Performance Requirements for Network Security Equipment

Overview

Guide to Network Security Best Practices | NetwrixThis article explores a range of network and security best practices and technologies you need to fortify.

Key Takeaways

Network security equipment must meet defined throughput, latency, and reliability benchmarks while maintaining security effectiveness under realistic operational conditions.Key Performance Metrics

Throughput and Latency: Security devices such as next-generation firewalls (NGFW) and intrusion prevention systems (IPS) must handle high network traffic without introducing significant latency. Throughput is measured under various configurations, including full security inspection, and latency should remain minimal to avoid network bottlenecks . Connection Handling and Scalability: Devices must support a large number of concurrent sessions and connections per second, ensuring scalability for enterprise or telecom networks. Performance testing should simulate realistic traffic patterns to validate these capabilities . Security Effectiveness: Performance testing must not compromise the device's ability to detect and block threats. Security features should be fully enabled during testing, except for machine learning or behavioral analysis features, which should be disabled to ensure reproducibility .

Benchmarking and Test Methodology

© 2026 JEWELBLU OPTICAL SYSTEMS - All rights reserved

Isolated Test Environment: Performance tests should be conducted in a controlled, isolated testbed to prevent external network limitations from affecting results. The testbed should minimize the use of external switches or routers to ensure accurate measurement of the device's capabilities . Reproducibility and Transparency: Benchmarks should follow standardized methodologies, including clearly defined test configurations, traffic profiles, and result reporting formats. This ensures that performance results are comparable across devices and vendors .

Security Assurance and Compliance

NESAS Requirements: For telecom network equipment, compliance with the GSMA Network Equipment Security Assurance Scheme (NESAS) ensures that devices meet both security and performance standards. NESAS defines Security Assurance Specifications (SCAS) that are testable, auditable, and consistently assessed by accredited laboratories . Configuration and Monitoring: Devices should be configured according to best practices, including secure management protocols, VPN support, and monitoring of network traffic for anomalies. Intrusion detection and prevention systems (NIDS/NIPS) should be deployed at network boundaries to detect and respond to threats in real time .

Best Practices for Maintaining Performance
• Regular Firmware Updates: Ensure devices are updated to maintain optimal performance and security.

• Baseline Monitoring: Establish baseline network traffic and monitor deviations to detect performance degradation or security incidents .

• Zero Trust Principles: Implement Zero Trust architecture to reduce the risk of internal and external threats while maintaining device performance .

• Protocol and Access Control: Disable insecure protocols (e.g., SMBv1, SNMPv1/v2) and enforce strict access controls to prevent unauthorized access that could impact performance . By adhering to these performance requirements, organizations can ensure that network security equipment operates efficiently, scales with network demands, and maintains robust protection against evolving threats.

© 2026 JEWELBLU OPTICAL SYSTEMS - All rights reserved

Article Content

Guide to Network Security Best Practices | Netwrix

This article explores a range of network and security best practices and technologies you need to fortify your network against

SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security

This document provides guidance on how to secure operational technology (OT) while addressing their unique

Network Infrastructure Security Guide

An administrator''s role is critical to securing the network against adversarial techniques and requires dedicated people

Guide to a Secure Enterprise Network Landscape

NIST SP 800-215 Guide to a Secure Enterprise November 2022 Network Landscape . Certain commercial entities, equipment, or

Understanding Network Requirements

These requirements also play a vital role in determining the speed of data transfer, the level of security, the scalability,

What is network security?

What is network security? Network security combines policies and technologies to protect systems and digital assets from

Cyber Security Standards

Abstract: The goal of cyber security standards is to improve the security of information technology (IT) systems, networks, and critical

Understanding Network Requirements

Conclusion Mastering your network requirements is the first step to building a fast, secure, and future-ready digital

Service availability | ASIC

Fair, strong and efficient financial system for all Australians.

