Cybersecurity Fundamentals

Module 4: Security Principles

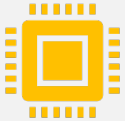
What is Networking?

A network is simply two or more computers linked together to share data, information or resources.

Types of Networks

LAN

WAN



Network Devices : Hub, Switch, Router, Firewall, Server, Endpoint

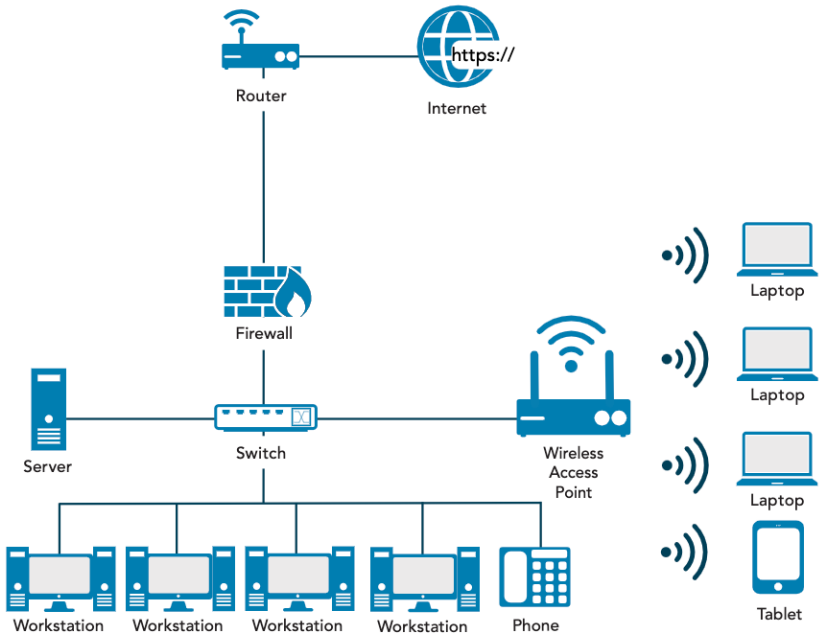
Other Networking Term :

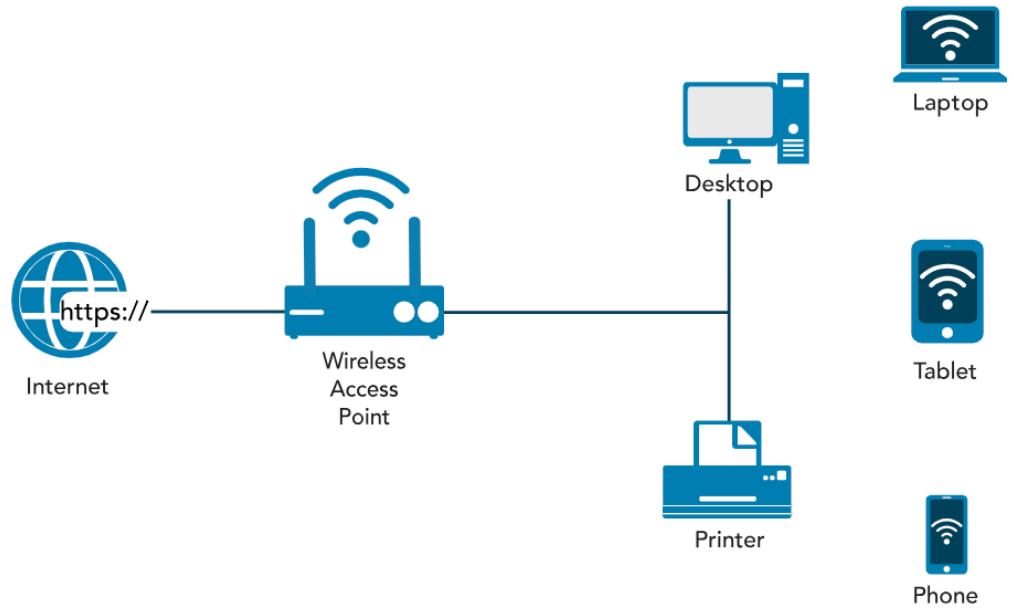
Ethernet

Device Address

- MAC Address
- IP Address

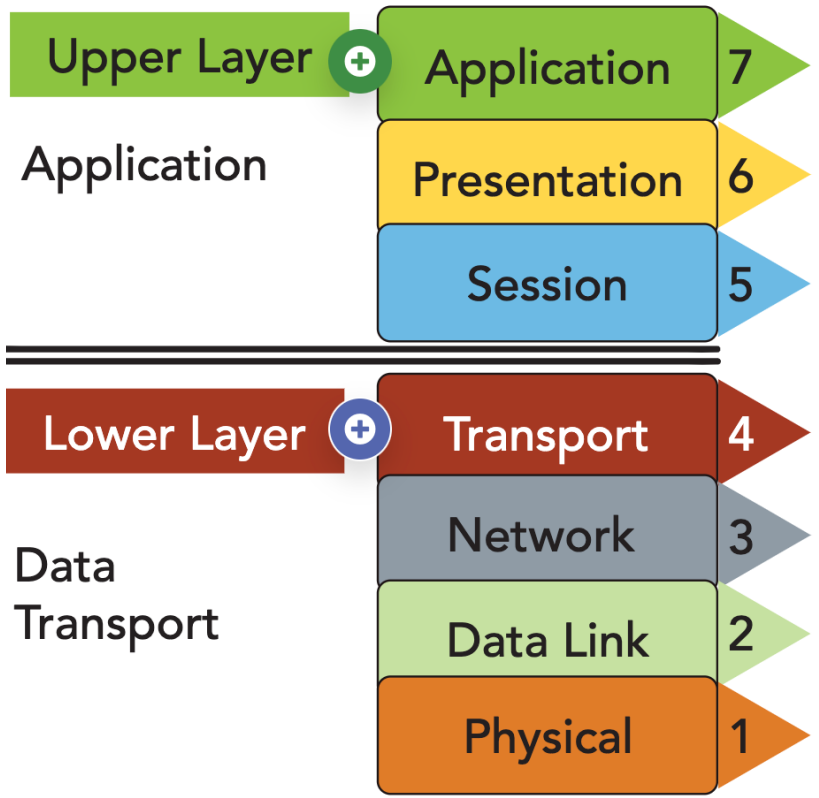
Networking at a Glance





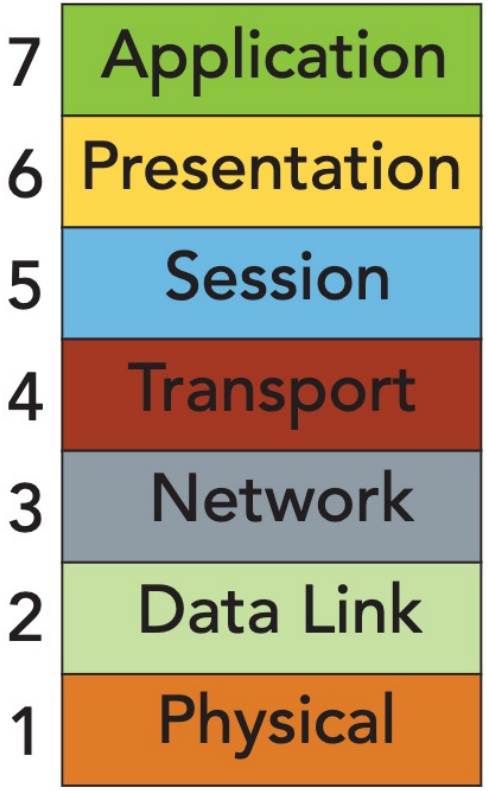
Networking Model

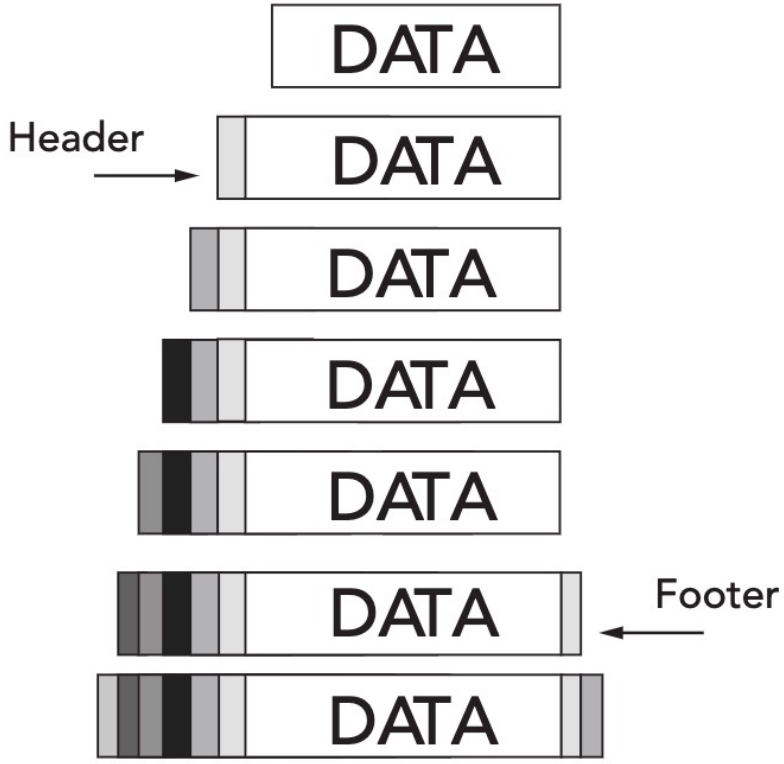
- The purpose of all communications is to exchange information and ideas between people and organizations so that they can get work done.
- Those simple goals can be re-expressed in network (and security) terms such as:
  - Provide reliable, managed communications between hosts (and users)
  - Isolate functions in layers
  - Use packets as the basis of communication
  - Standardize routing, addressing and control
  - Allow layers beyond internetworking to add functionality
  - Be vendor-agnostic, scalable and resilient



