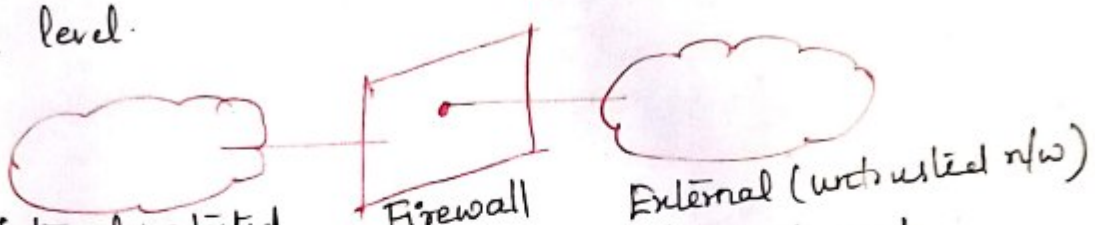
Semester : VI Subject : CSS Academic Year: 2023-2024

## FIREWALL

A firewall is a network security device, either hardware or software based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accept, reject or drop that specific traffic.

Accept :- Allow the traffic.
Reject :- Block the traffic but reply with an "unreachable error"
Drop :- Block the traffic with no reply.

A firewall is a type of network security device that filters incoming and outgoing network traffic with security policies that have previously been set up inside an organization. A firewall is essentially the way that separates a private internal network from the open Internet at its very basic level.




## Types of Firewall :-

* Packet filtering Firewall
* Stateful packet Inspection (SPI).
* Application Level Gateway.
* Circuit Level Gateway

Semester: VI Subject: CSS Academic Year: 2023-2024.

## Packet Filtering Firewall:-

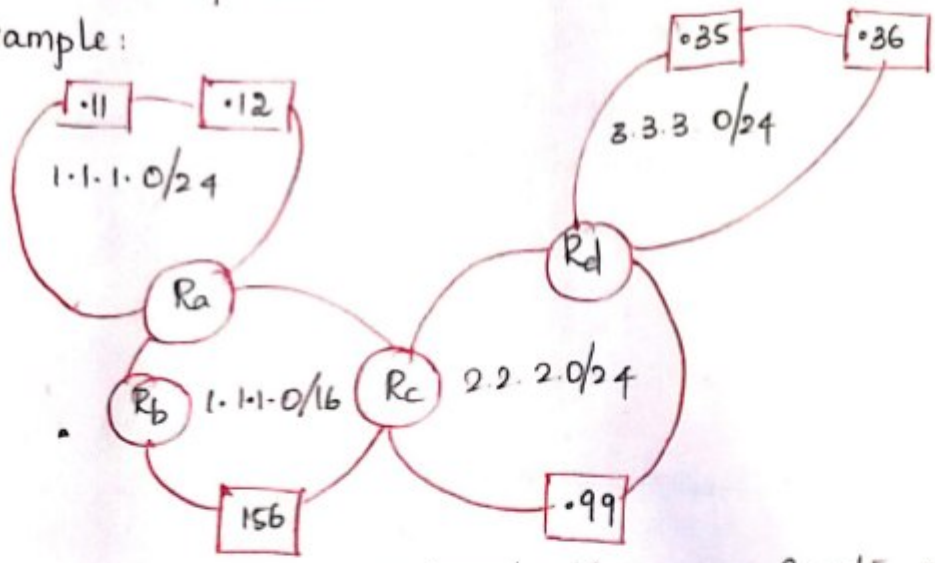
In packet filtering firewall we define the rules based on what should pass inside the network and what should go outside the network

The rules are set either to accept or to reject the packet.

Filteration is done based on IP address and port Number.

Every protocol has its own port number for eg: https-443, Ssh-22, http-80, Telnet-21.

Example:




Consider the above network diagram. Create a firewall table for the following rules.

