UNIT 3

UNIT 3

SECURITY TOOLS & TECHNOLOGIES

- Firewalls can be categorised by processing mode, development era, or intended structure
- Five processing modes that firewalls can be categorised by are:
  - Packet filtering
  - Application gateways
  - Circuit gateways
  - MAC layer firewalls
  - Hybrids

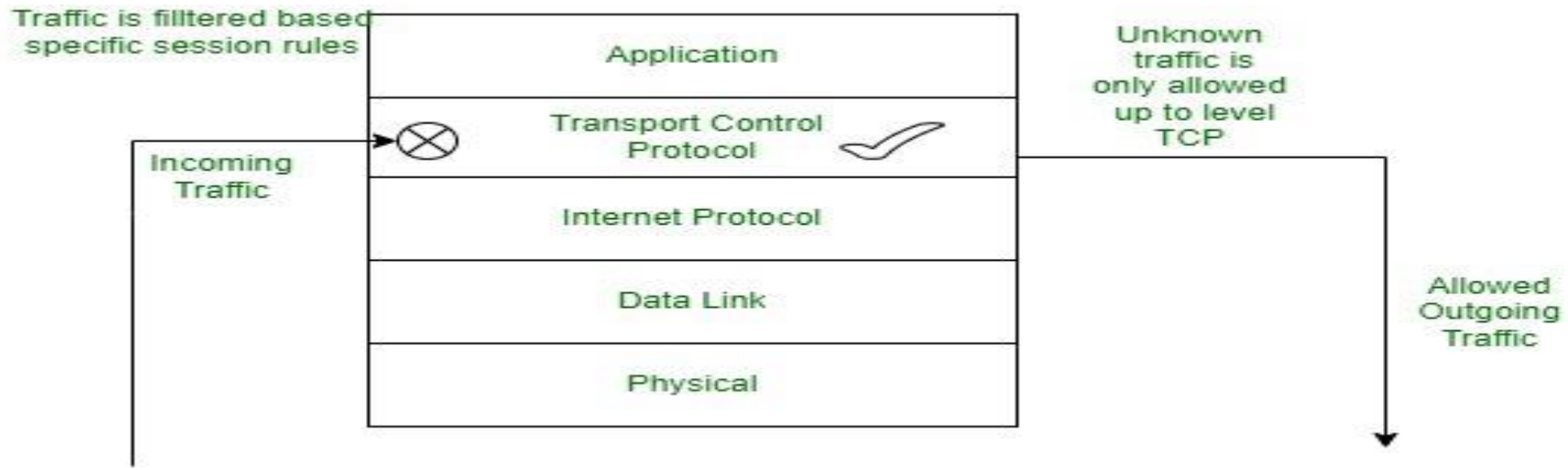
Basis	Transmission control protocol (TCP)	User datagram protocol (UDP)
Type of Service	TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.
Sequence	Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Header Length	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Weight	TCP is heavy-weight.	UDP is lightweight.
Handshaking Techniques	Uses handshakes such as SYN, ACK, SYN-ACK	It's a connectionless protocol i.e. No handshake
Broadcasting	TCP doesn't support Broadcasting.	UDP supports Broadcasting.
Protocols	TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.
Stream Type	The TCP connection is a byte stream.	UDP connection is message stream.
Overhead	Low but higher than UDP.	Very low.

1. HTTP is the backbone of the World Wide Web (WWW). It defines the format of messages through which Web Browsers (like Firefox, Chrome) and Web Servers communicate, whilst also defining how a web browser should respond to a particular web browser request.
2. FTP is the underlying protocol that is used to, as the name suggests, transfer files over a communication network.
    1. It establishes two TCP connections:
    2. **Control Connection** to authenticate the user, and
    3. **Data Connection** to transfer the files.
3. SMTP is what is used by Email servers all over the globe to communicate with each other so that the assignment you submitted at 11:59 pm reaches your professor’s inbox within the deadline.

- **TELNET** stands for **TE**rmina**L NET**work.
- It is a type of protocol that enables one computer to connect to local computer.
- It is a used as a standard TCP/IP protocol for virtual terminal service which is given by ISO.
- Computer which starts connection known as the local computer.
- Computer which is being connected to i.e. which accepts the connection known as remote computer.
- When the connection is established between local and remote computer.
- During telnet operation whatever that is being performed on the remote computer will be displayed by local computer.
- Telnet operates on client/server principle.
- Local computer uses telnet client program and the remote computers uses telnet server program.

