Enterprise Networking

Financial Institution Network System Design and Implementation

Jubilee Financial Services Ltd (JFSL) is a well-established finance service provider in Kenya, which offers online finance solutions and services to its clients. The company operates in the country's capital city, Nairobi, and is hosted within an eleven-story building. The company primarily operates from the seventh to the eighth floors where on each floor there are at least two departments. The company has the following five departments within its main headquarter Human resource (HR), Customer Service (CS), Marketing (MK), Legal Management (LM), and Information Technology (IT). The number of users and other devices per department include;

a. Seventh Floor- HR, CS & MK; each department has at least 40 user devices plus 40 IP phones, and one WIFI-AP.
b. Eighth Floor- LM & IT; each department has at least 20 user devices plus 20 IP phones, and one WIFI-AP**. N/B**- each user can have an associated VoIP phone (but not a must).

The network infrastructure is currently run and managed by a third-party firm called Infinitive IT Systems Kenya. The senior management has decided to own its network infrastructure including Local Area Network (LAN), Wide Area Network (WAN), and an external Server-Side location connected via appropriate WAN technology with prioritizing secure communication between the HQ network and the external site. The server-side site will host DHCP, DNS, WEB, and EMAIL servers. The Company is intending to subscribe to two ISPs (Safaricom and JTL ISPs) to provide redundancy and load-balancing in terms of internet provisions. The company has also purchased two Cisco Catalyst 2911 routers (one for HQ & other for serverside) plus one gateway router Catalyst 2811 router(for HQ VoIP), two multilayer switches(both for HQ), and six access switches for the departments.

Due to security requirements, it has been decided that all five departments will be on a separate network segment within the same local area network. None of the servers is located within the local area network but will be hosted from an external site accessible via a WAN connection. The network security policy will comprehensively dictate the user access to the external site using Access Control LIST (ACL).

You have been hired as a network security engineer to design the network for Jubilee Financial Services Ltd (JFSL) according to the requirements set by the senior management. You will consult an appropriate robust network design model to meet the design requirements. You will also implement Access Control Lists and Virtual Private Networks to enable secure communication considering security and network performance factors paramount to safeguard 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 JFSL network infrastructure design and implementation. The company will be using the following IP address: 192.168.20.0/24 for Data, 10.10.10.0/24 for Voice, and 190.200.100.0 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 at every layer.
3. **ISPs-** The network is also expected to connect to at least two ISPs to provide redundancy and each router is connected to the two ISPs.
4. **WIFI-** Each department is required to have a wireless network for the users.
5. **VoIP-** Each department should have IP phones and users in the department should be able to call each other.
6. **VLAN-** Each department should be in a different VLAN and a different subnetwork. The voice VLAN ID number will remain at VID 120 for the entire network.
7. **Subnetting-** Provided the networks above, carry out subnetting to allocate the correct number of IP addresses to each department.
8. **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.
9. **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.
10. **Core Switches-** The Multilayer switches are expected to carry out both routing and switching functionalities and thus will be assigned IP addresses.
11. **DHCP Server-** All devices in the network (except IP phones) are expected to obtain an IP address dynamically from the dedicated DHCP servers located at the server-side site.
12. **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 any of the l3-switches at HQ).
13. **Static Addressing-** Devices in the server room are to be allocated IP addresses statically.
14. **Telephony Service-** Configure VoIP on the voice gateway router and allocate dial numbers in format (4..).
15. **Routing Protocol-** Use OSPF as the routing protocol to advertise routes both on the routers and multilayer switches.
16. **Switchport security-** Configure port security for the server site department switch to allow only one device to connect to a switch port, and use the sticky method to obtain mac-address and violation mode shutdown.
17. **SSH-** Configure SSH in all the routers and layer three switches for remote login.
18. **Standard ACL for SSH-** configure a simple standard ACL on the line VTY to allow only the ICT department to carry out all remote administrative tasks using SSH.
19. **NAT + ACL-** Configure PAT to use the respective outbound router interface IPv4 address, and implement the necessary ACL rule.
20. **IPsec VPN + ACL-** Configure site-to-site IPsec VPN between the HQ router and the Server-side router, and implement the necessary ACL rule.
21. **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 SSH for secure Remote access.
12. Configuring OSPF as the routing protocol.
13. Configuring Standard ACL for VTY interfaces to restrict remote Access using SSH.
14. Configuring Port Address Traslations or PAT for NAT.
15. Configuring Standard ACL for PAT.
16. Configuring VoIP or Telephony service configuration in all routers.
17. Configuring site-to-site IPsec VPN on the gateway routers.
18. Configuring Standard ACL for site-to-site IPsec VPN.
19. Host Device Configurations.
20. Test and Verifying Network Communication.