Tab 1

**IT491 Capstone Project**

Cisco Track:

Network Segmentation for Ransomware Protection

**

Yoen Jun Eric Kim

Karla Izquierdo

Bryan Madewell

Adam Milewski

*Table of Contents*

1. **CHAPTER 1: INTRODUCTION**
   1. Project Background
   2. Problem Definition
   3. Glossary
   4. Iteration Updates
2. **CHAPTER 2: PROJECT MANAGEMENT**
   1. Task Analysis
   2. Roles
   3. WBS/Gantt Chart
   4. Risk Identification and Management
3. **CHAPTER 3: DEFINE**
   1. Stakeholders
   2. Requirements Gathering
   3. Project Scope
   4. FDD Requirement Grouping and Use Case Diagrams
4. **CHAPTER 4: DESIGN**
   1. Physical/Logical Layouts
   2. Network Diagrams

4.3 Implementation Details

4.4 Alternative Solutions

1. **CHAPTER 5: DEVELOPMENT**

5.1 Outputs/Screenshots and description of solution

5.2 Develop a brief User Manual

1. **CHAPTER 6: EVALUATION AND CONCLUSION**

6.1 Solution Testing

6.2 Verification

6.3 Validation/QA Analysis

6.4 Team Conclusions

**CHAPTER 1: INTRODUCTION**

**1.1 PROJECT BACKGROUND**

Ransomware attacks are a growing threat in the last years, causing significant financial and operational damage by encrypting a victim's data and demanding payment for decryption. It is essential for companies to implement any kind of protection against these threats.

Network segmentation is a highly effective strategy which is in charge of dividing a network into smaller and isolated segments, in which organizations can limit the spread of ransomware and contain its impact. This approach helps to prevent unauthorized access and minimizes potential damage. Our project focuses on a dedicated network which will be segmented to prove defenses and protect against ransomware.

**1.2 PROBLEM DEFINITION**

Ransomware is a major threat for organizations and businesses all over the world, it leads to data breaches, financial losses, and damage to organization’s reputation. Some of the security measures that are being used by companies at the moment like firewalls and antivirus software, are sometimes not enough to tackle sophisticated ransomware software attacks. Without a proper network segmentation, ransomware can spread across an entire network, causing chaos. Our project aims to address some of these problems which are the need for useful strategies to contain ransomware, enhancing network security through the segmentation to protect sensitive data and implementing a DMZ protection in the internal network.

**1.3 GLOSSARY**

| **TERM** | **DEFINITION** |
| --- | --- |
| **Ransomware** | **Software that encrypts a victim's data and demands payment .** |
| **Network Segmentation** | **Dividing a network into smaller segments or subnetworks to improve security and performance.** |
| **CISCO** | **A technology company known for networking and cybersecurity solutions.** |
| **Firewall** | **A network security device that monitors and controls incoming and outgoing network traffic.** |
| **Antivirus Software** | **A program designed to detect and remove malicious software.** |
| **Encryption** | **The process of converting data into a code to prevent unauthorized access.** |
| **Containment** | **Strategies to limit the spread of malicious software within a network.** |
| **Data Breach** | **An incident where sensitive or confidential data is accessed, disclosed, or stolen by unauthorized individuals.** |
| **Access Control List (ACL)** | **A list of rules that control network traffic and reduce security risks by allowing or denying traffic based on IP address or other criteria.** |
| **Local Area Network (LAN)** | **Computer network that connects devices within a limited geographical area.** |
| **Network Address Translation (NAT)** | **Technique used to map one IP address.** |
| **Demilitarized Zone** | **A part of the network that acts as a buffer between the networking-facing devices and the rest of the internal network.** |
| **VLAN (Virtual LAN)** | **A logical grouping of devices on a physical network, allowing for efficient traffic management and isolation.** |
| **Router on a Stick** | **A network design where a single router is connected to a switch via a single link.** |

**1.4 ITERATION UPDATES**

During this project, several iterations and revisions have been made to confirm a complete analysis and effective solutions. During the initial research phase, a review on ransomware attacks, network segmentation and prevention techniques, division of VLANs were conducted, identifying key elements and potential results. In the design phase, a preliminary design for network segmentation using a network on a stick was created, including detailed network diagrams and segmentation plans. The implementation phase involved setting up the network segmentation design on CISCO packet Tracer and testing its effectiveness in preventing malware spread. During the evaluation phase, the implementation results were analyzed, areas for improvement were identified, and necessary adjustments were made based on feedback and testing outcomes. Finally, in the last revision, findings were compiled, documentation was refined, and the final report was prepared for submission.

**CHAPTER 2: PROJECT MANAGEMENT**

**2.1 TASK ANALYSIS**

Our project involves implementing network segmentation to protect against ransomware using Cisco Packet Tracer. We broke down the project into several tasks: planning, design, implementation, testing, and evaluation. We studied each step and then decided to further divided into manageable sub-tasks to keep the project organized and on track for final revision.

Some of these tasks were subdivided into smaller tasks considering that tasks like Implementation will take more time to complete. There where several solutions that were implemented at the beginning of the project but those were not successful. The creation of the VLANs were time consuming as well as the IP addresses.

**2.2 ROLES**

The following roles were assigned to allow each team member to focus on their specific responsibilities, ensuring a fluid coordination and efficient implementation of a network segmentation for ransomware protection.

***Project Manager:*** Yoen JunEric Kim is in charge of the entire project, ensuring that timelines are met, and coordinating between team members. Also, with a vast experience in Networking area which has been helpful when implementing our solutions.

***Reports and Documentation:*** Karla Izquierdo is responsible for research about Network security that could be implemented in the project, and to document for future used.

***Graphic Designer:*** Bryan Madewell takes care of designing graphic solutions for the network, flyers and final presentation.

***Test Engineering :*** Adam Milewski conducts the testing side of the project solution to validate the network segmentation and its functionality.

