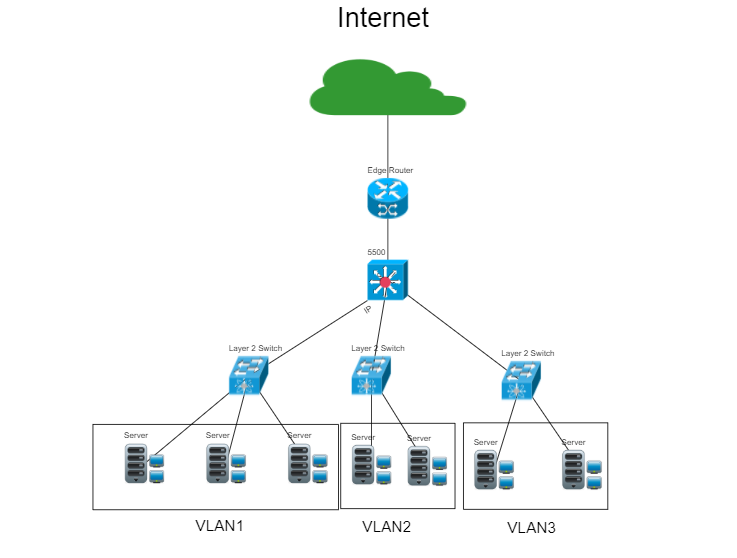
|  |  |  |
| --- | --- | --- |
| SCHOOL OF INFORMATION AND TECHNOLOGY | | |
| NAME: Magno, Ronnie L. Sueno, Johnray K. | DATE PERFORMED: 12/05/24 | /50 |
| Section: IDC2 | DATE SUBMITTED: 12/05/24 |

**Part 2. Network Scalability Analysis**

Recall the e-commerce website scenario we discussed earlier. Given the expected surge in traffic, analyze the provided network topology diagram. Identify potential bottlenecks and areas where scalability might be a concern. Propose specific strategies to improve the network's scalability and performance to ensure a seamless user experience during the peak traffic period. Consider factors such as increased user demand, new applications, and security threats.



**Potential Bottlenecks:**

* **Bandwidth Constraints on Uplinks:** The uplinks connecting Layer 2 switches to the Core Switch or the Core Switch to the Edge Router might not have sufficient bandwidth, especially if they are using older technologies like 1 Gbps Ethernet, limiting the overall throughput and causing delays during peak traffic.
* **Lack of Redundancy:** The network lacks redundant links between critical components such as routers, switches, and servers. A single point of failure, such as a broken link or hardware malfunction, could lead to significant downtime and service disruption.
* **Scalability Limits:** As user demand grows, the current architecture may not support adding more devices or servers without significant reconfiguration. Limited capacity in the current switch model could also restrict the ability to scale VLANs or handle additional traffic efficiently.
* **Inter-VLAN Traffic Congestion:** High inter-VLAN traffic would rely heavily on the Core Switch for routing, increasing its load and reducing performance. This issue can become particularly problematic if applications or services in different VLANs communicate frequently.
* **Security Vulnerabilities (No Firewalls)**:

Without firewalls, the network is directly exposed to external threats through edge routers. The lack of traffic filtering or inspection creates the following risks:

1. **External Attacks**: Vulnerability to unauthorized access, malware, and DDoS attacks.
2. **Internal Threats**: Devices within one VLAN can potentially compromise devices in other VLANs if ACLs and VLAN isolation are not effectively configured.
3. **Unrestricted Traffic**: Inbound and outbound traffic are not thoroughly inspected, allowing malicious packets to traverse the network undetected.

