White Paper

Cisco ACI Security: A New Approach to Secure the Next-Generation Data Center

What You Will Learn

Organizations are transitioning to next-generation data centers and clouds to increase business agility and reduce IT costs. To effectively make this transition, organizations need to address new security challenges to help ensure compliance, governance, and auditing and to mitigate business risks.

This document describes the Cisco® Application Centric Infrastructure (ACI) vision for securing the next- generation data center and cloud. This vision is based on:

- New application-centric policy model that decouples policy (security, auditing, service-level agreements (SLAs), user experience, etc.) from network topology and supports application mobility
- Centralized and automated lifecycle management of Layer 4 through 7 network security policy across the entire data center network
- Open and extensible policy framework that supports a defense-in-depth security strategy and helps protect investments
- Secure hardware-enforced network and application segmentation and multitenancy with performance and scalability
- Policy-based compliance with industry regulations such as Payment Card Industry (PCI) regulations and the Health Insurance Portability and Accountability Act (HIPAA)
- Deep visibility and accelerated threat response based on real-time network intelligence

Transition to Next-Generation Data Center and Cloud Poses New Security Challenges

With organizations transitioning to next-generation data centers and clouds, automation of security policies is needed to support on-demand provisioning and dynamic scaling of applications. Currently, most IT departments are manually configuring security policies in the data center network using a device-centric management approach. According to Gartner, through 2018 more than 95 percent of firewall breaches will be caused by firewall misconfiguration. In addition to lack of automation for moves, additions, and changes, a primary reason for misconfiguration is lack of application context in policy. Multiple enterprises have tens of thousands to millions of access control lists (ACLs) and firewall rules, and they either lack the operational processes to remove these policies in a timely way when applications are decommissioned or prefer to retain policies because they are uncertain about the potential effect of removal. This situation poses challenges for both securing the network and auditing the security stance for compliance reasons.

In the current cloud environment, data centers host critical business applications and corporate data that need to be securely accessed by multiple user groups (tenants). These user groups can be internal to the organization (for example, engineering, sales, marketing, and finance departments) or external to the organization (for example, customers and partners). When organizations move to a cloud-based operating model, the underlying network infrastructure must not only support the agility needed for rapid provisioning of network policies, but it must also offer secure multitenancy and segmentation to the scale needed by the organization.

Another important trend is the significant shift to east-west traffic in the data center caused by new application design methodologies, which use multiple application tiers to provide a service. This trend is accelerated by scale-out and clustered applications such as Hadoop and big data analytics, which have multiple scale-out components across the data center. As application workloads are being added or moved in a data center environment, the security policies need to be carried with the application endpoints. These policies must also be enforced at 1/10/40/100-Gbps line-rate for transport between server ports. Support for dynamic policy creation, deletion, migration, and line-rate enforcement is needed to secure east-west traffic and properly manage application mobility.

All these new requirements need to be supported while helping ensure compliance with industry regulations such as PCI regulations and HIPAA.

Host Virtualization-Based Software Overlay Solutions Aren't Complete Security Solutions

One of the approaches to address security needs for the next-generation data center is to use software overlay techniques at the host virtualization layer to support network virtualization and enable Layer 4 through 7 virtual network service chaining for security. This approach can help address business agility requirements by enabling rapid provisioning of multitenant virtual overlay networks across a physical network. However, this approach does not address several security, operational, and scalability challenges. These include:

- The requirement for a virtualization layer at endpoints limits the applicability of this approach to only virtualized applications (at x86 platforms). Many existing and mission-critical applications don't belong to this category (mainframe, UNIX systems, large databases, etc.). Additionally, new autoscale and big data applications such as Hadoop, many database clusters, and all bare-metal appliances aren't virtualized but instead run on dedicated physical servers, which aren't supported by this model.
- The need to separately manage underlay and overlay networks makes problems harder to troubleshoot, and diagnose, and manage, inclusive of root-cause analysis for compliance and forensics.
- The separate management interface for provisioning tenant networks, storage networks, infrastructure networks (live migration, IP storage, etc.), and associated security policies increases complexity.
- The limited visibility of underlying traffic reduces the scope of security-threat detection and response. In addition, attacks are less likely to be detected early in the attack lifecycle, before they affect the application.
- The hypervisor-based overlay approach requires each connection to pass through multiple policy enforcement points (source virtual machine, destination virtual machine, and optionally an external firewall for advanced security policies). This routing introduces overhead and complexity for each interapplication connection.
- Integration and support of existing policies that may exist on physical appliances may not be possible. Many customers have invested time and effort in defining security policies across a variety of physical appliances such as firewalls and intrusion detection and prevention systems (IDSs and IPSs). When these organizations deploy a host virtualization solution for security, these devices play a much more limited role.
- Multiple fragmented solutions are needed to support different hypervisors. As customers consider a multiple-hypervisor strategy, they will need to consider multiple security solutions with different levels of functions. As the number of solutions increase, so does the complexity of the environment and the cost to support it.

Cisco ACI Security Vision for the Next-Generation Data Center

The Cisco ACI security vision is a holistic, system-based approach to address security needs for next- generation data centers and clouds. It is unlike the software-only network overlay approach based on host virtualization, which offers limited visibility, performance, and scale and requires separate management of underlay and overlay network devices and security policies. Instead, the Cisco ACI security approach addresses the security needs of the next-generation data center by using an application-centric, unified, and automated approach to security policies in the data center and cloud infrastructure that is decoupled from the underlying network topology, supports application mobility, offers real-time compliance lifecycle management, and reduces the risk of security breaches.

New Application-Centric Policy Model

The traditional security policy model for the data center is based on static network topology (bound to network connections, VLAN, network interface, IP addressing etc.) and manual service chaining. This model requires policy configuration across multiple security devices (firewalls, IPSs, and IDSs), slows application deployment, and is hard to scale because applications are dynamically created, moved, and decommissioned in the data center. Other proposals attempt to take a virtualization-centric approach, but fail to address applications not running as virtual machines.

Cisco ACI enables a new open security policy framework that expresses policies using the language of the application rather than network. Policies are defined based on a language that is natural to application owners and not in terms of classical networking constructs like VLANs and IP and MAC addresses. This group-policy approach decouples security policy and segmentation from the underlying network topology. Cisco ACI is the only solution that is application centered and can deliver application segmentation.

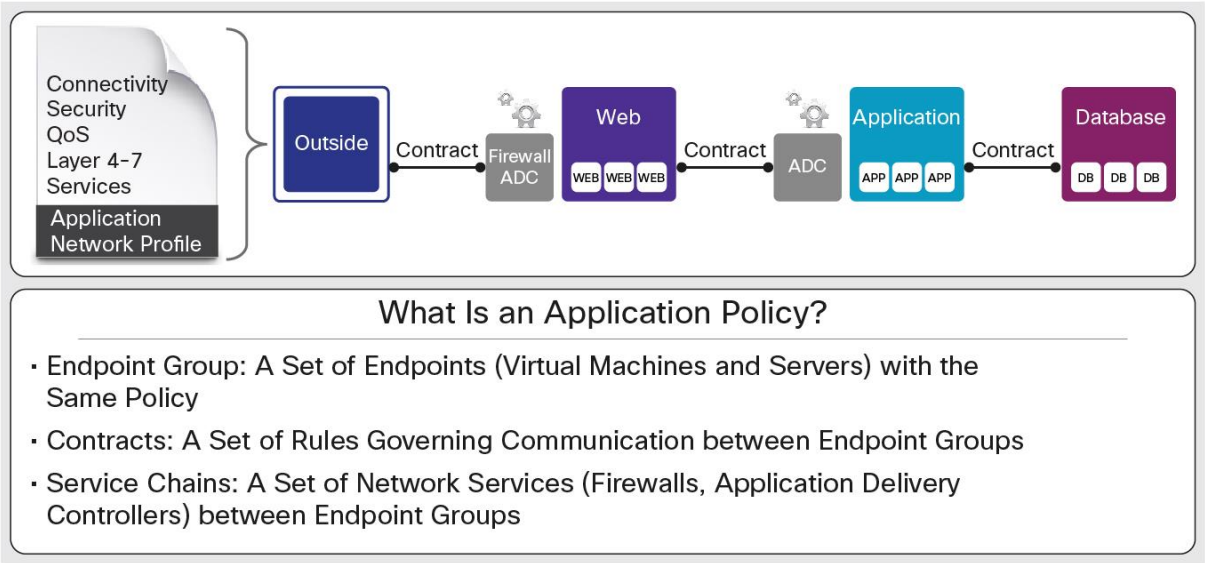
Policies Defined in Application Language

