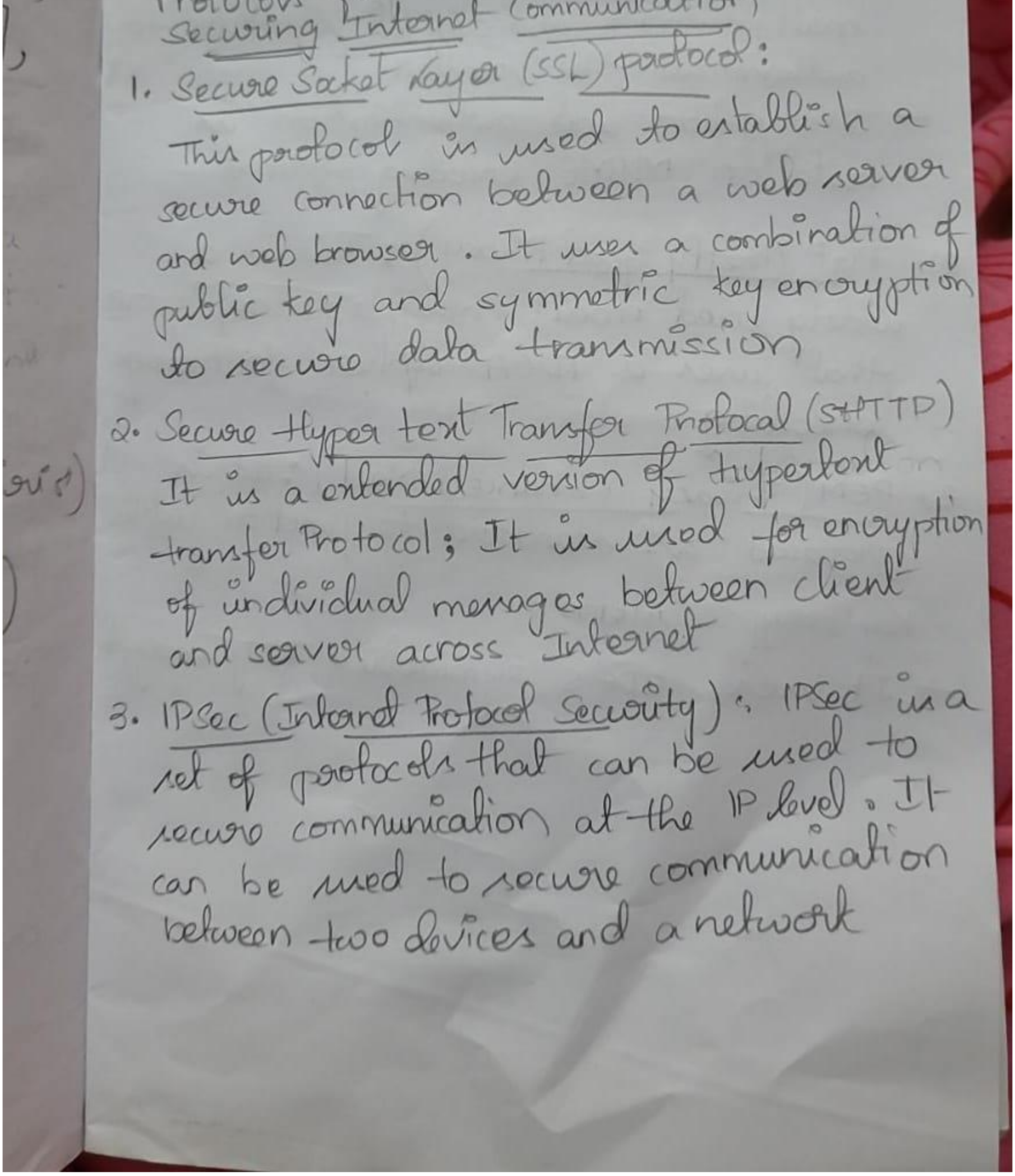
1. Explain different protocols used for secure communication?

