Q.1 Write a short note on IP security?

Ans. IPSec is a protocol suit for securing internet protocol (IP) communications by authenticating and encrypting each IP packet by authenticating and encrypting each packet of communication session.
It added to either current version of the IP (i.e., IPV4 or IPV6), by means of additional header.

Q.2 State some application of IP Security?

Ans. Applications of IPsec are:
IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.
Examples of its use include:

- **Secure branch office connectivity over the Internet**
- **Secure remote access over the Internet**
- **Establishing extranet and intranet connectivity with partners**
- **Enhancing electronic commerce security**

Q.3 What are the benefits of IPSec?
Ans.

1. When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.

2. IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.

3. IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.

4. IPsec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual sub-network within an organization for sensitive applications.

Q.4 State the services of IPSec.

Ans. The IPSec services are as follows:

- **Connectionless Integrity:-** Data integrity service is provided by IPSec via AH which prevents the data from being altered during transmission.
- **Data Origin Authentication**:- This IPSec service prevents the occurrence of

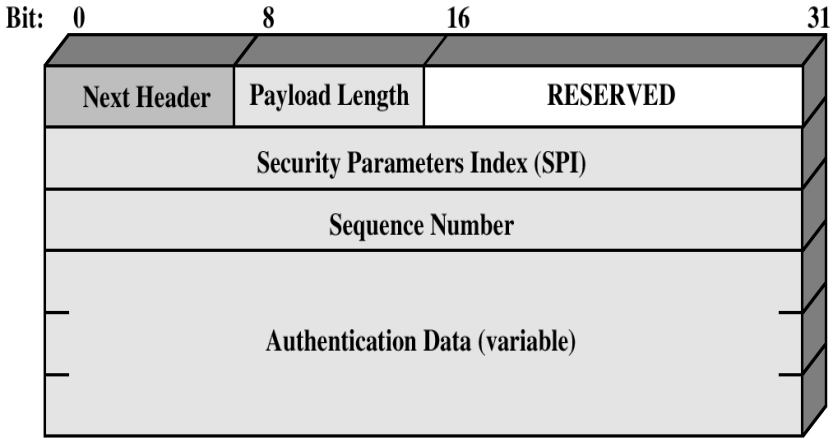
replay attacks, address spoofing etc., which can be fatal

- **Access Control**:- The cryptographic keys are distributed and the traffic flow is controlled in both AH and ESP protocols, which is done to accomplish access control over the data transmission.
- **Confidentiality**:- Confidentiality on the data packet is obtained by using an encryption technique in which all the data packets are transformed into cipher-text packets which are unreadable and difficult to understand.
- **Limited Traffic Flow Confidentiality**:- This facility or service provided by IPSec ensures that the confidentiality is maintained on the number of packets transferred or received. This can be done using padding in ESP.
- **Replay packets Rejection**:- The duplicate or replay packets are identified and discarded using the sequence number field in both AH and ESP.

Q.5 Explain the term Authentication Header.
Ans.

1. The Authentication Header provides support for data integrity and authentication of IP packets.
2. The data integrity feature ensures that undetected modification to a packet's content in transit is not possible.
3. The authentication feature enables an end system or network device to authenticate the user or application and filter traffic accordingly; it also prevents the address spoofing attacks observed in today's Internet.

The Authentication Header consists of the following fields:



IPSec Authentication Header

1. **Next Header (8 bits):** Identifies the type of header immediately following this header.
2. **Payload Length (8 bits):** Length of Authentication Header in 32-bit words, minus 2. For example, the default length of the authentication data field is 96 bits, or three

32-bit words. With a three-word fixed header, there are a total of six words in the header, and the Payload Length field has a value of 4.

