Project 11 - Secure Healthcare Information Network

Introduction

In the following project we will design and implement a Secure Healthcare Information Network System. The context is made in an Indian Healthcare Service provider specializing in diagnostic and related healthcare tests. Headquarters in Mumbay, the company conducts tests on blood, urine, and various human bodily tissues. It strategically employs information technology to digitize and securely access and market its services. The company's offices are located on the 35th, 36th and 37th floors of the Great Namaste Tower. The areas are distributed as follows:

- 35th Floor:
  - Pharmacy and Medical Labs – 200 users
  - Receptions and Guest Area – 1000 users

- 36th Floor:
  - Doctors and Consultancy – 200 users
  - Procurement, HR, and Finances Operations – 300 users

- 37th Floor:
  - Internal Auditors & Corporate Functions – 120 users
  - IT – 300 users Divided into: Brand and Digital MKT, IT Support, System/Network Admin, Network Security Engineers, Cybersecurity Analysts, Software Engineers, Cloud Engineers and IT Mgmt.

Recognizing substantial growth potential, the company anticipates that the user count for each department will double the following 5 years, necessitating focus on scalability during the design and implementation phases.

As an integral part of the company's ICT infrastructure, the following components have been incorporated:

a) **Internet Service Providers (ISP):** The company has established a subscription with Airtel S.A. to ensure internet connectivity.
b) **Network Security:** A **Cisco ASA Firewall** from the **5500-X series** has ben acquired to enhance network security.
c) **Network Routing:** A **Cisco WAN Router (2811)** has been deployed to facilitate efficient data routing within the network.
d) **Switching infrastructure:** The networks include **2 Catalyst 3650 24-Ports and 6 Catalyst 2960 24-Ports**, to ensure robust local network connectivity.
e) **Server and Hardware Virtualization: 2 HP Proliant DL38 Gen10 Servers** will be utlilized for virtualization through the **VMWare ESXi hypervisor**. They will host multiple virtual machines, including a Red Hat Directory Server responsible for managing user information in an LDAP-based directory. This server will handle DNS services and IPv4 address allocation for DHCP hosts. The two servers are used for fail-over purposes.

f) **Internal servers:** Internally hosted servers include a Health information System. Email server, and File server, ensuring data accessibility and security.
g) **Storage:** Two storage devices. NetApp product will be used to facilitate storage of resources.
h) **Voice and Wireless Infrastructure:** Cisco Voice Gateways will be employed for VoIP and telephony services. Additionally, **a Cisco Wireles LAN controller (WLC) and 10 Lightweigh Access Points (LAPs)** will centralize the management of the wireless network.

Cloud compiuting Technology as an important technology is used to connect clients across the world to the company services and resources thus the healthcare system is linked to the AWS cloud platform to facilitate service delivery, this this is one of the core business functions of the firm. The devs and cloud engineers use several cloud resources to ensure seamless business continuity. The proposed network should allow the team access to these resources.

Due to security requirements, it has been decided that all LAN, WLAN, and VoIP users will be on separate network segment within the same local area network. The firewall will be used to set security zones and filter traffic that moves in and out of the zones based on the configured inspection policies.

Perform a network according to the requirements: secured, reliable, scalable, and robust. Safeguarding the confidentiality, integrity, and availability of data and communication.

Requirements

The company places a strong emphasis on achieving top-tier performance, redundancy and scalability, and availability within its network infrastructure. The IP address ranges are shown as follows:

- WLAN: 10.10.0.0 /16
- LAN: 192.168.0.0 /20
- Voice: 172.16.0.0 /20
- DMZ: 10.20.10.0 /26
- Public Addresses: 197.200.100.0

