Unit-9

Introduction Security

Security:

- Freedom From risk and danger.
- The ability of a system to protect information and system resources with respect to confidentiality and integrity
- In a distributed system, security refers to the protection of the system's resources and data from unauthorized access, modification, or disruption. It involves implementing measures to ensure confidentiality, integrity, availability, and authenticity of the system and its components.

- **Security Goals:**

Security is about keeping system, programs and data secure. It is addresses three broad areas: **Confidentiality, integrity and availability.** Together these are referred to as the CIA Triad.

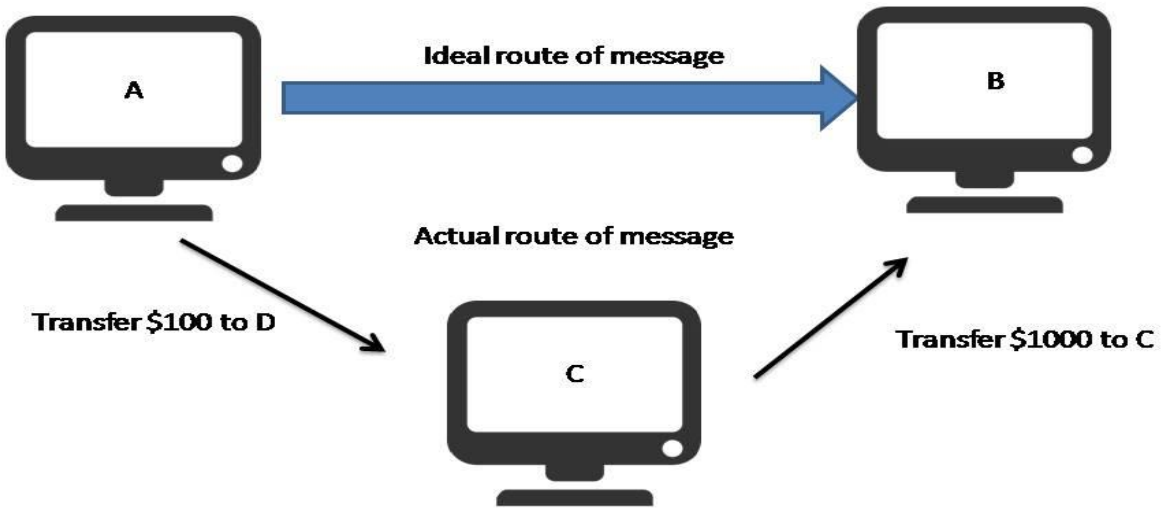
Confidentiality:

- It refers to the ability to hide the information from people who do not have the permission to access it. This helps to ensure that the data is not compromised and is not disclosed to unauthorized people. Some of the method employed to ensure confidentiality is encryption & cryptography.
- For example, when a lawyer is not able to reveal the secrets of his clients because he has a duty to keep those secrets to himself.

  Only account holders can view their bank account summary

Integrity:

Integrity is ensuring that the information is accurate complete,reliable,and is in its original form. Incomplete and corrupted data can do more harm than good.



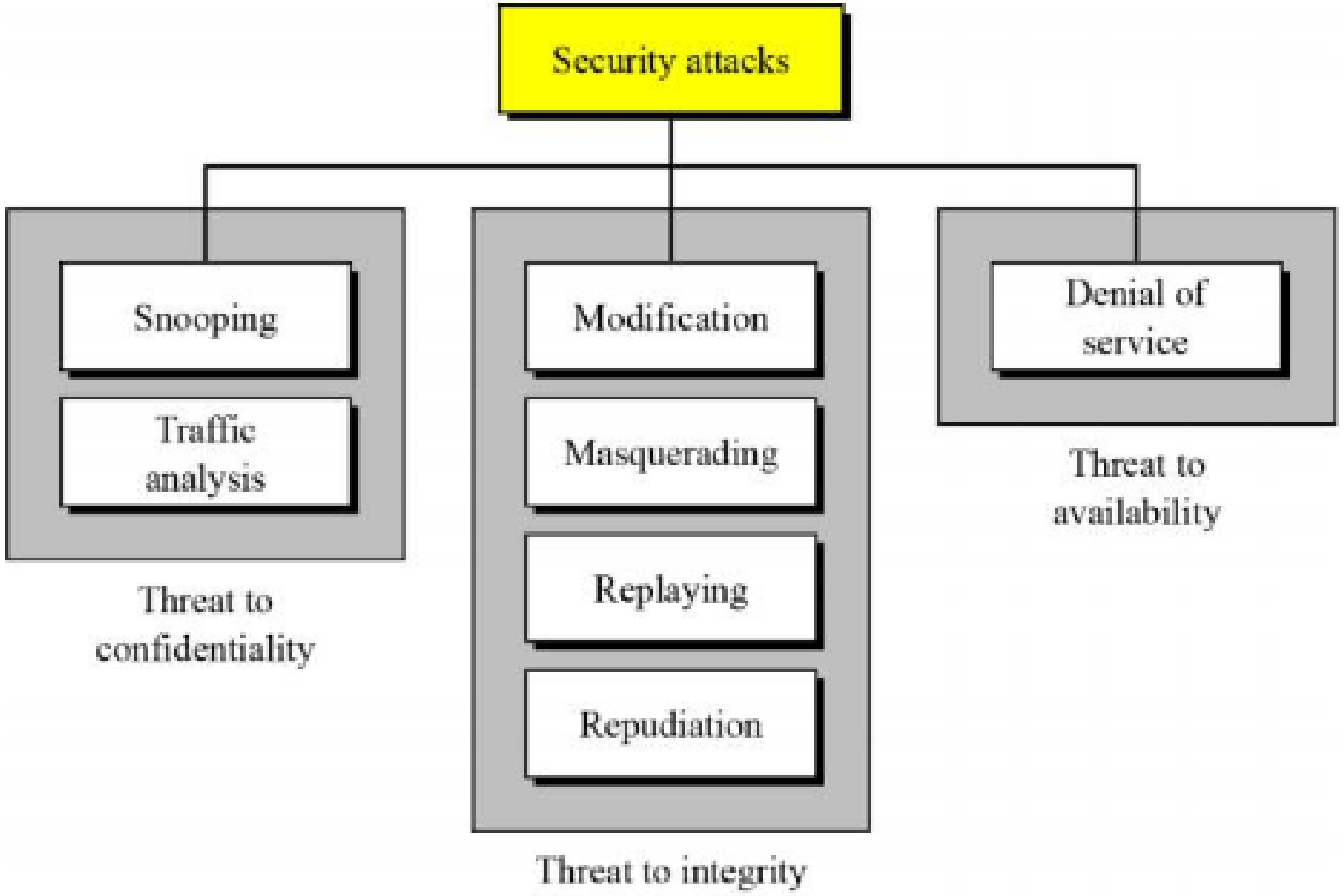
- **Availability:**

Though it is highly necessary to ensure that the data is unavailable to unauthorized people, it is equally important to make sure that the data is available to authorized people. People who are authorized to access information must not face any issues when accessing information that is needed.

