Glossary

1. **Networking**
2. **Networking at a Glance**
3. **Open Systems Interconnection (OSI) Model**
4. **Transmission Control Protocol/Internet Protocol (TCP/IP)**
5. **Internet Protocol (IPv4 and IPv6)**
6. **WiFi**
7. **Ports and Protocols (Applications/Services)**
8. **Types of Threats**
9. **Intrusion Detection Systems**
    - **Host-based Intrusion Detection System (HIDS)**
    - **Network Intrusion Detection System (NIDS)**
10. **Security Information and Event Management (SIEM)**
11. **Preventing Threat**
12. **Antivirus**
13. **Scans**
14. **Firewalls**
15. **Intrusion Prevention System (IPS)**
16. **On-Premises Data Centers**
17. **Redundancy**
18. **Memorandum of Understanding (MOU) Memorandum of Agreement (MOA)**
19. **Cloud**
20. **Service Model**
21. **Deployment Model**
22. **Managed Service Provider (MSP)**
23. **Service-Level Agreement (SLA)**
24. **Network Design**
25. **Defense in Depth**
26. **Zero Trust**
27. **Network Access Control (NAC)**
28. **Network Segmentation (Demilitarized Zone)**
29. **Segmentation for Embedded Systems and IoT**
30. **Microsegmentation**

1.NETWORKING:

A network is simply two or more computers linked together to share data, information or resources.
there are 2 types of network:

1.LAN:**spanning a single floor or building. This is commonly a limited geographical area.**

2.WAN: **assigned to the long-distance connections between geographically remote networks**

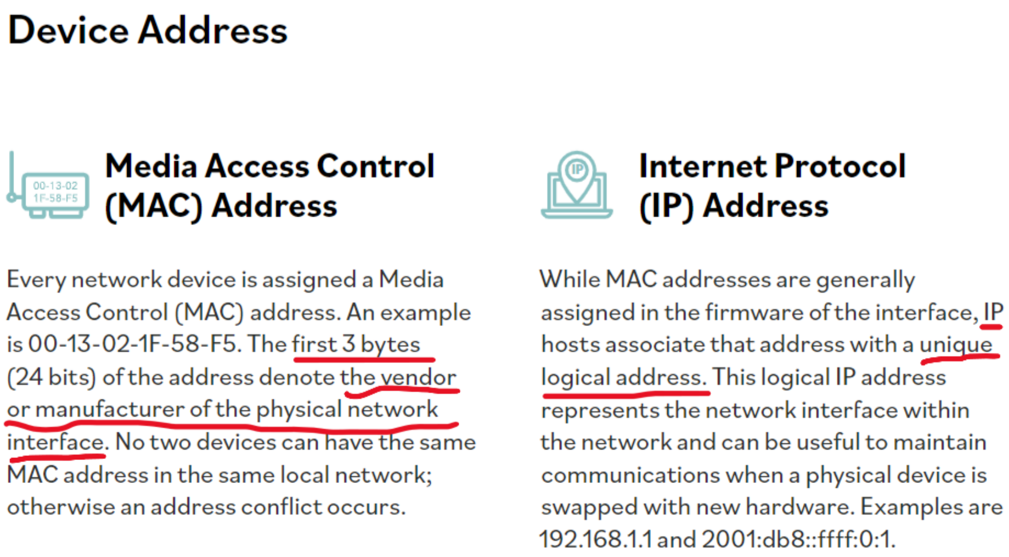
Network devices:

1.HUB:	**Hubs are used to connect multiple devices in a network. They're less likely to be seen in business or corporate networks than in home networks. Hubs are wired devices and are not as smart as switches or route**
2. Firewall	**Firewalls are essential tools in managing and controlling network traffic and protecting the network.** **A firewall is a network device used to filter traffic.** **It is typically deployed between a private network and the internet,** **but it can also be deployed between** **departments (segmented networks) within an organization (overall network).** **Firewalls filter traffic based on a defined set of rules, also called filters or access control list**
Switch	**Intelligent hub** **Switches are wired devices that know the addresses of the devices connected to them and route traffic to that port/device rather than retransmitting to all devices.** **Smarter than hub but not smarter than routers** **Switches can also create separate broadcast domains when used to create VLANs**
Server	**A server is a computer that provides information to other computers on a network.**

	Some common servers are web servers, email servers, print servers, database servers, and file servers. All of these are, by design, networked and accessed in some way by a client computer. Servers are usually secured differently than workstations to protect the information they contain
Router	Routers are used to control traffic flow on networks and are often used to connect similar networks and control traffic flow between them. Routers can be wired or wireless and can connect multiple switches. Smarter than hubs and switches, routers determine the most efficient “route” for the traffic to flow across the network.
Endpoint	Endpoints are the ends of a network communication link. One end is often at a server where a resource resides, and the other end is often a client making a request to use a network resource. An endpoint can be another server, desktop workstation, laptop, tablet, mobile phone, or any other end user device

Ethernet:

Ethernet (IEEE 802.3) is a standard that defines wired connections of networked devices.
This standard defines the way data is formatted over the wire to ensure disparate devices can communicate over the same cable.



Device Address

Media Access Control (MAC) Address

Every network device is assigned a Media Access Control (MAC) address. An example is 00-13-02-1F-58-F5. The first 3 bytes (24 bits) of the address denote the vendor or manufacturer of the physical network interface. No two devices can have the same MAC address in the same local network; otherwise an address conflict occurs.

Internet Protocol (IP) Address

While MAC addresses are generally assigned in the firmware of the interface, IP hosts associate that address with a unique logical address. This logical IP address represents the network interface within the network and can be useful to maintain communications when a physical device is swapped with new hardware. Examples are 192.168.1.1 and 2001:db8::ffff:0:1.

2.Networking at a Glance

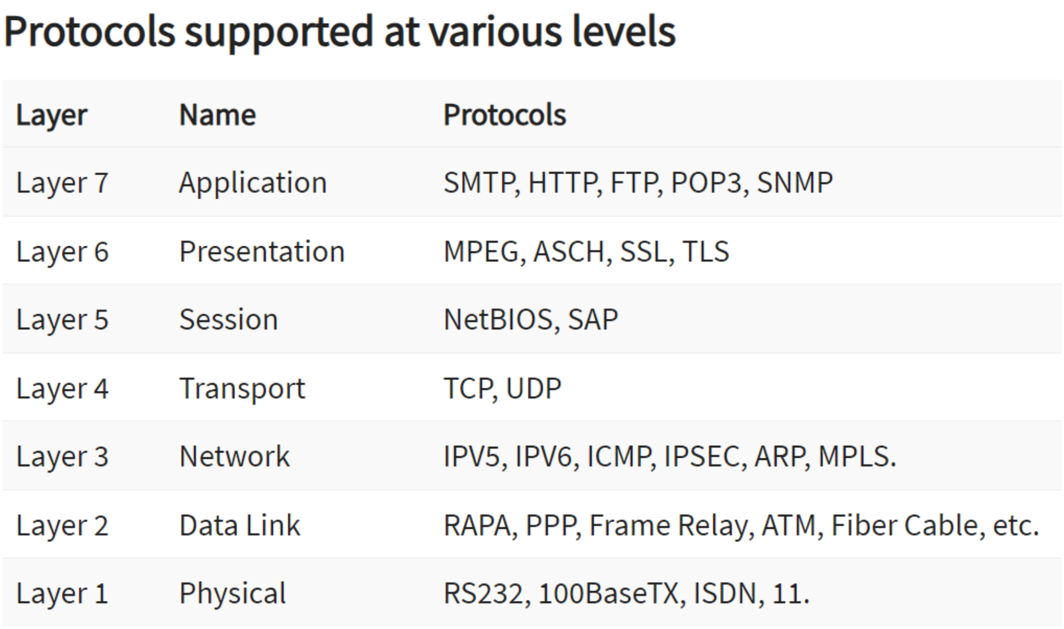
A Small Business Network: all devices behind the firewall connect via the network switch, and the firewall lies between the network switch and the internet.

A Typical Home Network: Notice the primary difference between the home network and the business network is that the router, firewall, and network switch are often combined into one device supplied by your internet provider and shown here as the wireless access point.

3.Open Systems Interconnection (OSI) Model

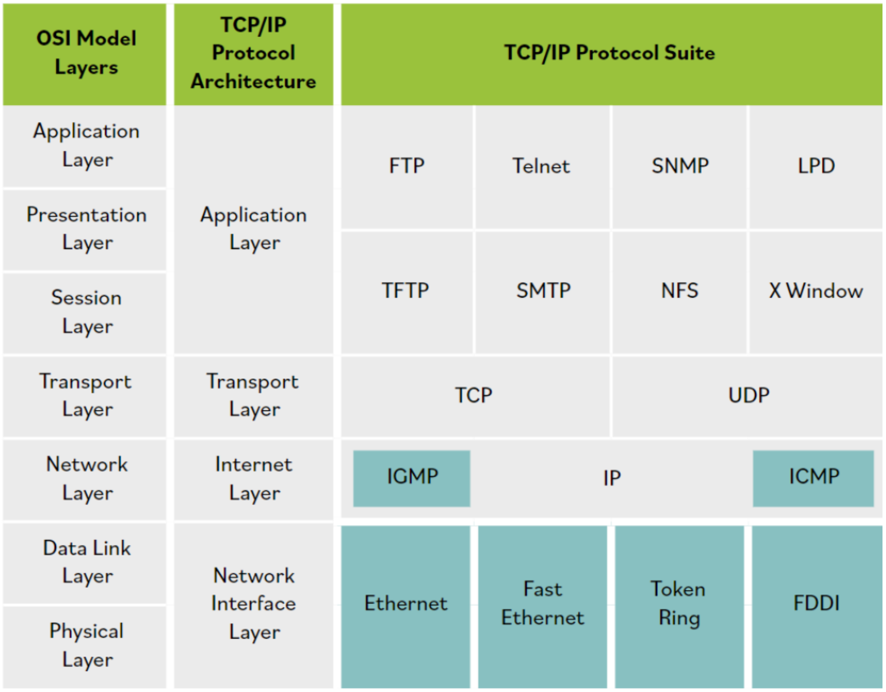
Layer No	**Layer Name**	**Responsibility**	**Information Form (Data Unit)**	**Device or Protocol**
7	Application Layer	Helps in identifying the client and synchronizing communication.	Message	SMTP

