ITI

Introduction to
Computer Networks & Cyber Security

Prepared By : Mohamed AboSehly

Part 2 (Cyber Security Essentials)

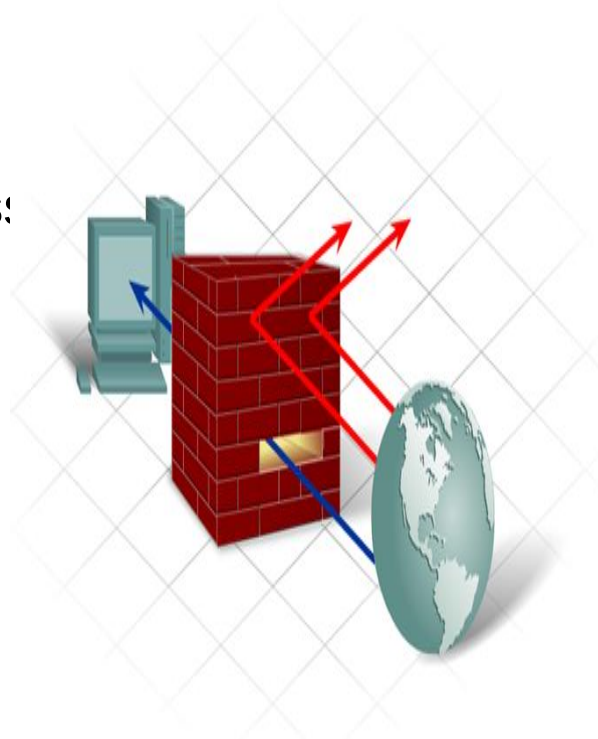
how to protect your Systems

Part2_ Attack Mitigation

- **Hardware**
  - Firewalls
  - DMZ
  - IDS/IPS
  - NGFW
- **Software**
  - Anti-virus
  - Anti-spam
  - Anti-malware
  - Security Patches
  - User Access Control

Part 2 _ Firewall

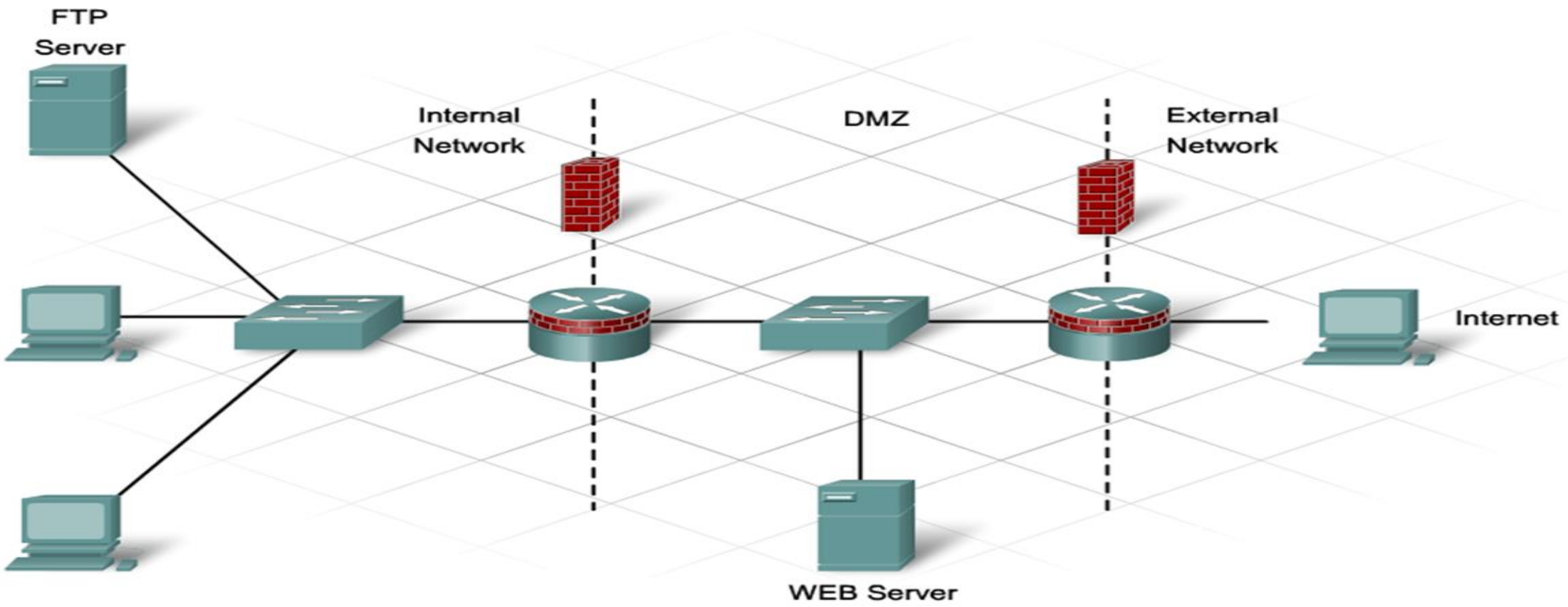
- A Firewall is one of the most effective security tools available for protecting internal network users from external threats As the first line of defense
- A firewall resides between two or more networks and controls the traffic between them as well as helps prevent unauthorized acces
- A firewall can be software-based or hardware-based



- **Static Packet Filtering (stateless firewall)**
  - - Prevents or allows access based on IP or MAC addresses.

