CO325 - LAB 02

Network Address Translation + Access Control Lists

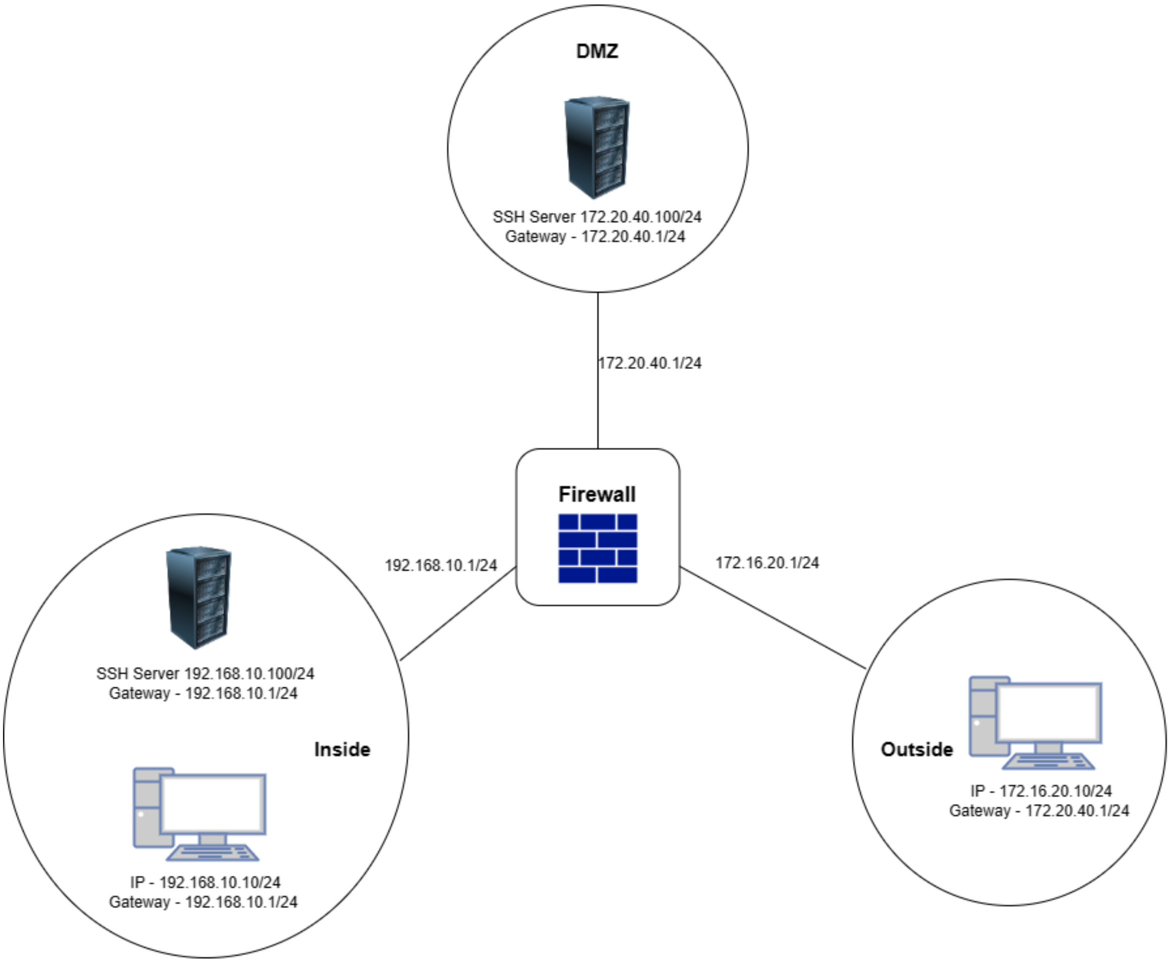
WIJERATHNE E.S.G.

E/18/397

SEMESTER 05

23/12/2022

01.



02.

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

ciscoasa(config-network-object)# host 172.20.40.100


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 172.20.40.3

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
```

03.

- **For network dmz-server**

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

- *creating a network object*

```
ciscoasa(config-network-object)# host 172.20.40.100
```

- *setting up IP address*

Giving accesses

```
ciscoasa(config)# access-list out2dmz extended permit tcp any object dmz-server eq ssh
```

- *allow any SSH traffic from the outside to the DMZ SSH Sever*

```
ciscoasa(config)# access-list out2dmz extended deny ip any any
```

- *deny all the traffic from the outside to the inside and the DMZ*

```
ciscoasa(config)# access-group out2dmz in interface outside
```

- *apply ACL inbound to the external interface*

- **for dmz-mapped-server**

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

- *creating a network object*

```
ciscoasa(config-network-object)# host 172.20.40.3
```

- *Define IP such that maps to the inside SSH server’s IP address.*

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

- *Create network object for inside network SSH server*

```
ciscoasa(config-network-object)# host 192.168.10.100
```

- *Setting IP for inside SSH server*

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

- *Using NAT rule which maps inside SSH IP address and DMZ SSHIP address with DMZ- mapped IP address. (So we can access inside SSH server from DMZ SSH server using mapped IP address which is 172.20.30.3)*

Rules

```
ciscoasa(config)# access-list dmz2in extended permit tcp object dmz-server object inside-real-server eq ssh
```

- *Allows any SSH traffic from DMZ to inside SSH sever.*

```
ciscoasa(config)# access-list dmz2in extended deny ip any any
```

- *Deny any other traffic from DMZ to inside*

```
ciscoasa(config)# access-group dmz2in in interface dmz
```

- *apply ACL inbound to the external interface*