Lab – Firewall Configuration on a Server

Overview:

A firewall is a network security device or software application that acts as a barrier between a trusted internal network and untrusted external networks, such as the Internet. It monitors and controls incoming and outgoing network traffic based on predetermined security rules. The primary purpose of a firewall is to protect the internal network from unauthorized access, malicious attacks, and other potential security threats. Firewalls operate by inspecting packets of data as they pass through the network and making decisions about whether to allow or block them based on predefined criteria. These criteria typically include factors such as the source and destination IP addresses, port numbers, protocols, and the connection state. Firewalls can be configured to enforce access control policies, filter network traffic, and log information about traffic patterns and security events.

There are several types of firewalls, including packet filtering firewalls, stateful inspection firewalls, and proxy firewalls, each with its mechanisms for analysing and controlling network traffic. Firewalls can be deployed at various points within a network, such as the perimeter, between different network segments, or on individual devices. Overall, firewalls play a crucial role in network security by helping to prevent unauthorised access to sensitive data, protect against cyber attacks, and maintain the integrity and confidentiality of network resources.

Lab Objectives:

- Understand the basics of Firewall.
- Configure Firewall on a server.

Configuring Firewall in Cisco Packet Tracer

Step 1: Create a network topology, as shown in Figure 1, and assign the IP address as defined in the table.

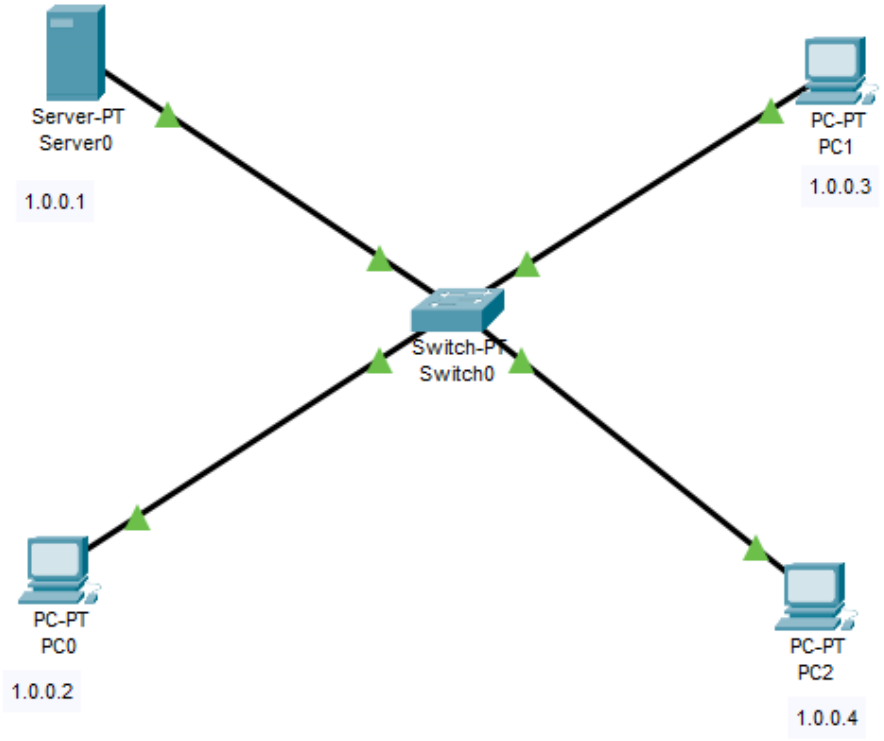

Figure 1: Network topology.

Device	IPv4 Address	Subnet Mask
Server	1.0.0.1	255.0.0.0
PC0	1.0.0.2	255.0.0.0
PC1	1.0.0.3	255.0.0.0
PC2	1.0.0.4	255.0.0.0

Step 2: Verify the connectivity between various devices in the network using the Ping command.

Step 3: Configuring the firewall in a server to **deny ICMP** packets and **allow browsing**.

