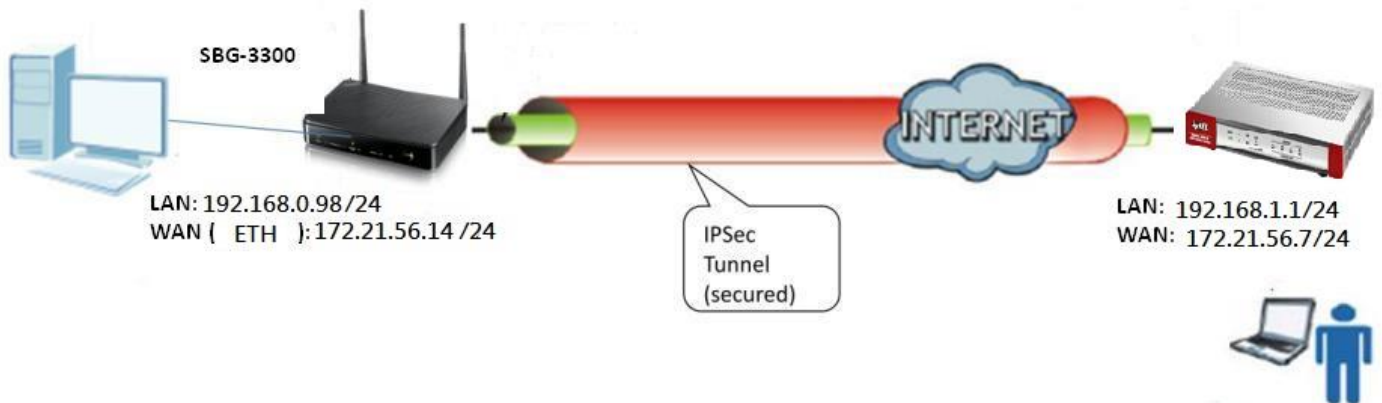


How to establish VPN Tunnel?

Topology:

Site-to-Site VPN



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

Screenshot of ZyXEL web interface showing Status page. The LAN Information section is highlighted with a red box, showing IP Address: 192.168.0.98 and IP Subnet Mask: 255.255.255.0. The WAN Status section is also highlighted with a red box, showing ETHWAN Up Active 172.21.56.14 IPoE 100M/100M.

WAN	Status	Mode	IP Address	Connection	Speed (DL/UL)
ADSL	Down	Active		IPoE	
DSL	Down	Active		IPoE	
ETHWAN	Up	Active	172.21.56.14	IPoE	100M/100M
pppoe3g	Down	Passive		Cellular	

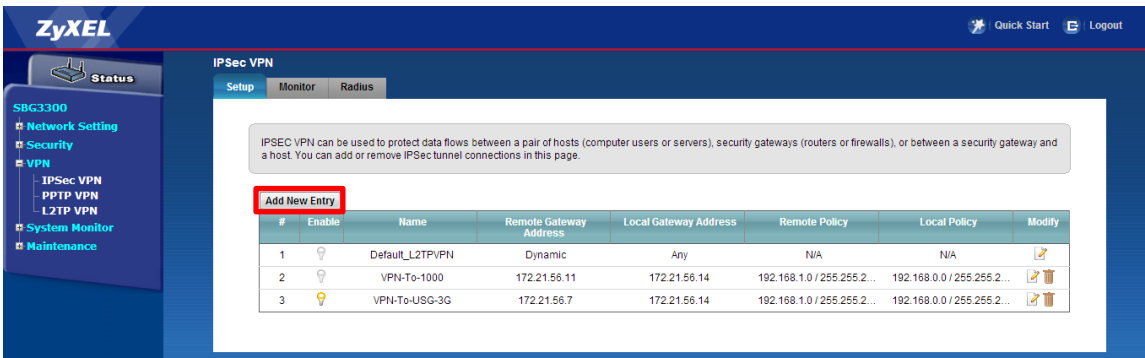
(Make sure the SBG can communication with USG)

Screenshot of ZyXEL web interface showing Diagnostic page. The Ping/TraceRoute Test section is highlighted with a red box, showing successful ping results for 172.21.56.7.

