Practical – 2

Aim : Implement firewall for a bank website using packet tracer.

Sol.

Firewall : A firewall is a type of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons.

The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through.

Types of firewall :

- *Packet-Filtering Firewalls :*

  As the most "basic" and oldest type of firewall architecture, packet-filtering firewalls basically create a checkpoint at a traffic router or switch. The firewall performs a simple check of the data packets coming through the router—inspecting information such as the destination and origination IP address, packet type, port number, and other surface-level information without opening up the packet to inspect its contents. If the information packet doesn't pass the inspection, it is dropped.

- *Circuit-Level Gateways :*

  As another simplistic firewall type that is meant to quickly and easily approve or deny traffic without consuming significant computing resources, circuit-level gateways work by verifying the transmission control protocol (TCP) handshake. This TCP handshake check is designed to make sure that the session the packet is from is legitimate.

- *Stateful Inspection Firewalls :*

  These firewalls combine both packet inspection technology and TCP handshake verification to create a level of protection greater than either of the previous two architectures could provide alone.

  However, these firewalls do put more of a strain on computing resources as well. This may slow down the transfer of legitimate packets compared to the other solutions.

- *Proxy Firewalls :*

  Proxy firewalls operate at the application layer to filter incoming traffic between your network and the traffic source—hence, the name “application-level gateway.” These firewalls are delivered via a cloud-based solution or another proxy device. Rather than letting traffic connect directly, the proxy firewall first establishes a connection to the source of the traffic and inspects the incoming data packet.

- *Next-Generation Firewalls :*

  Many of the most recently-released firewall products are being touted as “next-generation” architectures. However, there is not as much consensus on what makes a firewall truly next-gen.

  Some common features of next-generation firewall architectures include deep-packet inspection (checking the actual contents of the data packet), TCP handshake checks, and surface-level packet inspection. Next-generation firewalls may include other technologies as well, such as intrusion prevention systems (IPSs) that work to automatically stop attacks against your network.

- *Software Firewalls :*

  Software firewalls include any type of firewall that is installed on a local device rather than a separate piece of hardware (or a cloud server). The big benefit of a software firewall is that it's highly useful for creating defense in depth by isolating individual network endpoints from one another.

- *Hardware Firewalls :*

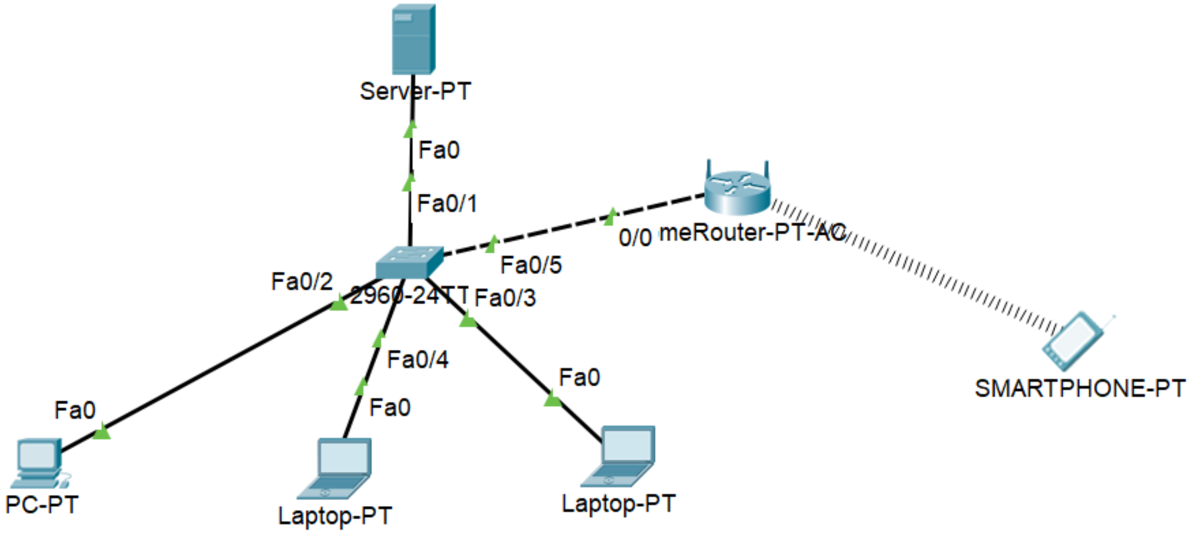
  Hardware firewalls use a physical appliance that acts in a manner similar to a traffic router to intercept data packets and traffic requests before they're connected to the network's servers. Physical appliance-based firewalls like this excel at perimeter security by making sure malicious traffic from outside the network is intercepted before the company's network endpoints are exposed to risk.

