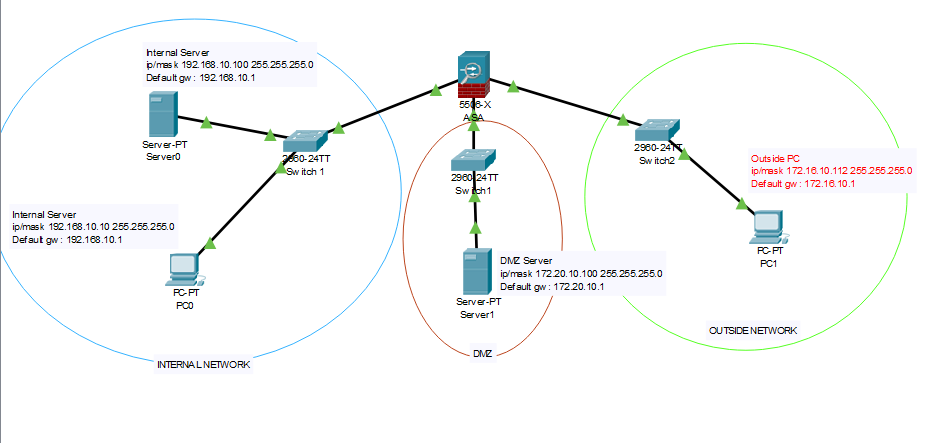
Premathilaka M.P.U

E/15/280

**C0325 – Lab 02: Network Address Translation + Access Control Lists**

**NETWORK DIAGRAM**

**NETWORK CONFIGURATION**

Internal SSH Server

* IP Address : 192.168.10.100
* Subnet Mask : 255.255.255.0
* Default Gateway : 192.168.10.1

Internal PC

* IP Address : 192.168.10.10
* Subnet Mask : 255.255.255.0
* Default Gateway : 192.168.10.1

External PC

* IP Address : 172.16.10.112
* Subnet Mask : 255.255.255.0
* Default Gateway : 172.16.10.1

DMZ (demilitarized zone) SSH Gateway Server

* IP Address : 172.20.10.100
* Subnet Mask : 255.255.255.0
* Default Gateway : 172.20.10.1

CISCO ASA

* Inside network int : 192.168.10.1

(GigabitEthernet 1/1)

IP Address

Default Gateway : 255.255.255.0

* Outside network int : 172.16.10.1

(GigabitEthernet 1/2)

IP Address

Default Gateway : 255.255.255.0

* DMZ network int : 172.20.10.1

(GigabitEthernet 1/3)

IP Address

Default Gateway : 255.255.255.0

**NAT+ACL RULES**

1. ASA configuration

ciscoasa(config)# interface gigabitEthernet 1/1

ciscoasa(config-if)# nameif inside

ciscoasa(config-if)# ip address 192.168.10.1 255.255.255.0

ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# security-level 100

ciscoasa(config-if)# exit

ciscoasa(config)# interface gigabitEthernet 1/2

ciscoasa(config-if)# nameif outside

ciscoasa(config-if)# ip address 172.16.10.1 255.255.255.0

ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# security-level 0

ciscoasa(config-if)# exit

ciscoasa(config)# interface gigabitEthernet 1/3

ciscoasa(config-if)# nameif dmz

ciscoasa(config-if)# ip address 172.20.10.1 255.255.255.0

ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# security-level 50

ciscoasa(config-if)# exit

1. **External access is allowed to the SSH service at the DMZ SSH Server.**
2. **External access is NOT allowed to any other service at the DMZ SSH Server.**

ciscoasa(config)# access-list out2dmzssh extended permit tcp any host 172.20.10.100 eq 22

ciscoasa(config)# access-list out2dmzssh extended deny ip any host 172.20.10.100

ciscoasa(config)# access-group out2dmzssh in interface outside

. As shown above, in order to facilitate condition 1 & 2, clients which use SSH protocol from the outside network can access to the DMZ ssh gateway server (ACL ‘out2dmzssh’ statement 1). Any other client that tries to access using different protocol is restricted using the ACL ‘out2dmzssh’ statement 2

1. **SSH Service is allowed between the DMZ SSH Server and the Internal SSH Server.**
2. **No other service in the internal SSH server is accessible from the DMZ.**
3. **No other device in the internal network is accessible from DMZ.**

ciscoasa(config)# access-list dmz2inSSH extended permit tcp host 172.20.10.100 host 192.168.10.100 eq 22

ciscoasa(config)# access-list dmz2inSSH extended deny ip any host 192.168.10.100

ciscoasa(config)# access-list dmz2inSSH extended deny ip any host 192.168.10.0

ciscoasa(config)# access-group dmz2inSSH in interface dmz

Only DMZ SSH gateway server is allowed to access to the internal network through the dmz interface only using the ssh protocol by applying ACL ‘dmz2inSSH’ statement 1.

Using ACL ‘dmz2inSSH’ statement 2, no other client is allowed to access internal server from DMZ network using different protocol. This states that only service provided by the internal network to the DMZ network is SSH

Using ACL ‘dmz2inSSH’ statement 3, any device in the network 192.168.10.0 255.255.255.0 is not accessible by any other client at the dmz interface.

1. **Internal network is NOT directly accessible in any way from the outside network.**

ciscoasa(config)# access-list out2in extended deny ip any 192.16.10.0 255.255.255.0

ciscoasa(config)# access-group out2in in interface outside

ACL out2in applied to the outside interface and it deny all the packets which destinated to the inside network directly.

There are 3 interfaces configured in the ASA for (ASA 550X) for internal network, outside network and demilitarized zone. Since, inside network has a higher security level (100), clients from the outside network (security level 0) and clients from DMZ (security level 50) cannot reach to the inside network by default.

Inorder to facilitate given 6 conditions multiple ACL’s are used