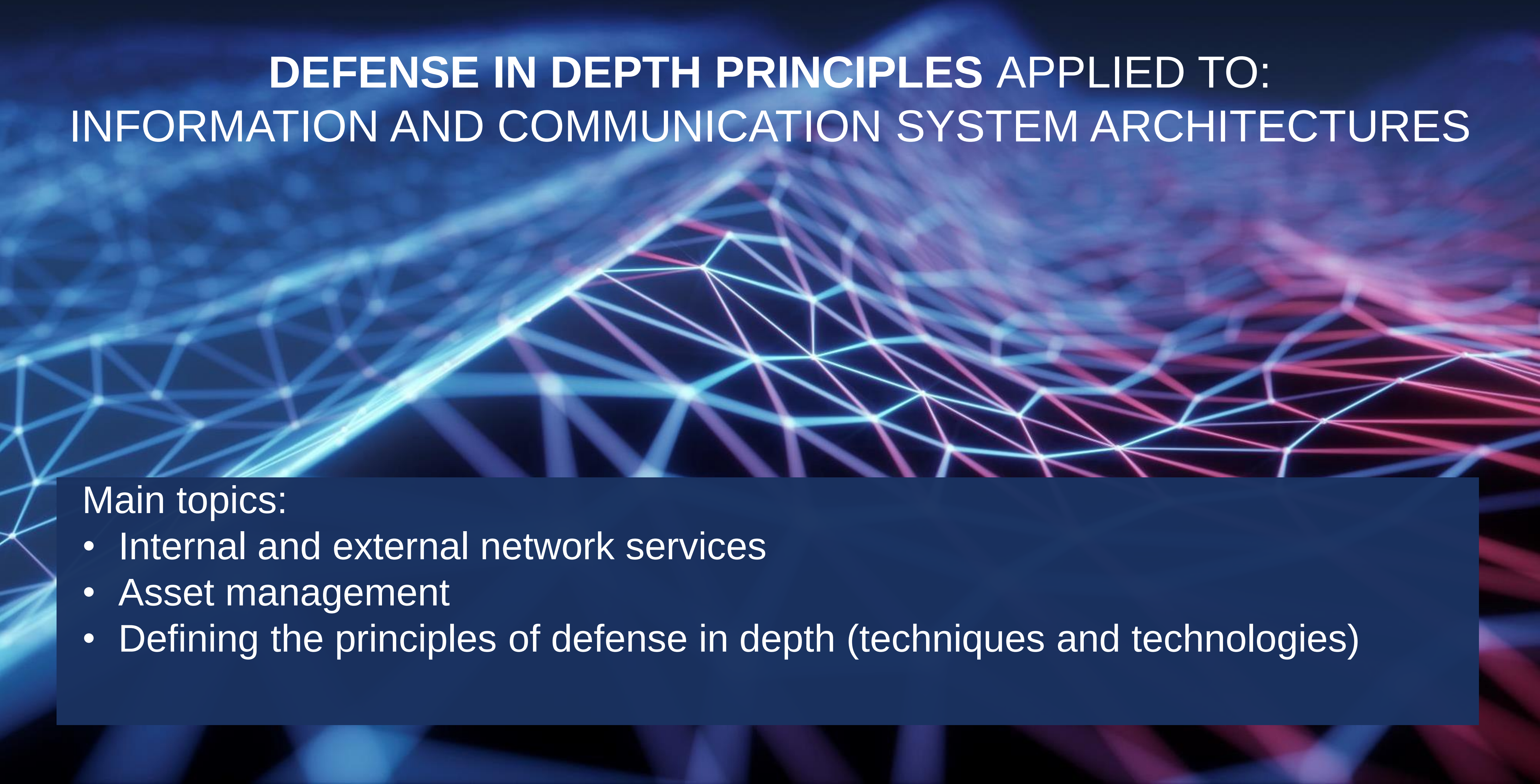


DEFENSE IN DEPTH PRINCIPLES APPLIED TO: INFORMATION AND COMMUNICATION SYSTEM ARCHITECTURES

Main topics:

- Internal and external network services
- Asset management
- Defining the principles of defense in depth (techniques and technologies)

COURSE STRUCTURE

Part 1

- Defining security zones
- Types of devices and their controls in each zone

Part 2

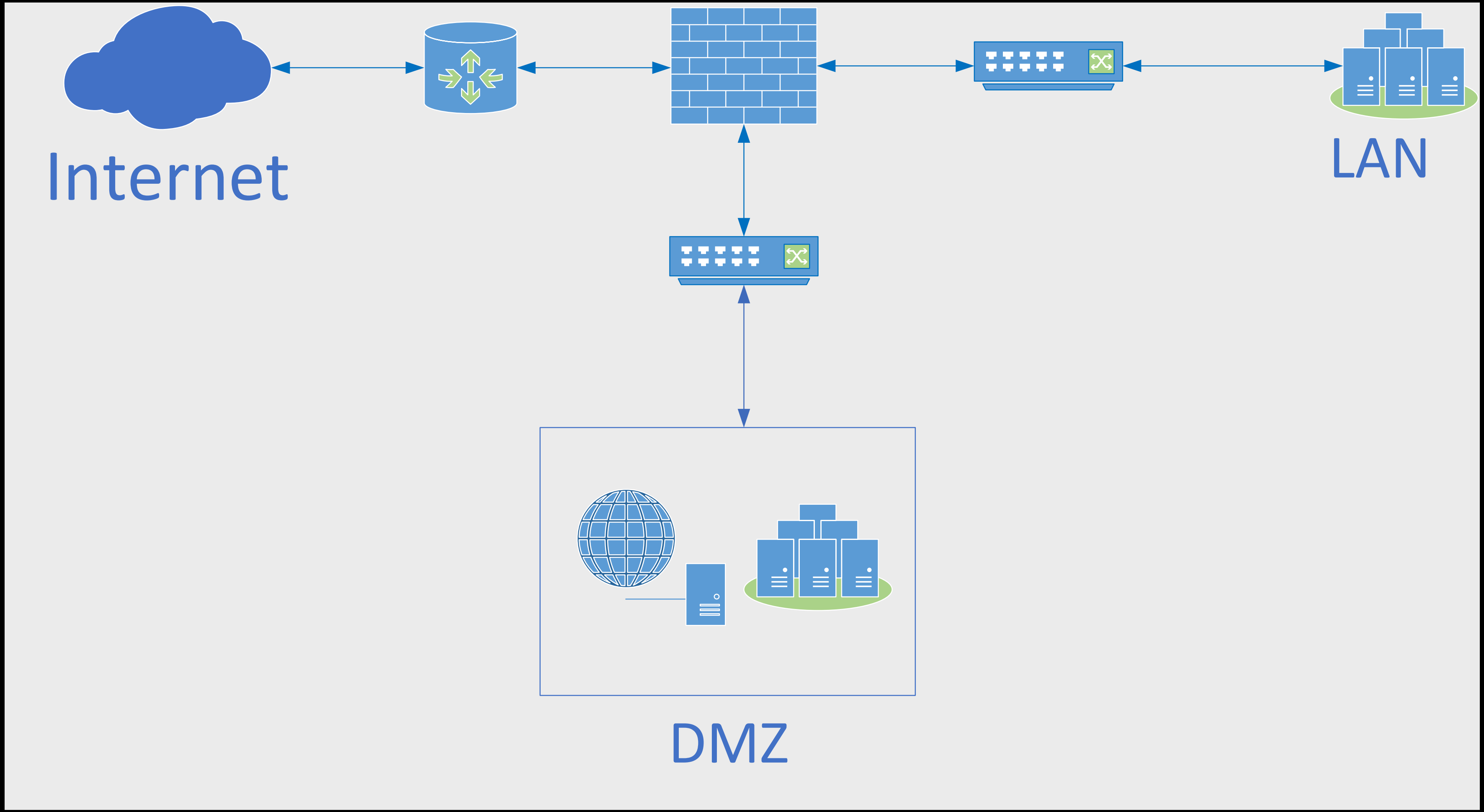
- Defining the services that are needed for a company
- Ways of securing these services

SECURITY ZONES

- **Internet**
(external zone)

- **DMZ**
(demilitarized zone)

- **LAN**
(internal zone)