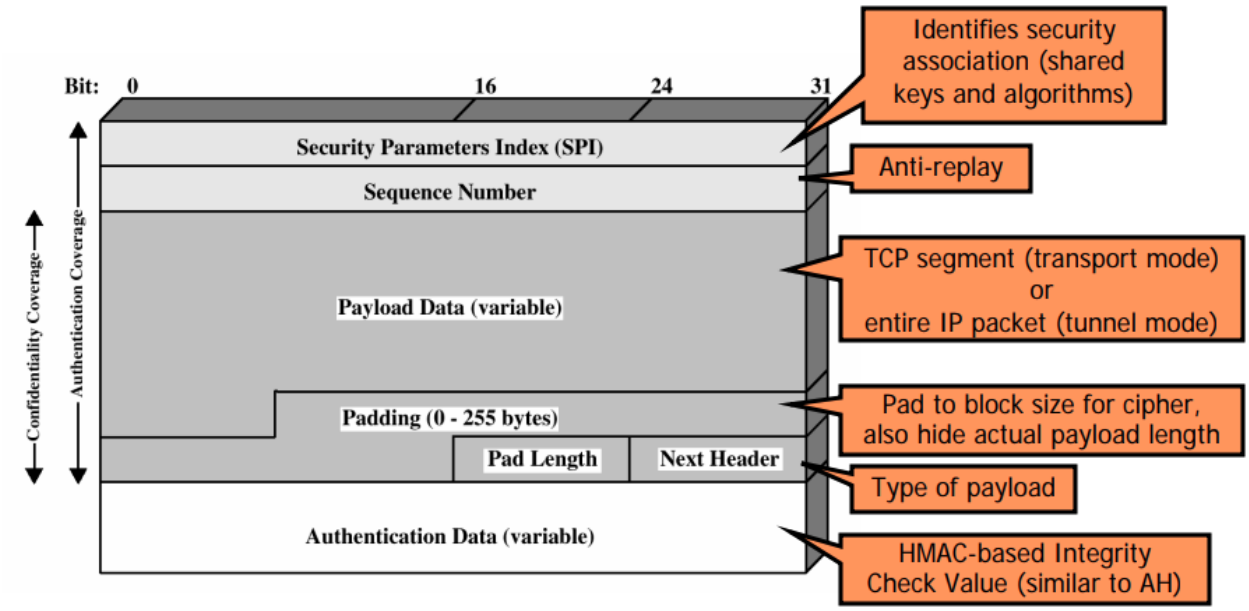
3. **Reserved (16 bits):** For future use.
4. **Security Parameters Index (32 bits):** Identifies a security association.
5. **Sequence Number (32 bits):** A monotonically increasing counter value, discussed later.
6. **Authentication Data (variable):** A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value (ICV), or MAC, for this packet.

Q.6 Explain the concept of Encapsulation security payload.

Ans.The Encapsulating Security Payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality. As an optional feature, ESP can also provide an authentication service.

ESP Format

The following figure shows the format of an ESP packet. It contains the following fields:



1. **Security Parameters Index** (32 bits): Identifies a security association.
2. **Sequence Number** (32 bits): A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH.
3. **Payload Data (variable):** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
4. **Padding (0-255 bytes):** This field is used to make the length of the plaintext to be

a multiple of some desired number of bytes. It is also added to provide confidentiality.

5. **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field.
6. **Next Header (8 bits):** Identifies the type of data contained in the payload data field by identifying the first header in that payload (for example, an extension header in IPv6, or an upper-layer protocol such as TCP).
7. **Authentication Data (variable):** A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field.

Q.7 Explain the concept of key management?

Ans. The key management portion of IPSec involves the determination and distribution of secret keys. The IPSec Architecture document mandates support for two types of key management:

1. **Manual:** A system administrator manually configures each system with its own keys and with the keys of other communicating systems. This is practical for small, relatively static environments.

2. **Automated:** An automated system enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration.

Q.8 Explain SET (Secure Electronic transaction) in detail.

Ans. SET (Secure Electronic Transaction):

