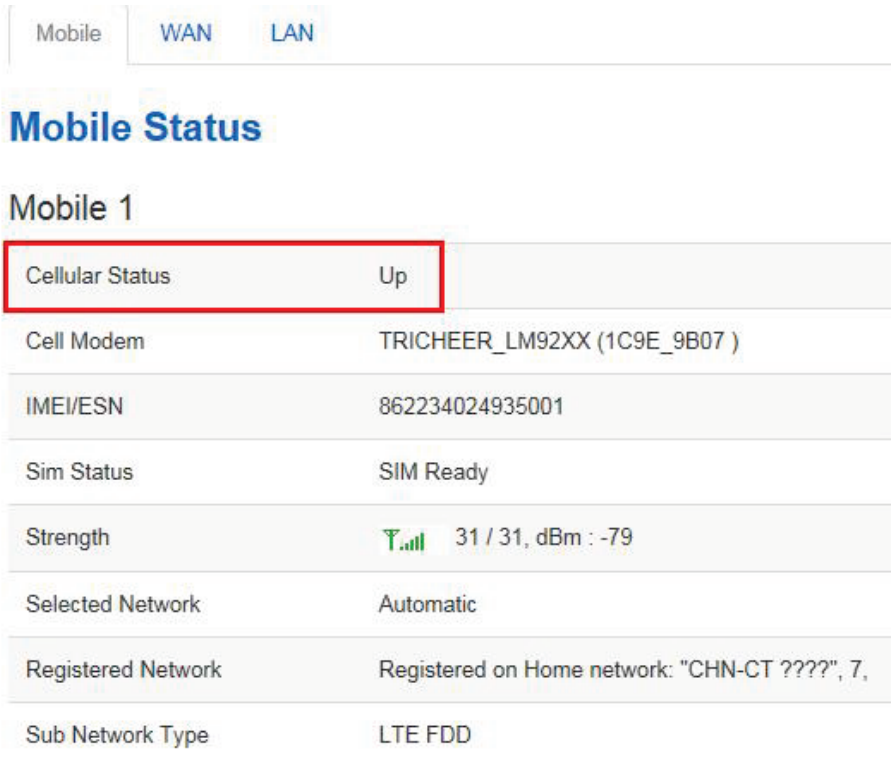


Click button “Save & Apply” if everything is done.

