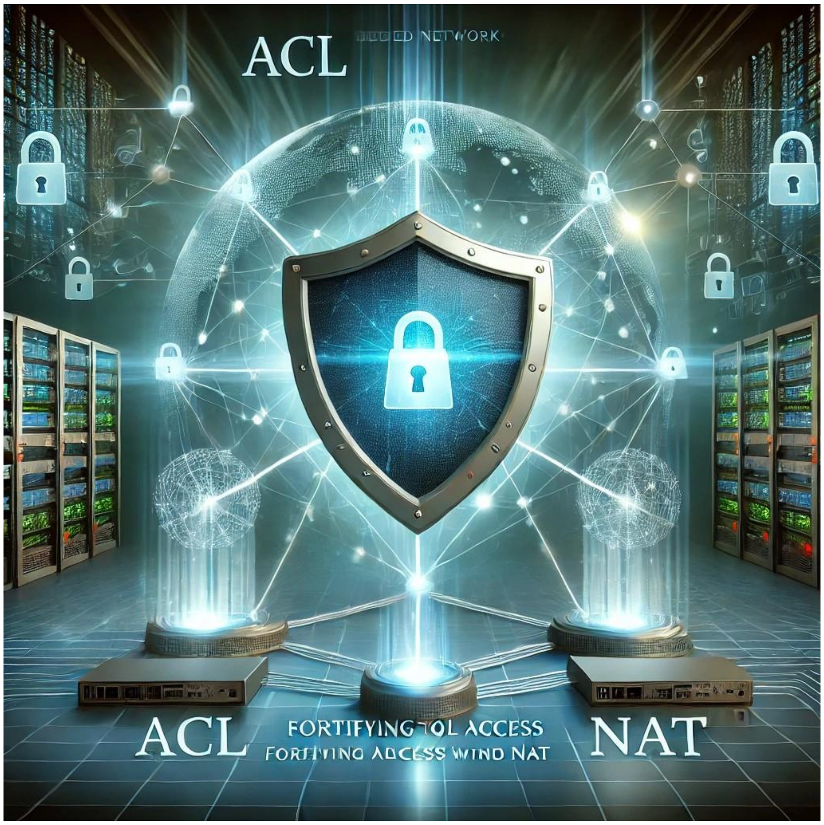
رواد مصر الرقمية



THE SHIELDED NETWORK

Fortifying Access with ACLs and NAT

Eng / Al Hussein Ahmed

TEAM MEMBERS:

Manar Nasser

Malak Abdelaziz

Yassin Tamer

Abdallah Mohamed

Zaid Ali

رواد مصر الرقمية

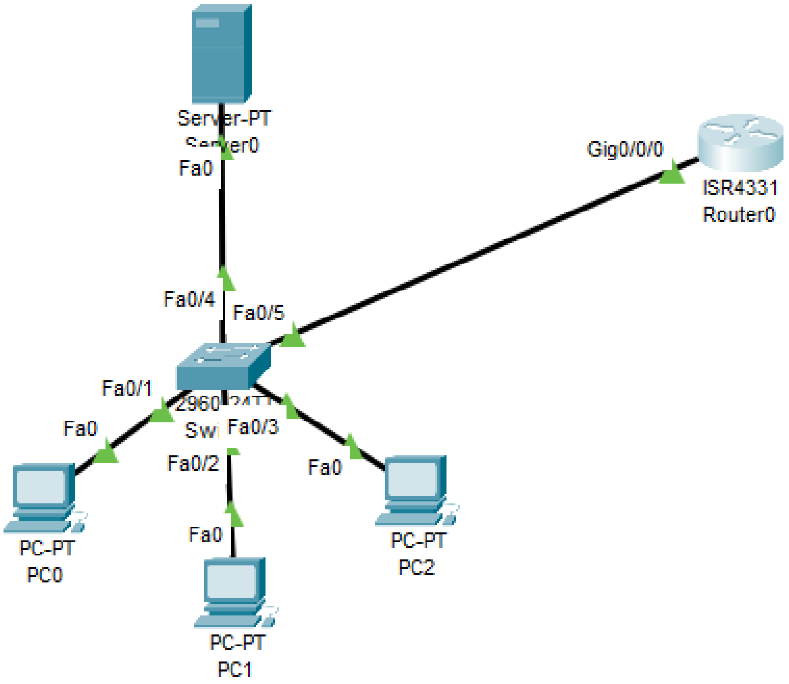
The Shielded Network

<< Fortifying Access with ACLs and NAT >>

Project Overview:

- **Objective:** Secure network traffic using ACLs and manage IP address usage using NAT.
- **Tools:** Cisco Packet Tracer
- **Scope:**
    - Filter network traffic using ACLs
    - Enable secure internet access using NAT
    - Ensure internal network devices are protected from unauthorized access

Network Topology Design:



- Router (R1): Connects the internal network to the internet.
- Switch (SW1): Connects internal devices.
- LAN (192.168.1.0/24): Private network.
- WAN (Public IP): Internet-facing interface.
- **Devices:**
    - PCs (192.168.1.3-5)
    - Server (192.168.1.2)
    - Internet Gateway

Project Plan:

Phase 1: NAT Configuration

- Configure NAT to allow internal devices to access the internet using a single public IP (PAT).

Phase 2: ACL Implementation

- Create and apply ACLs to:
    - Block unauthorized traffic.
    - Allow HTTP (Port 80) and HTTPS (Port 443) traffic.
    - Deny Telnet (Port 23) access from external networks.

Phase 3: Testing and Verification

- Verify NAT translations.
- Verify ACL rules.