FACULTY OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Computer Networks Laboratory - ENCS4130

Experiment. 10 Report

Cisco ASA Firewall Configuration

Prepared by: Layan Salem 1221026

Instructor: Dr. Sameh Awad

T.A: Eng. Tariq Odeh

Section: 3

Date: 25-May-2025

Place: Computer Network Lab

1 Abstract

In this experiment, the Cisco Adaptive Security Appliance (ASA) firewall was configured to secure a simulated network environment. The primary objectives were to set up security zones with appropriate security levels, implement Network Address Translation (NAT) through both static NAT and Port Address Translation (PAT), create and apply Access Control Lists (ACLs) to control traffic between different network zones, and configure a wireless access point to provide secure wireless connectivity for internal devices. The ASA was also configured as a DHCP server to dynamically assign IP addresses within the internal network. Testing was performed to validate DNS resolution, HTTP access, and ICMP behavior across the internal, DMZ, and external zones. It was expected that secure communication would be established, while necessary services such as web and DNS servers remained accessible. The expected outcomes were successfully achieved, with the firewall effectively managing and controlling network traffic.

2 Table of Content

3 Table of Figures

4 Table of tables

5 Introduction

A firewall is a network security system that monitors and controls network traffic based on established security rules. It acts as a barrier between a secure internal network and an untrusted external network such as the Internet. Firewalls are essential for protecting systems against unauthorized access, malware, and cyberattacks. They operate by inspecting incoming and outgoing traffic and determining whether to allow it based on predefined policies. There are different types of firewalls including packet-filtering, stateful inspection, proxy, and next-generation firewalls, each offering varying levels of protection and control.[1]

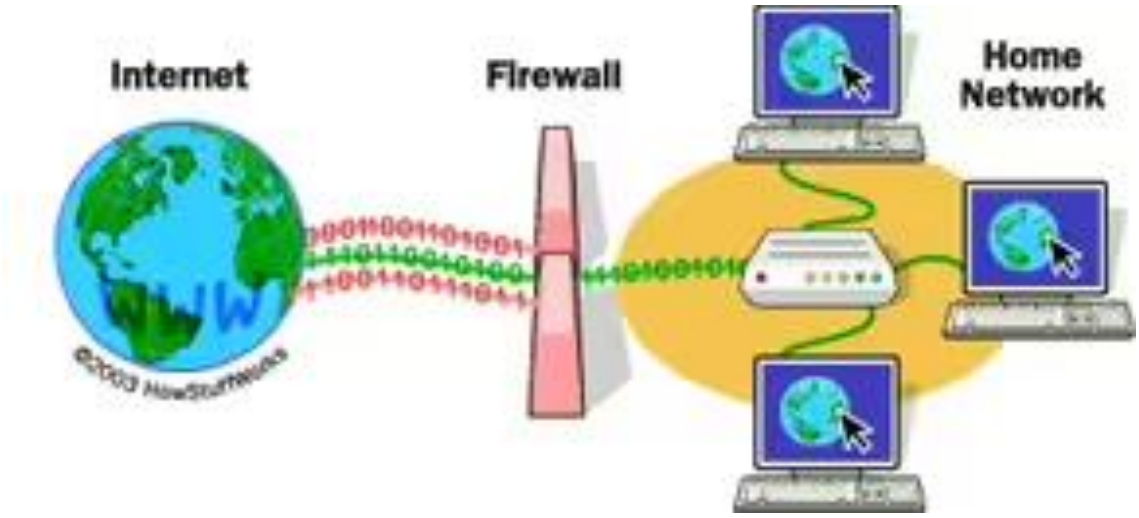


Figure 1 firewall [1]

5.1 Cisco Adaptive Security Appliance (ASA)

The Cisco Adaptive Security Appliance (ASA) is an integrated security solution that functions as a firewall while also offering capabilities such as intrusion prevention, antivirus filtering, and virtual private networking (VPN). ASA is designed to provide proactive threat defense by inspecting traffic and stopping attacks before they spread within the network. This makes it suitable for both small-scale and enterprise-level network environment [2].

Cisco ASA is the successor to the PIX firewall series and brings a comprehensive package of features into a single platform. It can be deployed as a perimeter firewall, VPN concentrator, or access control point between network zones such as internal LANs and public or semi-public zones like the DMZ. By default, Cisco ASA applies a security level system that prioritizes internal network safety by denying uninitiated inbound traffic from less trusted networks [3].

5.1.1 Demilitarized Zone (DMZ)

A Demilitarized Zone (DMZ) is a specialized subnet positioned between a secure internal network and an untrusted external network such as the Internet. It provides controlled access to services that need to be publicly accessible such as web servers, DNS servers, and FTP servers while isolating them from the internal network to limit the blast radius in case of a compromise [4].

The Cisco ASA enables DMZ implementation by assigning an intermediate security level (commonly 50) to a specific interface. This interface hosts public-facing services and is isolated from both the most trusted internal network (inside, level 100) and the least trusted external network (outside, level 0). In many enterprise architectures, the DMZ sits between two firewalls or interfaces an external-facing one that restricts public access and an internal one that guards internal resources. This configuration ensures layered defense, making it harder for attackers to pivot into the private network even if a DMZ server is compromised [3].

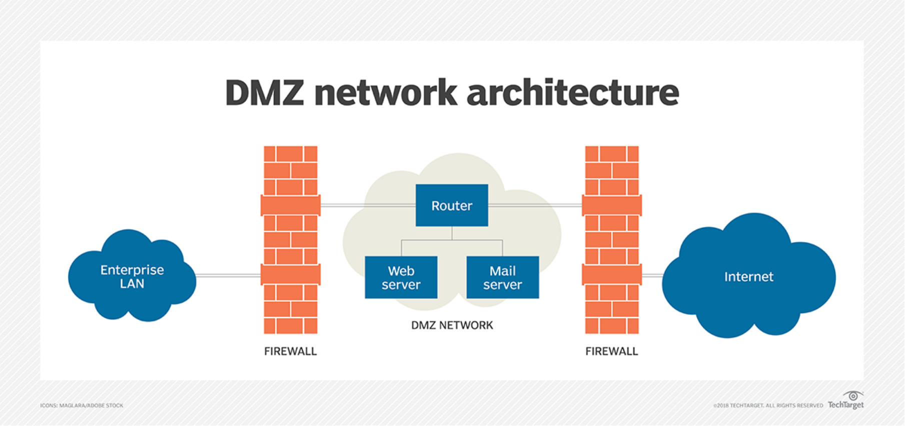


Figure 2 DMZ[4]

5.1.2 Network Address Translation (NAT)

Network Address Translation (NAT) is a method used in IP networking to allow multiple devices within a private network to access external networks using a limited number of public IP addresses. NAT functions by translating private IP addresses into public IPs before packets are forwarded to the Internet. This process not only conserves public address space but also adds a layer of privacy by hiding internal network structure [5].

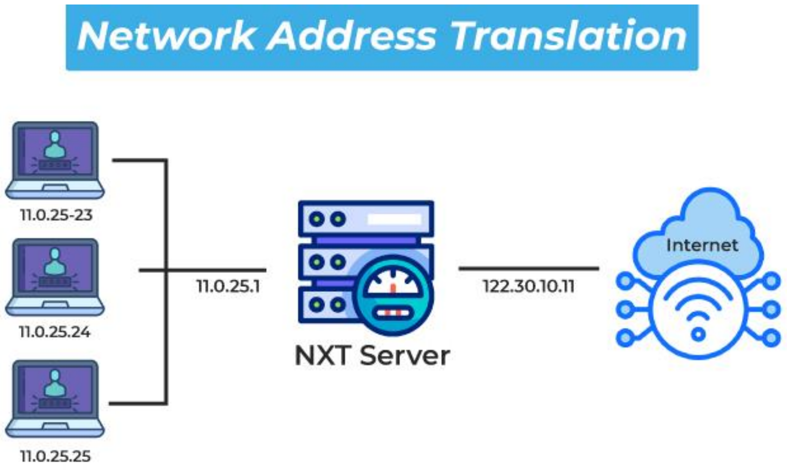


Figure 3 NAT

Cisco ASA supports several types of NAT:

- **Static NAT** provides a fixed one-to-one mapping, often used for DMZ servers that must always be reachable via the same public IP.
- **Dynamic NAT** maps internal addresses to a pool of public IPs as needed.
- **Port Address Translation (PAT)** allows multiple devices to share a single public IP using unique port numbers, making it the most efficient NAT type.

Although NAT is not primarily a security feature, it offers indirect protection by obscuring internal hosts from direct exposure to external networks. In combination with access control lists (ACLs), it helps reduce the attack surface. Cisco ASA implements NAT rules as part of its security policies, controlling how internal, DMZ, and external traffic is translated and routed [3].

5.1.3 Configuration of Cisco ASA Firewall

Configuring a Cisco ASA firewall involves several structured steps to ensure that security zones, traffic control, address translation, and routing are all properly managed. The ASA’s configuration model follows a zone-based architecture, using security levels, access control policies, and inspection mechanisms to regulate data flow across network segments such as the internal LAN, DMZ, and Internet-facing interfaces.

A. *Configure Interfaces and Security Zones*

In Cisco ASA, each interface must be configured with a name, IP address, and **security level**, which defines its trustworthiness. The security levels range from 0 (least trusted) to 100 (most trusted). Typical assignments are:

- Inside: 100 (trusted internal network)
- DMZ: 50 (semi-trusted public-facing servers)
- Outside: 0 (untrusted external network)

This tiered trust model simplifies traffic flow: by default, traffic is allowed to flow from higher to lower security levels but not vice versa. Administrators can define exceptions through Access Control Lists (ACLs) and inspection rules [3].

B. *Configure Port Address Translation (PAT)*

PAT, also known as **NAT Overload**, allows multiple internal devices to share a single public IP address by assigning each session a unique port number. This method is highly efficient for conserving IP addresses and is commonly used in enterprise settings for outbound Internet access.

PAT is implemented by defining network objects and dynamically mapping internal subnets to the firewall’s public interface. This setup not only provides scalability but also obscures internal IPs from the public, enhancing security through address masking [6].

