

Shared network security devices



AI Overview

Shared network security devices protect multi-user networks by monitoring traffic, controlling access, and preventing unauthorized activity across all connected devices. Overview of Shared Network Security Devices Shared network security devices are specialized tools designed to safeguard networks that are accessed by multiple users or devices. They ensure that sensitive data remains protected while allowing legitimate users to share resources such as files, printers, and internet connections. These devices can be hardware-based, software-based, or cloud-hosted, and they often combine multiple security functions to provide comprehensive protection.

Common Types of Shared Network Security Devices

- Firewalls** Firewalls act as a barrier between internal networks and external threats. They can be hardware, software, or next-generation firewalls (NGFW), providing packet filtering, stateful inspection, and intrusion prevention. Firewalls are essential for shared networks to control access and block malicious traffic.
- Intrusion Detection and Prevention Systems (IDS/IPS)** IDS monitors network traffic for suspicious activity, while IPS actively blocks threats. In shared networks, these systems protect all connected devices from attacks and alert administrators to potential breaches.
- Unified Threat Management (UTM) Devices** UTM devices combine multiple security functions—firewall, antivirus, content filtering, and VPN—into a single appliance. They are particularly useful in small to medium shared networks where centralized management is needed.
- Network Access Control (NAC)** NAC solutions enforce security policies by controlling which devices can access the network. They are critical in shared environments to ensure that only authorized users and devices can connect.
- VPN Gateways** VPN gateways provide secure remote access for users sharing a network across different locations. They encrypt traffic, ensuring that shared resources remain protected from eavesdropping.
- Email and Web Security G...**

Article Content

Network Security Devices Explained: Types, Examples ...

Network security devices provide automated functionality that can help stop network-based cyberattacks. In this post, we'll look at a variety of common network security devices and explore

Windows 11 Network and Sharing Security Settings Overview

This overview explains the important Windows 11 network and sharing security settings, where to find them, and how to use them in real-world situations. It focuses on practical choices:

Free Virtual USB: Share & Access USB Devices over Network

Unleash your USB devices with our free USB over Network software! Access any USB peripheral – from printers and webcams to specialized hardware and security dongles – from

New Malware Campaigns Turn Network Devices Into

Network security has taken another hard hit. Two previously unknown malware strains have emerged, quietly turning routers, IoT devices,

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....

China-Nexus Hackers Exploit Ruckus Routers to Build Operational

China-linked UAT-7810 exploits Ruckus routers to expand the LapDogs ORB network, hiding cyberattacks behind hijacked devices.

How to Secure Your Home Wi-Fi: A Step-by-Step Guide

Tips to secure your Wi-Fi network at home Here are the basics for protecting your home Wi-Fi network. Keep reading for more information on each

How to Setup a Guest WiFi Network? (2 Easy Steps)

Setting up a guest WiFi network is a great way to provide internet access to visitors while keeping your main network secure. In just 2 easy steps,

Top 8 Network Security Devices Every IT Professional

Discover the top 8 network security devices essential for protecting your business from cyber threats, including firewalls, VPNs, and more.

SmartThings could get Matter 1.6 support for easier device setup ...

SmartThings could soon gain Matter 1.6 features, including two-way NFC setup, Joint Fabric, enhanced security, and Thread Tools support.

Forescout's 2026 Riskiest Connected Devices Report

Forescout Technologies Inc., a global leader in cybersecurity, today released its “Riskiest Connected Devices in 2026” report from Forescout

What Are Network Security Devices? Types and Guide

Network security devices are specialized hardware, software, or cloud-based appliances that monitor, filter, and control traffic between networks, endpoints, and the internet. They enforce

Network access: Sharing and security model for local accounts

Best practices, security considerations, and more for the security policy setting, Network access Sharing and security model for local accounts.

Computer Network Tutorial

A computer network is a system of interconnected devices, such as computers, servers, smartphones, and printers, that communicate to exchange

Networking Products and Solutions

Securely connect users, devices, and workloads everywhere. Cisco networking solutions simplify operations, boost performance, and scale to meet your demands.

Network Devices

It is a network security system, comprising hardware, software, or both that monitors and controls incoming and outgoing network traffic based on predetermined security rules

Network security fundamentals | National Cyber Security Centre

Networks are fundamental to the operation, security and resilience of many organisations. This guidance provides an introduction to the key topics to consider when designing, maintaining, or...

Atlantic International University

Hier sollte eine Beschreibung angezeigt werden, diese Seite lässt dies jedoch nicht zu.

Wiley Online Library

Hier sollte eine Beschreibung angezeigt werden, diese Seite lässt dies jedoch nicht zu.

The Most Common Types of Network Security Devices to Protect

While there are multiple ways to categorize the various network security components, some of the more common network security device types include firewalls, access control, intrusion

CISA Urges Hardening Fortinet Devices After Reports of Credential ...

This activity, referred to as FortiBleed, involves the exposure of leaked credentials associated with approximately 74,000 Fortinet devices, including firewalls and virtual private network

5G Mobile Wi-Fi M8550

5G Mobile Wi-Fi M8550 Superior 5G - Up to 3.4 Gbps Download Speed Powerful Wi-Fi 6E - Tri-Band AXE3600 Network Gigabit WAN/LAN Port - Provide Stable

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

Zacks Investment Research

Hier sollte eine Beschreibung angezeigt werden, diese Seite lässt dies jedoch nicht zu.

Defending Against China-Nexus Covert Networks of Compromised Devices

United States Federal Bureau of Investigation (FBI) United States National Security Agency (NSA) Its purpose is to provide network defenders with the tools needed to defend against

Contact Us

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

Website: <https://www.tomor.eu>

Email: info@tomor.eu

Phone: +49 69 2381 5497

Address: Am Hauptbahnhof 10, 60329 Frankfurt am Main, Germany

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

