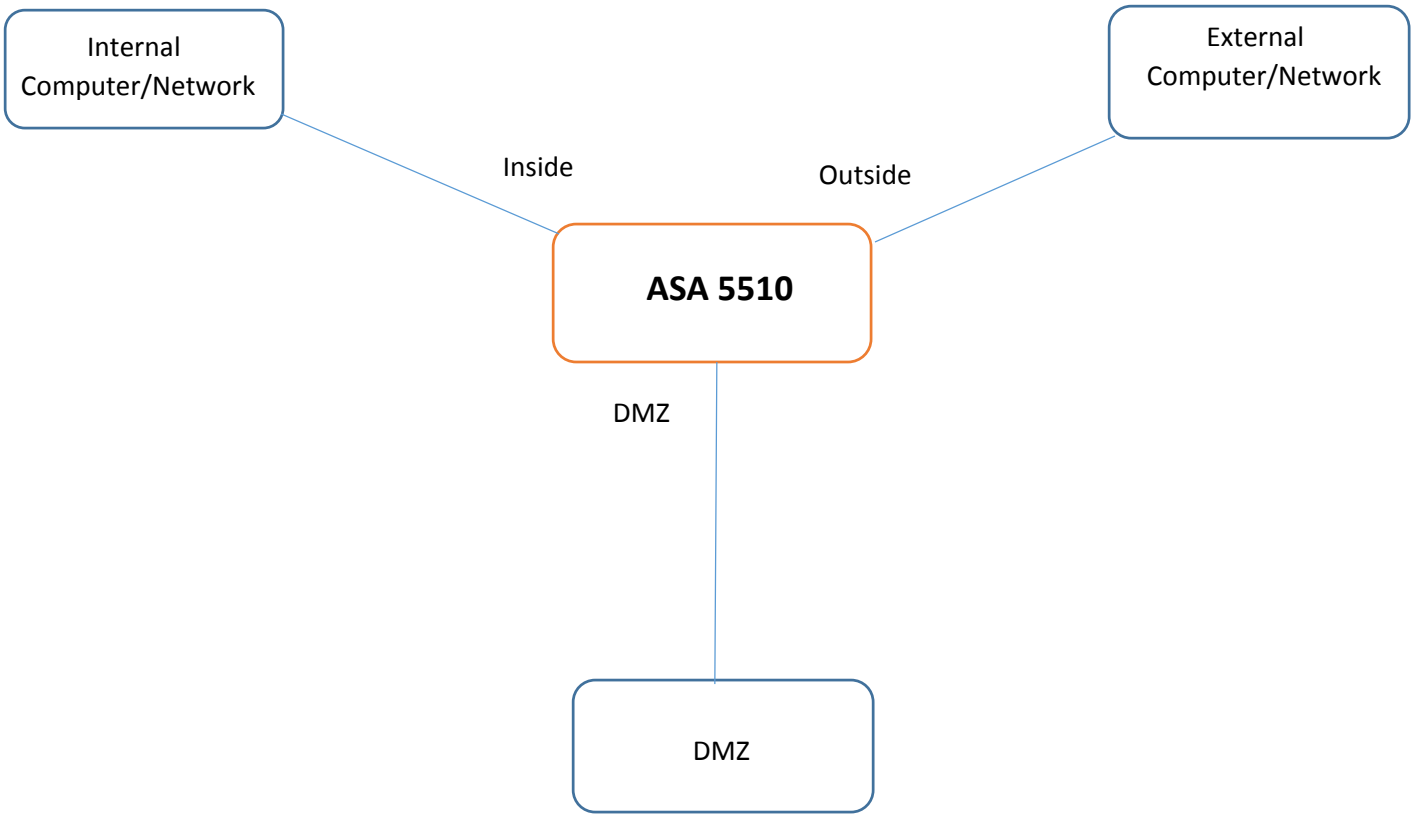
CO325 – Computer & Network Security

Lab 02: Network Address Translation + Access Control Lists

1. IP address/mask and gateway addresses used in the configuration of all the devices (ASA interfaces, internal SSH Server, Gateway SSH server and the client)