C. *Configure Static NAT*

Static NAT is used for one-to-one translation between internal private IPs and publicly routable IP addresses. This configuration is essential for making services like web or DNS servers in the DMZ reachable from external networks.

By ensuring consistent address mapping, static NAT enables reliable access to critical resources while maintaining the isolation and control benefits of a firewall. It is typically applied to hosts in the DMZ that require predictable public IPs for inbound traffic [7].

D. *Enable Legitimate Traffic Flow from Lower to Higher Security Levels*

Cisco ASA firewalls **block traffic from lower to higher security levels** by default (e.g., from outside to inside). To permit legitimate traffic such as HTTP requests to a DMZ server, **Access Control Lists (ACLs)** must be configured to explicitly allow specific protocols and source/destination pairs.

Additionally, ASA uses **stateful packet inspection**, meaning it tracks active sessions and allows return traffic for permitted connections. This ensures bidirectional communication while maintaining strict inbound control. Protocol inspection (e.g., HTTP, DNS) must be explicitly enabled for application-layer traffic to return properly to the initiating client

E. *Configure Static Route*

To ensure that outbound traffic reaches external destinations, the ASA must be configured with a **static route**, typically a default route that forwards packets to the next-hop gateway (usually an upstream router).

This is a fundamental part of routing logic and ensures Internet-bound traffic from internal and DMZ zones is correctly relayed out of the firewall. Static routing is essential when dynamic routing protocols are not used or necessary for the deployment [3].

F. *Configure DHCP*

Cisco ASA can function as a **DHCP server** for internal devices, dynamically allocating IP addresses and network configuration (such as DNS and gateway). This service simplifies device management by eliminating the need for manual IP setup.

DHCP can be restricted to specific interfaces (e.g., “inside”), and the IP pool can be adjusted to reserve static addresses for printers or other critical devices. ASA also allows assigning DNS server information through DHCP options, ensuring integrated name resolution in the network [3].

6 Procedure and Discussion

6.1 Topology

The topology after built in Cisco packet tracer, see fig 5.

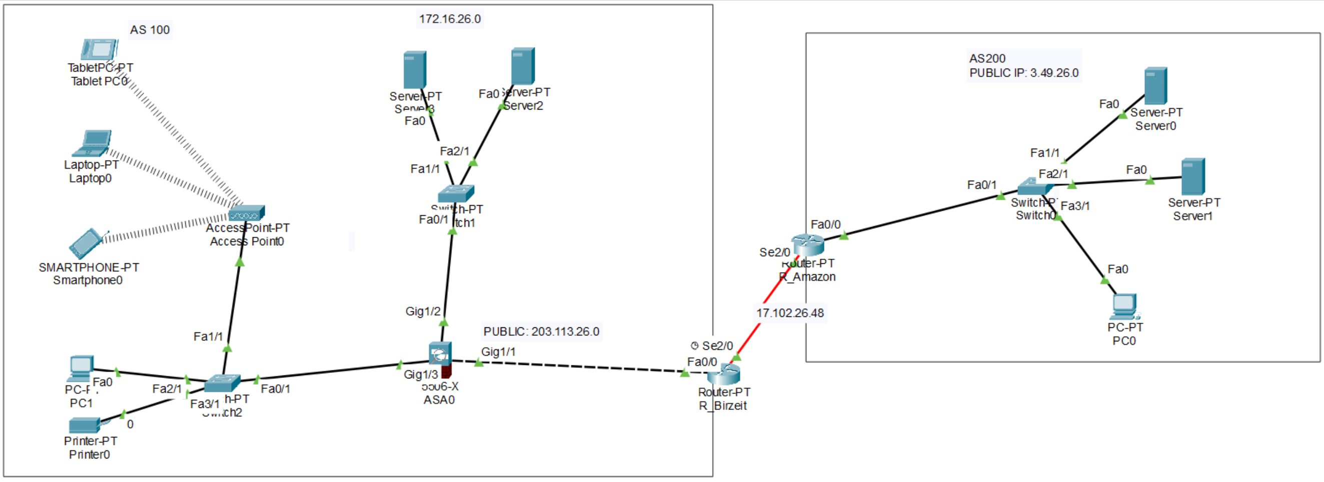
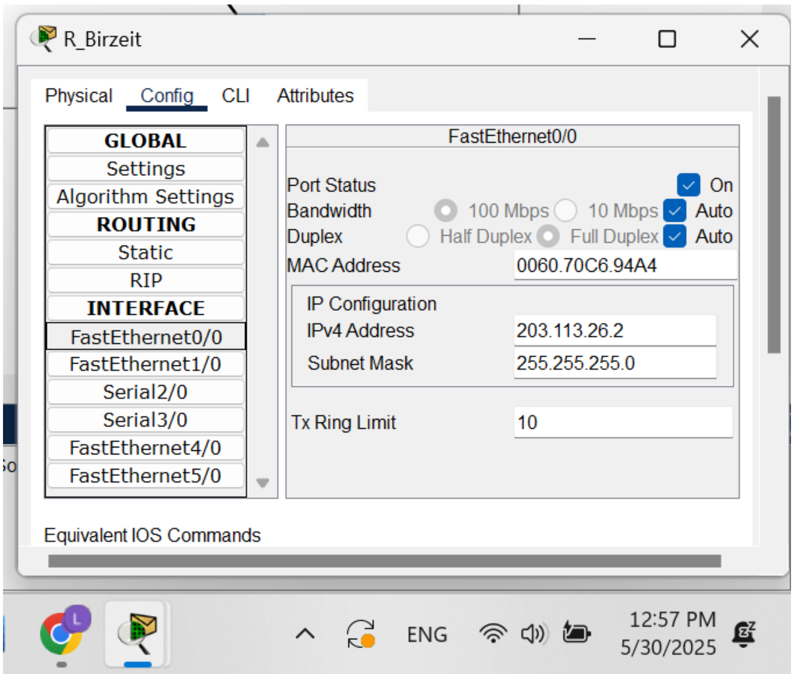


Figure 4 topology

6.2 Network Setup and Configuration

6.2.1 Configuring Static IPs for Routers Interfaces

First, I assigned static IP addresses to the router interfaces as shown in Figure 6:



FastEthernet0/0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0060.70C6.94A4

IP Configuration

IPv4 Address 203.113.26.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Figure 5 static IP for router0

The table below summarizes each router interface along with its assigned IP address.

Table 1 routers Ips

Device	Interface	Network IP address	Subnet Mask	Link
R_Birzeit	Fa0/0	203.113.26.2	255.255.255.0	ASA (Outside)
R_Birzeit	Se2/0	17.102.26.49	255.255.255.252	R_Amazon
R_Amazon	Fa0/0	17.102.26.50	255.255.255.252	R_Birzeit
R_Amazon	Se2/0	172.31.26.2	255.255.255.0	Amazon PC

6.2.2 Configuring OSPF and BGP Routing Protocols

To enable routing within and between networks, OSPF was configured for intra-domain routing, while BGP was used for inter-domain routing between R_Birzeit and R_Amazon.

1. on R_Birzeit, i use the following commands:
   - router ospf 1
   - log-adjacency-changes
   - redistribute bgp 100 subnets
   - network 203.113.26.0 0.0.0.255 area 0

   - router bgp 100
   - bgp log-neighbor-changes
   - no synchronization
   - neighbor 17.102.26.50 remote-as 200
   - redistribute ospf 1

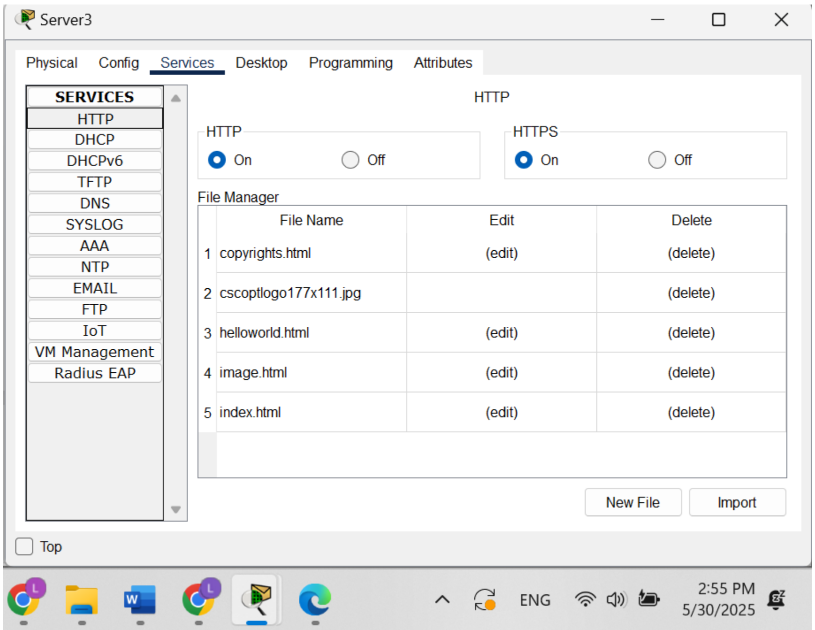
2. on R_Amazon, i use the following commands:
   - router ospf 1
   - log-adjacency-changes
   - redistribute bgp 200 subnets
   - network 203.113.26.0 0.0.0.255 area 0

   - router bgp 200
   - bgp log-neighbor-changes
   - no synchronization
   - neighbor 17.102.26.49 remote-as 100
   - redistribute ospf 1

6.3 Servers Configuration

6.3.1 Birzeit Web Server (www.birzeit.edu)

This server was placed in the DMZ and configured to support HTTP and HTTPS services. It was assigned a private IP and mapped to a public IP using static NAT on the ASA.



