How to configure VPN IPSec on the Comset CM685V, CM820V, CM685VX and CM950W

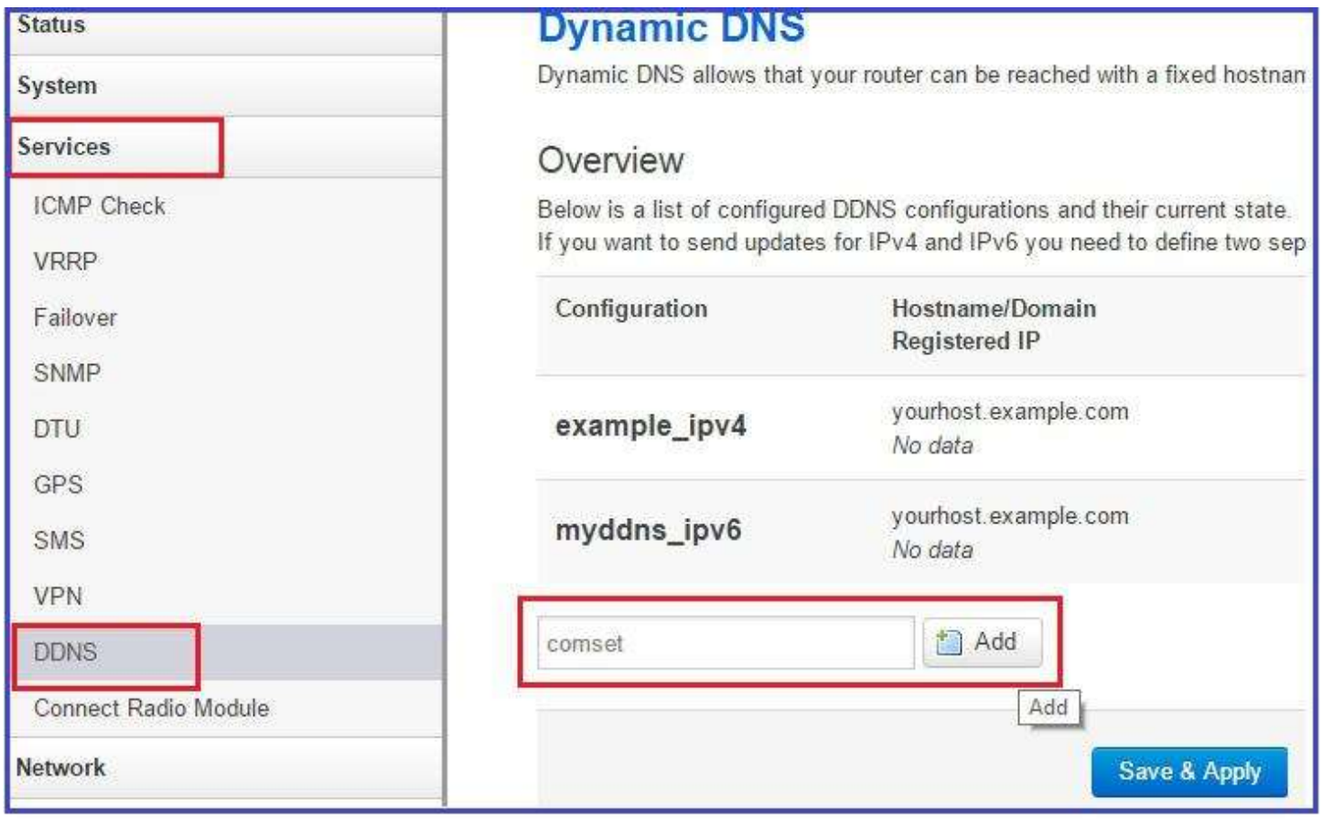
Network Case Scenario:

Router1 DDNS name: comset2016.dyndns.org or Public WAN IP
LAN IP Subnet: 192.168.1.0/24