**2.3 WBS/GANTT CHART**

We developed a Work Breakdown Structure to keep our work organized. This helps define the scope and ensure that all tasks are being covered. We also created a Gantt chart to visualize the project timeline and manage our schedule**:**

**WBS:**

1. **Planning**

Define project objectives

Set scope and deliverables

Develop project plan

1. **Design**

Research and select a diagram that could be useful for our project

Create a network segmentation layout

Develop security protocols

1. **Implementation**

Set up devices

Configure network segments

Implement security measures

1. **Testing**

Conduct initial testing

Validate network segmentation

Assess effectiveness against ransomware

1. **Evaluation**

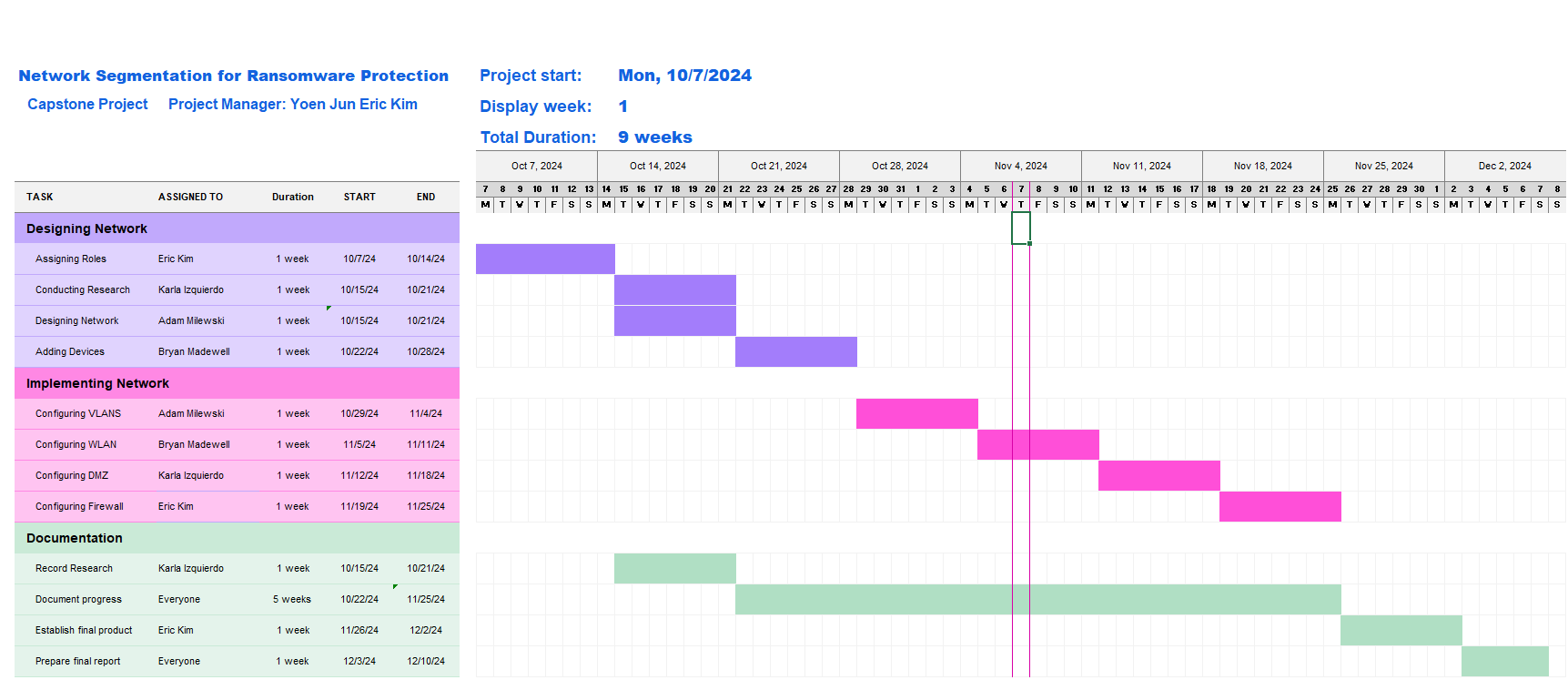
Analyze test results

Identify areas for improvement

Prepare final report

**Gantt Chart:**

The Gantt Chart helped us manage our time and ensure continued progress:

****

**2.4 RISK IDENTIFICATION AND MANAGEMENT**

To avoid any potential bumps down the road, we have created this section which outlines any possible risks that we might encounter and also a mitigation plan designed to deal with it.

| **RISK** | **LIKELIHOOD** | **IMPACT** | **MITIGATION** |
| --- | --- | --- | --- |
| **Unexpected Events** | **1** | **5** | **Contingency planning, flexible deadlines, backup plans** |
| **Hardware/Software Failures** | **2** | **3** | **Regular backups, redundancy, troubleshooting skills** |
| **Changes in Requirements** | **2** | **4** | **Flexible project planning, adaptability, and regular communication with the instructor** |
| **Conflict Within Team** | **3** | **4** | **Effective conflict resolution strategies, team-building exercises, open communication** |
| **Unequal Workload** | **3** | **3** | **Regular check-ins, clear task assignments, and equitable distribution of work** |
| **Technical Difficulties** | **3** | **3** | **Seek help from instructors or technical support; break down complex tasks into smaller steps** |
| **Lack of Communication** | **4** | **3** | **Regular team meetings, use of project management tools, clear communication channels** |
| **Poor Time Management** | **4** | **4** | **Detailed project schedule, time management techniques, regular progress reviews** |

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### **CHAPTER 3: DEFINE**

#### **3.1 STAKEHOLDERS**

Identifying the key stakeholders for our project is essential for its success. Stakeholders are individuals or groups who have an interest in the outcome of the project. For our network segmentation project aimed at ransomware protection using Cisco technologies, the primary stakeholders include:

1. Project Team: This includes all team members such as the Project Manager (Yoen Jun Eric Kim), Reports and Documentation (Karla Izquierdo), Graphic Designer (Bryan Madewell), and Test Engineer (Adam Milewski). This team is responsible for creating and executing the project.
2. NJIT and Capstone Professor: Professor Eljabiri, along with any TA’s/Graders are also stakeholders in this project.
3. Capstone Showcase Judges: The judges for the Capstone Showcase, for us being Firas Omar, and Professor Farley, are additional stakeholders in our project.
4. Capstone Showcase Attendees: Any visitors (friends, family) that visited our project and were interested in learning more about it.