Server3

Physical | Config | Services | Desktop | Programming | Attributes

SERVICES: HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, Radius EAP

HTTP

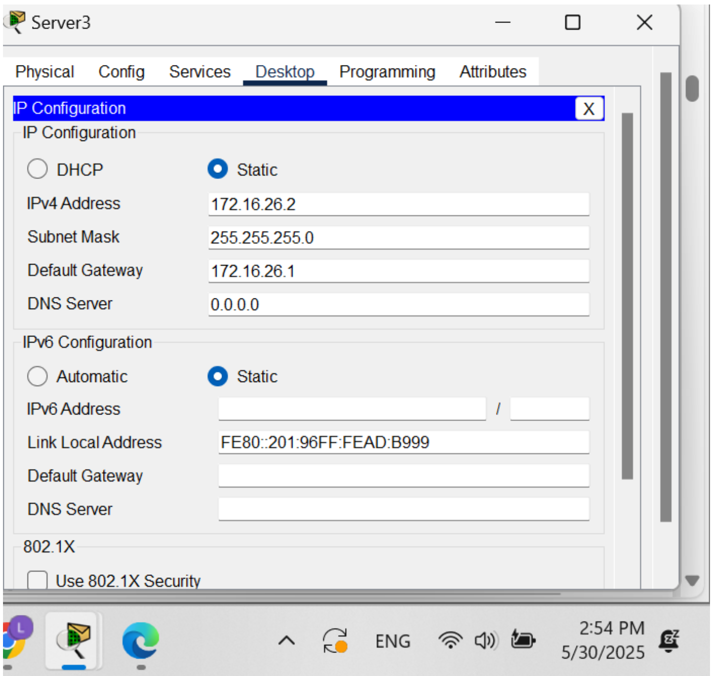
HTTP: ● On ○ Off

HTTPS: ● On ○ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

Figure 6 Configuration of Web Services on www.birzeit.edu



Server3

Physical | Config | Services | Desktop | Programming | Attributes

IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address	172.16.26.2
Subnet Mask	255.255.255.0
Default Gateway	172.16.26.1
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::201:96FF:FEAD:B999
Default Gateway	
DNS Server	

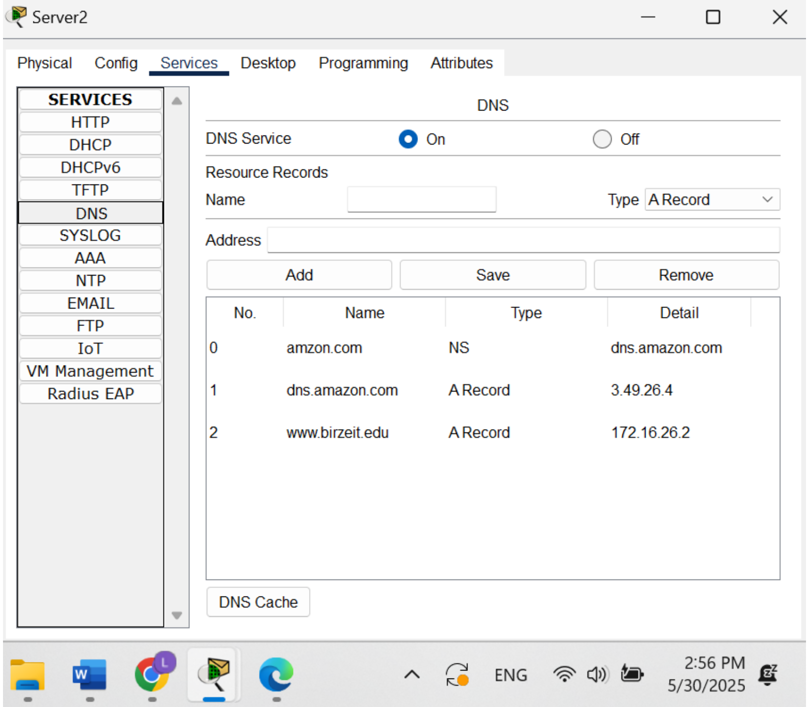
802.1X

□ Use 802.1X Security

Figure 7 IP Configuration of Birzeit Web Server.

6.3.2 Birzeit DNS Server (dns.birzeit.edu)

The DNS server in Birzeit was configured to resolve local domain names. DNS records were added to support resolution for all critical devices in the network.



Server2

Physical | Config | Services | Desktop | Programming | Attributes

DNS

DNS Service ● On ○ Off

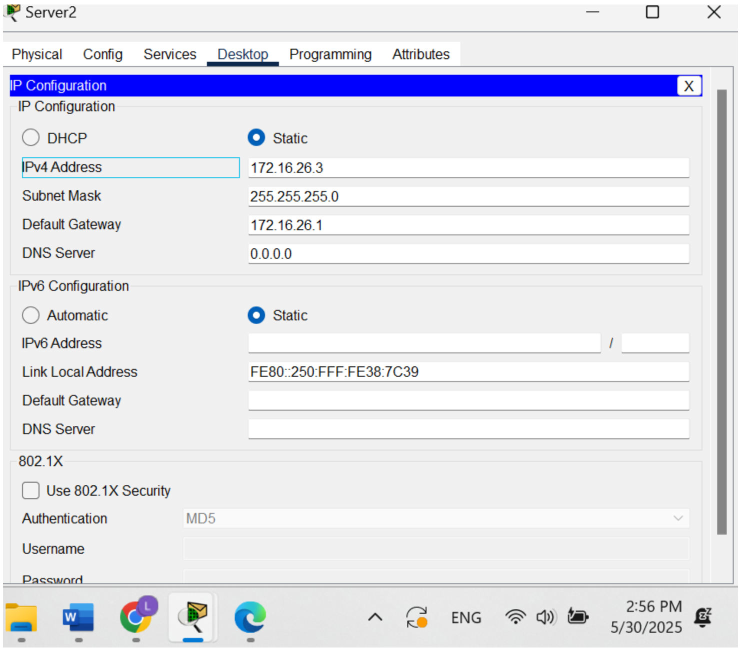
Resource Records

Name | Type A Record

Address

No.	Name	Type	Detail
0	amzon.com	NS	dns.amazon.com
1	dns.amazon.com	A Record	3.49.26.4
2	www.birzeit.edu	A Record	172.16.26.2

Figure 8 DNS Records Configuration on dns.birzeit.edu



Server2

Physical | Config | Services | Desktop | Programming | Attributes

IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address: 172.16.26.3

Subnet Mask: 255.255.255.0

Default Gateway: 172.16.26.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::250:FFF:FE38:7C39

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

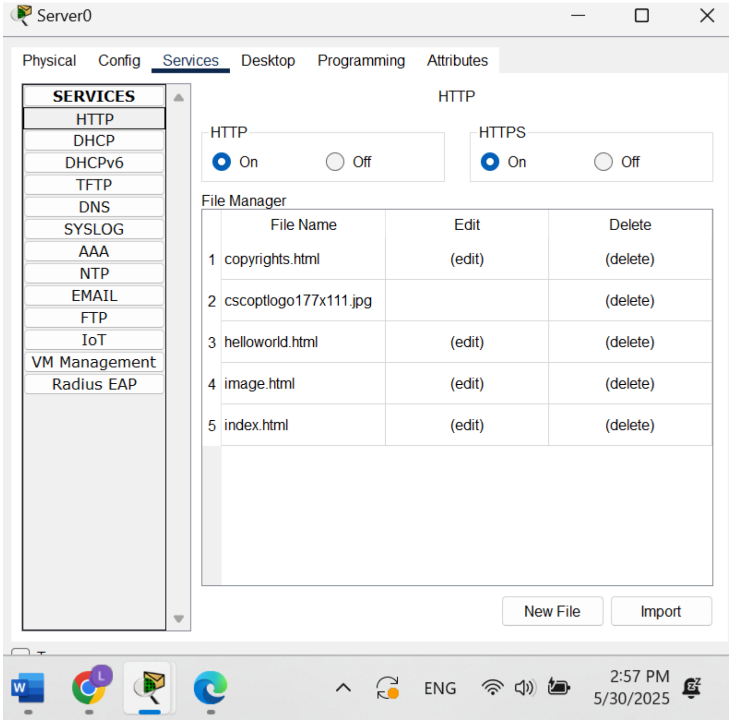
Username:

Password:

Figure 9 IP Configuration of Birzeit DNS Server

6.3.3 Amazon Web Server (www.amazon.com)

This web server was placed in the Amazon internal LAN. It was configured with a static IP and HTTP service was enabled.



HTTP

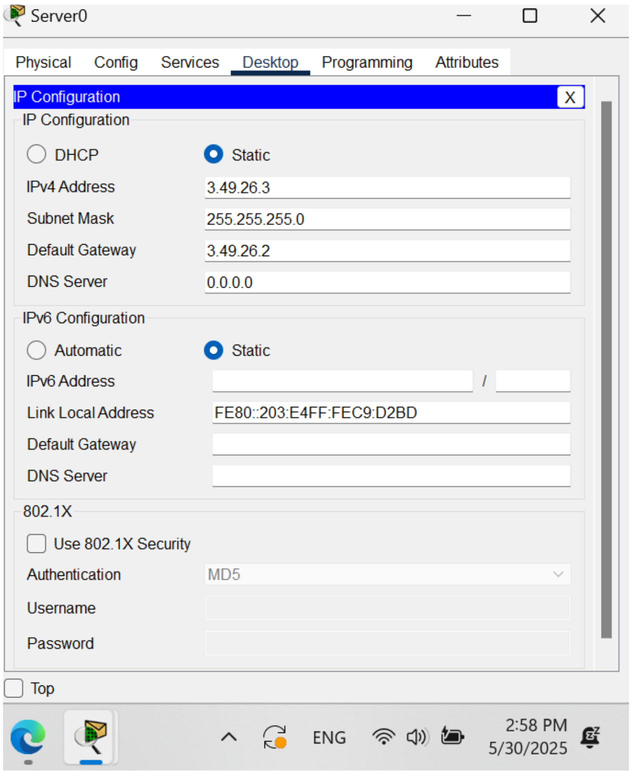
HTTP: ● On ○ Off

HTTPS: ● On ○ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

Figure 10 Configuration of Web Services on www.amazon.com.