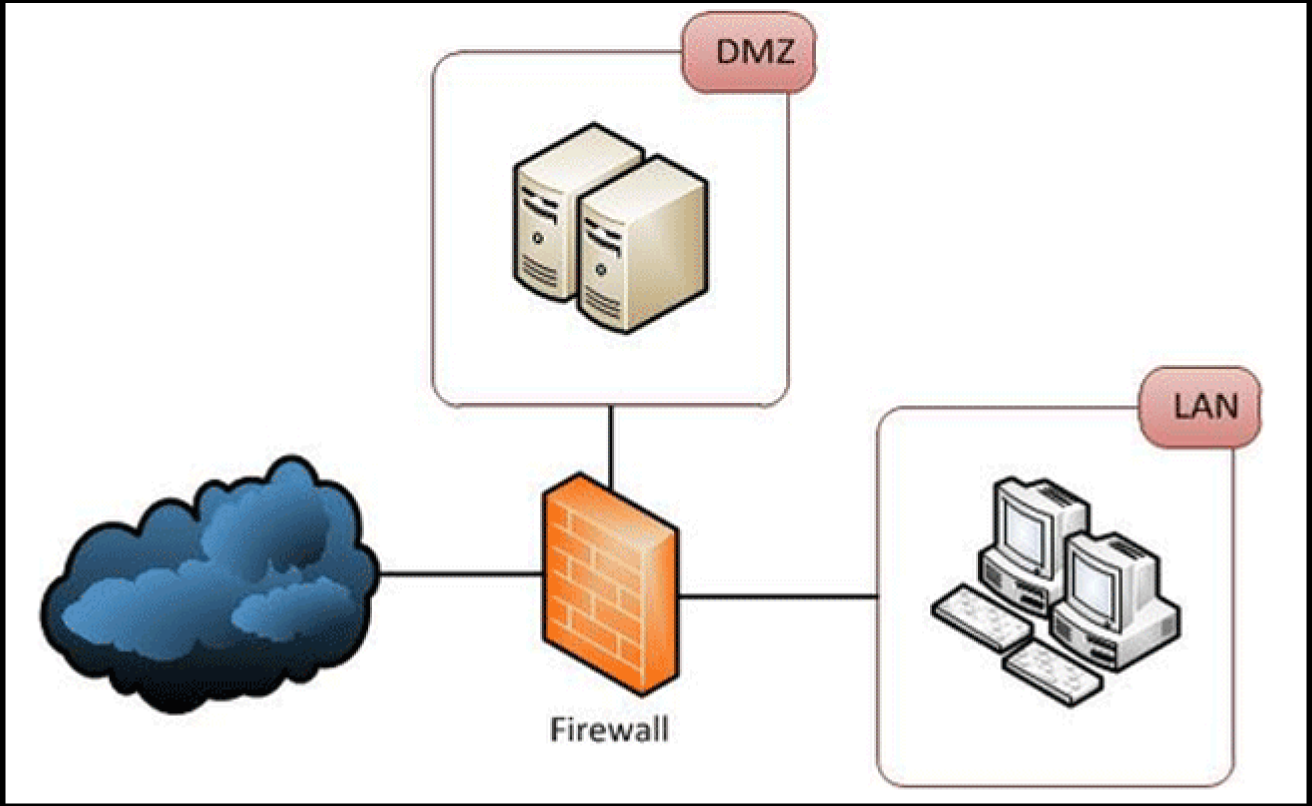
INTERNET

We must figure out what policies that can be adopted and enforced will protect people from the harmful side effects of this global infrastructure.

The question is, how do we collaborate not only to create the Internet, which is a grand global collaboration, but how do we also collaborate to make the Internet safer and more secure and a more trusted environment according to co-inventor of TCP/IP - *Vinton Gray Cerf.*

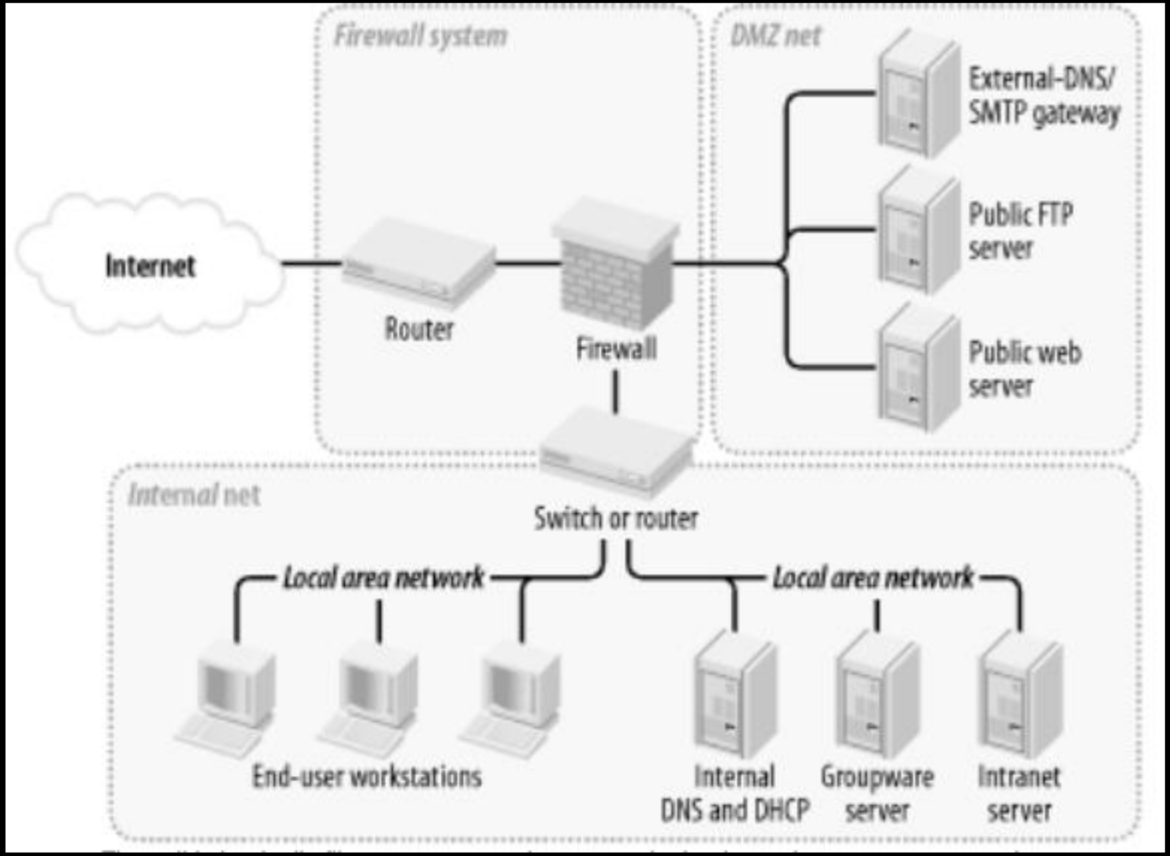
DMZ

DMZ or demilitarized zone (sometimes referred to as a perimeter network or screened subnet) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.



LAN (INTERNAL LAN)

Corporate Internal Network, in which all the services and corporate assets are connected.