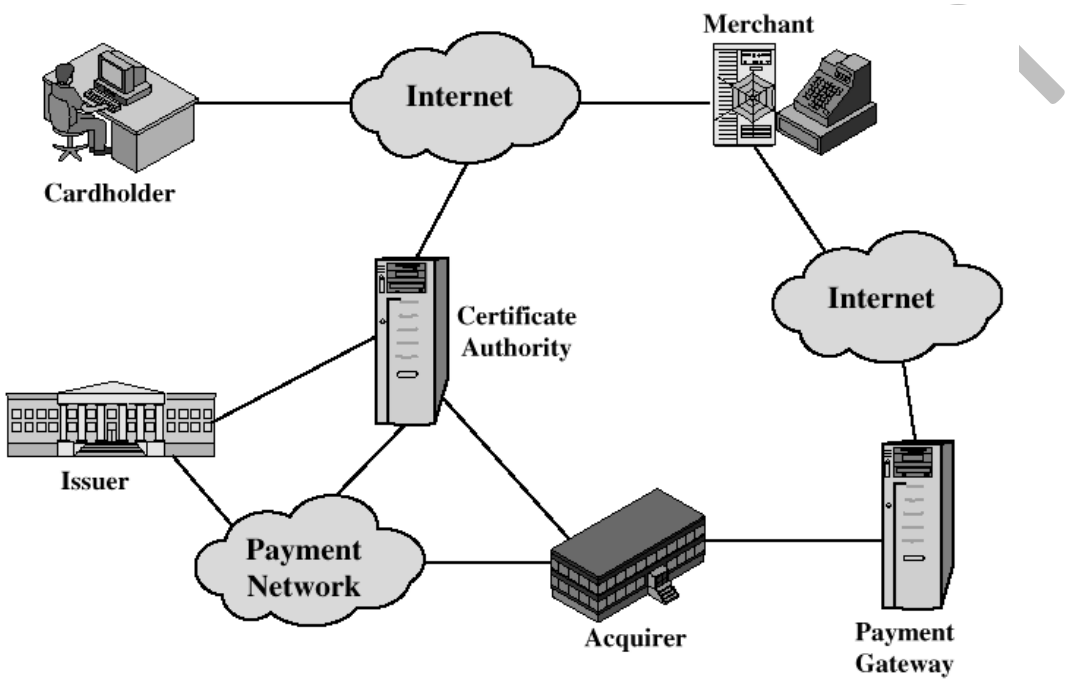
SET is an open encryption and security specification designed to protect credit card transactions on the Internet. SET is not itself a payment system. Rather it is a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network, such as the Internet, in a secure fashion. In essence, SET provides three services:

- Provides a secure communications channel among all parties involved in a transaction.
- Provides trust by the use of X.509v3 digital certificates
- Ensures privacy because the information is only available to parties in a transaction when and where necessary

Requirements:

1. Provide confidentiality of payment and ordering information.
2. Ensure the integrity of all transmitted data
3. Provide authentication that a cardholder is a legitimate user of a credit card account.

4. Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution.
5. Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction
6. Create a protocol that neither depends on transport security mechanisms nor prevents their use.
7. Facilitate and encourage interoperability among software and network providers

