PALO ALTO NETWORKS AND CISCO ACI

Key Features

- Insert next-generation firewalls between application endpoint groups (EPGs).
- Configure firewall networking attributes automatically and dynamically.
- Map sanctioned firewall security configuration to applications in Cisco APIC.
- Get uniform security policy and posture across physical and virtualized firewalls.
- Create dynamic security policies based on Cisco ACI constructs, such as endpoint groups, using Panorama.

Overview

Maintaining your competitive edge in today's business environment often hinges on how quickly you can deliver a new application or set of features to market. In some cases, the speed of application development and delivery may outstrip security policy deployment. The combination of Cisco ACI® and Palo Alto Networks Next-Generation Firewall ensures security is deployed in lockstep as your application infrastructure expands, contracts, and changes.

Cisco Application Centric Infrastructure

Cisco Application Centric Infrastructure (ACI) is a comprehensive, software-defined networking architecture that integrates physical and virtual environments under one policy model that automatically inserts Layer 4 through Layer 7 network services, such as load balancing and security, into the application flow. Cisco ACI lets you deploy unified security policies across physical and virtual workloads in your data center. Predefined application requirements and descriptions are built using application network profiles that automate provisioning of the network, application services, security policies, tenant subnets, and workload placement. From a security and filtering perspective, ACI performs some basic port and protocol filtering at the switch level.

We treat applications as security policy elements, irrespective of the network topology. When deployed within the ACI framework, the next-generation firewall is inserted to inspect traffic between devices in specific Endpoint Groups (EPGs). The firewall and advanced threat prevention features protect traffic as it flows through.

Next-Generation Security for Cisco ACI

To enable Palo Alto Networks next-generation firewalls to be deployed within Cisco ACI, a device package has been created that allows Cisco's Application Policy Infrastructure Controller (APIC) to configure Palo Alto Networks physical and virtualized firewalls via PAN-OS® APIs. Once inserted into the application flow using EPGs, policy contracts, and application network profiles through ACI, Palo Alto Networks next-generation firewalls and advanced threat prevention features can protect traffic flow at the application level.

Application-Centric Segmentation

Palo Alto Networks next-generation firewalls natively analyze all traffic in a single pass to determine the application, its content, and the user's identity. These elements then form integral components of your security policy, complementing the nature of ACI. Policy examples include:

- Isolate the Oracle-based credit card number repository in its own security zone.
- Control access to finance groups, forcing traffic across its standard ports and inspecting it for application vulnerabilities.
- Enable only the IT group to access the data center, using a fixed set of remote management applications (e.g., SSH, RDP, Telnet) across their standard ports.
- Allow only your administrative team to use Microsoft SharePoint® administration, but allow all other users to access SharePoint documents.

Prevent Known and Unknown Threats

Today's cyberthreats will commonly compromise an individual workstation or user, and then move across the network, looking for a target. They will move laterally, from server to server or VM to VM, placing your mission-critical applications and data at risk. Exerting application-level control between your physical and virtualized workloads will reduce your threat footprint, while applying policies to allowed applications will prevent known and unknown threats.

Centrally Manage Virtualized and Physical Firewalls

Panorama™ network security management allows you to manage a network of Palo Alto Networks firewalls, both physical and virtualized, ensuring consistent and cohesive policy. Rich, centralized logging and reporting capabilities provide visibility into all your applications, users, and content.

Palo Alto Networks Next-Generation Firewall and Cisco ACI Integration

We support two modes of integration with Cisco ACI.

Service Manager (Managed) Mode

Once the device package has been deployed, Panorama creates a security policy under the relevant device group or groups. Cisco APIC will then push the application profile containing the network configuration to the next-generation firewall and assign the security profile to Panorama. Subsequently, Panorama will push a security policy to the next-generation firewall to protect the traffic as defined in the profile.