Ans



LAQ's

5. Explain different protocols used for secure communication

Protocols for Secure Communication

Securing Internet Communication

1. Secure Socket Layer (SSL) protocol:

This protocol is used to establish a secure connection between a web server and web browser. It uses a combination of public key and symmetric key encryption to secure data transmission

2. Secure Hyper text Transfer Protocal (SHTTP)

It is a extended version of hypertext transfer Protocol; It is used for encryption of individual messages between client and server across Internet

3. IPSec (Internet Protocol Security): IPSec is a set of protocols that can be used to secure communication at the IP level. It can be used to secure communication between two devices and a network

Securing e-mail

1. S/MIME (Secure/Multi purpose Internet Mail Extentions)

→ S/MIME is a standard for secure email communication

→ It uses public key encryption to secure mail messages and digital signature to authenticate the sender

→ Encryption and authentication is build on MIME encoding format

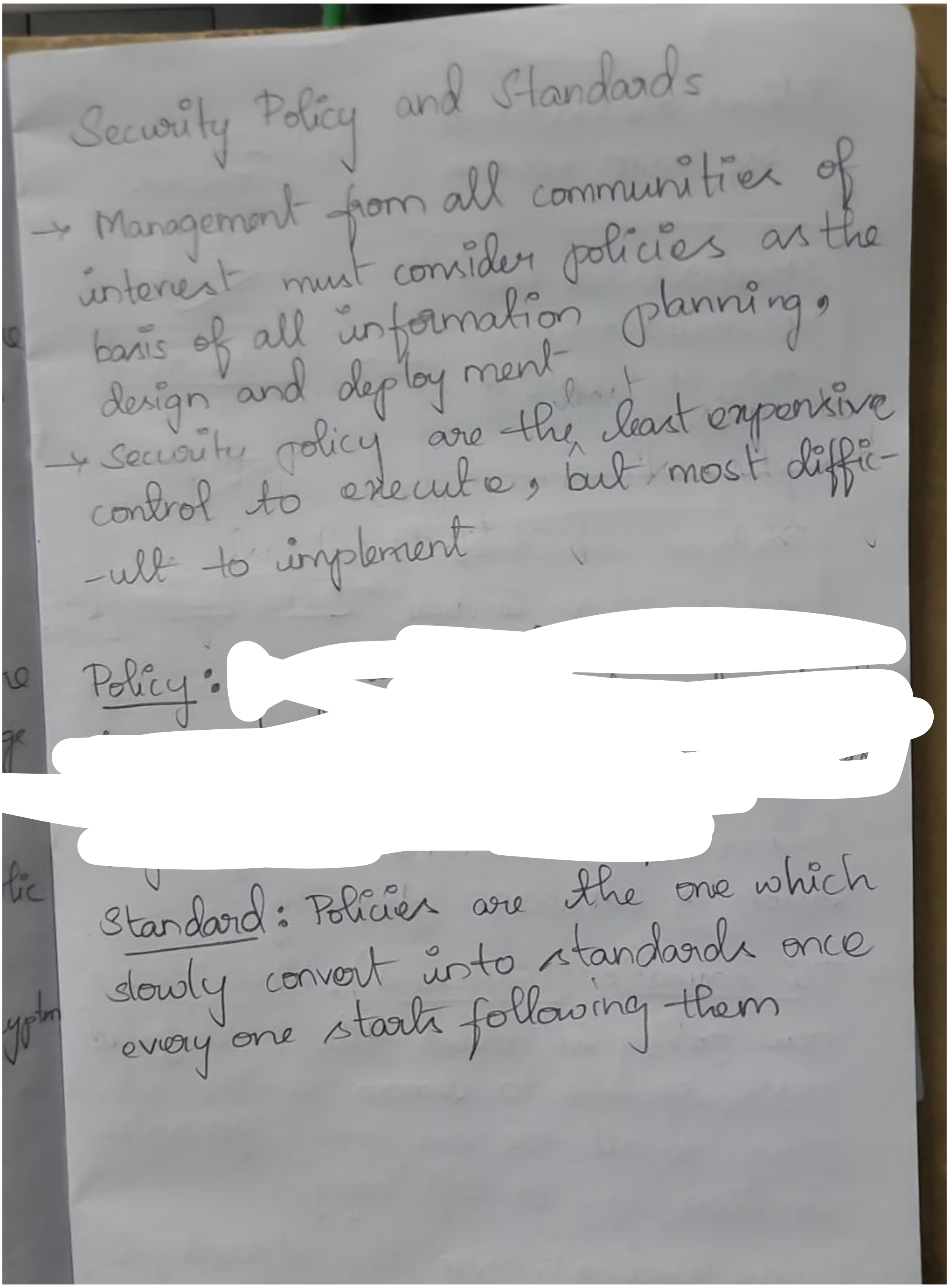
2. PGP (Pretty Good Privacy) : This is a widely used email encryption software that uses a IDEA cipher for message encoding

3. PEM (Privacy Enhanced Mail) : It is proposed as standard to function public Key cryptosystems :

→ It uses 3DES symmetric key encryption

2) Explain security policies and standards.