Layer No	Layer Name	Responsibility	Information Form (Data Unit)	Device or Protocol
6	Presentation Layer	Data from the application layer is extracted and manipulated in the required format for transmission.	Message	JPEG, MPEG, GIF
5	Session Layer	Establishes Connection, Maintenance, Ensures Authentication and Ensures security.	Message (or encrypted message)	Gateway NetBios
4	Transport Layer	Take Service from Network Layer and provide it to the Application Layer.	Segment	Firewall
3	Network Layer	Transmission of data from one host to another, located in different networks.	Packet	Router
2	Data Link Layer	Node to Node Delivery of Message.	Frame	Switch, Bridge,WAP
1	Physical Layer	Establishing Physical Connections between Devices.	Bits	Hub, Repeater, Modem, Cables



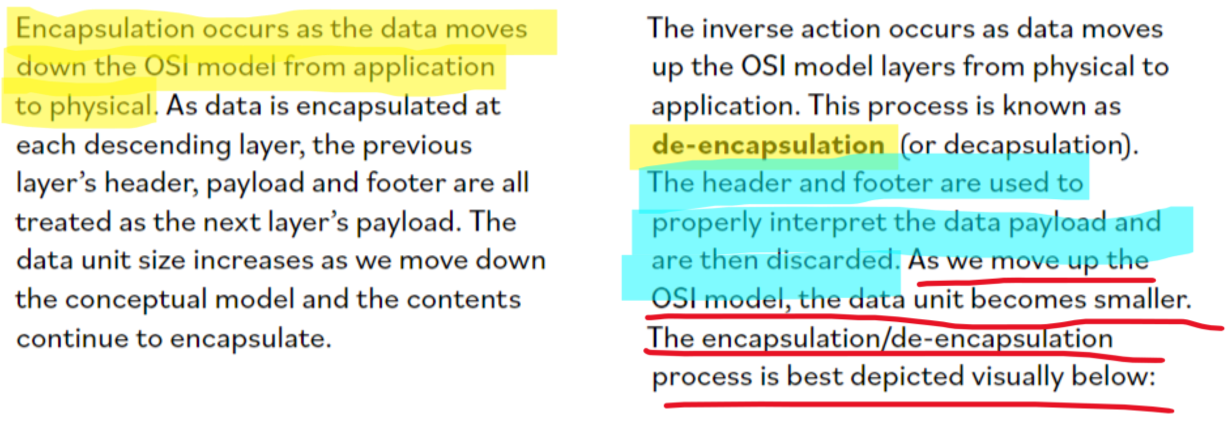
Protocols supported at various levels

Layer	Name	Protocols
Layer 7	Application	SMTP, HTTP, FTP, POP3, SNMP
Layer 6	Presentation	MPEG, ASCH, SSL, TLS
Layer 5	Session	NetBIOS, SAP
Layer 4	Transport	TCP, UDP
Layer 3	Network	IPV5, IPV6, ICMP, IPSEC, ARP, MPLS.
Layer 2	Data Link	RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc.
Layer 1	Physical	RS232, 100BaseTX, ISDN, 11.



<table>
<tr><th>OSI Model Layers</th><th>TCP/IP Protocol Architecture</th><th colspan="4">TCP/IP Protocol Suite</th></tr>
<tr><td rowspan="2">Application Layer</td><td rowspan="6">Application Layer</td><td rowspan="3">FTP</td><td rowspan="3">Telnet</td><td rowspan="3">SNMP</td><td rowspan="3">LPD</td></tr>
<tr></tr>
<tr><td rowspan="2">Presentation Layer</td></tr>
<tr><td rowspan="3">TFTP</td><td rowspan="3">SMTP</td><td rowspan="3">NFS</td><td rowspan="3">X Window</td></tr>
<tr><td rowspan="2">Session Layer</td></tr>
<tr></tr>
<tr><td>Transport Layer</td><td>Transport Layer</td><td colspan="2">TCP</td><td colspan="2">UDP</td></tr>
<tr><td>Network Layer</td><td>Internet Layer</td><td>IGMP</td><td colspan="2">IP</td><td>ICMP</td></tr>
<tr><td>Data Link Layer</td><td rowspan="2">Network Interface Layer</td><td rowspan="2">Ethernet</td><td rowspan="2">Fast Ethernet</td><td rowspan="2">Token Ring</td><td rowspan="2">FDDI</td></tr>
<tr><td>Physical Layer</td></tr>
</table>

Encapsulation is particularly important when discussing transport, network and data link layers (2-4)



Encapsulation occurs as the data moves down the OSI model from application to physical. As data is encapsulated at each descending layer, the previous layer's header, payload and footer are all treated as the next layer's payload. The data unit size increases as we move down the conceptual model and the contents continue to encapsulate.

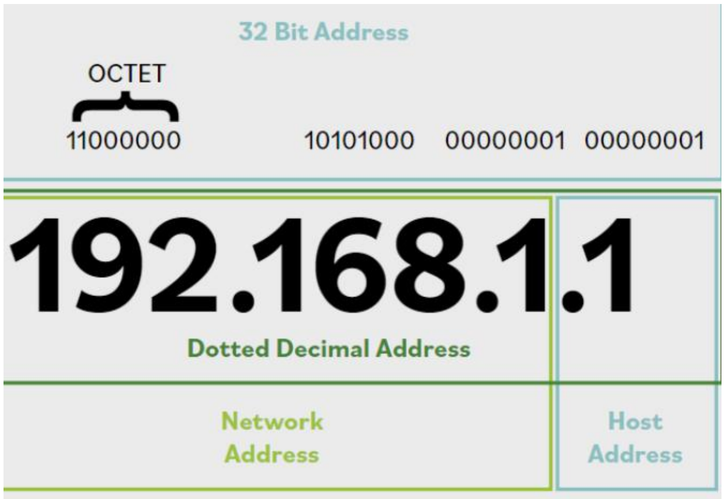
The inverse action occurs as data moves up the OSI model layers from physical to application. This process is known as **de-encapsulation** (or decapsulation). The header and footer are used to properly interpret the data payload and are then discarded. As we move up the OSI model, the data unit becomes smaller. The encapsulation/de-encapsulation process is best depicted visually below:

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

application	**Defines the protocols for the transport layer.** **Telnet, File Transfer Protocol (FTP), Simple Mail Transport Protocol (SMTP), and Domain Name Service (DNS**
Transport	**Permits data to move among device**
Internet layer	**Creates/inserts packet**
Network interface layer	**How data moves through the network**

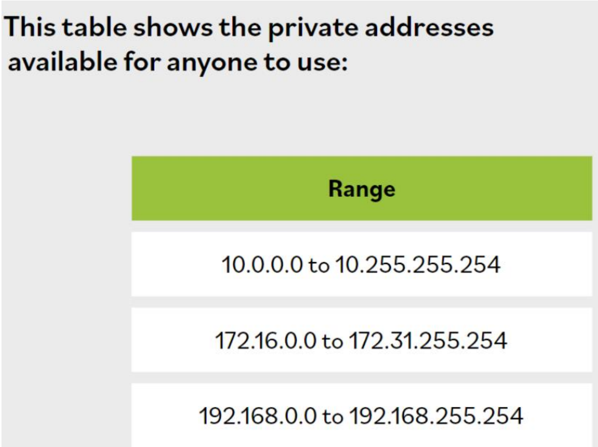
Internet Control Message Protocol (ICMP) is used to determine the health of a network or a specific link. ICMP is utilized by ping, traceroute, and other network management tools. The ping utility employs ICMP echo packets and bounces them off remote system

5.Internet Protocol (IPv4 and IPv6)



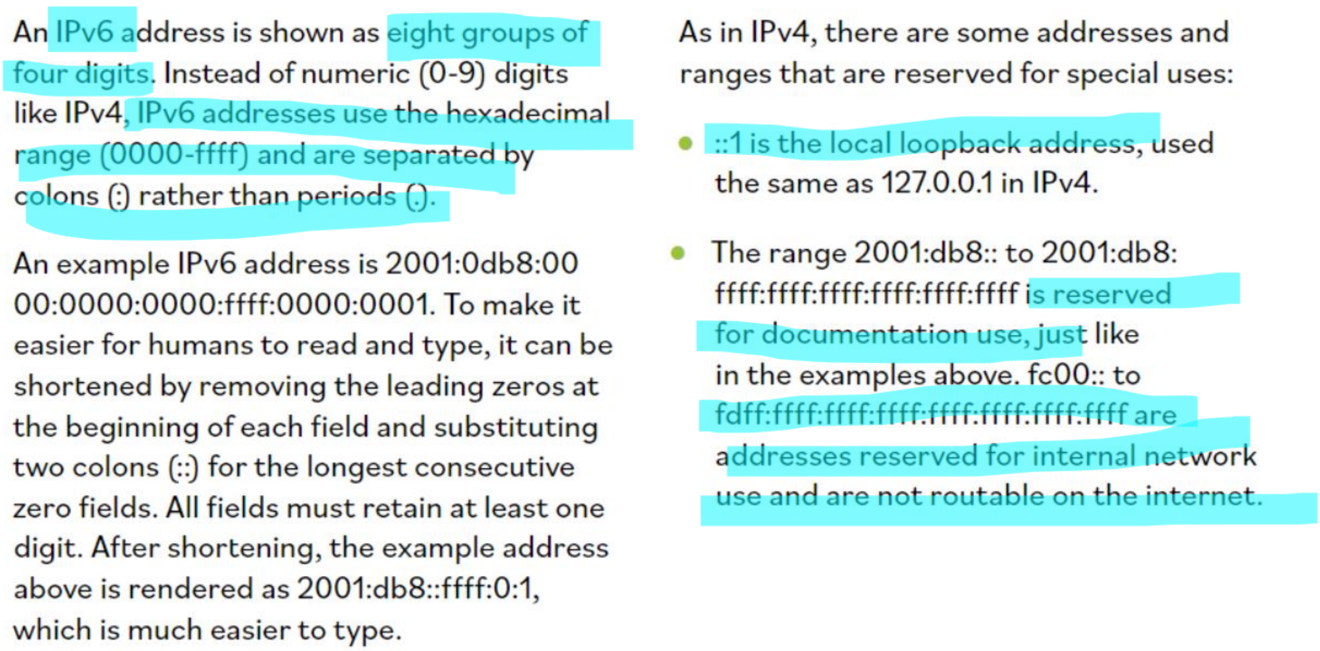
To ease network administration, networks are typically divided into subnets. Because subnets cannot be distinguished with the addressing scheme discussed so far, a separate mechanism, the subnet mask, is used to define the part of the address used for the subnet. The mask is usually converted to decimal notation like 255.255.255.0.

