BAIT1093 Introduction to Computer Security

Chapter 4: Communication and Network Security

Topics

4.1 Network Security Overview

4.2 Threats and Common Attacks to Network

4.3 Network Security Components and Defense Mechanisms

4.1 Network Security Overview [1]

- With the rapid growth of interest in the Internet, network security has become a major concern to companies throughout the world.
- Information and tools needed to penetrate the security of corporate networks are widely available nowadays.
- Because of this increased focus on network security, network administrators often spend more effort protecting their networks than on actual network set-up and administration.

4.1 Network Security Overview [1]

- Tools that probe for system vulnerabilities and some of the scanning and intrusion detection packages and appliances, but these tools only point out areas of weakness and may not provide a means to protect networks from all possible attacks.
- Thus, network administrators need to keep abreast of the large number of security issues in today's world.

4.1 Network Security Overview [1]

- The main goal of network security is to protect confidential information.
- Confidential information can reside in two states on a network.
  - Physical storage media (such as hard drive or memory)
  - In transit across the network in the form of packets ← involved network security issues

4.2 Threats and Common Attacks to Network[1]

- When a private network is connected to the Internet, it is estimated that the private network is connected to more than 50,000 unknown networks and all their users.
- Although such connections open the door to many useful applications and provide great opportunities for information sharing, most private networks contain some information that should not be shared with outside users on the Internet. In addition, not all Internet users are involved in lawful activities.

4.2 Threats and Common Attacks to Network[1]

- These two statements foreshadow the key questions behind most security issues on the Internet:
  - How do you protect confidential information from those who do not explicitly need to access it?
  - How do you protect your network and its resources from malicious users and accidents that originate outside your network?
- Common threats to network is theft, destruction, corruption , and introduction of information that can cause irreparable damage to sensitive and confidential data.

4.2 Threats and Common Attacks to Network[1]

Common Attacks to Network

- Network Packet Sniffers
- IP spoofing attacks and Denial of Service (DoS) attacks
- Distribution of sensitive internal information to external sources
- Man-in-the-middle attacks

4.2 Threats and Common Attacks to Network[1]

1) Network Packet Sniffers

- Before sending a large information to a network, usually the information will be broken into smaller pieces. These smaller pieces are called **network packets** .
- Several network applications distribute network packets in clear text; that is, the information sent across the network is not encrypted. Encryption is the transformation, or scrambling, of a message into an unreadable format by using a mathematical algorithm.
- Because the network packets are not encrypted, they can be processed and understood by any application that can pick them up off the network and process them.

4.2 Threats and Common Attacks to Network[1]

1) Network Packet Sniffers

- A network protocol specifies how packets are identified and labeled, which enables a computer to determine whether a packet is intended for it. Because the specifications for network protocols, such as TCP/IP, are widely published, a third party can easily interpret the network packets and develop a packet sniffer.
- The real threat today results from the numerous freeware and shareware packet sniffers that are available, which do not require the user to understand anything about the underlying protocols.
- A packet sniffer is a software application that uses a network adapter card in promiscuous mode (a mode in which the network adapter card sends all packets received on the physical network wire to an application for processing) to capture all network packets that are sent across a local-area network.

4.2 Threats and Common Attacks to Network[1]

1) Network Packet Sniffers

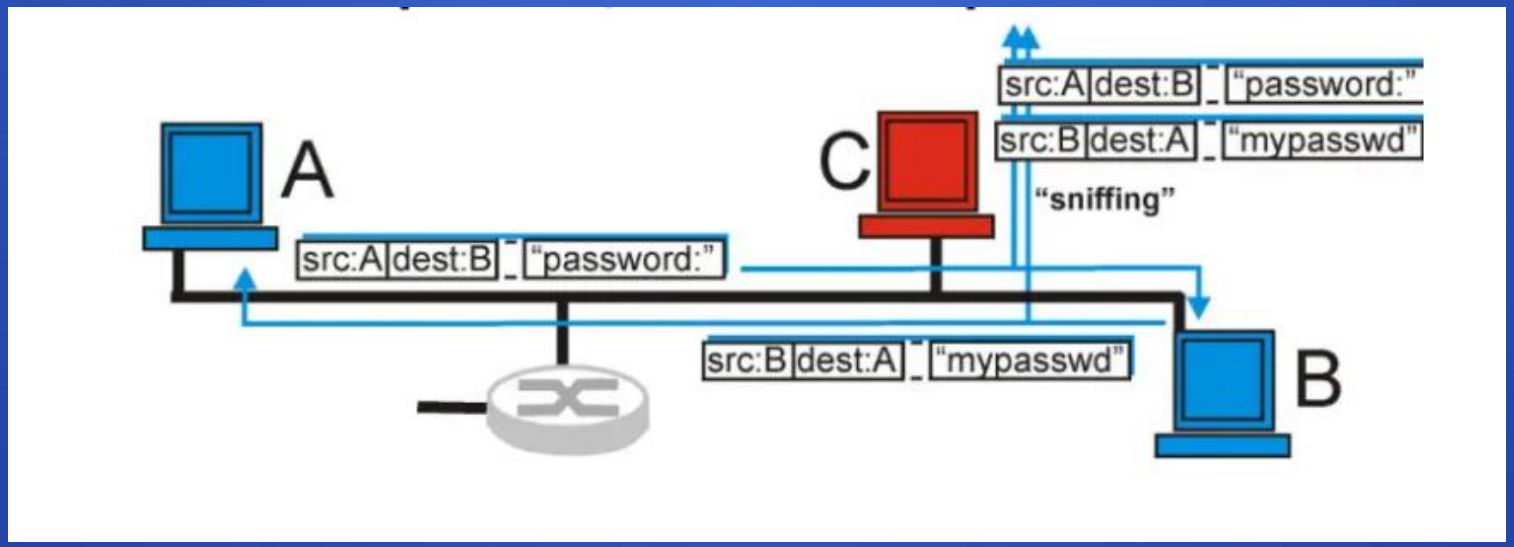
- Because several network applications distribute network packets in clear text, a packet sniffer can provide its user with meaningful and often sensitive information, such as user account names and passwords.
- If you use networked databases, a packet sniffer can provide an attacker with information that is queried from the database, as well as the user account names and passwords used to access the database.

.