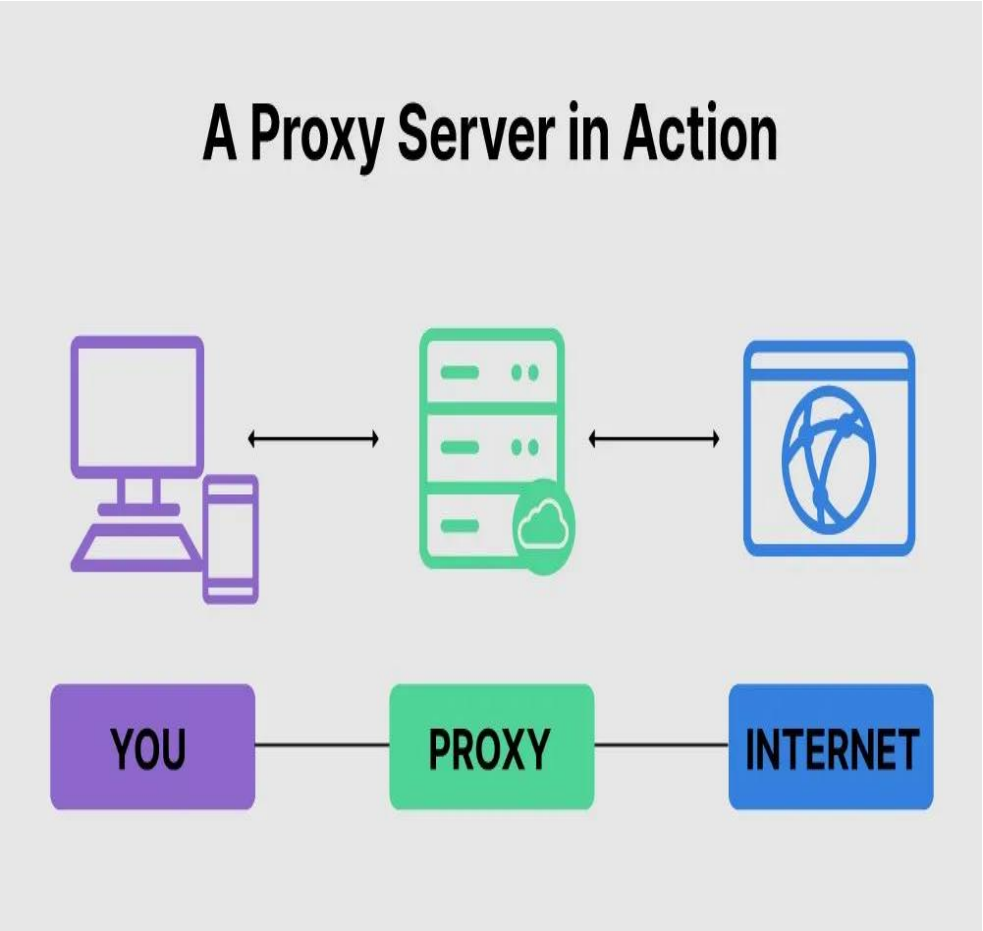
- **Dynamic Packet Filtering (state full firewall)**
  - Incoming packets must be legitimate responses to requests from internal hosts. filter out specific types of attacks such as DoS

