**NETWORK/INFORMATION SECURITY**

**GROUP A EXAM**

**GROUP MEMBERS**

1. **VU-BIT-2209-0716-EVE EKUDOT MOSES**
2. **VU-BIT-2209-0031-EVE NAMBOZO PHIONAH EDITH**
3. **VU-BIT-2209-0766-EVE OMOYO PETER**
4. **VU-DIT-2209-0725-EVE DRAPARI FRED**
5. **VU-BIT-2209-0719-EVE NAMAKULA MARGARET**
6. **VU-BIT-2209-0445-EVE KAMPI VINTA BALABYEKI**
7. **VU-DIT-2209-1035-EVE AJAMBO J MARY**
8. **VU-BIT-2209-0373-EVE LENKA STEPHEN**
9. **VU-BCS-2307-0392-EVE ISABIRYE GERALD**

**Answers.**

**Qn. 1**

**Network Security Measures**

1. **Device Authentication and Access Control:**

* Use 802.1X authentication for devices to ensure that only UBOS-approved tablets can access the network.
* Implement Network Access Control (NAC) to ensure that only authorized devices can connect to the network.

2**. Network Segmentation**:

* Create a separate VLAN for enumerators' tablets to segregate their traffic from other UBOS systems.
* Use Layer 3 switches or routers to implement ACLs (Access Control Lists) that restrict enumerators' access to only the Census system at the Head Office.

**3. Data Encryption:**

* Ensure that all data transmitted between the enumerators' tablets and the Census system is encrypted using VPN (Virtual Private Network) technology.
* Use SSL/TLS for securing data transmitted over the internet.

**4. Firewall and Intrusion Prevention Systems:**

* Deploy Next-Generation Firewalls (NGFW) at the perimeter of the network to inspect and filter traffic.
* Implement intrusion Detection and Prevention Systems (IDPS) to monitor and respond to suspicious activities.

**5. Secure Connectivity to Head Office:**

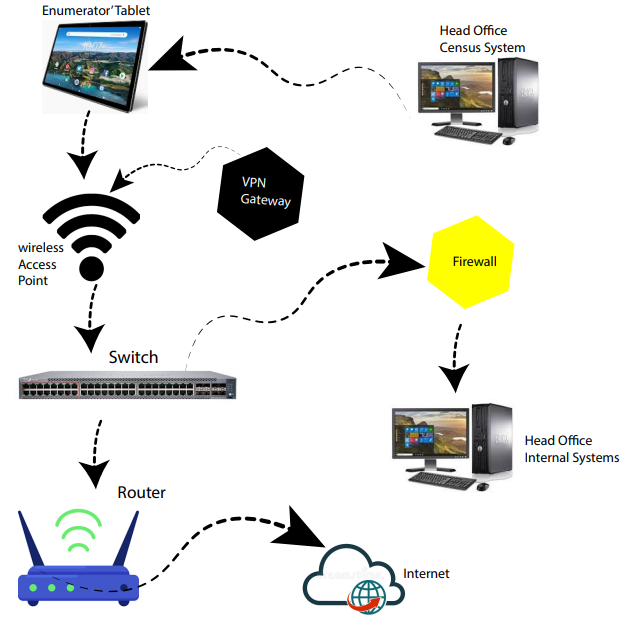
* + Use **VPN** connections from enumerators' tablets to the Head Office to ensure secure communication.

6. **Monitoring and Logging:**

* Implement centralized logging and monitoring systems using tools like SIEM (Security Information and Event Management) to detect and respond to anomalies in real-time.

**Network Diagram**

Below is a simplified network diagram illustrating the setup:



