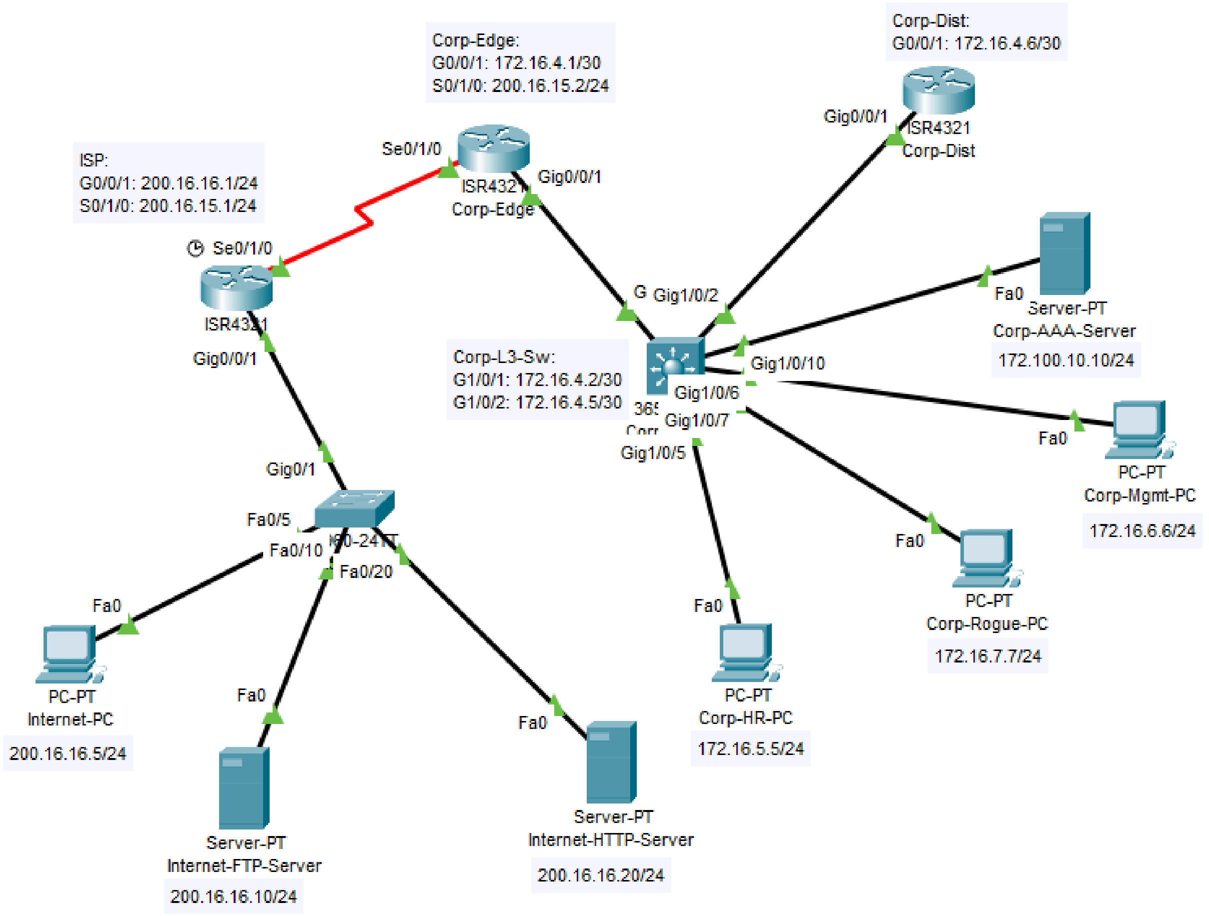
Eric Guzman 4/1/2025

Professor Cannistra Internet Security

Lab 4

Description: In this lab we secure our network with ACLs and Zone Based Policy Firewalls to control and inspect traffic.

Topology:



Syntax:

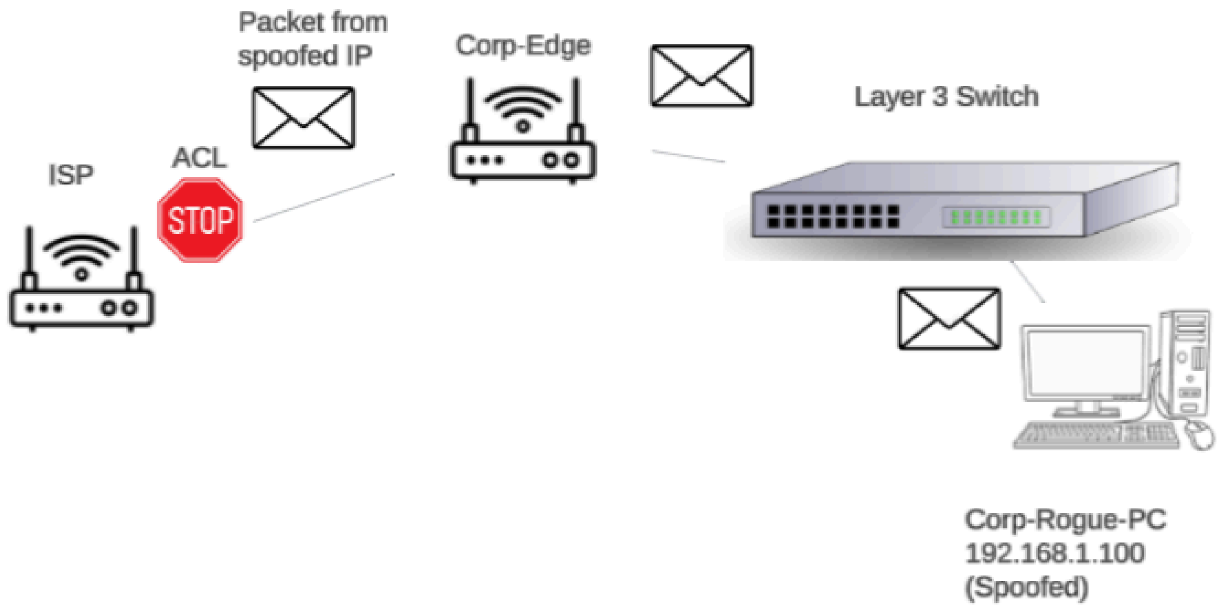
Command	Description	Mode of IOS
zone security corp zone security internet	Creates our ZPF security zones	Global configuration mode

ip access-list extended (name)	Creates an extended ACL	ACL configuration mode
zone-pair security corp-to-internet source corp destination internet	Applies a policy between two zones	Global configuration mode

Test Case Development:

Test Case 1: IPv4 Spoofing Attack Mitigation

Diagram -



Purpose:
This test case verifies that spoofed traffic using private IP ranges or loopback addresses is blocked at the edge of the network by ACLs that are on the ISP and Corp-Edge routers.

