Cisco ACI and AlgoSec

Policy-driven, multi-tenant, application-centric security management for data centers

Contents

AlgoSec Security Management Solution for Cisco ACI™ extends ACI's policy-driven automation to security devices in the fabric, helping customers automate policy enforcement for security devices in the fabric and ensure continuous compliance across multicloud ACI environments.

The need

The growing demand to support diverse applications across the data center and ensure that these applications are secure and compliant poses significant challenges to data center administrators. Managing network security policies in multicloud 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.

The solution

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.

Cisco ACI

Cisco ACI, an industry-leading software-defined networking solution, facilitates application agility and data center automation. ACI enables scalable multicloud networks with a consistent policy model and provides the flexibility to move applications seamlessly to any location or any cloud while maintaining security and high availability.

AlgoSec Security Policy Management Solution (ASMS)

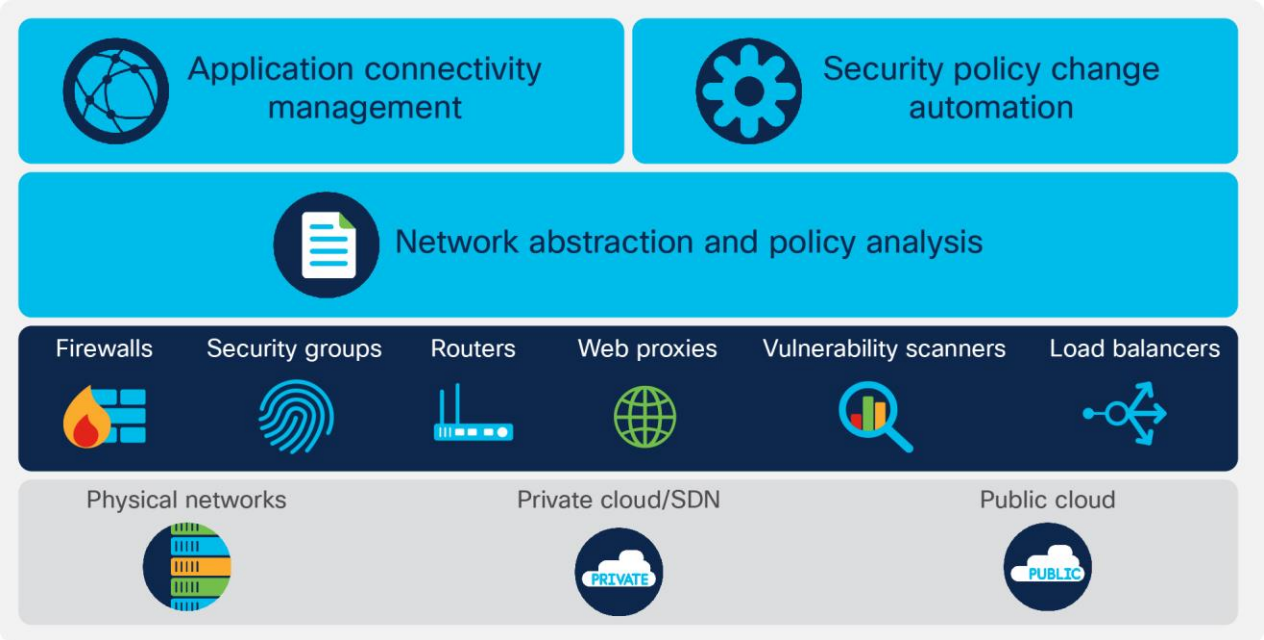
AlgoSec Security Policy Management Solution (ASMS) intelligently automates and orchestrates network security policy management to make enterprises more agile, more secure, and more compliant – all the time. Through a single pane of glass, users can determine application connectivity requirements, proactively analyze risk from the 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 their 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 ACI fabric and multivendor security devices connected to the ACI fabric, helping customers build secure data centers.