- *Cloud Firewalls :*

  Whenever a cloud solution is used to deliver a firewall, it can be called a cloud firewall, or firewall-as-a-service (FaaS). Cloud firewalls are considered synonymous with proxy firewalls by many, since a cloud server is often used in a proxy firewall setup.

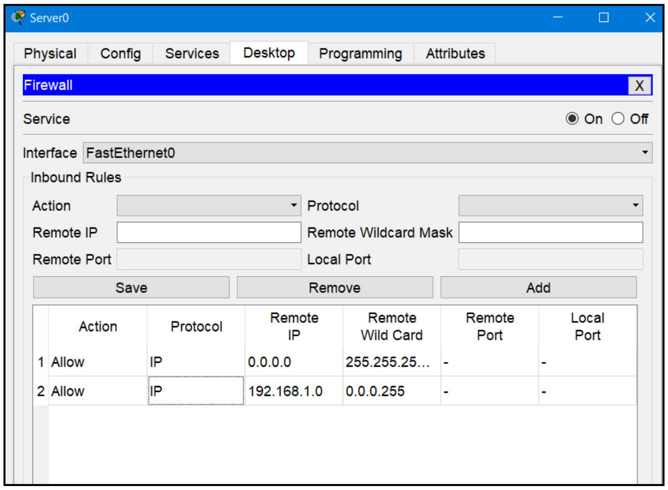
Implementation :

Step 1: Open Packet tracer and place and switch and connect some end devices and one server with the switch.



Step 2: Double click on server to open its configurations and make the below changes.

1) Give it a static IP address and enable DHCP for this server.
2) Goto Desktop section and open firewall option and turn it on. Then turn the firewall on and click on action and select allow and select protocol as IP. Then in remote ip, enter the ip of the server and enter the remote wilcard mask.

