Network Configuration Project Report

A. Analyze the Network Design and Choose the Right Devices

Objective:
To analyze the network design and choose the appropriate devices for implementation in Cisco Packet Tracer.

Network Design Overview:

- **Inside Zone (192.168.20.0/24):** Contains PC0 and PC1, which are internal workstations.
- **DMZ Zone (172.16.20.0/28):** Hosts Web Server 1 and Web Server 2, which are accessible from both inside and outside the network.
- **Outside Zone (110.20.20.0/29):** Contains PC3, representing an external workstation.

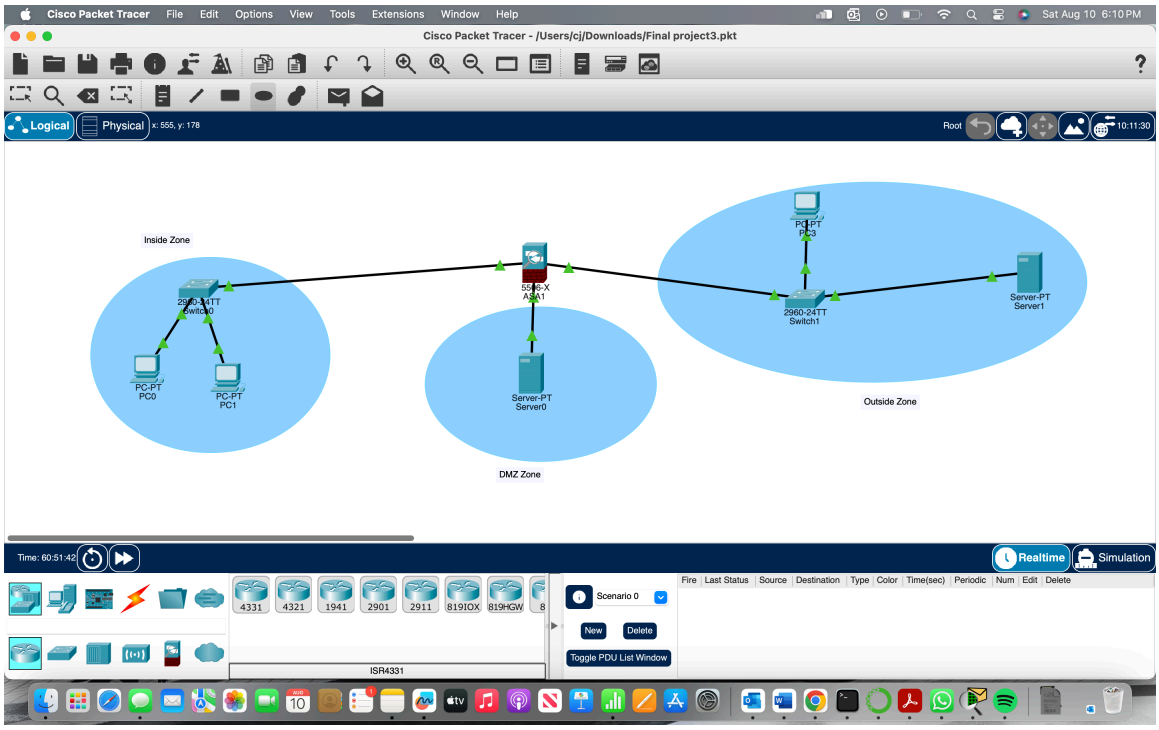
Device Selection Explanation:
1. Cisco ASA 5506 Firewall: A security appliance that controls traffic between different zones, ensuring that only permitted traffic flows between them.

2. PC0, PC1, PC3: These represent user endpoints in different zones, allowing testing of network accessibility and security rules.

3. Web Server 0 & Web Server 1: Servers hosted in the DMZ zone, providing web services accessible from both internal and external networks.

4.Switch0 and Switch1: Connects firewall PCs and Web servers.

Physical Topology:
The Cisco Packet Tracer topology was modified to accurately show the connections between devices and the correct firewall interfaces with copper cross cables. Copper cables were selected due to their compatibility with Ethernet connections, which are frequently utilized in small to medium-sized networks.