#### **3.2 REQUIREMENTS GATHERING**

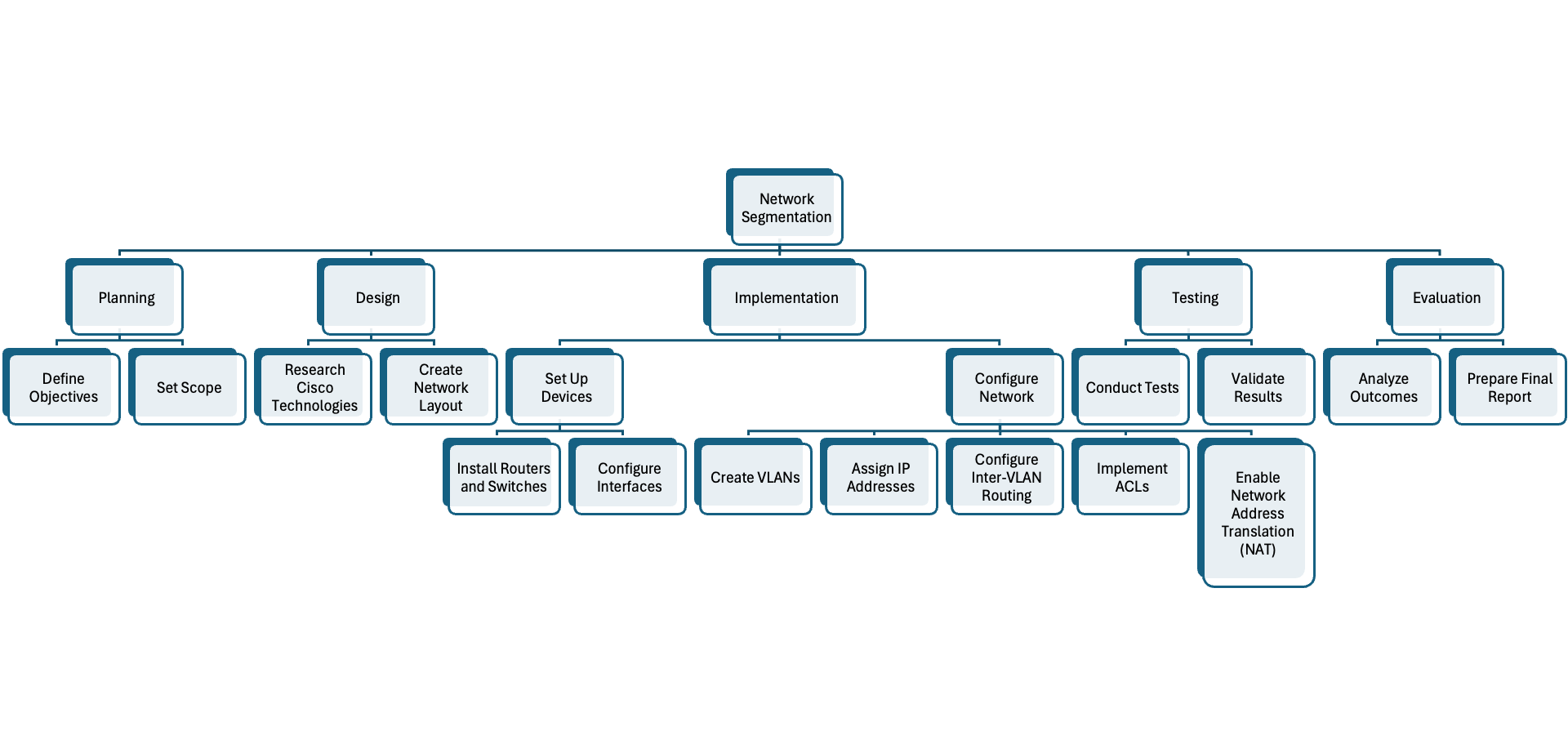
Gathering requirements involves understanding what is needed to successfully complete the project. This phase involves interacting with stakeholders to collect their needs and expectations. For our project, the requirements may include technical requirements, such as specifications for the network segmentation layout, necessary Cisco technologies, and security protocols; functional requirements, which detail how the network should operate after segmentation, including performance metrics and security standards; non-functional requirements, which include usability, scalability, and maintenance needs; and security requirements, which include measures to ensure data protection and integrity.

**3.3 PROJECT SCOPE**

Defining the project scope is about outlining what the project will accomplish and what it won't. Our project's scope includes the implementation of network segmentation using Cisco technologies to divide the network into smaller, manageable segments; enhancement of ransomware protection by establishing security protocols to prevent and contain ransomware attacks, testing and evaluation to validate the effectiveness of the network segmentation, and documentation. This involves preparing detailed reports and documentation for future reference and audit. The project will not cover non-ransomware related security measures or extend beyond the current network infrastructure.