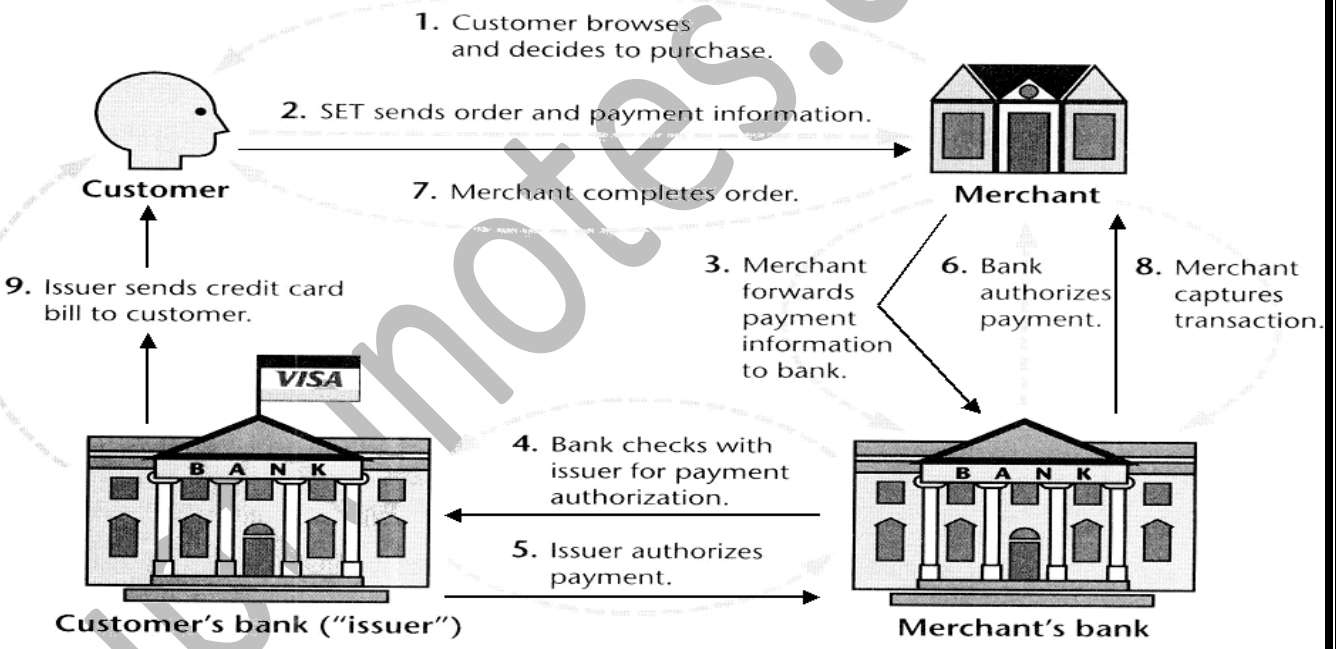


SET Participants

1. Cardholder: purchasers interact with merchants from personal computers over the Internet
2. Merchant: a person or organization that has goods or services to sell to the cardholder
3. Issuer: a financial institution, such as a bank, that provides the cardholder with the payment card.
4. Acquirer: a financial institution that establishes an account with a merchant and processes payment card authorizations and payments
5. Payment gateway: a function operated by the acquirer or a designated third party that processes merchant payment messages
6. Certification authority (CA): an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways

Key Features of SET:

- **Confidentiality of information:** Cardholder account and payment information is secured as it travels across the network. Conventional encryption by DES is used to provide confidentiality.
- **Integrity of data:** payment information sent from cardholders to merchants includes order information, personal data, and payment instructions. SET guarantees that these message contents are not altered in transit. RSA digital signatures, using SHA-1 hash codes, provide message integrity. Certain messages are also protected by HMAC using SHA-1.
- **Cardholder account authentication:** SET enables merchants to verify that a cardholder is a legitimate user of a valid card account number. SET uses X.509v3 digital certificates with RSA signatures for this purpose.
- **Merchant authentication:** SET enables cardholders to verify that a merchant has a relationship with a financial institution allowing it to accept payment cards. SET uses X.509v3 digital certificates with RSA signatures for this purpose.



Q.9 Define SSL(Secure Socet Layer).

Ans. SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser.

- This link ensures that all data passed between the web server and browsers remain private and integral.

- SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

- To be able to create an SSL connection a web server requires an SSL Certificate. When you choose to activate SSL on your web server you will be prompted to complete a number of questions about the identity of your website and your company. Your web server then creates two cryptographic keys - a Private Key and a Public Key.

- The complexities of the SSL protocol remain invisible to your customers. Instead their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session - the lock icon in the lower right-hand corner, clicking on the lock icon displays your SSL

Typically an SSL Certificate will contain your domain name, your company name, your address, your city, your state and your country. It will also contain the expiration date of the Certificate and details of the Certification

- Authority responsible for the issuance of the Certificate.
- When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user letting them know that the site is not secured by SSL.

Q.10 What are intruders?

Ans. There are two most publicized threats to security. Those are **intruders** & **Viruses.**

- Intruders are the attacker who attempt to breach (break) the security of Network.
- Intruders generally referred to as a hacker or cracker.
- They attack the network in order to get unauthorized access.

Intruders are 3 types:

1. **Masque reader:** Is an external user who is not authorized to use a computer, and yet tries to gain privileges (powers) to access a legitimate user's account.
   Masque reader Is generally done either using stolen Id's and passwords, or through by passing authentication mechanisms.

2. **Misfeasor:-** Is a legitimate user who either accesses some applications or data without sufficient privileges to access them or has privileges to access them but misuse these privileges.

3. **Clandestine user**: Is either an internal or external user, who gains administrative control of the system or uses this control to evade (avoid) access control and auditing information.

Q.11 Write a short note on Trojan Horse.

Ans. Trojan horse is a useful, or apparently useful program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function.

Trojan horse programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.

Example: To gain access to the files of another user on a shared system, a user could create a Trojan horse program that, when executed changed the invoking user's file permissions so that the files are readable by any user

Q.12 Explain the term virus.

