SECURE NETWORK DESIGN

By Safa, Kimberley, Maeks

NETWORK DESIGN FOR SKM company.

Architecture implemented : hierarchical with star topology.

Core layer ( network backbone, high speed data transport, fast packet forwarding is the 1st connectivity

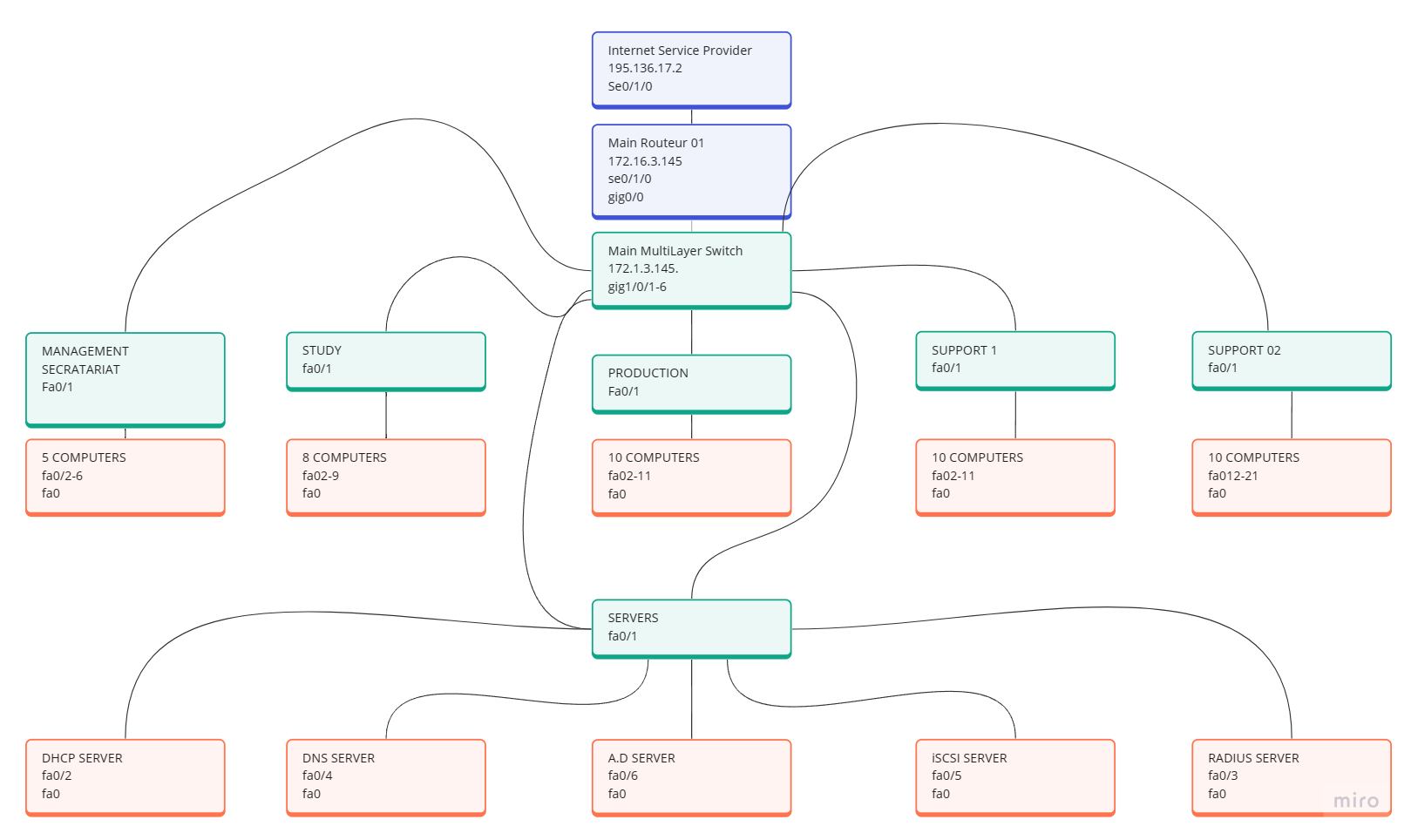
Distribution layer : here routingm filtering and policy enforcment services are implemented, it combines the serparated traffic from the access layer. Vlan segmentation and ACL are configured here

Access layer : entry point for end devices, brings together the traffic from all the access points.