Critical abstractions in the Cisco ACI policy model that enable the decoupling of network topology are the concepts of endpoint groups (EPGs), policy contracts, and application network profiles (ANPs), as shown in Figure 1.

- An EPG is a collection of endpoints that have common policies. For instance, the endpoints might be based on a variety of attributes (for example, version or patch level) and therefore be decoupled from underlying physical or logical topology (for example, network interfaces and IP subnets). EPGs can be defined in a variety of ways: by the application or application component of which they are a part, by the function in the network (infrastructure), by the location in the data center (DMZ), etc. An administrator can create EPGs for different tiers of an application, such as the web tier, application tier, and database tier. The EPG concept is flexible enough to allow the use of EPGs in the context of security zones, trust boundaries, and risk profiles. One such application could use EPGs to define zones such as development, quality assurance, and production for the different stages of an application lifecycle. EPGs are the foundation for dynamic segmentation across the Cisco ACI fabric.
- Contracts are policy rules that specify the way that communication occurs between EPGs and any advanced Layer 4 through 7 services required. Whereas EPGs provide secure segmentation within a tenant of a Cisco ACI multitenant environment, contracts can be viewed as Cisco ACI's security constructs, because they can have multiple subjects, each with particular filters and associated actions plus optional labels. Contracts allow network security administrators to specify rules and policies for groups of physical and virtual endpoints regardless of their physical location in the network. Contracts can be unidirectional or bidirectional when enforcing policies between two EPGs.

- An ANP within the fabric is a collection of EPGs and their connections and the policies that define those connections. ANPs are the logical representation of all of an application and its interdependencies on the Cisco ACI fabric.

Figure 1. Cisco ACI Application Policy Model for Security



Cisco ACI Whitelist-Based Policy Model Supports Zero-Trust Security Architecture

Zero-trust network architecture is an information security approach originally proposed by Forrester. It addresses the weakness of a perimeter-focused approach to security by assuming no default trust between entities (for example, application components) regardless of the location of the entity. Cisco ACI fits well into zero-trust network architecture because it assumes no trust by default between endpoint groups unless Cisco ACI fabric has a whitelist policy explicitly defined to allow connectivity. Policies are expressed as contracts that permit, deny, log, redirect, or instantiate traffic between two EPGs. Even if two endpoints belonging to distinct EPGs are connected to interfaces on the same physical or virtual switch, there is no connectivity between these endpoints unless there is an explicit whitelist policy on a contract to allow communication between these EPGs. This approach differs from the blacklist-based default connectivity model for existing network switches, which allows all traffic unless otherwise specified.

Cisco ACI Policy Supports Workload Mobility

Cisco ACI helps ensure that policies are associated with one (or more) EPGs, regardless of the physical location, even as endpoints are moved within the network. This feature addresses requirements in a data center environment in which security policies need to travel with application workloads as virtual machines and workloads are moved and changed in the data center.

Centralized Policy Lifecycle Management and Layer 4 Through 7 Service Automation

Cisco ACI automates and centrally manages security policies in the context of an application using a unified and innovative security policy abstraction model that works across physical and virtual boundaries, as shown in Figure 2. The central definition of these security policies through the Cisco ACI group-policy model is performed at the Cisco Application Policy Infrastructure Controller (APIC), either directly through the GUI or through JavaScript Object Notation (JSON) or XML through the open northbound Representational State Transfer (REST) API.

