جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

قسم الامن السيبراني

Department of Cyber Security

Subject: Fundamentals of Network Security: Firewalls and Cryptographic Systems

Class: 1stPrinciples of Cyber Security

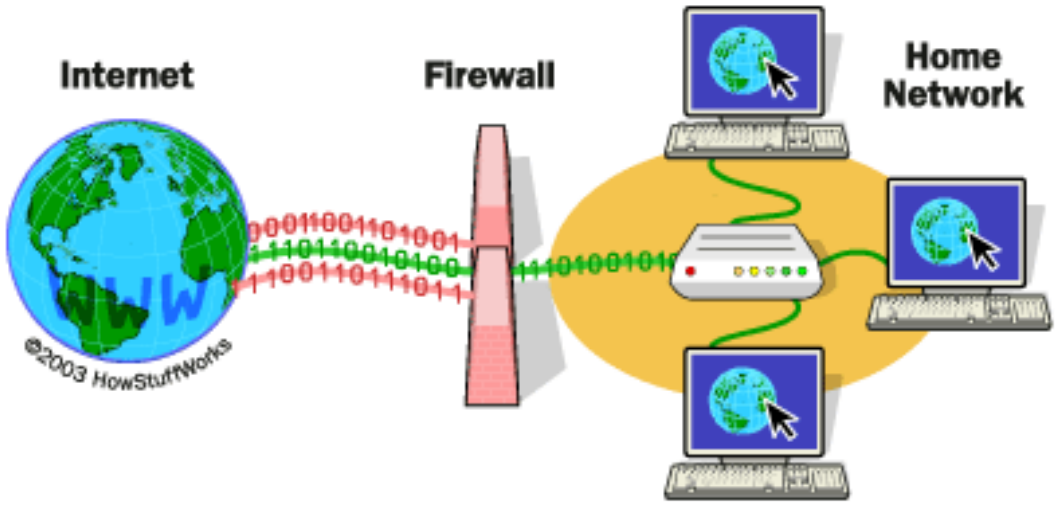
Lecture: (5+6)

