Open-Ended Lab Report

TOPIC: Implementation of Firewall Security Policies and Traffic Filtering in a VLAN-Based Campus Network Using Cisco Packet Tracer

COURSE: Routing & Switching Lab

SUBMITTED TO: Sir Mohsin Mubeen

GROUP MEMBERS:

NAMES	REG ID
FIZZA BAIG	63503
ABDUL SARIM KHAN	62527
MUHAMMAD JAHANZAIB	63843

REMARKS: ____________________

1. Abstract

This project demonstrates the design and execution of a secured campus network infrastructure. The primary objective was to enforce strict traffic separation between Administrative, Student, and Laboratory networks while maintaining centralized internet connectivity. The solution leverages a Cisco Multilayer Switch (Core) for high-speed Inter-VLAN routing and a Cisco ASA 5505 Firewall for edge security.

To ensure internal security, Extended Access Control Lists (ACLs) were deployed on the Core Switch to block Student and Lab users from accessing the Admin network. At the network edge, the ASA Firewall utilizes stateful packet inspection and security levels to protect the internal campus from external threats. The final configuration was verified through connectivity tests, confirming that security policies effectively isolate sensitive resources without disrupting legitimate traffic flows.

2. Introduction

2.1 Background

Educational institutions require robust network architectures that balance openness with security. A critical challenge is preventing students or lab users from accessing sensitive administrative data (e.g., grading systems, financial records). This project solves this by moving away from a flat network to a segmented VLAN architecture with enforced access controls.

2.2 Problem Statement

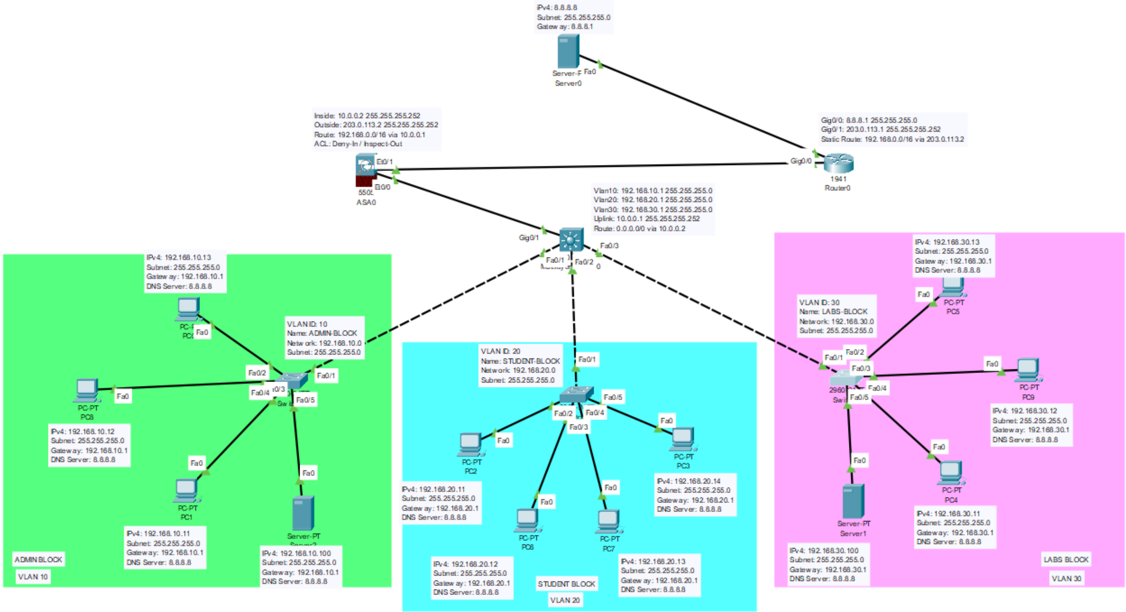
The project addresses the security vulnerability where unauthorized users (Students/Lab) could previously access the Administrative subnet. The goal is to implement a solution where:

1. **Student and Lab VLANs** are strictly prohibited from accessing the **Admin VLAN**.
2. **Return traffic** (like ping replies) is permitted so Administrators can monitor the network.
3. **Internet access** is centralized and protected by a dedicated Firewall.

2.3 Objectives

- To implement Inter-VLAN routing using a **Cisco 3560 Multilayer Switch**.
- To segment the network into **Admin (VLAN 10)**, **Student (VLAN 20)**, and **Lab (VLAN 30)**.
- To apply **Extended ACLs** (BLOCK_STUDENT_TO_ADMIN and BLOCK_LAB_TO_ADMIN) to enforce internal security policies.
- To configure a **Cisco ASA Firewall** with security-level zones and modular policy frameworks (MPF) for inspection.