Ans)



Security Policy and Standards

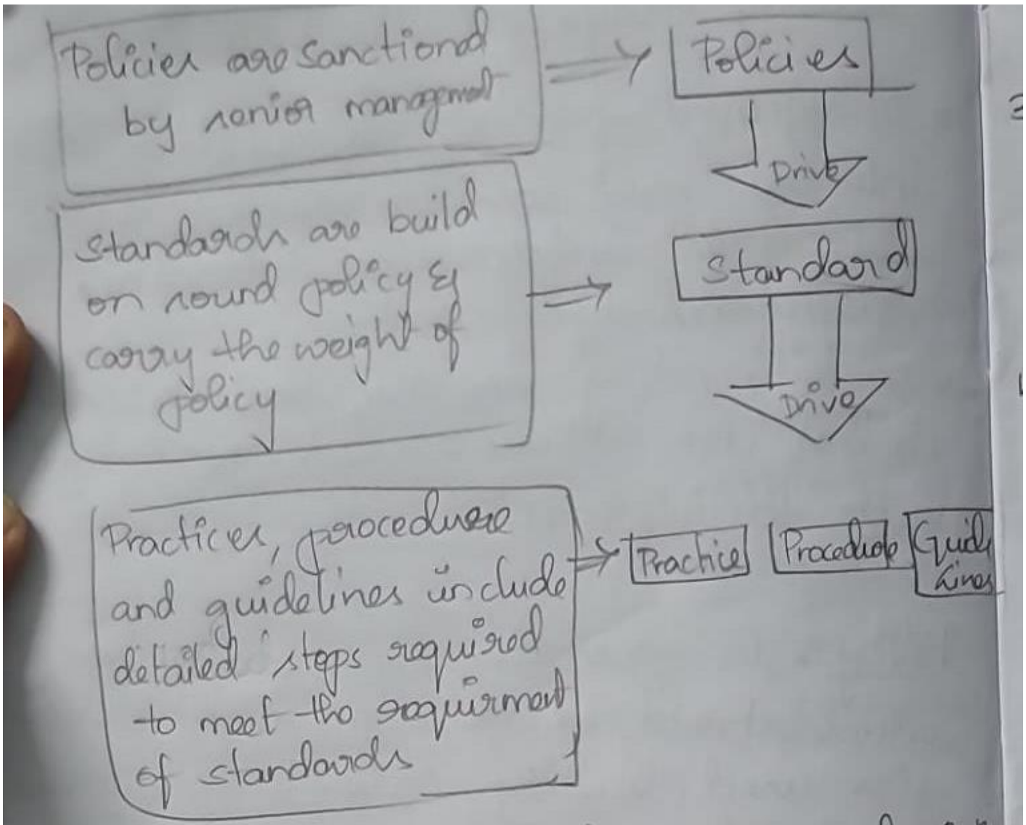
→ Management from all communities of interest must consider policies as the basis of all information planning, design and deployment

→ Security policy are the least expensive control to execute, but most difficult to implement

Policy: [redacted]

Standard: Policies are the one which slowly convert into standards once every one starts following them

A security policy (also called an information security policy or IT security policy) is a document that spells out the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data



Policies are sanctiond by senior management

Standards are build on sound policy & carry the weight of policy

Practices, procedure and guidelines include detailed steps required to meet the requirment of standards

→ Policies are prepared to support mission vision & stratergic planning

1. Dissemination (Distributed): When ever a new policy is added the organization must be able to demonstrate the relevant policy to all the employees for review in hard copy or soft copy

