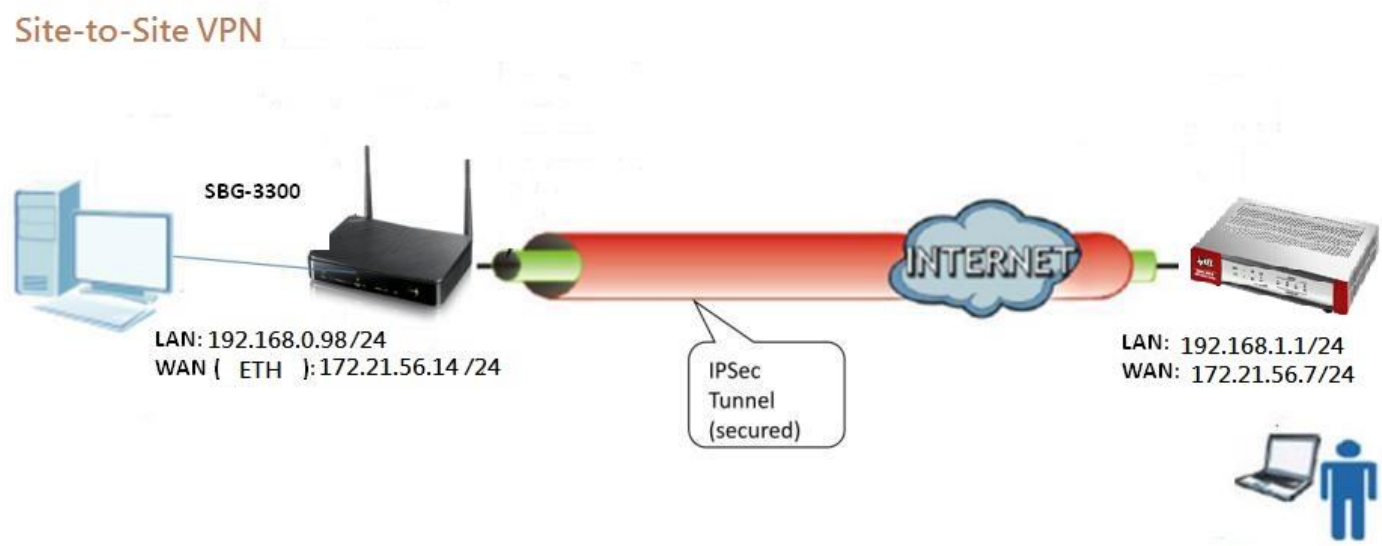
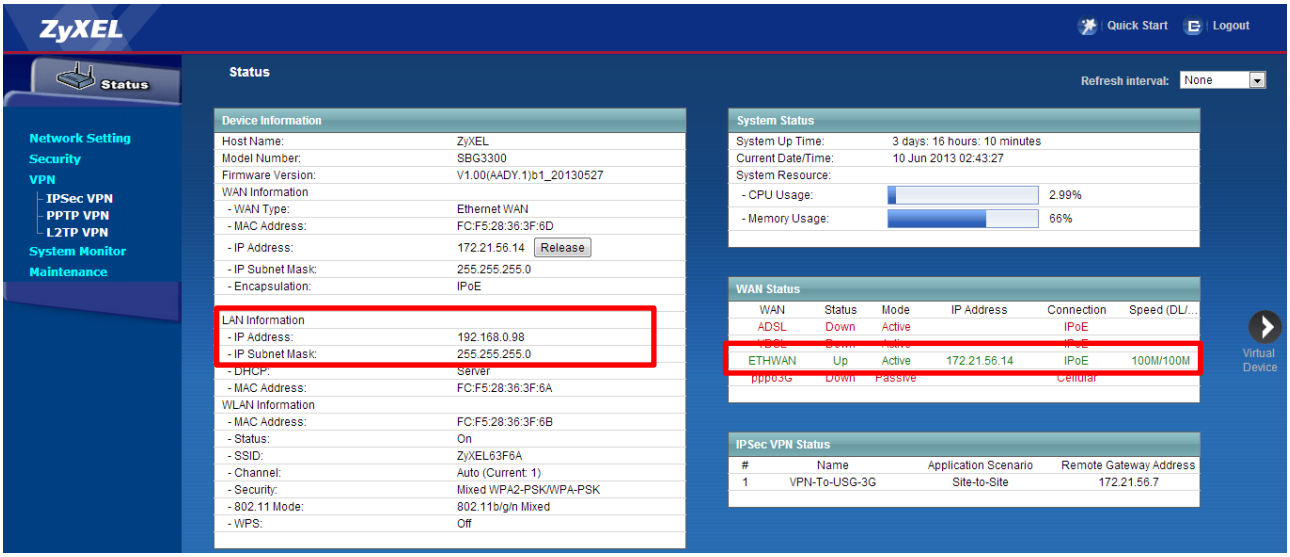
How to establish VPN Tunnel?