B. Update and Apply the Right IP Settings (Static) on All Devices

Objective:

To configure static IP addresses for all devices based on the network design.

IP Configuration Table:

Device	Interface	IP Address	Subnet Mask	Zone
PC0	FastEthernet0/2	192.168.20.2	255.255.255.0	Inside
PC1	FastEthernet0/3	192.168.20.3	255.255.255.0	Inside
PC3	FastEthernet0/2	110.20.20.2	255.255.255.248	Outside
Web Server 0	FastEthernet0/1	172.16.20.2	255.255.255.240	DMZ
Web Server 1	FastEthernet0/1	110.20.20.3	255.255.255.240	Outside
ASA Firewall	GigabitEthernet1/1	192.168.20.1	255.255.255.0	Inside
ASA Firewall	GigabitEthernet1/2	172.16.20.1	255.255.255.240	DMZ
ASA Firewall	GigabitEthernet1/3	110.20.20.1	255.255.255.248	Outside

Access the Firewall:

```
enable
configure terminal
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.20.1 255.255.255.0
no shutdown
```

This setup establishes three distinct network interfaces on a Cisco ASA firewall: the internal, DMZ, and external interfaces. The GigabitEthernet0/1 interface is labelled as "inside" and given a security level of 100, usually designated for trusted networks like the internal LAN.

It is set up with the IP address 192.168.20.1 and subnet mask of 255.255.255.0, serving as the default gateway for devices within the internal network. Afterwards, the interface is turned on using the no shutdown command.

```
interface GigabitEthernet0/2
nameif dmz
security-level 50
ip address 172.16.20.1 255.255.255.240
no shutdown
```

The interface GigabitEthernet0/2, known as "dmz," is assigned a security level of 50. The DMZ (Demilitarized Zone) is commonly utilized for hosting services such as web servers that require accessibility from both the internal network and external sources. This interface has been assigned the IP address 172.16.20.1 with a subnet mask of 255.255.255.240, serving as the gateway for devices in the DMZ.

```
interface GigabitEthernet0/3
nameif outside
security-level 0
ip address 110.20.20.1 255.255.255.248
no shutdown
```

Finally, the external interface (GigabitEthernet0/3) is labeled as "outside" and assigned a security level of 0, showing that it is the least reliable network, often linked to the web. Configured with the IP address 110.x.x.1 and subnet mask 255.255.255.248, it represents the external-facing IP of the firewall. This interface is activated by using the no shutdown command.

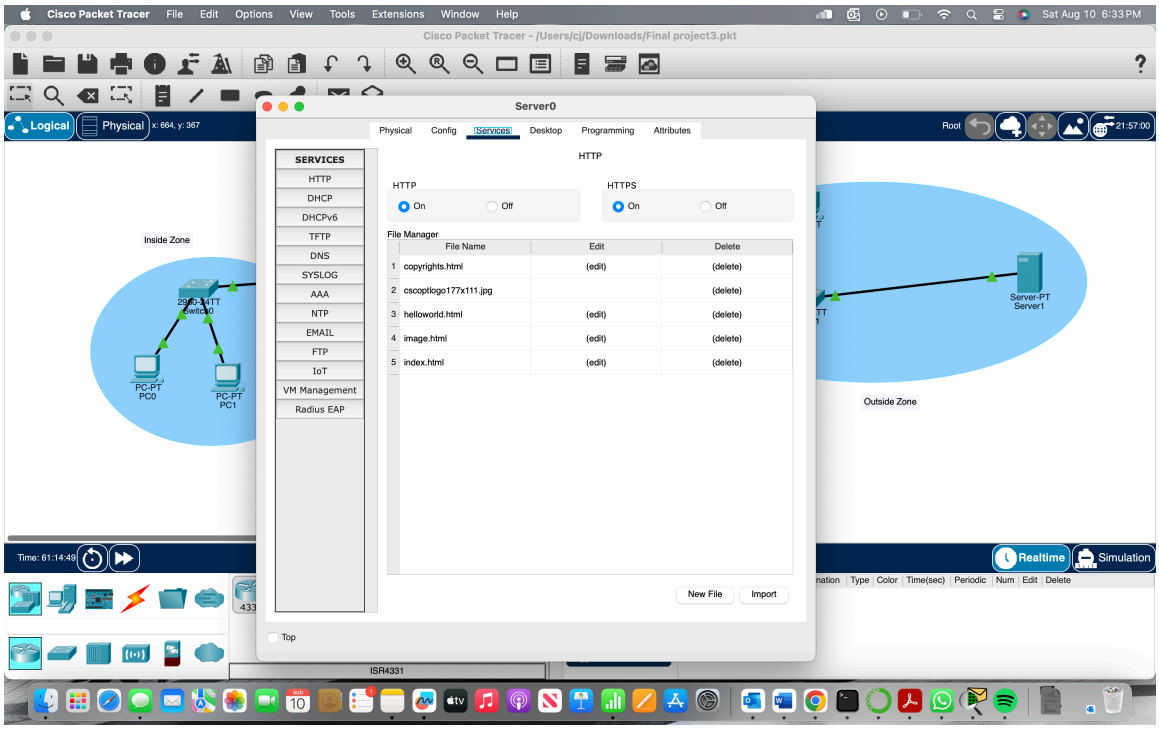
Static IP addresses were configured on all devices to ensure proper communication between them. Each zone is assigned its own subnet, and the ASA Firewall interfaces are set as the gateways for each respective subnet.