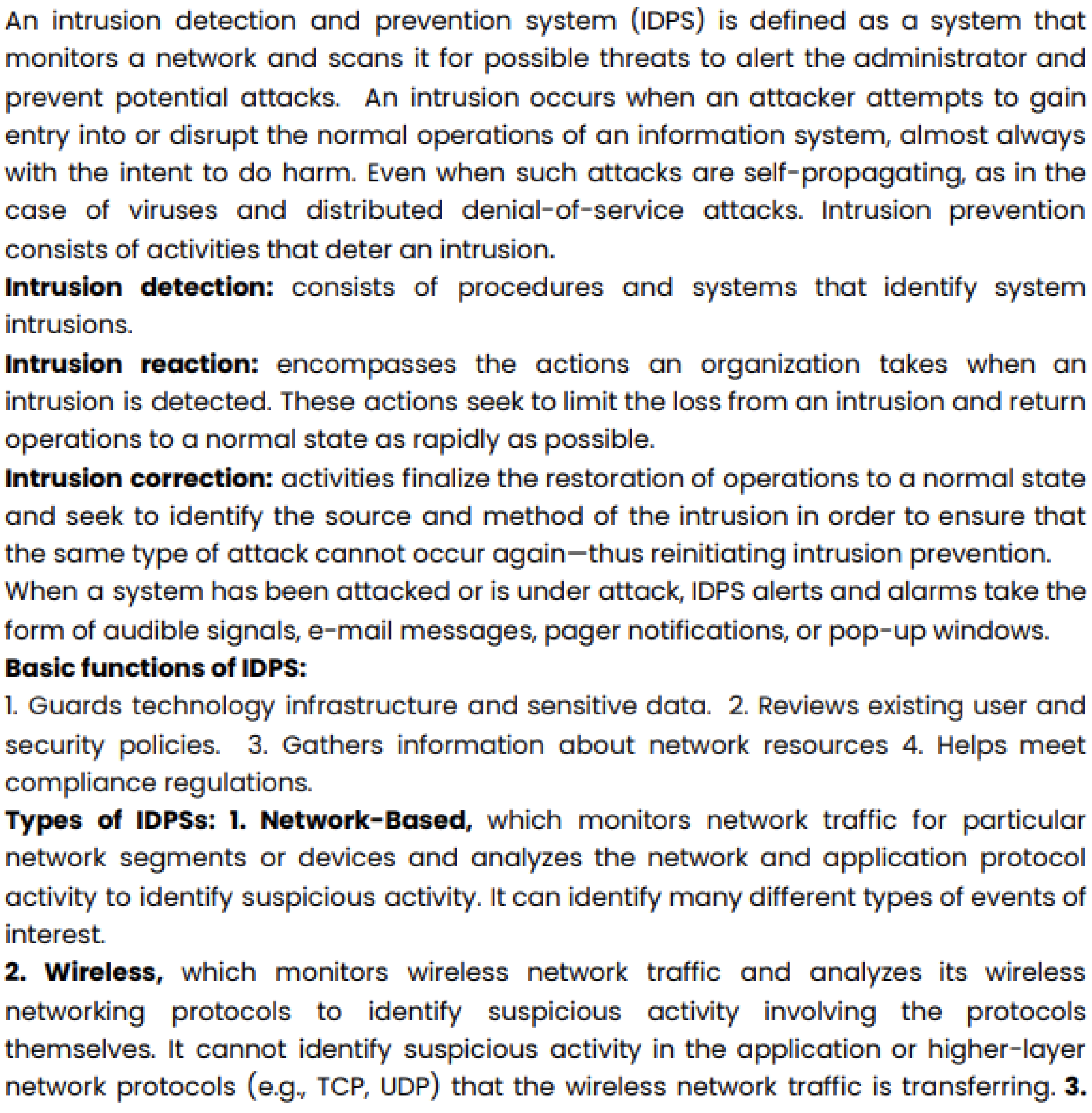
2. Review (Reading): Even the shared policy or rule should be in multiple format like audio, text, symbols. So that everyone can understand it

3. Comprehension: The policy should be understandable so that every employee can understand requirements and contents of the policy

4. Compliance (aggrement): For some policies even agremnents can be given

5. Uniform enforcement: Organization must

3) Explain in detail about information detection and prevention system.
Ans)



An intrusion detection and prevention system (IDPS) is defined as a system that monitors a network and scans it for possible threats to alert the administrator and prevent potential attacks. An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an information system, almost always with the intent to do harm. Even when such attacks are self-propagating, as in the case of viruses and distributed denial-of-service attacks. Intrusion prevention consists of activities that deter an intrusion.

Intrusion detection: consists of procedures and systems that identify system intrusions.

Intrusion reaction: encompasses the actions an organization takes when an intrusion is detected. These actions seek to limit the loss from an intrusion and return operations to a normal state as rapidly as possible.

Intrusion correction: activities finalize the restoration of operations to a normal state and seek to identify the source and method of the intrusion in order to ensure that the same type of attack cannot occur again—thus reinitiating intrusion prevention.