Circuit Gateway

- **A circuit-level gateway** firewall helps in providing the security between UDP and TCP using the connection.
- It also acts as a handshaking device between trusted clients or servers to untrusted hosts and vice versa.



Circuit Gateway

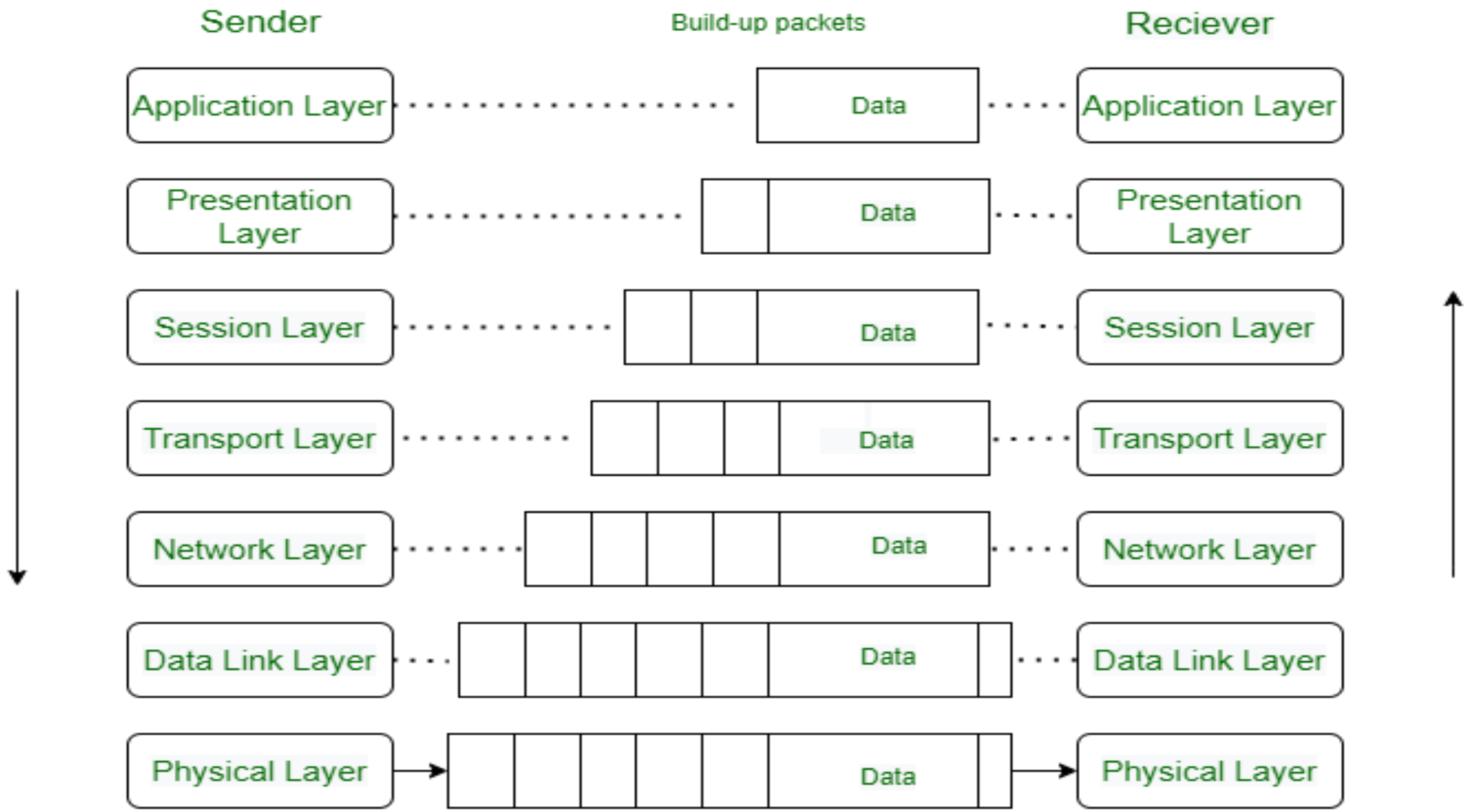
- **Advantage**

1. A circuit-level gateway acts as a proxy for hiding the internal host from the serving host.
2. It avoids the filtering of individual packets.
3. These gateways are inexpensive.
4. Address schemes can easily develop.
5. Simple to implement.
6. Every application does not require a separate proxy server.