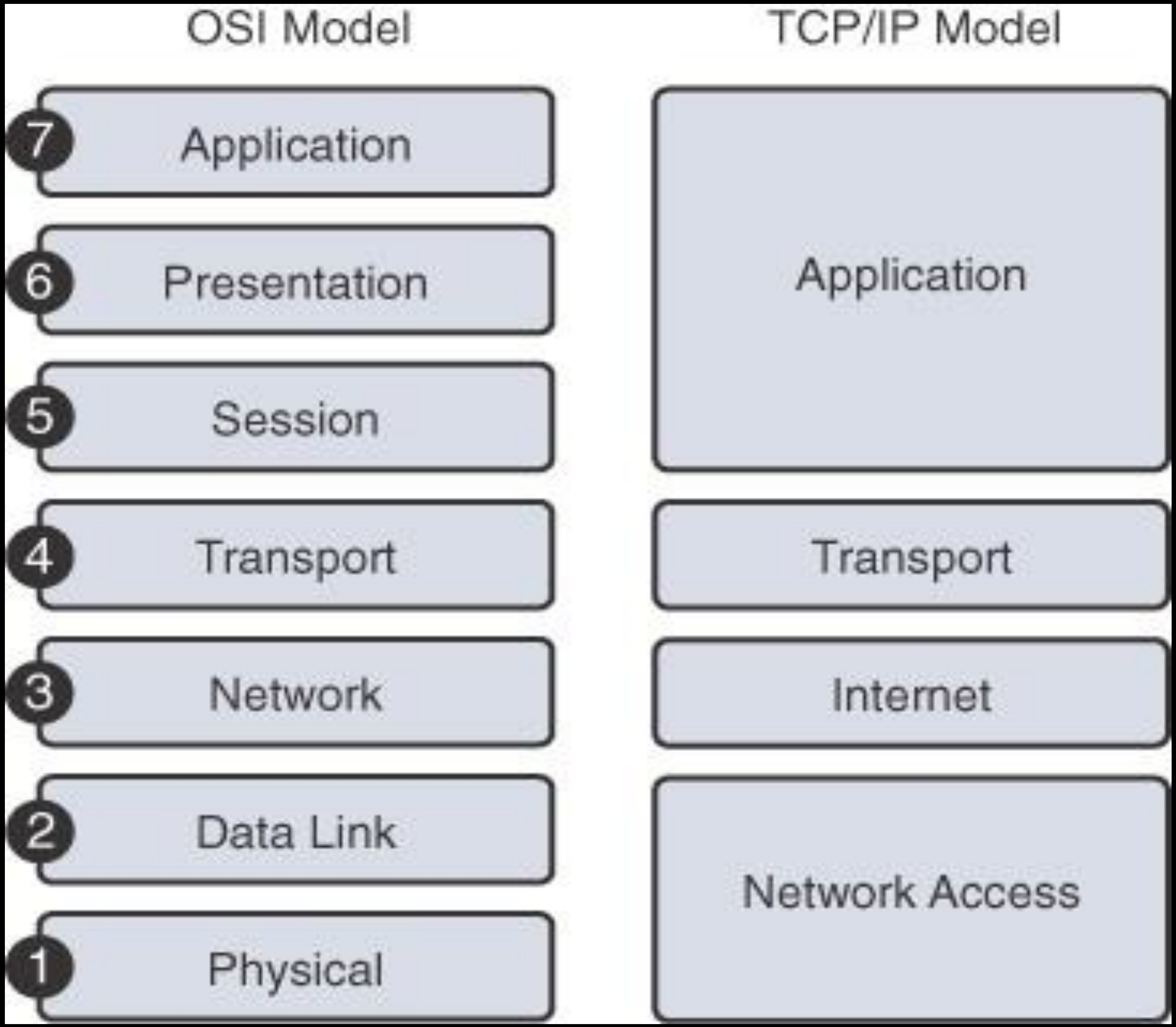


DEVICES AND THEIR CONTROLS IN EACH ZONE

OSI/TCP-IP STACKS

OSI

OSI (Open systems interconnect) is a reference model that depicts data communication over a network. It was created based on a proposal from International Organization for Standardization (ISO)



OSI Model

7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

TCP/IP Model

Application

Transport

Internet

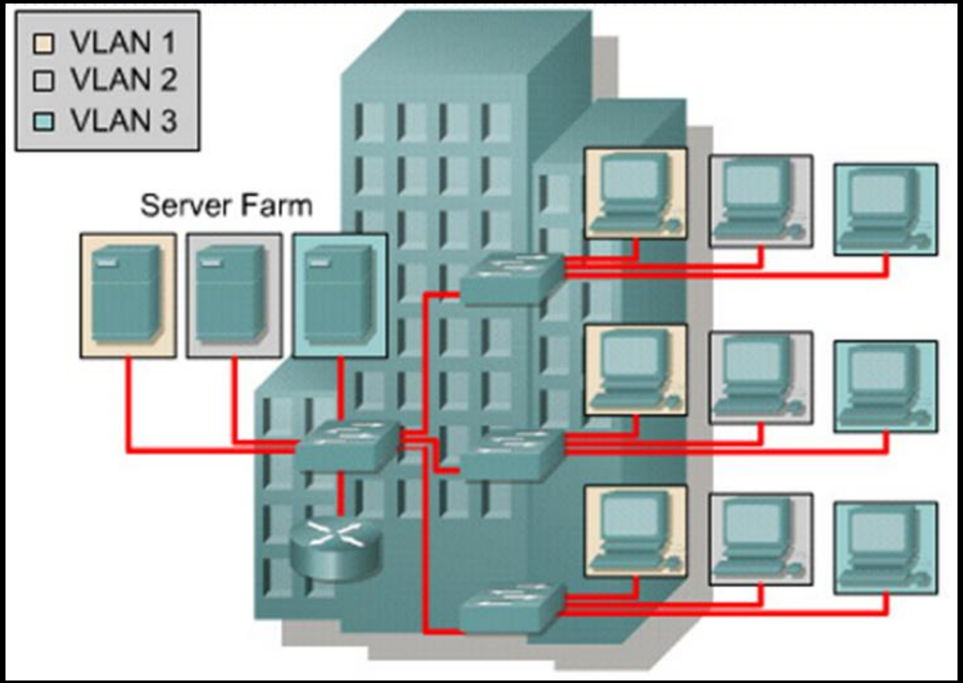
Network Access

TCP/IP

TCP (Transmission Control Protocol) /IP (Internet Protocol) was developed by the Department of Defense (DoD) project agency.

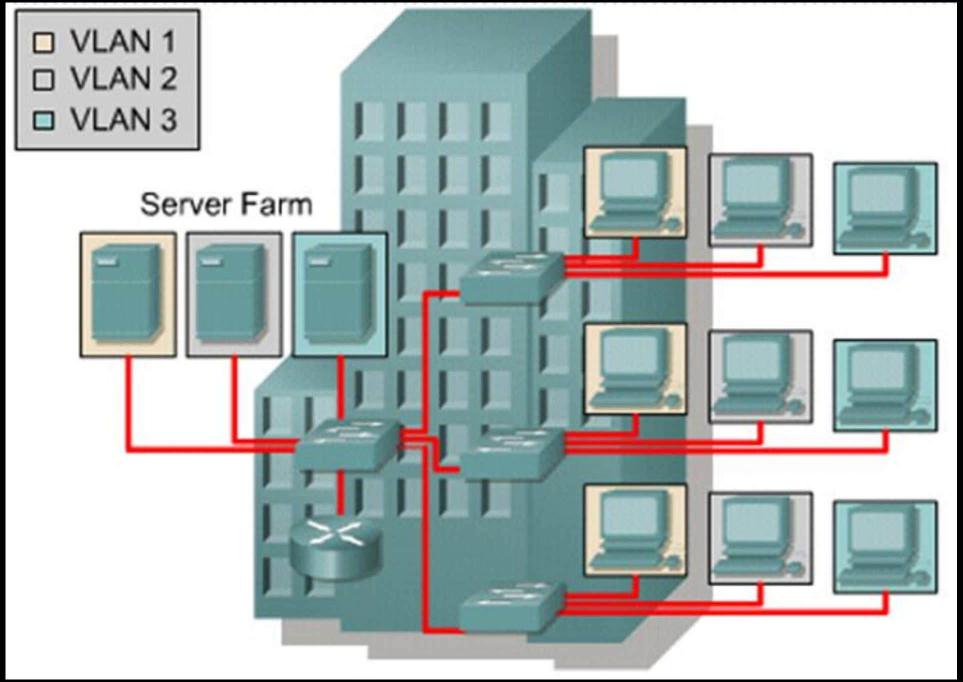
SWITCH

- Layer-2 device of the OSI model
- Modern switches can run up to L3 on OSI stack
- is working based on the CAM table
- Internal zone/DMZ zone
- Increase security through VLANs, L2/L3 ACLs, port security, DHCP Snooping, IP Source Guard, DAI, STP features



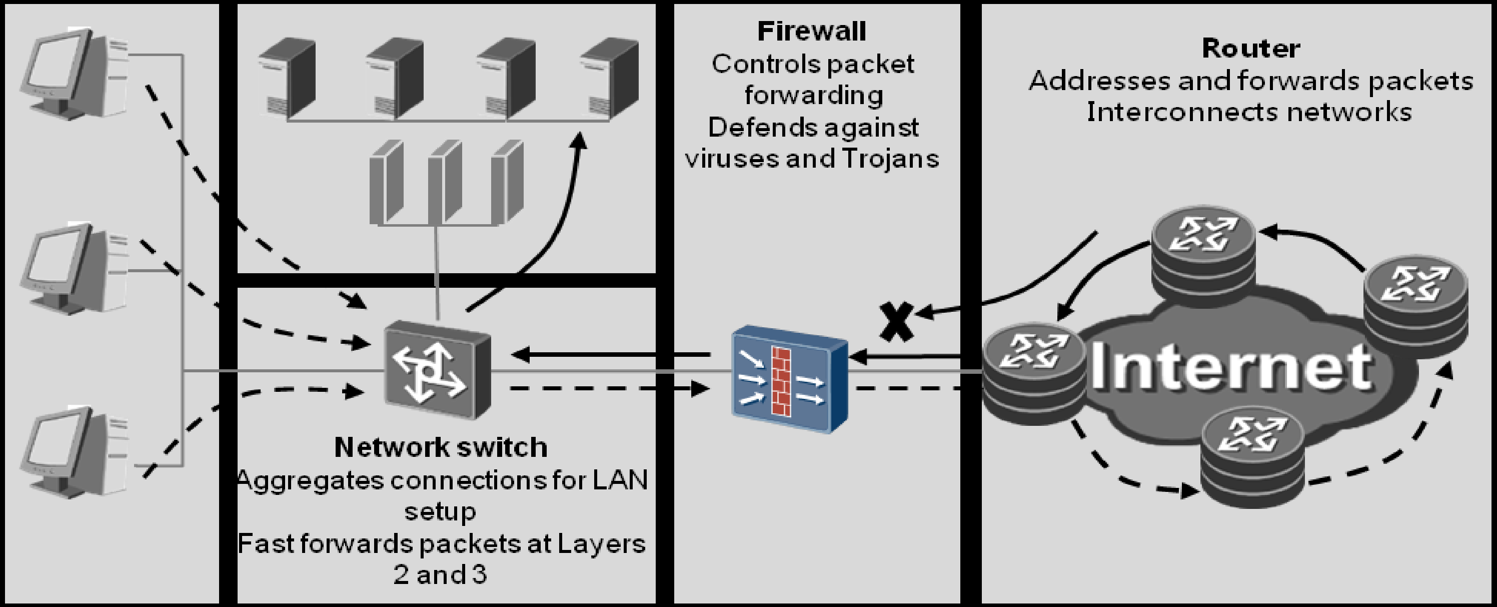
ROUTER

- Layer-3 device of the OSI model
- Forwarding is made based on the IP address
- Internal zone/External zone
- Increase security through ACLs, authentication for routing protocols, VPNs, adjust specific packet rates.



