Araziyah Safety Infrastructure (Pty) Ltd

Common Network Security Device Configuration

AI Overview

Network security devices should be configured using secure baseline standards, rigorous change management, access controls, and regular audits to prevent exploitation of vulnerabilities.Key Components of Secure ConfigurationBaseline Configuration Standards: Establish and implement baseline configurations for all network devices, including firewalls, routers, and switches. These standards should follow industry best practices and be tailored to the organization's security requirements, ensuring that default settings, unnecessary services, and open ports are minimized . Configuration Management: Maintain a documented configuration management process to track all changes. This includes recording current configurations, historical changes, the rationale for each change, and the responsible personnel. Automated tools can help compare current configurations against approved baselines and alert deviations . Change Control Process: Implement a formal change control process for all configuration modifications. Each change should undergo risk assessment, approval by authorized personnel, and thorough testing before deployment to prevent accidental vulnerabilities . Access Control and Administrative Security: Restrict access to management interfaces to authorized personnel only. Use multi-factor authentication and encrypted sessions for administrative access. Network engineers should perform administrative tasks on dedicated, isolated machines that are not connected to the Internet or used for general purposes . Patch and Vulnerability Management: Regularly update devices with the latest firmware and security patches. Subscribe to security bulletins to stay informed about newly discovered vulnerabilities and recommended mitigations . Traffic and Rule Documentation: Document all configuration rules that allow traffic t...

Article Content

Gartner Business Insights, Strategies & Trends For

Gain strategic business insights on cross-functional topics, and learn how to apply them to your function and role to drive stronger performance and innovation.

Questions with policies and profiles in Microsoft Intune

Common questions, answers, and scenarios with device policies and profiles in Microsoft Intune. Learn more about profile changes not applying to users or devices, how long it takes for new

Network Device Security: Guide and Best Practices

Network device security is the use of policies and configurations that a network administrator sets to monitor and protect the network devices from any

Common Wireless Network Security Threats

Starting with wireless security basics and moving into 7 common wireless network threats, Pluralsight teaches what you need to know. Begin learning now!

Network Configuration Basics: Everything You Should

Get to know the basics of network configuration, including setup, protocols, and tips to ensure smooth and secure connectivity

Network Device Configuration Security | Strobes

Expert guide to network device configuration reviews: routers, switches, firewalls. Discover best practices & Strobes solutions today.

Search Security Information, News and Tips from

Traditional network boundaries have all but disappeared. Enterprises must find new ways to protect their digital assets in a world where SaaS and

Guide for Security-Focused Configuration Management of ...

Abstract Guide for Security-Focused Configuration Management of Information Systems provides guidelines for organizations responsible for managing and administering the security of federal

Network Security Devices Explained: Types, Examples ...

Explore the most important network security devices—firewalls, intrusion prevention systems, VPNs, and more. Learn how each protects your business network and keeps your data secure.

Red Hat Enterprise Linux 9

Using SELinux Prevent users and processes from performing unauthorized interactions with files and devices by using Security-Enhanced Linux (SELinux) Securing networks Configuring secured

Securing Network Infrastructure Devices

Harden Network Devices A fundamental way to enhance network infrastructure security is to safeguard networking devices with secure configurations. Government agencies, organizations,

Microsoft Entra Conditional Access: Zero Trust Policy Engine ...

Modern security extends beyond an organization''s network perimeter to include user and device identity. Organizations now use identity-driven signals as part of their access control

VS Code for enterprise

Learn how to configure and manage Visual Studio Code in enterprise environments, including policies, extensions, AI settings, and network configuration.

Network Device Security: Guide + Recommended

Do you know how network devices can affect the security of your entire network? Find out network device configurations best practices to keep

Scenarios for using Conditional Access with Microsoft Intune ...

There are two types of Conditional Access policies you can use with Intune: device-based and app-based. This article covers common scenarios for both types. The information in this

Router in Computer Networks

Wireless Routers: Create Wi-Fi networks in homes or offices. Wired Routers: Connect multiple devices via Ethernet cables, common in schools and

Top 16 Network Security Devices [Updated 2025]

In this article, we will explore common types of network security devices, appliances and technologies that form a robust, multi-layered security strategy, including firewalls, intrusion

10 Most Common Network Devices & How to Monitor Them

This article is written for network admins, engineers, and system pros who want to sharpen their toolkit. We''ll look at the 10 most common network devices, break down how they work,

Network Device Security: Guide + Recommended Software

A network device configuration review involves systematically analyzing the settings and configurations of network devices, such as routers,

Red Hat Enterprise Linux | 8 | Red Hat Documentation

Security hardening Enhancing security of Red Hat Enterprise Linux 8 systems Using SELinux Prevent users and processes from performing unauthorized interactions with files and devices by using

Azure updates | Microsoft Azure

Subscribe to Microsoft Azure today for service updates, all in one place. Check out the new Cloud Platform roadmap to see our latest product plans.

Network Infrastructure Security Guide

While the guidance presented here can be applied to many types of network devices, the National Security Agency (NSA) has provided sample commands for Cisco Internetwork Operating

CIS Control 11: Secure Configuration for Network Devices, such as ...

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control

What Is Network Configuration?

Key Takeaways Network configuration involves defining and applying settings — such as IP addresses, protocols, and security rules — across devices

Guide to Network Device Configuration Review

A network device configuration review involves systematically analyzing the settings and configurations of network devices, such as routers, switches, and firewalls, to ensure they meet

Troubleshoot policies and configuration profiles in

This article provides troubleshooting guidance for common issues related to policies and configuration profiles in Microsoft Intune. including

Contact Us

For more information, pricing, or custom solutions, please contact us:

Website: https://www.araziyahsafety.co.za
Email: info@araziyahsafety.co.za
Phone: +27 72 418 3692
Address: 123 Rivonia Road, Sandton, Johannesburg, 2196, South Africa

This document is for informational purposes only. Specifications subject to change without notice.