

Daffodil International University

**Group Project**

**Submitted To : Ms. Chayti Saha**

**Lecturer, Department of Computer Science and Engineering Daffodil International University**

**Submitted By :**

|  |  |
| --- | --- |
| **Mobassir Mahmud Dibbo** | **1718** |
| **Md. Shahoriar Jami Tonmoy** | **1788** |
| **Apra Rani** | **1823** |
| **Mst.Lamiya Khatun** | **1840** |
| **Tasmim Noshrat Jahan Charu** | **1844** |

**Project Report: Security Protocol Implementation for DIU’s Online Examination System**

# Project Overview

## Objective:

The primary goal of this project is to establish a secure network environment to support an online examination system. This network is designed to protect sensitive exam data, manage access controls based on specified hours, and ensure continuous monitoring to prevent unauthorized access. The system leverages firewalls, intrusion prevention systems (IPS), and network address translation (NAT) to safeguard the internal network from external threats.

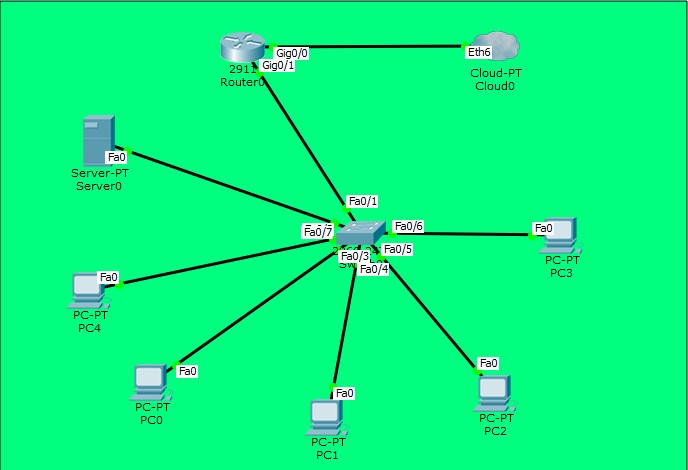
## System Requirements:

* 1. Implement a firewall to manage and restrict access to the exam server.
  2. Configure an intrusion prevention system (IPS) for proactive threat detection.
  3. Enable Network Address Translation (NAT) for internal network security.
  4. Use DHCP for dynamic IP allocation within the local network.
  5. Set up access control based on exam timings.
  6. Configure logging for monitoring and security analysis.

# Network Topology and Architecture

The network architecture is designed with layered security controls to minimize the risk of unauthorized access while allowing seamless access for students during exam hours.

## Figure:



**Devices and Roles:**

* **Router0 (Cisco 2911)**: Acts as the firewall and the main security device, managing access control, IPS, and NAT.
* **Switch0 (Cisco 2960)**: Connects all PCs and the server to Router0, facilitating internal communication.
* **Server0**: Hosts the online examination application and is configured as the exam server.
* **PCs (PC0 - PC4)**: Represent student workstations that will access the exam server.
* **Cloud0**: Simulates the internet connection, connecting Router0’s GigabitEthernet0/0 interface to external networks.

## Network Connections:

* **Router0 to Cloud0**: Connected through GigabitEthernet0/0, which acts as the WAN port for internet access.
* **Router0 to Switch0**: Connected via FastEthernet interfaces, allowing the router to manage internal network traffic.
* **Server0 to Switch0**: Connected through FastEthernet0, serving as the main point of access for students during exams.

## IP Address Allocation:

* **Internal Network**: 192.168.1.0/24 subnet.
* **Server IP**: 192.168.1.10.
* **DHCP IP Pool**: 192.168.1.11 - 192.168.1.20 for student PCs.

# Router0 Configuration (Firewall and Security Protocols)

Router0 serves as the core of the network’s security, providing firewall functions, IPS capabilities, NAT, DHCP, and time-based access control.

## Basic Router Setup

* + - **Hostname and Password Protection**:
      * The router hostname is set to DIU-ExamFirewall for identification.
      * A secure password is configured for privileged EXEC access using the command enable secret Exam$3cur3P@ss.
      * This ensures that only authorized administrators can configure the router settings.

## Interface Configuration

* + - **GigabitEthernet0/0** (Internet-Facing Interface):
      * This interface connects the router to the internet and has an IP assigned by the external network.
      * The interface is configured as ip nat outside to allow NAT translation for outgoing traffic.
    - **GigabitEthernet0/1** (Internal Network Interface):
      * This interface connects the router to the internal network.
      * IP Address: 192.168.1.1 (gateway for internal devices).
      * Configured as ip nat inside to enable NAT for internal traffic.