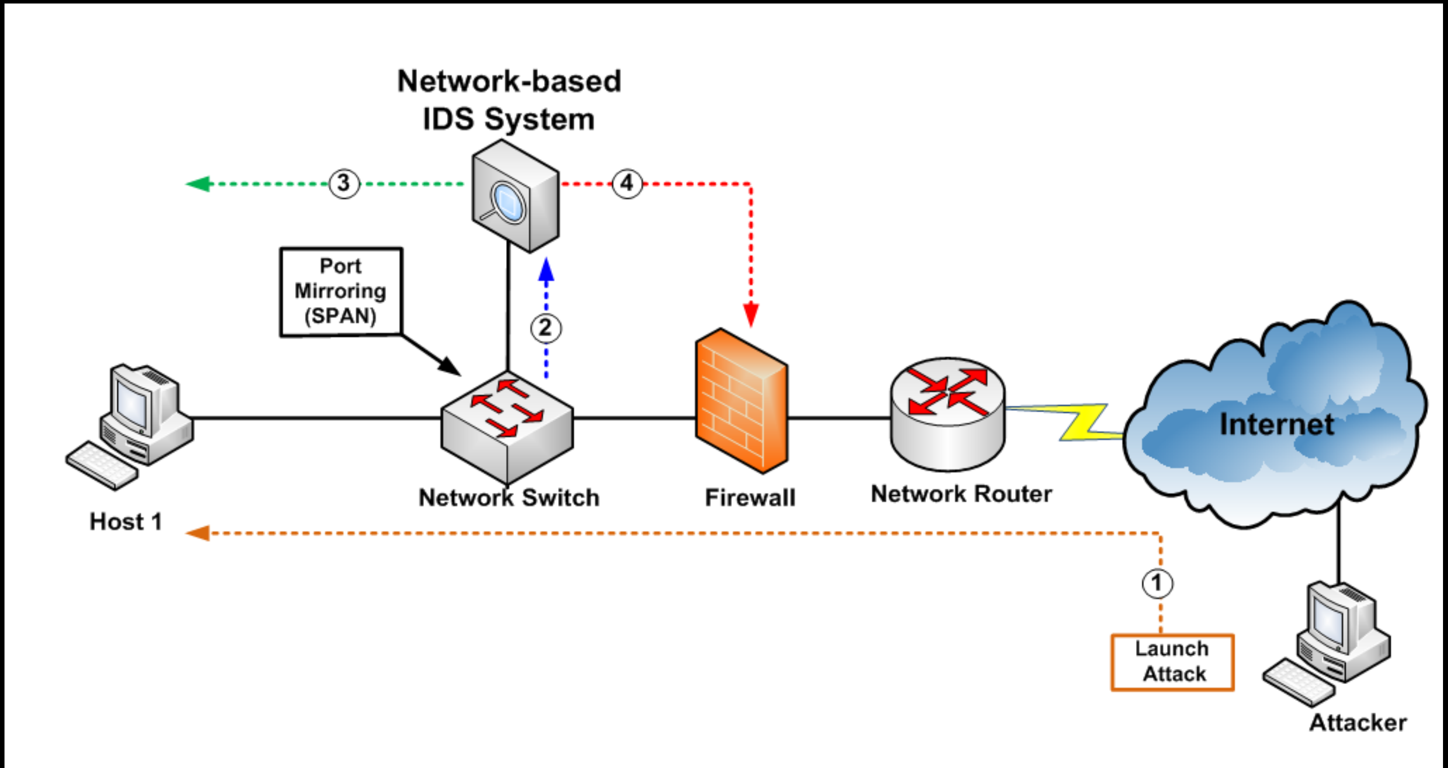
FIREWALL

- Layer-3 device of the OSI model, NGFW can go even higher on stack
- Packet filters act by inspecting packets transferred between computers
- Is working based on zones
- Boarder zone
- Stateful vs stateless
- Software vs hardware
- Whitelist vs blacklist


Firewall
Controls packet forwarding
Defends against viruses and Trojans
Router
Addresses and forwards packets
Interconnects networks
Internet
Network switch
Aggregates connections for LAN setup
Fast forwards packets at Layers 2 and 3

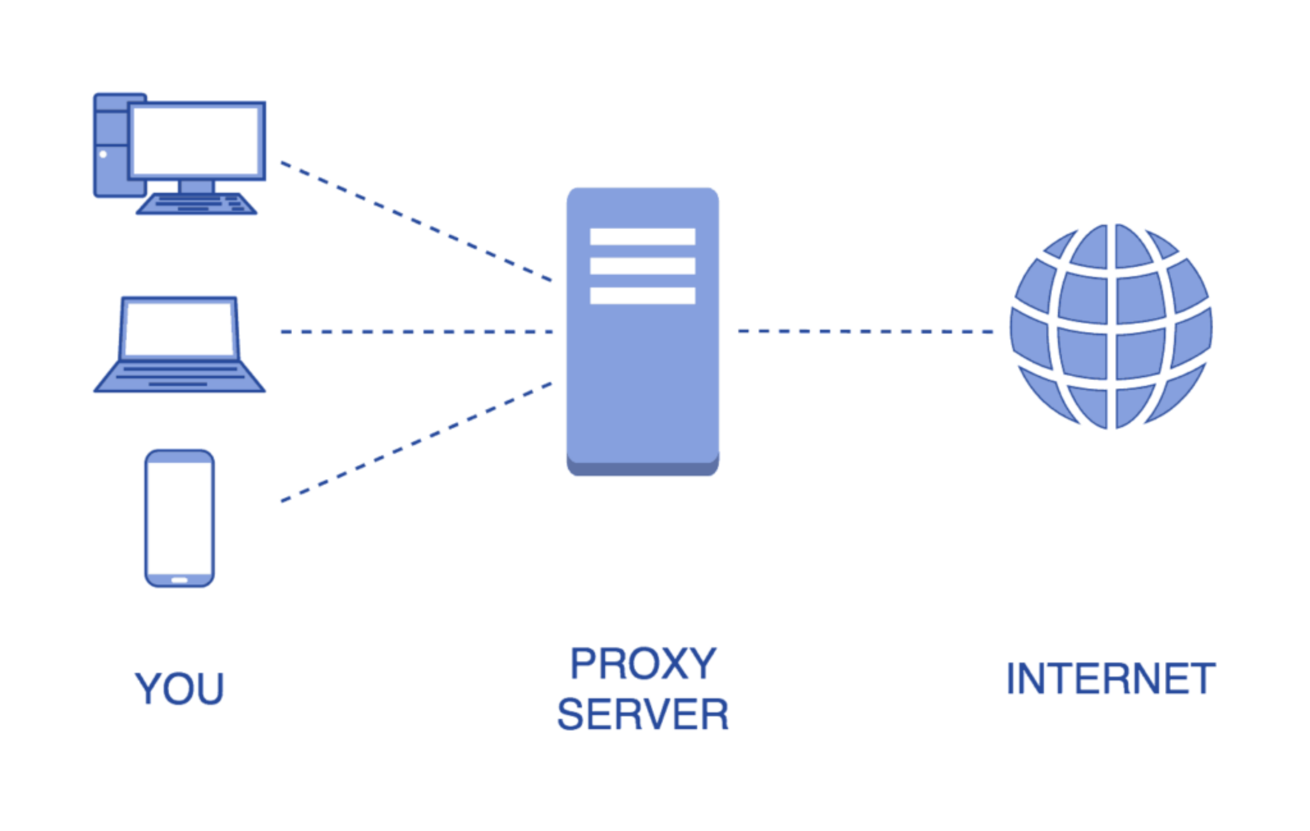
NETWORK-BASED IDS/IPS

- Intrusion Detection System versus Intrusion Prevention System
- Switch spanning port, network tap, inline
- Located in DMZ and internal LAN



