Faculty of Engineering and Technology
Electrical and Computer Engineering Department
ENCS4130 – Computer Network Laboratory

Experiment No. 10

Cisco ASA Firewall Configuration

■ Objectives

(a) Learn how to configure a Cisco adaptive security appliance (ASA) firewall.

(b) Learn how to set up network address translation (NAT).

(c) Learn how to configure an access point to provide wireless connectivity.

■ Requirements

(a) Cisco Packet Tracer software.

(b) One ASA firewall.

(c) Two routers.

(d) Three switches.

(e) One wireless access point.

(f) Four servers (two Web and two DNS servers).

(g) Two PCs, one laptop, one tablet, one smartphone, and one printer.

10.1 Introduction

A firewall is a network security device that ***inspects data packets*** and determines whether to allow or block them according to configured security rules. These rules can be based on several factors, including source and destination IP addresses, port numbers, and protocol types. Its primary function is to ***create a protective barrier*** between a *trusted internal network* and *untrusted external networks*.

By enforcing these controls, firewalls help prevent unauthorized access and protect against various threats such as hackers, bots, and malware attempting to infiltrate or overwhelm a private network. Without this safeguard, malicious actors could freely exploit the system and compromise sensitive information.

Firewalls can be implemented as either software or hardware (or a combination of both) and come in various forms, including:

- **Packet-Filtering Firewalls:** These analyze packets of data being sent to or from a network and allow or block them based on a set of rules, such as IP addresses, ports, or protocols.
- **Stateful Inspection Firewalls:** These track the state of active connections and make decisions based on the context of the traffic, not just individual packets.
- **Proxy Firewalls:** These act as intermediaries between the internal network and the Internet, making requests on behalf of users and then forwarding the responses back to them.
- **Next-Generation Firewalls:** These offer more advanced features, such as application awareness, intrusion prevention systems, and deep packet inspection, to provide more comprehensive security.
- **Cloud Firewalls:** These are hosted in the cloud and are typically used to protect cloud-based infrastructure and services.

10.1.1 Cisco Adaptive Security Appliance (ASA)

The Cisco ASA is a versatile network security device that integrates multiple security functions into a single platform. These include a ***firewall***, ***antivirus***, ***intrusion prevention***, and ***virtual private network (VPN)*** capabilities. In this lab, the ASA will be employed to demonstrate how such a device can provide **proactive threat defense** by stopping unauthorized access before threats can spread within the network.

By default, the Cisco ASA ***blocks all inbound traffic*** from external networks, creating a secure perimeter around the internal network. Despite this strict default posture, the ASA is equipped with *advanced traffic inspection capabilities* that allow it to recognize and permit legitimate connections based on customizable security policies. These policies can be tailored to allow specific types of traffic while maintaining strong security controls.

A) Demilitarized Zone (DMZ)

A key feature of the ASA firewall is its ability to create a DMZ, as illustrated in Figure 1. A DMZ is a logically or physically isolated subnetwork positioned between an organization's internal network and external, untrusted networks such as the Internet. Services

that require external access, such as domain name system (DNS), file transfer protocol (FTP) servers, web servers, and proxy servers, are typically placed within the DMZ. This setup allows for secure interaction with external networks while safeguarding the internal local area network (LAN). Essentially, the DMZ acts as a buffer zone, enabling controlled access to public-facing services while preventing direct exposure of internal systems.

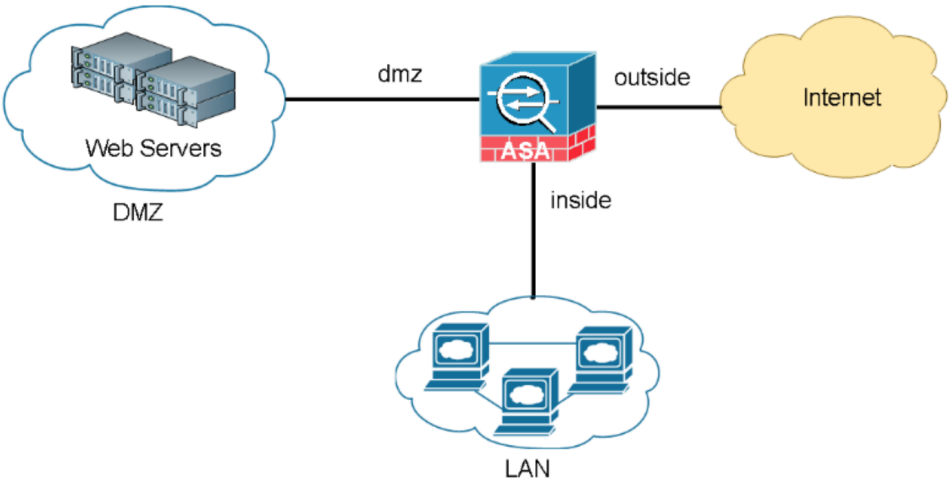

Figure 1: Organizational network overview featuring Cisco ASA as the security gateway.

B) Network Address Translation (NAT)

NAT is a key feature of the Cisco ASA firewall that enables secure and efficient communication between internal (private) and external (public) networks. NAT works by ***translating private IP addresses into public ones***, as illustrated in Figure 2. This process hides internal IP addresses from external users, helping to *prevent direct attacks on internal devices* and *preserve the limited pool of public IP addresses.*

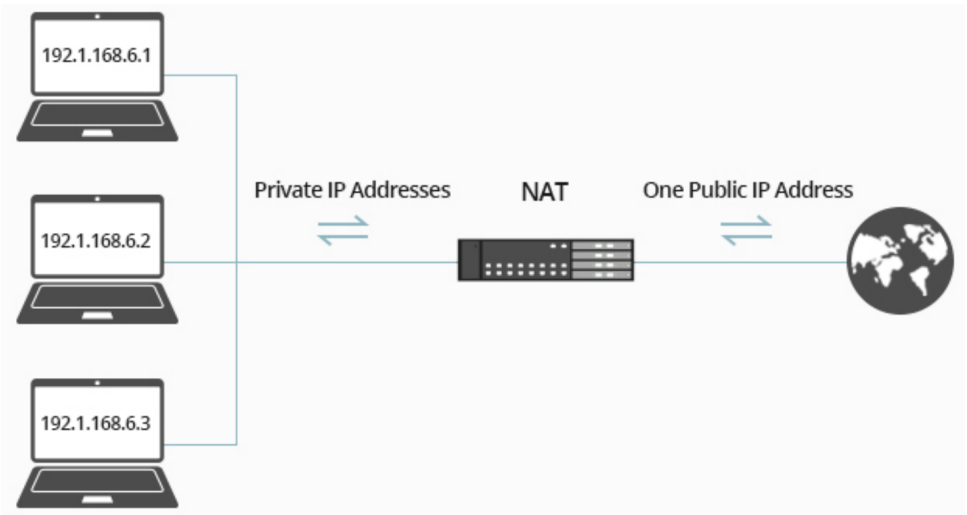

Figure 2: Overview of NAT.

