Implementing Network Security with ACLs and NAT for MMZA Factory

Overview:

This project simulates a network infrastructure for MMZA factory, which consists of three branches. Each branch operates its own private network, all of which are connected to the central server hub. The main goal was to enhance network security across all branches by implementing Access Control Lists (ACLs) and Network Address Translation (NAT), ensuring traffic control, IP address management, and improved security measures.

Objectives:

1. Configure standard and extended ACLs to control traffic flow and secure network access across the three branches.
2. Implement Static and Port Address Translation (PAT) to manage IP address translations for all branches.
3. Integrate ACLs and NAT into the network structure, ensuring seamless connection between the three branch networks and the central server hub.
4. Perform a comprehensive security assessment and document improvements in the overall network security.

Execution:

We successfully executed the project, completing all the assigned tasks. The network for each of the three branches was fully established and linked to the central servers, providing the required protection and efficiency. The ACLs and NAT configurations were implemented and tested, ensuring optimal performance across all networks.

Project Team (Cyber Guardians team) :

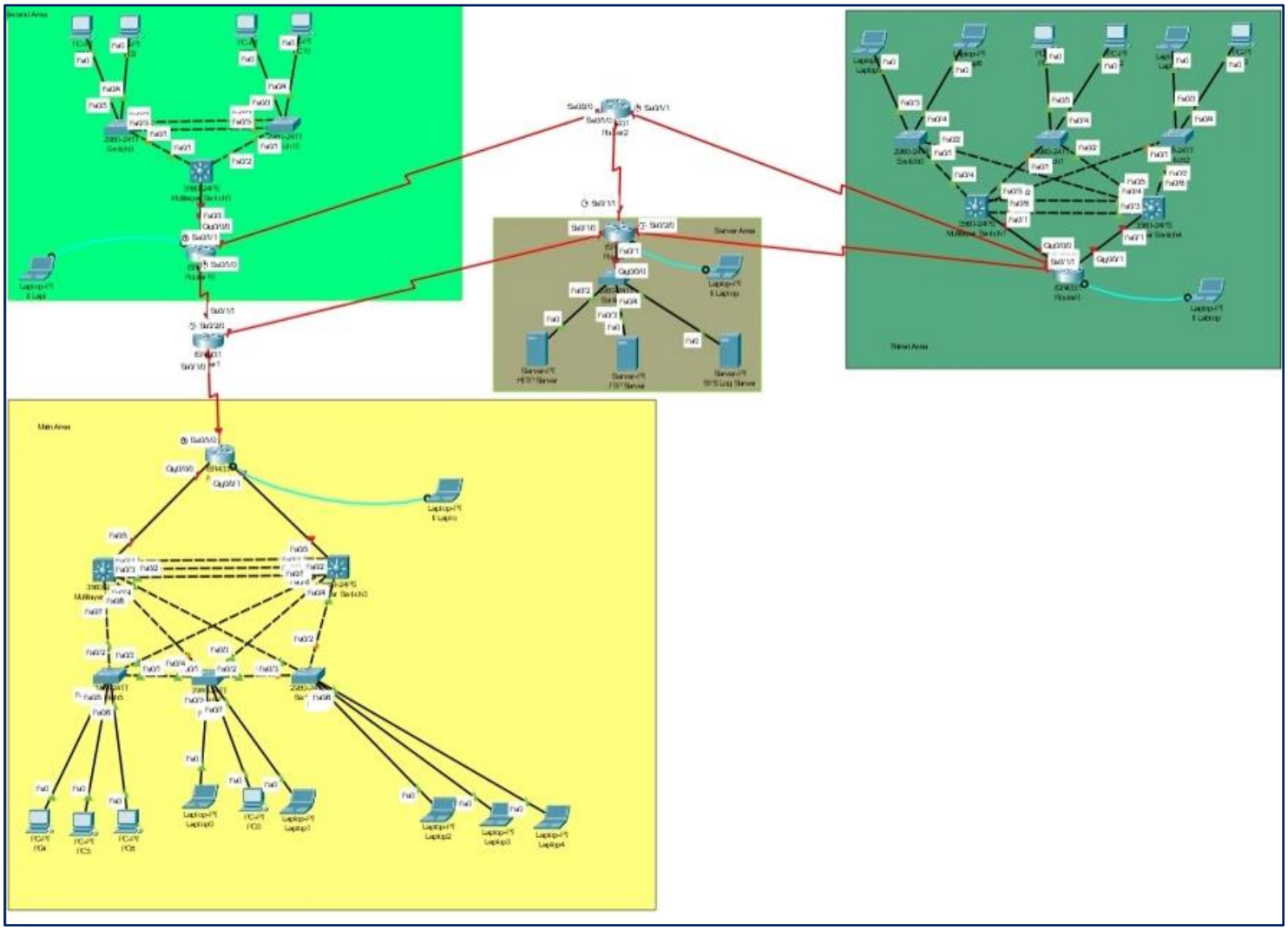
Ahmed Saleh Abdelmoneam – ID : **21031816**
Mostafa Ahmed Elsaid – ID : **21000192**
Zeyad Mohamed Zain Alabdein – ID : **320254015**
Mohamed Abdelmoneom Saad – ID : **21028599**

Team Responsibilities:

Mustafa: Responsible for setting up the network infrastructure.
Zeyad: Tasked with configuring standard and extended ACLs to control traffic flow.
Ahmed: Handled the implementation of NAT (Static and PAT) to manage IP address translations and enhance security.
Mohamed: Focused on integrating ACLs and NAT into the existing network, conducting a comprehensive security assessment, and implementing port, DHCP, and ARP security.

Network Diagram for MMZA Factory Simulation

The following image illustrates the complete network architecture for the MMZA factory. The network is designed to support three branches, each with its own isolated network, all connected to a central server hub. The layout ensures high-level security and efficient data transmission between the branches.



Network Description:

The network consists of three main areas, each representing a branch of the MMZA factory.
Each branch has its own private network, ensuring that internal communication remains secure.
All branches are connected to a central hub where critical servers are located, including FTP and HTTP servers.
ACLs (Access Control Lists) and NAT (Network Address Translation) have been implemented across the network to regulate traffic flow, enhance security, and manage IP addresses efficiently.
The configuration ensures that the servers are hidden and only accessible through secure and controlled access points, with all necessary backups in place to prevent data loss.

Timeline:

Week 1: ACL configuration for all branches.
Week 2: NAT implementation and testing.
Week 3: Integration of the branch networks with the central server hub, followed by a security assessment.
Week 4: Documentation and final presentation of network security improvements.

Conclusion:

The project has been completed successfully. All required tasks were executed, resulting in a secure and efficient network infrastructure for the MMZA factory's three branches. The organization now benefits from enhanced security, traffic control, and better IP address management across its networks.