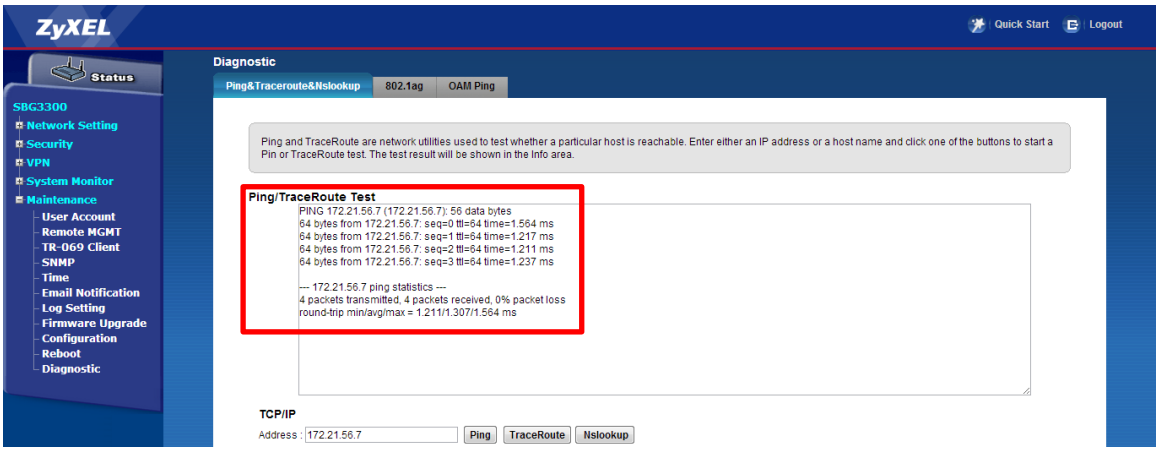
Topology:



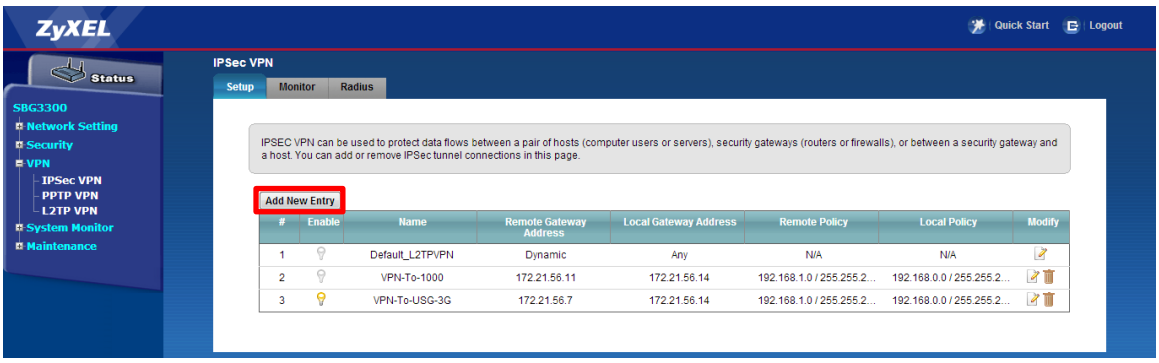
1. Check WAN/LAN status(up) and IP address



