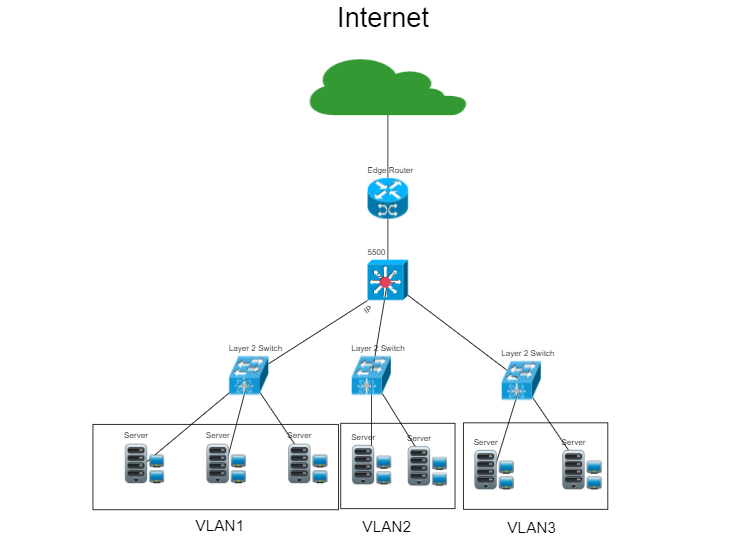
| SCHOOL OF INFORMATION AND TECHNOLOGY | | |
| --- | --- | --- |
| NAME: Patrick John M. Lansangan  Zhaun Gabrielle F. Pasion | DATE PERFORMED: 28/11/2024 | /50 |
| Section: IDC2 | DATE SUBMITTED: 5/12/2024 |

# SYSADM1 – Capacity Management & Planning

# **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.



### 

### 

### 

### 

### **Network Analysis**

#### **Potential Bottlenecks**

1. **Router and Multilayer Switch**:

* A single router or multilayer switch can become a bottleneck during peak traffic as all traffic flows through these devices.
* The 1Gbps bandwidth of the switch and router may not suffice when handling aggregated traffic from multiple servers and clients.

1. **Switch-to-Server Connections**:

* With each switch connecting 3 servers and 3 PCs, the uplink to the router (likely at 1Gbps) might struggle to handle simultaneous peak traffic from multiple users.
* Server connections may be constrained by the 1Gbps network bandwidth, particularly during high-traffic events or data-heavy operations

1. **Servers**:

* Limited to 5 servers, each with 8 CPU cores, 32GB RAM, and 1 Gbps bandwidth, the infrastructure may not support 5x traffic increases without performance degradation.

#### **Security Risks**

1. **Potential Cyber Threats**:

* Increased visibility during the holiday sale and the marketing campaign makes the network a target for Distributed Denial-of-Service (DDoS) attacks, phishing attempts, or unauthorized access.

1. **Insufficient Segmentation**:

* Without robust VLANs or firewalls, malicious traffic can propagate across servers and PCs.

1. **Lack of Intrusion Detection**:

* The topology doesn’t highlight any security measures such as firewalls, intrusion detection systems (IDS), or intrusion prevention systems (IPS).

#### **Capacity Limitations**

1. **CPU and RAM**:

* Limited scalability if application and database loads significantly increase.

1. **Bandwidth**:

* 1Gbps links are likely insufficient under high traffic, particularly if traffic spikes align with large file downloads or streaming.

### **Scalability Planning**

**1. Utilize Triple ISP Connections**

**Action**:

* Route external traffic dynamically across three ISPs using Border Gateway Protocol (BGP) for failover and load balancing.

**Benefits**: Eliminates dependency on a single ISP, ensuring continuous availability.

* Ensures high availability and uninterrupted service by eliminating dependency on a single ISP.
* Dynamically reroutes traffic during ISP outages or performance issues.

**Drawbacks**:

* Requires advanced BGP configuration expertise.
* Coordination with ISPs for proper implementation can be time-consuming.

##### 2. Add a Second Multilayer Switch

**Action**:

* Deploy a second multilayer switch and configure link aggregation (EtherChannel/LACP) to balance internal traffic and add redundancy.
* Ensure dynamic routing protocols like OSPF or EIGRP are configured for efficient traffic handling.

**Benefits**:

* Distributes traffic across multiple switches, preventing congestion and offering fault tolerance.
* Improves resiliency and enables seamless failover if one switch fails.

**Drawbacks**:

* Requires proper configuration of inter-switch links and protocols to avoid traffic loops or inefficiencies.
* Increases hardware costs.