Why ?

Scalability, simplified management, enhanced security ( granular control )

network diagram with annotations :



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SECTORS | NETWORK ADDRESS | SUBNET MASK | HOST ADDRESS RANGE | BROADCAST ADDRESS | VLAN |
| Management/  Secretariat | 172.16.1.0 | 255.255.255.128/25 | 172.16.1.1  172.16.1.126 | 172.16.1.127 | 10 |
| Study | 172.16.1.128 | 255.255.255.128/25 | 172.16.1.129  172.16.1.254 | 172.16.1.255 | 11 |
| Production | 172.16.1.0 | 255.255.255.128/25 | 172.16.2.1  172.16.2.126 | 172.16.2.127 | 12 |
| Support01 | 172.16.2.128 | 255.255.255.128/25 | 172.16.2.129  172.16.2.254 | 172.16.2.255 | 13 |
| Support02 | 172.16.3.0 | 255.255.255.128/25 | 172.16.3.1  172.16.3.126 | 172.16.3.127 | 14 |
| Servers | 172.16.3.128 | 255.255.255.240/28 | 176.16.3.129  176.16.3.142 | 172.16.3.143 | 60 |
| ISP | 195.136.17.0 | 255.255.255.252/30 | 195.136.17.1  196.136.17.2 | 195.136.17.3 | 20 |
| DHCP server | 172.16.3.130 | 255.255.255.240/28 | 176.16.3.129  176.16.3.142 | 172.16.3.143 | 60 |
| DNS server | 172.16.3.131 | 255.255.255.240/28 | 176.16.3.129  176.16.3.142 | 172.16.3.143 | 60 |
| ISCSI server | 172.16.3.132 | 255.255.255.240/28 | 176.16.3.129  176.16.3.142 | 172.16.3.143 | 60 |
| RADIUS server | 172.16.3.133 | 255.255.255.240/28 | 176.16.3.129  176.16.3.142 | 172.16.3.143 | 60 |
| Active directory server | 172.16.3.134 | 255.255.255.240/28 | 176.16.3.129  176.16.3.142 | 172.16.3.143 | 60 |