3. Network Design & Topology



3.1 Topology Overview

The network uses a hierarchical design centered around a Core Multilayer Switch.

- **Core Layer (Cisco 3560):** Acts as the default gateway for all VLANs and performs IP routing. It connects to the Firewall via a routed uplink.
- **Edge Layer (Cisco ASA 5505):** Connects the Core Switch to the ISP. It separates the "Inside" trusted network from the "Outside" untrusted internet.
- **Access Layer (Cisco 2960s):** Connects end devices to the Core Switch via specific FastEthernet ports.

3.2 IP Addressing & VLAN Schema

The following addressing scheme is implemented based on the device configurations:

Device	**Interface**	**VLAN ID**	**IP Address**	**Description**
Core Switch	Vlan 10	10	192.168.10.1	Admin Gateway
Core Switch	Vlan 20	20	192.168.20.1	Student Gateway
Core Switch	Vlan 30	30	192.168.30.1	Lab Gateway
ASA Firewall	Vlan 1 (Inside)	1	10.0.0.2	Inside Interface
ASA Firewall	Vlan 2 (Outside)	2	203.0.113.2	Outside Interface

4. Methodology

The project was executed in four distinct phases to ensure a structured approach to network security and connectivity.

Phase 1: Physical & Logical Network Design

The initial phase involved setting up the physical topology in Cisco Packet Tracer. A "Collapsed Core" architecture was selected, where the Core Switch handles both distribution and core functions. Three distinct Layer 2 switches were deployed to physically separate the departments (Admin, Student, and Lab). Access ports were configured on these switches to assign end-user traffic to their respective VLANs (10, 20, and 30) before trunking it to the Core Switch.

Phase 2: Layer 3 Configuration & Inter-VLAN Routing

To enable communication between the different subnets, IP routing was enabled on the Core Multilayer Switch. Switch Virtual Interfaces (SVIs) were created for VLANs 10, 20, and 30, assigning the first usable IP of each subnet as the Default Gateway. A point-to-point Layer 3 link was established between the Core Switch (GigabitEthernet0/1) and the ASA Firewall using a /30 subnet (10.0.0.0/30) to handle all internet-bound traffic.

Phase 3: Security Policy Formulation (ACLs)

Security was the central focus of the methodology. To strictly isolate the Admin network, two **Extended Acczess Control Lists (ACLs)** were formulated:

1. **Student Restriction:** An ACL named BLOCK_STUDENT_TO_ADMIN was created to deny all IP traffic from the Student subnet (192.168.20.0/24) to the Admin subnet.
2. **Lab Restriction:** A parallel ACL named BLOCK_LAB_TO_ADMIN was created to deny traffic from the Lab subnet (192.168.30.0/24).

Crucially, both ACLs were designed with a specific permit statement for icmp echo-reply. This methodological choice ensures that while students cannot initiate a connection to the Admin, an Admin can still ping a student and receive a reply, maintaining manageability. These ACLs were applied in the **Inbound** direction on the respective VLAN interfaces.

Phase 4: Edge Security Configuration

The final phase involved securing the network perimeter using the Cisco ASA 5505.

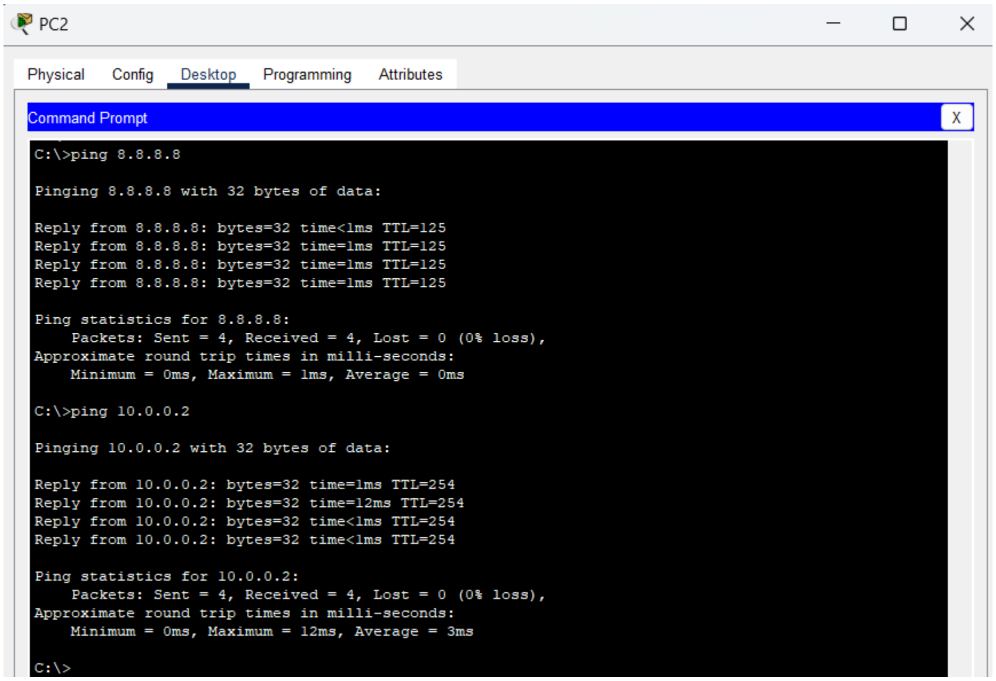
- **Zone Configuration:** Interfaces were assigned Security Levels. The internal interface was set to **Security Level 100** (Fully Trusted), while the external interface facing the ISP was set to **Security Level 0** (Untrusted).
- **Routing Logic:** A static route was configured on the ASA to direct traffic for the internal 192.168.x.x networks back to the Core Switch, ensuring bidirectional connectivity.
- **Inspection Policies:** A global policy map was verified to inspect standard protocols (ICMP, HTTP, DNS), allowing internal users to access the internet dynamically while keeping the network closed to unsolicited external traffic.

