|  |
| --- |
|  |
| Network Security |
|  |
| Network security |
| Stu188448 |
| Jerry Bent |
| 3000 |

**Network Security Design and Evaluation**

**Title:** Network Security Design and Evaluation  
**Subtitle:** Secure LAN Design, Current Network Security Enhancement, and Critical Appraisal  
**Date:** 24/7/2024

**Table of Contents**

1. Introduction
2. New Secure LAN Design
3. Securing the Current Network
4. Critical Appraisal of the Solution
5. Optimal Solution Formulation
6. Financial Implications
7. Reflective Evaluation
8. Conclusion
9. References
10. Appendix A: Security Controls Documentation and Test Validation

**1. Introduction**

**Purpose**

The purpose of this report is to provide a detailed analysis and implementation strategy for enhancing network security within the given topology. This includes designing a secure LAN for a new office (S2), securing the existing network configuration at HQ and S1, and critically appraising the implemented solutions against current and emerging network threats.

**Background**

The organization’s current network topology has several security challenges that need addressing. The goal is to implement robust security measures to protect against potential vulnerabilities while maintaining operational efficiency.

**Structure**

This report is structured to cover the design and implementation of a secure LAN for the new office, enhancements to the existing network, a critical appraisal of the implemented solutions, formulation of an optimal solution beyond current limitations, financial implications, and a reflective evaluation of the process.

**2. New Secure LAN Design**

**Requirements**

The new office (S2) requires a secure LAN design that ensures data integrity, confidentiality, and availability. The design must incorporate advanced security controls to mitigate threats.

**Design Overview**

The secure LAN design for S2 includes a segmented network architecture with VLANs, a robust firewall configuration, and access controls.

**Network Topology**

**Security Controls**

* **Firewall Configuration:** Implemented ASA 5506-X firewall to enforce security policies.
* **VLAN Segmentation:** Segregated different departments and functions into VLANs to limit broadcast domains and enhance security.
* **Access Control Lists (ACLs):** Configured ACLs to control traffic flow between VLANs and to the internet.
* **Secure Wireless Configuration:** Implemented WPA2-PSK encryption and strong authentication mechanisms for wireless networks.

**Defending the Security Controls, Protocols, Countermeasures, and Design Techniques**

**1. VLAN Segmentation**

Defense: VLAN segmentation is a fundamental network security practice that isolates different departments within the network. By creating separate VLANs for Finance, HR, and Sales, we limit the broadcast domain and reduce the risk of internal attacks. This segmentation ensures that even if one VLAN is compromised, the attacker cannot easily move laterally to other VLANs.

Implications for Development: Implementing VLANs requires careful planning of the IP addressing using subnetting and appropriate VLAN configuration on switches and routers using different ways on inter-VLAN routing SVI and ROAS.

**2. Inter-VLAN Routing with ACLs**

Defense: Inter-VLAN routing allows for controlled communication between VLANs. Using ACLs to restrict Sales access between VLANs and deny the access to Finance department.

Implications for Development: ACLs need to be meticulously crafted and regularly updated to reflect changing security policies and organizational needs. They provide granular control over network traffic but require careful management to avoid overly permissive or overly restrictive rules.

**3. Management VLAN**

**Defense: A dedicated management VLAN ensures that network management traffic is isolated from regular user traffic. This separation will protect sensitive management interfaces from unauthorized access**

**Implications for Development: Proper implementation involves configuring all management interfaces to use the management VLAN and securing it with strong authentication methods, such as SSH.**

**4. Layer 2 Security Measures**

Defense:

* Port Security: Limits the number of devices that can connect to a switch port, applying violation restrict mode and stick mac-address configuration
* BPDU Guard: Protects against STP manipulation ensuring the network's topology remains stable.
* DHCP Snooping: Prevents rogue DHCP servers from issuing incorrect IP addresses.

Implications for Development: These measures require enabling and configuring specific features on switches. They add an additional layer of security at the data link layer, mitigating common attacks such as MAC flooding, DHCP spoofing, and ARP spoofing.

**5. Firewall Security**

Defense: Firewalls at the network perimeter inspect and filter incoming and outgoing traffic based on security policies. It prevents unauthorized access and mitigates threats such as DDoS attacks

Implications for Development: Implementing a robust firewall solution involves configuring ACLs that align with security policies

**6. VPNs for Site-to-Site Security**

Defense: VPNs encrypt communication between sites (HQ, S1, and S2), ensuring data integrity and confidentiality over potentially insecure networks. IPsec VPNs provide robust encryption and authentication.

Implications for Development: Setting up VPNs involves configuring VPN endpoints, on our central T3SW1 and T3SW2 switches, and ensuring compatibility between devices. Updating encryption protocols and monitoring VPN connections are essential for maintaining security.