Test Steps -

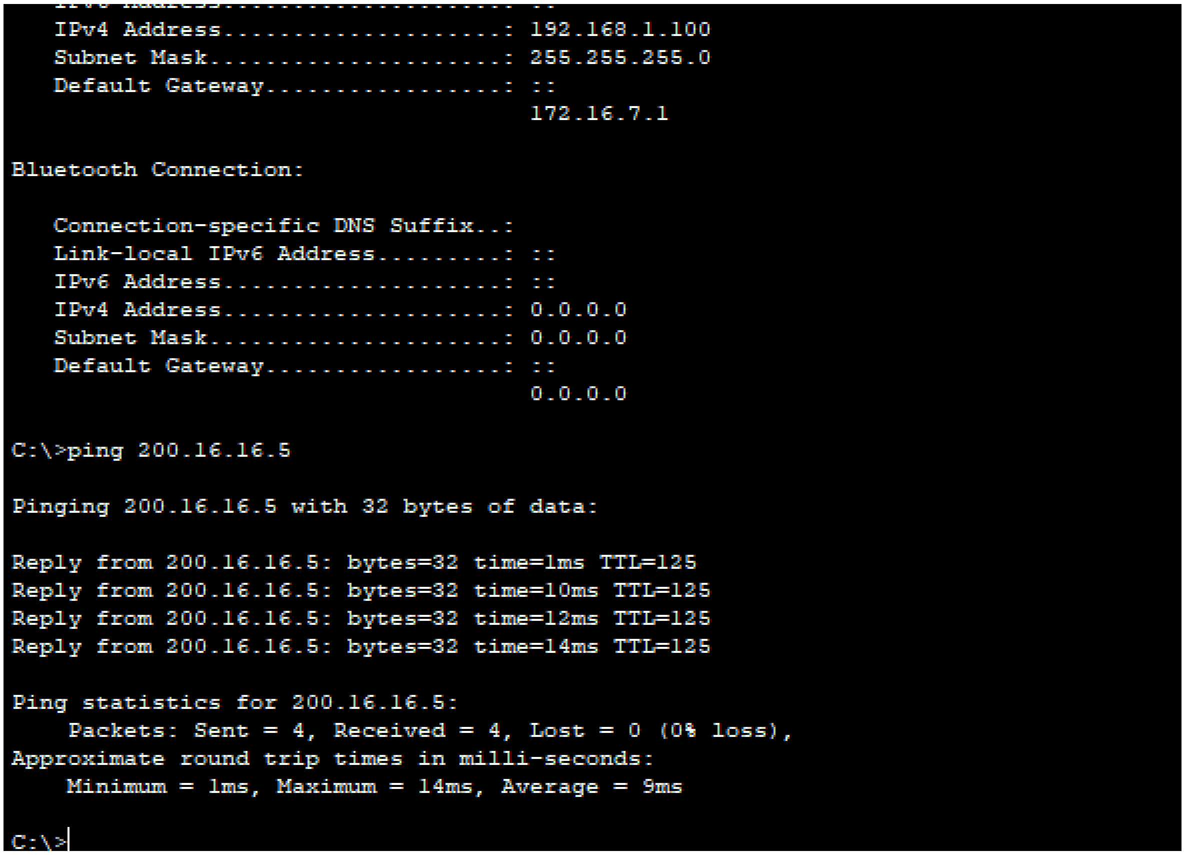
1. On Corp-Rogue-PC, spoof the source IP using a static assignment.
2. Ping a public IP, like 200.16.16.10 (Internet-FTP-Server).

3. Watch the ping failure and check ACL hit counters using show access-lists on ISP and Corp-Edge.
4. Run debug ip packet to confirm denial.
5. Restore the legitimate IP on the rogue PC after the test.

Expected Outcome:
All spoofed traffic should be denied. No ping replies should be received, and ACL counters should increment.

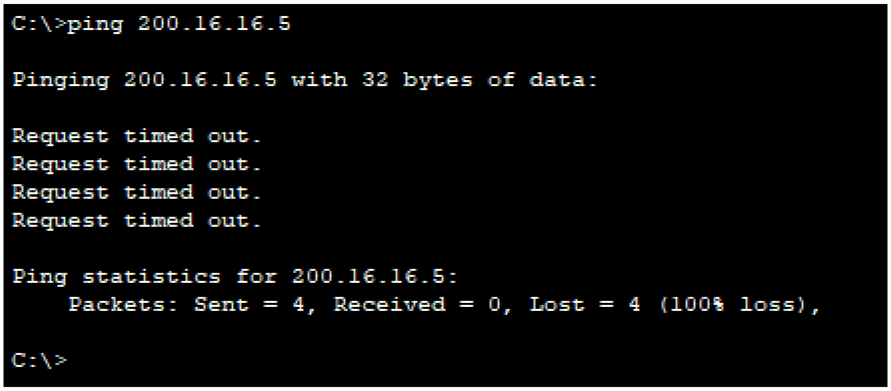
Actual Outcome:
Spoofed pings were successfully blocked, confirming ACLs are effectively mitigating private and loopback address spoofing.

Before Technology Implementation:
Before any ACLs were configured, spoofed traffic from Corp-Rogue-PC using the IP address 192.168.1.100 was sent through to 200.16.16.5.

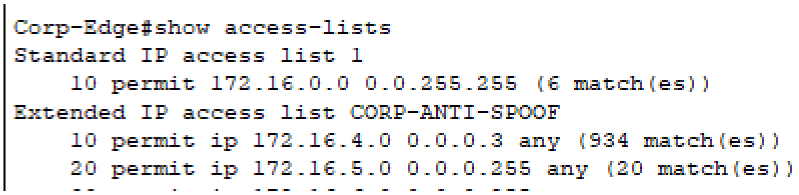


```
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.100
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     172.16.7.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 200.16.16.5

Pinging 200.16.16.5 with 32 bytes of data:

Reply from 200.16.16.5: bytes=32 time=1ms TTL=125
Reply from 200.16.16.5: bytes=32 time=10ms TTL=125
Reply from 200.16.16.5: bytes=32 time=12ms TTL=125
Reply from 200.16.16.5: bytes=32 time=14ms TTL=125

Ping statistics for 200.16.16.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 14ms, Average = 9ms

C:\>
```

After Technology Implementation:
After applying ACLs on ISP and Corp-Edge routers, the same spoofed ping attempt failed. The ACL hit counters also incremented, confirming that spoofed traffic was blocked.



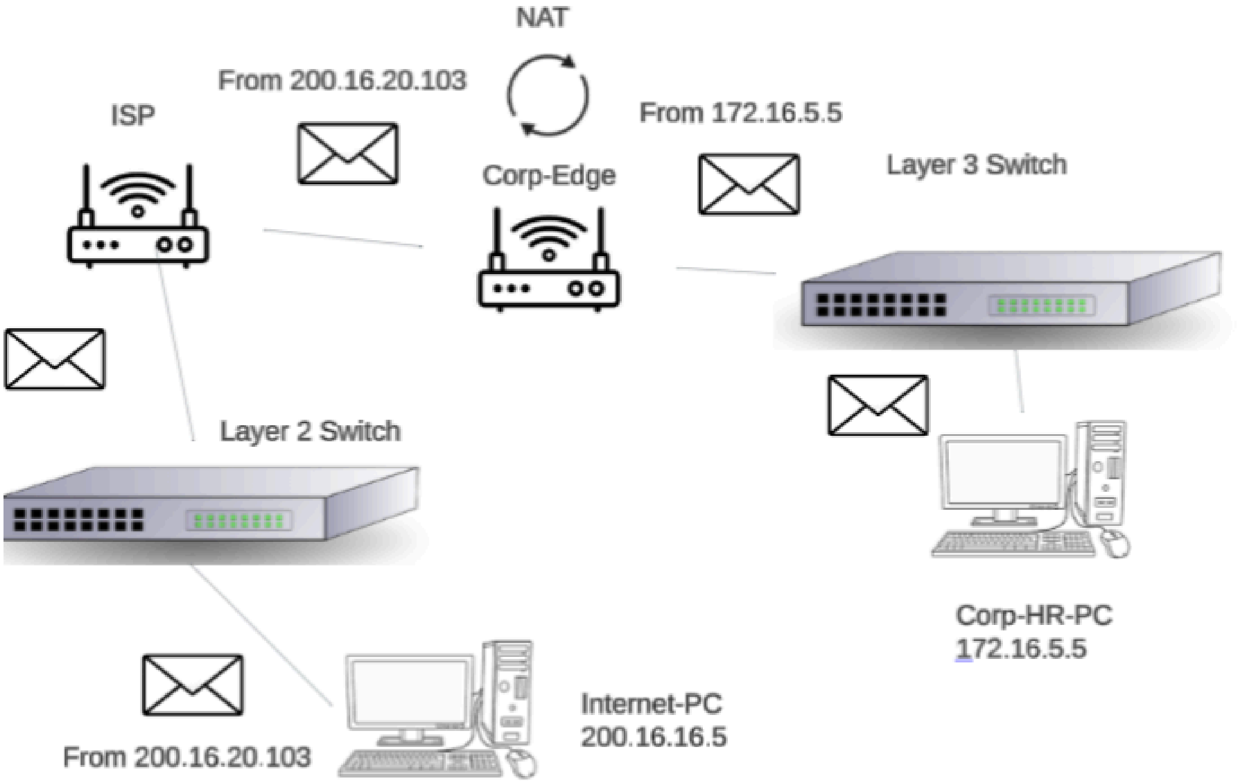
```
C:\>ping 200.16.16.5

Pinging 200.16.16.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 200.16.16.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



