Project 12- Complete Campus Area Network

Introduction

An recognized university has encompassed two campuses strategically positioned 100 miles apart within the United States. The university's organizational structure revolves around four key faculties, both in the main and branch campuses:

- Health and Services
- Business
- Engineering/Computing
- Art & Design

This diverse array of faculties accommodates the dynamic needs of both students and staff, fostering a rich academic environment. To ensure seamless connectivity and technological cohesion, an integral component oof the university is it IT department, situated at the main campus. This central hub orchestrates the management of both campuses, overseeing the intricate network that binds them together. Currently, the university caters to a substantial community, boasting a collective headcount of approximately 30000 users spread across the two campuses. In anticipation of significant growth, the university envisions a doubling of user counts within each department by the next 5 years. This foresight underscores the necessity for a robust and scalable infrastructure.

At the heart of the technological infrastructure lies the main campus, which hosts a server farm, often referred as de DMZ Zone. Within this zone, the following servers are housed: DHCP, DNS, FTP, WEB, and Email. Recognizing the importance of secure resource access, users at the branch campus are equipped with the capability to securely connect to and utilize these centralized servers. This safeguarded connectivity ensures that all resources of the university are available to all users, regardless of their physical location.

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

a) **Internet Service Provider (ISP):** The university has established a subscription to Airtel ISP.
b) **Network Security: The Cisco ASA Firewalls from the 5500-X** series have been acquired. Each campus will have its firewall but the main campus will contain the DMZ of the server farm.
c) **Network Routing:** Both the firewalls and the core switches will be used instead of a router.
d) **Switching infrastructure:** The network includes 2 Catalyst 3650 48-Port Switches for each campus, and Catalyst 2960 48-Port Switches per faculty to ensure robust LAN connectivity.
e) **Server Hardware and Virtualization:** Two physical servers will be utilized for virtualization through the hypervisor to achieve multiple VMs. For redundancy or failover, we will have 2 DHCP Servers running at the same time.
f) **Wireless Infrastructure:** A Cisco WLC and Lightweight APs (LAPs) will centralize the management of the wireless network. The WLC will be placed at the main campus and will be managing all the Aps in the network.
g) **Site-To-Site VPN:** Configure GRE over IPSec on the two firewalls to enable secure communication between the main and the branch campus.

Cloud computing as an important technology is used to connect clients across the world to University services and resources, thus the University system is linked to the Google Cloud platform to facilitate Service delivery, meaning that this is one of the core business functions of the firm. The proposed network should allow the team access to these resources.

It has been decided that all LAN and WLAN users will be on a 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. Finally, the two campuses should have a secure tunnel of communication via IPsec VPN.

Design an appropriate robust network design model to meet the design requirements that matches with a secured, reliable, and scalable top-tier network system that is paramount of safeguarding the confidentiality, integrity, and availability of data and communications.

Requirements

Implement the deployment of the network with the following address ranges:

- **Management Network: 192.168.10.0 /24** to all the Network
- **WLAN:** Main Campus **10.10.0.0 /16**, and Branch Campus **10.11.0.0 /16**
- **LAN:** Main campus **172.16.0.0 /16,** and Branch Campus **172.17.0.0 /16**
- **DMZ: 10.20.20.0 /27**
- **Public addresses:** For Main campus 105.100.50.0 /30, and for the branch campus 205.200.100.0 /30.

The following technical requirements are necessary to create a comprehensive network:

1. **Hierarchical Design:** Implement this model that incorporates redundancy and 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 to provide WiFi access to **Employees, Corporate Users, External auditors, and Guests**, all centrally managed by WLC.
4. **VLAN:** Maintain VLANs with the following IDs:
    a. Management: 10
    b. LAN: 20
    c. WLAN: 50
    d. Backhole: 199. In which all unused ports are placed
5. **Etherchannel:** Implement Link Aggregation Control Protocol (LACP) for EtherChannel configuration.
6. **STP PortFast and BPDU Guard:** Configure STP to expedite port transitions from blocking to forwarding states.
7. **Subnetting:** Utilize subnetting techniques to allocate the appropriate number of IP addresses to each network group.
8. **Basic Setrings:** Configure fundamental settings, including hostnames, console passwords, enable password, banner messages, password encryption, and disable IP domain lookup
9. **Inter-VLAN Routing:** enable devices in all departments to communicate with one another by configuring the respective multilayer switch for Inter-VLAN routing.

10. **Core Switch:** Assign IP addresses to Multilayer switches to enable both routing and switching functionalities.
11. **DHCP Server:** Ensure that all devices in the network obtain IP addresses dynamically from the DHCP servers located at the server farm site.
12. **HSRP:** Implement High-Availability router protocols such as HSRP to achieve redundancy and failover capabilities.
13. **Static Addressing:** Allocate static IP addresses to devices located in the server room.
14. **Routing Protocol:** Utilize OSPF to advertise routes on the Firewall, Routers and L3 Switches.
15. **Standar ACL for SSH:** Implement standard ACL to on VTY line to permit remote administrative access only from Authorized Engineer PC.
16. **Cisco ASA Firewall:** Configure default static routes, basic settings, security levels, zones and policies on the Firewall to define access control and resource utilization within the network.
17. **Final testing:** Do as many test as necessary to verify proper communication throughout the entire network.

Addressing

Network Address Allocation

Campus Network

CAMPUS NETWORK				
VLAN	**Network /mask**	**Host range**	**Default GW**	**Broadcast**
MGMT	192.168.10.0 /24	10.1 – 10.254	192.168.10.1	192.168.10.255
HQ-LAN	172.16.0.0 /16	0.1 – 255.254	172.16.0.1	172.16.255.255
Branch-LAN	172.17.0.0 /16	0.1 – 255.254	172.17.0.1	172.17.255.255
HQ-WLAN	10.10.0.0 /16	0.1 – 255.254	10.10.0.1	10.10.255.255
Branch-WLAN	10.11.0.0 /16	0.1 – 255.254	10.11.0.1	10.11.255.255
MGMT	192.168.10.0 /24	10.1 – 10.254	192.168.10.1	192.168.10.255
DMZ	10.20.20.0 /27	20.1 – 20.30	10.20.20.1	10.20.20.31

Point-to-Point links

Point-to-Point links	
Link	**Network /Mask**
Google Cloud	8.0.0.0 /8
HQ-Aritel-ISP <-> Internet	20.20.20.0 /30
Branch-Airtel-ISP <-> Internet	30.0.30.0 /30
HQ-FW <-> HQ-Airtel-ISP	105.100.50.0 /30
Branch-FW <-> Branch-Airtel-ISP	205.200.100.0 /30
HQ-FW <-> HQ-L3-SW1	10.20.20.32 /30
HQ-FW <-> HQ-L3-SW2	10.20.20.36 /30
Branch-FW <-> B-L3-SW1	10.20.20.40 /30
Branch-FW <-> B-L3-SW2	10.20.20.44 /30