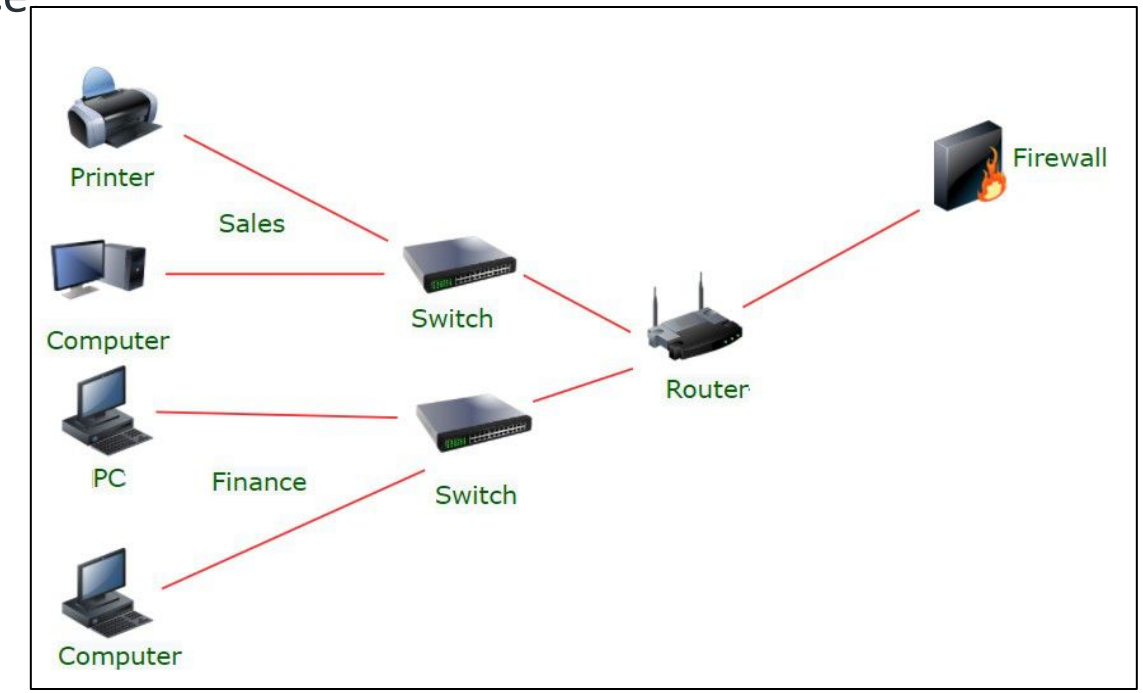
Introduction to Cyber Security

Course Incharge: **Yahya Batla**

Course Instructor: **Umar Bilal**

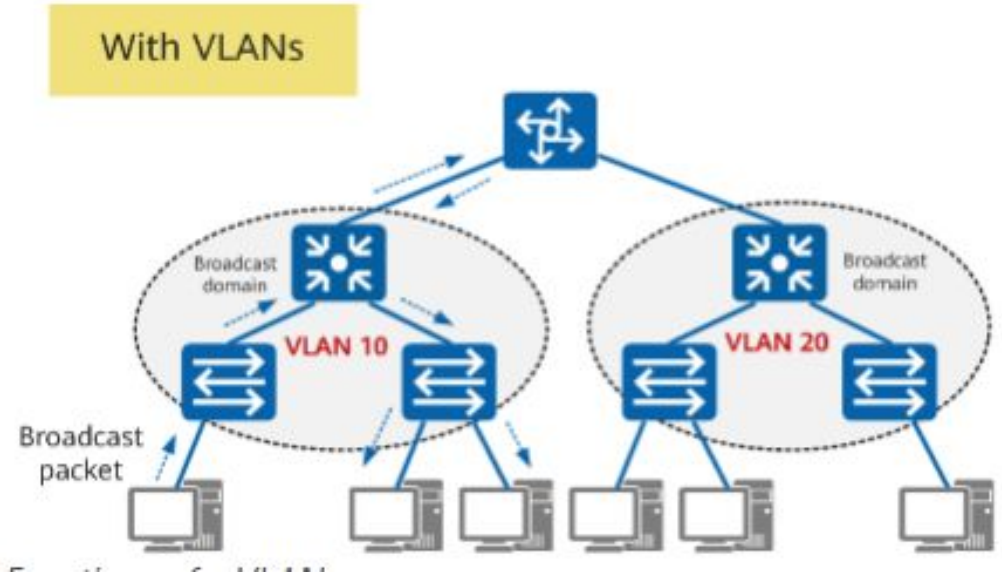
Network Segmentation :