Lecturer: Msc :Najwan thaeer ali

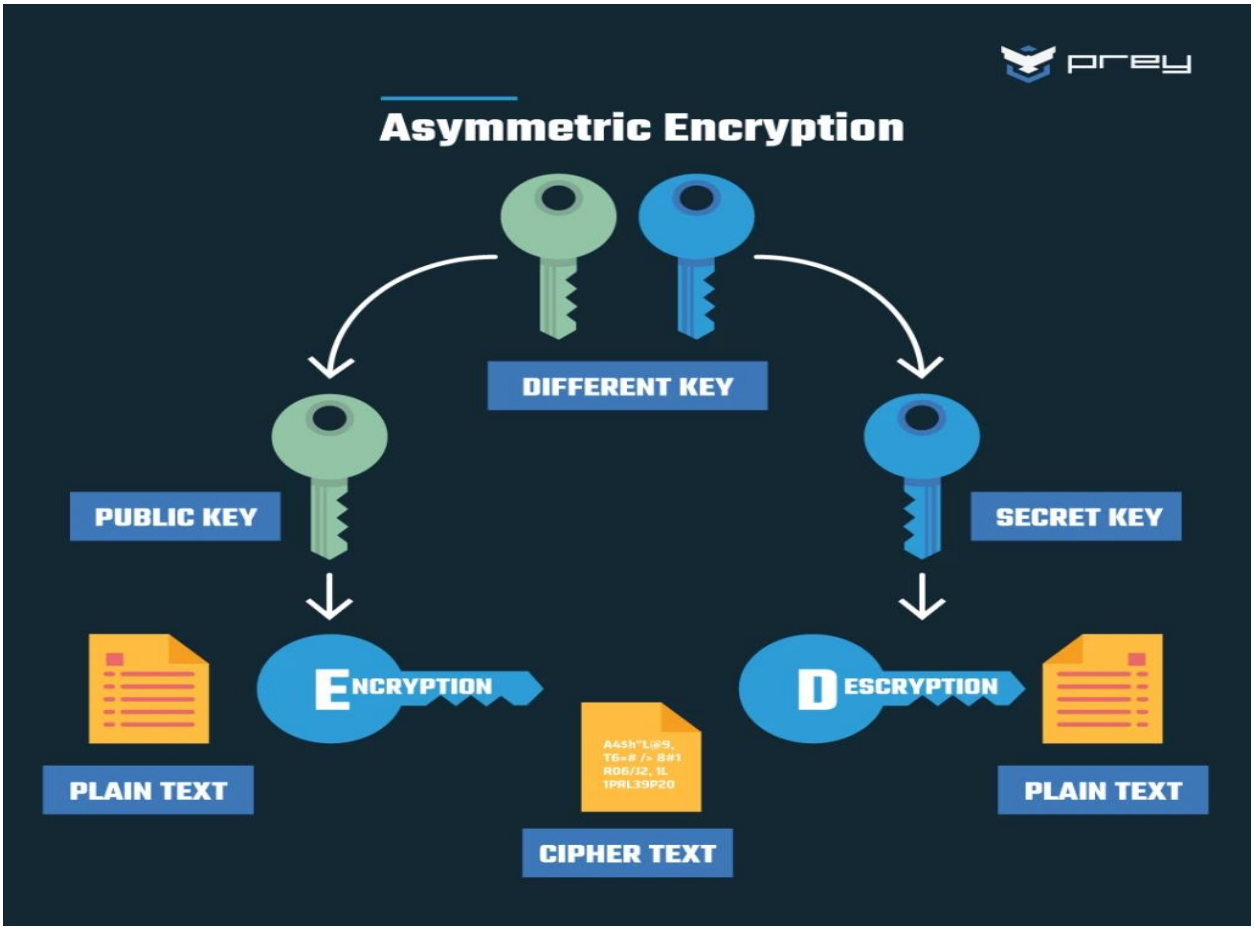
Introduction to Network and Information Security

Information security focuses on protecting systems, networks, and data from unauthorized access, misuse, and attacks.
Two essential security mechanisms are:

- **Firewalls** (network protection)



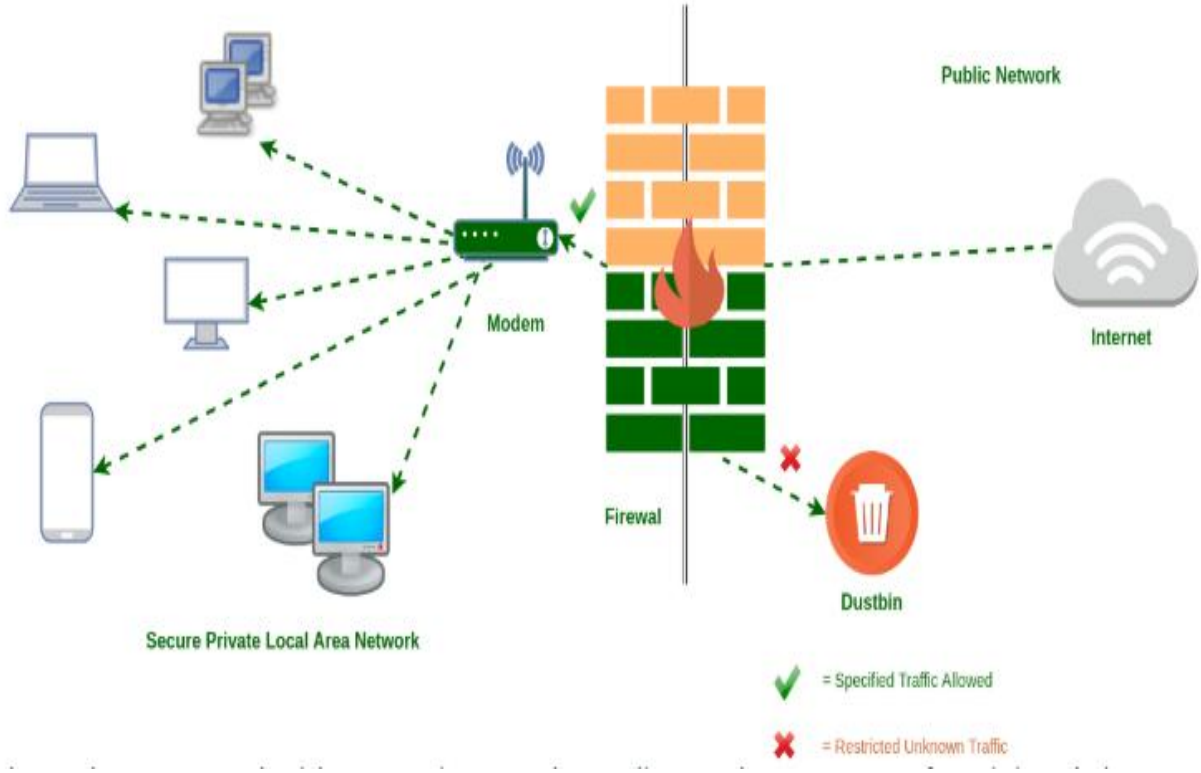
- **Cryptographic systems** (data protection)



