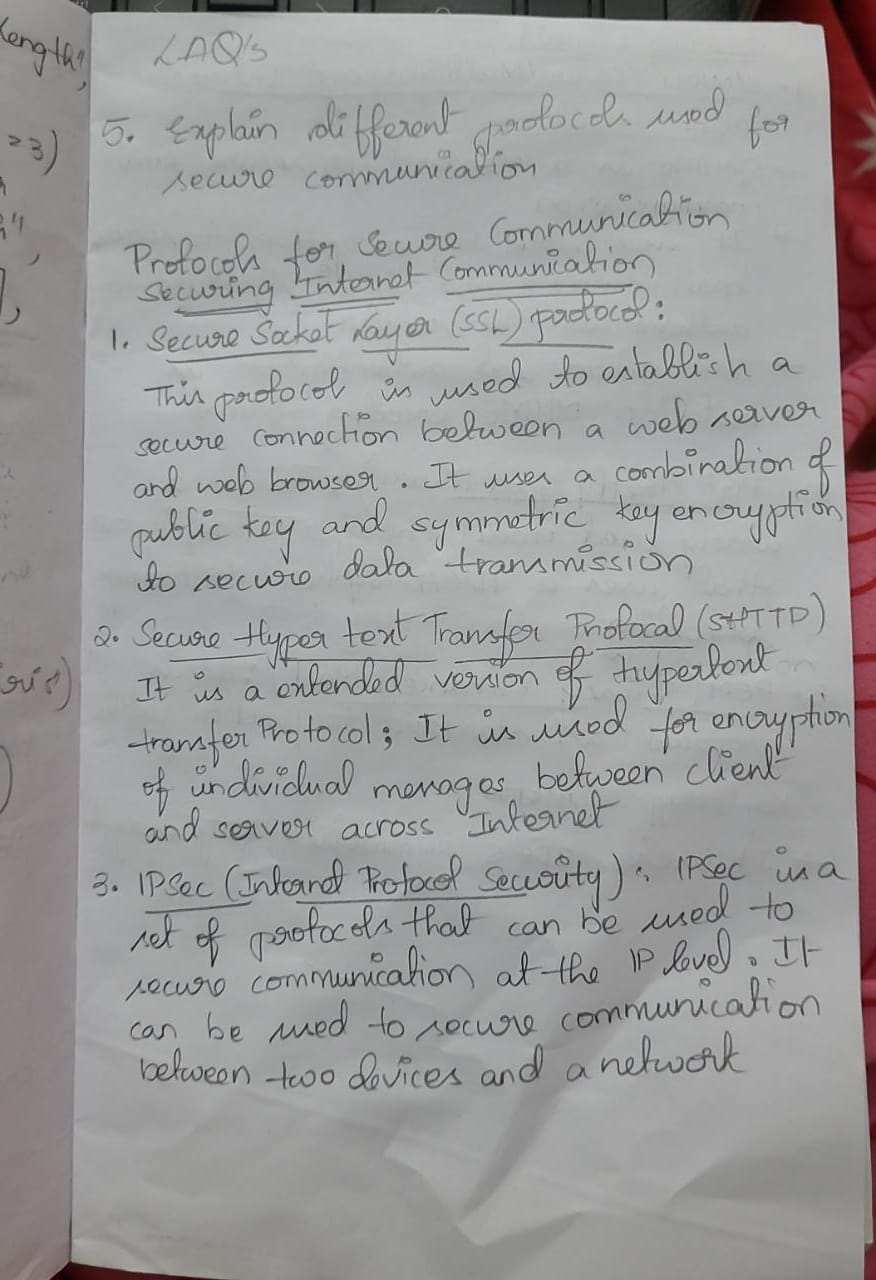
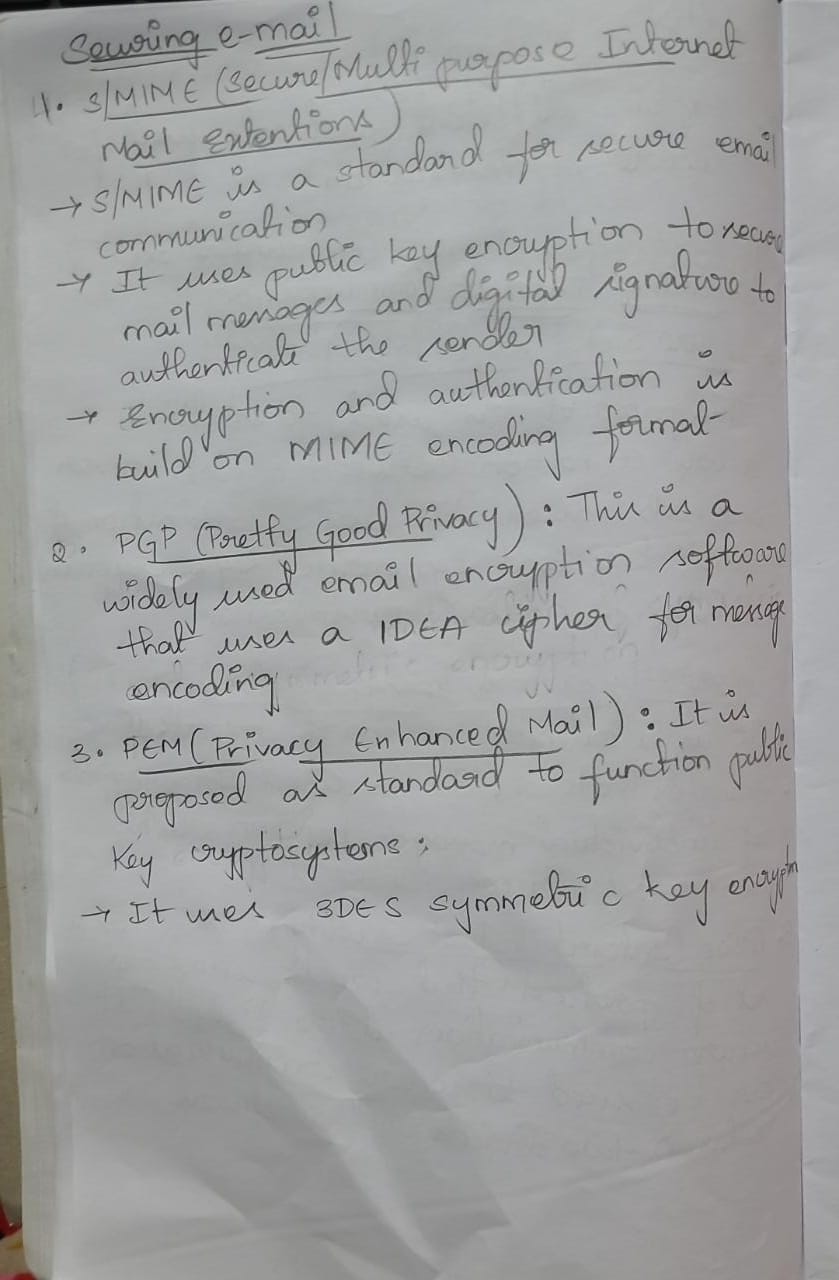