Technical requirements

1. **Hierarchical design:** Implement a hierarchical model that incorporates redundancy for enhanced network resilience.
2. **ISPs:** Establish connectivity to an Airtel ISP Router Within the network infrastructure.
3. **WLC:** Ensure that **each department** is equipped with a **Wireless Access Point (WAP)** to provide WiFi access to **Employees, Guests, Corporate Users and External Auditors, managed by WLC**.
4. **VoIP:** Deploy IP phones in each department to support VoIP communications.
5. **VLAN:** Create VLANs with the following IDs**: 10 for LAN, 50 for WLAN, 99 for VoIP** across the entire network.
6. **EtherChannel:** Implement Link Aggregation Control Protocol **(LACP) for EtherChannel** configuration.
7. **STP PortFast and BPDUguard:** Configure **Spanning Tree Protocol (STP) PortFast and BPDUguard** to expedite port transitions from blocking to forwarding states.

8. **Subnetting:** Utilize subnetting techniques to allocate the appropriate number of IP addresses to each network group.
9. **Basic Settings:** Configure fundamental devices settings, including hostnames, console passwords, enable passwords, banner messages, password encryption, and disable IP lookup domain.
10. **Inter-VLAN Routing:** Enable devices in all departments to communicate with one another by configuring respective L3 Switches.
11. **Core Switch:** Assign IP addresses to L3 Switches to enable both routing and switching functionalities.
12. **DHCP Server:** Ensure that all devices in the network (Excluding IP Phones) obtain IP addresses dynamically from Active Directory servers located at the server farm site.
13. **HSRP:** Implement high-availability router protocols such as HSRP to achieve redundancy, load balancing, and failover capabilities.
14. **Static Addressing:** Allocate with static IP addresses to devices located in the server room.
15. **Telephony Service:** Use the Cisco 2811 Router to deploy telephony services. Configure VoIP on the WAN router and assign dial number in the format (3…).
16. **Routing protocol:** Utilize OSPF as the routing protocol to advertise routes on the Firewall, routers, and L3 Switches.
17. **Standard ACL for SSH:** Establish an ACL on the VTY line to permit remote administrative tasks via SSH only for the Network Security Engineer PC.
18. **Cisco ASA Firewall:** Configure default static routes, basic settings, security levels, zones, and policies into the Cisco ASA Firewall to define access control and resource utilization within the network.
19. **Final testing:** Verify all functionalities on the entire network.

Addressing

Network Address Allocation

Initial Conditions

- WLAN: 10.10.0.0 /16
- LAN: 192.168.0.0 /20
- Voice: 172.16.0.0 /20
- DMZ: 10.20.10.0 /26
- Public Addresses: 197.200.100.0

CAIRO TELCO NETWORK				
VLAN	**Network /mask**	**Host range**	**Default GW**	**Broadcast**
WLAN	10.10.0.0 /16	0.1 – 255.254	10.10.0.1	10.10.255.254
LAN	192.168.0.0 /20	0.1 – 15.254	192.168.0.1	192.168.15.254
VoIP	172.16.0.0 /20	0.1 – 15.254	172.16.0.1	172.16.15.254
DMZ	10.20.10.0 /26	10.1 – 10.62	10.20.10.1	10.20.10.63

Point-to-Point links	
Link	**Network /Mask**
AWS Cloud	30.0.0.0 /8
ISP- AWS Cloud	20.20.20.0 /30
FW – ISP	197.200.100.0 /30
FW – WAN Router	10.30.10.0 /30
WAN Router - L3 SW1	10.30.10.4 /30
WAN Rouer – L3 SW2	10.30.10.8 /30

Device Configurations

ROUTERS

All Routers

```
En
Conf t
Banner motd **UNAUTHORIZED ACCESS IS PUNISHABLE**
Enable password cisco
Line console 0
Password cisco
No ip domain-lookup
Service password-encryption
Ip domain-name cisco.com
Username cisco password cisco
Crypto key generate rsa general-keys modulus 1024
Ip ssh version 2
```

