ETI 2508: NETWORK DESIGN AND MANAGEMENT_LABORATORY EXERCISES_LAB 3
BSC. TELECOMMUNICATION AND INFORMATION ENGINEERING 5TH YEAR 2023

STUDENT NAME	REG. NUMBER
VICTOR NZIA	ENE221-0270/2018
JOSHUA ODHIAMBO	ENE221-0134/2018
PATIENCE SIMIYU	ENE 221-0110/2018
OWEN ONDIEKI	ENE221-0133/2018
BRIAN MAIYO	ENE221-0285/2018
DOMINIC SAKWA	ENE221-0121/2018

PART A

Introduction

This laboratory session focused on enhancing the security of Cisco IOS-based routers, a critical aspect in computer networking operations. The primary objective was to initiate the process of "hardening" routers to establish a foundation for a secure network. This lab report summarizes the key activities performed during the session.

The laboratory exercise comprised three distinct security stages, each addressing crucial aspects of router security. In Security Stage 1, the emphasis was on identifying and closing down unnecessary default services while enabling essential services to bolster router security. This stage aimed at reducing the potential attack surface by deactivating services like Cisco Discovery Protocol (CDP), TCP and UDP Small Servers, Finger, HTTP Server, BOOTP Server, Configuration Auto-loading, IP Source Routing, SNMP, Domain Name Lookup Service, TCP Keepalives, and Interface-based default services.

Following the completion of Security Stage 1, the focus shifted to Security Stage 2, which involved the application of passwords and password encryption to different router access components and modes. The measures taken included setting up a "Message of the Day" notification and configuring passwords for user mode, remote connections, and auxiliary interfaces.

The final security stage, Security Stage 3, addressed the encryption of routing protocols, specifically Open Shortest Path First (OSPF) [1]. Routers were configured to use the OSPF protocol with Area 0 authentication using message digest encryption.

Throughout the lab, the testing of basic network configurations was emphasized to ensure the correct functioning of the network before implementing security measures. Activities such as ping tests and trace route commands were executed to verify end-to-end connectivity and identify potential issues.

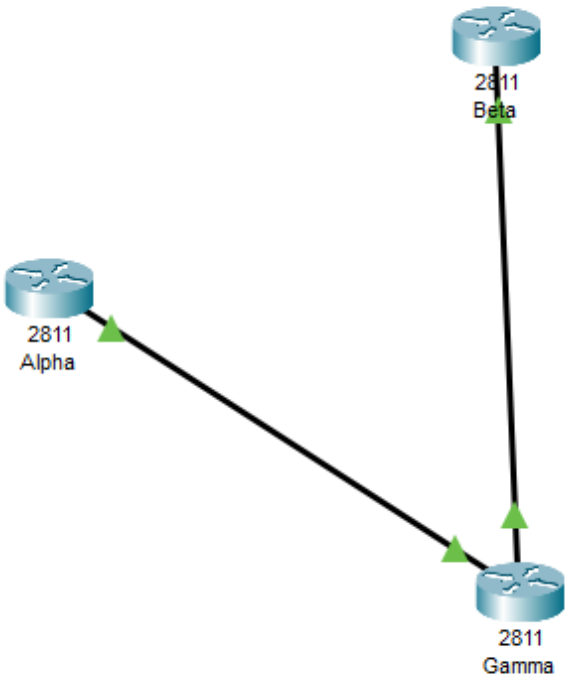
Objectives

1. To gain proficiency in configuring Cisco IOS routers to establish a foundation for secure network operation.
2. To evaluate the potential threats mitigated by each security measure and understand the rationale behind their implementation.

Procedure

The following is a summary of the steps we followed to complete the lab:

1. Network Setup and Basic Configuration: We initiated the lab by setting up a network as illustrated in the provided diagram. Following the provided IP scheme, we executed the basic configuration for routers Alpha, Beta, and Gamma, including the assignment of loopback and interface IP addresses.



