PRO MANAGE

SCD FOR NETWORK DEVICES

Security Configuration Document[SCD] for Network devices in a Company

1. Introduction

This document outlines the security configuration guidelines for network devices used within the company. The purpose of this document is to ensure that the network devices are configured securely to protect the company's information and systems.

2. Scope

This document applies to all network devices used within the company, including routers, switches, firewalls, and wireless access points.

3. Device Version

The company will use the latest version of the network devices to ensure that the devices are secure and that any known security vulnerabilities have been addressed.

4. Password Policy

- Passwords must be at least 8 characters in length and contain a combination of upper and lowercase letters, numbers, and special characters.
- Passwords must be changed every 90 days.
- Passwords must not be reused for at least 12 months.

5. User Access

- All network devices must be configured with unique accounts and must not share accounts.
- User accounts must be configured with the appropriate level of access based on their job function.
- User access must be reviewed and updated regularly.

6. Firewall Configuration

The company will use a firewall to protect its network and systems from unauthorized access.The firewall must be configured to only allow traffic from trusted sources and to block traffic from untrusted sources.

7. Access Control Lists (ACLs)

The company will use ACLs to control access to its network and systems.

ACLs must be configured to only allow traffic from trusted sources and to block traffic from untrusted sources.

8. Software Updates

The company will use software updates to keep its network devices up to date and to address any security vulnerabilities.
Software updates must be installed promptly to ensure that the network devices are protected from known security vulnerabilities.

9. VLAN Configuration

The company will use VLANs to segment its network and to increase network security. VLANs must be configured to only allow traffic from trusted sources and to block traffic from untrusted sources.

10. Remote Access

Remote access to the network devices must be secured using strong authentication methods. Remote access must be restricted to only authorized personnel.

11. Data Backup

- The company will back up its network device configuration regularly to ensure that it is protected in the event of a data loss.
- The configuration backup must be stored in a secure location and must be tested regularly to ensure that it can be restored if necessary.

12. Incident Response Plan

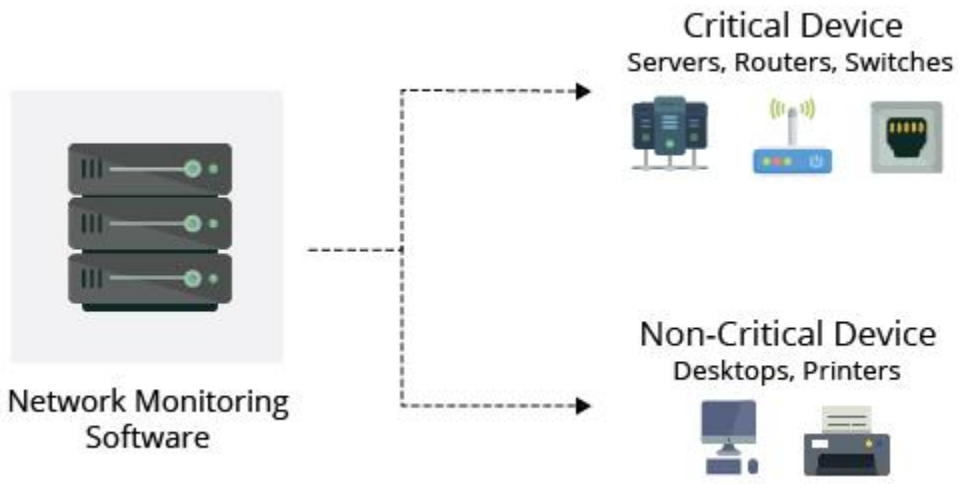
The company will have an incident response plan in place to respond to security incidents.

The incident response plan will include procedures for identifying, reporting, and responding to security incidents.

13. Conclusion

By following these security configuration guidelines, the company can ensure that its network devices are configured securely and that its information and systems are protected from security threats.

WORKFLOW :


Critical Device
Servers, Routers, Switches
Non-Critical Device
Desktops, Printers
Network Monitoring
Software