Cisco CCNA (200-301)

Configuring and Verifying Named ACLs

Learning Objectives: Configure and Verify Named ACLs

Description: Routers look at destination IP address to make a routing decision on how packets will leave that router. You will learn how to use the IOS Access Control List to identify traffic to either permit or deny it towards its destination.

Q: What is the purpose of ACLs on Cisco Devices?

- Help to identify traffic via IP address, Protocol that we want to allow or deny
- These examine every packet by the IP address according to configuration to control access
- There are 2 types access control lists: Standard and Extended. Today we are looking specifically deeper in configuring extended ACLs.

Q: How do they work?

- List is evaluated from top to bottom--Most specific rule to generic
    - It is evaluated until a match, then it stops.
- There is an implicit deny any traffic at the end of every list
    - If traffic does match any other rule in the list it will be *implicity denied.*

Q: How do we configure named ACLs?

- There are 2 types access control lists: Standard and Extended. Today, we are looking specifically deeper in configuring named ACLs.
- Configure a Named Access-List

```
NYEDGE1#configure terminal
NYEDGE1(config)#ip access-list extended permit-ftp
NYEDGE1(config-ext-nacl)#permit tcp host 192.168.16.10 host 172.15.0.10 eq ftp
NYEDGE1(config-ext-nacl)#deny icmp host 192.168.16.10 any
NYEDGE1(config-ext-nacl)#exit
NYEDGE1(config)#exit
NYEDGE1#
NYEDGE1#show ip access-lists permit-ftp
```

- Modify a Named Access-list

```
NYEDGE1#configure terminal
NYEDGE1(config)#ip access-list extended permit-ftp
NYEDGE1(config-ext-nacl)#15 permit tcp host 192.168.16.10 host 172.15.0.10 eq ftp-data
NYEDGE1(config-ext-nacl)#exit
NYEDGE1(config)#exit
NYEDGE1#show ip access-lists permit-ftp
```

- Apply to the interface

```
NYEDGE1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
NYEDGE1(config)#interface gigabitEthernet 0/0
NYEDGE1(config-if)#ip access-group permit-ftp in
NYEDGE1(config-if)#exit
NYEDGE1(config)#exit
NYEDGE1#
```

- Test from PLABCSCO01

```
 cmd
 ping 172.15.0.10
 ftp 172.15.0.10
```

Endnotes, External and Etc.

5.6 Configure and verify access control lists