Network security basics: TCP/IP vulnerabilities (Layer wise),Network Attacks: Packet Sniffing, ARP spoofing, port scanning, IP spoofing.

Uncovering the Layers:TCP/IPVulnerabilities

TCP/IP Vulnerabilities at the Physical Layer TCP/IP Vulnerabilities at the Data Link Layer TCP/IP Vulnerabilities at the Network Layer TCP/IP Vulnerabilities at the Transport Layer TCP/IP Vulnerabilities at the Session Layer TCP/IPVulnerabilities at the Application Layer

TCP/IP Vulnerabilities at thePhysical Layer.

The physical layer of TCP/IP is where data is transmitted through cables or wireless signals. This layer is vulnerable to attacks such as eavesdropping, interference, and jamming.

Eavesdropping occurs when an attacker intercepts data being transmitted and can readormodify it. Interference happens when a signal is disrupted by noise or other signals, causing errors in transmission. Jamming is a deliberate attempt to disrupt communication by flooding the channel with noise or interference.

TCP/IPVulnerabilities at the DataLink Layer.

The data link layer is responsible for transmittingdata between network devices. It is vulnerable to attacks such as MAC address spoofing, ARP spoofing, and VLAN hopping.

MAC address spoofing involves an attacker changing their MAC address to impersonate another device on the network. ARP spoofing is when an attacker sends fake ARP messages to associate their MAC address with the IP address of another device. VLAN hopping occurs when an attacker gains access to a VLAN they are not authorized to be in.

TCP/IP Vulnerabilities at the Network Layer.

The network layer is responsible for routing databetween networks. It is vulnerable to attacks such as IP spoofing, ICMP attacks, and routing table poisoning.a

IP spoofing involves an attacker forging the sourceIP address of packets to hide their identity or impersonate another device. ICMP attacks exploitvulnerabilities in the Internet Control Message Protocol to flood a network with traffic or causedenial of service. Routing table poisoning is whenan attacker modifies the routing tables of network devices to redirect traffic to a different destination.

TCP/IP Vulnerabilities at the Transport Layer.

The transport layer is responsible for ensuring reliable data transfer between applications. It is vulnerable to attacks such as SYN flooding, session hijacking, and UDP flooding.

SYN flooding involves an attacker sendinga large number of SYN packets to overwhelm a server and prevent legitimate connections. Session hijacking is when anattacker takes over an existing session between two devices to gain unauthorized access. UDP flooding is when an attacker floods a network with UDP packets to cause denial of service.

TCP/IP Vulnerabilities at the Session Layer.

The session layer is responsible for establishing and managing sessions between applications. It is vulnerable to attacks such as man-in-the-middle attacks, replay attacks, and denial-of-service attacks.

Man-in-the-middle attacks involve an attacker intercepting and modifying data between two devices to steal information or gain unauthorized access. Replay attacks involve an attacker intercepting and retransmitting data to gain unauthorized access. Denial-of-service attacks involve an attacker flooding a network with trafficto prevent legitimate connections.

TCP/IP Vulnerabilities at the Application Layer.

The application layer is responsible for providing services to users. It is vulnerable to attacks such as SQL injection, cross-site scripting, and buffer overflow attacks.

SQL injection involves an attacker inserting malicious code into a database query to gain unauthorized access or steal information. Cross-site scripting is when an attacker injects malicious code into a website to steal information or gain unauthorized access. Bufferoverflow attacks exploit vulnerabilities in software to execute malicious code.

Packet Sniffing

What is Packet Sniffing ?

When any data has to be transmitted over the computer network, it is broken down into smaller units at the sender's node called data packets and reassembled at receiver's node in original format. It is the smallest unit of communication over a computer network. It is also called a block, asegment, a datagram or a cell. The act of capturing data packet across the computer network is called packet sniffing. It is similar to as wire tapping to a telephone network. It is mostly used by crackers and hackers to collect information illegally about network. It is also used by ISPs, advertisers and governments. ISPs use packet sniffing to track all your activities such as:

- who is receiver of your email
- what is content of that email
- what you download
- sites you visit
- what you looked on that website
- downloads from a site

- streaming events like video, audio, etc

Packet Sniffer — Packet sniffing is done by using tools called packet sniffer. It can be either filteredor unfiltered. Filtered is used when only specific data packets have to be captured and Unfiltered is used when all the packets have to be captured. WireShark, SmartSniff are examples of packet- sniffing tools.
How to prevent packet sniffing ?

- Encrypting data you send or receive.
- using trusted Wi-Fi networks.
- Scanning your network for dangers or issues.

Advantages:
Network troubleshooting: Packet sniffing can be used to identify network problems by examining the packetsand identifying issues such as network congestion, packet loss, or improper configuration.
Security analysis: Packet sniffing can be used to detect and analyze security threats, such as networkintrusions, malware infections, or unauthorized access attempts.
Network optimization: Packet sniffing can be used to optimize network performance by identifying bottlenecksand optimizing the network configuration.
Protocol analysis: Packet sniffing can be used to analyze network protocols and identify areas where they canbe improved or optimized.

Disadvantages:
Privacy violations: Packet sniffing can be used to intercept sensitive information, such as passwords, creditcard numbers, or personal information, which can be used for malicious purposes.
Legal issues: In many jurisdictions, packet sniffing is illegal without the express consent of all parties involvedin the communication.
Resource usage: Packet sniffing can consume a significant amount of system resources, especially if largeamounts of network traffic are being analyzed.
Complexity: Packet sniffing can be a complex process, requiring specialized knowledge and tools to analyzenetwork traffic effectively.

ARP spoofing

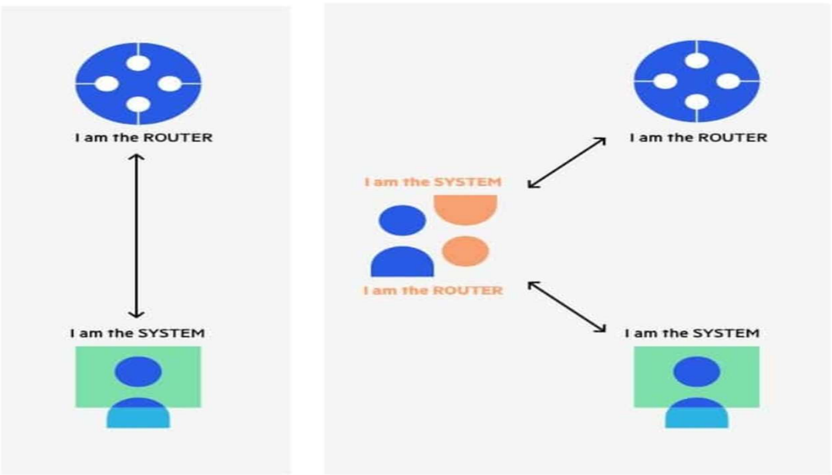
ARP Spoofing

What is the ARP Protocol ?
Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates InternetProtocol (IP) addresses to a Media Access Control (MAC) address, and vice versa. Most commonly, devices use ARP to contact the router or gateway that enables them to connect to the Internet

What is ARP Spoofing (ARP Poisoning)?
An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices. The attackworks as follows

1. The attacker must have access to the network. They scan the network todetermine the IP addresses of

The ARP spoofing attacker pretends to be both sides of a network communication channel



at least two devices—let’s say these are a workstation and a router.

2. The attacker uses a spoofing tool, such as Arpspoof or Driftnet, to send outforged ARP responses.
3. The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker’s MAC address. This fools both router and workstation to connect to the attacker’smachine, instead of to each other.
4. The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with eachother.
5. The attacker is now secretly in the middle of all communications.

Once the attacker succeeds in an ARP spoofingattack, they can:

- Continue routing the communications as- is—the attacker can sniff the packets and steal data, except if it is transferred overan encrypted channel like HTTPS.
- Perform session hijacking—if the attacker obtains a session ID, they can gain accessto accounts the user is currently logged into.
- Alter communication—for example pushing a malicious file or website to theworkstation.
- Distributed Denial of Service (DDoS)—theattackers can provide the MAC address ofa server they wish to attack with DDoS, instead of their own machine. If they do this for a large number of IPs, the targetserver will be bombarded with traffic.

How to Detect an ARP Cache Poisoning Attack

What is a computer port?

A port in computing has three main uses, each as a type of receptacle in networking,

computer hardware and software:

- A port in networking is a software-defined number associated to a networkprotocol that receives or transmits communication for a specific service.
- A port in computer hardware is a jack or socket that peripheral hardware plugs into.
- A port in computer software is when a piece of software has been translated orconverted to run on different hardware or operating system (OS) than it was originally designed for

PORTSCANNER

A port scanner is an application which is made to probe a host or server to identify open ports. Bad actors can use port scanners to exploit vulnerabilities by finding network services running on a host.They can also be used by security analysts to confirm network security policies.

PORT SCANNING PROCESS

Running a port scan on a network or server reveals which ports are open andlistening (receiving information) as well as revealing the presence of security devices, such as firewalls, that are present between the sender and the target.
This technique is known as fingerprinting.

It is also valuable for testing network security and the strength of the system’sfirewall. Due to this functionality, it is also a popular reconnaissance tool for attackers seeking a weak point of access to break into a computer.

Ports vary in their services offered. They are numbered from 0 to 65535, but certain ranges are more frequently used. Ports 0 to 1023 are identified as the “well-known ports” or standard ports and have been assigned services by theInternet ssigned Numbers Authority (IANA).

Some of the most prominent portsandtheirassignedservicesinclude:

- Port20(UDP)—FileTransferProtocol(FTP)fordatatransfer
- Port 22 (TCP) — Secure Shell (SSH) protocol for secure logins, FTP, andport forwardinG
- Port 23 (TCP) — Telnet protocol for unencrypted text commutations
- Port 53 (UDP) — Domain Name System (DNS) translates names of allcomputers on internet-to-IP addresses
- Port 80 (TCP) — World Wide Web HTTP

IP SPOOFING

WHAT IS IP SPOOFING?

IP spoofing is the creation of Internet Protocol (IP) packets which have a modifiedsource address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invokeDDoSattacksagainstatargetdeviceorthesurroundinginfrastructure.

Sending and receiving IP packets is a primary way in which networked computers and other devices communicate, and constitutes the basis of the modern internet. All IP packets contain a header which precedes the body of the packet and contains important routing information, including the source address. In a normal packet, the source IP address is the address of the sender of the packet. If the packet has been spoofed, the source address will be forged.

What is a Denial-of-Service (DoS) attack?

