Ryan Munger

Internetworking

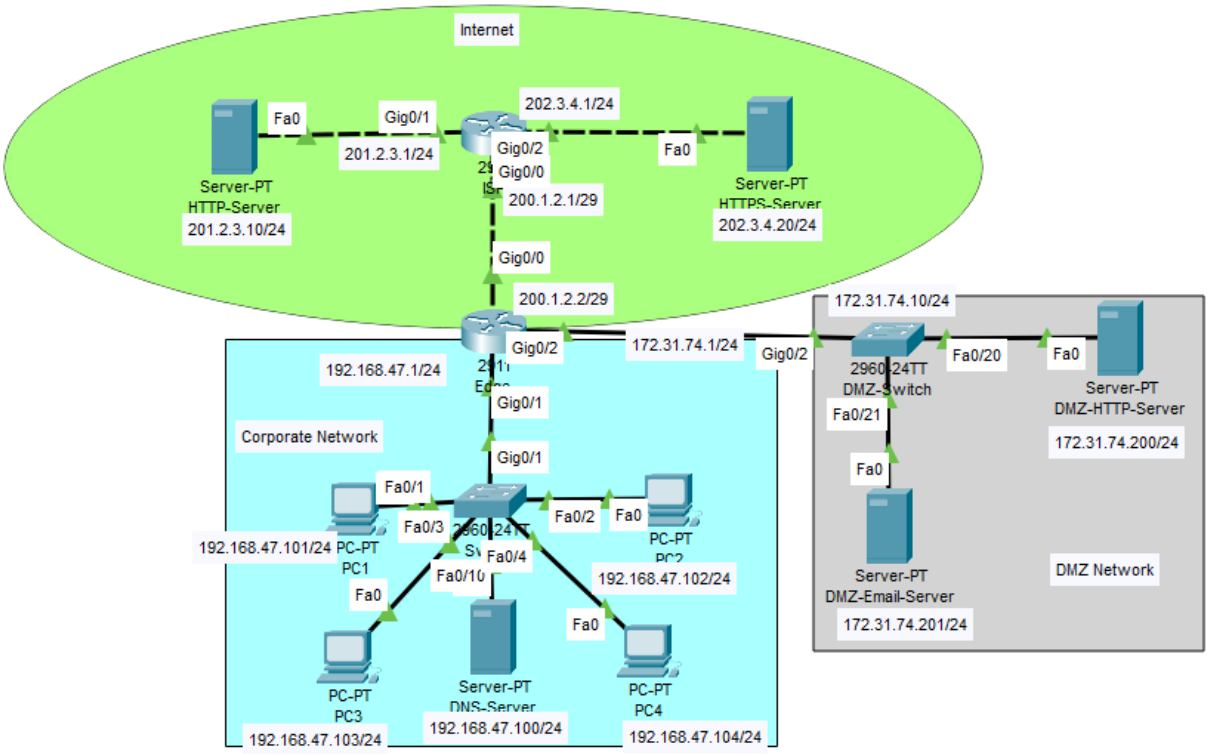
Professor Cannistra

11/21/23

Lab 6

Description: In this lab, I configured an IPv4 Access Control List to allow specific functionality on the networks consisting of a DMZ, a corporate network, and the internet.

Topology/Diagram:



Syntax:

CLI	Command	Description	Mode
Cisco IOS	ip access-list {standard/extended} NAME	creates an std/extended access list with the specified name	Global Config
Cisco IOS	remark <<text>>	creates a remark in the access list to describe the following entry	Access List Config
Cisco IOS	<<permit/deny>> <<protocol>> <<ip>> <<wildcard>> <<destination address>> eq <<port>>	permits/denies the specified connection	Access List Config
Cisco IOS	ip access-group <<number/name>> <<in/out>>	Enables the access list on the specified interface	Interface Config
Cisco IOS	sh access-list	shows access lists and their recorded matches	User Exec
Cisco IOS	sh ip int <int> | include access	shows access lists on the interface and their status (in/out)	User Exec

Test Cases:

Goals:

a) PC1 and PC2 should be able to access the Internet HTTP-Server via HTTP

Test1: PC1 & PC2's browsers are able to connect to this server using HTTP.

b) PC3 and PC4 should be able to access the Internet HTTPS-Server via HTTPS

Test2: PC3 & PC4's browsers are able to connect to this server using HTTPS.

c) All Corporate PCs should be able to access the DMZ-HTTP-Server via HTTPS

Test3: PC1, PC2, PC3, PC4's browsers are able to connect to this server using HTTPS.

d) All Corporate PCs should be able to access the DMZ-EMAIL-Server via SMTP & POP3

Test4: PC1, PC2, PC3, and PC4's traffic generators should be able to send an SMTP PDU and the match in the access list on the corporate router should increase.

