Improving Security with an Application-Centric Infrastructure

Cisco IT Insights

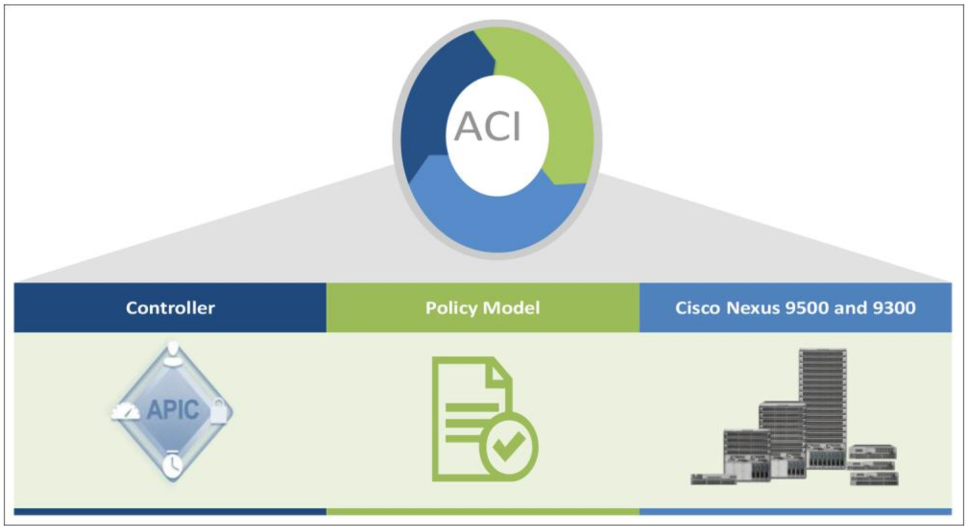
What: New Security Design and Solutions

Cisco IT will implement an application-centric infrastructure (Cisco® ACI™) in every data center, supporting all physical and virtual servers. One significant benefit of this move will be improved data security, achieved in part through use of the Cisco ACI Security Solutions. These solutions allow us to automate more security functions, receive more timely alerts, and reduce human error in defining and maintaining access policies.

The Cisco ACI Security Solutions use a common, policy-based operational model across the network. In traditional topology-oriented environments, policy rules are either pushed as a complete rule set or manually built and customized for each network device. In the ACI model, each application or service element can be programmed with only the security rules that are relevant to its data, function, or context.

The ACI Security Solutions we are implementing include the Cisco Adaptive Security Appliance (ASA) firewalls and the Cisco Application Policy Infrastructure Controller (Cisco APIC). (Figure 1)

Figure 1. Security Elements in a Cisco ACI Environment



Cisco IT has deployed Cisco ASA 5585-X firewalls as our frontline network security solution. We also use the Cisco ASAv virtual appliance for selected network areas.

The Cisco APIC is the policy controller that manages the ACI fabric (consisting of Cisco Nexus® 9500 or 9300 switches) to provide physical and virtual network interfaces and a centralized policy model for securing applications. It helps us improve security with functionality such as policy enforcement among ACI endpoint groups, centralized lifecycle management of security policies, and automated insertion of security services in an application's traffic flow.

"The Cisco APIC gives us a good way to automate much of our traffic analysis so our security staff can focus on the small portion of data that needs special handling," says David Ho, senior manager for data security, Cisco InfoSec.

Why: Improved Protection across the Network

The Cisco ACI Security Solutions help us improve protective measures as data enters, leaves, or moves within the Cisco network.

Improved Controls for Inbound Traffic

Today, access to the Cisco internal data center network by inbound traffic is managed through a large number of access control lists (ACLs), a method that has many challenges. For example, a single ACL can have a huge number of entries, many of which may be outdated because they have not been actively maintained.

In contrast, an ACI environment allows us to define a smaller set of security policies that are applied more broadly across hosts and areas of the Cisco data center network. Policy definition is a more intuitive way to define controls, and individual policies can be created dynamically based on current security threats and network conditions. As an example, dynamic definition of firewall rules helps us quickly isolate malware traffic.

The ability to define policies across the entire ACI fabric also reduces human error and the potential for missing situations that would require specific ACL rules. "This new approach to access control makes our systems more secure and helps Cisco IT improve the networks' overall service level and security posture," says Sidney Morgan, fty designss:distinguished engineer, Cisco IT.

Better Management of Security Policy

Maintaining data security means managing the traffic being sent across the data center fabric, especially when that traffic contains sensitive information such as network configurations, credit card information, or employee data. In an ACI environment, security policy is managed using the language of applications rather than traditional network terminology. The whitelist security model denies traffic between host groups unless a policy has been created to permit that traffic. ACI automates enforcement of this security policy across both physical and virtual network infrastructure, so the security policy follows the application as workloads move across the fabric.

This technique results in improved security because policy is applied and managed consistently across the data center. It reduces unexpected downtime for clients and applications due to human error. ACI also allows the network to more efficiently handle policy-controlled traffic in a way that's transparent to users and application teams.

"The policy can define that all data from a certain application can go here, but not there," says Ho. "Because only what we have defined is allowed, we have confidence about how an application's data moves across our network."

For More Information

Cisco IT Insights: Securing a Diverse, Global Network

Products and Solutions: Cisco Application Centric Infrastructure Security Solution, Cisco Application Policy Infrastructure Controller (APIC), and Cisco ASA 5500-X firewalls

To read additional Cisco IT case studies about a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT.

To view Cisco IT webinars and events about related topics, visit Cisco on Cisco Webinars & Events.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described. Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties; therefore, this disclaimer may not apply to you.

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.**