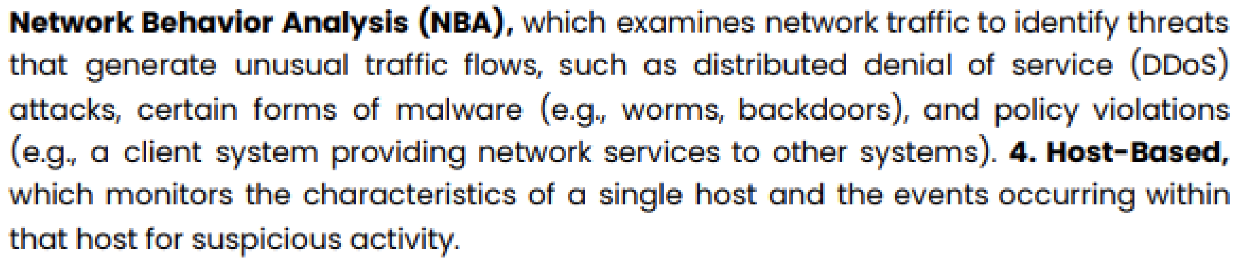
When a system has been attacked or is under attack, IDPS alerts and alarms take the form of audible signals, e-mail messages, pager notifications, or pop-up windows.

Basic functions of IDPS:

1. Guards technology infrastructure and sensitive data. 2. Reviews existing user and security policies. 3. Gathers information about network resources 4. Helps meet compliance regulations.

Types of IDPSs: 1. Network-Based, which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest.

2. Wireless, which monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves. It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring. **3.**

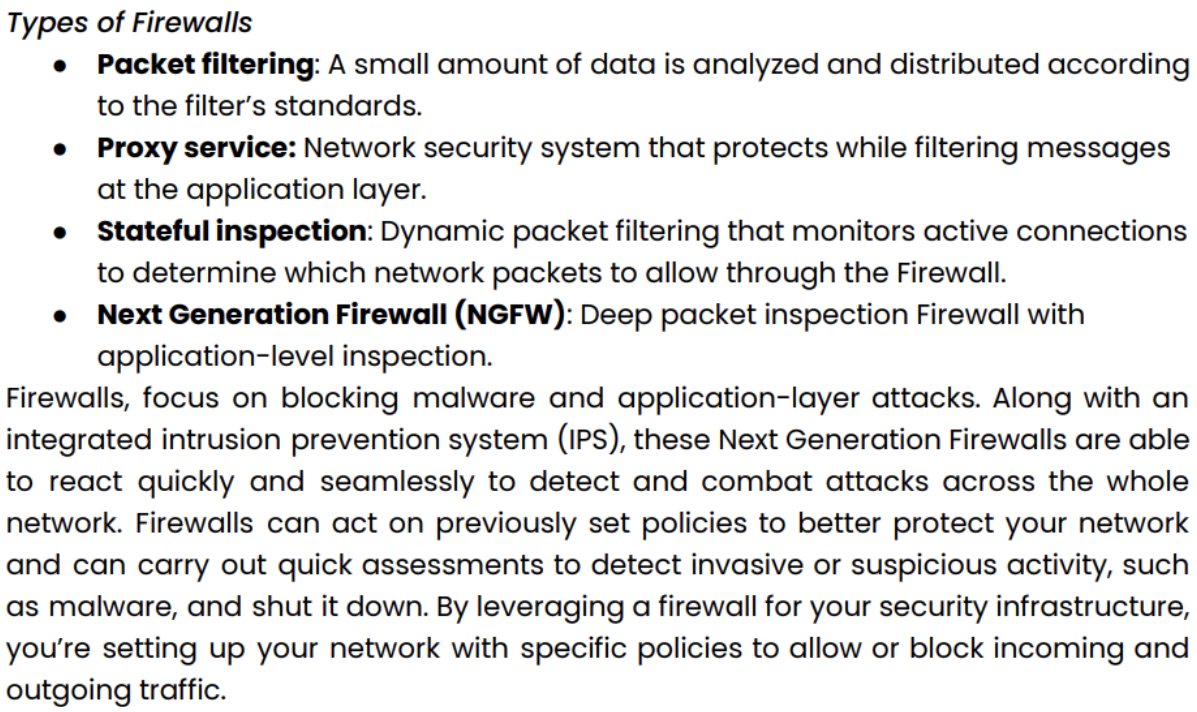


Network Behavior Analysis (NBA), which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems). **4. Host-Based,** which monitors the characteristics of a single host and the events occurring within that host for suspicious activity.

4) Explain firewalls and VPNs in detail.