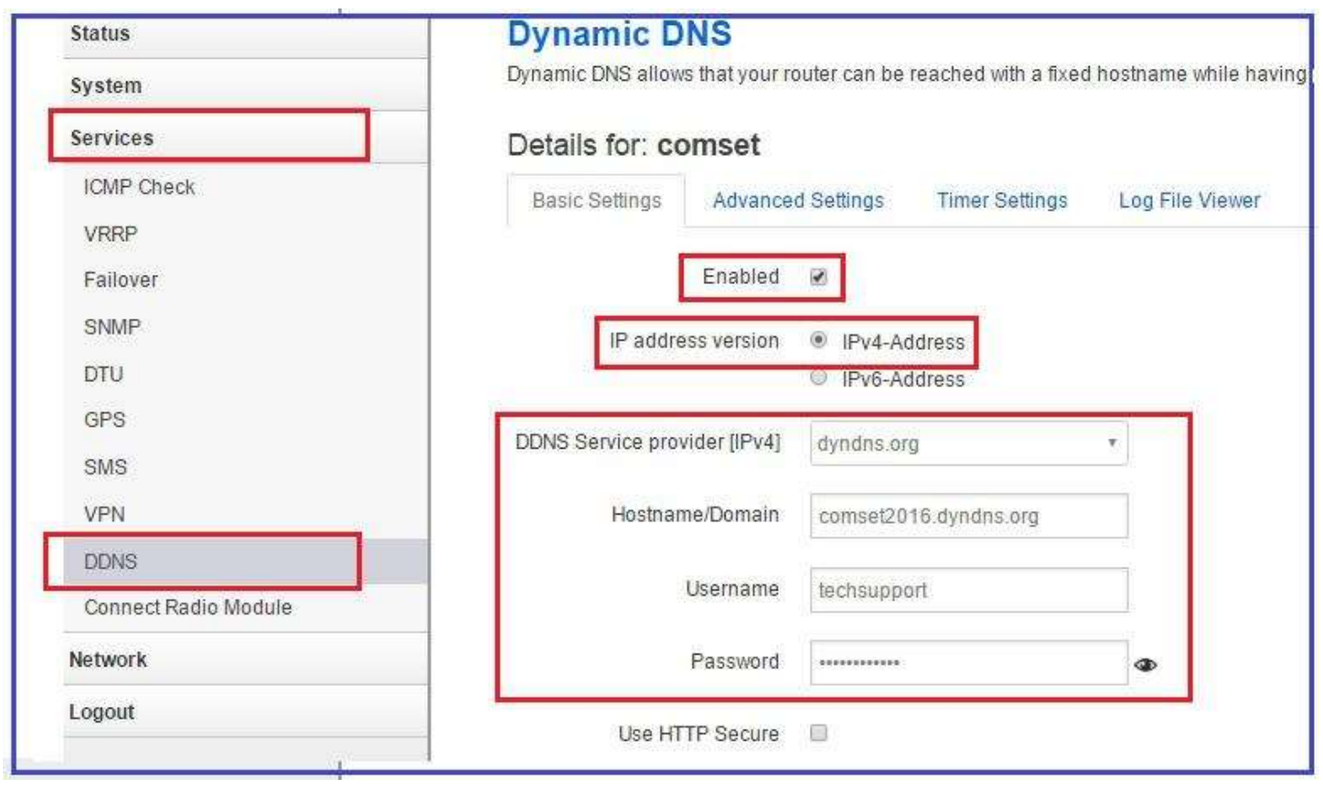
Router2 DDNS name: comset2018.dyndns.org or Public WAN IP
Lan IP Subnet: 192.168.10.0/24

A. Configure DynDNS

1. Navigate to Services -> DDNS -> Set a name for a new DDNS configuration and click “Add”:



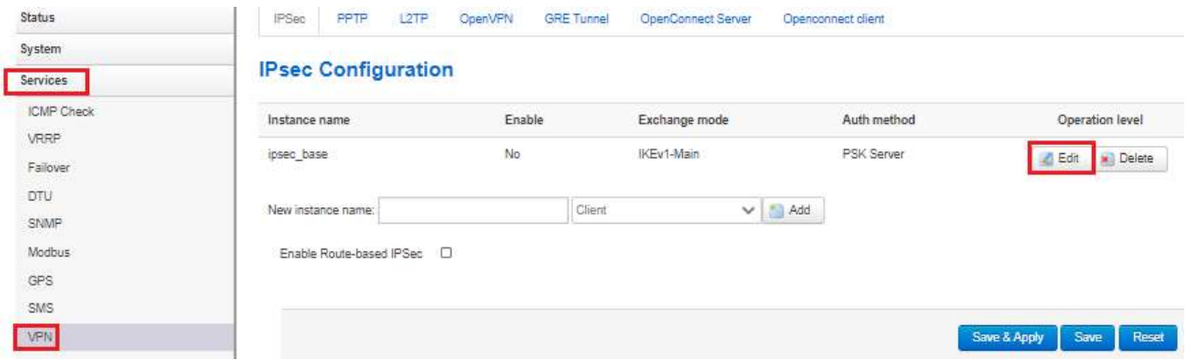
2. Check “Enabled” option and set DDNS provider->Hostname->username and password:



