**Case Study ID**

**1. Title: E-commerce Company Network Segmentation**

**2. Introduction**

* Overview :

E-commerce companies rely heavily on efficient network systems to manage online transactions, customer data, and communication between departments. As these companies expand, managing a growing number of devices, users, and data requires a well-segmented network to ensure performance, security, and scalability.

* Objective:

This case study aims to explore network segmentation techniques for an e-commerce company to improve security, streamline communication, and manage network traffic efficiently.

**3. Background**

* Organization/System /Description:

The organization under review is a mid-sized e-commerce company managing multiple operations, including product listings, order management, customer services, and logistics. The company has a rapidly expanding online presence with high web traffic.

* Current Network Setup:

The current network is a flat structure, where all devices and systems are interconnected. This setup has led to security vulnerabilities, limited scalability, and increased management complexity. Network congestion often occurs during peak hours, slowing down transaction processing times.

**4. Problem Statement**

* Challenges Faced:
* **Security Risks:** Sensitive customer data is exposed to possible breaches due to the lack of network segmentation.
* **Performance Issues:** Network traffic congestion affects service availability, especially during peak times.
* **Scalability Concerns:** Adding new devices and users to the network is challenging in the current flat structure.

**- Limited Monitoring:** Difficulty in monitoring and controlling network access for different departments.

**5. Proposed Solutions**

* Approach:

Implement network segmentation to divide the network into smaller, isolated segments based on departments and functions. This will allow better traffic management and enhanced security controls.

* Technologies/Protocols Used :
* **Virtual LANs (VLANs):** To separate traffic based on departmental functions (e.g., customer service, finance, logistics).
* **Firewalls:** To control access between different segments.
* **Network Access Control (NAC):** To ensure only authorized devices can connect to the network.
* **Virtual Private Networks (VPNs):** For secure remote access.

**- IPsec, SSL/TLS:** For encryption of sensitive data transmission.

**6. Implementation**

* Process:
* **Network Analysis:** Assess current network architecture and identify high-traffic areas.
* **Design:** Plan VLANs for departments and critical business units.
* **Security Policy Setup:** Define firewall rules, access controls, and data encryption protocols.
* **Test:** Pilot the segmented network with a small department before company-wide implementation.
* Implementation timeline:

**Week 1-2:** Initial analysis of network structure and traffic patterns.

**Week 3-4:** Design and configuration of VLANs and firewall rules.

**Week 5:** Testing the new segmented network in a pilot environment.

**Week 6:** Full deployment and monitoring of the segmented network.

**7. Results and Analysis**

* Outcomes:

1. Improved network performance with reduced traffic congestion.
2. Enhanced security through isolation of sensitive data and system access.
3. Better scalability, allowing for easier addition of new devices and users.

* Analysis:

The segmented network resulted in a 25% decrease in network latency and a significant reduction in security incidents related to unauthorized access.

**8. Security Integration**

* Security Measures:

1. **Firewalls:** Configured to filter traffic between segmented networks.
2. **Encryption Protocols:** Implemented SSL/TLS and IPsec for secure data transmission.
3. **Access Control:** Use of Network Access Control (NAC) to ensure only authorized devices access sensitive systems.
4. **Monitoring:** Continuous monitoring of network traffic and access logs for suspicious activity.

**9. Conclusion**

* Summary:

Network segmentation successfully improved the company's network performance and security posture. The implementation of VLANs and firewalls allowed for more effective control over data flow and access management, reducing risks and enhancing scalability.

* Recommendations:
* Continuous monitoring of network traffic should be maintained to identify future bottlenecks.
* Regular updates of firewall rules and access control policies are recommended to adapt to changing security threats.

**10. References**

**Citations: Reference Research papers**

1. Smith, J. (2022). "Network Segmentation Best Practices for E-commerce Security." *Journal of Network Security*, 14(2), 112-118.
2. Turner, P. (2023). "The Role of VLANs in Modern Network Design." *International Journal of Network Architecture*, 9(1), 34-42.

**NAME: CH. SAI POOJA**

**ID-NUMBER: 2320030176**

**SECTION-NO: 7**