Cisco ASA supports multiple NAT types, each suited to different networking needs:

1. **Static NAT:** Maps a single private IP address to a single public IP address. This is

commonly used for devices such as web and DNS servers that must be consistently reachable from the Internet.

2. **Dynamic NAT:** Maps private IP addresses to public IP addresses from a predefined pool. It is useful when multiple internal hosts need occasional external access.
3. **Port Address Translation (PAT)** (also known as NAT Overload)**:** Maps multiple private IP addresses to a single public IP address using unique port numbers for each session. This is the most efficient type of NAT and is widely used to conserve public IPs.

C) Configuration of Cisco ASA Firewall

Configuring a Cisco ASA firewall typically involves defining network interfaces, assigning security levels, NAT, and applying access control policies. The following is a general structure for setting up a Cisco ASA firewall with DMZ and NAT using the standard command syntax.

1. **Configure Interfaces and Security Zones**
   Assign a logical name, security level, and IP address to the ASA interface, and enable it.

```
ciscoasa(config)# interface <interface-name>
ciscoasa(config-if)# nameif <zone-name>
ciscoasa(config-if)# security-level <security-level>
ciscoasa(config-if)# ip address <ip-address>
                     <subnet-mask>
ciscoasa(config-if)# no shutdown
```

   - `<interface-name>`: The hardware interface identifier (e.g., `Fa0/0`, `Gig1/2`).
   - `<zone-name>`: Logical name for the interface (e.g., `inside`, `outside`, `dmz`). This simplifies configuration by allowing you to reference the interface by name instead of its physical identifier.
   - `<security-level>`: A numeric value from `0` to `100` that represents the trust level of the interface—the higher the value, the more trusted the network. Typically, `inside = 100` (most trusted), `dmz = 50` (moderately trusted), and `outside = 0` (least trusted).
   - `<ip-address>` and `<subnet-mask>`: IP configuration for the interface.

2. **Configure PAT**
   Translate internal (private) IPs to a public IP.

```
ciscoasa(config)# object network <object-name>
ciscoasa(config-network-object)# subnet <private-ip>
                                 <subnet-mask>
ciscoasa(config-network-object)# nat (<in-if>, <out-if>)
                                 dynamic interface
```

- `<object-name>`: A descriptive name for the network object (e.g., `INTERNAL-PAT`). This name simplifies configuration by allowing you to reference the object by name—rather than repeating full IP addresses or subnet definitions—across different settings such as NAT and access control lists (ACLs).
- `<private-ip>` and `<subnet-mask>`: Internal network IP address and mask.
- `<in-if>`: Interface name for the internal zone (e.g., `inside`).
- `<out-if>`: Interface name for the external zone (e.g., `outside`).

3. **Configure Static NAT**
Map a specific internal host to a fixed public IP address.

```
ciscoasa(config)# object network <object-name>
ciscoasa(config-network-object)# host <private-ip>
ciscoasa(config-network-object)# nat (<in-if>, <out-if>)
                                  static <public-ip>
```

- `<private-ip>`: Internal host IP address.
- `<public-ip>`: Assigned public IP address for external access.

4. **Enabling Legitimate Traffic Flow from Lower to Higher Security Levels**
In a Cisco ASA firewall, *traffic from a higher to a lower security level* (e.g., `inside` → `outside`) *is allowed by default*. However, to allow traffic from a lower to a higher security level, such as external access to web and DNS services in the DMZ from the Internet (i.e., `outside` → `dmz`), you must explicitly permit the traffic using ACLs.

Use the `access-list` command to specify the type of traffic you want to allow:

```
ciscoasa(config)# access-list <acl-name> extended permit
                  <protocol> <src-addr> <dst-addr>
```

- `<acl-name>`: Name of the access control list (e.g., `OUTSIDE-ACCESS`).
- `<protocol>`: Protocol to permit (e.g., `tcp`, `udp`, `icmp`, or `ip` for all).
- `<src-addr>`: Source IP address or network.
- `<dst-addr>`: Destination IP address or network.

Then, use the `access-group` command to bind the ACL to an interface in a specific direction:

```
ciscoasa(config)# access-group <acl-name> <in|out>
                  interface <interface-name>
```

- `<in|out>`: Direction of traffic relative to the interface.
- `<interface-name>`: Interface where the ACL is applied (e.g., `outside`).

The ASA firewall permits traffic initiated from the internal LAN to the DMZ or the Internet by default, since the LAN has a higher security level. However, if this traffic is a request—such as an HTTP request or a DNS query—the corresponding

response (e.g., HTTP response or DNS reply) would be blocked by default, as it originates from a lower security level returning to a higher one.

Fortunately, the ASA firewall is **stateful**, meaning it can track and allow return traffic if it ***inspects*** the connection. By default, the ASA inspects some protocols like **FTP**, **DNS**, and **TFTP** using a **global policy map** named `global_policy` and a **class map** named `inspection_default`. To enable inspection of additional protocols such as **HTTP**:

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http
```

This configuration ensures that return traffic (e.g., HTTP responses) is allowed, maintaining secure and functional two-way communication.

5. **Configure Static Route**
Define a default route or a route to a specific destination network to ensure that the ASA firewall knows how to forward traffic destined for external networks.

