L4 Network Security

Module 1: Understand Computer Networking

Domain D4.1.1, D4.1.2

What is Networking

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

To properly establish secure data communications, it is important to explore all of the technologies involved in computer communications. From hardware and software to protocols and encryption and beyond, there are many details, standards and procedures to be familiar with.

Types of Networks

There are two basic types of networks:

- Local area network (LAN) - A local area network (LAN) is a network typically spanning a single floor or building. This is commonly a limited geographical area.
- Wide area network (WAN) - Wide area network (WAN) is the term usually assigned to the long-distance connections between geographically remote networks.

Network Devices

- **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 routers.
- You might consider using **a switch**, or what is also known as an 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. Offering greater efficiency for traffic delivery and improving the overall throughput of data, switches are smarter than hubs, but not as smart as routers. Switches can also create separate broadcast domains when used to create VLANs, which will be discussed later.
- **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.
- **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 lists.

- 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.

- **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.

Other Networking Terms

- 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 cables.

- 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.

Networking Models

Many different models, architectures and standards exist that provide ways to interconnect different hardware and software systems with each other for the purposes of sharing information, coordinating their activities and accomplishing joint or shared tasks.

Computers and networks emerge from the integration of communication devices, storage devices, processing devices, security devices, input devices, output devices, operating systems, software, services, data and people.

Translating the organization’s security needs into safe, reliable and effective network systems needs to start with a simple premise. 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 (representation of data at L3 of OSI model) as the basis of communication
- Standardize routing, addressing and control
- Allow layers beyond internetworking to add functionality
- Be vendor-agnostic, scalable and resilient

In the most basic form, a network model has at least two layers:

- UPPER LAYER APPLICATION: also known as the host or application layer, is responsible for managing the integrity of a connection and controlling the session as well as establishing, maintaining and terminating communication sessions between two computers. It is also responsible for transforming data received from the Application Layer into a format that any system can understand. And finally, it allows applications to communicate and determines whether a remote communication partner is available and accessible.
    - APPLICATION
        - APPLICATION 7
        - PRESENTATION 6
        - SESSION 5
- LOWER LAYER: it is often referred to as the media or transport layer and is responsible for receiving bits from the physical connection medium and converting them into a frame. Frames are grouped into standardized sizes. Think of frames as a bucket and the bits as water. If the buckets are sized similarly and the water is contained within the buckets, the data can be transported in a controlled manner. Route data is added to the frames of data to create packets. In other words, a destination address is added to the bucket. Once we have the buckets sorted and ready to go, the host layer takes over.
    - DATA TRANSPORT
        - TRANSPORT 4
        - NETWORK 3
        - DATA LINK 2
        - PHYSICAL 1

Open Systems Interconnection (OSI) Model

The OSI Model was developed to establish a common way to describe the communication structure for interconnected computer systems. The OSI model serves as an abstract framework, or theoretical model, for how protocols should function in an ideal world, on ideal hardware. Thus, the OSI model has become a common conceptual reference that is used to understand the communication of various hierarchical components from software interfaces to physical hardware.

The OSI model divides networking tasks into seven distinct layers. Each layer is responsible for performing specific tasks or operations with the goal of supporting data exchange (in other words, network communication) between two computers. The layers are interchangeably referenced by name or layer number. For example, Layer 3 is also known as the Network Layer. The layers are ordered

specifically to indicate how information flows through the various levels of communication. Each layer communicates directly with the layer above and the layer below it. For example, Layer 3 communicates with both the Data Link (2) and Transport (4) layers.

The Application, Presentation, and Session Layers (5-7) are commonly referred to simply as data. However, each layer has the potential to perform encapsulation (enforcement of data hiding and code hiding during all phases of software development and operational use. Bundling together data and methods is the process of encapsulation; its opposite process may be called unpacking, revealing, or using other terms. Also used to refer to taking any set of data and packaging it or hiding it in another data structure, as is common in network protocols and encryption.). Encapsulation is the addition of header and possibly a footer (trailer) data by a protocol used at that layer of the OSI model. Encapsulation is particularly important when discussing Transport, Network and Data Link layers (2-4), which all generally include some form of header. At the Physical Layer (1), the data unit is converted into binary, i.e., 01010111, and sent across physical wires such as an ethernet cable.

It's worth mapping some common networking terminology to the OSI Model so you can see the value in the conceptual model.