Security Threats and Attacks:

1. **Interception :** It refers to the unauthorized party gaining access to a service or data.
2. **Interruption:** It refers to the situation in which services or data becoming unavailable, unusable, destroyed and so on.eg: DOS attack.
3. **Modification:** Unauthorized changing of data or service so that it no longer adheres to its original specification. Eg: Changing values in a data file, changing program to log secretly user's activities.

- **A security attack** refers to any deliberate action or technique employed by an individual or group with the intention of compromising the confidentiality, integrity, availability, or authenticity of a system, network, or data.
- **Types of Security Attack:**



- **Snooping:** Refers to unauthorized access to or interception of data.
- **Traffic analysis:** Refers to obtaining some other type of information by monitoring online traffic.
- **Modification:** means that the attacker intercepts the message and changes it.
- **Masquerading or spoofing:** It happens when the attacker impersonates somebody else.
- **Replaying:** It means the attacker obtains a copy of message sent by a user and later tries to replay it.
- **Repudiation:** means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has receives the message.
- **Denial of service (DOS):** It is a very common attack. It may slow down or totally interrupt the service of a system.

- **Security Policies and Mechanism:**
- Security policy describes precisely which action the entities in a system are allowed to take and which ones are prohibited.
- Once security policy has been laid down, it becomes possible to concentrate on the security mechanism. **The important security mechanism are:**

1. **Encryption:** It provides a means to implement data confidentiality. In addition , it allows user to verify data modification so, it also provides support for integrity checks.
2. **Authentication:** It is used to verify the claimed identify of a user, client, server, host or other entity are authentic clients.Typically users are authenticated by password, but there are many other ways to authenticate client.

- **Authorization:**

After a client has been authenticated, authorization is to check as a weather the client is authorized to perform specific task.

- **Auditing:**

Auditing tools are used to trace which client accessed what information, when and in which what they did so. Although auditing does not provide any protection against security threats. Audit logs can be useful for the analysis of a security breach, and subsequently taking measures against intruders.

Cryptography:

Cryptography is the practice of secure communication by converting plain, readable information (plaintext) into an unintelligible form (ciphertext) using various mathematical algorithms and techniques. It ensures that sensitive data remains confidential, secure, and tamper-proof during transmission and storage.

Cryptology is the science of making and breaking secret code.

The development and use of codes are cryptography. Study and breaking code is cryptanalysis.

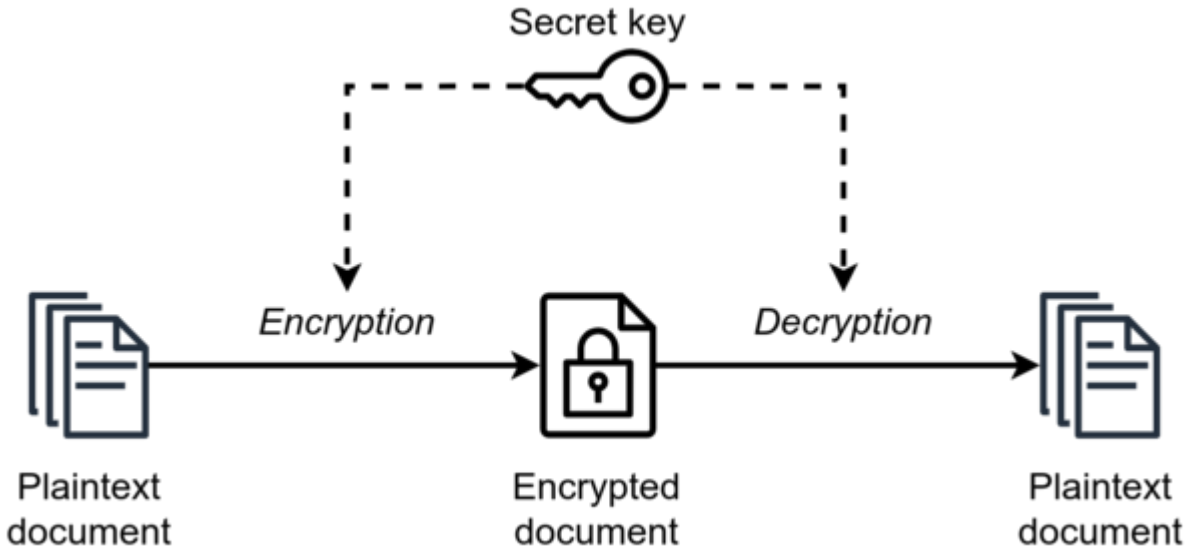
- **Terminologies:**
  - ***Plaintext:*** readable text with no information hidden.
  - ***Ciphertext:*** text with information hidden (the encrypted data).
  - ***Encryption:*** the process of converting plaintext to ciphertext.It is a mathematical process that prodeces a cipher text for any given plain text and encryption key.It is a cryptographic algorithm that takes plain text and an encryption key as input and produce a cipher text.
  - $C=E(P,K_e)$
  - ***Decryption:*** the process of reverting ciphertext to plaintext. It is a mathematical process, that produces a unique plaintext for any given cipher text and decryption key. It is a cryptographic algorithm that takes a cipher and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reserves the encryption algorithm and is thus closely related to it.
  - $P=D(C,K_d)$

  - ***Cipher:*** algorithm used for encryption and decryption.
  - ***Key:*** a secret piece of information which is used for encryption & decryption.

- **Encryption Key:** It is a value that is known to sender. The sender inputs the encryption key into the encryption algorithm along with the plain text in order to compute the cypher text.
- **Decryption Key:** It is a value that is known to the receiver. The decryption key is related to encryption key., but is not always identical to it.