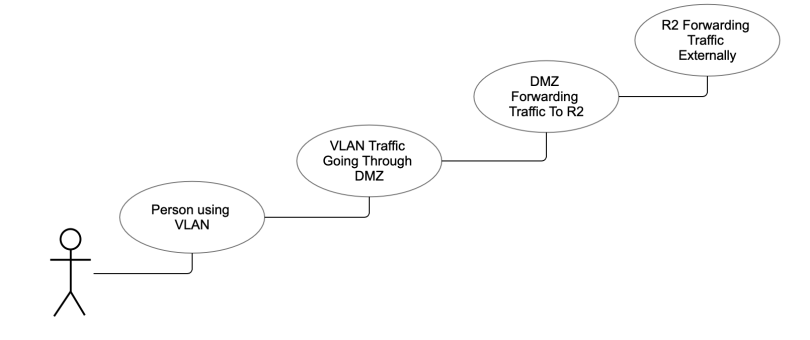
**3.4 FDD REQUIREMENT GROUPING AND USE CASE DIAGRAMS**

Functional Decomposition Diagrams (FDD) are useful for breaking down project requirements into manageable sections. Below is how we split up the different milestones and their specific goals:

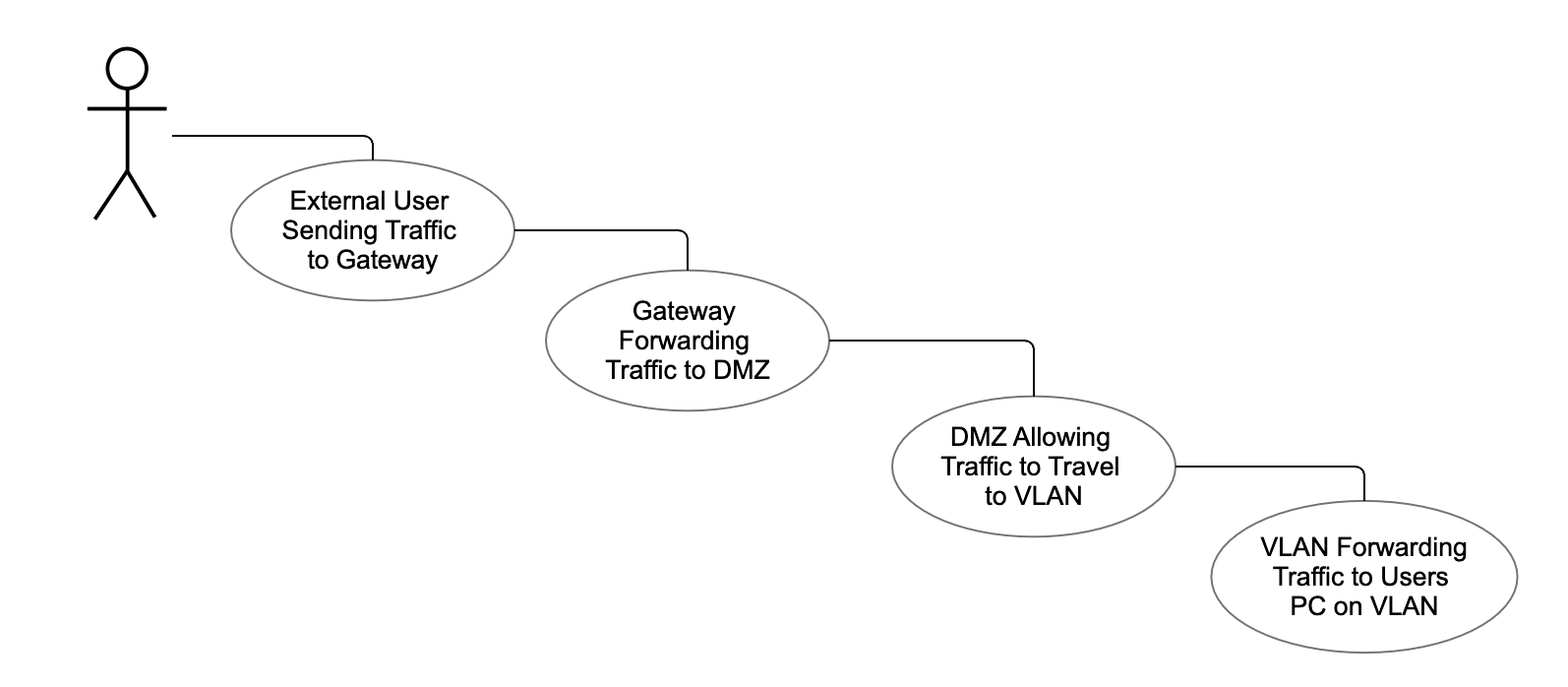
****

Below are the Use Case Diagrams that illustrate how both an internal and external user would interact with the network:

Internal User:

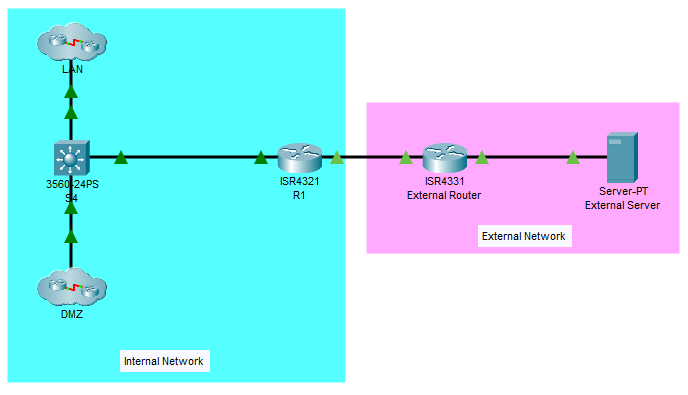


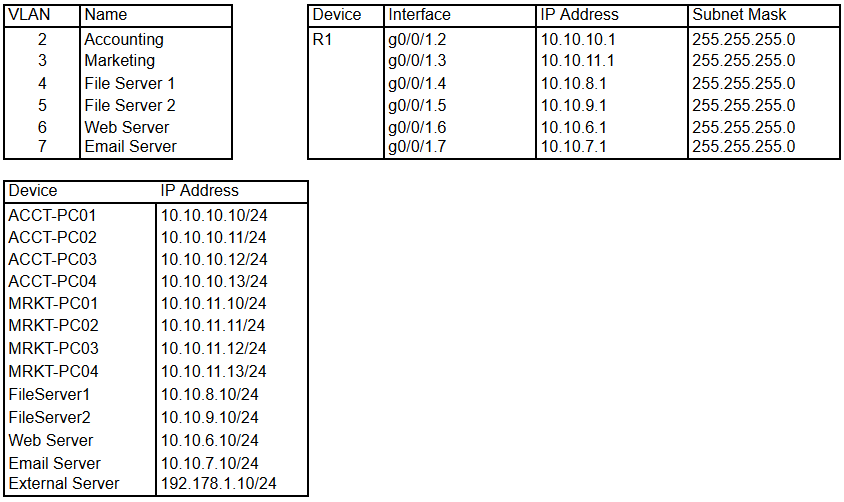
External User:



