Exp no : 01 Basic Firewall Configuration in Cisco Packet Tracer
Date 14/07/2025

Aim:

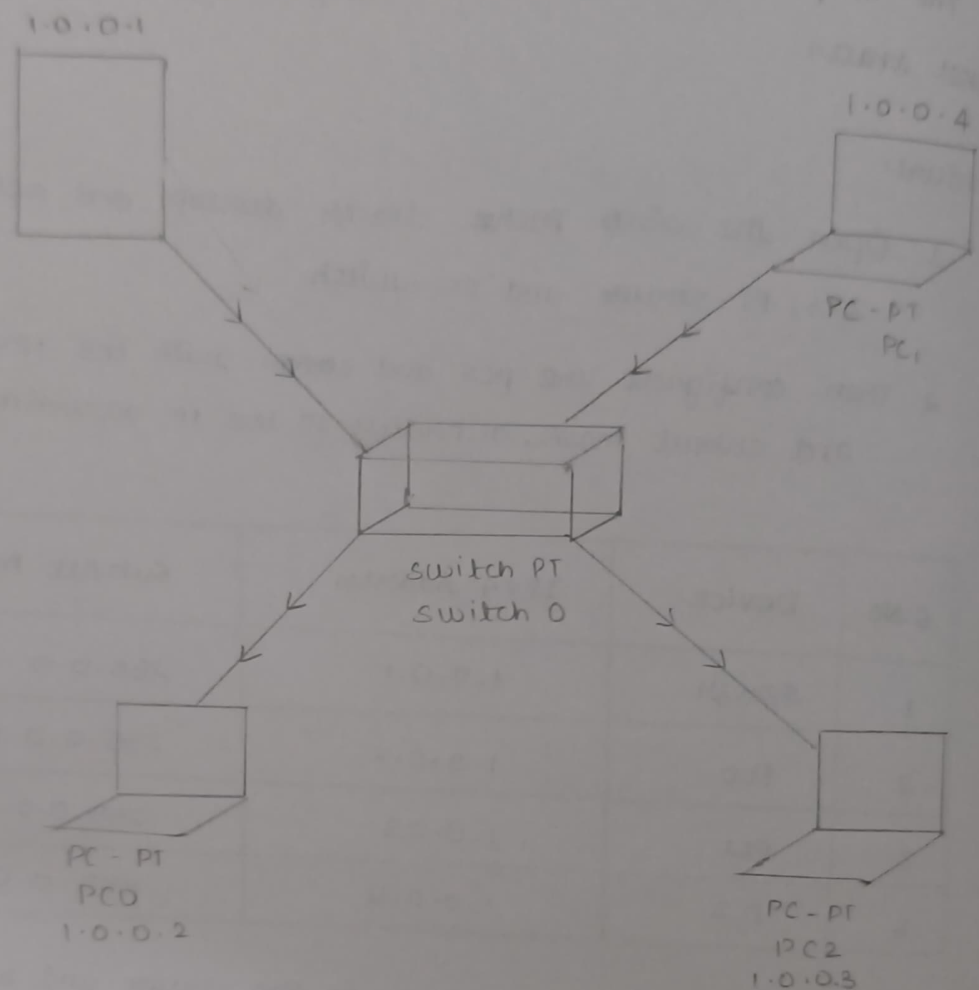
The steps to configure and verify firewall in cisco packet tracer

Procedure:

1. Open the cisco packet tracer desktop and select the devices: 3pcs, PT-server and PT-switch
2. Then configure the pcs and server with the IPv4 addresses and subnet mask, according to the IP addressing table

S.NO	Device	IPv4 Address	Subnet mask
1	server	1.0.0.1	255.0.0.0
2	PC0	1.0.0.2	255.0.0.0
3	PC1	1.0.0.3	255.0.0.0
4	PC2	1.0.0.4	255.0.0.0

3. configuring the firewall in the server and blocking packets and allowing web browsing
4. Click on server, then turn on the services. First, deny the ICMP protocol and set IP to 0.0.0.0 and remote wildcard 255.255.255.255
5. Then, allow the IP protocol and set IP remote to 0.0.0.0 and remote wildcard mask to 255.255.255.255
6. Verify the network by pinging the IP addresses of an PC. Type ping <IP address of targeted node>
This will ping the IP addresses of the server


1.0.0.1
1.0.0.4
PC-PT
PC1
Switch PT
Switch 0
PC - PT
PC0
1.0.0.2
PC-PT
PC2
1.0.0.3

7. "Getting no replies" which means the packets are blocked

8. If replies, which means the packets are not blocked

9. Check the web browser by entering IP address in URL

O/P:

1) Allow the IP Protocol and ping that command in PC2

C:\>ping 1.0.0.1

Pinging 1.0.0.1 with 32 bytes of data

Reply from 1.0.0.1: bytes = 32 time < 1ms TTL = 128

Reply from 1.0.0.1: bytes = 32 time < 1ms TTL = 128

Ping statistics for 1.0.0.1:

Packets: sent = 4, Received = 4, lost = 0 (0% loss).

Approximate round trip times in milli-seconds

Minimum = 0ms, Maximum = 0ms, Average = 0ms

2) Deny the ICMP protocol and ping that command in PC2:

C:\> ping 1.0.0.1

Pinging 1.0.0.1 with 32 bytes of data

Request timed out

Request timed out

Request timed out

Ping statistics for 1.0.0.1

Packets: sent = 4, Received = 0, lost = 4 (100% loss)

Result:

Thus, the firewall configuration and verifies firewall was successfully executed and the output is verified.