Ans)

A **firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules and policies. It can be hardware-based, such as a physical firewall appliance, or software-based, like firewall software installed on a server. Firewalls are designed to block unauthorized access while allowing authorized communication, and they can be configured to allow or block specific types of traffic based on IP address, port, and protocol. Some firewalls can also be configured to inspect and filter traffic at the application layer, which enables them to block malicious traffic even if it uses a legitimate protocol or port.



Types of Firewalls

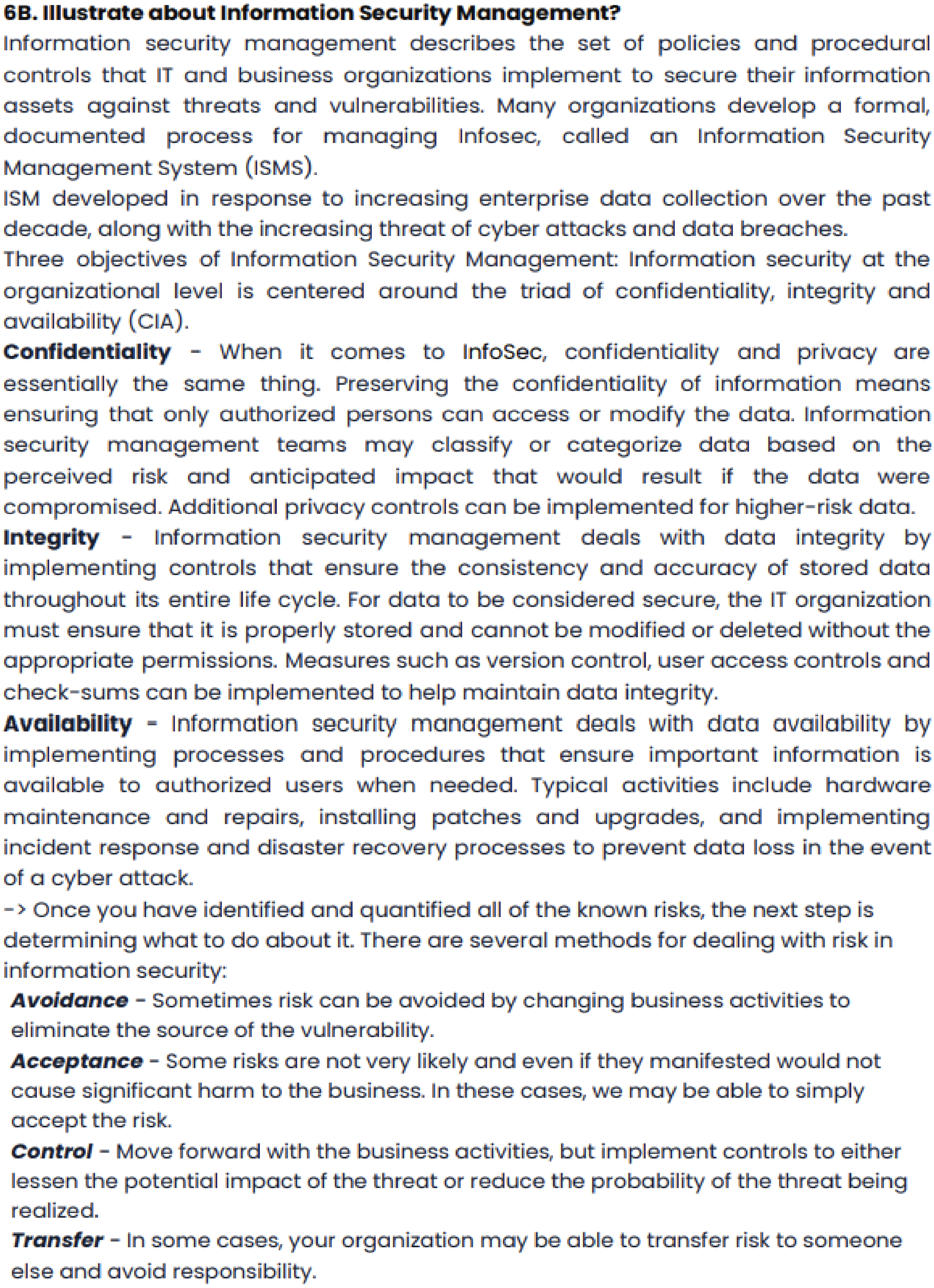
- **Packet filtering**: A small amount of data is analyzed and distributed according to the filter's standards.
- **Proxy service:** Network security system that protects while filtering messages at the application layer.
- **Stateful inspection**: Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.
- **Next Generation Firewall (NGFW)**: Deep packet inspection Firewall with application-level inspection.

