# Firewall and Web IP Configuration Report

## 1. Introduction

In this project, we utilized Cisco Packet Tracer to configure a network with a functional firewall that allows specific web IP access while restricting others. The objective was to simulate and validate firewall functionality in securing a network, ensuring only authorized IPs have access to specific services.

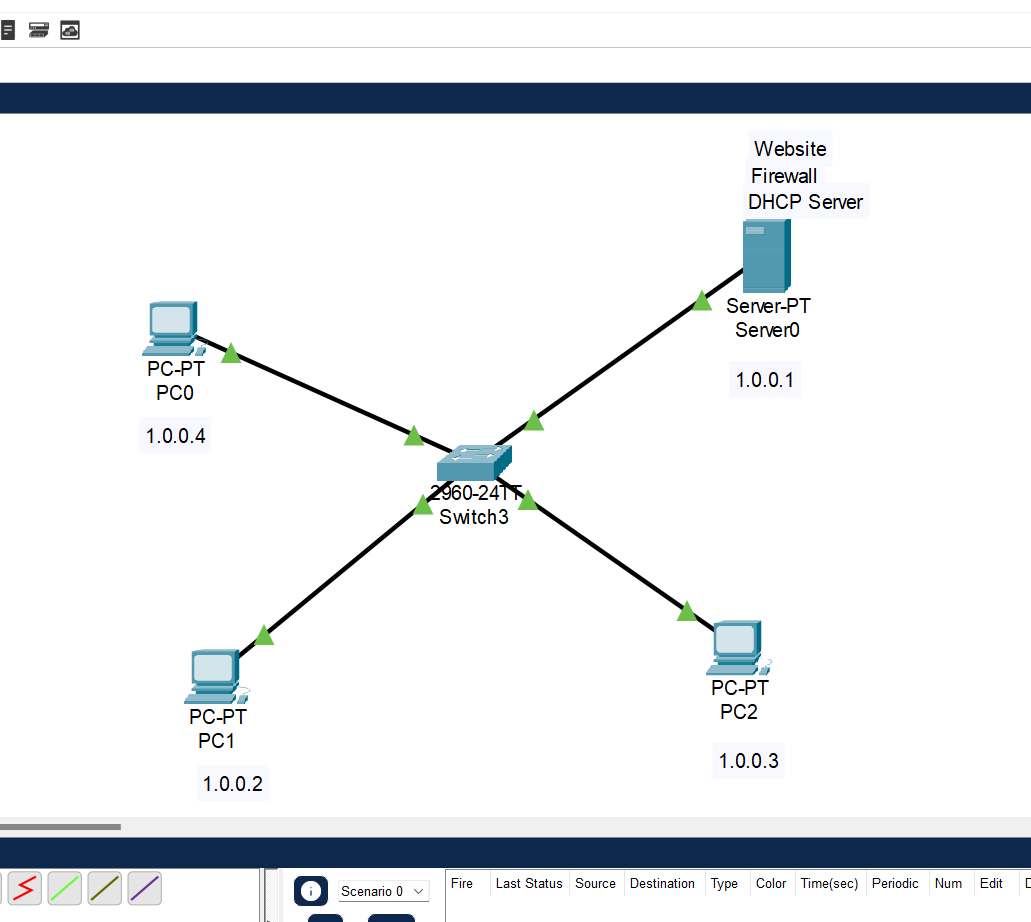
## 2. Network Topology

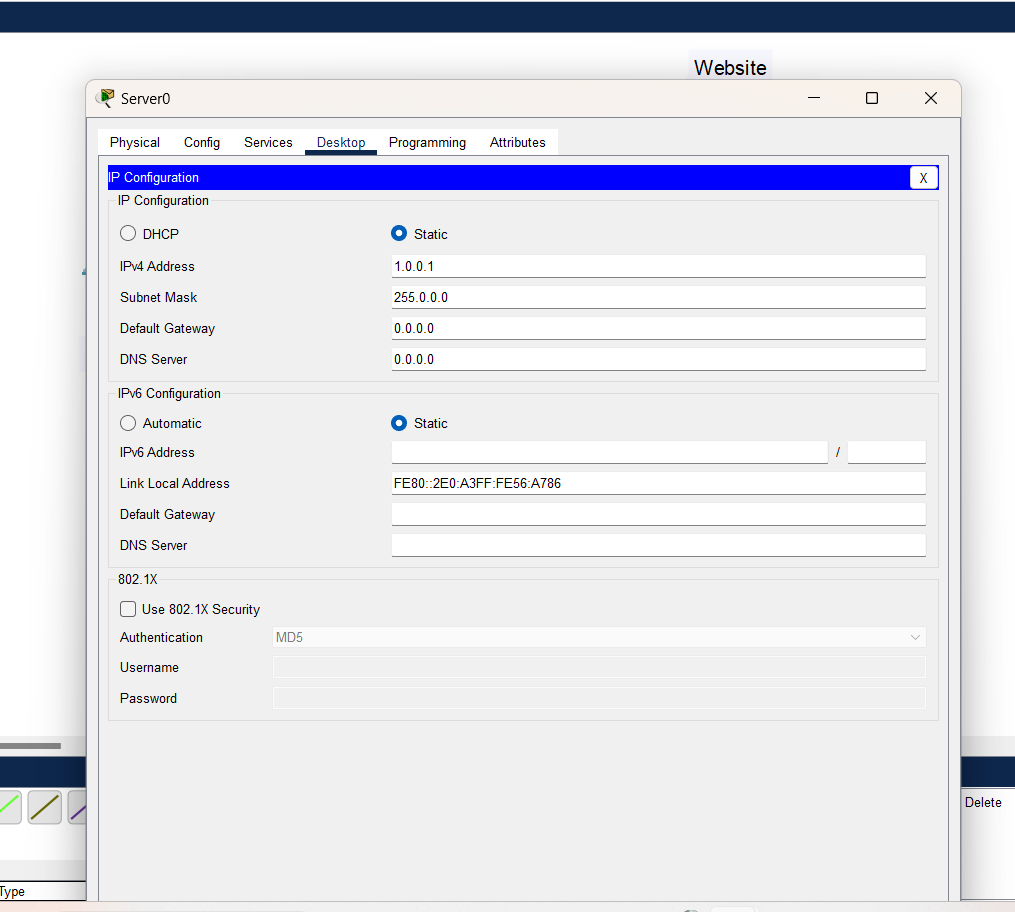
The network consisted of the following components:  
- DHCP Server: Automatically assigns IP addresses to devices in the network.  
- Three PCs (PC0, PC1, and PC2): Simulated client machines.  
- Router with Firewall Rules: Implements firewall policies.  
- Server: Hosts web services to test access rules.  
  
