Architecture of Network Security Devices

Article Overview

A network security architecture diagram visually maps security devices, zones, and traffic flows to illustrate how an organization protects its network from threats.

Key Components of a Network Security Architecture Diagram

Firewalls and Perimeter Security: Firewalls are placed at network boundaries to control incoming and outgoing traffic, often separating internal networks from the internet or untrusted zones. They enforce access rules and prevent unauthorized access to sensitive resources . Demilitarized Zones (DMZ): DMZs host public-facing services like web servers and email gateways. They act as a buffer between external networks and internal systems, reducing exposure of critical assets . Intrusion Detection and Prevention Systems (IDS/IPS): These devices monitor network traffic for suspicious activity and can block or alert on potential threats. They are strategically placed along key network paths . Network Segmentation and Trust Zones: Networks are divided into zones (public, internal, restricted) using VLANs, subnets, and firewalls. Micro-segmentation limits lateral movement in case of a breach and enforces policy-based access . Identity and Access Management (IAM): Integration with IAM systems ensures that access is granted based on user identity, role, and device trust rather than just IP addresses. This supports zero-trust security models . Monitoring and Logging: Security Information and Event Management (SIEM) systems aggregate logs from devices to detect anomalies, support compliance, and enable rapid incident response . Secure Protocols and Encryption: TLS, SSH, and IPsec are used to encrypt data in transit, while encryption at rest protects stored data. These protocols are often highlighted in diagrams to show secure communication paths ....

Article Content

Secure Network Architecture

Networking is one of the most critical components of a corporate environment but can often be overlooked from a security standpoint.

Network Infrastructure Security Guide

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

Firewalls, IDS, and IPS Explanation and Comparison

This article will discuss the differences between network security devices – firewalls, Intrusion Prevention Systems (IPS), and

What Is Network Architecture?

Network architecture is the way network devices and services are organized to connect client devices such as laptops, tablets,

AWS Skill Builder

AWS Skill Builder is an online learning center where you can learn from AWS experts and build cloud skills online. With access to

What are public, private, and hybrid clouds? | Microsoft Azure

Learn the difference between public, private, and hybrid clouds. Compare features, benefits, and use cases to choose the best cloud

Network security fundamentals

Network security fundamentals How to design, use, and maintain secure networks. Networks are fundamental to the operation,

Network Security Architecture: Key Components and Best Practices

Network security architecture is the structured framework of technologies, protocols, and measures designed to protect a network

What Are Network Topology Architectures? Examples & Use Cases

Learn how network topology architectures are designed and used: 3 Tier Architecture, 2 Tier Architecture, Spine Leaf, WAN, Cloud etc.

What is computer networking?

Computer networking is the process of connecting two or more computing devices to enable the transmission and exchange of

Contact Us

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

Website: https://www.gmarkconstruction.co.za
Email: sales@gmarkconstruction.co.za
Phone: +31-6-15-38-72-94
Address: Herengracht 456, 1017 BS Amsterdam, Netherlands

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