Networks & Network Security

Module 1: Network Architeccture

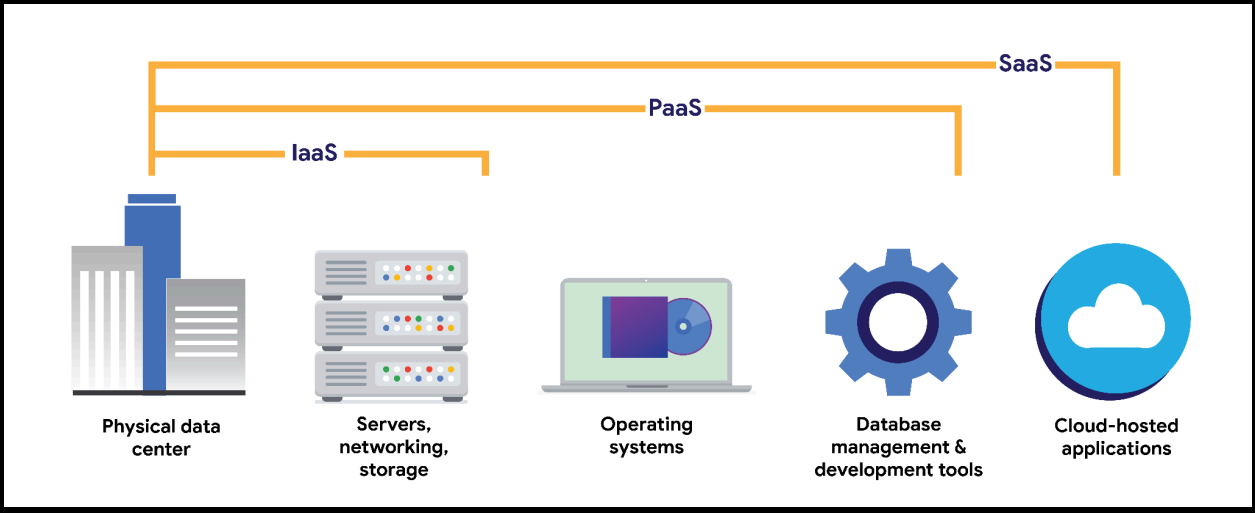
Computing processes in the cloud

Traditional networks are called on-premise networks, which means that all of the devices used for network operations are kept at a physical location owned by the company, like in an office building, for example. Cloud computing, however, refers to the practice of using remote servers, applications, and network services that are hosted on the internet instead of at a physical location owned by the company.

A cloud service provider (CSP) is a company that offers cloud computing services. These companies own large data centers in locations around the globe that house millions of servers. Data centers provide technology services, such as storage, and compute at such a large scale that they can sell their services to other companies for a fee. Companies can pay for the storage and services they need and consume them through the CSP's application programming interface (API) or web console.

CSPs provide three main categories of services:

- Software as a service (SaaS) refers to software suites operated by the CSP that a company can use remotely without hosting the software.
- Infrastructure as a service (IaaS) refers to the use of virtual computer components offered by the CSP. These include virtual containers and storage that are configured remotely through the CSP's API or web console. Cloud-compute and storage services can be used to operate existing applications and other technology workloads without significant modifications. Existing applications can be modified to take advantage of the availability, performance, and security features that are unique to cloud provider services.
- Platform as a service (PaaS) refers to tools that application developers can use to design custom applications for their company. Custom applications are designed and accessed in the cloud and used for a company's specific business needs.



Hybrid cloud environments

When organizations use a CSP's services in addition to their on-premise computers, networks, and storage, it is referred to as a hybrid cloud environment. When organizations use more than one CSP, it is called a multi-cloud environment. The vast majority of organizations use hybrid cloud environments to reduce costs and maintain control over network resources.

Software-defined networks

CSPs offer networking tools similar to the physical devices that you have learned about in this section of the course. Next, you'll review software-defined networking in the cloud. Software-defined networks (SDNs) are made up of virtual network devices and services. Just like CSPs provide virtual computers, many SDNs also provide virtual switches, routers, firewalls, and more. Most modern network hardware devices also support network virtualization and software-defined networking. This means that physical switches and routers use software to perform packet routing. In the case of cloud networking, the SDN tools are hosted on servers located at the CSP's data center.

Benefits of cloud computing and software-defined networks

Three of the main reasons that cloud computing is so attractive to businesses are reliability, decreased cost, and increased scalability.

Reliability

Reliability in cloud computing is based on how available cloud services and resources are, how secure connections are, and how often the services are effectively running. Cloud computing allows employees and customers to access the resources they need consistently and with minimal interruption.

Cost

Traditionally, companies have had to provide their own network infrastructure, at least for internet connections. This meant there could be potentially significant upfront costs for companies. However, because CSPs have such large data centers, they are able to offer virtual devices and services at a fraction of the cost required for companies to install, patch, upgrade, and manage the components and software themselves.

Scalability

Another challenge that companies face with traditional computing is scalability. When organizations experience an increase in their business needs, they might be forced to buy more equipment and software to keep up. But what if business decreases shortly after? They might no longer have the business to justify the cost incurred by the upgraded components. CSPs reduce this risk by making it easy to consume services in an elastic utility model as needed. This means that companies only pay for what they need when they need it.

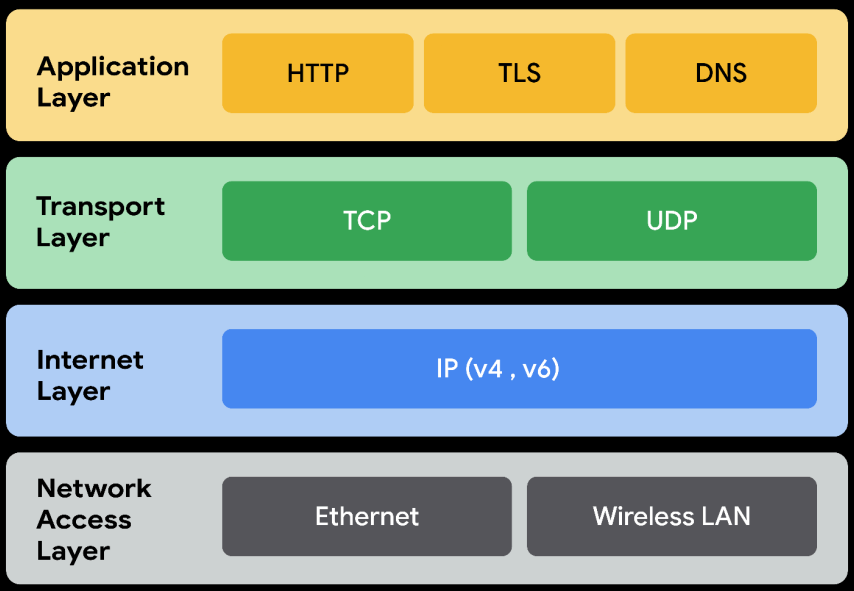
Changes can be made quickly through the CSPs, APIs, or web console—much more quickly than if network technicians had to purchase their own hardware and set it up. For example, if a company needs to protect against a threat to their network, web application firewalls (WAFs), intrusion detection/protection systems (IDS/IPS), or L3/L4 firewalls can be configured quickly whenever necessary, leading to better network performance and security.

The Four Layers of the TCP/IP Model

The TCP/IP model

The TCP/IP model is a framework used to visualize how data is organized and transmitted across a network. This model helps network engineers and network security analysts conceptualize processes on the network and communicate where disruptions or security threats occur.

The TCP/IP model has four layers: the network access layer, internet layer, transport layer, and application layer. When troubleshooting issues on the network, security professionals can analyze which layers were impacted by an attack based on what processes were involved in an incident.



Network access layer

The network access layer, sometimes called the data link layer, deals with the creation of data packets and their transmission across a network. This layer corresponds to the physical hardware involved in network transmission. Hubs, modems, cables, and wiring are all considered part of this layer. The address resolution protocol (ARP) is part of the network access layer. Since MAC addresses are used to identify hosts on the same physical network, ARP is needed to map IP addresses to MAC addresses for local network communication.

Internet layer

The internet layer, sometimes referred to as the network layer, is responsible for ensuring the delivery to the destination host, which potentially resides on a different network. It ensures IP addresses are attached to data packets to indicate the location of the sender and receiver. The internet layer also determines which protocol is responsible for delivering the data packets and ensures the delivery to the destination host. Here are some of the common protocols that operate at the internet layer:

- Internet Protocol (IP). IP sends the data packets to the correct destination and relies on the Transmission Control Protocol/User Datagram Protocol (TCP/UDP) to deliver them to the corresponding service. IP packets allow communication between two networks. They are routed from the sending network to the receiving network. TCP in particular retransmits any data that is lost or corrupt.
- Internet Control Message Protocol (ICMP). The ICMP shares error information and status updates of data packets. This is useful for detecting and troubleshooting network errors. The ICMP reports information about packets that were dropped or that disappeared in transit, issues with network connectivity, and packets redirected to other routers.

Transport layer

The transport layer is responsible for delivering data between two systems or networks and includes protocols to control the flow of traffic across a network. TCP and UDP are the two transport protocols that occur at this layer.

Transmission Control Protocol

The Transmission Control Protocol (TCP) is an internet communication protocol that allows two devices to form a connection and stream data. It ensures that data is reliably transmitted to the destination service. TCP contains the port number of the intended destination service, which resides in the TCP header of a TCP/IP packet.

User Datagram Protocol

The User Datagram Protocol (UDP) is a connectionless protocol that does not establish a connection between devices before transmissions. It is used by applications that are not concerned with the reliability of the transmission. Data sent over UDP is not tracked as extensively as data sent using TCP. Because UDP does not establish network connections, it is used mostly for performance sensitive applications that operate in real time, such as video streaming.

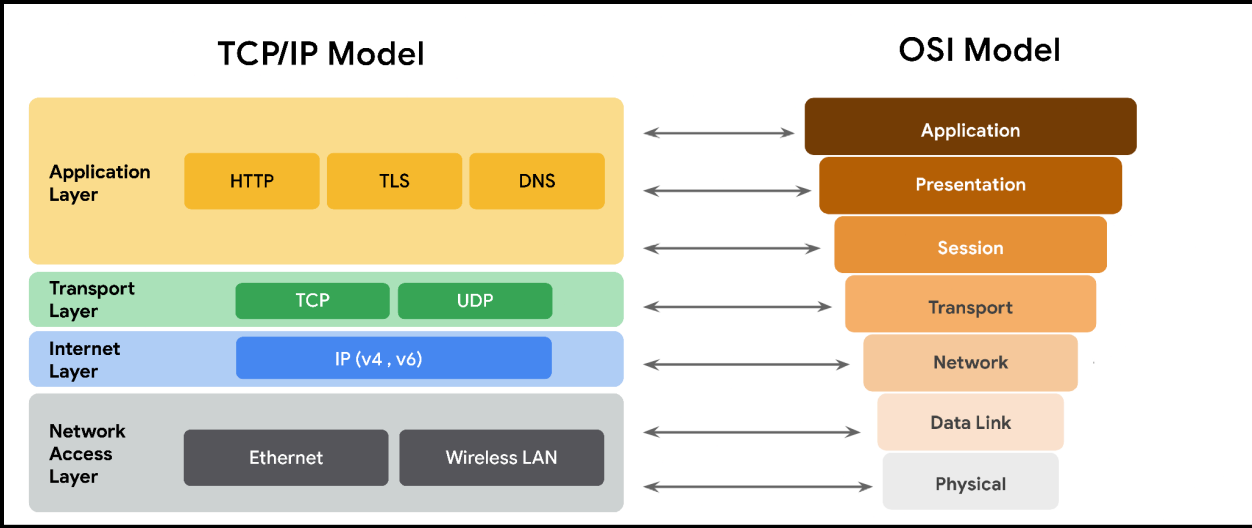
Application layer

The application layer in the TCP/IP model is similar to the application, presentation, and session layers of the OSI model. The application layer is responsible for making network requests or responding to requests. This layer defines which internet services and applications any user can access. Protocols in the application layer determine how the data packets will interact with receiving devices. Some common protocols used on this layer are:

- Hypertext transfer protocol (HTTP)
- Simple mail transfer protocol (SMTP)
- Secure shell (SSH)
- File transfer protocol (FTP)
- Domain name system (DNS)

Application layer protocols rely on underlying layers to transfer the data across the network.

