# Cisco Multidomain Integrations for Intent-Based Networking

## Policy and assurance integrations between technology domains

### Benefits

Cisco ACI with AppDynamics integration – identify problems faster by correlating applications and network data:

- Monitor performance, improve performance, and provide consistent security for your business applications wherever they go
- Enable visibility into application tiers and their correlation with networking constructs
- Correlate application health and network constructs for optimal application performance, deeper monitoring, and faster root cause analysis
- Cross-launch Cisco ACI, AppDynamics, and SD-Access to correlate network and application data

Cisco ACI with SD-Access integration – automate identity-access management from users to applications:

- Through a single pane of glass, consistently enforce segmentation policy based on the user's security profile as they access resources within the data center
- Enable security administrators to manage segmentation seamlessly from end to end, from user to application
- Provide a common and consistent identity-based microsegmentation capability from user to application

Cisco ACI with SD-WAN integration – help ensure a great application experience:

- Define application Service-Level Agreement (SLA) parameters once in the data center and propagate to SD-WAN automatically
- Let SD-WAN select the best path and prioritize the traffic appropriately through to the campus and branch user. Enable an optimum application experience

Cisco SD-Access with SD-WAN integration – extend consistent access control to all sites of the organization:

- Enforce identity-based access control throughout the enterprise, even between sites across the SD-WAN
- Avoid slow and complex tunneled links between sites

Consistent security – automate visibility, threat detection, and mitigation across all domains:

- Limit user and device access to protected resources, sensitive data, and critical applications with end-to-end segmentation
- Protect users no matter where they are, and the applications they are accessing – whether on the internet or in the data center or cloud – with comprehensive security applications



## Challenges

Large and medium-sized organizations need to adopt a holistic network infrastructure strategy to cope with the unique performance, security, and management challenges of highly distributed applications, data, users, and devices. Legacy approaches that have relied on manual processes to secure data and applications and control access to them are no longer adequate or sustainable.

The networking industry has recognized these challenges and is addressing them in the form of an intent-based architectural approach that builds on software-defined networking to allow continuous, dynamic network alignment with IT and business policies. This means that application, security, and compliance policies can be defined once and enforced and monitored between any groups of users or things and any application or service – or even between application and services themselves – wherever they are located.

### What's required to overcome these challenges?

To achieve this desired outcome requires an intent-based network architecture across all network domains, including campus, branches, SD-WAN, and private and public clouds. Cisco can help IT teams achieve this goal by guiding customers in a step-by-step journey that prioritizes their technology investments and accelerates intent-based infrastructure deployments across all of these domains.

Cisco's intent-based networking solutions extend across campus and branch access networks with Cisco DNA, across the WAN with Cisco® SD-WAN, and across distributed application environments with Cisco ACI™. We are now taking steps to apply policy and assurance integration across these domains to enable consistent performance, compliance, and security enforcement that allows IT and business intent to be expressed in one domain and then exchanged, enforced, and monitored across all of them. We are implementing our strategy toward this multidomain, intent-based networking with the following integrations:

- Cisco ACI with Cisco AppDynamics®
- Cisco ACI with Cisco SD-Access
- Cisco ACI with Cisco SD-WAN
- Cisco SD-Access with Cisco SD-WAN
- Comprehensive and consistent security over all domains

## Cisco ACI and AppDynamics assurance integration

Digital transformation is a complex team effort across business and IT, requiring end-to-end application management and awareness. AppDynamics provides IT teams the application-layer visibility and monitoring required in an intent-based architecture to validate that IT and business policies are being implemented across the network. Cisco ACI and AppDynamics integration provides dynamic correlation between application and network constructs. This combined solution provides high-quality application performance monitoring, richer diagnostic capability for application and network performance, and faster root-cause analysis of problems, with fast triage, sent to the right people quickly – for example, does a given problem pertain to an application or to the network?

Figure 1. Cisco ACI and AppDynamics integration


This integration does the following:

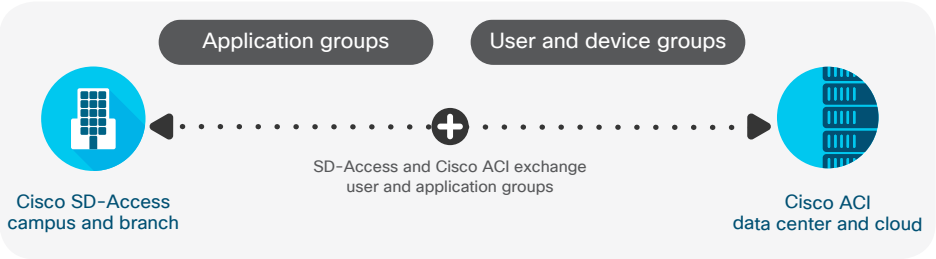
- Dynamically maps the application and service components to the Cisco ACI network elements, thus providing a shared view of the application and infrastructure across teams
- Provides a dynamic view of application use in the infrastructure for the network operations team
- Provides a cross-launch for application teams to correlate network and application fault and performance data
- Baselines application health status in AppDynamics by correlating the Cisco ACI network health and faults

Customers are on a continuous quest to correlate application service-level management with infrastructure monitoring. This new integration will significantly reduce the time it takes to identify and troubleshoot end-to-end application performance issues.