WLAN R1

```
En
Conf t
Hostname WLAN-R1

Int fa1/0
No shut
Ip address 10.30.10.6 255.255.255.252
Exit

Int fa1/1
No shut
Ip address 10.30.10.10 255.255.255.252
Exit

Int fa0/0
No shut
Ip address 10.30.10.2 255.255.255.252
Exit
```

//OSPF

```
Router ospf 10
Router id 3.3.3.3
Auto-cost reference-bandwidth 1000000
```

```
Network 10.30.10.0 0.0.0.3 area 0
Network 10.30.10.4 0.0.0.3 area 0
Network 10.30.10.8 0.0.0.3 area 0
Exit
Do wr
```

VoIP-Router

```
En
Conf t
Hostname VoIP-Router
```

//Router on a stick is needed to provide Ips to the phones

```
Int fa0/0
No shut
Int fa0/0.99
Encapsulation dot1q 99
Ip address 172.16.0.1 255.255.240.0
Exit
```

//DHCP

```
Ip dhcp pool VoIP
Network 172.16.0.0 255.255.240.0
Default-router 172.16.0.1
Option 150 ip 172.16.0.1
Exit

Telephony-service
Max-dn 20
Max-ephones 20
Auto assign 1 to 20
Ip source-address 172.16.0.1 port 2000
Exit

Ephone-dn 1
Number 3001
Exit

Ephone-dn 2
Number 3002
Exit

Ephone-dn 3
Number 3003
Exit

Ephone-dn 3
Number 3004
Exit

Ephone-dn 3
Number 3005
Exit

Ephone-dn 3
```

```
Number 3006
Exit

Ephone-dn 3
Number 3007
Exit

Ephone-dn 3
Number 3008
Exit

Ephone-dn 3
Number 3009
Exit

Ephone-dn 3
Number 3010
Exit

Do wr
```

Perimeter-FW

```
En

Conf t
Hostname Perimeter-FW
Domain-name cisco.com
```

//Security config to WAN-R1

```
Int gi1/1
No shut
Ip address 10.30.10.1 255.255.255.252
Nameif INSIDE
Security-level 100
Exit
```

//Security config to DMZ

```
Int g1/2
No shut
Ip address 10.20.10.1 255.255.255.192
Nameif DMZ
Security-level 70
Exit
```

//Security config to

```
Int gi1/3
No shut
Ip address 197.200.100.2 255.255.255.252
Nameif OUTSIDE
Security-level 0
Exit
```

//OSPF

```
Router ospf 25
Route-id 4.4.4.4
Auto-cost reference-bandwidth 1000000
Network 10.20.10.0 255.255.255.192 area 0
Network 10.30.10.0 255.255.255.252 area 0
Network 197.200.100.0 255.255.255.252 area 0
Exit
```

//Route going OUTSIDE interface – permit any ip with any mask should go to ISP-router 197.200.100.1

```
Route OUTSIDE 0.0.0.0 0.0.0.0 197.200.100.1
```

// NAT equivalence format: Object network NAME – Subnet to do NAT – NAT (From IFName, To IFName)

```
Object network LAN-INTERNET
Subnet 192.168.0.0 255.255.240.0
Nat (INSIDE,OUTSIDE) dynamic interface
Exit
Conf t

Object network WLAN-INTERNET
Subnet 10.10.0.0 255.255.0.0
Nat (INSIDE,OUTSIDE) dynamic interface
Exit
Conf t

Object network DMZ-INTERNET
Subnet 10.20.10.0 255.255.255.192
Nat (DMZ,OUTSIDE) dynamic interface
Exit
Conf t
```

//FW Policies. Ports: 80: HTTP – 67,68: DHCP - 63: DNS -

```
Access-list INSIDE-DMZ extended permit icmp any any
Access-list INSIDE-DMZ extended permit tcp any any eq 80
Access-list INSIDE-DMZ extended permit udp any any eq 67
Access-list INSIDE-DMZ extended permit udp any any eq 68
Access-list INSIDE-DMZ extended permit udp any any eq 53
Access-list INSIDE-DMZ extended permit tcp any any eq 53
Access-group INSIDE-DMZ in interface DMZ

Access-list INSIDE-OUTSIDE extended permit icmp any any
Access-list INSIDE-OUTSIDE extended permit tcp any any eq 80
Access-group INSIDE-OUTSIDE in interface OUTSIDE

Wr mem
```