Security Technical Implementation Guides | Cyber Exchange

This site contains the Security Technical Implementation Guides and Security Requirements Guides for the Department of Defense

© 2026 JEWELBLU OPTICAL SYSTEMS - All rights reserved

What is Network Security?

What is Network Security? Network Security protects your network and data from breaches, intrusions and other threats. This is a

Minimum requirements for Microsoft Defender for Endpoint

Hardware and software requirements Devices on your network must be running one of the operating systems listed in

Network Security Best Practices and Checklist

Test all configurations prior to deployment. Network Security Checklist Network security management should be

Cisco Secure Firewall Advanced Threat Protection

Cisco''s Secure Firewall hardware and software options enhance your security to block more threats and swiftly respond to breaches.

Driving impact by equipping changemakers with evidence and

Social and Economic Policy Research Urban is a leader in providing evidence and solutions on the issues that affect the well-being

Login

1,000,000+ Salespeople and marketers use our extension to prospect, connect, and convert leads faster. Get Apollo Chrome Extension

Login | Reuters Connect

Reuters Connect By continuing, you agree to the Reuters Connect Platform Terms and Conditions and Privacy Policy

What is network security?

What is network security? Network security combines policies and technologies to protect systems and digital assets from

Cyber Security Standards

Abstract: The goal of cyber security standards is to improve the security of information technology (IT) systems, networks, and critical

Understanding Network Requirements

Conclusion Mastering your network requirements is the first step to building a fast, secure, and future-ready digital

Service availability | ASIC

© 2026 JEWELBLU OPTICAL SYSTEMS - All rights reserved

Fair, strong and efficient financial system for all Australians.

Security Technical Implementation Guides | Cyber Exchange

This site contains the Security Technical Implementation Guides and Security Requirements Guides for the Department of Defense

What is Network Security?

What is Network Security? Network Security protects your network and data from breaches, intrusions and other threats. This is a

Guide to Network Security Best Practices | Netwrix

This article explores a range of network and security best practices and technologies you need to fortify your network against

SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security

This document provides guidance on how to secure operational technology (OT) while addressing their unique

Network Equipment Security Assurance Scheme – Requirements

Security Assurance Specification: Specification containing security requirements and test cases for a defined Network Function or a

Top Devices to Enhance Corporate Network Security and Performance

Discover top devices that improve corporate network security and performance, helping you enforce policies,

Guide to a Secure Enterprise Network Landscape

NIST SP 800-215 Guide to a Secure Enterprise November 2022 Network Landscape . Certain commercial entities, equipment, or

Network Infrastructure Security Guide

An administrator''s role is critical to securing the network against adversarial techniques and requires dedicated people

Network Security and Segmentation Requirements

Deep dive into PCI DSS Requirements 1 and 2 covering network security controls, firewall configuration, network segmentation of the

10 Essential Network Security Best Practices for IT Leaders

This guide provides a detailed roundup of the most critical network security best practices for modern enterprises. We will move

© 2026 JEWELBLU OPTICAL SYSTEMS - All rights reserved

Network Equipment Security Assurance Scheme – Methodology

The security evaluation of network equipment in NESAS consists of Evidence Evaluation and Network Product Evaluation, as further

Spotlight Paper

Network security products are expected to be able to flexibly adapt to dynamically shifting bandwidth and performance requirements,

Guide to Network Security Best Practices | Netwrix

This article explores a range of network and security best practices and technologies you need to fortify your network against

SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security

This document provides guidance on how to secure operational technology (OT) while addressing their unique

Network Infrastructure Security Guide

An administrator''s role is critical to securing the network against adversarial techniques and requires dedicated people

Guide to a Secure Enterprise Network Landscape

NIST SP 800-215 Guide to a Secure Enterprise November 2022 Network Landscape . Certain commercial entities, equipment, or

Contact Us

Continue your research online:

Website: https://jewelbluimages.co.za
Technical inquiry: https://jewelbluimages.co.za/contact.html

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

© 2026 JEWELBLU OPTICAL SYSTEMS - All rights reserved