2. Testing Basic Network Configuration: Before delving into security configurations, we performed essential tests to ensure the basic network was fully functional.
    - Using the console for router Alpha, we executed a ping command to the loopback interface of router Beta (ping 192.168.3.1) and verified the successful outcome.
    - Similarly, a ping command from the Beta console to the loopback interface of router Alpha (ping 192.168.1.1) confirmed end-to-end connectivity.
    - To visualize the path of ping packets, we utilized the trace command from Alpha to Beta (trace 192.168.3.1), ensuring proper functionality before proceeding.

```
Alpha#ping 192.168.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Alpha#
```

```
Beta>ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Beta>
```

```
Alpha#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms

Alpha#
```

```
Alpha#ping 192.168.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Alpha#trace 192.168.3.1
Type escape sequence to abort.
Tracing the route to 192.168.3.1

  1   10.0.0.2        0 msec    0 msec    0 msec
  2   10.0.0.5        1 msec    0 msec    0 msec
Alpha#
```

3. Security Stage 1: Identifying and Closing Unnecessary Services: We advanced to Security Stage 1 by entering global configuration mode on each router.
    - Commands were executed to disable unnecessary default services, including Cisco Discovery Protocol (CDP), TCP and UDP Small Servers, Finger, HTTP Server, BOOTP Server, Configuration Auto-loading, IP Source Routing, SNMP, Domain Name Lookup Service, TCP Keepalives, and Interface-based default services.
4. Security Stage 2: Applying Passwords and Encryption: Continuing to Security Stage 2, we established a "Message of the Day" notification using the banner motd command in global configuration mode.
    - Passwords for user mode, console, virtual terminal (telnet), and auxiliary interfaces were configured with the line console, line vty, and line aux commands.
    - To enhance security, the enable secret command was implemented in privileged mode, with the password "class" encrypted using MD5 encryption.
    - Password encryption for stored passwords in the configuration file was achieved using the service password-encryption command.

```
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
```

```
!
banner motd ^CTHIS ROUTER SHOULD BE ACCESSED BY AUTHORISED PERSONNEL ONLY !^C
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login
!
!
!
end


Beta#
```

5. Security Stage 3: Encrypting OSPF Routing Protocol: Transitioning to Security Stage 3, we encrypted the OSPF routing protocol to secure routing information exchanges.
    - Router OSPF configuration mode was accessed, and the area 0 authentication message-digest command was applied.
    - Authentication keys with the password "grape" were configured on each interface for OSPF using the ip ospf message-digest-key command.

```
Alpha>enable
Password:
Password:
Password:
Alpha#interface lo 0
                 ^
% Invalid input detected at '^' marker.

Alpha#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Alpha(config)#interface lo 0
Alpha(config-if)#
Alpha(config-if)#ip ospf message-digest-key 1 md5 grape
Alpha(config-if)#
Alpha(config-if)#interface fa0/0
Alpha(config-if)#
Alpha(config-if)#
Alpha(config-if)#ip ospf message-digest-key 1 md5 grape
Alpha(config-if)#
Alpha(config-if)#
```

```
Alpha#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/30 is directly connected, FastEthernet0/0
L       10.0.0.1/32 is directly connected, FastEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Loopback0
L       192.168.1.1/32 is directly connected, Loopback0

Alpha#
```

Discussion

After connection, the next step was testing the basic network configuration. Successful ping tests between routers Alpha and Beta, as well as Beta and Alpha, confirmed bidirectional communication. This is a fundamental prerequisite for a secure network, ensuring that routers can exchange data without hindrance. The positive results indicate that the basic network configuration, including IP addressing and routing, is correctly established. The trace route command provided insights into the routing path taken by packets between routers. This visualization is crucial for identifying any unexpected hops or potential issues in the network topology. The absence of anomalies in the trace route results validated the integrity of the routing configuration and the absence of disruptions.

After successful tests, we began securing our networks. The comprehensive approach to router security was designed to fortify our network against various types of unauthorized access and potential vulnerabilities. The deactivation of unnecessary default services, such as CDP, TCP and UDP Small Servers, Finger, HTTP Server, BOOTP Server, and others, aims to reduce the attack surface. By disabling these services, we prevent potential information leakage and minimize avenues for exploitation by malicious entities.

The following are justifications for disabling some operations and enabling others:

- Disabling Cisco Discovery Protocol (CDP): Disabling CDP enhances network stealth, as it eliminates the broadcast of device information, thus thwarting potential reconnaissance attacks [1].
- Disabling TCP and UDP Small Servers: TCP and UDP Small Servers include legacy services like echo, chargen, and discard. These services are rarely used in modern networks and may present security risks if left active. Disabling them eliminates unnecessary services that could be exploited by attackers.
- Disabling Finger Service: The Finger service allows remote listing of network users, providing information about user accounts. In a secure network, unauthorized users should not have access

to such user-related information. Disabling the Finger service prevents potential attackers from gathering user details and aids in maintaining user privacy and network security.

