Main Keyword	Network Segmentation
Search volume	8100
Length in Words	1K

1. Agile SEO Research

Short tail KWs

Phrase/word	Volume	Use?
What is Network Segmentation	1300	yes

Long tail KWs

Phrase/word	Volume	Use?
Benefits of Network Segmentation	140	yes
Network Segmentation Security	110	yes
network segmentation best practices	720	yes
types of network segmentation	110	yes

Top Search Results—URLs On First Page of Google

1. https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation
2. https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html
3. https://www.vmware.com/topics/glossary/content/network-segmentation.html
4. https://www.techtarget.com/searchnetworking/definition/network-segmentation
5. https://www.illumio.com/cybersecurity-101/network-segmentation
6. https://en.wikipedia.org/wiki/Network_segmentation
7. https://www.strongdm.com/blog/network-segmentation
8. https://www.comptia.org/blog/security-awareness-training-network-segmentation
9. https://www.zscaler.com/resources/security-terms-glossary/what-is-network-segmentation
10. https://www.geeksforgeeks.org/what-is-network-segmentation/

People Also Ask: What is Currently Showing in Google?

Questions showing immediately in Google search:

- What is meant by network segmentation?
- Which is an example of network segmentation?
- What are the 3 main purposes of network segmentation?

---

2. Proposed Outline

Article Length

To adequately cover this topic, we will need to upgrade the article to 2K words—it will then count as two articles. Do you approve?

YES, UPGRADE TO 2K / NO, LEAVE IT AS 1K

If not, we will need to remove some topics in the outline below. Please indicate if you have a preference which info to remove.

Outline

- What is Network Segmentation?What is Zero Trust
- Types of Network Segmentation
- What are the Benefits of Network Segmentation?
- Network Segmentation Security Best Practices
    - Assign Classification Labels to Each Asset
    - Map Data Flows Across the Network
    - Deploy a Segmentation Gateway
    - Audit Your Network Regularly
- Network Segmentation Challenges and New Approaches

==========

Article Info	Content
Page Main KW	Network Segmentation
Site Section	Cloud Native Academy → Application Security
Super Cluster	None
Topic Cluster	Application Security
Role in Cluster	Supporting Page
Cluster Plan	Aqua Content Clusters - Main Doc
Meta Title	What Is Network Segmentation?
Meta Description	Network segmentation is a method of dividing a computer network into multiple subnets to improve performance and security.
Planned Length	1000
Actual Length (excl. product content)	1149

What Is Network Segmentation?

Network segmentation is a method of dividing a computer network into multiple subnets to improve performance and security. By dividing the network into separate parts, network segmentation avoids single points of failure and makes it difficult for unauthorized users to compromise the entire network.

Network segmentation divides the network into zones and manages each zone separately. This means applying a traffic protocol to regulate traffic and identify if it is allowed to traverse a network segment or not. It also covers zone security protocols for managing security and compliance.

Network segments can be managed by their own dedicated hardware (physical segmentation) or via software (logical segmentation). Rules built into network configuration determine how users, services, and devices on a subnet can connect to each other and to other network segments.

This is part of a series of articles about application security.

In this article:

How Does Network Segmentation Promote Zero Trust?

Traditionally, segmentation has allowed network administrators to control traffic based on policies. Segmentation improves network monitoring, boosts performance, and isolates technical issues from other parts of the network.

Network segmentation with gateways and firewalls can also improve security in zero trust environments. Many companies have well-defined network structures that include a secure, internal network zone and an external, untrusted network zone. In a zero trust environment, all network zones are untrusted, including internal ones—segmentation can help protect sensitive network segments from others.

Segmentation allows network administrators to create micro-boundaries around their most important data, applications, assets, and systems. This is a second line of defense, in addition to authentication, which removes an attacker's ability to move laterally through the network.

Networks can be physically and logically segmented:

- **Physical segmentation** divides the network into smaller subnets separated by firewall gateways. In physical segmentation, subnets are physically separated from the architecture.
- **Logical segmentation** can achieve very similar results using addressing schemes and virtual local area networks (VLANs). This type of segmentation can be layered on top of an existing network, making it more flexible to structural changes.

When a network is segmented, traffic can be restricted through rules based on people, trust levels, departments, access control lists, and other modifiers, enabling zero trust network management.

Types of Network Segmentation

Physical segmentation techniques divide networks using dedicated hardware that supports each segment. It is the hardest type of segmentation to manage because each segment has a security perimeter and requires an Internet connection and firewall. Physically segmented networks don’t trust any external resources, but they usually trust everything internal.

Virtual segmentation encompasses the whole network, not only the perimeter. It uses switches to manage the virtual local area network (VLAN), with shared firewalls to reduce hardware requirements.

There are several ways to virtually segment a network:

- **VLAN segmentation**—uses subnets or VLANs to segment the network, connecting to hosts virtually or via network devices.
- **Firewall segmentation**—uses internally deployed firewalls to achieve segmentation between functional zones within the network.
- **SDN segmentation**—uses software-defined automation to create network overlays. This approach requires a complex setup to enable microsegmentation.

