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 ELECTRONICS AND COMMUNICATION ENGINEERING

COURSE NAME : 19EC625 – CYBER FORENSIC AND DATA SECURITY

III YEAR / VI SEMESTER

Unit II- E-MAIL SECURITY & FIREWALLS

Topic : Firewall Design in Cyber Forensics

INTRODUCTION

What is Firewall Design :

The process of determining how firewalls should be configured and deployed within a network to ensure effective protection and performance.

A **firewall** is a crucial network security device that monitors and controls the incoming and outgoing network traffic based on a set of security rules. It acts as a barrier between a trusted internal network and untrusted external networks (such as the internet), providing a line of defense against unauthorized access, cyber attacks, and potential data breaches.

Principles of Firewall Design

- **Security by Design**
  Ensure security is prioritized from the planning phase through deployment.
- **Least Privilege**
  Only allow the minimum necessary access to ensure security.
- **Default Deny**
  Block all traffic by default, then allow only the required services or applications.
- **Redundancy and Failover**
  Implement high availability to ensure network protection even during failures.

Firewall Architecture

- **Perimeter Defense**

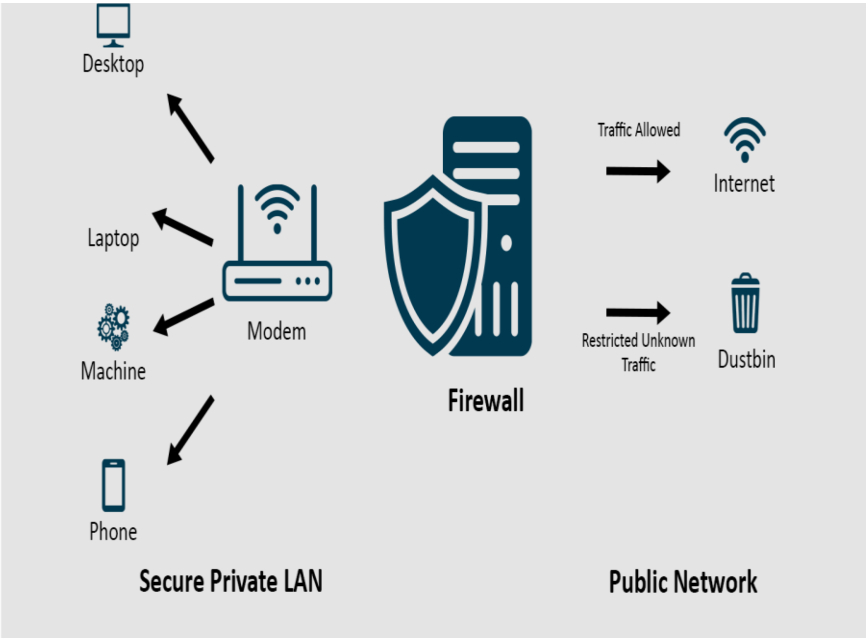
Deploy firewalls at network entry points to prevent unauthorized access.