4.2 Threats and Common Attacks to Network[1]

1) Network Packet Sniffers

- One serious problem with acquiring user account names and passwords is that users often reuse their login names and passwords across multiple applications, which is likely to gain access to other corporate resources.



Source: https://blog.flashrouters.com/2021/11/15/how-to-protect-yourself-from-packet-sniffers/

4.2 Threats and Common Attacks to Network[1]

1) Network Packet Sniffers

- When an attacker obtains the correct account information, he or she has the information about your network. In a worst-case scenario, an attacker gains access to a system-level user account, which the attacker uses to create a new account that can be used at any time as a back door to get into your network and its resources.
- The attacker can modify system-critical files, such as the password for the system administrator account, the list of services and permissions on file servers, and the login details for other computers that contain confidential information.

4.2 Threats and Common Attacks to Network[1]

1) Network Packet Sniffers

- Packet sniffers provide information about the topology of your network that many attackers find useful. This information, such as what computers run which services, how many computers are on your network, which computers have access to others, and so on, can be deduced from the information contained within the packets that are distributed across your network as part of necessary daily operations.

4.2 Threats and Common Attacks to Network[1]

2) IP Spoofing and Denial-of-Service Attack

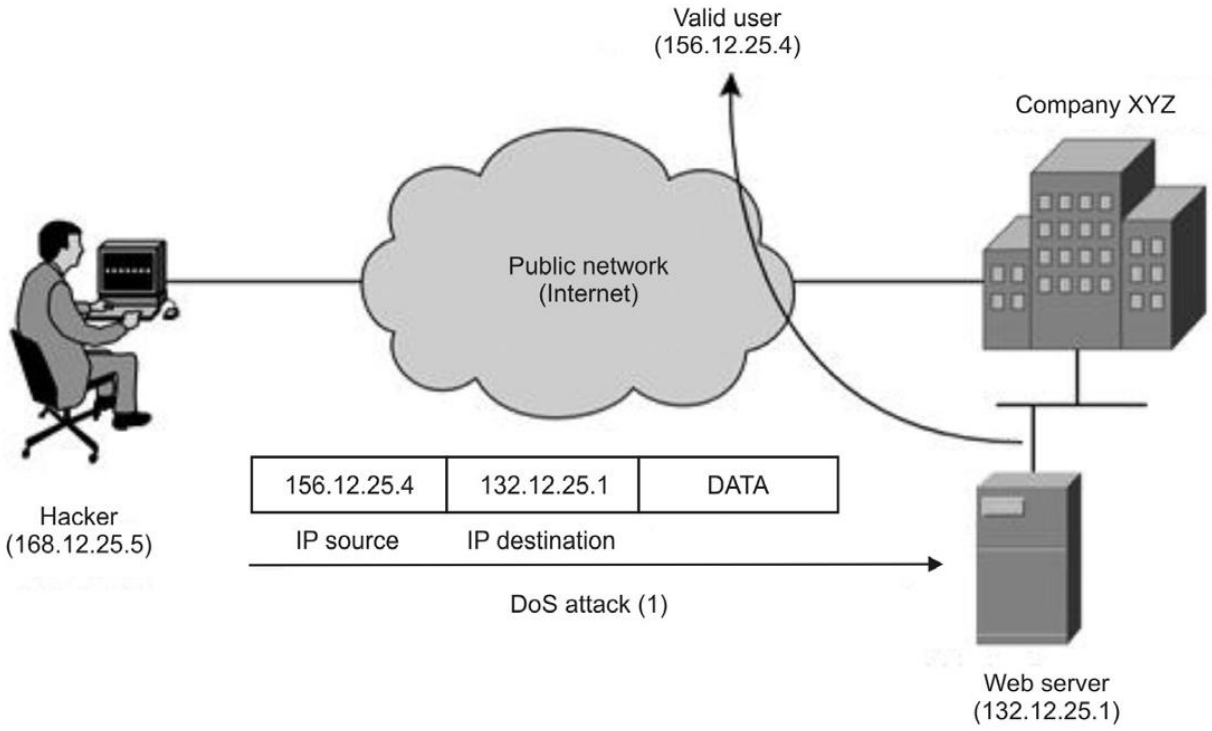


FIGURE 5.5 IP Spoofing and denial-of-service attacks

4.2 Threats and Common Attacks to Network[1]

2) IP Spoofing and Denial-of-Service Attack

- An IP spoofing attack occurs when an attacker outside your network pretends to be a trusted computer. This is facilitated either by using an IP address that is within the range of IP addresses for your network, or by using an authorized external IP address that you trust and to which you want to provide access to specified resources on your network.
- Normally, an IP spoofing attack is limited to the injection of data or commands into an existing stream of data passed between a client and server application or a peer-to-peer network connection. To enable bidirectional communication, the attacker must change all routing tables to point to the spoofed IP address. If the changes to the routing table is successful, he can receive all the network packets that are addressed to the spoofed address and can reply just as any trusted user can.

4.2 Threats and Common Attacks to Network[1]

2) IP Spoofing and Denial-of-Service Attack

- After IP spoofing, the attacker do not worry about receiving any response from the targeted host. The system receiving the requests becomes busy trying to establish a return communications path with the initiator, which is not using a valid IP address.
- The targeted host receives a TCP SYN and returns a SYN-ACK. It then remains in a wait state, anticipating the completion of the TCP handshake that never happens. Each wait state uses system resources until, eventually, the host cannot respond to other legitimate requests. This is called a Denial-of- Service (DOS) attack.
- IP spoofing and DOS attacks may attacked by people who are external or internal to the network.