Part 2 _Firewall



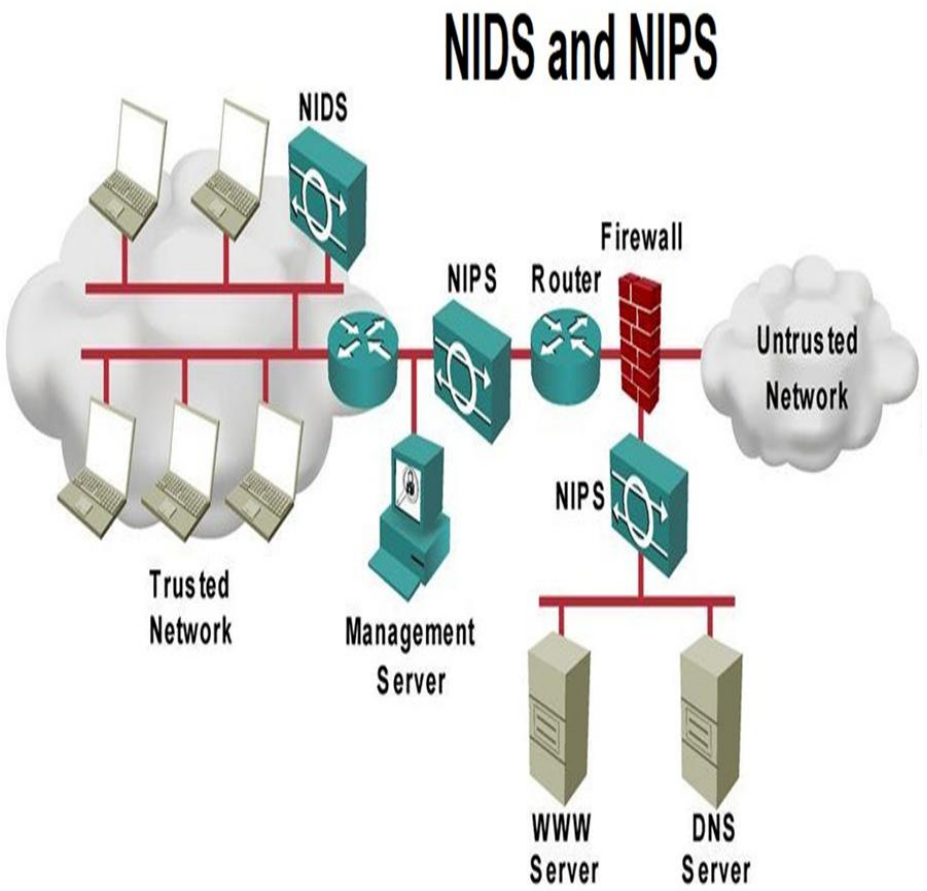
Part 2 _ Proxy Server

- A **computer system** (or an application program) that intercepts internal user requests and then processes that request on behalf of the user
- Goal is to **hide the IP address** of client systems inside the secure network



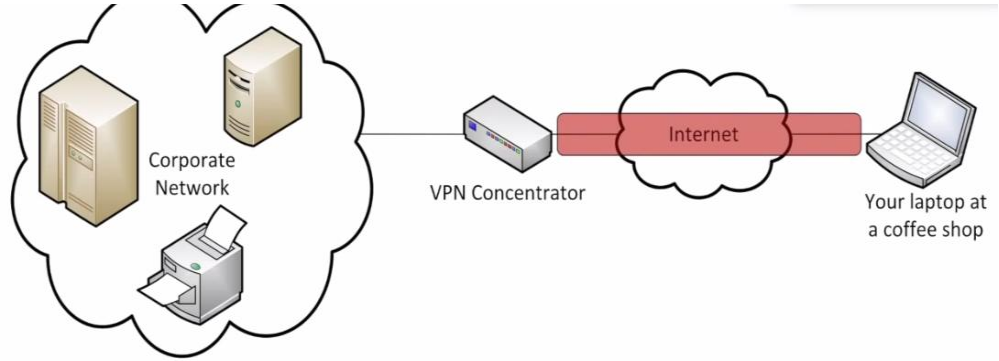
Part 2_ IDS/IPS

- Network Intrusion Detection System (NIDS):
  - **Watch** the Network Traffic and if there **is Intrusion it Detects** that there is Bad traffic Flow.
  - it **send alarms and logs**
- Network Intrusion prevention System (NIPS):
  - **Stops** the traffic if it **detects that there is intrusion**
- Types of IDS&IPS
  - **Signature-based:** look for the perfect match
  - **Anomaly-based:** Built a based line of what is normal
  - **Behavior-based:** **observe and report**



VPN

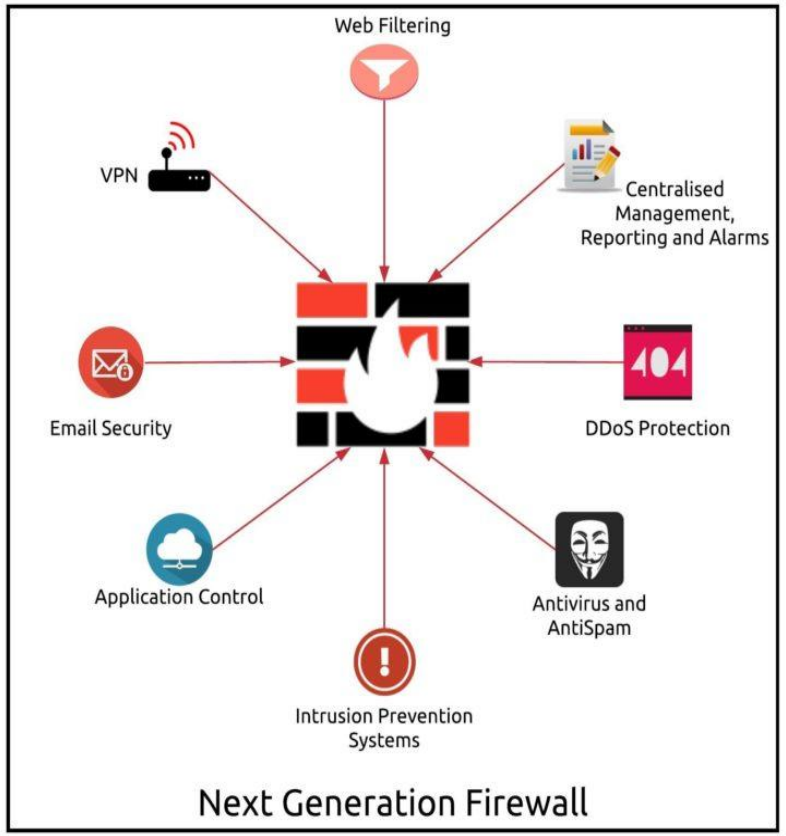
- It Tunnel the traffic between the Two Sides of Network
- Types:
  - Remote Access VPN
  - Site to Site VPN



SIte-to-Site VPN

Part 2 _ Next generation Firewall (NGFW)

- **Next generation Firewall (NGFW)**
  - a “deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall.”