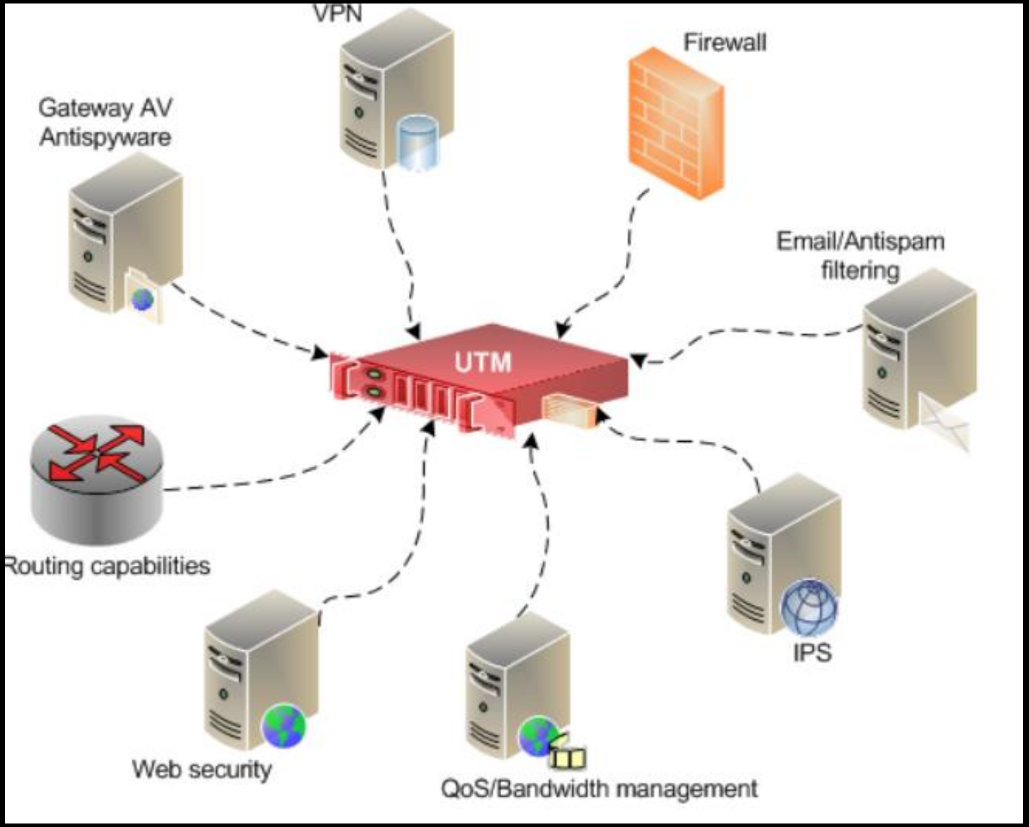
PROXY

- Proxy server acts as a gateway between you and the Internet.
- Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.
- Located in DMZ and Internet



UTM

- Unified Threat Management is a networking device or software program that helps reduce the complexity of securing a network.
- It accomplishes this by including an anti-malware, content filter, firewall, intrusion detection, and spam protection into a single package.
- Can be a network hardware appliance, virtual appliance or cloud service.



NETWORK ACCESS CONTROL (NAC)

- Is an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.

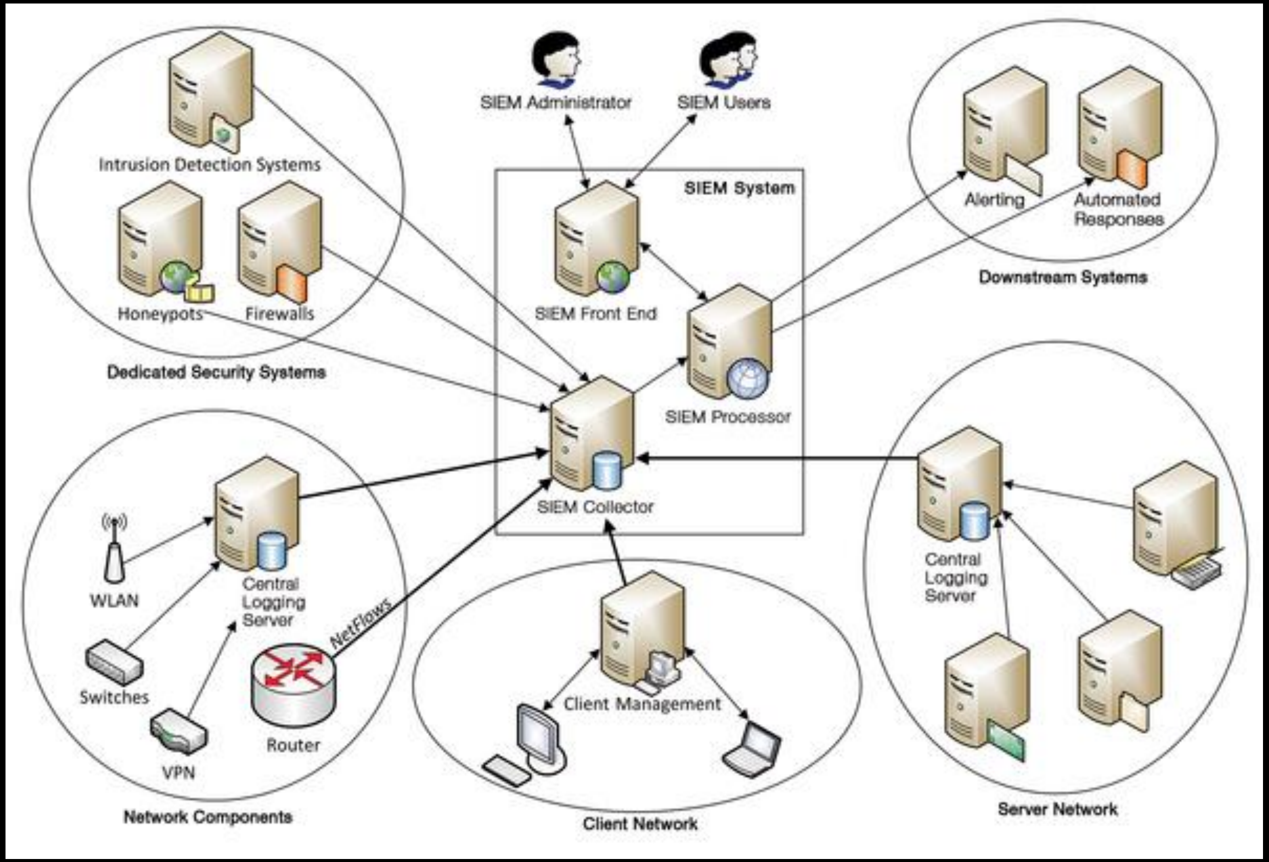
Minimum capabilities of NAC according to Gartner are:

- Dedicated policy management to define and administer security configuration requirements, and specify the access control actions for compliant and noncompliant endpoints
- Ability to conduct a security state baseline for any endpoint attempting to connect and determine the suitable level of access
- Access control so you can block, quarantine or grant varying degrees of access.
- The ability to manage guest access
- A profiling engine to discover, identify and monitor endpoints

SECURITY INFORMATION AND EVENT MANAGEMENT(SIEM)

- SIEM collects security data from network devices, servers, domain controllers, and more.

- SIEM stores, normalizes, aggregates, and applies analytics to that data to discover trends, detect threats, and enable organizations to investigate any alerts.

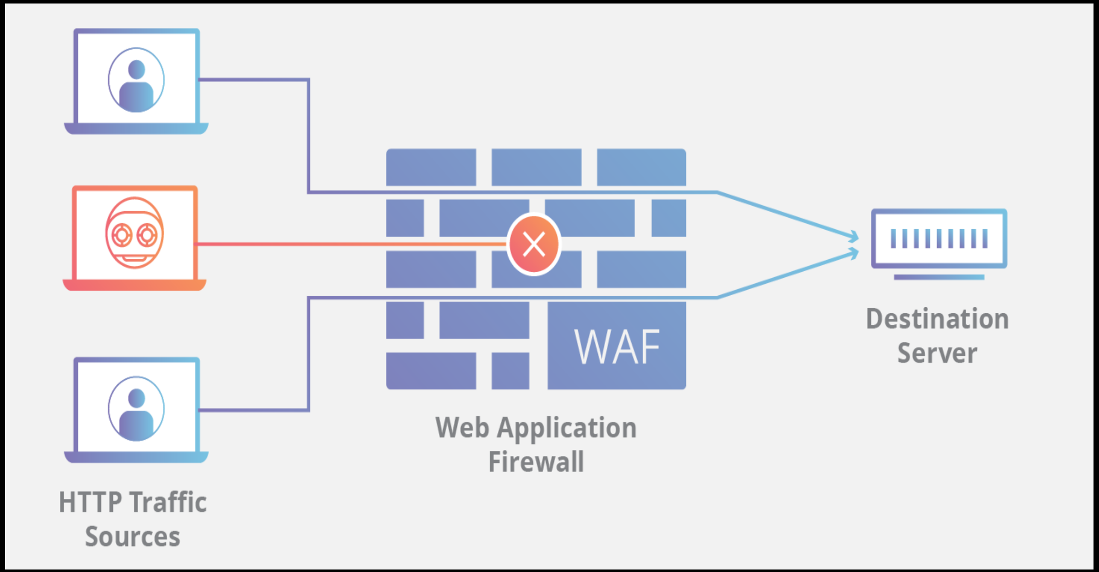


SANDBOX

- A sandbox is a security mechanism for separating running programs, usually to mitigate system failures or software vulnerabilities from spreading.
- It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users or websites, without risking to harm the host machine or operating system.
- Can sit in every security zone depending on the need for deployment.