4.2 Threats and Common Attacks to Network[1]

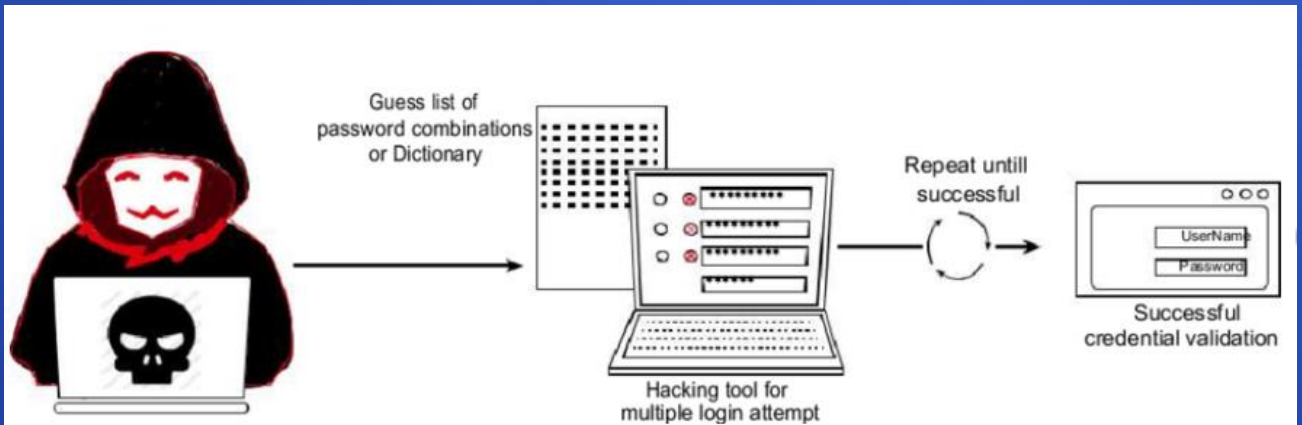
3) Password Attacks

- Password attacks can be implemented using several different methods, including brute-force attacks, Trojan horse programs, IP spoofing, and packet sniffers. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account and/or password; these repeated attempts are called brute-force attacks.
- A brute-force attack is performed using a dictionary program that runs across the network and attempts to log in to a shared resource, such as a server.

4.2 Threats and Common Attacks to Network[1]

3) Password Attacks

- When an attacker successfully gains access to a resource, that person has the same rights as the user whose account has been compromised to gain access to that resource.
- If this account has sufficient privileges, the attacker can create a back door for future access, without concern for any status and password changes to the compromised user account.



Depiction of generalised principle of a Password Attack

Source: https://www.researchgate.net/figure/Depiction-of-generalised-principle-of-a-Password-Attack_fig2_363888650

4.2 Threats and Common Attacks to Network[1]

4) Distribution of Sensitive Internal Information to External Sources

- Controlling the distribution of sensitive information is at the core of a network security policy.
- The majority of computer break-ins that organizations suffer are at the hands of disgruntled present or former employees. At the core of these security breaches is the distribution of sensitive information to competitors or others that will use it to your disadvantage.

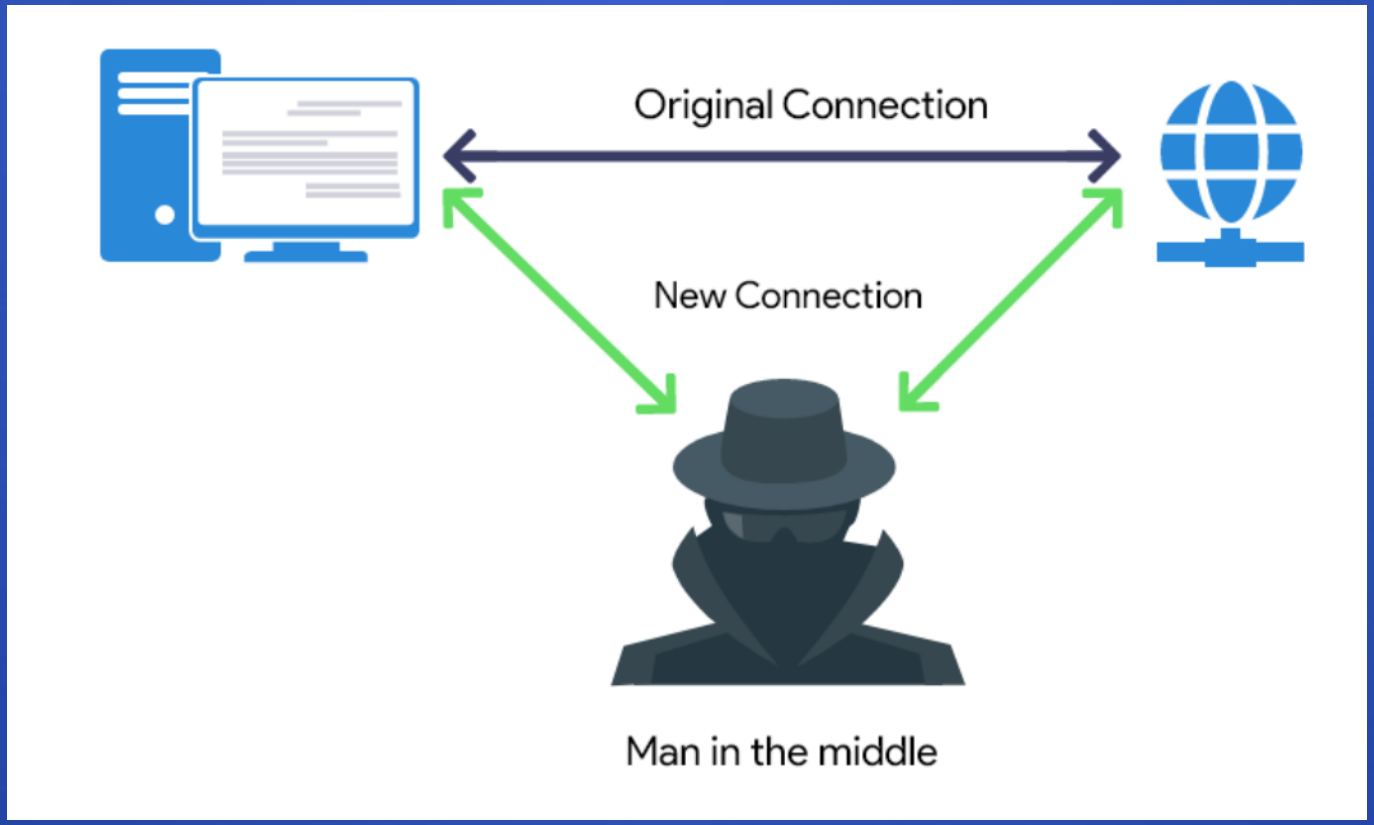
4.2 Threats and Common Attacks to Network[1]

4) Distribution of Sensitive Internal Information to External Sources

- An outside intruder can use password and IP spoofing attacks to copy information, and an internal user can easily place sensitive information on an external computer or share a drive on the network with other users. For example, an internal user could place a file on an external FTP server without ever leaving his or her desk. The user could also E-mail an attachment that contains sensitive information to an external user.

