The bridge to possible

Cisco SD-Access Visibility-Driven Segmentation

Control access and contain threats within zones of trust

You wake up to find out that another security incident has occurred. You're confused, and not sure how the attacker was able to get by your perimeter. But then you realize, you haven't had a perimeter for some time, because it has been pulled apart by cloud, mobility, and IoT.

Zero-trust is a security concept that solves for this dilemma by continually authorizing and granting minimal required access based on defined policies regardless of device location, and building "trust zones" to dynamically enforce these policies. Segmenting the network into trusted zones of access has been an accepted practice to control the lateral movement of traffic and malware. But this has rarely been accomplished in practice, leaving organizations with partial segmentation and partial protection.

Why? Because it has been slow to implement and impossible to continually ensure that the intent of the business is met and maintained as networks change. A barrier to network segmentation has been a lack of visibility into the identity of devices, how they interact with each other, and ensuring that policies don't cause reachability issues, thus shutting down critical business needs.

Benefits

- **Enhance visibility** using AI/ML-assisted device identification and grouping
- **Gain insights** into how endpoints are using the network and policy definitions
- **Reduce complexity** by easy-to-use policy authoring and enforcing tools
- **Enhance security by detecting** and responding quickly to threats and automating threat containment

The bridge to possible

"With Cisco SD-Access, we can automate and apply segmentation and security policies to our network devices up to 10 times faster than before."

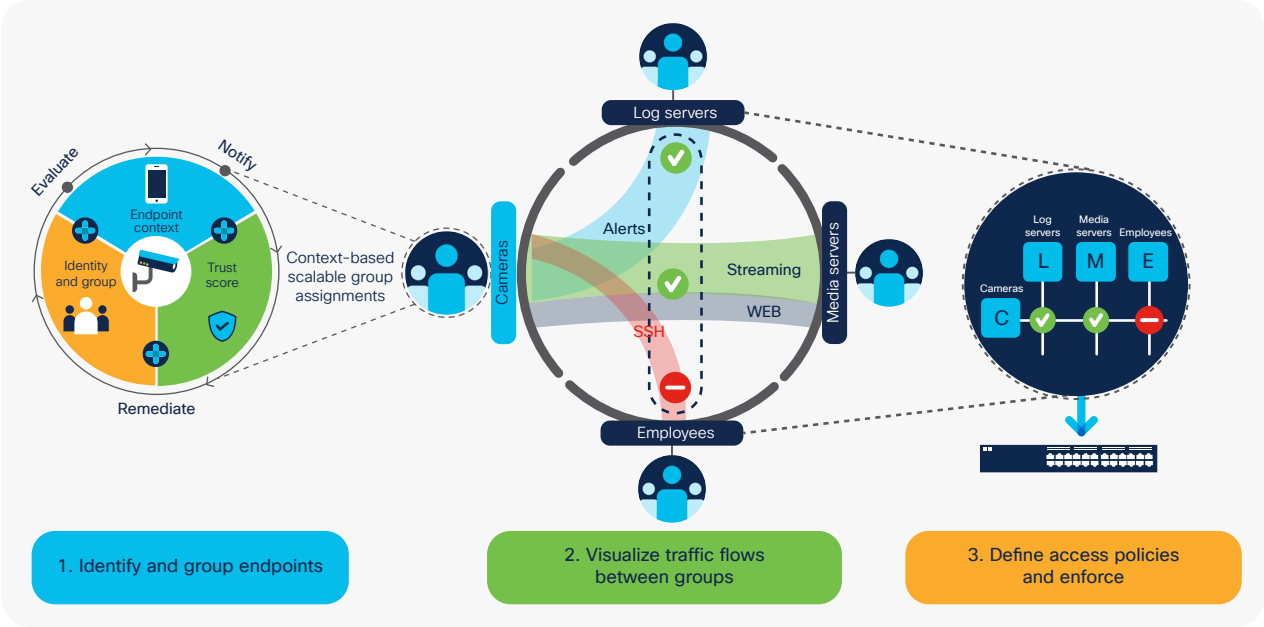
Frank Weiler
Head of Networking Department,
City of Luxembourg

Get started today

Achieving zero-trust with network segmentation is within reach, and easy with the Cisco SD-Access solution within Cisco Digital Network Architecture (Cisco DNA). For more details, please

- Read the white papers on AI Endpoint Analytics and group-based policy analytics
- Read the SD-Access solution overview
- Visit the SD-Access page

Figure 1. Three steps to visibility-driven segmentation.



Automate access control and policy enforcement

Visibility-driven segmentation within the Cisco® Software-Defined Access (SD-Access) solution extends zero-trust in the workplace to control access and contain threats within trusted zones. With the aid of machine learning and analytics, we dynamically identify devices, model and infer their behavior, and recommend segmentation policies. Policies are continually verified to ensure that providing protection does not disrupt the business intent and create reachability issues. Network segmentation has just been given an easy button. You can eliminate the manual configuration complexity of legacy approaches, which are tough to deploy, come with a lengthy manual process that does not keep up with rapid changes in the network, and are impossible to ensure. With visibility-driven network segmentation in place, organizations can shrink the attack surface, limit the spread of malware, and enable rapid threat containment, all while continually ensuring that this level of protection will not disrupt business outcomes.

C45-743709-03 06/21