**CHAPTER 4: DESIGN**

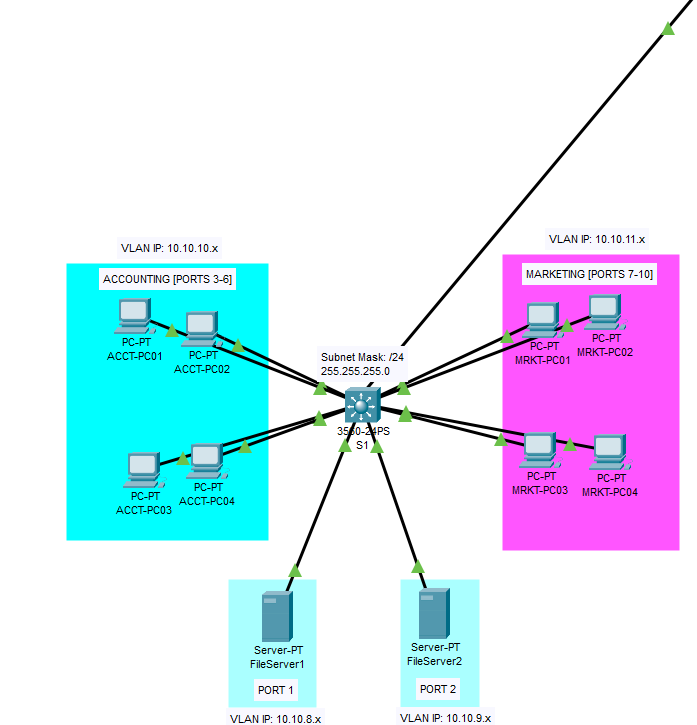
**4.1 PHYSICAL/LOGICAL LAYOUTS**



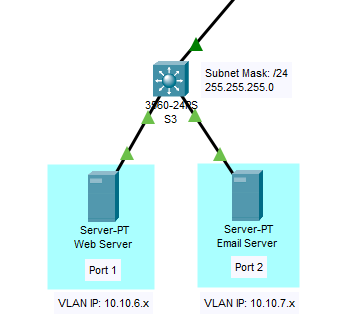
****

**4.2 NETWORK DIAGRAMS**

LAN:



DMZ:



**4.3 IMPLEMENTATION DETAILS**

Our network was broken down into two main components, internal and external networks. The two routers act as the link between these external and internal networks. The internal network then leads into the DMZ. The DMZ itself is split into multiple servers that exist within their own VLAN. Afterward, the internal network leads to the internal LAN, where the majority of the company would operate. Like the DMZ, the network is also split into multiple VLANS for added security. Our simulated departments, marketing, and accounting, have their own specified VLANS.

**4.4 ALTERNATIVE SOLUTIONS (FIND THREE)**

Solution 1: Adding third-party security tools to the DMZ

Why we did not implement: We were limited to the confines of CISCO packet tracer. A program that only simulates networks does not allow us to fully implement third-party security tools.

Solution 2: Zero Trust Architecture

Why we did not implement: The zero trust model to us seemed over bloated, to the point where it would clash with the efficiency of the network. The main idea of zero trust model is that the network treats each device connected as if new to the network and would have to be reverified whenever it requested access to data or communication across the network.