# Cisco ACI and SD-Access policy integration

Hyper-distributed applications and highly mobile users, increased cybersecurity threats, and increased regulatory requirements make network segmentation a must for reducing risk and achieving better compliance. Policy integration between Cisco ACI and SD-Access allows the marrying of Cisco ACI's application-based microsegmentation in the data center with Cisco SD-Access's user-group-based segmentation across the campus and branch. This integration automates the mapping and enforcement of segmentation policy based on the user's security profile as they access resources within the data center. It enables security administrators to manage segmentation seamlessly from end to end, user to application. A common and consistent identity-based microsegmentation capability is provided from the user to the application.

Figure 2. Cisco ACI and SD-Access integration




As a result of this integration, the attack surface is greatly reduced, and any unauthorized or suspicious access to resources and potential threats can quickly be controlled and remediated. The solution is fully qualified for up to 25,000 SD-Access campus users, with plans to expand scale as needed by our customers.

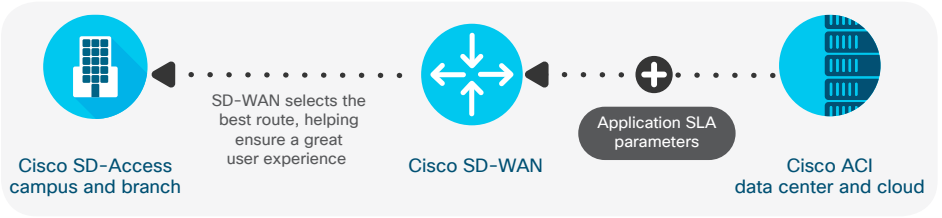
Use case: An Internet of Things (IoT) application and a finance application are both hosted in the data center. IoT devices are distributed throughout the extended enterprise network environment and segmented into a separate user group from the employees' group. By mapping between Cisco ACI and SD-Access segments, end-to-end policy can be enforced automatically so that only specific IoT devices and IT administrators have access to the IoT application.

At the same time, a policy can be set and enforced that gives only finance department employees and executives access to the finance application, regardless of their location. The result is a greatly reduced risk of breach for both the IoT and finance users and applications.

# Cisco ACI and SD-WAN application experience policy integration

Cisco ACI and SD-WAN integration extends operational domain and consistent policy to the branch and public cloud. This combined solution delivers high-performance, reliable branch access to public cloud services, on-premises data centers, and enterprise Software-as-a-Service (SaaS) applications.

Figure 3. Cisco ACI and SD-WAN integration




As new applications are introduced, and as applications dynamically move between an on-premises data center and public clouds, assuring a seamless, high-quality user experience with those applications can be challenging. This integration allows Cisco ACI to convey the applications' SLA requirements, consisting of delay, latency, jitter, etc., to the SD-WAN, which can then automatically select the best path and prioritize application traffic correctly to help ensure a great experience regardless of the application's or user's location.

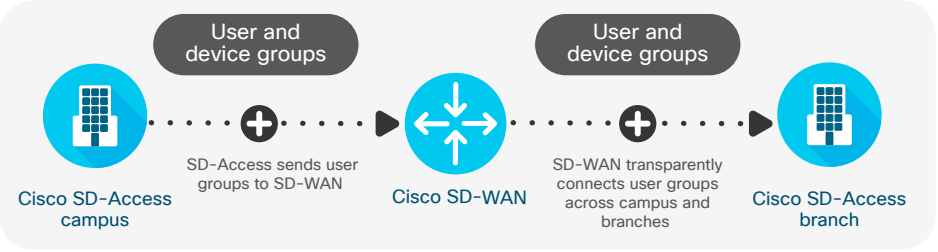
This integration allows you to:

- Define application SLA requirements once that are carried with the application no matter where it is hosted – in an on-premises data center or in the cloud
- Help ensure the best experience for the user no matter where the application and user are

# Cisco SD-Access and SD-WAN segmentation policy integration

Policy integration between Cisco SD-Access and SD-WAN extends SD-Access's group-based segmentation and creates a unified access fabric throughout the enterprise. Cisco SD-WAN transparently carries the segmentation elements across all sites for consistent policy enforcement.

