Cisco Software-Defined Access

What is Cisco® Software-Defined Access?

Cisco® Software-Defined Access (SD-Access) is a central part of the Cisco Digital Network Architecture (Cisco DNA™) solution and represents an exponential and fundamental shift in how we design, build, and manage networks, enabling enterprise customers to reduce Operating Expenditures (OpEx) and risk while creating an agile infrastructure that delivers consistent policies and services over wired, wireless, and hybrid networks.

This solution provides policy-based automation from the edge to the cloud with secure segmentation for users and things enabled through a single network fabric, drastically simplifying and scaling operations while providing complete visibility and delivering new services quickly.

By automating day-to-day tasks such as configuration, provisioning, and troubleshooting, SD-Access reduces the time it takes to adapt the network, improves issue resolution, and reduces the impact of security breaches. This results in significantly simpler operations and lower costs.

Is there a tool for the management of SD-Access?

SD-Access is managed with Cisco DNA Center, a centralized software dashboard for managing your enterprise network. Cisco DNA Center uses intuitive workflows to simplify provisioning of user access policies combined with advanced assurance capabilities. For more information on Cisco DNA Center, visit: http://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html.

Q
A

What are some of the capabilities of Software-Defined Access?

SD-Access includes the following capabilities:

End-to-end segmentation	▪ Identity-based segmentation on the network allows various secure corporate, facilities/IoT, and guest user devices to be kept separate and secure while on the same network infrastructure. ▪ Security provided by Cisco TrustSec® infrastructure (Security Group Tags [SGT], Security Group Access Control Lists [SGACL]) and Cisco segmentation capabilities (Cisco Locator/ID Separation Protocol [LISP], Virtual Extensible LAN [VXLAN], and Virtual Routing and Forwarding [VRF]). ▪ Identity context for users and devices, including authentication, posture validation, and device profiling, provided by the Cisco Identity Services Engine (ISE).
Network automation	▪ Simplified network operations through a single point of automation, orchestration and management of network functions using the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM). ▪ Ability to quickly enable services by using open APIs across a services ecosystem (for example, voice, Cisco Wide Area Application Services [WAAS)], native third-party apps).
Single network fabric	▪ Assurance visibility that delivers proactive operations and predicts performance through machine learning by automatically collecting device, application, and user data. The Network Data Platform (NDP) efficiently categorizes and correlates vast amounts of data into business intelligence and actionable insights. ▪ Complete network visibility: simple management of LAN, WLAN, and WAN as a single entity for simplified provisioning, consistent policy, and management across wired and wireless. ▪ Single-pane-of-glass network control with Cisco DNA Center software.

Q
A

What are the benefits of SD-Access?

SD-Access provides the following benefits:

Secure, policy-based automation	SD-Access enables policy-based, automated network enforcement for access, security, application quality, and monitoring across all network domains. Instead of defining a policy separately for your LAN, wireless LAN, and WAN, you define it only once and apply it to all three domains.
Complete network visibility	View the entire wired and wireless network fabric and enable flexible Layer 2 and 3 services on a wired, wireless, and WAN network that is managed as single entity.
Fast and easy service enablement	Quickly enable services through controller-based abstraction and open APIs, with fabric-aware security across a services ecosystem. This means you can provide your business with fast and easy service enablement to drive innovation and reduce costs.
Reduced network provisioning time	Allow IT to get a branch office running quickly, or to roll out new services and applications faster with efficiency and optimal experience. Controller-based abstractions provide simple workflows that follow Cisco best practices, so IT can focus on business intent and allow the controller to automate network management.
Improved issue resolution	Obtain deep insights into users' behavior, application performance, and threats, so you can take immediate action to optimize factors such as employee productivity, customer experience, and daily processes.
Fewer security breaches	Enhance the network to act as both a sensor and enforcer – all the way from the clients to the applications. Contain risk through integrated security services that rapidly detect and mitigate threats. Maintain and validate compliance with legal and security policies of the organization.

Q What's the difference between Software-Defined Networking (SDN) and Cisco DNA and SD-Access? How do they relate to one another?

A The Open Networking Foundation (ONF) defines SDN as "an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions, enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services."

Cisco DNA transcends the technology-centric collection of network technologies that make up SDN and concerns itself with bringing these technologies together into a holistic architecture to achieve business outcomes. Cisco DNA is a way to make network services relevant as well as easy to use in an enterprise architecture journey to digital transformation. It is an architectural suite that includes ready-to-use applications as well as easily consumed APIs. Cisco is committed to helping our customers successfully evolve to SDN while maximizing their investment protection.

SD-Access is the foundation of Cisco DNA. It enables network access in minutes for any user or device to any application, without compromise. With SD-Access the established policies automatically follow the user across all network domains.

Q Which Cisco hardware and software platforms support SD-Access?

A The following platforms support SD-Access:

- Cisco Catalyst® 9300, 9400, and 9500 Series Switches
- Cisco Catalyst 3850 and 3650 Series Switches
- Cisco Catalyst 4500E Series Switches with Supervisor Engine 8-E and 4700 line cards
- Cisco Catalyst 6880-X or 6840-X Switches
- Cisco Catalyst 6807-XL with Supervisor Engine 2T or 6T and 6800 Series 10 Gigabit Ethernet cards
- Cisco Catalyst 6500 Series Switches with Supervisor Engine 2T or 6T
- Cisco Nexus® 7700 Switches with Supervisor Engine 2E and M3 line cards
- Cisco ASR 1001-X, 1002-X, 1006-X, 1009-X, 1001-HX, and 1002-HX Routers
- Cisco 4431, 4432, and 4451-X Integrated Services Routers
- Cisco Cloud Services Router (CSR) 1000V
- Cisco 3504, 5520, 8510, and 8540 Wireless Controllers
- AireOs Wave 2 access points: Cisco Aironet® 1800, 2800, and 3800 Series

How does SD-Access save on OpEx?

A

The SD-Access solution simplifies LAN, WLAN, and WAN deployments, increases network reliability, reduces risk, and enables faster service delivery, all of which lead to increased business continuity and reduced OpEx.

For example, the growth of user and device mobility, the growth of the network, and an ever-evolving security landscape all force network administrators to constantly update security policies. This process is labor intensive and often leads to misconfigurations that cause service disruptions on the network, require troubleshooting, and increase costs. SD-Access allows network administrators to consistently and quickly apply policy updates in a few minutes instead of hours or weeks.

What is secure segmentation with SD-Access, and why is it important for an enterprise?

A

Different users and functions within a business need different levels of access on the network. For example, a guest should not have access to business-sensitive data. To implement segmentation today, an organization is probably using VRFs, VLANs, and ACLs. All of these options would achieve the desired secure segmentation, but they are also labor intensive, difficult to modify, and prone to error.

The SD-Access solution delivers the secure segmentation that enterprise networks require to protect their bottom line, and it does so using orchestration that simplifies implementation. Using SD-Access, it is easier to securely segment the network to support guest, corporate, facilities, and IoT-enabled infrastructure.

How is SD-Access licensed?

A

SD-Access is provided as a part of Cisco DNA, and services are delivered through Cisco ONE™ Software, which provides simplified, high-value solutions with license portability and purchase flexibility. Customers can start their Digital Network Architecture journey today on our current portfolio and know that they can continue to adopt network innovations in the months and years ahead through the power of software.

How do I get started?

A

Cisco Advanced Services and authorized Cisco partners can help you begin your journey with strategy and analysis services and readiness assessments, as well as planning, design, and migration services.

Where do I learn more?

A

http://www.cisco.com/go/sdaccess.

C67-739178-00 06/17