192.168.2.xxx for its internal network addresses, without fear that some other system can intercept traffic on their LAN



This table shows the private addresses available for anyone to use:

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



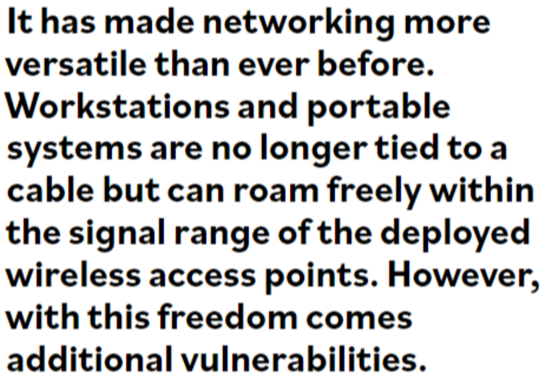
An IPv6 address is shown as eight groups of four digits. Instead of numeric (0-9) digits like IPv4, IPv6 addresses use the hexadecimal range (0000-ffff) and are separated by colons (:) rather than periods (.).

An example IPv6 address is 2001:0db8:0000:0000:0000:ffff:0000:0001. To make it easier for humans to read and type, it can be shortened by removing the leading zeros at the beginning of each field and substituting two colons (::) for the longest consecutive zero fields. All fields must retain at least one digit. After shortening, the example address above is rendered as 2001:db8::ffff:0:1, which is much easier to type.

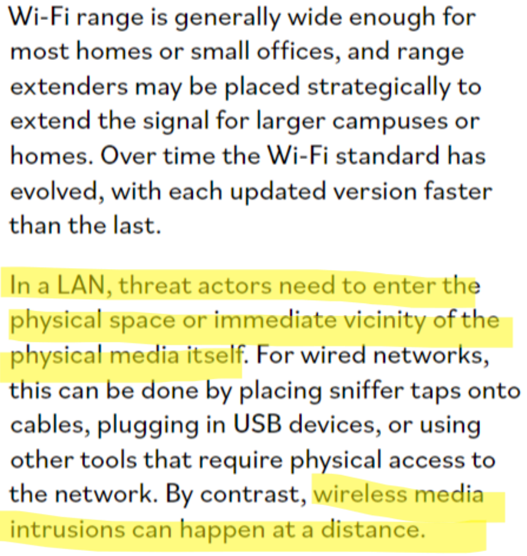
As in IPv4, there are some addresses and ranges that are reserved for special uses:

- ::1 is the local loopback address, used the same as 127.0.0.1 in IPv4.
- The range 2001:db8:: to 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff is reserved for documentation use, just like in the examples above. fc00:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff are addresses reserved for internal network use and are not routable on the internet.

6. WiFi



It has made networking more versatile than ever before. Workstations and portable systems are no longer tied to a cable but can roam freely within the signal range of the deployed wireless access points. However, with this freedom comes additional vulnerabilities.



Wi-Fi range is generally wide enough for most homes or small offices, and range extenders may be placed strategically to extend the signal for larger campuses or homes. Over time the Wi-Fi standard has evolved, with each updated version faster than the last.

In a LAN, threat actors need to enter the physical space or immediate vicinity of the physical media itself. For wired networks, this can be done by placing sniffer taps onto cables, plugging in USB devices, or using other tools that require physical access to the network. By contrast, wireless media intrusions can happen at a distance.

Wi-Fi Attacks:

1. Rogue Access Points:

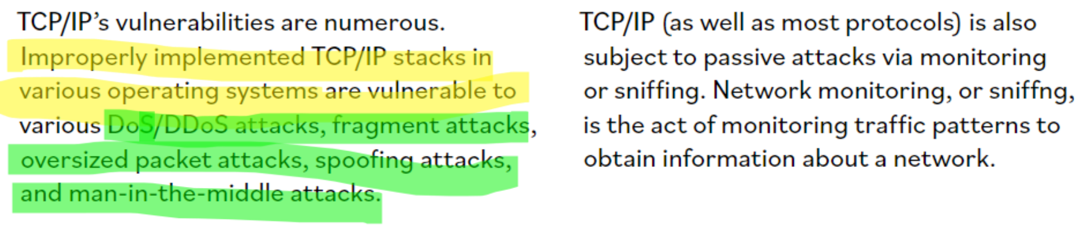
- **Unauthorized access points added to the network without knowledge.**
- **Can be malicious (attacker) or accidental (employee).**
- **Major concern if not monitored.**
- **Mitigation: Port security on switches and scanning for rogue access points.**
- **Compromises confidentiality and integrity.**

2. Jamming/Interference:

- **Overload of traffic on Wi-Fi frequencies or deliberate disruption (DoS attack).**
- **2.4 GHz band is shared by Bluetooth, microwaves, cordless phones, baby monitors, etc.**
- **Compromises integrity and availability.**

3. Evil Twin:

- **Attackers create rogue access points to gain network access or intercept information.**
- **Attacker's access point mimics the legitimate one, causing devices to connect automatically.**
- **Compromises confidentiality and integrity.**



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 sniffng, is the act of monitoring traffic patterns to obtain information about a network.

7. Ports and Protocols(Applications/Services)

There are physical ports that you connect wires to and logical ports that determine where the data/traffic goes

▪ The IP addresses can be seen as the number of an apartment building.

♦ The Port number is your apartment number.

♦ If you have 50 browser tabs open, each tab has its own port number(s).

▪ Well-known Ports:

♦ 0-1023 - Mostly used for protocols.

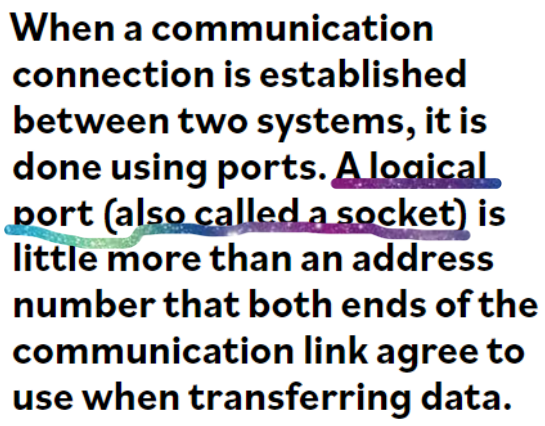
▪ Registered Ports:

♦ 1024 to 49151 - Mostly used for vendor specific applications.

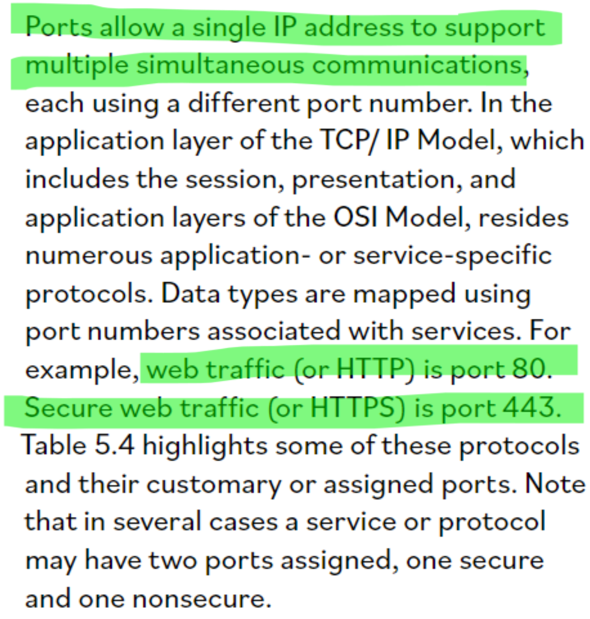
Physical Ports:

Physical ports are the ports on the routers,switches, servers, computers, etc., to which that you connect the wires (e.g., fiber-optic cables, Cat5 cables) to create a network.

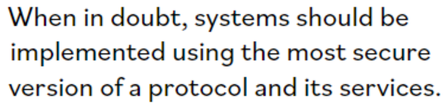
Logical Port:



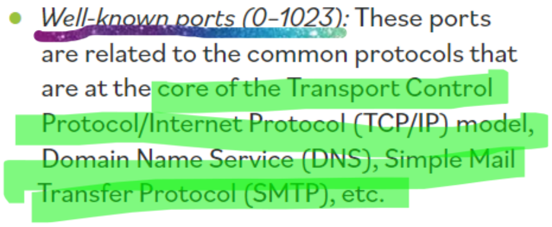
When a communication connection is established between two systems, it is done using ports. A logical port (also called a socket) is little more than an address number that both ends of the communication link agree to use when transferring data.