Open System Interconnection (OSI) Model

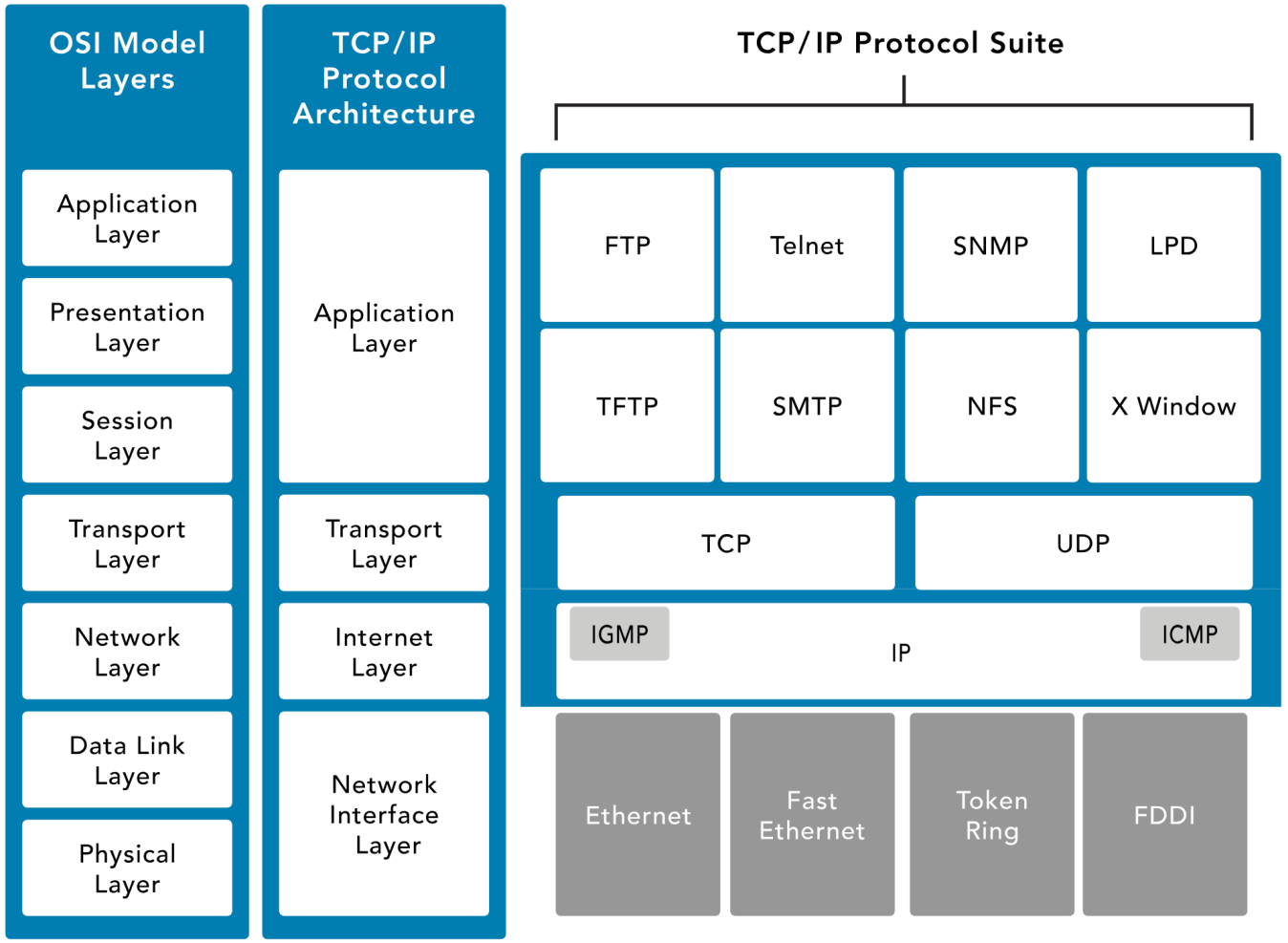
- Encapsulation : addition of header and possibly a footer (trailer) data by a protocol used at that layer of the OSI model.
- De-encapsulation



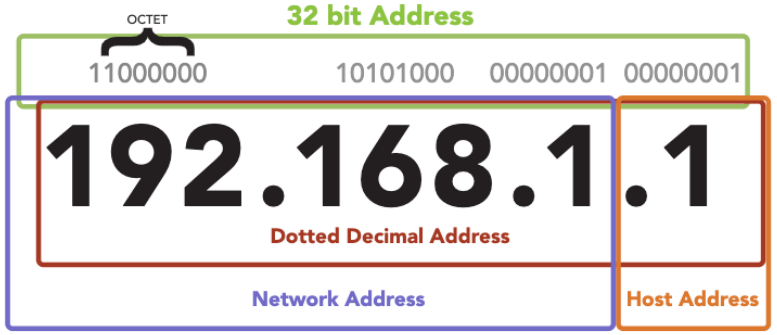


Transmission Control Protocol (TCP)/Internet Protocol (IP)

TCP/IP Protocol Architecture Layers	
Application Layer	Defines the protocols for the transport layer.
Transport Layer	Permits data to move among devices.
Internet Layer	Creates/inserts packets.
Network Interface Layer	How data moves through the network.



Internet Protocol (IPv4 & IPv6)



- IPv6 is a modernization of IPv4, which addressed a number of weaknesses in the IPv4 environment:
- A much larger address field: IPv6 addresses are 128 bits, which supports 2^{128} or 340,282,366,920,938,463,463,374,607,431,768,211,456 hosts. This ensures that we will not run out of addresses.
- Improved security: IPsec is an optional part of IPv4 networks, but a mandatory component of IPv6 networks. This will help ensure the integrity and confidentiality of IP packets and allow communicating partners to authenticate with each other.
- Improved quality of service (QoS): This will help services obtain an appropriate share of a network's bandwidth.

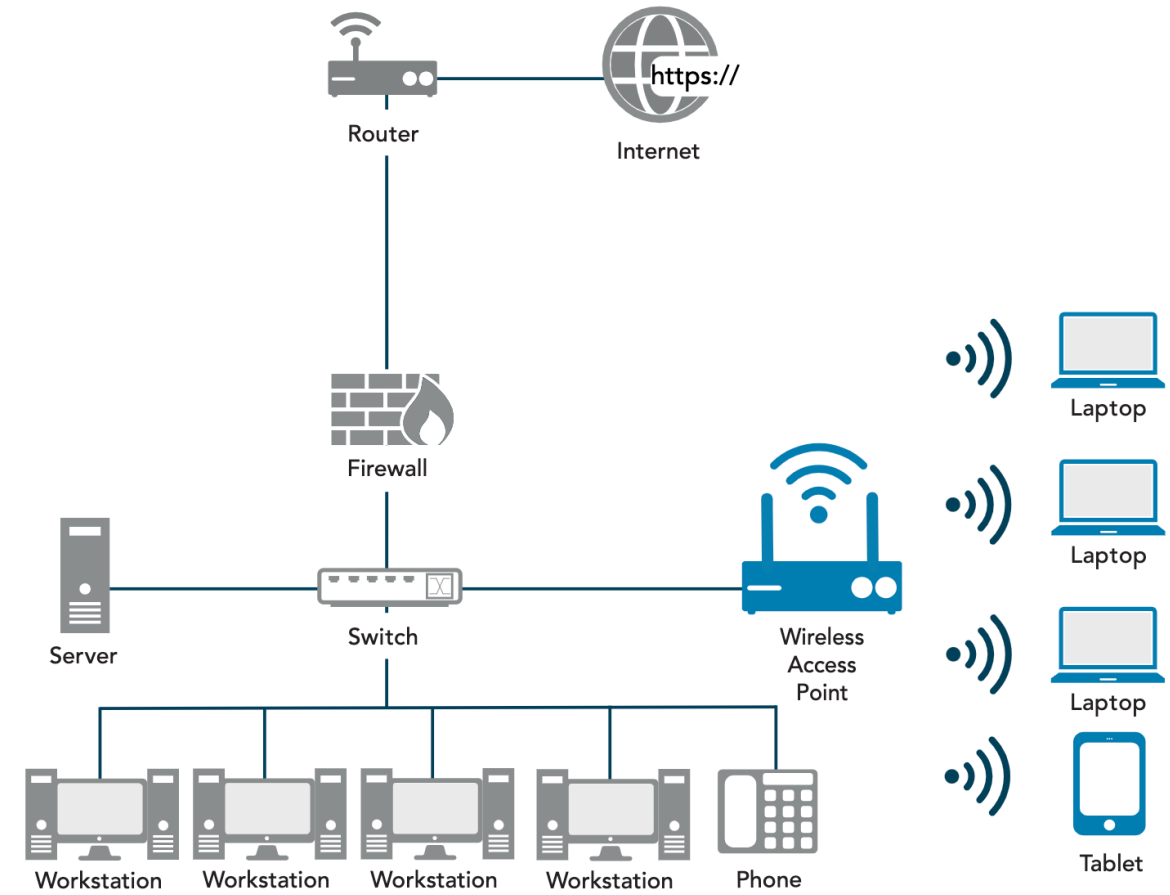
Range
10.0.0.0 to 10.255.255.254
172.16.0.0 to 172.31.255.254
192.168.0.0 to 192.168.255.254

Knowledge Check
: Formatting IPv6

Which of the following examples is a correctly shortened version of the address 2001:0db8:0000:0000:0000:ffff:0000:0001?