##### 3. Introduce a Load Balancer

**Action**:

* Deploy a load balancer to distribute incoming traffic across existing servers.
* Configuring GLBP for Multilayer Switch load balancing and redundancy.

**Benefits**:

* Prevents any single server from becoming overwhelmed, improving response times and reliability.
* Provides flexibility for scaling by adding more servers behind the load balancer.

**Drawbacks**:

* May require regular monitoring and fine-tuning to ensure optimal traffic distribution.
* Adds complexity to the network.

##### 4. Implement firewall and IDS/IPS

**Action**:

* Add a perimeter firewall between the ISP and the router to inspect incoming and outgoing traffic.
* Integrate a multilayer firewall after the router, before the switches, to segment and protect internal traffic between VLANs (e.g., between servers and PCs).
* Configure firewall rules to allow only authorized traffic while blocking malicious or unnecessary connections.
* Add IDS/IPS for monitoring traffic going in and out of the network segments.

**Benefits**:

* The perimeter firewall protects against external threats such as DDoS attacks and unauthorized access.
* The multilayer firewall isolates internal segments, ensuring malicious traffic cannot spread across VLANs.
* Granular control over network traffic using stateful inspection and application-aware filtering.
* Allows monitoring of traffic patterns to detect and block anomalies or attacks in real time.
* Helps ensure adherence to security policies and regulations
* Secures sensitive data on servers from unauthorized internal or external access.

**Drawbacks**:

* Managing multiple firewalls requires proper configuration and monitoring to avoid misconfigurations that could block legitimate traffic.
* Firewalls introduce additional processing overhead, which could cause latency, especially during high-traffic events.
* Hardware and software firewalls, especially enterprise-grade solutions, may require significant investment.
* Regular updates, tuning of rules, and log analysis require skilled personnel to prevent vulnerabilities.

### **Evaluation of Solutions**

#### **1. Triple ISP Connections**

* **Comprehensive Scalability Strategy**:
  + **Hardware Upgrade**: Implement three ISP connections using enterprise-grade routers that support dynamic routing with BGP (e.g., Cisco ASR Series or Juniper MX Series routers).
  + **Software Configuration**: Configure BGP for automatic failover and load balancing across the three ISPs. Set up monitoring tools like SolarWinds to track ISP performance and reroute traffic if necessary.
  + **Network Optimization**: Use Quality of Service (QoS) to prioritize traffic for critical operations, particularly during high-traffic periods like the holiday sale.
* **Justification**: By utilizing multiple ISPs, the network ensures continuous availability and a reduced risk of service disruption during peak traffic periods. It prevents reliance on a single ISP and provides redundancy in case of ISP failure.  
  **Cost and Complexity**:
  + **Cost**: High initial investment for BGP configuration and ISP setup.
  + **Complexity**: Requires skilled network engineers to configure and manage BGP routing and ISP coordination. Ongoing management to ensure redundancy and performance.

#### **2. Add a Second Multilayer Switch**

* **Comprehensive Scalability Strategy**:
  + **Hardware Upgrade**: Add a second high-performance multilayer switch (e.g., Cisco Catalyst 9000 series) to balance traffic and ensure redundancy.
  + **Software Configuration**: Configure link aggregation (EtherChannel/LACP) to combine multiple physical links, and deploy dynamic routing protocols like OSPF or EIGRP to ensure efficient traffic distribution.
  + **Network Optimization**: Enable VLAN segmentation to reduce broadcast domains and ensure faster communication within the network.
* **Justification**: The second switch improves redundancy, prevents traffic congestion, and enhances the overall reliability of the network, ensuring that internal traffic is balanced effectively.  
  **Cost and Complexity**:
  + **Cost**: Medium-to-high hardware cost, particularly for high-performance switches.
  + **Complexity**: Moderate complexity for configuration and management of dynamic routing and EtherChannel, requiring network expertise.