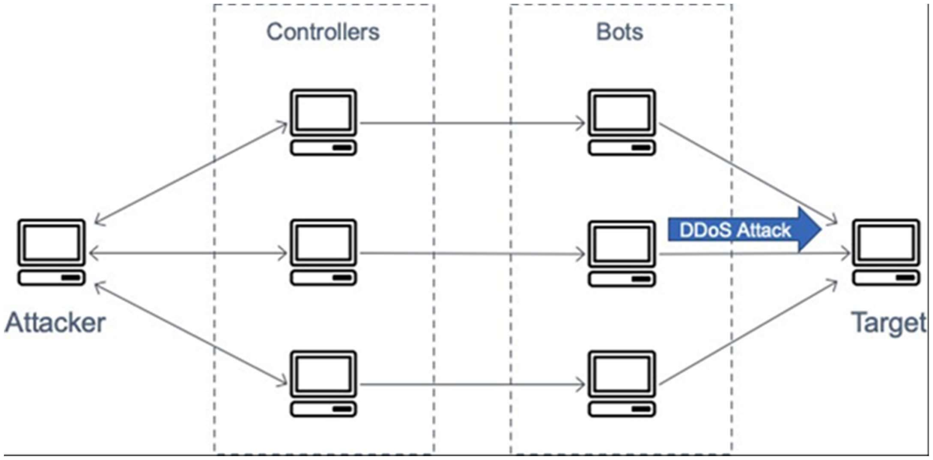
A **Denial-of-Service (DoS) attack** floods a server with traffic, making a website or resource unavailable.DoS and DDoS are attacks on the availability of CIA triads

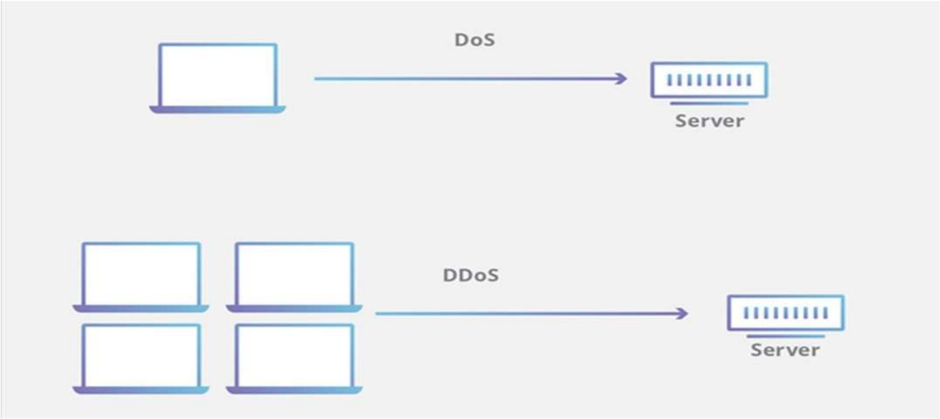
A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessibleto its intended users.

DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

In both instances, the **DoS attack** deprives legitimate users (i.e. employees, members, or account holders) of theservice or resource they expected.

Victims of DoS attacks are often web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theftor loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.



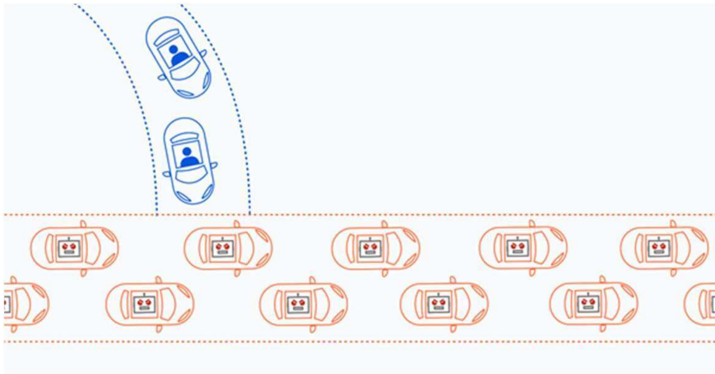


What is a DDoS attack?

A **distributed denial-of-service (DDoS) attack** is a DoS attack that uses multiple computers or machines to flood a targeted resource. Both types of attacks overload a server or web application with the goal of interrupting services.

EXAMPLE OF DDoS ATTACK :

A DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

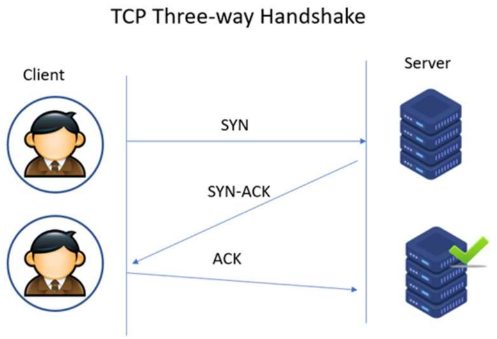


How does a DDoS attack work?

DDoS attacks are carried out with networks of Internet-connected machines.

These networks consist of computers and other devices (such as IoT devices)which have been infectedwith malware, allowing them to be controlled remotely by an attacker. These individual devices are referred toas bots , and a group of bots is called a botnet.

- DOS Stands for Denial of serviceattack.
- In Dos attack single systemtargets thevictim system
- Victim PC is loaded from the packet of data sent from a singlelocation.
- Dos attack is slower ascompared to DDoS.
- Can be blocked easily as onlyone system is used.
- DOS Attacks are Easy to trace.



DDoS

- DDOS Stands for Distributed Denial ofservice attack.
- In DDoS multiple systems attack thevictim's system.
- Victim PC is loaded from the packet ofdata sent from Multiple location
- DDoS attack is faster than Dos Attack.
- It is difficult to block this attack as multiple devices are sending packetsand attacking from multiple locations.
- DDOS Attacks are Difficult to trace.

ICMP FLOOD

- ICMP stands for Internet Control Message Protocol.
- It is a protocol used in computer networks to send error messagesand operational information about network conditions. ICMP is typically used by network devices, such as routers and servers, to communicate with each other and with other network devices.
- ICMP messages are sent as packets that contain information aboutnetwork conditions, such as packet delivery errors, network congestion, and network status updates.
- In ICMP, network congestion occurs when there is high volume of network traffic, causing delays in packet transmission and potentiallyleading to packet loss or other network problems.

Some common ICMP error messages include:

- Destination Unreachable: This message is sent when a network deviceis unable to reach the destination IP address specified in the IP packet.
- Time Exceeded: This message is sent when a packet's time to live (TTL) value reaches zero, indicating that it has been on the networkfor too long.
- Parameter Problem: This message is sent when there is an error in theIP header of the packet, such as an incorrect field value.
- To protect against ICMP floods, network administrators can configurefirewalls and routers to limit the amount of ICMP traffic that can passthrough.
- They can also use intrusion detection systems (IDS) and other securitytools to monitor network traffic and detect and block suspicious activity.
- Here IDS is a type of security software or hardware that is used to monitor network traffic and detect suspicious or malicious activity.
- When an IDS system detects a potential intrusion (means an unauthorized attempt to access or disrupt a computer system), itgenerates an alert or notification that can be used by network administrators to investigate and respond to the threat

SYNFLOODATTACK

A SYN flood attack is a type of denial-of-service (DoS) attack on a computer server. This exploit is also known as a ***half-open attack***.

- SYN floods are one of several common vulnerabilities that take advantage of TCP/IP to overwhelm target systems. SYN flood attacks use a process known as the *TCP three-way handshake*.

TCPTHREE-WAYHANDSHAKE

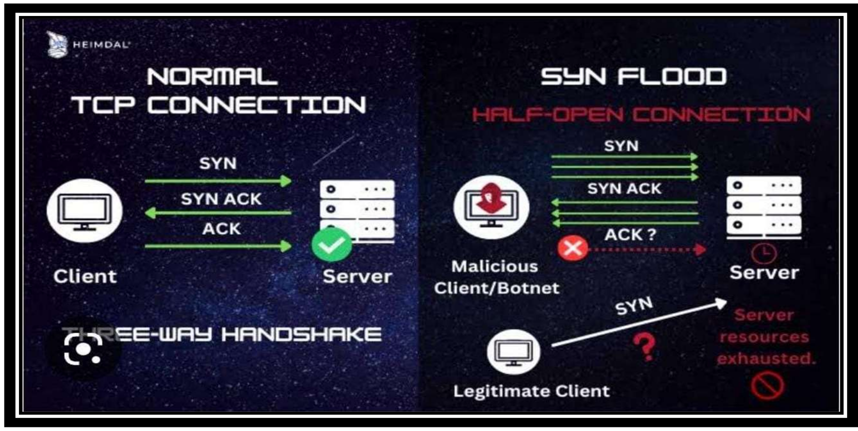
A three-way handshake involves the following three steps:

1. The client sends a SYN packet to initiate communication with theserver.
2. The server responds, sending a SYN-ACK packet.
3. The client returns a final ACK packet to confirm that the server'sSYN-ACK packet was received.

1. Direct SYN Flood Attack

- In this method, the hacker initiates the attack using his own IP address.He sends multiple SYN requests to the server. However, when the server responds with SYN-ACK, as an acknowledgment, he doesn't respond with ACK but keeps sending the new SYN request to the victim server.
- While the server waits for ACK, the arrival of SYN packets preserves the Server resources with a half-open connection session for a certain time, which eventually makes the server unable to operate normally and deny the requests from the legitimate client.
- **SYN Spoofed Attack**
- As an alternative to avoid being detected, the malicious attack sends the SYN packets from spoofed/forged IP addresses. Upon receiving the SYN request, the server sends the SYN-ACK to the forged IP address and waits for a response. Since the spoofed source didn't send the packets, they don't respond.

- **DDoS (Distributed Denial of Service) SYN attack**
- In this variant of SYN flood attack, the victim server receives SYN packets simultaneously from several infected computers under the control of the attacker. This combination of hijacked machines is called a **botnet.** For an added level of obfuscation, an attacker may have each distributed device also spoof the IP addresses from which it sends packets. If the attacker is using a botnet such as the Mirai botnet,they generally won't care about masking the IP of the infected device.
- In networking, when a server is leaving a connection open but the machine on the other side of the connection is not, the connection isconsidered half-open.



Prevent SYN Flood Attacks:You can prevent SYN Flood attack by:

1- Installing an IPS to detect anomalous traffic patterns.IPS :
Organizations choose IPS technologies over traditional reactive network security efforts because IPSproactively detects and prevents harm from malicious traffic. IPS protection identifies potential threats by monitoring network traffic in real time by using network behavior analysis.

If an unauthorized attacker gains network access, the IPS identifies the suspicious activity, records the IP address, and launches an automated response to the threat based on rules set up in advanceby the network administrator.

2- If capability exists, configure the onsite firewall for SYN AttackThresholds and SYN Flood protection

3- adaptive thresholding algorithm

4- Installing up to date networking equipment that has rate-limiting capabilities.

5- Installing commercial tools to gain visibility across the entirenetwork with the ability to see and analyze traffic from different parts of the network.

Tools:

Access control Application securityEmail security
Firewall
Virtual private network (VPN)Websecurity

Wirelesssecurity

UDP FLOOD

What is UDP ?