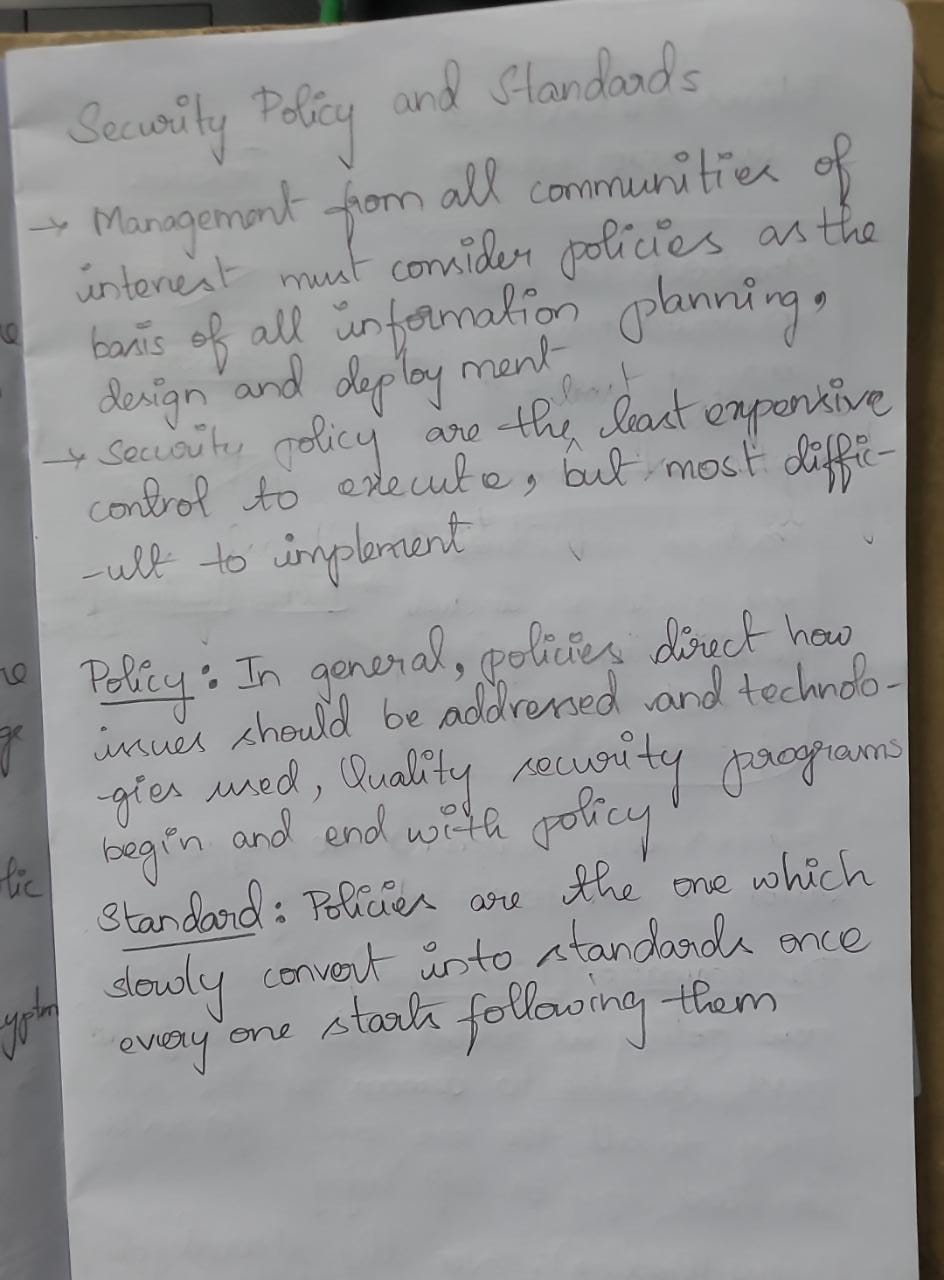
1. Explain different protocols used for secure communication?