(1) Block the external users from using the ssh which has the IP address 1.1.1.11

(2) Block access to Webserver on Network 3.3.3.0/24 for .12

Semester: VI Subject: CSS Academic Year: 2023-2024

| Rule | Source | Destination | Protocol | Action. |
|---|---|---|---|---|
| 1. | * | 1.1.1.11:22 | TCP | DROP |
| 2. | 1.1.1.12:* | 3.3.3.0/24 | TCP | DROP |
| Default | *:* | *:* | * | ACCEPT. |

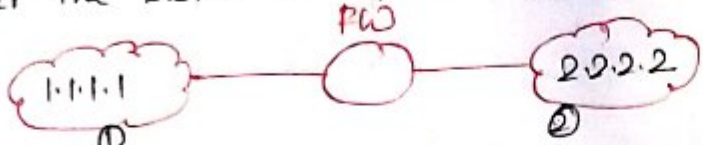
Example 2:


Block computer 2 from accessing WebServer on computer 1 with default policy as accept.

| Rule | Source | Destination | Protocol | Action. |
|---|---|---|---|---|
| 1. | 2.2.2.2:* | 1.1.1.1:80 | TCP | DROP |
| Default | *:* | *:* | * | ACCEPT. |

Stateful Packet Inspection:

Consider the below example:



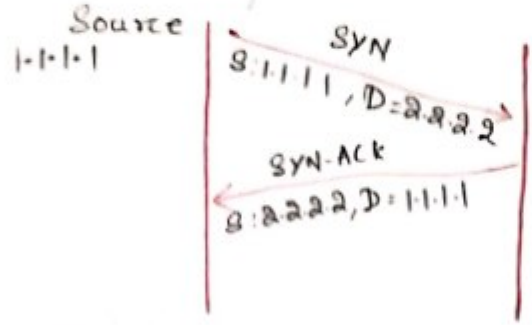

Allow WebBrowser on computer ① to access WebServer in computer 2. with default policy as DROP.

| Rule | Source | Destination | Protocol | Action |
|---|---|---|---|---|
| 1. | 1.1.1.1:* | 2.2.2.2:80 | TCP | Accept. |
| Default | *:* | *:* | * | Drop. |

This table will not give the expected answer. Even the rule no. 1 will not work.

Semester: VI Subject: CSS Academic Year: 2023-2024.

Since TCP protocol transmits 3 packets — SYN, SYN-ACK & ACK




The SYN-ACK packet cannot be transmitted because of the rules in firewall table. It will drop.

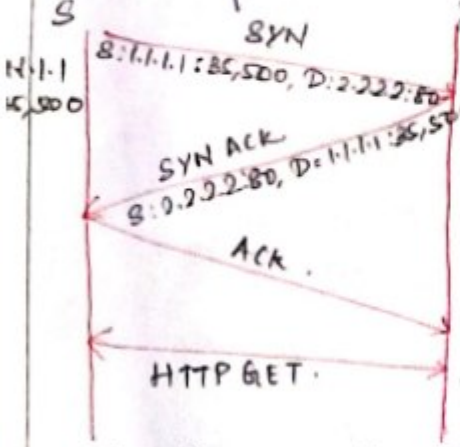
So even the rule 1 will not work properly.

To overcome this problem, we use stateful packet Inspection firewall.

It maintains the state information and allows the packet to enter the network based on the state information.

Along with the normal firewall table it also creates a SPI (Stateful Packet Inspection) Table where the packet informations are entered

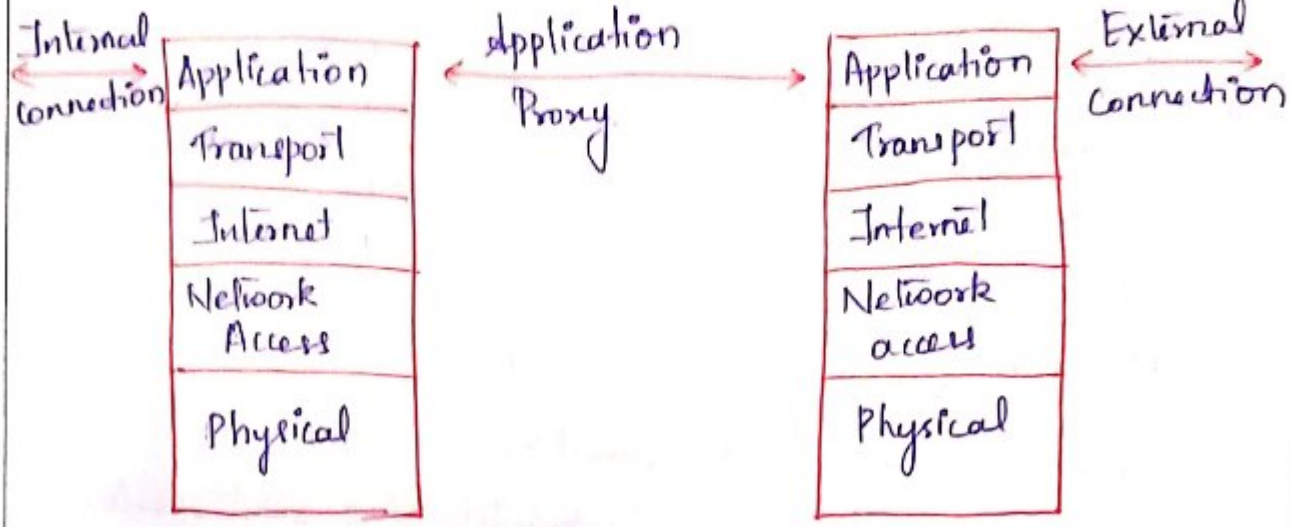
| Src | Destination | Protocol | Action | State |
|---|---|---|---|---|
| 1.1.1.1:35,500 | 2.2.2.2:80 | TCP | ACCEPT | Setting up connection<br>~~Half~~ open.<br>Established.<br>Closed. |