**7. Access Control**

Defense: Implementing Security credentials network access control ensures that only authenticated devices can connect to the network.

Implications for Development: Deploying access passwords configuring switches and authentication servers, such as RADIUS.

**Emerging Threats**

Adaptability: The network design must be adaptable to counter emerging threats such as ransomware, APTs, and zero-day exploits. This requires a proactive approach to security, including regular updates, threat intelligence integration, and advanced security solutions.

Continuous Improvement: Security controls and protocols should be continuously evaluated and improved based on the evolving threat landscape. This involves adopting new technologies and practices, such as machine learning for anomaly detection and zero-trust architectures.

**Recommendations**

Further improvements can include the adoption of zero-trust architecture and continuous security monitoring.

**Optimal Solution Formulation**

**Limitations of Current Topology and PoC Software**

The current topology and Packet Tracer's limitations restrict the full implementation of advanced security features.

**Proposed Optimal Solution**

* **Enhanced Security Measures:** Implementation of zero-trust architecture, AI-driven threat   
  detection, and more granular access controls.
* **Advanced Technologies:** Integration of SD-WAN for secure and optimized connectivity.

**Financial Considerations**

Cost-Benefit Analysis: While implementing advanced security measures incurs initial costs, the long-term benefits of preventing data breaches and maintaining network integrity justify the investment. Organizations should consider the cost of potential security incidents versus the investment in robust security solutions.

Budget Allocation: Adequate budget allocation for security technologies, training, and maintenance is crucial. This includes investing in NGFWs, IDS/IPS, VPN solutions, and regular security audits.

**Testing and Validation**

Validation was conducted through violating applied rules and monitoring network traffic to ensure security controls functioned as intended. Screenshots and logs are provided in Appendix A.

**Reflective Evaluation**

Learning and Development

Conducting this investigation provided significant learning opportunities, including hands-on experience with network security tools and concepts.

**Skills Acquired**

* Skills in:
  + configuring firewalls: get in touch with the way the cisco firewall functioning. There are differences between configuring firewall, router or a switch each of them has a different configuration brain. The idea of configuring the ports as inside, outside and DMZ and how the traffic cannot pass unless there are some extended ACL rules to allow that traffic besides how to assign the default route on the firewall for the outside LAN internet.
  + implementing VLANs, and for traffic isolation, besides inter-VLAN routing using two different ways which are ROAS and SVI on L3 switches
  + Applying standard and extended ACLs on the VLAN to permit the traffic between the departments and from or to the outside network
  + Implemented a management network for management of all the devices in the sites only accessible by the IT Admins through a specific VLAN traffic.
  + IP phones and the separation between DATA and Voice VLANS on the same ports using different commands through the same line one device can get a separate IP from the DHCP server
  + Performing network redundancy using HSRP v2 splitting the topology into tiers adding  
     tier of switches to work as the support or the standby gate way to make sure that the  
     network is always reliable and available
  + Redundant Paths with the use of STP Allows the creation of backup links that become active if the primary path fails.
  + Using HTTPs to access internal services securely over the firewall providing username and password for each user

**Future Application**

The knowledge and skills gained will be valuable in future projects and professional practice, it will be uploaded on github as a security project for a position in a security engineer. A valuable step gaining the knowledge in the security field to ace the masters of cyber security journey .

**Conclusion**

The recommended security controls, protocols, and design techniques provide  
a comprehensive defense against current and emerging network threats. By implementing these measures, the organization ensures robust protection of its network infrastructure, sensitive data, and critical resources. Continuous evaluation, adaptation, and investment in security are essential for maintaining a secure network posture.

**10. Appendix A: Security Controls Documentation and Test Validation**

**Validation Results**

* Summary of test results validating the effectiveness of security controls.

Steps taken to configure the secure LAN in Packet Tracer:

1. All department traffic should be isolated and for that we used Vlans
   * 1. For each of the departments (Sales,HR,Finance) to isolate all department traffic and to be able to secure each department independent of the other departments.
     2. Used normal vlan implementation (access and trunking ports ),in addition to SVI for inter-vlan routing on some of the vlans and ROAS on the other parts .