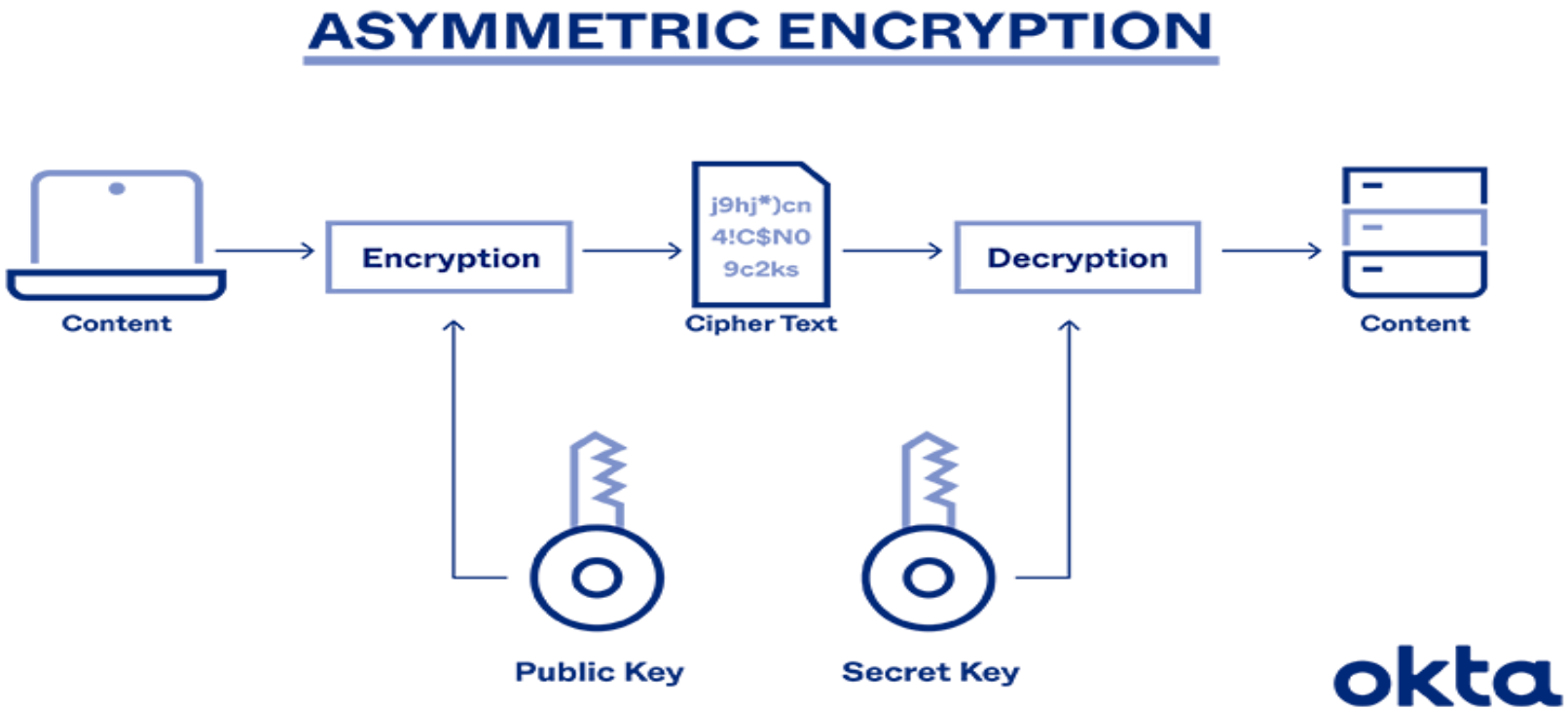
- **Symmetric-key encipherment (Secret-key cryptography or private-key encryption):**

=> Symmetric key cryptography is a type of encryption scheme in which the similar key is used both to encrypt and decrypt messages. Such an approach of encoding data has been largely used in the previous decades to facilitate secret communication between governments and militaries

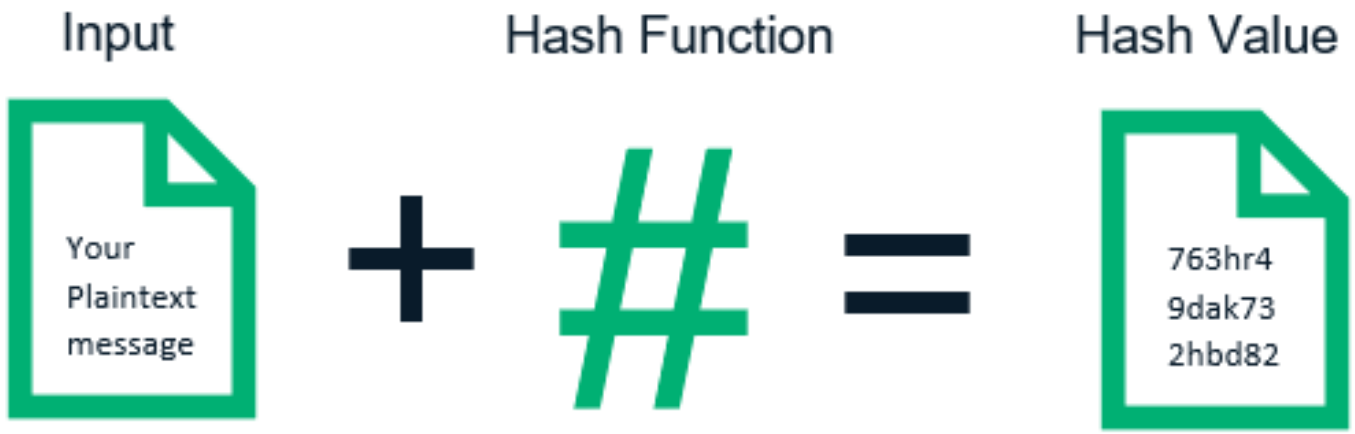


- **Asymmetric key encipherment (public key encryption or public-key cryptography):**

Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys -- one public key and one private key -- to encrypt and decrypt a message and protect it from unauthorized access or use.



- **Hashing:**
- In computer science and cryptography, a hash function is a deterministic procedure that takes an input (or “message”) and returns a string of characters of a fixed size—which is usually a “digest”—that is unique to the input.
- A hash function is used in many cybersecurity algorithms and protocols, such as password storage and digital signature. Hashing is also used in a data structure, such as a hash table (a data structure that stores data), for a quick search and insertion.