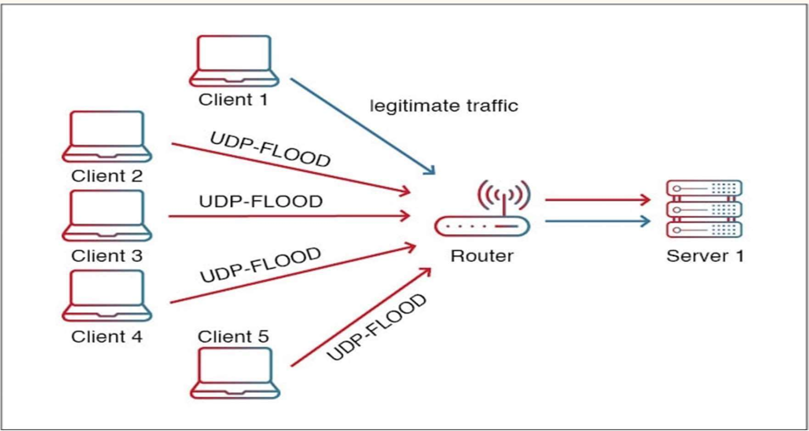
User Datagram Protocol (UDP) is a connectionless, unreliable protocol used in computer networks. It operates on the transport layer of the Internet Protocol (IP)and provides fast, efficient data transfer across networks. Unlike TCP – its more reliable counterpart – UDP does not provide end-to-end reliability or flow control.

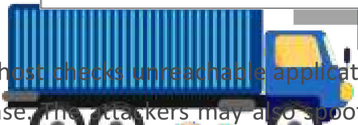
In computer networking, the User Datagram Protocol is one of the core communication protocols of the Internet protocol suite used to send messages toother hosts on an Internet Protocol network. Within an IP network, UDP does notrequire prior communication to set up communication channels or data paths.

UDP FLOOD ATTACK :

A UDP flood is a type of denial-of-seívice attack in which a laíge numbeí of Useí Datagíam Píotocol (UDP) packets aíe sent to a taígeted seíveí with the aim of oveíwhelming that device's ability to píocess and íespond. I̋he fiíewall píotecting the taígeted seíveí can also become exhausted as a íesult of UDP flooding, íesulting in a denial-of-seívice to legitimate tíaffic.

How does a UDP flood attack work?





An attacker will send a large number of UDP packets with random data to the target port.The receiving host checks unreachable applications and ports (by design by the attacker) associated with these datagrams and responds back with a “Destination Unreachable” response. The attackers may also spoof of the return IPaddress making it unreachable as well. As more and more such packets are received, the server becomes flooded and unable to process legitimate requests or respond to other client requests.

How can a UDP flood attack be mitigated?

A UDP flood attack can be mitigated by utilizing a variety of methods.

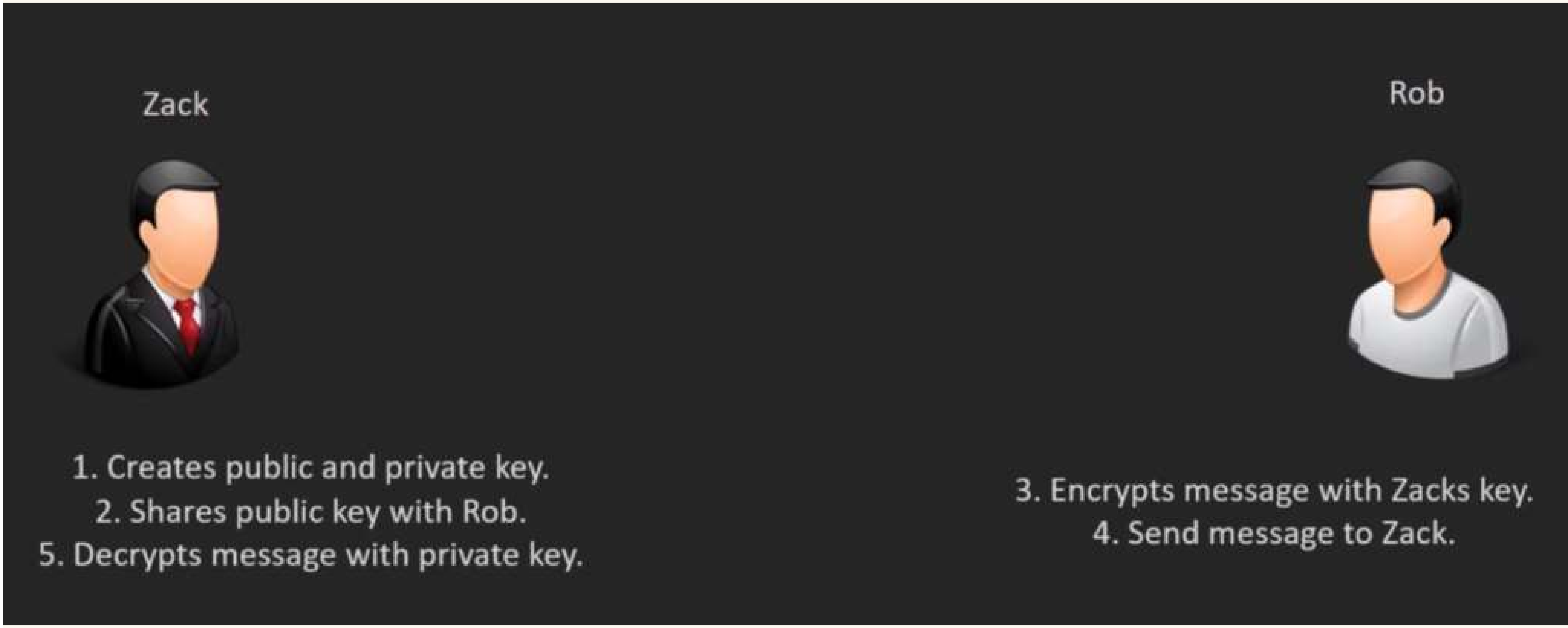
1. One of the most effective measures is to implement rate-limiting on incoming traffic.Rate-limiting is a technique that allows the server to limit the number of packets sent by each individual source address over a certain period of time. However, rate limitingmay prevent legitimate traffic during surge conditions.

2.Radware DDoS protection (DefensePro, Cloud DDoS Protection Service), WAF (AppWall and Cloud WAF) and application delivery (Alteon with integrated WAF) solutions mitigate UDP Flood attacks by using machine-learning and behavioral-basedalgorithms to understand what constitutes a legitimate behavior profile and then automatically block malicious attacks. Radware manages user connections effectively without impacting legitimate requests, increasing protection accuracy while minimizing false positives and disruption to legitimate users

Internet Security Protocols:PGP, SSL, IPSEC.

EXPLAIN INTERNET SECURITY PROTOCALL

INTERNET SECURITY PROTOCOLS ARE A SET OF RULES AND PROCEDURES DESIGNED TO ENSURE THE SECURE TRANSFER OF DATA OVER THE INTERNET. THESE PROTOCOLS PROVIDE MECHANISMS TOAUTHENTICATEUSERS AND ENSURE THE CONFIDENTIALITY, INTEGRITY,AND AVAILABILITY OF DATA TRANSMITTED OVER THEINTERNET.



Zack

Rob

1. Creates public and private key.
2. Shares public key with Rob.
5. Decrypts message with private key.

3. Encrypts message with Zacks key.
4. Send message to Zack.

SSL

SECURE SOCKETS LAYER (SSL):

- SSL IS A PROTOCOL USED TO SECURE DATA TRANSMISSION OVER THE INTERNET.
- IT PROVIDES A SECURE CHANNEL BETWEEN A CLIENT AND A SERVER BY ENCRYPTING DATA EXCHANGED BETWEEN THEM.
- SSL IS COMMONLY USED FOR SECURE ONLINE TRANSACTIONS, SUCH AS ONLINE SHOPPING AND BANKING.
- SSL PROVIDES MECHANISMS FOR AUTHENTICATION, INTEGRITY, AND CONFIDENTIALITY TO ENSURE THAT DATA TRANSMITTED OVER THE INTERNET IS SECURE.

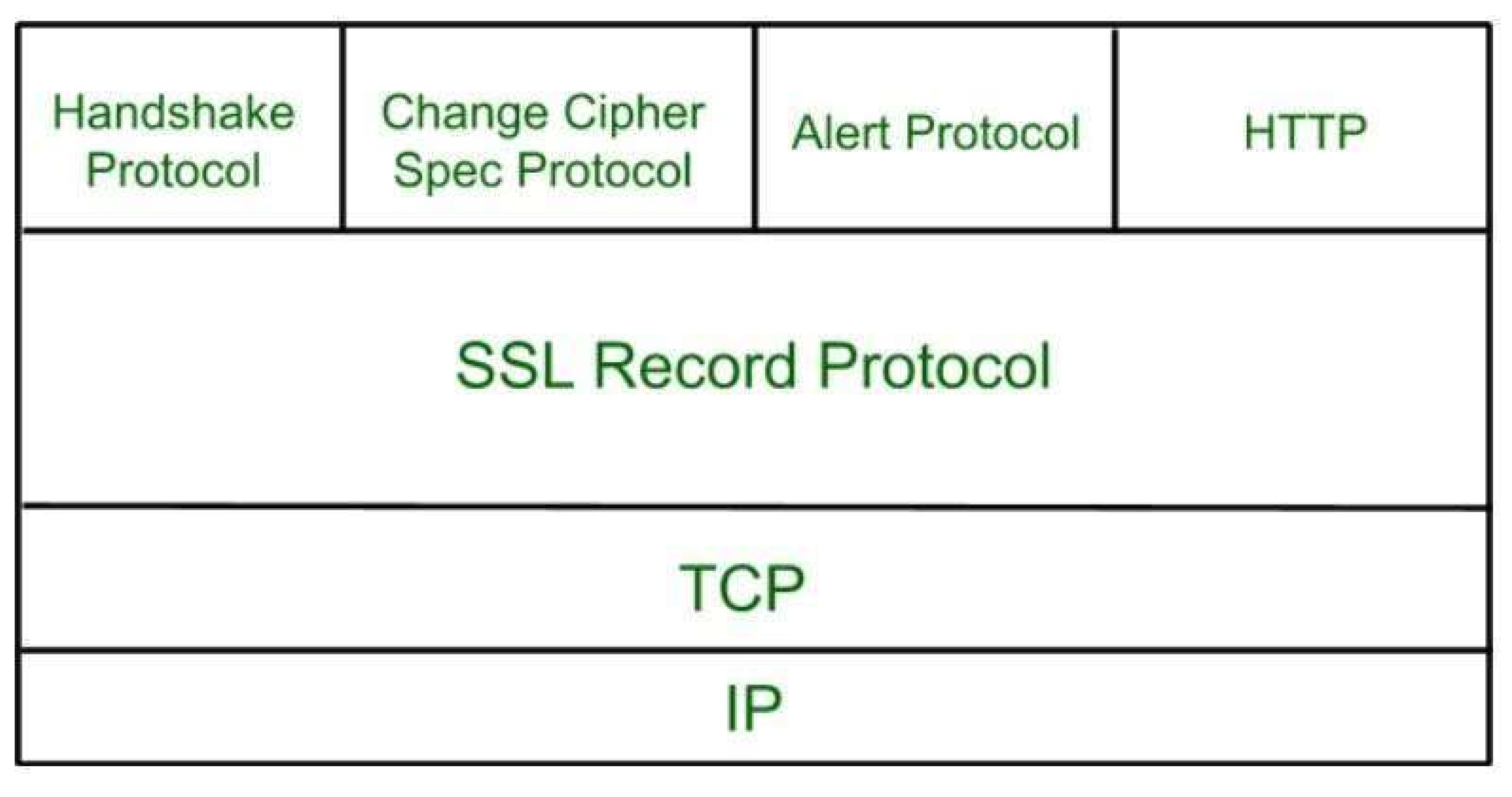
- SSL HAS BEEN REPLACED BY TLS (TRANSPORT LAYER SECURITY), BUT SSL IS STILL COMMONLYUSED TO REFER TO THE PROTOCOLSUITE.
- THE SSL DIAGRAM SHOWS A CLIENT (SUCH AS A WEB BROWSER) COMMUNICATING WITH ASERVER (SUCH AS A WEBSITE) OVER THE INTERNET.
- THE CLIENT INITIATES A CONNECTION BY SENDING A "HELLO" MESSAGE TO THE SERVER.
- THE SERVERRESPONDSBY SENDING ITS DIGITALCERTIFICATE TO THE CLIENT, WHICH CONTAINSITS PUBLIC KEY AND OTHER IDENTIFYING INFORMATION.
- THE CLIENT VERIFIES THE DIGITAL CERTIFICATETO ENSURE THAT IT IS LEGITIMATE AND HAS NOTBEEN TAMPERED WITH.