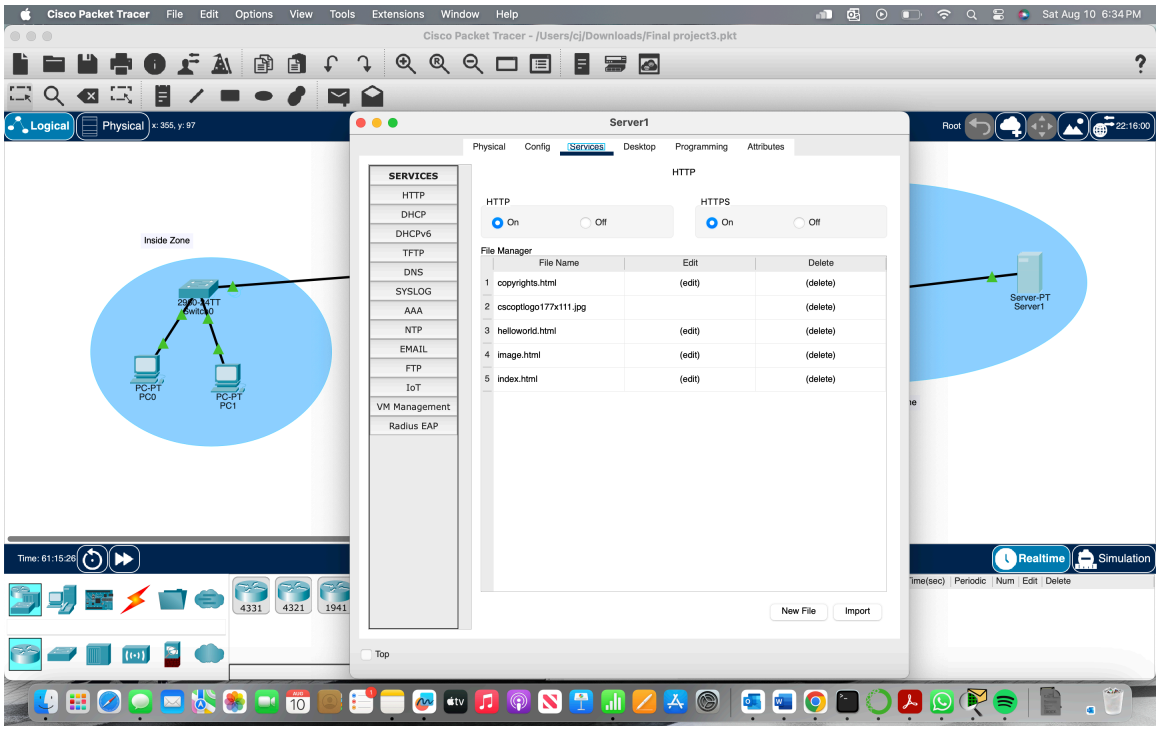
C. Initialize the Firewall and Web Servers (with HTTPs)

Objective:
To configure the ASA Firewall and Web Servers to support secure HTTP (HTTPS) traffic.

