```
ciscoasa(config)#interface gigabitEthernet 1/1

ciscoasa(config-if)#nameif inside

ciscoasa(config-if)#security-level 100

ciscoasa(config-if)#ip address 192.168.10.1 255.255.255.0

ciscoasa(config-if)#no shut
```

```
ciscoasa(config)#interface gigabitEthernet 1/2

ciscoasa(config-if)#nameif outside

ciscoasa(config-if)#security-level 0

ciscoasa(config-if)#ip address 172.16.20.1 255.255.255.0

ciscoasa(config-if)#no shut
```

```
ciscoasa(config)#interface gigabitEthernet 1/3

ciscoasa(config-if)#nameif dmz

ciscoasa(config-if)#security-level 50

ciscoasa(config-if)#ip address 172.20.30.1 255.255.255.0

ciscoasa(config-if)#no shut
```

inside network pc -> ip : 192.168.10.100/24

-> gateway : 192.168.10.1/24

outside netwrok pc -> ip : 172.16.20.112/24

->gateway : 172.16.20.1/24

dmz ssh server -> ip : 172.20.30.100/24

->gateway : 172.20.30.1/24

-----configure dmz with a mapped static ip for outside-------

```
ciscoasa(config)#object network dmz-real-server

ciscoasa(config-network-object)#host 172.20.30.100

ciscoasa(config-network-object)#nat (dmz,outside) static 172.20.30.3
```

--------allow ssh access from outside to the dmz mapped host-----

```
ciscoasa(config)#access-list out2dmztcpssh extended permit tcp any object dmz-real-server eq 22

ciscoasa(config)#access-group out2dmztcpssh in interface outside
```

---------allow ssh access from dmz to inside host-------------

```
ciscoasa(config)#access-list dmz2insidetcpssh extended permit tcp object dmz-real-server  host 192.168.10.100 eq 22

ciscoasa(config)#access-group dmz2insidetcpssh in interface dmz
```

3) By the NAT rules when any outside host try to access the DMZ ssh server, it goes through the 172.20.30.3 ip, which is mapped to 172.20.30.100 (real ip address of ssh server) at the dmz interface.

Then from the out2dmztcpssh ACL rule it allows **only the tcp ssh traffic** from outside, to access the dmz ssh server. So it is declared in the outside interface.

From dmz2insidetcpssh ACL rule it **only allows tcp ssh traffic** from **one host** which is 172.20.30.100 (DMZ ssh server) to access the **only one inside host** which is 192.168.10.100 (inside ssh host).

Here I have not declared any ACL rule connected with inside and outside network, so the default rules are applied. Because of that outside network cannot access the inside network directly through ssh or any other method.

If outside network want to access the inside network through ssh, first they have to log in to the DMZ ssh server and from that log in to the inside ssh service. So outside network can access only ssh service of inside network indirectly.