Network Segmentation Use Cases

Network segmentation is useful for various industry sectors:

- **Manufacturing—**manufacturers can separate their production lines and facilities to increase security and facilitate management. Network segmentation also helps provide

evidence of the backup systems' operational status for auditing purposes. Keeping production lines separate helps protect them from cyberattacks and ensures product integrity.
- **Healthcare**—providers can separate VLANs for different types of devices. For example, a hospital may create a VLAN for imaging devices such as MRI machines, another VLAN for monitoring devices like patient vital signs monitors, and a separate VLAN for administrative devices like computers and printers. This approach allows the hospital to better manage and secure these devices, as well as ensure that they are all operating on a network that is optimized for their specific needs.
- **Finance**—organizations can create a separate network segment for online banking transactions. This segment would be logically separated from other network segments, such as the segment for general internet browsing or internal company operations.

Here are some common use cases for network segmentation within an organization:

- **Employee network**—you can establish a dedicated network for employees with special access policies and rules. It allows you to monitor and filter employee activities or limit Internet access.
- **Remote-access network**—you can create a separate network with the VPN client enabled to support remote work.
- **Guest network**—create a secure network to protect guests and manage the activities of users outside your organization.
- **Quarantine**—you can put new devices on the network in a different environment with rules to block their access to the Internet or specific sites.
- **Device isolation**—you can create dedicated networks for specific IoT device categories (e.g., video cameras, security sensors). These devices can only communicate within the isolated network.

Network Segmentation vs. Microsegmentation

Traditional network segmentation divides the network into zones. A zone typically consists of multiple devices and hosted applications. Microsegmentation goes a step further and places each device or application in its own segment. It inspects all traffic between devices or applications for potentially malicious content, violations of corporate security policies, and access control rules.

Microsegmentation is implemented using software-defined networking (SDN). SDN's network infrastructure virtualization ensures that all traffic is routed through checkpoints such as next-generation firewalls (NGFWs). An NGFW can identify potential attacker lateral movements and block inappropriate access to corporate resources.

Microsegmentation is a more sophisticated form of network segmentation. It provides more granular visibility and security control, and ensures that all traffic between devices or applications within a network zone is inspected by NGFW, improving security.

Learn more in our detailed guide to microsegmentation (coming soon)

Network Segmentation Security Best Practices

Classify All Assets

Classify assets based on their business value and data sensitivity and attach labels to make asset management easier. Assets containing sensitive business and customer data usually require additional protection measures to ensure compliance with internal security policies and data regulations.

Visualize the Network's Data Flows

Network segmentation limits lateral movement but does not block all data flows. Some traffic traversing segment boundaries is necessary.

Map all the data flows throughout the network, including:

- **Northbound traffic**—goes out of the corporate network.
- **Southbound traffic**—enters a network segment.
- **East-west traffic**—moves between internal systems (within the perimeter).

Enforce Network Policies

Network policies enable more granular control over user access to different parts of the network. By monitoring user access to each network segment, organizations can ensure that only authorized users have access to sensitive data or systems. Creating access policies that meet specific user needs allows for a more efficient use of network resources and can help to prevent unauthorized access or data breaches.

By creating access policies that limit the access of users to specific parts of the network, organizations can make it more difficult for attackers to move laterally through the network and gain access to sensitive systems.

Audit the Network Regularly

Periodic audits are crucial to protecting the network and verifying that attackers cannot move from one segment to another. A poorly monitored network is a vulnerable one—you need to monitor traffic constantly to catch gaps in the network architecture. Audits also help inform you when updating the network architecture.

Securing Cloud Native Applications with Aqua Security

Aqua replaces outdated signature-based approaches with modern controls that leverage the cloud-native principles of immutability, microservices and portability. Using dynamic threat analysis, machine-learned behavioral whitelisting, integrity controls and nano-segmentation, Aqua enables modern application security protection across the lifecycle.

Aqua's full lifecycle security approach provides coverage for all clouds and platforms, integrating with enterprises' existing infrastructure and the cloud native ecosystem.

Secure the Build

Accelerate development by detecting security issues in your artifacts early and shortening time to remediate. "Shift left" security into the CI/CD pipeline, get full visibility into the security posture of your pipeline and reduce the application attack surface before application deployment.

Secure the Infrastructure

Enforce compliance across the stack, gain real-time visibility and control over your security posture. Monitor, detect, and automatically remediate configuration issues across public cloud services and Kubernetes clusters. Ensure conformity with CIS benchmarks, PCI-DSS, HIPAA, GDPR and other regulations.

Secure the Workloads

Protect applications in runtime using a zero trust model, with granular controls that accurately detect and stop attacks. Unify security across VMs, containers, and serverless on any cloud, orchestrator, and operating system. Leverage micro-services concepts to enforce immutability and micro-segmentation.

Key features:

- **Vulnerability scanning**: Scan CI pipelines and registries, container images, VM images, and functions. Find known vulnerabilities, malware, embedded secrets, OSS licensing, configuration, and permissions issues and prioritize based on potential impact

- **Dynamic Threat Analysis**: Detect and mitigate hidden malware and supply chain attacks in container images using a secure sandbox

- **Cloud Security Posture Management (CSPM)**: Continuously audit cloud accounts and services for security risks and auto-remediate misconfigurations

- **Container Security**: Use scan results to set policies for image deployment and prevent the use of unapproved images. Mitigate known vulnerabilities with Aqua vShield, preventing exploits with no code changes. Enforce container immutability by preventing drift against their originating images