Test5: PC1, PC2, PC3, and PC4's traffic generators should be able to send a POP3 PDU and the match in the access list on the corporate router should increase.

e) All Corporate PCs should be able to "ping" the ISP interface connected to the Edge router

Test6: PC1, PC2, PC3, and PC4's command prompts are able to ping the interface.

f) All other traffic should not be permitted

Test7: PC1, PC2, PC3, and PC4's command prompts are not able to ping any other interface or host that is not on their LAN save for the permitted ISP interface.
Test8: PC1 & PC2's browsers cannot connect to the Internet-HTTP server using HTTPS.
Test9: PC3 & PC4's browsers cannot connect to the Internet-HTTP server using HTTP.
TestA: PC3 & PC4's browsers cannot connect to the Internet-HTTP server using HTTPS.
TestB: PC3 & PC4's browsers cannot connect to the Internet-HTTPS server using HTTP.
TestC: PC1 & PC2's browsers cannot connect to the Internet-HTTPS server using HTTP.
TestD: PC1 & PC2's browsers can't connect to the Internet-HTTPS server using HTTPS.
TestE: PC1, PC2, PC3, & PC4's browsers cannot connect to the DMZ-HTTP server using HTTPS.

Verification:

Test Initial Connectivity: PC3 can reach other corporate PCs, the router, and the servers.

```
C:\>ping 192.168.47.101

Pinging 192.168.47.101 with 32 bytes of data:

Reply from 192.168.47.101: bytes=32 time<1ms TTL=128
Reply from 192.168.47.101: bytes=32 time<1ms TTL=128
Reply from 192.168.47.101: bytes=32 time=1ms TTL=128
Reply from 192.168.47.101: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.47.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.47.1

Pinging 192.168.47.1 with 32 bytes of data:

Reply from 192.168.47.1: bytes=32 time<1ms TTL=255
Reply from 192.168.47.1: bytes=32 time=1ms TTL=255
Reply from 192.168.47.1: bytes=32 time<1ms TTL=255
Reply from 192.168.47.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.47.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 201.2.3.10

Pinging 201.2.3.10 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 201.2.3.10: bytes=32 time=1ms TTL=126
Reply from 201.2.3.10: bytes=32 time=1ms TTL=126

Ping statistics for 201.2.3.10:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
C:\>ping 202.3.4.20

Pinging 202.3.4.20 with 32 bytes of data:

Request timed out.
Reply from 202.3.4.20: bytes=32 time<1ms TTL=126
Reply from 202.3.4.20: bytes=32 time=2ms TTL=126
Reply from 202.3.4.20: bytes=32 time<1ms TTL=126

Ping statistics for 202.3.4.20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 172.31.74.201

Pinging 172.31.74.201 with 32 bytes of data:

Request timed out.
Reply from 172.31.74.201: bytes=32 time=1ms TTL=127
Reply from 172.31.74.201: bytes=32 time<1ms TTL=127
Reply from 172.31.74.201: bytes=32 time<1ms TTL=127

Ping statistics for 172.31.74.201:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 172.31.74.200

Pinging 172.31.74.200 with 32 bytes of data:

Request timed out.
Reply from 172.31.74.200: bytes=32 time<1ms TTL=127
Reply from 172.31.74.200: bytes=32 time=1ms TTL=127
Reply from 172.31.74.200: bytes=32 time=1ms TTL=127

Ping statistics for 172.31.74.200:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Edge Router's IPv4 Routing Table:

```
Gateway of last resort is 200.1.2.1 to network 0.0.0.0

     172.31.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.31.74.0/24 is directly connected, GigabitEthernet0/2
L       172.31.74.1/32 is directly connected, GigabitEthernet0/2
     192.168.47.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.47.0/24 is directly connected, GigabitEthernet0/1
L       192.168.47.1/32 is directly connected, GigabitEthernet0/1
     200.1.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.1.2.0/29 is directly connected, GigabitEthernet0/0
L       200.1.2.2/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 200.1.2.1
```

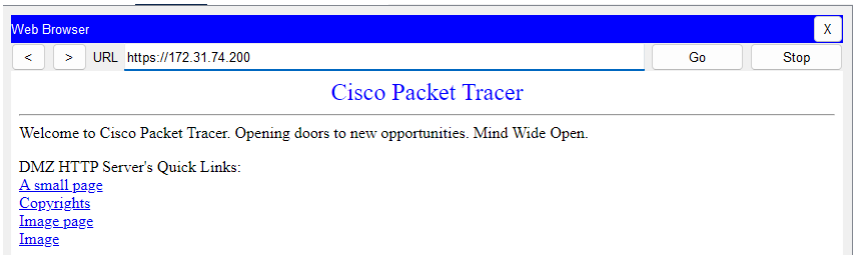
My ACL:

```
Edge#sh access-list
Extended IP access list SERVER-ACCESS
    10 permit tcp host 192.168.47.101 host 201.2.3.10 eq www
    20 permit tcp host 192.168.47.102 host 201.2.3.10 eq www
    30 permit tcp host 192.168.47.103 host 202.3.4.20 eq 443
    40 permit tcp host 192.168.47.104 host 202.3.4.20 eq 443
    50 permit tcp 192.168.47.0 0.0.0.255 host 172.31.74.200 eq 443
    60 permit tcp 192.168.47.0 0.0.0.255 host 172.31.74.201 eq smtp
    70 permit tcp 192.168.47.0 0.0.0.255 host 172.31.74.201 eq pop3
    80 permit icmp 192.168.47.0 0.0.0.255 host 200.1.2.1 echo
    90 deny ip any any
```

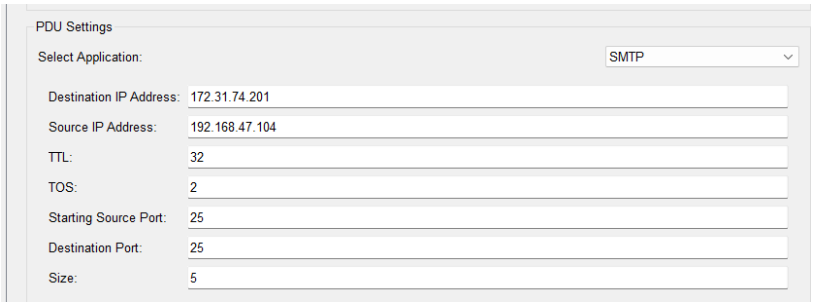
Tests before & after:
Test1: PC1 & PC2 can access Internet-HTTP server via HTTP before as well as after.

Test2: PC3 & PC4 can access Internet-HTTPS server via HTTPS before as well as after.

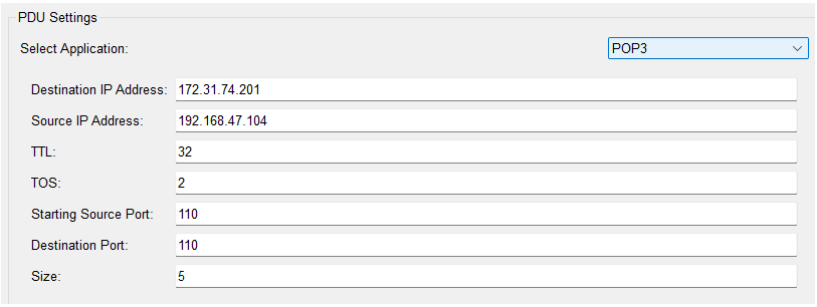
Test3: PC1, PC2, PC3, and PC4 can access DMZ-HTTPS-Server using HTTPS before & after.



Test4 & Test 5: All PCs can send SMTP and POP3 PDUs on the network to the DMZ-Email-Server. This worked before & after. After the ACL is configured, the matches for the permit entry increase when this occurs.




```
60 permit tcp 192.168.47.0 0.0.0.255 host 172.31.74.201 eq smtp (6 match(es))
```




```
70 permit tcp 192.168.47.0 0.0.0.255 host 172.31.74.201 eq pop3 (5 match(es))
```

Test6: PC1, PC2, PC3, and PC4's command prompts are able to ping the ISP interface the edge router is connected to. This works before and after.

```
C:\>ping 200.1.2.1

Pinging 200.1.2.1 with 32 bytes of data:

Reply from 200.1.2.1: bytes=32 time<1ms TTL=254
Reply from 200.1.2.1: bytes=32 time<1ms TTL=254
Reply from 200.1.2.1: bytes=32 time=1ms TTL=254
Reply from 200.1.2.1: bytes=32 time=1ms TTL=254

Ping statistics for 200.1.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Test7: Pinging other interfaces than the ISP connection to the edge router. This worked before the ACL, but it no longer does.