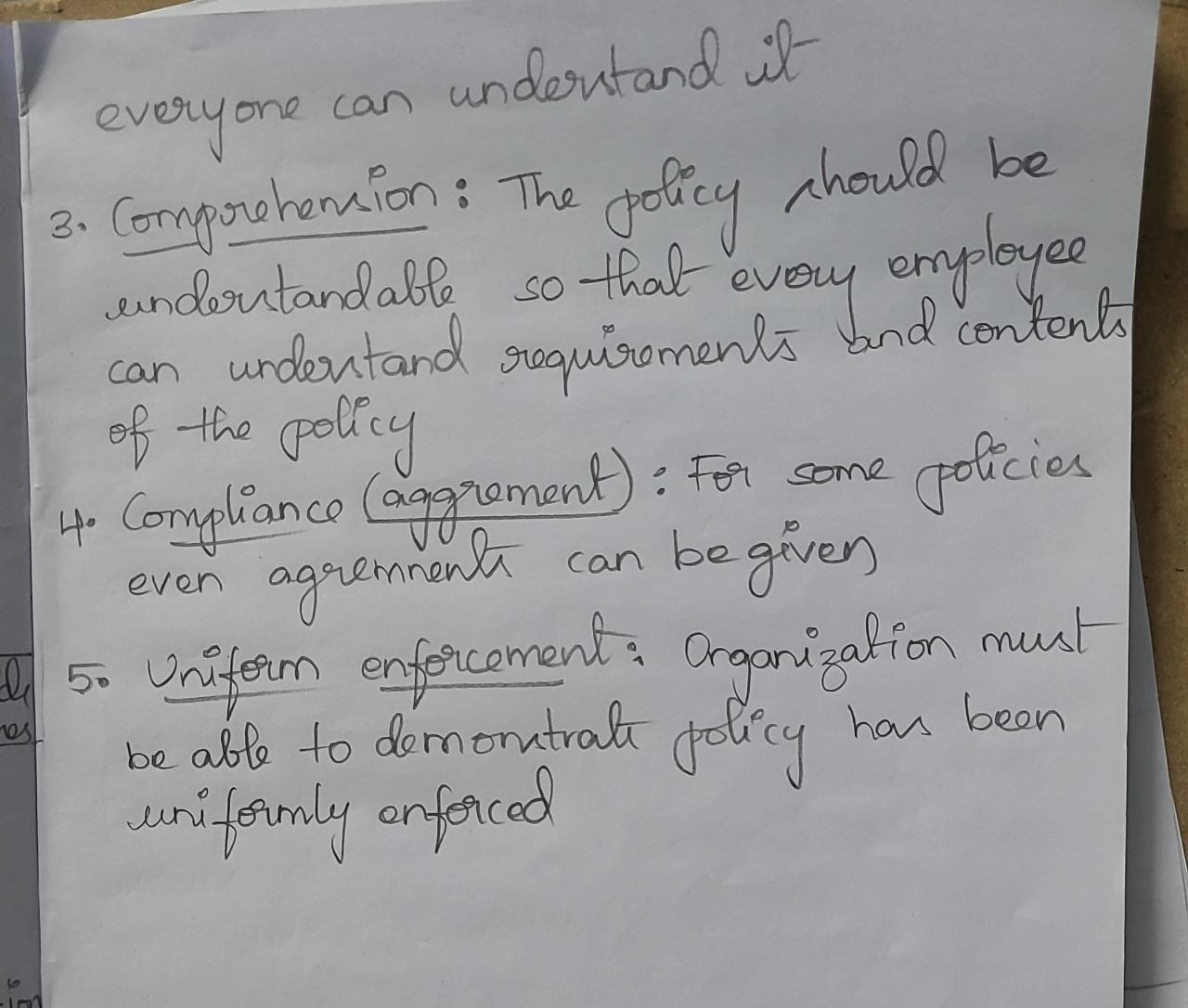