Network segmentation has several benefits for organizations. It does not have a single purpose, but primarily it is used to organize networks. Segmentation also allows for more efficient use of bandwidth by reducing the size of broadcast domains and getting rid of unnecessary traffic on the network. Another benefit of having a segmented network is that it enhances security by reducing an organization's attack surface by not keeping all computers in the same network space



Virtual Local Area Network

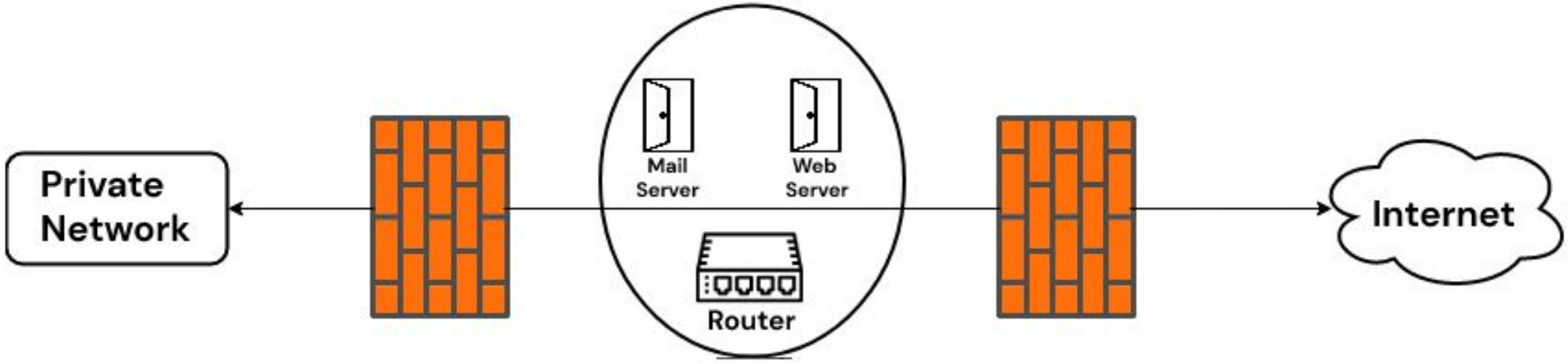
VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.



Demilitarized zone network

Demilitarized zones, or DMZ for short, are used in cybersecurity. DMZs separate internal networks from the internet and are often found on corporate networks. A DMZ is typically created on a company's internal network to isolate the company from external threats. While the name might sound negative, a DMZ can be a helpful tool for network security.

DMZ is a network barrier between the trusted and untrusted network in a company's private and public network. The DMZ acts as a protection layer through which outside users cannot access the company's data. DMZ receives requests from outside users or public networks to access the information, website of a company.



Benefits of Using a DMZ

Preventing network reconnaissance:

By providing a buffer between the internet and a private network, a DMZ prevents attackers from performing the reconnaissance work they carry out the search for potential targets. Servers within the DMZ are exposed publicly but are offered another layer of security by a firewall that prevents an attacker from seeing inside the internal network. Even if a DMZ system gets compromised, the internal firewall separates the private network from the DMZ to keep it secure and make external reconnaissance difficult.

Blocking Internet Protocol (IP) spoofing:

Attackers attempt to find ways to gain access to systems by spoofing an IP address and impersonating an approved device signed in to a network. A DMZ can discover and stall such spoofing attempts as another service verifies the legitimacy of the IP address.

DMZ Services:

Services of a DMZ include:

- DNS servers
- FTP servers
- Mail servers
- Proxy servers
- Web servers

Cloud Computing:

Cloud computing refers to the use of hosted services, such as data storage, servers, databases, networking, and software over the internet. The data is stored on physical servers, which are maintained by a cloud service provider. Computer system resources, especially data storage and computing power, are available on-demand, without direct management by the user in cloud computing.

On-Premises Infrastructure:

On-premises refers to the traditional way of managing computing resources, networking, storage, and software, where everything is housed on a company's own physical site, such as a data center. An organization retains total control over hardware and software, along with settings and configurations. This may be an important consideration for organizations with strict security requirements or regulatory concerns

Factor	Cloud Computing	On-Premises Computing
Cost	Pay for what you use; no upfront investment in hardware	More expensive in the long run due to investment in hardware
Scalability	Easily scalable without additional investment in hardware	Difficult to scale; requires investment in additional hardware
Reliability	High levels of reliability with guaranteed uptime	More prone to downtime and interruptions
Security	Improved security measures with dedicated security teams	Complete control over security measures and data
Flexibility	Accessible from anywhere with an internet connection	Limited to on-site access
Data Control	Entrusting data to a third-party provider	Complete control over data and compliance measures

Types Of Cloud Computing:

- Private Cloud
- Public Cloud
- Hybrid Cloud

Private Cloud :

Private cloud, the computing services are offered over a private IT network for the dedicated use of a single organization. Also termed internal, enterprise, or corporate cloud, a private cloud is usually managed via internal resources and is not accessible to anyone outside the organization.