IP Configuration

○ DHCP ● Static

IPv4 Address	3.49.26.3
Subnet Mask	255.255.255.0
Default Gateway	3.49.26.2
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::203:E4FF:FEC9:D2BD
Default Gateway	
DNS Server	

802.1X

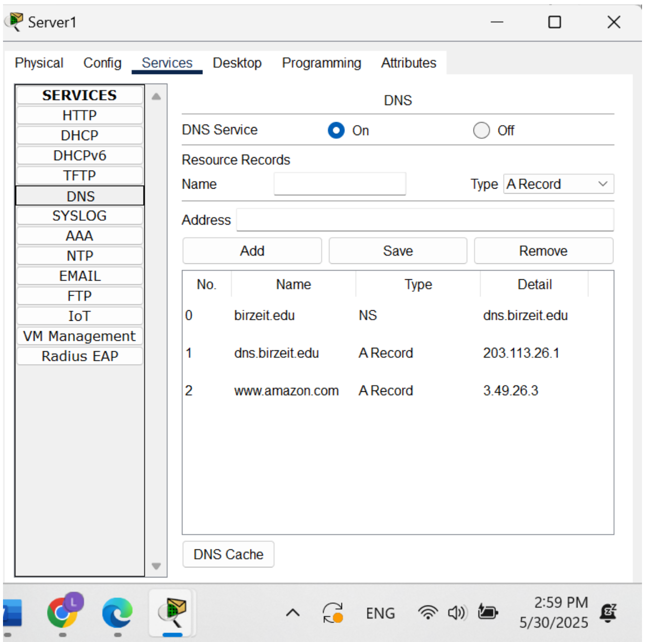
□ Use 802.1X Security

Authentication	MD5
Username	
Password	

Figure 11 IP Configuration of Amazon Web Server.

6.3.4 Amazon DNS Server (dns.amazon.com)

The DNS server for the Amazon network was configured with static IP settings and DNS entries for internal devices.



DNS

DNS Service ● On ○ Off

Resource Records

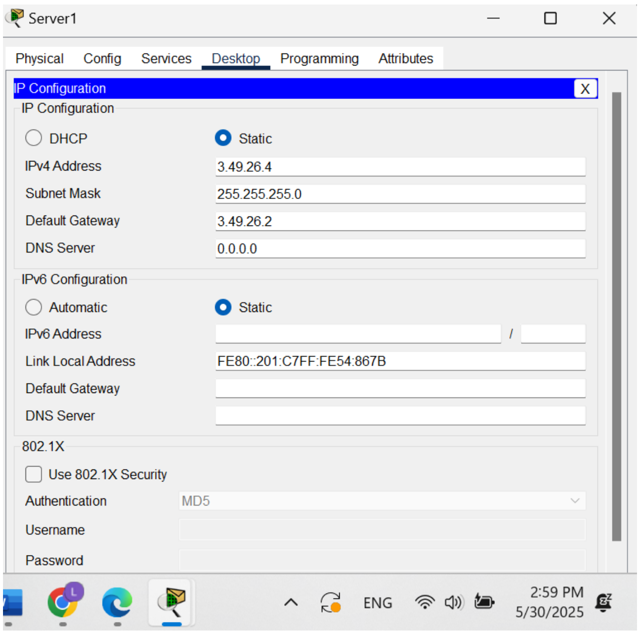
Name

Type A Record

Address

No.	Name	Type	Detail
0	birzeit.edu	NS	dns.birzeit.edu
1	dns.birzeit.edu	A Record	203.113.26.1
2	www.amazon.com	A Record	3.49.26.3

Figure 12 DNS Records on dns.amazon.com.



IP Configuration

○ DHCP ● Static

IPv4 Address 3.49.26.4

Subnet Mask 255.255.255.0

Default Gateway 3.49.26.2

DNS Server 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::201:C7FF:FE54:867B

Default Gateway

DNS Server

802.1X

□ Use 802.1X Security

Authentication MD5

Username

Password

Figure 13 IP Configuration of Amazon DNS Server.

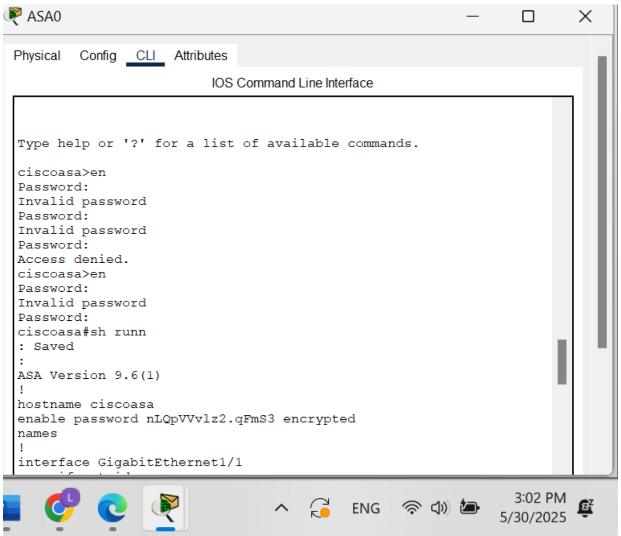
Configuring the web and DNS servers validated how services are made publicly accessible (via DMZ and NAT) or remain private (within the LAN). These servers simulated real-world infrastructure for hosting and resolving domain names, which were later tested from different network zones.

6.4 ASA Firewall Configuration

6.4.1 Configuring Privileged Mode Password

A password was set for privileged EXEC mode to secure administrative access to the ASA firewall.

- enable
- configure terminal
- enable password encs4130



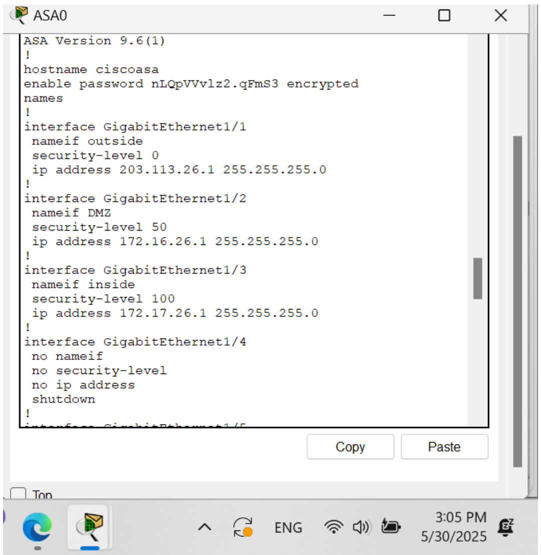
```
Type help or '?' for a list of available commands.

ciscoasa>en
Password:
Invalid password
Password:
Invalid password
Password:
Access denied.
ciscoasa>en
Password:
Invalid password
Password:
ciscoasa#sh runn
: Saved
:
ASA Version 9.6(1)
!
hostname ciscoasa
enable password nLQpVVvlz2.qFmS3 encrypted
names
!
interface GigabitEthernet1/1
```

Figure 14 ASA Privileged Mode Password Configuration.

6.4.2 Configuring Interfaces and Security Zones

Three ASA interfaces were configured and assigned appropriate names and security levels:

- Inside (100), DMZ (50) , Outside (0)



```
ASA Version 9.6(1)
!
hostname ciscoasa
enable password nLQpVVvlz2.qFmS3 encrypted
names
!
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 203.113.26.1 255.255.255.0
!
interface GigabitEthernet1/2
 nameif DMZ
 security-level 50
 ip address 172.16.26.1 255.255.255.0
!
interface GigabitEthernet1/3
 nameif inside
 security-level 100
 ip address 172.17.26.1 255.255.255.0
!
interface GigabitEthernet1/4
 no nameif
 no security-level
 no ip address
 shutdown
!
```

Figure 15 ASA Interface and Zone Configuration.

6.4.3 Configuring PAT for the Internal Network

PAT was set up for inside users to access the outside world using a single public IP on the ASA outside interface.

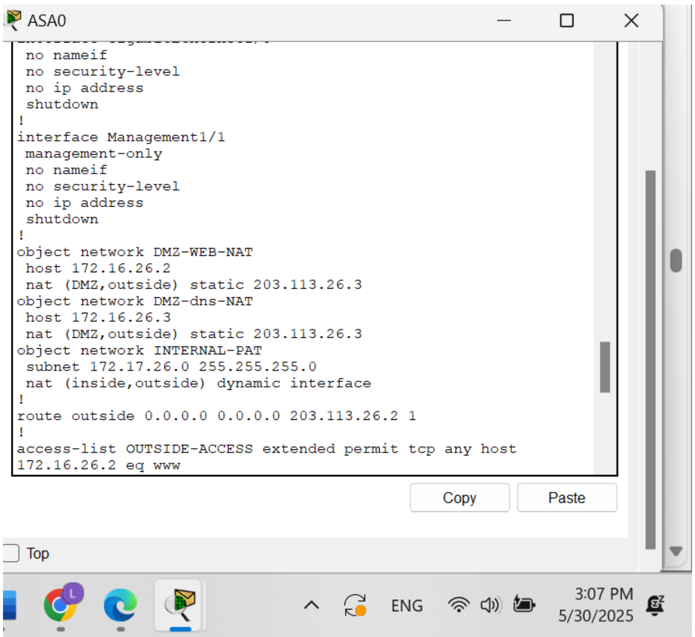
Commands:

- object network INTERNAL-PAT
- subnet 172.17.26.0 255.255.255.0
- nat (inside,outside) dynamic interface

6.4.4 Configuring Static NAT for the DMZ Network

Static NAT was applied for DMZ servers so they could be accessed from the public network via their public IP addresses.