|  |  |
| --- | --- |
| mainswitchML#show running-config  Building configuration...  Current configuration : 5363 bytes  !  version 16.3.2  no service timestamps log datetime msec  no service timestamps debug datetime msec  service password-encryption  !  hostname mainswitchML  !  !  enable password 7 0836495C061A0E  no ip cef  ip routing  !  no ipv6 cef  username skm password 7 0836495C061A0E  ip ssh version 2  no ip domain-lookup  ip domain-name ourcreation.org  spanning-tree mode pvst  interface GigabitEthernet1/0/1  no switchport  ip address 172.16.3.145 255.255.255.252  duplex auto  speed auto  !  interface GigabitEthernet1/0/2  switchport mode trunk  ip access-group 101 in  ip access-group 101 out  !  interface GigabitEthernet1/0/3  switchport mode trunk  !  interface GigabitEthernet1/0/4  switchport mode trunk  !  interface GigabitEthernet1/0/5  switchport mode trunk  !  interface GigabitEthernet1/0/6  switchport mode trunk  !  interface GigabitEthernet1/0/7  switchport trunk allowed vlan 10-14,20  switchport mode trunk  interface Vlan1  no ip address  shutdown  !  interface Vlan10  mac-address 000a.418d.9801  ip address 172.16.1.1 255.255.255.128  ip helper-address 172.16.3.130  ip access-group 101 out  !  interface Vlan11  mac-address 000a.418d.9802  ip address 172.16.1.129 255.255.255.128  ip helper-address 172.16.3.130  ip access-group 102 out  !  interface Vlan12  mac-address 000a.418d.9803  ip address 172.16.2.1 255.255.255.128  ip helper-address 172.16.3.130  ip access-group 103 out  !  interface Vlan13  mac-address 000a.418d.9804  ip address 172.16.2.129 255.255.255.128  ip helper-address 172.16.3.130  ip access-group 104 out  !  interface Vlan14  mac-address 000a.418d.9805  ip address 172.16.3.1 255.255.255.128  ip helper-address 172.16.3.130  ip access-group 105 out  !  interface Vlan20  mac-address 000a.418d.9807  ip address 195.136.17.0 255.255.0.0  ip access-group 20 in  ip access-group 107 out  !  interface Vlan60  mac-address 000a.418d.9806  ip address 172.16.3.129 255.255.255.240  ip helper-address 172.16.3.130 | !  router ospf 10  router-id 1.1.1.1  log-adjacency-changes  network 172.16.1.0 0.0.0.127 area 0  network 172.16.1.128 0.0.0.127 area 0  network 172.16.2.0 0.0.0.127 area 0  network 172.16.2.128 0.0.0.127 area 0  network 172.16.3.0 0.0.0.127 area 0  network 172.16.3.128 0.0.0.15 area 0  network 172.16.3.144 0.0.0.3 area 0  !  ip classless  ip route 0.0.0.0 0.0.0.0 GigabitEthernet1/0/1  !  ip flow-export version 9  !  !  access-list 101 deny ip 172.16.1.0 0.0.0.127 172.16.1.128 0.0.0.127  access-list 101 deny ip 172.16.1.0 0.0.0.127 172.16.2.0 0.0.0.127  access-list 101 deny ip 172.16.1.0 0.0.0.127 172.16.2.128 0.0.0.127  access-list 101 deny ip 172.16.1.0 0.0.0.127 172.16.3.0 0.0.0.127  access-list 101 deny ip 172.16.1.0 0.0.0.127 172.16.3.128 0.0.0.127  access-list 101 deny ip 172.16.1.0 0.0.0.127 172.16.3.128 0.0.0.15  access-list 102 deny ip 172.16.1.128 0.0.0.127 172.16.1.0 0.0.0.127  access-list 102 deny ip 172.16.1.128 0.0.0.127 172.16.2.0 0.0.0.127  access-list 102 deny ip 172.16.1.128 0.0.0.127 172.16.2.128 0.0.0.127  access-list 102 deny ip 172.16.1.128 0.0.0.127 172.16.3.128 0.0.0.127  access-list 102 deny ip 172.16.1.128 0.0.0.127 172.16.3.0 0.0.0.127  access-list 103 deny ip 172.16.2.0 0.0.0.127 172.16.1.0 0.0.0.127  access-list 103 deny ip 172.16.2.0 0.0.0.127 172.16.1.128 0.0.0.127  access-list 103 deny ip 172.16.2.0 0.0.0.127 172.16.2.128 0.0.0.127  access-list 103 deny ip 172.16.2.0 0.0.0.127 172.16.3.0 0.0.0.127  access-list 103 deny ip 172.16.2.0 0.0.0.127 172.16.3.128 0.0.0.15  access-list 104 deny ip 172.16.2.128 0.0.0.127 172.16.1.0 0.0.0.127  access-list 104 deny ip 172.16.2.128 0.0.0.127 172.16.1.128 0.0.0.127  access-list 104 deny ip 172.16.2.128 0.0.0.127 172.16.2.0 0.0.0.127  access-list 104 deny ip 172.16.2.128 0.0.0.127 172.16.3.128 0.0.0.15  access-list 104 permit ip any any  access-list 105 deny ip 172.16.3.0 0.0.0.127 172.16.1.0 0.0.0.127  access-list 105 deny ip 172.16.3.0 0.0.0.127 172.16.1.128 0.0.0.127  access-list 105 deny ip 172.16.3.0 0.0.0.127 172.16.2.0 0.0.0.127  access-list 105 deny ip 172.16.3.0 0.0.0.127 172.16.3.128 0.0.0.127  access-list 105 permit ip any any  access-list 106 deny ip 172.16.3.128 0.0.0.15 172.16.1.0 0.0.0.127  access-list 106 deny ip 172.16.3.128 0.0.0.15 172.16.1.128 0.0.0.127  access-list 106 deny ip 172.16.3.128 0.0.0.15 172.16.2.0 0.0.0.127  access-list 106 deny ip 172.16.3.128 0.0.0.15 172.16.2.128 0.0.0.127  access-list 106 deny ip 172.16.3.128 0.0.0.15 172.16.3.0 0.0.0.127  access-list 107 deny ip 195.136.17.0 0.0.0.3 any  line con 0  password 7 0836495C061A0E  logging synchronous  login  !  line aux 0  !  line vty 0 4  login local  transport input ssh  line vty 5 15  login local  transport input ssh  end |