Reasons for Popularity of Private Cloud Environments :

A private cloud is suitable to use when:

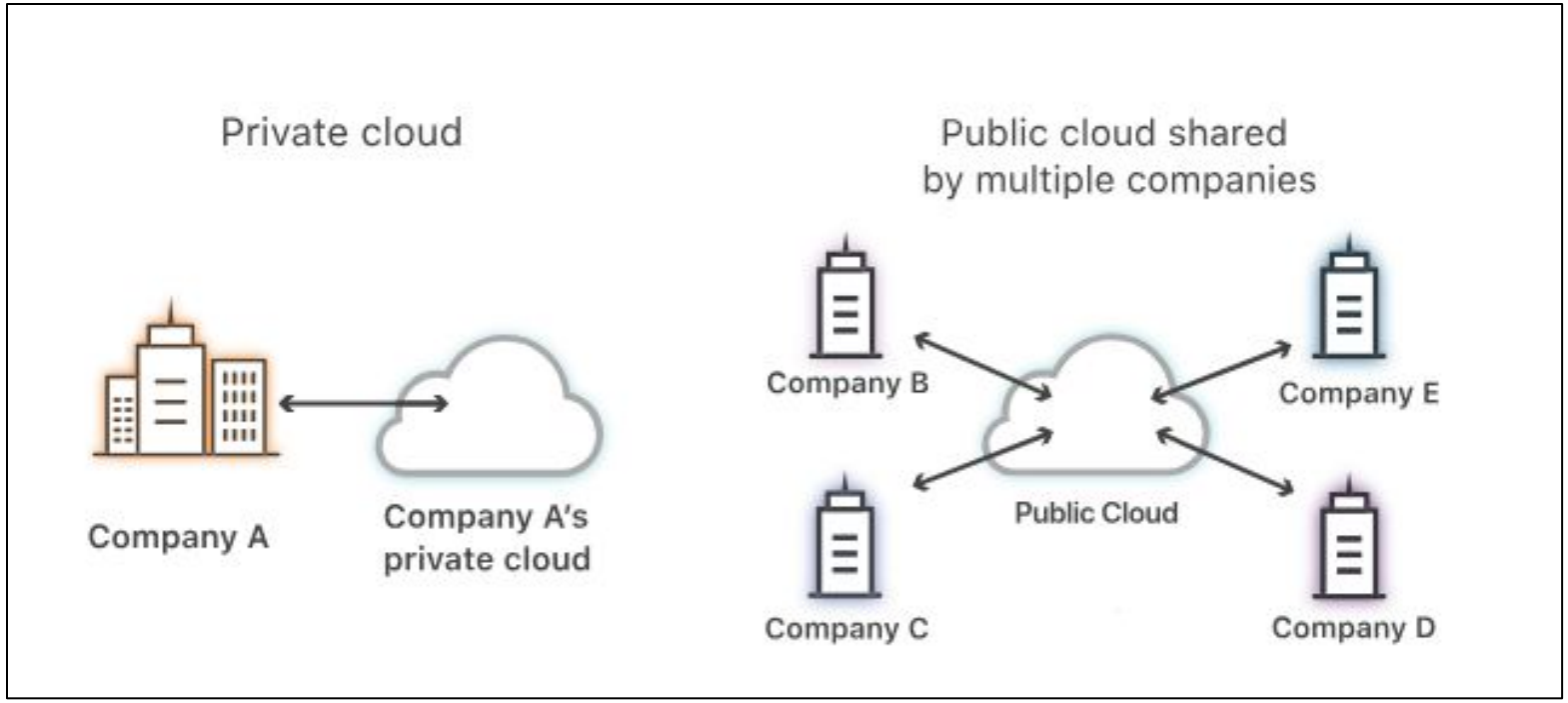
1) There is a requirement for high security for sensitive data as the resources in a private cloud can be accessed only by trusted people within an organization. It is not accessible over the public internet.
2) The organization requires high control and more isolation in the system and resources.
3) A high level of resource customization is required for any business logic. Since the infrastructure is dedicated, it becomes easier to customize.

Public Cloud:

Public cloud refers to computing services offered by third-party providers over the internet. Unlike private cloud, the services on public cloud are available to anyone who wants to use or purchase them. These services could be free or sold on-demand, where users only have to pay per usage for the CPU cycles, storage, or bandwidth they consume.