- object network DMZ-WEB-NAT
- host 172.16.26.2
- nat (DMZ,outside) static 203.113.26.3
- object network DMZ-dns-NAT
- host 172.16.26.3
- nat (DMZ,outside) static 203.113.26.3
- object network INTERNAL-PAT
- subnet 172.17.26.0 255.255.255.0
- nat (inside,outside) dynamic interface



```
 no nameif
 no security-level
 no ip address
 shutdown
!
interface Management1/1
 management-only
 no nameif
 no security-level
 no ip address
 shutdown
!
object network DMZ-WEB-NAT
 host 172.16.26.2
 nat (DMZ,outside) static 203.113.26.3
object network DMZ-dns-NAT
 host 172.16.26.3
 nat (DMZ,outside) static 203.113.26.3
object network INTERNAL-PAT
 subnet 172.17.26.0 255.255.255.0
 nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 203.113.26.2 1
!
access-list OUTSIDE-ACCESS extended permit tcp any host
172.16.26.2 eq www
```

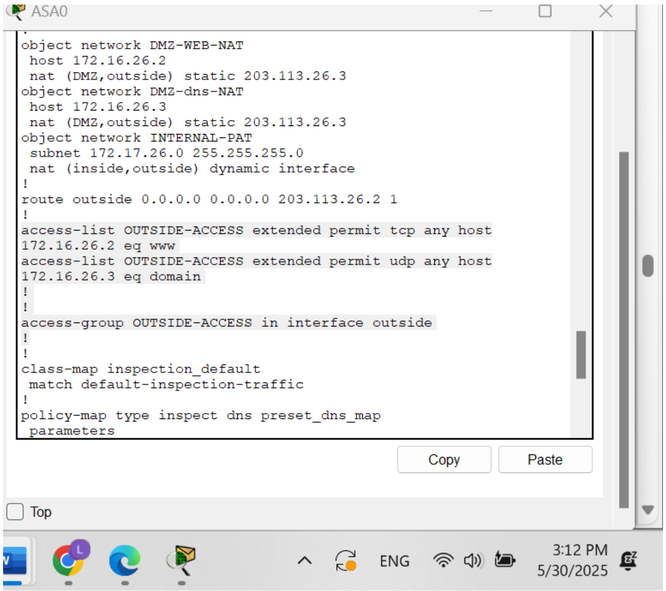
Figure 16 Static NAT Configuration for DMZ Servers.

6.4.5 Enabling External Access to DMZ Servers

Access Control Lists (ACLs) were applied to the outside interface to allow inbound HTTP and DNS requests to reach the DMZ servers.

Commands:

- access-list OUTSIDE-ACCESS extended permit tcp any host 172.16.26.2 eq www
- access-list OUTSIDE-ACCESS extended permit udp any host 172.16.26.3 eq domain
- access-group OUTSIDE-ACCESS in interface outside

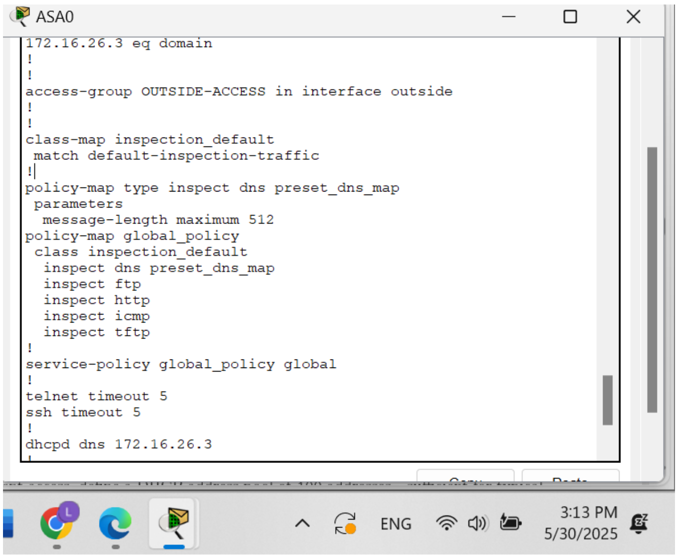


```
object network DMZ-WEB-NAT
 host 172.16.26.2
 nat (DMZ,outside) static 203.113.26.3
object network DMZ-dns-NAT
 host 172.16.26.3
 nat (DMZ,outside) static 203.113.26.3
object network INTERNAL-PAT
 subnet 172.17.26.0 255.255.255.0
 nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 203.113.26.2 1
!
access-list OUTSIDE-ACCESS extended permit tcp any host
172.16.26.2 eq www
access-list OUTSIDE-ACCESS extended permit udp any host
172.16.26.3 eq domain
!
!
access-group OUTSIDE-ACCESS in interface outside
!
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
```

Figure 17 ACL Rules Allowing Access to DMZ Servers.

6.4.6 Enabling Return Traffic for HTTP, DNS, and ICMP to the Internal LAN

Protocol inspection was enabled for HTTP, DNS, and ICMP to allow return traffic for internal users communicating with external services.



```
172.16.26.3 eq domain
!
!
access-group OUTSIDE-ACCESS in interface outside
!
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect http
  inspect icmp
  inspect tftp
!
service-policy global_policy global
!
telnet timeout 5
ssh timeout 5
!
dhcpd dns 172.16.26.3
```

Figure 18 Protocol Inspection Configuration on ASA.

6.4.7 Configuring Default Routing

A default static route was added on the ASA to route all unknown traffic to the next-hop IP on the outside network.

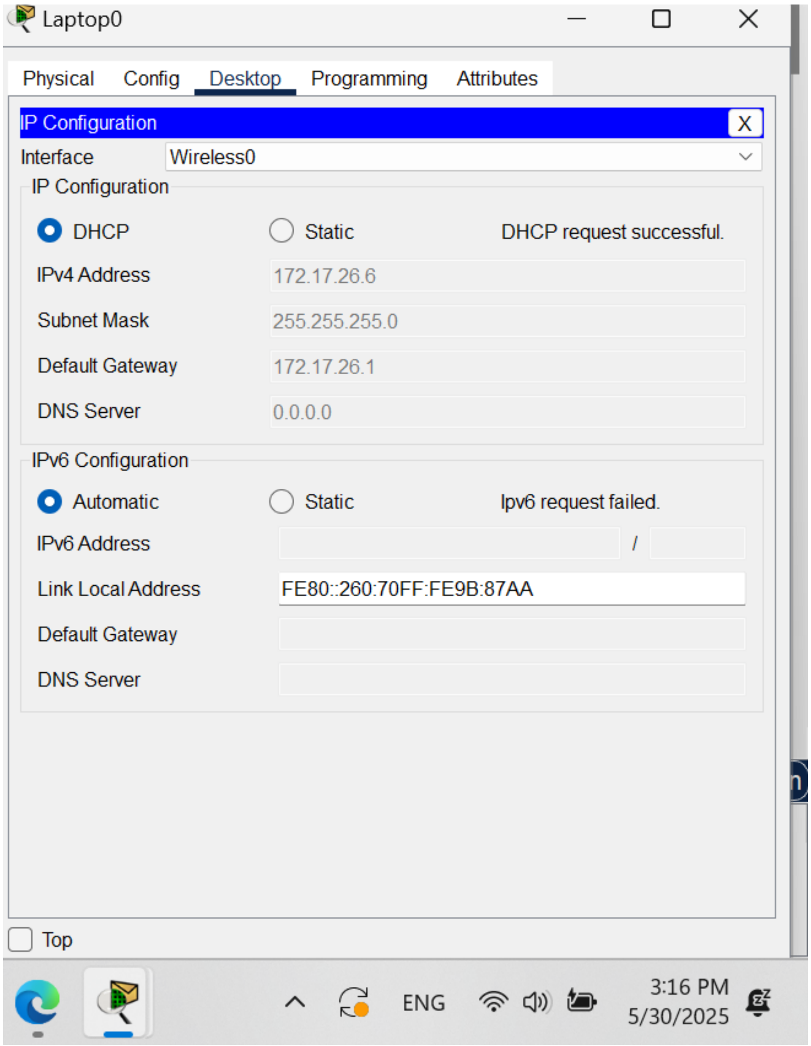
- route outside 0.0.0.0 0.0.0.0 203.113.26.2 1

6.4.8 Configuring ASA as a DHCP Server for the Internal LAN

The ASA was configured to provide DHCP services on the inside interface. A pool was defined to allocate IP addresses to internal clients.

DHCP Server Configuration on ASA:

- dhcpd dns 172.16.26.3
- dhcpd address 172.17.26.3-172.17.26.102 inside
- dhcpd enable inside



Interface: Wireless0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 172.17.26.6

Subnet Mask: 255.255.255.0

Default Gateway: 172.17.26.1

DNS Server: 0.0.0.0

IPv6 Configuration

● Automatic ○ Static Ipv6 request failed.

IPv6 Address: /

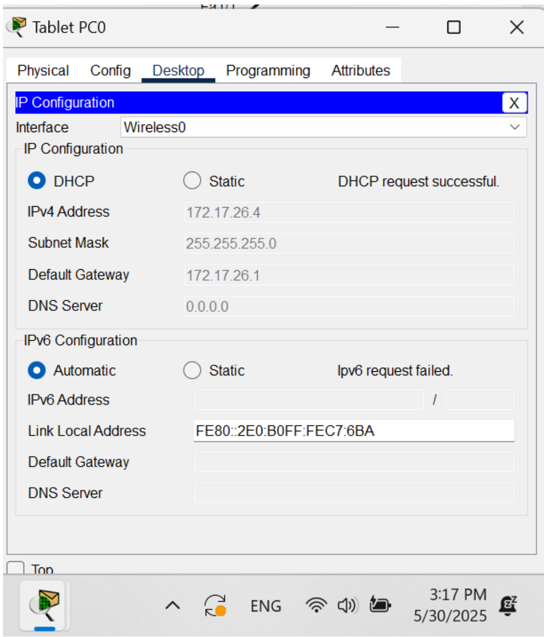
Link Local Address: FE80::260:70FF:FE9B:87AA

Default Gateway:

DNS Server:

□ Top

Figure 19 DHCP Lease Information for laptop



IP Configuration

Interface: Wireless0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 172.17.26.4

Subnet Mask: 255.255.255.0

Default Gateway: 172.17.26.1

DNS Server: 0.0.0.0

IPv6 Configuration

● Automatic ○ Static Ipv6 request failed.