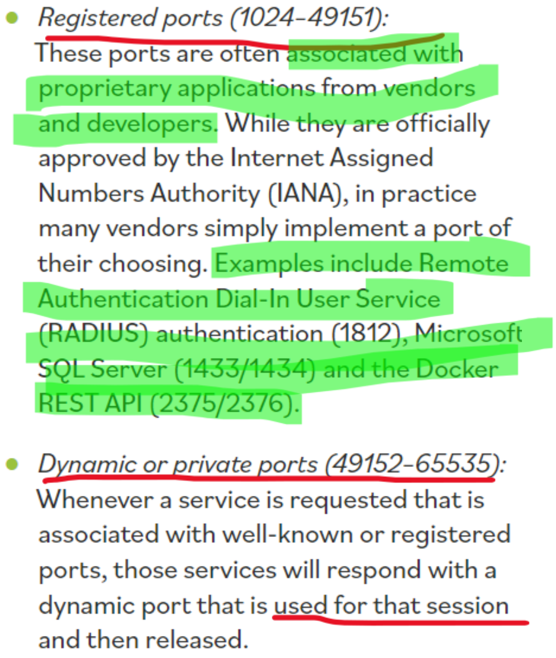
Ports allow a single IP address to support multiple simultaneous communications, each using a different port number. In the application layer of the TCP/ IP Model, which includes the session, presentation, and application layers of the OSI Model, resides numerous application- or service-specific protocols. Data types are mapped using port numbers associated with services. For example, web traffic (or HTTP) is port 80. Secure web traffic (or HTTPS) is port 443. Table 5.4 highlights some of these protocols and their customary or assigned ports. Note that in several cases a service or protocol may have two ports assigned, one secure and one nonsecure.



When in doubt, systems should be implemented using the most secure version of a protocol and its services.



- *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 Port

Network sniffing could also reveal the content of documents and other files if they are sent via insecure protocols.

Insecure Port	Description	Protocol	Secure Alternative port	Protocol
21-FTP	Port 21 (FTP): • Sends username and password using plaintext. • Vulnerable to interception by attackers, who could retrieve confidential information. Secure Alternative - SFTP: • Uses port 22. • Encrypts user credentials and data packets, enhancing security.	File Transfer Protocol	SFTP-22	
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. 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	SSH-22	
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
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

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)
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 and is no longer considered secure. It is now recommended that web servers and clients use Transport Layer Security (TLS) 1.3 or higher for the best protection.	HyperText Transfer Protocol	443-HTTPS	HyperText Transfer Protocol (SSL/TLS)
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
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.	Simple Network Management Protoco	161/162-SNMP	SNMPv3
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 passthrough a	Server Message Block	2049-NFS	Network File System

	firewall at the network perimeter. Amore secure alternative is port 2049, it is recommended that NFS not be allowed through firewalls either			
389-LDAP	Port 389, Lightweight Directory Access Protocol (LDAP), is used to communicate directory information from serversto 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, itis susceptible to sniffingand manipulation attacks. Lightweight Directory Access Protocol Secure (LDAPS)adds SSL/TLS security to protect the information while in transit	Lightweight Directory Access Protoco	636-LDAPS	Lightweight Directory Access Protocol Secure

8. Types of Threats

1. Spoofing	This is 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 addresses, usernames, system names, wireless network SSIDs, email addresses, and many other types of logical identification.
2. 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.
3. 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.(nneche)
4. 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.

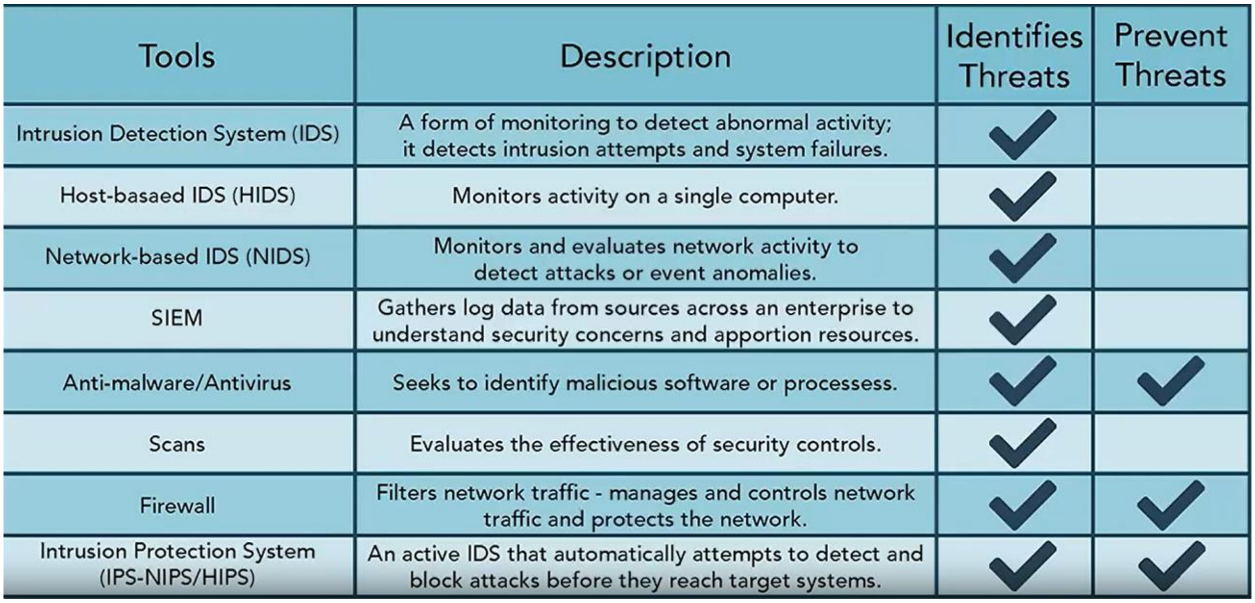
	A virus is a self-replicating piece of code that spreads without the consent of a user, but frequently with their assistance—for example, a user must click on a link or open a file.
5. Trojan	the Trojan is a software program that appears benevolent but carries a malicious, behind-the-scenes payload that has the potential to wreak havoc on a system or network. Malicious code embedded in a system - A Trojan is a type of software that looks harmless or even helpful, but it actually hides something dangerous inside. It's like a gift that seems nice on the outside, but inside, there's something harmful - So, a Trojan tricks you into letting it in, and then it can do a lot of damage behind the scenes. 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.
6. 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.
7. 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
8. Side Channel Attack	A side-channel attack is a passive, noninvasive attack to observe the operation of a device. Methods include power monitoring, timing and fault analysis attack
9. 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
10.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 threa
11.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
12.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.

A Denial-of-Service (DoS) attack is like when someone deliberately tries to overload a system or website so that it can't handle any more requests, causing it to stop working for legitimate users. Think of it like someone calling a store repeatedly, blocking the line so that real customers can't get through.

A Distributed Denial-of-Service (DDoS) attack is a bigger version of this. Instead of one person making those calls, it's like hundreds or thousands of people (or computers) all calling at the same time, making it even harder for the store to function. These people or computers don't even know they're participating in the attack—they're just being controlled by the attacker.

Example: Imagine you want to visit a popular website. Normally, the website can handle many visitors at once, but during a DDoS attack, the attacker uses thousands of computers to flood the website with fake requests. As a result, the website becomes so overwhelmed that it can't respond to real visitors like you, so it crashes or becomes very slow. This means you, and many others, can't access the website because it's too busy dealing with the attack.



Tools	Description	Identifies Threats	Prevent Threats
Intrusion Detection System (IDS)	A form of monitoring to detect abnormal activity; it detects intrusion attempts and system failures.	✓	
Host-basaed IDS (HIDS)	Monitors activity on a single computer.	✓	
Network-based IDS (NIDS)	Monitors and evaluates network activity to detect attacks or event anomalies.	✓	
SIEM	Gathers log data from sources across an enterprise to understand security concerns and apportion resources.	✓	
Anti-malware/Antivirus	Seeks to identify malicious software or processess.	✓	✓
Scans	Evaluates the effectiveness of security controls.	✓	
Firewall	Filters network traffic - manages and controls network traffic and protects the network.	✓	✓
Intrusion Protection System (IPS-NIPS/HIPS)	An active IDS that automatically attempts to detect and block attacks before they reach target systems.	✓	✓

9. Intrusion Detection Systems

An intrusion occurs when an attacker is able to bypass or thwart security mechanisms and gain access to an organization's resource.

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 IDS is intended as part of a defense-in-depth security plan. It will work with, and complement, other security mechanisms such as firewalls, but it does not replace them.

Intrusion Detection Systems (IDSs) can recognize attacks that come from external connections, such as an attack from the internet, and attacks that spread internally, such as a malicious worm.

Once they detect a suspicious event, they respond by sending alerts or raising alarms. A primary goal of an IDS is to provide a means for a timely and accurate response to intrusions. Intrusion detection and prevention refer to capabilities that are part of isolating and protecting a more secure or more trusted domain or zone from one that is less trusted or less secure. These are natural functions to expect of a firewall, for example.

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.

Host-based Intrusion Detection System (HIDS)

A HIDS monitors activity on a single computer, including process calls and information recorded in system, application, security, and host-based firewall logs. It can often examine events in more detail than a NIDS can, and it can pinpoint specific files compromised in an attack. It can also track processes employed by the attacker. A benefit of HIDSs over NIDSs is that HIDSs can detect anomalies on the host system that NIDSs cannot detect.

For example, a HIDS can detect infections where an intruder has infiltrated a system and is controlling it remotely. HIDSs are more costly to manage than NIDSs because they require administrative attention on each system, whereas NIDSs usually support centralized administration. A HIDS cannot detect network attacks on other systems.

Network Intrusion Detection System (NIDS)

A NIDS monitors and evaluates network activity to detect attacks or event anomalies.

It cannot monitor the content of encrypted traffic but can monitor other packet details. A single NIDS can monitor a large network by using remote sensors to collect data at key network locations that send data to a central management console. These sensors can monitor traffic at routers, firewalls, network switches that support port mirroring, and other types of network taps.

A NIDS has very little negative effect on the overall network performance, and when it is deployed on a single-purpose system, it doesn’t adversely affect performance on any other computer. A NIDS is usually able to detect the initiation of an attack or ongoing attacks, but they can’t always provide information about the success of an attack. They won’t know if an attack affected specific systems, user accounts, files, or applications.