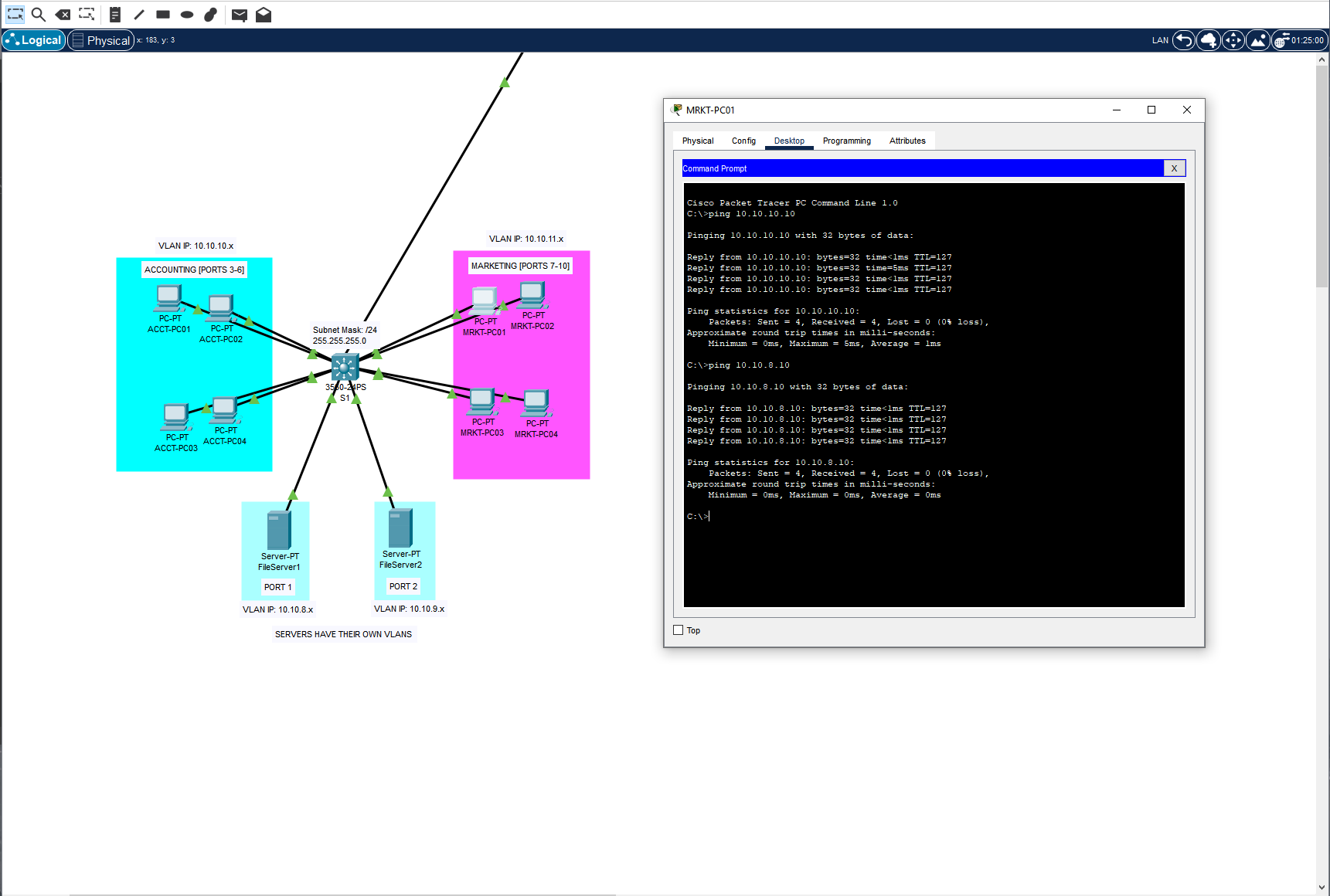
Solution 3: Cloud Networking

Why we did not implement: We felt it prudent to emphasize the strength of the physical network before implementing any cloud features. A cloud network is not inherently secure, and first needs to be secured with measures such as the ones chosen in our project.