Ans. Virus is a Malware that, when executed, tries to replicate itself into other executable code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.

This ability to replicate, can affect your computer without your permission and without your knowledge

Q.13 Write a short note on worms.

Ans. Worm is a computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network.

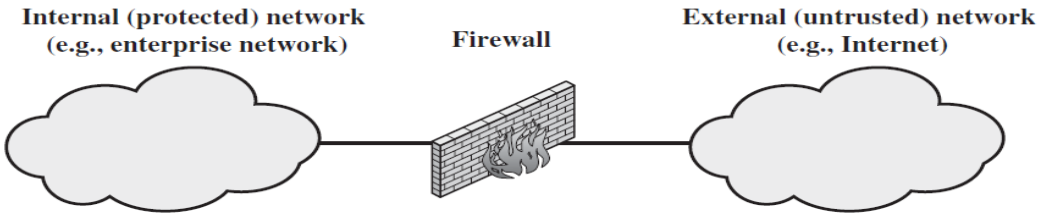
A worm (or worm) is a particular type of virus that can replicate through terminals connected to a network, then to perform certain actions which would impair the integrity of operating systems.

Q.14 Explain the term firewall in detail.

Ans. Firewall is software or hardware based network security system that controls the incoming and outgoing network traffic, based on applied rule set.

- A fire wall establishes a barrier between a trusted secure internal network and another network.

- Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet.



THE NEED FOR FIREWALLS

- Centralized data processing system, with a central mainframe supporting a number of directly connected terminals
- Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe
- Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two
- Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN)
- Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN

FIREWALL CHARACTERISTICS

The following design goals for a firewall:

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible available in fire wall.

2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this chapter.

3. The firewall itself is immune to penetration.

Firewall controls:
Firewalls use to control access and enforce the site's security policy. Originally, firewalls focused primarily on service control, but they have since evolved to provide all four:

1. **Service control:** Determines the types of Internet services that can be accessed, inbound or outbound.

2. **Direction control**: Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

3. **User control:** Controls access to a service according to which user is attempting to access it.

4. **Behavior control:** Controls how particular services are used.

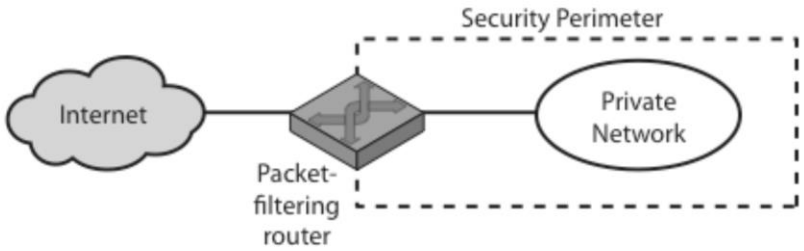
Q.15 Explain different type of firewall.

Ans. TYPES OF FIREWALLS:

a) Packet Filtering Firewall
b) Application Level Gateway
c) Circuit Level Gateway

a). Packet Filtering Firewall:

Packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet .The firewall is typically configured to filter packets going in both directions (from and to the internal network).

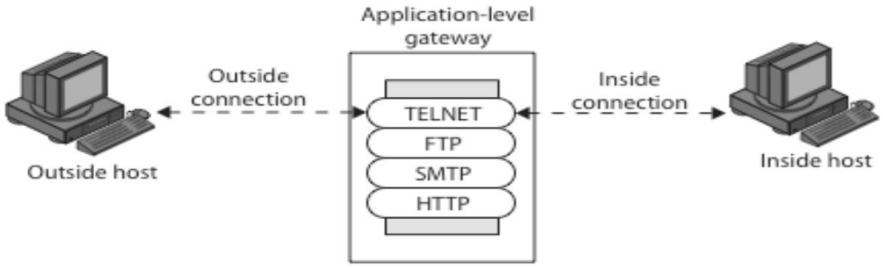


(a) Packet-filtering router

b). Application Level Gateway (or Proxy)

Application Level gateway have application specific gateway / proxy .It has full access to Protocol