Each component was configured to communicate efficiently while adhering to firewall policies.

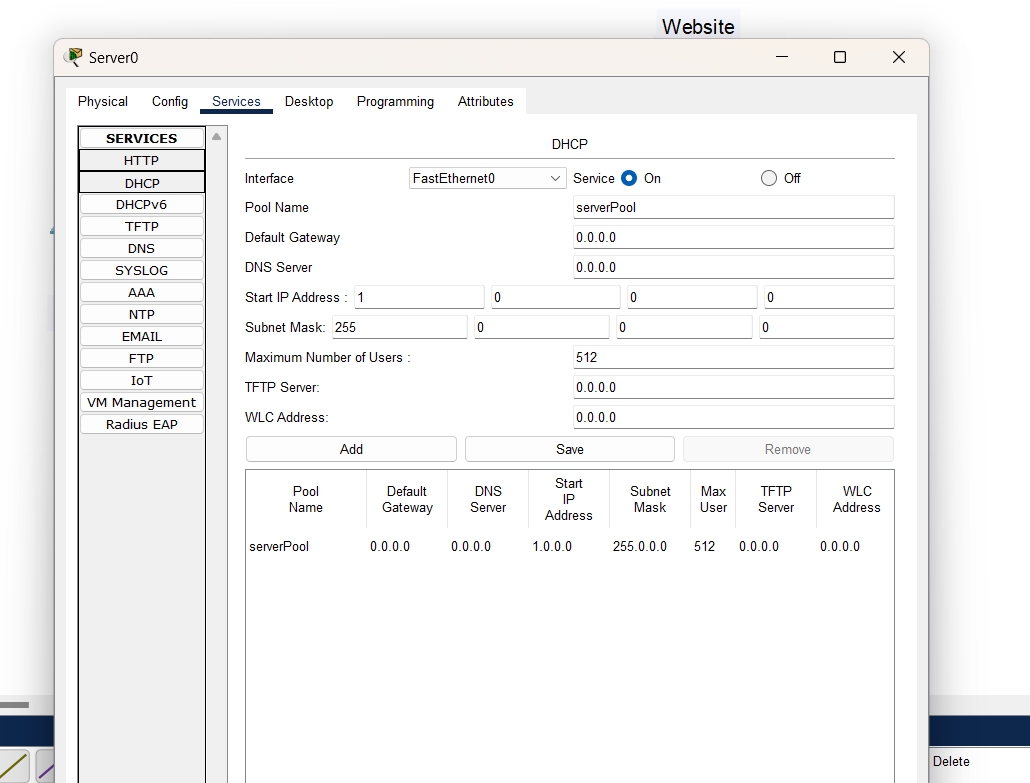
## 3. Configuration Steps

### 3.1 Setting Up the DHCP Server

A DHCP server was configured to automate IP address allocation across devices in the network. The configuration ensured no manual IP address assignment was needed.