## DHCP Configuration

* + - **DHCP IP Pool (EXAM\_POOL)**:
      * Configured to allocate IPs dynamically within the range 192.168.1.11 - 192.168.1.20.
      * Excluded IPs: 192.168.1.1 - 192.168.1.10 to prevent conflicts with static IPs for the gateway and server.
      * DHCP ensures that student PCs can easily connect to the network without manual IP configuration.

## Network Address Translation (NAT)

* + - **NAT for Security**:
      * NAT is configured to map internal IPs to a single public IP for secure external communication.
      * This prevents external users from directly accessing internal IPs, adding a layer of security by keeping internal devices hidden.

## Time-Based Access Control (ACLs)

* + - **Exam Access Control List (EXAM\_HOURS)**:
      * ACL EXAM\_HOURS is created to restrict access to the exam server (192.168.1.10) based on specified exam timings.
      * Only traffic to and from the server on specific ports (e.g., HTTP/HTTPS) is allowed during EXAM\_TIME.

## Time Range Configuration (EXAM\_TIME):

* + - * Defined to enforce access only during weekdays from 9:00 AM to 5:00 PM.
      * The router checks the time before permitting access, ensuring that the exam server is only accessible during scheduled hours.

## Intrusion Prevention System (IPS) Configuration

* + - **IPS for Threat Detection**:
      * IPS configuration, labeled EXAM\_IPS, monitors network traffic to detect and prevent intrusions.
      * IPS is set to log suspicious activity and alert administrators for immediate response.
      * Categories are specified to classify different types of attacks (e.g., basic-attack- category).

## Logging Configuration

* + - **Logging and Monitoring**:
      * Logging is configured to buffer messages and capture security-related events for review.
      * Console logging is enabled to display real-time alerts, and critical logs are stored for later analysis.
      * This setup helps in monitoring access attempts, identifying unauthorized users, and reviewing potential security breaches.

# Server0 Configuration

The exam server (Server0) is configured with a static IP to ensure stable connectivity and reliable access during exams.

## Server0 IP Configuration

* **IP Address**: 192.168.1.10 (static)
* **Subnet Mask**: 255.255.255.0
* **Default Gateway**: 192.168.1.1
* **DNS Server**: 8.8.8.8 (for internet name resolution)

The server is isolated from external traffic except during scheduled exam hours, thanks to the ACL configurations on Router0. Only internal IPs in the specified range can access the server, ensuring that only authenticated users within the local network are granted access.

# PC Configuration (PC0 - PC4)

Each student PC (PC0 - PC4) is configured to receive IP addresses dynamically via DHCP from Router0, simplifying network management and ensuring seamless connectivity.

## PC DHCP Configuration

* **IP Allocation**: Dynamic (within 192.168.1.11 - 192.168.1.20 range)
* **Network Mask**: 255.255.255.0
* **Default Gateway**: 192.168.1.1

The PCs are designed for exam access only during the specified hours, with all internet traffic routed through the router’s firewall, where IPS and NAT further secure the network.

# Security Features

This network design incorporates multiple security layers to ensure the integrity and confidentiality of the online examination system:

## Firewall

* + - The firewall blocks unauthorized traffic and enforces access control rules based on IP and port.
    - Access is restricted to the exam server and only permitted during exam hours.

## Intrusion Prevention System (IPS)

* + - IPS is configured to detect malicious traffic patterns and prevent potential threats.
    - Suspicious activities are logged, allowing for quick responses to attempted intrusions.

## Network Address Translation (NAT)

* + - NAT hides internal IPs from external networks, ensuring that external users cannot directly reach internal devices.

## Time-Based Access Control

* + - Access control lists (ACLs) restrict traffic based on defined exam times.
    - Access is denied outside of exam hours, securing the server from unauthorized or accidental access.

## Logging and Monitoring

* + - Logging helps track all security events and can assist in investigating security incidents.
    - Buffering logs and console alerts provide administrators with a detailed view of network activity.

# Conclusion

This project effectively implements a secure network environment for DIU’s online examination system. The setup includes firewall rules, IPS, NAT, DHCP, and time-based access control to restrict access to authorized users and timeframes. By enforcing strict access controls and logging, the network protects sensitive exam information and ensures reliability during exams.

This report serves as a blueprint for the secure deployment and management of an online examination platform, showcasing a layered security approach essential for academic institutions.