Access Control Lists (ACLs)

1. Objectives

- Use of **Access Control Lists (ACLs)** defined in Routers to control access in a network.
- Difference between **Standard** and **Extended ACLs**.
- Configuring and applying **Standard** and **Extended ACLs** in Cisco routers.

2a. Access Control Lists (ACLs)

The **Access Control List (ACL)** is a collection of security rules or policies that allows or denies packets after looking at the packet headers and other attributes. Each **permit** or **deny** statement in the ACL is referred to as **an access control entry (ACE)**. These ACEs can classify packets by **inspecting Layer 2 through Layer 4 headers** for a number of parameters, including the following:

- ■ Layer 2 protocol information such as EtherTypes
- ■ Layer 3 protocol information such as ICMP, TCP, or UDP
- ■ Layer 3 header information such as source and destination IP addresses
- ■ Layer 4 header information such as source and destination TCP or UDP ports

After an ACL has been properly configured, you can **apply it to an interface** to filter traffic. The security appliance can filter packets in both the **inbound** and **outbound direction** on an interface. When an **inbound ACL** is applied to an interface, the security appliance analyzes packets against the ACEs after receiving them. If a packet is permitted by the ACL, the firewall continues to process the packet and eventually passes the packet to the defined interface.

2b. Standard ACLs

Standard access control lists (ACLs) are router configuration scripts that control whether a router permits or denies packets based on the **source address only**. Tasks are: **defining filtering criteria**, **configuring standard ACLs**, **applying ACLs to router interfaces**, and **verifying and testing the ACL implementation**.

Example:

a. Create an ACL using the number 1 on **R2** with a statement that denies access to the 192.168.20.0/24 network from the 192.168.11.0/24 network.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

b. By default, an access list denies all traffic that does not match a rule. To permit all other traffic, configure the following statement:

```
R2(config)# access-list 1 permit any
```

c. For the ACL to actually filter traffic, it must be applied to some router operation. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out
```

2c. Extended ACLs

Extended access control lists (ACLs) are extremely powerful. They offer a much greater degree of control than standard ACLs as to the types of traffic that can be filtered, as well as where the traffic originated and where it is going. Extended ACLs can filter traffic in many different ways. Extended ACLs can filter on **source IP addresses**, **source ports**, **destination IP addresses**, **destination ports**, as well as **various protocols and services**. Tasks are: **defining filtering criteria**, **configuring extended ACLs**, **applying ACLs to router interfaces**, and **verifying and testing the ACL implementation**.

a. Create two access list statements to permit tcp for accessing FTP server at 172.22.34.62 and permit ICMP (ping, etc.) traffic from **172.22.34.64/27** network to **Server** at 172.22.34.62. Note that the access list number remains the same and a specific type of ICMP traffic does not need to be specified.

```
R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62
eq ftp
```

b. Enter interface configuration mode and apply the ACL.

```
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip access-group 100 in
```