WEB APPLICATION FIREWALL (WAF)

- A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.
- It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.
- A WAF is a protocol layer 7 defense (in the OSI model) and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors.
- Can be found in the DMZ

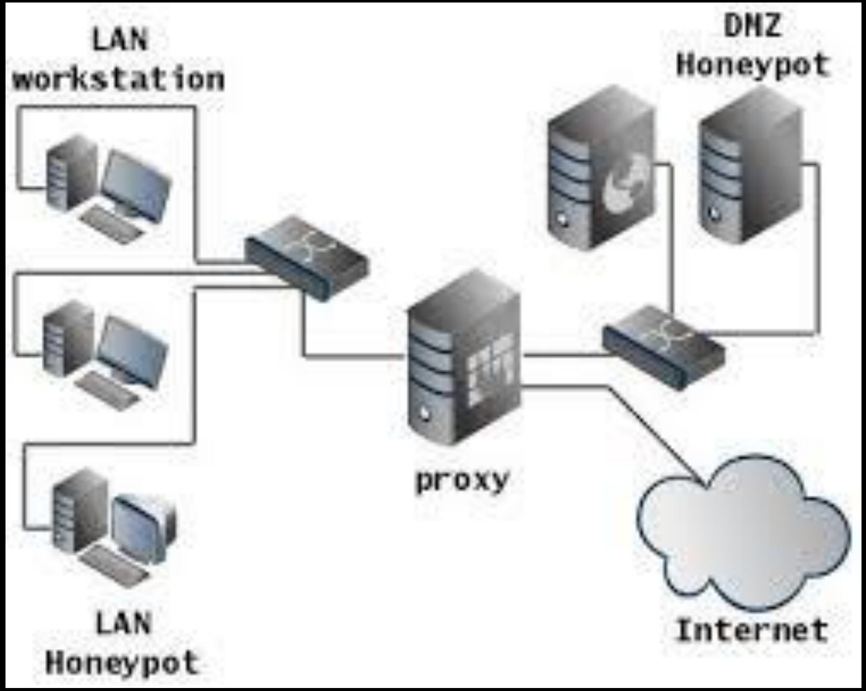


HONEYPOT & HONEYNETS

- A honeypot is a network-attached system set up as a decoy to lure cyberattacks and to detect, deflect or study hacking attempts in order to gain unauthorized access to information systems

- A honeypot is built to trick attackers into breaking into that system instead of elsewhere.

- Virtual machines are often used to host honeypots, so if it is compromised by malware, for example, the honeypot can be quickly restored.
- Two or more honeypots on a network form a honeynet, while a honey farm is a centralized collection of honeypots and analysis tools.



VPN SERVICE

Remote-access VPN

A remote-access VPN connection allows an individual user to connect to a private network from a remote location using a laptop or desktop computer connected to the internet.

A site-to-site VPN

A site-to-site VPN connection lets branch offices use the internet as a conduit for accessing the main office's intranet.

- <u>Intranet-based</u> — If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect each separate LAN to a single WAN.
- <u>Extranet-based</u> — When a company has a close relationship with another company (such as a partner, supplier or customer), it can build an extranet VPN that connects those companies' LANs. This extranet VPN allows the companies to work together in a secure, shared network environment while preventing access to their separate intranets.

ANTIVIRUS SOFTWARE

The primary method of preventing the propagation of malicious code involves the use of antivirus software. **Antivirus software** is an application that is installed on a system to protect it and to scan for viruses as well as worms and Trojan horses. Most viruses have characteristics that are common to families of virus. Antivirus software looks for these characteristics, or fingerprints, to identify and neutralize viruses before they impact you.

AV Types:

- Signature-based detection
- Heuristics
- Behavior-based

HOST-BASED IDS

A host-based IDS is responsible for monitoring activity on the system and alerting you of suspicious activity. The key point to remember about a HIDS is that it monitors activity only on the system the software has been installed on.

The following are some key areas that the HIDS monitors:

- Memory
- System files
- Log files
- File system
- Connections

SECURITY OPERATIONS CENTER (SOC)

An information security operations center (ISOC or SOC) is a facility where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.
A SOC is related to the people, processes and technologies that provide situational awareness through the detection, containment, and remediation of IT threats.

A SOC will handle, on behalf of an institution or company, any threatening IT incident, and will ensure that it is properly identified, analyzed, communicated, investigated and reported.

The SOC also monitors applications to identify a possible cyber-attack or intrusion (event) and determines if it is a genuine malicious threat (incident), and if it could affect business.

NETWORK OPERATIONS CENTER (NOC)

A network operations center (NOC), also known as a "network management center", is one or more locations from which network monitoring and control, or network management, is exercised over a computer, telecommunication or satellite network.

WIRELESS ACCESS POINT (WAP)

In computer networking, a wireless access point (WAP), or more generally just access point (AP), is a networking hardware device that allows other Wi-Fi devices to connect to a wired network.

The AP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself.

An AP is differentiated from a hotspot, which is the physical location where Wi-Fi access to a WLAN is available.

DATA LOSS PREVENTION

Data loss prevention software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in use (endpoint actions), in motion (network traffic), and at rest (data storage).

DEFINING THE SERVICES THAT ARE NEEDED FOR A COMPANY

NETWORK ADDRESS TRANSLATION (NAT)

A NAT (Network Address Translation or Network Address Translator) is the virtualization of Internet Protocol (IP) addresses. NAT helps improve security and decrease the number of IP addresses an organization needs.

DHCP

- It’s a service which is running on a server
- In enterprise architecture you might find multiple DHCP servers.
- Located in DMZ or local zone

DNS

- It’s a service which is running on a server
- In enterprise architecture you might find multiple DNS servers.
- Located in DMZ or local zone

WEB SERVICE

- A Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computer's HTTP clients. Dedicated computers and appliances may be referred to as Web servers as well.
- The process is an example of the client/server model. All computers that host Web sites must have Web server programs. Leading Web servers include Apache, Microsoft's Internet Information Server (IIS) and nginx (pronounced engine X) from NGNIX. Other Web servers include Novell's NetWare server, Google Web Server (GWS) and IBM's family of Domino servers.
- Located in DMZ or local zone

SQL/ DATABASE SERVICE

- A SQL Server is a relational database management system that supports a wide variety of transaction processing, business intelligence and analytics applications in corporate IT environments.
- It can be used to detect attacks or deflect them from a legitimate target.
- It can also be used to gain information about how cybercriminals operate.
- Located in DMZ

EMAIL SERVICE

- It’s a computer attached to a network that provides a location for shared disk access, i.e. shared storage of computer files (such as text, image, sound, video) that can be accessed by the workstations that are able to reach the computer that shares the access through a computer network.
- Located in DMZ or local zone

FILE SHARE/FILE TRANSFER SERVICE

- It’s a computer attached to a network that provides a location for shared disk access, i.e. shared storage of computer files (such as text, image, sound, video) that can be accessed by the workstations that are able to reach the computer that shares the access through a computer network.
- Located in DMZ or local zone

AAA SERVICE

- It’s a computer attached to a network that provides a location for shared disk access, i.e. shared storage of computer files (such as text, image, sound, video) that can be accessed by the workstations that are able to reach the computer that shares the access through a computer network.
- Located in DMZ or local zone

VOIP SERVER

- Voice over IP (VoIP) technology makes it possible to encode voice into data packets which are then broken down into smaller units and transmitted electronically
- A VoIP server can either be a software or hardware.
- The workings of VoIP Servers are similar to a proxy server. The Server receives the requests from users and through various processes assists in the establishment of the IP phone system.
- Features like video conferencing, IVR (Interactive Voice Response)
- SIP (Session Initiation Protocol)

SNMP SERVICE

- Simple Network Management Protocol (SNMP) is one of the most widely accepted protocols for network monitoring
- SNMP talks to your network to find out information related to this network device activity
- The process is an example of the client/server model, more like an agent
- Is working based on MIBs and traps

NTP SERVER

- Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
- NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).
- NTP can usually maintain time to within tens of milliseconds over the public Internet and can achieve better than one millisecond accuracy in local area networks under ideal conditions.

BYOD NETWORK

- AAA
- Guest network/VLAN
- 802.1X
- Proxy traffic
- Captive portal

SEGMENTATION

- Device or system level access controls are a good way to block data compromise. However, it’s better to prevent attacks from getting to critical components in the first place.
- Network segmentation allows placement of critical systems into isolated network segments.
- Access controls determine whether specific network traffic is allowed on the segment or blocked

ACCESS CONTROLS

Types of access controls:

- administrative
- technical
- physical

Administrative controls consist of policies, standards, and guidelines which govern user behavior.