Part 2 _Wireless Security

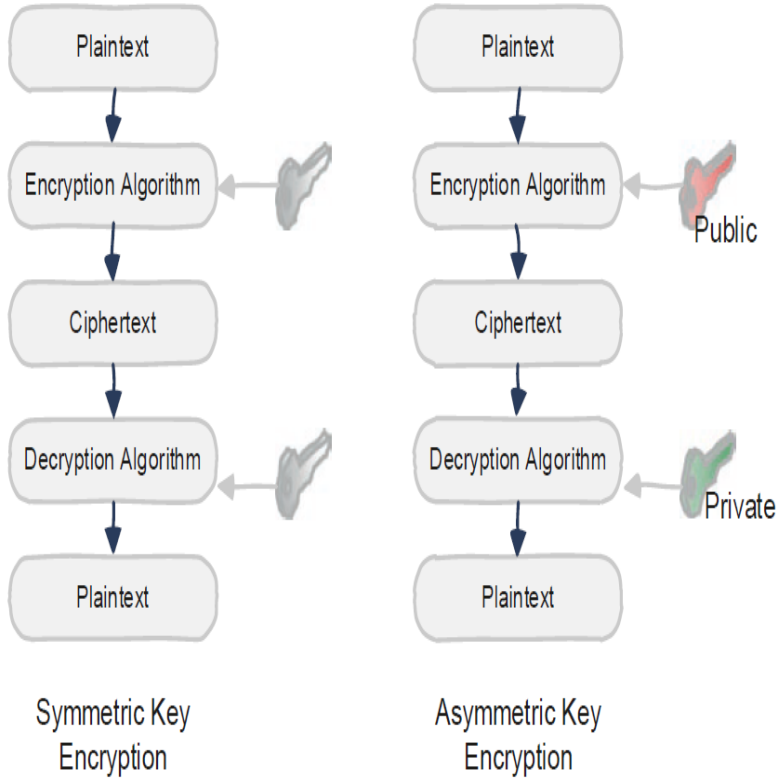
- Open Access
  - SSID
  - No encryption
  - Basic authentication
  - Not a security handle
- WPA2
  - AES Encryption
  - Authentication
- WPA3
  - Protected from Brute-force attack

Part 2_Controlling Wireless LAN Access

- SSID broadcasts from access points are off
- MAC Address filtering is enabled
- WPA2 / WPA3 Security implemented

Part 2_ Encryption

- **Encryption**
  - encryption is the process of **encoding information.** This process converts the original representation of the information, known as **plaintext**, into an alternative form known as **ciphertext.**
  - Unencrypted data, called plaintext, is sent through an encryption algorithm to generate a ciphertext. **A key** is used for encryption.
  - in **a symmetric encryption** algorithm, the **same key** is also **used for decryption**. (Not secure) needs to be a secure way for the two sides to have the same key

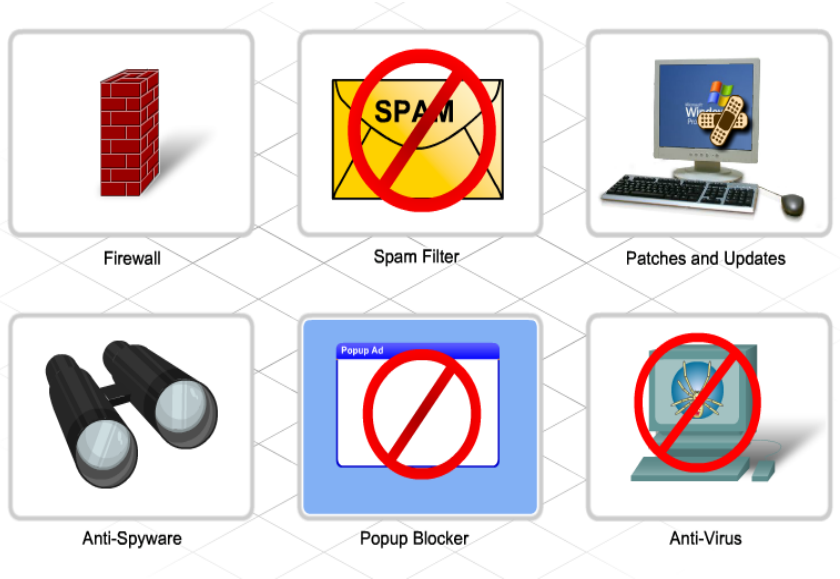


Part2 lab Practices

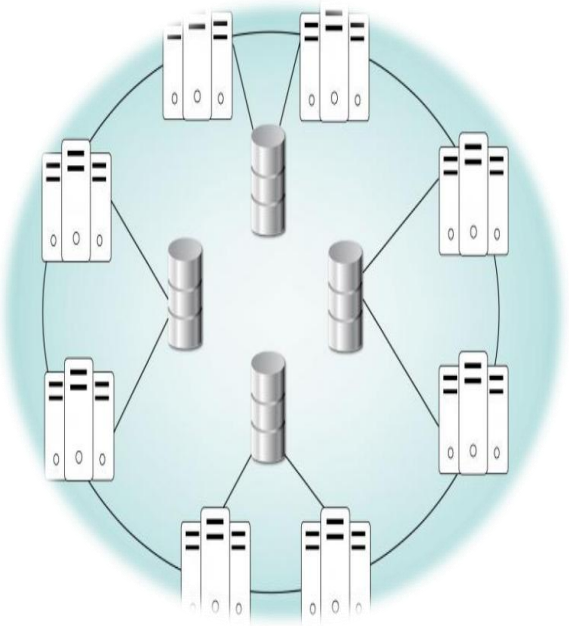
- How to use your local firewall to block a port and stop DOS attack from a zombie device