```
ciscoasa(config)# route <interface-name> <dst-network>
                  <subnet-mask> <next-hop-ip-address>
```

- `<interface-name>`: Outbound interface for the route (e.g., `outside`).
- `<dst-network>`: Destination network address (e.g., `0.0.0.0` for default route).
- `<subnet-mask>`: Mask for the destination (e.g., `0.0.0.0` for default).
- `<next-hop-ip-address>`: Next-hop router's IP address.

6. **Configure DHCP**
In Cisco ASA, the DHCP server is **interface-specific**, meaning it must be explicitly enabled on each interface where IP address assignment is required. The DHCP service allows the ASA to automatically assign IP addresses and related configuration to devices within a designated network zone.

```
ciscoasa(config)# dhcpd address <start-ip>-<end-ip>
                  <interface-name>
ciscoasa(config)# dhcpd dns <dns-server-ip>
ciscoasa(config)# dhcpd enable <interface-name>
```

- `<start-ip>-<end-ip>`: Specifies the range of IP addresses to be assigned to DHCP clients (e.g., `172.17.X.3 - 172.17.X.20`).
- `<interface-name>`: Logical name of the interface on which the DHCP service is enabled (e.g., `inside`, `dmz`).
- `<dns-server-ip>`: DNS server IP to be provided to DHCP clients.

Note:

The IP address assigned to `<interface-name>` will automatically be used as the ***default gateway*** for DHCP clients on that network segment.

10.2 Procedure

In this lab, we will configure a Cisco ASA 5506-X firewall alongside routers, switches, and multiple end devices distributed across different network zones. The ASA will function as a DHCP server for the internal network, while the DMZ will host public-facing services assigned static IP addresses. NAT will be implemented to securely enable internal clients to access external networks and to map DMZ servers to public IPs. Firewall rules will govern traffic flow between the internal network, DMZ, and external network to ensure secure communication. Additionally, the open shortest path first (OSPF) will be used for dynamic routing within the same autonomous system (AS), and the border gateway protocol (BGP) will be configured for routing between different ASes.

10.2.1 Building the Topology

Construct the network topology shown in Figure 3, which consists of the following devices:

- Firewall: From "*Network Devices - Security*", use **5506-X**.
- Routers: Use **Router-PT**.
- Switches: Use **Switch-PT**.
- Access point: From "*Network Devices - Wireless Devices*", use **AccessPoint-PT**.
- Servers, PCs, Laptop, Tablet, Smartphone, and Printer: From "*End Devices*", use **Server-PT**, **PC-PT**, **Laptop-PT**, **TabletPC-PT**, **SMARTPHONE-PT**, and **Printer-PT**.
- Use the "**Automatically Choose Connection Type**" to connect devices.

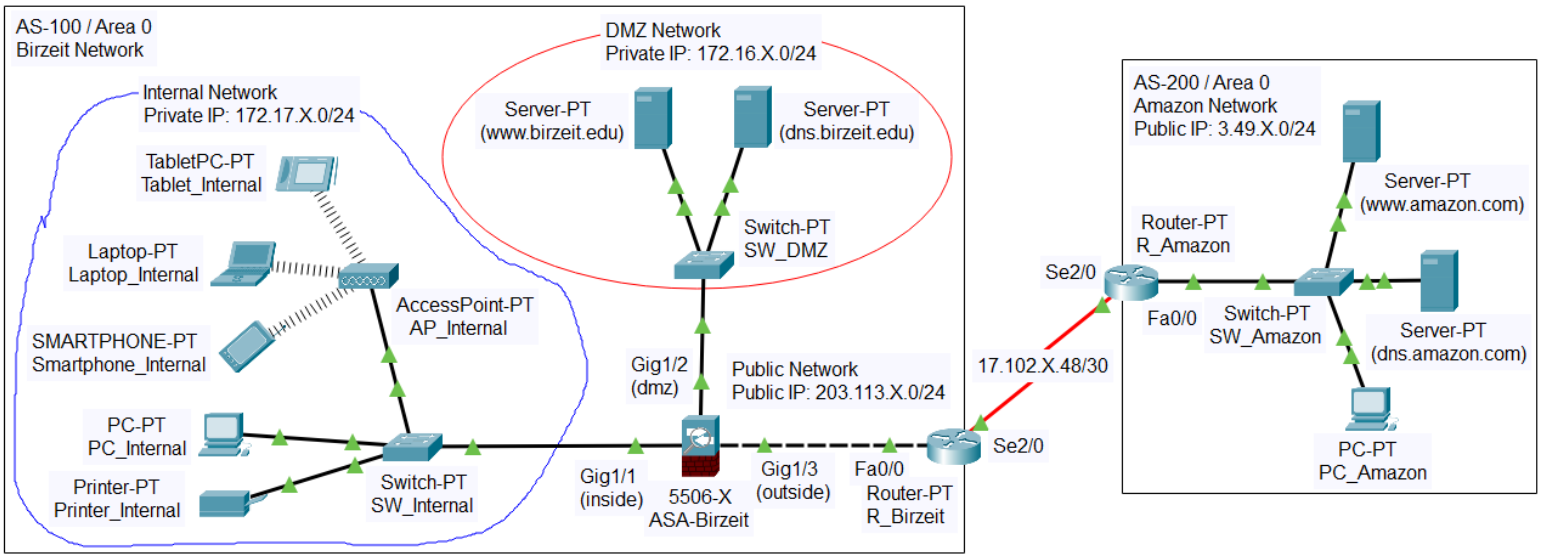

Figure 3: Firewall topology.

10.2.2 Routers Configuration

A) Configuring the Routers' Interfaces

Set up the interfaces on the **R_Birzeit** router using the following commands:

```
R_Birzeit(config)# interface FastEthernet0/0
R_Birzeit(config-if)# ip address 203.113.X.2 255.255.255.0
R_Birzeit(config-if)# no shutdown
```

```
R_Birzeit(config)# interface Serial2/0
R_Birzeit(config-if)# ip address 17.102.X.49 255.255.255.252
R_Birzeit(config-if)# no shutdown
```

Configure the **R_Amazon** router similarly, using its designated IP addresses.

B) Configuring OSPF and BGP Routing Protocols

On **R_Birzeit**, configure OSPF with process ID `1` to advertise the public network and redistribute BGP routes into OSPF:

```
R_Birzeit(config)# router ospf 1
R_Birzeit(config-router)# network 203.113.X.0 0.0.0.255
                          area 0
R_Birzeit(config-router)# redistribute bgp 100 subnets
```

Next, configure BGP by specifying the eBGP neighbor (**R_Amazon**) and redistributing OSPF routes into BGP:

```
R_Birzeit(config)# router bgp 100
R_Birzeit(config-router)# neighbor 17.102.X.50 remote-as 200
R_Birzeit(config-router)# redistribute ospf 1
```

Repeat the same configuration steps on **R_Amazon**, adjusting for its internal network, AS number, and the appropriate neighbor IP.

10.2.3 Servers Configuration

Configure the Web and DNS servers for both the Birzeit and Amazon networks as described in **Experiment No. 6**.

A) Birzeit Web Server (`www.birzeit.edu`)

- Assign a static IP configuration, as shown in Figure 4.
- Enable HTTP and HTTPS (Secure HTTP) protocols.
- Customize the `index.html` page to display the title: "**Birzeit University**".

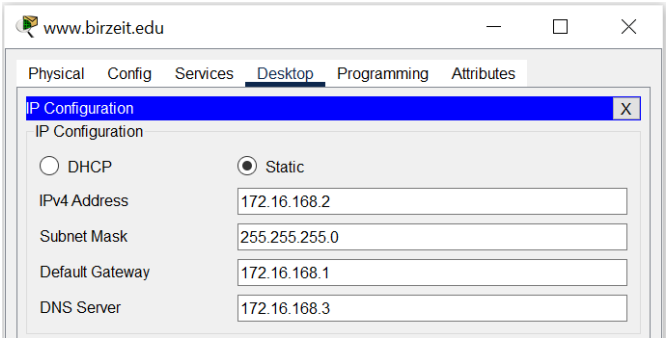

Figure 4: IP configuration of Birzeit Web server.

B) Birzeit DNS Server (`dns.birzeit.edu`)

- Assign a static IP configuration.
- Enable only the DNS service.
- Add the resource records listed in Table 1, as illustrated in Figure 5.

Table 1: Resource records in Birzeit DNS server.

Name	Value	Type
`www.birzeit.edu`	The IP address of the `www.birzeit.edu` server	A
`dns.amazon.com`	The IP address of the `dns.amazon.com` server	A
`amazon.com`	`dns.amazon.com`	NS

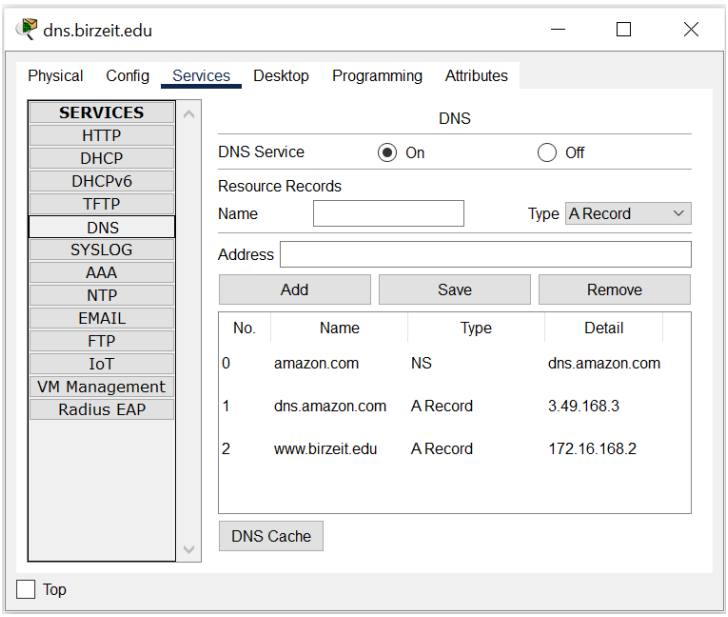

Figure 5: DNS service configuration of Birzeit DNS server.

C) Amazon Web Server (`www.amazon.com`)

- Assign a static IP configuration.
- Enable HTTP and HTTPS (Secure HTTP) protocols.

- Customize the `index.html` page to display the title: "**Amazon E-commerce Company**".

D) Amazon DNS Server (`dns.amazon.com`)

- Assign a static IP configuration.
- Enable only the DNS service.
- Add the resource records listed in Table 2, as illustrated in Figure 6.

Table 2: Resource records in Amazon DNS server.

Name	Value	Type
`www.amazon.com`	The IP address of the `www.amazon.com` server	A
`dns.birzeit.edu`	The **public** IP address of the `dns.birzeit.edu` server	A
`birzeit.edu`	`dns.birzeit.edu`	NS

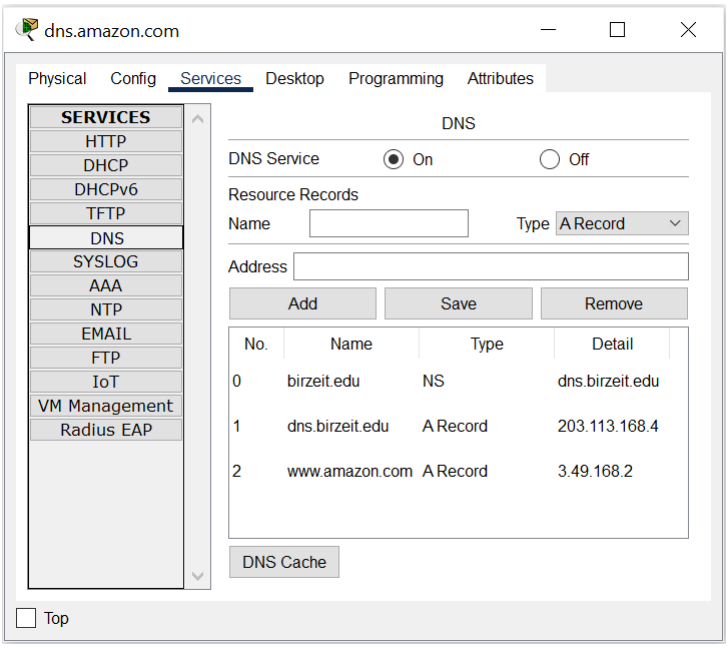

Figure 6: DNS service configuration of Amazon DNS server.

10.2.4 ASA Firewall Configuration

A) Configuring Privileged Mode Password

The default password for the privileged mode on the ASA firewall is the **blank**. So, when requested for the privileged mode password, just press the **Enter** key. The following commands change the password to "`encs4130`":