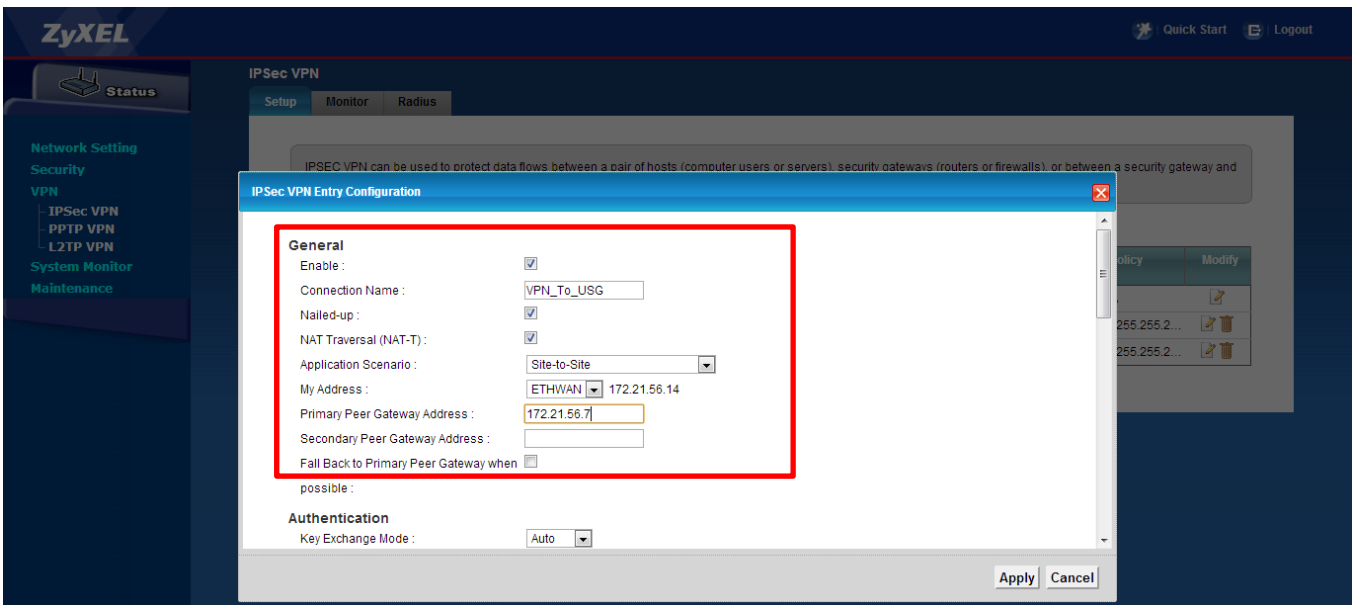
```
PING 172.21.56.7 (172.21.56.7): 56 data bytes
64 bytes from 172.21.56.7: seq=0 ttl=64 time=1.564 ms
64 bytes from 172.21.56.7: seq=1 ttl=64 time=1.217 ms
64 bytes from 172.21.56.7: seq=2 ttl=64 time=1.211 ms
64 bytes from 172.21.56.7: seq=3 ttl=64 time=1.237 ms

--- 172.21.56.7 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.211/1.307/1.564 ms
```

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.