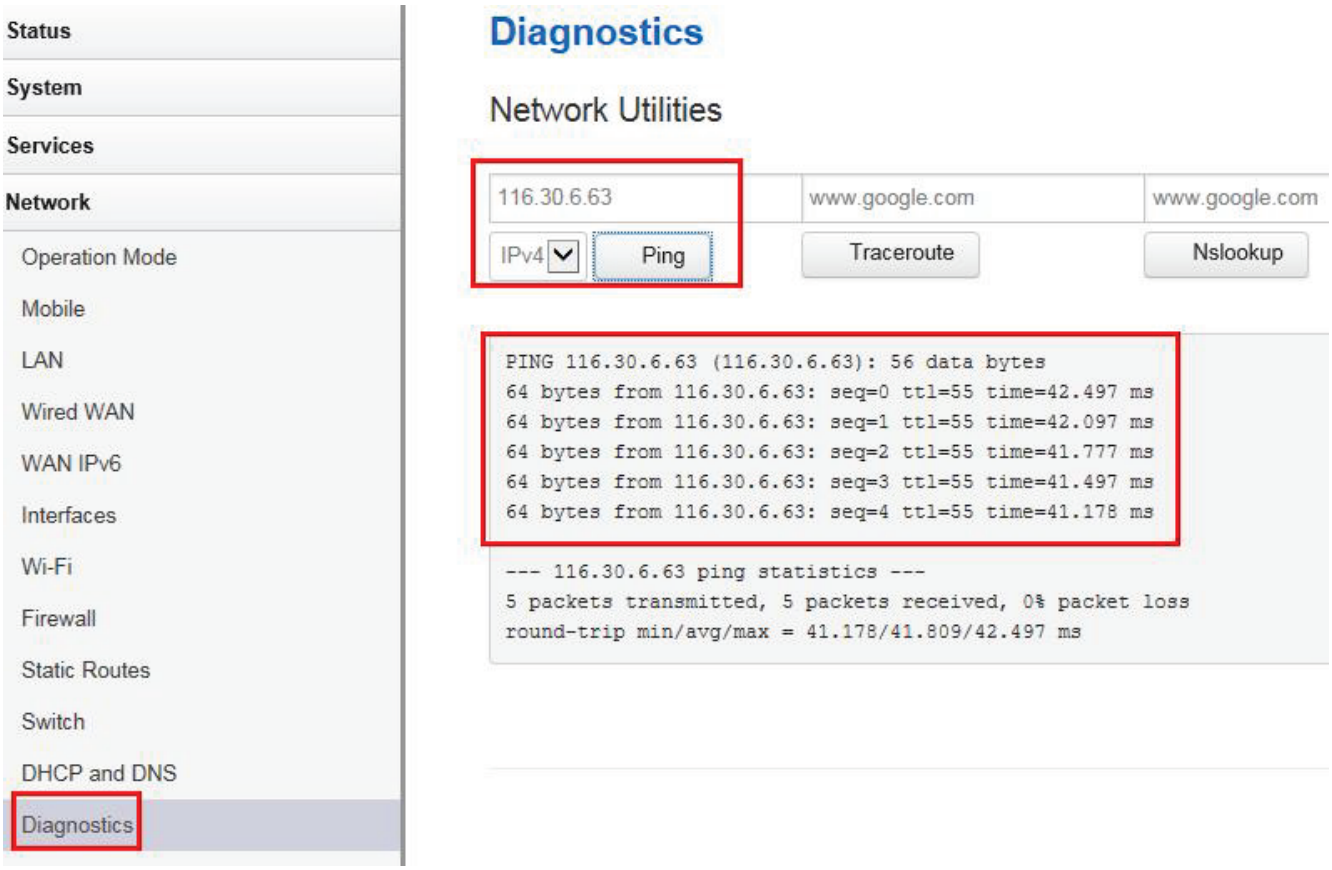
IPSEC Client Side

1. Make sure the IPSEC Client Router is online.

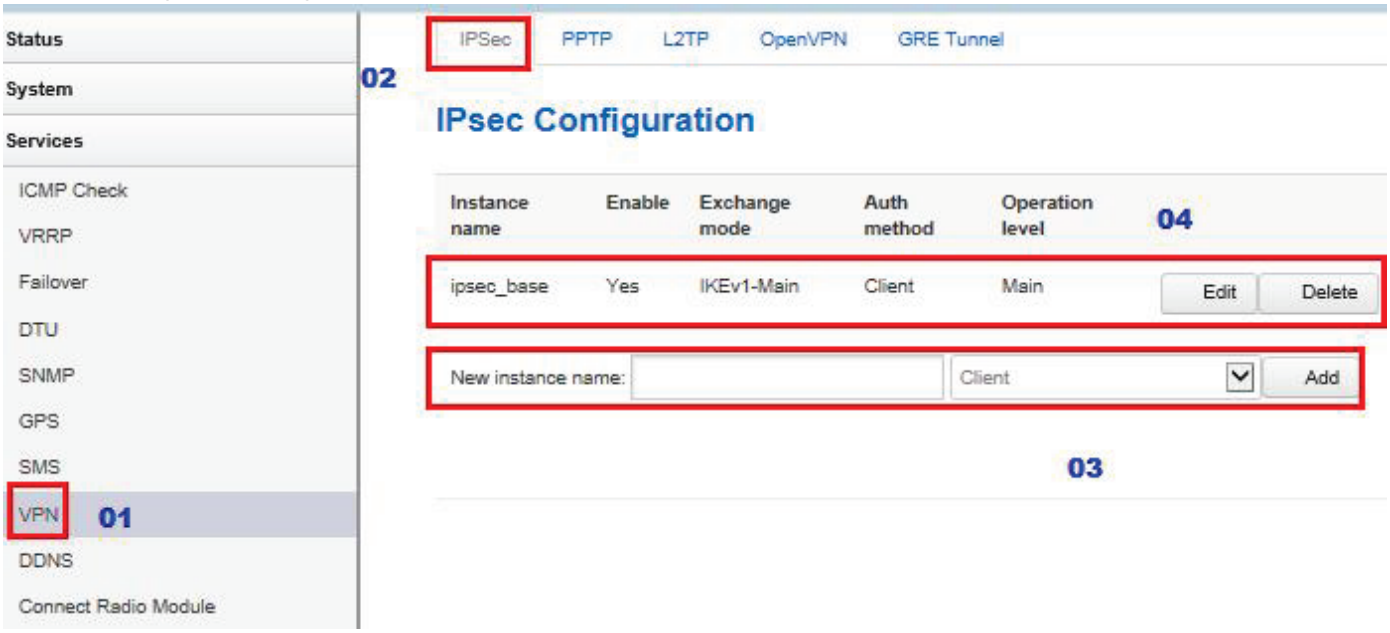




2. Check if IPSEC Client Router can visit IPSEC Server Router without IPSEC. If cannot visit, the IPSEC will not be connected.