- **Secure Channels:**
- A secure channel protects sender and receivers against interception, modification and fabrication of message. It does not necessarily protect against interruption. A secure channel provide for authentication, confidentiality and message integrity.
- **Authentication:**
- Authentication is the process of validating the identity of someone or something. It uses information provided to the authenticator to determine whether someone or something is in fact who or what it is declared to be.
- Generally authentication requires the presentation of credentials or items of value to really prove the claim of who you are.
- The items of value or credential are based in several unique factors that show something you know(password, pin, phrases).
- something you have(SecureID,CryptoCard, SafeWord).
- or something you are(DNA patterns , retina, heartbeat, finger print):

- **Authentication method:**

1. Password Authentication
2. Public-key Authentication
3. Remote Authentication
4. Certificate based authentication

Message Integrity and Confidentiality:

Besides authentication, a secure channel should also provide guarantees for message integrity and confidentiality. Message integrity means that message protected against surreptitious modification; confidentiality ensure that message cannot be intercepts and red by eavesdroppers.

Confidentiality simply established by encrypting a message before sending it.For protecting message integrity it is difficult task however we can use digitial signature.

- **Secure group Communication:**

Example :Kerberos

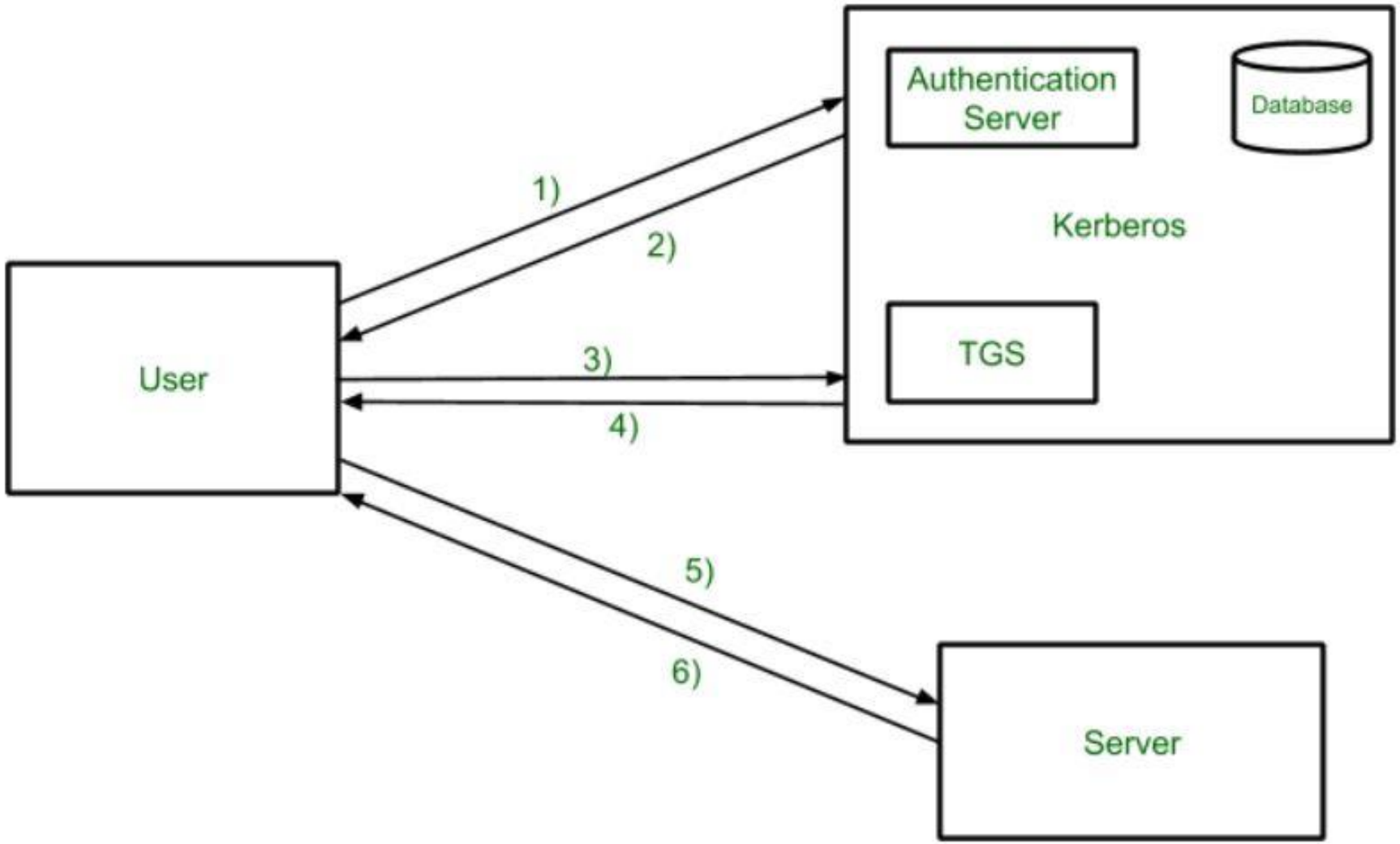
Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC). Each user and service on the network is a principal.

The main components of Kerberos are:

- **Authentication Server (AS):**
  The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.

- **Database:**
  The Authentication Server verifies the access rights of users in the database.

- **Ticket Granting Server (TGS):**
  The Ticket Granting Server issues the ticket for the Server


Authentication Server
Database
Kerberos
TGS
User
1)
2)
3)
4)
5)
6)
Server

- **Step-1:**
  User login and request services on the host. Thus user requests for ticket-granting service.

- **Step-2:**
  Authentication Server verifies user's access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using the Password of the user.

- **Step-3:**
  The decryption of the message is done using the password then send the ticket to Ticket Granting Server. The Ticket contains authenticators like user names and network addresses.