- A. 2001:db8::ffff:0000:1
- B. 2001:0db8:0:ffff::1
- C. 2001:0db8::ffff:0:0001
- D. 2001:db8::ffff:0:1

What is Wifi?


Router
https://
Internet
Firewall
Server
Switch
Wireless Access Point
Laptop
Laptop
Laptop
Tablet
Workstation
Workstation
Workstation
Workstation
Phone

Security of the Network

- TCP/IP's vulnerabilities are numerous. Improperly implemented TCP/IP stacks in various operating systems are vulnerable to various DoS/DDoS attacks, fragment attacks, oversized packet attacks, spoofing attacks, and man-in-the-middle attacks.
- TCP/IP (as well as most protocols) is also subject to passive attacks via monitoring or sniffing. Network monitoring, or sniffing, is the act of monitoring traffic patterns to obtain information about a network.

Ports and Protocols (Applications/Services)

- Physical Ports : Physical ports are the ports on the routers, switches, servers, computers, etc. that you connect the wires, e.g., fiber optic cables, Cat5 cables, etc., to create a network.
- Logical Ports : Ports allow a single IP address to be able to support multiple simultaneous communications, each using a different port number
    - Well-known ports (0–1023): These ports are related to the common protocols that are at the core of the Transport Control Protocol/Internet Protocol (TCP/IP) model, Domain Name Service (DNS), Simple Mail Transfer Protocol (SMTP), etc.
    - Registered ports (1024–49151): These ports are often associated with proprietary applications from vendors and developers. While they are officially approved by the Internet Assigned Numbers Authority (IANA), in practice many vendors simply implement a port of their choosing. Examples include Remote Authentication Dial-In User Service (RADIUS) authentication (1812), Microsoft SQL Server (1433/1434) and the Docker REST API (2375/2376).
    - Dynamic or private ports (49152–65535): Whenever a service is requested that is associated with well-known or registered ports, those services will respond with a dynamic port that is used for that session and then released.

Secure Ports - FTP

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
21 - FTP	Port 21, File Transfer Protocol (FTP) sends the username and password using plaintext from the client to the server. This could be intercepted by an attacker and later used to retrieve confidential information from the server. The secure alternative, SFTP, on port 22 uses encryption to protect the user credentials and packets of data being transferred.	File Transfer Protocol	22* - SFTP	Secure File Transfer Protocol

Secure Ports - Telnet

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
23 - Telnet	Port 23, telnet, is used by many Linux systems and any other systems as a basic text-based terminal. All information to and from the host on a telnet connection is sent in plaintext and can be intercepted by an attacker. This includes username and password as well as all information that is being presented on the screen, since this interface is all text. Secure Shell (SSH) on port 22 uses encryption to ensure that traffic between the host and terminal is not sent in a plaintext format.	Telnet	22* - SSH	Secure Shell

Secure Ports - SMTP

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
25 - SMTP	Port 25, Simple Mail Transfer Protocol (SMTP) is the default unencrypted port for sending email messages. Since it is unencrypted, data contained within the emails could be discovered by network sniffing. The secure alternative is to use port 587 for SMTP using Transport Layer Security (TLS) which will encrypt the data between the mail client and the mail server.	Simple Mail Transfer Protocol	587 - SMTP	SMTP with TLS

Secure Ports - Time

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
37 - Time	Port 37, Time Protocol, may be in use by legacy equipment and has mostly been replaced by using port 123 for Network Time Protocol (NTP). NTP on port 123 offers better error-handling capabilities, which reduces the likelihood of unexpected errors.	Time Protocol	123 - NTP	Network Time Protocol

Secure Ports - DNS

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
53 - DNS	Port 53, Domain Name Service (DNS), is still used widely. However, using DNS over TLS (DoT) on port 853 protects DNS information from being modified in transit.	Domain Name Service	853 - DoT	DNS over TLS (DoT)

Secure Ports - HTTP

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
80 - HTTP	Port 80, HyperText Transfer Protocol (HTTP) is the basis of nearly all web browser traffic on the internet. Information sent via HTTP is not encrypted and is susceptible to sniffing attacks. HTTPS using TLS encryption is preferred, as it protects the data in transit between the server and the browser. Note that this is often notated as SSL/TLS. Secure Sockets Layer (SSL) has been compromised is no longer considered secure. It is now recommended for web servers and clients to use Transport Layer Security (TLS) 1.3 or higher for the best protection.	HyperText Transfer Protocol	443 - HTTPS	HyperText Transfer Protocol (SSL/TLS)

Secure Ports - IMAP

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
143 - IMAP	Port 143, Internet Message Access Protocol (IMAP) is a protocol used for retrieving emails. IMAP traffic on port 143 is not encrypted and susceptible to network sniffing. The secure alternative is to use port 993 for IMAP, which adds SSL/TLS security to encrypt the data between the mail client and the mail server.	Internet Message Access Protocol	993 - IMAP	IMAP for SSL/TLS

Secure Ports - SNMP

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
161/162 - SNMP	Ports 161 and 162, Simple Network Management Protocol, are commonly used to send and receive data used for managing infrastructure devices. Because sensitive information is often included in these messages, it is recommended to use SNMP version 2 or 3 (abbreviated SNMPv2 or SNMPv3) to include encryption and additional security features. Unlike many others discussed here, all versions of SNMP use the same ports, so there is not a definitive secure and insecure pairing. Additional context will be needed to determine if information on ports 161 and 162 is secured or not.	Simple Network Management Protocol	161/162 - SNMP	SNMPv3

Secure Ports - SMB

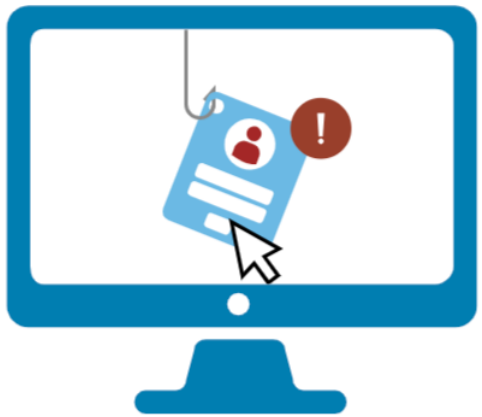
Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
445 - SMB	Port 445, Server Message Block (SMB), is used by many versions of Windows for accessing files over the network. Files are transmitted unencrypted, and many vulnerabilities are well-known. Therefore, it is recommended that traffic on port 445 should not be allowed to pass through a firewall at the network perimeter. A more secure alternative is port 2049, Network File System (NFS). Although NFS can use encryption, it is recommended that NFS not be allowed through firewalls either.	Server Message Block	2049 - NFS	Network File System

Secure Ports - LDAP

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
389 - LDAP	Port 389, Lightweight Directory Access Protocol (LDAP), is used to communicate directory information from servers to clients. This can be an address book for email or usernames for logins. The LDAP protocol also allows records in the directory to be updated, introducing additional risk. Since LDAP is not encrypted, it is susceptible to sniffing and manipulation attacks. Lightweight Directory Access Protocol Secure (LDAPS) adds SSL/TLS security to protect the information while it is in transit.	Lightweight Directory Access Protocol	636 - LDAPS	Lightweight Directory Access Protocol Secure

Type of Threats - Spoofing

An attack with the goal of gaining access to a target system through the use of a falsified identity. Spoofing can be used against IP addresses, MAC address, usernames, system names, wireless network SSIDs, email addresses, and many other types of logical identification.



Type of Threats - Phishing

An attack that attempts to misdirect legitimate users to malicious websites through the abuse of URLs or hyperlinks in emails could be considered phishing.

Type of Threats – DOS/DDOS

A denial-of-service (DoS) attack is a network resource consumption attack that has the primary goal of preventing legitimate activity on a victimized system. Attacks involving numerous unsuspecting secondary victim systems are known as distributed denial-of-service (DDoS) attacks.