Firewalls, focus on blocking malware and application-layer attacks. Along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls are able to react quickly and seamlessly to detect and combat attacks across the whole network. Firewalls can act on previously set policies to better protect your network and can carry out quick assessments to detect invasive or suspicious activity, such as malware, and shut it down. By leveraging a firewall for your security infrastructure, you're setting up your network with specific policies to allow or block incoming and outgoing traffic.

VPN (Virtual Private Network) is a technology that enables users to securely access a private network, such as a company's internal network, from a remote location using the internet. VPNs work by creating a secure, encrypted tunnel between the user's device and the VPN server. This encrypted tunnel protects the data transmitted over the internet from being intercepted by third parties, and it allows the user to access the private network as if they were physically connected to it. VPNs use a variety of protocols such as PPTP, L2TP, IPSec and OpenVPN to establish the secure connection. They can be used to protect the internet activity of individuals, as well as by remote employees to access company resources. VPNs are also commonly used by organisations to connect multiple branch offices together securely over the public internet. Additionally, VPNs can also be used to bypass geo-restriction and censorship to access the internet freely.

5) Explain about Information Security Management?

Ans)



6B. Illustrate about Information Security Management?

Information security management describes the set of policies and procedural controls that IT and business organizations implement to secure their information assets against threats and vulnerabilities. Many organizations develop a formal, documented process for managing Infosec, called an Information Security Management System (ISMS).

ISM developed in response to increasing enterprise data collection over the past decade, along with the increasing threat of cyber attacks and data breaches.

Three objectives of Information Security Management: Information security at the organizational level is centered around the triad of confidentiality, integrity and availability (CIA).

Confidentiality - When it comes to InfoSec, confidentiality and privacy are essentially the same thing. Preserving the confidentiality of information means ensuring that only authorized persons can access or modify the data. Information security management teams may classify or categorize data based on the perceived risk and anticipated impact that would result if the data were compromised. Additional privacy controls can be implemented for higher-risk data.

Integrity - Information security management deals with data integrity by implementing controls that ensure the consistency and accuracy of stored data throughout its entire life cycle. For data to be considered secure, the IT organization must ensure that it is properly stored and cannot be modified or deleted without the appropriate permissions. Measures such as version control, user access controls and check-sums can be implemented to help maintain data integrity.

Availability - Information security management deals with data availability by implementing processes and procedures that ensure important information is available to authorized users when needed. Typical activities include hardware maintenance and repairs, installing patches and upgrades, and implementing incident response and disaster recovery processes to prevent data loss in the event of a cyber attack.

-> Once you have identified and quantified all of the known risks, the next step is determining what to do about it. There are several methods for dealing with risk in information security:

Avoidance - Sometimes risk can be avoided by changing business activities to eliminate the source of the vulnerability.

Acceptance - Some risks are not very likely and even if they manifested would not cause significant harm to the business. In these cases, we may be able to simply accept the risk.

Control - Move forward with the business activities, but implement controls to either lessen the potential impact of the threat or reduce the probability of the threat being realized.

Transfer - In some cases, your organization may be able to transfer risk to someone else and avoid responsibility.

1) List Security Policies.

a) Security Program Policy
b) enterprise information security policy (EISP)
c) Issue-Specific Security Policy (ISSP)
d) Systems-Specific Policy (SysSP)

2) Define IDS

An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal
operations of an information system, almost always with the intent to do harm. Even
when such attacks are self-propagating, as in the case of viruses and distributed
denial-of-service attacks
Intrusion prevention consists of activities that deter an intrusion.

Three activities to summarize:
• **Intrusion detection:** consists of procedures and systems that identify system
intrusions.
• **Intrusion reaction:** encompasses the actions an organization takes when an intrusion is
detected. These actions seek to limit the loss from an intrusion and return operations
to a normal state as rapidly as possible.
• **Intrusion correction:** activities finalize the restoration of operations to a normal state
and seek to identify the source and method of the intrusion in order to ensure that the
same type of attack cannot occur again—thus reinitiating intrusion prevention.