```
ASA-Birzeit> enable
Password:
ASA-Birzeit# configure terminal
ASA-Birzeit(config)# enable password encs4130
```

B) Configuring Interfaces and Security Zones

Each ASA interface must be configured with a name, security level, IP address, and enabled. The recommended security levels and roles for the Birzeit network are as follows:

- **Inside (Sec Level 100):** Represents the most trusted zone, Birzeit's internal network.
- **DMZ (Sec Level 50):** A semi-trusted zone that hosts externally accessible servers.
- **Outside (Sec Level 0):** The untrusted zone connected to the public Internet.

To configure the `inside` interface (internal network):

```
ASA-Birzeit(config)# interface Gig1/1
ASA-Birzeit(config-if)# nameif inside
ASA-Birzeit(config-if)# security-level 100
ASA-Birzeit(config-if)# ip address 172.17.X.1 255.255.255.0
ASA-Birzeit(config-if)# no shutdown
```

Repeat the same steps to configure the `outside` and `dmz` interfaces using the appropriate interface names, security levels, and IP addresses.

C) Configuring PAT for the Internal Network

PAT enables the devices in Birzeit internal network to share a single public IP address when accessing the Internet. To map all internal devices in the `172.17.X.0/24` subnet to the ASA firewall's `outside` interface IP address, use the following configuration:

```
ASA-Birzeit(config)# object network INTERNAL-PAT
ASA-Birzeit(config-network-object)# subnet 172.17.X.0
                                    255.255.255.0
ASA-Birzeit(config-network-object)# nat (inside,outside)
                                    dynamic interface
```

D) Configuring Static NAT for the DMZ Network

To make DMZ servers accessible from external networks, static NAT is used to map each private IP address to a public IP address from the `203.113.X.0/24` subnet. Since `203.113.X.1` is assigned to the ASA's `outside` interface and `203.113.X.2` is used by the **R_Birzeit** router, public IP assignments begin from `203.113.X.3`.

To configure static NAT for the Web server (Private IP: `172.16.X.2`, Public IP: `203.113.X.3`), use the following commands:

```
ASA-Birzeit(config)# object network DMZ-WEB-NAT
ASA-Birzeit(config-network-object)# host 172.16.X.2
ASA-Birzeit(config-network-object)# nat (dmz,outside) static
                                    203.113.X.3
```

Repeat these steps to configure static NAT for the **DNS** server, using the appropriate object name, private IP, and public IP addresses.

E) Enabling External Access to DMZ Servers

To allow external users to access Web and DNS services hosted in the DMZ, create an ACL that permits the required traffic from external networks to the DMZ servers.

```
ASA-Birzeit(config)# access-list OUTSIDE-ACCESS extended
                     permit tcp any host 172.16.X.2 eq www
ASA-Birzeit(config)# access-list OUTSIDE-ACCESS extended
                     permit udp any host 172.16.X.3 eq domain
```

Then, apply the `OUTSIDE-ACCESS` ACL to the `outside` interface:

```
ASA-Birzeit(config)# access-group OUTSIDE-ACCESS in interface
                     outside
```

Note:

This access list is applied `inbound` on the `outside` interface to control traffic from external users. It ensures that only specific services, such as Web and DNS, are permitted to reach DMZ servers, while preventing any traffic directed to internal network. This enhances security by restricting unnecessary or unauthorized access.

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

The ASA firewall is stateful, meaning it can track connections and allow return traffic for inspected protocols. This prevents legitimate responses from the DMZ or the Internet to internal clients from being blocked.

By default, *DNS inspection is enabled*. To allow ***HTTP responses***, you must explicitly enable HTTP inspection by updating the **global policy map** using the following commands:

```
ASA-Birzeit(config)# policy-map global_policy
ASA-Birzeit(config-pmap)# class inspection_default
ASA-Birzeit(config-pmap-c)# inspect http
```

Repeat the same steps to enable inspection for **ICMP**, allowing replies (e.g., ping responses) from the DMZ or Internet to reach the internal clients that initiated the requests.

G) Configuring Default Routing

To enable Internet access for internal and DMZ devices, configure a default route that forwards all external traffic to the **R_Birzeit** router.

```
ASA-Birzeit(config)# route outside 0.0.0.0 0.0.0.0
                     203.113.X.2
```

Note:

The destination **0.0.0.0 0.0.0.0** represents any IP address with any subnet mask. This means that any traffic not matched by a more specific route will be forwarded to the next-hop IP address `203.113.X.2` via the ASA's `outside` interface.

H) Configuring ASA as a DHCP Server for the Internal LAN

To enable dynamic IP address allocation for internal LAN devices, configure the ASA to act as a DHCP server on the `inside` interface. Since `172.17.X.1` is reserved for the `inside` interface and the printer requires a static IP configuration (e.g., `172.17.X.2`) for consistent access, define a DHCP address pool of `100` addresses—sufficient for typical internal use—starting from `172.17.X.3`. Also, specify the DNS server (e.g., `172.16.X.3`) in the DHCP configuration.

