University of the People

CS4404 Advanced Networking and data security

Unit 7 Written Assignment 7

Anonymous Student

**Introduction**

By incorporating strong security strategies into the WAN design for the financial institution, the sensitive financial data can be effectively protected from unauthorized access, interception, and tampering.

**Three Security Strategies**

When designing a wide area network (WAN) for a financial institution to protect sensitive data, it is crucial to incorporate robust security strategies. Three key security strategies to consider are:

1. Encryption Protocols and Access Control and Authentication Mechanisms: Implementing strong encryption protocols such as AES (Advanced Encryption Standard) for data transmitted over the WAN is essential. Encryption ensures that sensitive financial data remains secure during transit, making it significantly more difficult for unauthorized parties to intercept and decipher the information. When comes to wireless network security protocol, it necessary to use the higher version of Wifi protected access (WPA) to better security.
2. Utilizing strong access control and authentication mechanisms is vital for protecting sensitive financial data within the WAN. This involves implementing multi-factor authentication (MFA)(*Multi-Factor Authentication (MFA) for SonicWall WAN GroupVPN - Rublon*, n.d.), role-based access control (RBAC), and strict user access policies to ensure that only authorized personnel can access and manipulate the data(*Systems and Interfaces Configuration Guide, Cisco SD-WAN Release 20.x - Role-Based Access Control [Cisco SD-WAN] - Cisco*, n.d.).
3. Intrusion Detection and Prevention Systems (IDPS): Deploying robust intrusion detection and prevention systems within the WAN infrastructure can help identify and mitigate potential security breaches. These systems continuously monitor network traffic, detect unusual patterns or anomalies, and can automatically take action to prevent unauthorized access or data exfiltration(*What Is an Intrusion Detection and Prevention System (IDPS)?*, n.d.).
4. Mobile Device Management (MDM) Solutions: Given the prevalence of mobile devices in the modern workplace, implementing Mobile Device Management (MDM) solutions is critical for securing the WAN network. MDM solutions enable the financial institution to manage and secure mobile devices connected to the network, enforcing security policies, and ensuring that devices are up-to-date with the latest security patches. By implementing MDM solutions, the institution can mitigate the risks associated with mobile devices and prevent unauthorized access to sensitive financial data(*How to Improve Your WAN Security - Bleuwire*, n.d.).

**Conclusion**

In conclusion, incorporating Encryption Protocols and Access Control and Authentication Mechanisms, IDPS security features, and MDM solutions into the WAN network design will significantly enhance the security posture of the financial institution's network, thereby meeting the client's requirements for a secure and robust WAN infrastructure.

**Reference**

*How to Improve Your WAN Security - Bleuwire*. (n.d.). Retrieved January 1, 2024, from https://bleuwire.com/how-to-improve-your-wan-security/

*Multi-Factor Authentication (MFA) for SonicWall WAN GroupVPN - Rublon*. (n.d.). Retrieved January 1, 2024, from https://rublon.com/doc/sonicwall-wan/

*Systems and Interfaces Configuration Guide, Cisco SD-WAN Release 20.x - Role-Based Access Control [Cisco SD-WAN] - Cisco*. (n.d.). Retrieved January 1, 2024, from https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/vedge-20-x/systems-interfaces-book/rbac.html

*What is an intrusion detection and prevention system (IDPS)?* (n.d.). Retrieved January 1, 2024, from https://www.redhat.com/en/topics/security/what-is-an-IDPS