In addition, the automation of security policy implementation (and programmatic reuse or replacement of this policy) is also native to Cisco ACI. Cisco ACI enables a distributed policy enforcement model that can scale to more than a hundred-thousand endpoints. As applications are decommissioned, all the corresponding policies associated with the ANP are automatically removed. This approach enables IT agility without compromising security, therefore automating compliance. In addition, it reduces management complexity through automation.

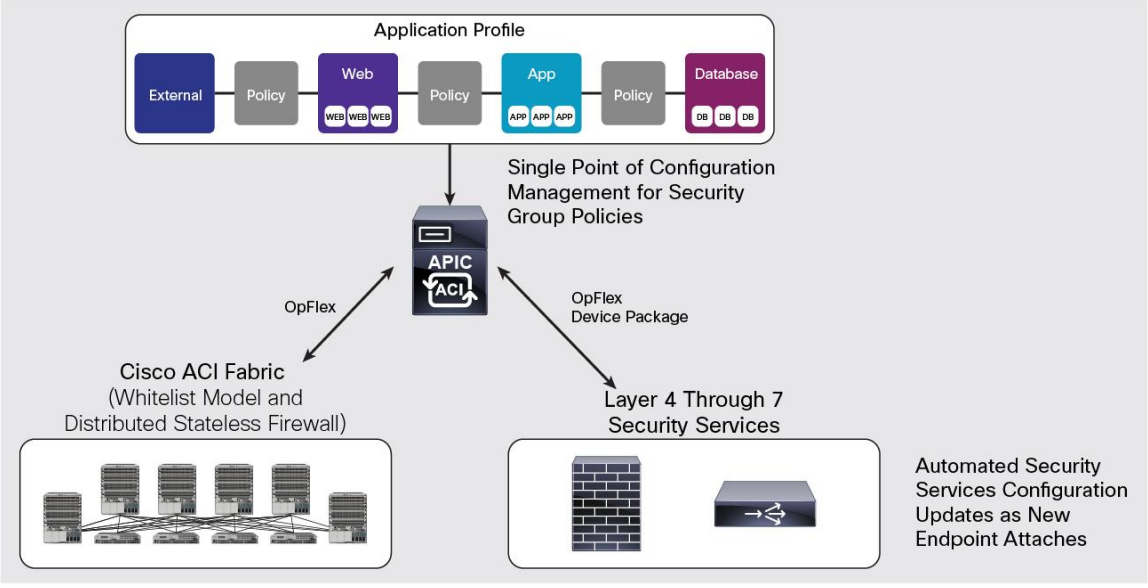
In contrast, with the current data center model as described earlier, the ACLs and firewall rules related to applications often are not removed even when applications are decommissioned because the organization may have millions of ACLs and firewall rules and be unsure of the effect of removing them. This puts the organization at risk of noncompliance during auditing and also increases risk to the organization because new ACLs may conflict with existing, stale ACLs and firewall rules.

Open and Extensible Policy Framework Supports Defense in Depth

Cisco ACI also supports flexible third-party service insertion and policy automation for critical security services such as firewalls, IDSs, and IPSs in the application flow associated with one (or more) ANPs, regardless of the location of these third-party services in the data center. This integration is open and can be performed either through exposure of the functions and services provided by the third party through a device package or directly by calling Cisco ACI's open southbound protocol and API (OpFlex). This feature allows the security administrator to keep, integrate, or extend previous defined security policies by using these third-party services and devices when connecting them to the Cisco ACI fabric. Several Layer 4 through 7 security device vendors are working with Cisco to develop device packages for Cisco ACI, including A10 Networks, Citrix, Embrane, F5, and Radware. In addition, Cisco ASA Adaptive Security Appliances and Sourcefire security products are being integrated with Cisco ACI to offer a fully supported combined solution by Cisco. A complete list of ecosystem partners integrating with Cisco ACI (including Layer 4 through 7 security vendors, security intelligence vendors such as Splunk, and compliance vendors such as Catbird) is available at http://www.cisco.com/c/en/us/solutions/data-center-virtualization/unified-fabric/aci_ecosystem.html.