- ASA interfaces:
  Inside interface -
  Ip address - 192.168.10.1
  Netmask - 255.255.255.0

  Outside interface -
  Ip address - 172.16.20.1
  Netmask - 255.255.255.0

DMZ interface –

Ip address - 172.20.30.1
Netmask - 255.255.255.0

- External network: client

  Ip address – 172.16.20.112
  Netmask – 255.255.255.0
  Default gateway – 172.16.20.1

- Internal SSH Server

  Ip address – 192.168.10.100
  Netmask – 255.255.255.0
  Default gateway – 192.168.10.1

- Gateway SSH server

  Ip address – 172.20.30.100
  Netmask – 255.255.255.0
  Default gateway – 172.20.30.1

2. NAT and ACL rules to facilitate the operation explained above, complying with the conditions.

   ASA 5510 CLI,

```
ciscoasa(config)# interface gigabitEthernet 1/3
ciscoasa(config-if)#nameif inside2
ciscoasa(config-if)#ip address 192.168.10.1 255.255.255.0
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#no shutdown

ciscoasa(config)# interface gigabitEthernet 1/4
ciscoasa(config-if)#nameif outside2
ciscoasa(config-if)#ip address 172.16.20.1 255.255.255.0
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#no shutdown
```

```
ciscoasa(config)# interface gigabitEthernet 1/5
ciscoasa(config-if)#nameif dmz
ciscoasa(config-if)#ip address 172.20.30.1 255.255.255.0
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)#no shutdown
```

NAT

```
ciscoasa(config)# object network outside2-mapped-server
ciscoasa(config-network-object)# host 172.16.20.10

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

ciscoasa(config-network-object)# nat (dmz, outside2) static outside2-mapped-server
```

ACL1

```
ciscoasa(config)# access-list outany2dmz extended permit tcp any object dmz-real-
                  server eq ssh
ciscoasa(config)# access-group outany2dmz in interface outside2
```

ACL2

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

3. Explain clearly how you have satisfied each of the conditions given above with your NAT and ACL rules.

In ASA 5510 first I have configured 3 interfaces for internal network, external network and demilitarized zone. I have named them as inside2, outside2 and dmz respectively.

If outside network wants to communicate with internal SSH server it should be a two step process. First outside device has to login to the gateway server, and then login to the internal SSH server.

In our configurations external access is allowed to the SSH service at the DMZ SSH Server and external access is not allowed to use any other service at the DMZ SSH Server. That means any device (more than one device) in the external network should be able to used gateway SSH server at DMZ.

In this case I have created two network objects one in demilitarized zone for real dmz gateway SSH server (172.20.30.100) and other one in outside2 for mapped ip (172.16.20.10). Then I have created a static NAT rule to map the dmz network object to its mapped IP address. I have used static NAT because the mapping is for a server. The connection is not going to dynamically. A static NAT works by creating a one-to-one relationship between the public and private IP address. This means the private IP address can be mapped to only one public IP address at a time. The end user, on the other hand, has a transparent view of the remote device/network and accesses it using the mapped public IP address.

ACL1 is for the external network and the demilitarized zone. This ACL rule has allowed any device in the subnet at the external network to use TCP service which is equal to SSH to communicate with only host 172.20.30.100 (DMZ gateway SSH server) in demilitarized zone. Then no device in the external network can use other services at the DMZ SSH server because of this ACL.

Then SSH Service is allowed between the DMZ SSH Server and the Internal SSH Server, no other service in the internal SSH server is accessible from the DMZ and no other device in the internal network is accessible from DMZ.

To satisfy above requirement I have used ACL2. In ACL2 rule it gives permission to dmz gateway server ip 172.20.30.100 to communicate with internal network SSH server 192.168.10.100. So no other device in dmz can use SSH server at internal network and and no other service in internal server can be used by devices in dmz.

According to the requirements internal network is not directly accessible in any way from the outside network. So I haven't created any ACL rule for inside and outside networks then default rules are applied. Then the above requirement has satisfied.