**Real-Life Vendor Devices**

1. Wireless Access Points (APs):

* Cisco Aironet 2800 Series
* Aruba 300 Series

2. Switches:

* Cisco Catalyst 9300 Series
* HPE Aruba 2930F Series

3. Firewalls:

* Palo Alto Networks PA-220
* Fortinet FortiGate 60E

4. VPN Gateway:

* Cisco ASA 5506-X with FirePOWER services
* Juniper SRX300

5. Router:

* Cisco ISR 4000 Series
* Juniper MX204

6. Monitoring and Logging:

* Splunk Enterprise
* IBM QRadar SIEM

**Explanation of Diagram Components**

**Enumerators' Tablets**: These devices connect to the wireless network using approved and authenticated devices only.

**Wireless Access Points:** Provide wireless connectivity to the tablets and enforce 802.1X authentication.

**Switch**: Connects APs to the network and supports VLANs for network segmentation.

**Firewall:** Protects the network perimeter by filtering traffic and enforcing security policies.

**Router:** Routes traffic between different network segments and the internet.

**VPN Gateway:** Ensures secure communication between enumerators and the Head Office.

**Head Office Census System:** The central system where census data is collected and processed.

**Head Office Internal Systems:** Other UBOS systems which are segmented and protected from enumerators' access.

This setup ensures that enumerators can securely and efficiently collect census data without compromising the security of other UBOS systems.

**Qn.2**

**Implementation Plan for the Data Link Layer**

**Network Design Overview**

The Data Link Layer is responsible for node-to-node data transfer and error checking. The goal is to ensure that each department can communicate efficiently and securely within the office network. For Future Architects Ltd, we'll implement a switched Ethernet LAN using devices from reputable vendors such as Cisco and HPE Aruba.

**Network Requirements:**

1**. Switches**:

* + Managed switches for each floor to handle traffic efficiently.
  + VLAN configuration to separate departmental traffic.

2**. Access Points:**

* + Wireless access points for wireless connectivity.

**3. Network Security:**

* + Basic security features like MAC address filtering and port security.

**4. Redundancy:**

* Ensure network uptime with redundant links and switches.

**Implementation Plan**

Step 1**: Hardware Selection**

**Switches:**

- Cisco Catalyst 9200 Series 24-Port Switches

- One switch per floor for connectivity and management.

- Supports VLANs, PoE (Power over Ethernet) for access points, and high-speed uplinks.

**Access Points:**

- HPE Aruba AP-515

- Dual-band wireless access points for comprehensive wireless coverage.

- Supports the latest Wi-Fi standards and security protocols.

**Cabling:**

- Cat6 Ethernet cables for all wired connections.

Step 2**: Network Design and VLAN Configuration**

**1. First Floor Layout:**

- Departments: Customer Relations, ICT, Sales

- Devices connected to a Cisco Catalyst 9200 Switch.

- VLANs:

- VLAN 10: Customer Relations

- VLAN 20: ICT

- VLAN 30: Sales

2. **Second Floor Layout:**

- Departments: Finance, Procurement, HR

- Devices connected to a Cisco Catalyst 9200 Switch.

- VLANs:

- VLAN 40: Finance

- VLAN 50: Procurement

- VLAN 60: HR

Step 3**: Physical Setup**

1. **Switch Placement:**

- Place switches in secure locations on each floor (e.g., network closets).

2. **Cabling:**

- Run Cat6 cables from the switch to each department’s network points.

- Ensure proper labeling and documentation of all connections.

3. **Access Point Placement:**

- Install Aruba AP-515 access points strategically to cover all office areas.

- Connect access points to switches using PoE.

Step 4: **Configuration**

1. **Switch Configuration:**

- Assign IP addresses to switches for management.

- Create VLANs and assign ports to respective VLANs.

- Configure inter-VLAN routing if needed for inter-department communication.

- Enable security features like port security and MAC address filtering.

2. **Access Point Configuration:**

- Configure SSIDs for wireless access.

- Set up WPA3 encryption for secure wireless connections.

- Enable client isolation to enhance security.

Step 5: **Testing and Documentation**

1. **Testing:**

- Test connectivity for wired and wireless devices.

- Verify VLAN segmentation and inter-VLAN routing.

- Ensure all security measures are functioning correctly.