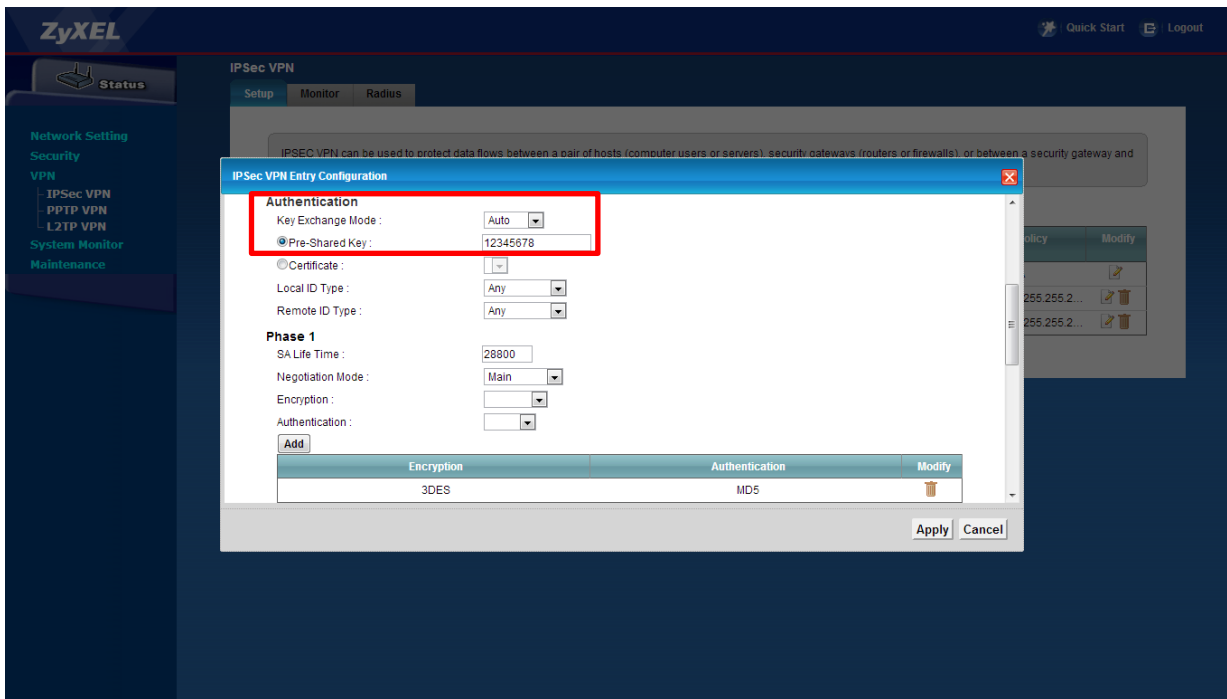
Site-to-site with Dynamic Peer

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

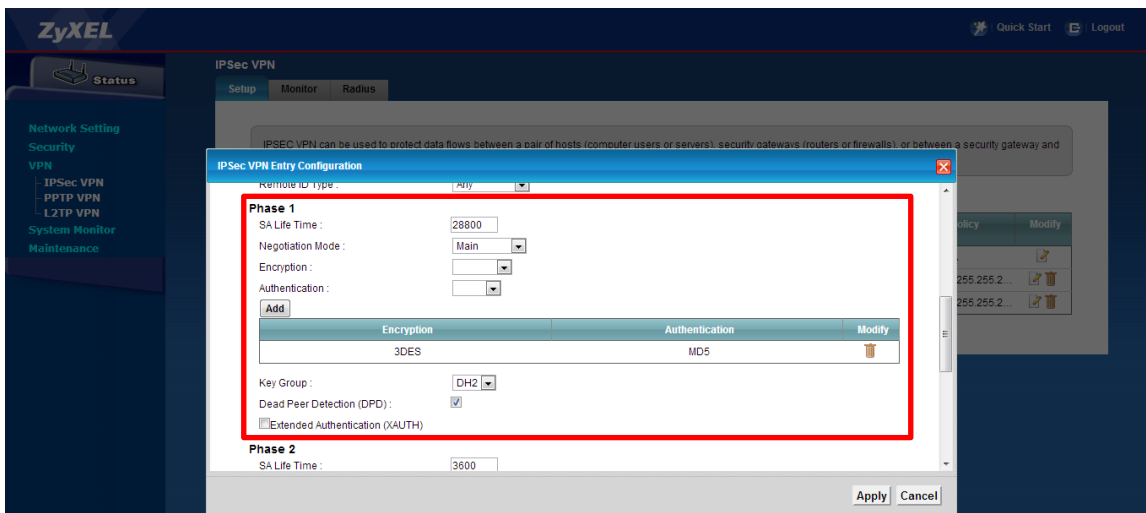
Remote Access (Server Role)

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.

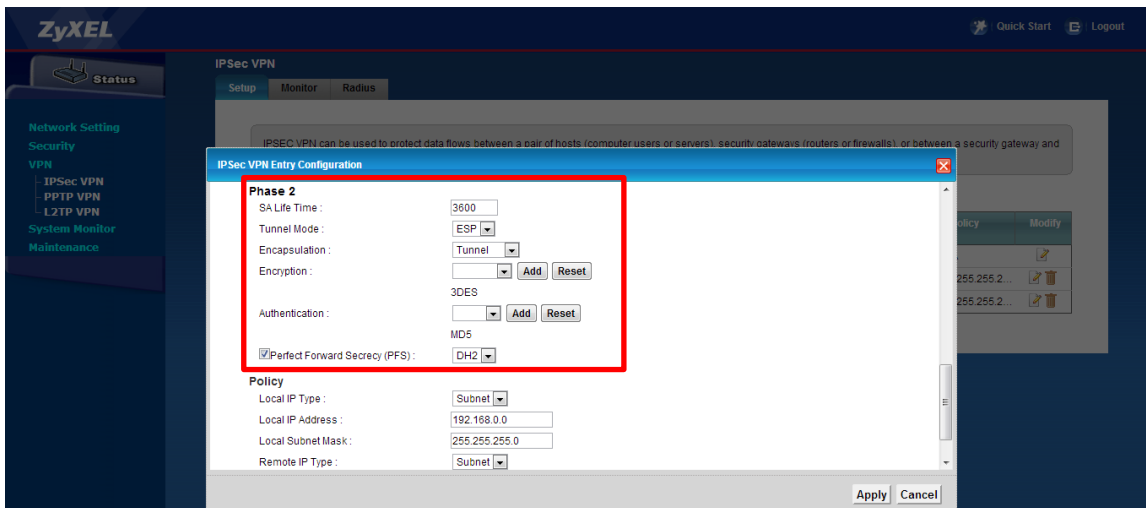
4. Setting Pre-Shared Key(The pre-shared must be the same with each other)