```
Corp-Edge#show access-lists
Standard IP access list 1
    10 permit 172.16.0.0 0.0.255.255 (6 match(es))
Extended IP access list CORP-ANTI-SPOOF
    10 permit ip 172.16.4.0 0.0.0.3 any (934 match(es))
    20 permit ip 172.16.5.0 0.0.0.255 any (20 match(es))
```

Test Case 2: NAT Using PAT Functionality

Diagram -



Purpose:
This test case confirms that internal hosts can reach the internet using NAT with (PAT) through the Corp-Edge router.

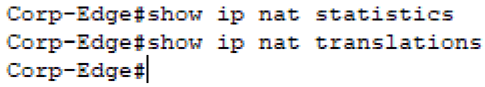
Test Steps -

1. From Corp-HR-PC, open the command prompt.
2. Ping 200.16.16.20 (Internet-HTTP-Server).
3. On Corp-Edge, use show ip nat translations to view active NAT entries.
4. Use show ip nat statistics to confirm translation hits.
5. Check for proper IP-to-port translation in the NAT table.

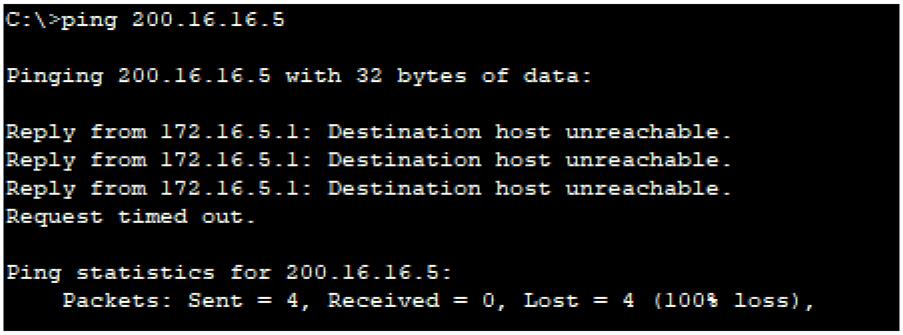
Expected Outcome:
The internal IP (172.16.5.5) should be translated to an external IP from the NAT pool (200.16.20.100–110) with a dynamic port assignment.

Actual Outcome:
Pings succeeded, and NAT translation entries showed dynamic mapping between internal and global IPs, confirming PAT functionality.

Before Technology Implementation:
Before NAT was implemented, we can see in these screenshots that the ping to 200.16.16.5 fails as NAT is not there to map the private IP.



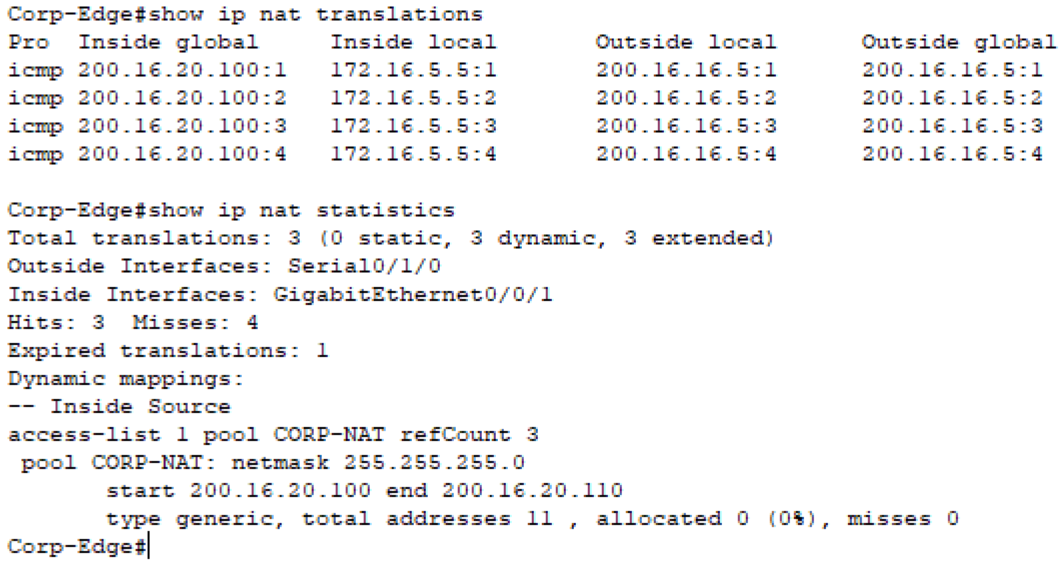
```
Corp-Edge#show ip nat statistics
Corp-Edge#show ip nat translations
Corp-Edge#
```



```
C:\>ping 200.16.16.5

Pinging 200.16.16.5 with 32 bytes of data:

Reply from 172.16.5.1: Destination host unreachable.
Reply from 172.16.5.1: Destination host unreachable.
Reply from 172.16.5.1: Destination host unreachable.
Request timed out.

Ping statistics for 200.16.16.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

After Technology Implementation:
After the implementation of NAT, this screenshot shows that NAT with PAT is working properly since the show ip nat translations command shows

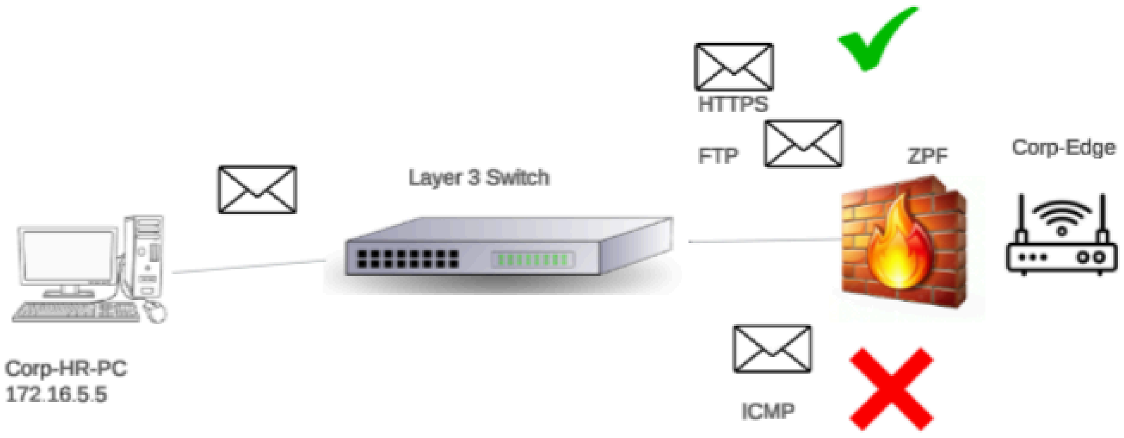
three active dynamic ICMP translations from 172.16.5.5 to public IPs in the NAT pool. The show ip nat statistics command shows that three dynamic translations are active and the NAT pool is from 200.16.20.100–110.



```
Corp-Edge#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.16.20.100:1   172.16.5.5:1       200.16.16.5:1      200.16.16.5:1
icmp 200.16.20.100:2   172.16.5.5:2       200.16.16.5:2      200.16.16.5:2
icmp 200.16.20.100:3   172.16.5.5:3       200.16.16.5:3      200.16.16.5:3
icmp 200.16.20.100:4   172.16.5.5:4       200.16.16.5:4      200.16.16.5:4

Corp-Edge#show ip nat statistics
Total translations: 3 (0 static, 3 dynamic, 3 extended)
Outside Interfaces: Serial0/1/0
Inside Interfaces: GigabitEthernet0/0/1
Hits: 3  Misses: 4
Expired translations: 1
Dynamic mappings:
-- Inside Source
access-list 1 pool CORP-NAT refCount 3
 pool CORP-NAT: netmask 255.255.255.0
       start 200.16.20.100 end 200.16.20.110
       type generic, total addresses 11 , allocated 0 (0%), misses 0
Corp-Edge#
```