Together, they ensure confidentiality, integrity, and secure communication in modern digital environments.

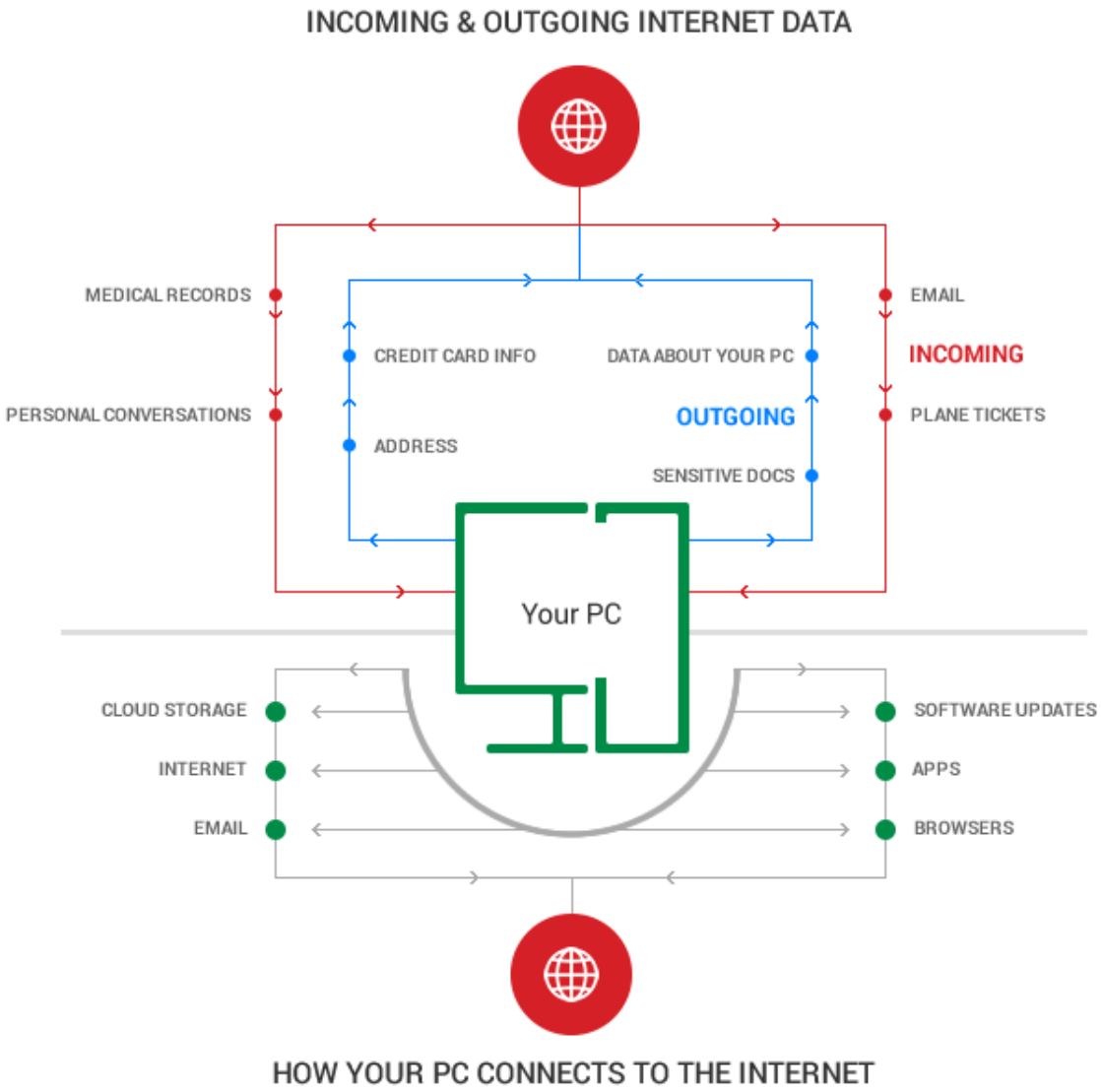
Firewall – Definition and Concepts

A **Firewall** is a hardware or software-based security system that monitors and controls incoming and outgoing network traffic based on predefined security rules.



Key Concepts:

- Acts as a barrier between **trusted internal networks** and **untrusted external networks**
- Filters network traffic
- Prevents unauthorized access and cyber attacks
- Enforces security policies



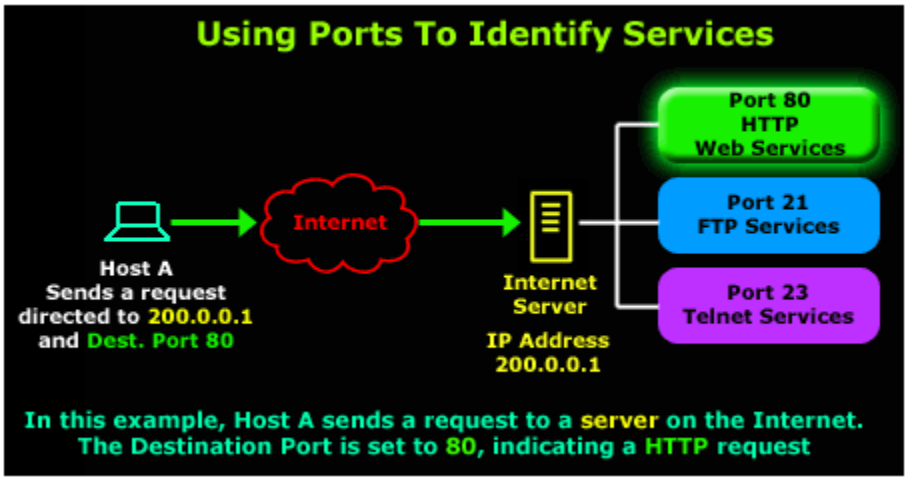
Firewall Conditions

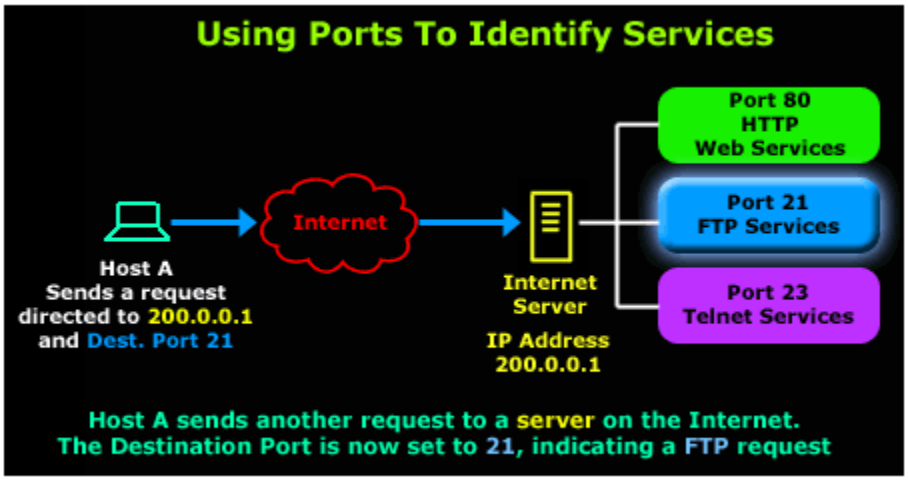
Firewall decisions are based on specific conditions, including:

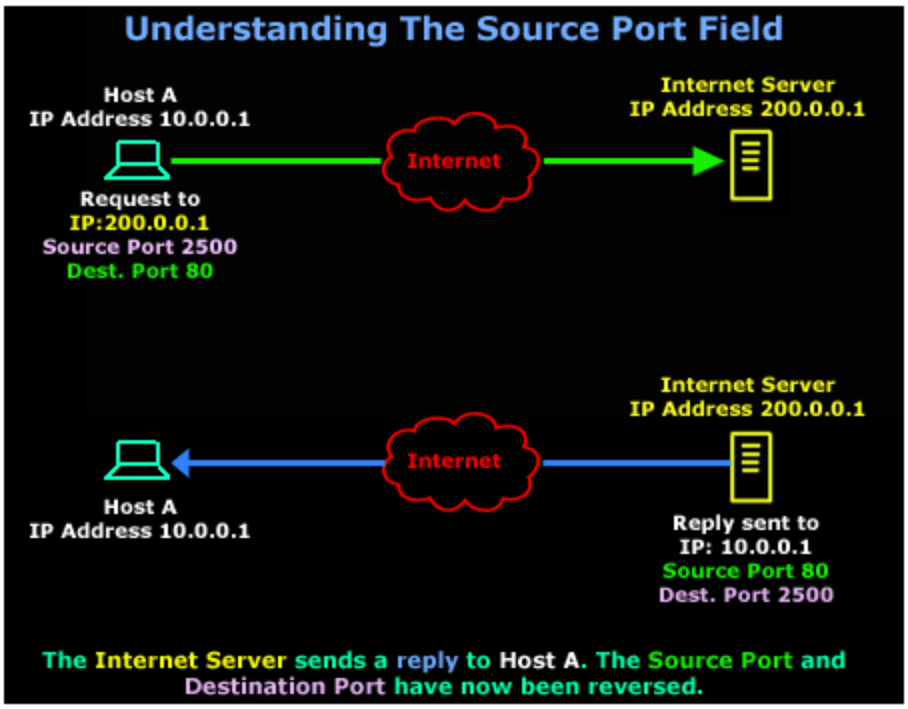
- Source IP address
- Destination IP address

- Port number (e.g., 80, 443)
- Protocol type (TCP, UDP, ICMP)
- Traffic direction (incoming or outgoing)

Based on these conditions, traffic is either **allowed** or **denied**.







Components of a Cryptographic System

A **cryptographic system** protects data by transforming it into a secure form.

Main Components:

- **Plaintext:** Original readable data
- **Encryption Algorithm:** Converts plaintext into ciphertext
- **Key:** Controls the encryption and decryption process

HELLO الرسالة

MyPassword123 الرمز السري او كلمة المرور

Key: 3

Encryption Algorithms

Encryption algorithms are used to secure data.

Types:

- **Symmetric Encryption:**
  - One key for encryption and decryption
  - Fast and efficient
  - Example: AES, DES

  Example:
  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

الحرف الأصلي	موقعه	حروف 3+	الحرف الجديد
H	8	11	K
E	5	8	H
L	12	15	O
L	12	15	O
O	15	18	R

- **Asymmetric Encryption:**
  - Two keys (public and private)
  - More secure for key exchange
  - Example: RSA

Conclusion:

Firewalls protect **networks**, while cryptography protects **data**. Both are fundamental pillars of information security.

References

https://www.geeksforgeeks.org/computer-networks/difference-between-source-port-and-destination-port/