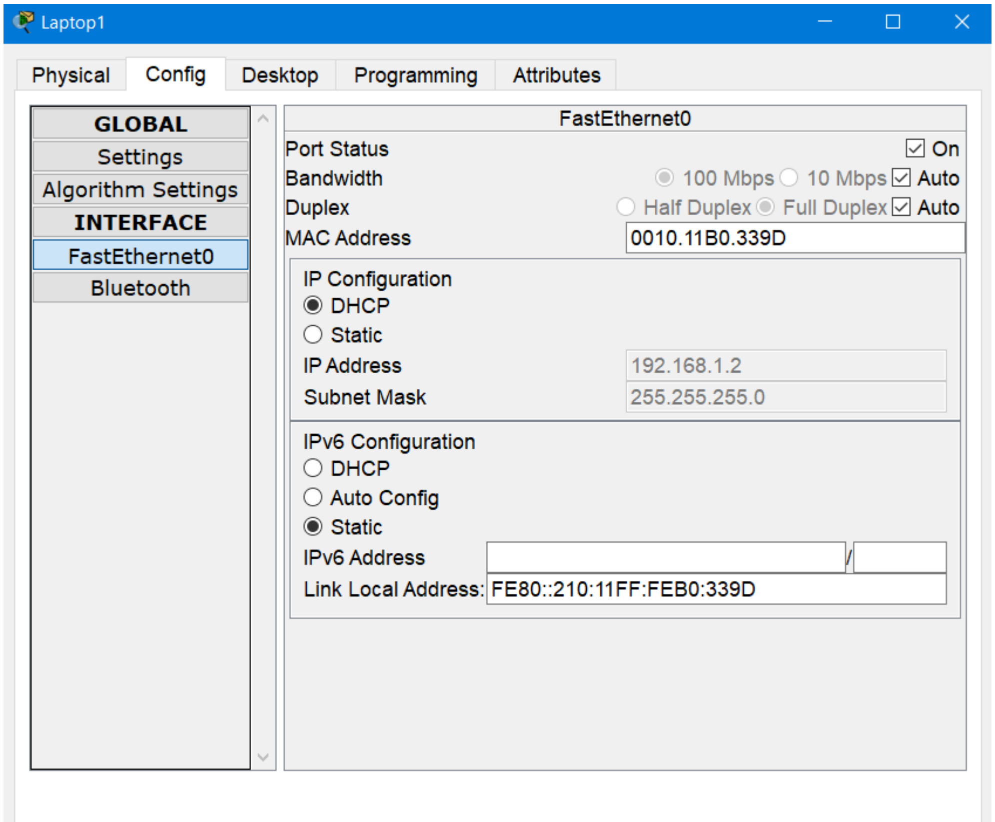


Service ● On ○ Off

Interface FastEthernet0

	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Allow	IP	0.0.0.0	255.255.25...	-	-
2	Allow	IP	192.168.1.0	0.0.0.255	-	-

Step 3: Open the client end devices and enable DCHP while configuring the IP addresses for them.



FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0010.11B0.339D

IP Configuration

● DHCP

○ Static

IP Address 192.168.1.2

Subnet Mask 255.255.255.0

IPv6 Configuration

○ DHCP

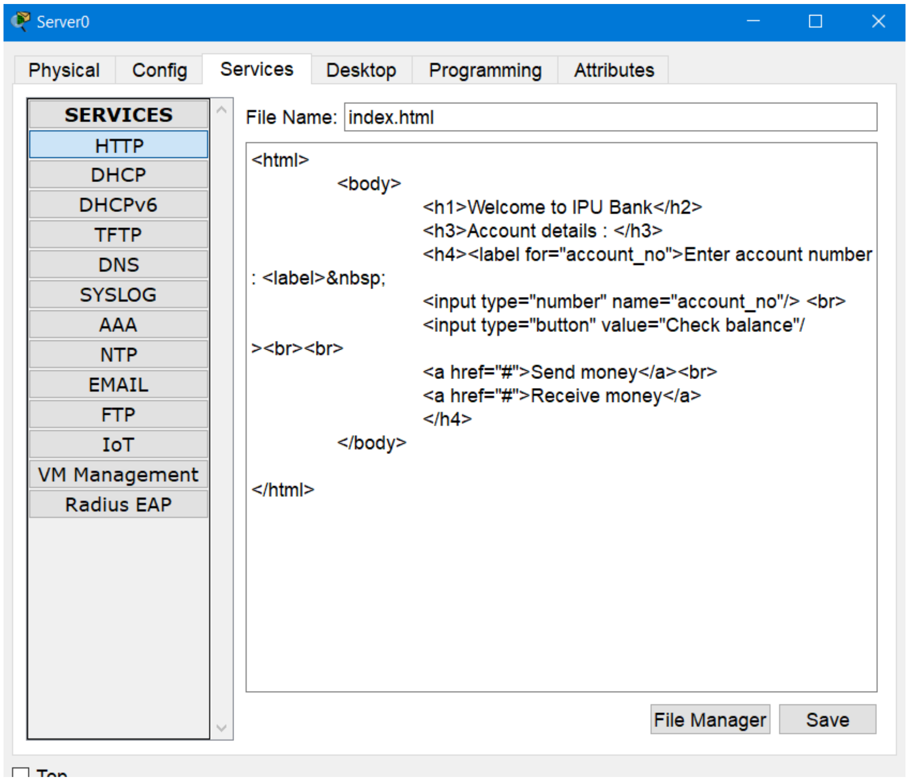
○ Auto Config

● Static

IPv6 Address /

Link Local Address: FE80::210:11FF:FEB0:339D

Step 4: Save the bank website or webpages in the server file explorer.