Firewall Configuration for HTTPS:
The ASA Firewall is configured to allow HTTPS traffic to the Web Servers in the DMZ zone. This is done by creating access control lists (ACLs) that permit HTTPS (port 443) traffic to the servers. Additionally, the firewall itself is enabled for HTTPS management access.

Web Server Configuration for HTTPS:
The web servers in the DMZ are configured with a secure HTTP server. This involves enabling the HTTPS service on each server and ensuring that the necessary certificates are installed if applicable.





D. Make Web Server 1/2 Available for PC0/1 (Browse by IP Addresses)

Objective:

To allow internal PCs (PC0 and PC1) to access the web servers in the DMZ via their IP addresses.

```
access-list inside_access_in extended permit tcp any host 172.16.20.2 eq www
access-list inside_access_in extended permit tcp any host 172.16.20.2 eq 443
access-list inside_access_in extended permit tcp any host 110.20.20.3 eq www
access-list inside_access_in extended permit tcp any host 110.20.20.3 eq 443
```

These instructions generate ACL entries that permit HTTP (port 80) and HTTPS (port 443) traffic from any IP (such as PC0 and PC1) to access Web Server 1 (172.16.20.2) and Web Server 2 (172.16.20.3). The port number is specified by the keyword eq.

The ACL named inside_access_in is enforced on the inside interface, governing the traffic that originates from the inside network.

```
access-group inside_access_in in interface inside
```

This command applies the inside_access_in ACL to the inside interface, filtering incoming traffic.

Allowing ICMP Traffic (Ping) to Web Servers

```
access-list inside_access_in extended permit icmp any host 172.16.20.2
access-list inside_access_in extended permit icmp any host 110.20.20.3
```

To ensure that ICMP (ping) traffic is allowed from PC0 and PC1 to Web Servers, additional ACL entries are required.

These commands allow ICMP traffic from any IP (such as PC0 and PC1) to Web Server 1 (172.16.20.2) and Web Server 2 (172.16.20.3). This ensures that ping requests to the servers do not time out and are properly responded to

```
access-list outside_access_in extended permit icmp any host 110.20.20.2
```

This command allows ICMP traffic from any source to Web Server 1's public IP address (110.20.20.2), ensuring that pings are allowed from the outside network.

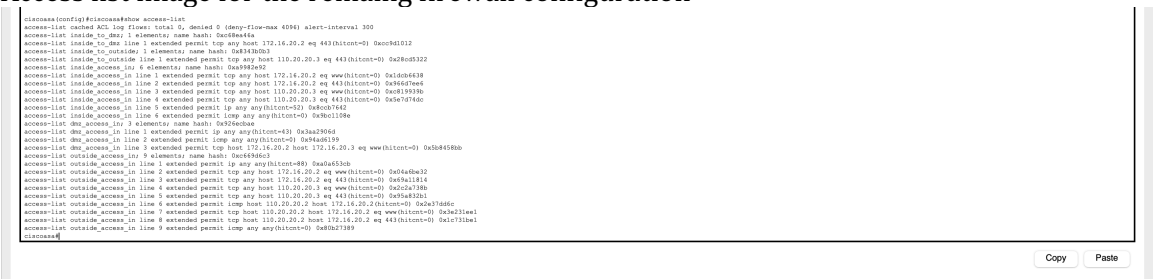
```
access-group outside_access_in in interface outside
```

This command applies the outside_access_in ACL to the outside interface, filtering incoming traffic from the outside network.

```
configure terminal
policy-map global_policy
class inspection_default
inspect icmp
exit
service-policy global_policy global
exit
write memory
```