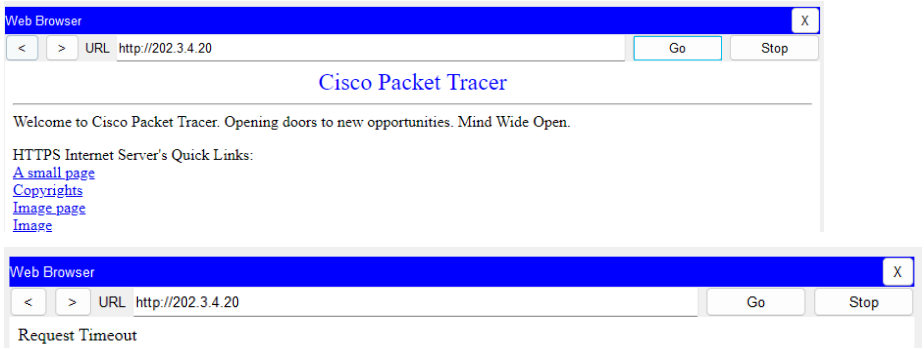
```
C:\>ping 172.31.74.200

Pinging 172.31.74.200 with 32 bytes of data:

Reply from 172.31.74.200: bytes=32 time<1ms TTL=128
Reply from 172.31.74.200: bytes=32 time<1ms TTL=128
Reply from 172.31.74.200: bytes=32 time=1ms TTL=128
Reply from 172.31.74.200: bytes=32 time<1ms TTL=128

Ping statistics for 172.31.74.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>ping 172.31.47.200

Pinging 172.31.47.200 with 32 bytes of data:

Reply from 192.168.47.1: Destination host unreachable.
Reply from 192.168.47.1: Destination host unreachable.
Reply from 192.168.47.1: Destination host unreachable.
Reply from 192.168.47.1: Destination host unreachable.

Ping statistics for 172.31.47.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

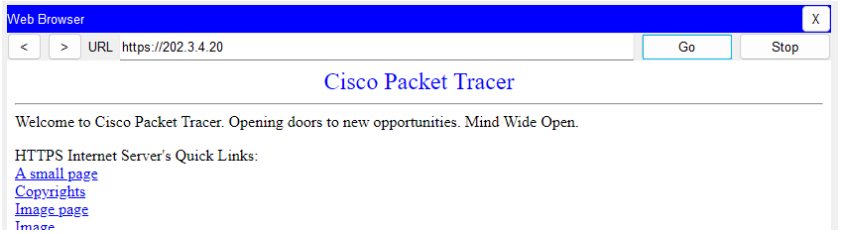
Test8: PC1 & PC2 can access Internet-HTTP-Server using HTTPS. This worked before, but it no longer works now that the ACL is implemented.

Test9 & TestA: PC3 & PC4 can access Internet-HTTP-Server. This was functional before on both HTTP and HTTPs, and is now not functional on either.

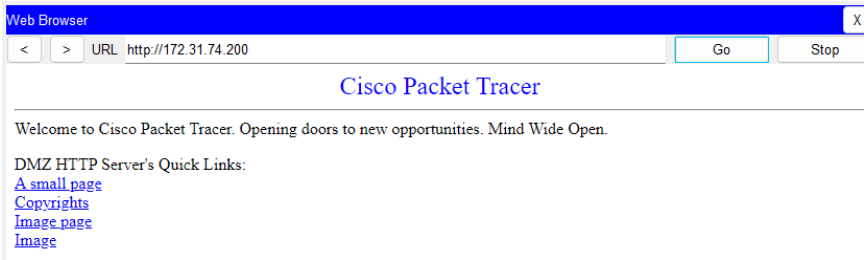
TestB: PC3 & PC4 can access the Internet-HTTPS-Server via HTTP. This worked before but is now blocked due to the ACL.

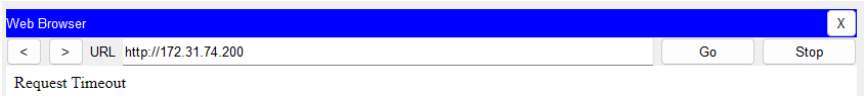


TestC & TestD: PC1 & PC2 can access the Internet-HTTPS-Server via HTTP and HTTPs. This worked before but is now blocked due to the ACL.



TestE: All PC connections to the DMZ-HTTP server through HTTP were functional before, but are now denied due to the ACL.





Test Conclusion: The ACL is functioning as specified. All other connectivity than what is permitted fails.

Conclusion: Everything went smoothly in this lab except for a mistake I made while testing the ACL. I did not clear the list before re-configuring it, leaving the deny ip any any above my new entries. After that was resolved, my ACL provided the desired functionality.