3) List cryptographic tools

a) Public Key Infrastructure (PKI): integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely
b) Digital Signatures: Encrypted messages that can be mathematically proven to be authentic
c) Digital Certificates: Electronic document containing key value and identifying information about entity that controls key

4) Define VPN’s

A VPN provides a secure, encrypted connection between two points. Before setting up the VPN connection, the two endpoints of the connection create a shared encryption key. This can be accomplished by providing a user with a password or using a key sharing algorithm.

VPNs are designed to provide a private, encrypted connection between two points – but does not specify what these points should be. This makes it possible to use VPNs in a few different contexts:

a) Site-to-Site VPN: A site-to-site VPN is designed to securely connect two geographically-distributed sites.

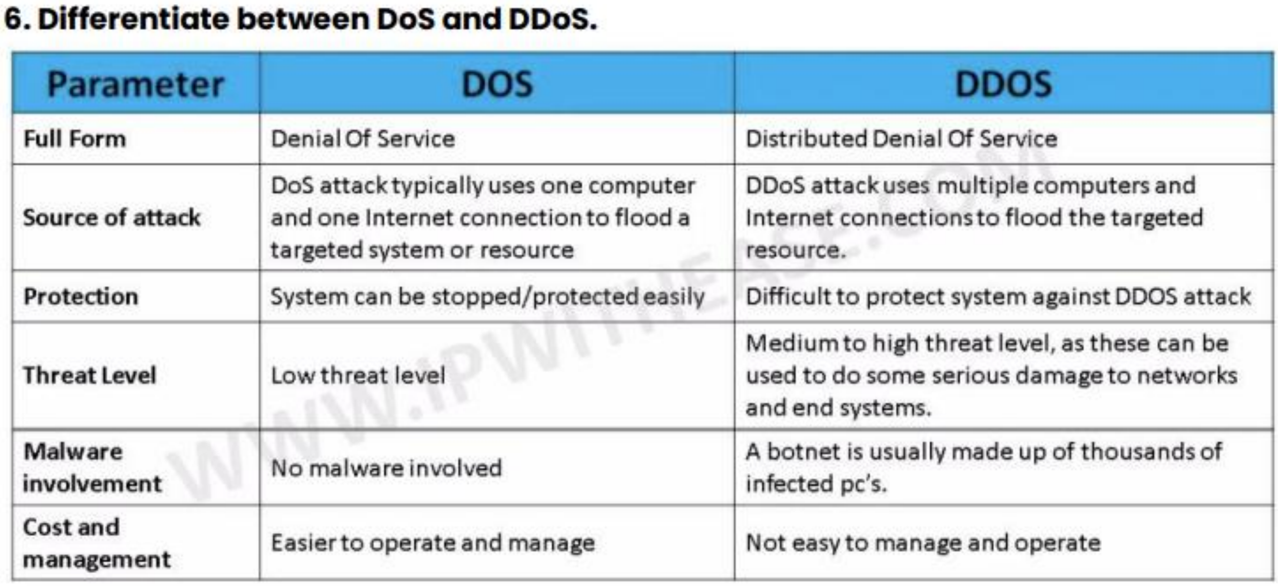
b) Remote Access VPN: A remote access VPN is designed to link remote users securely to a corporate network.

c) VPN as a Service: VPN as a Service or a cloud VPN is a VPN hosted in cloud-based infrastructure where packets from the client enter the Internet from that cloud infrastructure instead of the client’s local address.

5)List Maintenance Models.

Ans)

The five domains of the security maintenance model are **external monitoring, planning and risk assessment, internal monitoring, readiness and review, and vulnerability assessment and remediation**. External monitoring focuses on evaluating external threats to the organization.



6. Differentiate between DoS and DDoS.

Parameter	DOS	DDOS
Full Form	Denial Of Service	Distributed Denial Of Service
Source of attack	DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource	DDoS attack uses multiple computers and Internet connections to flood the targeted resource.
Protection	System can be stopped/protected easily	Difficult to protect system against DDOS attack
Threat Level	Low threat level	Medium to high threat level, as these can be used to do some serious damage to networks and end systems.
Malware involvement	No malware involved	A botnet is usually made up of thousands of infected pc’s.
Cost and management	Easier to operate and manage	Not easy to manage and operate

7. Define firewall.

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out. A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

8. What is information security Blueprint?

-> Basis for design, selection, and implementation of all security policies, education and training programs, and technological controls. -> More detailed version of security framework (outline of overall information security strategy for organization). -> Should specify tasks to be accomplished and the order in which they are to be realized. -> Should also serve as a scalable, upgradeable, and comprehensive plan for information security needs for coming years.