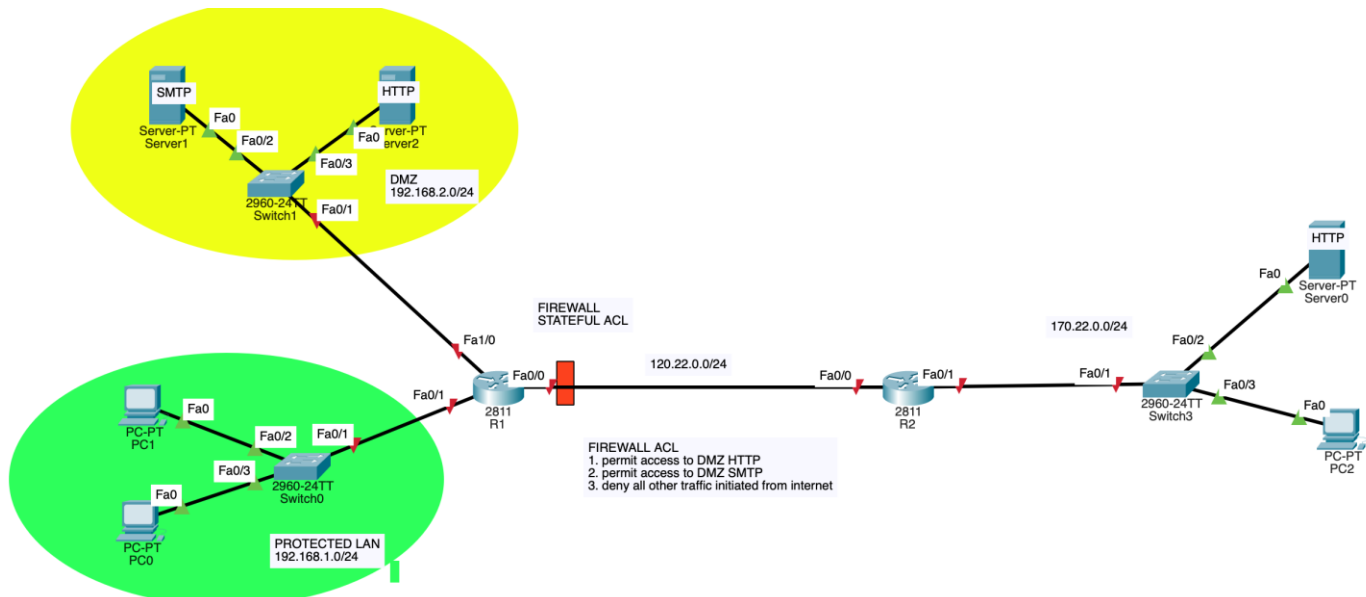


## NET 463

## Lab #6 – ACL Lab

Version 1 – ERIC SOMOGYI June 8, 2024


In Lab #6, you will create a named extended ACL in *Packet Tracer* based on the topology provided in the network diagram below.

**Lab set-up procedure:**

1. Set the hostname on each router and end device to the appropriate name shown in the network diagram.  
NOTE: The device name of device (routers and end devices) **must** be set to include your initials at the end. For example, if the lab includes routers R1 and R2 and hosts Host1 and Host2 and your initials are "AB", you **MUST** set the names of these device to R1-AB, R2-AB, Host1-AB and Host2-AB. This is required so that the prompts in ALL of your screen captures you provide show that it is your work.
2. Create the network as shown in the network diagram using Packet tracer. Configure all interfaces with IP addresses.
3. Either create default routes in each of the routers or configure them to run a routing protocol (your choice) to enable successful pings between any two devices in the network.
4. On the DMZ web server, create a web page that returns "Enterprise web server – <your name> SPRING 2024" when retrieved using HTTP.
5. ON the Internet web server, create a web page that returns "Internet web server – <your name> SPRING 2024" when retrieved using HTTP.
6. Go to the Lab Report/Question section

**Lab Report/Questions:**

1. (5%) On PC 2, **ping** PC 1 and **paste results** here. It should be successful since there is no ACL applied that would filter out any packets.

 PC2-ES

```
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>|
```

2. (5%) On router R1, enter **show ip route** and **paste results** here.

```
R1-ES>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 120.22.0.2 to network 0.0.0.0

    120.0.0.0/24 is subnetted, 1 subnets
C       120.22.0.0 is directly connected, FastEthernet0/0
C       192.168.1.0/24 is directly connected, FastEthernet0/1
C       192.168.2.0/24 is directly connected, FastEthernet1/0
S*     0.0.0.0/0 [1/0] via 120.22.0.2

R1-ES>|
```