Network Policy (Unmanaged) Mode

The Panorama plugin for Cisco ACI enables the unmanaged mode integration. This mode does not require the Palo Alto Networks device package for Cisco ACI. The firewalls operating in this mode need to be configured out of band from the APIC. The Panorama plugin enables security administrators to write policies based on Dynamic Address Groups by mapping them directly to Cisco ACI EPGs and other dynamic constructs, such as application profile, tenants, and Micro Endpoint Groups (uEPGs) for micro-segmentation.

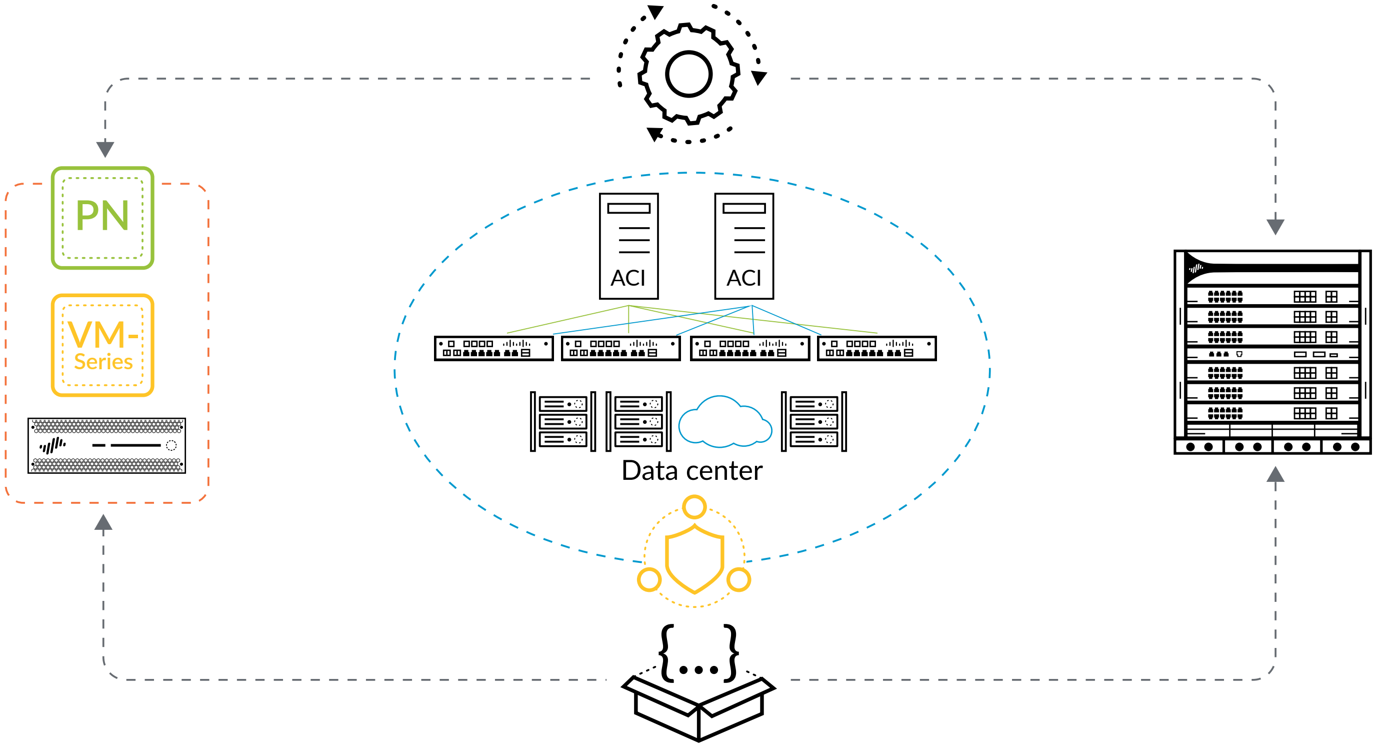

Figure 1: Next-generation firewall and Cisco ACI integration

3000 Tannery Way
Santa Clara, CA 95054

Main:	+1.408.753.4000
Sales:	+1.866.320.4788
Support:	+1.866.898.9087

www.paloaltonetworks.com