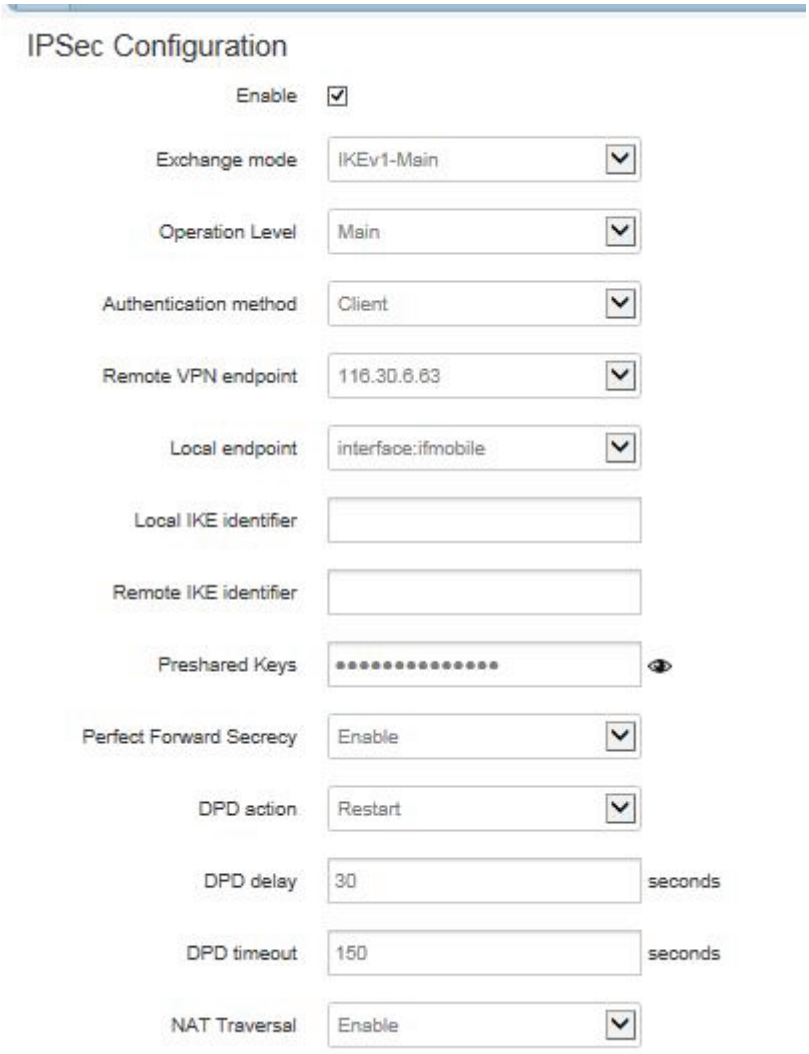


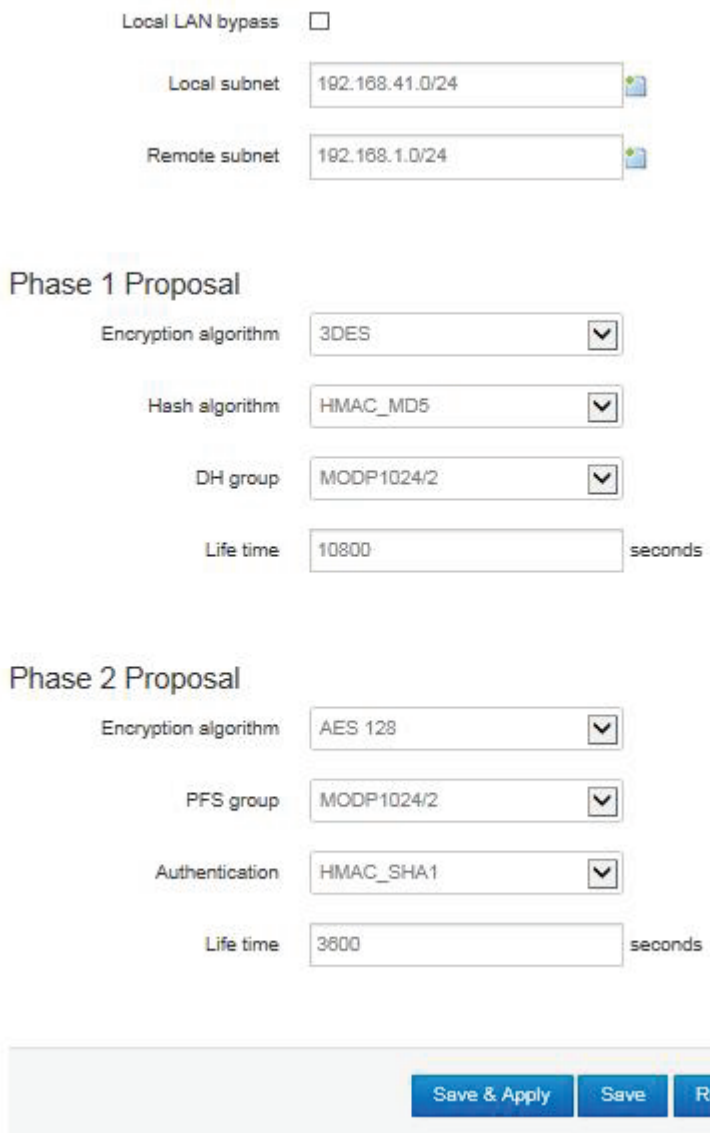
3. Open web management page, click “Services”-→”VPN” at the left navigation bar, then click “IPSEC” to open IPSEC Configuration page.



