CMPD414  Data and Computer Security

Chapter 5:
Network Security
Simple View of Network

- Workstation (Client)
- Communications Medium
- Host (Server)
Structure of DMZ Network

**Trusted LAN:**
It is a network where the user can only be connected on invitation by network administrator. By default, it can not communicate with outside, unless by invitation.
DEMILITARIZED ZONE (DMZ)
(sometimes referred to as a perimeter network)

• A physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet.

• The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network.

• The name is derived from the term "demilitarized zone", an area between nation states in which military operation is not permitted.
A **demilitarized zone, DMZ** is an area in which treaties or agreements between nations, military powers or contending groups forbid military installations, activities or personnel. A DMZ often lies along an established frontier or boundary between two or more military powers or alliances. For example, the 38th parallel between North and South Korea. Other examples of demilitarized zones are a 120-mile (190 km) area between Iraq and Kuwait,
Firewall = Packet Filter
In computing, a **firewall** is a network security system that monitors and controls the **incoming** and **outgoing** network traffic based on **predetermined security rules**.

A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted.

In simplest term, it is also known as **packet filter**.
Why setting firewall is not enough? Is firewall = anti virus?

Remember!

Task of firewall is only to filter:

• IP address
• port (source/destination)

It is NOT to filter virus.
A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day exploit.