Type of Threats - Virus

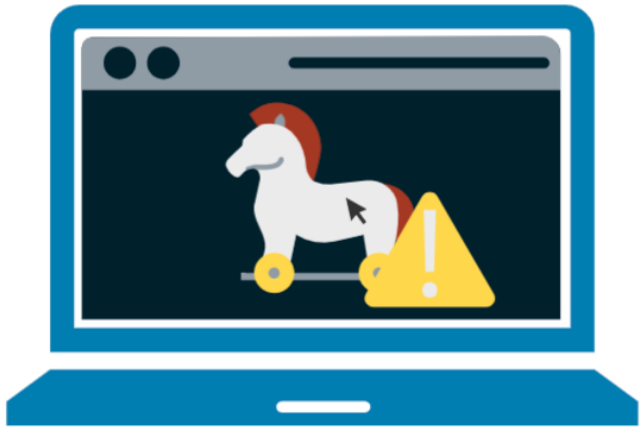
The computer virus is perhaps the earliest form of malicious code to plague security administrators. As with biological viruses, computer viruses have two main functions—propagation and destruction. A virus is a self-replicating piece of code that spreads without the consent of a user, but frequently with their assistance (a user has to click on a link or open a file).

Type of Threats - Worm

Worms pose a significant risk to network security. They contain the same destructive potential as other malicious code objects with an added twist—they propagate themselves without requiring any human intervention.

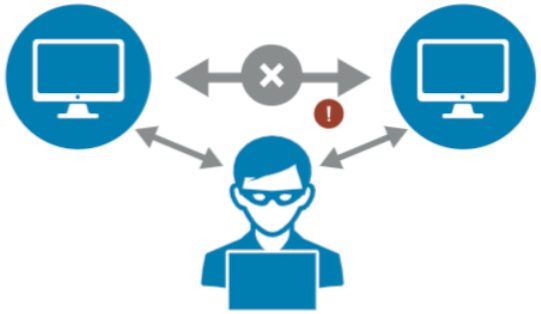
Type of Threats - Trojan

Named after the ancient story of the Trojan horse, the Trojan is a software program that appears benevolent but carries a malicious, behind-the-scenes payload that has the potential to wreak havoc on a system or network. For example, ransomware often uses a Trojan to infect a target machine and then uses encryption technology to encrypt documents, spreadsheets and other files stored on the system with a key known only to the malware creator.



Type of Threats – On-path Attack

In an on-path attack, attackers place themselves between two devices, often between a web browser and a web server, to intercept or modify information that is intended for one or both of the endpoints. On-path attacks are also known as man-in-the-middle (MITM) attacks.



Type of Threats – Side Channel

A side-channel attack is a passive, noninvasive attack to observe the operation of a device. Methods include power monitoring, timing and fault analysis attacks.

Type of Threats – Advanced Persistent Threat (APT)

Advanced persistent threat (APT) refers to threats that demonstrate an unusually high level of technical and operational sophistication spanning months or even years. APT attacks are often conducted by highly organized groups of attackers.

Type of Threats – Insider Threat

Insider threats are threats that arise from individuals who are trusted by the organization. These could be disgruntled employees or employees involved in espionage. Insider threats are not always willing participants. A trusted user who falls victim to a scam could be an unwilling insider threat.

Type of Threats - Malware

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications or operating system or otherwise annoying or disrupting the victim.

Type of Threats - Ransomware

Malware used for the purpose of facilitating a ransom attack. Ransomware attacks often use cryptography to “lock” the files on an affected computer and require the payment of a ransom fee in return for the “unlock” code.

Knowledge Check – Identify Malware Threats

Which threats are directly associated with malware? Select all that apply.

- [ ] APT
- [ ] Ransomware
- [ ] Trojan
- [ ] DDoS
- [ ] Phishing
- [ ] Virus

Identify Threats and Tools Used to Prevent Them

If a system doesn’t need a service or protocol, it should not be running. Attackers cannot exploit a vulnerability in a service or protocol that isn’t running on a system.

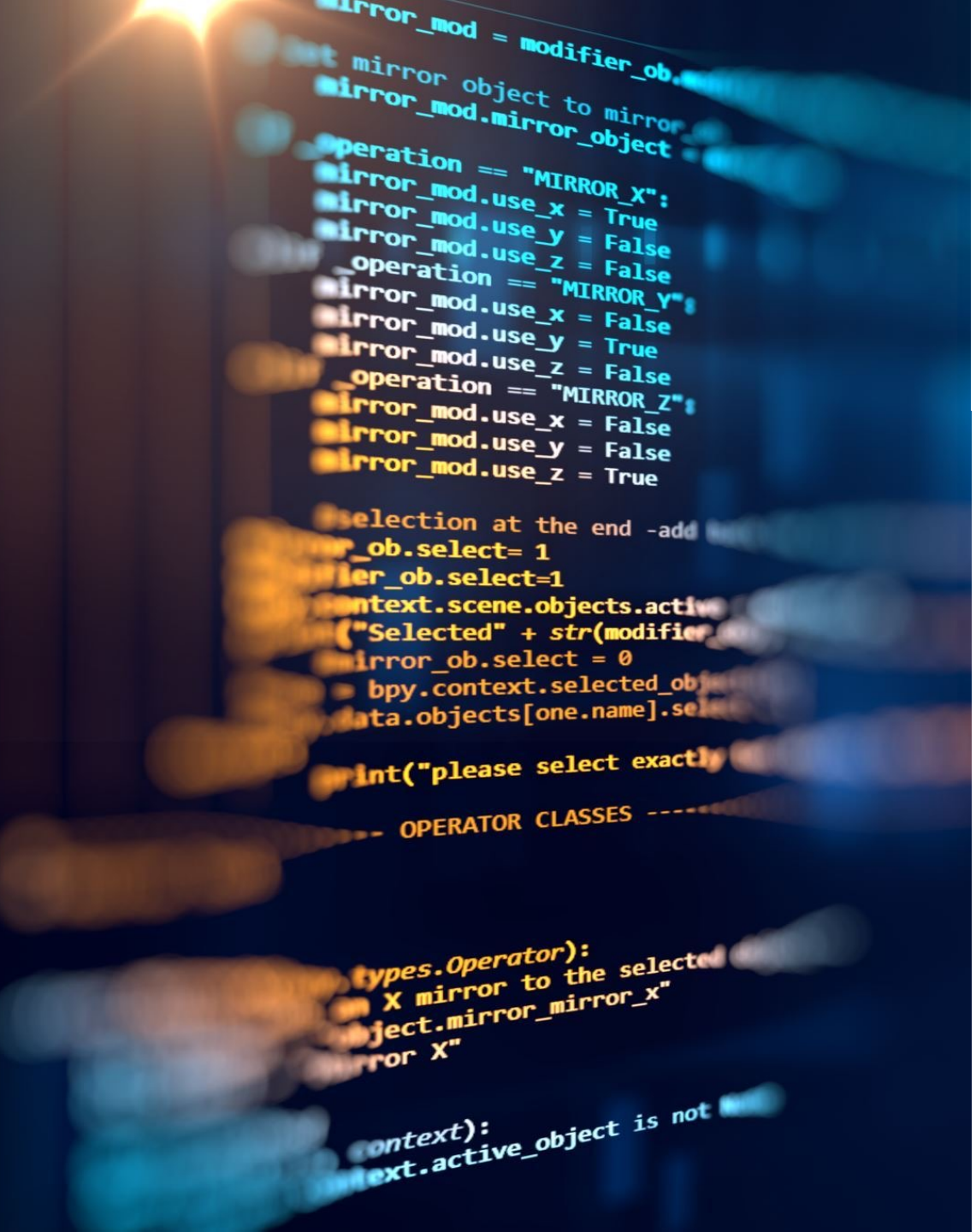
Firewalls can prevent many different types of attacks. Network-based firewalls protect entire networks, and host-based firewalls protect individual systems.

Intrusion Detection System (IDS)

- Intrusion detection is a specific form of monitoring that monitors recorded information and real-time events to detect abnormal activity indicating a potential incident or intrusion.
- An intrusion detection system (IDS) automates the inspection of logs and real-time system events to detect intrusion attempts and system failures.
- A primary goal of an IDS is to provide a means for a timely and accurate response to intrusions.
- IDS types are commonly classified as host-based and network-based. A host-based IDS (HIDS) monitors a single computer or host. A network-based IDS (NIDS) monitors a network by observing network traffic patterns.

Preventing Threats

- Keep systems and applications up to date. Vendors regularly release patches to correct bugs and security flaws, but these only help when they are applied. Patch management ensures that systems and applications are kept up to date with relevant patches.
- Remove or disable unneeded services and protocols. If a system doesn't need a service or protocol, it should not be running. Attackers cannot exploit a vulnerability in a service or protocol that isn't running on a system. As an extreme contrast, imagine a web server is running every available service and protocol. It is vulnerable to potential attacks on any of these services and protocols.
- Use intrusion detection and prevention systems. As discussed, intrusion detection and prevention systems observe activity, attempt to detect threats and provide alerts. They can often block or stop attacks.
- Use up-to-date anti-malware software. We have already covered the various types of malicious code such as viruses and worms. A primary countermeasure is anti-malware software.
- Use firewalls. Firewalls can prevent many different types of threats. Network-based firewalls protect entire networks, and host-based firewalls protect individual systems. This chapter included a section describing how firewalls can prevent attacks.