- THE CLIENT GENERATES A RANDOM SYMMETRICENCRYPTION KEY AND ENCRYPTS IT USING THE SERVER'S PUBLIC KEY, WHICH IS OBTAINED FROM THE DIGITAL CERTIFICATE.
- THE ENCRYPTED KEY IS SENT TO THE SERVER,WHICH DECRYPTS IT USING ITS PRIVATE KEY.
- BOTH THE CLIENT AND SERVER USE THE SYMMETRIC ENCRYPTION KEY TO ENCRYPT AND DECRYPT ALL DATA TRANSMITTED BETWEEN THEM.
- THIS CREATES A SECURE "TUNNEL" THROUGHWHICH ALL COMMUNICATION TAKES PLACE, ENSURING THAT DATA IS PROTECTED FROM UNAUTHORIZED ACCESS OR INTERCEPTION.

Secure Socket Layer (SSL)

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

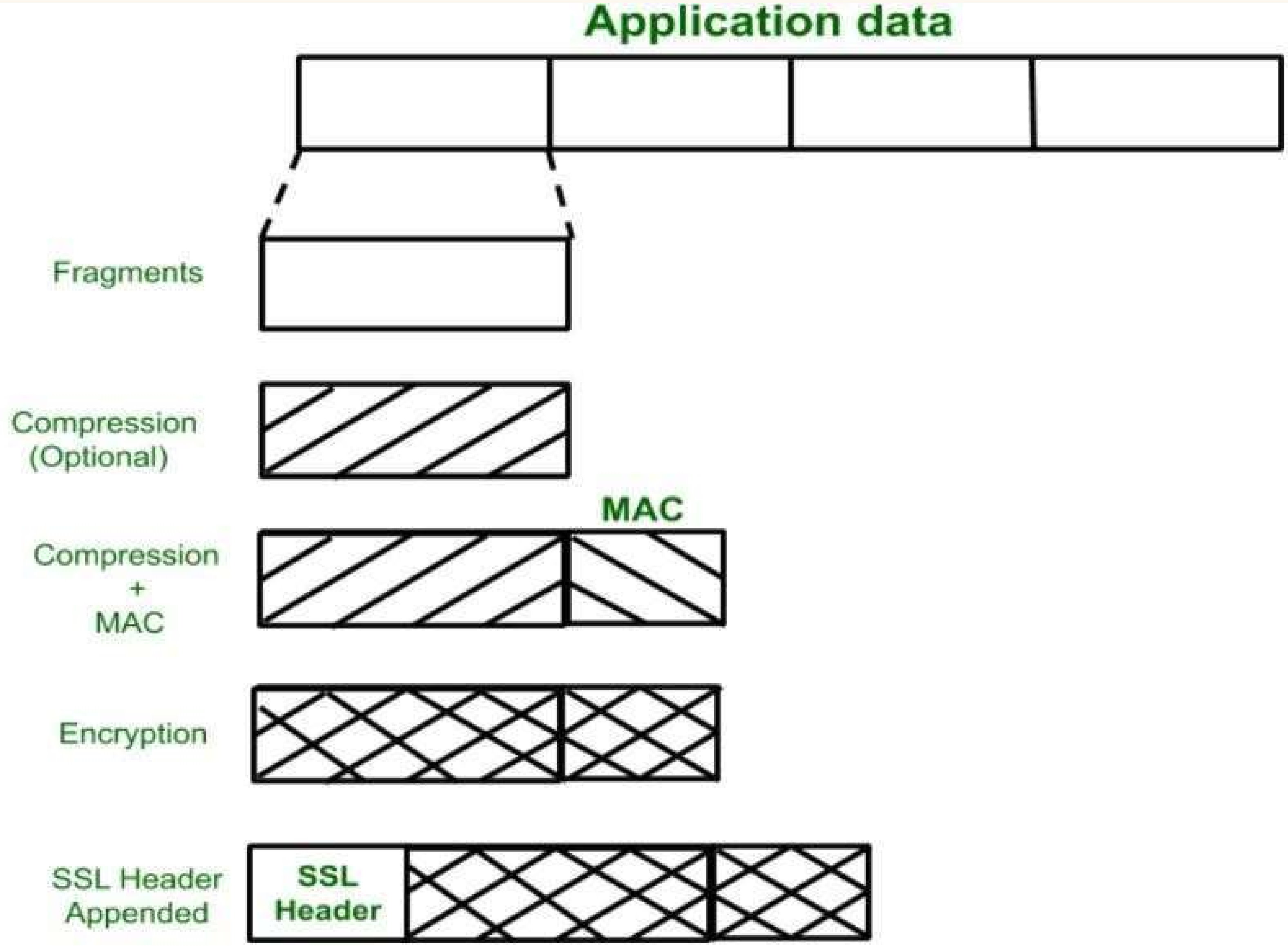


SSL Record Protocol:

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. Afterthat encryption of the data is done and in last SSL header is appended to the data.


Application data
Fragments
Compression
(Optional)
MAC
Compression
+
MAC
Encryption
SSL Header
Appended
SSL
Header

Handshake Protocol:

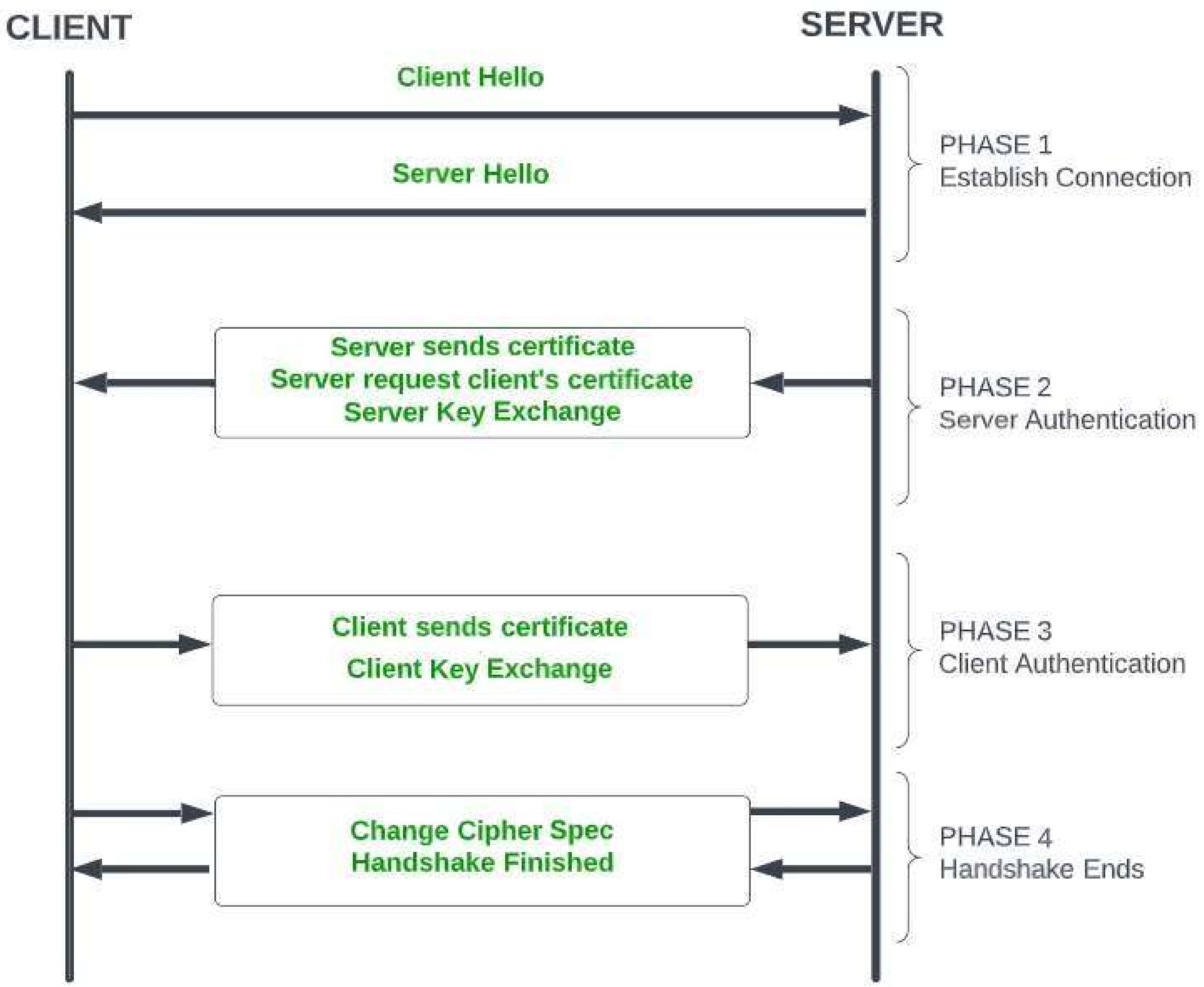
Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate eachother by sending a series of messages to each other. Handshake protocol uses four phases to complete itscycle.

- **Phase-1:** In Phase-1 both Client and Server send hello- packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.

- **Phase-2:** Server sends his certificate and Server-key- exchange. The server end phase-2 by sending the Server-hello-end packet.

- **Phase-3:** In this phase, Client replies to the server bysending his certificate and Client-exchange-key.

- **Phase-4:** In Phase-4 Change-cipher suite occurs andafter this the Handshake Protocol ends.



SSL HANDSHAKE PROTOCOL

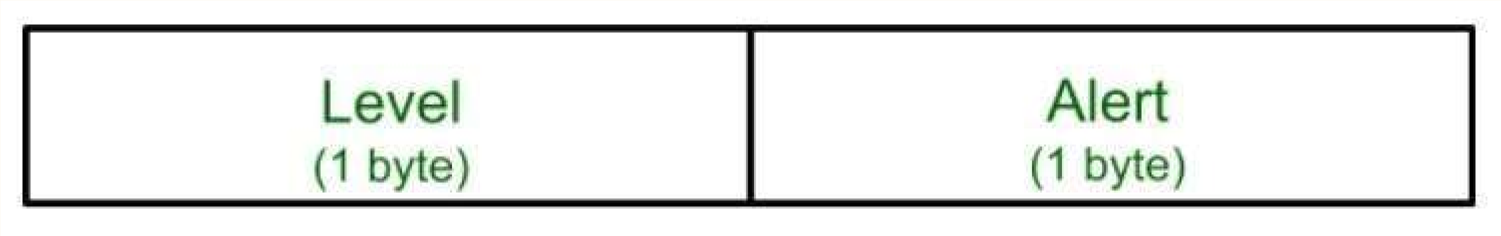
Change-cipher Protocol:

This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, theSSL record Output will be in a pending state. After the handshake protocol, the Pending state is converted into the current state.

Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol's purpose is to cause the pending state to be copiedinto the current state.

Alert Protocol:

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.



This level can be further divided into two parts :-

Warning (level = 0)
This alert has no impact on the connection between sender and receiver. Some of them are:

Bad Certificate :- When the received certificate is corrupt.
No certificate: When an appropriate certificate is not available.
Certificate expired: When a certificate has expired.
Certificate unknown: When some other unspecified issue arose in processing the certificate, rendering it unacceptable.
Close notify: It notifies that the sender will no longer send any messages in theconnection.
Unsupported certificate: The type of certificate received is not supported.Certificate revoked: The certificate received is in revocation list.

Fatal Error (level = 2):

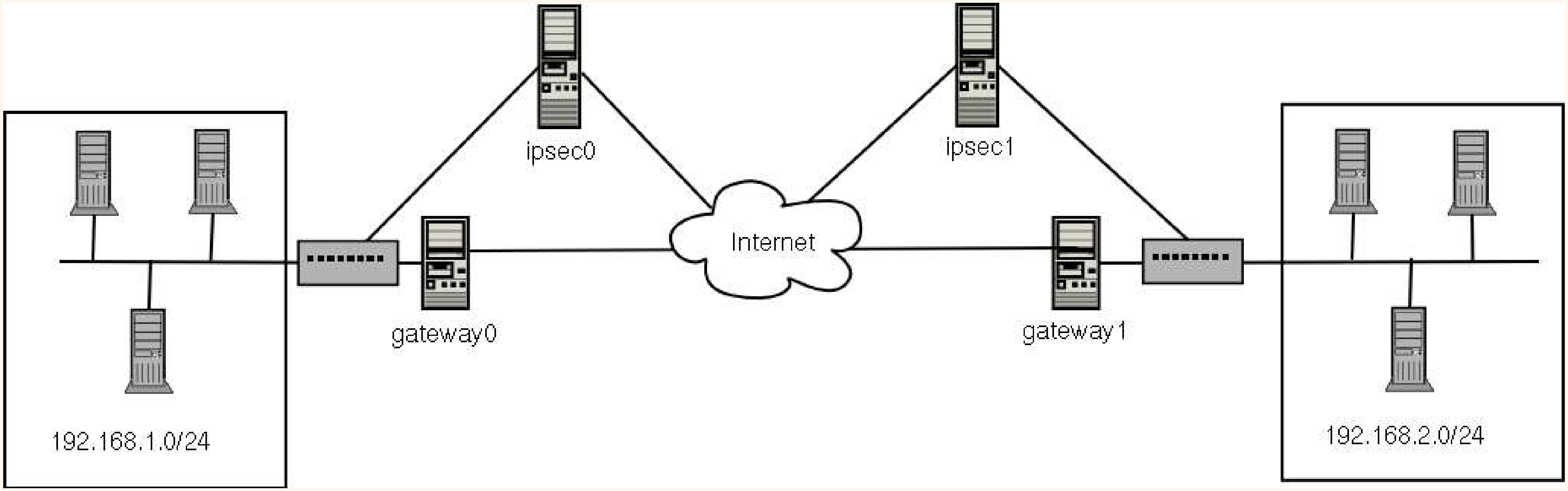
This Alert breaks the connection between sender and receiver. The connection will be stopped, cannot be resumed but can be restarted. Some of them are :

Handshake failure: When the sender is unable to negotiate an acceptable set of security parameters given the options available.
Decompression failure: When the decompression function receives improper input.
Illegal parameters: When a field is out of range or inconsistent with other fields.
Bad record MAC: When an incorrect MAC was received.
Unexpected message: When an inappropriate message is received.The second byte in the Alert protocol describes the error.

IPSEC

INTERNET PROTOCOL SECURITY (IPSEC):

- IPSEC IS APROTOCOL USED TOSECURE INTERNET COMMUNICATIONS ATTHE NETWORK LAYER.
- ITPROVIDES MECHANISMS FOR AUTHENTICATION, ENCRYPTION, AND INTEGRITY CHECKING TO ENSURE THAT DATA TRANSMITTED OVER THE INTERNET IS SECURE.
- IPSEC CAN BE USED TOSECURE AWIDE RANGE OFINTERNET- BASED APPLICATIONS, INCLUDING EMAIL, WEB BROWSING, AND FILE TRANSFERS.
- IPSEC IS COMMONLY USED IN VIRTUAL PRIVATENETWORKS (VPNS) TO PROVIDE SECURE REMOTEACCESS TO CORPORATE NETWORKS.



- THE TWO NETWORKS ARE CONNECTED BY TWO IPSEC

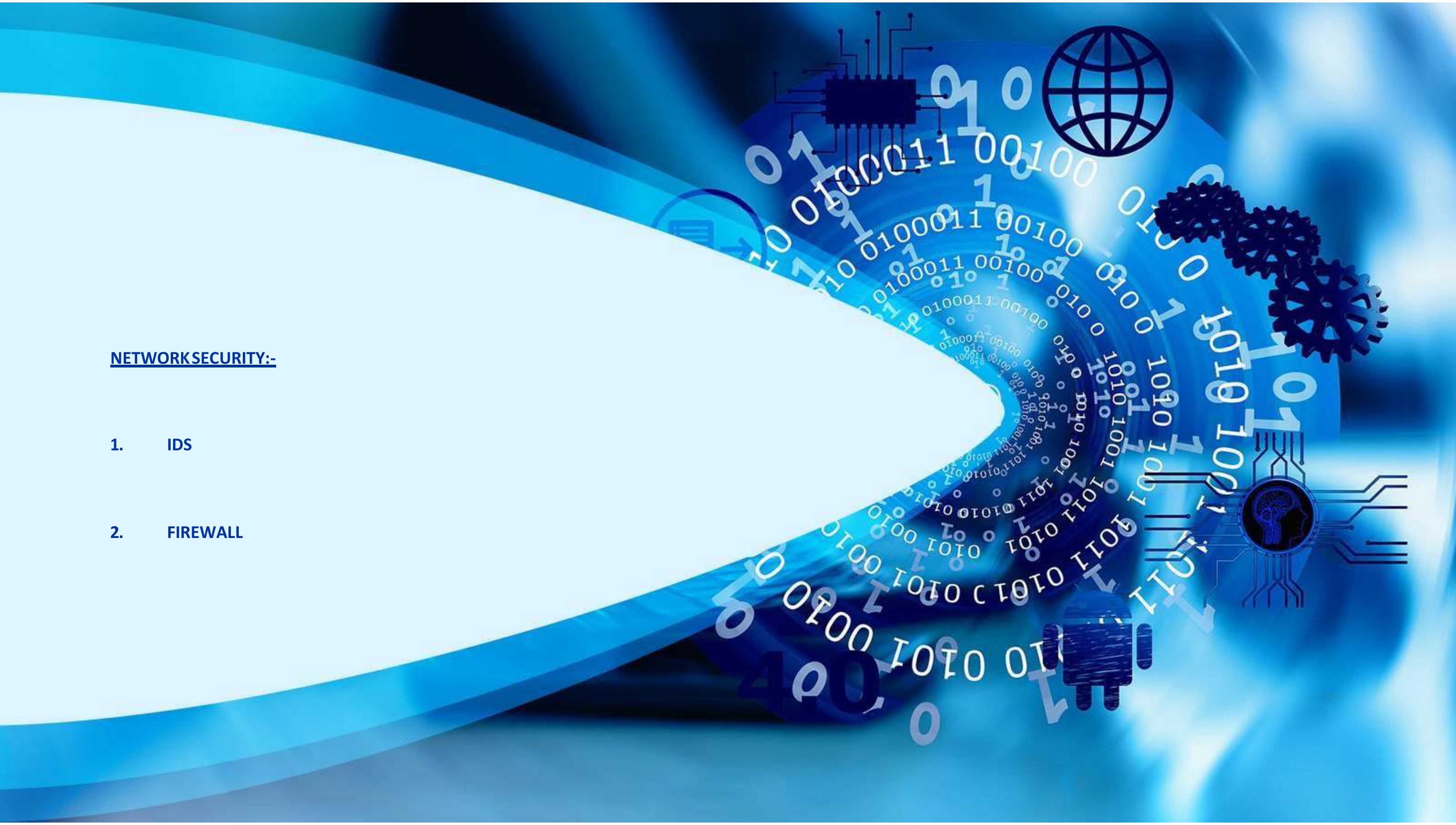
  GATEWAYS (GATEWAY A AND GATEWAY B) THAT ACT AS

  INTERMEDIARIES BETWEEN THE TWO NETWORKS.
- THE IPSEC GATEWAYS ESTABLISH A SECURE TUNNELBETWEEN THEM USING THE IPSEC PROTOCOL SUITE.THE SECURE TUNNEL CAN BE SEEN AS A "VIRTUAL"

  PRIVATE NETWORK (VPN) THAT CONNECTS THE TWO
- NETWORKS.
- ALL TRAFFIC BETWEEN THE TWO NETWORKS IS

  ENCRYPTED AND TRANSMITTED THROUGH THE SECURE

  TUNNEL.
- ANY UNAUTHORIZED ATTEMPTS TO ACCESS THE SECURETUNNEL OR IN TERCEPT THE ENCRYPTED TRAFFIC WILL BEDETECTED AND PREVENTED BY THE IPSEC GATEWAYS.



NETWORK SECURITY:-

1. **IDS**

2. **FIREWALL**

What is Network security?

- Network security is a level of guarantee that all the machines in a networkare working optimally and the users of these machines only possess the rights that were granted to them.
- This can include: Preventing unauthorized people from acting on thesystem maliciously preventing users from performing involuntary operations that are capable of harming the system.
- Securing data by anticipating failures guaranteeing that services are notinterrupted.

Why do we need network security?