The AlgoSec solution

The network security management solution from AlgoSec and Cisco comprises three 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 helps you process security policy changes in a fraction of the time, 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 AppViz add-on accelerates identification and mapping of all the network attributes and rules that support business-critical applications – making it easier for organizations to make changes to their applications across any on-premise 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's 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.



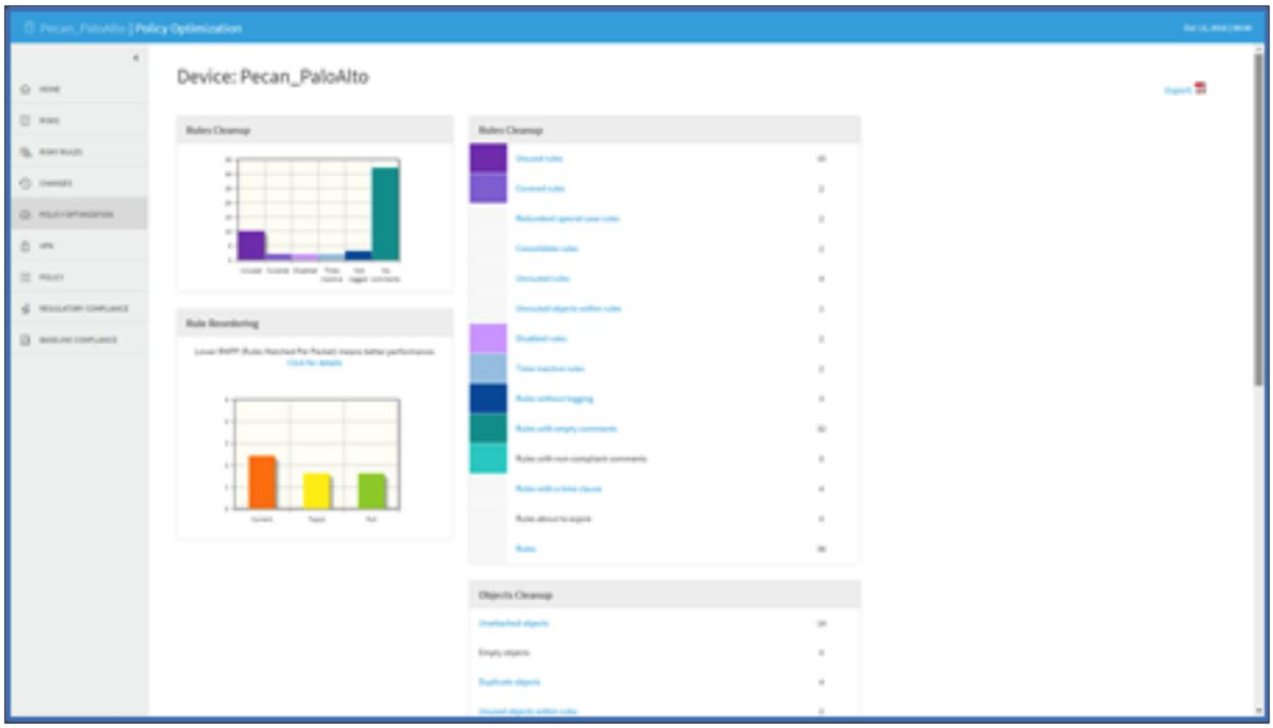
The integrated Cisco ACI and AlgoSec offering

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 the ACI fabric
- Provides a detailed change history for every firewall and other managed devices, current risk status, and device topology
- Quick access to key findings via the AlgoSec App for the Cisco ACI App Center