```
ASA-Birzeit(config)# dhcpd address 172.17.X.3-172.17.X.102
                     inside
ASA-Birzeit(config)# dhcpd dns 172.16.X.3
ASA-Birzeit(config)# dhcpd enable inside
```

10.2.5 Access Point Configuration

The access point provides wireless connectivity within the internal network. To configure the wireless network, go to the "**Config**" tab and set the access point with the following parameters, as shown in Figure 7:

- **Name:** `BZU-WiFi`
- **Security Model:** `WPA2-PSK`
- **Pre-Shared Key (PSK):** `EnCs4130`, wireless devices must enter this key to connect to the access point.
- **Encryption Type:** `AES`

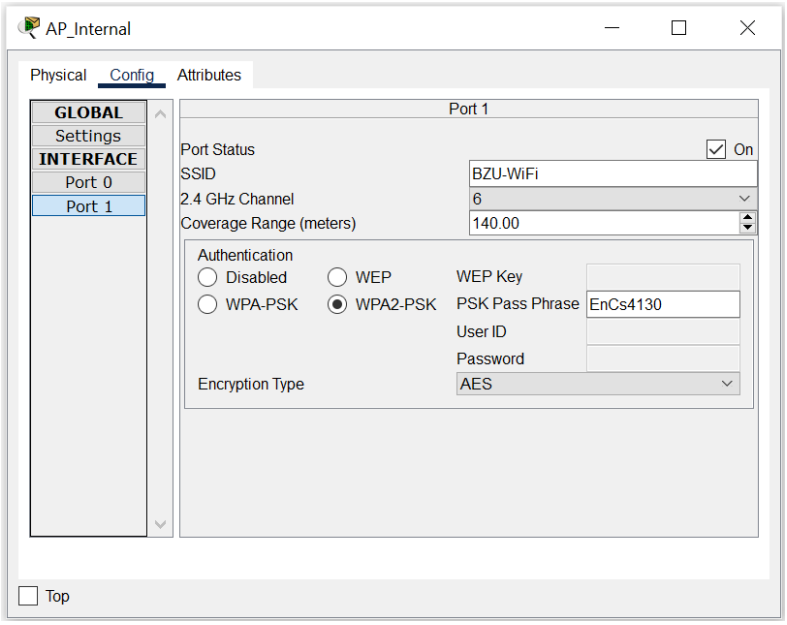

Figure 7: Configuring the access point for Birzeit internal network.

10.2.6 Connecting Wireless Devices and Configuring Dynamic IP Addresses

The tablet, laptop, and smartphone connect wirelessly to the internal network through the access point. However, unlike the tablet and smartphone, the *laptop does not have a*

built-in wireless interface. To enable wireless connectivity, you must replace the laptop's wired LAN module with a **WPC300N wireless adapter**.

Follow these steps to install the wireless module on the laptop:

1. Click on the laptop and navigate to the "**Physical**" tab.
2. Turn off the device and remove the existing FastEthernet module.
3. Insert the **WPC300N** wireless adapter from the module list.
4. Power the laptop back on to activate the new module.

Figure 8 illustrates how to connect the laptop to the "`BZU-WiFi`" network and configure it to obtain an IP address dynamically.

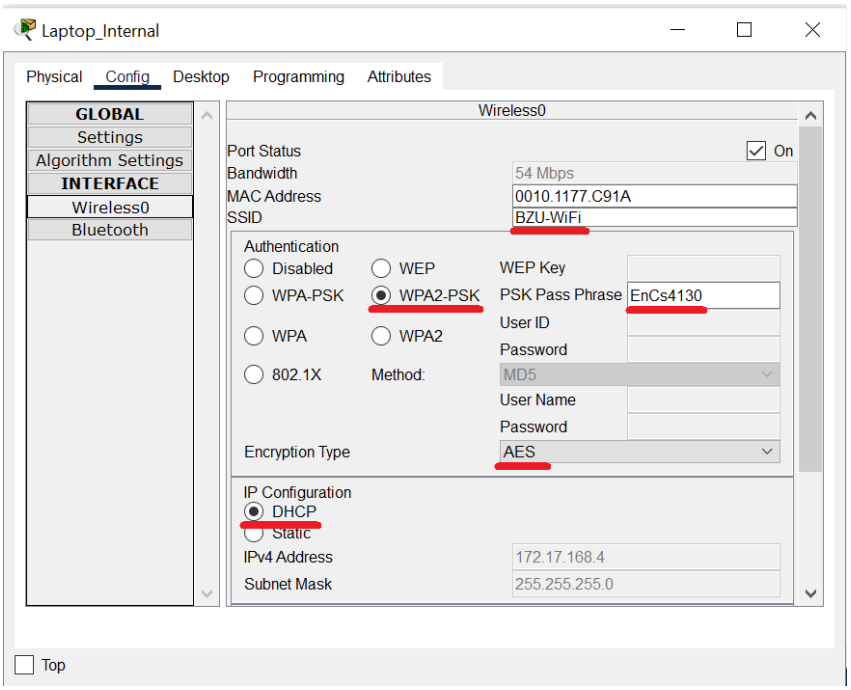

Figure 8: Connecting the laptop to `BZU-WiFi` and enabling dynamic IP configuration.

Repeat the same steps for the **smartphone** and **tablet** to connect them to the wireless network and assign them dynamic IP addresses.

Also, configure the **PC_Internal** to use dynamic IP addressing.

