Assignment

a. Software Defined Perimeter (SDP)

- Software defined perimeter is a way to hide the internet-connected infrastructure so that external parties and attackers cannot see it when it is hosted in cloud. It makes a boundary at the network layer of a company which restrict outsiders. It provide secure access to network based services and applications. Purpose of SDP software is to give the perrimeter security model to the company.

Software defined perimeter works as a broker between internal application and users who can provide only access. Like an application has front door which is always closed. when user will give proper data then SDP varifies the visiter and opened. after he enter in application it will again closed.

SDP can uses in different ways like User identity verification: It will check the user Id and password for more secure it checks also some sort of hardware token.
Device verification: It checks the device or user which is working for company that software is upto date or not.

SDP controller approval: It is responsible for determining which devices and servers should be allow to connect.

User access: The user is able to access previously hidden network resources and can continue using their device like normal.

SDP help secure hybrid and private clouds.

b. In simple words zero trust security means that noone is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network. It is the main technology that enables organizations to implement zero trust security. It is configured slightly different by each organization or vendor. There are several underlying principles that remain constant across zero trust security Access architectures.

Application vs Network Access:-

Zero trust Network Access treats application access separately from network access connecting to a network doesnot automatically grant a user to right to access the application.

Device security:-

Zero trust Network access can incorporate the risk and security posture of devices as the factors in access decissions.

Additional factors:-

unlike traditional access control which only grants access based on user identity and role, ZTNA can evaluate risks associated with additional factors like location timing etc.

Agent vs service:-

ZTNA can either use an end point agent or based on cloud

principles:-

The zero trust framework is based on four fundamental principles.

(i) Never trust always verify:-

The system should continusly ask users and devices to verify their identities, devices, locations and other attributes to ensure that only previleged.

(ii) continuous monitoring and observing:-

It enables you to have real time understanding of which users are attempting to access which resources and the out come of evaluation.

iii) Least previleges:-

Ensuring that your users only have access to the base minimum of necessary resources is a core tenet of the zero trust frame work.

iv) microsegementation:-

we can minimize the scope and blast radius of a breach or security incident by segmenting your DAAs into smaller, more focused segments within your network.

when we have zero trust security in place we can provide security to anywhere and everywhere on whatever device. we can strengthen security fourthen by including access managemed as the zero trust architerture to create a zero trust extended