Consider the following examples:

- When someone references an image file like a JPEG or PNG, we are talking about the Presentation Layer (6).
- When discussing logical ports such as NetBIOS, we are discussing the Session Layer (5).
- When discussing TCP/UDP, we are discussing the Transport Layer (4).
- When discussing routers sending packets, we are discussing the Network Layer (3).
- When discussing switches, bridges or WAPs sending frames, we are discussing the Data Link Layer (2).

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:

7	Application		DATA					
6	Presentation	Header -->			DATA			
5	Session					DATA		

4	Transport						DATA			
3	Network							DATA		
2	Data Link								DATA	
1	Physical									DATA

Transmission Control Protocol/Internet Protocol (TCP/IP)

The OSI model wasn't the first or only attempt to streamline networking protocols or establish a common communications standard. In fact, the most widely used protocol today, TCP/IP, was developed in the early 1970s. The OSI model was not developed until the late 1970s. The TCP/IP protocol stack focuses on the core functions of networking.

	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	

The most widely used protocol suite is TCP/IP, but it is not just a single protocol; rather, it is a protocol stack comprising dozens of individual protocols. TCP/IP is a platform-independent protocol based on open standards. However, this is both a benefit and a drawback. TCP/IP can be found in just about every available operating system, but it consumes a significant amount of resources and is relatively easy to hack into because it was designed for ease of use rather than for security.

At the Application Layer, TCP/IP protocols include **Telnet**, File Transfer Protocol (**FTP**), Simple Mail Transport Protocol (**SMTP**), and Domain Name Service (**DNS**). The two primary Transport Layer protocols of TCP/IP are **TCP and UDP**. **TCP is a full-duplex connection-oriented protocol, whereas UDP is a simplex connectionless protocol**. In the Internet Layer, **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 systems. Thus, you can use ping to determine whether the remote system is online, whether the remote system is responding promptly, whether the intermediary systems are supporting communications, and the level of performance efficiency at which the intermediary systems are communicating.

- Application, Presentation and Session layers at OSI model is equivalent to Application Layer at TCP/IP, and the protocol suite is: FTP, Telnet, SNMP, LPD, TFPT, SMTP, NFS, X Window.
- Transport layer are the same between OSI model and TCP/IP model, protocol suite: TCP, UDP

- Network layer at OSI model is equivalent to Internet layer at TCP/IP model, and protocol suite is: IGMP, IP, ICMP
- Data link and Physical layer at OSI model is equivalent at Network Interface layer at TCP/IP, and protocol suite is: Ethernet, Fast Ethernet, Token Ring, FDDI

Base concepts

- Switch: A device that routes traffic to the port of a known device
- Server: A computer that provides information to other computers
- Firewall: A device that filters network traffic based on a defined set of rules
- Ethernet: A standard that defines wired communications of networked devices
- IP Address: Logical address representing the network interface
- MAC Address: Address that denotes the vendor or manufactures of the physical network interface

Internet Protocol (IPv4 and IPv6)

IPv4 provides a 32-bit address space. IPv6 provides a 128-bit address space. The first one is exhausted nowadays, but it is still used because of the NAT technology. 32 bits means 4 octets of 8 bits, which is represented in a dotted decimal notation such as 192.168.0.1, which means in binary notation 11000000 10101000 00000000 00000001

IP hosts/devices associate an address with a unique logical address. An IPv4 address is expressed as four octets separated by a dot (.), for example, 216.12.146.140. Each octet may have a value between 0 and 255. However, **0 is the network itself (not a device on that network), and 255 is generally reserved for broadcast purposes**. Each address is subdivided into two parts: **the network number and the host**. The network number assigned by an external organization, such as the Internet Corporation for Assigned Names and Numbers (ICANN), represents the organization's network. The host represents the network interface within the network.

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. **With the ever-increasing number of computers and networked devices, it is clear that IPv4 does not provide enough addresses for our needs.** To overcome this shortcoming, **IPv4 was sub-divided into public and private address ranges.** Public addresses are limited with IPv4, but this issue was addressed in part with private addressing. Private addresses can be shared by anyone, and it is highly likely that everyone on your street is using the same address scheme.