3. (5%) On router R2, enter **show ip route** and **paste results** here.

```
R2-ES>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 120.22.0.1 to network 0.0.0.0

    120.0.0.0/24 is subnetted, 1 subnets
C       120.22.0.0 is directly connected, FastEthernet0/0
    170.22.0.0/24 is subnetted, 1 subnets
C       170.22.0.0 is directly connected, FastEthernet0/1
S*    0.0.0.0/0 [1/0] via 120.22.0.1

R2-ES>
```

4. (10%) Now create a named extended ACL that when applied to router R1 will perform the following:

- Permit HTTP services to the HTTP server in the DMZ from the "internet" (outside of the enterprise)
- Permit mail services to the SMTP server in the DMZ from the "internet" (outside of the enterprise)
- Deny all other access from the "internet" to any device in the enterprise
- Permit any device within the protected LAN of the enterprise to query the HTTP server in the "internet"

- Answer:

5. (5%) **List the ACL statement commands below** that accomplishes these requirements

- Answer: Note for teacher: My ip address for HTTP Server in the public internet is 170.22.0.2 and my IP address for my HTTP Server in the DMZ is 192.168.2.3

```
R1-ES(config)#ip access-list extended FROM_PUBLIC_IN
R1-ES(config-ext-nacl)#permit tcp any host 192.168.2.3 eq 80
R1-ES(config-ext-nacl)#permit tcp any host 192.168.2.2 eq 25
R1-ES(config-ext-nacl)#permit tcp host 170.22.0.2 eq 80 192.168.1.0 0.0.0.255 established
R1-ES(config-ext-nacl)#exit
```

```
R1-ES(config)#int fa0/0
```

```
R1-ES(config-if)#ip access-group FROM_PUBLIC_IN in
```

```
R1-ES#show access-list FROM_PUBLIC_IN
Extended IP access list FROM_PUBLIC_IN
    permit tcp any host 192.168.2.3 eq www
    permit tcp any host 192.168.2.2 eq smtp
    permit tcp host 170.22.0.2 eq www 192.168.1.0 0.0.0.255
    established
```

```
R1-ES#
```

6. (5%) After applying the ACL attempt to **ping** from PC2 in the “internet” to PC1 and **paste results** here. **Explain** WHY the **ping** was unsuccessful.

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

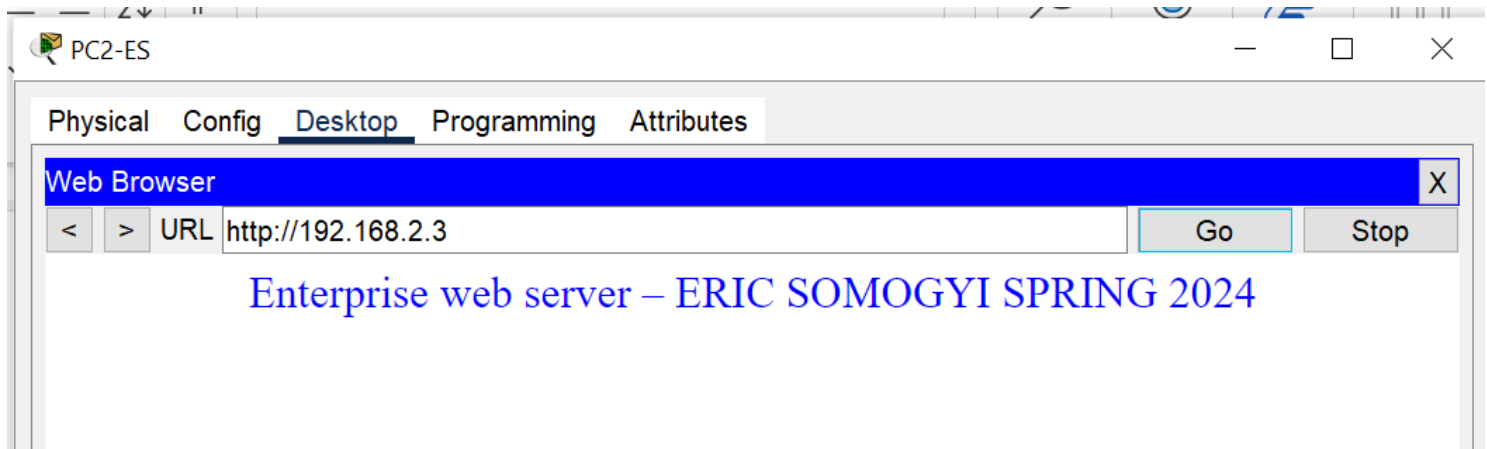
Reply from 120.22.0.1: Destination host unreachable.
Reply from 120.22.0.1: Destination host unreachable.
Reply from 120.22.0.1: Destination host unreachable.
Reply from 120.22.0.1: Destination host unreachable.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

