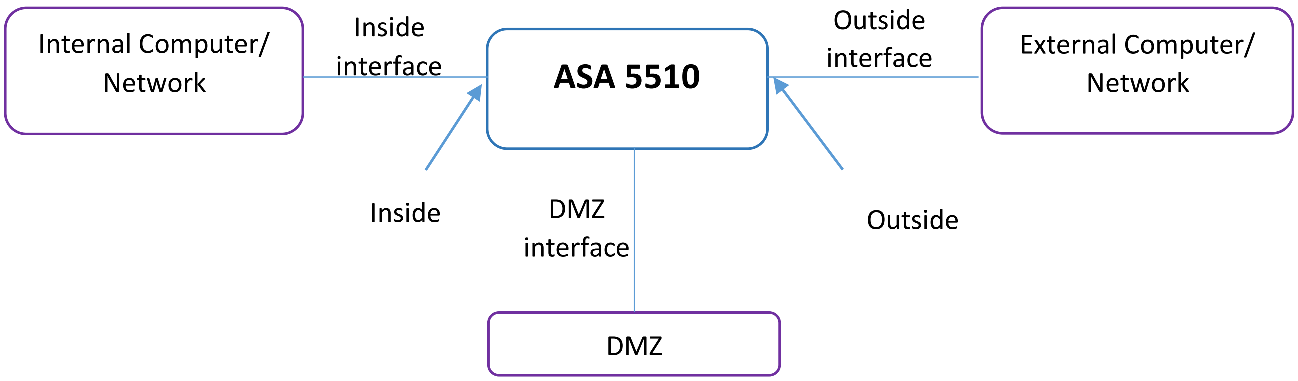
CO325 – Computer & Network Security

Lab 02: Network Address Translation + Access Control Lists

Assignment:



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).

		IP Address	Netmask	Gateway address
ASA interfaces	Inside interface	192.168.10.1/24	255.255.255.0	192.168.10.1
	Outside interface	172.16.20.1/24	255.255.255.0	172.16.20.1
	DMZ interface	172.20.40.1/24	255.255.255.0	172.20.40.1
Gateway SSH Server		172.20.40.100/24	255.255.255.0	172.20.40.1
Internal SSH server		192.168.10.100/24	255.255.255.0	192.168.10.1
Client (External)		172.16.20.112/24	255.255.255.0	172.16.20.1

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

- ASA configuration

  Inside network configuration

```
ciscoasa(config)#interface gigabitEthernet 1/1
ciscoasa(config-if)#nameif inside1
ciscoasa(config-if)#ip address 192.168.10.1 255.255.255.0
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#no shutdown
```

Outside network configuration

```
ciscoasa(config)#interface gigabitEthernet 1/2
ciscoasa(config-if)#nameif outside1
ciscoasa(config-if)#ip address 172.16.20.1 255.255.255.0
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#no shutdown
```

DMZ configuration

```
ciscoasa(config)#interface gigabitEthernet 1/3
ciscoasa(config-if)#nameif dmz
ciscoasa(config-if)#ip address 172.20.40.1 255.255.255.0
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)#no shutdown
```

NAT

(map a static ip to dmz for outside communication)

```
ciscoasa(config)#object network dmz-real-server
ciscoasa(config-network-object)#host 172.20.40.100
ciscoasa(config-network-object)#nat (dmz,outside) static 172.20.40.20
```

ACL rules

1. (Allow SSH access from outside any host to the mapped DMZ host)

```
ciscoasa(config)# access-list outside_acl_any2dmz extended permit tcp any object dmz-real-server eq ssh

ciscoasa(config)# access-group outside_acl_any2dmz in interface outside1
```

2. **(Allow SSH access from DMZ to the inside host 192.168.10.100)**

```
ciscoasa(config)# access-list acl_dmz2inside extended permit tcp object dmz-real-server host 192.168.10.100 eq ssh

ciscoasa(config)# access-group acl_dmz2inside in interface dmz
```

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

The basic ASA configuration setup is of three interfaces connected to three network segments. The ISP network segment is connected to the gigabitEthernet1/1 interface and labelled **outside1** with a security level of 0. The internal network has been connected to gigabitEthernet1/2 and labelled as **inside1** with a security level of 100. The DMZ segment, where the SSH server resides, is connected to gigabitEthernet1/3 and labelled as **dmz** with a security level of 50.

ASA's **inside** interface is set with the IP address of 192.168.10.1. The ASA's **outside** interface is configured with the IP address 172.16.20.1 . dmz interface is configured with the IP address of 172.20.40.1 .

ACLs on the ASA allow you to override the default security behavior which is as follows:

- Traffic that goes from a **lower** security interface is **denied** when it goes to a **higher** security interface.
- Traffic that goes from a **higher** security interface is **allowed** when it goes to a **lower** security interface.

So without the addition of any ACLs to the configuration, this traffic works:

- Hosts on the **inside1** (security level 100) can connect to hosts on the **dmz** (security level 50).
- Hosts on the **inside1** (security level 100) can connect to hosts on the **outside1** (security level 0).
- Hosts on the **dmz** (security level 50) can connect to hosts on the **outside1** (security level 0).

However, this traffic is denied:

- Hosts on the **outside1** (security level 0) cannot connect to hosts on the **inside1** (security level 100).
- Hosts on the **outside1** (security level 0) cannot connect to hosts on the **dmz** (security level 50).

- Hosts on the **dmz** (security level 50) cannot connect to hosts on the **inside1** (security level 100).

So to satisfy the given conditions, we have to set NAT and ACL rules as declared above.

If any outside host tries to enter the DMZ server, it goes through 172.20.40.20 which will be mapped to DMZ interface ip 172.16.40.100 of SSH server, by the NAT rules.

Rule one of ACL rules says that it will only allow tcp ssh traffic for any host from outside to access DMZ Server.

Rule two of ACL rules says that it will only allows tcp ssh traffic only for the inside host 192.168.10.100 from DMZ server.

So, according to the rules, if outside network wants to access inside host through SSH, it has to follow two step process - login to the gateway server, and then login to the internal SSH server.