SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

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

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

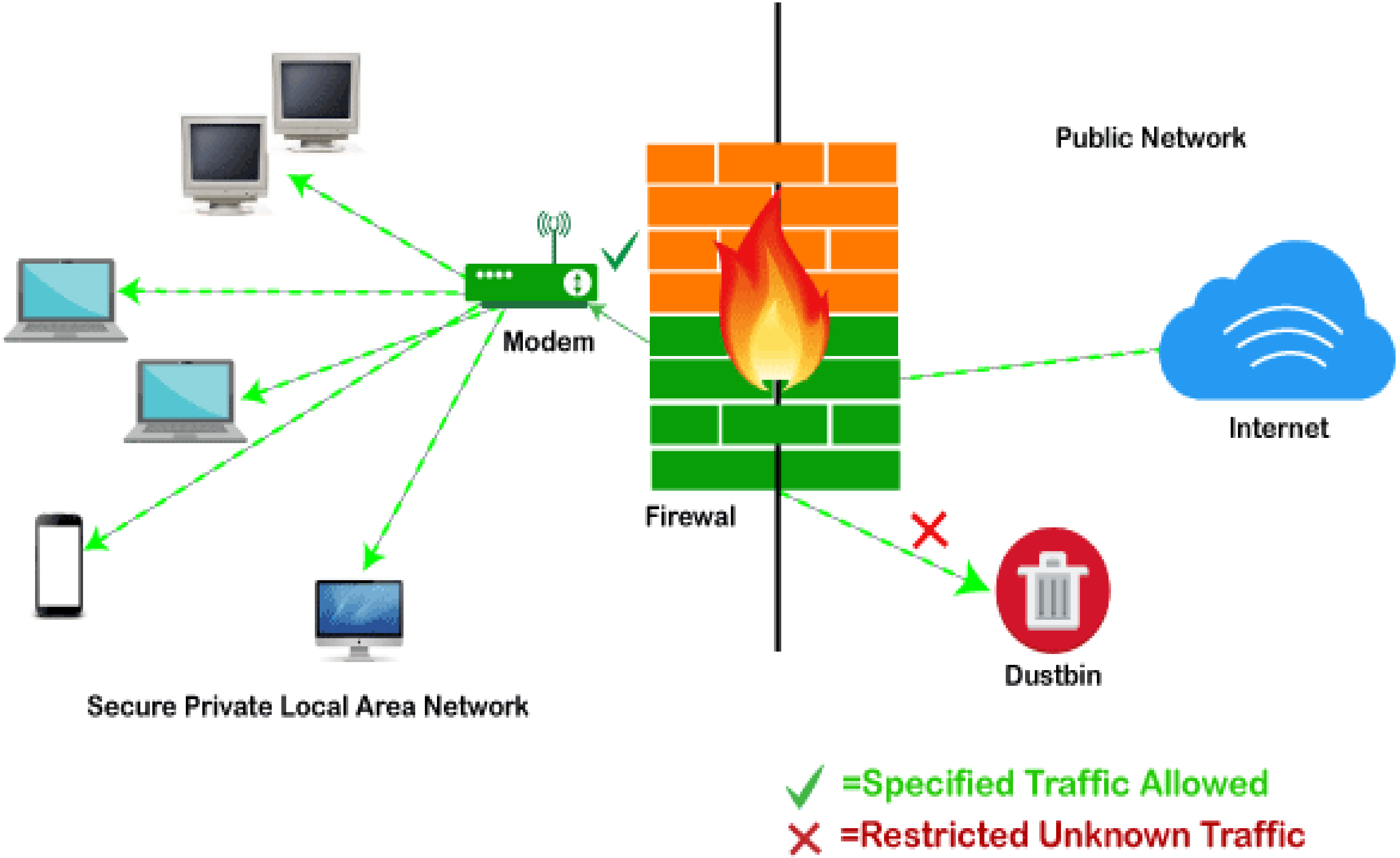
Unit IV- SECURITY ELEMENTS

Topic :Firewalls

FIREWALL

- A **firewall** is a combination of software and hardware components that controls the traffic that flows between a secure network (usually an office LAN) and an insecure network (usually the Internet).
- Using rules defined by the **system administrator**. The firewall sits at the gateway of a network or sits at a connection between the two networks.
- All traffic, from one network to the other, passes through the firewall. The firewall stops or allows traffic based on the security policy as defined in **rules' table.**
- The secure trusted network is said to be '**inside**' the firewall; the insecure untrusted network is said to be '**outside**' the firewall

- Philosophy behind firewall can be thought of as a pair of mechanisms such as:
- It exists to block traffic
- It exists to permit traffic.
- Before Firewalls, network security was performed by **Access Control Lists** (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.


