ASA Deep Dive

NAT

Configuring Dynamic NAT

- NAT can be configured in two ways.
  - Manual NAT (Configured Globally)
  - Auto NAT (Configured under the object)
- Manual NAT comes in Section 1 or Section 3. Default is Section 1.
- Auto NAT comes in Section 2.
- The order in which NAT is checked.
  - Section 1 is checked first, top-down.
  - If no match in Section 1, it moves to Section 2.
  - In Section 2, again rules are checked top-down.
  - If no match in Section 2, it moves to Section 3.
  - If no match in Section 3, the traffic is untranslated.
- Section 1 wins over Section 2.
- Within a Section it's the sequence number which takes preference.
- If a NAT rule matches then it needs to translated. Else, it would be dropped. So, if there is no pool or free IP available, traffic gets dropped.
- In ASA code 9.6, access-list hits after NAT when request comes from lower security-level destined to higher security-level. So, we would always need private IP address as destination and private port as destination port.

Configuring Dynamic NAT

- Dynamic NAT translates a group of real addresses to a pool of mapped addresses that are routable on the destination network.
- Dynamic NAT is uni-directional. (Only the source IP address is translated)
- Dynamic NAT
  - Example 1
    - In this example when 192.168.65.0 who is behind inside segment accesses any destination on the outside segment , the source 192.168.65.0/24 would be translated to any ip from the pool 74.0.0.150-74.0.0.160. The Source Port, Destination Port and Destination IP remains unchanged.

```
object network OBJECT-REAL
 subnet 192.168.65.0 255.255.255.0
object network OBJECT-MAPPED
 range 74.0.0.150 74.0.0.160
```

```
nat (INSIDE,OUTSIDE) source dynamic OBJECT-REAL OBJECT-MAPPED
```

```
ASAx1(config)# sh nat
Manual NAT Policies (Section 1)
1 (INSIDE) to (OUTSIDE) source dynamic OBJECT-REAL OBJECT-MAPPED
    translate hits = 0, untranslate hits = 0
```

Configuring Dynamic NAT

- Dynamic NAT
  - Example 2
    - In this example when 74.0.0.0 who is behind outside segment accesses any destination on the inside segment , the source 74.0.0.0/24 would be translated to any ip from the pool 192.168.65.150-192.168.65.160. The Source Port, Destination Port and Destination IP remains unchanged. However you would additionally need ACL from lower to higher.

```
object network OBJECT-R4
 subnet 74.0.0.0 255.255.255.0
object network OBJECT-R4-LAN
 range 192.168.65.150 192.168.65.160
```

```
ASAx1(config)# sh run nat
nat (OUTSIDE,INSIDE) source dynamic OBJECT-R4 OBJECT-R4-LAN
```

```
ASAx1(config)# sh nat
Manual NAT Policies (Section 1)
1 (OUTSIDE) to (INSIDE) source dynamic OBJECT-R4 OBJECT-R4-LAN
    translate_hits = 0, untranslate_hits = 0
```

Configuring Dynamic NAT

- Dynamic NAT
  - Example 3
    - In this example when 192.168.65.0 who is behind inside segment accesses any destination on the outside segment , the source 192.168.65.0/24 would be translated to any ip from the pool 74.0.0.150-74.0.0.160. The Source Port, Destination Port and Destination IP remains unchanged. This would be seen in Section 2.

```
ASAx1(config)# sh run object
object network OBJECT-REAL
 subnet 192.168.65.0 255.255.255.0
object network OBJECT-MAPPED
 range 74.0.0.150 74.0.0.160
```

```
ASAx1(config)# sh run nat
!
object network OBJECT-REAL
 nat (INSIDE,OUTSIDE) dynamic OBJECT-MAPPED
```

```
ASAx1(config)# sh nat

Auto NAT Policies (Section 2)
1 (INSIDE) to (OUTSIDE) source dynamic OBJECT-REAL OBJECT-MAPPED
    translate_hits = 0, untranslate_hits = 0
```