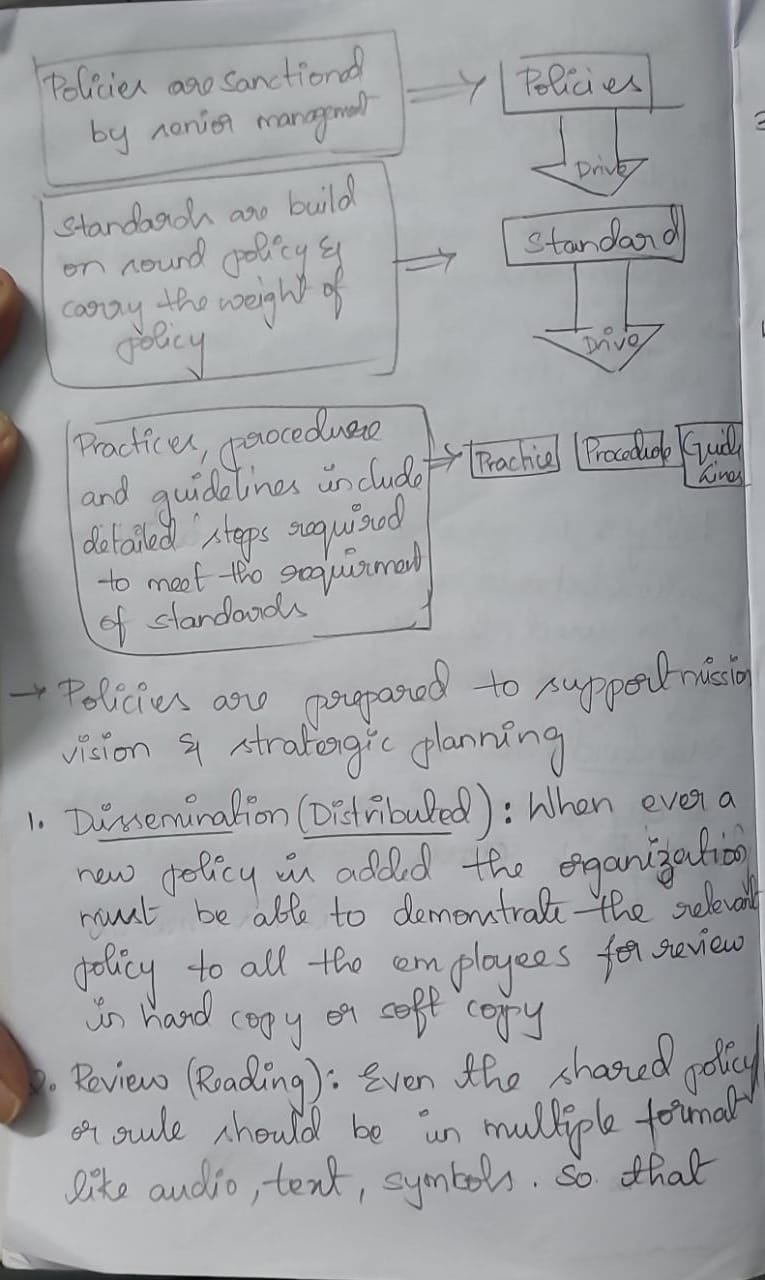
Ans