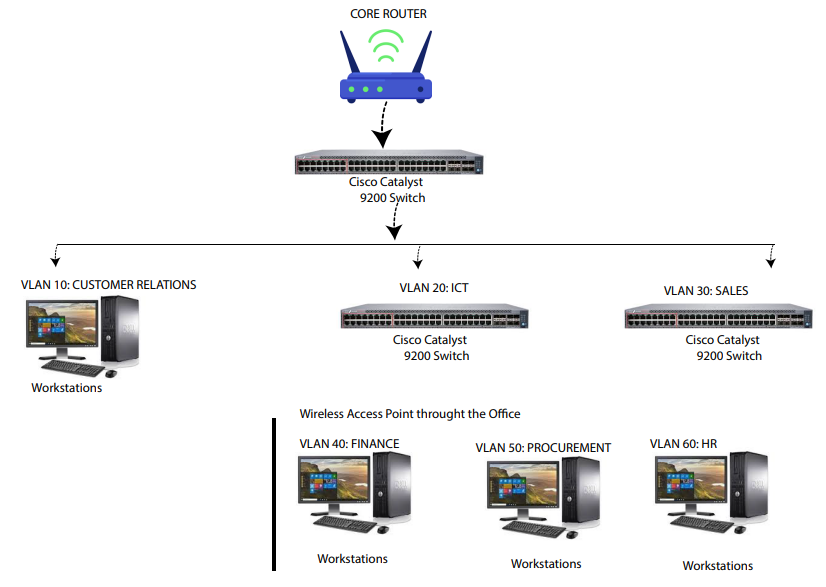
2. **Documentation:**

- Document the network design, IP address scheme, VLAN configuration, and device settings.

- Provide a network diagram showing the layout and connections.

**Network Diagram**

Here's a simplified network diagram for Future Architects Ltd:



This implementation plan ensures that Future Architects Ltd's network is robust, secure, and efficient. Using high-quality Cisco and Aruba devices guarantees reliability and performance. Proper VLAN segmentation and security measures ensure that departmental communications are isolated and protected, promoting both performance and security.

**Qn. 3**

**How a Firewall Works**

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted network and an untrusted network, such as the internet. Here's how three key features of a firewall fit into the different layers of the OSI model:

1. **Packet Filtering (Network Layer)**

**Description:** Packet filtering is one of the most fundamental features of a firewall. It involves inspecting each packet that passes through the firewall and accepting or rejecting it based on user-defined rules. These rules can include criteria such as IP addresses, port numbers, and protocols.

**Corresponding Layer**: This feature operates at the Network Layer (Layer 3) of the OSI model. At this layer, packet filtering examines the header information of IP packets to make filtering decisions.

**Example Use:** Blocking all incoming traffic from a specific IP address to prevent a known threat from entering the network.

**2. Stateful Inspection (Transport Layer)**

**Description**: Stateful inspection, also known as dynamic packet filtering, tracks the state of active connections and makes decisions based on the context of the traffic. Unlike simple packet filtering, which only looks at individual packets, stateful inspection monitors the state of network connections such as TCP streams.

**Corresponding Layer**: This feature operates at the Transport Layer (Layer 4) of the OSI model. At this layer, the firewall keeps track of TCP and UDP sessions, ensuring that packets are part of an established connection or a new, legitimate connection.

**Example Use**: Allowing return traffic from an external server only if it is part of an already established session initiated by an internal user.

**3. Deep Packet Inspection (Application Layer)**

**Description**: Deep packet inspection (DPI) involves examining the data part (and possibly the header) of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or predefined criteria to decide whether the packet may pass or if it needs to be routed to a different destination.

**Corresponding Layer**: This feature operates at the Application Layer (Layer 7) of the OSI model. At this layer, DPI analyzes the payload of packets for content-based filtering and application-level threats.

**Example Use**: Blocking specific types of web traffic (such as HTTP traffic containing malware signatures) while allowing legitimate traffic through.

**Proposed Firewall Models**

**1. Cisco Firepower 2100 Series**

Supplier: Cisco Systems

**Features:**

* + Next-Generation Intrusion Prevention System (NGIPS): Provides advanced threat detection and prevention capabilities.
  + Application Visibility and Control (AVC): Allows the identification and control of over 4000 applications traversing the network.
  + Advanced Malware Protection (AMP): Detects, blocks, and remediates malware across the network.

**Suitability**: Cisco Firepower 2100 Series integrates state-of-the-art security features such as NGIPS and AMP, providing comprehensive protection against modern threats. It is well-suited for environments that require robust security and extensive application visibility and control.

**2. Fortinet FortiGate 6000F Series**

Supplier: Fortinet

**Features:**

* + FortiGuard Security Services: Offers real-time threat intelligence from Fortinet's global security research team.
  + High-Performance SSL Inspection: Decrypts and inspects SSL/TLS traffic without impacting network performance.
  + Integrated SD-WAN: Enhances network performance and security across distributed networks with integrated Secure SD-WAN capabilities.