L3-SWITCHES

All L3-Switches

```
En
Conf t
Banner motd **UNAUTHORIZED ACCESS IS PUNISHABLE**
Enable password cisco
Line console 0
```

```
Password cisco
No ip domain-lookup
Service password-encryption
Ip domain-name cisco.com
Username cisco password cisco
Crypto key generate rsa general-keys modulus 1024
Ip ssh version 2


Vlan 10
Name LAN
Vlan 50
Name WLAN
Vlan 99
Name Voice
Vlan 100
Name native
exit

Int ran gi1/0/21-24
No shut
Channel-group 1 mode active
Exit
Int port-channel 1
Switchport mode trunk
Switchport trunk native vlan 100
Exit

Int ran gi1/0/2-8
No shut
Switchport mode trunk
Switchport trun native vlan 100
Exit
```

CoreL3-SW1

```
En
Conf t
Hostname CoreL3-SW13

Int gi1/0/1
No shut
No switchport
Ip address 10.30.10.5 255.255.255.252
Ip routing
Exit
```

// HSRP Config through SVIs except vlan 99 (voice) which is managed by VoIP-Router. Group standby numbers must match on both sides.

```
Int vlan 10
ip address 192.168.0.3 255.255.240.0
Ip helper-address 10.20.10.10
Standby 10 priority 150
Standby 10 ip 192.168.0.1
Exit
```

```
Int vlan 50
Ip address 10.10.10.3 255.255.0.0
ip helper-address 10.20.10.10
Standby 50 priority 150
Standby 50 ip 10.10.0.1
Exit
```

//OSPF

```
Router ospf 10
Auto-cost reference-bandwidth 1000000
Router-id 1.1.1.1
Network 10.30.10.4 0.0.0.3 area 0
Network 10.10.0.0 0.0.255.255 area 0
Network 192.168.0.0 0.0.15.255 area 0
Network 172.16.0.0 0.0.15.255 area 0
Do wr
```

CoreL3-SW2

```
En
Conf t
Hostname CoreL3-SW2

Int gi1/0/1
No shut
No switchport
Ip address 10.30.10.9 255.255.255.252
Ip routing
```

// HSRP Config through SVIs except vlan 99 (voice) which is managed by VoIP-Router. Group standby numbers must match on both sides.

```
Int vlan 10
Ip address 192.168.0.2 255.255.240.0
Ip helper-address 10.20.10.10
Standby 10 priority 100
Standby 10 192.168.0.1
Exit

Int vlan 50
Ip address 10.10.0.2 255.255.0.0
Ip helper-address 10.20.10.10
Standby 50 priority 100
Standby 50 ip 10.10.0.1
Exit

Int vlan 99
Ip address 172.16.0.2 255.255.240.0
Ip helper-address 10.20.10.10
Standby 99 priority 100
Standby 99 ip 172.16.0.1
Exit
Do wr
```

//OSPF

```
Router ospf 10
Auto-cost reference-bandwidth 1000000
Router-id 2.2.2.2
Network 10.30.10.8 0.0.0.3 area 0
Network 10.10.0.0 0.0.255.255 area 0
Network 192.168.0.0 0.0.15.255 area 0
Network 172.16.0.0 0.0.15.255 area 0
Exit
Do wr
```

Airtel-ISP

```
En
Conf t
Hostname Airtel-ISP

Int gi0/0/0
No shut
Ip address 197.200.100.1 255.255.255.252
Exit

Int gi0/0/1
No shut
Ip address 20.20.20.2 255.255.255.252
Exit
```