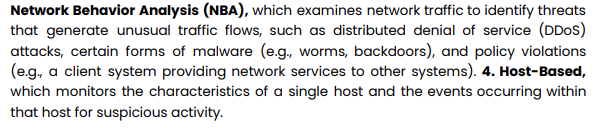
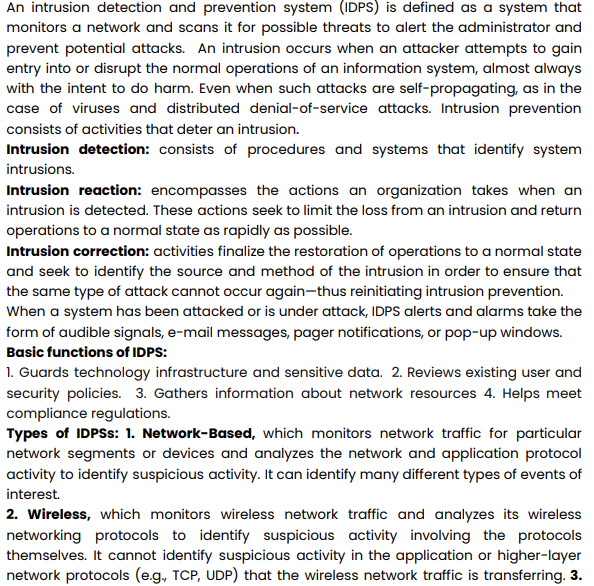
**2) Explain security policies and standards.**

