Network Security Principles

Network Segmentation -> Splitting a network into multiple segments or subnets
Network Isolation -> Isolate a system, a computer for all network, have no contact with any other device, this is used in a security incident

Security Zones -> Segments within a network that have distinct levels of security controls

- External
- Internal
- DMZ

Attack Surface -> Total number of points where an unauthorized user can try to enter or extract data, all areas that are vulnerable to cyber attacks
Device Attribute:
Active -> Can block or change the traffic flow -> Firewall/Endpoint
Passive -> Only monitor the traffic flow -> SIEM

Jump Server -> It is a secure computer that acts as a controlled entry point into a remote network or server group, it's a gateway between two networks to manage and access devices in a separate security zone
Proxy Server -> Acts as an intermediary between a user's computer and the internet.

- It mask the user's IP address
- Control internet usage blocking access to specific websites
- Can cache frequently accessed content

1. Forward Forward -> No direct connection is made between the client nd the internet
2. Reverse Proxy -> Sits in front of web servers and directs client requests to the appropriate backend server, used for load balancing, caching or SSL encryption
3. Open Proxy -> Conceals your IP address from the websites you visit, providing a degree of anonymity

SD-WAN -> Approach to simplify branch office networking and assure optimal application performance, centralized control function to securely and intelligently direct traffic across the WAN (Company use part of the data from On prem and part from Cloud)