- Disabling HTTP Server: Some Cisco IOS devices support web-based configuration management programs through the HTTP server. If not actively used, this service should be disabled to eliminate the risk of unauthorized access through web interfaces. Disabling the HTTP server prevents potential attackers from exploiting vulnerabilities in web-based services and ensures that router configuration is accessed only through secure channels.
- Disabling BOOTP Server: BOOTP (Bootstrap Protocol) is used for booting networked devices. Disabling the BOOTP server on a router is crucial, especially if it is not intended to serve as a boot server for other routers [2]. Allowing a BOOTP server to operate without necessity could potentially lead to unauthorized routers booting from the network, posing a security risk. Disabling this service prevents such unauthorized booting and enhances overall network security.
- Disabling Configuration Auto-loading: Configuration auto-loading allows a router to attempt to load its configuration via a TFTP server. If not actively used, this feature should be disabled to prevent potential attacks where a malicious entity could attempt to load unauthorized configurations onto the router. Disabling this service ensures that configurations are not inadvertently altered or replaced, enhancing the security of the router [3].
- Disabling IP Source Routing: IP source routing allows packets to specify their own routes, potentially facilitating malicious activities by ensuring packets reach specific parts of a network. Disabling IP source routing prevents this feature from being exploited by attackers for directing packets along unauthorized paths. This is a proactive measure to enhance network security by restricting the ability of attackers to manipulate packet routes.

In addition, the implementation of passwords for user mode, console, virtual terminal (telnet), and auxiliary interfaces serves as a fundamental access control mechanism. This measure prevents unauthorized access to the router's different modes, safeguarding against unauthorized configuration changes and potential disruptions [3]. The "Message of the Day" notification further reinforces the importance of authorized access.

Also, encrypting stored passwords in the configuration file using the service password-encryption command enhances confidentiality. Without encryption, passwords in clear text pose a security risk if the configuration file is compromised. Encrypting these passwords mitigates the risk of unauthorized personnel gaining access to sensitive information.

Finally, encrypting the OSPF routing protocol addresses the potential threat of unauthorized routers injecting false routing information. By applying message digest encryption with a shared key ("grape"), we ensure that OSPF routing information exchanges are authenticated. This measure safeguards against the introduction of rogue routers attempting to manipulate the network's routing table.

LABORATORY PART B

This exercise aimed to provide us with hands-on experience in setting up and configuring a security appliance, focusing on the Cisco ASA 5505 device, within the simulated environment of Packet Tracer. The primary objectives of this session included establishing the default configuration on the Cisco ASA 5505 and subsequently customizing the appliance to suit the network topology defined for the lab. The

network architecture involved multiple routers, interconnected through various Ethernet interfaces, with the Cisco ASA 5505 serving as a central security gateway. Throughout the lab, we delved into configuring the ASA 5505 interfaces, defining security levels, and establishing communication between different segments of the network. Additionally, we encountered challenges such as DHCP configuration on the outside interface, which prompted critical thinking and creative problem-solving to ensure a seamless configuration.

Understanding the significance of security levels (ranging from 0 to 100) within the Cisco ASA framework was a key aspect of the lab. Security levels dictate the traffic flow between different interfaces, influencing the level of trustworthiness assigned to each segment of the network. As we progressed through the configuration steps, we not only applied fundamental networking concepts but also encountered and resolved practical issues that commonly arise in network deployment.

Procedure

1. We began the lab by adding the routers and end devices to the Cisco Packet Tracer and making appropriate connections.
2. Initiating the Cisco ASA 5505 Device: Step 1 was followed by accessing the Cisco ASA 5505 device on Packet Tracer and logging in using the default credentials. The initial step involved entering the privileged exec mode by typing en and pressing Enter, followed by accessing the global configuration mode with the conf t command.
3. Setting Factory Defaults: To establish a baseline configuration, we executed the configure factory-default command. This command erased any existing configurations, warning us about the potential loss of DHCP bindings and addressing the need to verify a valid image on disk0.
4. Configuring Interfaces: Proceeding with interface configurations, we navigated to each interface using commands like interface Ethernet 0/0. For the inside interfaces (Ethernet 0/1, 0/2, 0/3), we set them to VLAN 1, ensuring connectivity within the internal network. The outside interface (Ethernet 0/0) was assigned to VLAN 2. We also activated each interface with no shutdown.
5. Configuring VLANs and Assigning Security Levels: We assigned names to VLANs using the nameif command. For the outside interface, we set the security level to 0 with security-level 0, and for the inside interfaces, we set the security level to 100. These security levels influence the traffic flow between interfaces.
6. Assigning IP Addresses to Interfaces: Moving on, we configured IP addresses on the inside interfaces (VLAN 1) using commands like ip address 192.168.1.1 255.255.255.0.
7. Defining NAT (Network Address Translation): We created a network object using object network obj_any and configured NAT with the nat (inside,outside) dynamic interface command. This translation enabled communication between internal and external networks.
8. Enabling HTTP Access and DHCP: HTTP server functionality was enabled with http server enable, allowing ASDM access. We permitted HTTP access from the internal network using http 192.168.1.0 255.255.255.0 inside. DHCP service for the internal network was configured with dhcpd address 192.168.1.5-192.168.1.36 inside.
9. Saving Configuration: To retain the configured settings, we executed write memory to save the configuration to the device's memory.
10. The screenshots in the next pages depict each of the above steps.