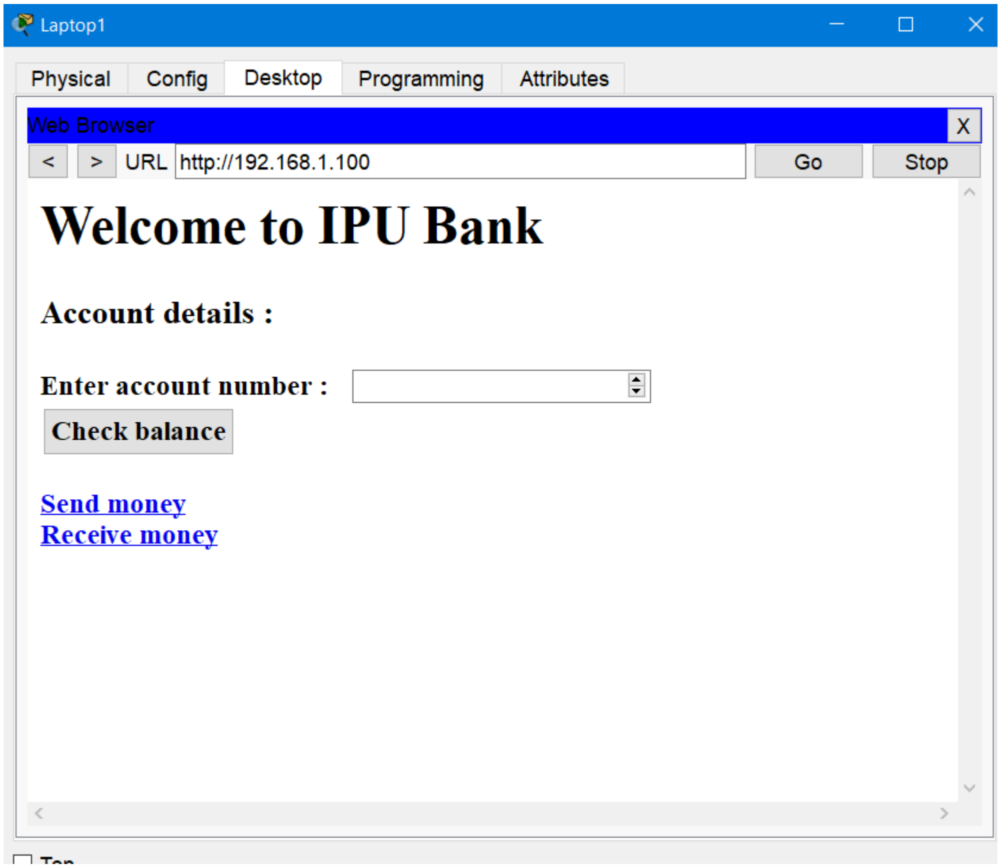


File Name: index.html

```
<html>
		<body>
				<h1>Welcome to IPU Bank</h2>
				<h3>Account details : </h3>
				<h4><label for="account_no">Enter account number
: <label>&nbsp;
				<input type="number" name="account_no"/> <br>
				<input type="button" value="Check balance"/
><br><br>
				<a href="#">Send money</a><br>
				<a href="#">Receive money</a>
				</h4>
		</body>

</html>
```

<u>Step 5:</u> Open any client device and open the IP address allocated to the bank website.



URL http://192.168.1.100

Welcome to IPU Bank

Account details :

Enter account number :

Check balance

Send money
Receive money