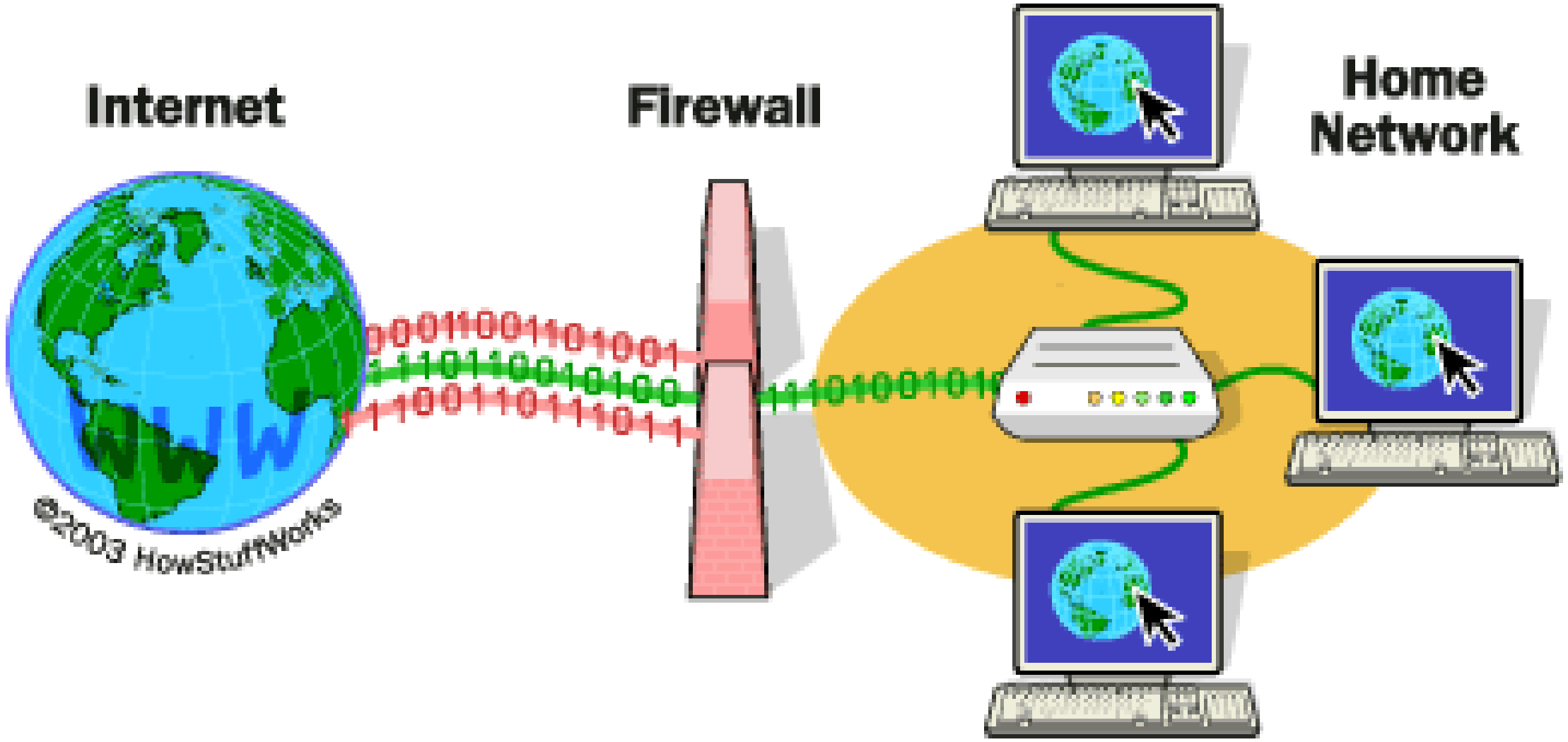
- **Step-4:**
  Ticket Granting Server decrypts the ticket sent by User and authenticator verifies the request then creates the ticket for requesting services from the Server.

- **Step-5:**
  The user sends the Ticket and Authenticator to the Server.

- **Step-6:**
  The server verifies the Ticket and authenticators then generate access to the service. After this User can access the services.

Firewall

- A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).
- The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.
- It blocks connections from unauthorized network.
- It filters data by monitoring IP packets that are traversed.
- It involves network and transport layer data


Internet
Firewall
Home Network
WWW
©2003 HowStuffWorks

Working of firewall

- A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.
- Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP- addresses, or sources.

Types of firewall

1. Packet filters
2. Circuit level Gateway
3. Application gateway
4. Stateful packet filtering Firewall

Packet filter Firewall (Router)

Key points

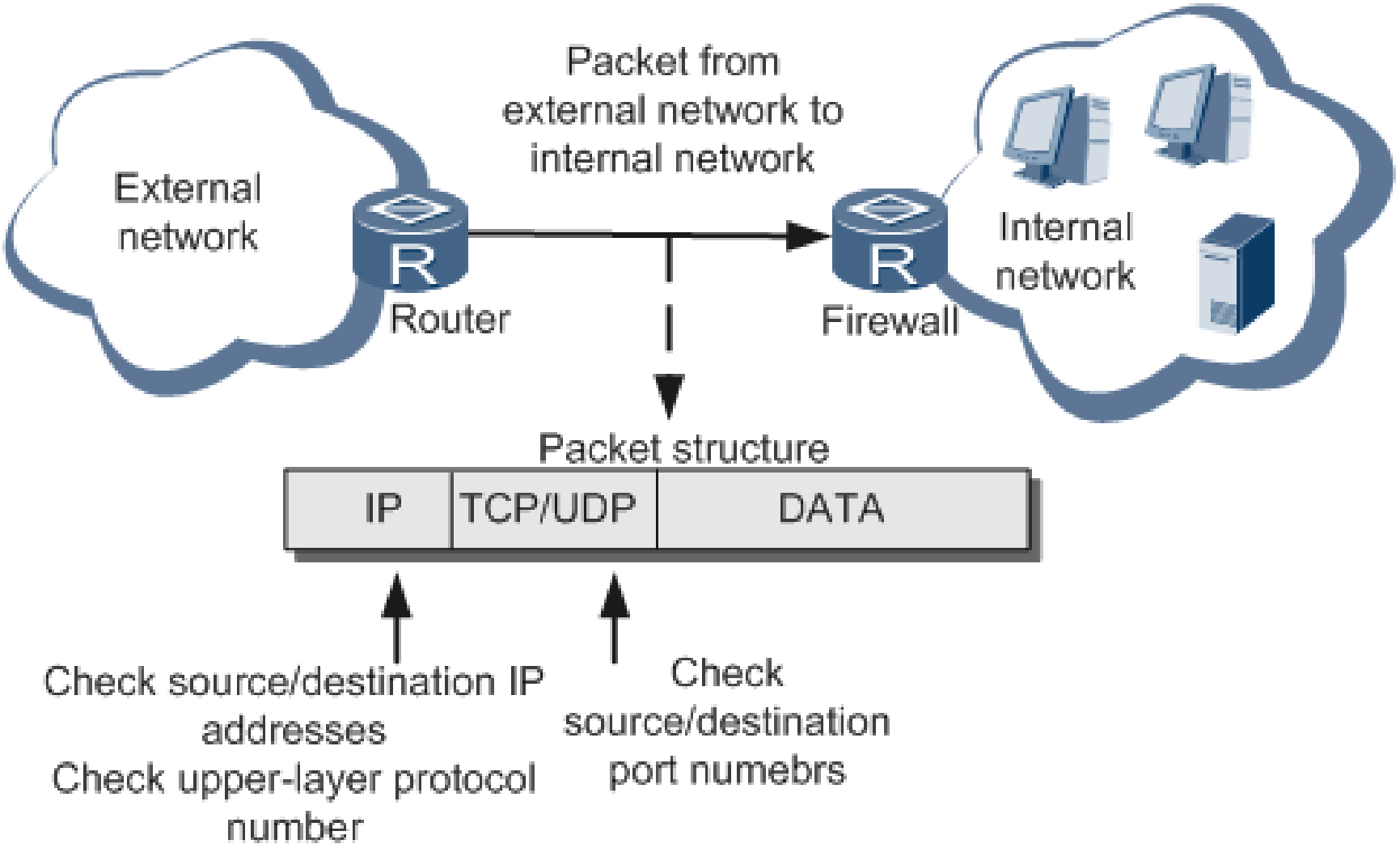
- Set of rules
- SA,DA,Port number, Protocols
- If rules match fordward,discard
- Default action
- Data/Payload