5. Testing & Analysis

5.1 Connectivity Test

- **Test:** Student PC (192.168.20.x) pings an External IP.
- **Result: Successful**.

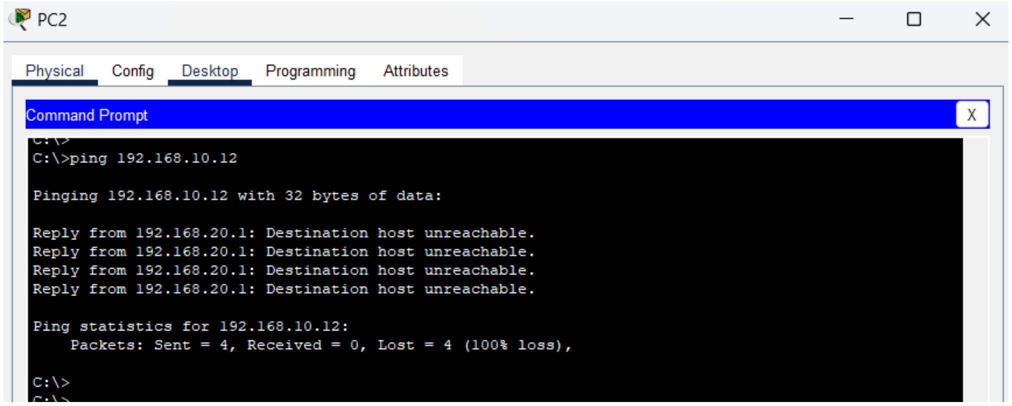
- **Analysis:** The packet travels from VLAN 20 to the Core Switch. The ACL **BLOCK_STUDENT_TO_ADMIN** hits the permit ip any any rule. The packet is routed to the ASA, inspected, and forwarded to the ISP.



```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time<1ms TTL=125
Reply from 8.8.8.8: bytes=32 time=1ms TTL=125
Reply from 8.8.8.8: bytes=32 time=1ms TTL=125
Reply from 8.8.8.8: bytes=32 time=1ms TTL=125

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=1ms TTL=254
Reply from 10.0.0.2: bytes=32 time=12ms TTL=254
Reply from 10.0.0.2: bytes=32 time<1ms TTL=254
Reply from 10.0.0.2: bytes=32 time<1ms TTL=254

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>
```

5.2 Security Test A

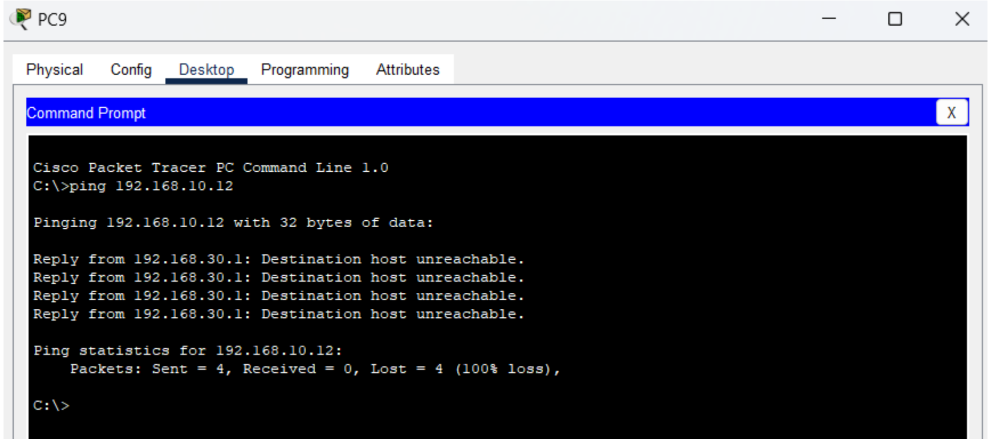
- **Test:** Student PC attempts to ping Admin PC (192.168.10.1).
- **Result: Failed (Destination Unreachable / Timeout)**.
- **Analysis:** The packet enters the Core Switch on VLAN 20. The Inbound ACL **BLOCK_STUDENT_TO_ADMIN** identifies the destination as 192.168.10.x. The deny rule triggers, and the packet is dropped immediately.



```
C:\>
C:\>ping 192.168.10.12

Pinging 192.168.10.12 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.10.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>
```