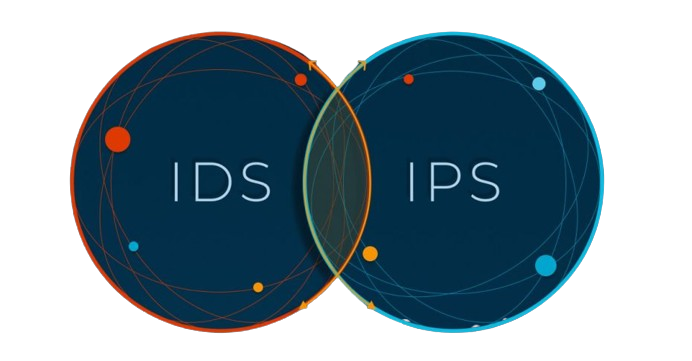
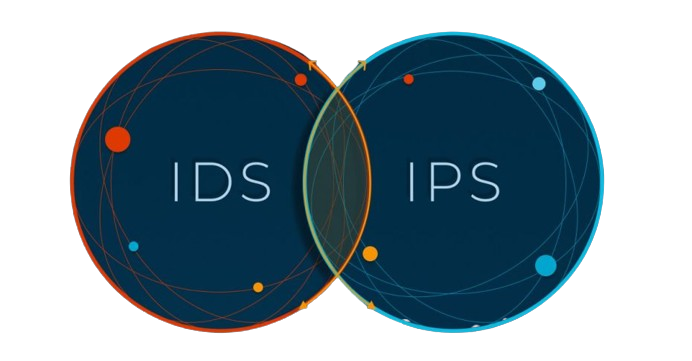
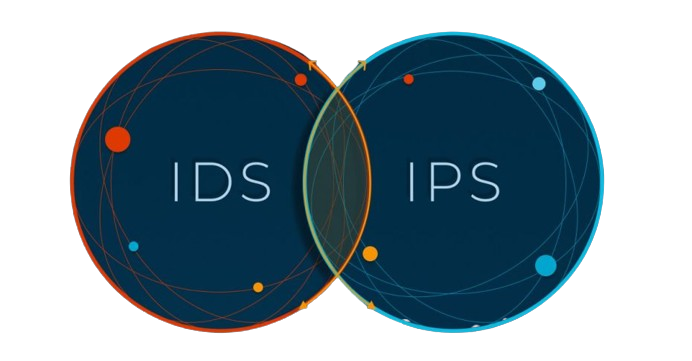
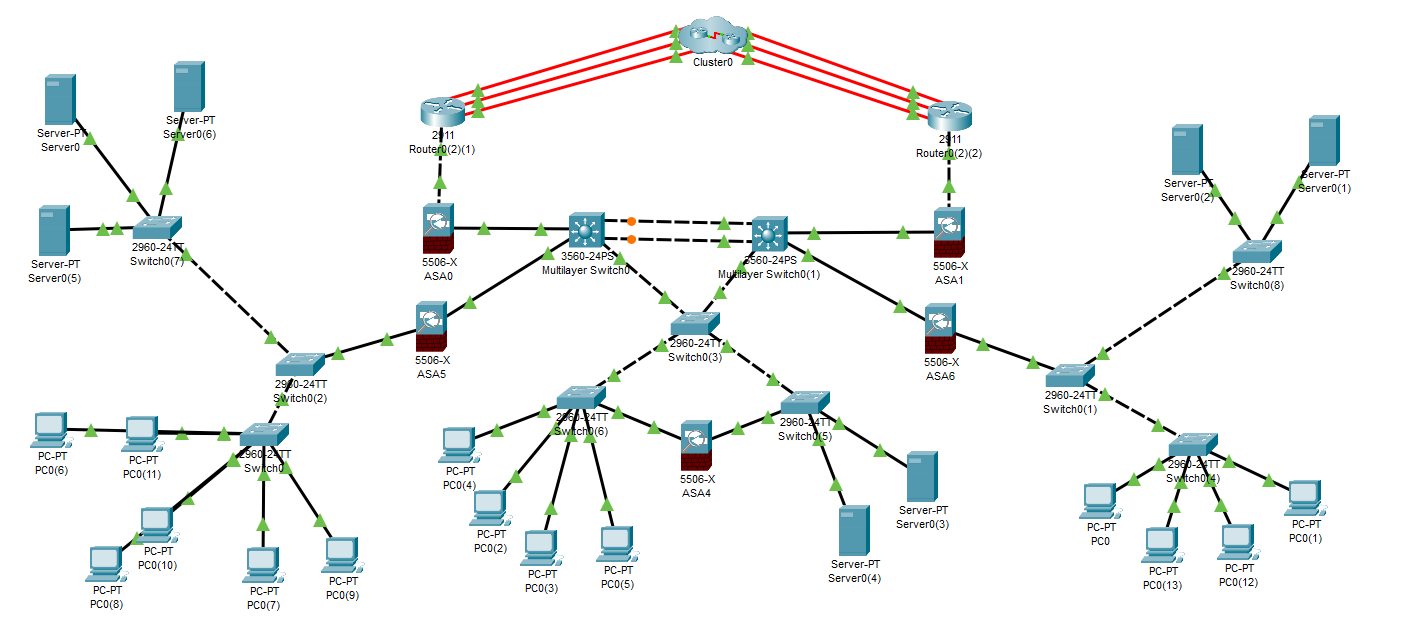
#### **3. Application-Level Load Balancer**