Best Practices

- ✓ Define security policies
- ✓ Physically secure servers and network equipment
- ✓ Set login and file access permissions
- ✓ Update OS and applications
- ✓ Change permissive default settings
- ✓ Run anti-virus and anti-spyware
- ✓ Update antivirus software files
- ✓ Activate browser tools –
- ✓ Popup stoppers, anti-phishing, plug-in monitors
- ✓ Use a firewall



Distributed Systems & Cloud Computing



Session 3 (Distributed Systems)

- **Outlines**
  - **Distributed Systems overview**
    - Definition and Basic Terminologies
  - **Why build a distributed system?**
  - **Types of Distributed Systems**
    - The 4 Distributed Systems architecture
  - **Cloud computing**
    - Cloud computing service models
    - Cloud computing deployment models

What is Distributed Systems ?

Distributed Systems

-Is a group of computers working together as to appear as a single computer to the end-user.

-Is a collection of independent components located on different machines that share messages with each other in order to **achieve common goals.**

Centralized system VS Distributed system

- **Centralized system:** State stored on a **single computer**
  - Simpler
  - Easier to understand
  - Can be faster for a single user

- **Distributed system:** State divided over **multiple computers**
  - More robust (can tolerate failures)
  - More scalable (often supports many users)
  - More complex

Why build a distributed system?

- **One interface** to the end-user.
- **Performance**
  - maximize resources and information while preventing failures
- **Reliability**
  - if one system fails, it won't affect the availability of the service
- **Dependency on cloud**
- **Scaling**

Distributed system is growing…They are everywhere!

- modern applications no longer run in isolation. The vast majority of products and applications rely on distributed systems such as :

➢ **Networks**
  - LAN/ Internet

➢ **Distributed Real-time Systems**
  - **Uber and logistics** use real-time tracking systems.

➢ **Parallel Processing**
  - Could Computing

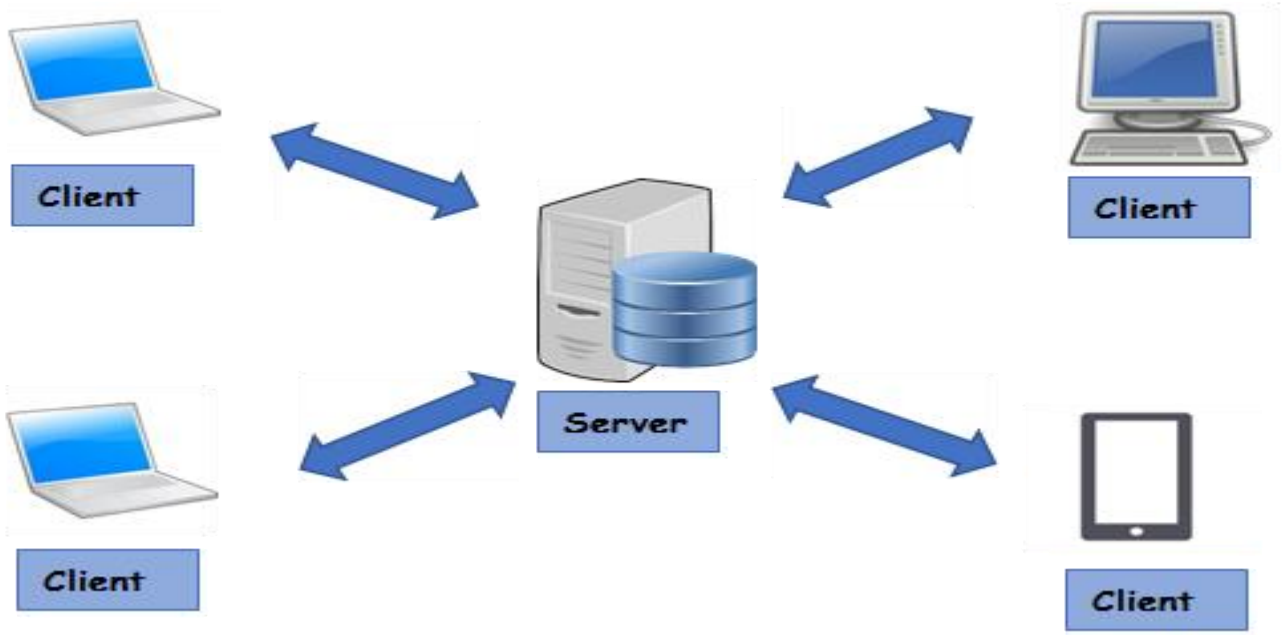
➢ **Distributed Database Systems**
  - **Multiple servers and/or physical locations**. The data can either be **replicated o**r duplicated across systems.