10. Security Information and Event Management (SIEM)

Security management involves the use of tools that collect information about the IT environment from many disparate sources to better examine the overall security of the organization and streamline security efforts.

These tools are generally known as security information and event management (or SI-E-M, pronounced "SIM") solutions. The general idea of a SIEM solution is to gather log data from various sources across the enterprise to better understand potential security concerns and apportion resources accordingly. SIEM systems can be used along with other components (defense-in-depth) as part of an overall information security program.

11.Preventing Threat

basic steps you can take that help reduce the risk of many types of threat:

1. 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.

2. 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.

3. Use intrusion detection and prevention systems. Intrusion detection and prevention systems observe activity, attempt to detect threats, and provide alerts. They can often block or stop attacks.

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

5. Use up-to-date anti-malware software. A primary countermeasure is anti-malware software.

Antivirus

The use of antivirus products is strongly encouraged as a security best practice and is a requirement for compliance with the Payment Card Industry Data Security Standard (PCI DSS). There are several antivirus products available, and many can be deployed as part of an enterprise solution that integrates with several other security products. 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.

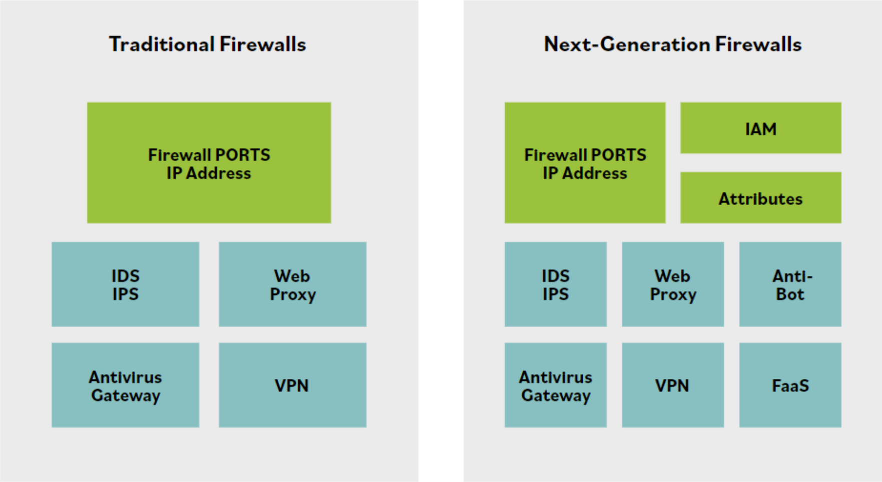
Scans

Here is an example scan from Zenmap showing open ports on a host. 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.

Firewalls

In building construction or vehicle design, a firewall is a specially built physical barrier that prevents the spread of fire from one area of the structure to another or from one compartment of a vehicle to another. Early computer security engineers borrowed that name for the devices and services that isolate network segments from each other as a security measure. As a result, firewalling refers to the process of designing, using, or operating different processes in ways that isolate high-risk activities from lower-risk ones. Firewalls enforce policies by filtering network traffic based on a set of rules. While a firewall should always be placed at internet gateways, other internal network considerations and conditions determine where a firewall would be employed, such as network zoning or segregation of different levels of sensitivity.

Firewalls have rapidly evolved over time to provide enhanced security capabilities. This growth in capabilities can be seen in the graphic below, which contrasts an oversimplified view of traditional and next-generation firewalls. It integrates a variety of threat management capabilities into a single framework, including proxy services, intrusion prevention services (IPS), and tight integration with the identity and access management (IAM) environment to ensure only authorized users are permitted to pass traffic across the infrastructure. While firewalls can manage traffic at Layers 2 (MAC addresses), 3 (IP ranges), and 7 (application programming interface (API) and application firewalls), the traditional implementation has been to control traffic at Layer 4.



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 Centers

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. The facility wiring infrastructure is integral to overall information system security and reliability. Protecting access to the physical layer of the network is important in minimizing intentional or unintentional damage. Proper protection of the physical site must address these sorts of security challenges.

1. Data Center/Closets

Data centers and wiring closets may include the following:

- Phone, network, special connections
- ISP or telecommunications provider equipment
- Servers
- Wiring and/or switch components

2. Heating, Ventilation, and Air Conditioning (HVAC) / Environmental

High-density equipment and equipment within enclosed spaces requires adequate cooling and airflow. Well-established standards for the operation of computer equipment exist, and equipment is tested against these standards. For example, the recommended range for optimized maximum uptime and hardware life is from 64° to 81°F (18° to 27°C), and it is recommended that a rack have three temperature sensors, positioned at the top, middle, and bottom of the rack, to measure the actual operating temperature of the environment. Proper management of data center temperatures, including cooling, is essential.

Cooling is not the only issue with airflow: Contaminants like dust and noxious fumes require appropriate controls to minimize their impact on equipment. Monitoring for water or gas leaks, sewer overflow, or HVAC failure should be integrated into the building control environment, with appropriate alarms to signal to organizational staff. Contingency planning to respond to the warnings should prioritize the systems in the building, so the impact of a major system failure on people, operations, or other infrastructure can be minimized.

3. Power

Data centers and information systems in general consume a tremendous amount of electrical power, which needs to be delivered both constantly and consistently. Wide fluctuations in the quality of power affect system lifespan, while disruptions in supply completely stop system operations.

Power at the site is always an integral part of data center operations. Regardless of fuel source, backup generators must be sized to provide for the critical load (the computing resources) and the supporting infrastructure. Similarly, battery backups must be properly sized to carry the critical load until generators start and stabilize. As with data backups, testing is necessary to ensure the failover to alternate power works properly.

4. Fire Suppression

For server rooms, appropriate fire detection/suppression must be considered based on the size of the room, typical human occupation, egress routes, and risk of damage to equipment.

For example, water used for fire suppression would cause more harm to servers and other electronic components. Gas-based fire suppression systems are more friendly to the electronics, but can be toxic to humans.

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

Memorandum of Understanding (MOU) Memorandum of Agreement (MOA)

Some organizations seeking to minimize downtime and enhance BC (Business Continuity) and DR (Disaster Recovery) capabilities will create agreements with other, similar organizations. They agree that if one of the parties experiences an emergency and cannot operate within their own facility, the other party will share its resources and let them operate within theirs to maintain critical functions. These agreements often include competitors, because their facilities and resources meet the needs of their particular industry.

For example, Hospital A and Hospital B are competitors in the same city. The hospitals create an agreement with each other: if something bad happens to Hospital A (e.g., a fire, flood, bomb threat, loss of power), that hospital can temporarily send personnel and systems to work inside Hospital B to stay in business during the interruption, and Hospital B can relocate to Hospital A, if Hospital B has a similar problem. The hospitals have decided that they are not going to compete based on safety and security—they are going to compete on service, price, and customer loyalty. This way, they protect themselves and the healthcare industry as a whole.

These agreements are called joint operating agreements (JOA), memoranda of understanding (MOU), or memoranda of agreement (MOA). Sometimes these agreements are mandated by regulatory requirements, or they might be part of the administrative safeguards instituted by an entity within the guidelines of its industry. The difference between an MOA or MOU and a service-level agreement (SLA) is that an MOU is more directly related to what can be done with a system or the information.

The service-level agreement goes down to the granular level. For example, if you are outsourcing the IT services, then you will need two full-time technicians readily available, at least from Monday through Friday during business hours.

With cloud computing, you need access to the information in the backup systems within 10 minutes. An SLA specifies the more intricate aspects of the services. We must be cautious when outsourcing cloud-based services because we must understand exactly what we are agreeing to. If the SLA promises 100% accessibility to information, is the access directly to you at the moment, or is it access to their website or through their portal when they open on Monday? That's where you'll rely on your legal team, who can supervise and review the conditions carefully before you sign on the dotted line.

Cloud

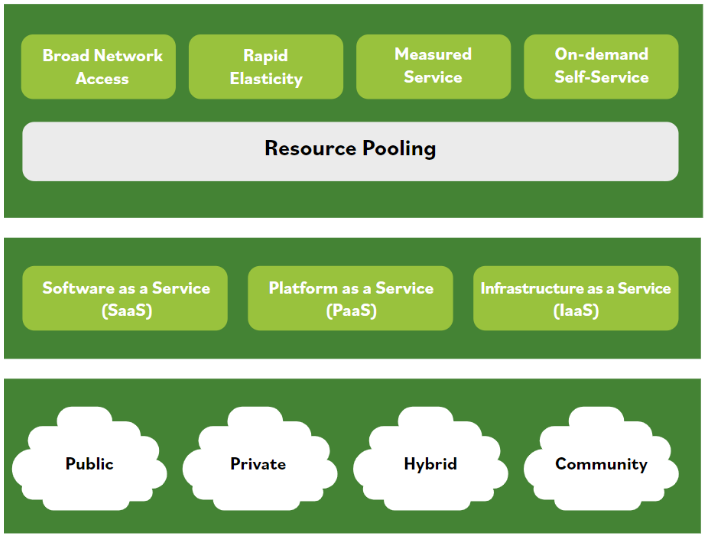
Cloud computing is usually associated with an internet-based set of computing resources, and typically sold as a service provided by a cloud service provider (CSP).

Cloud computing is similar to the electrical or power grid. It is provisioned in a geographic location and is sourced using an electrical means that is not necessarily obvious to the consumer. However, when you want electricity, it's available via a common standard interface, and you pay only for what you use.

