AKAMAI PRODUCT BRIEF

Discover Application Dependencies and Automate East-West Security Policy on the Aruba CX 10000

Accelerate network performance, visibility, and security controls by deploying agentless Akamai Guardicore Segmentation for a true Zero Trust security fabric in the data center

As the number and types of applications that companies deploy in the data center accelerates rapidly, security risks grow with them. North-south firewalls, although valuable, don't provide the capability required to secure east-west traffic within the data center. Given the growth of distributed applications, virtualization, and containerization, nearly 80% of traffic in the data center is now east-west, creating two complex security challenges inside the data center itself.

The two challenges of securing east-west flows in the data center

Challenge #1: Inserting security in this east-west fabric. Current-generation appliance–based or VM-based approaches offer macrosegmentation but fail to secure between workloads on the same VLAN.

Challenge #2: Visualizing app-to-app network activity and determining the necessary security rules easily and accurately. While being able to secure flows is critical, knowing which rules to deploy in an area of the data center where security has not been sufficiently addressed requires further insight.

Addressing these challenges with the Aruba CX 10000 and Akamai Guardicore Segmentation

Together, Aruba and Akamai offer a unique solution to both of these challenges.

Solving challenge #1: The Aruba CX 10000 is the industry's first Distributed Services Switch, providing a variety of infrastructure services that scale to support all workloads — starting with security. As traffic passes into this top-of-rack switch, every flow is evaluated and appropriate security policies are applied. This makes security simply part of the fabric instead of a bolt-on service, as has been the case until now.

Solving challenge #2: Akamai Guardicore Segmentation automatically discovers application dependencies and flows, creating contextual maps that simplify the visibility within the data center and the creation of policy. The telemetry from the Aruba CX 10000 is passed to the Akamai Guardicore Segmentation engine where this context is built from the actual network traffic. This enables east-west firewall policies to be created dynamically and pushed back to the Aruba CX 10000 for inline enforcement.

BENEFITS TO YOUR BUSINESS

Simplified implementation of Zero Trust segmentation in the data center

Modernized east-west security at the data center edge as part of the fabric

Fully scaled distributed security with automatic rule creation

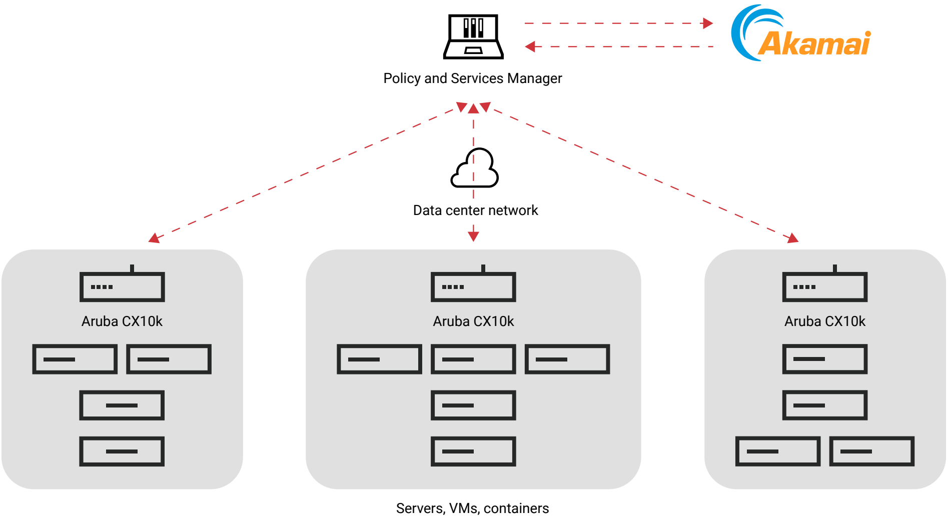
Wire speed throughput and increased agility from the distributed firewall in the Aruba CX 10000

State-of-the-art visibility and rules policy engine from a single interface

Akamai

How it works

- Syslog telemetry from Aruba CX 10000 top-of-rack switches are streamed to Akamai Guardicore Segmentation.
- Akamai Guardicore Segmentation visualizes east-west and app-to-app communications based on combined flow and workload events from CX 10000 syslogs.
- Akamai Guardicore Segmentation suggests rules for microsegmentation policy for relevant applications.
- Policies are pushed back to the CX 10000 via the Policy and Services Manager REST API, where the rules are distributed to all relevant CX 10000s.
- Akamai can extend security to agent-based security workloads in other parts of the data center or the cloud that are not covered by the Aruba CX 10000.



For more information or to see a demo, please contact esg-bd@akamai.com.

| Support | Published 01/23