Types of Distributed System Architectures:

Four architecture types :

1- Client-server:

- a server as a shared resource like (a printer, database, or a web server)
- Multiple clients use the shared resource.

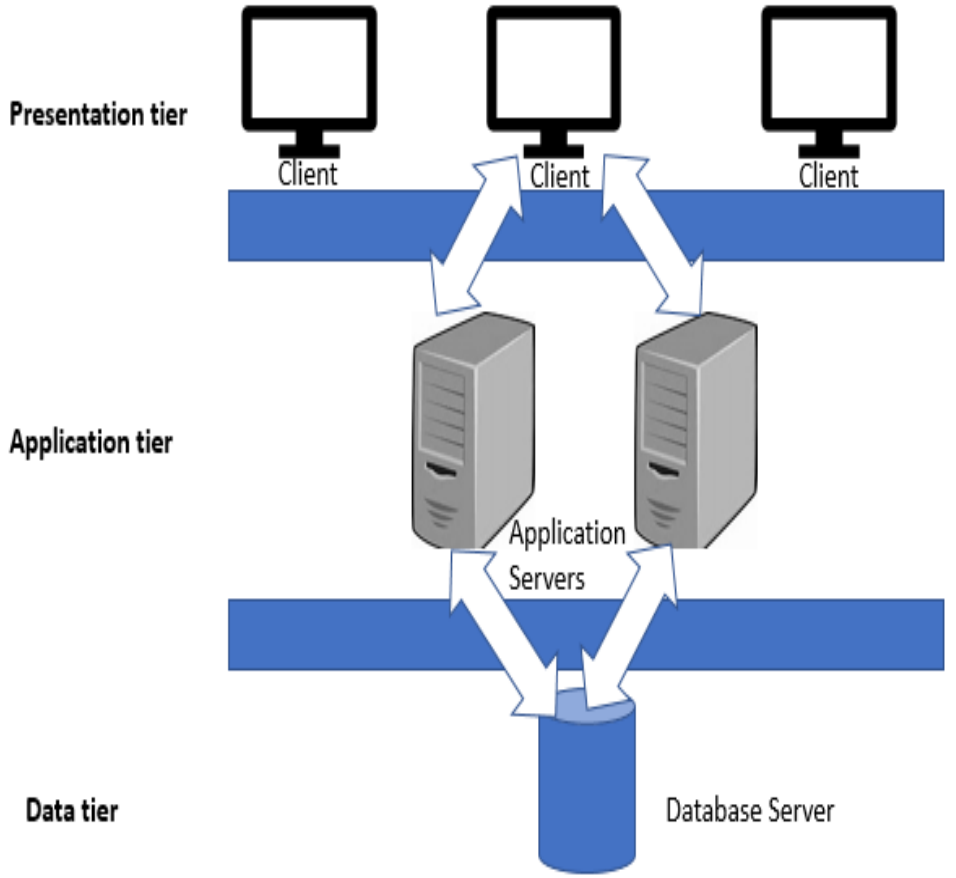


Types of Distributed System Architectures:

Four architecture types :

2- Three-tier:

- clients no longer need to be intelligent
- can rely on a **middle tier** to do the **processing and decision making**.
- Most of the first web applications fall under this category.
- **The middle tier** could be **called an agent** that receives requests from clients, and then forwards it on to the servers.



Types of Distributed System Architectures:

Four architecture types :

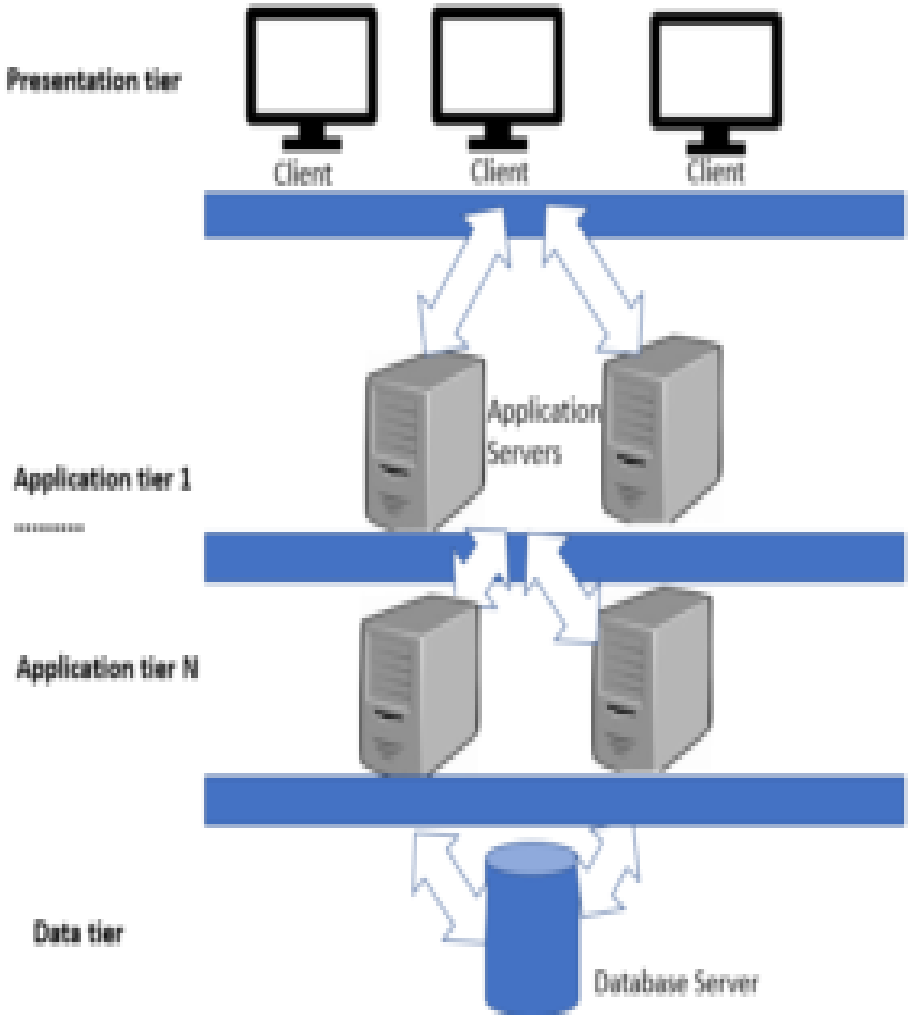
3- Multi-tier:

- Enterprise web services first created **n-tier or multi-tier systems architectures**.

-This popularized the application servers that contain the business logic

- n-tier interacts both with the data tiers and presentation tiers.

- Ex : google.com



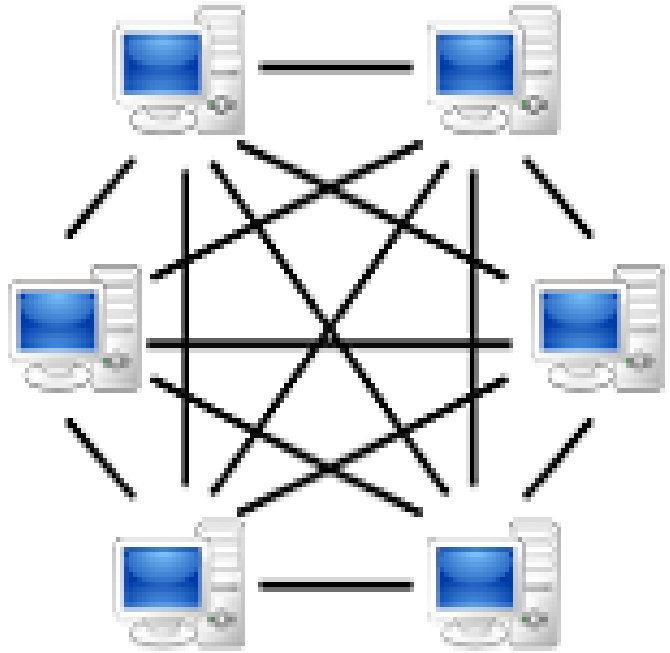
Types of Distributed System Architectures:

Four architecture types :

4- Peer-to-peer :

- **No centralized** or special machine that does the heavy lifting and intelligent work in this architecture.

- All the **decision** making and responsibilities are **split up amongst the machines** involved and each could take on client or server roles.
  - Blockchain is a good example of this.



Examples of Distributed Systems

Distributed system Examples

- Domain Name System (DNS)
  - Distributed lookup table of hostname to IP address
- Facebook & Google use distributed systems extensively
  - Massive scale
  - Fast enough
  - Very reliable
- Email servers (SMTP)

Session 3 (Virtualization)