Test Case 3: ZPF Functionality

Diagram -



Purpose:

The purpose of this test case is to verify that the ZPF inspects and only allows FTP and HTTPS traffic between the corp network and the internet.

Test Steps -

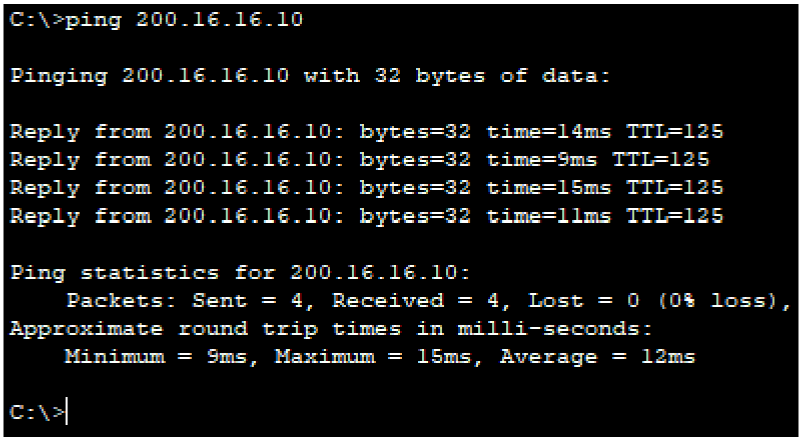
1. From Corp-HR-PC, access https://200.16.16.20 (HTTPS server).
2. From the same PC, attempt ftp 200.16.16.10 (FTP server).

3. Try accessing an HTTP site (http://200.16.16.20) to confirm it is blocked.
4. On Corp-Edge, run show policy-map type inspect zone-pair sessions to view active sessions.
5. Confirm that FTP and HTTPS traffic is inspected and allowed, while HTTP is denied.

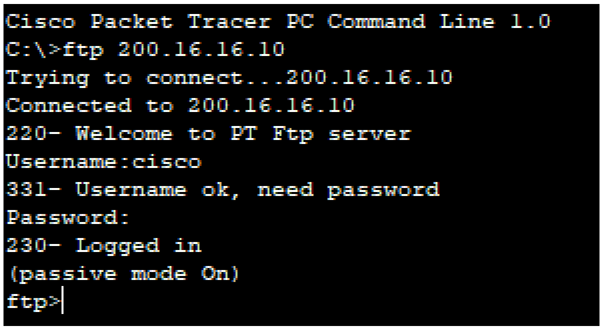
Expected Outcome:
Only HTTPS and FTP connections should succeed. HTTP should be blocked. Firewall session output should show inspection of allowed protocols.

Actual Outcome:
FTP and HTTPS sessions were successful and inspected by the firewall. HTTP traffic was denied, confirming the ZPF works.