4.2 Threats and Common Attacks to Network[1]

5) Man-in-the-Middle Attack



Source: https://beaglesecurity.com/blog/article/man-in-the-middle-attack.html

4.2 Threats and Common Attacks to Network[1]

5) Man-in-the-Middle Attack

- A man-in-the-middle attack requires that the attacker has access to the network packets that come across the networks. An example of such a configuration could be someone who is working for your Internet Service Provider (ISP), who can gain access to all network packets transferred between your network and any other network. Such attacks are often implemented using network packet sniffers and routing and transport protocols.
- The possible uses of such attacks are the theft of information, hijacking of an ongoing session to gain access to your internal network resources, traffic analysis to derive information about your network and its users, denial-of-service, corruption of transmitted data, and introduction of new information into network sessions.

4.3 Network Security Components and Defense Mechanisms [2]

- Malware Scanners
- Firewalls
- Antispyware
- Intrusion Detection Systems (IDSs)
- Digital Certificates
- Secure Socket Layer (SSL) or Transport Layer Security (TLS)
- Virtual Private Networks
- Wi-Fi Security

4.3 Network Security Components and Defense Mechanisms [2]

Malware Scanners

- Software that tries to prevent a malware from infecting a system
- Malware scanners work in 2 ways:
  - whether match with any signature from a list of all known malware definitions
    - Files that lists known malware and their file sizes, properties and behaviours.
    - Periodically updated by vendors of malware scanners
    - Typically a small file, often called a .dat file (short for data).
  - Look for malware-like behaviour
    - Whether the process is manipulating the Registry or looking through other documents.

4.3 Network Security Components and Defense Mechanisms [2]

Malware Scanners

- Malware-Scanning Techniques
  - Email and attachment scanning
    - Email and its attachment are scanned before a user have a chance to open them and release malware on the system.
  - Download scanning
    - Files downloaded via a web link or an FTP program should be scanned to check whether it is infected or not
  - File Scanning
    - Files on the system are checked on a regular basis and on demand basis

4.3 Network Security Components and Defense Mechanisms [2]

Malware Scanners

- Malware-Scanning Techniques (Cont.)
  - Heuristic Scanning
    - To detect a malware using behavior analysis instead of using malware definition list. However, there are chance of false positive and false negative.
  - Sandbox
    - A separate protected area of memory on the system for any file or attachment to be run and tested whether it is an infected files/attachment. Will not affect the operating system.
  - Machine Learning
    - Allow malware scanners to adapt to changing attacks using machine learning algorithms. However, still not well developed and more research needs to be done.

4.3 Network Security Components and Defense Mechanisms [2]

Firewalls

- A barrier between two computers or computer systems or different networks.
- Filter incoming packets based on certain parameters, such as packet size, source IP address, protocol, and destination port.
- Linux and Windows by default has a simple firewall. All firewalls at end devices and at network perimeter should be turned on, installed with the right configuration.
- In an organizational setting, a dedicated firewall between internal network and the outside network should be installed. Can be a router with a built-in firewall capabilities or it might be a server that is dedicated solely to run firewall software.

4.3 Network Security Components and Defense Mechanisms [2]

Firewalls

- Benefits of Firewalls:
  - Block certain traffic based on a set of rules which determine which traffic is allowed and which traffic is not allowed.
  - Prevent a Denial of Service (DoS) attack
  - Prevent external threat actors from scanning the internal details of a company's network.
- Limitations of Firewalls:
  - Cannot block every attack. Eg:
    - It will not block users to download a Trojan horse.
    - Cannot stop internal attacks.

4.3 Network Security Components and Defense Mechanisms [2]

Firewalls

- Firewall Types:
  - Stateless Packet Filtering
  - Stateful Packet Inspection
  - Application

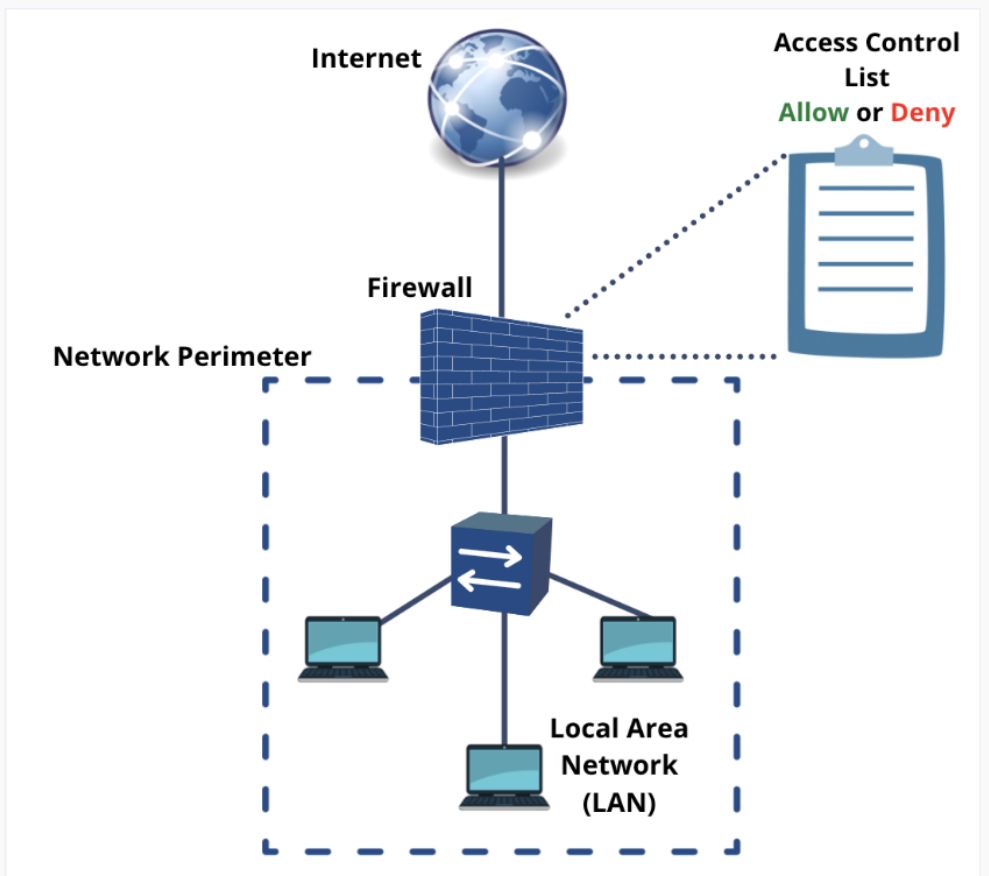
4.3 Network Security Components and Defense Mechanisms [2]

Firewalls → 1) Stateless Packet Filtering

- Basic packet filtering is the simplest form of firewall.
- Look at packets and check to see if each packet meets the firewall rules.
- Common to consider 3 questions:
  - Is this packet using a **protocol** that the firewall allows?
  - Is this packet destined for a **port** that the firewall allows?
  - Is the packet coming from an **IP address** that the firewall has not blocked?
- Each packet is treated as a singular event, without reference to the preceding conversation.
- This makes packet filtering firewall quite susceptible to some DoS attacks, such as SYN floods.

