White Paper

Cisco Application Centric Infrastructure Microsegmentation Solution

Cisco® Application Centric Infrastructure (Cisco ACI™) simplifies the deployment and management of microsegmentation policies across all virtual switch and bare-metal server environments for any type of workload (physical, virtual, or container) based on virtual machine or network attributes or endpoint-group isolation policy

BENEFITS

- Microsegmentation for any multitiered application with physical or virtual workloads across any hypervisors
- Use of the same policy model to isolate workloads for VMware vSphere, Microsoft Hyper-V, OpenStack containers, and bare-metal servers
- Microsegmentation classification using workload attributes such as virtual machine attributes and network attributes (IP and MAC addresses), providing more specific control at the individual virtual machine level
- Hypervisor-independent intra-EPG isolation policy across virtual machines and bare-metal devices
- Simple, automatic creation of a quarantine security zone for a multitiered application when a rogue endpoint or threat is identified, followed by automated remediation

Overview

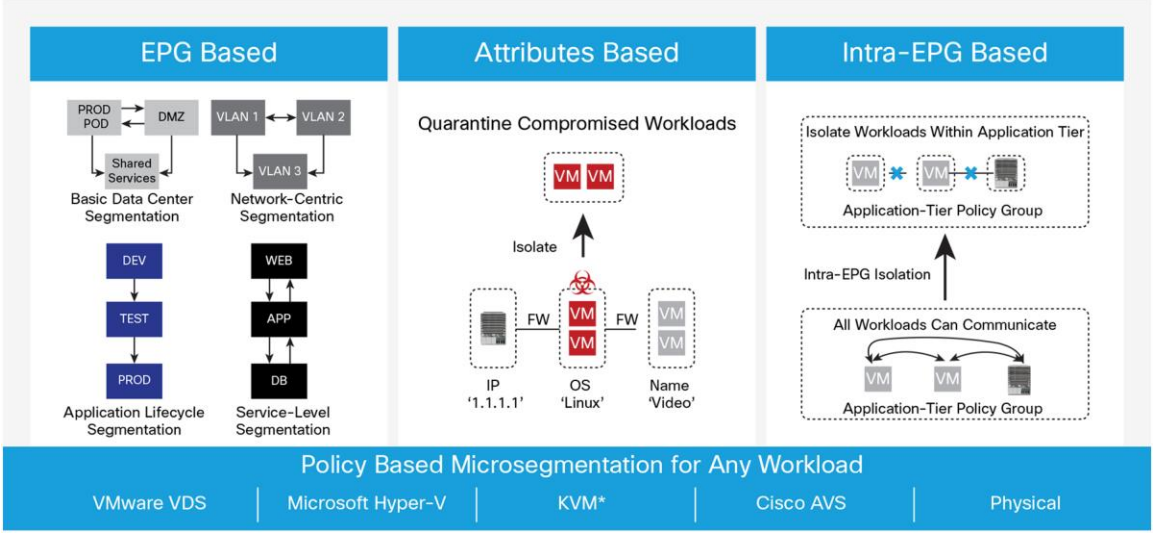
Data center architectures have continually evolved to meet the needs of mobile, social, big data, and cloud applications. Security architectures have been evolving as well to support the security needs of these distributed applications in distributed data centers.

Organizations are under unrelenting attack, and security breaches are happening every day. According to Cisco, 75 percent of all attacks begin stealing data within minutes, but detection takes longer. After an attack has been discovered, several weeks may pass before full containment and remediation are achieved.

To address this problem, Cisco ACI provides embedded security and policy-based automation using the endpoint group (EPG) and contract constructs. An EPG by definition is a microsegment, and its security enforcement policy is defined by a contract that consists of a built-in stateless whitelist firewall and Layer 4 through Layer 7 (L4-L7) service insertion policy that supports a robust ecosystem of L4-L7 partners for next-generation firewall (NGFW) and next-generation intrusion prevention system (NG-IPS) solutions, application analytics, and more.

Cisco ACI extends microsegmentation and intra-EPG isolation security for physical and virtual workloads in a data center using simple policy constructs. Cisco ACI now normalizes policy-based microsegmentation to secure any type of workload regardless of the application topology or the location of the workload (Figure 1).