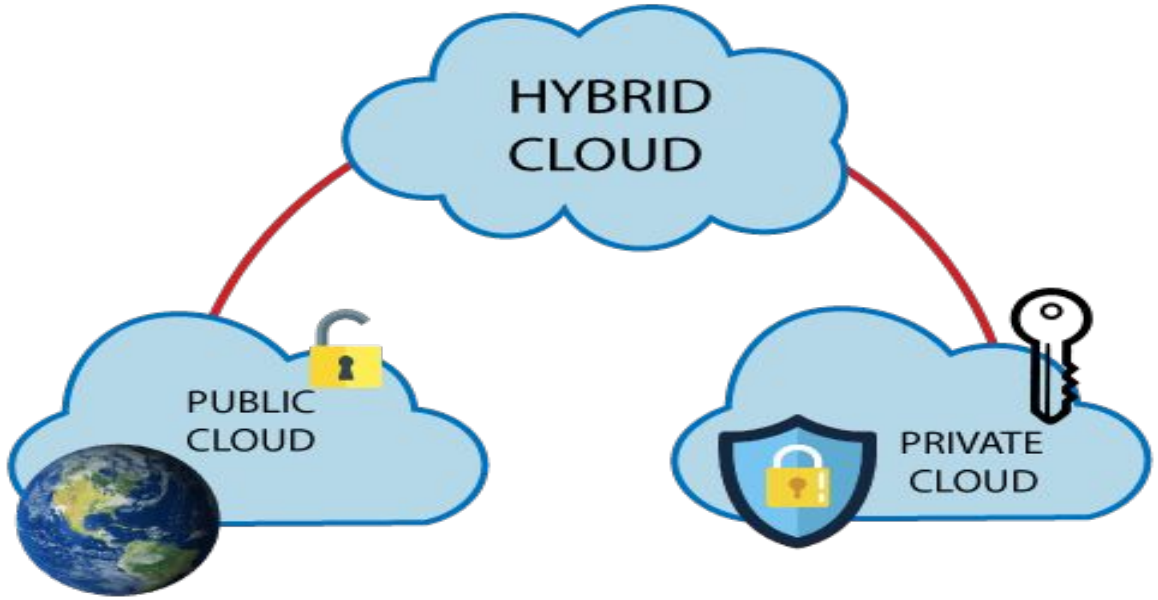
- Public Cloud provides a shared platform that is accessible to the general public through an Internet connection.
- Public cloud operated on the pay-as-per-use model and administrated by the third party, i.e., Cloud service provider.
- In the Public cloud, the same storage is being used by multiple users at the same time.

Public Cloud VS Private Cloud :



Hybrid Cloud :

A hybrid cloud integrates infrastructure components on-premises, private, and public cloud sources into one centralized, distributed computing environment. It enables you to manage and orchestrate traditional and cloud native workloads across various infrastructure components, allowing you to use the most suitable resource for each scenario while centralizing management.



Model of Cloud Computing :

Platform as a service (PaaS)

Software as a service (SaaS)

Infrastructure as a service (IaaS)

Platform as a service (PaaS):

Platform as a service or PaaS is a type of cloud computing that provides a development and deployment environment in cloud that allows users to develop and run applications without the complexity of building or maintaining the infrastructure. It provides users with resources to develop cloud-based applications. In this type of service, a user purchases the resources from a vendor on a pay-as-you-go basis and can access them over a secure connection.

Model of Cloud Computing :

Platform as a service (PaaS)

Software as a service (SaaS)

Infrastructure as a service (IaaS)

Software as a service (SaaS)

SaaS or software as a service allows users to access a vendor's software on cloud on a subscription basis. In this type of cloud computing, users don't need to install or download applications on their local devices. Instead, the applications are located on a remote cloud network that can be directly accessed through the web or an API. Software as a Service is commonly accessed through a web browser, with users logging into the system using a username and password. Instead of each user having to install the software on their computer, the user can access the program via the internet.

Model of Cloud Computing :

Platform as a service (PaaS)

Software as a service (SaaS)

Infrastructure as a service (IaaS)

Infrastructure as a service (IaaS)

Infrastructure as a service is also known as Hardware as a Service (HaaS). It is one of the layers of the cloud computing platform. It allows customers to outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources. Customers access these resources on the Internet using a pay-as-per use model.

In traditional hosting services, IT infrastructure was rented out for a specific period of time, with pre-determined hardware configuration. The client paid for the configuration and time, regardless of the actual use. With the help of the IaaS cloud computing platform layer, clients can dynamically scale the configuration to meet changing requirements and are billed only for the services actually used.

Best Cloud Service Provider :

Google Cloud (GCP)

Amazon (AWS)

Microsoft (Azure)

THANK YOU