|  |  |
| --- | --- |
| ManagementSecretariat-SW#show running-config  Building configuration...  Current configuration : 2130 bytes  !  version 15.0  no service timestamps log datetime msec  no service timestamps debug datetime msec  service password-encryption  !  hostname ManagementSecretariat-SW  !  enable password 7 0836495C061A0E  !  !  !  no ip domain-lookup  !  !  !  spanning-tree mode pvst  spanning-tree extend system-id  !  interface FastEthernet0/1  switchport trunk allowed vlan 10  switchport mode trunk  !  interface FastEthernet0/2  switchport access vlan 10  switchport mode access  !  interface FastEthernet0/3  switchport access vlan 10  switchport mode access  !  interface FastEthernet0/4  switchport access vlan 10  switchport mode access  !  interface FastEthernet0/5  switchport access vlan 10  switchport mode access  !  interface FastEthernet0/6  switchport access vlan 10  switchport mode access  interface Vlan1  no ip address  shutdown  !  interface Vlan10  ip address 172.16.1.1 255.255.255.128  line con 0  password 7 0836495C061A0E  logging synchronous  login  !  line vty 0 4  login  line vty 5 15  login  !  !  !  !  end | Study-SW#show running-config  Building configuration...  Current configuration : 2542 bytes  !  version 15.0  no service timestamps log datetime msec  no service timestamps debug datetime msec  service password-encryption  !  hostname Study-SW  !  enable password 7 0836495C061A0E  !  !  !  no ip domain-lookup  !  !  !  spanning-tree mode pvst  spanning-tree extend system-id  !  interface FastEthernet0/1  switchport trunk allowed vlan 11  switchport mode trunk  !  interface FastEthernet0/2  switchport access vlan 11  switchport mode access  !  interface FastEthernet0/3  switchport access vlan 11  switchport mode access  !  interface FastEthernet0/4  switchport access vlan 11  switchport mode access  !  interface FastEthernet0/5  switchport access vlan 11  switchport mode access  !  interface FastEthernet0/6  switchport access vlan 11  switchport mode access  !  interface FastEthernet0/7  switchport access vlan 11  switchport mode access  !  interface FastEthernet0/8  switchport access vlan 11  switchport mode access  !  interface FastEthernet0/9  switchport access vlan 11  switchport mode access  !  interface Vlan1  no ip address  shutdown  line con 0  password 7 0836495C061A0E  logging synchronous  login  !  line vty 0 4  login  line vty 5 15  login  end |

|  |  |
| --- | --- |
| mainsrouteur01#show running-config  Building configuration...  Current configuration : 2989 bytes  !  version 15.1  no service timestamps log datetime msec  no service timestamps debug datetime msec  service password-encryption  !  hostname mainsrouteur01  !  !  !  enable password 7 0836495C061A0E  !  !  !  !  !  aaa new-model  !  aaa authentication login default group radius local  aaa authentication enable default group radius local  !  !  !  !  !  !  !  ip cef  no ipv6 cef  !  !  !  username skm password 7 0836495C061A0E  !  !  license udi pid CISCO1941/K9 sn FTX15242Z2M-  !  !  !  !  !  !  !  !  !  ip ssh version 2  no ip domain-lookup  ip domain-name ourcreation.org  !  !  spanning-tree mode pvst  !  !  !  !  !  !  interface Loopback0  ip address 10.0.10.1 255.255.255.0  !  interface GigabitEthernet0/0  ip address 172.16.3.146 255.255.255.252  ip nat inside  duplex auto  speed auto  !  interface GigabitEthernet0/1  no ip address  duplex auto  speed auto  !  interface Serial0/1/0  ip address 195.136.17.1 255.255.255.252  ip nat outside  clock rate 64000  !  interface Serial0/1/1  no ip address  clock rate 2000000  !  interface Vlan1  no ip address  shutdown  !  router ospf 10  router-id 2.2.2.2  log-adjacency-changes  network 172.16.3.144 0.0.0.3 area 0  network 195.136.17.0 0.0.0.3 area 0  !  ip nat inside source list 1 interface Serial0/1/0 overload  ip classless  ip route 0.0.0.0 0.0.0.0 Serial0/1/0  !  ip flow-export version 9  !  radius server 172.16.3.133  address ipv4 172.16.3.133 auth-port 1645  key 666  !  !  !  line con 0  password 7 0836495C061A0E  logging synchronous  !  line aux 0  !  line vty 0 4  transport input ssh  line vty 5 15  transport input ssh  !  !  !  end | Servers-SW#show running-config  Building configuration...  Current configuration : 2676 bytes  !  version 15.0  no service timestamps log datetime msec  no service timestamps debug datetime msec  service password-encryption  !  hostname Servers-SW  !  enable password 7 0836495C061A0E  !  !  !  no ip domain-lookup  !  !  !  spanning-tree mode pvst  spanning-tree extend system-id  !  interface FastEthernet0/1  switchport mode trunk  !  interface FastEthernet0/2  switchport access vlan 60  switchport mode access  !  interface FastEthernet0/3  switchport access vlan 60  switchport mode access  !  interface FastEthernet0/4  switchport access vlan 60  switchport mode access  !  interface FastEthernet0/5  !  interface FastEthernet0/6  switchport access vlan 60  switchport mode access  !  interface FastEthernet0/7  !  interface FastEthernet0/8  !  interface FastEthernet0/9  !  interface FastEthernet0/10  !  interface FastEthernet0/11  !  interface FastEthernet0/12  !  interface FastEthernet0/13  !  interface FastEthernet0/14  !  interface FastEthernet0/15  !  interface FastEthernet0/16  !  interface FastEthernet0/17  !  interface FastEthernet0/18  !  interface FastEthernet0/19  !  interface FastEthernet0/20  !  interface FastEthernet0/21  !  interface FastEthernet0/22  !  interface FastEthernet0/23  !  interface FastEthernet0/24  !  interface GigabitEthernet0/1  !  interface GigabitEthernet0/2  !  interface Vlan1  no ip address  shutdown  !  !  !  line con 0  password 7 0836495C061A0E  logging synchronous  login  !  line vty 0 4  login  line vty 5 15  login  !  !  !  !  end |