When first packet SYN enters the network, it checks the first table rule and makes the entry in SPI Table. When second packet (SYN-ACK) enters it refers the IP addresses in SPI table, & if it matches then allows. The same process continues till connection is closed. Once the connection is closed, the entire SPI table is deleted and new table is created when new packet arrives in the network.

Semester: VI Subject: CGS Academic Year: 2023-2024

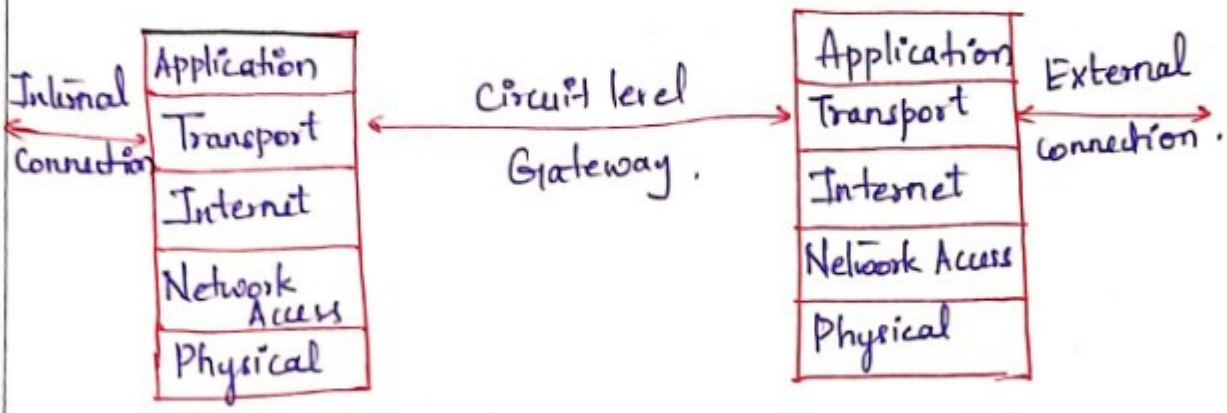
## (3) APPLICATION LEVEL GATEWAY:




→ It works in Application Layer.
→ It uses proxies. Client and server connect to proxy.
→ Communication is done through proxy server.
→ When client requests access to server resources such as file, webpage, database then the client first connects with proxy server, which then establishes connection with main server.
→ Application Gateway resides on the client and the server firewall.
→ The proxy server hides IP address and other secure information on the client.
→ They decide whether to drop a packet or send them based on application information.
→ They handle complex protocol.
(eg) Attacks over http like sending long string in the host field would be dropped because they have been tampered by an intruder.

Semester : VI Subject : CSS Academic Year: 2023-2024

## (4) CIRCUIT LEVEL GATEWAY :




→ It provides UDP and TCP connection security.
→ It monitors TCP data packet handshaking and session fulfillment of firewall rules and policies.
→ It checks the validity of connections (ie. circuits) at the transport layer against a table of allowed connections before a session can be opened and data exchanged.
→ It acts as a proxy and has the same advantage as an application level gateway in hiding the internal host from the serving host.
→ Disadvantage is absence of checking and filtering individual packet.
→ It can be implemented along with application-level gateway or as stand-alone systems.
→ Provides high-level secure network connection.