قســـــــم الامـــــــــــــــــن
الــــــــــــــــــــــــــســيبرانــــــــــــــــــــــــ
ـي

**DEPARTMENT OF CYBER SECURITY**

**SUBJECT:** **PRINCIPLES OF CYBER SECURITY**

**CLASS:** **1ST**

# LECTURE: (5)

## MANAGING NETWORK SECURITY

**LECTURER:** **MSC :NAJWAN THAEER ALI**

## Overview

This lecture focuses on security threats directed at endpoints, such as servers, workstations, and mobile devices, that are attached to an enterprise network or the Internet. Detailed discussion of the countermeasures implemented on the endpoints, such as antivirus software, is beyond our scope. Instead, this lecture looks at endpoint security from a network perspective.

## Lecture Objectives

**5.1** List and discuss the various types of firewalls and the common approaches to firewall implementation.

**5.2** Define and describe the types of intrusion detection and prevention systems and the strategies on which they are based

**OB.5.1:** List and discuss the various types of firewalls and the common approaches to firewall implementation.

### 5.1.1 Managing Network Security

The InfoSec professionals are under increasing pressure to provide global access to information assets without sacrificing security.

### Firewalls:

The firewall is an important complement to host-based security services such as intrusion detection systems. Typically, a firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and auditing can be imposed. Firewalls are also deployed internal to the enterprise network to segregate portions of the network.

The firewall provides an additional layer of defense, insulating internal systems from external networks or other parts of the internal network. This follows the classic military doctrine of “defense in depth,” which is just as applicable to IT security.

## Firewall Characteristics

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this section.

2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this lecture.

3. The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system (OS). Trusted computer systems are suitable for hosting a firewall and are often required in government applications.

## Types of Firewalls

A firewall may act as a packet filter. It can operate as a positive filter, allowing to pass only packets that meet specific criteria, or as a negative filter, rejecting any packet that meets certain criteria. Depending on the type of firewall, it may examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets. In this section, we look at the principal types of firewalls.
Firewalls are security devices or software that monitor and control incoming and outgoing network traffic based on predetermined security rules. There are several types of firewalls, each with its own characteristics and functionalities. Here are some common types of firewalls:

- **Packet Filtering Firewalls:**

• Examines individual packets of data and makes decisions to allow or block them based on predefined rules.

- **Stateful Inspection Firewalls:**

• Keeps track of the state of active connections and makes decisions based on the context of the traffic.

**Principles of Cyber Security:** Lecture 05- Managing Network Security

- **Proxy Firewalls:**

• Acts as an intermediary between internal and external networks, handling communication on behalf of the clients.

- **Application-layer Gateways (Proxy Firewalls):**

• Monitors and filters traffic at the application layer, providing more detailed control over specific applications or services.

- **Circuit-level Gateways:**

• Works at the session layer of the OSI model, making decisions based on the context of the traffic's source and destination.

- **Next-Generation Firewalls (NGFW):**

• Integrates traditional firewall features with additional capabilities such as intrusion prevention, deep packet inspection, and application awareness.

- **Hardware Firewalls:**

• Implemented as a standalone physical device, often used to protect an entire network.

- **Software Firewalls:**

• Implemented as a software application, often installed on individual devices.

**OB.5.2:** Define and describe the types of intrusion detection and prevention systems and the strategies on which they are based.

### 5.2.1 Intrusion Detection and Prevention Systems

**Intrusion:**

Violations of security policy, usually characterized as attempts to affect the confidentiality, integrity, or availability of a computer or network. These violations can come from attackers accessing systems from the Internet or from authorized users of the systems who attempt to overstep their legitimate authorization levels or who use their legitimate access to the system to conduct unauthorized activity.

**Intrusion detection:**

The process of collecting information about events occurring in a computer system or network and analyzing them for signs of intrusions.

**Intrusion detection system:**

Hardware or software products that gather and analyze information from various areas within a computer or a network for the purpose of finding, and providing real-time or near-real-time warning of, attempts to access system resources in an unauthorized manner.

## Intrusion detection systems (IDSs) can be classified as follows:

- ### Host-based IDS:

Monitors the characteristics of a single host and the events occurring within that host for suspicious activity. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the OS. Furthermore, unlike network-based IDSs, hostbased IDSs can more readily see the intended outcome of an at tempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.

- ### Network-based IDS:

Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.