Cloud computing is scalable, elastic, and easy to use for the provisioning and deployment of Information Technology (IT) services. There are various definitions of what cloud computing means per leading standards, including NIST's. This NIST definition is commonly used around the globe, cited by professionals to clarify what the term "cloud" means:

"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



Broad Network Access

Rapid Elasticity

Measured Service

On-demand Self-Service

Resource Pooling

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

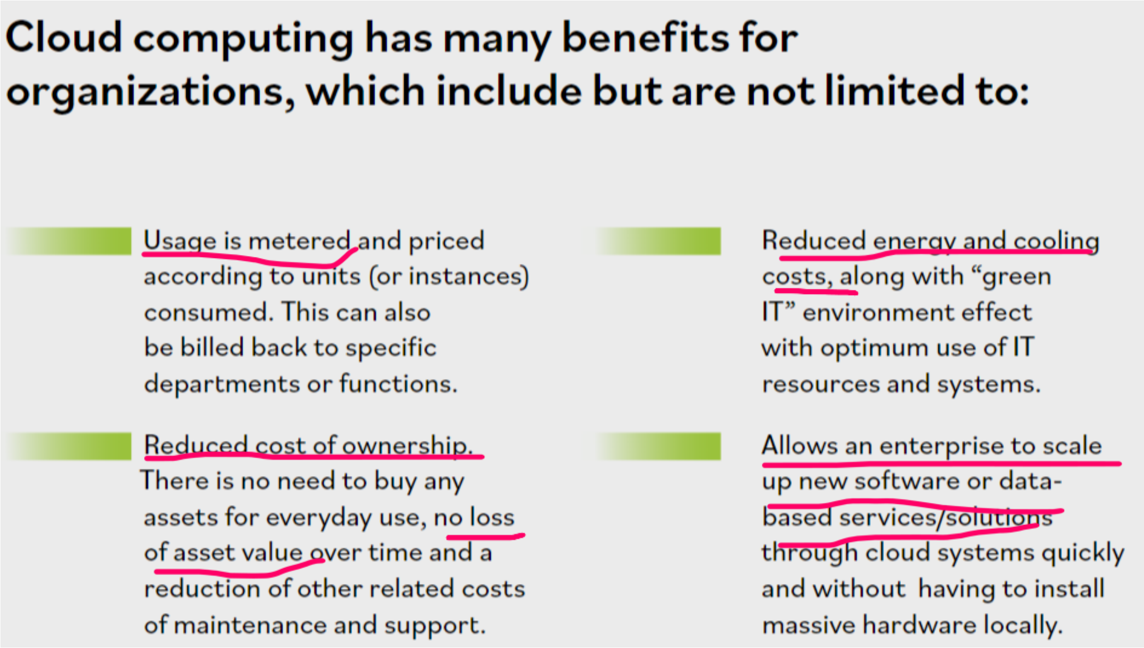
Public

Private

Hybrid

Community

Cloud computing refers to on-demand access to computing resources available from almost anywhere, and cloud computing resources are highly available and easily scalable. Organizations typically lease cloud-based resources from outside the organization.



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 Model

There are varying levels of responsibility for assets depending on the service model. This includes maintaining the assets, ensuring they remain functional, and keeping the systems and applications up to date with current patches.

IaaS - (Infrastructure as a Service)

Access to fundamental computer resources

The vendor provides infrastructure up to the OS; the customer adds the OS and up.

The Infrastructure as a Service (IaaS) model provides customers with fundamental computing resources (such as processing, storage, or networks) where the consumer is able to deploy and run arbitrary software,and also to choose the operating system

Infrastructure as a Service (IaaS) provides the capability to provision processing, storage, networks, and other fundamental computing resources

Infrastructure as a Service (IaaS) is a cloud service model that allows the customer to manage the computing resources (including the operating systems).

PaaS - (Platform as a Service)

The vendor provides pre-configured OSs, then the customer adds all programs and applications.

In Platform as a Service (PaaS), the cloud customer does not manage or control the underlying cloud infrastructure (wnich includes the network, servers, operating systems, and storage) but has control over the deployed applications and libraries.

.Platform as a Service (PaaS) enables the provisioning of applications, programming libraries, services, and tools that the provider supports. Unlike IaaS, consumers do not control their underlying cloud infrastructure (including operating systems and storage).

Platform as a Service (PaaS) is a service model that provides a platform for building, deploying and managing applications; however, like SaaS, it does not offer the ability to access the underlying infrastructure (including the operating system). An SLA is simply a service-level agreement (and not a cloud service deployment model)

SaaS - (Software as a Service)

Less responsibility over infrastructure

The vendor provides the OS and applications/programs. Either the customer interacts with the software

In Software as a Service (SaaS), consumers may control user-specific application configuration settings, but neither the underlying application logic nor the infrastructure.

Software as a Service (SaaS) is a model that provides customers with access to software applications (typically on a subscription-based or pay-per-use model) but does not allow them to access the underlying infrastructure.

Both Software as a Service (SaaS) and Function as a Service (FaaS) models abstract away from underlying computing infrastructure, thereby allowing providers to focus on providing end users with applications, rather than worrying about how their underlying infrastructure functions

In the Function as a Service (FaaS) model, cloud customers deploy application-level functionality (typically as microservices) and are charged only when this functionality is executed

Deployment Model

There are four cloud deployment models. The cloud deployment model also affects the breakdown of responsibilities of the cloud-based assets

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

It seems there are some formatting issues in the text you provided. I'll correct them and present the text exactly as you've written it, without changing any words.

Public

Public clouds are commonly referred to as clouds for the public user. It is easy to access a public cloud. There is no real mechanism, other than applying for and paying for the cloud service. It is open to the public and is, therefore, a shared resource that many people can use as part of a resource pool. A public cloud deployment model includes assets available for any consumers to rent or lease and is hosted by an external cloud service provider (CSP). Service-level agreements can be effective at ensuring the CSP provides the cloud-based services at a level acceptable to the organization.

Shared tenancy – A company builds massive infrastructures and rents it out to anyone who wants it. (Amazon AWS, Microsoft, Google, IBM).

Private

Private clouds begin with the same technical concept as public clouds, except that instead of being shared with the public, they are generally developed and deployed for a private organization that builds its own cloud. Organizations can create and host private clouds using their own resources. Therefore, this deployment model includes cloud-based assets for a single organization. As such, the organization is responsible for all maintenance. However, an organization can also rent resources from a third party and split maintenance requirements based on the service model (SaaS, PaaS, or IaaS). Private clouds provide organizations and their departments private access to the computing, storage, networking, and software assets that are available in the private cloud.

Organizations build and run their own cloud infrastructure (or they pay someone to do it for them).

Hybrid

The cloud deployment model where a company has resources on-premise and in the cloud

A hybrid cloud deployment model is created by combining two forms of cloud computing deployment models, typically a public and private cloud. Hybrid cloud computing is gaining popularity with organizations by providing them with

the ability to retain control of their IT environments, conveniently allowing them to use public cloud service to fulfill non-mission-critical workloads, and taking advantage of flexibility, scalability, and cost savings. Important drivers or benefits of hybrid cloud deployments include: Retaining ownership and oversight of critical tasks and processes related to technology, Reusing previous investments in technology within the organization, Control over most critical business components and systems, and cost-effective means to fulfilling noncritical business functions.

A mix of Private and Public Cloud Computing. An organization can choose to use Private Cloud for sensitive information and Public Cloud for non-sensitive data.

Community

Community clouds can be either public or private.

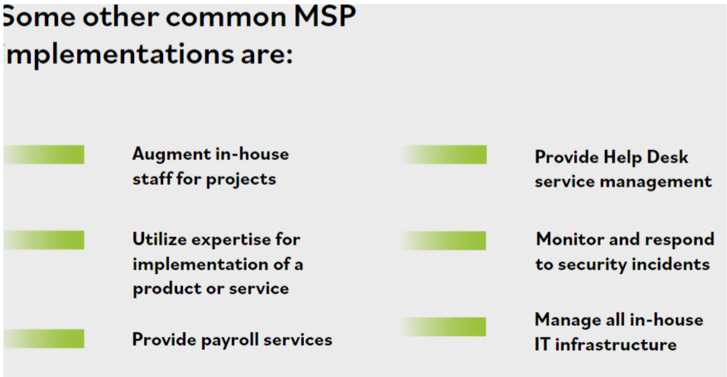
What makes them unique is that they are generally developed for a particular community. An example could be a public community cloud focused primarily on organic food, or maybe a community cloud focused specifically on financial services. The idea behind the community cloud is that people of like minds or similar interests can get together, share IT capabilities and services, and use them in a way that is beneficial for the particular interests that they share.

A community cloud is an infrastructure where multiple organizations share resources and services based on common technological and regulatory necessities. Multi-tenancy refers to a context where several of a cloud vendor's customers share the same computing resources.

Managed Service Provider (MSP)

A managed service provider (MSP) is a company that manages information technology assets for another company. Small and medium-sized businesses commonly outsource part or all of their information technology functions to an MSP to manage day-to-day operations or to provide expertise in areas the company does not have. Organizations may also use an MSP to provide network

and security monitoring and patching services. Today, many MSPs offer cloud-based services augmenting SaaS solutions with active incident investigation and response activities. One such example is a managed detection and response (MDR) service, where a vendor monitors firewall and other security tools to provide expertise in triaging events.