The nature of the addressing scheme established by IPv4 meant that network designers had to start thinking in terms of IP address reuse. IPv4 facilitated this in several ways, such as its creation of the private address groups; this allows every LAN in every SOHO (small office, home office) situation to use addresses such as 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

The first octet of **127 is reserved for a computer's loopback address**. Usually, the address 127.0.0.1 is used. **The loopback address is used to provide a mechanism for self-diagnosis and troubleshooting at the machine level**. This mechanism allows a network administrator to treat a local machine as if it were a remote machine and ping the network interface to establish whether it is operational.

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 2128 or 340,282
* Improved security:** IPsec is an optional part of IPv4 networks, but a mandatory component o
* Improved quality of service (QoS): This will help services obtain an appropriate share of a
```

An IPv6 address is shown as **8 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
* **fc00**:: to **fdff**:ffff:ffff:ffff:ffff:ffff:ffff:ffff are addresses reserved for interna
```

What is WiFi?

Wireless networking is a popular method of connecting corporate and home systems because of the ease of deployment and relatively low cost. 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.

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: 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 be able 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) reside 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. You'll note that in several cases a service (or protocol) may have two ports assigned, one secure and one insecure. When in doubt, systems should be implemented using the most secure version as possible 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 Ports

Some network protocols transmit information in clear text, meaning it is not encrypted and should not be used. Clear text information is subject to network sniffing. This tactic uses software to inspect packets of data as they travel across the network and extract text such as usernames and passwords. Network sniffing could also reveal the content of documents and other files if they are sent via insecure protocols. The table below shows some of the insecure protocols along with recommended secure alternatives.

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
21	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
23	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**	Telnet	22* - SSH	Secure Shell

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
	terminal is not sent in a plaintext format			
25	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	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	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	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	HyperText Transfer Protocol	443 - HTTPS	HyperText Transfer Protocol (SSL/TLS)

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
	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			
143	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	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

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
445	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
389	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

SYN, SYN-ACK, ACK

Module 2 Understand Network (Cyber) Threats and Attacks

Domain D4.1.2, D4.2.2, D4.2.3

Types 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.
- Phising: an attack that **attempts to misdirect legitimate users to malicious websites through** the abuse of **URLs or hyperlinks in emails could be considered phishing**.
- 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.
- 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).
- 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.
- 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. 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.
- 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**.
- 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.
- Advanced Persistent Threat: 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.
- 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.

- 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.
- 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.

Identify Threats and Tools Used to Prevent Them

Here are some examples of steps that can be taken to protect networks.

- 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.

Identify Threats and Tools Used to Prevent Them Continued

- Instrusion Detection System (IDS) is a form of monitoring to detect abnormal activity; it detects intrusion attempts and system failures. Identifies Threats, Do not prevent threats
- Host-based IDS (HIDS) monitors activity on a single computer. Identifies threats, Do not prevent Threats.
- Network-based IDS (NIDS) monitors and evaluates network activity to detect attacks or event anomalies. Identifies threats, Do not prevent Threats.
- SIEM gathers log data from sources across an enterprise to understand security concerns and apportion resources. Identifies threats, Do not prevent Threats.
- Anti-malware/Antivirus seeks to identify malicious software or processes. Identifies and Prevent threats.
- Scans evaluates the effectiveness of security controls. Identifies threats, Do not prevent Threats.
- Firewall filters network traffic - managers and controls network traffic and protects the network. Identifies and Prevent threats.
- Intrusion Protection System (IPS-NIPS/HIPS) is an active IDS automatically attempts to detect and block attacks before they reach target systems. Identifies and Prevent threats.

Intrusion Detection System (IDS)

An intrusion occurs when an attacker is able to bypass or thwart security mechanisms and gain access to an organization's resources. 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**. An IDS is intended as part of a **defense-in-depth security plan**. **IDSs can** recognize attacks that come from external

connections and attacks that spread internally. 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.

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.

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 S-I-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.

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.

Antivirus: it is a requirement for **compliance with the Payment Card Industry Data Security Standard (PCI DSS)**. 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: 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: 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. **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**. Traditional firewalls have PORTS IP Address, IDS/IPS, Antivirus Gateway, WebProxy, VPN; NG Firewalls have PORTS IP Address, IAM Attributes, IDS/IPS, WebProxy, Anti-Bot, Antivirus Gateway, VPN, FaaS.

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).

Module 3 Understand Network Security Infrastructure

Domain D4.3.1, D4.3.2

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**.