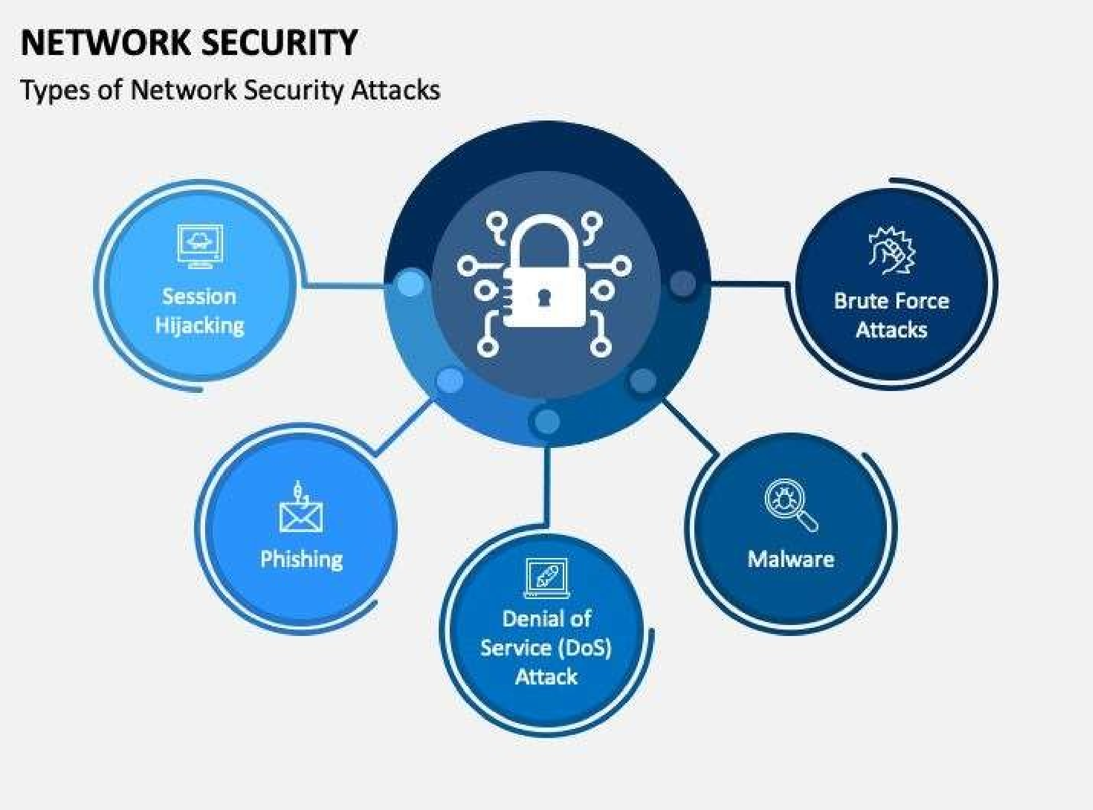
In the past, hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Todayalmost anyone can become a hacker by downloading tools from the Internet.

These complicated attack tools and generally open networks have generatedan increased need for network security and dynamic security policies.

The easiest way to protect a network from an outside attack is to close it offcompletely from the outside world.

A closed network provides connectivity only to trusted known parties andsites; a closed network does not allow a connection to public networks.

Network Attack Methods:-



NETWORK SECURITY

Types of Network Security Attacks

Advantages of Network Security

- Network Security helps in protectingpersonal data of clients existing on network.
- Network Security facilitates protection ofinformation that is shared between computers on the network.
- Hacking attempts or virus/spyware attacksfrom the internet will not be able to harm physical computers.
- External possible attacks are prevented.

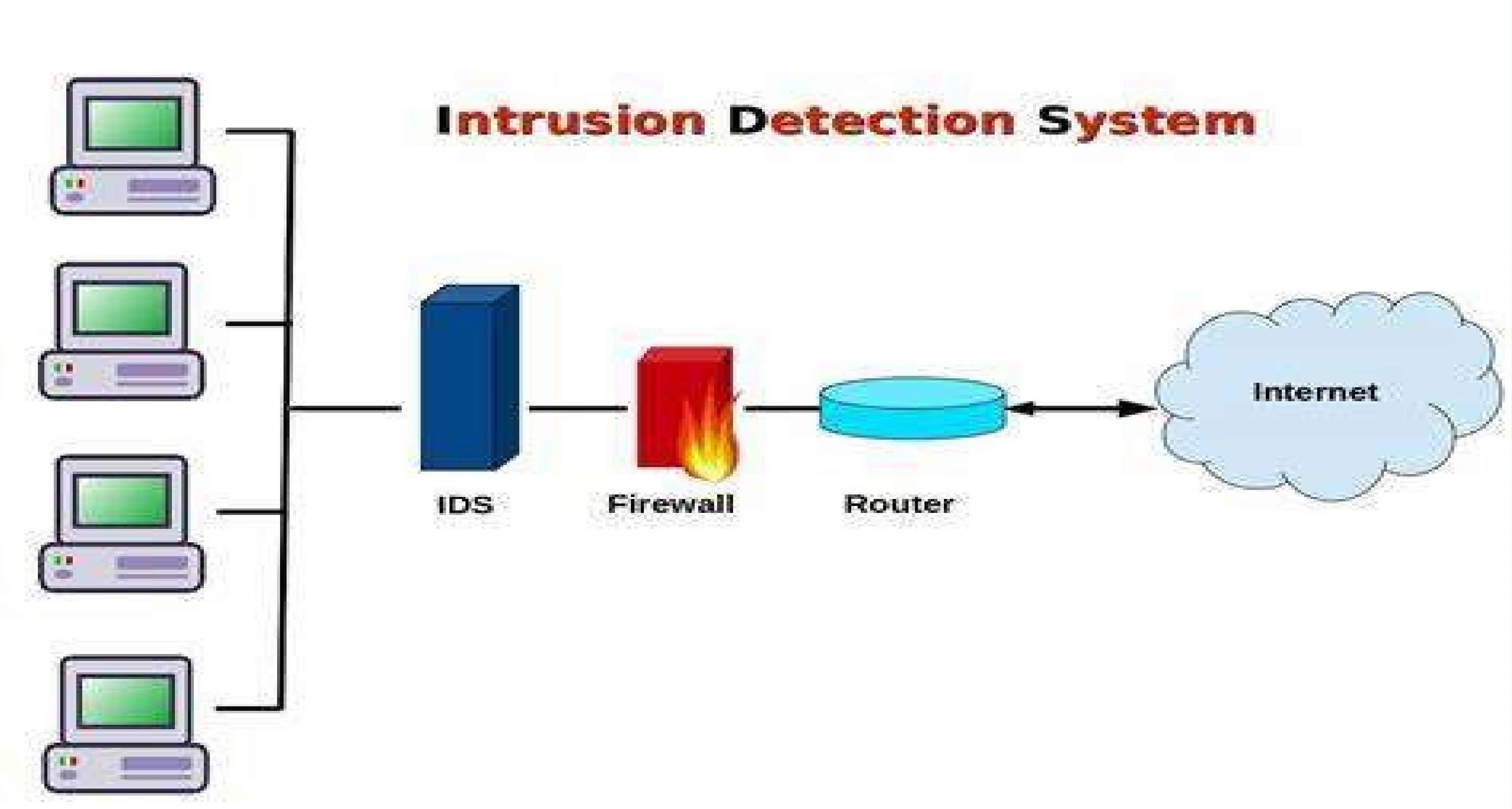
IDS (INTRUSION DETECTION SYSTEM)

- Intrusion detection is the process of identifying and responding to maliciousactivity targeted at resources
- IDS is a system designed to test/analyze network system traffic/events against agiven set of parameters and alert/capture data when these thresholds are met.
- IDS uses collected information and predefined knowledge-based system to reasonabout the possibility of an intrusion.
- IDS also provides services to cop with intrusion such as giving alarms, activatingprograms to try to deal with intrusion, etc.

FUNCTIONS OF IDS

- An IDS detects attacks as soon as possible and takesappropriate action.
- An IDS does not usually take preventive measures when anattack is detected.
- It is a reactive rather than a pro-active agent.
- It plays a role of informant rather than a police officer.

DIAGRAM OF IDS:-



DIFFERENT TYPES OF IDS

- Network IDS (NIDS):-

Examines all network traffic that passes the NIC that the sensoris running on

- Host based IDS (HIDS):-

An agent on the host that monitors host activities and log files

- Stack-Based IDS

An agent on the host that monitors all of the packets that leaveor enter the host.
Can monitor a specific protocol(s) (e.g. HTTP for webserver)

HIDS(Host-based)

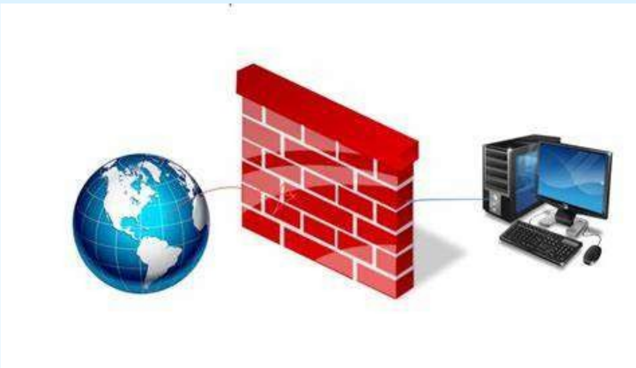
- It works in switched network environments.
- It operates in encrypted environments.
- HIDS detects and collects the most relevant informationin the quickest possible manner.
- It also keep tracks on behavior changes associated withmisuse.
- It requires the use of the resources of a host server - diskspace, RAM and CPU time.
- It does not protect entire infrastructure.

NIDS(Network-based)

- NIDS uses a passive interface to capture network packets foranalyzing.
- NIDS sensors placed around the globe can be configured to reportback to a central site, enabling a small team of security experts to support a large enterprise.
- NIDS systems scale well for network protection because the number of actual workstations, servers, or user systems on thenetwork is not critical the amount of traffic is what matters
- Most network-based IDSs are OS-Independent
- Provide better security against DOS attacks

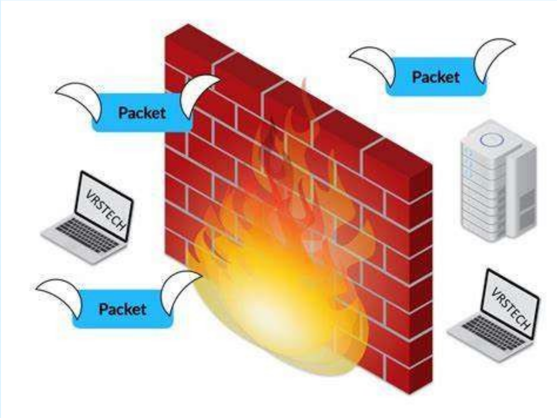
WHAT IS A FIREWALL?

- A firewall may be a hardware, software or a combination of both that is used to prevent unauthorized program or internetusers from accessing a private network or a single computer.
- All message entering or leaving the intranet pass through the firewall, which examines each message & blocks those that donot meet the specified security criteria.