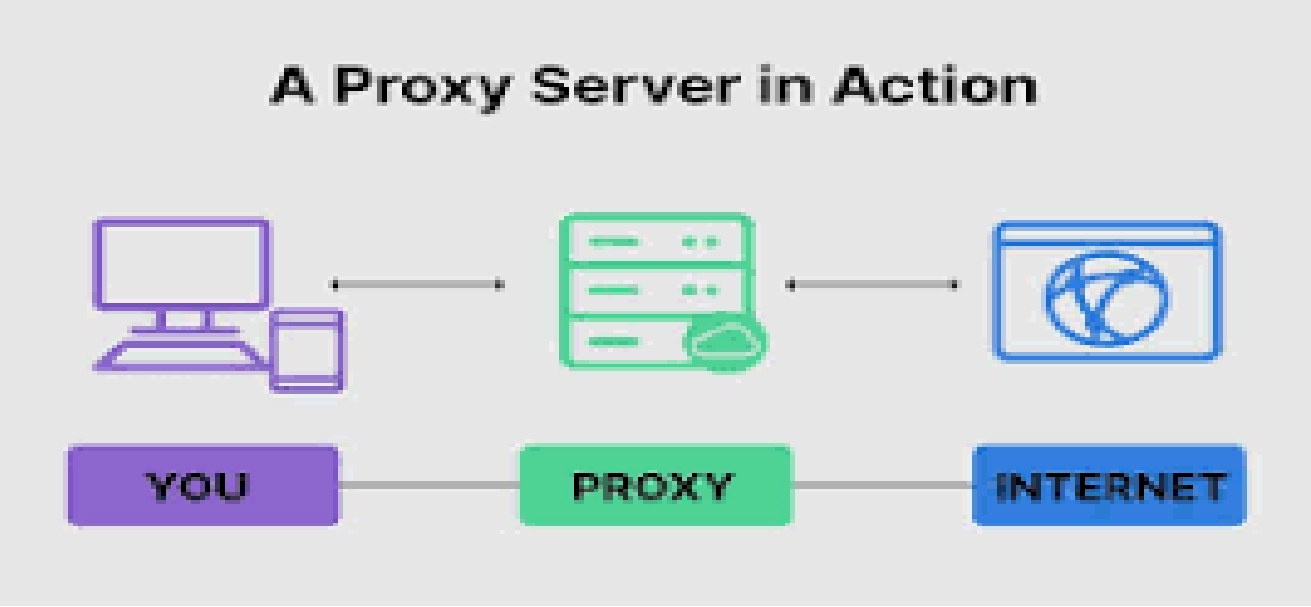
- **Disadvantage**

1. Circuit-level Gateway does not filter the individual packets
2. Frequent updates are required
3. Within the firewall, it does not offer protection against data leakage from devices.
4. For using Circuit level gateways the TCP/IP stacks are mandatory to be modified by the vendor.

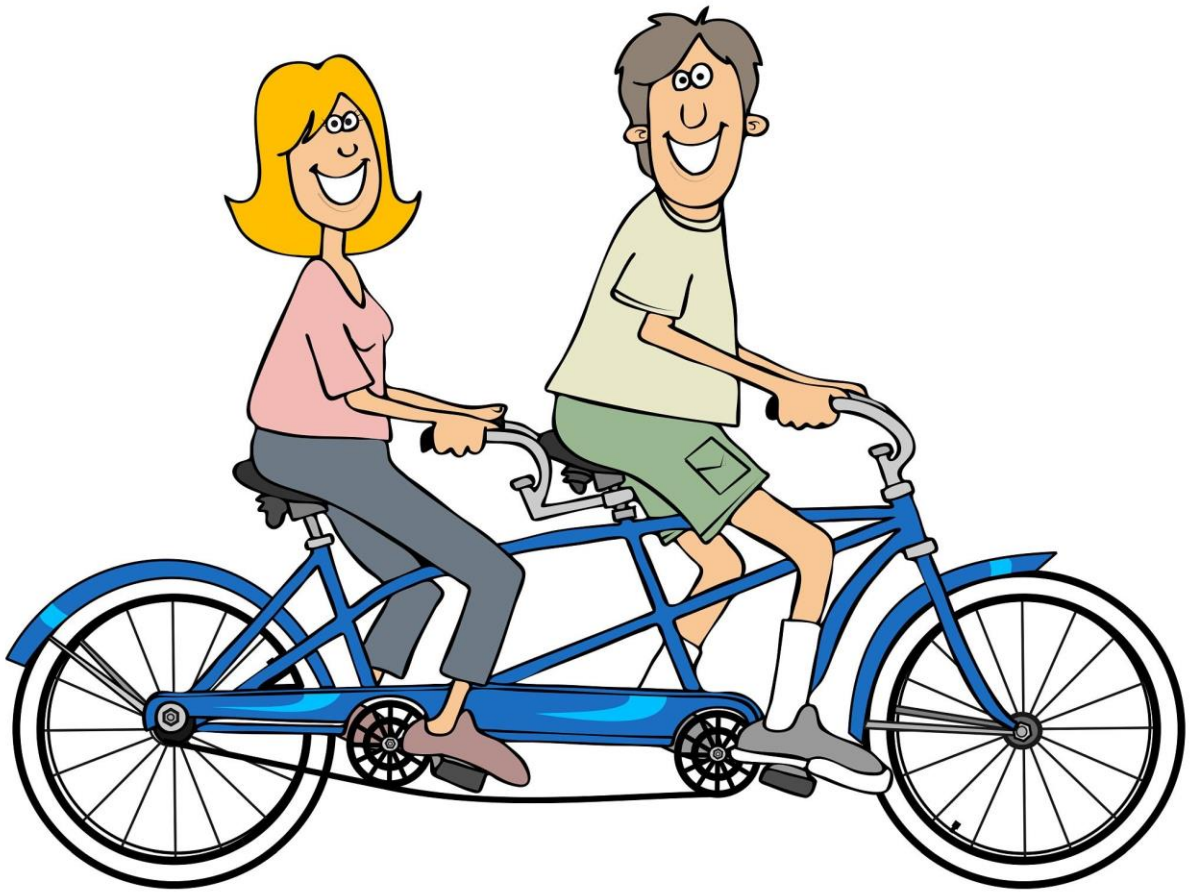
The communication process in the OSI/ISO model



