The bridge to possible

Cisco Software-Defined Access

Introducing an entirely new era in networking.

Cisco® Software-Defined Access (SD-Access), a solution within Cisco Digital Network Architecture (Cisco DNA) which is built on intent-based networking principles, provides a transformational shift in building, managing, and securing networks, making them faster and easier to operate, with improved business efficiency. By decoupling network functions from hardware, it creates a virtual overlay over the underlying physical networking infrastructure. SD-Access helps ensure policy consistency by preventing unauthorized access and containing breaches, enabling faster launches of new business services and significantly improving issue-resolution times while being open, extensible, and reducing operational expenses. Digital transformation is forcing enterprises to search for new ways to enable digital capabilities, deliver IT services, and manage assets. We're moving toward a very different world. We need a very different network to get us there.

Benefits

- **Enhance visibility** of endpoints and traffic flows by using advanced analytics and AI/ML techniques to help define group-based access policies
- **Segment to secure** by dynamically applying the defined group-based access policies
- **Verify trust** by continuously scrutinizing the behavior of connected endpoints and isolate rogue or compromised endpoints to reduce threat proliferation
- **Exchange operating policies** and help ensure their consistency throughout the organization's access, WAN, and multicloud data center networks

The bridge to possible

Cisco Services

Accelerate your journey to a digital-ready network with Cisco Software-Defined Access services.

Cisco Services provide expert guidance to help you achieve a streamlined operational model across wired and wireless environments at a lower cost. With proven experience, best practices, and innovative tools, Cisco Services work with you to easily manage, scale, and secure your Cisco SD-Access solution. By choosing from a comprehensive life cycle of services–including advisory, implementation, optimization, and technical services–you can move to a secure and automated unified network with ease and confidence. Learn more.

C45-738181-07 12/20

Why SD-Access?

Rapid digital transformation of organizations has resulted in an increasing dependency on IT, and networks are called upon to be more agile and respond to changing business needs faster. But with the growing number of users, surging use of IoT devices, and rising adoption of clouds, traditional networks have struggled to keep up. Intent-based networking (IBN), an industry initiative, transforms a hardware-centric, manual network into a controller-led network that captures business intent and translates it into policies that can be automated, can be applied consistently across the network, and can make the network stay in step with business requirements.

Cisco DNA defines a campus-and-branch architecture that implements the IBN framework. SD-Access, a solution within Cisco DNA, applies policies derived from business intent to control access, increase scale, and boost security. You can use SD-Access capabilities to:

- **Enhance your visibility into endpoints and traffic patterns:** AI endpoint analytics uses deep packet inspection (DPI), telemetry sources, and AI/ML techniques to identify, profile, and group endpoints. Group-based policy analytics examines traffic flows between groups and helps you formulate and fine-tune group-based access policies
- **Achieve zero-trust security by granular segmentation:** Enforce group-based policies through the network infrastructure for segmenting the network and controlling traffic flows without using complex firewalls, access control lists (ACLs), and virtual LANs (VLANs) that can be difficult and costly to maintain
- **Continuously verify trust:** Unlike traditional approaches that implicitly trust everything inside the corporate network, SD-Access continuously ensures that the original tenets used to establish trust are true, and that the traffic is not threat traffic, to detect anomalous or malicious behavior or a compromised endpoint
- **Help ensure enterprise-wide consistency** by exchanging policies with other networking domains so that access control is enforced from access to application – spanning access (SD-Access), WAN (Cisco SD-WAN), and multicloud data center (Cisco ACI®) networks using the Cisco intent-based networking multidomain architecture

How do you get started?

For more information about SD-Access:

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