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

ciscoasa(config)#interface Vlan1
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit
ciscoasa(config)#
ciscoasa(config)#interface Vlan2
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address dhcp setroute
                                     ^
% Invalid input detected at '^' marker.

ciscoasa(config-if)#ip address 172.16.1.1 255.255.255.0
ciscoasa(config-if)#
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit
ciscoasa(config)#
ciscoasa(config)#object network obj_any
ciscoasa(config-network-object)#subnet 0.0.0.0 0.0.0.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#exit
ciscoasa#
ciscoasa#http server enable
         ^
% Invalid input detected at '^' marker.

ciscoasa#configure terminal
```

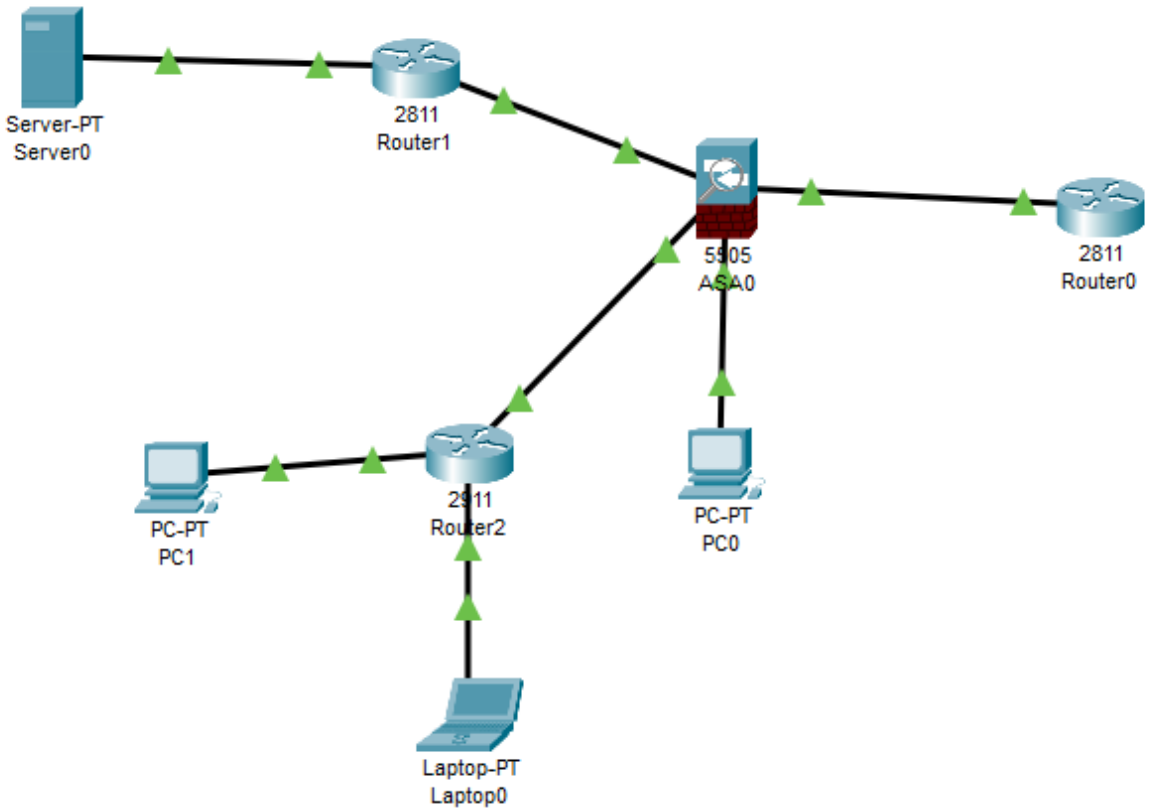
```
ciscoasa(config-if)#ip address 172.16.1.1 255.255.255.0
ciscoasa(config-if)#
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit
ciscoasa(config)#
ciscoasa(config)#object network obj_any
ciscoasa(config-network-object)#subnet 0.0.0.0 0.0.0.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#exit
ciscoasa#
ciscoasa#http server enable
         ^
% Invalid input detected at '^' marker.