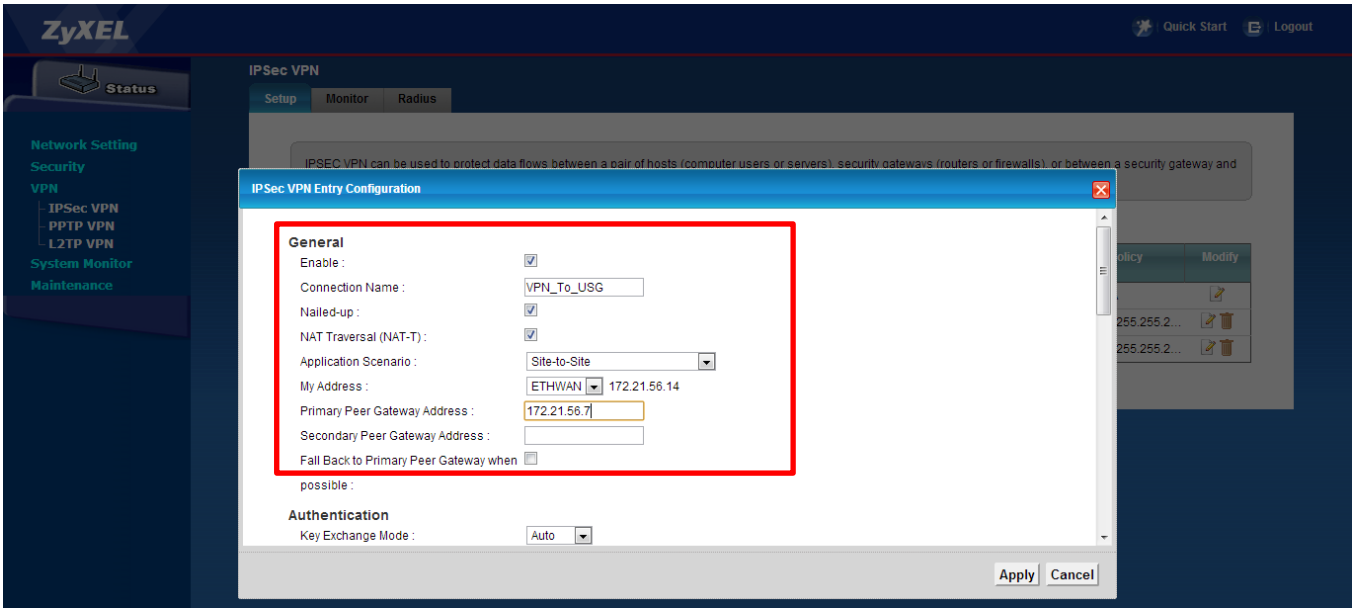
(Make sure the SBG can communication with USG)



2. 「Add New Entry」



3. Check the “Enable” box for IPSec VPN→Fill up the “Connection Name”→Choose “Application Scenario”→My address “ETHWAN”→Primary Peer Gateway Address(USG WAN IP Address)



Select the scenario that best describes your intended VPN connection.

Site-to-site

Choose this if the remote IPSec router has a static IP address or a domain name. This SP Gateway can initiate the VPN tunnel.