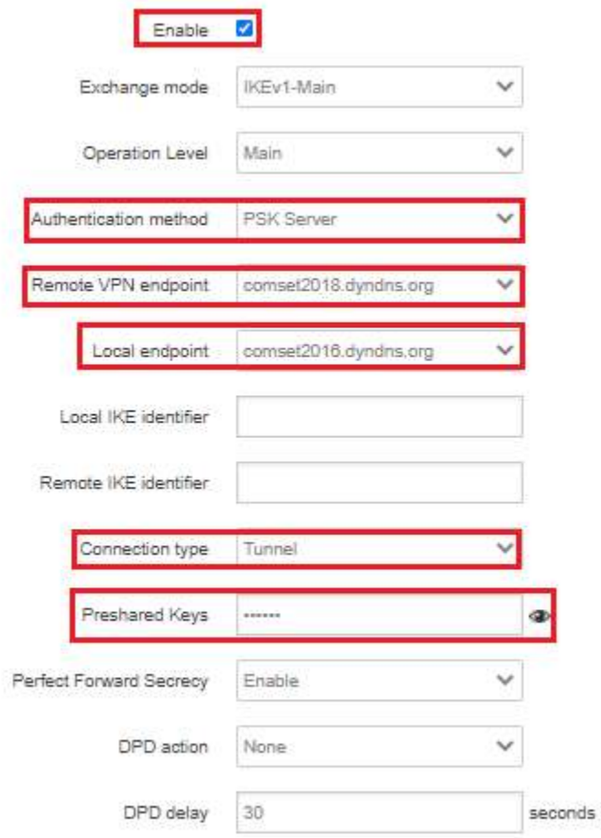
After clicking the “Save and Apply” button, click the “Start” button:

B. Configure VPN IPsec server side on the CM685V

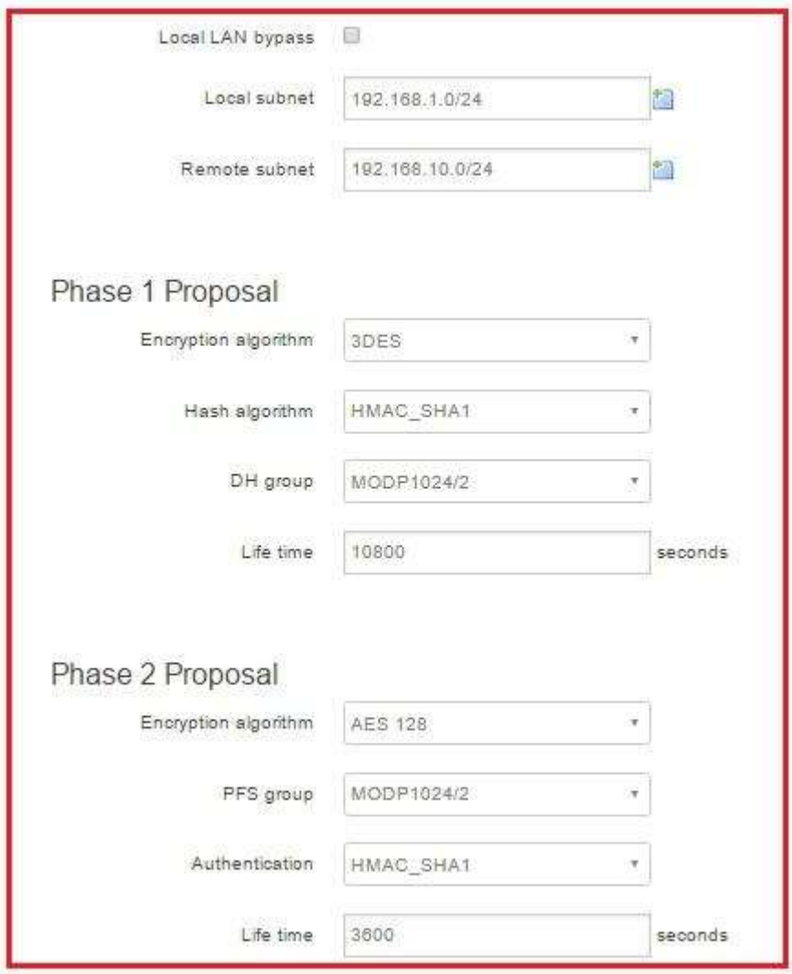
1. Navigate to Services -> VPN and click on “Edit” to configure VPN IPsec server side:



