Project 4

Supervised by: Eng Khaled Abd Rabo

Name	tasks
Mazen Tarek(team leader)	Project management ACL's troubleshooting
Adel Mohammed	NAT ACL's troubleshooting
Mohammed Gamal	Security A**ssessment** NAT Documentation
Peter Samir	Documentation Network Design
Youssif Aly	ACL's Presentation Network Design
Mahmoud Ragab	Presentation Network Design

Introduction

Implementing Network Security with ACLs and NAT, focuses on enhancing network security by using Access Control Lists (ACLs) and Network Address Translation (NAT). The goal is to secure internal resources while allowing controlled access to external networks. This project was structured into four weeks, where each phase built upon the previous to create a secure and manageable network infrastructure.

- Week 1: Configuration of Standard and Extended ACLs to control traffic flow and manage access to network resources.
- Week 2: Implementation of NAT to manage IP address translations.
- Week 3: Integration of ACLs and NAT with a thorough security assessment.
- Week 4: Documentation of findings, configuration details, and network performance improvements.

The project demonstrates the practical application of ACLs and NAT to secure a network, ensuring access control and protecting internal resources from external threats.

Network Design Overview

Network Components:

PCs:

- PC0: 192.168.1.10/24
- PC1: 192.168.1.20/24
- PC2: 192.168.3.10/24
- PC3: 192.168.3.20/24

Servers:

- HTTP Server: 192.168.2.10/24
- FTP Server: 192.168.2.20/24
- Server2 192.168.200.10/24 (Mapped to Public IP: 41.44.170.253)

Routers:

R1:

- Gig0/0: 192.168.1.1/24
- Gig0/1: 172.16.10.1/30
- Gig0/2: 192.168.2.1/24
- Static Route: 0.0.0.0/0 → 172.16.10.2

R2:

- Gig0/0: 172.16.10.2/30
- Gig0/1: 10.0.0.1/30
- Gig0/2: 10.20.20.1/30
- **Dynamic NAT Pool**: 209.165.200.226 - 209.165.200.240

R3:

- Gig0/0: 10.0.0.2/30
- Gig0/1: 192.168.3.1/24
- **Static Route**: 0.0.0.0/0 → 10.0.0.1

R4:

- Gig0/0: 10.20.20.2/30
- Gig0/1: 192.168.200.1/24
- Static NAT: 192.168.200.10 → 41.44.170.253 (Public IP)

Switches:

- Sw1: Connected to PC0, PC1, and R1.
- Sw2: Connected to HTTP and FTP servers (Server0 and Server1).
- Sw4: Connected to public server (Server2) and R4.

Configuration Details

Week 1: ACL Configuration

Task: Implement ACLs to control traffic and secure network access.

Standard ACL 10 (on Router R3):

- Denies access to internal network (192.168.3.0/24).
- Allows other traffic from public sources.

- Extended ACL 100 (on Router R1):

- Allows PC0 and PC1 to communicate with the HTTP server (192.168.2.10) but only PC1 can communicate with the FTP server (192.168.2.20).
- Restricts access to other services for internal security.

Week 2: NAT Implementation and Testing

Task: Implement NAT (Static and PAT) for IP address management and security.

-Dynamic NAT: Configured on Router R2 using a pool of public IPs (209.165.200.226 - 209.165.200.240). This allows internal users from any LAN to access the internet using an external public IP address.

-Static NAT: Configured on Router R4 to map the internal server (192.168.200.10) to a public IP address (41.44.170.253). This enables public access to the server while protecting the internal network.

Week 3: Integration and Security Assessment

Task: Integrate ACLs and NAT into the network and perform a security assessment.

- Integration: The ACLs and NAT were integrated, ensuring that:
  - PC0 and PC1 can access the HTTP server.
  - Only PC1 has access to the FTP server.
  - PCs from LAN 3 (PC2 and PC3) can only access the internet and not internal resources.
  - External entities are denied access to LAN1, HTTP, and FTP servers.

-Security Assessment: Conducted to evaluate potential vulnerabilities. The assessment showed that unauthorized access attempts to internal resources were blocked, ensuring that the network adhered to security best practices.

Overall all security measurements were checked.

Week 4: Documentation and Final Presentation

Task: Document the entire project, including configurations, improvements, and performance analysis.

- Final Report: Detailed the configuration of ACLs and NAT, integration results, and overall security improvements. Specific areas of improvement included enhanced access control for internal users and isolation of guest network segments.

Network Behavior

- LAN 1 (PC0, PC1):
  - PC0 can access the HTTP server.
  - PC1 can access both HTTP and FTP servers.
  - Both PCs are restricted from allowing outsiders into LAN 1.

LAN 3 (PC2, PC3:

- PCs are isolated and can only access the internet (no internal resources).

- Internet Access:

- All users from any LAN can access the internet via the NAT setup.

- LAN 2 Public Server (Server2 the internet) :

- External users can access Server2 (mapped via static NAT to public IP 41.44.170.253).

Conclusion

This project successfully demonstrated the implementation of ACLs and NAT to enhance network security. By controlling traffic using ACLs and managing public IP addresses with NAT, the network was secured against unauthorized access, while allowing controlled access to necessary resources. The final security assessment confirmed the effectiveness of the implemented solutions, ensuring that internal network resources were protected while maintaining efficient network performance.