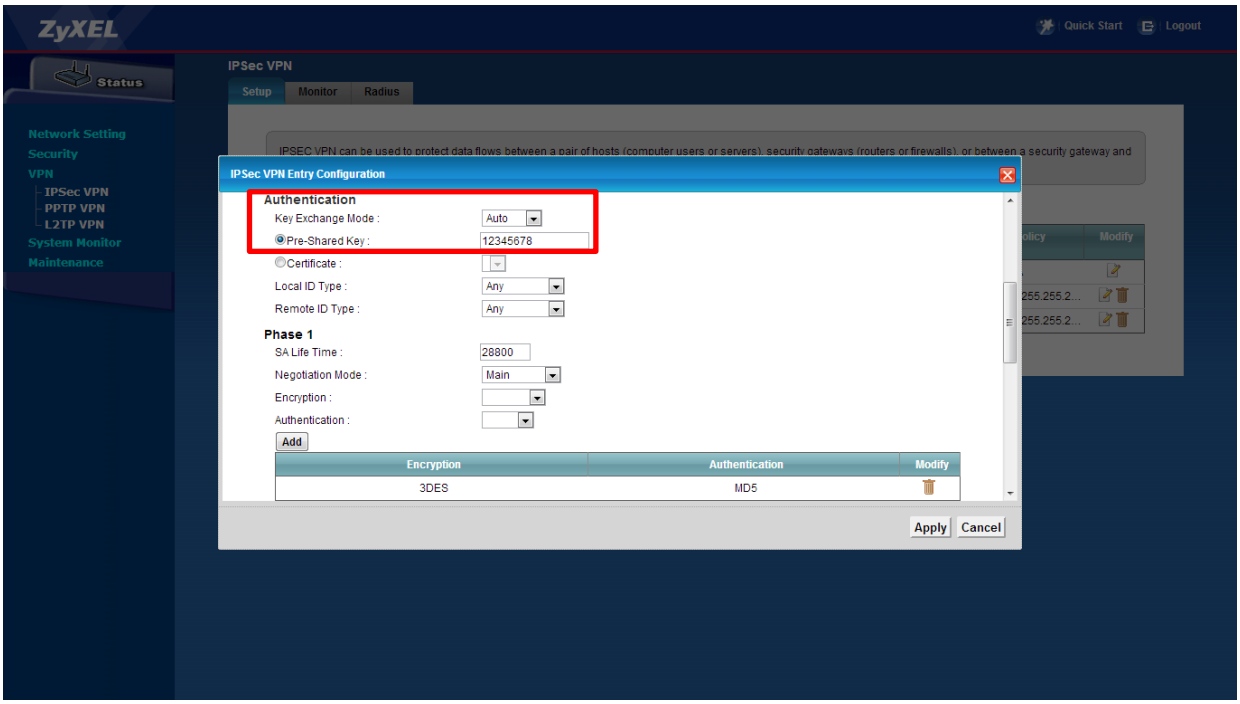
Site-to-site with Dynamic Peer

Choose this if the remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel.

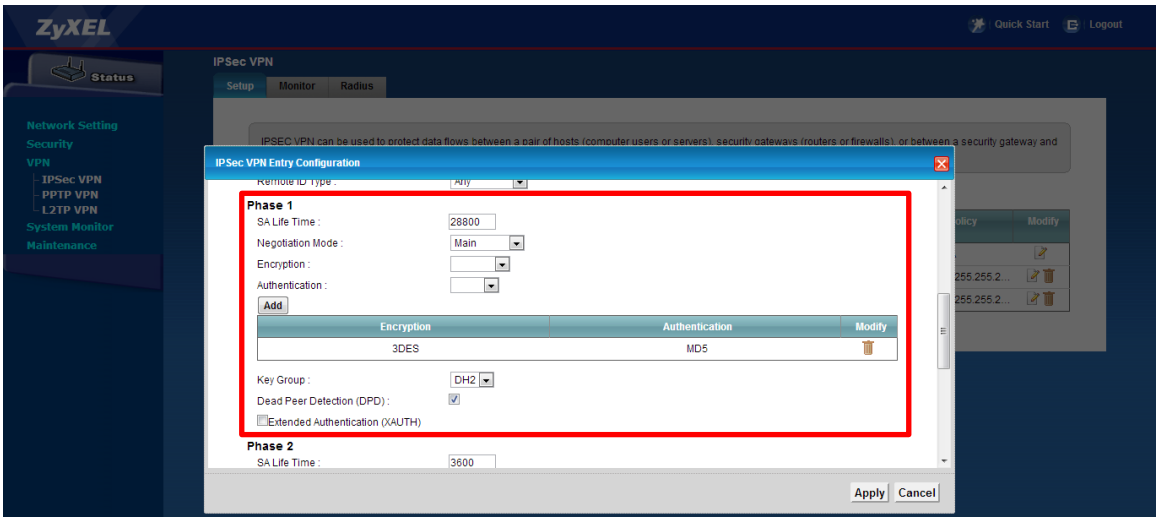
Remote Access (Server Role)

Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.

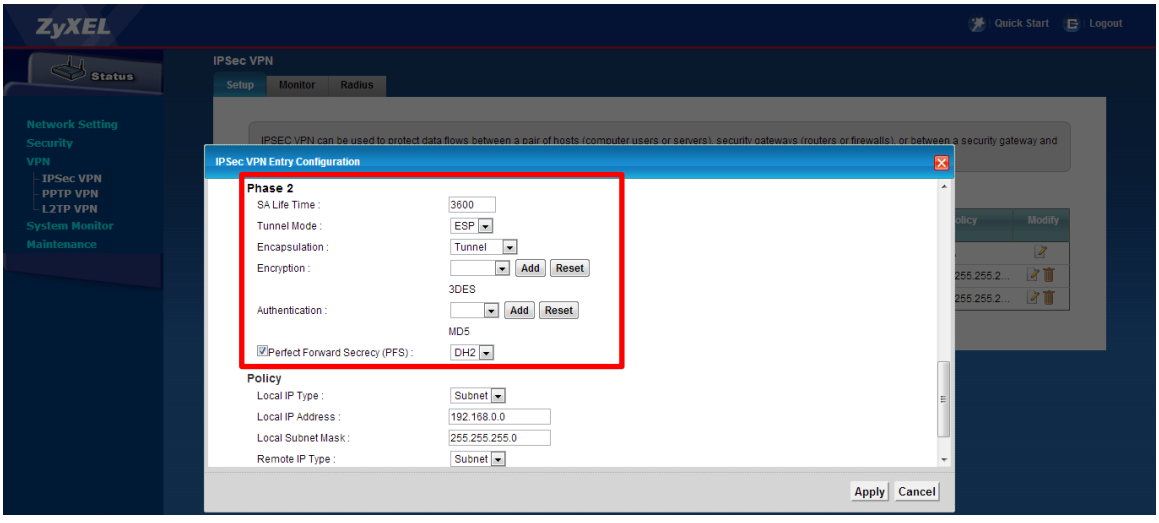
4. Setting Pre-Shared Key(The pre-shared must be the same with each other)



5. At the process pre-shared key, phase1&2, all setting should be same with each other!
   Phase1: Negotiation Mode(Main)→Encryption(3DES)→Authentication(MD5)→Key Group(DH2)

