Advanced Enterprise Networking

Design and Implementation of a Secure Telecommunication Company Network System

Cairo Telco is a fast-growing telecommunication company in Egypt, which offers IT solutions and services to its clients. The company is located in the Egyptian capital city, Cairo, and has occupied the fourth and fifth floors of Pharaoh's Mega Plaza. The company has its fourth floor hosting HR and Finance(40), Product Brand and Marketing(45), and finally, Admin and Corporate departments(35). The fifth floor is designed for IT Network & Support(45), Software Engineering(36), and Cloud Engineering departments(32).

As part of ICT infrastructure, the company has subscribed to Seacom ISP for internet services and also has purchased one 5525-X Cisco ASA Firewall, one Catalyst 3850 48-Port Switch, 3 Catalyst 2960 48-Port Switches, 2 Catalyst 2960 24-Port Switches, 1 Cisco Voice Gateway, 1 Cisco WLC, and 6 LAPs. The company uses Windows Server 2022 to manage the Active Directory and Radius Server, the server is responsible for DNS services and for allocating IPv4 addresses to the DHCP hosts in the network. The company has an internally hosted ERP system, Email server, and File server. The company has settled on using Cisco Voice Gateways to provide VoIP or telephony services in the network and Cisco WLC to provide central management for Aps.

Cairo Telco leverages using Microsoft Azure cloud platform to facilitate service delivery thus this is one of the core business functions of the firm. The developers and cloud engineers use several MS Azure resources like VM, blob storage, networking, and security among others 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 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.
You have been hired as a network security engineer to design the network for Cairo Telco according to the requirements set by the senior management. You will consult an appropriate robust network design model to meet the design requirements. You are required to design and implement a secured, reliable, scalable, and robust network system that is paramount to safeguarding the Confidentiality, Integrity, and Availability of data and communication.

Requirements

The company has emphasized high performance, redundancy, scalability, and availability, and hence you are required to provide a complete Cairo Telco network infrastructure design and implementation. The company will be using the following IP address: 10.20.0.0/16 for WLAN, 192.168.10.0/24 for LAN, 172.16.10.0/24 for Voice, 10.10.10.0/28 for DMZ and 197.200.100.0 for public addresses.

Requirements

1. **Design Tool-** Use Cisco Packet Tracer to design and implement the network solution.
2. **Hierarchical Design-** Use a hierarchical model providing redundancy.
3. **ISPs-** The network is also expected to connect to a Seacom ISP Router.
4. **WLC-** Each department is required to have a WAP providing both employees and guest WIFI managed by WLC.
5. **VoIP-** Each department should have IP phones.
6. **VLAN-** The LAN, WLAN, and VoIP VLANs remain at 50, 60 & 101 respectively for the entire network.
7. **EtherChannel-** Use standard LACP as a method of link aggregation.
8. **STP PortFast and BPDUguard-** configure the two protocols to enable faster port transition from blocking to forwarding.
9. **Subnetting-** Provided the networks above, carry out subnetting to allocate the correct number of IP addresses to each department.
10. **Basic settings-** Configure basic device settings such as hostnames, and console passwords, enable passwords, and banner messages, encrypt all passwords, and disable IP domain lookup.
11. **Inter-VLAN Routing-** Devices in all the departments are required to communicate with each other with the respective multilayer switch configured for inter-VLAN routing.
12. **Core Switch-** The Multilayer switches are expected to carry out both routing and switching functionalities and thus will be assigned IP addresses.
13. **DHCP Server-** All devices in the network (except IP phones) are expected to obtain an IP address dynamically from the AD servers located at the server farm site.
14. **Cisco 2811 Router-** Ensure to have a router that can support telephony service i.e Cisco Catalyst 2811(the VoIP router should be connected to the l3-switch).
15. **Static Addressing-** Devices in the server room are to be allocated IP addresses statically.
16. **Telephony Service-** Configure VoIP on the voice gateway router and allocate dial numbers in format (1...).
17. **Routing Protocol-** Use OSPF as the routing protocol to advertise routes both on the routers and multilayer switches.
18. **Standard ACL for SSH-** configure a simple standard ACL on the line VTY to allow only the Senior Network Security Engineer to carry out all remote administrative tasks using SSH.
19. **Cisco ASA Firewall-** Configure security levels, zones, and policies to define how resources are accessed in the network
20. **Final-** Test Communication, ensure everything configured is working as expected.

Technologies Implemented

1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Configuring Basic device settings.
5. Creating VLANs and assigning ports VLAN numbers.
6. Creating both data and voice VLANs and assigning ports VLAN numbers.
7. Subnetting and IP Addressing.
8. Configuring Inter-VLAN Routing both on the Switches (SVI) and Routers (router-on-a-stick).
9. Configuring Dedicated DHCP Server device for Data to provide dynamic IP allocation.
10. Configuring Routers as DHCP server for Voice to provide IP Phones dynamic IP allocation.
11. Configuring Spanning-Tree Protocol - STP PortFast and BPDUGuard.
12. Configuring Active Directory as DHCP Server.
13. Configuring SSH for secure Remote access.
14. Configuring OSPF as the routing protocol.
15. Configuring Standard ACL for VTY interfaces to restrict remote Access using SSH.
16. Configuring VoIP or Telephony service configuration in all routers.
17. Configuring WLAN network- Wireless LAN Controller + Wireless Lighweight Access Points .
18. Configuring Cisco ASA Firewall Interface descriptions, zones and security levels.
19. Configuring Cisco ASA Firewall Object Network + Network Address Translation (NAT).
20. Configuring Cisco ASA Firewall OSPF + Default Static Routes.
21. Configuring Cisco ASA Firewall Inspection Policiesto filter traffic based on predetermined ACLs .
22. Host Device Configurations.
23. Test and Verifying Network Communication.