4.3 Network Security Components and Defense Mechanisms [2]

Firewalls → 1) Stateless Packet Filtering



Source: https://digital.com/best-vpn-services/what-are-the-type-of-firewalls/

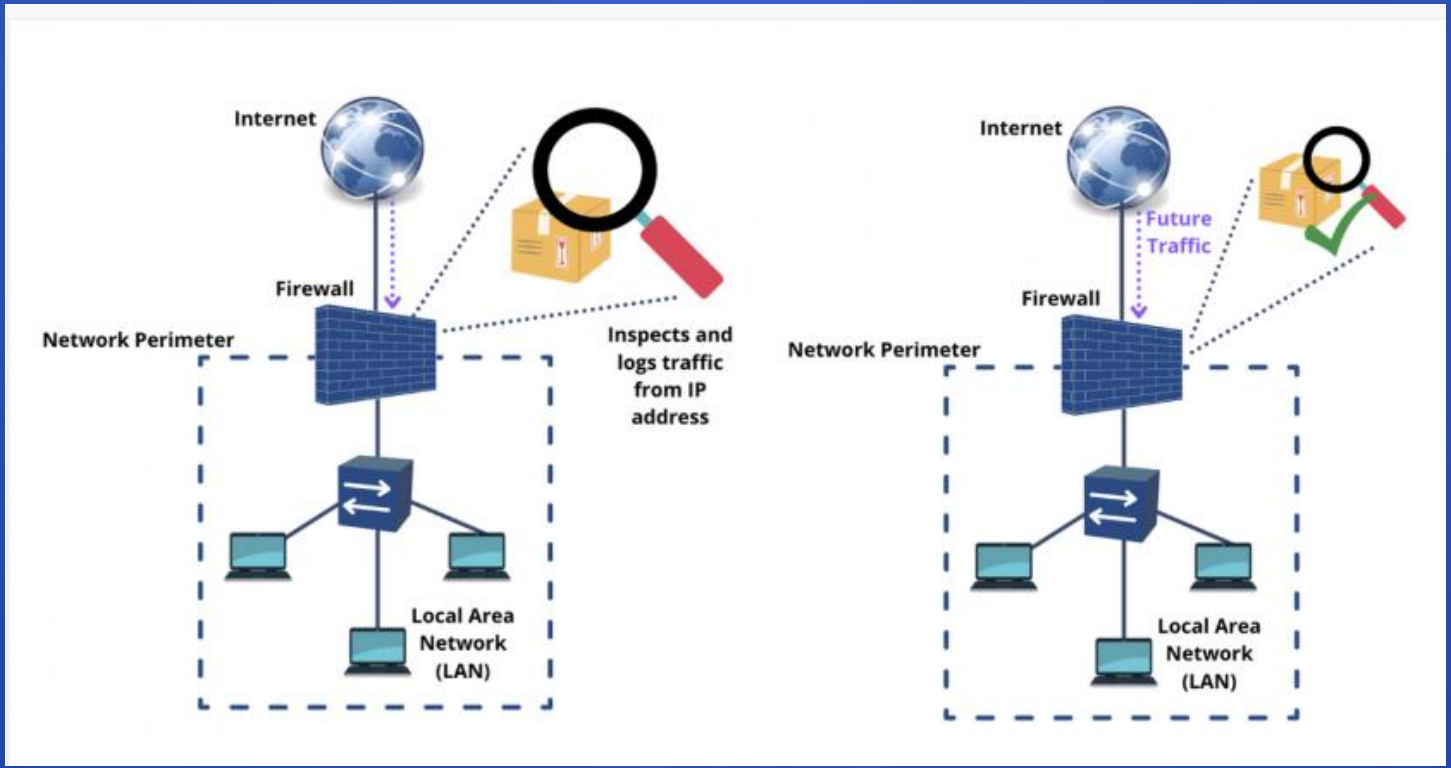
4.3 Network Security Components and Defense Mechanisms [2]

Firewalls → 2) Stateful Packet Inspection

- Any stateful packet inspection (SPI) firewall will examine each packet and deny or permit access based not only on the examination of the current packet but also on data derived from previous packets in the conversation.
- The firewall is therefore aware of the context in which a specific packet was sent. This makes SPI firewall less susceptible to ping floods, SYN floods and spoofing.
- Eg. The firewall detects that the current packet is an ICMP packet and a stream of several thousand packets have been continuously coming from the same source IP, the firewall will see that this is clearly a DoS attack, and it will block the packets.
- A SPI firewall can look at the actual contents of a packet, which allows for some very advanced filtering capabilities. Most high-end firewalls use the SPI method and this is the recommended type of firewall.

