Cisco Application Centric Infrastructure Security Solutions

What Is the Value of Cisco's Application Centric Infrastructure Security Solutions?

Cisco® Application Centric Infrastructure Security Solutions help secure next-generation data center and cloud environments by fully integrating security into the Cisco Application Centric Infrastructure (ACI) network. Cisco ACI Security Solutions allows administrators to treat security as a pool of resources and intelligently stitch them to applications and transactions using the Cisco Application Policy Infrastructure Controller (Cisco APIC). Cisco's ACI Security Solutions scale on demand, have programmable automation, and operate in both physical and virtual environments.

Cisco's ACI Security Solutions allow organizations to take a holistic, system-based approach to data center security. They use a common policy-based operational model across Cisco ACI-ready networks, thereby reducing cost and complexity without compromising security.

What Problems Does It Help Solve?

According to an April 2013 *Network World* report, 85 percent of organizations feel that their data center implementations have been compromised by the limitations of traditional firewall solutions. Cisco has completely reengineered its critical data center security solutions. Because Cisco ACI Security Solutions has been fully integrated into the fabric of the Cisco ACI network, it allows organizations to take full advantage of the power, flexibility, and performance of their new data center environments without compromising functionality or security.

Cisco Application Centric Infrastructure Security Solutions

The initial offerings of Cisco's ACI Security Solutions include the Cisco ASA next-generation firewalls, which have been designed to integrate security transparently into Cisco ACI networks.

- The Cisco ASA 5585-X Adaptive Security Appliance has been updated and certified to interoperate with Cisco ACI networks, and includes advanced clustering capabilities to enhance scalability and simplify management.
- The new Cisco ASA Virtual Firewall (ASAv)-provides the exact same security as all other Cisco ASA solutions but has now been completely redesigned for virtual environments.

  It can maintain its own data path with no dependency on the Cisco vSwitches, vMotion, or the Cisco Nexus 1000V hypervisor. In addition it can operate like a traditional firewall or be deployed as a flexible service that can be dynamically attached to any data flow or transaction.

What Are the Benefits of Cisco Application Centric Infrastructure Security?

For organizations migrating to or implementing an intelligent Cisco ACI fabric architecture, the Cisco ASA 5585-X appliances and ASAv instances create the quickest path to protecting the next-generation data center architecture. They eliminate the limitations of traditional network-oriented security solutions and provide the following features:

- **Agile Provisioning:** Because application flows within a Cisco ACI environment change dynamically, Cisco ASA security can be deployed as a service for any transaction flow, completely independent of the underlying topology.
- **Elastic Scalability:** The ASAv solution allows security to be distributed across the entire application environment and to dynamically scale as business demands change.
- **Service Virtualization:** The ASAv allows security to be stitched into the data center fabric as well as selected and deployed as a virtual service based on policy on a per-transaction basis.
- **Unified Configuration and Visibility:** Cisco ACI management tools provide a single point of network and security management, provisioning of security as a service, flow-policy control, and monitoring for a unified view of the infrastructure. At the same time, it allows for the contextual reuse of common security elements in an end-to-end design.
- **Policy Set Simplification:** In traditional topology-oriented environments, policy rules are either pushed as a complete rule set or manually built and customized for each network device. With a services-based approach, each service element can be contextually programmed with only the security rules that are relevant to its specific transactions, creating a truly distributed and simplified policy set.

Why Cisco?

Cisco's architectural approach provides a continuous and pervasive way to weave security into the fabric of today's dynamic, application-oriented data centers. The new Cisco ACI Security Solutions deliver visibility across the entire application- and services-oriented environment and along the entire attack continuum. Cisco ACI Security Solutions enable organizations to deploy security measures more quickly and effectively where and when they are needed. They will protect the company before, during, and after an attack while never compromising on network performance, agility, or functionality.

For More Information

www.cisco.com/go/aciss

C45-730100-00 11/13