The bridge to possible

AlgoSec Security Management Solution for Cisco ACI and Cisco Nexus Dashboard

The bridge to possible

Value Statement

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.

Overview

Networks are becoming ever more distributed and complex, making it increasingly difficult to minimize risk and ensure compliance and security. AlgoSec Security Management for Cisco ACI delivers application-centric security policy change management, providing unified visibility across the entire network estate. It leverages policy-driven automation to manage security changes, assess risk, and maintain compliance.

AlgoSec Security Policy Management Solution (ASMS) 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 of glass, users can determine application connectivity requirements, proactively analyze risk from a business perspective, and rapidly plan and execute network security changes – all with zero-touch deployment and provisioning, seamlessly orchestrated in multicloud network environments.

AlgoSec integrates with Cisco ACI to extend ACI's policy-based automation to all security devices across the data center, on its edges, and in the cloud. AlgoSec Security Management Solution for ACI enables customers to ensure continuous compliance and automates the provisioning of security policies across the Cisco ACI fabric and multivendor security devices connected to the ACI fabric, helping customers build secure data centers.

Key benefits of the integrated solution for Cisco ACI customers

- Provides visibility into the security posture of the Cisco ACI fabric
- Delivers risk and compliance analysis and supports all major regulatory standards
- Reduces time and effort through security policy automation
- Facilitates and automates network segmentation within the data center
- Helps avoid outages and eliminate security device misconfigurations
- Significantly simplifies and reduces audit preparation efforts and costs

The bridge to possible

Trends and Challenges

The growing demand to support diverse applications across the data center and ensure that these applications are secure and compliant poses significant challenges to datacenter administrators. Managing network security policies in multi-cloud environments, with multivendor security devices spread out across physical and virtual devices, is a delicate balancing act. There is a tradeoff between reducing risk and provisioning connectivity for critical business applications.

With thousands of firewall rules across many different security devices, frequent changes, a lack of trained security personnel, and lack of visibility, managing security policies manually is now impossible. It is too complex, too time consuming, and riddled with errors – causing outages, security risks, and compliance violations.

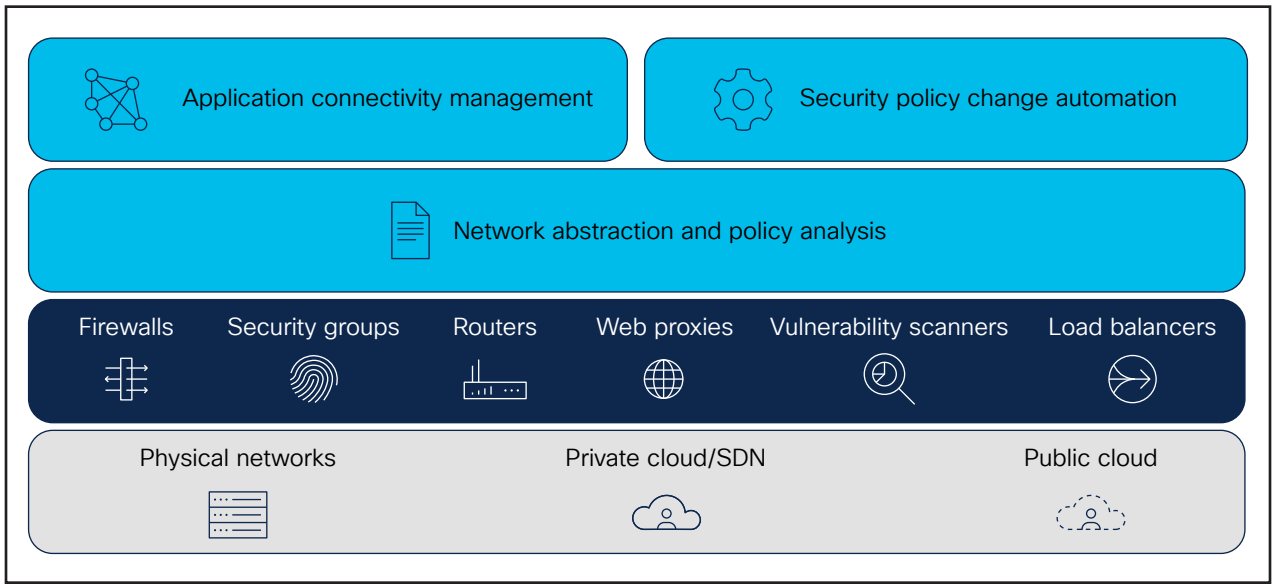

Figure 1. AlgoSec Security Policy Management Solution stack

The AlgoSec solution

The network security management solution from AlgoSec and Cisco comprises several key components:

1. **AlgoSec Firewall Analyzer (AFA) – network security policy analysis, auditing, and compliance**
   AlgoSec Firewall Analyzer delivers visibility and analysis of complex network security policies across Cisco ACI, firewalls attached to the ACI fabric, and other upstream security devices. The solution automates and simplifies security operations, including troubleshooting, auditing policy cleanup, risk and compliance analysis, and audit preparations.