**Suitability**: Fortinet FortiGate 6000F Series is ideal for large enterprises and institutions like universities due to its high-performance capabilities and integrated security features. Its advanced SSL inspection and SD-WAN integration make it an excellent choice for complex network environments.

**Qn. 4**

**Network Report for Victoria University's Gulu Campus**

**1. Introduction**

Victoria University’s new campus in Gulu aims to support 3000 students, 700 computers in ICT labs, and 100 staff members. Establishing a robust and secure network infrastructure is critical for the campus's operational efficiency and security. This report outlines the necessary network devices, provides a network diagram, and recommends security technologies to protect the network at each stage.

**2. Network Devices Required**

1. Routers

- Function: Route data between the Gulu campus and the main campus via VPN.

- Security: Implement access control lists (ACLs) to filter traffic.

2. Switches

- Function: Connect multiple devices within the campus network.

- Security: Use managed switches with VLAN support to segment the network.

3. Firewalls

- Function: Monitor and control incoming and outgoing network traffic.

- Security: Deploy next-generation firewalls (NGFW) for deep packet inspection and intrusion prevention.

4. Wireless Access Points (APs)

- Function: Provide wireless network connectivity for students and staff.

- Security: Use APs with WPA3 encryption and 802.1X authentication.

5. VPN Gateway

- Function: Securely connect the Gulu campus to the main campus.

- Security: Use IPsec or SSL VPN protocols with strong encryption.

6. Network Servers

- Function: Provide services such as DHCP, DNS, and authentication.

- Security: Harden servers against attacks, use secure configurations, and implement regular patch management.

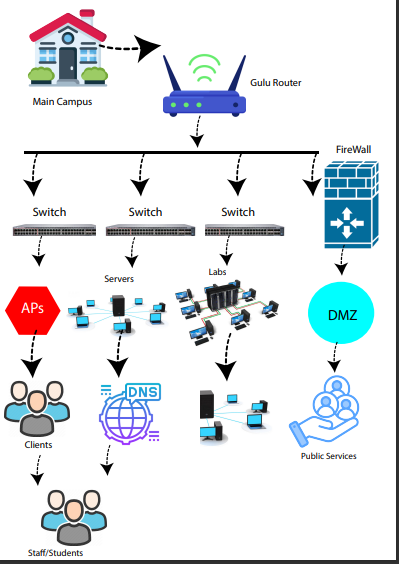
7. Uninterruptible Power Supplies (UPS)

- Function: Provide backup power to network devices.

- Security: Ensure continuous operation during power outages to maintain security controls.

3**. Network Diagram**

Below is a high-level network diagram for the Gulu campus.



**4. Network Security Technologies**

**1. Routers**

- ACLs: Control access to network resources by defining which users or devices can connect to different parts of the network.

- Encryption: Use encrypted protocols (e.g., IPSec) for secure data transmission.

**2. Switches**

- VLANs: Segment network traffic to isolate sensitive areas from general access areas.

- Port Security: Limit the number of devices that can connect to a switch port.

3. **Firewalls**

- NGFW: Provide advanced security features such as application awareness, intrusion prevention, and threat intelligence.

- DMZ: Create a demilitarized zone for public-facing services, adding an additional layer of protection.

4. **Wireless Access Points**

- WPA3 Encryption: Ensure data transmitted over the wireless network is encrypted.

- 802.1X Authentication: Authenticate users before granting access to the wireless network.

5. **VPN Gateway**

- IPSec/SSL VPN: Securely encrypt data traveling between the Gulu campus and the main campus.

- Multi-Factor Authentication (MFA): Add an additional layer of security for remote access.

**6. Network Servers**

- Hardening: Disable unnecessary services, apply security patches regularly, and configure firewalls.

- Antivirus and Anti-malware: Protect against malicious software.

7. General Security Measures

- Network Monitoring and Intrusion Detection Systems (IDS/IPS): Monitor network traffic for suspicious activity and respond to threats.

- Regular Audits and Penetration Testing: Assess network security regularly to identify and fix vulnerabilities.

- Security Awareness Training: Educate staff and students on best practices for network security.

**5. Conclusion**

Implementing the outlined network devices and security technologies will ensure that Victoria University’s Gulu campus has a robust and secure network infrastructure. This will support the operational needs of the students, staff, and ICT labs while protecting against potential security threats.