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
Exchange mode
IKEv1-Main
Operation Level
Main
Authentication method
Client
Remote VPN endpoint
116.30.6.63
Local endpoint
interface:ifmobile
Local IKE identifier
Remote IKE identifier
Preshared Keys
Perfect Forward Secrecy
Enable
DPD action
Restart
DPD delay
30
seconds
DPD timeout
150
seconds
NAT Traversal
Enable

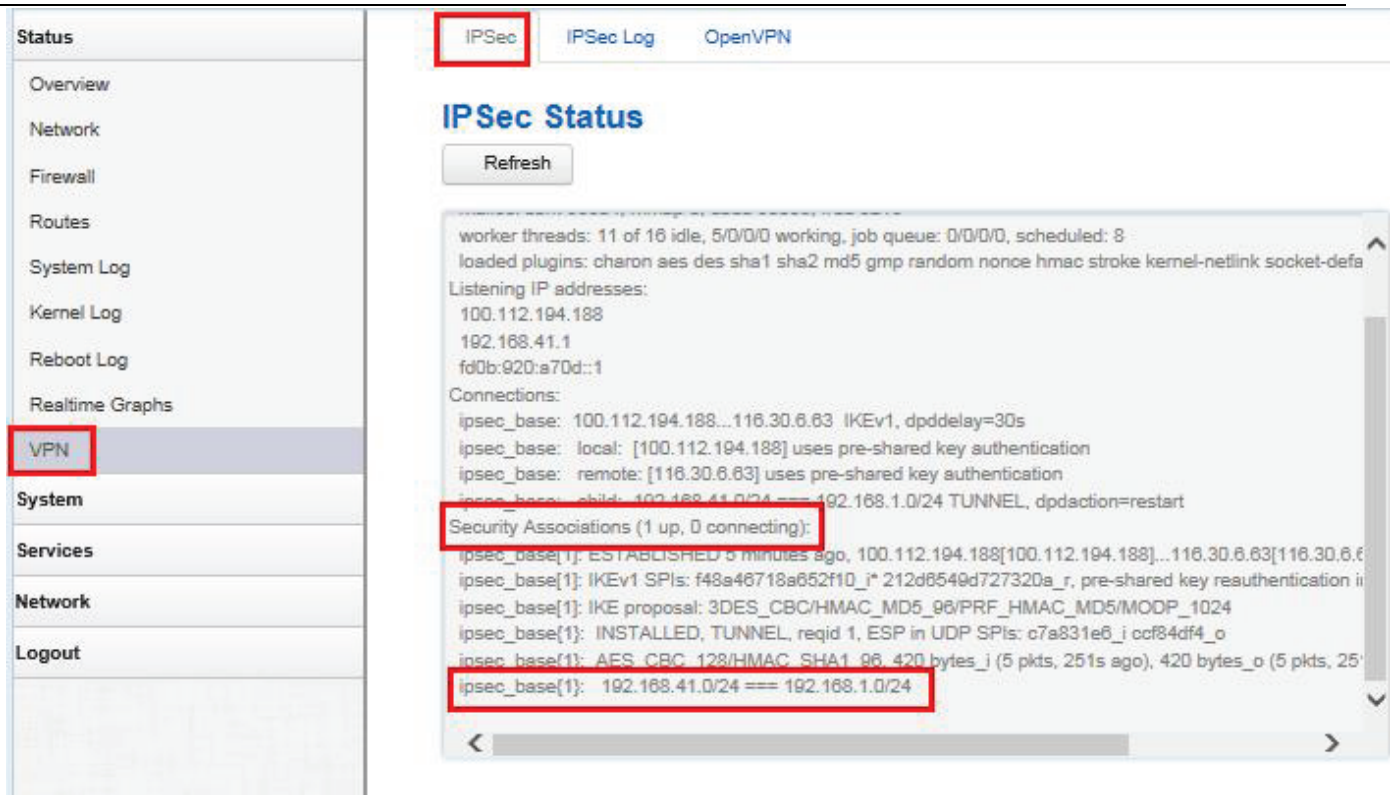


Checked “Enable”, fill in value of “Remote VPN endpoint” as IPSEC Server WAN IP address. Here our IPSEC Server Router has WAN IP address 116.30.6.63 and LAN IP address 192.168.1.1;

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”.