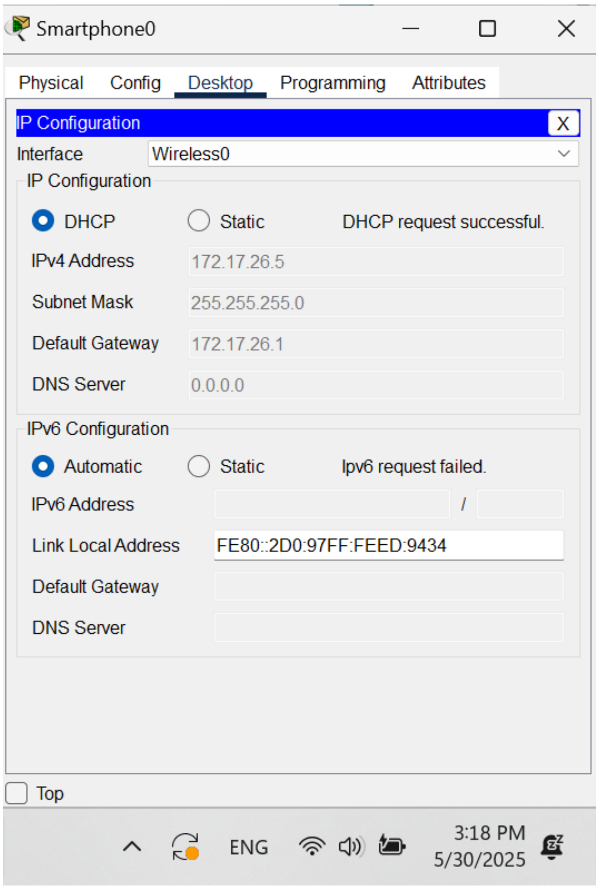
IPv6 Address: /

Link Local Address: FE80::2E0:B0FF:FEC7:6BA

Default Gateway:

DNS Server:

Figure 20 DHCP Lease Information for tablet



IP Configuration

Interface: Wireless0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 172.17.26.5

Subnet Mask: 255.255.255.0

Default Gateway: 172.17.26.1

DNS Server: 0.0.0.0

IPv6 Configuration

● Automatic ○ Static Ipv6 request failed.

IPv6 Address: /

Link Local Address: FE80::2D0:97FF:FEED:9434

Default Gateway:

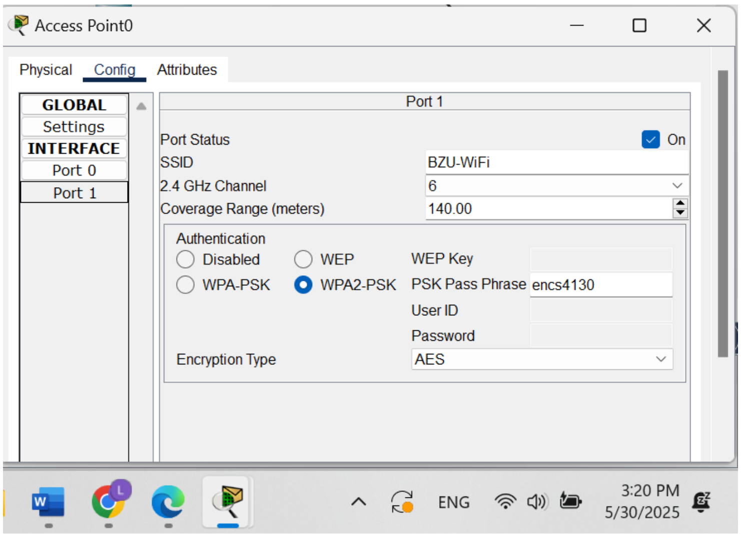
DNS Server:

Figure 21 DHCP Lease Information for phone

This section highlighted the ASA's versatility. Security zones were used to enforce trust boundaries, PAT enabled inside users to access the Internet, and static NAT exposed DMZ servers safely. ACLs ensured granular access control, while DHCP simplified IP assignment for internal clients.

6.5 Access Point Configuration

An access point was added to the internal LAN to support wireless connectivity. WPA2 encryption and a secure pre-shared key were used.



Access Point0

Physical | Config | Attributes

GLOBAL
Settings
INTERFACE
Port 0
Port 1

Port 1

Port Status ☑ On
SSID BZU-WiFi
2.4 GHz Channel 6
Coverage Range (meters) 140.00

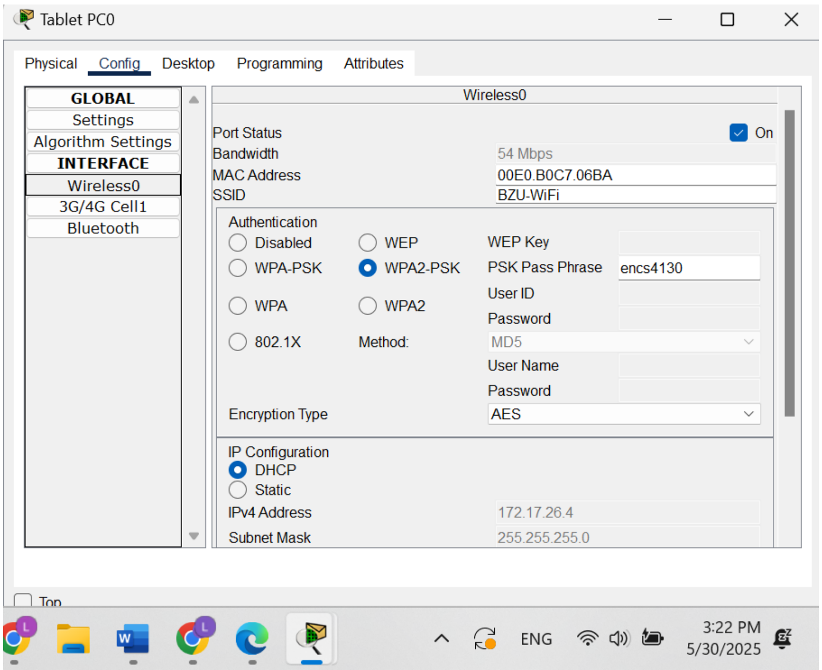
Authentication
○ Disabled ○ WEP
○ WPA-PSK ● WPA2-PSK
WEP Key
PSK Pass Phrase encs4130
User ID
Password
Encryption Type AES

Figure 22 Wireless Access Point Configuration (SSID and WPA2 Setup).

Adding a wireless access point showcased secure Wi-Fi deployment. Enabling WPA2 encryption and DHCP for wireless clients simulated a realistic BYOD scenario in enterprise networks.

6.6 Connecting Wireless Devices and Configuring Dynamic IP Addresses

A laptop was connected to the wireless network and set to obtain its IP address dynamically. It successfully received IP configuration from the ASA’s DHCP service.



Tablet PC0

Physical | Config | Desktop | Programming | Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
Wireless0
3G/4G Cell1
Bluetooth

Wireless0

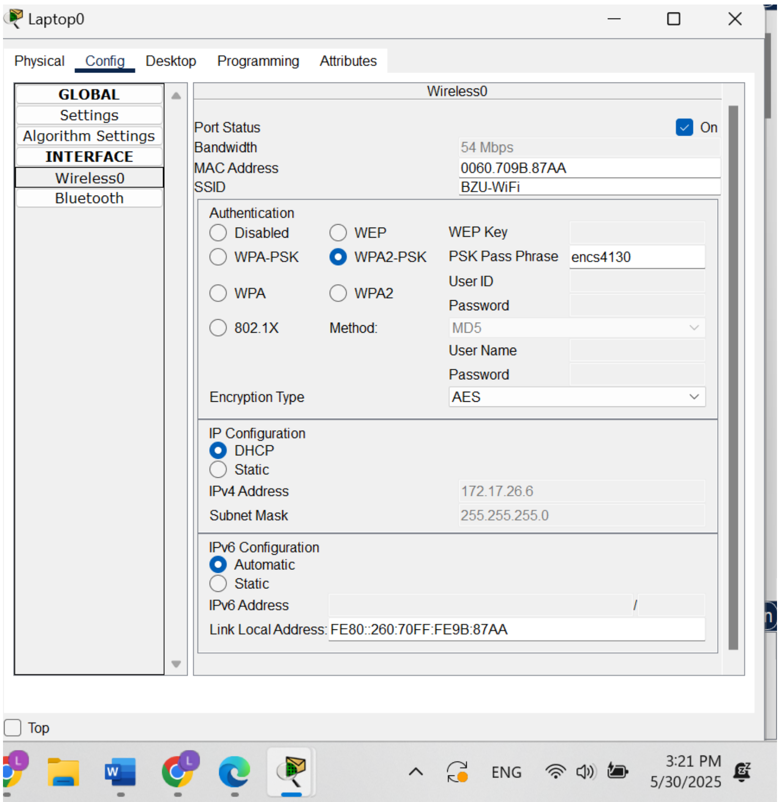
Port Status ☑ On
Bandwidth 54 Mbps
MAC Address 00E0.B0C7.06BA
SSID BZU-WiFi

Authentication
○ Disabled ○ WEP
○ WPA-PSK ● WPA2-PSK
○ WPA ○ WPA2
○ 802.1X Method: MD5
WEP Key
PSK Pass Phrase encs4130
User ID
Password
User Name
Password
Encryption Type AES

IP Configuration
● DHCP
○ Static
IPv4 Address 172.17.26.4
Subnet Mask 255.255.255.0

□ Top

Figure 23 tablet Wireless Configuration and DHCP Assignment.