|  |  |
| --- | --- |
| Production-SW#show running-config  Building configuration...  Current configuration : 2814 bytes  !  version 15.0  no service timestamps log datetime msec  no service timestamps debug datetime msec  service password-encryption  !  hostname Production-SW  !  enable password 7 0836495C061A0E  !  !  !  no ip domain-lookup  !  !  !  spanning-tree mode pvst  spanning-tree extend system-id  !  interface FastEthernet0/1  switchport trunk allowed vlan 12  switchport mode trunk  !  interface FastEthernet0/2  switchport access vlan 12  switchport mode access  !  interface FastEthernet0/3  switchport access vlan 12  switchport mode access  !  interface FastEthernet0/4  switchport access vlan 12  switchport mode access  !  interface FastEthernet0/5  switchport access vlan 12  switchport mode access  !  interface FastEthernet0/6  switchport access vlan 12  switchport mode access  !  interface FastEthernet0/7  switchport access vlan 12  switchport mode access  !  interface FastEthernet0/8  switchport access vlan 12  switchport mode access  !  interface FastEthernet0/9  switchport access vlan 12  switchport mode access  !  interface FastEthernet0/10  switchport access vlan 12  switchport mode access  !  interface FastEthernet0/11  switchport access vlan 12  switchport mode access  line con 0  password 7 0836495C061A0E  logging synchronous  login  !  line vty 0 4  login  line vty 5 15  login  end | Support01/02-SW#show running-config  Building configuration...  Current configuration : 3534 bytes  !  version 15.0  no service timestamps log datetime msec  no service timestamps debug datetime msec  service password-encryption  !  hostname Support01/02-SW  !  enable password 7 0836495C061A0E  !  !  !  no ip domain-lookup  !  !  !  spanning-tree mode pvst  spanning-tree extend system-id  !  interface FastEthernet0/1  switchport trunk allowed vlan 13-14  switchport mode trunk  !  interface FastEthernet0/2  switchport access vlan 13  switchport mode access  !  interface FastEthernet0/3  switchport access vlan 13  switchport mode access  !  interface FastEthernet0/4  switchport access vlan 13  switchport mode access  !  interface FastEthernet0/5  switchport access vlan 13  switchport mode access  !  interface FastEthernet0/6  switchport access vlan 13  switchport mode access  !  interface FastEthernet0/7  switchport access vlan 13  switchport mode access  !  interface FastEthernet0/8  switchport access vlan 13  switchport mode access  !  interface FastEthernet0/9  switchport access vlan 13  switchport mode access  !  interface FastEthernet0/10  switchport access vlan 13  switchport mode access  !  interface FastEthernet0/11  switchport access vlan 13  switchport mode access  !  interface FastEthernet0/12  switchport access vlan 14  switchport mode access  !  interface FastEthernet0/13  switchport access vlan 14  switchport mode access  !  interface FastEthernet0/14  switchport access vlan 14  switchport mode access  !  interface FastEthernet0/15  switchport access vlan 14  switchport mode access  !  interface FastEthernet0/16  switchport access vlan 14  switchport mode access  !  interface FastEthernet0/17  switchport access vlan 14  switchport mode access  !  interface FastEthernet0/18  switchport access vlan 14  switchport mode access  !  interface FastEthernet0/19  switchport access vlan 14  switchport mode access  !  interface FastEthernet0/20  switchport access vlan 14  switchport mode access  !  interface FastEthernet0/21  switchport access vlan 14  switchport mode access  line con 0  password 7 0836495C061A0E  logging synchronous  login  !  line vty 0 4  login  line vty 5 15  login  end |