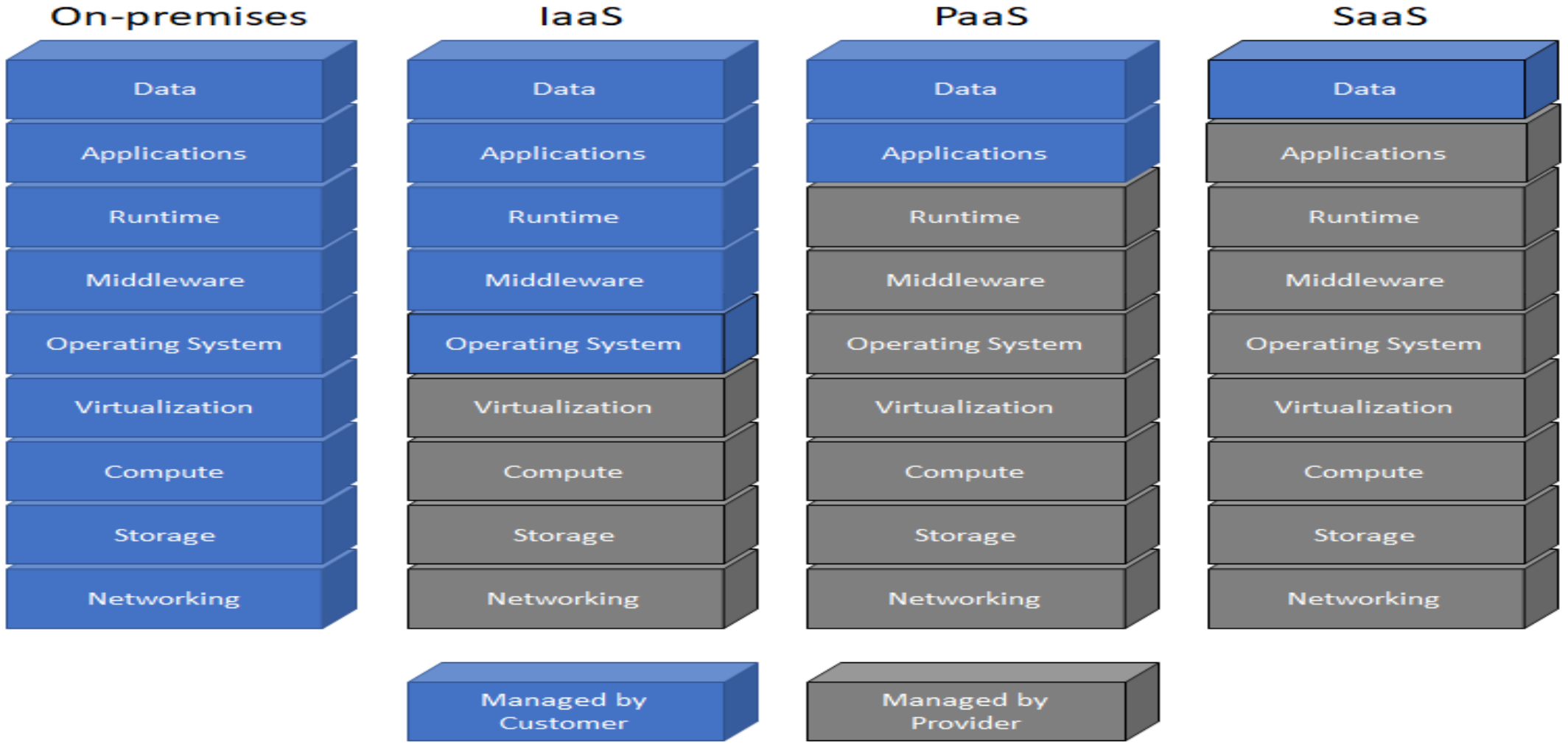
- **Virtualization**
  - Is a technology that run multiple same or different operating systems which is completely isolated from each other
  - Example: run both windows and Linux on the same machine

  - Virtualization is different from Dual Boot ?
  - Dual Boot run only one OS at the same time Virtualization run multiple OS at the same time
- **Virtualization Benefits**
  - Redundancy
  - Legacy hardware
  - Migration
  - Centralized management

Cloud computing

- **Cloud computing**
  - A pool of resources that can be rapidly provisioned in an automated, on-demand manner.
- **Value of cloud computing is :**
  - Economies of scale
  - Elastic enough to scale with the needs of your organization.
  - Cost and operational benefits
  - Easily accessed by users no matter where they reside

Cloud computing service models



Cloud computing service models

- **Software as a service (SaaS).**
  - Customers are provided access to **an application** running on a cloud infrastructure.
  - but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure.
- **Platform as a service (PaaS).**
  - Customers can **deploy supported applications** onto the provider's cloud infrastructure,
  - but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure.
  - The company owns the deployed applications and data, and it is therefore responsible for the security of those applications and data.
- **Infrastructure as a service (IaaS).**
  - Customers can provision **processing, storage, networks, and other computing resources**, and **deploy and run operating systems and applications.**
  - the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over operating systems, storage, and deployed applications, along with some networking components (for example, host firewalls).
  - The company owns the deployed applications and data, and it is therefore responsible for the security of those applications and data.

Cloud computing deployment models:

- **Public.**
  - A cloud infrastructure that is open to use by the general public. It's owned, managed, and operated by a third party (or parties), and it exists on the cloud provider's premises.
- **Community.**
  - A cloud infrastructure that is used exclusively by a specific group of organizations.
- **Private.**
  - A cloud infrastructure that is used exclusively by a single organization. It may be owned, managed, and operated by the organization or a third party (or a combination of both), and it may exist on premises or off premises.
- **Hybrid.**
  - A cloud infrastructure that comprises two or more of the aforementioned deployment models, bound by standardized or proprietary technology that enables data and application portability (for example, fail over to a secondary data center for disaster recovery or content delivery networks across multiple clouds).

Pros and Cons of Distributed Systems

- **Cons**
  - **Complexity is the biggest disadvantage** of distributed systems.

    There are more machines, more messages, more data being passed between more parties which leads to issues with:

    - **Data Integration & Consistency**
    - **Network and Communication Failure**
    - **Management Overhead**

- **Pros**
  - The ultimate **goal** of a distributed system is to **enable the scalability**, **performance and high availability** of applications.
  - **Major benefits include:**

    - **Unlimited Horizontal Scaling** - machines can be added whenever required.
    - **Low Latency** - having machines that are geographically located closer to users, it will reduce the time it takes to serve users. (google servers)
    - **Fault Tolerance** - if one server or data center goes down, others could still serve the users of the service.

Part3 lab Practices

- Use the VMware Workstation tool to host the two different
- OS on your machine

Thank You