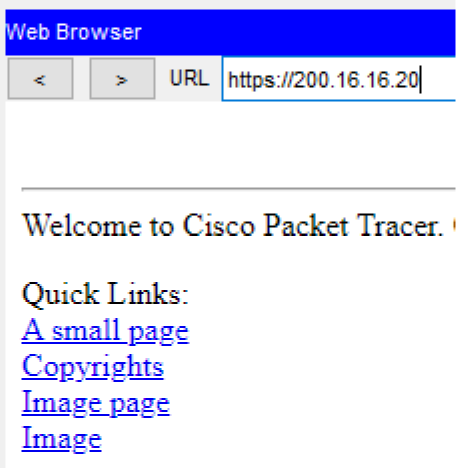
Before Technology Implementation:
Before the ZPF was configured, all outbound traffic was allowed by default. The Corp-HR-PC was able to use FTP and HTTPS, while also able to ping internet facing devices as seen in the screenshots below.



```
C:\>ping 200.16.16.10

Pinging 200.16.16.10 with 32 bytes of data:

Reply from 200.16.16.10: bytes=32 time=14ms TTL=125
Reply from 200.16.16.10: bytes=32 time=9ms TTL=125
Reply from 200.16.16.10: bytes=32 time=15ms TTL=125
Reply from 200.16.16.10: bytes=32 time=11ms TTL=125

Ping statistics for 200.16.16.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 15ms, Average = 12ms

C:\>
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 200.16.16.10
Trying to connect...200.16.16.10
Connected to 200.16.16.10
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



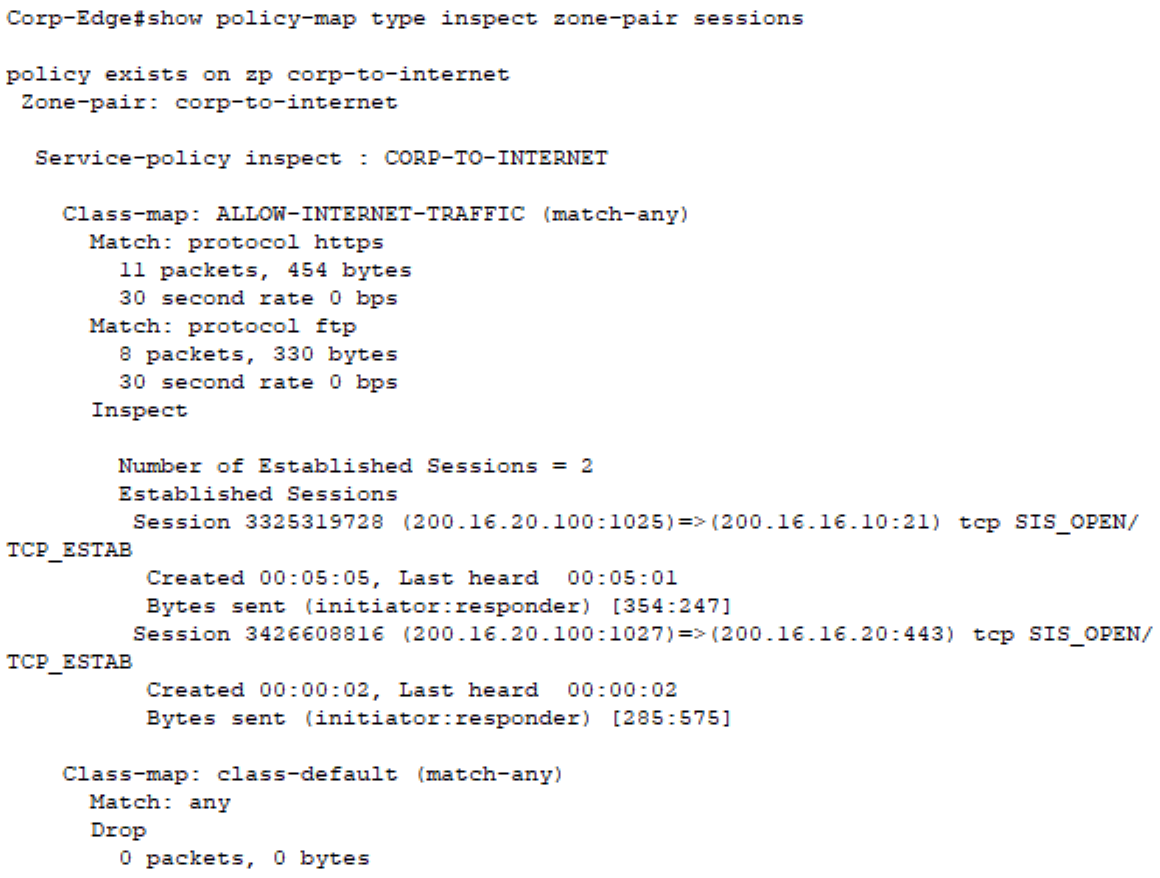
https://200.16.16.20

Welcome to Cisco Packet Tracer.

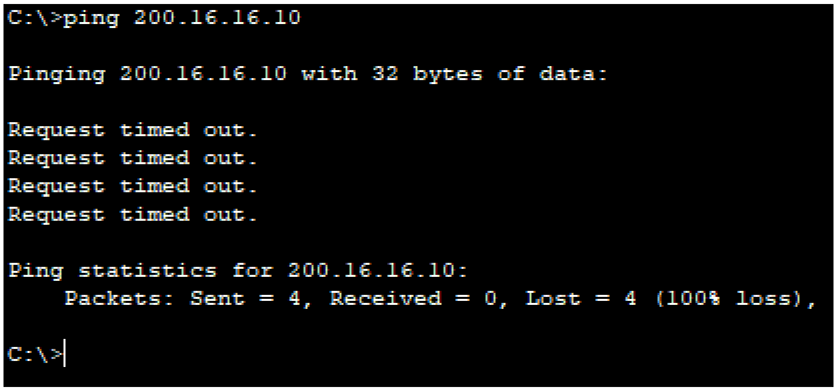
Quick Links:
A small page
Copyrights
Image page
Image

After Technology Implementation:

After applying the ZPF, FTP and HTTPS traffic from the corp network still functions properly and is inspected by the firewall. ICMP traffic was denied like we wanted. The screenshot below shows the command show policy-map type inspect zone-pair sessions which displays two active TCP sessions that are successfully being inspected and tracked. This proves that ZPF is working and monitoring all traffic.



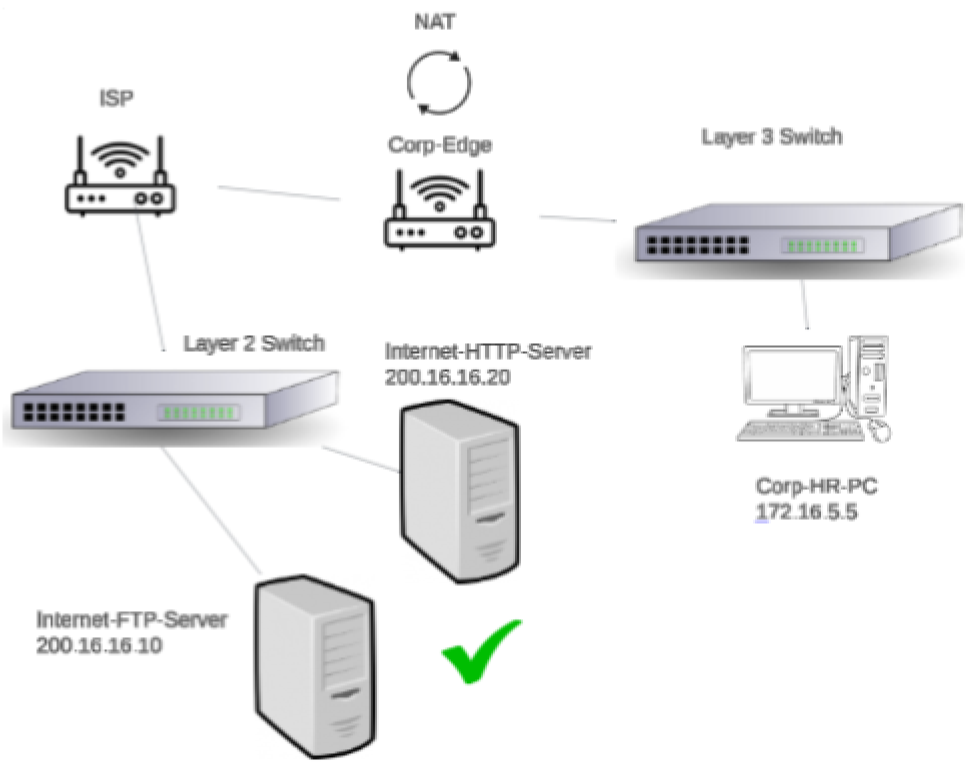
```
Corp-Edge#show policy-map type inspect zone-pair sessions

policy exists on zp corp-to-internet
 Zone-pair: corp-to-internet

  Service-policy inspect : CORP-TO-INTERNET

    Class-map: ALLOW-INTERNET-TRAFFIC (match-any)
      Match: protocol https
        11 packets, 454 bytes
        30 second rate 0 bps
      Match: protocol ftp
        8 packets, 330 bytes
        30 second rate 0 bps
      Inspect

        Number of Established Sessions = 2
        Established Sessions
         Session 3325319728 (200.16.20.100:1025)=>(200.16.16.10:21) tcp SIS_OPEN/
TCP_ESTAB
          Created 00:05:05, Last heard  00:05:01
          Bytes sent (initiator:responder) [354:247]
         Session 3426608816 (200.16.20.100:1027)=>(200.16.16.20:443) tcp SIS_OPEN/
TCP_ESTAB
          Created 00:00:02, Last heard  00:00:02
          Bytes sent (initiator:responder) [285:575]

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```



```
C:\>ping 200.16.16.10

Pinging 200.16.16.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 200.16.16.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Test Case 4: FTP and HTTPS Server Verification

Diagram -



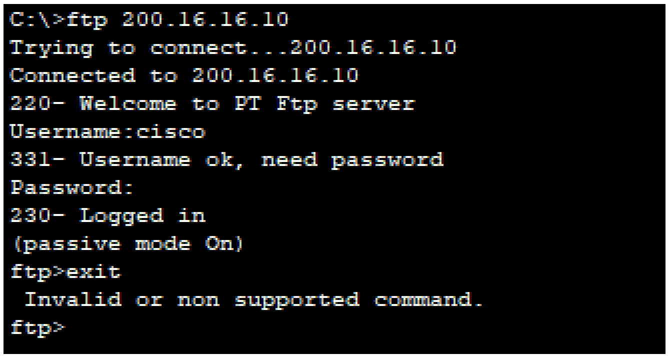
Purpose:
The purpose of this test case is to confirm that internal users can access FTP and HTTPS servers that are past the ISP.

Test Steps -

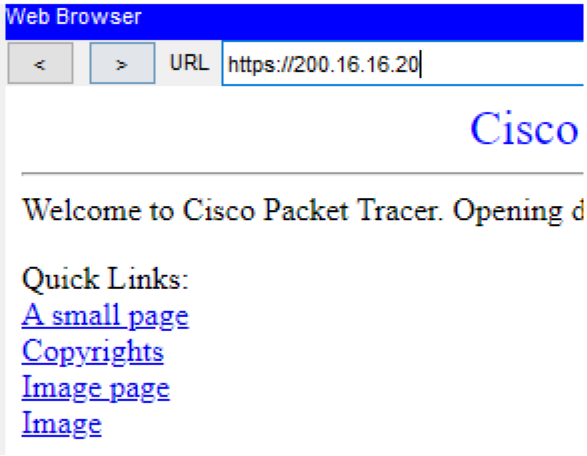
1. On Corp-HR-PC, start a FTP session to 200.16.16.10.
2. Use a browser to open https://200.16.16.20.
3. Observe whether the connections succeed.
4. Monitor logs or firewall session tables on Corp-Edge.
5. Take screenshots of the FTP connection and web page load.

Expected Outcome:
Both services should be available for any device at the point this is being tested.

Actual Outcome:
Both services were accessed successfully confirming that our previous technologies were set up properly. The screenshots below show that this is true for both HTTPS and FTP.



