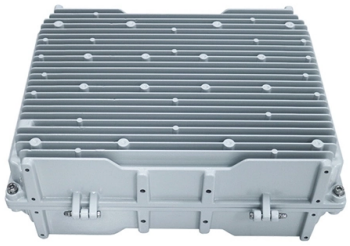
Network Security Equipment Acceptance Standards



Overview

GSMA Network Equipment Security Assurance Scheme (NESAS)The purpose of the scheme is to audit and test network equipment vendors, and their products, again.

Key Takeaways

Network security equipment should include firewalls, intrusion prevention systems, VPN gateways, and endpoint protection devices that comply with recognized standards such as NIST and NSA guidelines.

Key Types of Network Security Devices

Firewalls – Act as a barrier between internal networks and external traffic, filtering connections based on IP addresses, ports, and protocols. Next-generation firewalls (NGFWs) provide advanced features like application awareness, intrusion prevention, and web filtering, operating at the application layer for enhanced protection. Intrusion Prevention Systems (IPS) – Monitor network traffic in real-time to detect and block suspicious patterns or anomalies, complementing firewalls by proactively preventing attacks.

VP

© 2026 ENSAA OPTICAL NETWORKS - All rights reserved

N Gateways – Ensure secure remote access by encrypting data transmitted over public networks, essential for remote work and cloud-based services. Unified Threat Management (UTM) Systems – Combine multiple security functions, including firewall, IPS, antivirus, and content filtering, into a single appliance, suitable for small to medium-sized businesses. Web Application Firewalls (WAFs) – Protect web applications from attacks such as SQL injection, cross-site scripting, and file inclusion, available as host-based, network-based, or cloud-based solutions.

Network Access Control (NAC) – Enforce policies for device authentication and access, ensuring only authorized devices connect to the network. Standards and ComplianceNIST Guidelines – NIST IR 8425A provides cybersecurity requirements for consumer-grade routers and network devices, emphasizing secure configuration, firmware updates, and protection against unauthorized access.

Following NIS

T standards ensures devices meet minimum security outcomes for confidentiality, integrity, and availability.

NS

A Recommendations – The NSA's network infrastructure security guide outlines best practices for device configuration, Zero Trust implementation, and mitigation of common vulnerabilities. Compliance with these guidelines helps prevent adversaries from exploiting network weaknesses. Best Practices for ImplementationDefense-in-Depth – Deploy multiple layers of security so that if one layer fails, others continue to protect the network.

This includes combining firewalls, IPS, endpoint protection, and secure access controls. Regular Updates and Monitoring – Ensure devices are properly configured, patched, and continuously monitored to detect emerging threats. Integration with Security Policies – Align device deployment with organizational cybersecurity policies, including access control, incident response, and compliance requirements.

By selecting network security equipment that adheres to NIST and NSA standards and implementing a multi-layered defense strategy, organizations can effectively safeguard their networks against evolving cyber threats while maintaining regulatory compliance.

© 2026 ENSAA OPTICAL NETWORKS - All rights reserved

Article Content

GSMA Network Equipment Security Assurance Scheme (NESAS)

The purpose of the scheme is to audit and test network equipment vendors, and their products, against a security baseline. So they can demonstrate to network operators that they are conforming to the

Network Equipment Security Assurance Scheme – GSMA NESAS

NESAS defines security requirements and an assessment framework for secure Vendor Development and Product Lifecycle Processes, as well as security test cases for the security evaluation of network

NESAS — Network Equipment Security Assurance Scheme | 3GPP

NESAS is a joint 3GPP and GSMA security assurance framework that standardizes security requirements and evaluation processes for mobile network equipment vendors, providing operators

Product Certification: Network Equipment Security Assurance Scheme ...

A list of requirements, regarding the operational environment that must be met for secure operation of the network product. This list shall consider the mitigation of threats according to [TR 33.926] chapter

Certification according to BSI NESAS

The "Network Equipment Security Assurance Scheme" (NESAS) is a framework developed by the Groupe Speciale Mobile Association (GSMA) and the 3rd Generation Partnership Project (3GPP) to

NESAS Certification

The Network Equipment Security Assurance Scheme (NESAS) is a globally recognised security certification framework developed collaboratively by the Global System for Mobile Communications

List of Equipment and Services Covered By Section 2 of The Secure ...

Pursuant to the Commission''s rules, the Public Safety and Homeland Security Bureau will maintain this list on the Commission''s website, and will monitor the status of any determinations in

Cybersecurity Policies and Standards | SANS Institute

In partnership, the Cybersecurity Risk Foundation (CRF) and SANS have created a library of free cybersecurity policy templates to help organizations quickly define, document, and

© 2026 ENSAA OPTICAL NETWORKS - All rights reserved

Network Infrastructure Security Guide

Guidance for securing networks continues to evolve as adversaries exploit new vulnerabilities, new security features are implemented, and new methods of securing devices are

Home page

BACnet (Building Automation and Control Network) is the global data communications standard for building automation and control networks. It provides vendor-independent interoperability for

Join a Microsoft Teams Meeting by ID | Microsoft Teams

Learn how to join a Microsoft Teams meeting quickly and easily with just a meeting ID. Once you''re in, explore Teams features to make your meeting successful.

ANSI/NETA ATS

ANSI/NETA ATS-2025 Standard for Acceptance Testing Specifications for Electrical Power Equipment and Systems Scope These specifications are designed to assure that tested electrical equipment

Keysight: Design, Emulate, and Test to Accelerate Innovation

Keysight empowers innovators with software-centric design, emulation, and test solutions to deliver tomorrow''s breakthroughs at speed and with reduced risk.

ANSI/NETA ATS-2013 Electrical Power Equipment Testing Standard

ANSI/NETA ATS-2013 standard for acceptance testing of electrical power equipment and systems. Guidelines for electrical testing and safety.

STANDARD FOR ACCEPTANCE

Purchasers may reproduce and use all or a portion of the ANSI/NETA ATS-2013 provided ANSI/NETA Standard for Acceptance Testing Specifications for Electrical Power Equipment and Systems are

Top 15 IT security frameworks and standards explained

Learn about the top IT security frameworks and standards available and get advice on choosing the ones that will help protect your company''s data.

STANDARD FOR ACCEPTANCE

American National Standard Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by

© 2026 ENSAA OPTICAL NETWORKS - All rights reserved

STANDARD FOR ACCEPTANCE TESTING SPECIFICATIONS for

Section 7 of the ANSI/NETA Standard for Acceptance Testing Specifications for Electrical Power Equipment and Systems may be reproduced and used on a “cut and paste” basis for the particular

Contact Us

Continue your research online:

Website: https://ensaa.es
Technical inquiry: https://ensaa.es/contact.html

This document is for preliminary research. Verify specifications against current standards, product documentation and project requirements.

© 2026 ENSAA OPTICAL NETWORKS - All rights reserved