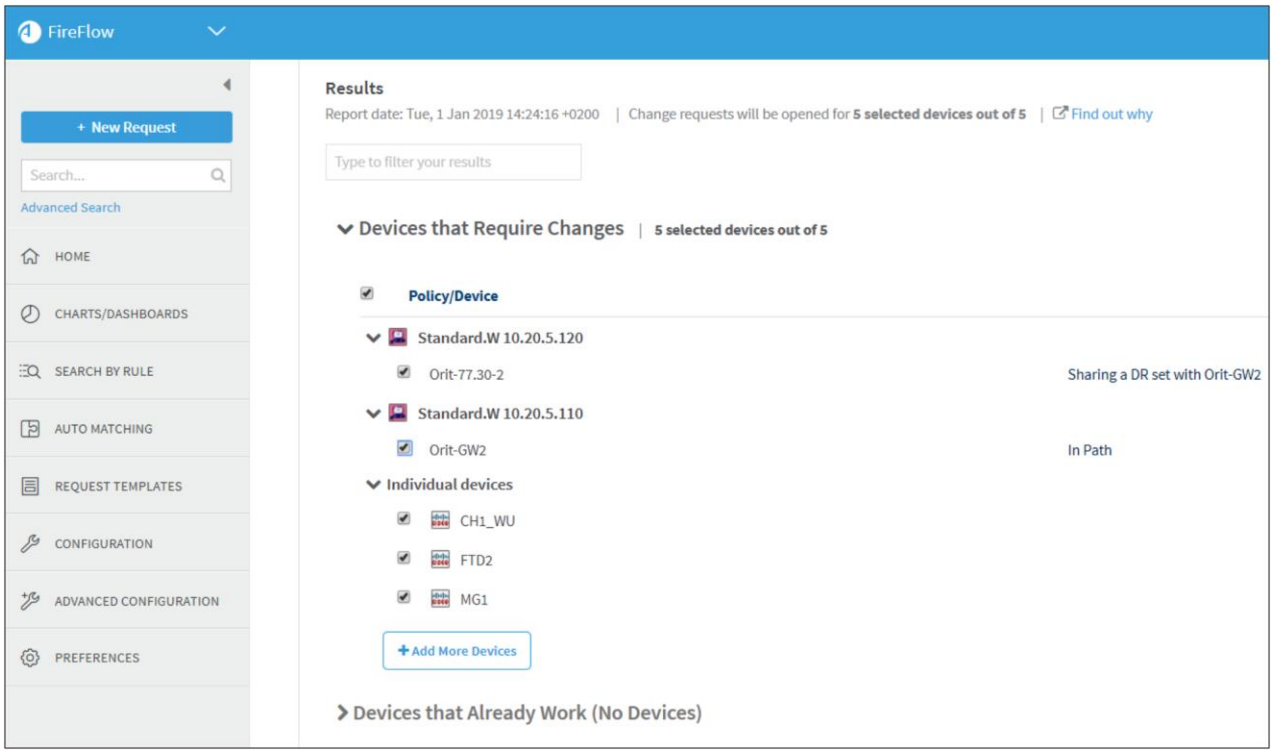


Compliance

- Proactively performs a risk assessment for the policies (contracts) defined in the ACI fabric and policies defined for firewalls in the fabric; It also recommends the 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 ACI fabric

Policy automation

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



Policy-driven application connectivity management

- Map application connectivity to ACI contracts and EPGs as well as in-fabric firewall policies
- Migrate application connectivity to Cisco ACI
- Visualize and instantly provision connectivity for business applications
- Assess the impact of network changes on application availability to minimize outages
- View risk and vulnerabilities from the business application perspective and recommend potential changes to the application policies in the ACI fabric

AlgoSec App for Cisco ACI App Center

AlgoSec also delivers an App for the Cisco ACI App Center, making key benefits of the integrated solution easily accessible from the APIC-user interface. The AlgoSec App for ACI provides visibility into security and compliance posture of the ACI fabric (including firewalls in the ACI fabric) and enables contract connectivity troubleshooting and the automating of security policy changes on firewalls connected to the ACI fabric.