* **Comprehensive Scalability Strategy**:
  + **Hardware/Software Upgrade**: Deploy a dedicated load balancer (e.g., F5 BIG-IP or Citrix ADC) or use software load balancers like HAProxy or NGINX Plus.
  + **Software Configuration**: Implement server health-checks and SSL termination on the load balancer to offload CPU-intensive tasks from the servers.
  + **Network Optimization**: Configure the load balancer to distribute incoming traffic evenly across the servers, ensuring no server is overwhelmed.
* **Justification**: Load balancing optimizes server utilization, ensuring a smooth user experience during peak periods by distributing traffic evenly. SSL offloading improves server efficiency by reducing the encryption load.  
  **Cost and Complexity**:
  + **Cost**: The cost of dedicated hardware load balancers can be high, but software options like HAProxy offer a more affordable solution.
  + **Complexity**: Moderate complexity; load balancer setup requires proper configuration and ongoing monitoring to maintain optimal performance.

#### **4. Implement Firewalls and IDS/IPS**

* **Comprehensive Scalability Strategy**:
  + **Hardware Upgrade**: Deploy next-generation firewalls (NGFW) at critical network junctures—perimeter firewall between ISP and router, and multilayer firewalls between routers and internal switches.
  + **Software Configuration**: Set up application-aware filtering, intrusion detection/prevention systems (IDS/IPS), and access control policies.
  + **Network Optimization**: Implement firewall rules to protect critical internal services, ensuring that only authorized traffic is allowed and filtering out malicious traffic.
* **Justification**: Firewalls enhance network security by filtering traffic, preventing unauthorized access, and protecting against cyberattacks such as DDoS during high-traffic events.  
  **Cost and Complexity**:
  + **Cost**: Firewalls, especially next-gen devices, can be costly, both in terms of hardware and software licenses.
  + **Complexity**: Firewalls require careful configuration and ongoing management to avoid misconfigurations, which could block legitimate traffic.

### **Proposed Design**



#### **Implementation Plan**

##### Phase 1: Core Layer Implementation

* Configure the multilayer switches to enable inter-VLAN routing.
* Establish redundant connections between the two multilayer switches for high availability.
* Connect the routers (e.g., Router 2(1) and Router 2(2)) to the multilayer switches for internet and WAN connectivity.

##### Phase 2: Distribution Layer Implementation

* Deploy ASA firewalls between the core and access layers.
* Configure firewalls with security policies for VLAN traffic filtering and VPN connections.
* Ensure dual connections to the multilayer switches for redundancy.

##### Phase 3: Access Layer Implementation

* Connect endpoint devices (PCs and servers) to the access switches.
* Assign appropriate VLANs to the access ports based on device type (e.g., PCs in VLAN 10, servers in VLAN 20).
* Uplink access switches to the distribution layer firewalls.

##### Phase 4: Testing and Validation

* Test connectivity between devices in the same and different VLANs.
* Validate security policies on the firewalls to ensure proper traffic filtering.
* Simulate failure scenarios to test redundancy

### **Evaluation and Justification**

#### **1. Cost Analysis:**

* **Triple ISP Connections**: High initial cost for BGP configuration and enterprise-grade routers, as well as ongoing ISP fees.
* **Second Multilayer Switch**: Medium cost for an additional switch and hardware for link aggregation.
* **Application-Level Load Balancer**: High cost for hardware-based load balancers (F5), or moderate cost for software solutions like HAProxy.
* **Firewalls**: High upfront cost for next-generation firewalls, along with ongoing maintenance and software updates.

#### **2. Complexity:**

* **Triple ISP Connections**: Requires skilled network professionals to configure BGP and manage ISP coordination.
* **Second Multilayer Switch**: Configuration complexity includes managing link aggregation, VLANs, and dynamic routing.
* **Application-Level Load Balancer**: Complexity arises in configuring server health checks, SSL offloading, and traffic distribution.
* **Firewalls**: Firewalls require careful configuration, continuous monitoring, and regular updates to ensure security.

#### **3. Potential Impact:**

* **Scalability**: The proposed solutions enhance scalability by ensuring that the network can handle a significant increase in traffic. Triple ISP connections ensure availability, while the second switch and load balancer improve internal and external traffic management.
* **Security**: The firewall implementation significantly reduces the risk of cyber threats such as DDoS attacks and unauthorized access.
* **Performance**: The load balancer and multilayer switches optimize network performance by distributing traffic and reducing congestion.

#### **4. Risk Mitigation:**

* **Redundancy**: The dual ISP, switch, and firewall configurations minimize the risk of service disruption due to hardware failures or external attacks.
* **Security Threats**: Firewalls, IDS/IPS systems, and network segmentation reduce the likelihood of security breaches.

| 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 |