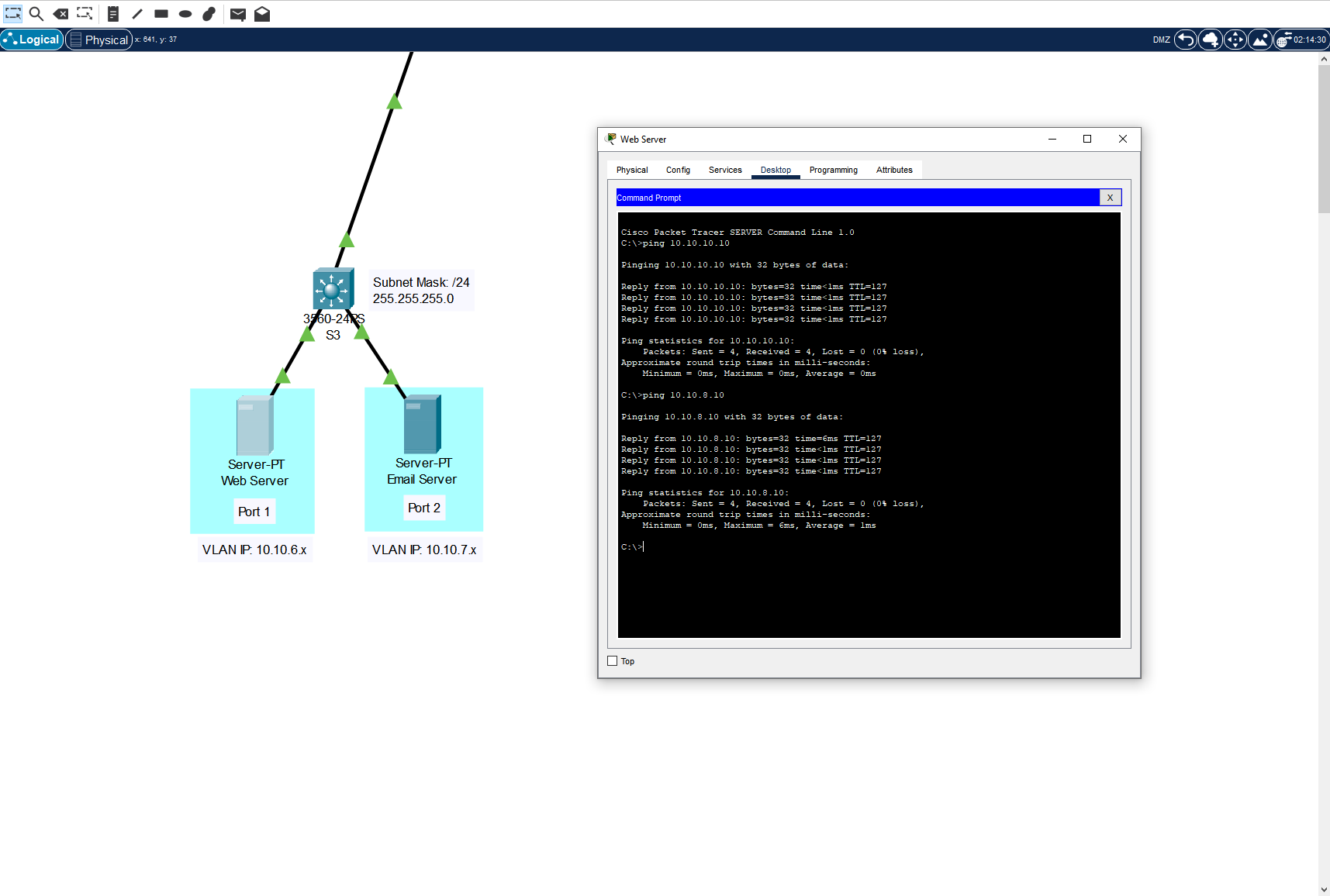
**CHAPTER 5: DEVELOPMENT**

**5.1 OUTPUT/SCREENSHOTS AND DESCRIPTION OF SOLUTION**

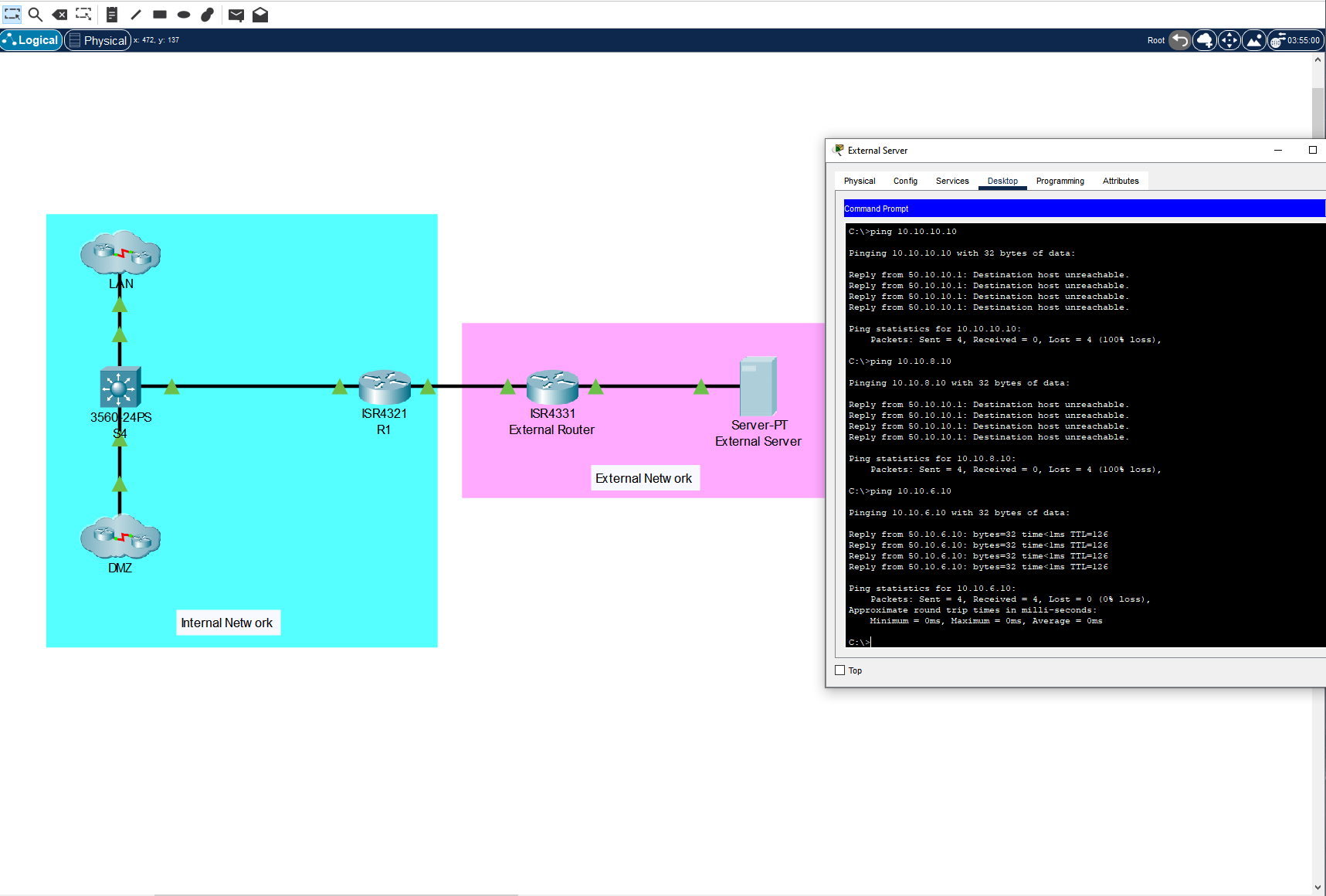
LAN Devices able to communicate one another:

****

DMZ devices able to communicate with LAN devices:



External network UNABLE to communicate with LAN devices, but can reach the DMZ:



**Description of our solution:**

In order to maximize network segmentation in order to prevent malware attacks, the team decided that we were going to adopt a DMZ very early on in the project’s life cycle. We concurred that the best way to implement network segmentation was by isolating all external-facing devices into their own LAN called the DMZ. Giving these devices unique permissions that enabled them to still communicate normally with external devices while acting as both points of ingress and egress for the rest of the internal LAN. This funneling of traffic can allow the team to better monitor the traffic that flows in and out of our network, giving us even more control over security measures and identifying potential threats.

We achieved the implementation of the DMZ by first separating the different departments of the network into their VLANs. Servers would also exist within their own separate VLANs, thus achieving another layer of segmentation. The VLANs would be enabled to communicate with each other through a router-on-a-stick, effectively granting the various network devices the ability to trunk all tagged traffic and distribute this traffic accordingly. The next step was to enable access control lists that disabled any external traffic from reaching the devices within the internal LAN. This would force all external devices to communicate with a DMZ device in order to conduct business within our internal network. Finally, a simple NAT table also ensured that the inside private IP addresses of the DMZ devices remained hidden from the outside world, establishing the final level of segmentation within our network.