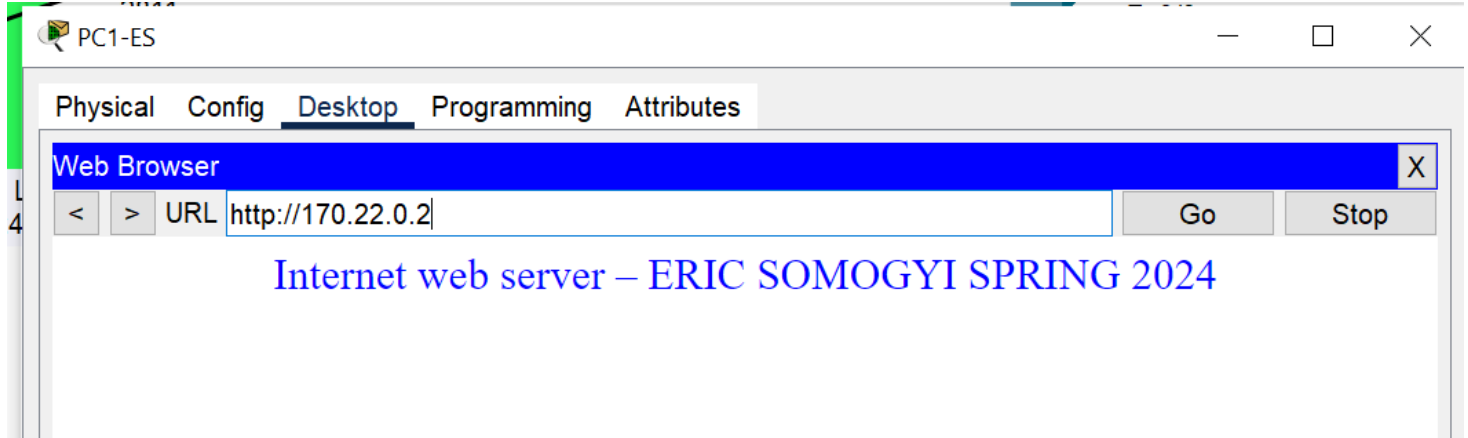
C:\>
```

Answer: The ping was unsuccessful because we only permitted the Host “170.22.0.2” to come in through port 80 from the public internet.

7. (15%) On PC2 in the “internet”, request an HTTP service from the HTTP server in the DMZ and **paste results** here. The request should be successful.



8. (15%) On PC1 in the “enterprise”, request an HTTP service from the HTTP server in the “internet” and **paste results** here. The request should be successful.



9. (10%) Explain the difference in filtering actions between the two possible configuration commands in your ACL.  
**Explain in a clear couple of sentences.**

```
R1(config-ext-nacl)# permit tcp any eq 80 192.168.1.0 0.0.0.255
```

vs

```
R1(config-ext-nacl)# permit tcp any eq 80 192.168.1.0 0.0.0.255 established
```

Answer: The top command is permitting any HTTP tcp connections from source port 80 to any host within the Enterprise protected LAN subnet of 192.168.1.0/24. The bottom command is permitting any HTTP based connections to be access into the 192.168.1.0/24 subnet from the outside internet, only if it is part of an established connection.

10. (5%) From PC1 in the “enterprise”, **ping** PC 2 in the “internet” and **paste results** here (note that this should not be successful). EXPLAIN why this ping is not successful.

```
C:\>ping 170.22.0.3

Pinging 170.22.0.3 with 32 bytes of data:

Request timed out.

Ping statistics for 170.22.0.3:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
C:\>
```

- a) Answer: This ping is not successful because we did not allow any outgoing traffic from the protected LAN to reach the outside internet so outgoing pings from PC1 in the enterprise will not be able to get outside of R1-ES.

11. (5%) What is the configuration command that needs to be added to the ACL in order for the ping in Q11 to be successful? **Add the configuration command line below.**

a) Answer:

```
R1-ES(config)#ip access-list extended FROM_PUBLIC_IN
```

```
R1-ES(config-ext-nacl)#permit icmp 192.168.1.3 170.22.0.3 echo
```

```
R1-ES(config-ext-nacl)#permit icmp any 192.168.1.3 0.0.0.255 echo-reply
```

```
R1-ES(config-ext-nacl)#exit
```

12. (10%) In your ACL, add a statement to permit ping echo response from the “internet”. From PC1, ping PC2 and **paste results** here. This should now be successful.

a) Answer: The second statement allows for the echo response to be received. I tried pinging after the first command but it was not enough.

```
C:\>ping 170.22.0.3

Pinging 170.22.0.3 with 32 bytes of data:

Reply from 170.22.0.3: bytes=32 time<1ms TTL=126
Reply from 170.22.0.3: bytes=32 time=10ms TTL=126
Reply from 170.22.0.3: bytes=32 time<1ms TTL=126
Reply from 170.22.0.3: bytes=32 time<1ms TTL=126

Ping statistics for 170.22.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>
```