2. Configure VPN IPSec configuration page:



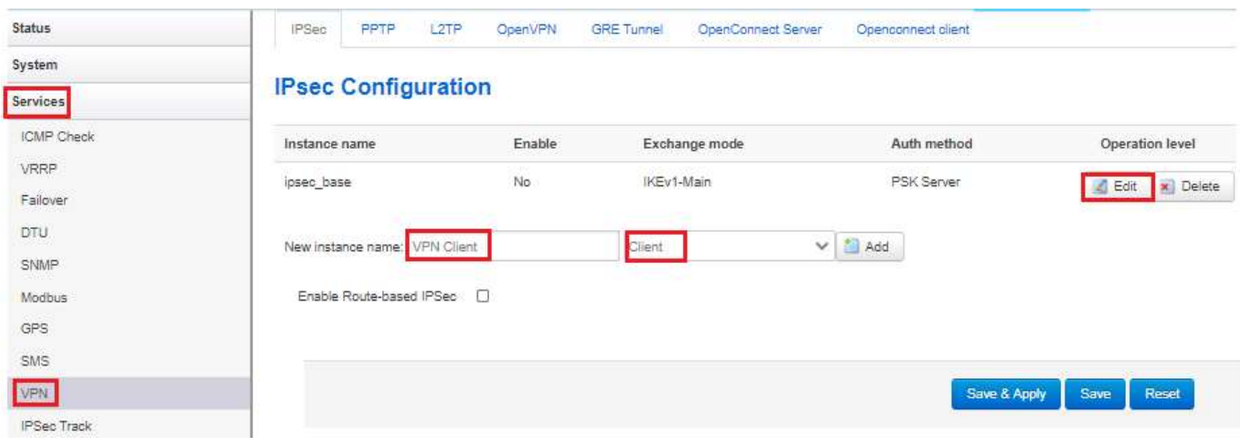
3. Specify local and remote subnets for VPN Tunnel as well as Phase proposals, authentications and encryptions.



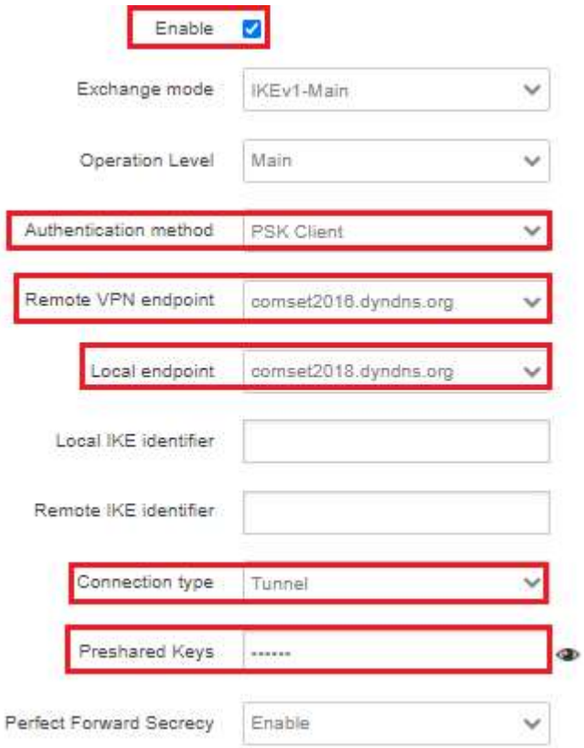
Note: Pre-shared keys, Phase proposals, authentication, encryption on both routers should be the same.

C. Configure VPN IPsec client side on the CM685V

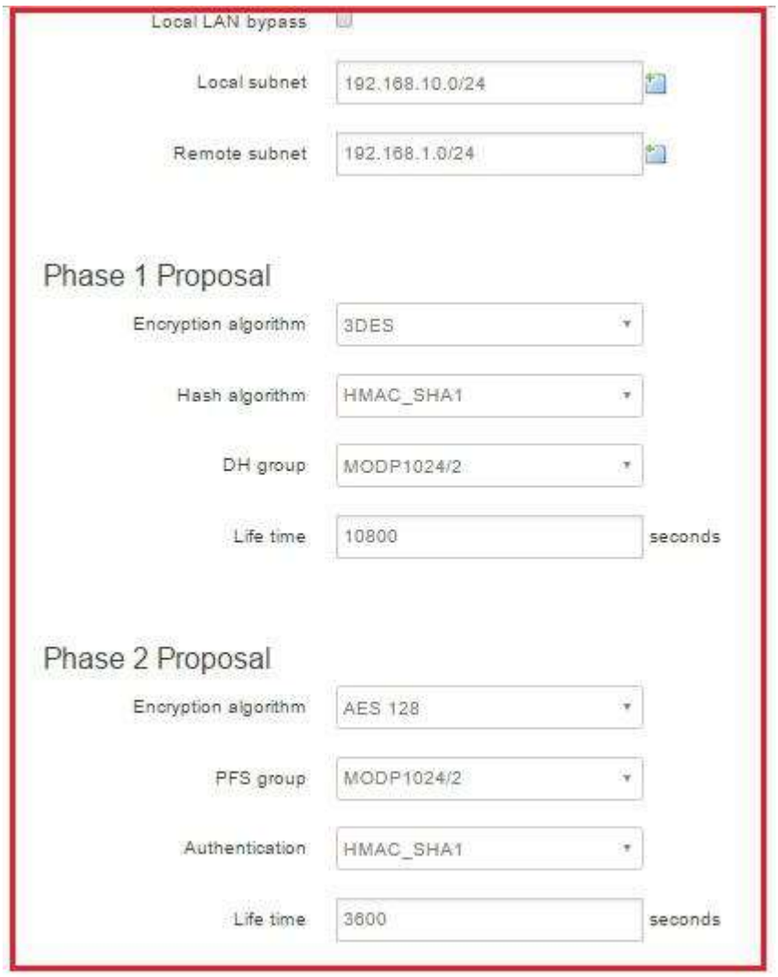
1. Navigate to Services -> VPN. Set a name for VPN client and click on the “Add” button. See below:



2. Configure VPN IPSec client Configuration page:



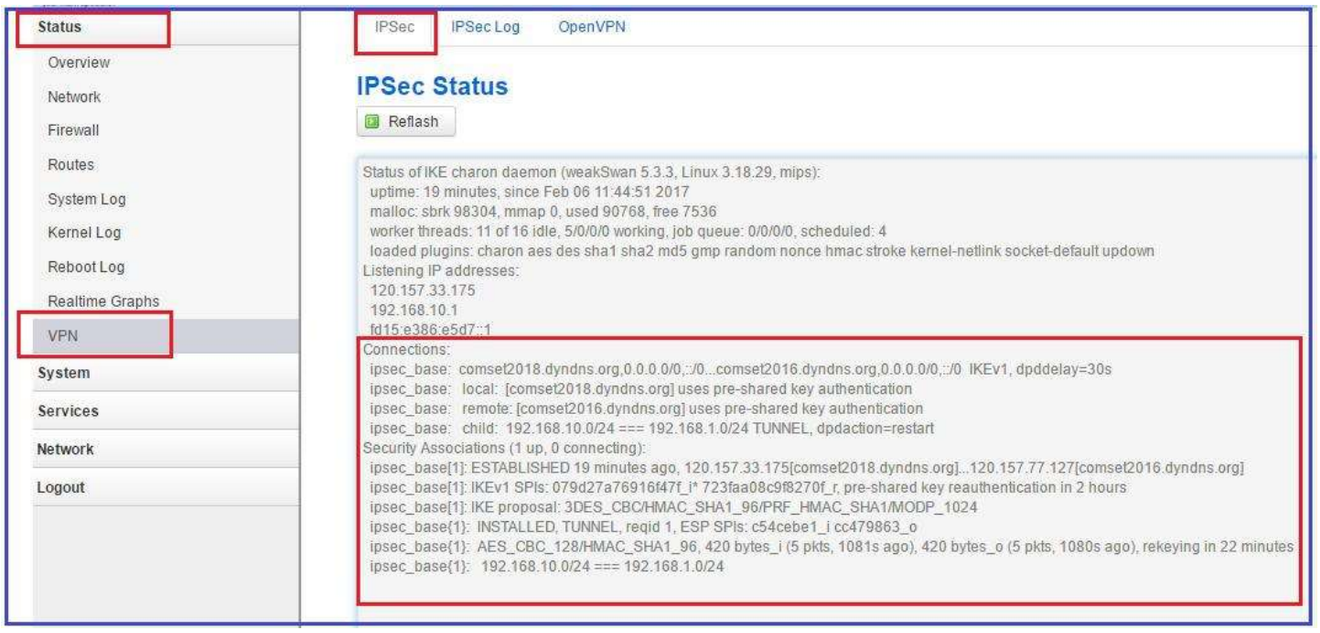
3. Specify local and remote subnets for VPN Tunnel as well as Phase proposals, authentications and encryptions.



Note: Pre-shared keys, Phase proposals, authentication, encryption on both routers should be the same.

D. <u>Checking VPN IPsec logs status and testing remote LAN via ping command.</u>

1. Navigate to Status -> VPN -> IPsec Logs. See below:



2. On the remote VPN router (comset2018.dyndns.org), we have connected a smart phone via WIFI to test VPN connection behind the router. See Network LAN DHCP status below:

3. On the VPN server side, we can now ping the remote LAN device through the VPN IPSec connection.