SOLUTION BRIEF

Managing Network Policies with Akamai and AlgoSec

Simplify your security operations by using the easy integration of Akamai Guardicore Segmentation with AlgoSec. Security teams can now manage multivendor policies more effectively and consolidate labeling for better firewall management across all devices in just a few steps.

The challenge: Limiting complexity and ensuring full visibility

The security needs of today's hybrid cloud environments necessitate the deployment of internal controls to restrict east-west traffic. In addition, organizations must consider the continued use of existing perimeter firewalls to restrict north-south traffic. AlgoSec provides a single solution for hybrid firewall management, making north-south traffic inspection and control much easier for security teams.

But what about east-west visibility and control? This is where Akamai Guardicore Segmentation comes in. Our solution will provide you with the enhanced visibility and flexibility necessary for segmenting business-critical applications to control lateral communications. Policies are dynamic and will follow the workload throughout the DevOps lifecycle.

And how do you monitor and control both north-south and east-west traffic in a way that doesn't overburden your firewall managers and result in potential misconfigurations? Using Akamai and AlgoSec together will give you a fuller picture of what's communicating across your IT estate and ensure that security policy extends seamlessly to your perimeter firewalls.

Better together: Akamai Guardicore Segmentation and AlgoSec

By combining AlgoSec's policy-driven automation and visibility for north-south traffic control with Akamai's microsegmentation and Zero Trust approach for east-west traffic control, businesses can achieve:

- A resilient security posture that proactively mitigates risks
- A simplified, unified approach to managing policy in complex, dynamic networks
- The ability to align security with business goals and ensure compliance and operational excellence

Benefits for your business

Keep it simple
Streamline internal firewall management and eliminate the complexity of maintaining policy across different security solutions — Akamai Guardicore Segmentation plays nicely with AlgoSec from day one

Protect your investment
Continue to use your existing perimeter firewalls and your existing internal workflows to manage and maintain security policy changes on these systems

Consolidate security
Ensure that asset labeling and security policy are consistent across the data center, including legacy systems, with no duplication or miscommunication

Extend visibility
Import precise labeling and segmentation policies and use them throughout your hybrid cloud data center to visualize and control east-west traffic down to the process level

Increase efficiency
Troubleshoot network issues faster by using the visibility provided by our Reveal map via AlgoSec AppViz in a few quick steps

We do this by providing:

- **End-to-end visibility**
  Comprehensive insight into application connectivity and lateral traffic, spanning clouds and on-premises environments, gives you a full picture of what's communicating within your network and improves your security posture.
- **Unified macro- and microsegmentation**
  Policies automatically push from the Akamai Guardicore engine to AlgoSec as drafts, which can be approved and published right from AlgoSec, eliminating the need to manually rewrite rules. Firewall managers will know immediately which application the rules are for, as they'll see the Akamai Guardicore labels appear within AlgoSec (instead of just getting a list of IPs with no additional context). This makes rule management easier and reduces the chance of a misconfiguration that leads to a breach.
- **Streamlined operations**
  In large, complex networks, pushing out new rules to the firewalls is a lot of work. Tools like AlgoSec AppViz simplify network security policy management by providing visibility into application connectivity and security policies across hybrid environments. Now, security teams can reduce manual tasks even more by automating policy export from Akamai Guardicore Segmentation to AlgoSec AppViz, enabling them to respond more quickly to threats and ease the burden of day-to-day operational tasks.

Here's how it works

The integration allows you to convert labels and segmentation policy rules from Akamai Guardicore Segmentation into network objects and application flows in AlgoSec, which can, in turn, be forwarded to managed devices covered by AlgoSec in the data center.

- **Step 1 — Reveal**
  Akamai Guardicore Segmentation automatically visualizes applications and flows, including all application dependencies.
- **Step 2 — Segment**
  Akamai Guardicore Segmentation enables the creation of granular segmentation policies to control traffic between the applications, down to the process level, using human-readable labels.
- **Step 3 — Export**
  Enable the management configuration to bring over labels and policy rules from Akamai Guardicore Segmentation, defining the scope of export as well as when the export should take place.
- **Step 4 — Manage**
  The labels and segmentation rules created in Akamai Guardicore Segmentation are now in AlgoSec and can be used for all other managed devices, as well as to consolidate existing policies.

For more information on simplifying policy management with Akamai and AlgoSec, speak with one of our experts.