Wireless0

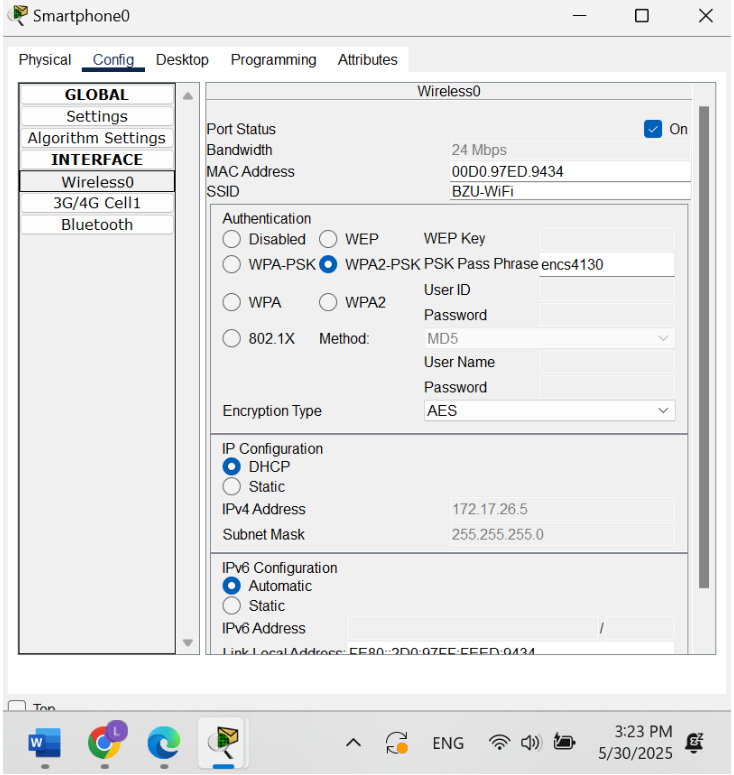
Port Status ☑ On
Bandwidth 54 Mbps
MAC Address 0060.709B.87AA
SSID BZU-WiFi

Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase encs4130
○ WPA ○ WPA2 User ID
Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type AES

IP Configuration
● DHCP
○ Static
IPv4 Address 172.17.26.6
Subnet Mask 255.255.255.0

IPv6 Configuration
● Automatic
○ Static
IPv6 Address /
Link Local Address: FE80::260:70FF:FE9B:87AA

Figure 24 Laptop Wireless Configuration.



Wireless0

Port Status ☑ On
Bandwidth 24 Mbps
MAC Address 00D0.97ED.9434
SSID BZU-WiFi

Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase encs4130
○ WPA ○ WPA2 User ID
Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type AES

IP Configuration
● DHCP
○ Static
IPv4 Address 172.17.26.5
Subnet Mask 255.255.255.0

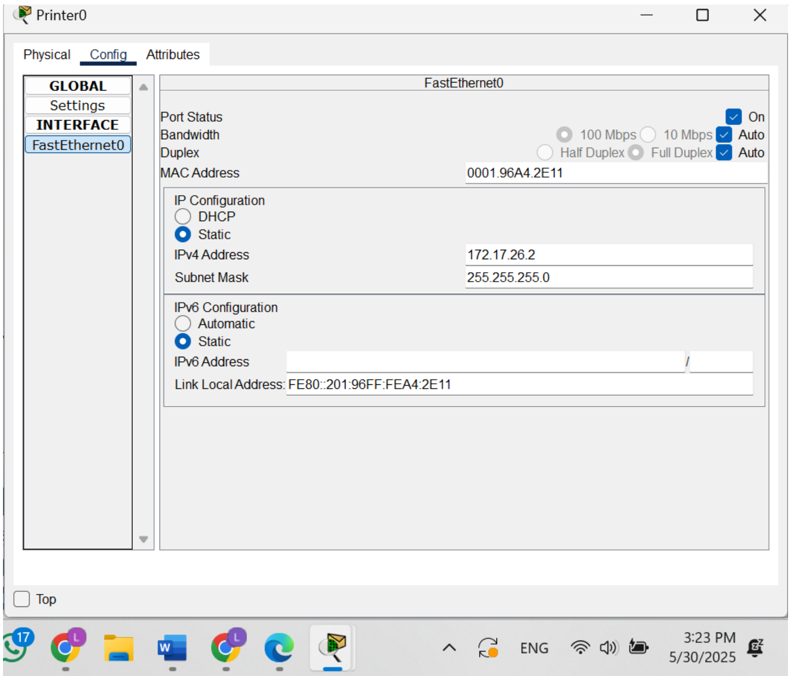
IPv6 Configuration
● Automatic
○ Static
IPv6 Address /
Link Local Address: FE80::2D0:97FF:FEED:9434

Figure 25 phone Wireless Configuration.

The successful dynamic configuration of the laptop verified that ASA's DHCP server could assign proper addressing parameters. It also confirmed wireless integration with security and routing policies in place.

6.7 Configuring End Devices with Static IP Addresses

Some end devices, such as the internal printer and the PC in the Amazon network, were assigned static IP addresses for consistent communication.



Printer0

Physical | Config | Attributes

GLOBAL
Settings
INTERFACE
FastEthernet0

FastEthernet0

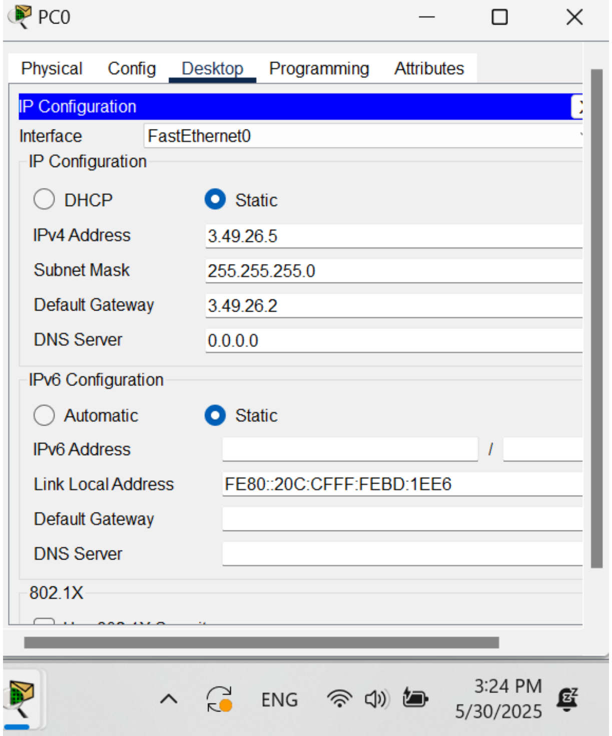
Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address 0001.96A4.2E11

IP Configuration
○ DHCP
● Static
IPv4 Address 172.17.26.2
Subnet Mask 255.255.255.0

IPv6 Configuration
○ Automatic
● Static
IPv6 Address /
Link Local Address: FE80::201:96FF:FEA4:2E11

□ Top

Figure 26 Static IP Configuration of Internal Printer.



PC0

Physical | Config | Desktop | Programming | Attributes

IP Configuration

Interface FastEthernet0

IP Configuration
○ DHCP ● Static
IPv4 Address 3.49.26.5
Subnet Mask 255.255.255.0
Default Gateway 3.49.26.2
DNS Server 0.0.0.0

IPv6 Configuration
○ Automatic ● Static
IPv6 Address /
Link Local Address FE80::20C:CFFF:FEBD:1EE6
Default Gateway
DNS Server

802.1X

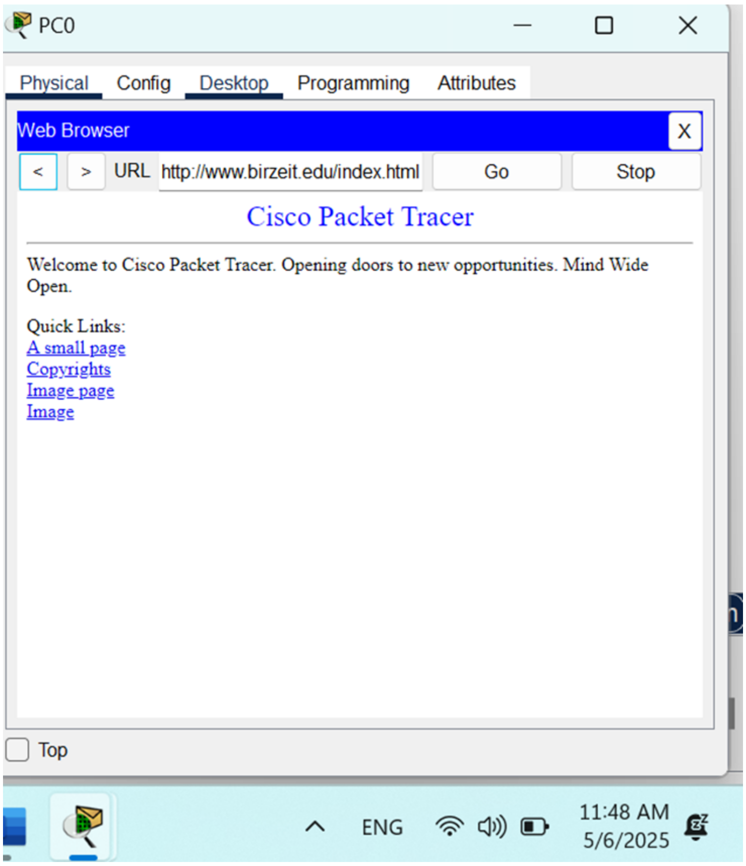
Figure 27 Static IP Configuration of Amazon Network PC.

Manually assigning static IPs to the printer and Amazon PC ensured consistent addressing for services that required reliability, like printing and internal file access. It also allowed mixed environments of static and dynamic addressing.

7 Testing and Verification

7.1 Accessing “www.birzeit.edu” from PC Amazon (Internet)

To verify static NAT and ACL configurations, we attempted to access the Birzeit web server (www.birzeit.edu) from PC Amazon, which resides in the external (Internet) zone. The server's public IP address was entered into a browser, and DNS resolution was tested using ping.