4.3 Network Security Components and Defense Mechanisms [2]

Firewalls → 2) Stateful Packet Inspection



Source: https://digital.com/best-vpn-services/what-are-the-type-of-firewalls/

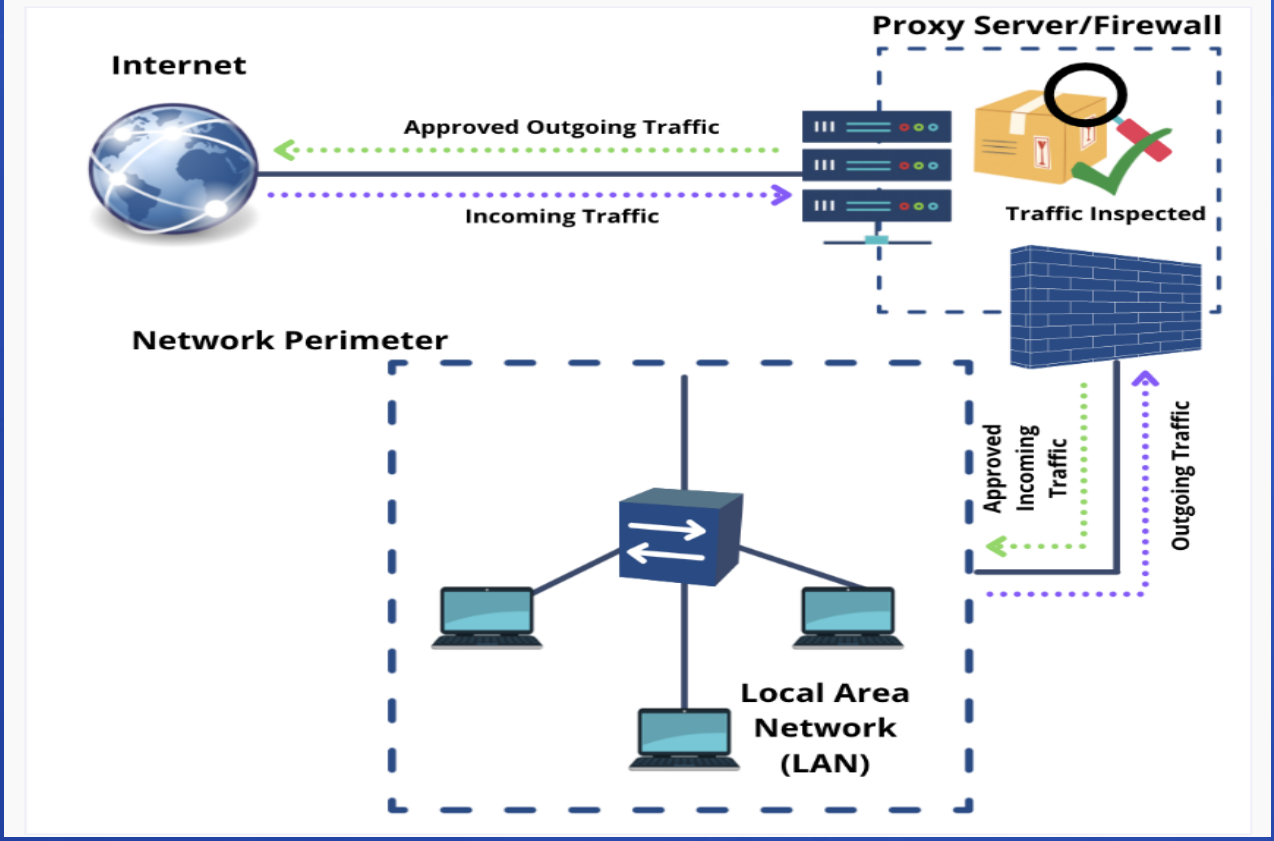
4.3 Network Security Components and Defense Mechanisms [2]

Firewalls → 3) Application Gateway (also known as application proxy or application-level proxy)

- Program that runs on a firewall
- When a client program, such as a web browser, establishes a connection to a destination service, such as a web server, it connects to an application gateway, or proxy.
- The client then negotiates with the proxy server in order to gain access to the destination service.
- The proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall.
- This process actually creates two connections. There is one connection between the client and the proxy server, and there is another connection between proxy server and the destination.

4.3 Network Security Components and Defense Mechanisms [2]

Firewalls → 3) Application Gateway (also known as application proxy or application-level proxy)



Source: https://digital.com/best-vpn-services/what-are-the-type-of-firewalls/

4.3 Network Security Components and Defense Mechanisms [2]

Firewalls → 3) Application Gateway (Cont.)

- Once a connection is established, the application gateway makes all the decisions about which packets to forward.
- It is common to have an application firewall that also includes stateful packet inspection.

4.3 Network Security Components and Defense Mechanisms [2]

Antispyware

- Scans devices whether there is any spyware running.
- Check against a list of known spyware which are included in the antimalware solutions.
- It is advisable to enhanced web browser's security settings, cautious about downloads from email or any website,and avoid using unnecessary add-ins or extensions.

4.3 Network Security Components and Defense Mechanisms [2]

IDSs

- Inspects all inbound and outbound port activity on a machine/firewall/system, looking for patterns that might indicate break-in attempts.
- For example, if an IDS finds that a series of ICMP packets were sent to each port in sequence, this probably indicates that the system is being scanned by network-scanning software.
- IDS category:
  - Passive IDSs
  - Active IDSs (also called an intrusion prevention system, or IPSs)

