Design and Implementation of a Secure Company Network System

Cyton Innovation Ltd is a dynamic and forward-thinking company specializing in providing innovative cloud solutions to clients worldwide. Leveraging cutting-edge technology and a team of highly skilled professionals, cyton Innovation focuses on developing and implementing cloud-based solutions tailored to meet the evolving needs of businesses across various industries. With a strong emphasis on creativity, agility, and customer-centricity, cyton Innovation aims to empower organizations to enhance their operational efficiency, scalability, and competitiveness in today's digital landscape.

With a workforce of 600 staff, cyton Innovation Ltd recently expanded and is preparing to move to a new building. The new building, comprising three floors, will house various departments, including Sales and Marketing, Human Resources and Logistics, Finance and Accounts, Administrator and Public Relations, ICT, and a Server Room. The ICT department further hosts Software Developers, Cloud Engineers, Cybersecurity Engineers, Network Engineers, System Administrators, IT Support Specialists, Business Analysts and Project Managers.

Prior to the move, a new network service needs to be designed and implemented in the new building. To ensure robust security, cyton Innovation will implement several security measures to protect the network from internal and external threats. The firewall will have outside, inside, and DMZ security zones, with essential servers strategically housed within the fortified zone. Additionally, Active Directory (AD) servers, responsible for managing and authenticating users, computers, and resources within the internal network, will be placed on the Inside zone of the firewall- this implies that servers such as DHCP, DNS, and Radius will all be on the inside zone, while other servers such as FTP, WEB, Email, APP, and NAS storage will be located in the DMZ- the zone can be attached to any firewall as of now. This meticulous planning and deployment of security measures will safeguard the network and ensure smooth operations for cyton Innovation Ltd in its new building.

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

a) Internet Services Provider (ISP): The University has established a subscription with two ISPs (SEACOM & Safaricom) to ensure redundant internet connectivity.

b) Network Security: Two Cisco ASA Firewalls from the 5500-X series have been acquired to enhance network security and redundancy.

c) Network Routing: Both the firewalls and the core switches will be used instead of a router.

d) Switching Infrastructure: The network includes two Catalyst 3850 48-Port Switches, and Catalyst 2960 48-Port Switches to ensure robust local network connectivity. e) Server Hardware and Virtualization: Two physical servers will be utilized for virtualization through the hypervisor to achieve multiple virtual machines for various services.

f) Wireless Infrastructure: A Cisco Wireless LAN Controller (WLC) and various Lightweight Access. Points (LAPs) will centralize the management of the wireless network.
g) VoIP or IP Phones: A Cisco Voice Gateway will be used to enable telephony service in the network.

Cloud computing as an important technology is used to connect clients across the world to the company services and resources thus the proposed network should allow the team access to these resources.

Therefore, as a key member of the Networks Team, you have been tasked to design a network for the new building. At this stage, logical design is required, which shows the measures that you would put in place to ensure that the new network meets the current business need and is future proofed.

Requirements

The company pfaces a strong emphasis on achieving top-tier performance, redundancy, scalability, and availability within its network infrastructure. As such, your task involves creating a comprehensive network design and executing its implementation. To facilitate this endeavor, the University has designated specific IP address ranges:

- **Management Network:** For the management, the IP address range of 192.168.10.0/24 has been allocated.
- **WLAN:** The WLAN network will operate within the IP address range of 10.20.0.0/16.
- **LAN:** For the local area network (LAN), the IP address range of 172.16.0.0/16.
- **VoIP:** For the local area network (LAN), the IP address range of 172.30.0.0/16.
- **DMZ:** The Demilitarized Zone (DMZ) will be assigned IP addresses from the range 10.11.11.0/27.
- **Public Addresses:** Public IP addresses from the range 105.100.50.0/30 from SEACOM and 197.200.100.0/30 from Safaricom.

Technical Requirements

1. **Design Tool:** Utilize Cisco Packet Tracer for designing and implementing the network solution.
2. **Hierarchical Design:** Implement a hierarchical model that incorporates redundancy for enhanced network resilience.
3. **ISPs:** Establish connectivity to the two ISPs within the network infrastructure.
4. **WLC:** Ensure that each department is equipped with a Wireless Access Point (WAP) to provide WIFI access to employees, corporate users, external auditors, and guests, all centrally managed by the Wireless LAN Controllers (WLC).
5. **VLAN:** Maintain VLANs with the following IDs: 10 for Management, 20 for LAN, 50 for WLAN, 70 for VoIP, and finally, 199 for Blackhole in which all unused ports are placed.
6. **EtherChannel:** Implement the Link Aggregation Control Protocol (LACP) for EtherChannel configuration, enhancing link aggregation efficiency.
7. **Telephony Service:** Configure VoIP on the voice gateway router and allocate dial numbers in format (4..).
8. **STP PortFast and BPDUguard**: Configure Spanning Tree Protocol (STP) PortFast and BPDUguard to expedite port transitions from blocking to forwarding states.
9. **Subnetting:** Utilize subnetting techniques to allocate the appropriate number of IP addresses to each network group.

10. **Basic Settings:** Configure fundamental device settings, including hostnames, and console passwords, enable passwords, banner messages, password encryption, and disable IP domain lookup.
11. **Inter-VLAN Routing:** Enable devices in all departments to communicate with one another by configuring the respective multilayer switch for inter-VLAN routing.
12. **Core Switch:** Assign IP addresses to Multilayer switches to enable both routing and switching functionalities.
13. **DHCP Server:** Ensure that all devices in the network obtain IP addresses dynamically from the DHCP servers located at the server farm site.
14. **HSRP:** Implement high-availability router protocols such as HSRP to achieve redundancy, load balancing, and failover capabilities.
15. **Static Addressing:** Allocate static IP addresses to devices located in the server room.
16. **Routing Protocol:** Utilize Open Shortest Path First (OSPF) as the routing protocol to advertise routes on the firewall, routers, and multilayer switches.
17. **Standard ACL for SSH:** Establish a simple standard Access Control List (ACL) on the VTY line to permit remote administrative tasks via SSH only for the Senior Network Security Engineer PC.
18. **Cisco ASA Firewall:** Configure default static routes, basic settings, security levels, zones, and policies on the Cisco ASA Firewall to define access control and resource utilization within the network.
19. **Final Testing:** Conduct thorough testing to verify proper communication and ensure that all configured elements function as intended.