**5.2 DEVELOP A BRIEF USER MANUAL**

These are the various techniques used throughout the course of the project:

1. Demilitarized Zone (DMZ)
   1. Acts as the buffer between the internal and external network. This is where all external traffic should be directed towards. All DMZ devices should be those that require external communication to perform their tasks, such as web servers and email servers.
2. VLANs
   1. Every department and server within the internal network exist within their own VLAN. This ensures that the subnet that they exist on remains separate from the others. This segmentation ensures that any potential threat propagation is either prevented or diminished.
3. Router-on-a-Stick
   1. Configuring trunking on all the internal network switches as well as the main router ensures that all devices within different VLANs can still communicate with one another. This ensures that regular organizational functions can still be performed.
4. Access Control Lists (ACL)
   1. The current ACL’s assigned to the VLANs within the internal LAN dictate that only VLAN traffic can flow in and out of the internal LAN. This means that traffic originating from external devices cannot reach these LAN devices. Any attempts for an internal device communicating with an external device is likewise thwarted.
5. Network Address Translation (NAT)
   1. Translating the private IP address of the DMZ into a new public address for external devices adds the final layer of segmentation security to this project. This address translation ensures that external devices will never know of the IP addressing scheme used by the rest of the internal network, preventing them from figuring out the potential private IP addresses of the devices within the internal LAN.

Overall, the adoption of a DMZ and the security measures that were implemented alongside it contributed towards a security solution that was quite capable of deterring external devices from accessing private parts of the internal network. Future contributions to the project would build upon this solid foundation, such as adding extended ACLs or implementing DHCP services.

**CHAPTER 6: EVALUATION AND CONCLUSION**

**6.1 SOLUTION TESTING**

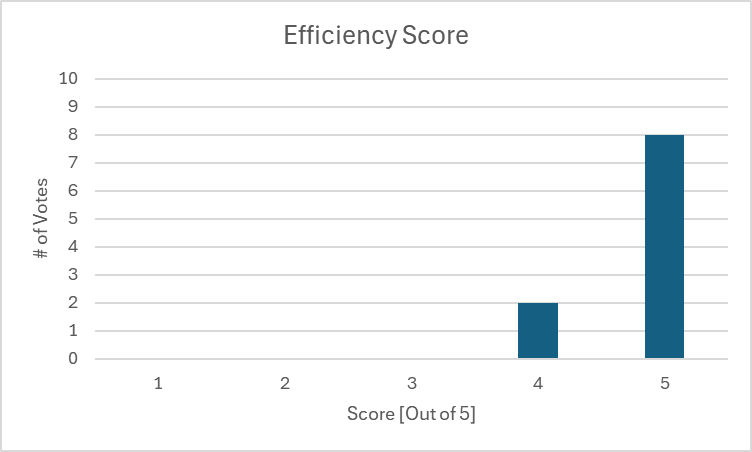
In order to test our solution, the team performed a variety of pings in order to ensure devices in both the internal and external network are only able to communicate with what the ACL’s allow them to. This test was performed on both incoming and outgoing packets of each device. Cisco Packet Tracer’s Simulation Mode came in especially handy for this purpose, allowing us to visualize the movement of packets and where they are potentially stopped based on our implemented security measures. Additional tests were also performed in order to ensure that proper NAT was established for the DMZ devices.

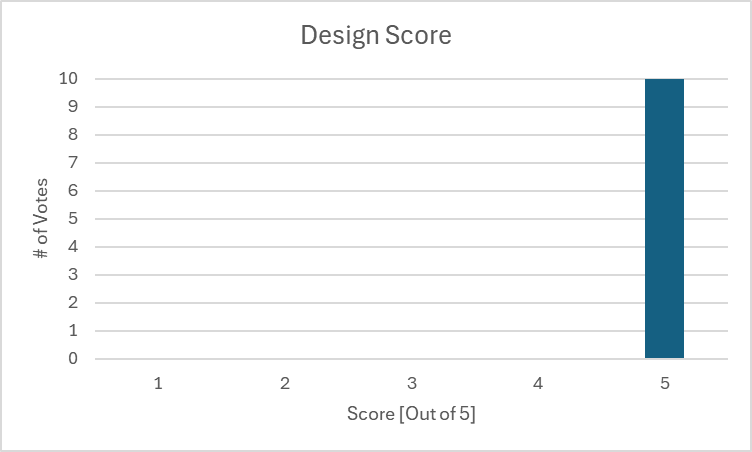
**6.2 VERIFICATION**

After running substantial testing and making the necessary amendments to our security settings, the team finally reached a point where we were satisfied with the performance of our project’s segmentation policies. We verified that proper VLAN communication was established throughout the entire internal network, established a safe zone through the implementation of the DMZ, authenticated both incoming and outgoing network traffic through the use of access control lists, and demonstrated effective internal obfuscation through the use of NAT.

**6.3 VALIDATION/QA ANALYSIS**

In order to validate the effectiveness of our solution, we gathered feedback during the showcase that took place on December 7, 2024 at the NJIT Campus Center. In total, we were able to gather the responses of 10 individuals.





| **Metric** | **Result** |
| --- | --- |
| Design | 5/5 |
| Efficiency | 4/5 |
| Recommendation Rate | 100% |

These individuals also contributed constructive criticism, pointing out their favorite feature and offering ideas on how to better improve the network’s security:

**Best Feature:** *Ergonomic Design, Efficient Segmentation*

**Top Suggestion:** *Implementing extended ACLs, Improving port security*

**6.4 TEAM CONCLUSIONS**

Overall, the team believes that we succeeded in creating a security solution that implements segmentation in a manner that best combats ransomware attacks. The knowledge gained from our time spent in Cisco Academy contributed greatly to the methodology we adopted in order to accomplish our goal. By learning about and applying techniques like VLANs, router-on-a-stick, ACLs, NAT, and even a DMZ, the team was able to gain impressive knowledge on proper network configuration procedure while creating a worthwhile and impressive product.

After accomplishing our QA analysis during the showcase and gathering constructive criticism from seasoned professionals, we believe that there are still portions of the network that can be improved. Though we would change nothing about how the team designed the work breakdown structure or schedule, one thing we all agreed upon was that an increased pace of education in Cisco Academy would have contributed to a more complex product. By accomplishing the academy courses faster, the team would have been able to apply their gained knowledge for a longer period of time, perhaps even applying the suggestions mentioned during the QA Analysis process, such as extending ACLs and improving port security. However, the final product still remains a robust measure against ransomware attacks, serving as a solid foundation where future settings and policies can be implemented.