Preventing Threats - Antivirus

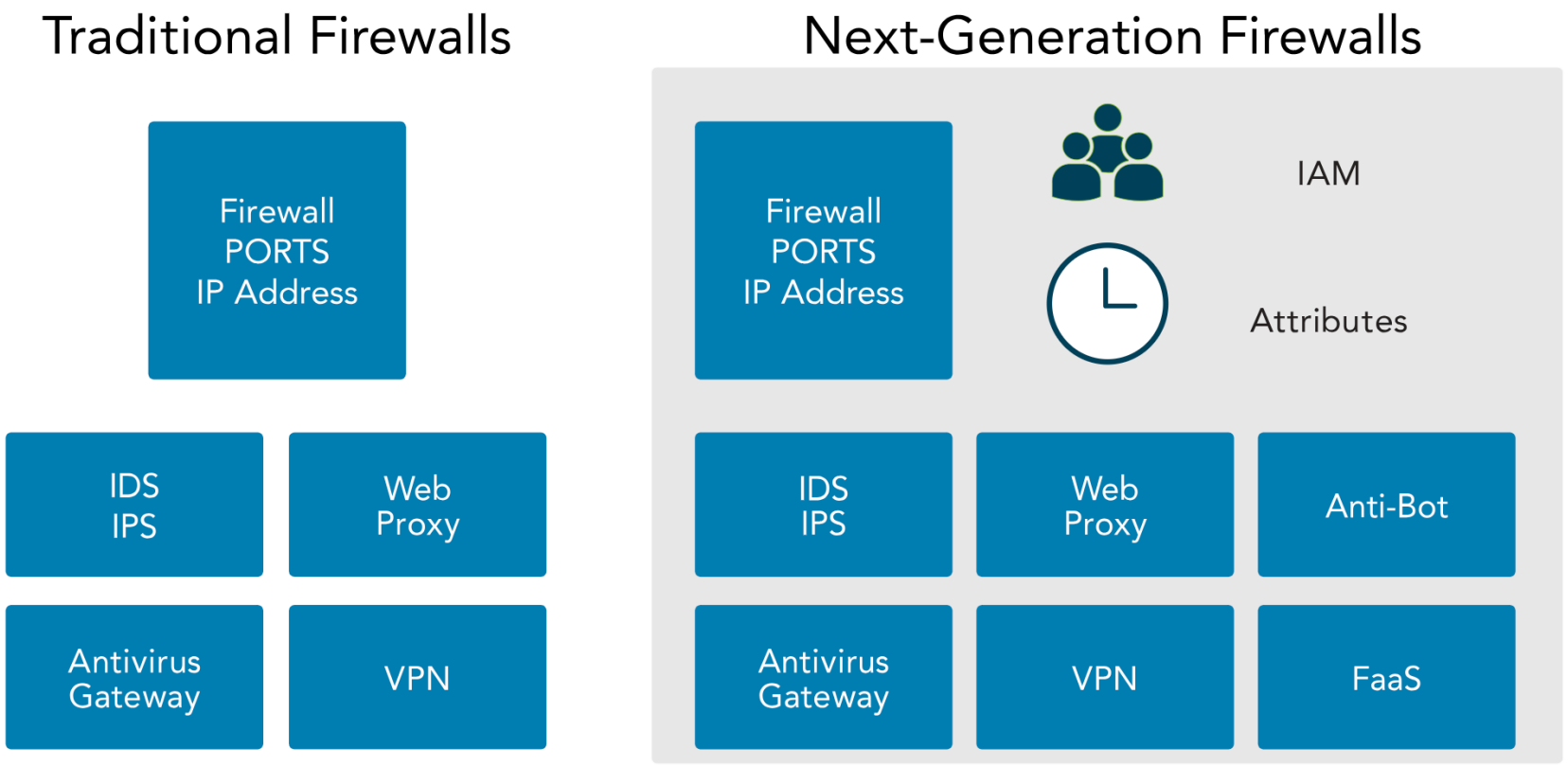
- Antivirus systems try to identify malware based on the signature of known malware or by detecting abnormal activity on a system. This identification is done with various types of scanners, pattern recognition and advanced machine learning algorithms.
- Anti-malware now goes beyond just virus protection as modern solutions try to provide a more holistic approach detecting rootkits, ransomware and spyware. Many endpoint solutions also include software firewalls and IDS or IPS systems.

Preventing Threats - Scan

- Regular vulnerability and port scans are a good way to evaluate the effectiveness of security controls used within an organization. They may reveal areas where patches or security settings are insufficient, where new vulnerabilities have developed or become exposed, and where security policies are either ineffective or not being followed. Attackers can exploit any of these vulnerabilities.

```
Scanning 6 hosts [1000 ports/host]
Discovered open port 143/tcp on 172.20.1.131
Discovered open port 80/tcp on 172.20.1.129
Discovered open port 22/tcp on 172.20.1.132
Discovered open port 22/tcp on 172.20.1.129
Discovered open port 135/tcp on 172.20.1.131
Discovered open port 80/tcp on 172.20.1.131
Discovered open port 22/tcp on 172.20.1.131
Discovered open port 3306/tcp on 172.20.1.131
Discovered open port 443/tcp on 172.20.1.131
Discovered open port 445/tcp on 172.20.1.131
Discovered open port 110/tcp on 172.20.1.131
Discovered open port 139/tcp on 172.20.1.131
Discovered open port 80/tcp on 172.20.1.127
Discovered open port 25/tcp on 172.20.1.131
Discovered open port 21/tcp on 172.20.1.131
Discovered open port 22/tcp on 172.20.1.127
Discovered open port 49153/tcp on 172.20.1.131
Discovered open port 49154/tcp on 172.20.1.131
Discovered open port 443/tcp on 172.20.1.127
```

Preventing Threats - Firewall

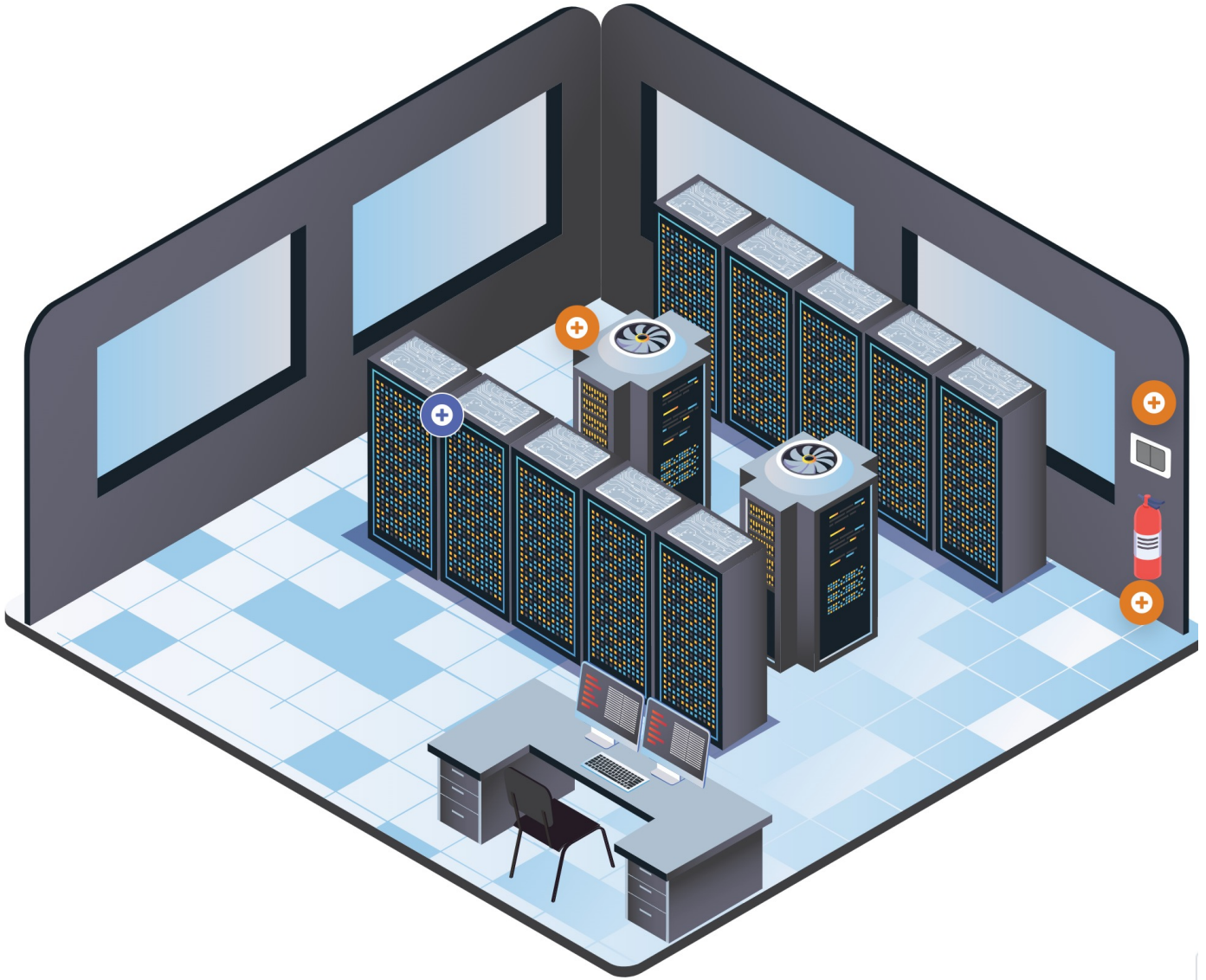


Preventing Threats – Intrusion Prevention System (IPS)

- An intrusion prevention system (IPS) is a special type of active IDS that automatically attempts to detect and block attacks before they reach target systems.
- A distinguishing difference between an IDS and an IPS is that the IPS is placed in line with the traffic. In other words, all traffic must pass through the IPS and the IPS can choose what traffic to forward and what traffic to block after analyzing it. This allows the IPS to prevent an attack from reaching a target. Since IPS systems are most effective at preventing network-based attacks, it is common to see the IPS function integrated into firewalls.
- Just like IDS, there are Network-based IPS (NIPS) and Host-based IPS (HIPS).