4.3 Network Security Components and Defense Mechanisms [2]

IDSs → 1) Passive IDSs

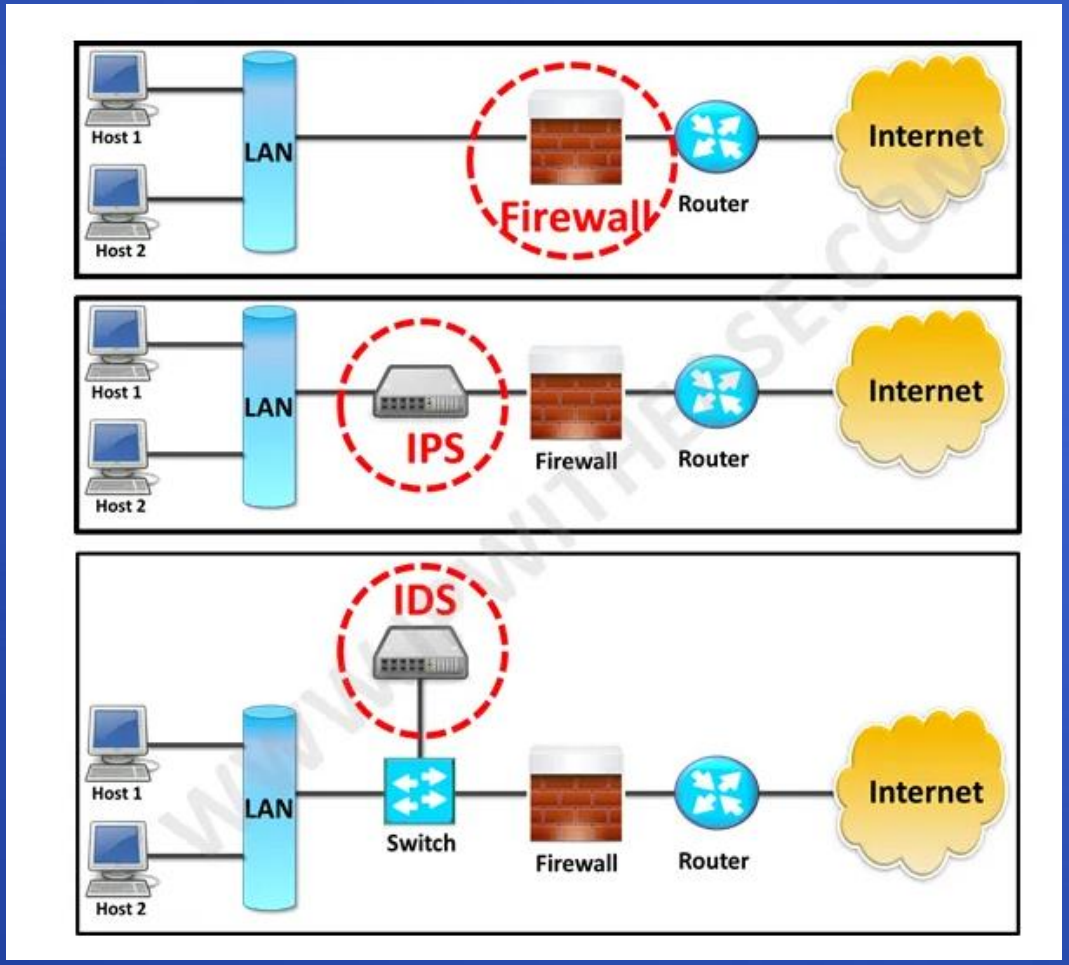
- Just monitor suspicious activity and logs it.
- May notify the administrator of the activity in question
- Any modern system should have a minimum of a passive IDS along with the firewall, antimalware and other basic security measures

4.3 Network Security Components and Defense Mechanisms [2]

IDSs → 2) Active IDSs or IPS

- Takes the added step of shutting down the suspicious communication.
- Possible to have a false positive. Might suspect something is an attack when in fact it is a legitimate traffic. Eg of a false positive case → IDS is looking at the threshold monitoring to determine if any attack is occurring. A particular user usually works from 8 am to 5 pm, use relatively small amount of bandwidth. If the IDS detects the user use the system at 10 pm using 10 times his normal bandwidth, it might perceive it as an attack and shut down the offending traffic. However, it may be found later that this was a legitimate user working late on a critical project that was due to a client the next day, and the IPS prevented that from happening

4.3 Network Security Components and Defense Mechanisms [2]



Firewall vs IPS vs IDS

Source: https://ipwithease.com/firewall-vs-ips-vs-ids/

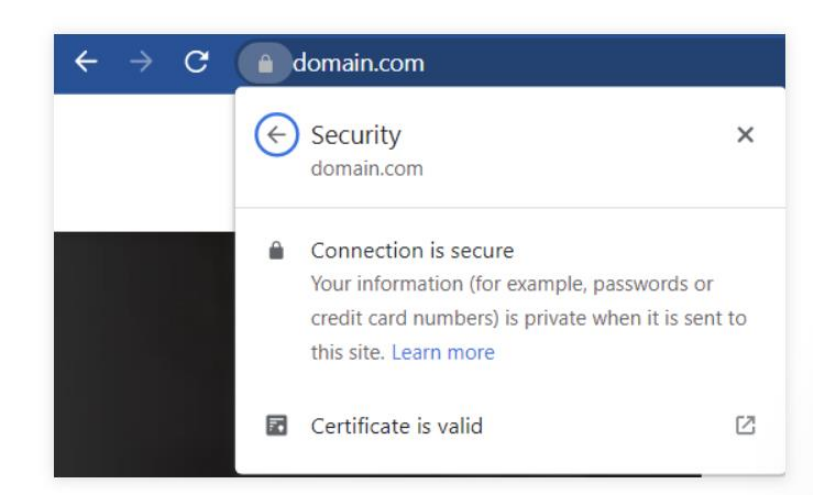
4.3 Network Security Components and Defense Mechanisms [2]

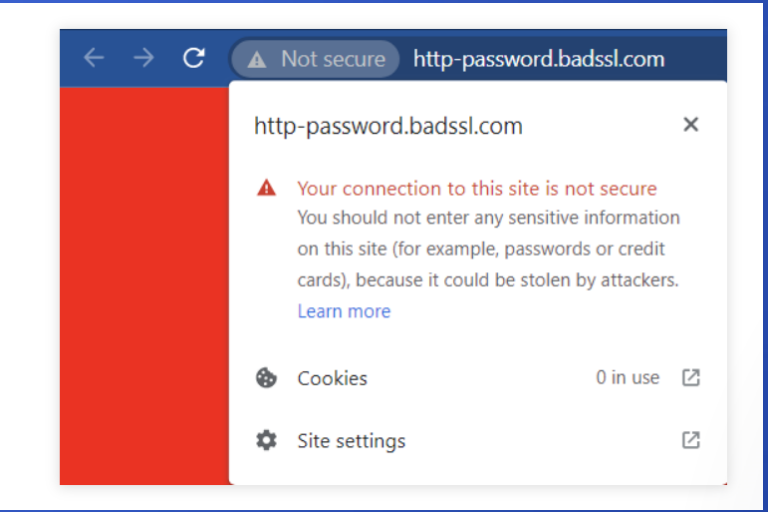
Digital Certificates

- contains the user's public key along with other information to encrypt messages.
- Provide a means for authenticating that the holder of the certificate is who he or she claims to be.
- X.509 is an international standard for the format and information contained in a digital certificate.
- X.509 is the most common type of digital certificate in the world.
- It is a digital document that contains a public key signed by the trusted third party that is known as a certificate authority (CA).