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)

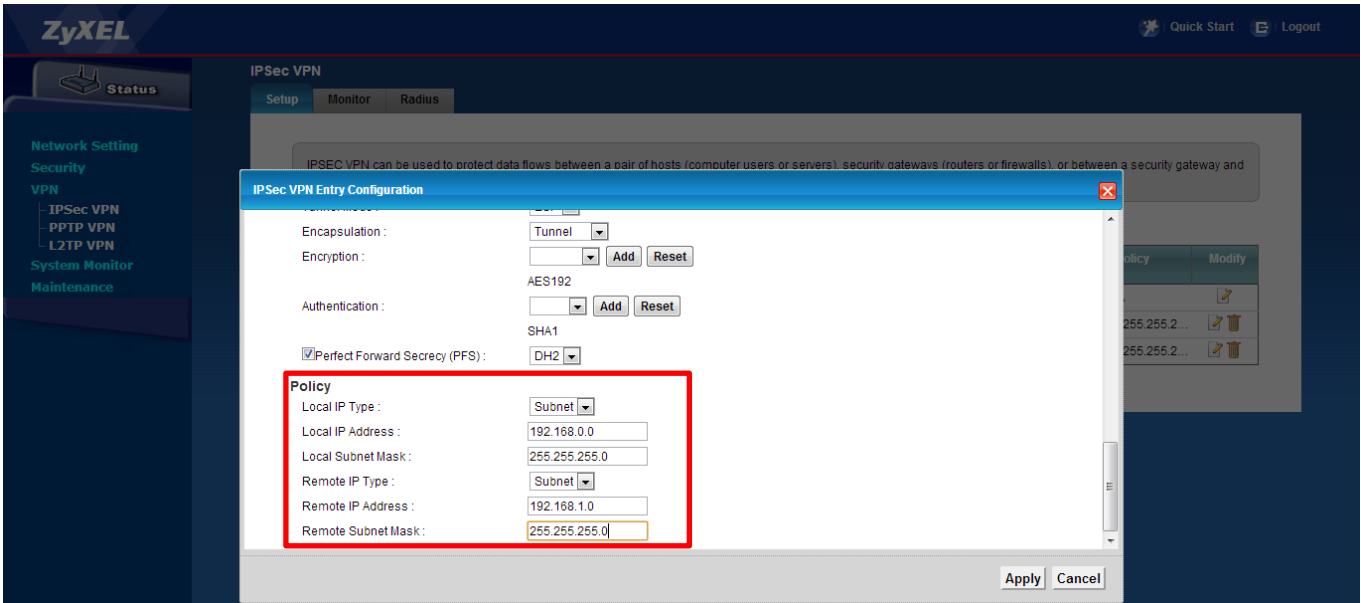


6. Phase2: Tunnel Mode(ESP)→Encapsulation(Tunnel)→Encryption(3DES)→Authentication(MD5)

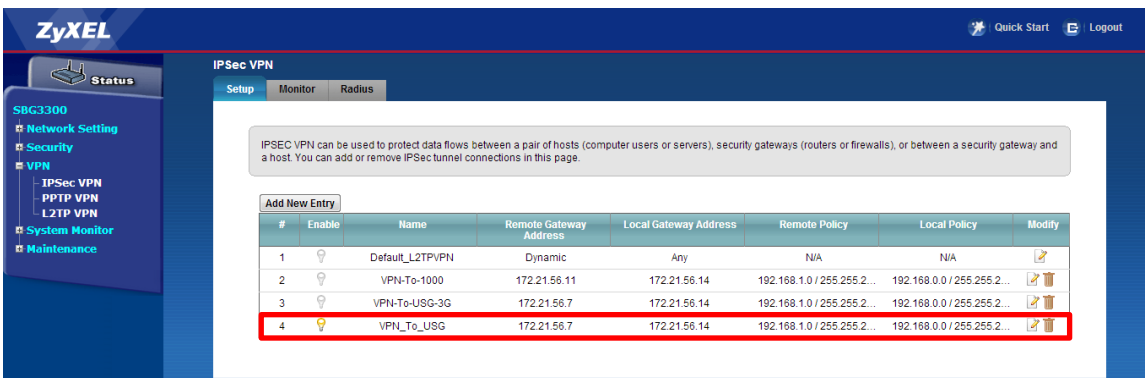


7. Policy: Setting the Local IP(SBG LAN)/Remote IP(USG WAN)

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