Ensure ICMP inspection is enabled to allow ping responses

Access list image for the remaing firewall configuration



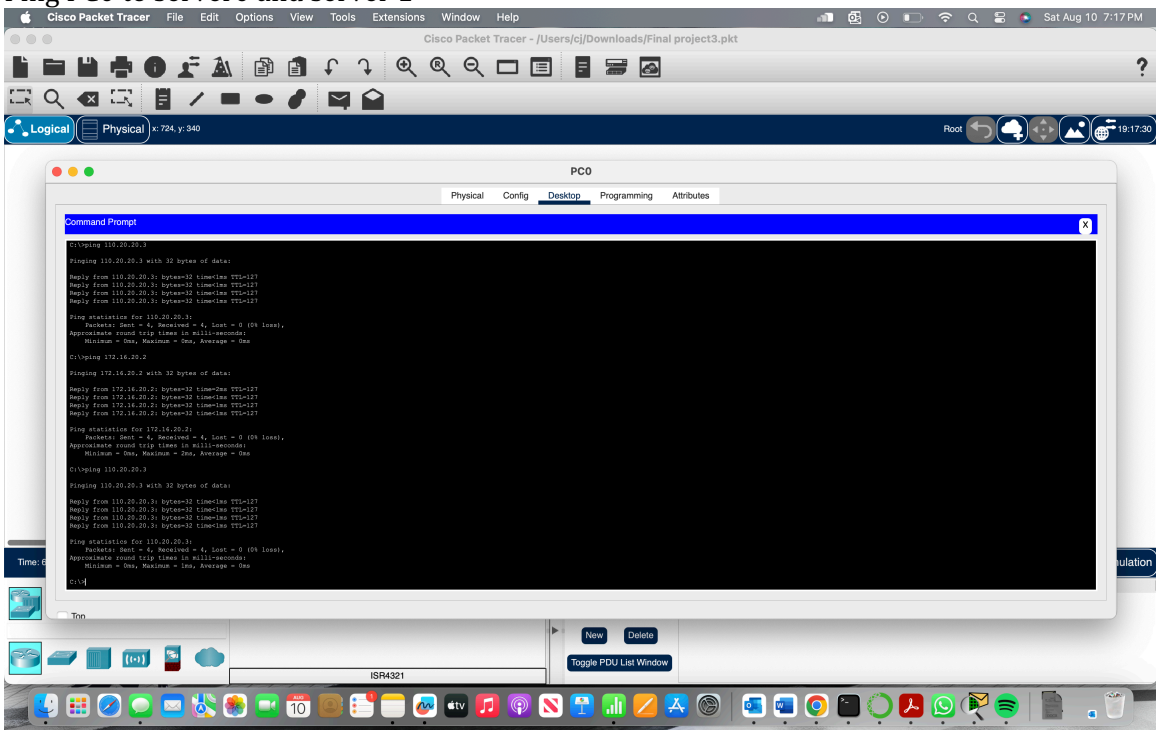
NAT Configuration

object network inside-network
subnet 192.168.20.0 255.255.255.0
nat (inside,outside) dynamic interface

