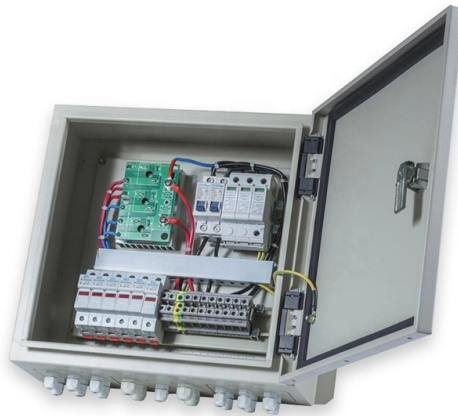


Network Security Equipment Control Standards



AI Overview

Maintaining secure network equipment requires rigorous configuration management, compliance with standards, and hardware-based identity verification. Secure Configuration and Management Network devices should be configured securely from the start and actively managed over time. Default settings from manufacturers often prioritize ease of deployment over security, leaving open ports, default accounts, and outdated protocols that attackers can exploit. Implement a configuration management and change control process to track, report, and correct device settings regularly, ensuring that exceptions are justified, documented, and removed when no longer needed. Regular reviews, ideally monthly, help prevent misconfigurations that could lead to breaches. Compliance with Security Standards Adhering to recognized frameworks such as ISO 27001, SOC 2, and NIST 800-53 ensures that network equipment meets industry security requirements. For example, firewall rules should be simple, clearly named, and limited to necessary ports and protocols, satisfying multiple compliance controls simultaneously. Threat modeling and risk assessment should guide which controls are implemented, aligning security measures with the specific threats your network faces. Hardware-Based Security and Device Identity Using Trusted Platform Modules (TPMs) and cryptographic device identifiers enhances security by providing a hardware root of trust. TPMs protect private keys, resist physical attacks, and allow devices to assert their identity securely. Standards like IEEE 802.1AR define unique per-device identifiers (DevID), enabling trust verification for network access and preventing unauthorized devices from connecting. Network Segmentation and Access Control Segmenting networks into isolated zones limits lateral movement by attackers, slowing potential breaches. Implement least...

Article Content

ESTABLISHING NETWORK EQUIPMENT SECURITY

For improved network security, the Trusted Computing Group (TCG) is developing standards/guidance that specifically addresses the security of networking equipment. The TCG Guidance for Securing

Guide to a Secure Enterprise Network Landscape

NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to

IEC homepage

IEC everywhere for a safer and more efficient world. The IEC is a global, not-for-profit membership organization that brings together more than 170 countries and coordinates the work of 20,000

Setting up a wireless network in Windows | Microsoft Support

Learn about modems and Internet connections, security, sharing files and printers, and how to set up a wireless network in your home.

DoW Foreign Clearance Guide (FCG) 2.0

Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose. This IS

SP 800-53 Rev. 5, Security and Privacy Controls for Information

The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and

Guide to Operational Technology (OT) Security

National Institute of Standards and Technology Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology Certain commercial equipment, instruments, software,

SP 800-53 Rev. 5, Security and Privacy Controls for Information

This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other

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

ISO/IEC 27033-1:2015

ISO/IEC 27033-1:2015 provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security.

Network security fundamentals | National Cyber Security Centre

The controls you incorporate into your network should align with the specific threats you need to guard against. If you don't perform "threat modelling", it is highly likely you will waste

Network Infrastructure Security Guide

An administrator's role is critical to securing the network against adversarial techniques and requires dedicated people to secure the devices, applications, and information on the network....

Securing Network Infrastructure Devices

Limiting administrative privileges for infrastructure devices is crucial to security because intruders can exploit administrative privileges that are improperly authorized, granted widely, or not

Guide to a Secure Enterprise Network Landscape

ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security

ISO 27001 A.7.8 Equipment Siting & Protection: Requirements

ISO 27001 Annex A.7.8 requires organizations to purposefully position and protect their physical IT equipment—such as servers, routers, printers, and workstations—to minimize risks.

ISA/IEC 62443 Series of Standards

The ISA/IEC 62443 standards set best practices for cybersecurity and provide a way to assess the level of security performance.

Network security standards: All you need to know | NordVPN

Network security standards are key to keeping information safe in a world where everything runs on networks. Whether you're a business owner, IT professional, or just someone

Network Security Architecture: Best Practices & Tools

This article explores network security architecture components, goals, best practices, frameworks, implementation, and benefits as well as where you can learn more about network

Network Security Standards: Essential Guidelines for Businesses

Discover the key network security standards every business needs to follow. Find out how SearchInform can enhance your network security measures.

The Network-Security Compliance Checklist: 25 Controls, Mapped

This network security compliance checklist maps 25 must-have controls to ISO 27001, SOC 2, and NIST 800-53, and shows you how to collect evidence automatically so you're always

SP 800-215, Guide to a Secure Enterprise Network Landscape | CSRC

This document is meant to provide guidance to this new enterprise network landscape from a secure operations perspective. Hence, it starts by examining the security limitations of current

Security and Privacy Controls for Information Systems and ...

ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security of other than national security-related

Mixed-signal and digital signal processing ICs | Analog

Analog Devices is global leader in the design and manufacturing of analog, mixed signal, and DSP integrated circuits to help solve the toughest engineering

Understanding Network Security Standards: A Comprehensive Guide

Explore the world of network security standards with our comprehensive guide. Get insights on keeping data safe and network secure.

Cyber Security Standards

Cyber Security Standards Karen Scarfone, Dan Benigni and Tim Grance National Institute of Standards and Technology (NIST), Gaithersburg, Maryland Abstract: The goal of cyber security standards is to

Guidelines for networking

Should an organisation choose to risk manage implementing VLANs between networks belonging to different security domains, such as at the same classification, additional controls for

ISO 27001:2022 Annex A Control 8.20 Explained

ISO 27001:2022 Annex A 8.20 focuses on network security by implementing controls to prevent unauthorised access, ensure secure data transmission, segment network traffic, and monitor

Contact Us

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

Website: <https://estlascleaning.co.za>

Email: info@estlascleaning.co.za

Phone: +27 63 214 8579

Address: 22 Oxford Road, Parktown, Johannesburg, 2193, South Africa

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