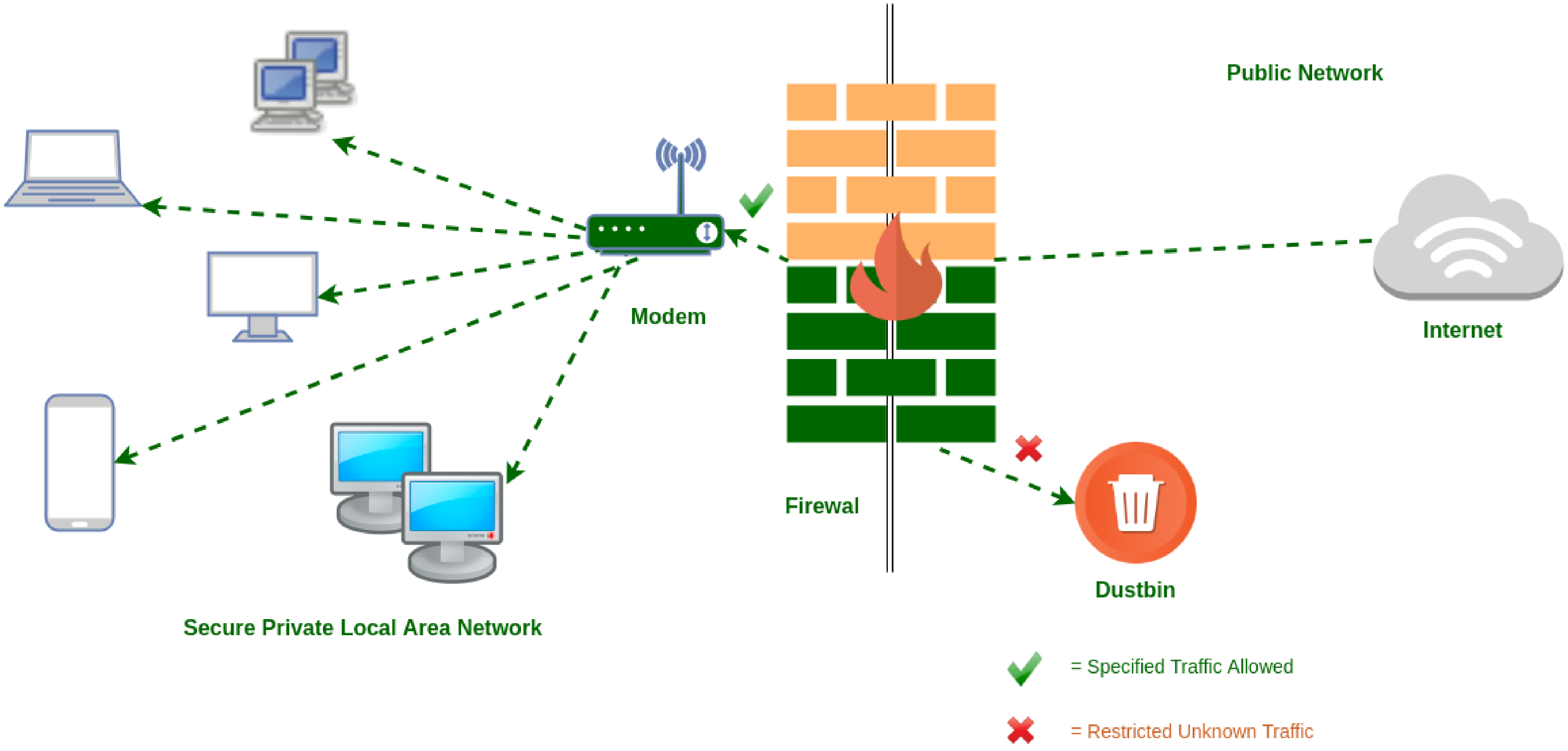
- **Internal Segmentation**

Use firewalls to segment internal networks into different security zones (e.g., production, guest, admin).

- **Demilitarized Zone (DMZ)**

Design a DMZ for public-facing services (e.g., web servers) with strict access control from both internal and external networks.





Public Network

Modem

Firewal

Internet

Dustbin

Secure Private Local Area Network

✓ = Specified Traffic Allowed

✗ = Restricted Unknown Traffic

Types of Firewall Deployment

- **Network-based Firewalls :**
  Deployed at the network perimeter to protect the entire internal network.
- **Host-based Firewalls** :
  Installed directly on devices like servers and workstations to protect individual systems.
- **Cloud-based Firewalls** :
  Firewalls deployed in the cloud environment to protect cloud infrastructure and applications.

Firewall Rule Design

Defining Rules

- Rules should define allowed traffic based on source, destination, port, protocol, and application.

Basic Rule Format

- **Source IP**: Address of the client or service initiating the traffic.
- **Destination IP**: Address of the target system or service.
- **Ports & Protocols**: Specifies which application or service the traffic is targeting.
- **Action**: Allow, Deny, or Log.

Best Practice for Rules

- **Explicit Deny**: Default deny all and allow only required traffic.
- **Granular Rules**: Be specific about the IPs, services, and protocols allowed.

Challenges in Firewall Design

- **Complexity of Rule Management**
  As networks grow, managing and auditing firewall rules becomes challenging.
- **Performance Impact**
  Firewalls can introduce latency and affect network performance if not properly configured.
- **Evolving Threats**
  Firewalls must adapt to new types of attacks (e.g., advanced persistent threats, zero-day vulnerabilities).

Any Query????

Thank you……