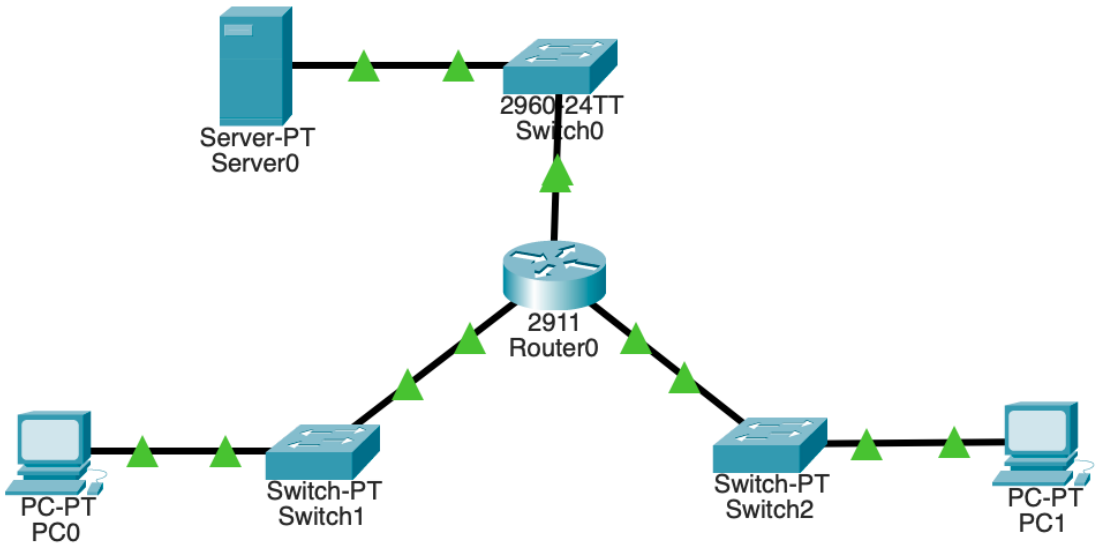
21BDS0340

Abhinav Dinesh Srivatsa

Information Security Management

Digital Assignment – II

Network Configuration for Standard/Extended ACL



Pinging before ACL Implementation

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time=1ms TTL=127
Reply from 10.0.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms


Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=1ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Implementing Standard ACL

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list standard block20
Router(config-std-nacl)#deny 20.0.0.0 0.255.255.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#int gig0/0
Router(config-if)#ip access-group block20 out
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Explaining the Commands

1. Creating a standard access list called block20
2. Adding a rule to deny any packet from the network 20.0.0.0/8
3. Adding a rule to permit any other packets
4. Applying the rule as an out rule to the gigabit interface 0/0, where the server is connected.
5. The makes sure devices on the network 20.0.0.0/8 cannot access the server.

Pinging after Standard ACL Implementation

```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 20.0.0.1: Destination host unreachable.
Reply from 20.0.0.1: Destination host unreachable.
Reply from 20.0.0.1: Destination host unreachable.
Reply from 20.0.0.1: Destination host unreachable.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=43ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time=7ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 43ms, Average = 12ms
```

Implementing Extended ACL

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 deny icmp 20.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255 echo
Router(config)#access-list 101 permit ip any any
Router(config)#int gig0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Explaining the Commands

1. Adding a rule to the extended ACL list 101 to deny any ICMP echo packets originating from the network 20.0.0.0/8 that are sent to any device in 10.0.0.0/8
2. Adding a rule to the extended ACL list 101 the permit any packet otherwise.
3. Applying the rule as an in rule to the gigabit interface 0/1, where the network 20.0.0.0/8 is connected to the router.
4. This enables any device on the 20.0.0.0/8 network to not access the server via ICMP echoes but can still view the HTTP page.

Pinging after Extended ACL Implementation

```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 20.0.0.1: Destination host unreachable.
Reply from 20.0.0.1: Destination host unreachable.
Reply from 20.0.0.1: Destination host unreachable.
Reply from 20.0.0.1: Destination host unreachable.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

HTTP Request after Extended ACL Implementation