Solution Overview

Cisco ACI and AlgoSec Solution: Enhanced Security Policy Visibility and Change, Risk, and Compliance Management

With the integration of AlgoSec into the Cisco® Application Centric Infrastructure (Cisco ACI™) architecture, customers can monitor security policy changes across their Cisco ACI system, obtain risk and compliance context for both managed and unmanaged security devices, and extend automation across their entire security environment.
The Need
In today's fast-paced world, the growing demand to support a variety of applications across the data center and help ensure the compliance and security of these applications is posing significant challenges for data center administrators. The management of network security policies across physical and virtual networks and multivendor security devices requires a delicate balance between strategies to reduce risk and strategies to provision connectivity for critical business applications to increase productivity.

With thousands of firewall rules across many different security devices, numerous and frequent changes, and a lack of visibility, management of security policies through manual processes is now impossible. It is too complex, too time consuming, and too prone to errors, causing outages, security risks, and compliance violations.

Companies need to take an application-centric approach, which delivers unified visibility across the entire network and uses intelligent automation to manage security changes, assess risk, and maintain compliance.

Cisco ACI Architecture
The Cisco ACI architecture is a comprehensive software-defined networking (SDN) solution. This policy-based automation solution supports a business-relevant application policy language, increased scalability through a distributed enforcement system, and greater network visibility. These benefits are achieved through the integration of physical and virtual environments under one policy model for networks, servers, storage, services, and security.

AlgoSec Security Policy Management
The AlgoSec solution intelligently automates and orchestrates network security policy management to make enterprises more agile, more secure, and more compliant—all the time. Through a single pane, users can determine application connectivity requirements, proactively analyze risk from the business perspective, and rapidly plan and implement network security changes—all without manual intervention and transparently orchestrated across heterogeneous environments, including software-defined and cloud environments.

The Integrated Cisco ACI and AlgoSec Solution
Through transparent integration, AlgoSec complements the Cisco ACI architecture by extending and enhancing its policy-based automation to all security devices across the enterprise network, both inside and outside the data center. With AlgoSec’s visibility and unified security policy management capabilities, customers can now process and apply security policy changes quickly, assess and reduce risk, help ensure compliance, and maintain a strong security posture across their entire environment. With these capabilities, customers can rapidly achieve the full potential of their Cisco ACI deployment.

Main Features of the Integrated Solution
The main features of the Cisco and AlgoSec integrated solution include the following:

- Provides a network topology map of the entire fabric, covering both devices managed by the Cisco ACI solution and other network security devices (Figure 1)
• Monitors and proactively identifies policy changes in Cisco ACI contracts and automatically applies them to network security devices across the enterprise network
• Proactively assesses risk in Cisco ACI contracts and recommends the changes necessary to eliminate misconfigurations and compliance violations (Figure 2)
• Proactively confirms that policies for managed firewalls are correct
• Documents all contracts and endpoint groups (EPGs) and enables the user to search the entire rule base, including associated firewalls and unrelated firewalls for analysis and troubleshooting (Figure 3)
• Provides a detailed change history for every device, the current risk status, and the device topology
• Automatically generates audit-ready regulatory compliance reports for the entire Cisco ACI fabric

Main Benefits of the Integrated Solution
• Provides visibility across the entire network, including the Cisco ACI security environment
• Delivers risk and compliance analysis and supports all the regulatory standards
• Reduces time and effort through automation
• Helps avoid outages and eliminate device misconfiguration
• Significantly simplifies and reduces audit preparation efforts and costs
Main Use Cases for the Integrated Solution

Table 1 lists the main use cases for the AlgoSec and Cisco ACI integrated solution.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
</table>
| Simplifying audits and helping ensure compliance across the entire network security estate | • Instantly generate audit-ready reports for all major regulations, including Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act, and North American Electric Reliability Corporation (NERC) regulations, and many others.  
  • Proactively uncover gaps in your firewall compliance posture across your entire system.  
  • Proactively check every change for compliance violations—and remediate problems before an audit.  
  • Get a complete audit trail of all firewall changes and approval processes. |
| Automated security policy change management                    | • Automate the entire change-management process.  
  • Proactively assess the risk of every proposed change.  
  • Intelligently design rule changes and validate the correct implementation.  
  • Push policy changes directly to the device.  
  • Document changes and generate an audit trail.  
  • Transparently integrate with existing ticketing systems. |
| Security policy risk mitigation                               | • Instantly view all risks in the network security policy across multivendor firewalls and cloud security groups.  
  • Map risky traffic flows to the applications they serve.  
  • Proactively assess the risk of every change before it is implemented.  
  • Safely tighten overly permissive rules.  
  • Securely remove firewall rules for decommissioned applications, without removing necessary access to other applications. |
How It Works

The AlgoSec security management solution for the Cisco ACI architecture is delivered through a software license (a hardware appliance can be provided if needed). It supports enterprise-scale deployments. AlgoSec uses Cisco Application Policy Infrastructure Controller (APIC) northbound representational state transfer (REST) APIs to learn the APIC policy configuration and security devices connected to the Cisco ACI fabric (Figure 4).

![Figure 4. AlgoSec and Cisco ACI Integrated Solution](image)

In addition to Cisco ACI and Cisco network security devices, AlgoSec integrates with all leading brands of traditional and next-generation firewalls and cloud security controls, as well as routers, load balancers, and web proxies, to deliver unified security policy management across your enterprise network.

For More Information

[www.cisco.com/go/aci](http://www.cisco.com/go/aci)