```
C:\>ftp 200.16.16.10
Trying to connect...200.16.16.10
Connected to 200.16.16.10
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>exit
 Invalid or non supported command.
ftp>
```



https://200.16.16.20

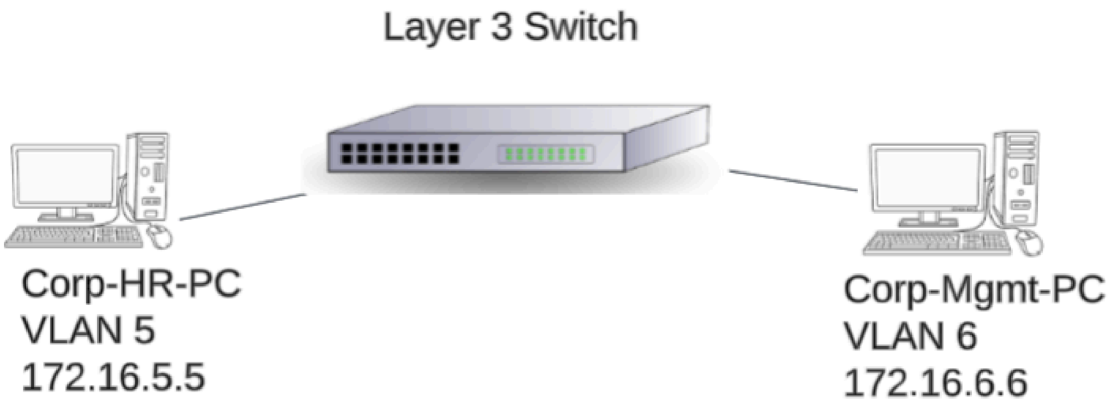
Cisco

Welcome to Cisco Packet Tracer. Opening d

Quick Links:
A small page
Copyrights
Image page
Image

Test Case 5: Internal Communication Between VLANs

Diagram -



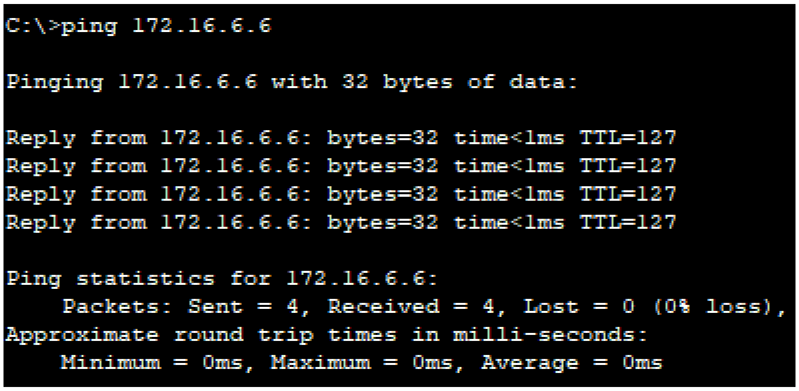
Purpose:

This test case verifies that hosts that are on separate VLANs within the corporate network can successfully communicate, making sure that inter VLAN routing works correctly on the layer 3 switch.

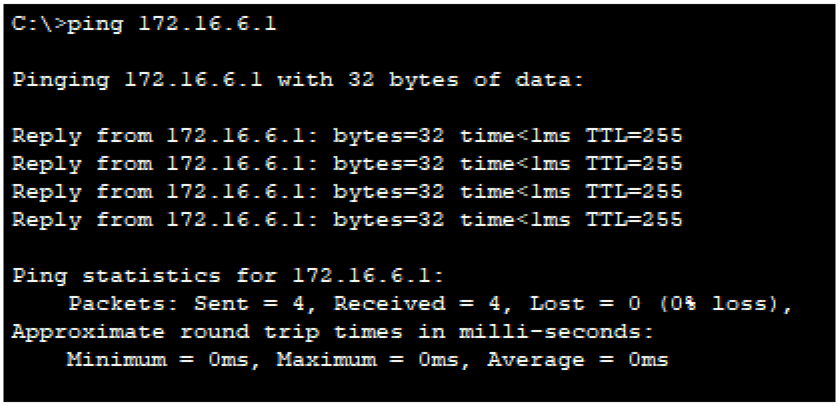
Test Steps -
1. Open the command prompt on the Corp-HR-PC.
2. Enter the command ping 172.16.6.6
3. Open the command prompt on the Corp-Mgmt-PC.
4. Enter the command ping 172.16.5.5
5. Monitor the results from both PCs and troubleshoot results on the switch if needed.

Expected Outcome:
Both pings should reply successfully, have minimal packet loss and prove that inter-VLAN routing is successful.

Actual Outcome:
All ping tests were successful and confirmed that Corp-HR-PC and Corp-Mgmt-PC can communicate across VLANs, as can be seen in the screenshots below:



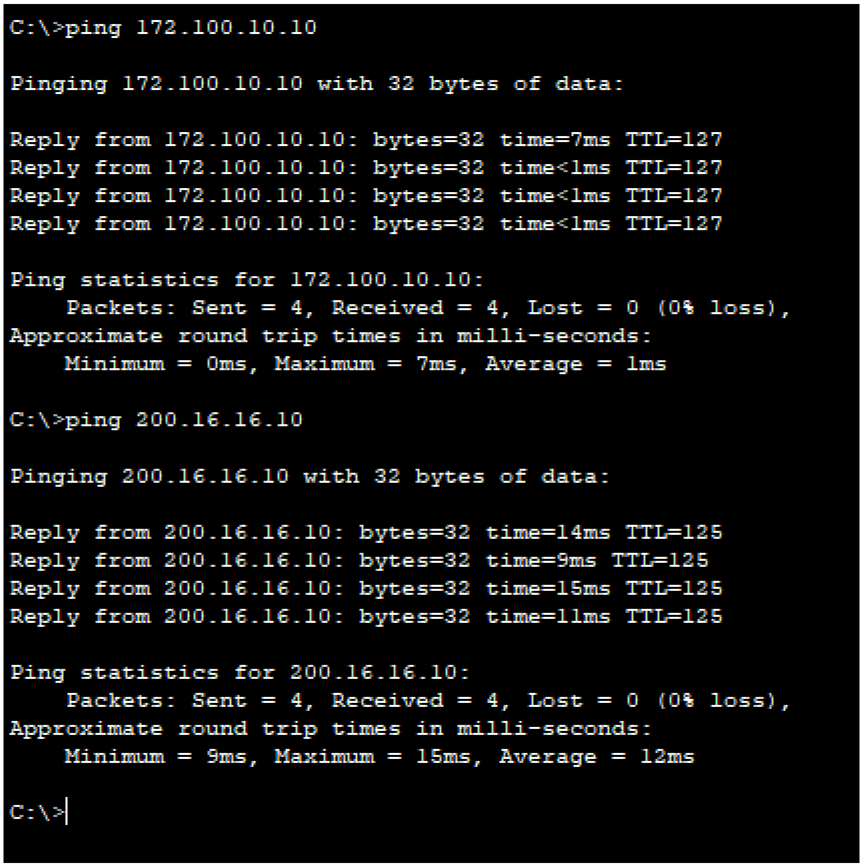
```
C:\>ping 172.16.6.6

Pinging 172.16.6.6 with 32 bytes of data:

Reply from 172.16.6.6: bytes=32 time<1ms TTL=127
Reply from 172.16.6.6: bytes=32 time<1ms TTL=127
Reply from 172.16.6.6: bytes=32 time<1ms TTL=127
Reply from 172.16.6.6: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.6.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



```
C:\>ping 172.16.6.1

Pinging 172.16.6.1 with 32 bytes of data:

Reply from 172.16.6.1: bytes=32 time<1ms TTL=255
Reply from 172.16.6.1: bytes=32 time<1ms TTL=255
Reply from 172.16.6.1: bytes=32 time<1ms TTL=255
Reply from 172.16.6.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.6.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Verification:

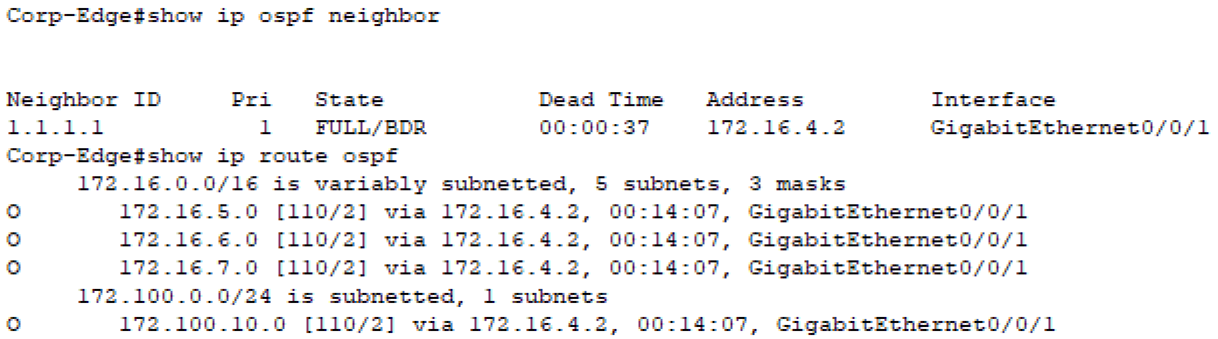
1. Basic Connectivity (Before Security)



```
C:\>ping 172.100.10.10

Pinging 172.100.10.10 with 32 bytes of data:

Reply from 172.100.10.10: bytes=32 time=7ms TTL=127
Reply from 172.100.10.10: bytes=32 time<1ms TTL=127
Reply from 172.100.10.10: bytes=32 time<1ms TTL=127
Reply from 172.100.10.10: bytes=32 time<1ms TTL=127

Ping statistics for 172.100.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 1ms

C:\>ping 200.16.16.10

Pinging 200.16.16.10 with 32 bytes of data:

Reply from 200.16.16.10: bytes=32 time=14ms TTL=125
Reply from 200.16.16.10: bytes=32 time=9ms TTL=125
Reply from 200.16.16.10: bytes=32 time=15ms TTL=125
Reply from 200.16.16.10: bytes=32 time=11ms TTL=125

Ping statistics for 200.16.16.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 15ms, Average = 12ms

C:\>
```

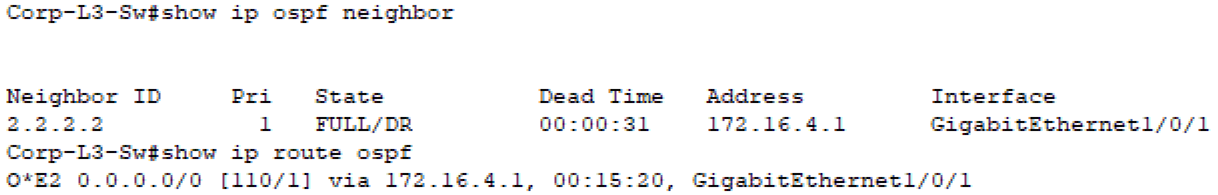
This screenshot shows that Corp-HR-PC can ping across the network before any security has been added showing that the topology has full connectivity.

2. OSPF Routing



```
Corp-Edge#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:37    172.16.4.2      GigabitEthernet0/0/1
Corp-Edge#show ip route ospf
     172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O       172.16.5.0 [110/2] via 172.16.4.2, 00:14:07, GigabitEthernet0/0/1
O       172.16.6.0 [110/2] via 172.16.4.2, 00:14:07, GigabitEthernet0/0/1
O       172.16.7.0 [110/2] via 172.16.4.2, 00:14:07, GigabitEthernet0/0/1
     172.100.0.0/24 is subnetted, 1 subnets
O       172.100.10.0 [110/2] via 172.16.4.2, 00:14:07, GigabitEthernet0/0/1
```

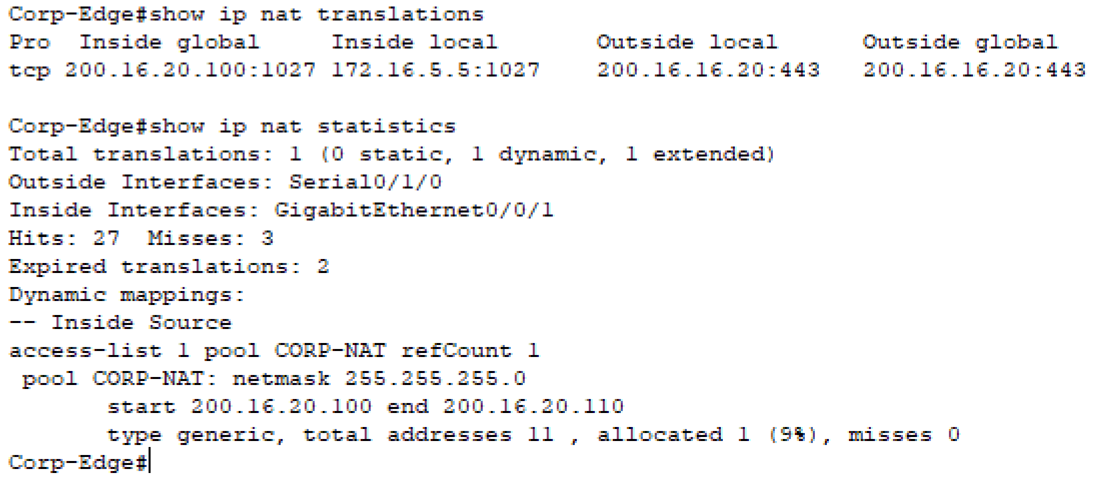
This screenshot shows that the Corp-Edge router is OSPF neighbors with the layer 3 switch by using the command show ip osfp neighbor. I also used the show ip route ospf command to show that routes for the 172.16.5.0, 172.16.6.0, 172.16.7.0 and 172.100.10.0 networks.