Some other common MSP implementations are:

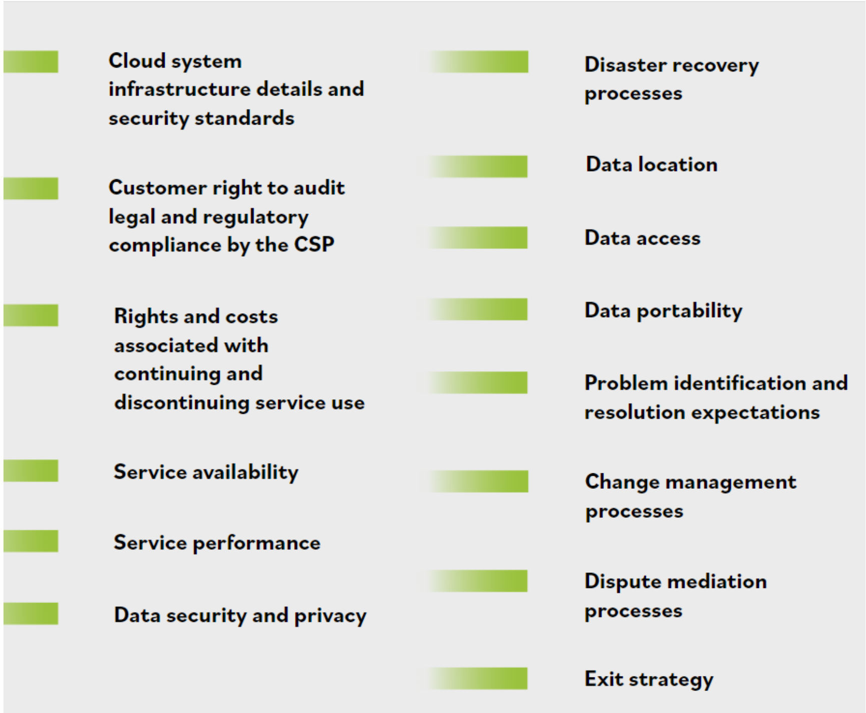
- Augment in-house staff for projects
- Utilize expertise for implementation of a product or service
- Provide payroll services
- Provide Help Desk service management
- Monitor and respond to security incidents
- Manage all in-house IT infrastructure

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. It characterizes the quality of the cloud services delivered in terms of a set of measurable properties specific to cloud computing (business and technical) and a given set of cloud computing roles (cloud service customer, cloud service provider, and related sub-roles).

Think of a rule book and legal contract—that combination is what you have in a service-level agreement (SLA). Let us not underestimate or downplay the importance of this document/agreement. In it, the minimum level of service, availability, security, controls, processes, communications, support, and many other crucial business elements are stated and agreed to by both parties. The purpose of an SLA is to document specific parameters, minimum service levels, and remedies for any failure to meet the specified requirements. It should also affirm data ownership and specify data return and destruction details.

Other 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:

The objective of network design is to satisfy data communication requirements and achieve the result of efficient overall performance.

Network 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.

Demilitarized 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.

Virtual Local Area Network (VLAN)

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

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.

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.

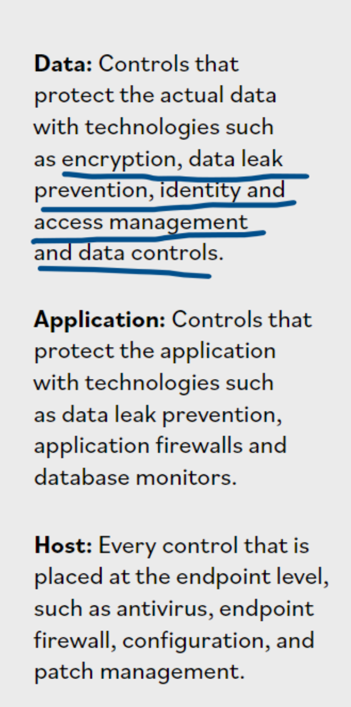
Network Access Control (NAC)

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

Defense in Depth

Defense in depth uses a layered approach when designing the security posture of an organization. Think about a castle that holds the crown jewels. The jewels will be placed in a vaulted chamber in a central location watched over by security guards. The castle is built around the vault with additional layers of security—soldiers, walls, and a moat. The same approach is true when designing the logical security of a facility or system. Using layers of security will deter many attackers and encourage them to focus on other, easier targets.

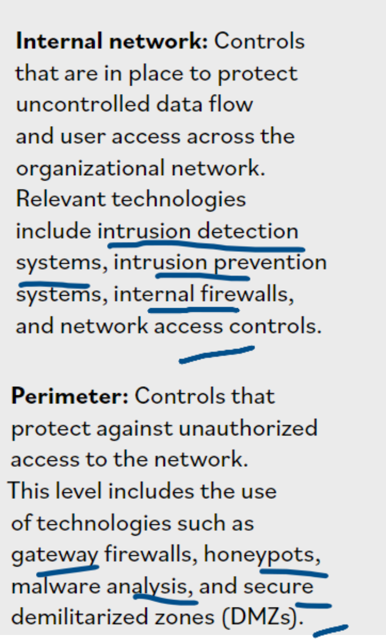
Defense in depth provides more of a starting point for considering all types of controls—administrative, technological, and physical—that empower insiders and operators to work together to protect their organization and its systems. Here are some examples that further explain the concept of defense in depth:



Data: Controls that protect the actual data with technologies such as encryption, data leak prevention, identity and access management and data controls.

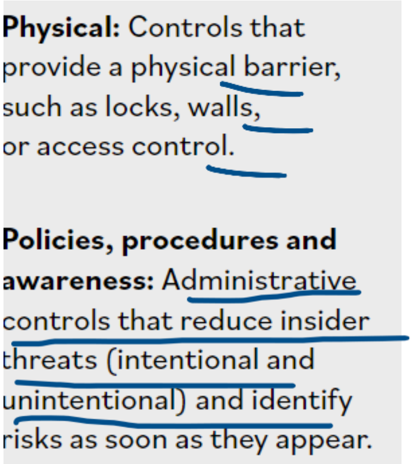
Application: Controls that protect the application with technologies such as data leak prevention, application firewalls and database monitors.

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.

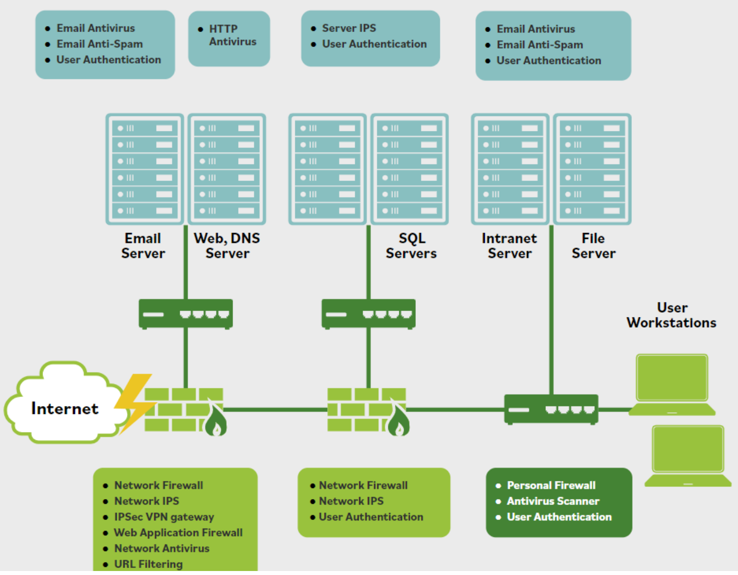
Zero Trust

This concept recognizes that once inside a trust-but-verify environment, a user has perhaps unlimited capabilities to roam around, identify assets and systems, and potentially find exploitable vulnerabilities. Placing a greater number of firewalls or other security boundary control devices throughout the network increases the number of opportunities to detect a troublemaker before harm is done. Many enterprise architectures are pushing this to the extreme of microsegmenting their internal networks, which enforces frequent reauthentication of a user ID, as depicted in this image.

Consider a rock music concert. If traditional perimeter controls, such as firewalls, are employed, you would show your ticket at the gate and have free access to the venue, including backstage where the real rock stars are.

In a zero-trust environment, additional checkpoints are added. Your identity (ticket) is validated to access the floor-level seats, and again to access the backstage area. Your credentials must be valid at all three levels to meet the stars of the show.

Zero trust is an evolving design approach that recognizes 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.



Network AccessControl (NAC)

An organization’s network is perhaps one of its most critical assets. As such, it is vital that you both know and control access to it, both from insiders (e.g., employees, contractors) and outsiders (e.g., customers, corporate partners, vendors). You must see who and what is attempting to make a network connection.

At one time, network access was limited to internal devices. Gradually, that was extended to remote connections, although initially, those were the exceptions rather than the norm. This started to change with the concepts of bring your own device (BYOD) and Internet of Things (IoT).

Considering just IoT for a moment, it is important to understand the range of devices that might be found within an organization. They include heating, ventilation, and air conditioning (HVAC) systems that monitor the ambient temperature and adjust the heating or cooling levels automatically, or air monitoring systems, to security systems, sensors, and cameras, right down to vending and coffee machines. Look around your own environment and you will quickly see their scale of use.

Having identified the need for a NAC solution, you need to identify what capabilities a solution may provide. As you know, everything begins with a policy. The organization's access control policies and associated security policies should be enforced via the NAC devices. Remember, of course, that an access control device only enforces a policy and doesn't create one. The NAC device will provide the network visibility needed for access security and may later be used for incident response. Aside from identifying connections, it should also provide isolation for noncompliant devices within a quarantined network and provide a mechanism to "fix" the noncompliant elements, such as turning on endpoint protection. In short, the goal is to ensure that all devices wishing to join the network do so only when they comply with the requirements laid out in the organization's policies. This visibility will encompass internal users as well as any temporary users such as guests or contractors, and any devices brought with them into the organization.

Let's consider some possible use cases for NAC deployment:

- Medical devices

- IoT devices
- BYOD/mobile devices (e.g., laptops, tablets, smartphones)
- Guest users and contractors

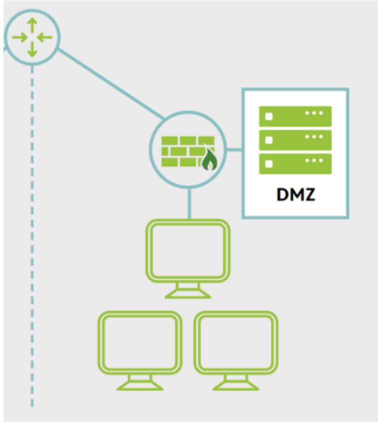
It is critically important that all mobile devices, regardless of their owner, go through an onboarding process, ideally each time a network connection is made, and that the device is identified and interrogated to ensure the organization's policies are met.

