**Basic Firewall Configuration in Cisco Packet Tracer**

A firewall is a hardware or software network security device that monitors all incoming and outgoing traffic based on a defined set of security rules, it accepts, rejects, or drops that specific traffic.

* **Accept**: Allow traffic.
* **Reject**: Block traffic but respond with “reachable error”.
* **Drop:** Block unanswered traffic firewall establishes a barrier between secure internal networks and untrusted external networks, such as the Internet.

**Steps to Configure and Verify Firewall in Cisco Packet Tracer:**

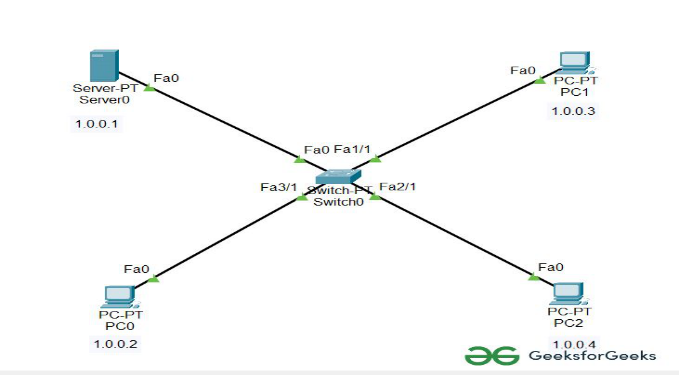
**Step 1**: First, open the Cisco packet tracer desktop and select the devices given below:

| **S.NO** | **Device** | **Model Name** | **Quantity** |
| --- | --- | --- | --- |
| **1.** | PC | PC | 3 |
| **2.** | server | PT-Server | 1 |
| **3.** | switch | PT-Switch | 1 |

**IP Addressing Table:**

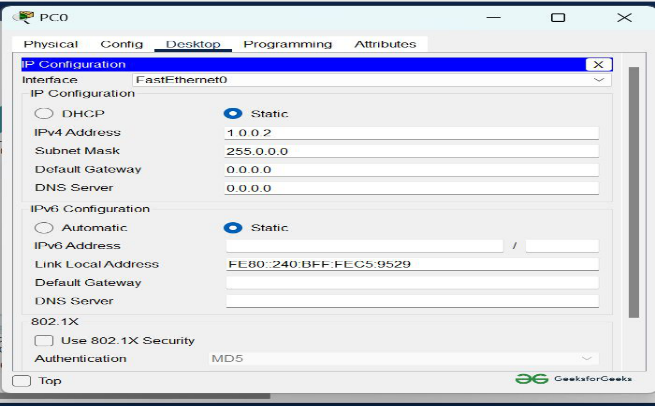
| **S.NO** | **Device** | **IPv4 Address** | **Subnet Mask** |
| --- | --- | --- | --- |
| **1.** | Server | 1.0.0.1 | 255.0.0.0 |
| **2.** | PC0 | 1.0.0.2 | 255.0.0.0 |
| **3.** | PC1 | 1.0.0.3 | 255.0.0.0 |
| **4.** | PC2 | 1.0.0.4 | 255.0.0.0 |

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



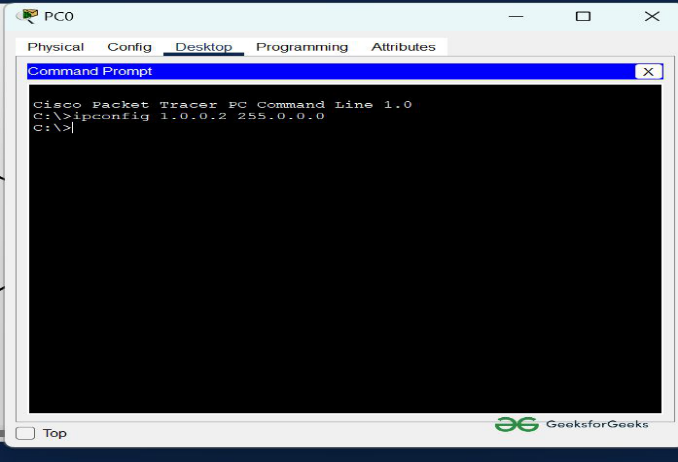
**Step 2**: Configure the PCs (hosts) and server with IPv4 address and Subnet Mask according to the IP addressing table given above.

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



* Assigning an IP address using the ipconfig command, or we can also assign an IP address with the help of a command.
* Go to the command terminal of the PC.
* Then, type iPConfig <IPv4 address><subnet mask><default gateway>(if needed)

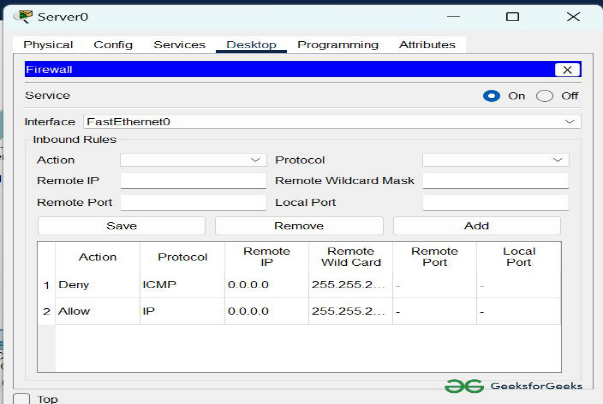
Example: ipconfig 1.0.0.2 255.0.0.0



* Repeat the same procedure with other PCs to configure them thoroughly.

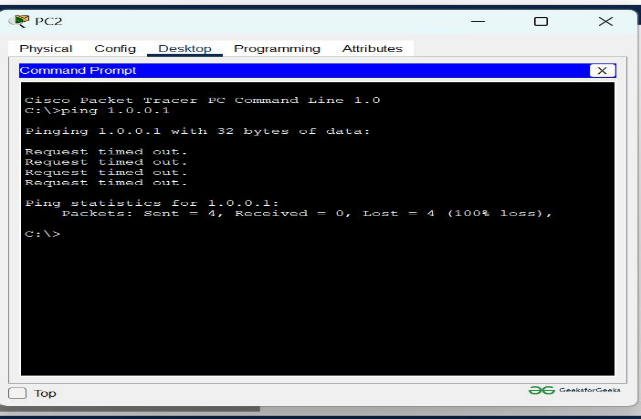
**Step 3**: Configuring the firewall in a server and blocking packets and allowing web browser.

* 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.



**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.