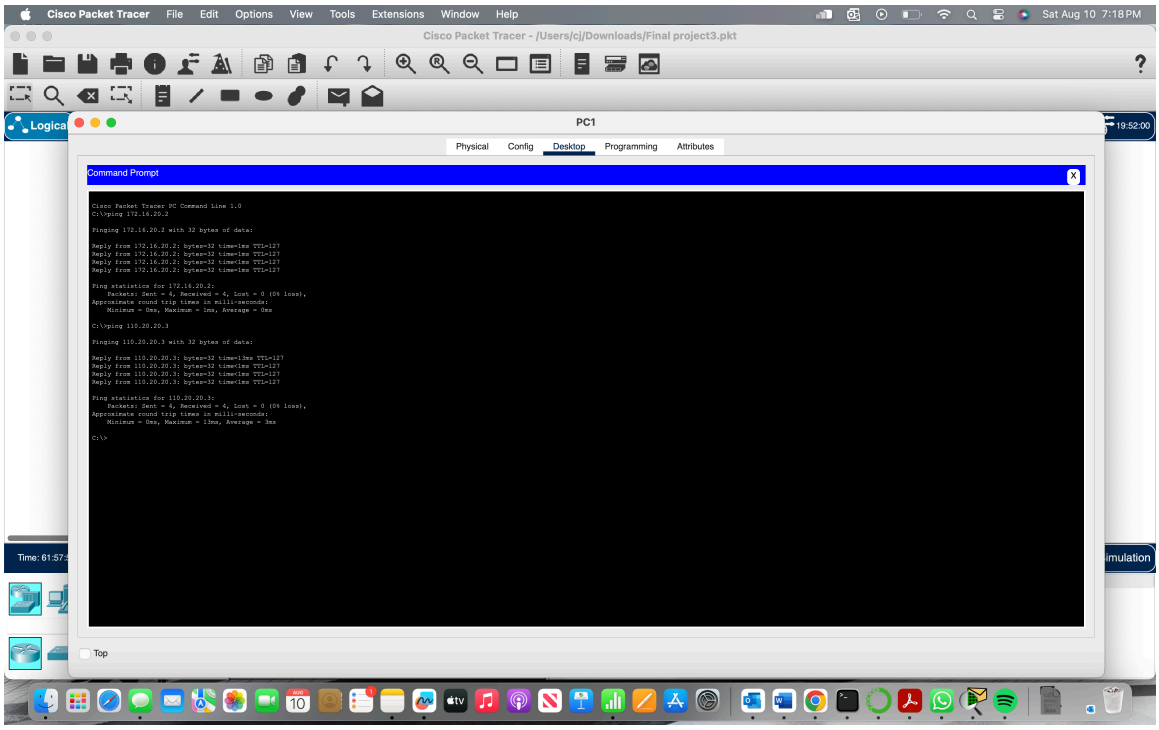
object network dmz-network
subnet 172.16.20.0 255.255.255.240
nat (dmz,outside) dynamic interface

Network Objects: Defined are two network objects (inside-network and dmz-network) that represent the internal and DMZ subnets.
NAT Configuration: The nat command sets up dynamic NAT for the internal and DMZ networks, enabling the transformation of internal IP addresses to the firewall's external IP address during external communication.

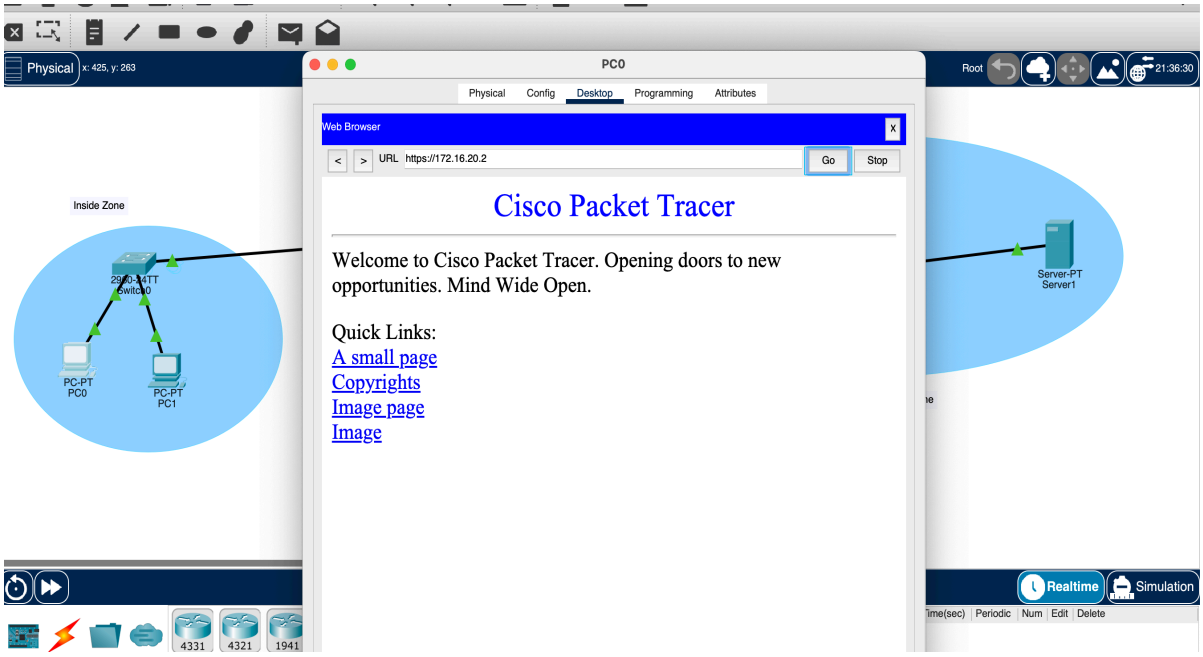
Now to check access
Ping PC0 to server0 and server 1