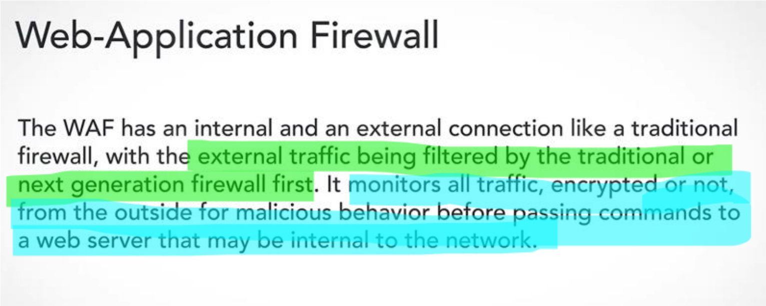
At its simplest form, Network Access Control, or NAC, is a way to prevent unwanted devices from connecting to a network. Some NAC systems allow for the installation of required software on the end user's device to enforce device compliance to policy prior to connecting.

Network Segmentation (Demilitarized Zone)

Network segmentation is an effective way to achieve defense in depth for distributed or multitiered applications. The use of a demilitarized zone (DMZ), for example, is a common practice in security architecture.

With a DMZ, host systems that are accessible through the firewall are physically separated from the internal network by means of secured switches or by using an additional firewall to control traffic between the web server and the internal network. Application DMZs (or semi-trusted networks) are frequently used today to limit access to application servers to those networks or systems that have a legitimate need to connect.





Web-Application Firewall

The WAF has an internal and an external connection like a traditional firewall, with the external traffic being filtered by the traditional or next generation firewall first. It monitors all traffic, encrypted or not, from the outside for malicious behavior before passing commands to a web server that may be internal to the network.

Segmentation for Embedded Systems and IoT

An embedded system is a computer implemented as part of a larger system. The embedded system is typically designed around a limited set of specific functions in relation to the larger product of which it is a component.

Embedded system-> control something physical

Examples of embedded systems include network-attached printers, smart TVs, HVAC controls, smart appliances, smart thermostats, and medical devices.

Network-enabled devices are any type of portable or non-portable device that has native network capabilities. This generally assumes the network in question is a wireless type of network, typically provided by a mobile telecommunications company. Network-enabled devices include smartphones, mobile phones, tablets, smart TVs or streaming media players (e.g., Roku Player, Amazon Fire TV, Google Android TV/Chromecast), network-attached printers, game systems, and more.

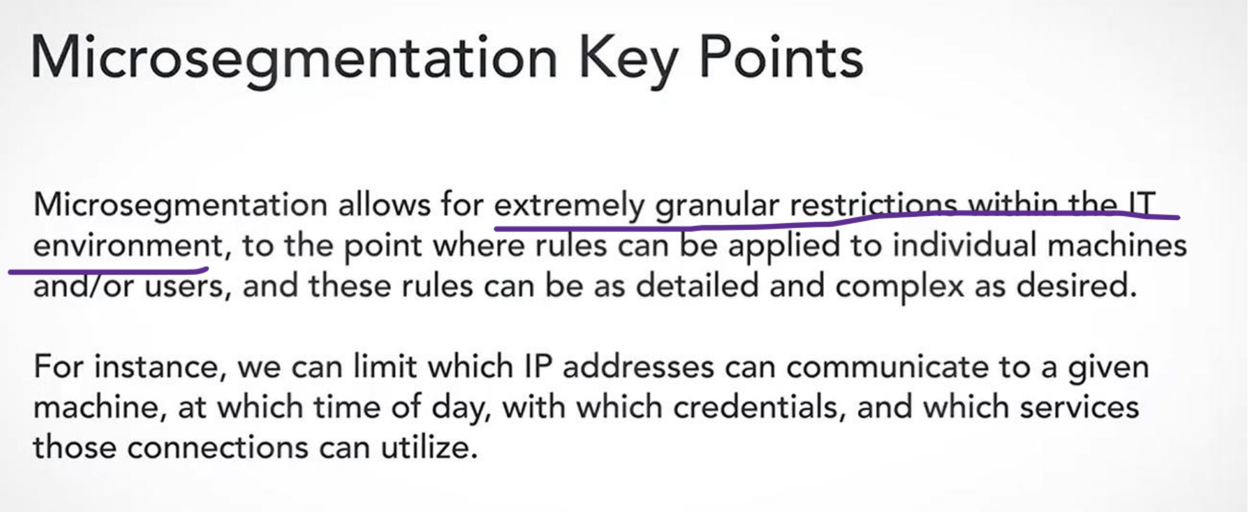
The Internet of Things (IoT) is the collection of devices that can communicate over the internet with one another or with a control console to affect and monitor the real world. IoT devices might be labeled as smart devices or smart-home equipment. Many of the ideas of industrial environmental control found

in office buildings are finding their way into more consumer-available solutions for small offices or personal homes.

Embedded systems and network-enabled devices that communicate with the internet are considered IoT devices and need special attention to ensure that communication is not used in a malicious manner.

Because an embedded system is often in control of a mechanism in the physical world, a security breach could cause harm to people and property. Since many of these devices have multiple access routes, such as ethernet, wireless, or Bluetooth, special care should be taken to isolate them from other devices on the network. You can impose logical network segmentation with switches using VLANs, or through other traffic-control means, including MAC addresses, IP addresses, physical ports, protocols, or application filtering, routing, and access control management. Network segmentation can be used to isolate IoT environments.

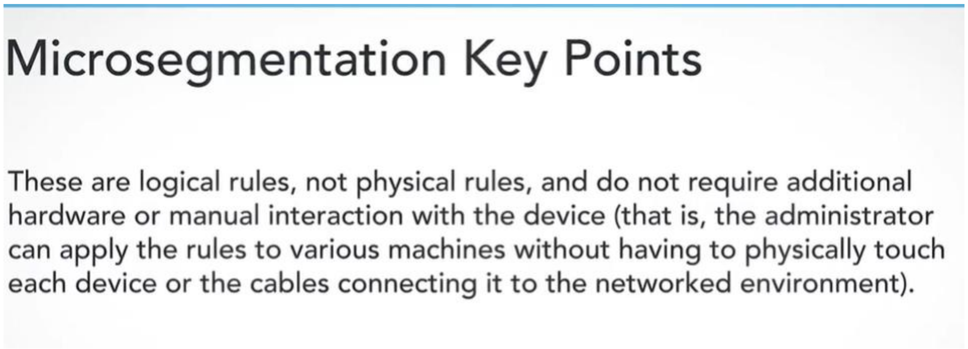
If these devices are properly segmented, or separated, on the network from corporate servers and other corporate networking, a compromise on an IoT device or a compromised embedded system will not be able to access those corporate data and systems.



Microsegmentation Key Points

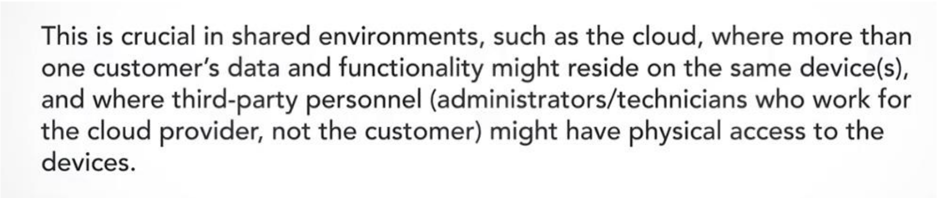
Microsegmentation allows for extremely granular restrictions within the IT environment, to the point where rules can be applied to individual machines and/or users, and these rules can be as detailed and complex as desired.

For instance, we can limit which IP addresses can communicate to a given machine, at which time of day, with which credentials, and which services those connections can utilize.

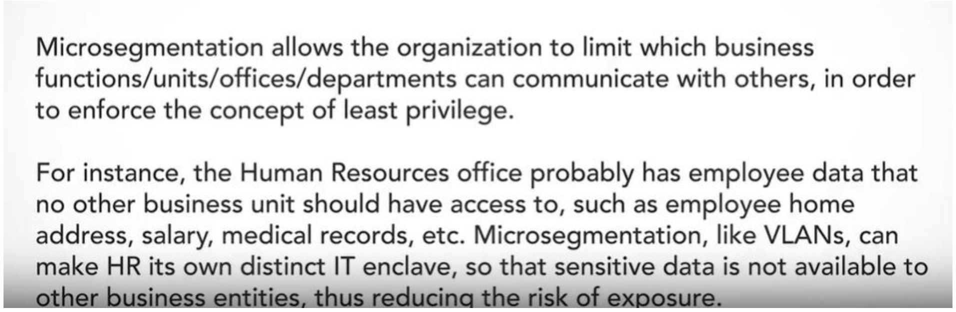


Microsegmentation Key Points

These are logical rules, not physical rules, and do not require additional hardware or manual interaction with the device (that is, the administrator can apply the rules to various machines without having to physically touch each device or the cables connecting it to the networked environment).

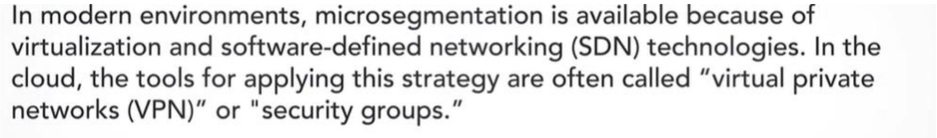


This is crucial in shared environments, such as the cloud, where more than one customer's data and functionality might reside on the same device(s), and where third-party personnel (administrators/technicians who work for the cloud provider, not the customer) might have physical access to the devices.



Microsegmentation allows the organization to limit which business functions/units/offices/departments can communicate with others, in order to enforce the concept of least privilege.

For instance, the Human Resources office probably has employee data that no other business unit should have access to, such as employee home address, salary, medical records, etc. Microsegmentation, like VLANs, can make HR its own distinct IT enclave, so that sensitive data is not available to other business entities, thus reducing the risk of exposure.



In modern environments, microsegmentation is available because of virtualization and software-defined networking (SDN) technologies. In the cloud, the tools for applying this strategy are often called "virtual private networks (VPN)" or "security groups."