- A proxy server is **a system or router that provides a gateway between users and the internet**.
- Therefore, it helps prevent cyber attackers from entering a private network.
- It is a server, referred to as an “intermediary” because it goes between end-users and the web pages they visit online.



- Hybrid model ---tandem



Virtual private network

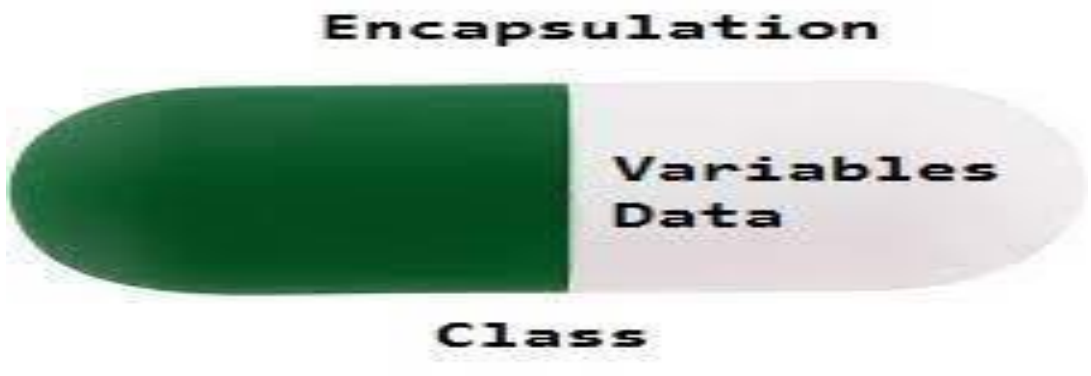
A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

How does a VPN work?

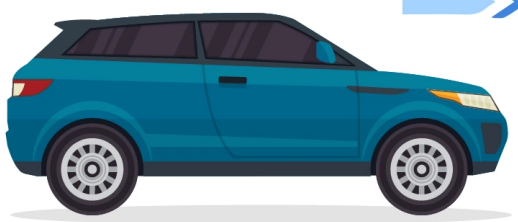
- A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host.
- This means that if you surf online with a VPN, the VPN server becomes the source of your data.
- This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online.
- A VPN works like a filter that turns all your data into "gibberish".
- Even if someone were to get their hands on your data, it would be useless.

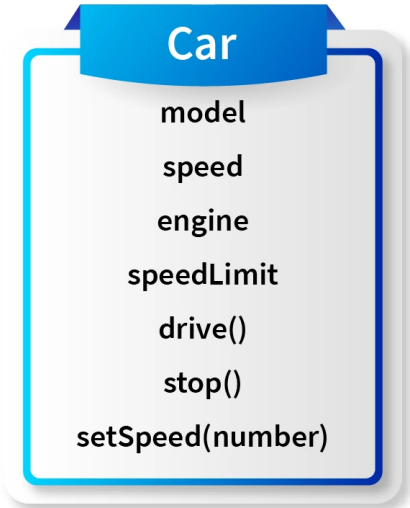
Encapsulation

- Encapsulation is defined as **the wrapping up of data under a single unit**.
- It is the mechanism that binds together code and the data it manipulates.
- Another way to think about encapsulation is, it is a protective shield that prevents the data from being accessed by the code outside this shield.