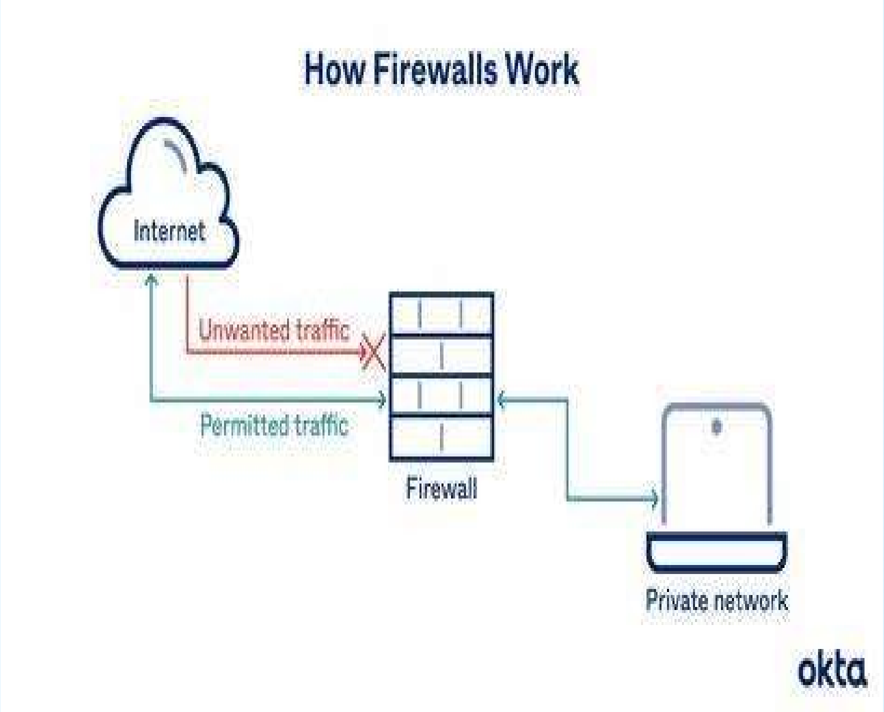


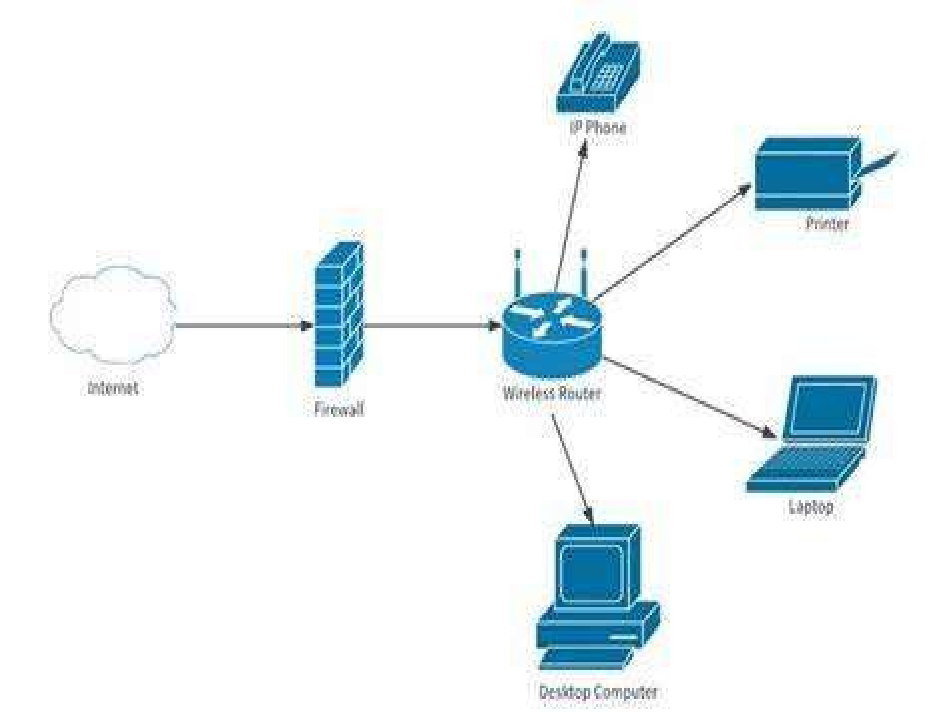
Why we need firewall

- To protect confidential information from those whodo not explicitly need to access it.
- To protect our network & its resources from malicious users & accidents that originate outsideof our network.



Working of Firewall





Types of Firewalls

Hardware Firewalls

- It is a physical device.
- It can be installed between themodem and computer.
- It can be incorporated into a broadband router being used to share the internet connection.
- Firewall is a part of a router or astandalone device.

Software Firewalls

- It is a software application.
- It is installed onto the computersystem that you wish to protect.
- Protect a single computer
- This is usually the computer withmodem attached to it.
- Usually less expensive, easier toconfigure

Hardware Firewalls

- E.g.- Cisco pix, netscreen, watchfuardetc.

Contd…….

Software Firewalls

- E.g.- Norton internet security,MacAfee internet security etc.

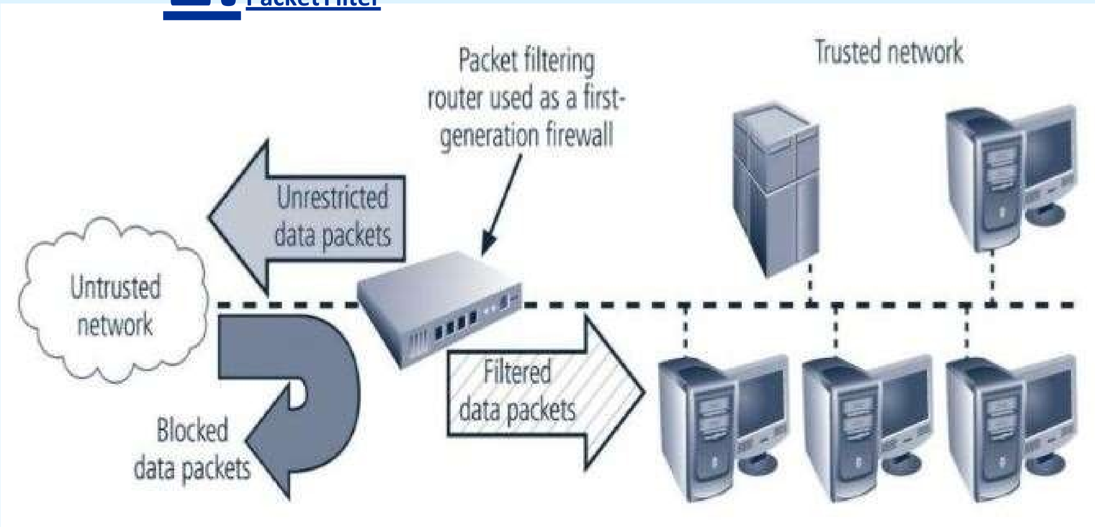
Different Types Of Firewall Techniques

- Packet filter
- Application gateway/proxy application gateway
- Circuit-level gateway
- Bastion host

1. Packet Filter

- The first type of network firewall was the packet filter which would look atnetwork addresses and ports of the packet to determine if that packet should be allowed or blocked.
- In this type of firewall deployment, the internal network is connected tothe external network/Internet via a router firewall. The firewall inspectsand filters data packet-by packet.
- Packet-filtering firewalls allow or block the packets mostly based on criteria such as source and/or destination IP addresses, protocol, source and/or destination port numbers, and various other parameters within theIP header.

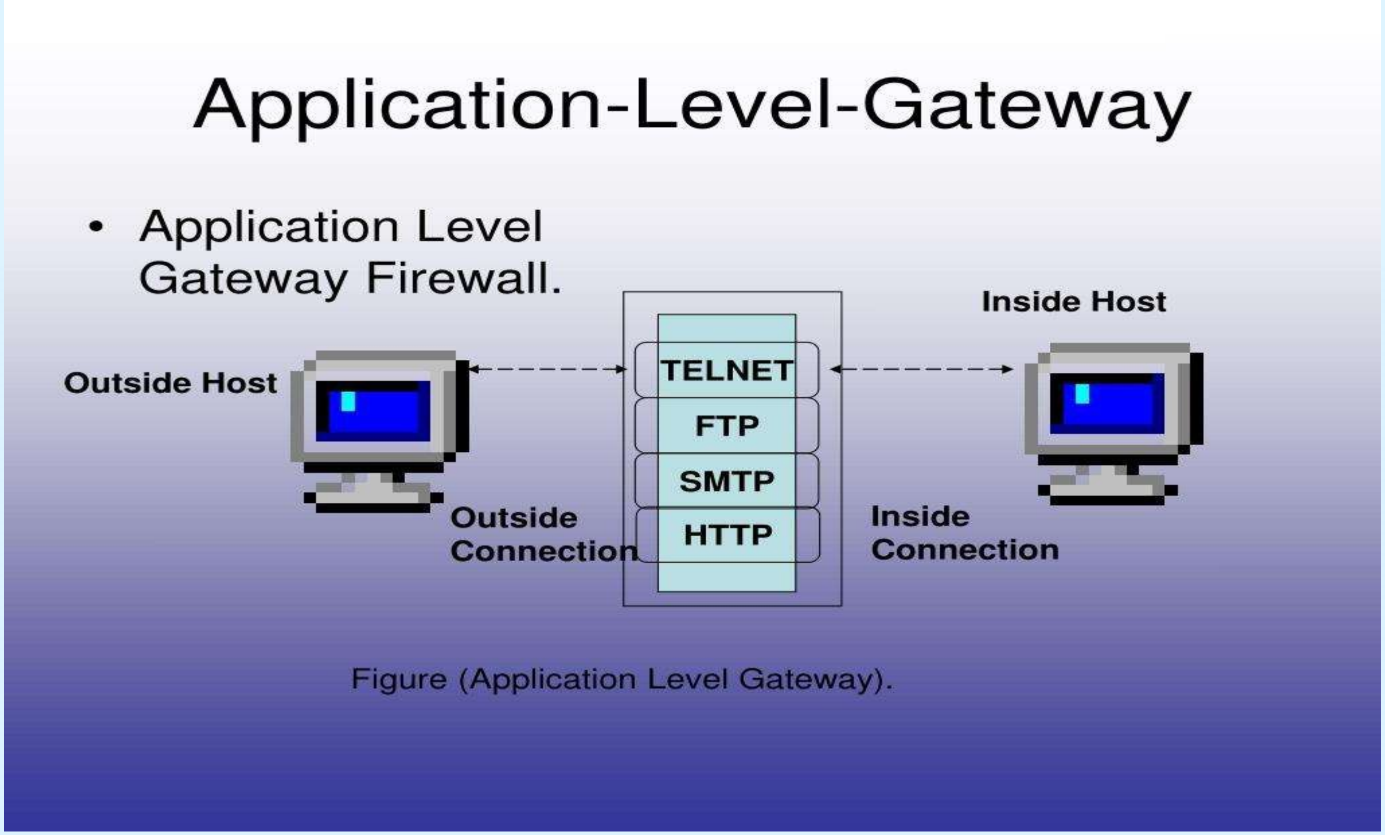
1. Packet Filter



2. Application gateway

- Application-level gateways tend to be more secure than packet filters. Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden atthe TCP and IP level, the application-level gateway need only scrutinize a few allowable applications.
- In addition, it is easy to log and audit all incoming traffic at theapplication level.