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

**SVI** :

A screenshot of a computer screen

Description automatically generated

**ROAS**:

A screenshot of a computer screen

Description automatically generated

1. Security best practices applied at Layer 2.
   * Implementing first line passwords on the configuration modes, console line and line VTY
   * The management connection using ssh
   * enabling port security for ant violation to restrict the violated port.
   * Enabling the mac address to sticky for the first device to connect
   * Adding unsed ports to vlan 404

**Unused ports added to vlan 404 :**

A screenshot of a computer

Description automatically generated

**Port-security and sticky mac address:**

A screenshot of a computer program

Description automatically generated

1. Sales should not be allowed to access the Finance network
   * Using Standard ACLs (are used in network devices like routers to control   
     traffic based on the source IP address. They are basically filtering mechanisms  
     that allow or deny packets moving through the network ) on the router and applying it to the port going to the finance network
   * Preventing all traffic coming from sales into finance department

Sales cannot access the finance :

A screenshot of a computer

Description automatically generated

1. Secure network for management of switches, only accessible by the IT devices in HQ.
   * Implementing the ssh configuration on all the devices
   * Creatig MGMT vlans for the switches to assign an ip address for each device so that we can ssh to all the devices using IT admin credentials
   * Adding loopback interface for each Router or L3 switch to have the ability to connect over ssh
   * Using RSA 512 for the ssh encryption
   * Creating admin user that has the ability to configure all network devices through on pc dedicated in the HQ office
   * For the Wirless network I used WPA2-PASK (Wi-Fi Protected Access 2 - Pre-Shared Key) is a security protocol for wireless networks. It provides strong encryption to protect data transmitted over Wi-Fi
   * Screenshots for the ssh connection to each of the devices is available:

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A computer screen shot of a black screen

Description automatically generated

Wireless security :

A screenshot of a computer

Description automatically generated

1. All network devices should be secured following best practices.
   * For all network devices the default credentials are all changed
   * Applied secret encrypted passwords to all the devices to prevent any type of attack through the physical network
   * Applied ssh settings on all devices to allow the management through ssh connections
   * All unused ports have been added to VLAN 404 and shutdown to prevent any bad use of them
   * For the used ports port security is used and restrict mode as a security violation have been used with the use of sticky mac address with a 1 mac only allowed for the port to prevent any security violation through interfaces.

Sticky mac and security violation

A screenshot of a computer program

Description automatically generated

Password enabling on the devices :

A screenshot of a computer

Description automatically generated

1. Access to the Internet for Sales only
   * ACL is applied on the inside and outside interfaces of the firewall to allow the traffic of the sales department to access the internet
   * Nat is performed to go for only one public IP from the inside network and no to waste leased addresses

Among HR, finance and Sales only the sales can access the internet with the policy applied on the firewall that allows the sales to access the internet and allowing the public network to get the services from the DMZ servers farm.

A screenshot of a computer

Description automatically generated

1. Resilient links where appropriate
   * Implementing HSRP V2 which ensures high availability of gateway routers  
     including two routers in the as a gateway with the same Virtual Ip address  
     and the way it work the when of the gateway falls the other one sends a Gratuitous ARP REPLY to inform the devices with it virtual mac address so that the traffic keeps going .
   * That could be to load balance the traffic between the vlans .

A computer network diagram with text and symbols

Description automatically generated

A screenshot of a computer

Description automatically generated

This L3 switch is a gateway for vlans 50 and 100 using but not vlan 60

Using HSRPV2 used for load balancing between the two routers

A screenshot of a computer screen

Description automatically generated

1. Implement appropriate security controls at Layer 3.
   * Shutting down all unnecessary services on all the devices as per the servers turned all unused services off .
   * The implementation of ACL and Firewall assured the security at L3 as per that no traffic will pass through the firewall unless it has an access list entity that permits the traffic to pass

A diagram of a diagram

Description automatically generated

Nat translation is a networking protocol that add the ability to   
multiple private IP address to reac out using the same public IP address  
and should be applied to the firewall in the best practice scenario :

A screen shot of a computer code

Description automatically generated

VPN Tunneling between T3SW1 and T3SW2 :

A diagram of a network

Description automatically generated

A computer screen shot of a black screen

Description automatically generated

1. All traffic entering the corporate network should be secured
   * Firewall general policy prevents any traffic to move neither inside or outside or to the DMZ zone by default, as a result for that ACL is applied to allow the coming public traffic to reach the inside services located the servers farm DMZ zone as shown in as a public pc can reach the DMZ zone:

A screenshot of a computer

Description automatically generated

Only https is allowed :

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Public traffic should only be able to access the Corp Web Server:
   * ACL is applied to allow the coming public traffic to reach the inside services  
     located the servers farm DMZ zone as shown in the figure:

A screenshot of a computer

Description automatically generated

This draft report provides a comprehensive analysis and documentation of the security measures implemented and evaluated within the given network topology. Adjustments and further details should be added based on specific configurations and results obtained during testing.

A holistic view for the topology.

A computer network diagram with many different colored circles and dots

Description automatically generated with medium confidence