- **Data Center/Closets**: 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. Data centers and wiring closets may include the following: Phone, network, special connections; ISP or telecommunications provider equipment; Servers; Wiring and/or switch components.

- **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 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.

- 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.

- 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.

Which of the following is typically associated with an on-premises data center? **Fire suppression is associated**, **HVAC is associated**, **Power is associated** are all associated with an on-premises data center.

Which of the following is not a source of redundant power? **HVAC is not a source of redundant power**, but it is something that needs to be protected by a redundant power supply, which is what the other three options will provide. What happens if the HVAC system breaks and equipment gets too hot? If the temperature in the data center gets too hot, then there is a risk that the server will shut down or fail sooner than expected, which presents a risk that data will be lost. So that is another system that requires redundancy in order to reduce the risk of data loss. But it is not itself a source of redundant power.

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 in order to maintain critical functions. These agreements often even include competitors, because their facilities and resources meet the needs of their particular industry.

These agreements are called joint operating agreements (JOA) or memoranda of understanding (MOU) or memoranda of agreement (MOA). Sometimes these agreements are mandated by regulatory requirements, or they might just be part of the administrative safeguards instituted by an entity within the guidelines of its industry.

The difference between an MOA or MOU and an SLA is that a Memorandum of Understanding 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 I'm outsourcing the IT services, then I will need to have two full-time technicians readily available, at least from Monday through Friday from eight to five. With cloud computing, I need to have access to the information in my backup systems within 10 minutes. An SLA specifies the more intricate aspects of the services.

We must be very cautious when outsourcing with cloud-based services, because we have to make sure that we understand exactly what we are agreeing to. If the SLA promises 100 percent 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 the dotted line at the bottom.

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)**. **It is a very scalable, elastic and easy-to-use "utility" for the provisioning and deployment of Information Technology (IT) services**. There are various definitions of what cloud computing means according to the leading standards, **including NIST**. This NIST definition is commonly used around the globe, cited by professionals and others alike 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

Cloud Characteristics

Cloud-based assets include any resources that an organization accesses using cloud computing. **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:

- Resource Pooling
    - Broadnetwork Access
    - Rapid Elasticity
    - Measured Service
    - On-Demand Self-Service
- 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

Some cloud-based services only provide data storage and access. When storing data in the cloud, organizations must ensure that security controls are in place to prevent unauthorized access to the data. 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. In some cases, the cloud service provider is responsible for these steps. In other cases, the consumer is responsible for these steps.

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

- Services
    - Software As Service (SaaS): A cloud provides access to **software applications such as email or office productivity tools**. SaaS **is a distributed model** where software applications are hosted by a vendor or cloud service provider and made available to customers over network resources. SaaS has many benefits for organizations, which include but are not limited to: **Ease of use and limited/minimal administration**. **Automatic updates and patch management**. **The user will always be running the latest version and most up-to-date deployment of the software release, as well as any relevant security updates, with no manual patching required**. Standardization and compatibility. All users will have the same version of the software release.
    - Platform As Service (PaaS): **A cloud provides an environment for customers to use to build and operate their own software**. PaaS is **a way for customers to rent hardware, operating systems, storage and network capacity over the internet from a cloud service provider**. The service delivery model allows customers **to rent virtualized servers and associated services for running existing applications or developing and testing new ones**. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application-hosting environment configurations. **A PaaS cloud provides a toolkit for conveniently developing, deploying and administering application software that is structured to support large numbers of consumers, process very large quantities of data and potentially be accessed from any point on the internet**. PaaS clouds will typically provide a set of software building blocks and a set of development tools such

as programming languages and supporting run-time environments that facilitate the construction of high-quality, scalable applications. Additionally, PaaS clouds will typically provide tools that assist with the deployment of new applications. In some cases, deploying a new software application in a PaaS cloud is not much more difficult than uploading a file to a web server. PaaS clouds will also generally provide and maintain the computing resources (e.g., processing, storage and networking) that consumer applications need to operate. PaaS clouds provide many benefits for developers, including that the operating system can be changed and upgraded frequently, along with associated features and system services.