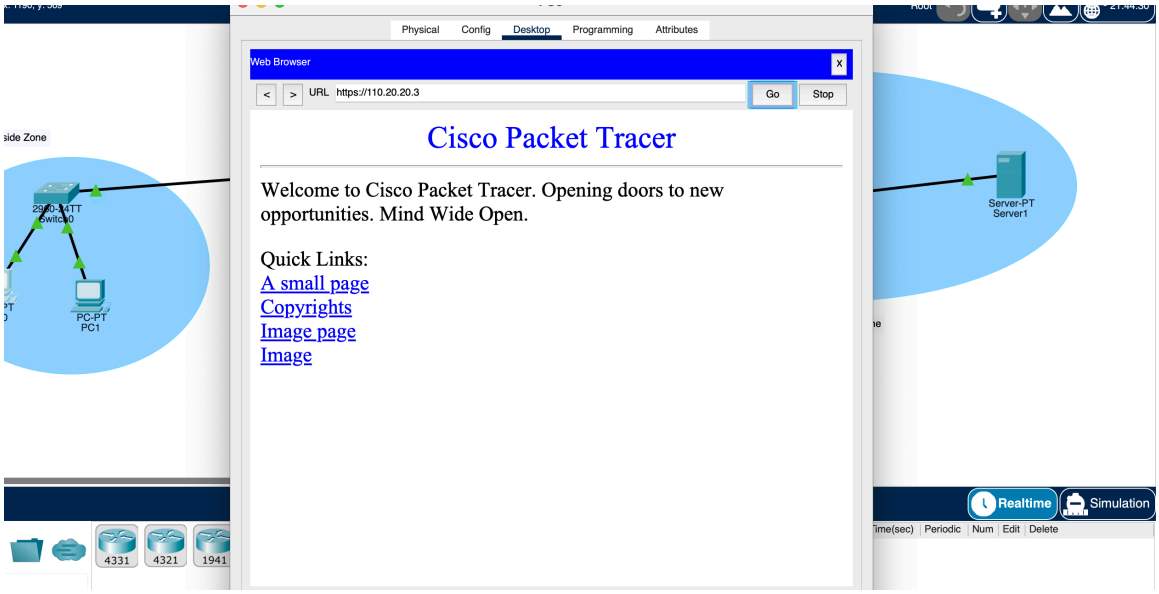


Ping PC1 to server0 and server1.