10.2.7 Configuring End Devices with Static IP Addresses

The **Printer_Internal** and **PC_Amazon** are configured with **static IP addresses**, including their **default gateway** and **DNS server** settings. Each device must have a unique IP address within the valid host range of its subnet.

Figure 9 shows the Printer's configuration.

Next, configure the **PC_Amazon** to use a static IP address.

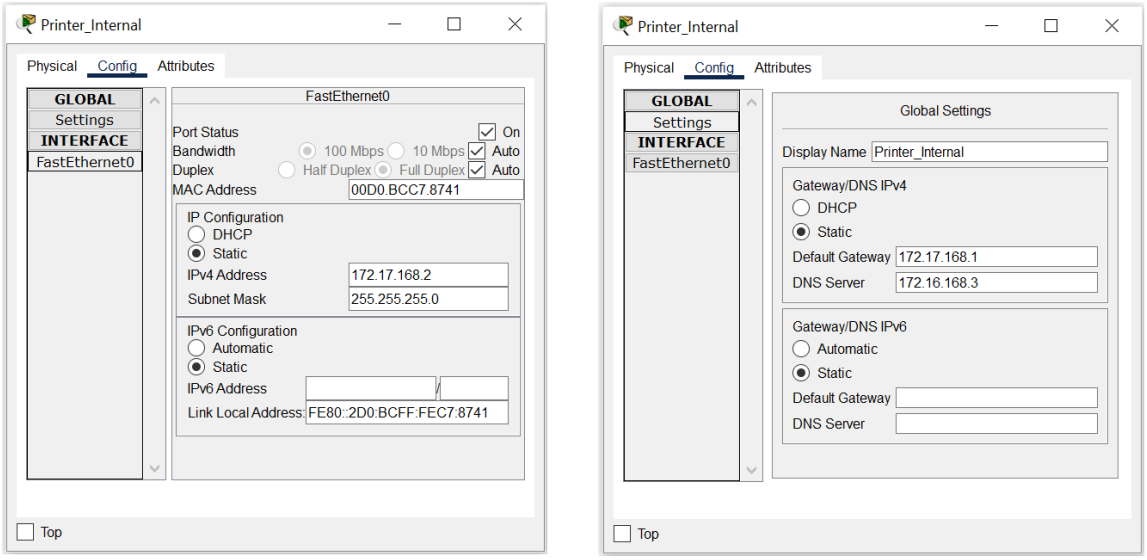

Figure 9: Configuring the Printer.

10.3 Testing Connectivity

To verify end-to-end functionality of DNS resolution and HTTP access between the Internet (Amazon), the DMZ, and the Birzeit internal network, perform the following tests:

- **Test 1 – Accessing "`www.birzeit.edu`" from PC_Amazon (Internet):**

  From the PC in the Amazon (Internet) network, attempt to access the DMZ web server using the domain name "`www.birzeit.edu`", as shown in Figure 10.

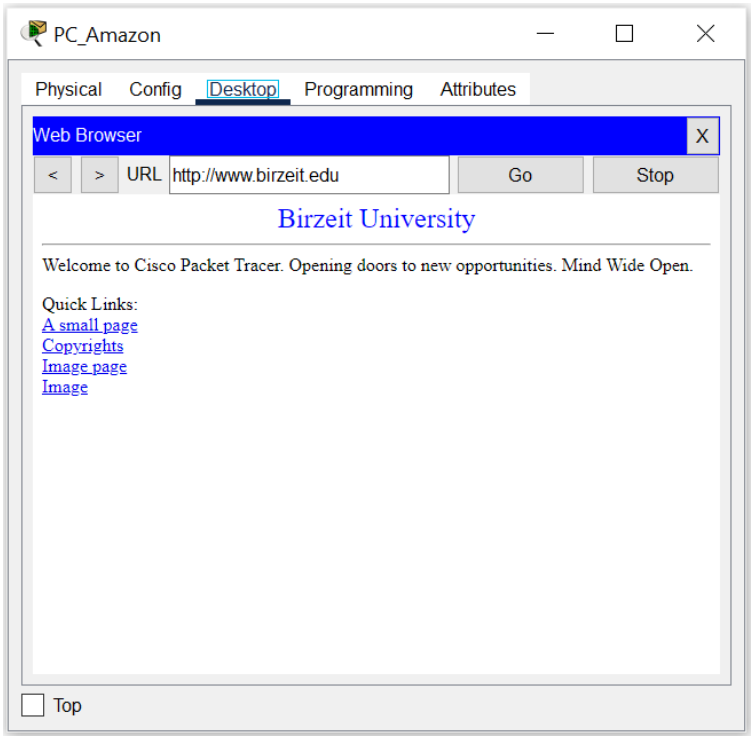

Figure 10: Accessing "`www.birzeit.edu`" from Amazon network.

The DNS query is forwarded to "`dns.birzeit.edu`" via Amazon's DNS server using an `NS` record. The `A` record for "`www.birzeit.edu`" resolves to the private IP address of the Birzeit web server. The ASA firewall translates this private IP to its corresponding public IP address, which is then used to send the HTTP request to the DMZ server.

- **Test 2 – Accessing "`www.amazon.com`" from Smartphone (Birzeit Internal Network):**

  From the Smartphone connected to the Birzeit internal wireless network, try to access "`www.amazon.com`", as shown in Figure 11.

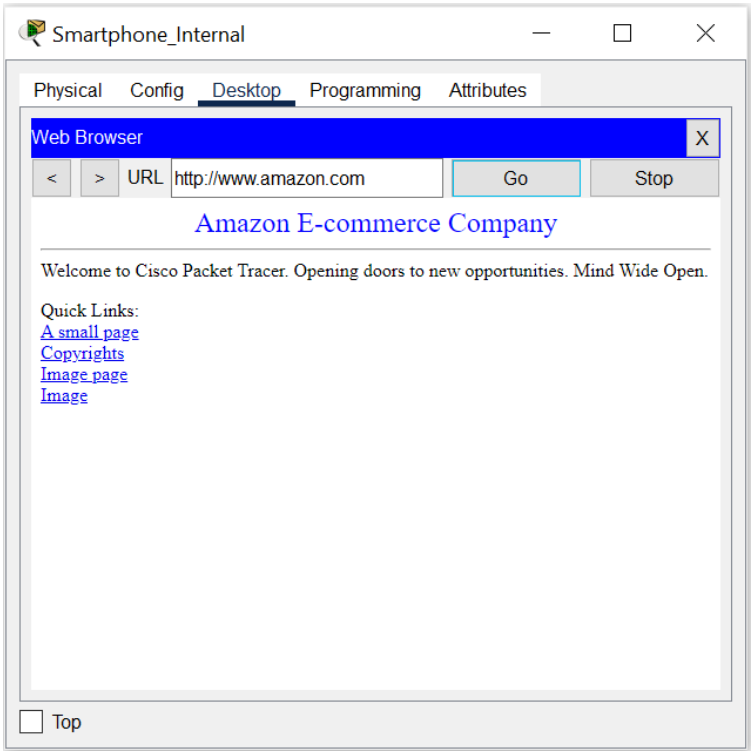

Figure 11: Accessing "`www.amazon.com`" from Birzeit internal network.