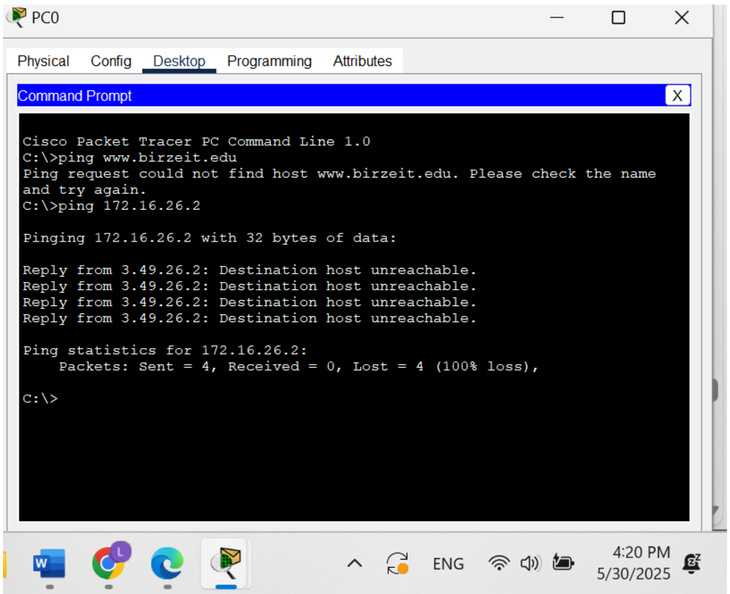
URL http://www.birzeit.edu/index.html

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Figure 28 Web browser accessing www.birzeit.edu from PC Amazon.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping www.birzeit.edu
Ping request could not find host www.birzeit.edu. Please check the name
and try again.
C:\>ping 172.16.26.2

Pinging 172.16.26.2 with 32 bytes of data:

Reply from 3.49.26.2: Destination host unreachable.
Reply from 3.49.26.2: Destination host unreachable.
Reply from 3.49.26.2: Destination host unreachable.
Reply from 3.49.26.2: Destination host unreachable.

Ping statistics for 172.16.26.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 29 Ping test from PC Amazon to www.birzeit.edu showing successful response.

7.2 Accessing “www.amazon.com” from Smartphone (Birzeit Internal Network)

This test checks if PAT and DNS forwarding are working correctly from the inside network. The wireless smartphone, connected to the BZU-WiFi access point, was used to access the Amazon web server located in the Amazon LAN.

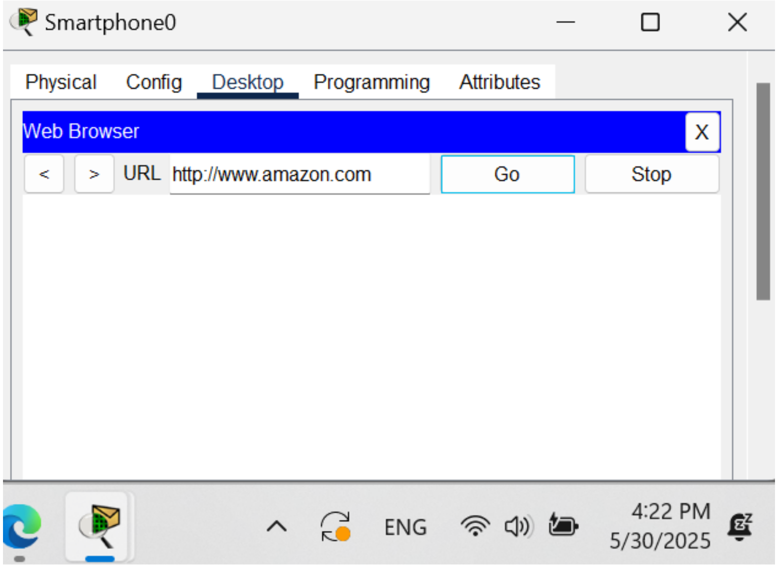
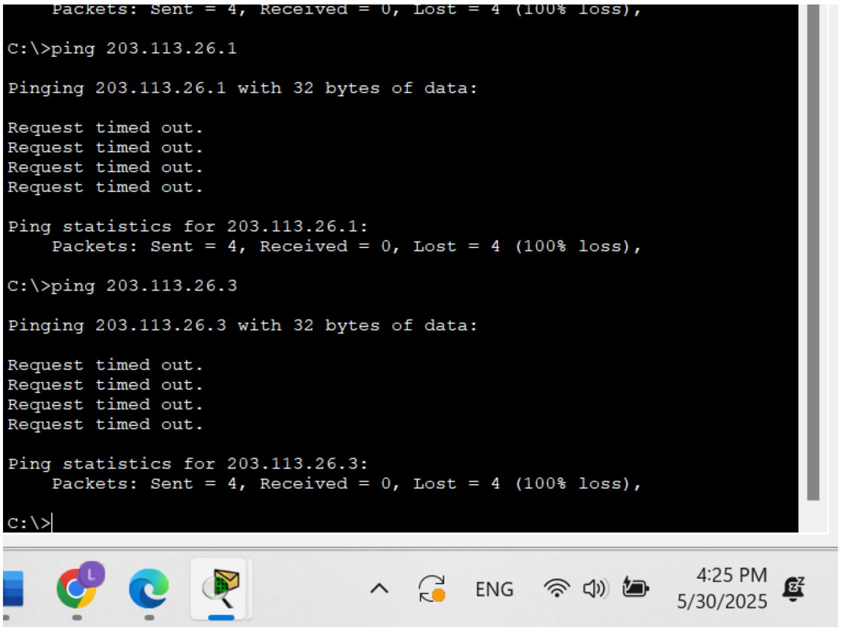


Figure 30 Web browser on the smartphone accessing www.amazon.com

7.3 Pinging a Host in Birzeit Network from PC Amazon (Internet)

This test verifies that ICMP access is correctly denied from a lower to higher security zone by default. From PC Amazon (outside), an ICMP ping was sent to an internal host in the Birzeit network (e.g., PC with IP 172.17.26.3).

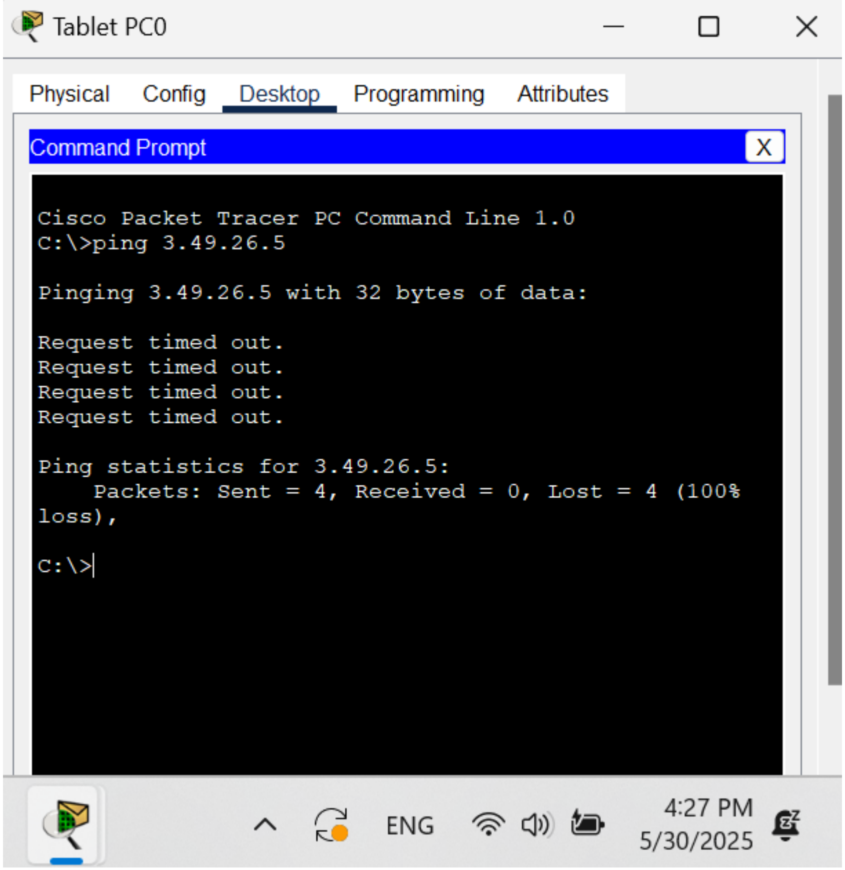


```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 203.113.26.1

Pinging 203.113.26.1 with 32 bytes of data:

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

Ping statistics for 203.113.26.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 203.113.26.3

Pinging 203.113.26.3 with 32 bytes of data:

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

Ping statistics for 203.113.26.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 31 Failed ping from PC Amazon to internal Birzeit PC.

7.4 Pinging PC Amazon (Internet) from a Host in Birzeit Network

This test ensures that ICMP return traffic is permitted when initiated from a higher to lower security zone. A Birzeit PC located in the Inside zone sent a ping to PC Amazon in the Outside zone.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 3.49.26.5

Pinging 3.49.26.5 with 32 bytes of data:

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

Ping statistics for 3.49.26.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100%
loss),

C:\>
```

Figure 32 ping from Birzeit tablet to PC Amazon.

8 Conclusion

The main objectives of configuring the ASA firewall, establishing secure network zones, implementing NAT and ACLs, and enabling secure wireless connectivity were successfully met. The expected results were achieved, with secure and controlled communication being established between the network segments. Important security principles, including the use of ACLs to manage access, the application of stateful inspection, and the integration of dynamic addressing through DHCP, were thoroughly understood and applied. The experiment reinforced the significance of firewalls in safeguarding network environments and highlighted the role of proactive security policies in protecting sensitive data and resources.

9 Feedback

The experiment was found to be highly educational and provided a practical demonstration of firewall security configurations. It allowed for the application of theoretical concepts, such as ACLs and NAT, in a simulated environment. However, it was felt that the allocated lab time was somewhat limited, as additional time would have been beneficial for addressing troubleshooting issues and exploring the configurations in greater depth. Despite this, the overall learning experience was valuable and relevant to real-world security practices.

10 References

[1] https://computer.howstuffworks.com/firewall.htm. [Accessed on 25th May at 3:50 PM]]

[2] https://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/index.html[Accessed on 25th May at 4:30 PM]]

[3] Lab Manual: Cisco ASA Firewall Configuration (ENCS4130).[Accessed on 25th May at 6:00 PM]

[4] https://www.techtarget.com/searchsecurity/definition/DMZ [Accessed on 26th May at 2:10 PM]]

[5] https://www.uninets.com/blog/what-is-nat-network-address-translation [Accessed on 26th May at 2:50 PM]

[6] https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/16412-pix-pat.html [Accessed on 26th May at 3:25 M]

[7] https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/118659-technote-nat-00.html. [Accessed on 26th May at 4:05 PM]]