- Packet filtering firewalls are the oldest, most basic type of firewalls. Operating at the network layer, they simply check a data packet for its source IP and destination IP, the protocol, source port and destination port against predefined rules to determine whether to pass or discard the packet.

- Packet filtering firewalls are fast, cheap and effective. But the security they provide is very basic. Since these firewalls cannot examine the content of the data packets, they are incapable of protecting against malicious data packets coming from trusted source IPs

- **Packet filtering firewall advantages**
- A single device can filter traffic for the entire network
- Extremely fast and efficient in scanning traffic
- Inexpensive
- Minimal effect on other resources, network performance and end-user experience
- **Packet filtering firewall disadvantages**
- Because traffic filtering is based entirely on IP address or port information, packet filtering lacks broader context that informs other types of firewalls
- Doesn't check the payload and can be easily spoofed
- Not an ideal option for every network

Packet Filter Firewall

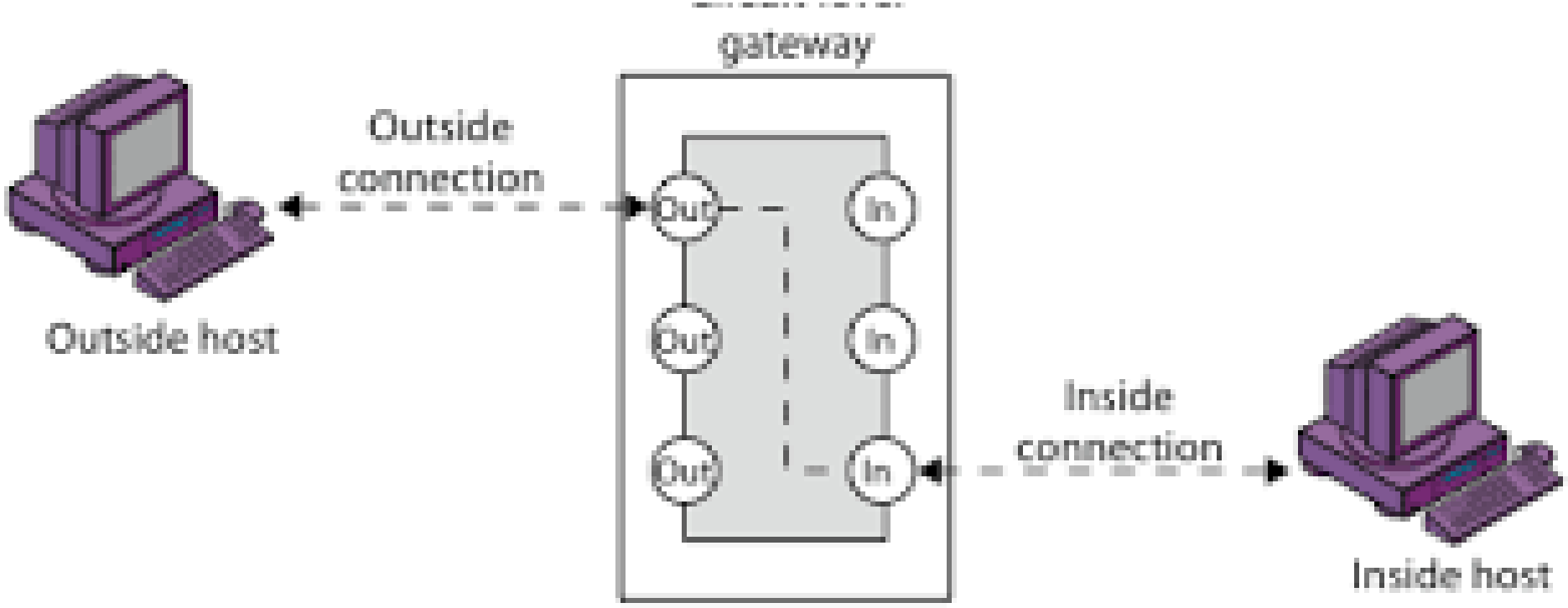


Circuit level gateway

- Working at the session layer, circuit-level gateways verify established Transmission Control Protocol (TCP) connections and keep track of the active sessions
- Uses two tcp connection