5.3 Security Test B

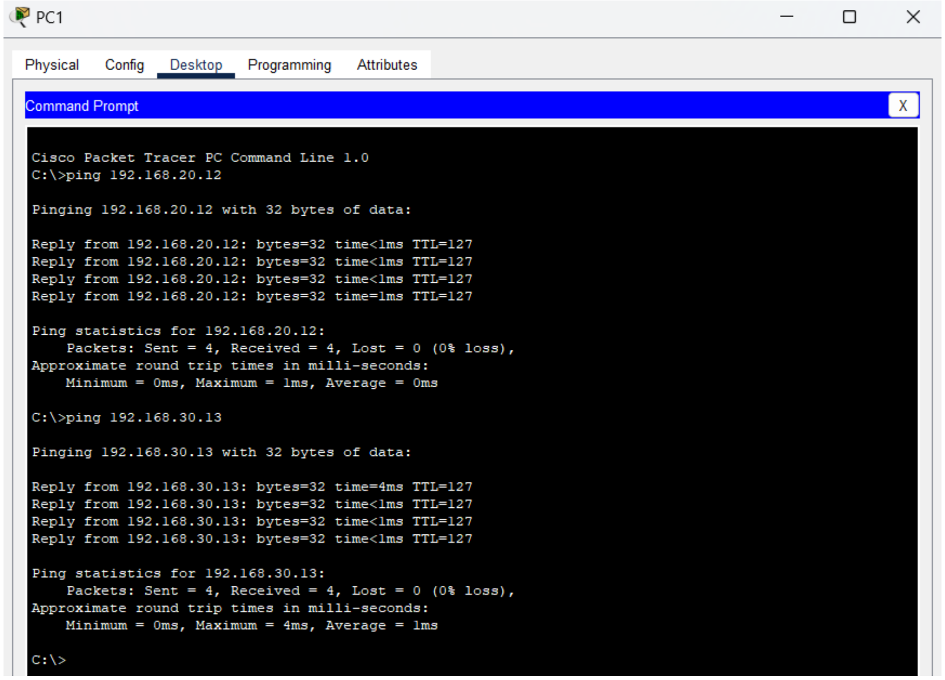
- **Test:** Lab PC attempts to ping Admin PC.
- **Result: Failed (Destination Unreachable / Timeout)**.
- **Analysis:** The packet is intercepted on the VLAN 30 interface by the **BLOCK_LAB_TO_ADMIN** ACL and dropped, confirming the Lab network is isolated from the Admin sector.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.12

Pinging 192.168.10.12 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.10.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

5.4 Administrative Monitoring Test

- **Test:** Admin PC pings Student PC.
- **Result: Successful**.
- **Analysis:** The Admin sends an Echo Request. The Student receives it and sends an Echo Reply. When the reply hits the VLAN 20 interface on the Core Switch, the ACL **BLOCK_STUDENT_TO_ADMIN** allows it because of the specific *permit icmp ... echo-reply* rule.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.12

Pinging 192.168.20.12 with 32 bytes of data:

Reply from 192.168.20.12: bytes=32 time<1ms TTL=127
Reply from 192.168.20.12: bytes=32 time<1ms TTL=127
Reply from 192.168.20.12: bytes=32 time<1ms TTL=127
Reply from 192.168.20.12: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.20.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.30.13

Pinging 192.168.30.13 with 32 bytes of data:

Reply from 192.168.30.13: bytes=32 time=4ms TTL=127
Reply from 192.168.30.13: bytes=32 time<1ms TTL=127
Reply from 192.168.30.13: bytes=32 time<1ms TTL=127
Reply from 192.168.30.13: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>
```

6. Conclusion

This project successfully achieved all objectives. The network topology is robust, scalable, and secure. By offloading internal routing to the Core Switch and dedicating the ASA to edge security, network efficiency was maximized. Most importantly, the methodology of applying Extended ACLs provided a verifiable security barrier, effectively protecting the Administrative department from unauthorized access by Student and Lab networks.