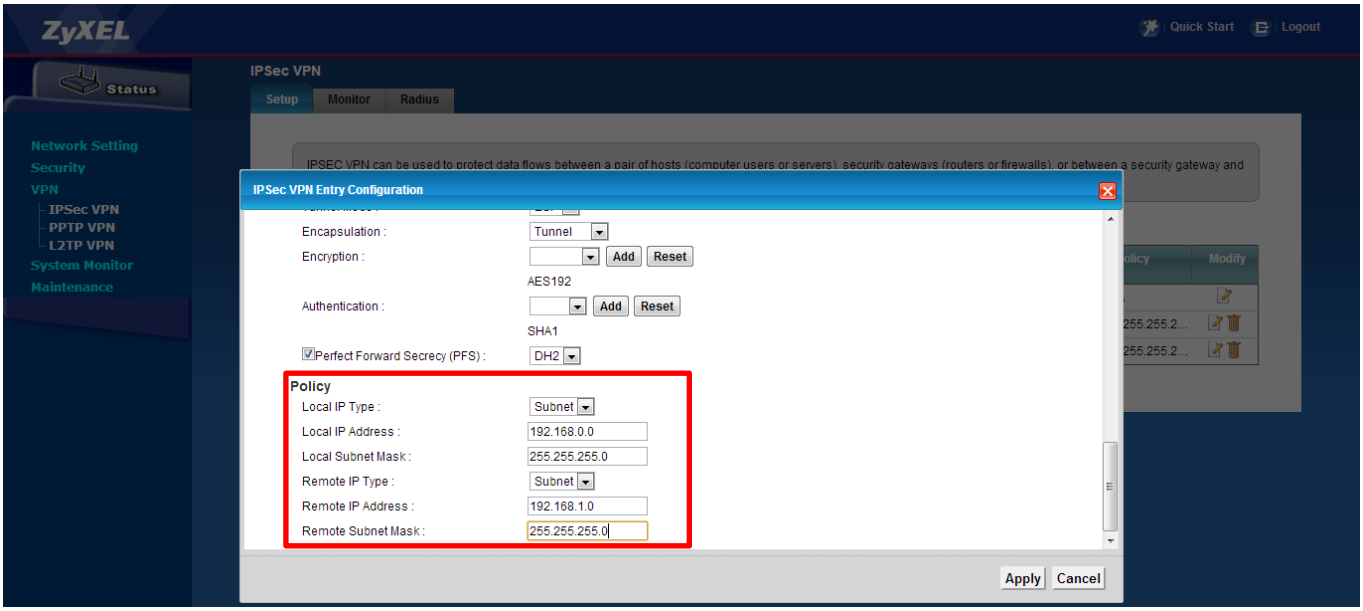


6. Phase2: Tunnel Mode(ESP)→Encapsulation(Tunnel)→Encryption(3DES)→Authentication(MD5)

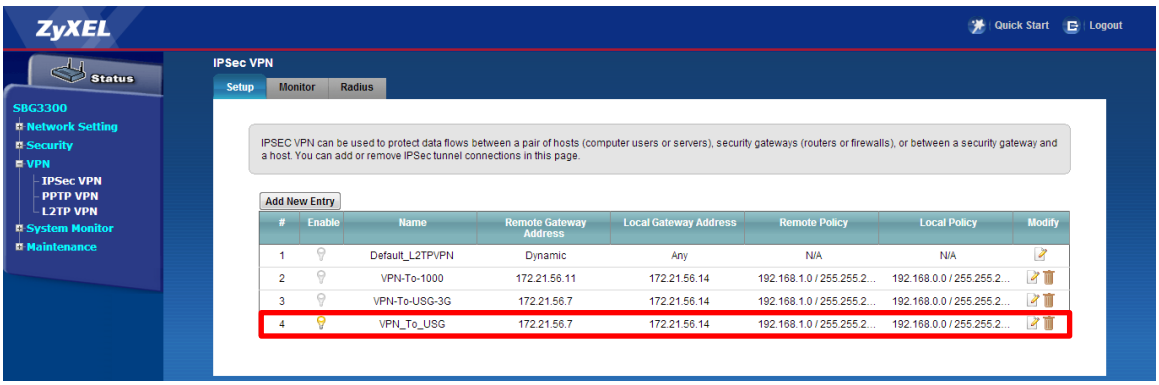


7. Policy: Setting the Local IP(SBG LAN)/Remote IP(USG WAN)

   Note: The Local IP Address must different with Remote IP Address



8. After the setting done, please verify the “Entry” enable and the SBG will take a while to establish the VPN Tunnel with USG



9. You can also check the VPN Tunnel status by Monitor and the status page