Encapsulation

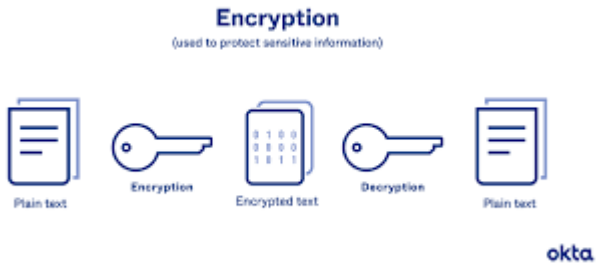




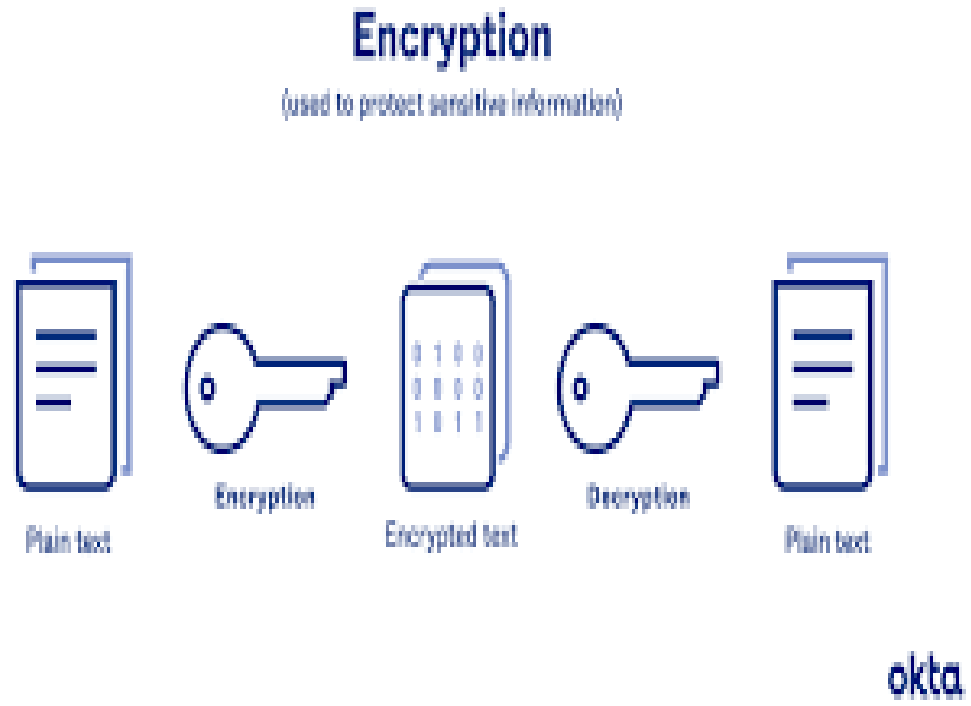
SCALER Topics

Encryption

- Encryption is **a means of securing digital data using one or more mathematical techniques, along with a password or "key" used to decrypt the information**.
- The encryption process translates information using an algorithm that makes the original information unreadable.