4.3 Network Security Components and Defense Mechanisms [2]

Digital Certificates



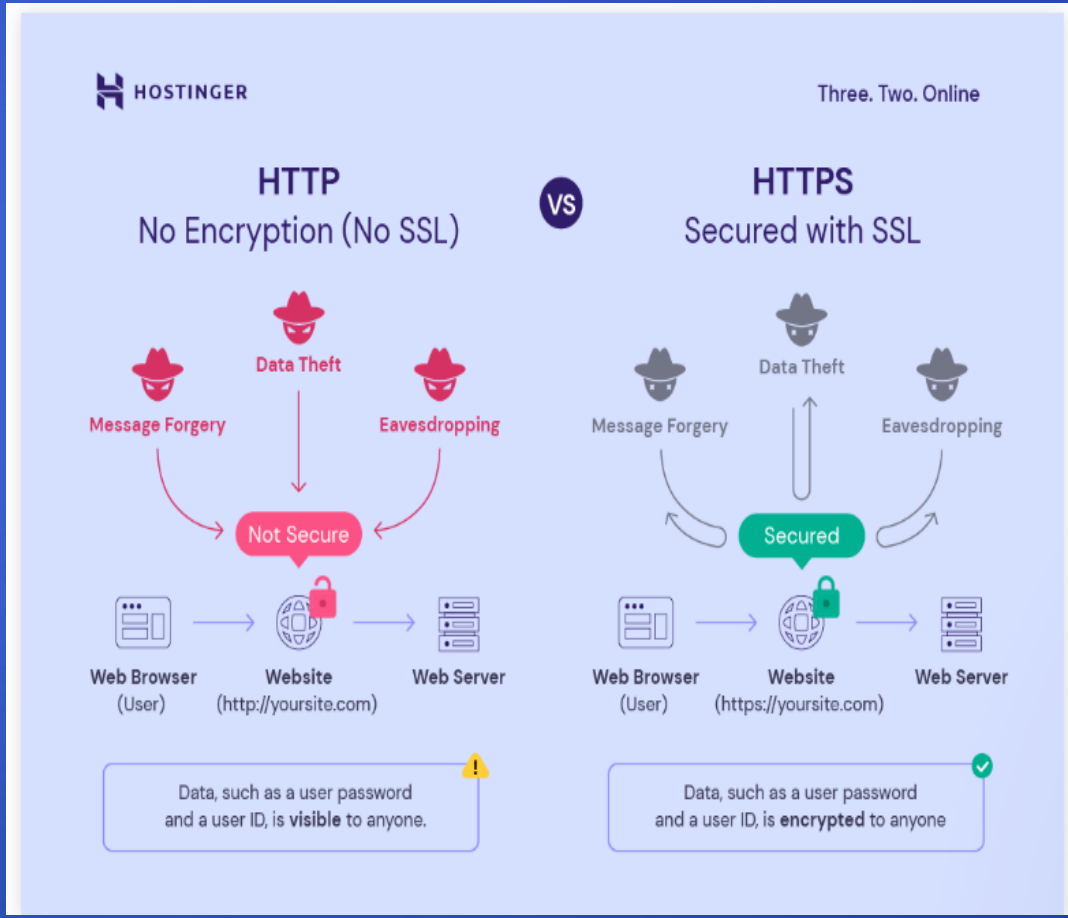


Source: https://www.hostinger.com/tutorials/what-is-ssl-tls-https

4.3 Network Security Components and Defense Mechanisms [2]

SSL/TLS

- Websites with HTTPS at the beginning, rather than HTTP, the S denotes "Secure". It means that the traffic between a web browser and the web server is encrypted, usually with either SSL (Secure Sockets Layer) or TLS (Transport Layer Security). SSL and TLS are both asymmetric and symmetric systems (will cover more in depth in Chap 5).

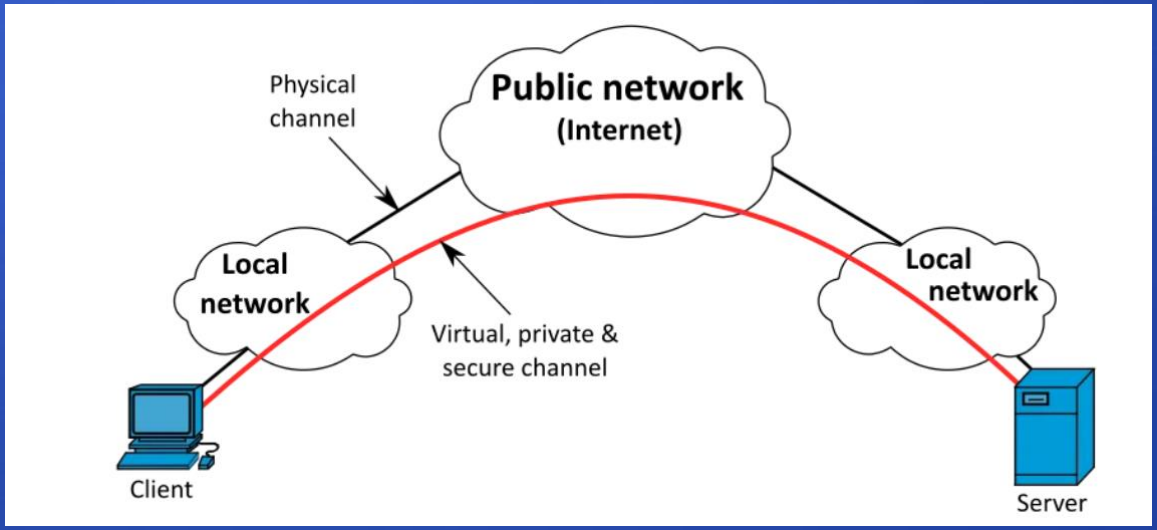


Source: https://www.hostinger.com/tutorials/what-is-ssl-tls-https

4.3 Network Security Components and Defense Mechanisms [2]

Virtual Private Networks (VPNs)

- Provides a way to use the Internet to create a virtual connection between a remote user or site and a central location.
- The packets sent back and forth over this connection are encrypted, thus making it private.
- The VPN must emulate a direct network connection.



Source: https://en.wikipedia.org/wiki/File:VPN_overview-en.svg

4.3 Network Security Components and Defense Mechanisms [2]

Wi-Fi Security

- Wireless networks are commonly used today → wireless network security is important
- Four Wi-Fi Security protocols, ranging from the older and least secure (WEP) to the most recent and most secure (WPA3):
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA)
  - WPA2
  - WPA3

Main References

[1] Chauhan, S. R., and Jangra S., 2020, Computer Security and Encryption: An Introduction, Mercury Learning & Information. https://tarc.idm.oclc.org/login?url=https://ebookcentral.proquest.com/lib/tarc-ebooks/detail.action?docID=6404902

[2] Easttom, Chuck. 2020. Computer Security Fundamentals. 4th ed. Pearson