2. **AlgoSec FireFlow (AFF) – automation of security policy changes**
   AlgoSec FireFlow automation helps you process security policy changes in a fraction of the time it takes to make manual adjustments, so you can respond to business requirements with the agility they demand. AlgoSec FireFlow automates the entire security policy change process — from design and submission to proactive risk analysis, implementation, validation, and auditing with support for automated policy enforcement on Cisco ACI and multivendor security devices.

3. **AlgoSec AppViz – application visibility add-on**
   The AlgoSec AppViz add-on accelerates identification and mapping of all network attributes and rules that support business-critical applications – making it easier for organizations to make changes to their applications across any on-premises and cloud platform, and to troubleshoot network and change management issues across the entire enterprise environment.
4. **AlgoSec AppChange – application lifecycle change management add-on**
   AlgoSec AppChange automatically updates network security policy changes on all relevant devices across the entire network. This saves time for IT and security teams and eliminates manual errors and misconfigurations. AppChange addresses the critical issues of human error and configuration mistakes, which are the biggest causes of network and application outages.

The integrated Cisco ACI and AlgoSec offering

Through a seamless integration, AlgoSec complements Cisco ACI by extending and enhancing its policy-based automation to all security devices across the enterprise network – inside and outside the data center.

With AlgoSec's enhanced visibility and unified security policy management capabilities, customers can now process and apply security policy changes quickly, assess and reduce risk, ensure compliance, and maintain a strong security posture across their entire environment – thereby rapidly realizing the full potential of their Cisco ACI deployment.

Key features of the integrated solution

Visibility

- Provides complete visibility into tenants, endpoints, EPGs, and contracts in a Cisco ACI fabric
- Provides a detailed change history for every firewall and other managed devices, current risk status, and device topology
- Offers quick access to key findings through the AlgoSec App for the Cisco ACI App Center

Compliance

- Proactively performs a risk assessment for the policies (contracts) defined in the Cisco ACI fabric and policies defined for firewalls in the fabric. It also recommends necessary changes to eliminate misconfigurations and compliance violations
- Proactively assesses risks for new policy-change requests (before enforcement) to ensure continuous compliance
- Automatically generates audit-ready regulatory compliance reports for the entire Cisco ACI fabric

Policy automation

- Automatically pushes security policy changes to Cisco ACI by creating contracts and filters to enforce data-center permit-list policies
- Automatically pushes changes to firewalls in the Cisco ACI fabric and other network security controls in the data center

Policy-driven application connectivity management

- Maps application connectivity to Cisco ACI contracts and EPGs as well as in-fabric firewall policies
- Migrates application connectivity to Cisco ACI
- Visualizes and instantly provisions connectivity for business applications
- Assesses the impact of network changes on application availability to minimize outages
- Views risks and vulnerabilities from a business application perspective and recommends potential changes to the application policies in the Cisco ACI fabric

The bridge to possible

How it works

AlgoSec uses APIC northbound REST APIs to learn the APIC policy configuration.

AlgoSec then uses this information from Cisco ACI and adds to it the configurations and policies of the network firewalls, routers, load balancers, web proxies, and cloud-security controls, to deliver a unified security policy management solution for the Cisco ACI fabric. This, in turn, provides benefits including compliance, automation, and visibility of the entire network estate.