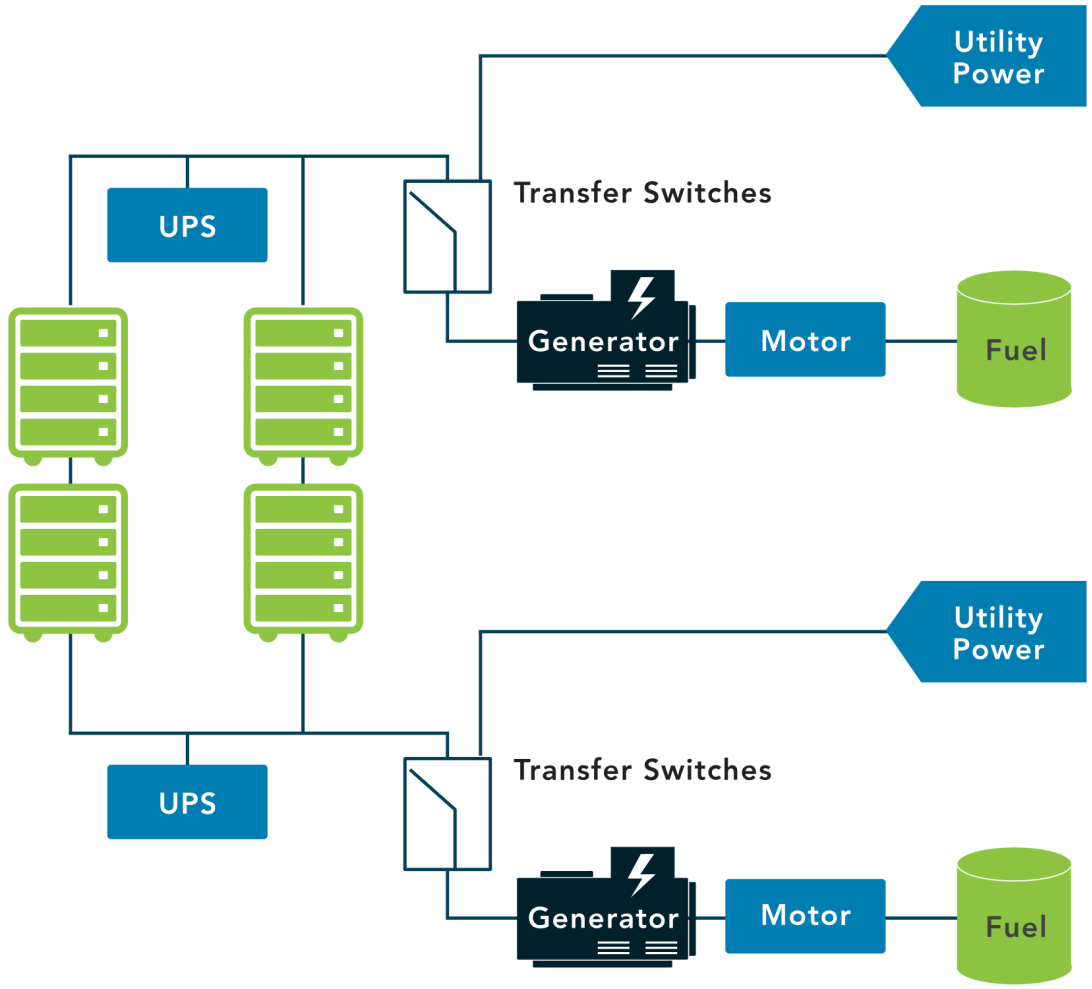
On-Premises Data Center

- When it comes to data centers, there are two primary options: organizations can outsource the data center or own the data center. If the data center is owned, it will likely be built on premises. A place, like a building for the data center is needed, along with power, HVAC, fire suppression and redundancy.



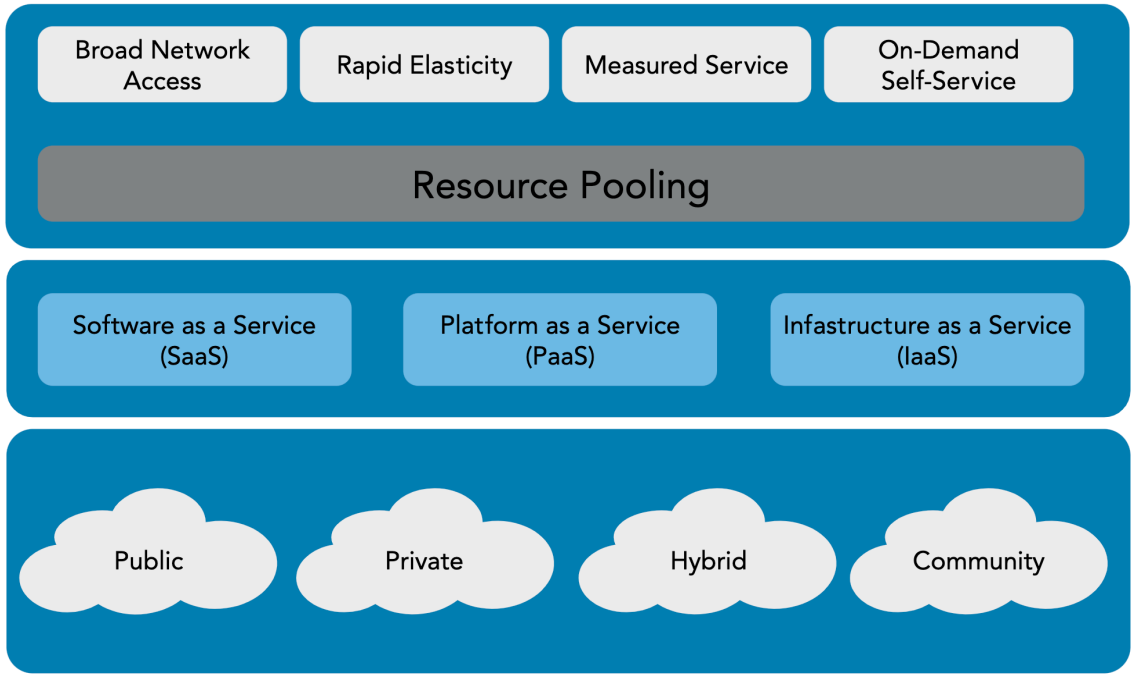
Redundancy

- The concept of redundancy is to design systems with duplicate components so that if a failure were to occur, there would be a backup. This can apply to the data center as well. Risk assessments pertaining to the data center should identify when multiple separate utility service entrances are necessary for redundant communication channels and/or mechanisms.
- If the organization requires full redundancy, devices should have two power supplies connected to diverse power sources. Those power sources would be backed up by batteries and generators. In a high-availability environment, even generators would be redundant and fed by different fuel types.