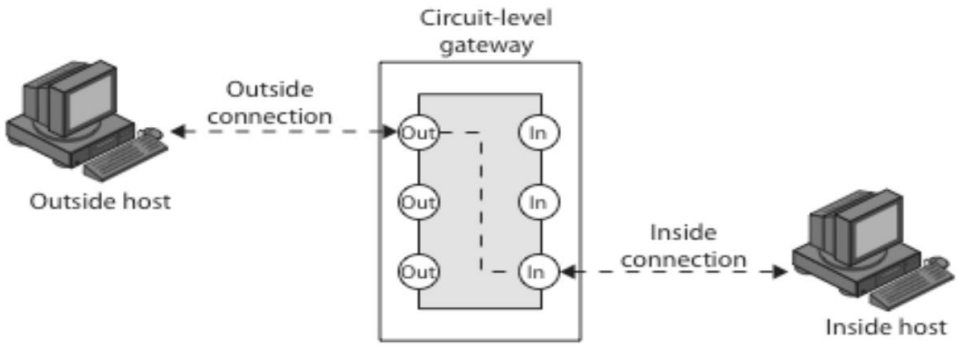
- User requests service from proxy
- Proxy validates request as legal
- Then actions request and returns result to user
- Can log / audit traffic at application level.



(b) Application-level gateway

c).Circuit Level Gateway:

- It is a stand a-lone system or it can be a specialized function performed by an application level gate way for certain applications.
- It does not permit end to end TCP connection; this relays two TCP connections, one between itself and a TCP user on an inner host, and one between itself and TCP user on outside host.
- Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the content.



(c) Circuit-level gateway

Q.16 List the difference between transparent mode and tunnel mode.

Ans. Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.
Tunnel mode protects the internal routing information by encrypting the IP header of the original packet. The original packet is encapsulated by another set of IP headers.

Transport mode is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host—for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination. The transport mode encrypts only the payload and ESP trailer; so the IP header of the original packet is not encrypted.

	Transport Mode SA	Tunnel Mode SA
AH	**Authenticates** IP payload and selected portions of IP header and IPv6 extension headers	**Authenticates** entire inner IP packet plus selected portions of outer IP header
ESP	**Encrypts** IP payload and any IPv6 extension header	**Encrypts** inner IP packet
ESP with authentication	**Encrypts** IP payload and any IPv6 extension header. **Authenticates** IP payload but no IP header	**Encrypts** inner IP packet. **Authenticates** inner IP packet.

IP sec can be used (both AH packets and ESP packets) in two modes

- **Transport mode:** the IP sec header is inserted just after the IP header –this contains the security information, such as SA identifier, encryption, authentication

1. Typically used in end-to-end communication
2. IP header not protected

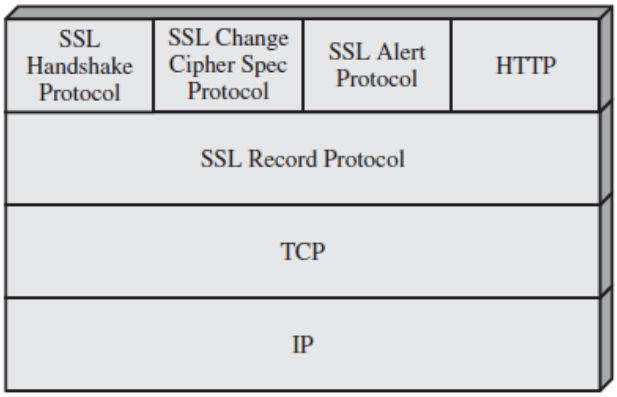
- **Tunnel mode:** the entire IP packet, header and all, is encapsulated in the body of a new IP packet with a completely new IP header.

1. Typically used in firewall-to-firewall communication
2. Provides protection for the whole IP packet
3. No routers along the way will be able (and will not need) to check the content of the packets

Q.17 What is the difference between SSL connection and SSL session? Discuss SSL protocol architecture.

Ans. SSL Architecture:

SSL is designed to make use of TCP to provide a reliable end-to-end secure service. SSL is not a single protocol but rather two layers of protocols, as illustrated in the fig.



SSL Protocol Stack

Two important SSL concepts are the SSL session and the SSL connection, which are defined in the specification as follows.

1. **Connection:** A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session.

2. **Session:** An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

A session state is defined by the following parameters.