Technical access controls consist of user accounts, tokens, access control lists, or other mechanisms used to prevent or allow system, application, or user access to information resources.

Physical access controls prevent intruders from unauthorized access, as defined by policies, standards, and guidelines, which require actual physical contact with a system, including theft or destruction of one or more components of a system, laptop, aso

SERVER HARDENING

- USER ACCOUNTS AND PASSWORD
- OPERATING SYSTEM CONFIGURATION
- FILESYSTEM PERMISSIONS
- CLIENT/SERVER NETWORK SECURITY
- SOFTWARE AND APPLICATIONS IMAGE/ PATCHING AND UPDATES
- AUDITING AND CHANGE CONTROL

ENDPOINT HARDENING

- Patching/Updates
- Reduce attack surface
- HIDS/HIPS
- Enable logging/remote logging
- AV

Device hardening is the most basic controls used to protect data and systems. It consists of the timely application of patches and the careful configuration of system components, removing the most fundamental security vulnerabilities.

Supported by a well-designed and actively managed patch management process, proper device configuration is the most effective method of repelling exploits.

POLICIES, STANDARDS AND GUIDELINES

- Access policies
- AD policies(Local GP and Domain GP)
- Password management

Policies are business statements of intent, setting the direction for secure information processing and storage. Expanded into standards and guidelines, they build a framework around which a security strategy is built.

VULNERABLY MANAGEMENT

- Determine the attack surface

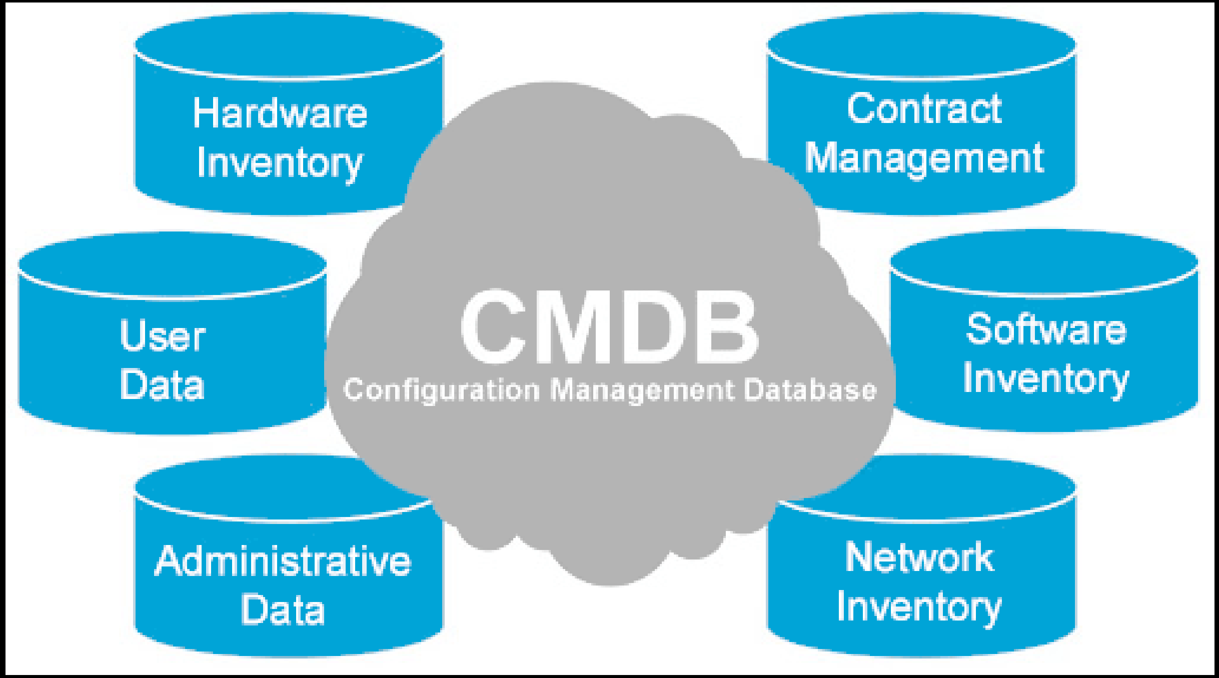
- Impact and Criticality of the vulnerabilities

- **CVE (Common Vulnerabilities and Exposures)** is a list of entries each containing an identification number, a description, and at least one public reference for publicly known cybersecurity vulnerabilities.

- **CVSS** (Common Vulnerability Scoring System) is an open framework for communicating the characteristics and severity of software vulnerabilities.

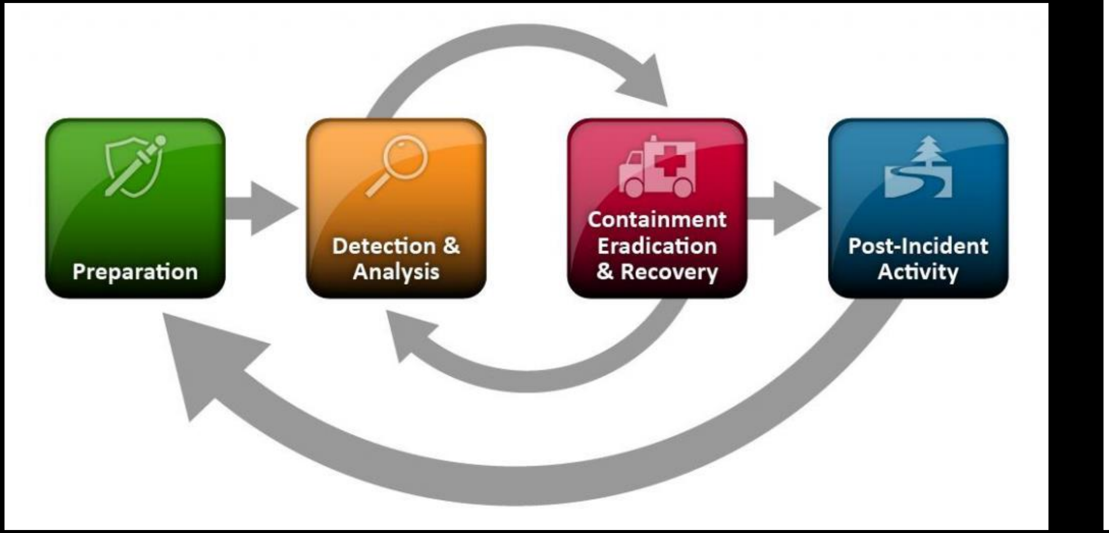
ASSETS AND USERS MANAGEMENT

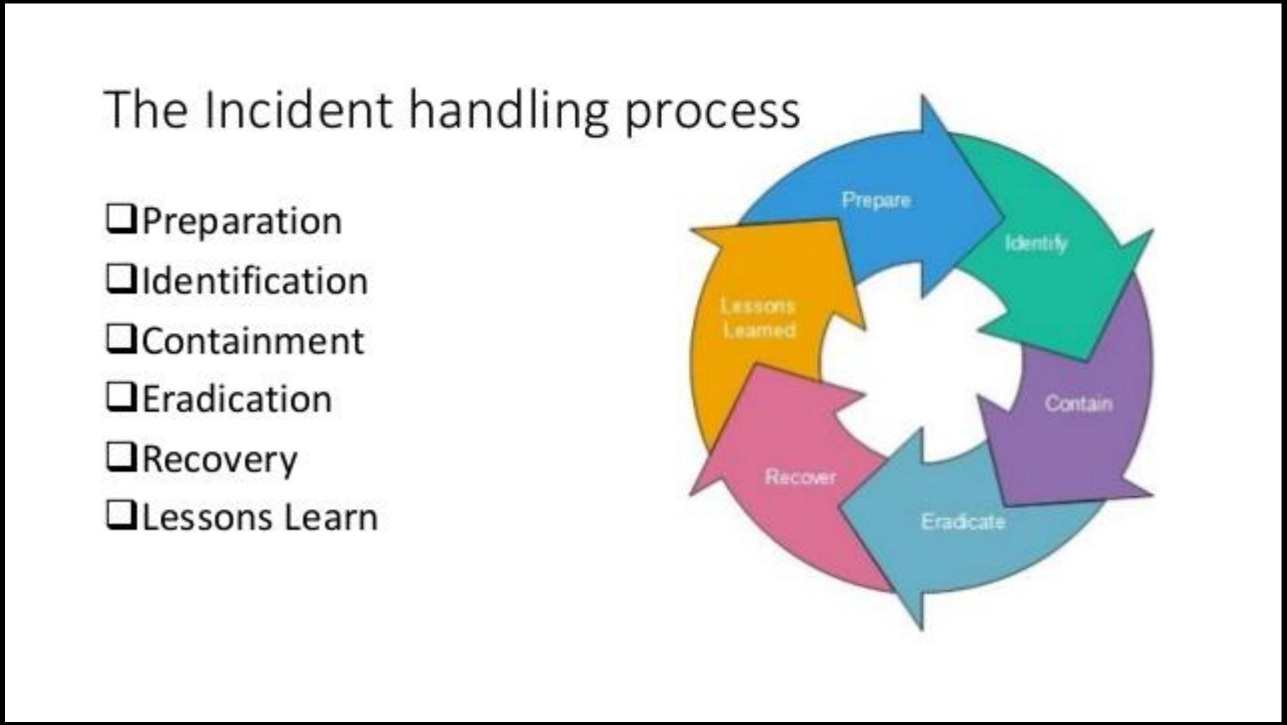
- SCCM (CMDB)
- Active Directory Service