- Infrastrucuture As Service (IaaS): A cloud provides network access **to traditional computing resources such as processing power and storage**. IaaS models **provide basic computing resources to consumers**. This includes **servers, storage, and in some cases, networking resources.** Consumers install operating systems and applications and perform all required maintenance on the operating systems and applications. Although the consumer has use of the related equipment, the cloud service provider retains ownership and is ultimately responsible for hosting, running and maintenance of the hardware. IaaS is also referred to as hardware as a service by some customers and providers. IaaS has a number of benefits for organizations, which include but are not limited to: Ability to scale up and down infrastructure services based on actual usage. This is particularly useful and beneficial where there are significant spikes and dips within the usage curve for infrastructure. Retain system control at the operating system level.

Deployment Models

Clouds * Public: what we commonly **refer to as the cloud for the public user**. **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 will be able to 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.

```
* Private: it begins with the same technical concept as public clouds, **except that instead o

* Hybrid: it is created by **combining two forms of cloud computing deployment models, typical

* Community: it can be either public or private. **What makes them unique is that they are gen
```

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 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

- **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.
- **A DMZ, which stands for Demilitarized Zone,** 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.
- **VLANs, which stands for Virtual Private Network**, are created by **switches to logically segment a network without altering its physical topology**.

- **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** uses multiple **types of access controls in literal or theoretical layers** to help an organization avoid a monolithic security stance.
- **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 guarded by security guards. The castle is built around the vault with additional layers of security—soldiers, walls, 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**.

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 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 networks are often **microsegmented networks, with firewalls at nearly every connecting point**. Zero trust encapsulates information assets, the services that apply to them and their security

properties. **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 re-authentication of a user ID**.

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.

Network Access Control (NAC)

We need to be able to 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.

The organization's **access control policies and associated security policies should be enforced via the NAC device(s). 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 be able to 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 policies. This visibility will encompass internal users as well as any temporary users such as guests or contractors, etc., and any devices they may bring with them into the organization.

Let's consider some possible use cases for NAC deployment: Medical devices; IoT devices; BYOD/mobile devices (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 being met.

Network Segmentation (Demilitarized Zone (DMZ))

Network segmentation is also **an effective way to achieve defense in depth for distributed or multi-tiered 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.

Segmentation for Embedded Systems and IoT

Network-enabled devices are any type of portable or nonportable 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**, network-attached printers, game systems, and much 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 in order 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, Bluetooth, etc., 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.

Microsegmentation

The toolsets of current adversaries are polymorphic in nature and allow threats to bypass static security controls. **Modern cyberattacks take advantage of traditional security models to move easily between systems within a data center**. Microsegmentation aids in protecting against these threats. A fundamental design requirement of **microsegmentation is to understand the protection requirements for traffic within a data center and traffic to and from the internet traffic flows**.

When organizations avoid infrastructure-centric design paradigms, they are more likely to become more efficient at service delivery in the data center and become apt at detecting and preventing advanced persistent threats.

Virtual Local Area Network (VLAN)

Virtual local area networks (VLANs) allow network administrators **to use switches to create software-based LAN segments**, which can **segregate or consolidate traffic across multiple switch ports**. **Devices that share a VLAN communicate through switches as if they were on the same Layer 2 network**. Since VLANs act as discrete networks, communications between VLANs must be enabled. Broadcast traffic is limited to the VLAN, reducing congestion and reducing the effectiveness of some attacks. Administration of the environment is simplified, as the VLANs can be reconfigured when individuals change their physical location or need access to different services. VLANs can be configured based on switch port, IP subnet, MAC address and protocols. VLANs do not guarantee a network's security. At first glance, it may seem that traffic cannot be intercepted because communication within a VLAN is restricted to member devices. However, there are attacks that allow a malicious user to see traffic from other VLANs (so-called VLAN hopping). The VLAN technology is only one tool that can improve the overall security of the network environment.

Virtual Private Network (VPN)

A virtual private network (VPN) **is not necessarily an encrypted tunnel**. It is simply **a point-to-point connection between two hosts that allows them to communicate**. Secure communications can, of course, be provided by the VPN, but only if the security protocols have been selected and correctly configured to provide a trusted path over an untrusted network, such as the internet. Remote users employ VPNs to access their organization's network, and depending on the VPN's implementation, they may have most of the same resources available to them as if they were physically at the office. As an alternative to expensive dedicated point-to-point connections, organizations use gateway-to-gateway VPNs to securely transmit information over the internet between sites or even with business partners.