Encryption

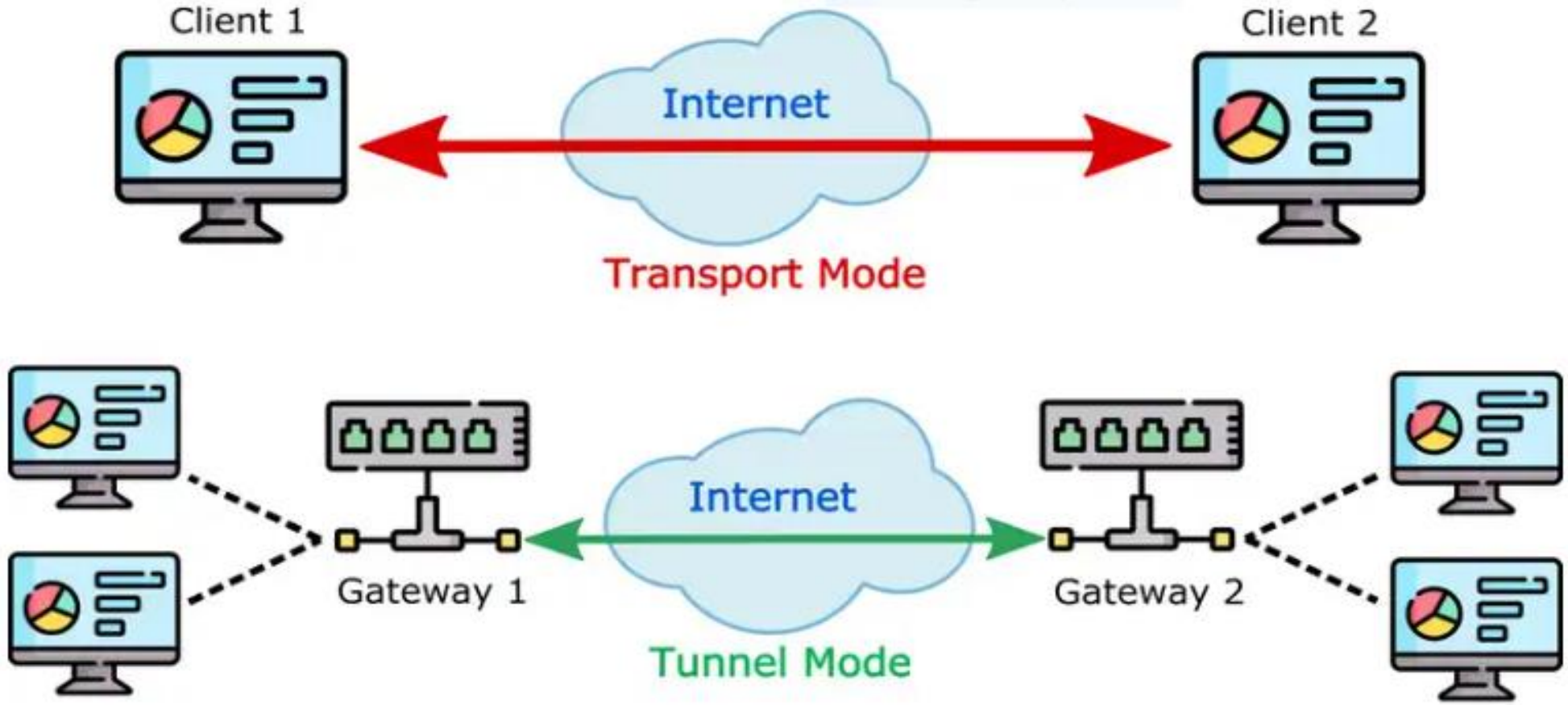

Encryption
(used to protect sensitive information)
Plain text
Encryption
Encrypted text
Decryption
Plain text
okta

Authentication

- Authentication is **the process of determining whether someone or something is, in fact, who or what it says it is**.
- Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

Authentication

IPSec Modes



A diagram showing IPsec encapsulation modes

What are the benefits of a VPN connection?

- A VPN connection disguises your data traffic online and protects it from external access.
- Unencrypted data can be viewed by anyone who has network access and wants to see it.
- With a VPN, hackers and cyber criminals can’t decipher this data.

What are the benefits of a VPN connection?

Secure encryption:

- To read the data, you need an *encryption key* .
- Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack .
- With the help of a VPN, your online activities are hidden even on public networks.

What are the benefits of a VPN connection?

- **Disguising your whereabouts** :
- VPN servers essentially act as your proxies on the internet.
- Because the demographic location data comes from a server in another country, your actual location cannot be determined.
- In addition, most VPN services do not store logs of your activities.
- Some providers, on the other hand, record your behavior, but do not pass this information on to third parties.
- This means that any potential record of your user behavior remains permanently hidden.

What are the benefits of a VPN connection?

- **Access to regional content:**
- Regional web content is not always accessible from everywhere.
- Services and websites often contain content that can only be accessed from certain parts of the world.
- Standard connections use local servers in the country to determine your location.
- This means that you cannot access content at home while traveling, and you cannot access international content from home.
- With **VPN location spoofing** , you can switch to a server to another country and effectively “change” your location.

What are the benefits of a VPN connection?

- **Secure data transfer:**
- If you work remotely, you may need to access important files on your company's network.
- For security reasons, this kind of information requires a secure connection.
- To gain access to the network, a VPN connection is often required.
- VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

Signature-based-ids

- Signature-based IDS is **the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware**.
- This terminology originates from anti-virus software, which refers to these detected patterns as signatures.

