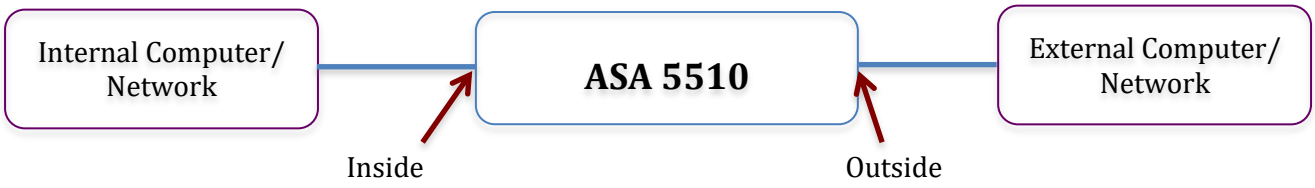
CO325 – Computer & Network Security

Lab 02: Network Address Translation + Access Control Lists

1. NAT Configurations – Learning

Network Diagram



Group A use the Interfaces 0/0 and 0/1 – Use **x =10** as the third octet in IP addresses
Group B use the interfaces 0/2 and 0/3 – Use **x =20** as the third octet in IP addresses

```
ASA inside interface IP: 192.168.x.1/24
ASA outside interface IP: 172.16.x.1/24
```

For **each scenario** (different NAT configuration) you test, do the following *after establishing the SSH connections through the ASA*:

- Use `netstat -an` command in both SSH client & server to see the IP addresses and ports (source/destination) of the connection.
- Use `show conn` and `show xlate` commands in the ASA to check the connections and the NAT translations through the ASA

a. SSH/HTTP Server Inside

```
Inside SSH/HTTP Server IP Address: 192.168.x.100/24
Outside client IP Address: 172.16.x.112/24
```

Set Inside server's gateway to ASA inside interface IP
Set outside client's gateway to ASA outside interface IP

i. No NAT + ACL

Create a network object (for a host) and define its IP address.

```
ciscoasa(config)# object network inside-net-obj
ciscoasa(config-network-object)# host 192.168.x.100
```

include the object in an ACL to permit traffic from outside to inside

```
ciscoasa(config)# access-list out2in extended permit ip any object inside-net-obj
ciscoasa(config)# access-group out2in in interface outside
```

Connect to the SSH server by using its IP address (Check *netstat, show conn* and *show xlate* outputs as instructed earlier). Disconnect and clear the access rules and the network objects you created (remember to do that after each scenario). E.g.,

```
no access-list out2in extended permit ip any object inside-net-obj
no object network inside-net-obj
```

ii. Static NAT + ACL

Create network objects for a real host and the IP address it's mapped to.
Create a Static NAT rule to map the inside network object to its mapped IP address (notice that this is done from within the inside network object)

```
ciscoasa(config)# object network outside-mapped-server
ciscoasa(config-network-object)# host 172.16.x.3

ciscoasa(config)# object network inside-real-server
ciscoasa(config-network-object)# host 192.168.x.100
ciscoasa(config-network-object)# nat (inside,outside) static outside-mapped-server

ciscoasa(config)# access-list out2in extended permit ip any object inside-real-
server
ciscoasa(config)# access-group out2in in interface outside
```

Connect to the SSH/HTTP server by using the mapped IP address (172.16.x.3).

iii. Static PAT + ACL

Create a network object for the IP address the servers are mapped to.
Create network objects for the real host for each service (e.g., SSH, HTTP).
Create Static PAT rules to map *a specific port* (service) of the inside network object to *a specific port* of its mapped IP address (note: to define the port in each case you can use the known service name or specify your own numeric value).

```
ciscoasa(config)# object network outside-mapped-servers
ciscoasa(config-network-object)# host 172.16.x.3

ciscoasa(config)# object network inside-real-ssh
ciscoasa(config-network-object)# host 192.168.x.100
ciscoasa(config-network-object)# nat (inside,outside) static outside-mapped-servers
service tcp ssh ssh
ciscoasa(config)# object network inside-real-http
ciscoasa(config-network-object)# host 192.168.x.100
ciscoasa(config-network-object)# nat (inside,outside) static outside-mapped-servers
service tcp http 8080

ciscoasa(config)# access-list out2in extended permit ip any object inside-real-ssh
ciscoasa(config)# access-list out2in extended permit ip any object inside-real-http
ciscoasa(config)# access-group out2in in interface outside
```

Connect to the SSH server and HTTP server (port 8080) by using the mapped IP address

b. SSH/HTTP Server outside

```
SSH/HTTP Server IP Address: 172.16.x.37
Inside client IP address: 192.168.x.107
```