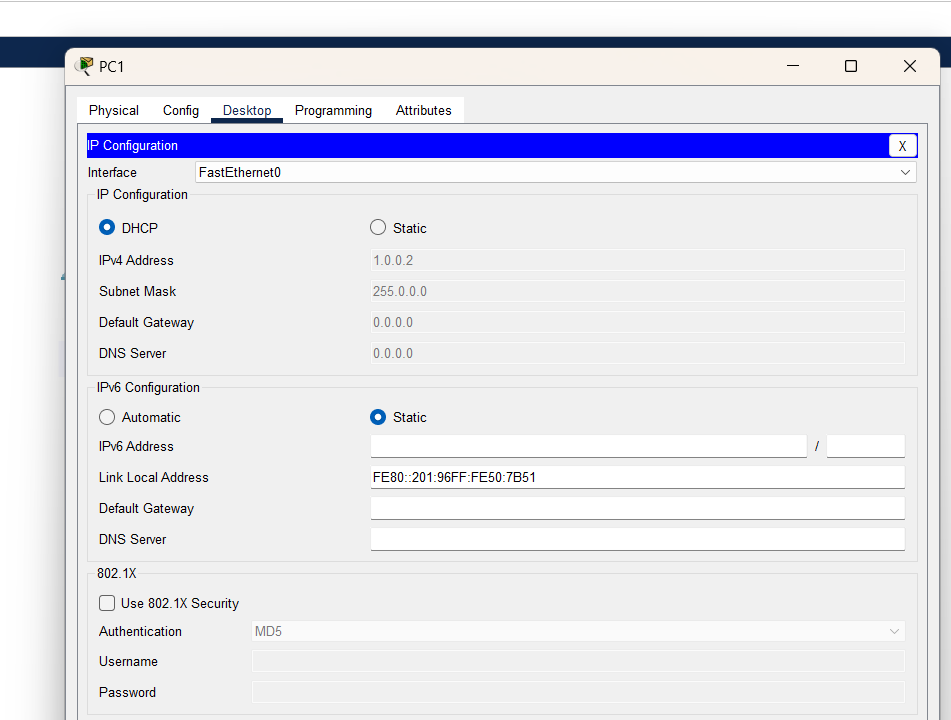




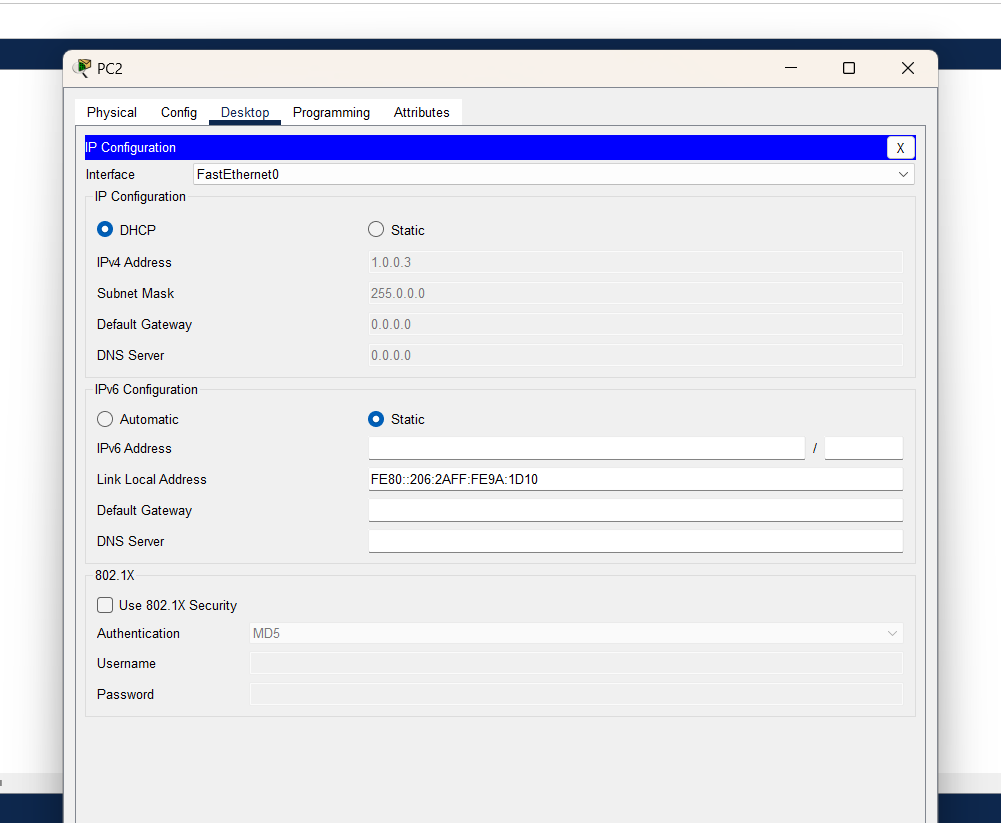
### 3.2 Assigning IP Addresses

The DHCP server assigned IP addresses to all devices. Here are the details of the assigned IPs:

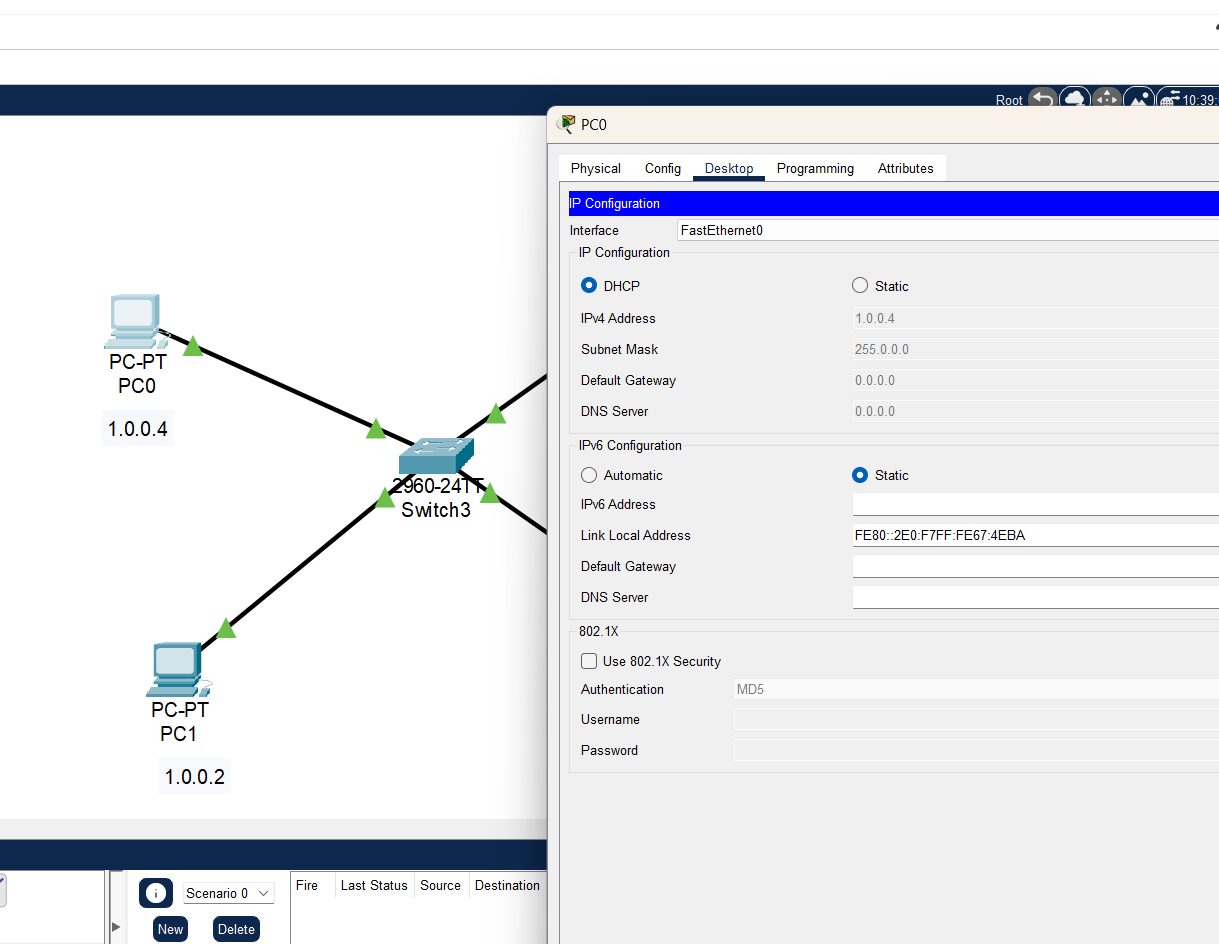
**IP Address of PC1**



**IP Address of PC2**



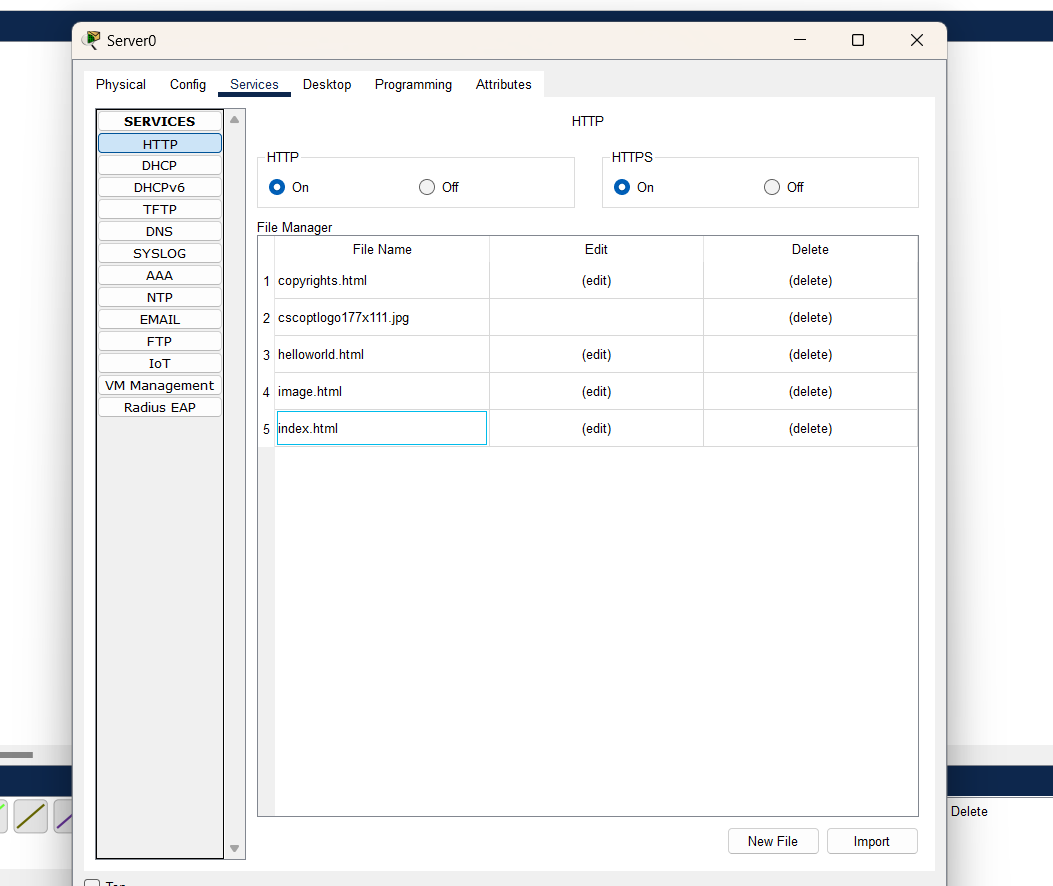
**IP Address of PC0**

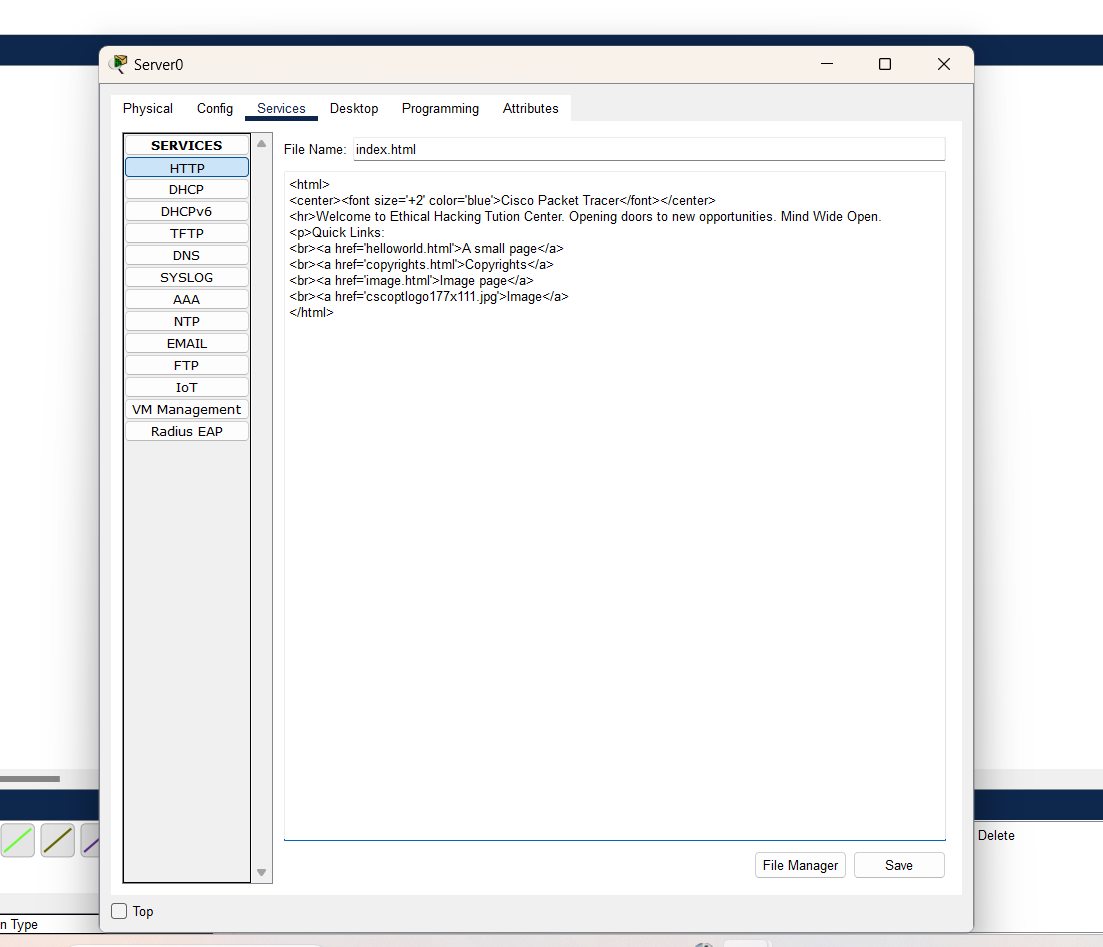


### 3.3 Editing HTTP Settings

The HTTP settings on the server were modified to allow web service access. This step was essential for verifying the firewall’s ability to control access.