1. Between Internal host and gateway
2. Between external host and gateway

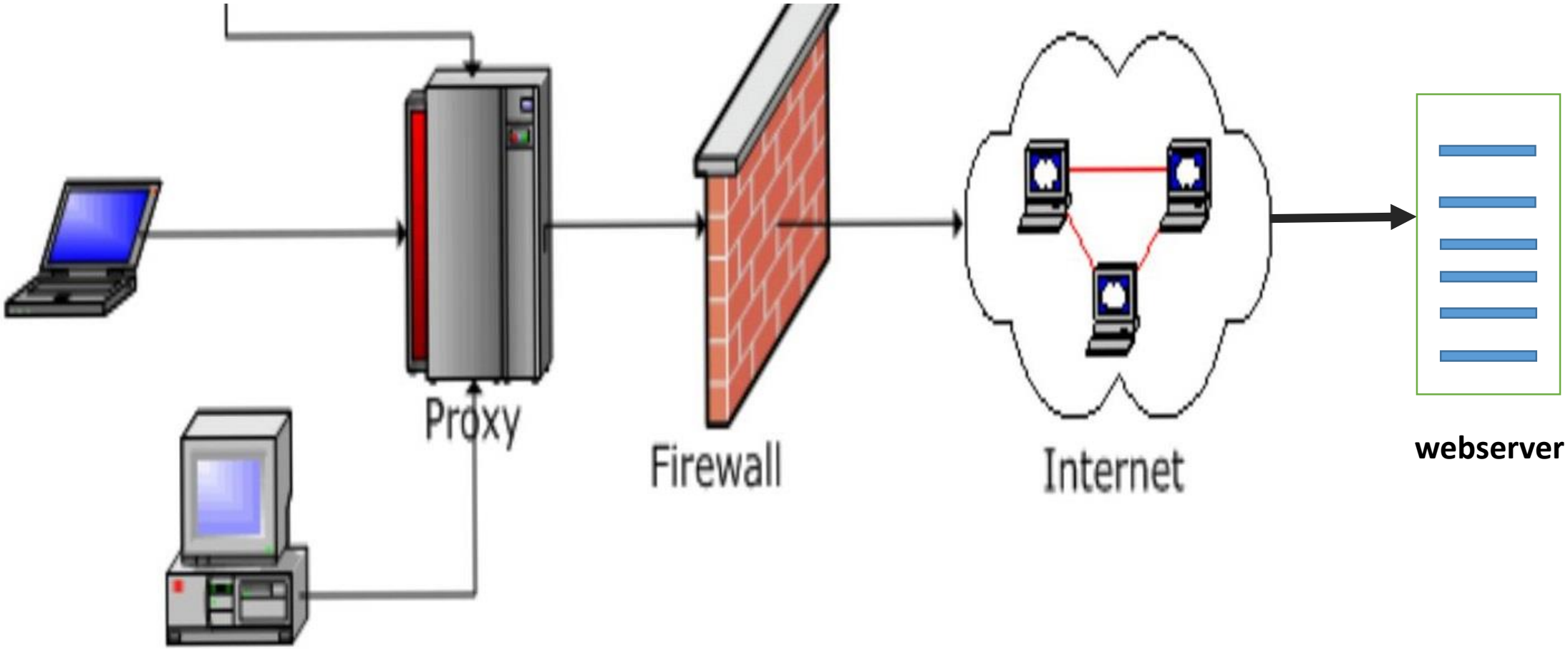
- Security checks done before setting up a connection. Once the connection is established all the data will be passed.
- Circuit level gateway are relatively inexpensive and they do not filter individual packets.



(c) Circuit-level gateway

Application Gateway

- Application Gateway is also known as the proxy firewall is a network security system that protects network resources by filtering messages at the application layer.
- Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server. This protects the client's identity and other suspicious information, keeping the network safe from potential attacks. Once the connection is established, the proxy firewall inspects data packets coming from the source. If the contents of the incoming data packet are protected, the proxy firewall transfers it to the client. This approach creates an additional layer of security between the client and many different sources on the network.
- Examines all communications between outside sources and devices behind the firewall, checking not just address, port and TCP header information, but the content itself before it lets any traffic pass through the proxy
- Provides fine-grained security controls that can, for example, allow access to a website but restrict which pages on that site the user can open

