Amir hosein sedaghati_ Tuesday at **8** (network laboratory) and **13:50** (computer networks)_ Qods University

DVR vs NVR:

DVR (Digital Video Recorder)	NVR (Digital Video Recorder)
The DVR system processes data at the **recorder**.	the NVR system encrypts and processes data at the **camera** before sending it to the recorder for storage and remote viewing.
It has **HD analog** or **analog** cameras.	It has **IP** cameras.
a DVR based surveillance system is a **wired** system.	a NVR based surveillance system is a **wired** or **wireless** system.
It is **affordable**.	It is **non-affordable**.
It has **high flexibility**, and **high complexity**.	It has **low flexibility**, and **low complexity**.
Sending video to a recorder by a **digital signal**.	Sending video to a recorder by a **analog signal** or **wireless network**.
Sending video to a recorder by **CAT5** or **CAT6** cable.	Sending video to a recorder by **coaxial** cable.

What is the WAP?

WAP(Wireless Application Protocol) is **a set of communication protocols** that **allow wireless devices** (like NVR, TV remote controls, radios, GPS phones, tablets, Bluetooth mice and keyboards, and wireless routers) **to access the Internet** and other network utilities, such as e-mail and chat_Most wireless networks are supported by WAP ,and WAP is supported by all operating systems as well.

What is the Firewall and what are the types of Firewalls?

The Definition of Firewalls:

A firewall is software or firmware that prevents unauthorized access to a network. It inspects incoming and outgoing traffic using a set of rules to identify and block threats.

Types of Firewalls:

Firewalls are either categorized by the way they **filter** data, or by the system they **protect**.

When categorizing by what they **protect**, the two types are: network-based and host-based.

- Network-based firewalls guard entire networks and are often hardware.
- Host-based firewalls guard individual devices and are often software.

When categorizing by filtering method, the main types are:

- A **packet-filtering firewall** examines packets in isolation and does not know the packet's context.

- A **stateful inspection firewall** examines network traffic to determine whether one packet is related to another packet.
- A **proxy firewall** inspects packets at the application layer of the Open Systems Interconnection (OSI) reference model.
- A **Next Generation Firewall (NGFW)** uses a multilayered approach to integrate enterprise firewall capabilities with an intrusion prevention system (IPS) and application control.

FIREWALL TYPES	ADVANTAGES	DISADVANTAGES
Packet filtering firewall	▪ A single device can filter traffic for the entire network ▪ Efficient and fast at processing packets ▪ Enables complex security policies through filtering on protocol headers ▪ Inexpensive ▪ It has Minimal impact on other resources, network performance, and end-user experience	▪ Incapable of filtering at the application layer ▪ Lacks broad context of other firewall options ▪ Can be difficult to securely configure ▪ Lacks features like user authentication, logging ▪ Vulnerable to spoofing attacks ▪ Access controls lists can be difficult to set up and manage
Circuit-Level gateway	▪ Provides privacy for data passing in/out of private network ▪ More efficient processing traffic than application-level gateways ▪ Relatively inexpensive ▪ Easier to set up and manage ▪ It has Minimal impact on end-user experience	▪ Protects circuits (network sessions) rather than individual packets ▪ Requires modification to network protocol stack ▪ Incapable of content filtering ▪ Should be used in conjunction with other firewall technologies ▪ Does not offer application-layer monitoring

Application-level gateway	▪ Capable of detecting and blocking attacks not visible at the OSI model network or transport layers ▪ Obscures private network details ▪ Protects user anonymity ▪ Enables more fine-grained security controls	▪ Complex to configure and maintain ▪ High processing overhead ▪ Requires a proxy be set up for every network application in use ▪ Can affect network performance
Stateful Inspection firewall	▪ Capable of blocking types of attacks that exploit protocol vulnerabilities ▪ Can operate with fewer open ports, reducing attack surface ▪ Capable of blocking many types of denial-of-service attacks	▪ Can require high degree of skill to securely configure ▪ Does not support authenticated connections ▪ Not effective against exploits of stateless protocols ▪ High processing overhead
Next-Generation firewall	▪ Provides traditional firewall functionality combined with other security functions, including intrusion detection/prevention systems (IDS/IPS), advanced threat intelligence, malware scanning and others ▪ Capable of monitoring network protocols from the data link layer (Layer 2 of the OSI model) through the application layer (Layer 7 of the OSI model) ▪ Offers substantive logging capabilities ▪ Can be more efficient at processing network traffic than combination of firewall plus IDS/IPS and malware scanning	▪ Consolidation of security functions makes the NGFW a single point of failure ▪ Requires high front-end investment of resources to acquire, configure and deploy these complex systems ▪ Depending on architecture, may be processing-intensive ▪ Not all organizations will require all the functionality of an NGFW ▪ Can hinder network performance ▪ More expensive than other firewall options