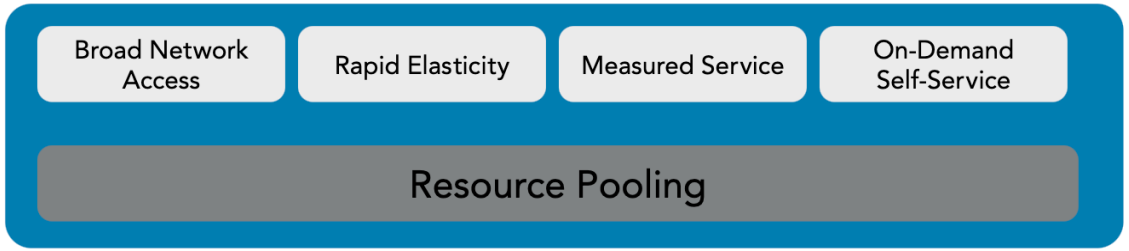
Cloud

- Cloud computing is usually associated with an internet-based set of computing resources, and typically sold as a service, provided by a cloud service provider (CSP).
- *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." NIST SP 800-145*



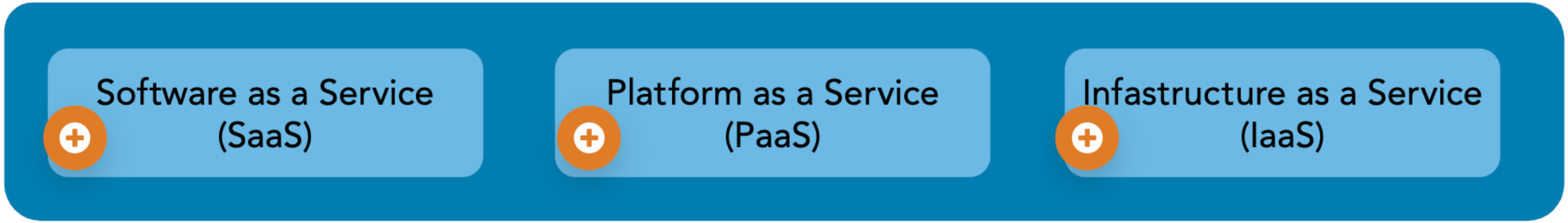
Cloud Characteristics

- Cloud computing has many benefits for organizations, which include but are not limited to:
  - Usage is metered and priced according to units (or instances) consumed. This can also be billed back to specific departments or functions.
  - Reduced cost of ownership. There is no need to buy any assets for everyday use, no loss of asset value over time and a reduction of other related costs of maintenance and support.
  - Reduced energy and cooling costs, along with “green IT” environment effect with optimum use of IT resources and systems.
  - Allows an enterprise to scale up new software or data-based services/solutions through cloud systems quickly and without having to install massive hardware locally.



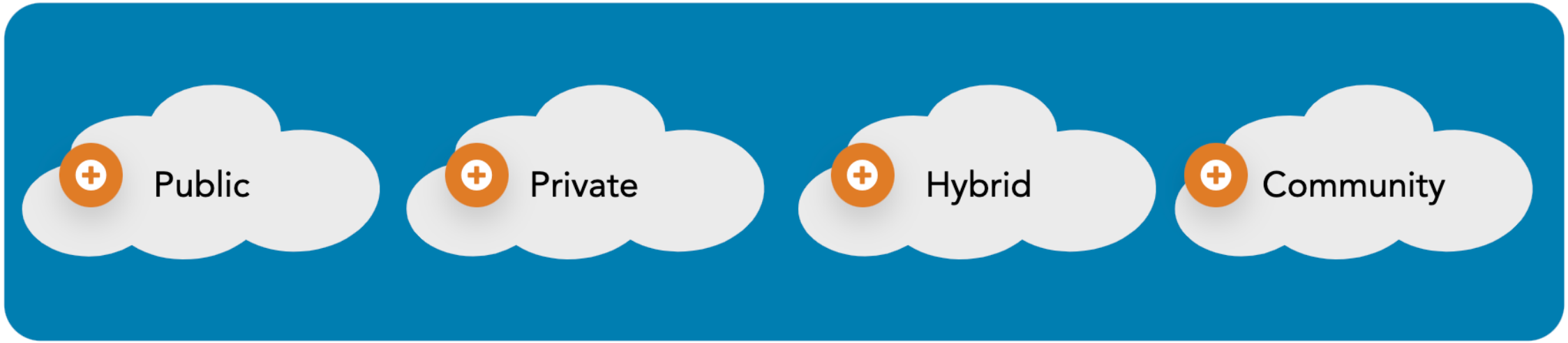
Service Models

- Types of cloud computing service models include Software as a Service (SaaS) , Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

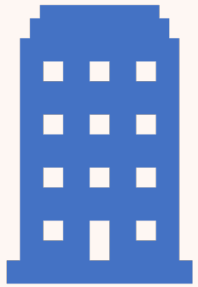


Deployment Models

- The four cloud models available are public, private, hybrid and community .



Managed Service Provider (MSP)



A managed service provider (MSP) is a company that manages information technology assets for another company.

Some other common MSP implementations are:

Augment in-house staff for projects
Utilize expertise for implementation of a product or service
Provide payroll services
Provide Help Desk service management
Monitor and respond to security incidents
Manage all in-house IT infrastructure

Service-Level Agreement (SLA)

The cloud computing service-level agreement (cloud SLA) is an agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing– specific terms to set the quality of the cloud services delivered.

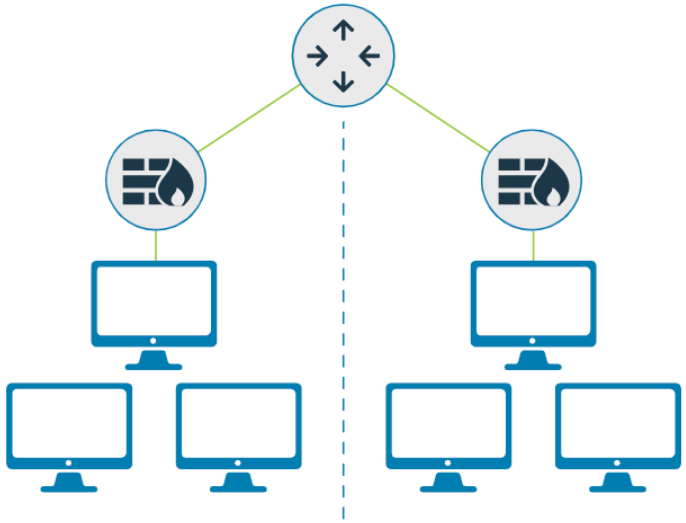
The purpose of an SLA is to document specific parameters, minimum service levels and remedies for any failure to meet the specified requirements.

important SLA points to consider include the following:

- Cloud system infrastructure details and security standards
- Customer right to audit legal and regulatory compliance by the CSP
- Rights and costs associated with continuing and discontinuing service use
- Service availability
- Service performance
- Data security and privacy
- Disaster recovery processes
- Data location
- Data access
- Data portability
- Problem identification and resolution expectations
- Change management processes
- Dispute mediation processes
- Exit strategy

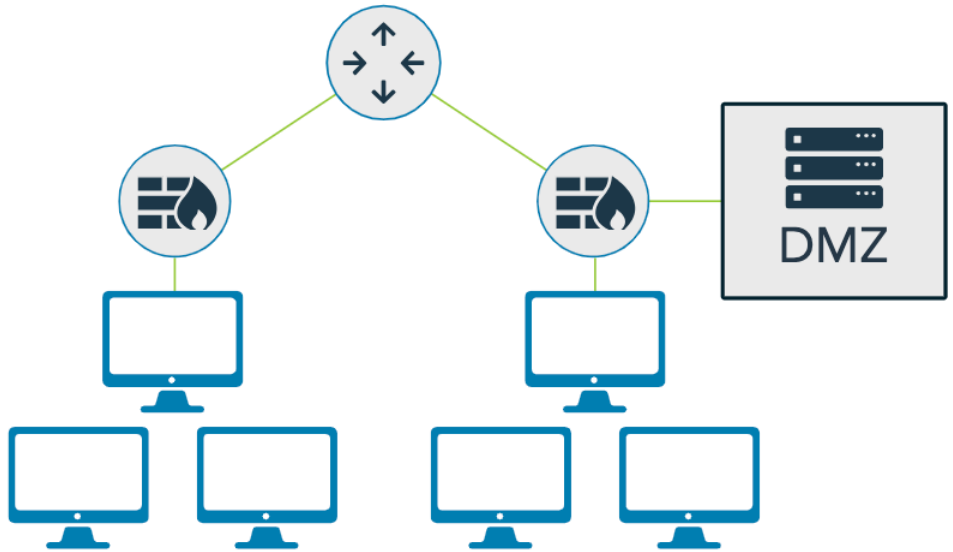
Network Design : Segmentation

Network segmentation involves controlling traffic among networked devices. Complete or physical network segmentation occurs when a network is isolated from all outside communications, so transactions can only occur between devices within the segmented network.



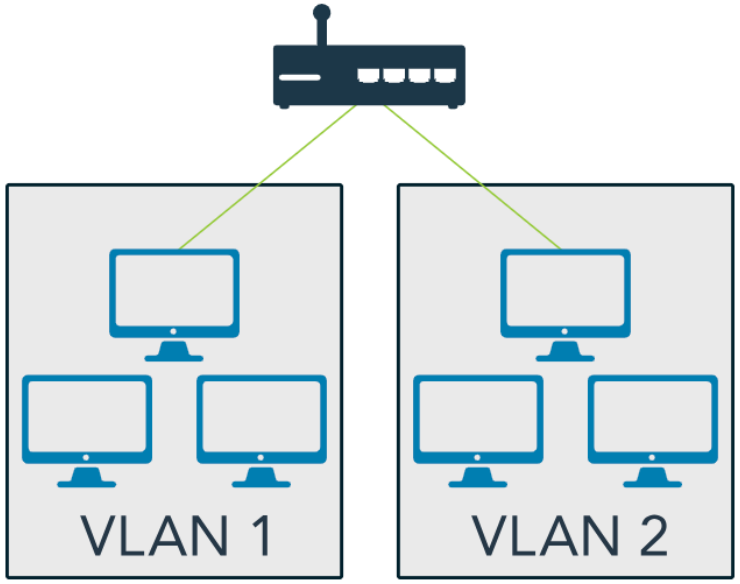
Network Design : Demiliterized Zone (DMZ)

A DMZ is a network area that is designed to be accessed by outside visitors but is still isolated from the private network of the organization. The DMZ is often the host of public web, email, file and other resource servers.