2. Application gateway



Application-Level-Gateway

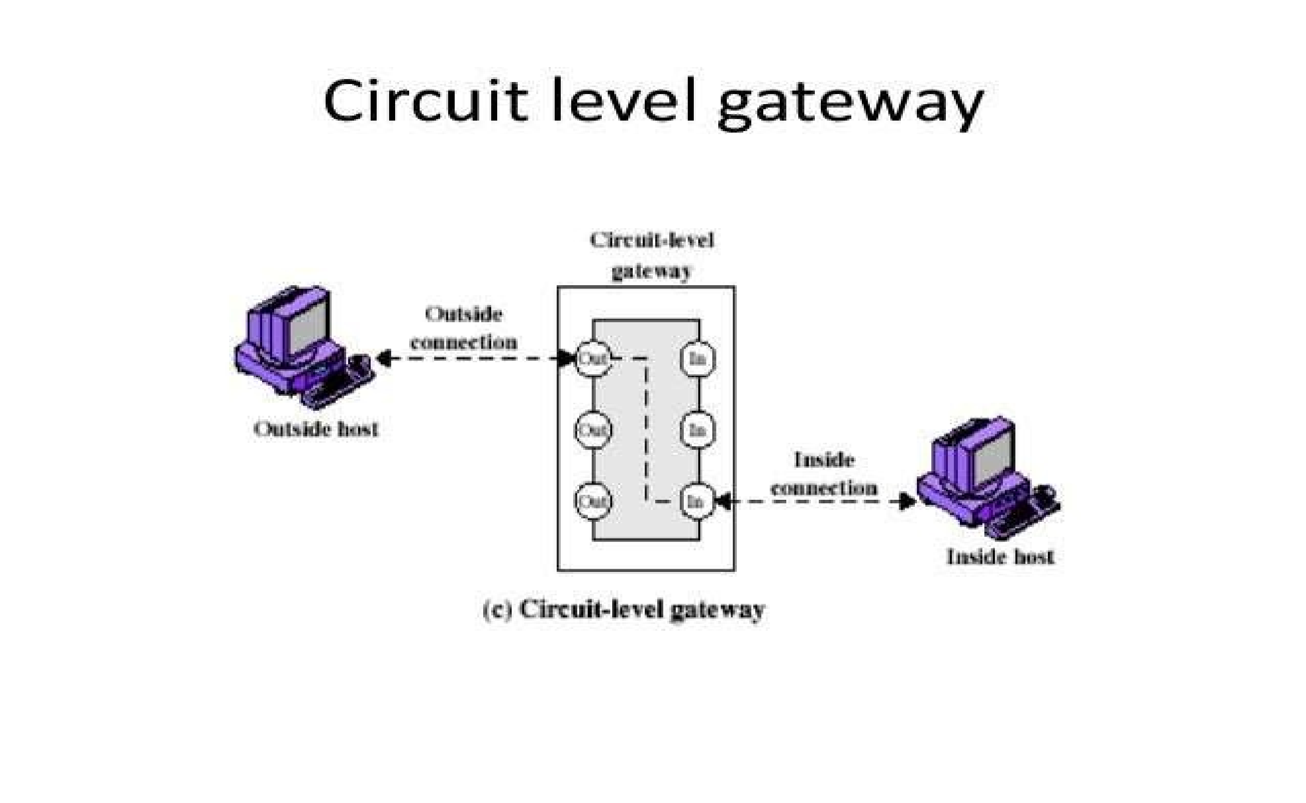
- Application Level Gateway Firewall.

Figure (Application Level Gateway).

3. Circuit-level gateway

- Circuit-level gateway work at the session layer of the OSI model, or as a "shim- layer" between the application layer and the transport layer of the TCP/IP stack.
- A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the twoconnections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents.
- A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections.

3. Circuit-level gateway



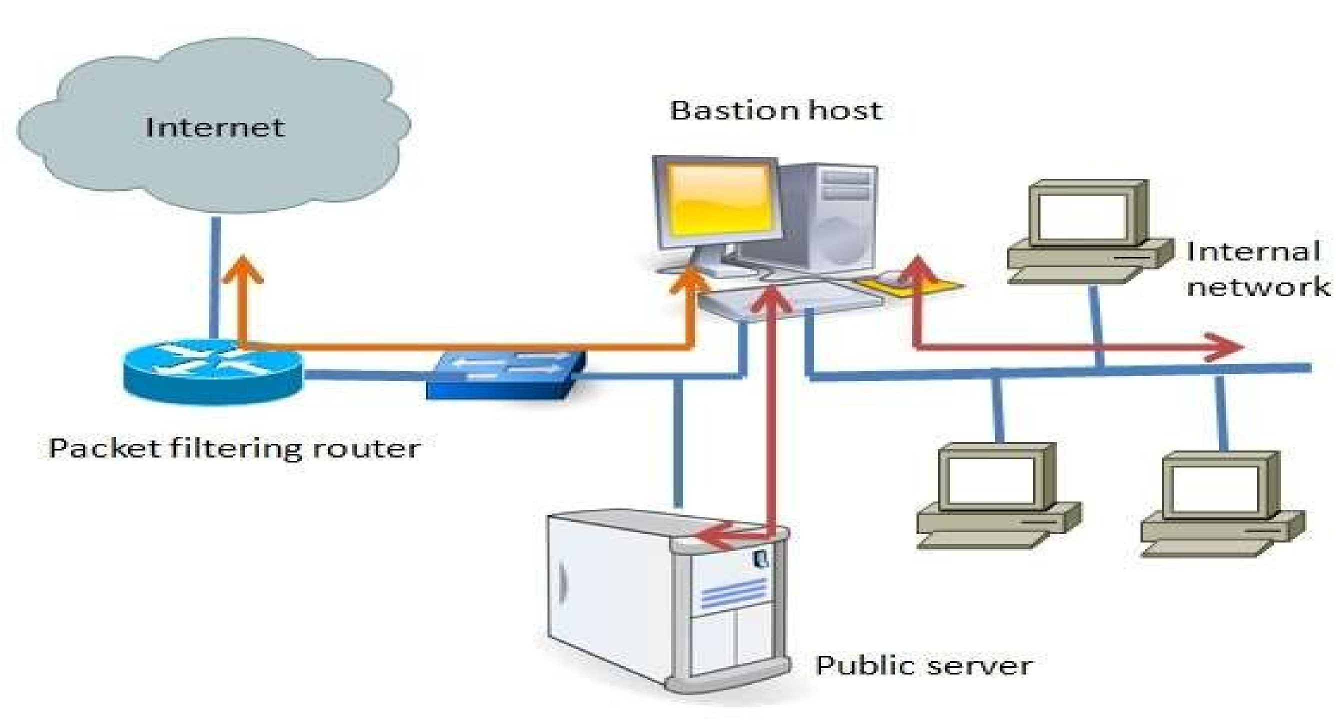
Circuit level gateway

(c) Circuit-level gateway

4. Bastion host

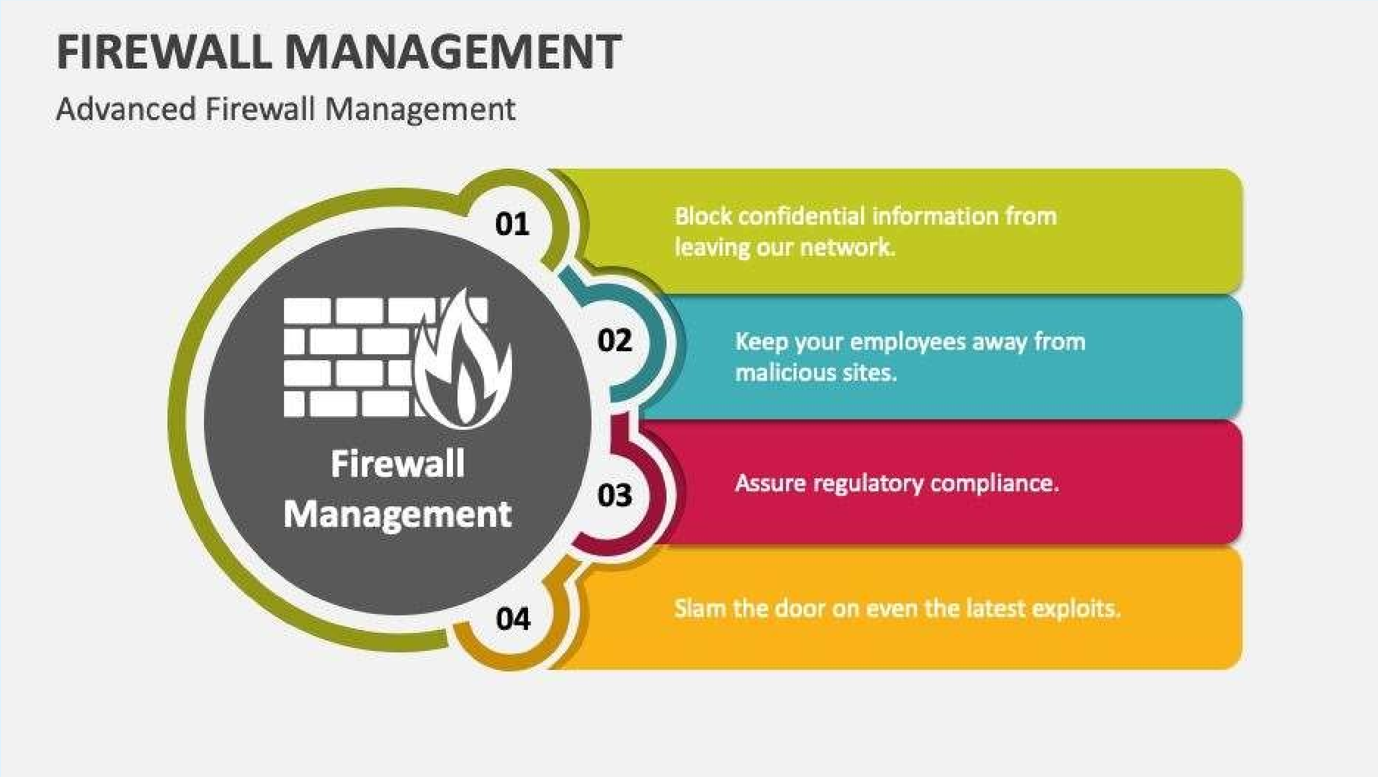
- Bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks.
- It generally hosts a single application, provides platformfor application gateway and circuit-level gateway.
- It supports limited/specific applications to reduce thethreat to the computer.
- Includeapplication-Telnet, SMTP, FTP

4. Bastion host



Screened host firewall (Dual-homed bastion host)

Firewall Management:-



FIREWALL MANAGEMENT

Advanced Firewall Management

Firewall Management

01 Block confidential information from leaving our network.

02 Keep your employees away from malicious sites.

03 Assure regulatory compliance.

04 Slam the door on even the latest exploits.

IDS v/s FIREWALL

IDS

- An intrusion detection system (IDS) is a device or software application that monitors a traffic for maliciousactivity or policy violations and sends alert on detection.
- Working:- Detects real time traffic and looks for trafficpatterns or signatures of attack and them generates alerts.
- Configuration mode:- Inline or as end host (via span) for monitoring and detection Non-Inline through port span (or via tap).
- Traffic patterns are analyzed.
- When unauthorized traffic is detected,it alerts/alarmson detection.

FIREWALL

- Firewall is a network security device that filters incomingand outgoing network traffic based on predetermined rules.
- Working:- Filters traffic based on IP address and portnumbers.
- Configuration mode:- Layer 3 mode or transparentmode.
- Traffic patterns are not analyzed.
- When unauthorized traffic is detected it blocks thetraffic