//OSPF

```
Router ospf 10
Router-id 5.5.5.5
Auto-cost reference-bandwidth 1000000
Network 20.20.20.0 0.0.0.3 area 0
Network 197.200.100.0 0.0.0.3 area 0
Exit
Do wr
```

AWS-Cloud

```
En
Conf t
Hostname AWS-Cloud

Int gi0/0/0
No shut
Ip address 20.20.20.1 255.255.255.252
Exit

Int gi0/0/1
No shut
Ip address 30.0.0.1 255.0.0.0
Exit
```

//OSPF

```
Router ospf 10
Router-id 6.6.6.6
Auto-cost reference-bandwidth 1000000
```

```
Network 30.0.0.0 0.255.255.255 area 0
Network 20.20.20.0 0.0.0.3 area 0
Exit

Do wr
```

SWITCHES

All Switches – except DMZ and WLC SW

```
En
Conf t
Banner motd **UNAUTHORIZED ACCESS IS PUNISHABLE**
Enable password cisco
Line console 0
Password cisco
No ip domain-lookup
Service password-encryption
Ip domain-name cisco.com
Username cisco password cisco
Crypto key generate rsa general-keys modulus 1024
Ip ssh version 2

Vlan 10
Name LAN
Vlan 50
Name WLAN
Vlan 99
Name Voice
Vlan 100
Name Native
Exit

Int ran gi0/1-2
No shut
Switchport mode trunk
Switchport trunk native vlan 100
Exit

Int ran fa0/1-20
Switchport mode access
Switchport access vlan 10
Switchport voice vlan 99
Exit

Int ran fa0/21-24
Switchport mode access
Switchport access vlan 50
Exit

Int ran fa0/1-24
Spanning-tree portfast
Spanning-tree bpduguard enable
Exit

Do wr
```

Pharm&Med-SW

```
En
Conf t
Hostname Pharm&Med-SW
```

Rec&Guest-SW

```
En
Conf t
Hostname Rec&Host-SW
```

Doc&Cons-SW

```
En
Conf t
Hostname Doc&Cons-SW
```

PR-HR-FIN-SW

```
En
Conf t
Hostname PH-HR-FIN-SW
```

IA&Corp-SW

```
En
Conf t
Hostname IA&Corp-SW
```

IT-SW

```
En
Conf t
Hostname IT-SW
```

WLC-SW

```
En
Conf t
Hostname WLC-SW

En
Conf t
Banner motd **UNAUTHORIZED ACCESS IS PUNISHABLE**
Enable password cisco
Line console 0
Password cisco
No ip domain-lookup
Service password-encryption
Ip domain-name cisco.com
Username cisco password cisco
Crypto key generate rsa general-keys modulus 1024
Ip ssh version 2

Vlan 10
Name LAN
```

```
Vlan 50
Name WLAN
Vlan 99
Name Voice
Vlan 100
Name Native
Exit
```

//VoIP-Router in Fa0/1 must be trunk to give Ips to phones

```
Int fa0/1
No shut
Switchport mode trunk
Switchport trunk native vlan 100
Exit

Int ran gi0/1-2
No shut
Switchport mode trunk
Switchport trunk native vlan 100
Exit

Int ran fa0/2-20
No shut
Switchport mode access
Switchport access vlan 10
Switchport voice vlan 99
Exit

Int ran fa0/21-24
No shut
Switchport mode access
Switchport access vlan 50
Switchport voice vlan 99
Exit

Int ran fa0/4-24
No shut
Spanning-tree portfast
Spanning-tree bpduguard enable
Exit
```

DMZ-SW

```
En
Conf t
Hostname DMZ-SW

En
Conf t
Banner motd **UNAUTHORIZED ACCESS IS PUNISHABLE**
Enable password cisco
Line console 0
Password cisco
No ip domain-lookup
Service password-encryption
Ip domain-name cisco.com
```

```
Username cisco password cisco
Crypto key generate rsa general-keys modulus 1024
Ip ssh version 2
```