**SECURITY FEATURES**

implementation of :

**no ip domain look-up command ->**

prevents information leakage where wrong commands could be interpretated as DNS queries, revealing internal network details to external DNS servers. This command allows mistyped stuff to be treated as errors with no DNS resolution attempt. Reduces also attack surface (no dns spoofing or dns responses manipulation are a potential attack vector. This is a good network security hygiene.

**line console 0 ->**

secures and manages a cisco device, so when you want to physically connect to a device, and adding a password means the person is prompted to enter a password before being granted access to the devices command line interface. Here security is implemented by reducing risks of unauthorized access ( but password can be guessed through brute-force attack to an extend)

**RADIUS service ->**

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol for centralized authentication, authorization, and accounting (AAA). It verifies user identities, controls access to network resources, and logs user activity. RADIUS is widely used in enterprise and ISP networks, providing a scalable and secure solution. It centralizes user management, enforcing access policies and tracking network usage. RADIUS operates at the application layer, typically using UDP for communication. It offers encryption and message integrity to protect sensitive data. RADIUS servers authenticate users against a centralized database and determine access rights based on predefined policies. It facilitates seamless authentication for various network devices, including routers, switches, RADIUS enhances network security and simplifies user management across distributed environments. BUT it is also OUT DATED as it works with telnet.

**SSH version 2 ->**

with 4096 bits RSA key for encryption, SSH (Secure Shell) is a network protocol used for secure remote access to devices over a network. It provides encrypted communication between client and server, ensuring confidentiality and integrity of data. SSH facilitates secure login and command execution on remote systems. It operates on port 22 by default and offers authentication using passwords or cryptographic keys. SSH is widely adopted for managing network devices, servers, and cloud instances. It supports various authentication methods and allows secure file transfer (SFTP) and port forwarding. SSH enhances network security by protecting against eavesdropping and unauthorized access. It enables secure administration and communication in distributed environments, improving overall system reliability and integrity.

**NAT ->**

provides a level of security by hiding the internal IP addresses of devices on the local network from external sources, making it more difficult for attackers to directly target individual devices, it translates private addresses into public ones.

**VLANs and ACLs implemented in DMZ concept ->**

A DMZ is a network design strategy that involves creating a buffer zone between an organization's internal network, a “safe” network, and external “unsafe” networks, such as the internet.

The DMZ serves as a segregated area where our public-facing services and resources are hosted,here the DNS server with its DNS and HTTP services.

This provides an additional layer of security to protect sensitive internal data from external threats.The segmentation provided by VLANs isolates critical data from potential threats, ACLs provide granular control over traffic flow and access permissions, reducing the attack surface and protecting against unauthorized access.

ACLs are applied to the interfaces connecting the VLANs to enforce access control policies and regulate traffic flow between network segments. ACLs specify which types of traffic are allowed or denied based on predefined criteria, such as source and destination IP addresses, ports, or protocols.

ACLs are used to filter traffic entering and exiting the DMZ, allowing only authorized traffic to reach public-facing services while blocking or restricting access to sensitive resources in the internal network. For example, ACLs may permit inbound web traffic to reach web servers in the DMZ while blocking direct access to internal databases or file servers. NAT -> NAT provides a level of security by hiding the internal IP addresses of devices on the local network from external sources, making it more difficult for attackers to directly target individual devices.