1. **Session identifier:** An arbitrary byte sequence chosen by the server to identify an active or resumable session state.
2. **Peer certificate:** An X509.v3 certificate of the peer. This element of the state may be null.
3. **Compression method:** The algorithm used to compress data prior to encryption.
4. **Cipher spec:** Specifies the bulk data encryption algorithm (such as null,AES, etc.) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as the hash_size.
5. **Master secret:** 48-byte secret shared between the client and server.
6. **Is resumable:** A flag indicating whether the session can be used to initiate new connections.

A connection state is defined by the following parameters

1. **Server and client random**: Byte sequences that are chosen by the server and client for each connection.
2. **Server write MAC secret:** The secret key used in MAC operations on data sent by the server.
3. **Client write MAC secret:** The secret key used in MAC operations on data sent by the client.
4. **Server write key:** The secret encryption key for data encrypted by the server and decrypted by the client.
5. **Client write key**: The symmetric encryption key for data encrypted by the client and decrypted by the server.
6. **Initialization vectors:** When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL Handshake Protocol. Thereafter, the final cipher-text block from each record is preserved for use as the IV with the following record.

Q.18 Write a note on Intrusion Detection?

Ans. To prevent intruders form getting unauthorized access to the system, intrusion prevention & intrusion detection can be used.

- Intrusion prevention is a process that involves detecting the signs of intrusion and attempting to stoop the intrusion efforts.
- Intrusion detection is a process that involves monitoring the actions occurring on the network or in computer system.
- Is not possible to completely prevent the efforts of intruders, find their way into the secured system.
- In information security, intruder detection is the art of detecting intruders behind attacks as unique persons. This technique tries to identify the person behind an attack by analyzing their computational behaviour.

There are generally two approaches for intrusion detection:

1. Statistical anomaly detection
2. Rule based Detection

Statistical anomaly detection: Involves the collection of data relating to the behavior of legitimate users over a period of time.

Statistical anomaly detection techniques fall into two broad categories:

1. Threshold detection and

2. Profile-based systems.

Rule-based detection: Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder. Means this detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious

Q.19 What is the difference between virus and firewall.

Ans.

BASIS FOR COMPARISON	FIREWALL	ANTIVIRUS
Implemented in	Both hardware and software	Software only
Operations performed	Monitoring and Filtering (Specifically IP filtering)	Scanning of infected files and software.
Deals with	External threats	Internal as well as external threats.
Inspection of attack is based on	Incoming packets	Malicious software residing on a computer
Counter attacks	IP spoofing and routing attacks	No counter attacks are possible once a malware has removed

Q.20 Explain the definition, phases, and types of virus and structures of viruses?

Ans. Virus is a Malware that, when executed, tries to replicate itself into other executable code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.

This ability to replicate, can affect your computer without your permission and without your knowledge

Types of Virus:

1. **Parasitic virus:** Traditional and common virus. This will be attached with EXE files and search for other EXE file to infect them.
2. **Memory Resident Virus**: Present in your system memory as a system program. From here onwards it will infects all program that executes.
3. **Boot Sector Virus:** Infects the boot record and spread when the system is booted from the disk containing the virus.
4. **Stealth Virus**: This virus hides itself from detection of antivirus scanning.

Phases of Virus:

1. **Dormant phase:**The virus is idle. The virus will eventually be activated by some event, such as a date, presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.

2. **Propagation stage:**The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.

3. **Triggering phase**:The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.

4. **Execution phase**:The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

Q.21 Compare the Virus , Worm and Trojan Horse

Ans.

	Virus	**Worm**	**Trojan Horse**
Meaning	A computer program that connects itself to another legitimate program to cause harm to the computer system or the network.	It eats resources of a system to bring it down rather than performing destructive actions.	It permits an intruder to obtain some confidential information about a computer network.
Execution	Depends on the transfer of a file.	Replicates itself without any human action.	Downloaded as software and executed.
Replication occurs	Yes	Yes	No

Remotely controlled	No	Yes	Yes
Rate of spreading	Moderate	Faster	Slow
Infection	Initiates by attaching a virus to an executable file.	Utilizes system or application weaknesses.	Attaches itself to a program and interpret as useful software.
Purpose	Modification of the information.	Halt the CPU and memory.	Steals the user's information.