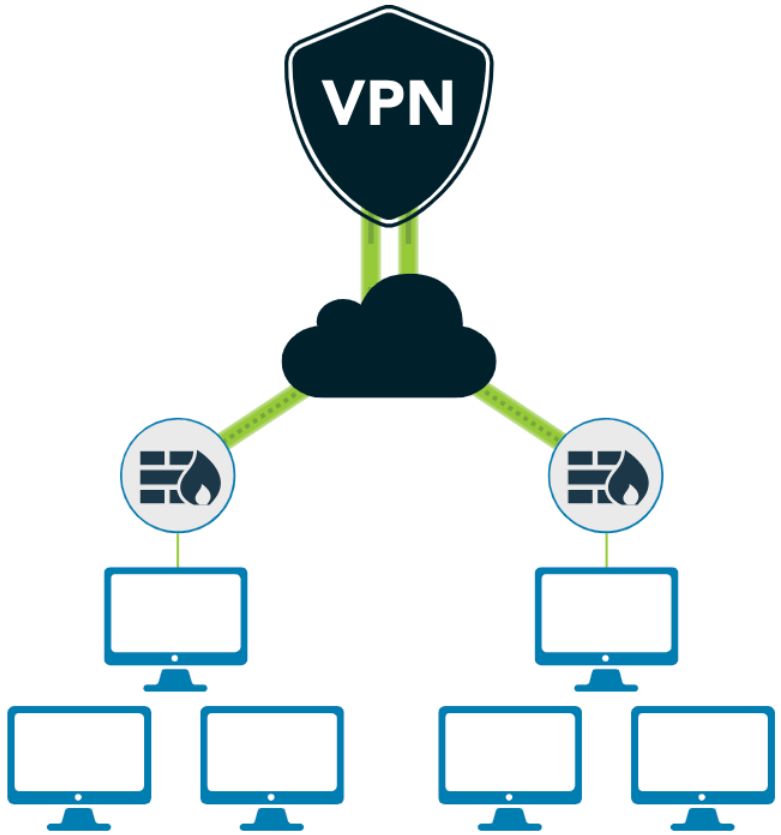
Network Design : Virtual Local Area Network (VLAN)

VLANs are created by switches to logically segment a network without altering its physical topology.



Network Design : Virtual Private Network (VPN)

A virtual private network (VPN) is a communication tunnel that provides point-to-point transmission of both authentication and data traffic over an untrusted network.

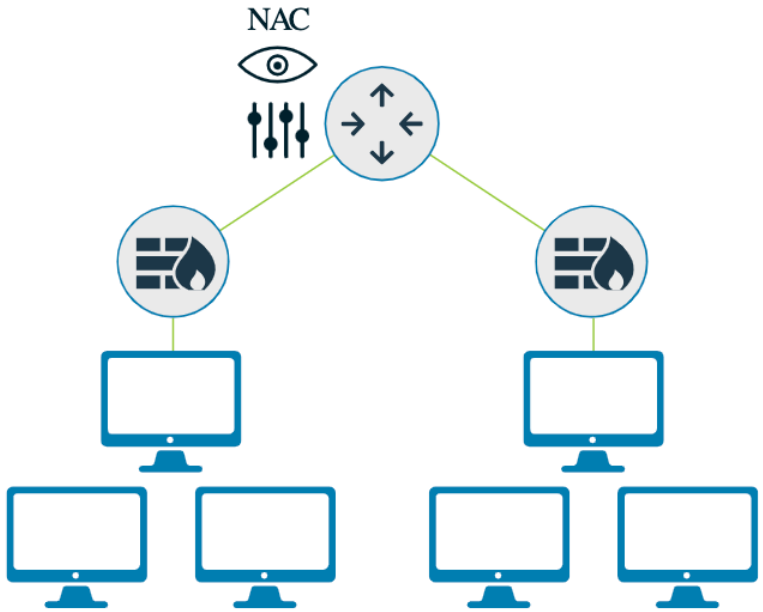


Network Design : Defense in Depth

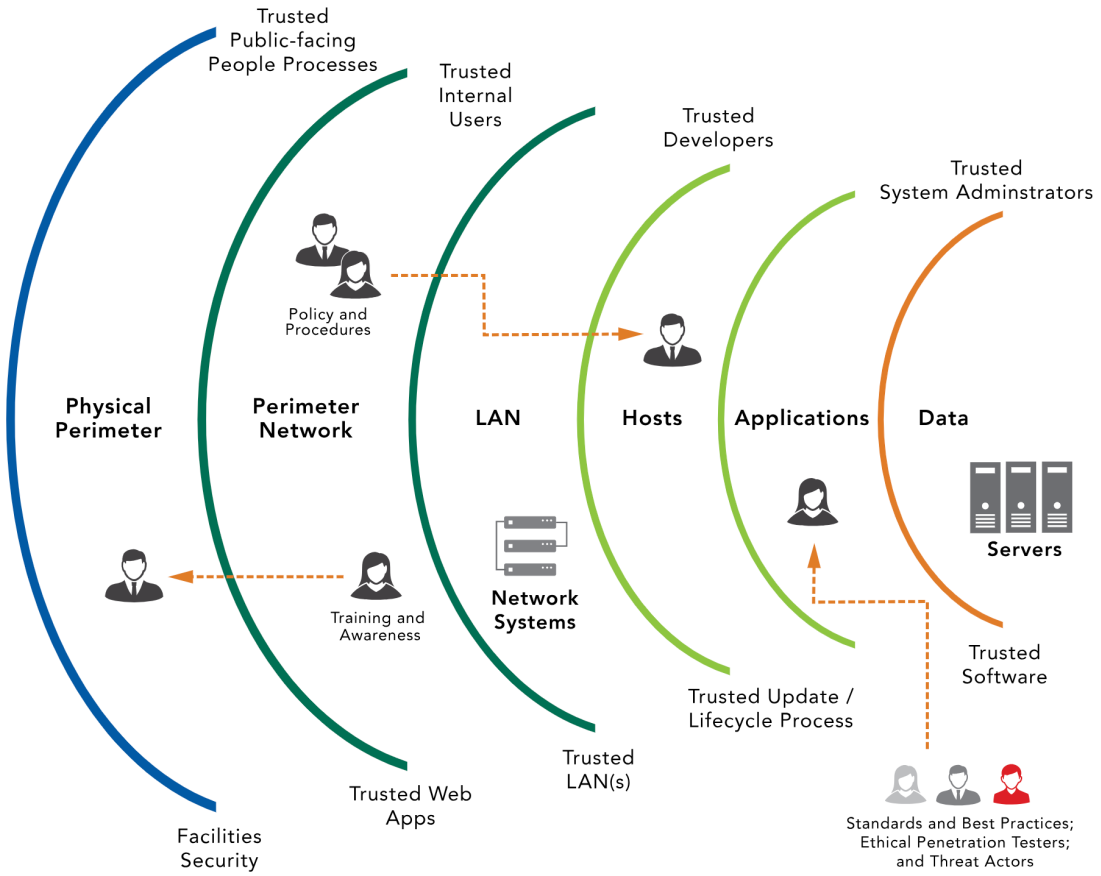
Defense in depth uses multiple types of access controls in literal or theoretical layers to help an organization avoid a monolithic security stance.

Network Design : Network Access Control (NAC)

Network access control (NAC) is a concept of controlling access to an environment through strict adherence to and implementation of security policy.



Deep Dive Defense in Depth



- Data: Controls that protect the actual data with technologies such as encryption, data leak prevention, identity and access management and data controls.
- Application: Controls that protect the application itself with technologies such as data leak prevention, application firewalls and database monitors.
- Host: Every control that is placed at the endpoint level, such as antivirus, endpoint firewall, configuration and patch management.
- Internal network: Controls that are in place to protect uncontrolled data flow and user access across the organizational network. Relevant technologies include intrusion detection systems, intrusion prevention systems, internal firewalls and network access controls.
- Perimeter: Controls that protect against unauthorized access to the network. This level includes the use of technologies such as gateway firewalls, honeypots, malware analysis and secure demilitarized zones (DMZs).
- Physical: Controls that provide a physical barrier, such as locks, walls or access control.
- Policies, procedures and awareness: Administrative controls that reduce insider threats (intentional and unintentional) and identify risks as soon as they appear.

Zero Trust

- Zero trust is an evolving design approach which recognizes that even the most robust access control systems have their weaknesses. It adds defenses at the user, asset and data level, rather than relying on perimeter defense. In the extreme, it insists that every process or action a user attempts to take must be authenticated and authorized; the window of trust becomes vanishingly small.
- While microsegmentation adds internal perimeters, zero trust places the focus on the assets, or data, rather than the perimeter. Zero trust builds more effective gates to protect the assets directly rather than building additional or higher walls.