**Case Study ID: 70**

**1. Title Securing IPv6 Traffic with Advanced Firewall ACL Policies**

**2. Introduction**

**• Overview: This case study examines the security concerns associated with unauthorized IPv6 traffic as a company transitions to IPv6.**

**• Objective: To propose a solution to secure IPv6 traffic and ensure only authorized communication is permitted.**

**3. Background**

**• Organization/System Description:**

* **A company is transitioning to IPv6 to take advantage of the increased address space and improved security features. • Current Network Setup:**
* **The company's current network setup lacks adequate security measures to control IPv6 traffic, leaving it vulnerable to security threats.**

**4. Problem Statement**

**• Challenges Faced:**

* **The company faces security concerns with unauthorized IPv6 traffic, which can lead to security breaches and vulnerabilities.**

**5. Proposed Solutions**

**• Approach:**

* **Implement advanced firewall ACL policies to control both inbound and outbound IPv6 traffic. • Technologies/Protocols Used:**
* **Firewall ACL policies, IPv6 protocol.**

**6. Implementation**

**• Process:**

* **Configure advanced firewall ACL policies to regulate IPv6 traffic. • Implementation:**
* **Implement the policies on the company's network infrastructure. • Timeline:**
* **The implementation timeline will depend on the complexity of the network setup and the resources available.**

**7. Results and Analysis**

**• Outcomes:**

* **The implementation of advanced firewall ACL policies is expected to result in:**
  + **Secured IPv6 traffic**
  + **Reduced security risks**
  + **Improved network visibility • Analysis:**
* **The solution will provide an additional layer of security, protecting the company's network from potential security threats and vulnerabilities associated with unauthorized IPv6 traffic.**

**8. Security Integration**

**• Security Measures:**

* **The advanced firewall ACL policies will provide an additional layer of security, ensuring that only authorized IPv6 traffic is permitted.**

**9. Conclusion**

**• Summary:**

* **The proposed solution to implement advanced firewall ACL policies is a sound approach to address the security concerns of unauthorized IPv6 traffic as the company transitions to IPv6. • Recommendations:**
* **Regularly review and update the firewall ACL policies to ensure they remain effective in securing IPv6 traffic.**

**10. References**

* **RFC 4291: IP Version 6 Addressing Architecture (Hinden, R., & Deering, S. (2006))**
* **IPv6 Security: A Guide to Implementing IPv6 Securely (Chittimaneni, K. (2017))**
* **NIST Special Publication 800-119: Guidelines for the Secure Deployment of IPv6 (Frankel, S., & Owens, R. (2010))**
* **Cisco Systems: IPv6 Security Design Guide (Cisco Systems, 2020)**

**NAME: SAI TEJA AMBHILIGE**

**ID-NUMBER: 2320090077**

**SECTION-NO: 1**