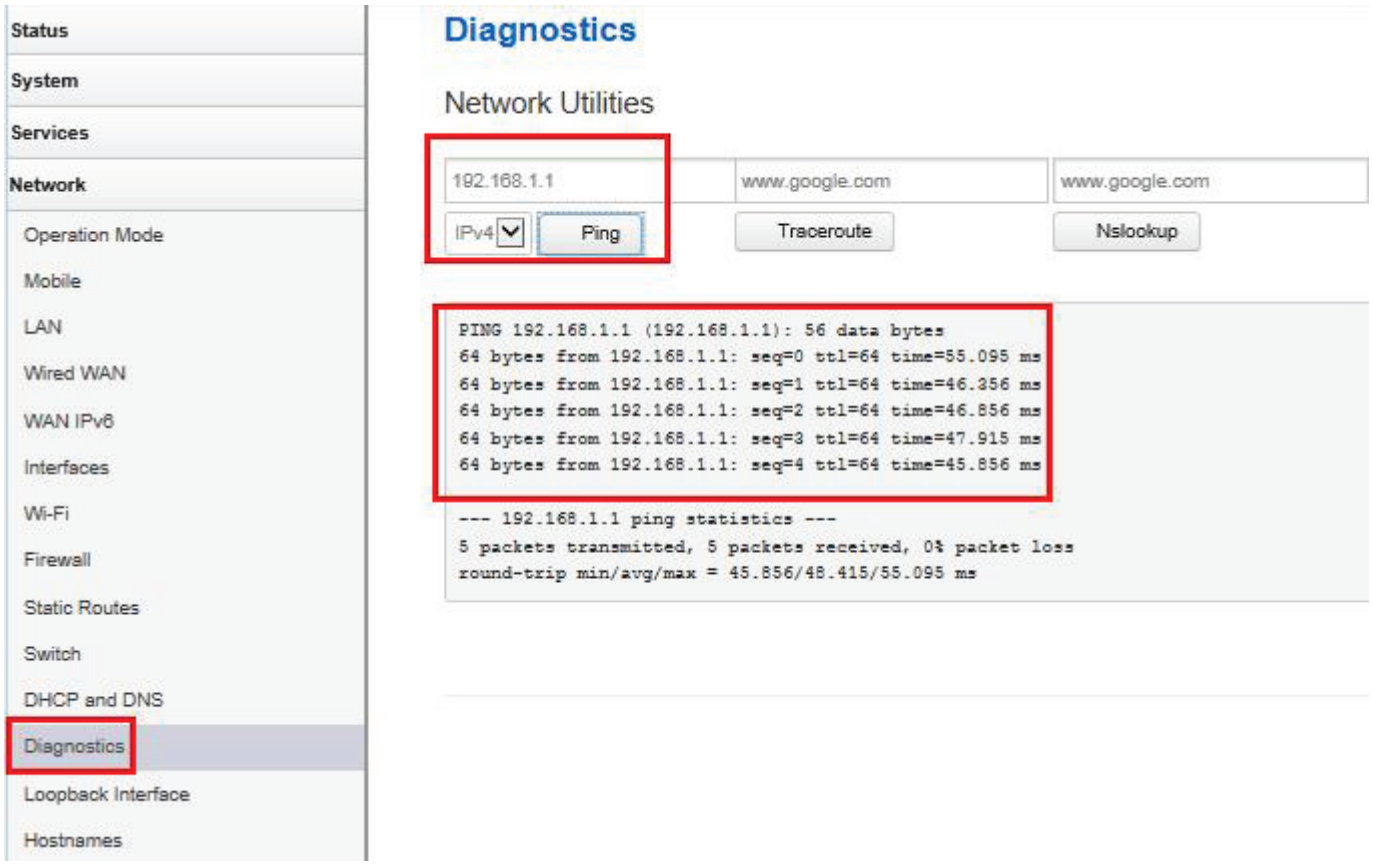
Click button “Save & Apply” if everything is done.

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



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
Ping
Traceroute
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