ciscoasa#configure terminal
ciscoasa(config)#
ciscoasa(config)#http server enable
% This version of Cisco Packet Tracer does not support this option.
ciscoasa(config)#http 192.168.1.0 255.255.255.0 inside
% This version of  Cisco Packet Tracer does not support this option.
ciscoasa(config)#dhcpd address 192.168.1.5-192.168.1.36 inside
ciscoasa(config)#dhcpd enable inside
ciscoasa(config)#
ciscoasa(config)#logging asdm informational
                ^
% Invalid input detected at '^' marker.

ciscoasa(config)#write memory
Building configuration...
Cryptochecksum: 7d5f19fe 2c3021dd 4eb72676 2c8439ea

872  bytes copied in 2.236 secs (389 bytes/sec)
[OK]
ciscoasa(config)#
```

11. Finally, we configured the rest of the interfaces on the router accpording to the table provided and the resulting network is shown below.

```
Press RETURN to get started!



Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Router0
Router0(config)#interface FastEthernet0/0
Router0(config-if)#ip address 12.1.1.1 255.255.255.0
Router0(config-if)#no shutdown

Router0(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
exit
Router0(config)#
```

```
Router1>enable
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#interface FastEthernet0/0
Router1(config-if)#ip address 172.16.1.2 255.255.255.0
Router1(config-if)#no shutdown

Router1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
exit
Router1(config)#interface FastEthernet0/1
Router1(config-if)#ip address 172.16.2.1 255.255.255.0
Router1(config-if)#no shutdown

Router1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
exit
Router1(config)#
```

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.2.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
exit
Router(config)#write memory
              ^
% Invalid input detected at '^' marker.

Router(config)#
Router(config)#hostname Router2
Router2(config)#interface GigabitEthernet0/1
Router2(config-if)#ip address 192.168.3.1 255.255.255.0
Router2(config-if)#
Router2(config-if)#no shutdown

Router2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
exit
Router2(config)#interface GigabitEthernet0/2

Router2(config-if)#ip address 192.168.4.1 255.255.255.0
Router2(config-if)#
Router2(config-if)#no shutdown

Router2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
exit
```



Discussion

The assignment of security levels (0 to 100) was a critical aspect of our configuration. The security levels determine the trustworthiness of each network segment, influencing the flow of traffic between interfaces [1]. By setting the inside interfaces to a higher security level (100) and the outside interface to a lower security level (0), we established a security hierarchy, allowing communication from higher to lower security levels by default.

The utilization of VLANs played a pivotal role in segmenting the network, and defining distinct broadcast domains for enhanced security [1]. We leveraged VLANs to logically group interfaces and assigned security levels accordingly. The Network Address Translation (NAT) configuration allowed for the seamless translation of internal private IP addresses to the public IP address assigned to the outside interface, facilitating communication with external networks.

Conclusion

In conclusion, the successful completion of this lab not only equipped us with practical skills in configuring the Cisco ASA 5505 but also deepened our understanding of fundamental networking concepts. The challenges encountered served as valuable learning experiences, requiring us to adapt and

problem-solve in a simulated real-world environment. This lab lays the foundation for more advanced security configurations and positions us to apply these skills in real-world scenarios as Telecommunications Engineering professionals.

References

[1] M. Lubis and A. R. Lubis, “Designing secured cafe network with Security Awareness Domain and resource (sadar) by simulation using cisco packet tracer,” *The 10th International Conference on Computer and Communications Management*, 2022. doi:10.1145/3556223.3556258

[2] A. Smith and C. Bluck, “Multiuser collaborative practical learning using packet tracer,” *2010 Sixth International Conference on Networking and Services*, 2010. doi:10.1109/icns.2010.56

[3] T. Macaulay, *Securing converged IP Networks*, 2006. doi:10.1201/9780849375811