TCP/IP model versus OSI model



The OSI visually organizes network protocols into different layers. Network professionals often use this model to communicate with each other about potential sources of problems or security threats when they occur.

The TCP/IP model combines multiple layers of the OSI model. There are many similarities between the two models. Both models define standards for networking and divide the network communication process into different layers. The TCP/IP model is a simplified version of the OSI model.

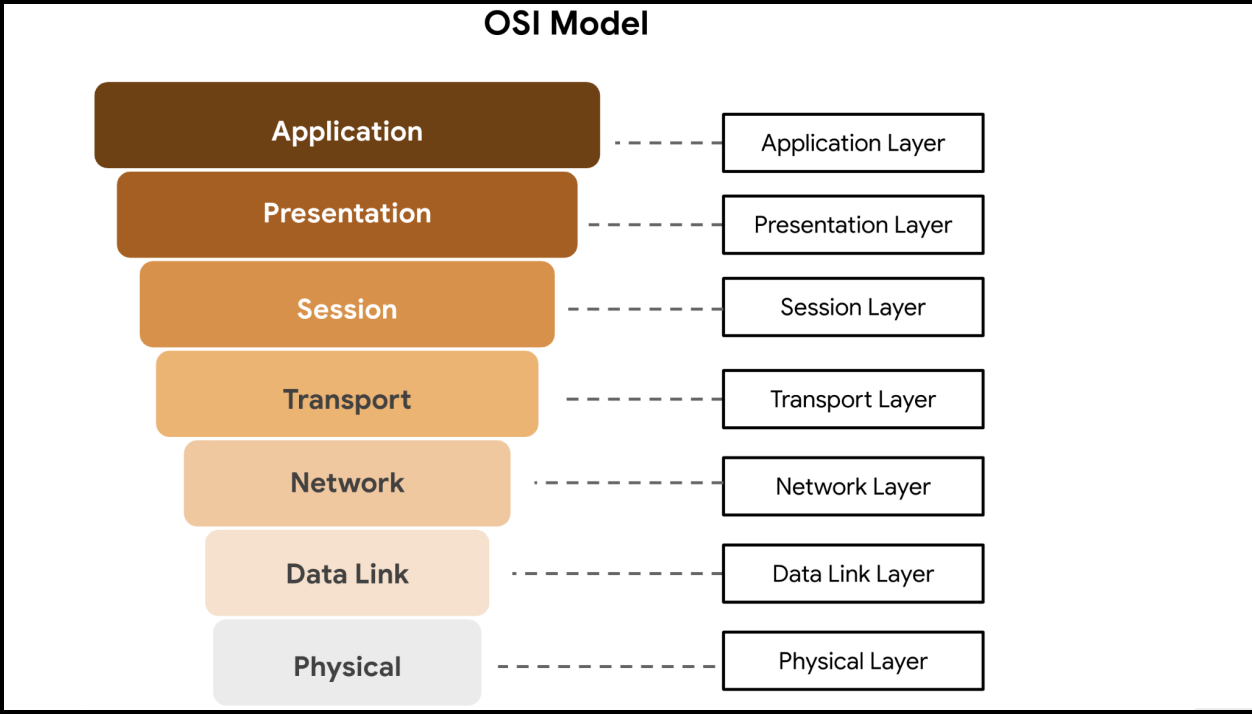
[The OSI Model]

The TCP/IP model vs. the OSI model

The TCP/IP model is a framework used to visualize how data is organized and transmitted across a network. This model helps network engineers and security analysts conceptualize processes on the network and communicate where disruptions or security threats occur.

The TCP/IP model has four layers: the network access layer, internet layer, transport layer, and application layer. When analyzing network events, security professionals can determine what layer or layers an attack occurred in based on what processes were involved in the incident.

The OSI model is a standardized concept that describes the seven layers computers use to communicate and send data over the network. Network and security professionals often use this model to communicate with each other about potential sources of problems or security threats when they occur.



Some organizations rely heavily on the TCP/IP model, while others prefer to use the OSI model. As a security analyst, it's important to be familiar with both models. Both the TCP/IP and OSI models are useful for understanding how networks work.

Layer 7: Application layer

The application layer includes processes that directly involve the everyday user. This layer includes all of the networking protocols that software applications use to connect a user to the internet. This characteristic is the identifying feature of the application layer—user connection to the internet via applications and requests.

An example of a type of communication that happens at the application layer is using a web browser. The internet browser uses HTTP or HTTPS to send and receive information from the website server. The email application uses simple mail transfer protocol (SMTP) to send and receive email information. Also, web browsers use the domain name system (DNS) protocol to translate website domain names into IP addresses which identify the web server that hosts the information for the website.

Layer 6: Presentation layer

Functions at the presentation layer involve data translation and encryption for the network. This layer adds to and replaces data with formats that can be understood by applications (layer 7) on both sending and receiving systems. Formats at the user end may be different from those of the receiving system. Processes at the presentation layer require the use of a standardized format.

Some formatting functions that occur at layer 6 include encryption, compression, and confirmation that the character code set can be interpreted on the receiving system. One example of encryption that takes place at this layer is SSL, which encrypts data between web servers and browsers as part of websites with HTTPS.

Layer 5: Session layer

A session describes when a connection is established between two devices. An open session allows the devices to communicate with each other. Session layer protocols keep the session open while data is being transferred and terminate the session once the transmission is complete.

The session layer is also responsible for activities such as authentication, reconnection, and setting checkpoints during a data transfer. If a session is interrupted, checkpoints ensure that the transmission picks up at the last session checkpoint when the connection resumes. Sessions include a request and response between applications. Functions in the session layer respond to requests for service from processes in the presentation layer (layer 6) and send requests for services to the transport layer (layer 4).

Layer 4: Transport layer

The transport layer is responsible for delivering data between devices. This layer also handles the speed of data transfer, flow of the transfer, and breaking data down into smaller segments to make them easier to transport. Segmentation is the process of dividing up a large data transmission into smaller pieces that can be processed by the receiving system. These segments need to be reassembled at their destination so they can be processed at the session layer (layer 5). The speed and rate of the transmission also has to match the connection speed of the destination system. TCP and UDP are transport layer protocols.

Layer 3: Network layer

The network layer oversees receiving the frames from the data link layer (layer 2) and delivers them to the intended destination. The intended destination can be found based on the address that resides in the frame of the data packets. Data packets allow communication between two networks. These packets include IP addresses that tell routers where to send them. They are routed from the sending network to the receiving network.

Layer 2: Data link layer

The data link layer organizes sending and receiving data packets within a single network. The data link layer is home to switches on the local network and network interface cards on local devices.

Protocols like network control protocol (NCP), high-level data link control (HDLC), and synchronous data link control protocol (SDLC) are used at the data link layer.

Layer 1: Physical layer

As the name suggests, the physical layer corresponds to the physical hardware involved in network transmission. Hubs, modems, and the cables and wiring that connect them are all considered part of the physical layer. To travel across an ethernet or coaxial cable, a data packet needs to be translated into a stream of 0s and 1s. The stream of 0s and 1s are sent across the physical wiring and cables, received, and then passed on to higher levels of the OSI model.

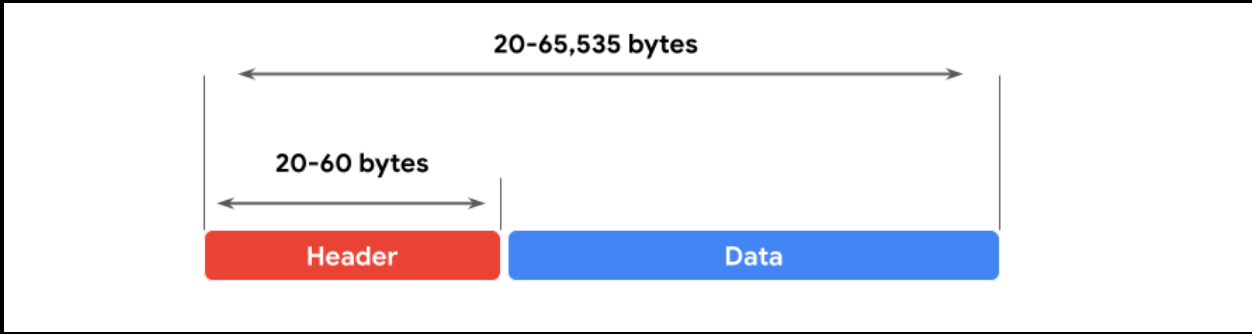
Components of Network Layer Communication

Operations at the network layer

Functions at the network layer organize the addressing and delivery of data packets across the network from the host device to the destination device. This includes directing the packets from one router to another router across the internet, till it reaches the internet protocol (IP) address of the destination network. The destination IP address is contained within the header of each data packet. This address will be stored for future routing purposes in routing tables along the packet's path to its destination.

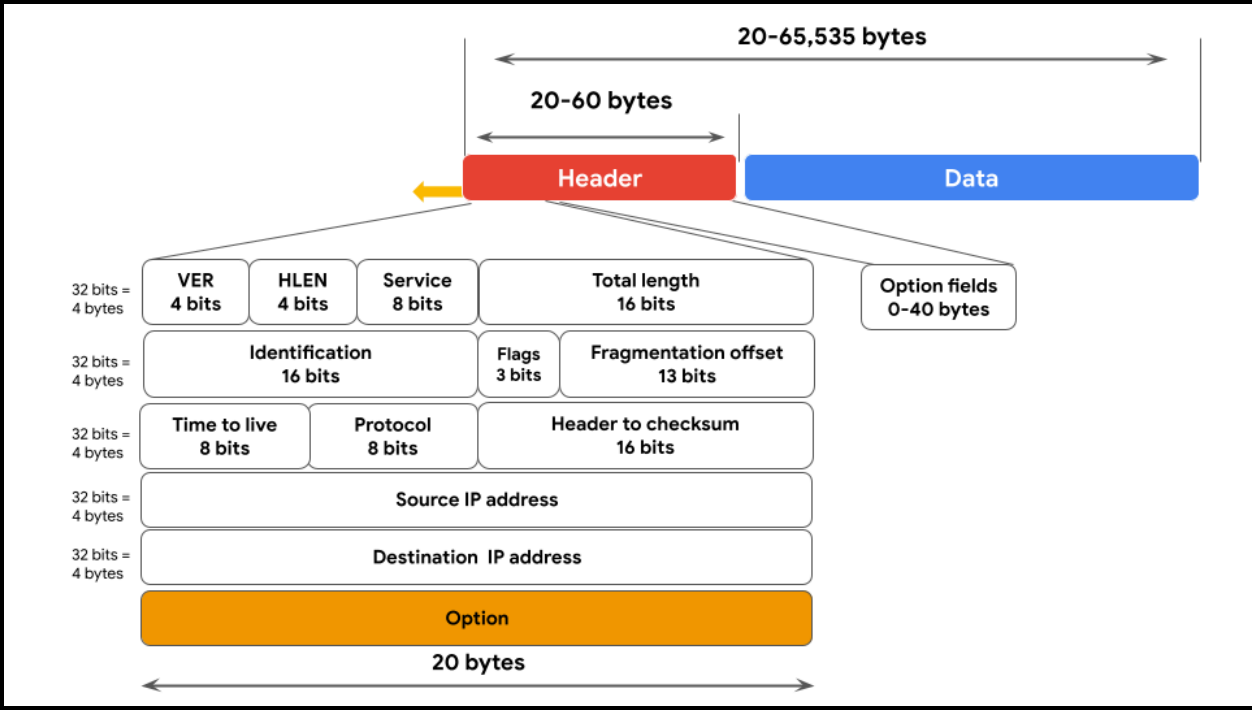
All data packets include an IP address. A data packet is also referred to as an IP packet for TCP connections or a datagram for UDP connections. A router uses the IP address to route packets from network to network based on information contained in the IP header of a data packet. Header information communicates more than just the address of the destination. It also includes information such as the source IP address, the size of the packet, and which protocol will be used for the data portion of the packet.