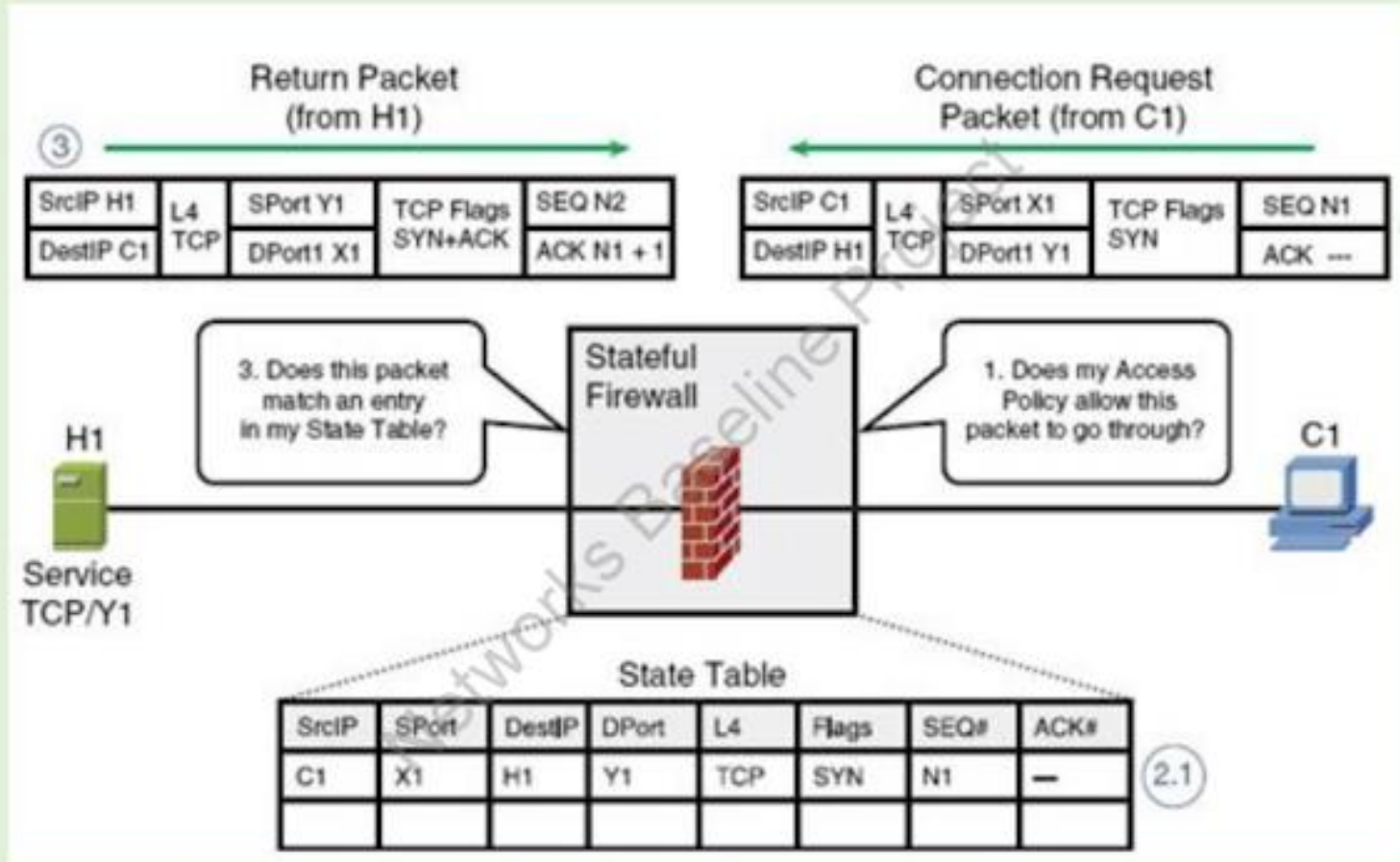

Proxy
Firewall
Internet
webserver

Stateful packet filtering Firewall

- State-full packet filtering is a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.
- State-full packet filtering creates a state table for examine each packet,and also keep track of whether or not that packet is part of an established TCP session.
- In this type of firewall if assign a rule for outbound connection then we don’t need to set a extra rule for the return connection.
- Whatever information is transmitted to the host to destination or vice-versa all the information are stored in a state table
- Stateful firewalls can watch traffic streams from one end to other end.They can aware of communication path and can implement various IP Security functions such as tunnels and encryption.
- Most of the firewall which is used today are stateful firewall
- For ex: Palo Alto Firewall,CISCO ASA Firewall(**Adaptive Security Appliance**.), Checkpoint Firewall

Note: It combines the aspects of other three types of firewall

Basic Stateful Firewalls and feature sets



Stay Connected : www.routexp.com

Networks-Baseline Innovation Project

- **Secure mobile code:**
- Secure mobile code refers to a concept in distributed systems where code or software components are executed securely on mobile devices. In a distributed system, mobile code refers to code that can be transferred from one device to another and executed remotely.
- The idea behind secure mobile code is to ensure that the execution of code on mobile devices is safe and does not compromise the security or integrity of the device or the system as a whole. This is particularly important in situations where mobile devices may be untrusted or owned by different entities.
- To achieve secure mobile code execution, various security measures can be employed, including:

- **Code verification**: The code can be verified to ensure that it is authentic and has not been tampered with during transmission or execution.
- **Code isolation**: The execution environment can be isolated from the rest of the system to prevent unauthorized access or interference. Techniques such as sandboxing or virtualization can be used to create a secure execution environment.
- **Access control**: Mobile code may require access to sensitive resources or data on the device. Access control mechanisms can be implemented to ensure that only authorized code can access such resources.
- **Permission-based execution**: The mobile code may be granted permissions based on the specific actions it needs to perform. This can limit the capabilities of the code and reduce the risk of malicious actions.
- **Secure communication**: Communication between the mobile code and other components in the distributed system should be encrypted and authenticated to prevent eavesdropping or tampering.

Two major issues are:

1. Securing agent **malicious agents** that attempt to damage a mobile agent environment.
2. Securing a mobile agent from a **malicious environment** that attempts to interfere with the working of the mobile agent.

*Protecting an Agent:

In many cases it is impossible to protect an agent against all type of attack. The emphasis is on being able to detect modification to an agent. This approach has been followed in the agent system which uses public-key technologies to implement this idea.

Read Only state: The read only agent system of an agent consists of a collection of data items that is signed by the agent owner. Signing takes place when the agent is constructed and initialized before it is sent off to other host. The owner first constructs a message digest , which it subsequently encrypts with its private key. When the agent arrives at a host, that host can easily detect whether the read-only state has been tampered with by verifying the state against the signed message digest of the original state.

- **Append only logs:**

To allow an agent to collect information while moving between host, Agent provides secure append-only logs. These logs are characterized by the fact that can only be appended to the log; there is no way that data can be removed or modified without the owner being able to detect this.

- **Selective Revealing:** Agent supports selective revealing of state by providing an array of data items, where each entry is intended for a designated server. Each entry is encrypted with the designated server's public key to ensure confidentiality. The entire array is signed by the agent's owner to ensure integrity of the array as a whole. In other words , if any entry is modified by a malicious host, any of the designated servers will notice and can take appropriate action

Denial of Service Attack:

- A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a computer system, network, or website, making it inaccessible to its intended users. The objective of a DoS attack is to overwhelm the targeted system's resources, such as bandwidth, processing power, or memory, causing it to become unresponsive or crash.
- There are various types of DoS attacks, including:
- **Flooding attacks**: These attacks involve sending a large volume of traffic or requests to the targeted system, overwhelming its capacity to handle them. Examples include:
  - **TCP/IP SYN Flood**: Exploits the TCP handshake process by sending a flood of connection requests without completing the handshake, exhausting the system's resources.
  - **Ping flood**: Sends an excessive number of ICMP echo requests (pings) to the target, consuming network bandwidth and causing network congestion.
- **Application layer attacks**: These attacks target vulnerabilities in the application layer of a system, aiming to exhaust its resources or disrupt its services. Examples include:
  - **HTTP/S floods**: Overwhelms a web server by flooding it with a massive number of HTTP/S requests, exhausting server resources.
  - **Slowloris**: Exploits web server limitations by opening multiple connections and keeping them open, exhausting server resources and preventing new connections.

Security Management

- Security management in a distributed system involves implementing measures to protect the system's resources, data, and communications from unauthorized access, malicious activities, and other security threats. Here are some key aspects of security management in a distributed system:
- **Access Control**: Implementing robust access control mechanisms to ensure that only authorized users or systems can access resources within the distributed system.
- **Encryption**: Protecting sensitive data by encrypting it during storage and transmission.
- **Network Security**: Implementing measures to secure the network infrastructure and communications within the distributed system.
- **Security Auditing and Logging**: Enabling logging mechanisms to record and monitor activities within the distributed system.

Key Management:

Key management is the process of putting certain standards in place of ensure the security of cryptographic keys in an organization. Key management deal with the creation, exchange, storage, deletion, and refreshing of keys.

There are two aspects for Key Management:

- Distribution of public keys.
- Use of public-key encryption to distribute secrets.
- **Distribution of public key:**

1. **Public Announcement**
2. **Public Available directory**
3. **Public key certificate**

- **Secure group management:**

1. KDC(Key distribution system)

A key distribution center (KDC) in cryptography is a system that is responsible for providing keys to the users in a network that shares sensitive or private data. Each time a connection is established between two computers in a network, they both request the KDC to generate a unique password which can be used by the end system users for verification.

1. Diffie-Hellman Key exchange

The Diffie-Hellman key exchange (also known as exponential key exchange) is a method for securely exchanging cryptographic keys over an insecure channel. It is a fundamental building block of many secure communication protocols, including SSL/TLS and SSH