Configure the default gateway on inside clients to 192.168.x.1 (inside interface IP)
In each of the cases below, connect to the SSH/HTTP server by using its real IP address

i. NO NAT

```
-- nothing --
```

ii. Static NAT

Create a network object for the IP address ***Range*** the clients are mapped to.
Create network object for the clients in a selected IP Address ***Range***
(Note: Both mapped and real IP address ranges should be of the same size)
Map the internal IP address range to outside IP range using a Static NAT rule

```
ciscoasa(config)# object network out-mapped-clients
ciscoasa(config-network-object)# range 172.16.x.200 172.16.x.209
ciscoasa(config)# object network in-real-clients
ciscoasa(config-network-object)# range 192.168.x.100 192.168.x.109
ciscoasa(config-network-object)# nat (inside,outside) static out-mapped-clients
```

iii. Dynamic NAT

Create a network object for the IP address Range the clients are mapped to.
Create network object for the clients using their IP Address Range.
(Note: IP address ranges could be of different sizes)
Map the internal IP address range to outside IP range using a Dynamic NAT rule

```
ciscoasa(config)# object network dyn-out-mapped-clients
ciscoasa(config-network-object)# range 172.16.x.200 172.16.x.209
ciscoasa(config)# object network in-real-clients
ciscoasa(config-network-object)# range 192.168.x.100 192.168.x.199
ciscoasa(config-network-object)# nat (inside,outside) dynamic dyn-out-mapped-
clients
```

iv. Dynamic PAT with another IP

Create a network object for the IP address Range the clients are mapped to.
Map the internal IP address range to an outside IP address using a Dynamic PAT rule (in this case, the ASA will use port mapping to for NAT)

```
ciscoasa(config)# object network in-real-clients
ciscoasa(config-network-object)# range 192.168.x.100 192.168.x.109
ciscoasa(config-network-object)# nat (inside,outside) dynamic 172.16.x.222
```

v. Dynamic PAT with interface IP

Create a network object for the IP address Range the clients are mapped to.
Map the internal IP address range to the ***interface IP*** of the outside network using a Dynamic PAT rule.

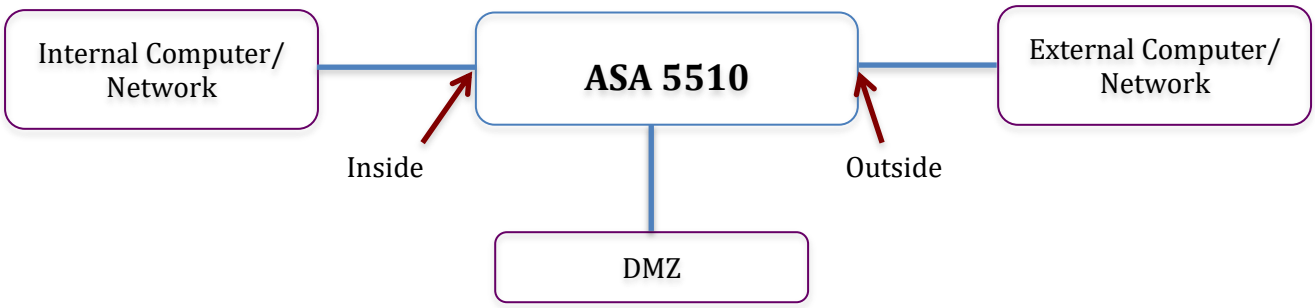
```
ciscoasa(config)# object network in-real-clients
ciscoasa(config-network-object)# range 192.168.x.100 192.168.x.109
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
```

2. Assignment

Scenario: We want to restrict direct access to our internal (inside) network from outside. However, we also want to provide SSH access to one of our devices in the internal network from outside. The solution proposed for this is to establish a demilitarized zone (DMZ) and to put an SSH Server in the DMZ to act as the SSH gateway (you can either use a two-step process – login to the gateway server, and then login to the internal SSH server – OR use *SSH tunneling* to establish one-step login).

Network diagram of the proposed network is given below.

By definition, the DMZ will have a security level in between the inside & outside networks (i.e., if *inside* and *outside* networks have the security levels *100* and *0*, respectively, the *DMZ* should be defined with a security level in the range 1-99).



Your Task: Create the Necessary NAT and ACL rules to facilitate this operation. Your solution should satisfy the following conditions:

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.
3. SSH Service is allowed between the DMZ SSH Server and the Internal SSH Server.
4. No other service in the internal SSH server is accessible from the DMZ.
5. No other device in the internal network is accessible from DMZ.
6. Internal network is NOT directly accessible in any way from the outside network.

Use the IP addresses 172.20.x.1/24 and 172.20.x.100/24 for the ASA DMZ Interface and DMZ SSH server, respectively.

Submission: Your submission should contain the following

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).

   [10 marks]

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

   [40 marks]

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

   [50 marks]