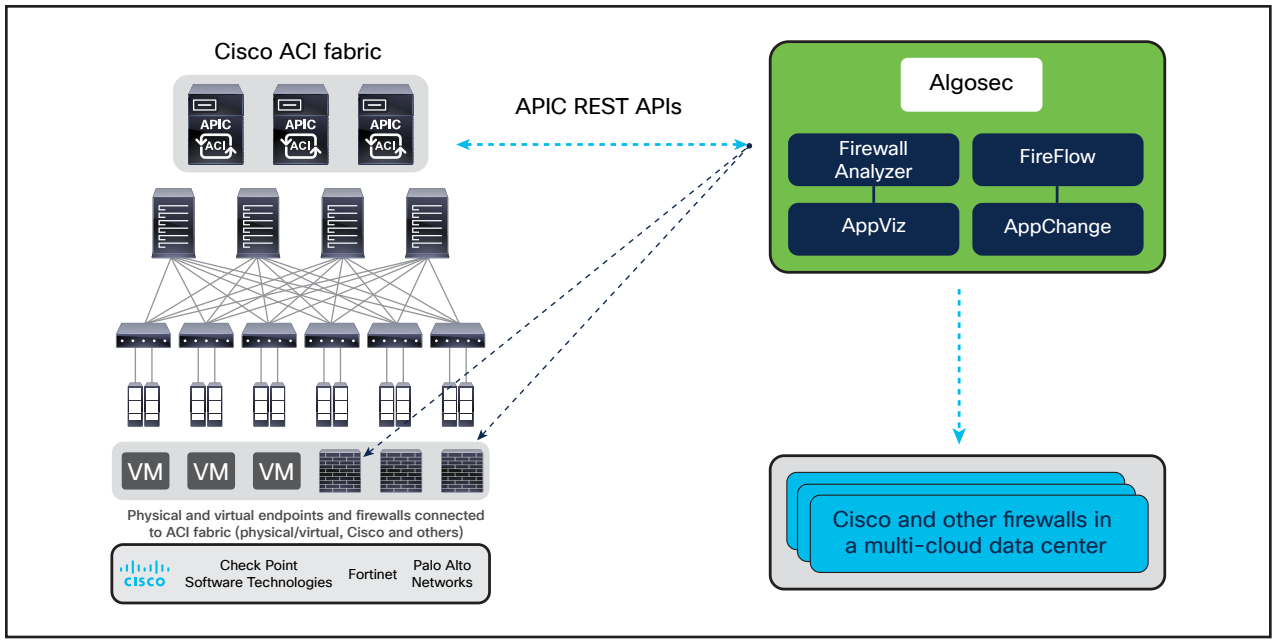

Figure 2. AlgoSec Security Management Solution for Cisco ACI

Use Cases

Key benefit	Use case description
Automated security policy change management	▪ Automate security policy change management for multivendor firewalls ▪ Automatically create and push Cisco ACI contracts and EPGs ▪ Get “on-the-fly” risk and compliance assurance during policy changes of Cisco ACI and in-fabric firewalls ▪ Design rule changes and validate correct implementation ▪ Push policy changes directly to the device ▪ Document changes and generate an audit trail ▪ Seamlessly integrate with existing ticketing systems

Key benefit	Use case description
Risk mitigation and compliance reporting	• Instantly generate audit-ready reports for all major regulations, including PCI DSS, HIPAA, SOX, NERC, GDPR, and many others • Get risk and compliance analysis for Cisco ACI contracts and for firewall security policies • Proactively uncover gaps in your firewall compliance posture across your entire network estate • 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
Application connectivity and security modeling	• Map application connectivity to Cisco ACI contracts and EPGs • Map application connectivity to Cisco ACI fabric firewall policies • Simplify application and server migrations to the data center • Accelerate application delivery • Reduce the cost of manual application connectivity mapping efforts • Avoid application outages due to network device misconfigurations • Provide risk and compliance per application • Align application, security, and network teams
Data-center and cloud migration	• Provide application connectivity mapping assistance by connecting to configuration management databases among other ways • Map the security devices and policies to Cisco ACI's application data constructs • Provide risk assessment to application connectivity as depicted by Cisco ACI • Minimize business disruption and avoid application outages during migration • Get in-depth visibility of the security migration process • Unify security policy management across multicloud environments

Gartner Prediction No. 1: By 2025, 70% of organizations will implement structured infrastructure automation to deliver flexibility and efficiency, up from 20% in 2021.

Gartner Prediction No. 2: By 2025, only 50% of enterprises will develop skills for infrastructure automation across hybrid and multicloud platforms, up from less than 10% in 2021.

Leading financial technology provider reduces risks and gains visibility over their application delivery pipeline.

Challenge: NCR needed to connect its DevOps pipeline with its network security. With over 4500 policy changes made annually, it was difficult to securely manage their entire networking and security environment while being responsive to application owners but still achieve zero trust. Strategically, they were aiming to automate and orchestrate security policy changes across their entire hybrid network, so they could securely accelerate application delivery.

Solution: NCR Corporation implemented the AlgoSec Security Policy Management solution with their Cisco ACI fabric. Using this suite of solutions enabled them to:

- Discover, identify, and map business applications across their entire hybrid network; analyze complex network security policies across the network, and automate and simplify security operations, including troubleshooting, auditing, and risk analysis
- Automate the entire security policy change process from design and submission to proactive risk analysis, implementation, validation, and auditing
- Provide visibility for their network applications, enabling secure application delivery
- Make changes at the business application level, including during application migrations, server deployment, and decommissioning projects

Results: AlgoSec is a strategic component of NCR VOYIX's network security, managing its entire network security infrastructure. The AlgoSec platform enables the NCR VOYIX Corporation to manage application connectivity from end to end across their network – including public cloud, Cisco ACI, and physical firewalls. "Most products don't understand the end-to-end environment. AlgoSec does," noted Scott Theriault, Global Manager, Network Perimeter Security.

Some of the ways that NCR VOYIX Corporation benefits from AlgoSec include:

- **Launched migration** of their on-premises data centers into the Cisco ACI fabric
- **Extended micro-segmentation** to Cisco ACI environment
- **Achieved complete visibility** of their global security posture from a single dashboard
- **Automated risk analysis**, achieving visibility and insights into the risk that changes introduced
- **Streamlined auditing process** with to automatic logging and audit-ready compliance reports
- **Cleaned up and reduced firewall policies** with rule cleanup, object cleanup, and policy tuning

"As we aspire to achieve zero-trust, when moving into the cloud, micro-segmentation and container security come into play. Therefore, we need tools like AlgoSec to assist us in the journey because most application owners don't know what access is needed. This tool helps them learn what needs to be implemented to reduce the attack surface," stated Scott Theriault, NCR VOYIX Corporation's Global Manager of Network Perimeter Security.

Learn more

The AlgoSec Security Policy Management Solution for Cisco ACI is available on the Cisco Global Price List (GPL) through the Cisco SolutionsPlus Program. Please contact Cisco sales or the Cisco partner network for more details.

C22-3971495-00 12/23