Format of an IPv4 packet



Next, you can review the format of an IP version 4 (IPv4) packet and review a detailed graphic of the packet header. An IPv4 packet is made up of two sections, the header and the data:

- An IPv4 header format is determined by the IPv4 protocol and includes the IP routing information that devices use to direct the packet. The size of the IPv4 header ranges from 20 to 60 bytes. The first 20 bytes are a fixed set of information containing data such as the source and destination IP address, header length, and total length of the packet. The last set of bytes can range from 0 to 40 and consists of the options field.
- The length of the data section of an IPv4 packet can vary greatly in size. However, the maximum possible size of an IPv4 packet is 65,535 bytes. It contains the message being transferred over the internet, like website information or email text.



There are 13 fields within the header of an IPv4 packet:

- Version (VER): This 4 bit component tells receiving devices what protocol the packet is using. The packet used in the illustration above is an IPv4 packet.
- IP Header Length (HLEN or IHL): HLEN is the packet's header length. This value indicates where the packet header ends and the data segment begins.
- Type of Service (ToS): Routers prioritize packets for delivery to maintain quality of service on the network. The ToS field provides the router with this information.
- Total Length: This field communicates the total length of the entire IP packet, including the header and data. The maximum size of an IPv4 packet is 65,535 bytes.
- Identification: IPv4 packets can be up to 65, 535 bytes, but most networks have a smaller limit. In these cases, the packets are divided, or fragmented, into smaller IP packets. The identification field provides a unique identifier for all the fragments of the original IP packet so that they can be reassembled once they reach their destination.
- Flags: This field provides the routing device with more information about whether the original packet has been fragmented and if there are more fragments in transit.
- Fragmentation Offset: The fragment offset field tells routing devices where in the original packet the fragment belongs.
- Time to Live (TTL): TTL prevents data packets from being forwarded by routers indefinitely. It contains a counter that is set by the source. The counter is decremented by one as it passes through each router along its path. When the TTL counter reaches zero, the router currently holding the packet will discard the packet and return an ICMP Time Exceeded error message to the sender.
- Protocol: The protocol field tells the receiving device which protocol will be used for the data portion of the packet.
- Header Checksum: The header checksum field contains a checksum that can be used to detect corruption of the IP header in transit. Corrupted packets are discarded.
- Source IP Address: The source IP address is the IPv4 address of the sending device.
- Destination IP Address: The destination IP address is the IPv4 address of the destination device.
- Options: The options field allows for security options to be applied to the packet if the HLEN value is greater than five. The field communicates these options to the routing devices.

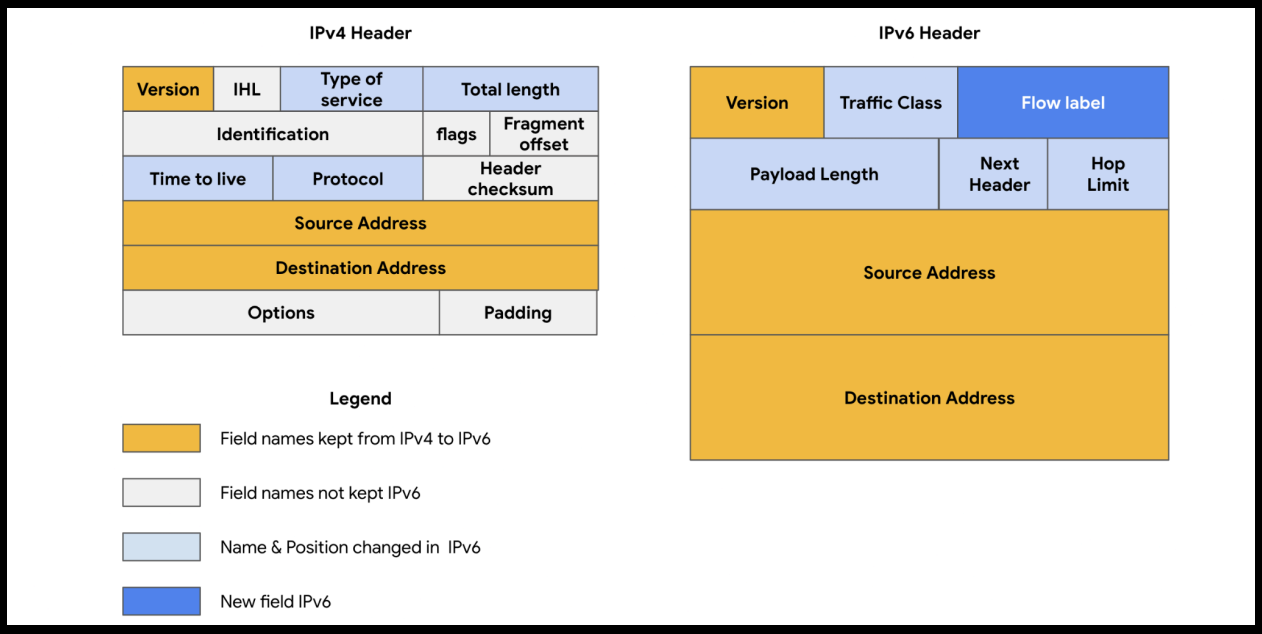
Difference between IPv4 and IPv6

In an earlier part of this course, you learned about the history of IP addressing. As the internet grew, it became clear that all of the IPv4 addresses would eventually be depleted; this is called IPv4 address exhaustion. At the time, no one had anticipated how many computing devices would need an IP address. IPv6 was developed to mitigate IPv4 address exhaustion and other related concerns.

Some of the key differences between IPv4 and IPv6 include the length and the format of the addresses. IPv4 addresses are made up of four decimal numbers separated by periods, each number ranging from 0 to 255. Together the numbers span 4 bytes, and allow for up to 4.3 billion possible addresses. An example of an IPv4 address would be: 198.51.100.0. IPv6 addresses are made of eight hexadecimal numbers separated by colons, each number consisting of up to four hexadecimal digits. Together, all numbers span 16 bytes, and allow for up to 340 undecillion addresses (340 followed by 36 zeros). An example of an IPv6 address would be: 2002:0db8:0000:0000:0000:ff21:0023:1234.

*Note: to represent one or more consecutive sets of all zeros, you can replace the zeros with a double colon "::", so the above IPv6 address would be "*2002:0db8::ff21:0023:1234."

There are also some differences in the layout of an IPv6 packet header. The IPv6 header format is much simpler than IPv4. For example, the IPv4 Header includes the IHL, Identification, and Flags fields, whereas the IPv6 does not. The IPv6 header only introduces the Flow Label field, where the Flow Label identifies a packet as requiring special handling by other IPv6 routers.



There are some important security differences between IPv4 and IPv6. IPv6 offers more efficient routing and eliminates private address collisions that can occur on IPv4 when two devices on the same network are attempting to use the same address.

Module 2: Network Operations

Overview of network protocols

A network protocol is a set of rules used by two or more devices on a network to describe the order of delivery and the structure of data. Network protocols serve as instructions that come with the information in the data packet. These instructions tell the receiving device what to do with the data. Protocols are like a common language that allows devices all across the world to communicate with and understand each other.

Even though network protocols perform an essential function in network communication, security analysts should still understand their associated security implications. Some protocols have vulnerabilities that malicious actors exploit. For example, a nefarious actor could use the Domain Name System (DNS) protocol, which resolves web addresses to IP addresses, to divert traffic from a legitimate website to a malicious website containing malware. You'll learn more about this topic in upcoming course materials.

Three categories of network protocols

Network protocols can be divided into three main categories: communication protocols, management protocols, and security protocols. There are dozens of different network protocols, but you don't need to memorize all of them for an entry-level security analyst role. However, it's important for you to know the ones listed in this reading.

Communication protocols

Communication protocols govern the exchange of information in network transmission. They dictate how the data is transmitted between devices and the timing of the communication. They also include methods to recover data lost in transit. Here are a few of them.

- Transmission Control Protocol (TCP) is an internet communication protocol that allows two devices to form a connection and stream data. TCP uses a three-way handshake process. First, the device sends a synchronize (SYN) request to a server. Then the server responds with a SYN/ACK packet to acknowledge receipt of the device's request. Once the server receives the final ACK packet from the device, a TCP connection is established. In the TCP/IP model, TCP occurs at the transport layer.
- User Datagram Protocol (UDP) is a connectionless protocol that does not establish a connection between devices before a transmission. This makes it less reliable than TCP. But it also means that it works well for transmissions that need to get to their destination quickly. For example, one use of UDP is for sending DNS requests to local DNS servers. In the TCP/IP model, UDP occurs at the transport layer.
- Hypertext Transfer Protocol (HTTP) is an application layer protocol that provides a method of communication between clients and website servers. HTTP uses port 80. HTTP is considered insecure, so it is being replaced on most websites by a secure version, called HTTPS that uses encryption from SSL/TLS for communication. However, there are still many websites that use the insecure HTTP protocol. In the TCP/IP model, HTTP occurs at the application layer.
- Domain Name System (DNS) is a protocol that translates internet domain names into IP addresses. When a client computer wishes to access a website domain using their internet browser, a query is sent to a dedicated DNS server. The DNS server then looks up the IP address that corresponds to the website domain. DNS normally uses UDP on port 53. However, if the DNS reply to a request is large, it will switch to using the TCP protocol. In the TCP/IP model, DNS occurs at the application layer.

Management Protocols

The next category of network protocols is management protocols. Management protocols are used for monitoring and managing activity on a network. They include protocols for error reporting and optimizing performance on the network.

- Simple Network Management Protocol (SNMP) is a network protocol used for monitoring and managing devices on a network. SNMP can reset a password on a network device or change its baseline configuration. It can also send requests to network devices for a report on how much of the network's bandwidth is being used up. In the TCP/IP model, SNMP occurs at the application layer.
- Internet Control Message Protocol (ICMP) is an internet protocol used by devices to tell each other about data transmission errors across the network. ICMP is used by a receiving device to send a report to the sending device about the data transmission. ICMP is commonly used as a quick way to troubleshoot network connectivity and latency by issuing the "ping" command on a Linux operating system. In the TCP/IP model, ICMP occurs at the internet layer.

Security Protocols

Security protocols are network protocols that ensure that data is sent and received securely across a network. Security protocols use encryption algorithms to protect data in transit. Below are some common security protocols.

- Hypertext Transfer Protocol Secure (HTTPS) is a network protocol that provides a secure method of communication between clients and website servers. HTTPS is a secure version of HTTP that uses secure sockets layer/transport layer security (SSL/TLS) encryption on all transmissions so that malicious actors cannot read the information contained. HTTPS uses port 443. In the TCP/IP model, HTTPS occurs at the application layer.
- Secure File Transfer Protocol (SFTP) is a secure protocol used to transfer files from one device to another over a network. SFTP uses secure shell (SSH), typically through TCP port 22. SSH uses Advanced Encryption Standard (AES) and other types of encryption to ensure that unintended recipients cannot intercept the transmissions. In the TCP/IP model, SFTP occurs at the application layer. SFTP is used often with cloud storage. Every time a user uploads or downloads a file from cloud storage, the file is transferred using the SFTP protocol.

Note: The encryption protocols mentioned do not conceal the source or destination IP address of network traffic. This means a malicious actor can still learn some basic information about the network traffic if they intercept it.

Network Address Translation

The devices on your local home or office network each have a private IP address that they use to communicate directly with each other. However, in order for the devices with private IP addresses to communicate with the public internet, they need to have a single public IP address that represents all devices on the LAN to the public. For outgoing messages, the router can replace a private source IP address with its public IP address and perform the reverse operation for responses. This process is known as Network Address Translation (NAT) and it generally requires a router or firewall to be specifically configured to perform NAT. NAT is a part of layer 2 (internet layer) and layer 3 (transport layer) of the TCP/IP model.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is in the management family of network protocols. DHCP is an application layer protocol used on a network to configure devices. It works with the router to assign a unique IP address to each device and provide the addresses of the appropriate DNS server and default gateway for each device. DHCP servers operate on UDP port 67 while DHCP clients operate on UDP port 68.

Address Resolution Protocol

By now, you are familiar with IP and MAC addresses. You've learned that each device on a network has a public IP address, a private IP address, and a MAC address that identify it on the network. A device's IP address may change over time, but its MAC address is permanent because it is unique to a device's network interface card. The MAC address is used to communicate with devices within the same network, but sometimes, the MAC address is unknown. This is why the Address Resolution Protocol (ARP) is needed. ARP is mainly a network access layer protocol in the TCP/IP model used to translate the IP addresses that are found in data packets into the MAC address of the hardware device.

Each device on the network performs ARP and keeps track of matching IP and MAC addresses in an ARP cache. ARP does not have a specific port number since it is a layer 2 protocol and port numbers are associated with the layer 7 application layer.

Telnet

Telnet is an application layer protocol that is used to connect with a remote system. Telnet sends all information in clear text. It uses command line prompts to control another device similar to secure shell (SSH), but Telnet is not as secure as SSH. Telnet can be used to connect to local or remote devices and uses TCP port 23.

Secure shell

Secure shell protocol (SSH) is used to create a secure connection with a remote system. This application layer protocol provides an alternative for secure authentication and encrypted communication. SSH operates over the TCP port 22 and is a replacement for less secure protocols, such as Telnet.

Post office protocol

Post office protocol (POP) is an application layer (layer 4 of the TCP/IP model) protocol used to manage and retrieve email from a mail server. POP3 is the most commonly used version of POP. Many organizations have a dedicated mail server on the network that handles incoming and outgoing mail for users on the network. User devices will send requests to the remote mail server and download email messages locally. If you have ever refreshed your email application and had new emails populate in your inbox, you are experiencing POP and internet message access protocol (IMAP) in action. Unencrypted, plaintext authentication uses TCP/UDP port 110 and encrypted emails use Secure Sockets Layer/Transport Layer Security (SSL/TLS) over TCP/UDP port 995. When using POP, mail has to finish downloading on a local device before it can be read. After downloading, the mail may or may not be deleted from the mail server, so it does not guarantee that a user can sync the same email across multiple devices.

Internet Message Access Protocol (IMAP)

IMAP is used for incoming email. It downloads the headers of emails and the message content. The content also remains on the email server, which allows users to access their email from multiple devices. IMAP uses TCP port 143 for unencrypted email and TCP port 993 over the TLS protocol. Using IMAP allows users to partially read email before it is finished downloading. Since the mail is kept on the mail server, it allows a user to sync emails across multiple devices.

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) is used to transmit and route email from the sender to the recipient's address. SMTP works with Message Transfer Agent (MTA) software, which searches DNS servers to resolve email addresses to IP addresses, to ensure emails reach their intended destination. SMTP uses TCP/UDP port 25 for unencrypted emails and TCP/UDP port 587 using TLS for encrypted emails. The TCP port 25 is often used by high-volume spam. SMTP helps to filter out spam by regulating how many emails a source can send at a time.

Protocols and port numbers

Remember that port numbers are used by network devices to determine what should be done with the information contained in each data packet once they reach their destination. Firewalls can filter out unwanted traffic based on port numbers. For example, an organization may configure a firewall to only allow access to TCP port 995 (POP3) by IP addresses belonging to the organization.

As a security analyst, you will need to know about many of the protocols and port numbers mentioned in this course. They may be used to determine your technical knowledge in interviews, so it's a good idea to memorize them. You will also learn about new protocols on the job in a security position.

The Evolution of Wireless Security Protocols

Introduction to wireless communication protocols

Many people today refer to wireless internet as Wi-Fi. Wi-Fi refers to a set of standards that define communication for wireless LANs. Wi-Fi is a marketing term commissioned by the Wireless Ethernet Compatibility Alliance (WECA). WECA has since renamed their organization Wi-Fi Alliance.

Wi-Fi standards and protocols are based on the 802.11 family of internet communication standards determined by the Institute of Electrical and Electronics Engineers (IEEE). So, as a security analyst, you might also see Wi-Fi referred to as IEEE 802.11.

Wi-Fi communications are secured by wireless networking protocols. Wireless security protocols have evolved over the years, helping to identify and resolve vulnerabilities with more advanced wireless technologies.

In this reading, you will learn about the evolution of wireless security protocols from WEP to WPA, WPA2, and WPA3. You'll also learn how the Wireless Application Protocol was used for mobile internet communications.

Wired Equivalent Privacy

Wired equivalent privacy (WEP) is a wireless security protocol designed to provide users with the same level of privacy on wireless network connections as they have on wired network connections. WEP was developed in 1999 and is the oldest of the wireless security standards.

WEP is largely out of use today, but security analysts should still understand WEP in case they encounter it. For example, a network router might have used WEP as the default security protocol and the network administrator never changed it. Or, devices on a network might be too old to support newer Wi-Fi security protocols. Nevertheless, a malicious actor could potentially break the WEP encryption, so it's now considered a high-risk security protocol.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) was developed in 2003 to improve upon WEP, address the security issues that it presented, and replace it. WPA was always intended to be a transitional measure so backwards compatibility could be established with older hardware.

The flaws with WEP were in the protocol itself and how the encryption was used. WPA addressed this weakness by using a protocol called Temporal Key Integrity Protocol (TKIP). WPA encryption algorithm uses larger secret keys than WEPs, making it more difficult to guess the key by trial and error.

WPA also includes a message integrity check that includes a message authentication tag with each transmission. If a malicious actor attempts to alter the transmission in any way or resend at another time, WPA's message integrity check will identify the attack and reject the transmission.

Despite the security improvements of WPA, it still has vulnerabilities. Malicious actors can use a key reinstallation attack (or KRACK attack) to decrypt transmissions using WPA. Attackers can insert themselves in the WPA authentication handshake process and insert a new encryption key instead of the dynamic one assigned by WPA. If they set the new key to all zeros, it is as if the transmission is not encrypted at all.

Because of this significant vulnerability, WPA was replaced with an updated version of the protocol called WPA2.

WPA2 & WPA3

WPA2

The second version of Wi-Fi Protected Access—known as WPA2—was released in 2004. WPA2 improves upon WPA by using the Advanced Encryption Standard (AES). WPA2 also improves upon WPA's use of TKIP. WPA2 uses the Counter Mode Cipher Block Chain Message Authentication Code Protocol (CCMP), which provides encapsulation and ensures message authentication and integrity. Because of the strength of WPA2, it is considered the security standard for all Wi-Fi transmissions today. WPA2, like its predecessor, is vulnerable to KRACK attacks. This led to the development of WPA3 in 2018.

Personal

WPA2 personal mode is best suited for home networks for a variety of reasons. It is easy to implement, initial setup takes less time for personal than enterprise version. The global passphrase for WPA2 personal version needs to be applied to each individual computer and access point in a network. This makes it ideal for home networks, but unmanageable for organizations.

Enterprise

WPA2 enterprise mode works best for business applications. It provides the necessary security for wireless networks in business settings. The initial setup is more complicated than WPA2 personal mode, but enterprise mode offers individualized and centralized control over the Wi-Fi access to a business network. This means that network administrators can grant or remove user access to a network at any time. Users never have access to encryption keys, this prevents potential attackers from recovering network keys on individual computers.

WPA3

WPA3 is a secure Wi-Fi protocol and is growing in usage as more WPA3 compatible devices are released. These are the key differences between WPA2 and WPA3:

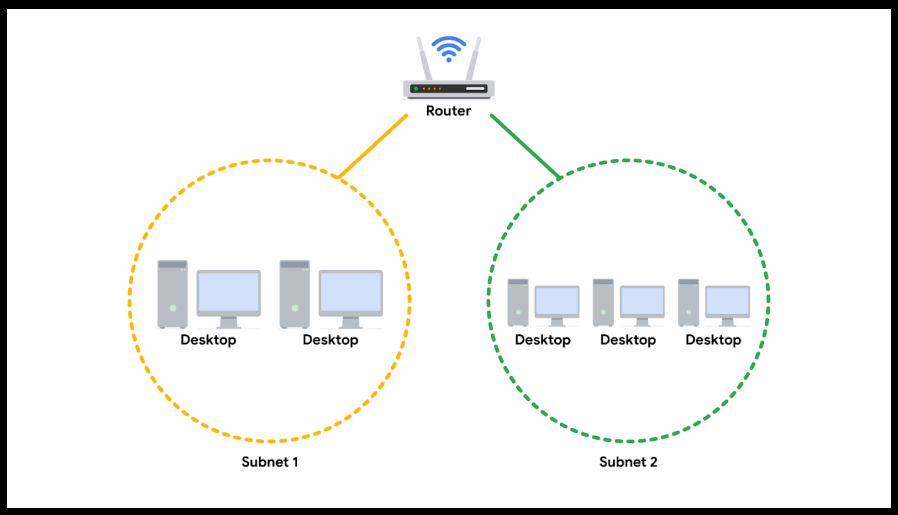
- WPA3 addresses the authentication handshake vulnerability to KRACK attacks, which is present in WPA2.
- WPA3 uses Simultaneous Authentication of Equals (SAE), a password-authenticated, cipher-key-sharing agreement. This prevents attackers from downloading data from wireless network connections to their systems to attempt to decode it.
- WPA3 has increased encryption to make passwords more secure by using 128-bit encryption, with WPA3-Enterprise mode offering optional 192-bit encryption.

Subnetting and CIDR

Overview of subnetting

Subnetting is the process of taking one large network and dividing it into several smaller, organized groups called subnets. Think of it like this: If your company's network is a large city, each subnet is a distinct neighborhood within that city.

Subnetting divides up a network address range into smaller subnets within the network. These organized subnets are defined by the unique combination of the IP address and the network mask assigned to every device, effectively creating a "network within a network." Subnetting creates a network of devices to function as their own network. This makes the network more efficient and can also be used to create security zones. If devices on the same subnet communicate with each other, the switch changes the transmissions to stay on the same subnet, improving speed and efficiency of the communications.



Classless Inter-Domain Routing notation for subnetting

Classless Inter-Domain Routing (CIDR) is a method of assigning subnet masks to IP addresses to create a subnet. Classless addressing replaces classful addressing. Classful addressing was used in the 1980s as a system of grouping IP addresses into classes (Class A to Class E). Each class included a limited number of IP addresses, which were depleted as the number of devices connecting to the internet outgrew the classful range in the 1990s. Classless CIDR addressing expanded the number of available IPv4 addresses.

CIDR allows cybersecurity professionals to segment classful networks into smaller chunks. CIDR IP addresses are formatted like IPv4 addresses, but they include a slash (“/”) followed by a number at the end of the address, This extra number is called the IP network prefix. For example, a regular IPv4 address uses the 198.51.100.0 format, whereas a CIDR IP address would include the IP network prefix at the end of the address, 198.51.100.0/24. This CIDR address encompasses all IP addresses between 198.51.100.0 and 198.51.100.255. The system of CIDR addressing reduces the number of entries in routing tables and provides more available IP addresses within networks. You can try converting CIDR to IPv4 addresses and vice versa through an online conversion tool, like IPAddressGuide, for practice and to better understand this concept.

Note: For now, focus on understanding the concept of CIDR as a flexible addressing method used for modern subnetting. A deeper dive into the technical mathematics of CIDR is a valuable skill you can develop further in future training if needed.

Security benefits of subnetting

Subnetting allows network professionals and analysts to create a network within their own network without requesting another network IP address from their internet service provider. This process uses network bandwidth more efficiently and improves network performance. Subnetting is one component of creating isolated subnetworks through physical isolation, routing configuration, and firewalls.

Virtual Networks and Privacy

Common network protocols

Network protocols are used to direct traffic to the correct device and service depending on the kind of communication being performed by the devices on the network. Protocols are the rules used by all network devices that provide a mutually agreed upon foundation for how to transfer data across a network.

There are three main categories of network protocols: communication protocols, management protocols, and security protocols.

1. Communication protocols are used to establish connections between servers. Examples include TCP, UDP, and Simple Mail Transfer Protocol (SMTP), which provides a framework for email communication.
2. Management protocols are used to troubleshoot network issues. One example is the Internet Control Message Protocol (ICMP).
3. Security protocols provide encryption for data in transit. Examples include IPSec and SSL/TLS.

Some other commonly used protocols are:

- HyperText Transfer Protocol (HTTP). HTTP is an application layer communication protocol. This allows the browser and the web server to communicate with one another.
- Domain Name System (DNS). DNS is an application layer protocol that translates, or maps, host names to IP addresses.
- Address Resolution Protocol (ARP). ARP is a network layer communication protocol that maps IP addresses to physical machines or a MAC address recognized on the local area network.

Wi-Fi

This section of the course also introduced various wireless security protocols, including WEP, WPA, WPA2, and WPA3. WPA3 encrypts traffic with the Advanced Encryption Standard (AES) cipher as it travels from your device to the wireless access point. WPA2 and WPA3 offer two modes: personal and enterprise. Personal mode is best suited for home networks while enterprise mode is generally utilized for business networks and applications.

Network security tools and practices

Firewalls

Previously, you learned that firewalls are network virtual appliances (NVAs) or hardware devices that inspect and can filter network traffic before it's permitted to enter the private network. Traditional firewalls are configured with rules that tell it what types of data packets are allowed based on the port number and IP address of the data packet.

There are two main categories of firewalls.

- Stateless: A class of firewall that operates based on predefined rules and does not keep track of information from data packets
- Stateful: A class of firewall that keeps track of information passing through it and proactively filters out threats. Unlike stateless firewalls, which require rules to be configured in two directions, a stateful firewall only requires a rule in one direction. This is because it uses a "state table" to track connections, so it can match return traffic to an existing session

Next generation firewalls (NGFWs) are the most technologically advanced firewall protection. They exceed the security offered by stateful firewalls because they include deep packet inspection (a kind of packet sniffing that examines data packets and takes actions if threats exist) and intrusion prevention features that detect security threats and notify firewall administrators. NGFWs can inspect traffic at the application layer of the TCP/IP model and are typically application aware. Unlike traditional firewalls that block traffic based on IP address and ports, NGFWs rules can be configured to block or allow traffic based on the application. Some NGFWs have additional features like Malware Sandboxing, Network Anti-Virus, and URL and DNS Filtering.

Proxy servers

A proxy server is another way to add security to your private network. Proxy servers utilize network address translation (NAT) to serve as a barrier between clients on the network and external threats. Forward proxies handle queries from internal clients when they access resources external to the network. Reverse proxies function opposite of forward proxies; they handle requests from

external systems to services on the internal network. Some proxy servers can also be configured with rules, like a firewall. For example, you can create filters to block websites identified as containing malware.

Virtual Private Networks (VPN)

A VPN is a service that encrypts data in transit and disguises your IP address. VPNs use a process called encapsulation. Encapsulation wraps your unencrypted data in an encrypted data packet, which allows your data to be sent across the public network while remaining anonymous. Enterprises and other organizations use VPNs to help protect communications from users' devices to corporate resources. Some of these resources include servers or virtual machines that host business applications. Individuals also use VPNs to increase personal privacy. VPNs protect user privacy by concealing personal information, including IP addresses, from external servers. A reputable VPN also minimizes its own access to user internet activity by using strong encryption and other security measures. Organizations are increasingly using a combination of VPN and SD-WAN capabilities to secure their networks. A software-defined wide area network (SD-WAN) is a virtual WAN service that allows organizations to securely connect users to applications across multiple locations and over large geographical distances.

Security Zones

Understanding Security Zones

- Security zones act as barriers to internal networks, maintaining privacy and preventing issues from spreading across the entire network.
- An example is a hotel separating its public Wi-Fi from its staff network, or a university having separate subnets for faculty and students.

Types of Security Zones

- Uncontrolled Zone: This refers to any network outside an organization's control, such as the internet.
- Controlled Zone: This is a subnet that protects the internal network from the uncontrolled zone and includes various sub-zones.

Zones within the Controlled Network

- Demilitarized Zone (DMZ): This outer layer contains public-facing services like web servers, proxy servers, and DNS servers, acting as a perimeter to the internal network.
- Restricted Zone: Located within the internal network, this zone protects highly confidential information accessible only to privileged employees. These zones are typically protected by firewalls to control traffic and prevent attacks from spreading.

VPN Protocols: Wireguard and IPSecc

Remote access and site-to-site VPNs

Individual users use remote access VPNs to establish a connection between a personal device and a VPN server. Remote access VPNs encrypt data sent or received through a personal device. The connection between the user and the remote access VPN is established through the internet.

Enterprises use site-to-site VPNs largely to extend their network to other networks and locations. This is particularly useful for organizations that have many offices across the globe. IPSec is commonly used in site-to-site VPNs to create an encrypted tunnel between the primary network and the remote network. One disadvantage of site-to-site VPNs is how complex they can be to configure and manage compared to remote VPNs.

WireGuard VPN vs. IPSec VPN

WireGuard and IPSec are two different VPN protocols used to encrypt traffic over a secure network tunnel. The majority of VPN providers offer a variety of options for VPN protocols, such as WireGuard or IPSec. Ultimately, choosing between IPSec and WireGuard depends on many factors, including connection speeds, compatibility with existing network infrastructure, and business or individual needs.

WireGuard VPN

WireGuard is a high-speed VPN protocol, with advanced encryption, to protect users when they are accessing the internet. It’s designed to be simple to set up and maintain. WireGuard can be used for both site-to-site connection and client-server connections. WireGuard is relatively newer than IPSec, and is used by many people due to the fact that its download speed is enhanced by using fewer lines of code. WireGuard is also open source, which makes it easier for users to deploy and debug. This protocol is useful for processes that require faster download speeds, such as streaming video content or downloading large files.

IPSec VPN

IPSec is another VPN protocol that may be used to set up VPNs. Most VPN providers use IPSec to encrypt and authenticate data packets in order to establish secure, encrypted connections. Since IPSec is one of the earlier VPN protocols, many operating systems support IPSec from VPN providers.

Although IPSec and WireGuard are both VPN protocols, IPSec is older and more complex than WireGuard. Some clients may prefer IPSec due to its longer history of use, extensive security testing, and widespread adoption. However, others may prefer WireGuard because of its potential for better performance and simpler configuration.

Module 3: Secure Against Network Intrusions

How intrusions compromise your system

In this section of the course, you learned that every network has inherent vulnerabilities and could become the target of a network attack.

Attackers could have varying motivations for attacking your organization's network. They may have financial, personal, or political motivations, or they may be a disgruntled employee or an activist who disagrees with the company's values and wants to harm an organization's operations. Malicious actors can target any network. Security analysts must be constantly alert to potential vulnerabilities in their organization's network and take quick action to mitigate them.

In this reading, you'll learn about network interception attacks and backdoor attacks, and the possible impacts these attacks could have on an organization.

Network interception attacks

Network interception attacks work by intercepting network traffic and stealing valuable information or interfering with the transmission in some way.

Malicious actors can use hardware or software tools to capture and inspect data in transit. This is referred to as packet sniffing. In addition to seeing information that they are not entitled to, malicious actors can also intercept network traffic and alter it. These attacks can cause damage to an organization's network by inserting malicious code modifications or altering the message and interrupting network operations. For example, an attacker can intercept a bank transfer and change the account receiving the funds to one that the attacker controls.

Later in this course you will learn more about malicious packet sniffing, and other types of network interception attacks: on-path attacks and replay attacks.

Backdoor attacks

A backdoor attack is another type of attack you will need to be aware of as a security analyst. An organization may have a lot of security measures in place, including cameras, biometric scans and access codes, to ensure employees do not enter and exit unseen. However, an employee might work around the security measures by finding a backdoor to the building that is not as heavily monitored, allowing them to sneak out for the afternoon without being seen.

In cybersecurity, backdoors are weaknesses intentionally left by programmers or system and network administrators that bypass normal access control mechanisms. Backdoors are intended to help programmers conduct troubleshooting or administrative tasks. However, backdoors can also be installed by attackers after they've compromised an organization to ensure they have persistent access.

Once the hacker has entered an insecure network through a backdoor, they can cause extensive damage: installing malware, performing a denial of service (DoS) attack, stealing private information or changing other security settings that leaves the system vulnerable to other attacks. A DoS attack is an attack that targets a network or server and floods it with network traffic.

Possible impacts on an organization

As you've learned already, network attacks can have a significant negative impact on an organization. Let's examine some potential consequences.

- Financial: When a system is taken offline with a DoS attack or some other tactic, they prevent a company from performing tasks that generate revenue. Depending on the size of an organization, interrupted operations can cost millions of dollars. Reparation costs to rebuild software infrastructure and to pay large sums associated with potential ransomware can be financially difficult. In addition, if a malicious actor gets access to the personal information of the company's clients or customers, the company may face heavy litigation and settlement costs if customers seek legal recourse.
- Reputation: Attacks can also have a negative impact on the reputation of an organization. If it becomes public knowledge that a company has experienced a cyber attack, the public may become concerned about the security practices of the organization. They may stop trusting the company with their personal information and choose a competitor to fulfill their needs.
- Public safety: If an attack occurs on a government network, this can potentially impact the safety and welfare of the citizens of a country. In recent years, defense agencies across the globe are investing heavily in combating cyber warfare tactics. If a malicious actor gained access to a power grid, a public water system, or even a military defense communication system, the public could face physical harm due to a network intrusion attack.

Denial of Service (DoS) Attacks

- DoS attacks flood a network or server with traffic to disrupt normal business operations.
- The goal is to overload a network device, causing it to crash or become unresponsive to legitimate users.

Distributed Denial of Service (DDoS) Attacks

- DDoS attacks use multiple devices or servers from various locations to flood a target network.
- The use of numerous devices increases the likelihood of overwhelming the target server.

Common Network-Level DoS Attacks

- SYN Flood Attack: This attack exploits the TCP handshake process by flooding a server with SYN requests, overwhelming its available ports.
- ICMP Flood Attack: Attackers repeatedly send ICMP packets to a server, consuming bandwidth and causing it to crash.
- Ping of Death: This attack involves sending an oversized ICMP packet (larger than 64 kilobytes) to a vulnerable server, leading to a system crash.

Read tcpdump logs

A network protocol analyzer, sometimes called a packet sniffer or a packet analyzer, is a tool designed to capture and analyze data traffic within a network. They are commonly used as investigative tools to monitor networks and identify suspicious activity. There are a wide variety of network protocol analyzers available, but some of the most common analyzers include:

- SolarWinds NetFlow Traffic Analyzer
- ManageEngine OpManager
- Azure Network Watcher
- Wireshark
- tcpdump

This reading will focus exclusively on tcpdump, though you can apply what you learn here to many of the other network protocol analyzers you'll use as a cybersecurity analyst to defend against any network intrusions. In an upcoming activity, you'll review a tcpdump data traffic log and identify a DoS attack to practice these skills.

tcpdump

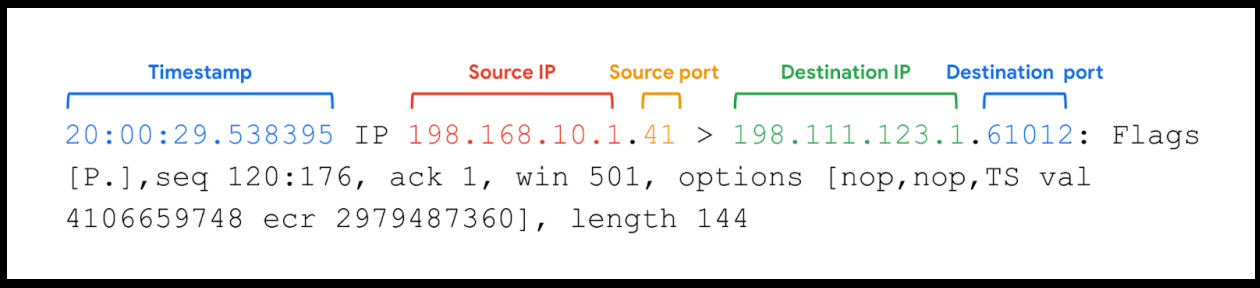
tcpdump is a command-line network protocol analyzer. It is popular, lightweight–meaning it uses little memory and has a low CPU usage–and uses the open-source libpcap library. tcpdump is text based, meaning all commands in tcpdump are executed in the terminal. It can also be installed on other Unix-based operating systems, such as macOS®. It is preinstalled on many Linux distributions.

tcpdump provides a brief packet analysis and converts key information about network traffic into formats easily read by humans. It prints information about each packet directly into your terminal. tcpdump also displays the source IP address, destination IP addresses, and the port numbers being used in the communications.

Interpreting output

tcpdump prints the output of the command as the sniffed packets in the command line, and optionally to a log file, after a command is executed. The output of a packet capture contains many pieces of important information about the network traffic.

– – Continued – –



Some information you receive from a packet capture includes:

- Timestamp: The output begins with the timestamp, formatted as hours, minutes, seconds, and fractions of a second.
- Source IP: The packet's origin is provided by its source IP address.
- Source port: This port number is where the packet originated.
- Destination IP: The destination IP address is where the packet is being transmitted to.
- Destination port: This port number is where the packet is being transmitted to.

Note: By default, tcpdump will attempt to resolve host addresses to hostnames. It'll also replace port numbers with commonly associated services that use these ports.

Common uses

tcpdump and other network protocol analyzers are commonly used to capture and view network communications and to collect statistics about the network, such as troubleshooting network performance issues. They can also be used to:

- Establish a baseline for network traffic patterns and network utilization metrics.
- Detect and identify malicious traffic
- Create customized alerts to send the right notifications when network issues or security threats arise.
- Locate unauthorized instant messaging (IM), traffic, or wireless access points.

However, attackers can also use network protocol analyzers maliciously to gain information about a specific network. For example, attackers can capture data packets that contain sensitive information, such as account usernames and passwords. As a cybersecurity analyst, It's important to understand the purpose and uses of network protocol analyzers.

Real-life DDoS attack

Previously, you were introduced to Denial of Service (DoS) attacks. You also learned that volumetric distributed DoS (DDoS) attacks overwhelm a network by sending unwanted data packets in such large quantities that the servers become unable to service normal users. This can be detrimental to an organization. When systems fail, organizations cannot meet their customers' needs. They often lose money, and in some cases, incur other losses. An organization's reputation may also suffer if news of a successful DDoS attack reaches consumers, who then question the security of the organization.

In this reading you'll learn about a 2016 DDoS attack against DNS servers that caused major outages at multiple organizations that have millions of daily users.

A DDoS targeting a widely used DNS server

In previous videos, you learned about the function of a DNS server. As a review, DNS servers translate website domain names into the IP address of the system that contains the information for the website. For instance, if a user were to type in a website URL, a DNS server would translate that into a numeric IP address that directs network traffic to the location of the website's server.

On the day of the DDoS attack we are studying, many large companies were using a DNS service provider. The service provider was hosting the DNS system for these companies. This meant that when internet users typed in the URL of the website they wanted to access, their devices would be directed to the right place. On October 21, 2016, the service provider was the victim of a DDoS attack.

Leading up to the attack

Before the attack on the service provider, a group of university students created a botnet with the intention to attack various gaming servers and networks. A botnet is a collection of computers infected by malware that are under the control of a single threat actor, known as the “bot-herder." Each computer in the botnet can be remotely controlled to send a data packet to a target system. In a botnet attack, cyber criminals instruct all the bots on the botnet to send data packets to the target system at the same time, resulting in a DDoS attack.

The group of university students posted the code for the botnet online so that it would be accessible to thousands of internet users and authorities wouldn’t be able to trace the botnet back to the students. In doing so, they made it possible for other malicious actors to learn the code to the botnet and control it remotely. This included the cyber criminals who attacked the DNS service provider.

The day of attack

At 7:00 a.m. on the day of the attack, the botnet sent tens of millions of DNS requests to the service provider. This overwhelmed the system and the DNS service shut down. This meant that all of the websites that used the service provider could not be reached. When users tried to access various websites that used the service provider, they were not directed to the website they typed in their browser. Outages for each web service occurred all over North America and Europe.

The service provider’s systems were restored after only two hours of downtime. Although the cyber criminals sent subsequent waves of botnet attacks, the DNS company was prepared and able to mitigate the impact.

Malicious Packet Sniffing

Understanding Packet Sniffing

- Packet sniffing involves using software to examine data packets as they traverse a network.
- These packets contain valuable information, including sender/receiver IP addresses and potentially sensitive personal or financial data in their body.

Malicious Use of Packet Sniffing

- Threat actors can use packet sniffing to intercept and spy on data not intended for them, similar to opening someone else's mail.
- They can insert themselves into a connection between devices to monitor and even alter data packets, such as changing bank account numbers.

Types of Packet Sniffing Attacks

- **Passive packet sniffing** involves reading data packets in transit without altering them, much like a postal worker reading mail they are supposed to deliver.

- **Active packet sniffing** involves manipulating data packets in transit, such as redirecting them or changing their content, akin to a neighbor intercepting and altering mail before delivery.

Preventing Malicious Packet Sniffing

- Using a Virtual Private Network (VPN) encrypts data, making it unreadable to attackers even if intercepted.
- Ensuring websites use HTTPS encrypts data during transmission, preventing eavesdropping.
- Avoiding unprotected public Wi-Fi networks, which often lack encryption, is crucial unless a VPN is used.

IP Spoofing

Understanding IP Spoofing

- IP spoofing involves an attacker altering the source IP address to impersonate an authorized system, bypassing firewall rules and gaining network access.
- The attacker pretends to be a legitimate user to communicate with a target computer.

Common IP Spoofing Attacks

- **On-path attacks**: The attacker positions themselves between two communicating devices, intercepts data, and learns IP and MAC addresses to impersonate either device.
- **Replay attacks**: A malicious actor intercepts a data packet and either delays it to cause connection issues or repeats it later to impersonate an authorized user.
- **Smurf attacks**: This combines a DDoS attack with IP spoofing, where the attacker floods an authorized user's IP address with packets, overwhelming the target and potentially bringing down the network.

Protecting Against IP Spoofing

- Encryption: Always implement encryption to prevent malicious actors from reading data during network transfers.
- Firewall configuration: Configure firewalls to reject incoming traffic from the internet that has the same IP address as the local network, as this indicates a spoofing attempt.

Overview of Interception Tactics

A closer review of packet sniffing

As you learned in a previous video, packet sniffing is the practice of capturing and inspecting data packets across a network. On a private network, data packets are directed to the matching destination device on the network.

The device’s Network Interface Card (NIC) is a piece of hardware that connects the device to a network. The NIC reads the data transmission, and if it contains the device’s MAC address, it accepts the packet and sends it to the device to process the information based on the protocol. This occurs in all standard network operations. However, a NIC can be set to promiscuous mode, which means that it accepts all traffic on the network, even the packets that aren’t addressed to the NIC’s device. You’ll learn more about NIC’s later in the program. Malicious actors might use software like Wireshark to capture the data on a private network and store it for later use. They can then use the personal information to their own advantage. Alternatively, they might use the IP and MAC addresses of authorized users of the private network to perform IP spoofing.

A closer review of IP spoofing

After a malicious actor has sniffed packets on the network, they can impersonate the IP and MAC addresses of authorized devices to perform an IP spoofing attack. Firewalls can prevent IP spoofing attacks by configuring it to refuse unauthorized IP packets and suspicious traffic. Next, you'll examine a few common IP spoofing attacks that are important to be familiar with as a security analyst.

On-path attack

An on-path attack happens when a hacker intercepts the communication between two devices or servers that have a trusted relationship. The transmission between these two trusted network devices could contain valuable information like usernames and passwords that the malicious actor can collect. An on-path attack is sometimes referred to as a meddler-in-the middle attack because the hacker is hiding in the middle of communications between two trusted parties.

Or, it could be that the intercepted transmission contains a DNS system look-up. You'll recall from an earlier video that a DNS server translates website domain names into IP addresses. If a malicious actor intercepts a transmission containing a DNS lookup, they could spoof the DNS response from the server and redirect a domain name to a different IP address, perhaps one that contains malicious code or other threats. The most important way to protect against an on-path attack is to encrypt your data in transit, e.g. using TLS.

Smurf attack

A smurf attack is a network attack that is performed when an attacker sniffs an authorized user's IP address and floods it with packets. Once the spoofed packet reaches the broadcast address, it is sent to all of the devices and servers on the network.

In a smurf attack, IP spoofing is combined with another denial of service (DoS) technique to flood the network with unwanted traffic. For example, the spoofed packet could include an Internet Control Message Protocol (ICMP) ping. As you learned earlier, ICMP is used to troubleshoot a network. But if too many ICMP messages are transmitted, the ICMP echo responses overwhelm the servers on the network and they shut down. This creates a denial of service and can bring an organization's operations to a halt.

An important way to protect against a smurf attack is to use an advanced firewall that can monitor any unusual traffic on the network. Most next generation firewalls (NGFW) include features that detect network anomalies to ensure that oversized broadcasts are detected before they have a chance to bring down the network.

DoS attack

As you've learned, once the malicious actor has sniffed the network traffic, they can impersonate an authorized user. A Denial of Service attack is a class of attacks where the attacker prevents the compromised system from performing legitimate activity or responding to legitimate traffic. Unlike IP spoofing, however, the attacker will not receive a response from the targeted host. Everything about the data packet is authorized including the IP address in the header of the packet. In IP spoofing attacks, the malicious actor uses IP packets containing fake IP addresses. The attackers keep sending IP packets containing fake IP addresses until the network server crashes.

Pro Tip: Remember the principle of defense-in-depth. There isn't one perfect strategy for stopping each kind of attack. You can layer your defense by using multiple strategies. In this case, using industry standard encryption will strengthen your security and help you defend from DoS attacks on more than one level.

Module 4: Security Hardening

Brute Force Attacks and OS Hardening

Brute force attacks

A brute force attack is a trial-and-error process of discovering private information. There are different types of brute force attacks that malicious actors use to guess passwords, including:

- ***Simple brute force attacks***. When attackers try to guess a user's login credentials, it's considered a simple brute force attack. They might do this by entering any combination of usernames and passwords that they can think of until they find the one that works.
- ***Dictionary attacks*** use a similar technique. In dictionary attacks, attackers use a list of commonly used passwords and stolen credentials from previous breaches to access a system. These are called "dictionary" attacks because attackers originally used a list of words from the dictionary to guess the passwords, before complex password rules became a common security practice.

Using brute force to access a system can be a tedious and time consuming process, especially when it's done manually. There are a range of tools attackers use to conduct their attacks.

Assessing vulnerabilities

Before a brute force attack or other cybersecurity incident occurs, companies can run a series of tests on their network or web applications to assess vulnerabilities. Analysts can use virtual machines and sandboxes to test suspicious files, check for vulnerabilities before an event occurs, or to simulate a cybersecurity incident.

Virtual machines (VMs)

Virtual machines (VMs) are software versions of physical computers. VMs provide an additional layer of security for an organization because they can be used to run code in an isolated environment, preventing malicious code from affecting the rest of the computer or system. VMs can also be deleted and replaced by a pristine image after testing malware.

VMs are useful when investigating potentially infected machines or running malware in a constrained environment. Using a VM may prevent damage to your system in the event its tools are used improperly. VMs also give you the ability to revert to a previous state. However, there are still some risks involved with VMs. There's still a small risk that a malicious program can escape virtualization and access the host machine.

You can test and explore applications easily with VMs, and it's easy to switch between different VMs from your computer. This can also help in streamlining many security tasks.

Sandbox environments

A sandbox is a type of testing environment that allows you to execute software or programs separate from your network. They are commonly used for testing patches, identifying and addressing bugs, or detecting cybersecurity vulnerabilities. Sandboxes can also be used to evaluate suspicious software, evaluate files containing malicious code, and simulate attack scenarios.

Sandboxes can be stand-alone physical computers that are not connected to a network; however, it is often more time- and cost-effective to use software or cloud-based virtual machines as sandbox environments. Note that some malware authors know how to write code to detect if the malware is executed in a VM or sandbox environment. Attackers can program their malware to behave as harmless software when run inside these types of testing environments.

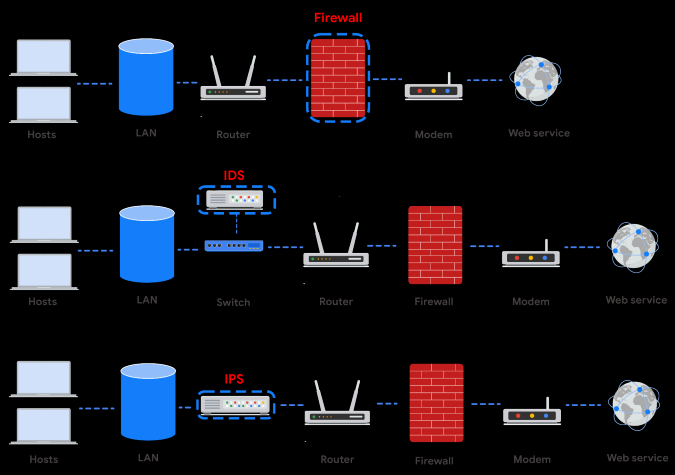
Prevention measures

Some common measures organizations use to prevent brute force attacks and similar attacks from occurring include:

- **Salting and hashing**: Hashing converts information into a unique value that can then be used to determine its integrity. It is a one-way function, meaning it is impossible to decrypt and obtain the original text. Salting adds random characters to hashed passwords. This increases the length and complexity of hash values, making them more secure.
- **Multi-factor authentication (MFA) and two-factor authentication (2FA)**: MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network. This verification happens using a combination of authentication factors: a username and password, fingerprints, facial recognition, or a one-time password (OTP) sent to a phone number or email. 2FA is similar to MFA, except it uses only two forms of verification.
- **CAPTCHA and reCAPTCHA**: CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It asks users to complete a simple test that proves they are human. This helps prevent software from trying to brute force a password. reCAPTCHA is a free CAPTCHA service from Google that helps protect websites from bots and malicious software.
- **Password policies**: Organizations use password policies to standardize good password practices throughout the business. Policies can include guidelines on how complex a password should be, how often users need to update passwords, whether passwords can be reused or not, and if there are limits to how many times a user can attempt to log in before their account is suspended.

– – Continued – –

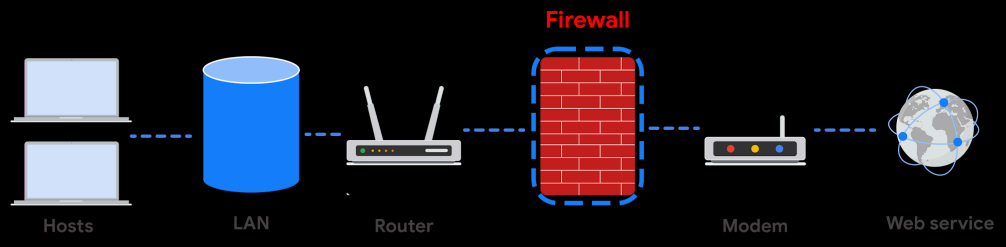
Network Security Applications



Take note of where each tool is located on the network. Each tool has its own place in the network's architecture. Security analysts are required to understand the network topologies shown in the diagrams throughout this reading.

Firewall

Most firewalls are similar in their basic functions. Firewalls allow or block traffic based on a set of rules. As data packets enter a network, the packet header is inspected and allowed or denied based on its port number. NGFWs are also able to inspect packet payloads. Each system should have its own firewall, regardless of the network firewall.

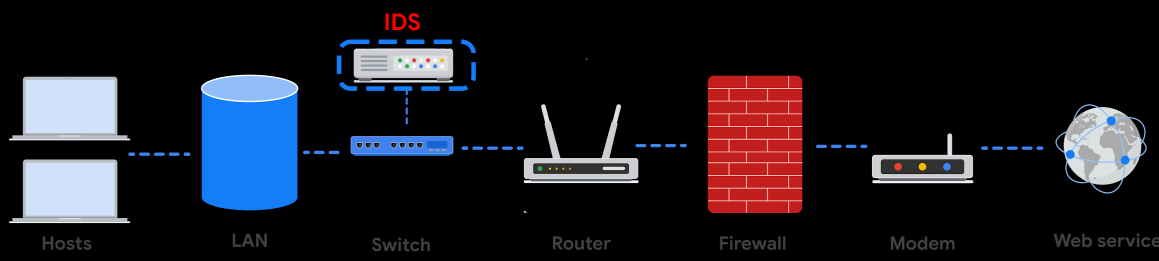


Intrusion Detection System

An intrusion detection system (IDS) is an application that monitors system activity and alerts on possible intrusions. An IDS alerts administrators based on the signature of malicious traffic.

The IDS is configured to detect known attacks. IDS systems often sniff data packets as they move across the network and analyze them for the characteristics of known attacks. Some IDS systems review not only for signatures of known attacks, but also for anomalies that could be the sign of malicious activity. When the IDS discovers an anomaly, it sends an alert to the network administrator who can then investigate further.

The limitations to IDS systems are that they can only scan for known attacks or obvious anomalies. New and sophisticated attacks might not be caught. The other limitation is that the IDS doesn't actually stop the incoming traffic if it detects something awry. It's up to the network administrator to catch the malicious activity before it does anything damaging to the network.



When combined with a firewall, an IDS adds another layer of defense. The IDS is placed behind the firewall and before entering the LAN, which allows the IDS to analyze data streams after network traffic that is disallowed by the firewall has been filtered out. This is done to reduce noise in IDS alerts, also referred to as false positives.

Intrusion Prevention System

An intrusion prevention system (IPS) is an application that monitors system activity for intrusive activity and takes action to stop the activity. It offers even more protection than an IDS because it actively stops anomalies when they are detected, unlike the IDS that simply reports the anomaly to a network administrator.

An IPS searches for signatures of known attacks and data anomalies. An IPS reports the anomaly to security analysts and blocks a specific sender or drops network packets that seem suspect.

The IPS (like an IDS) sits behind the firewall in the network architecture. This offers a high level of security because risky data streams are disrupted before they even reach sensitive parts of the network. However, one potential limitation is that it is inline: If it breaks, the connection between the private network and the internet breaks. Another limitation of IPS is the possibility of false positives, which can result in legitimate traffic getting dropped.

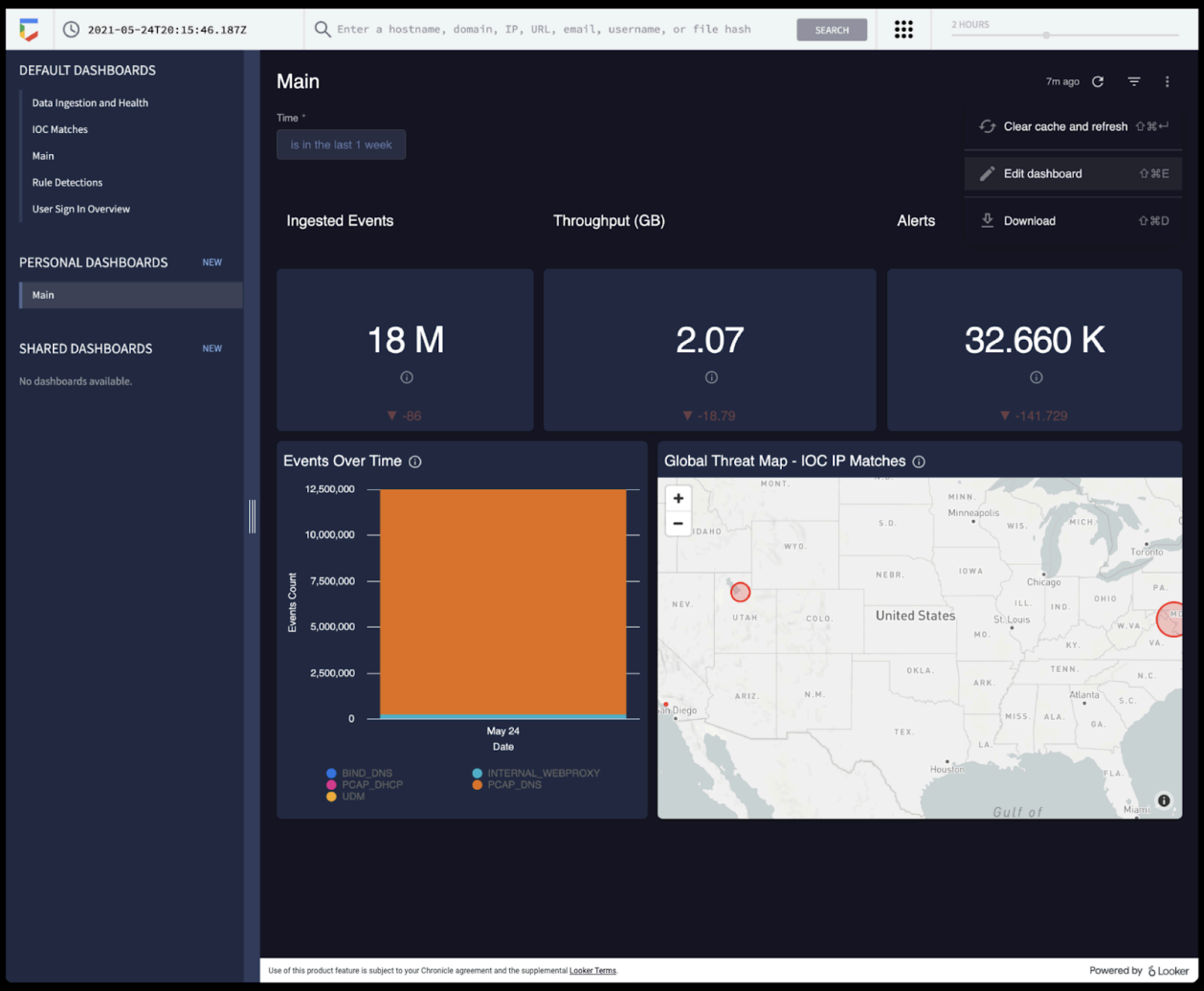
Full packet capture devices

Full packet capture devices can be incredibly useful for network administrators and security professionals. These devices allow you to record and analyze all of the data that is transmitted over your network. They also aid in investigating alerts created by an IDS.

Security Information and Event Management

A security information and event management system (SIEM) is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools work in real time to report suspicious activity in a centralized dashboard. SIEM tools additionally analyze network log data sourced from IDSs, IPSs, firewalls, VPNs, proxies, and DNS logs. SIEM tools are a way to aggregate security event data so that it all appears in one place for security analysts to analyze. This is referred to as a single pane of glass.

Below, you can review an example of a dashboard from Google Cloud's SIEM tool, Chronicle. Chronicle is a cloud-native tool designed to retain, analyze, and search data.



Splunk is another common SIEM tool. Splunk offers different SIEM tool options: Splunk Enterprise and Splunk Cloud. Both options include detailed dashboards which help security professionals to review and analyze an organization's data. There are also other similar SIEM tools available, and it's important for security professionals to research the different tools to determine which one is most beneficial to the organization.

A SIEM tool doesn't replace the expertise of security analysts, or of the network- and system-hardening activities covered in this course, but they're used in combination with other security methods. Security analysts often work in a Security Operations Center (SOC) where they can monitor the activity across the network. They can then use their expertise and experience to determine how to respond to the information on the dashboard and decide when the events meet the criteria to be escalated to oversight.

Secure the Cloud

Cloud security considerations

Many organizations choose to use cloud services because of the ease of deployment, speed of deployment, cost savings, and scalability of these options. Cloud computing presents unique security challenges that cybersecurity analysts need to be aware of.

Identity access management

Identity access management (IAM) is a collection of processes and technologies that helps organizations manage digital identities in their environment. This service also authorizes how users can use different cloud resources. A common problem that organizations face when using the cloud is the loose configuration of cloud user roles. An improperly configured user role increases risk by allowing unauthorized users to have access to critical cloud operations.

Configuration

The expanding cloud ecosystem introduces significant complexity to network management. Each cloud service necessitates precise configuration to uphold security and compliance standards. This challenge intensifies during cloud migrations, where ensuring accurate configuration for every migrated process is critical. Neglect in this area can expose the network to vulnerabilities. Misconfigured cloud services are a frequent source of security breaches, underscoring the importance of meticulous attention to detail by network administrators and architects during the migration and ongoing management of cloud services.

Attack surface

Cloud service providers (CSPs) offer numerous applications and services for organizations at a low cost.

Every service or application on a network carries its own set of risks and vulnerabilities and increases an organization's overall attack surface. An increased attack surface must be compensated for with increased security measures.

Cloud networks that utilize many services introduce lots of entry points into an organization's network. However, if the network is designed correctly, utilizing several services does not introduce more entry points into an organization's network design. These entry points can be used to introduce malware onto the network and pose other security vulnerabilities. It is important to note that CSPs often defer to more secure options, and have undergone more scrutiny than a traditional on-premises network.

Zero-day attacks

Zero-day attacks are an important security consideration for organizations using cloud or traditional on-premise network solutions. A zero day attack is an exploit that was previously unknown. CSPs are more likely to know about a zero day attack occurring before a traditional IT organization does. CSPs have ways of patching hypervisors and migrating workloads to other virtual machines. These methods ensure the customers are not impacted by the attack. There are also several tools available for patching at the operating system level that organizations can use.

Visibility and tracking

Network administrators have access to every data packet crossing the network with both on-premise and cloud networks. They can sniff and inspect data packets to learn about network performance or to check for possible threats and attacks.

This kind of visibility is also offered in the cloud through flow logs and tools, such as packet mirroring. CSPs take responsibility for security in the cloud, but they do not allow the organizations that use their infrastructure to monitor traffic on the CSP's servers. Many CSPs offer strong security measures to protect their infrastructure. Still, this situation might be a concern for organizations that are accustomed to having full access to their network and operations. CSPs pay for third-party audits to verify how secure a cloud network is and identify potential vulnerabilities. The audits can help organizations identify whether any vulnerabilities originate from on-premise infrastructure and if there are any compliance lapses from their CSP.

Things change fast in the cloud

CSPs are large organizations that work hard to stay up-to-date with technology advancements. For organizations that are used to being in control of any adjustments made to their network, this can be a potential challenge to keep up with. Cloud service updates can affect security considerations for the organizations using them. For example, connection configurations might need to be changed based on the CSP's updates.

Organizations that use CSPs usually have to update their IT processes. It is possible for organizations to continue following established best practices for changes, configurations, and other security considerations. However, an organization might have to adopt a different approach in a way that aligns with changes made by the CSP.

Cloud networking offers various options that might appear attractive to a small company—options that they could never afford to build on their own premises. However, it is important to consider that each service adds complexity to the security profile of the organization, and they will need security personnel to monitor all of the cloud services.

Shared responsibility model

A commonly accepted cloud security principle is the shared responsibility model. The shared responsibility model states that the CSP must take responsibility for security involving the cloud infrastructure, including physical data centers, hypervisors, and host operating systems. The company using the cloud service is responsible for the assets and processes that they store or operate in the cloud.

The shared responsibility model ensures that both the CSP and the users agree about where their responsibility for security begins and ends. A problem occurs when organizations assume that the CSP is taking care of security that they have not taken responsibility for. One example of this is cloud applications and configurations. The CSP takes responsibility for securing the cloud, but it is the organization's responsibility to ensure that services are configured properly according to the security requirements of their organization.

Cryptography and Cloud Security

Cloud security hardening

There are various techniques and tools that can be used to secure cloud network infrastructure and resources. Some common cloud security hardening techniques include incorporating IAM, hypervisors, baselining, cryptography, and cryptographic erasure.

Identity access management (IAM)

Identity access management (**IAM**) is a collection of processes and technologies that helps organizations manage digital identities in their environment. This service also authorizes how users can leverage different cloud resources.

Hypervisors

A hypervisor abstracts the host's hardware from the operating software environment. There are two types of hypervisors. Type one hypervisors run on the hardware of the host computer. An example of a type one hypervisor is VMware®'s ESXi. Type two hypervisors operate on the software of the host computer. An example of a type two hypervisor is VirtualBox. Cloud service providers (CSPs) commonly use type one hypervisors. CSPs are responsible for managing the hypervisor and other virtualization components. The CSP ensures that cloud resources and cloud environments are available, and it provides regular patches and updates. Vulnerabilities in hypervisors or misconfigurations can lead to virtual machine escapes (VM escapes). A VM escape is an exploit where a malicious actor gains access to the primary hypervisor, potentially the host computer and other VMs. As a CSP customer, you will rarely deal with hypervisors directly.

Baselining

Baselining for cloud networks and operations cover how the cloud environment is configured and set up. A baseline is a fixed reference point. This reference point can be used to compare changes made to a cloud environment. Proper configuration and setup can greatly improve the security and performance of a cloud environment. Examples of establishing a baseline in a cloud environment include: restricting access to the admin portal of the cloud environment, enabling password management, enabling file encryption, and enabling threat detection services for SQL databases.

Cryptography in the cloud

Cryptography can be applied to secure data that is processed and stored in a cloud environment. Cryptography uses encryption and secure key management systems to provide data integrity and confidentiality. Cryptographic encryption is one of the key ways to secure sensitive data and information in the cloud.

Encryption is the process of scrambling information into ciphertext, which is not readable to anyone without the encryption key. Encryption primarily originated from manually encoding messages and information using an algorithm to convert any given letter or number to a new value. Modern encryption relies on the secrecy of a key, rather than the secrecy of an algorithm. Cryptography is an important tool that helps secure cloud networks and data at rest to prevent unauthorized access. You'll learn more about cryptography in-depth in an upcoming course.

Cryptographic erasure

Cryptographic erasure is a method of erasing the encryption key for the encrypted data. When destroying data in the cloud, more traditional methods of data destruction are not as effective. Crypto-shredding is a newer technique where the cryptographic keys used for decrypting the data are destroyed. This makes the data undecipherable and prevents anyone from decrypting the data. When crypto-shredding, all copies of the key need to be destroyed so no one has any opportunity to access the data in the future.

Key Management

Modern encryption relies on keeping the encryption keys secure. Below are the measures you can take to further protect your data when using cloud applications:

- Trusted platform module (TPM). TPM is a computer chip that can securely store passwords, certificates, and encryption keys.
- Cloud hardware security module (CloudHSM). CloudHSM is a computing device that provides secure storage for cryptographic keys and processes cryptographic operations, such as encryption and decryption.

Organizations and customers do not have access to the cloud service provider (CSP) directly, but they can request audits and security reports by contacting the CSP. Customers typically do not have access to the specific encryption keys that CSPs use to encrypt the customers' data. However, almost all CSPs allow customers to provide their own encryption keys, depending on the service the customer is accessing. In turn, the customer is responsible for their encryption keys and ensuring the keys remain confidential. The CSP is limited in how they can help the customer if the customer's keys are compromised or destroyed. One key benefit of the shared responsibility model is that the customer is not entirely responsible for maintenance of the cryptographic infrastructure. Organizations can assess and monitor the risk involved with allowing the CSP to manage the infrastructure by reviewing a CSPs audit and security controls. For federal contractors, FEDRAMP provides a list of verified CSPs.