Signature-based-ids

- One of the biggest limitations of signature-based IDS solutions is their inability to detect unknown attacks.
- Malicious actors can simply modify their attack sequences within malware and other types of attacks to avoid being detected.
- Traffic may also be encrypted in order to completely bypass signature-based detection tools.
- Also, APTs (usually involve threat actors that change their signature over 60% of the time.

- What is APT detection?
- APT Detection and Protection **Measures**

Advanced Persistent Threat

Statistical anomaly-based IDS

- Anomaly detection is the identification of rare events, items, or observations which are suspicious because they differ significantly from standard behaviors or patterns.
- Anomalies in data are also called standard deviations, outliers, noise, novelties, and exceptions.

Network Based Intrusion Detection System (NIDS)

- A Network Based Intrusion Detection System (NIDS), or Network Based IDS, is **security hardware that is placed strategically to monitor critical network traffic**.
- Traditional Network Based IDS analyzes passing network traffic and matches that traffic to a library of known attacks in its system.

Host Intrusion Detection System (HIDS):

- Host intrusion detection systems (HIDS) run on independent hosts or devices on the network.
- A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.
- It takes a snapshot of existing system files and compares it with the previous snapshot.
- If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate.
- An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

Application Protocol-based Intrusion Detection System (APIDS):

- Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers.
- It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols.
- For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

Spoofing

- Spoofing is a broad term for the type of behavior that involves a cybercriminal masquerading as a trusted entity or device to get you to do something beneficial to the hacker — and detrimental to you.
- Any time an online scammer disguises their identity as something else, it's spoofing.

NIST

- The **National Institute of Standards and Technology** (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) organizes basic cybersecurity activities at their highest level.

DMZ

- In computer security, a DMZ Network (sometimes referred to as a “**demilitarized zone**”) functions as a subnetwork containing an organization's exposed, outward-facing services.
- It acts as the exposed point to an untrusted networks, commonly the Internet.

- Linger : Stay in a place longer than necessary because of a reluctance to leave

- Subnetwork ：
- A subnetwork or subnet is a logical subdivision of an IP network.
- The practice of dividing a network into two or more networks is called subnetting.
- Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses.

DEPLOYING NIDS

- Deploying NIDSs (1) • NIST recommends four locations for NIDSs: –
- Location 1: behind each external firewall, in the network DMZ –
- Location 2: outside an external firewall –
- Location 3: on major network backbones –
- Location 4: on critical subnet

