SNS COLLEGE OF TECHNOLOGY
Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

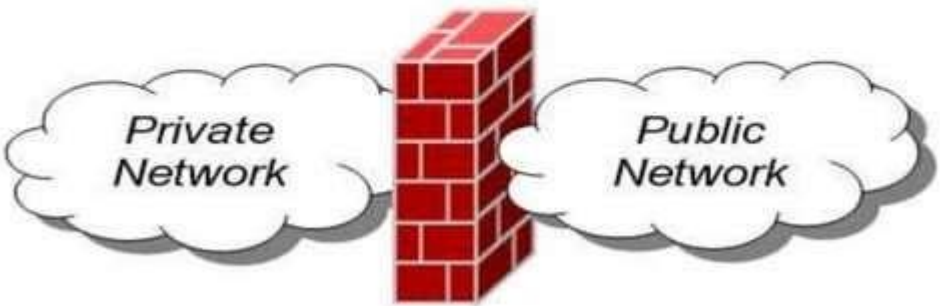
19ECT301-COMMUNICATION NETWORKS III YEAR/ V SEMESTER

UNIT 4- NETWORK & DATA SECURITY

TOPIC 6 –Firewalls

Firewall

- **Definition**: A Network Firewall is a system or group of systems used to control access between two networks -- a trusted network and an untrusted network -- using pre-configured rules or filters.



- Firewall is device that provides secure connectivity between networks (internal/ external).

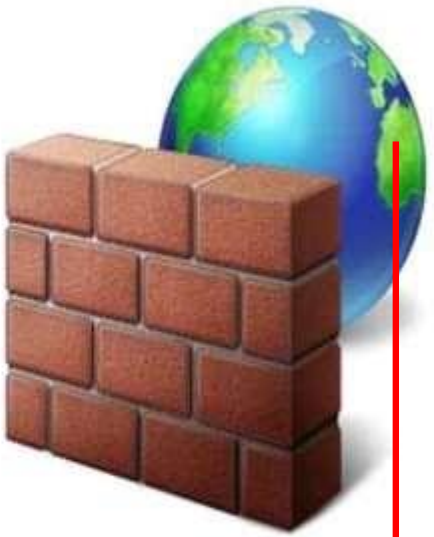
- It is used to implement and enforce a security policy for communication between networks.

- A firewall may be a hardware, software or a combination of both that is used to prevent unauthorized program or internet users from accessing a private network or a single computer.

- All messages entering or leaving the intranet pass through the firewall, which examines each message & blocks those that do not meet the specified security criteria.

Why do we need a firewall?

- To protect confidential information from those who do not explicitly need to access it.
- To protect our network & its resources from malicious users & accidents that originate outside of our network.



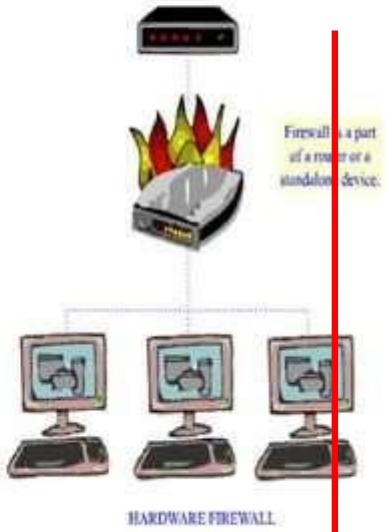
Types of firewall

1. Hardware firewall

1. Software firewall

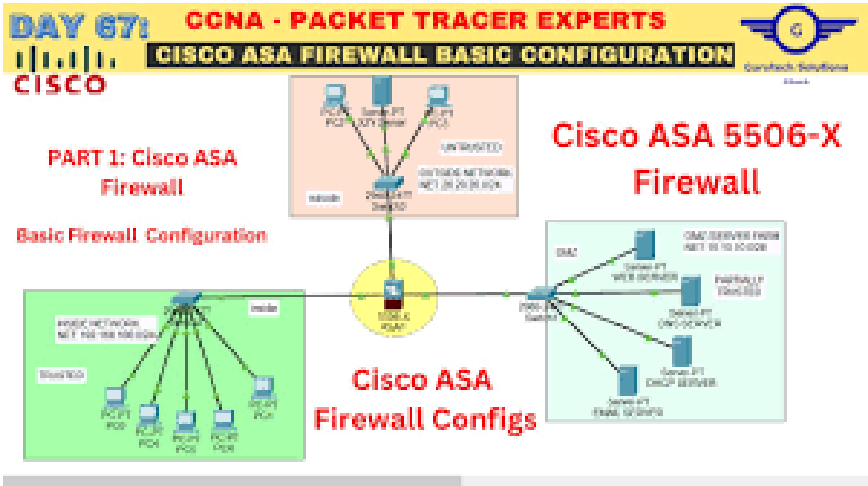
1. Hardware Firewall

- It is a physical device.
- It can be installed between the modem and computer.
- It can be incorporated into a broadband router being used to share the internet connection.
- Protects an entire network.



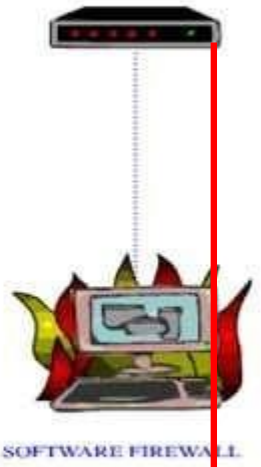
- Usually more expensive, harder to configure.

- E.g.- Cisco pix, Netscreen, Watchfuard etc.



2. Software Firewall

- It is a software application.
- It is installed onto the computer system that you wish to protect .
- Protects a single computer.
- This is usually the computer with modem attached to it.



- Usually less expensive, easier to configure.
- E.g.- Norton internet security, MacAfee internet security etc.

ASSESSMENT

An organization is experiencing frequent DoS attacks. Suggest how they can use firewalls to mitigate the issue.

Implement Rate Limiting: Use firewalls to limit traffic from individual IPs.

Block Malicious IPs: Add known attack sources to the blacklist.

Enable Stateful Inspection: Detect and drop anomalous traffic.

Use an NGFW: Employ DPI and application control to identify attack patterns.


Thank You!