Figure 1. Cisco ACI Microsegmentation Works Across VMware, Microsoft, and OpenStack Virtual Machines, Bare-Metal Servers, and Containers



Why Micro-segmentation Matters

Although the broad constructs of segmentation are relevant, today's application and security requirements mandate increasingly specific methods that are more secure and operationally simpler. This need has led to the evolution of microsegmentation, which has the following goals:

- Programmatically define segments on an increasingly specific basis, achieving greater flexibility (for example, limit the lateral movement of a threat or quarantine a compromised endpoint within a broader system).
- Automatically program segment and policy management across the entire application lifecycle (from deployment to decommissioning).
- Enhance security and scalability by enabling a zero-trust approach for heterogeneous workloads.

Cisco ACI microsegmentation embodies four main functions: isolation, segmentation with integrated security, closed-loop feedback, and automated remediation.

Main Features

Cisco ACI takes an elegant approach to microsegmentation, with policy definition separating segments from the broadcast domain.

It uses a new application-aware construct called the endpoint group, or EPG, that allows application designers to define the endpoints that belong to the EPG regardless of their IP addresses or the subnets to which they belong. In addition, the endpoint can be a physical server, a virtual machine, a Linux container, or even traditional mainframe computers: that is, the type of endpoint is normalized and therefore irrelevant, thereby offering simplicity and flexibility in the treatment of endpoints.

Cisco ACI provides microsegmentation support for VMware vSphere Distributed Switch (VDS), Microsoft Hyper-V virtual switch, and bare-metal endpoints, allowing highly specific endpoint security enforcement. Customers can dynamically enforce forwarding and security policies, quarantine compromised or rogue endpoints based on virtual machine attributes (such as the name, guest OS, or virtual machine identifier) and network attributes (such as the IP address), and restore cleaned endpoints to the original EPG.

Data center microsegmentation can provide enhanced security for east-west traffic within the data center. Its true value lies in its integration with application design and holistic network policy, and it must interoperate transparently with a wide variety of hypervisors, bare-metal servers, L4-L7 devices, and orchestration platforms.

Cisco Application Centric Infrastructure: Agile, Open, and Secure

Cisco ACI is the industry's most comprehensive software-defined networking (SDN) architecture. It dramatically reduces total cost of ownership (TCO), automates IT tasks, and accelerates data center application deployments. It supports a business-relevant application policy language, greater scalability through a distributed enforcement system, and greater network visibility through the integration of physical and virtual environments across networks, servers, storage, security, and services.

Cisco ACI lets your technology team respond more quickly to changing business and application needs, enhances agility, and adds more value to your organization. Microsegmentation provides internal control of traffic within the data center and can greatly enhance a data center's security posture. Cisco ACI is the only solution available today that enables true microsegmentation with the performance, scalability, and visibility that modern applications demand.

Use Cases

Table 1 summarizes common use cases for Cisco ACI microsegmentation.

Table 1. Common Use Cases

Use Case	Description
Microsegmentation to quarantine vulnerable virtual machines across multihypervisor domains	• Use common policy automation to secure workloads even across an environment with mixed hypervisors and bare-metal servers. • Isolate a rogue virtual machine or threat within a bridge domain or EPG.
Microsegmentation of a multitiered application with L4-L7 service insertion	Insert L4-L7 load-balancer or firewall services between microsegments defined using workload virtual machine or network attributes.
Microsegmentation of a multitiered application for remediation	Quarantine within a web tier of workloads to protect the rest of the web and other application tiers.

Why Cisco ACI?

Cisco ACI supports a business-relevant application policy language, greater scalability through a distributed enforcement system, and greater network visibility through the integration of physical and virtual environments within one policy model for networks, servers, storage, services, and security. Through Cisco ACI, customers are reducing application deployment times from weeks to minutes, and dramatically improving IT alignment with business objectives and policy requirements. With Cisco ACI microsegmentation, IT departments can benefit from more targeted isolation and segmentation, segmentation with integrated security, closed-loop feedback, and automated remediation.

Next Steps

To learn more about how a Cisco ACI solution can benefit your organization, visit http://www.cisco.com/go/aci.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-736420-00 12/15