To configure the firewall, follow these instructions:

- Click on server0 then go to the desktop.
- Then click on firewall IPv4.
- Turn the service on.
- First, Deny the ICMP protocol and set the remote IP to 0.0.0.0 and Remote wildcard mask to 255.255.255.255, then add this rule with the add button. This will deny all.
- Then, allow browsing by allowing HTTP protocol. This can be done by first selecting the TCP protocol as HTTP is one of the TCP protocols. Then, set the remote IP to

0.0.0.0 and Remote wildcard mask to 255.255.255.255, and the local port to 80. Then, add this rule.

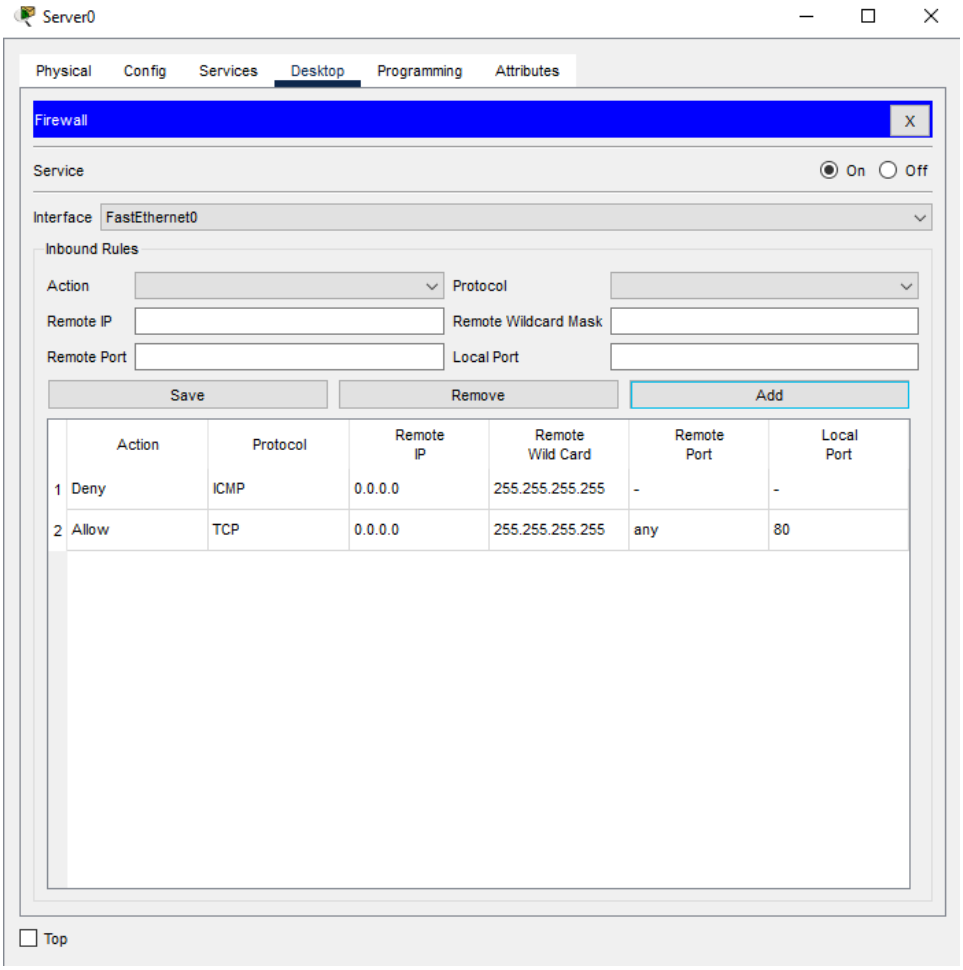

Figure 2: Adding rules to the firewall.

Step 4: Verify the network by pinging the IP address of the firewall from any PC.

What can you observe?

Does the firewall block the ping (ICMP) packets or not?

From the same PC, Check the web browser by entering the IP address of the firewall in the URL.

What can you observe?

Does the firewall permit IP packets including web browsing?

References:

1. Basic Firewall Configuration in Cisco Packet Tracer - https://www.geeksforgeeks.org/basic-firewall-configuration-in-cisco-packet-tracer/

2. Firewall Fundamentals - https://rootissh.in/firewall-fundamentals-1012f37e55ca