Figure 4. Cisco SD-Access and SD-WAN policy integration



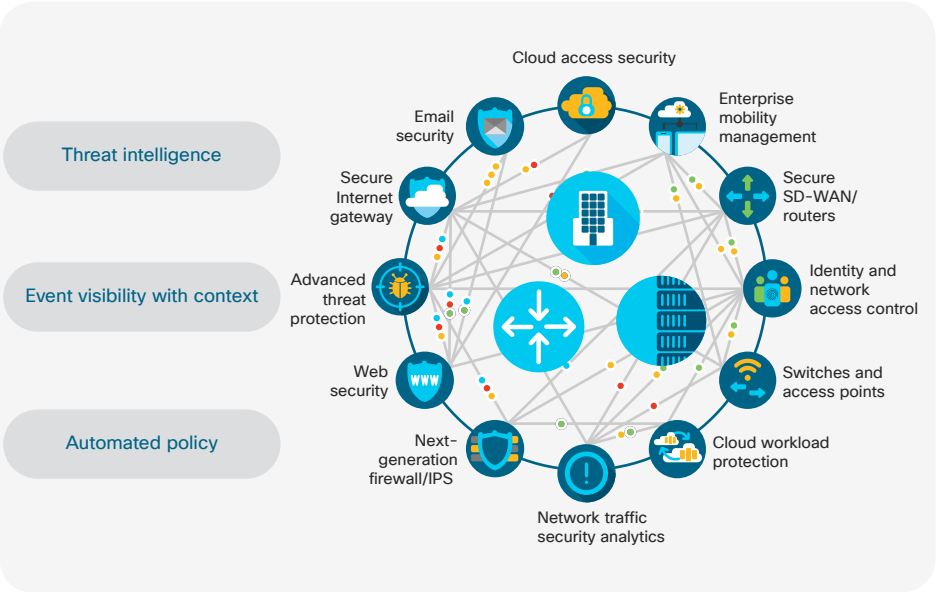

Cisco SD-Access creates an overlay for network segmentation and assigns users and things to one of these segments based on their access privileges. This overlay network enforces separation of traffic and prevents unauthorized access to protected resources. Without the policy integration, WAN networks are not able to transport the overlay, creating uneven segmentation, monitoring, and assurance. This integration allows you to:

- Enforce a common set of access control policies uniformly throughout the enterprise
- Avoid slow and complex VPN or tunneling connections between sites
- Enhance enterprise-wide data collection, analytics, and assurance

# Cisco multidomain security

Security applications from Cisco help ensure complete coverage over all networking domains. End-to-end segmentation from user access to the cloud separates traffic and protects resources from unauthorized use. In the campus and branches, Cisco Advanced Malware Protection (AMP) provides maximum protection against advanced malware. In the cloud, Cisco Stealthwatch® public cloud monitoring extends threat detection to the public cloud infrastructure, including Google Cloud Platform, Microsoft Azure, and Amazon Web Services. Cisco Umbrella™, a secure internet gateway in the cloud, uses DNS to stop threats over all ports and protocols, routes requests to risky domains for deeper URL and file inspection, and prevents connections to an attacker's servers.

Figure 5. Cisco multidomain security




Although the threat sources might be different, security needs across networking domains are similar. Cisco security applications for networking domains meet the following security needs:

- Continuous visibility: Identify who and what is on the network and how they are communicating, and determine their risk profile
- Trusted access: Verify user, application, and traffic identity before granting access to the network
- Constant protection: Detect and mitigate threats across endpoints, network, and cloud

## Call to action

For a demo of Cisco ACI and AppDynamics integration, see: https://www.cisco.com/c/m/en_us/products/data-center/software-demos/aci/aci-appd-integration-demo.html

For a demo of Cisco ACI and SD-Access, see: https://www.cisco.com/c/m/en_us/products/data-center/software-demos/aci/aci-ise-integration-demo.html

Learn more about Cisco ACI: https://www.cisco.com/go/aci

Learn more about Cisco SD-Access: https://www.cisco.com/go/sda

Learn more about Cisco SD-WAN: https://www.cisco.com/go/sdwan

## Cisco is uniquely positioned to deliver intent-based networking throughout the enterprise

- Only Cisco is executing on the vision of end-to-end intent-based networking – from any user anywhere to any workload anywhere
- Only Cisco has leadership and best-in-class, purpose-built, intent-based networking across campus, branch, WAN, data center, colocation centers, and multicloud domains
- Only Cisco integrates security uniformly across all domains



C45-741877-01 06/19