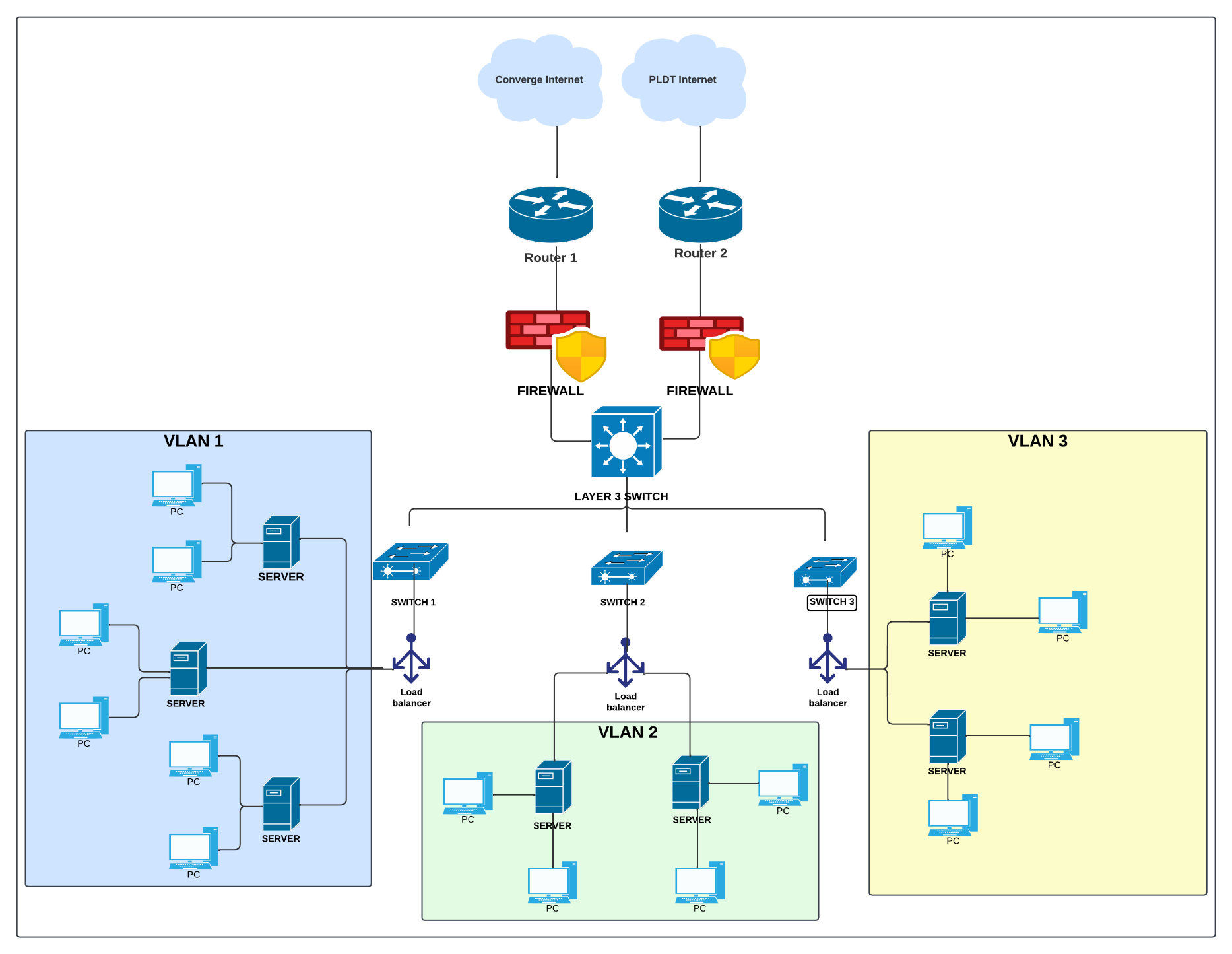
* **Security Processing Delays:** Increased security processing for monitoring and filtering traffic in a high-demand environment can slow down packet forwarding and response times if security measures like intrusion detection/prevention systems are not scaled appropriately. The absence of firewalls places a greater burden on edge routers to handle basic security tasks like ACLs and intrusion detection. If these systems are not scaled appropriately, they can slow down packet forwarding and response times.

**SOLUTION:**

To improve the scalability and performance of the network, several strategies are recommended, focusing on both hardware enhancements and software configurations. First, the deployment of dual edge routers connected to Converge and PLDT ISPs with failover capabilities ensures reliable internet connectivity. This setup minimizes the risk of downtime by providing load balancing and redundancy, effectively addressing potential failures. The existing Layer 3 core switch will remain central to the network, handling inter-VLAN routing efficiently without the need for upgrading the Layer 2 access switches. To further enhance network performance, high-speed 10Gbps uplinks should be implemented between the core switch and both the edge routers and the Layer 2 access switches. These uplinks will accommodate increased traffic volumes, reducing congestion and ensuring faster data transfers, especially during peak periods.

Load balancing is crucial for VLAN 1, where multiple servers handle user requests. Installing load balancers will distribute traffic evenly among the servers, preventing overload and improving response times. Security is also a priority, and the addition of redundant firewalls between the edge routers and the core switch will protect the network from external threats. Also, VLAN isolation and the implementation of Access Control Lists (ACLs) on the Layer 3 core switch will safeguard sensitive resources and restrict unauthorized access. To proactively monitor and manage network performance, integrating tools like SNMP will enable real-time tracking, allowing IT personnel to identify and address potential bottlenecks promptly.

While these strategies significantly improve scalability, reliability, and performance, they also present challenges. Upgrades such as 10Gbps uplinks, load balancers, and firewalls involve considerable costs, which may affect limited budgets. Additionally, the increased complexity of managing redundant systems, load balancers, and monitoring tools requires skilled IT staff to ensure smooth operations. Despite these challenges, this proposed design effectively prepares the network for future growth and peak traffic demands while maintaining a secure and reliable infrastructure.

**Proposed Network Design**

|  |  |  |  |
| --- | --- | --- | --- |
| Criteria | Excellent | 10pts | Good | 7pts | Needs Improvement | 4pts |
| **Network Analysis** | Accurately identifies potential bottlenecks, security risks, and capacity limitations. | Identifies key network components and some potential bottlenecks. | Identifies some basic network components but lacks a comprehensive analysis. |
| **Scalability Planning** | Proposes multiple relevant solutions and provides detailed explanations, including potential drawbacks and benefits. | Proposes some relevant scalability strategies but lacks detail. | Proposes limited scalability strategies. |
| **Evaluation of Solutions** | Proposes comprehensive scalability strategies, including specific recommendations for hardware upgrades, software configurations, and network optimizations. | Provides a basic evaluation of the proposed solutions, but lacks depth. | Does not evaluate the proposed solutions or provides a superficial evaluation. |
| **Proposed Design** | Provides a detailed and well-justified design, including network diagrams, configuration details, and implementation plans. | Provides a basic design but lacks specific details and justifications. | Does not provide a clear and detailed design. |
| **Evaluation and Justification** | Provides a thorough evaluation of the proposed solutions, considering factors like cost, complexity, and potential impact. | Provides a basic evaluation of the proposed solutions, but lacks depth. | Does not evaluate the proposed solutions or provides a superficial evaluation |
| Score: | | | /50 |