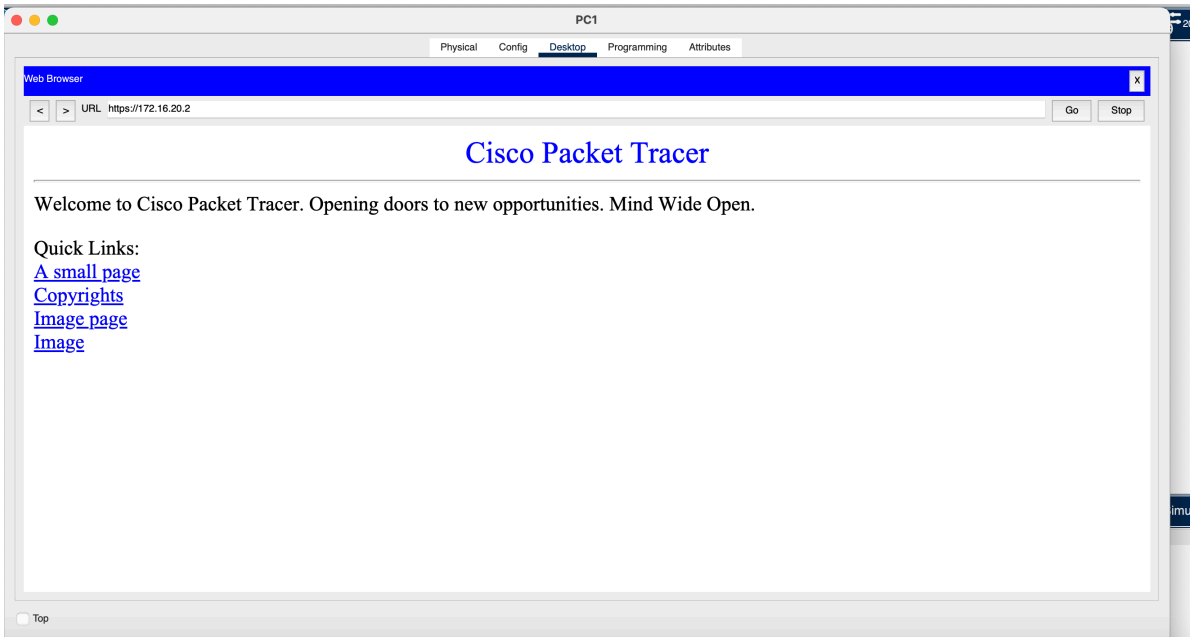


Lets check web access for PC0





Lets check web access for PC1



E. Design, Deploy, and Test Firewall Exceptional Rule (PC3 to Web Server 1)

Objective:
To create a firewall rule that allows PC3 (in the Outside zone) to access Web Server 1 (in the DMZ zone).
Configuration Steps:

access-list outside_access_in extended permit tcp host 110.20.20.2 host 172.16.20.2 eq www
access-list outside_access_in extended permit tcp host 110.20.20.2 host 172.16.20.2 eq 443

Objective: These regulations allow TCP communication from PC3 (IP 110.20.20.2) to Web Server 1 (IP 172.16.20.2) on ports 80 (HTTP) and 443 (HTTPS), essential for internet navigation.

Security is maintained by defining the origin and destination IP addresses, along with the service (port), in order to restrict only HTTP/HTTPS traffic from PC3 to Web Server 1, thereby minimizing the chance of unauthorized entry.

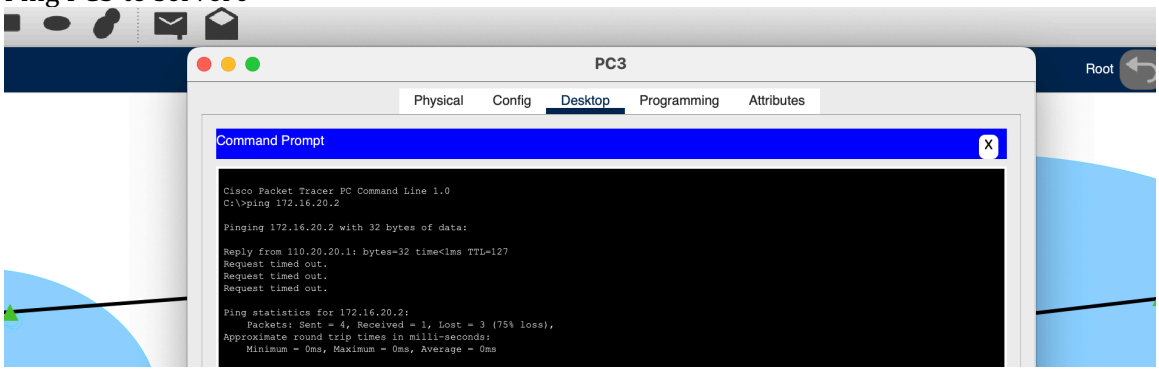
access-list outside_access_in extended permit icmp any any

This rule allows ICMP traffic, which is necessary for ping requests, enabling PC3 to ping Web Server 1.

access-group outside_access_in in interface outside
access-group dmz_access_in in interface dmz

These commands apply the access control lists (outside_access_in and dmz_access_in) to the appropriate interfaces, ensuring that the defined rules are enforced.

Ping PC3 to server0



We experience packet loss but we were able to receive one

Browser access.