**Ans)**



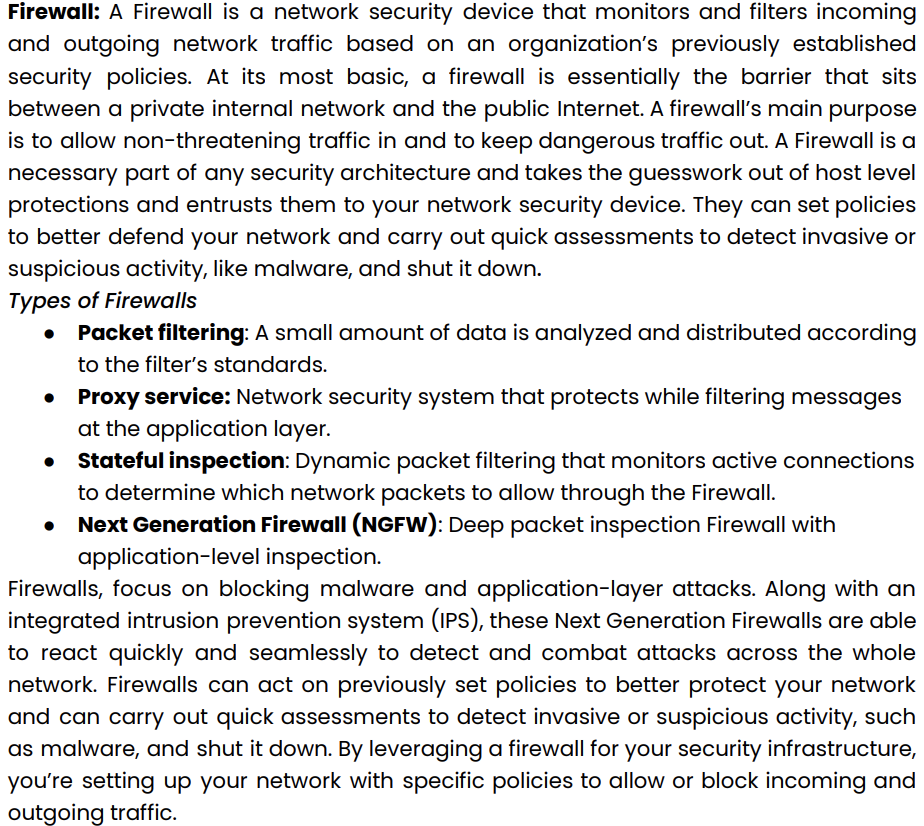
**3) Explain in detail about information detection and prevention system.**

**Ans)**



**4) Explain firewalls and VPNs in detail.**

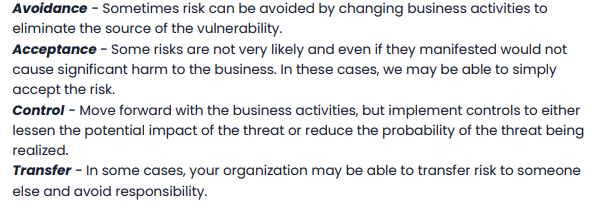
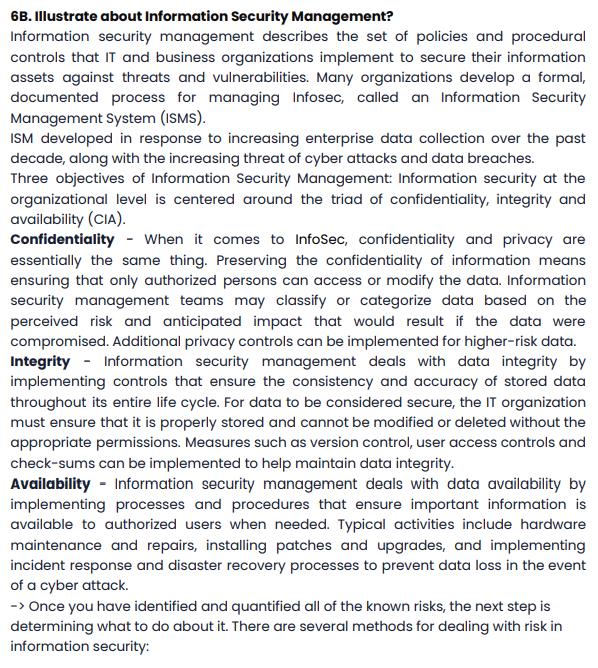
Ans)

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.

**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)



**1) List Security Policies.**

1. Security Program Policy
2. enterprise information security policy (EISP)
3. Issue-Specific Security Policy (ISSP)
4. 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**

1. Public Key Infrastructure (PKI): integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely
2. Digital Signatures: Encrypted messages that can be mathematically proven to be authentic
3. 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:

1. Site-to-Site VPN: A site-to-site VPN is designed to securely connect two geographically-distributed sites.
2. Remote Access VPN: A remote access VPN is designed to link remote users securely to a corporate network.
3. 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.