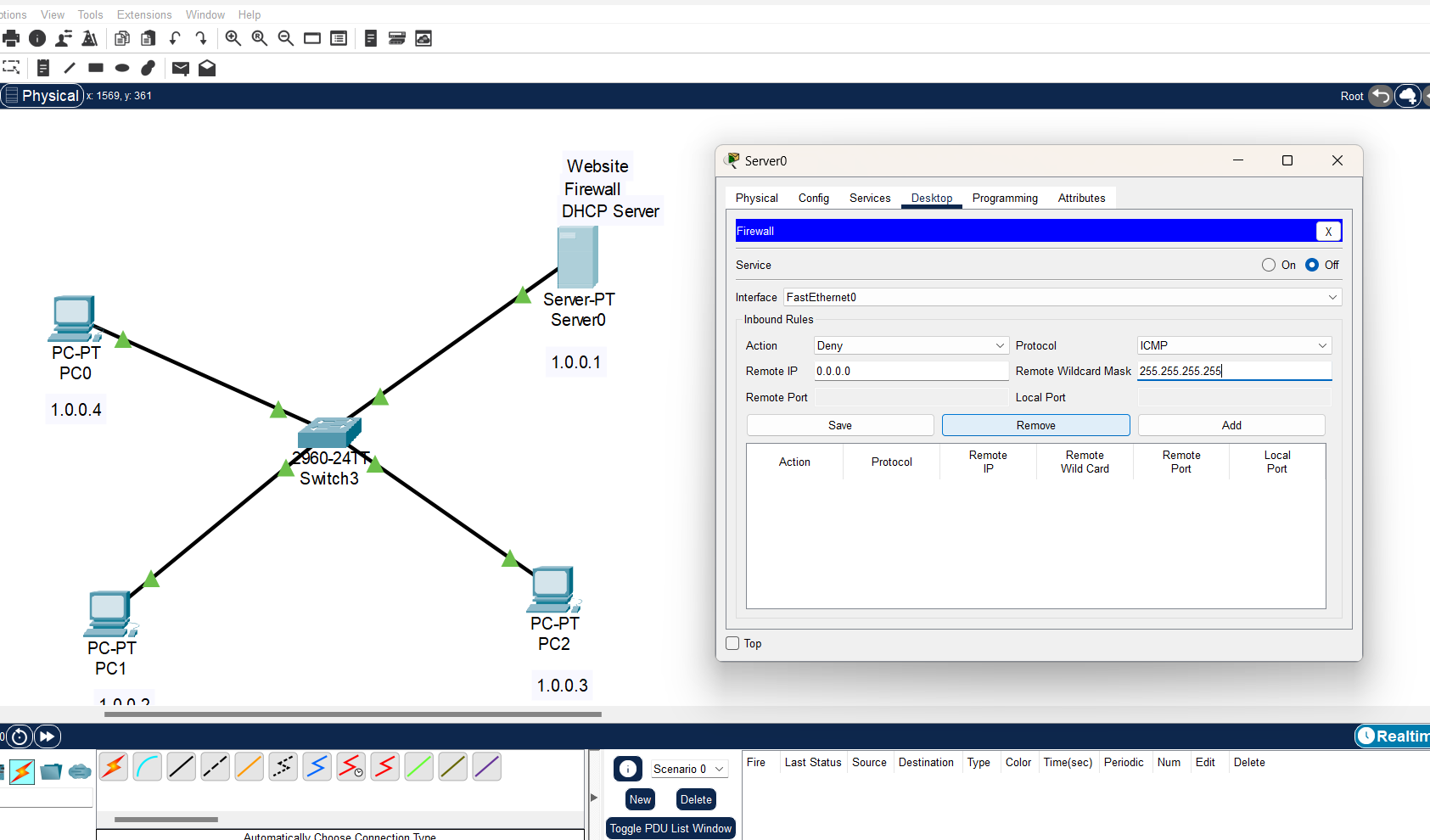
**HTTP Settings**

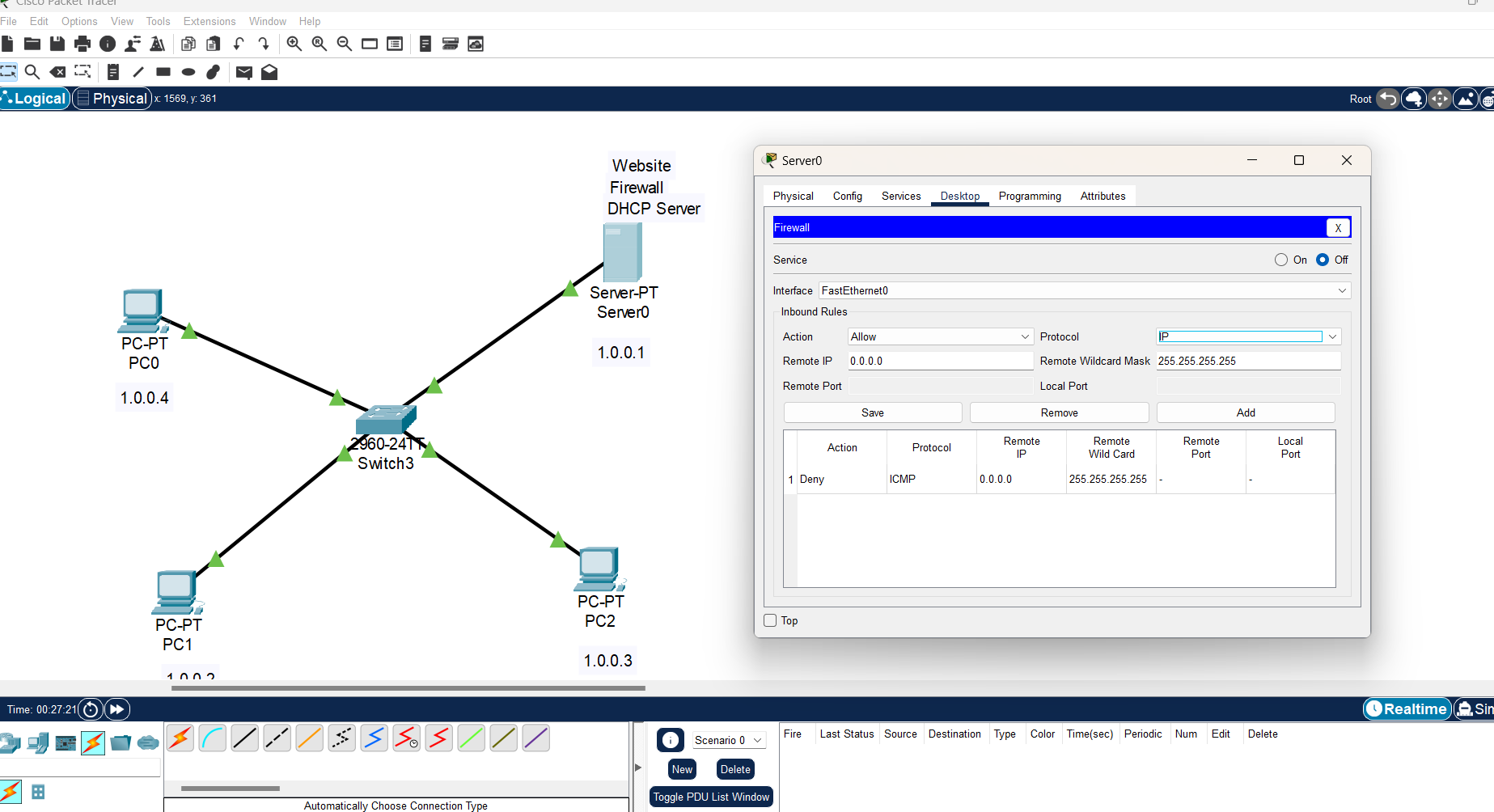


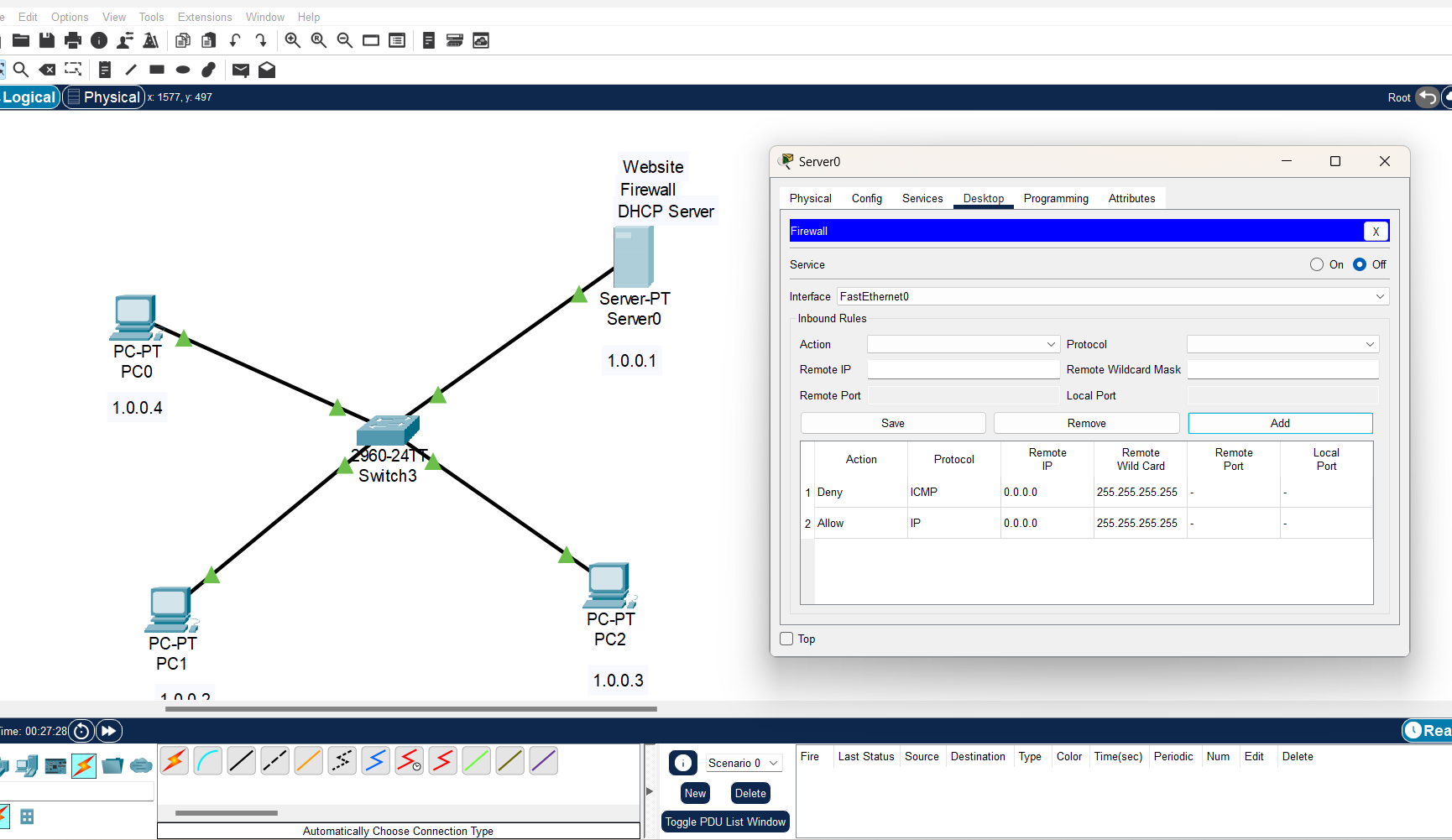


### 3.4 Configuring Firewall Rules

Two firewall rules were added to regulate traffic:  
1. Deny ICMP: Prevents ping requests to the server, ensuring minimal exposure.  
2. Allow Specific IPs: Grants access to authorized IPs for web services.





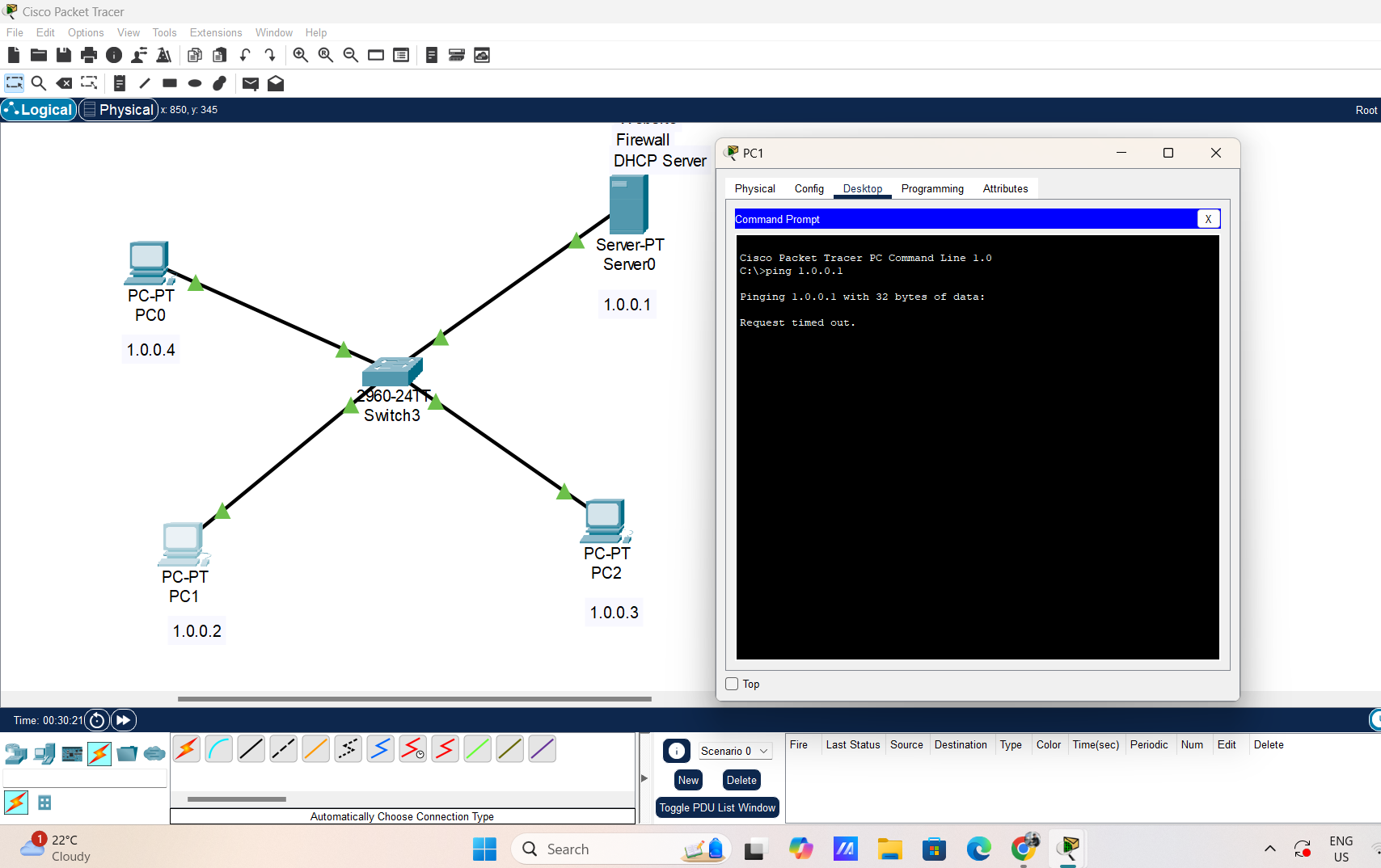


### 3.5 Testing the Firewall

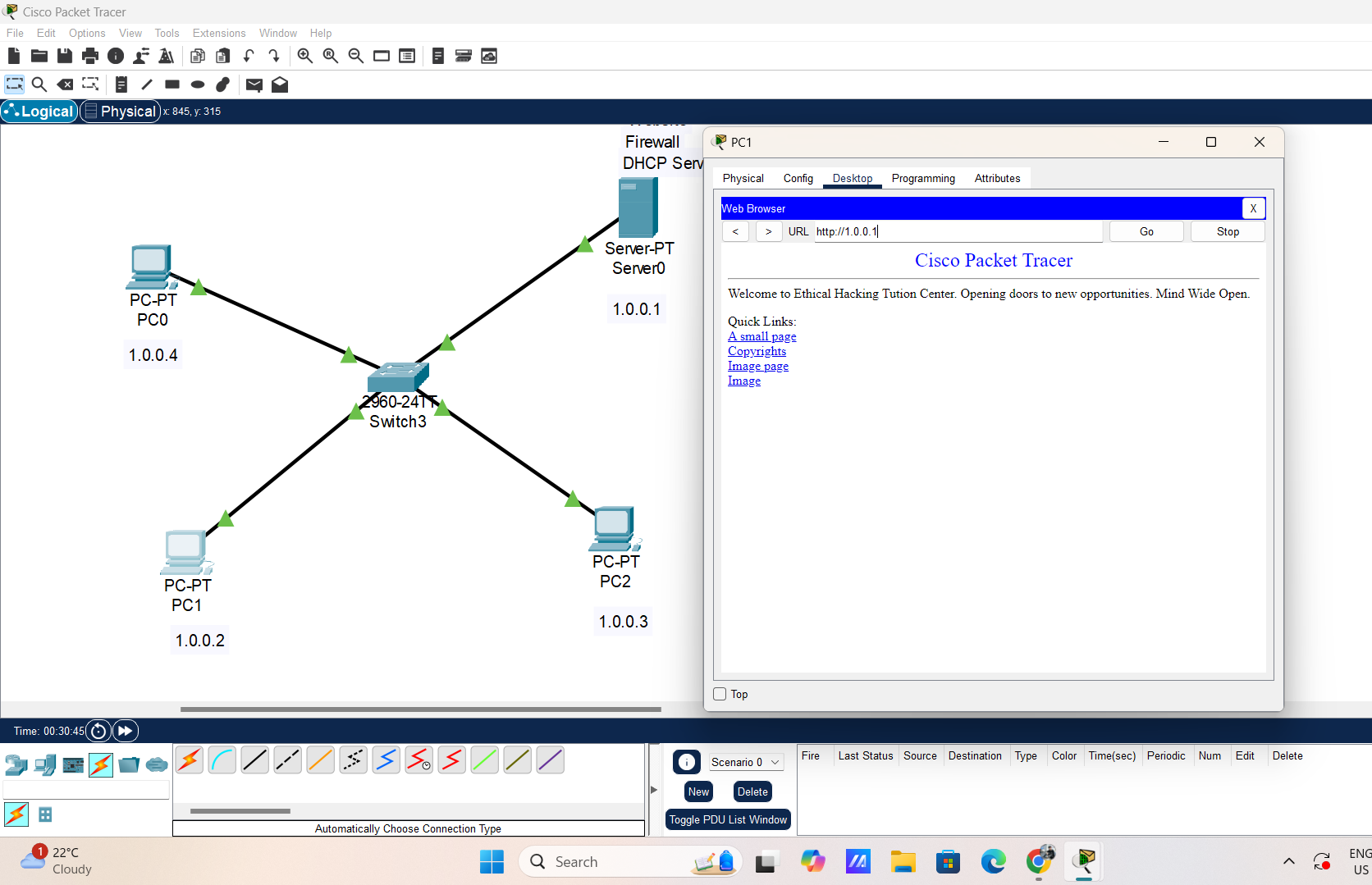
To validate the configurations, we conducted the following tests:

1. Denying ICMP: Attempted to ping the server from a client PC.  
2. Allowing Web IPs: Accessed the web server from an allowed IP.  
3. Ping Test: Verified network connectivity and tested exceptions in firewall rules.

**Testing Deny ICMP**



**Testing Allow IP**



## 4. Results and Observations

The configured firewall successfully restricted ICMP traffic while allowing web access to specific IPs. These results validate the effectiveness of the implemented rules in protecting network resources and ensuring controlled access.

## 5. Conclusion

This project demonstrated how to configure a functional firewall in Cisco Packet Tracer. By implementing specific rules, we ensured secure web access while preventing unauthorized traffic. This setup is an example of foundational network security practices, which can be expanded with more complex policies for advanced scenarios.