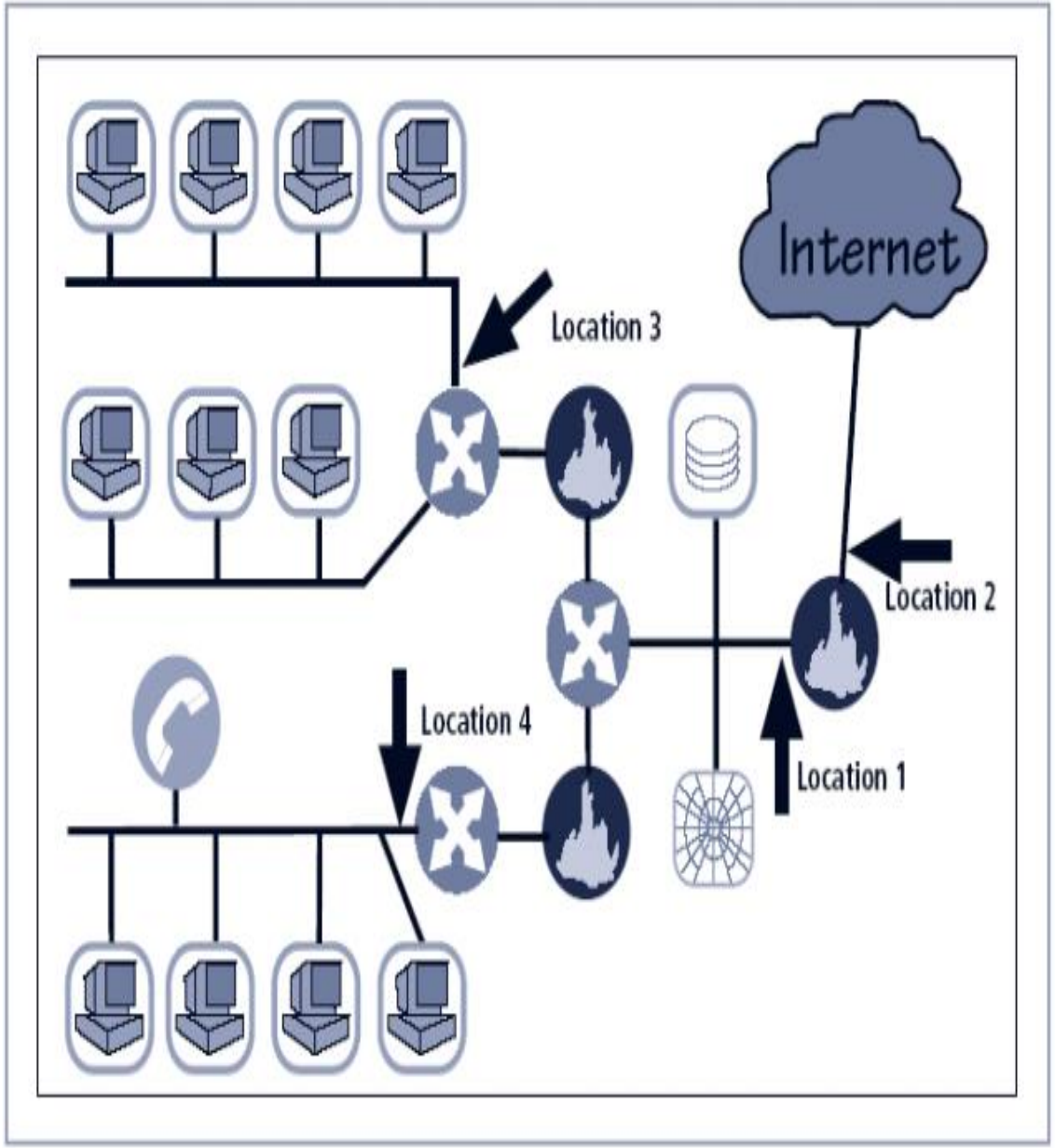


FIGURE 7-7 Network IDS Sensor Locations[17]

Honeypot

- **Honeypot** is a network-attached system used as **a trap for cyber-attackers** to detect and study the tricks and types of attacks used by hackers.
- It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.
- Honeypots are mostly used by large companies and organizations involved in cybersecurity.
- It helps cybersecurity researchers to learn about the different type of attacks used by attackers.
- It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information.

Honeypot

- The cost of a honeypot is generally high because it requires specialized skills and resources to implement a system such that it appears to provide an organization’s resources still preventing attacks at the backend and access to any production system.
- A honeynet is a combination of two or more honeypots on a network.

Types of Honeypot:

Honeypots are classified based on their

- deployment and the
- involvement of the intruder.

Based on their deployment, honeypots are divided into :

- **Research honeypots-** These are used by researchers to analyze hacker attacks and deploy different ways to prevent these attacks.
- **Production honeypots-**
  - Production honeypots are deployed in production networks along with the server.
  - These honeypots act as a frontend trap for the attackers, consisting of false information and giving time to the administrators to improve any vulnerability in the actual system.

Types of Honeypot:

- Based on interaction, honeypots are classified into:
    1. Low interaction honeypots
    2. Medium Interaction Honeypots
    3. High Interaction honeypots

Advantages of honeypot:

1. Acts as a rich source of information and helps collect real-time data.
2. Identifies malicious activity even if encryption is used.
3. Wastes hackers' time and resources.
4. Improves security.

Disadvantages of honeypot:

1. Being distinguishable from production systems, it can be easily identified by experienced attackers.
2. Having a narrow field of view, it can only identify direct attacks.
3. A honeypot once attacked can be used to attack other systems.
4. Fingerprinting(an attacker can identify the true identity of a honeypot).

Honeynets

- A honeynet is a network that is set up to attract potential attackers and distract them from your production network.
- In a honeynet, attackers will not only find vulnerable services or servers but also find vulnerable routers, firewalls, and other network boundary devices, security applications, and so forth.

Difference between honeypot and honeynet

In computing terms the difference between honeypot and honeynet. is that

- Honeypot is (computing) a trap set to detect or deflect attempts at unauthorized use of information systems

  While

- Honeynet is (computing) an entire computer network that serves as a honeypot, or trap for potential attackers.

What is padded cell system in information security?

- Paddock cells are simulated environments that can present fake data to keep intruders interested.
- Intrusion detection systems (IDS) that are installed on a single computer and can monitor its activities are known as host-based IDSs (HIDS).

What is the key difference between honeypots and padded cell systems?

- Padded cells are honey pots that have been protected against intrusion in such a way that it is difficult to compromise.
- The padded cell can also be described as a "hardened honey pot".
- As well as delivering tempting data to attackers, padded cells work in tandem with a traditional intrusion detection system.

- Leading IDS And IPS Solutions
- https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/