ASA Deep Dive

ACL, Objects & Object Groups

Configuring OSPF on ASA

- Objects or Object-Groups are used to identify networks or services.
- Objects can only have one entry inside it.
- Object-Groups can have multiple entries inside it.
- There are two types of Objects that you can create.
  - Network
  - Service
- There are six types of Object-Groups that you can create.
  - Network
  - Service
  - Protocol
  - User
  - ICMP-Type
  - Security

Configuring OSPF on ASA

- Configuring Objects
  - Example 1

```
object network O-PC
 host 192.168.0.100
```

  - Example 2

```
object network O-Subnet
 subnet 192.168.0.0 255.255.255.0
```

  - Example 3

```
object network O-Range
 range 192.168.0.1 192.168.0.10
```

Configuring OSPF on ASA

- Configuring Objects
  - Example 4

```
object service O-telnet
 service tcp destination eq telnet
```

  - Example 5

```
object service O-dns
 service udp destination eq domain
```

  - Example 6

```
object service O-SourcePort
 service tcp source eq 1234
```

Configuring OSPF on ASA

- Configuring Object-Groups.
  - Example 1

```
object-group network OG-Subnets
 network-object 192.168.0.0 255.255.255.0
 network-object 192.168.1.0 255.255.255.0
```

  - Example 2

```
object-group network OG-Hosts
 network-object host 10.0.0.1
 network-object host 10.0.0.2
```

  - Example 3

```
object-group network OG-Hosts_and_Subnets
 network-object host 10.0.0.1
 network-object 192.168.0.0 255.255.255.0
```

Configuring OSPF on ASA

- Configuring Object-Groups.
  - Example 4

```
object-group service OG-Telnet_DNS
 service-object tcp destination eq telnet
 service-object udp destination eq domain
```

Configuring OSPF on ASA

- Access-lists are used to define permissions for traffic flow.
- You can create two kinds of Access-lists.
  - Interface-Based
  - Global
- Interface based ACL's take precedence over Global ACL's.
- Order of check for ACL's.
  - Step 1: Match traffic using Interface-Based ACL. If no match, then move to Step 2.
  - Step 2: Match traffic using Global ACL. If no match, then move to Step 3.
  - Step 3: Match traffic using Adaptive Security Algorithm.

    (All traffic from higher security-level to lower security-level is permitted and all traffic from lower security-level to higher security-level is denied by default.)

Configuring OSPF on ASA

- Configuring Interface-Based ACL.
  - Example 1

```
access-list OUT_IN extended permit tcp any host 10.0.0.1 eq telnet
```

  - Example 2

```
access-list OUT_IN extended permit tcp any 192.168.0.0 255.255.255.0 eq telnet
```

  - Example 3

```
access-list OUT_IN extended permit tcp any object O-PC eq telnet
```

  - Example 4

```
access-list OUT_IN extended permit object O-telnet any object O-Subnet
```

  - Example 5

```
access-list OUT_IN extended permit tcp any object-group OG-Hosts_and_Subnets eq telnet
```

Configuring OSPF on ASA

- Configuring Interface-Based ACL.
  - Example 6

```
access-list OUT_IN extended permit object-group OG-Telnet_DNS any object-group OG-Hosts_and_Subnets
```

- Applying ACL to interface.
  - Example 1

```
access-group OUT_IN in interface OUTSIDE
```

  - Example 2

```
access-group OUT_IN out interface OUTSIDE
```

Configuring OSPF on ASA

- Configuring Global ACL.
  - Example 1

```
access-list GLOBAL_ACL extended permit udp any any eq domain
```

- Applying ACL globally.
  - Example 1

```
access-group GLOBAL_ACL global
```