This feature enables investment protection and mitigates security risk by supporting a defense-in-depth security strategy.

Figure 2. Cisco ACI Automates Layer 4-7 Security Policy Across Physical and Virtual Workloads



Secure Multitenancy and Built-in Stateless Layer 4 Firewall

Cisco ACI fabric supports secure multitenancy at scale and enables complete isolation of network traffic and security policy administration for each tenant. All tenants can define their own private networks using one or more contexts (analogous to the Virtual Routing and Forwarding [VRF] construct). Tenant users can define their own ANPs, bridged domains, and security policies for their applications. The Cisco ACI multitenancy security model enables complete separation of management, administration, and troubleshooting and the underlying network infrastructure.

In many cases, customers need to enforce basic firewall policy to allow traffic only on certain ports to certain parts of the network. These are typically stateless firewall rules (zone-based firewalling). In such scenarios, customers can use Cisco ACI embedded capabilities to provide a stateless Layer 4 distributed firewall to allow traffic between two endpoint groups (through contracts) based on Layer 4 criteria such as protocol and Layer 4 port and range. Policy within a Cisco ACI fabric is applied between two EPGs. Unlike with a traditional ACL, which statically binds filtering policies to particular source and destination IP addresses, these policies can be applied in either unidirectional or bidirectional mode between any given pair of EPGs. These policies then define the allowed communication between EPGs.

For advanced threat mitigation and next-generation firewall services, Cisco ACI can also redirect traffic based on policy to external Layer 4 through 7 security devices using service chaining and automate the provisioning of rules for those devices. These two capabilities are not mutually exclusive and can be used concurrently on a per-contract basis, hence potentially allowing the replacement of multiple zone-based stateless firewalls usually spread across the data center network. The capability to enforce policy in the Cisco ACI fabric also enables it to scale without compromise. To support stateful high scalability, Cisco ACI is fully interoperable with such solutions as Cisco ASA clustering, which allows aggregation of up to 16 high-performance firewall appliances into a single logical firewall service producer. Cisco ACI can reuse the single cluster for multiple firewall device instances, combining stateful security with multitenancy while allowing the underlying hardware to be upgraded and maintained with no impact on the transit application connections.

Automated Policy Compliance

Cisco ACI fabric supports multitenancy and network and application segmentation that addresses the compliance requirements for a secure trusted network. Cisco ACI also helps ensure that the policy configuration in the fabric is synchronized with the policy defined in Cisco APIC at any time. Northbound APIs can be used to pull the policy and audit logs, centrally, from Cisco APIC and create compliance reports (for example, for PCI and other regulations). Security administrators also benefit from the visibility provided by Cisco ACI (inclusive of health scores) to better evaluate the availability aspect of data security when performing capacity planning and analyzing security breaches. This view enables real-time IT risk assessment and reduces the risk to organizations resulting from noncompliance.

Deep Visibility and Accelerated Threat Detection and Mitigation

Cisco ACI supports policy counters and logging in hardware to provide deep visibility and forensics information. Cisco APIC gathers time-stamped network traffic data from the Cisco ACI fabric to offer real-time network intelligence and global visibility across physical and virtual network boundaries. This feature enables real-time visibility into network traffic and accelerates threat detection for network and security administrators. Cisco APIC northbound APIs can be used to integrate with security information and event management platforms and automate response to threats identified on the network based on policies.

Conclusion

To effectively transition from a traditional data center operation model to a next-generation data center and cloud, organizations need to address new security challenges in the data center. The host virtualization-based software-overlay approach doesn't effectively address the security requirements of next-generation data centers because it lacks support for physical workloads, offers limited visibility and scalability, and lacks unified management. 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 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.

For More Information

Cisco ACI policy model white paper: http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-731310.html.

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 C11-732354-00 08/14