```
Corp-L3-Sw#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:31    172.16.4.1      GigabitEthernet1/0/1
Corp-L3-Sw#show ip route ospf
O*E2 0.0.0.0/0 [110/1] via 172.16.4.1, 00:15:20, GigabitEthernet1/0/1
```

This screenshot shows the layer three switch and the ip ospf neighbor command proving that there is a successful OSPF neighbor relationship with the Corp-Edge router. The show ip route ospf command shows that the switch has learned a default route to the Corp-Edge router.

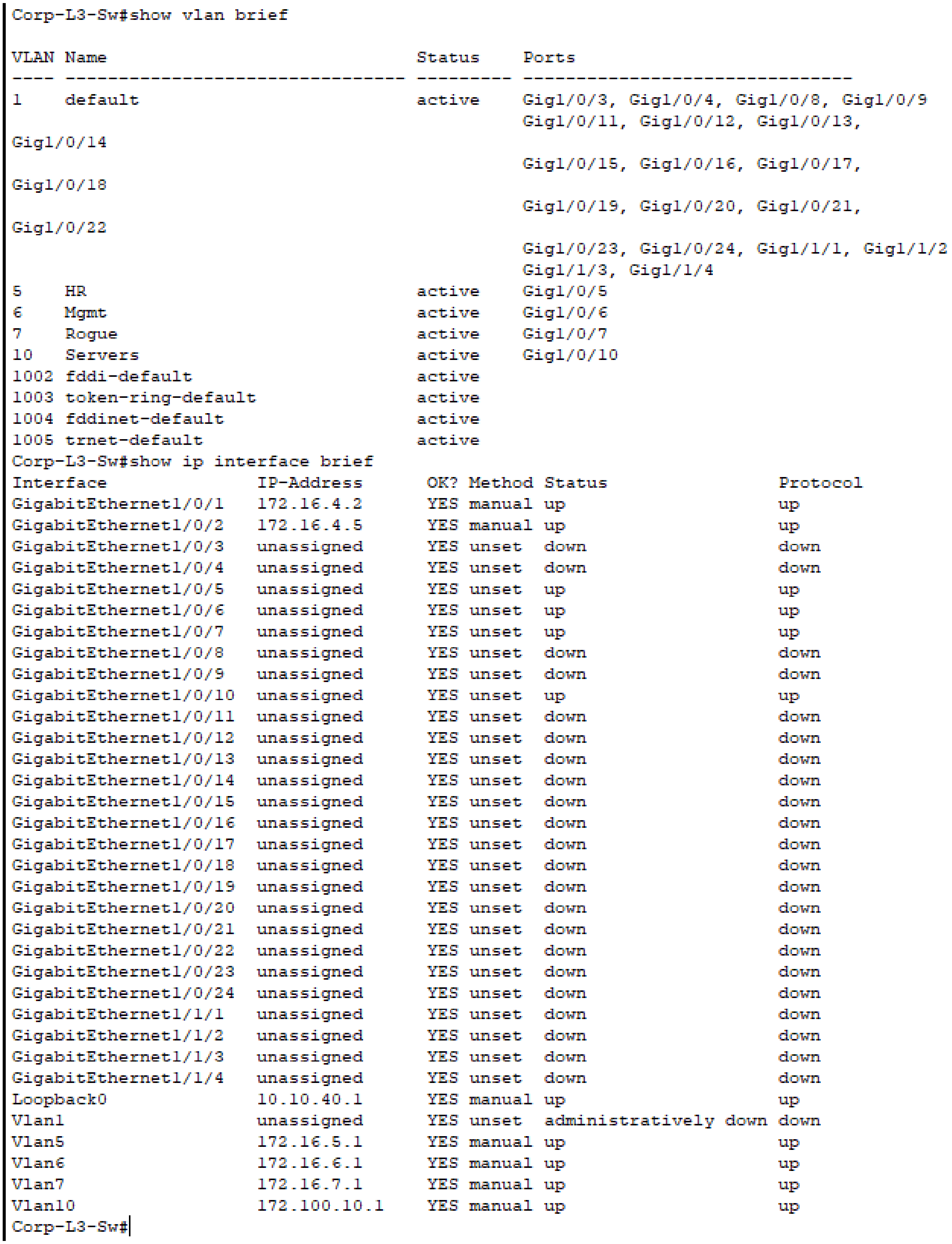
3. NAT with PAT



```
Corp-Edge#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 200.16.20.100:1027 172.16.5.5:1027    200.16.16.20:443   200.16.16.20:443

Corp-Edge#show ip nat statistics
Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/1/0
Inside Interfaces: GigabitEthernet0/0/1
Hits: 27  Misses: 3
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool CORP-NAT refCount 1
 pool CORP-NAT: netmask 255.255.255.0
       start 200.16.20.100 end 200.16.20.110
       type generic, total addresses 11 , allocated 1 (9%), misses 0
Corp-Edge#
```

This screenshot shows that NAT/PAT is working properly on the Corp-Edge router. The show ip nat translations command show that 172.16.5.5 was translated to 200.16.20.100 for HTTPS access. The show ip nat statistics command shows that there is one dynamic translation active. The NAT pool of Corp-NAT allocates addresses from the 200.16.20.100 to 200.16.20.110 range.

4. VLAN Configuration



```
Corp-L3-Sw#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/3, Gig1/0/4, Gig1/0/8, Gig1/0/9
                                                Gig1/0/11, Gig1/0/12, Gig1/0/13,
Gig1/0/14
                                                Gig1/0/15, Gig1/0/16, Gig1/0/17,
Gig1/0/18
                                                Gig1/0/19, Gig1/0/20, Gig1/0/21,
Gig1/0/22
                                                Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2
                                                Gig1/1/3, Gig1/1/4
5    HR                               active    Gig1/0/5
6    Mgmt                             active    Gig1/0/6
7    Rogue                            active    Gig1/0/7
10   Servers                          active    Gig1/0/10
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Corp-L3-Sw#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1/0/1   172.16.4.2      YES manual up                    up
GigabitEthernet1/0/2   172.16.4.5      YES manual up                    up
GigabitEthernet1/0/3   unassigned      YES unset  down                  down
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
GigabitEthernet1/0/6   unassigned      YES unset  up                    up
GigabitEthernet1/0/7   unassigned      YES unset  up                    up
GigabitEthernet1/0/8   unassigned      YES unset  down                  down
GigabitEthernet1/0/9   unassigned      YES unset  down                  down
GigabitEthernet1/0/10  unassigned      YES unset  up                    up
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
GigabitEthernet1/0/13  unassigned      YES unset  down                  down
GigabitEthernet1/0/14  unassigned      YES unset  down                  down
GigabitEthernet1/0/15  unassigned      YES unset  down                  down
GigabitEthernet1/0/16  unassigned      YES unset  down                  down
GigabitEthernet1/0/17  unassigned      YES unset  down                  down
GigabitEthernet1/0/18  unassigned      YES unset  down                  down
GigabitEthernet1/0/19  unassigned      YES unset  down                  down
GigabitEthernet1/0/20  unassigned      YES unset  down                  down
GigabitEthernet1/0/21  unassigned      YES unset  down                  down
GigabitEthernet1/0/22  unassigned      YES unset  down                  down
GigabitEthernet1/0/23  unassigned      YES unset  down                  down
GigabitEthernet1/0/24  unassigned      YES unset  down                  down
GigabitEthernet1/1/1   unassigned      YES unset  down                  down
GigabitEthernet1/1/2   unassigned      YES unset  down                  down
GigabitEthernet1/1/3   unassigned      YES unset  down                  down
GigabitEthernet1/1/4   unassigned      YES unset  down                  down
Loopback0              10.10.40.1      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Vlan5                  172.16.5.1      YES manual up                    up
Vlan6                  172.16.6.1      YES manual up                    up
Vlan7                  172.16.7.1      YES manual up                    up
Vlan10                 172.100.10.1    YES manual up                    up
Corp-L3-Sw#
```

This screenshot shows that VLANs 5 (HR), 6 (Mgmt), 7 (Rogue), and 10 (Servers) are active on the Layer 3 switch. Each VLAN has a corresponding SVI with an assigned IP address, and all are up. This confirms that VLAN segmentation and inter-VLAN routing are working correctly.

5. **Access Control Lists**
   Verified in Test Case 1. ACLs were configured and applied on ISP and Corp-Edge routers to block spoofed IP traffic. Successful denial of RFC1918 and loopback addresses confirms the ACL work.
6. **Zone-Based Policy Firewall**
   Verified in Test Cases 3 and 4. ZPF was configured to inspect FTP and HTTPS traffic. Firewall session inspection and successful access to approved services confirmed proper configuration.

Conclusion:

Overall, I enjoyed this lab even if it felt like a good amount of effort. I liked developing the test cases for each significant technology as it really proves and shows that you did everything properly and know how to explain exactly how to recreate it. Everything worked pretty well for me as we did most of it in class, so it did not feel completely new.