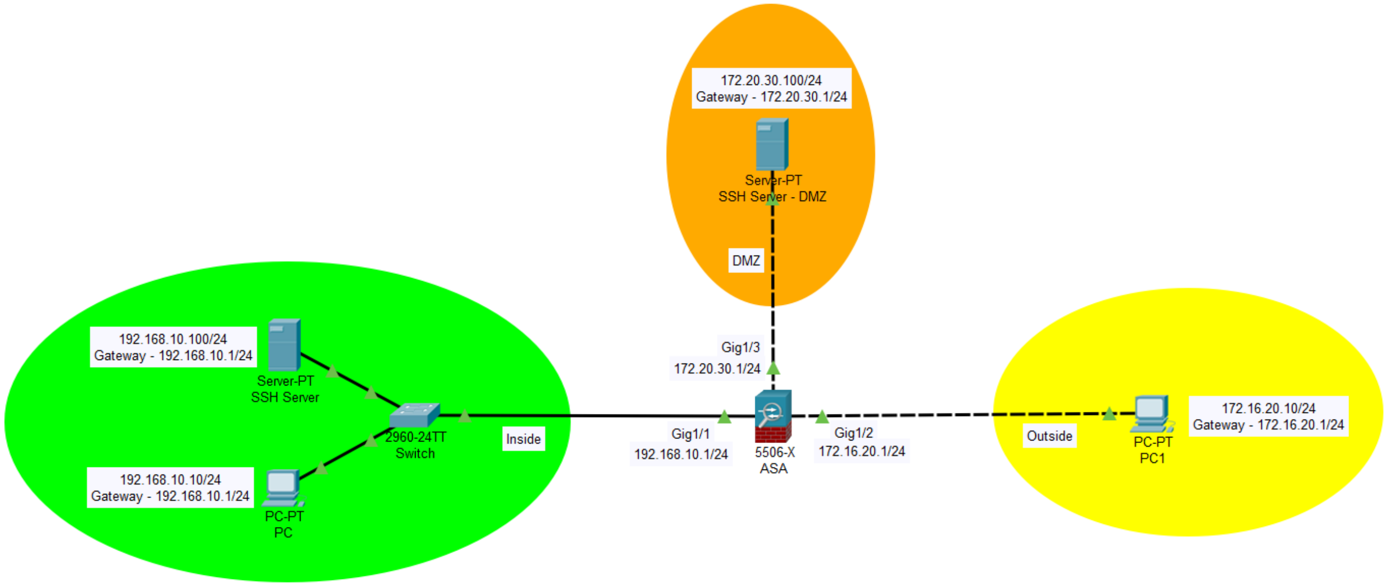
E/15/220

Maliththa k.h.h.

CO325 – LAB02

1)



2)

```
ciscoasa(config)# object network dmz-server
ciscoasa(config-network-object)# host 172.20.30.100

ciscoasa(config)# access-list out2dmz extended permit tcp any object dmz-server eq ssh
ciscoasa(config)# access-list out2dmz extended deny ip any any
ciscoasa(config)# access-group out2dmz in interface outside

ciscoasa(config)# object network dmz-mapped-server
ciscoasa(config-network-object)# host 172.20.30.3

ciscoasa(config)# object network inside-real-server
ciscoasa(config-network-object)# host 192.168.10.100
ciscoasa(config-network-object)# nat (inside,dmz) static dmz-mapped-server

ciscoasa(config)# access-list dmz2in extended permit tcp object dmz-server object inside-real-server eq ssh
ciscoasa(config)# access-list dmz2in extended deny ip any any
ciscoasa(config)# access-group dmz2in in interface dmz
```

3)

```
ciscoasa(config)# object network dmz-ssh
ciscoasa(config-network-object)# host 172.20.30.100
```

```
ciscoasa(config)# access-list out2dmz extended permit tcp any object dmz-ssh-obj eq ssh
ciscoasa(config)# access-list out2dmz extended deny ip any any
ciscoasa(config)# access-group out2dmz in interface outside
```

First create a network object (for a host) and define dmz ssh server IP address. Here first access rule allow any ssh traffic from outside to dmz ssh server. Second access rule deny any other traffic from outside to inside and dmz.

```
ciscoasa(config)# object network dmz-mapped-server
ciscoasa(config-network-object)# host 172.20.30.3
```

```
ciscoasa(config)# object network inside-real-server
ciscoasa(config-network-object)# host 192.168.10.100
ciscoasa(config-network-object)# nat (inside,dmz) static dmz-mapped-server
```

```
ciscoasa(config)# access-list dmz2in extended permit tcp object dmz-server object inside-real-server eq
ssh
ciscoasa(config)# access-list dmz2in extended deny ip any any
ciscoasa(config)# access-group dmz2in in interface dmz
```

Here create a network object (for a host) and define IP address that maps to inside ssh server ip address. Next network object has inside ssh server ip address and nat rule. This nat rule map inside ssh ip address with dmz mapped ip address. So you can access inside ssh server from dmz ssh server using mapped ip address (172.20.30.3). Here first access rule allow any ssh traffic from dmz to inside ssh server. Second access rule deny any other traffic from dmz to inside.