INCIDENT HANDLING

- SOC (ITIL compliant)
- NOC (ITIL compliant)
- NIST
- PICERL

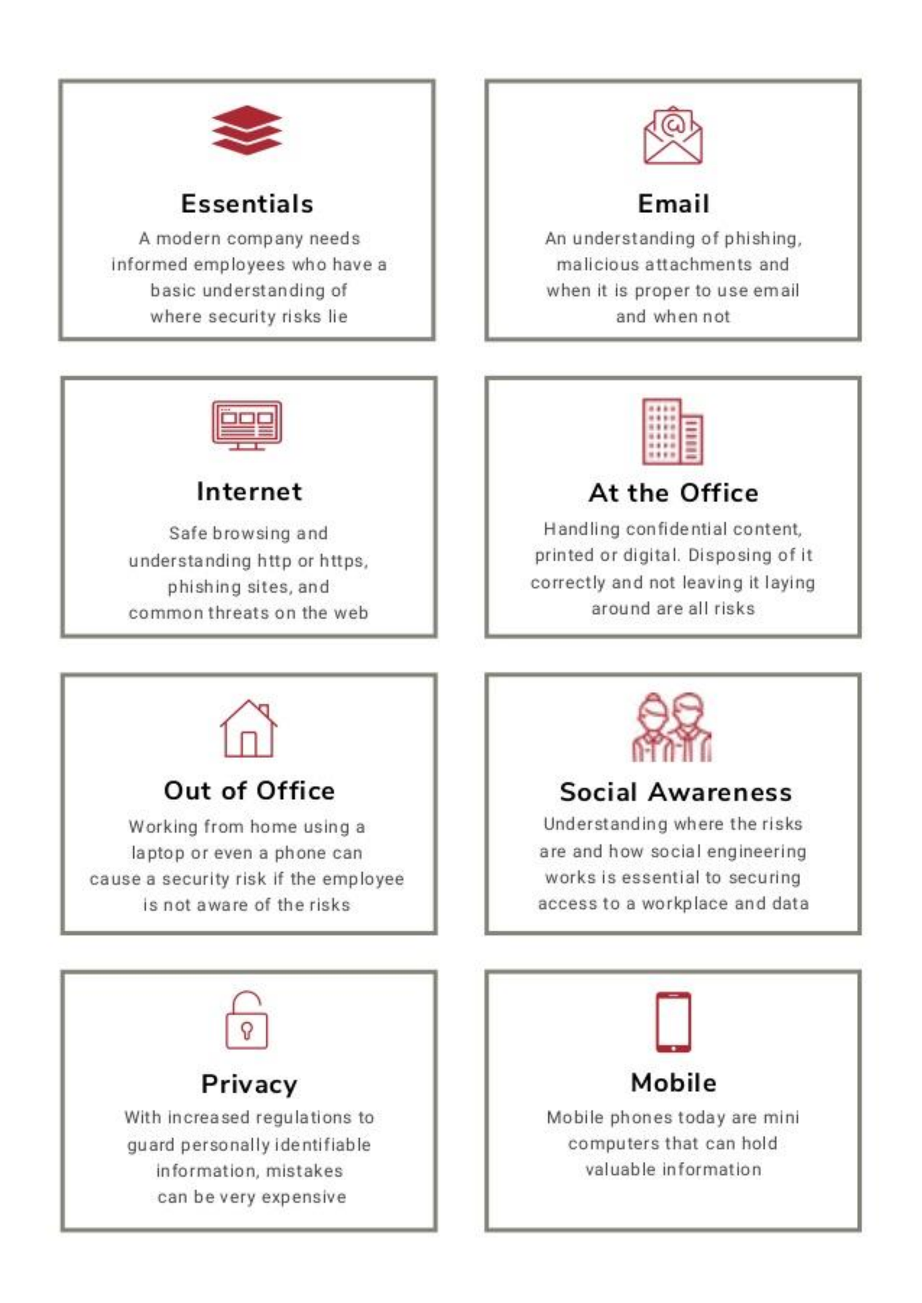



The Incident handling process

- ❑Preparation
- ❑Identification
- ❑Containment
- ❑Eradication
- ❑Recovery
- ❑Lessons Learn

USER SECURITY AWARENESS

Well written policies and supporting processes have little value without user awareness and participation. Employees at all levels must understand what is and is not acceptable behavior.



Essentials

A modern company needs informed employees who have a basic understanding of where security risks lie

Email

An understanding of phishing, malicious attachments and when it is proper to use email and when not

Internet

Safe browsing and understanding http or https, phishing sites, and common threats on the web

At the Office

Handling confidential content, printed or digital. Disposing of it correctly and not leaving it laying around are all risks

Out of Office

Working from home using a laptop or even a phone can cause a security risk if the employee is not aware of the risks

Social Awareness

Understanding where the risks are and how social engineering works is essential to securing access to a workplace and data

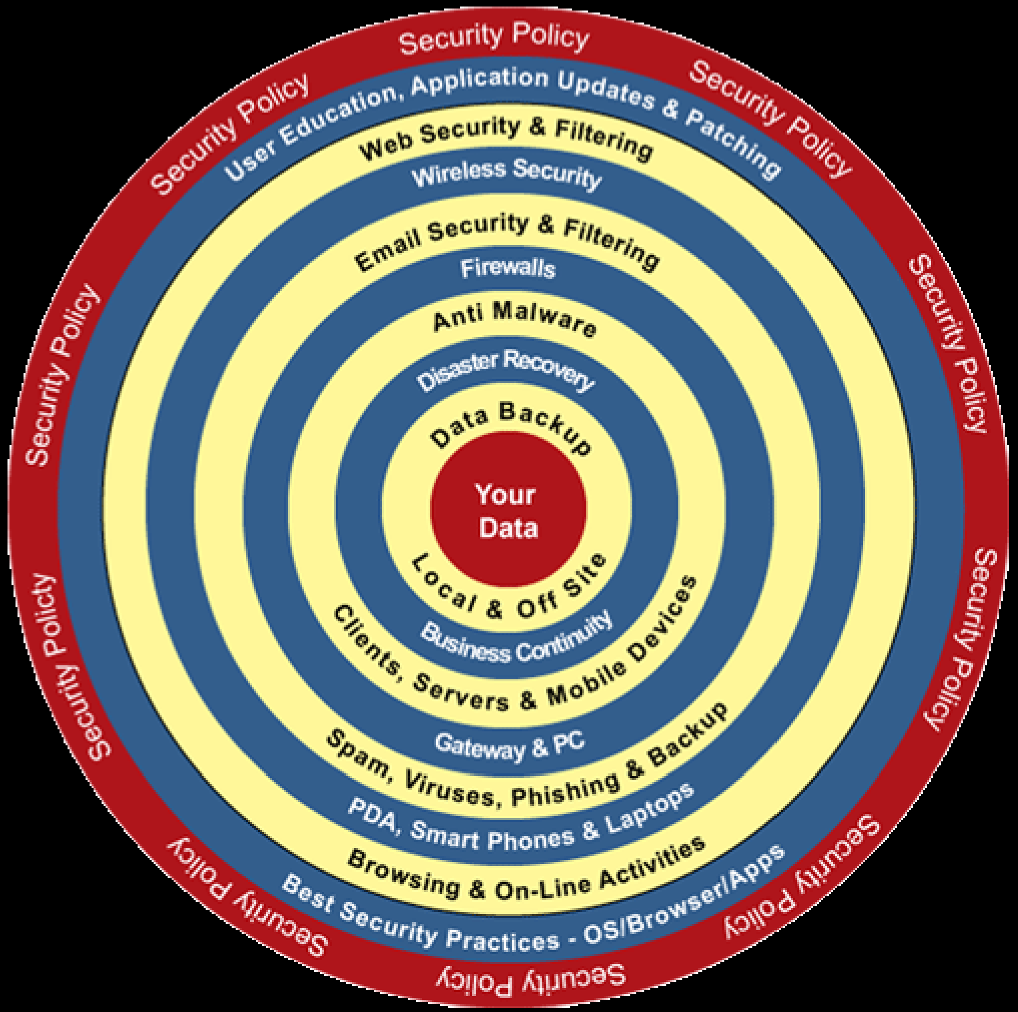
Privacy

With increased regulations to guard personally identifiable information, mistakes can be very expensive

Mobile

Mobile phones today are mini computers that can hold valuable information

DEFENSE IN DEPTH



Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack