Experiment -1

Date: 9/7/25

Basic Firewall Configuration in Cisco Packet Tracer

AIM:

To configure and verify basic firewall settings in Cisco Packet Tracer.

PROCEDURE:

1. Step 1: First, open the Cisco packet tracer desktop and select the devices given below:

- IP Addressing Table:

Then, create a network topology as shown below the image.
Use an Automatic connecting cable to connect the devices with others.

2. Step 2: Configure the PCs (hosts) and server with IPv4 address and Subnet Mask according to the IP addressing table given above.

To assign an IP address in PC0, click on PC0.
Then, go to desktop and then IP configuration and there you will find IPv4 configuration.
Fill IPv4 address and subnet mask.
Repeat the same procedure with the server.

3. Step 3: Configuring the firewall in a server and blocking packets and allowing web browser.

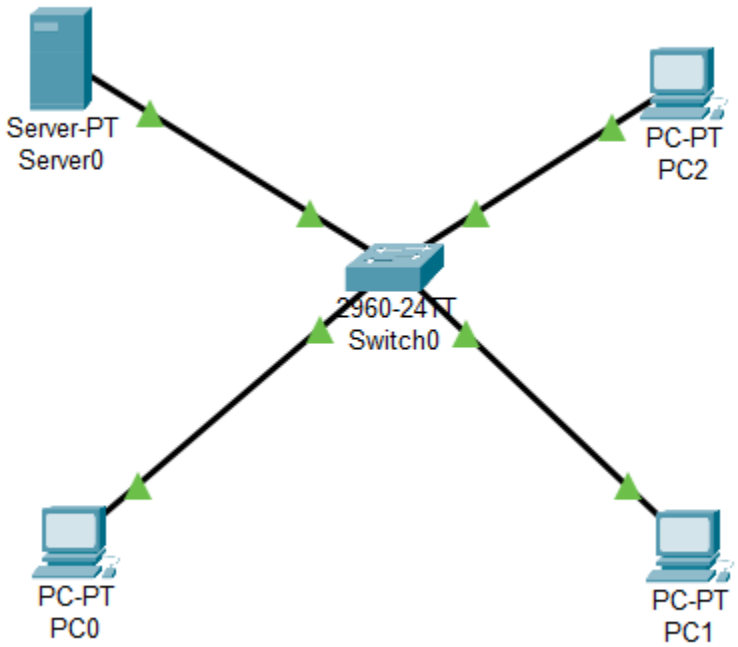
Click on server0 then go to the desktop.
Then click on firewall IPv4.
Turn on the services.
First, Deny the ICMP protocol and set remote IP to 0.0.0.0 and Remote wildcard mask to 255.255.255.255.
Then, allow the IP protocol and set remote IP to 0.0.0.0 and Remote wildcard mask to 255.255.255.255.
And add them.

4. Step 4: Verifying the network by pinging the IP address of any PC.

We will use the ping command to do so.
First, click on PC2 then Go to the command prompt.
Then type ping <IP address of targeted node>.
We will ping the IP address of the server0.
As we can see in the below image we are getting no replies which means the packets are blocked.

Check the web browser by entering the IP address in the URL.
Click on PC2 and go to desktop then web browser.

OUTPUT:



RESULT:

The ICMP protocol is blocked as expected and HTTP traffic is allowed, verified using the web browser.