Cisco Application Centric Infrastructure Security

Cisco Application Centric Infrastructure Overview

Cisco® Application Centric Infrastructure (ACI) is an innovative architecture that radically simplifies, optimizes, and accelerates the entire application deployment lifecycle.

Cisco ACI uses a holistic systems-based approach, with tight integration between physical and virtual elements, an open ecosystem model, and innovation-spanning application-specific integrated circuits (ASICs), hardware, and software. This unique approach uses a common policy-based operating model across network and security elements that support Cisco ACI (computing; storage in the future), overcoming IT silos and drastically reducing costs and complexity.

Security Problems Addressed by Cisco ACI

Cisco ACI addresses the security and compliance challenges of next-generation data center and cloud environments.

With organizations transitioning to next-generation data center and cloud environments, automation of security policies is needed to support on-demand provisioning and dynamic scaling of applications. The manual device-centric approach to security management is both error prone and insecure. As application workloads are being added, modified, and moved in an agile data center environment, the security policies need to be carried with the application endpoints. Dynamic policy creation and deletion is needed to secure east-west traffic and handle application mobility. Visibility into the traffic is important to identify and mitigate new advanced targeted attacks and secure the tenants.

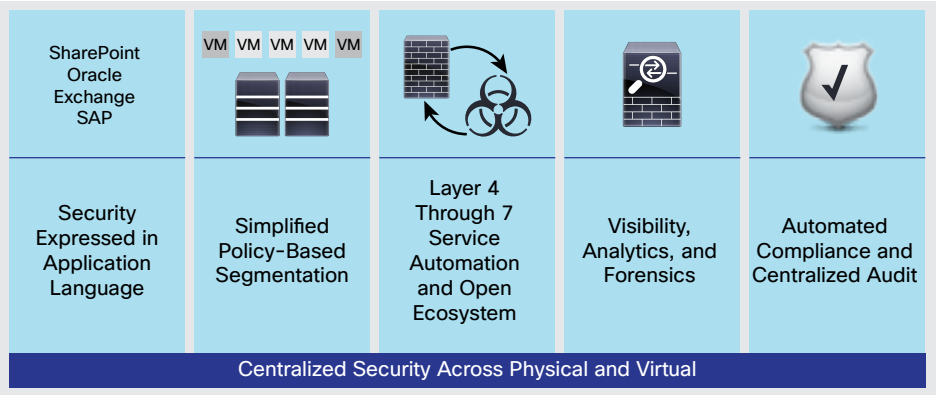
These new requirements need to be supported while helping ensure compliance with industry regulations such as Payment Card Industry (PCI) and Health Insurance Portability and Accountability Act (HIPAA) mandates.

Cisco ACI Security for Next-Generation Data Center and Cloud

The Cisco ACI Security Solution uses a holistic, systems-based approach to address security needs for next-generation data center and cloud environments (Figure 1). Unlike alternative overlay-based virtualized network security solutions, which offer limited visibility and scale and require separate management of underlay and overlay network devices and security policies, the Cisco ACI Security Solution uniquely addresses the security needs of the next-generation data center by using an application-centric approach and a common policy-based operations model while helping ensure compliance and reducing the risk of security breaches.

The Cisco ACI Security enables unified security policy lifecycle management with the capability to enforce policies anywhere in the data center across physical and virtual workloads. It offers complete automation of Layer 4 through 7 security policies and supports a defense-in-depth strategy with broad ecosystem support while enabling deep visibility, automated policy compliance, and accelerated threat detection and mitigation. Cisco ACI is the only approach that focuses on the application by delivering segmentation that is dynamic and application centered.

Figure 1. Cisco ACI Addresses Next-generation Datacenter and Cloud Security Requirements



Main Benefits of Cisco ACI Security

Main features and benefits of the Cisco ACI Security include:

- **Application-centric policy model:** Cisco ACI provides a higher-level abstraction using endpoint groups (EPGs) and contracts to more easily define policies using the language of applications rather than network topology. The Cisco ACI whitelist-based policy approach supports a zero-trust model by denying traffic between EPGs unless a policy explicitly allows traffic between the EPGs.
- **Unified Layer 4 through 7 security policy management:** Cisco ACI automates and centrally manages Layer 4 through 7 security policies in the context of an application using a unified application-centric policy model that works across physical and virtual boundaries as well as third-party devices. This approach reduces operational complexity and increases IT agility without compromising security.

- **Policy-based segmentation:** Cisco ACI enables detailed and flexible segmentation of both physical and virtual endpoints based on group policies, thereby reducing the scope of compliance and mitigating security risks.
- **Automated compliance:** Cisco ACI helps ensure that the configuration in the fabric always matches the security policy. Cisco APIs can be used to pull the policy and audit logs from the Cisco Application Policy Infrastructure Controller (APIC) and create compliance reports (for example, a PCI compliance report). This feature enables real-time IT risk assessment and reduces the risk of noncompliance for organizations.
- **Integrated Layer 4 security for east-west traffic:** The Cisco ACI fabric includes a built-in distributed Layer 4 stateless firewall to secure east-west traffic between application components and across tenants in the data center.
- **Open security framework:** Cisco ACI offers an open security framework (including APIs and OpFlex protocol) to support advanced service insertion for critical Layer 4 through 7 security services such as intrusion detection systems (IDS) and intrusion prevention systems (IPS), and next-generation firewall services (such as the Cisco Adaptive Security Virtual Appliance (ASAv), the Cisco ASA 5585-X Adaptive Security Appliance, and third-party security devices) in the application flow regardless of their location in the data center. This feature enables a defense-in-depth security strategy and investment protection.
- **Deep visibility and accelerated attack detection:** Cisco ACI gathers time-stamped network traffic data and supports atomic counters to offer real-time network intelligence and deep visibility across physical and virtual network boundaries. This feature enables accelerated attack detection early in the attack cycle.
- **Automated incident response:** Cisco ACI supports automated response to threats identified in the network by enabling integration with security platforms using northbound APIs.

Why Cisco?

The Cisco ACI architectural approach provides a continuous and pervasive way to weave security into the fabric of today's dynamic, application-oriented data centers. The Cisco ACI Security delivers visibility across the entire application and services-oriented environment and along the entire attack continuum. The Cisco ACI Security enables organizations to deploy security measures more quickly and effectively where and when they are needed. The solution protects the company before, during, and after an attack without compromising network performance, agility, or functions.

For More Information

Cisco ACI Security: A New Approach to Secure the Next-Generation Data Center
http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-732354.html

C45-732546-00 09/14