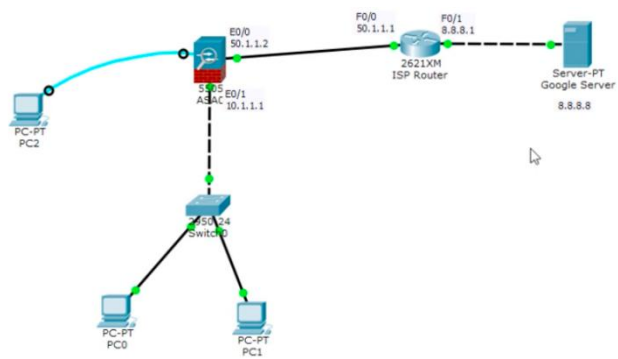




1. Make Topology
2. Assign IP Accordingly on ASA & ISP Router
3. Set Inside and Outside on ASA Firewall
4. Configure DHCP Server and DNS IP on ASA
5. Configure Default Route on ASA
6. Configure OSPF on ISP Router
7. Create Object Network & Enable NAT on ASA
8. Create ACL on ASA
9. Verify

Security-Level

100 - Inside
0 - Outside
1-99 DMZ



1. Remove existing information

sh running-config

```
helnet timeout 5
ash timeout 5
|
Shcpd address 192.168.1.5-192.168.1.35 inside
Shcpd enable inside
|
Shcpd auto_config outside
|
```

Remove above

no <dhcpd address ----->

2. Configure Firewall

config t

int vlan 1

ip address 10.1.1.1 255.0.0.0

no shut

Nameif inside

security-level 100

exit

int e0/1

switchport access vlan 1

exit

int vlan 2

ip address 50.1.1.2 255.0.0.0

no shut

nameif outside

security-level 0

exit

int e0/0

switchport access vlan 2

exit

3. Configure Router

4. Configure Server (IP 8.8.8.8 & IP Gateway 8.8.8.1)
5. Configure 2 PC -> DHCP mode
6. @firewall

```
config t
  dhcpd address 10.1.1.10-10.1.1.30 inside
  dhcpd dns 8.8.8.8 interface inside
```
7. check ip -> pc with dns
8. Default route in firewall

```
route outside 0.0.0.0 0.0.0.0 50.1.1.1
```
9. At Router

```
router ospf 1
net 50.0.0.0 0.255.255.255 area 0
net 0.0.0.0 0.255.255.255 area 0
```
- @Firewall

```
object network LAN
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic interface
```
10. Open PC1, PC2 -> ping -t 8.8.8.8 -> no reply -> dont close
11. @Firewall

```
Config t
access-list uti extended permit tcp any any
access-list uti extended permit icmp any any
access-group uti in interface outside
```
12. Both PC-> ping will get reply
13. @ Firewall

```
show xlate
show nat
```