Public Network
Modem
Firewal
Internet
Dustbin
Secure Private Local Area Network
✓ =Specified Traffic Allowed
✗ =Restricted Unknown Traffic

Firewalls are generally of two types:

1) **Host-based**

2) **Network-based.**

Host- based Firewalls

- Host-based firewall is installed on each network node which **controls each incoming and outgoing packet**.
- It is a **software application** or suite of applications, comes as a part of the operating system.
- **Host-based firewalls** are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from **attacks and unauthorized access.**

Network-based Firewalls

- Network firewall function **on network level**. In other words, these firewalls filter all incoming and outgoing traffic across the network.
- It protects the **internal network by filtering the traffic** using rules defined on the firewall.
- A Network firewall might have two or more **network interface cards (NICs).** A network-based firewall is usually a dedicated system with proprietary software installed.

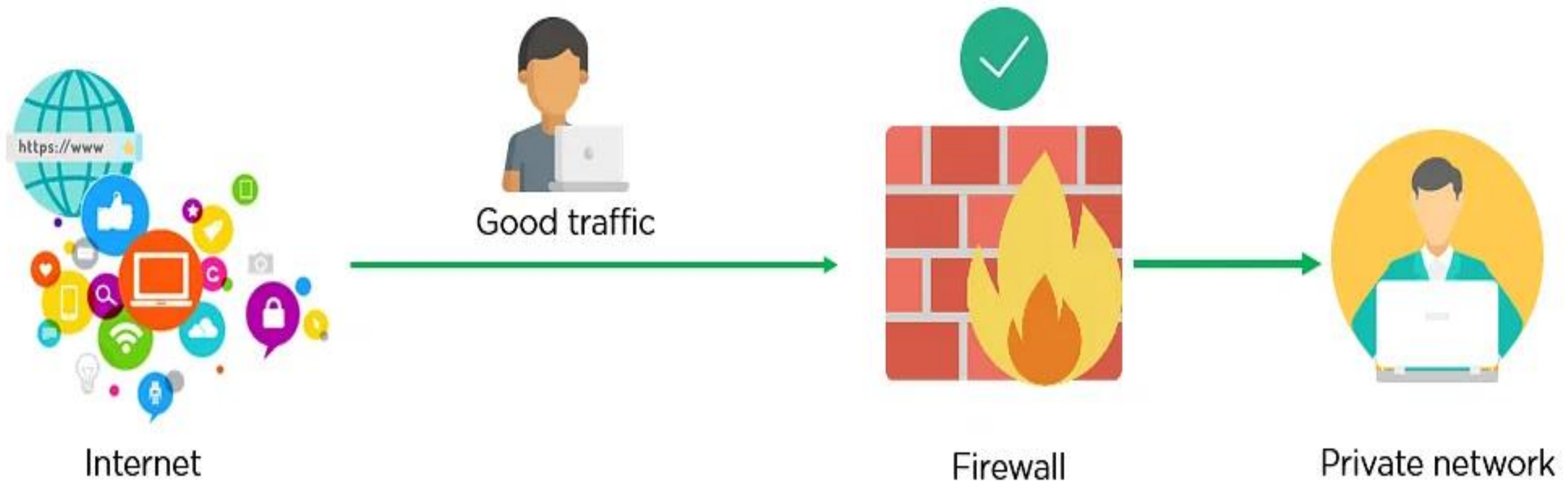
Functions of Firewall

- The most important function of a firewall is that it creates **a border** between **an external network and the guarded network** where the firewall inspects all packets (**pieces of data for internet transfer**) entering and leaving the guarded network**.**
- Once the inspection is completed, a firewall can differentiate between **benign and malicious packets** with the help of a set of pre-configured rules**.**
- The firewall abides such packets, whether they come in a rule set or not, so that they should not enter into the guarded network.
- This packet form information includes **the information source, its destination, and the content.** These might differ at every level of the network, and so do the rule sets. Firewalls read these packets and reform them concerning rules to tell the protocol where to send them.

How Does a Firewall Work?

- Firewalls filter the network traffic within a private network. It analyses which traffic should be allowed or restricted based on a set of rules. Think of the firewall like a **gate keeper** at your computer’s entry point which only allows **trusted sources, or IP addresses, to enter your network.**
- A firewall welcomes only those incoming traffic that has been configured to accept. It distinguishes between **good and malicious traffic** and either allows or blocks specific data packets on pre-established security rules.
- These rules are based on several aspects indicated by the **packet data, like their source, destination, content, and so on**. They block traffic coming from suspicious sources to prevent cyberattacks.

For example, the image depicted below shows how a firewall allows good traffic to pass to the user’s private network.



Advantages of Using Firewalls

- Protection from unauthorized access
- Prevention of malware and other threats
- Control of network access
- Monitoring of network activity
- Regulation compliance
- Network segmentation

Disadvantages of Using Firewalls

- Complexity
- Limited Visibility
- False sense of security
- Limited adaptability
- Performance impact
- Limited scalability
- Limited VPN support

Any Query????

Thank you……