Micro-segmentation

Cisco Partner
https://cs.co/1page

Micro-segmentation creates secure zones across the perimeter, campus, cloud and data center environments to isolate applications and secure them individually. Utilizing solutions to limit east-west traffic based on a zero-trust security approach to reduce attack surfaces and prevent the lateral movement of threats and breaches.

Benefits:

- Develop a highly secure segmentation strategy aligned with business objectives
- Reduce risk to your organization's data and assets
- Apply effective security and policy controls across multiple security disciplines
- Simplify your audit profile for reduced audit time and cost savings
- Secure data and intellectual property from internal and external cyber attacks
- Meet board-level requirements for security and compliance
- Effectively implement data classification programs

Conversation Starters:

Is containment or prevention of the lateral movement of threats a part of your organization's security strategy?

How does compliance factor into your industry, and what impact does it have on your security operations?

How are you getting visibility into application behavior? Managing policies?

How are you currently protecting and isolating sensitive data and critical assets?

How is your organization approaching zero trust?

What is your strategy for securing guests and their devices on your network?

Does your organization rely on firewall appliances to provide segmentation?

Use Cases:

Enterprise Segmentation for Compliance and Security: Separating lines of business, authenticated users from guests, or different types of traffic such as video surveillance from transactional data.

Workload Security: Automated micro-segmentation policy generation based on application dependencies.

Hybrid Mesh Firewall Use Cases: Enforcing identity and behavior-based segmentation policies across data center, cloud, campus, and factory environments. Protecting vulnerable IoT devices, reducing attack surfaces, and preventing lateral movement of threats. Supporting zero-trust principles with least-privilege access enforcement.

Related Solutions:

Cisco Duo: Enables identity-based micro-segmentation by integrating user, device, and application security into access policies.

Cisco Hypershield: An AI-native security architecture that embeds micro-segmentation into the network fabric from servers to cloud workloads providing granular protection beyond traditional perimeter firewalls. This approach reduces lateral movement to secure data centers and hybrid clouds.

Cisco Identity Services Engine (ISE): Control access and limit lateral movement of threats, all while simplifying guest access. Build segmentation and automate policy enforcement directly into the network, shutting down access closest to the resource to turn your network into the enforcer.

Cisco Rapid Threat Containment: A security framework that integrates Cisco ISE with network security tools (e.g. Secure Firewall) to automatically detect, quarantine, and mitigate infected endpoints.

Cisco Secure Workload: A micro-segmentation platform to secure applications across hybrid environments to provide visibility, automated policy recommendations to limit lateral movement of threats.

Hybrid Mesh Firewall: Creates micro-perimeters across hybrid, multi-cloud, and edge environments, enforcing Zero Trust policies using AI-driven management to coordinate security across firewalls, switches, and cloud-native applications.

Isovalent: Identity-aware micro-segmentation for containers and VMs. This enables granular, zero-trust security across hybrid cloud and Kubernetes environments leveraging eBPF for kernel-level visibility and control.

Multi Cloud Defense: Standardize multi-cloud threat defense and remove complexity.

Security Cloud Control: Centralized, consistent segmentation and threat defense across multi-cloud environments vs. challenging multi-vendor management.

Resources:

Micro-segmentation At-a-Glance		CISA Net Segmentation	NIST Sec Seg.
Network Segmentation	TrustSec	OWASP Net Segmentation	Public Page