The DNS query is sent to "`dns.birzeit.edu`", which forwards it to "`dns.amazon.com`" using an `NS` record. The `A` record for "`www.amazon.com`" resolves to the appropriate IP address. The HTTP request is then sent to the Amazon web server. The ASA inspects the DNS and HTTP traffic to ensure the request is permitted and the response is delivered to the smartphone.

- **Test 3 – Pinging a Host in Birzeit Network from PC_Amazon (Internet):**

  Attempting to send ICMP packets (ping) to a device within the Birzeit network from the Amazon PC will fail, as shown in Figure 12. This is due to the ASA firewall's default security policy, which blocks traffic initiated from a lower security level (e.g., the Internet) to a higher security level (e.g., the internal network), unless explicitly permitted.

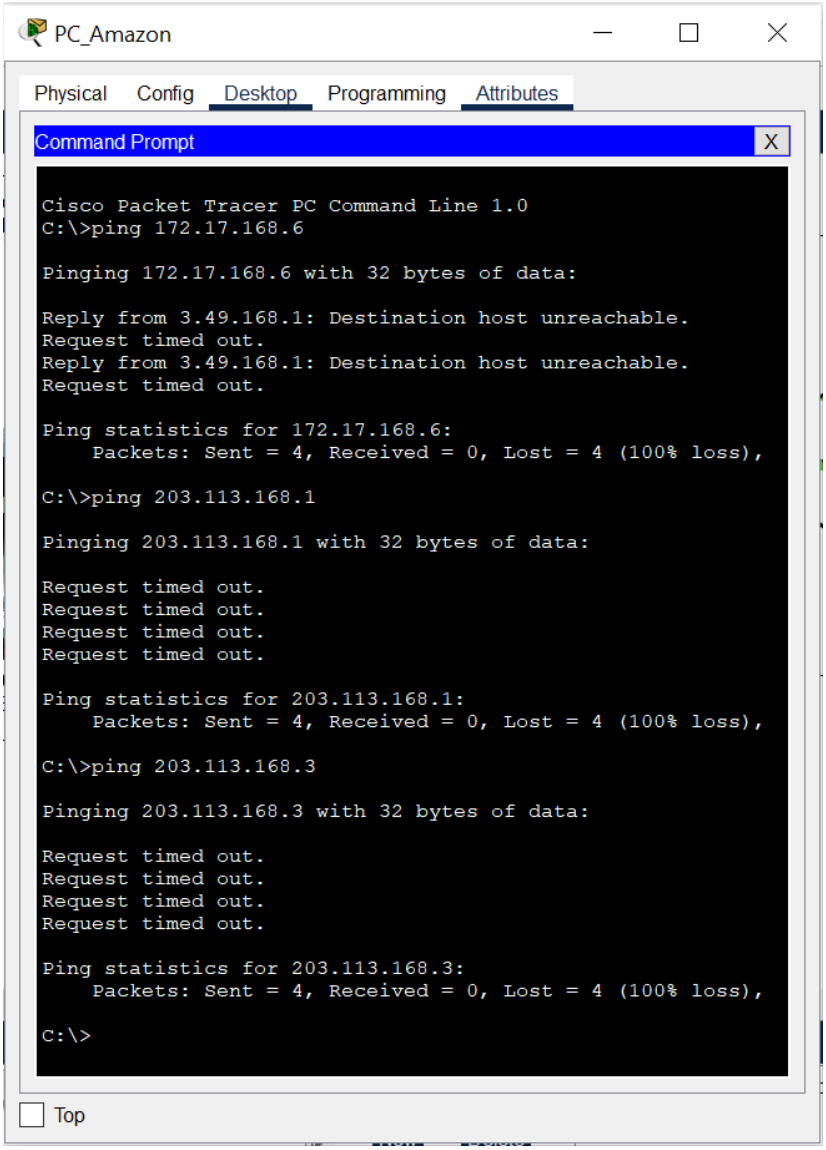

Figure 12: Blocked attempt from Internet to Birzeit internal network.

- **Test 4 – Pinging PC_Amazon (Internet) from a Host in Birzeit Network:**

  From the tablet in the Birzeit internal network, send ICMP packets (ping) to the Amazon PC, as shown in Figure 13. This traffic is allowed by default, as the ASA permits outbound connections from higher to lower security levels. Because ICMP inspection is enabled on the ASA, the ping replies from the Internet (lower security level) back to the internal network (higher security level) are also allowed.

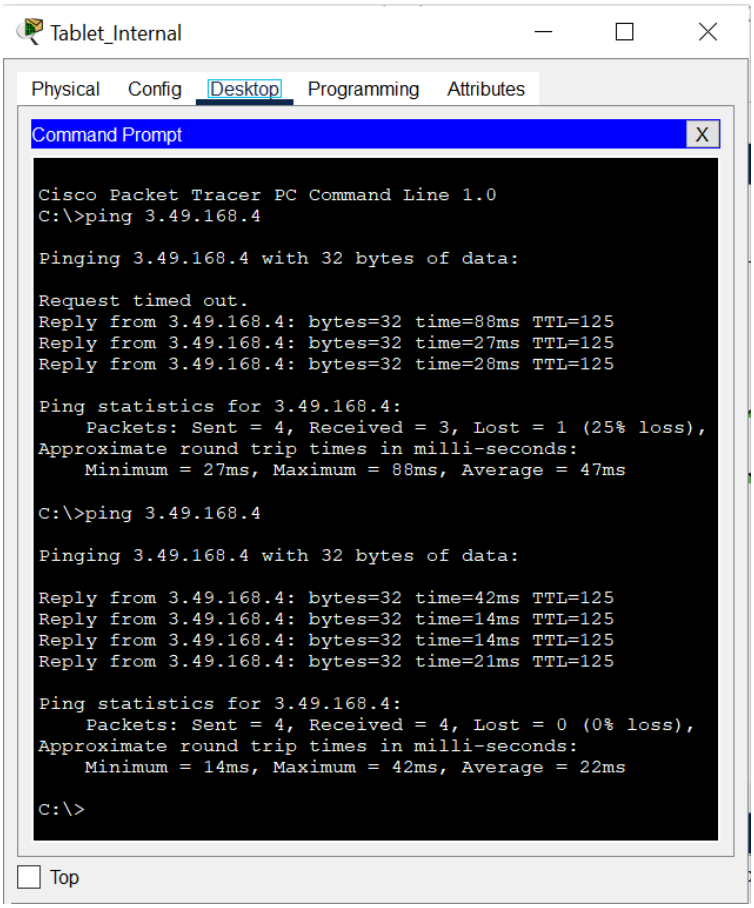

Figure 13: Allowed attempt from Birzeit internal network to Internet.

Important:

To reinforce your understanding of DNS resolution, HTTP access, ICMP behavior, and firewall operations, **try each of the above test cases using Cisco Packet Tracer's Simulation Mode**. This allows you to observe packet flow, inspect protocol exchanges (such as DNS queries, HTTP requests, and ICMP echo messages), and visualize how the ASA firewall handles traffic between different network zones. Exploring these scenarios interactively will help solidify key networking concepts.

10.4 ToDo

This section will be provided by the instructor.