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

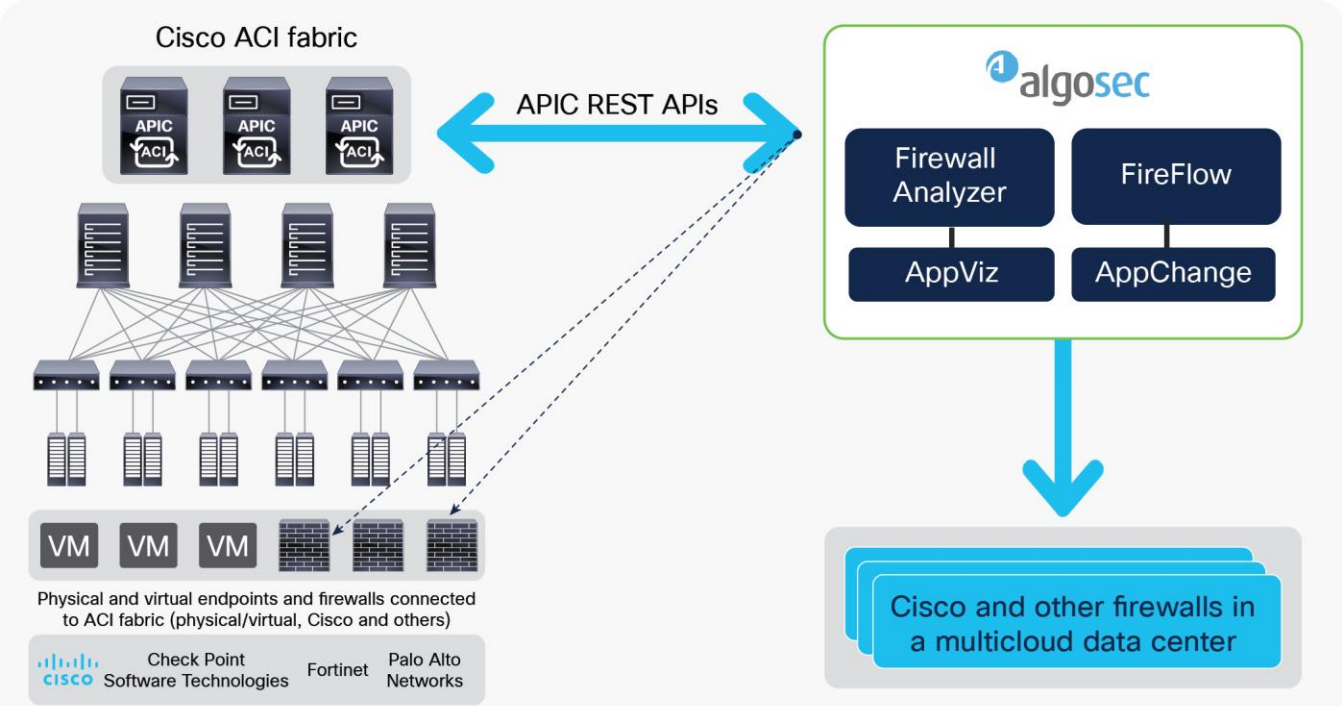
Key use cases of the integrated solution:

Automated security policy change management	• Automate security policy change management for multivendor firewalls • Automatically create and push ACI contracts and EPGs • "On-the-fly" risk and compliance assurance during policy changes of 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
Risk mitigation and compliance reporting	• Instantly generate audit-ready reports for all major regulations, including PCI DSS, HIPAA, SOX, NERC, GDPR, and many others • Risk and compliance analysis for Cisco ACI contracts and for firewall security policies • Proactively uncover gaps in your firewall compliance posture across your entire 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 ACI contracts and EPGs • Map application connectivity to ACI fabric firewall polices • 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 CMDBs among other ways • Map the security devices and policies to ACI's application data constructs • Provide risk assessment to application connectivity as depicted by ACI • Minimize business disruption and avoid application outages during migration • In-depth visibility of the security migration process • Unify security policy management across multicloud environments

How it works

AlgoSec uses NoAPIC 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 ACI fabric. This, in turn, provides benefits including compliance, automation, and visibility of the entire network estate.



AlgoSec Security Management Solution for Cisco ACI

AlgoSec software components compatible with Cisco ACI:

AlgoSec component	AlgoSec product version	Supported firewall devices
AlgoSec Firewall Analyzer (AFA)	V2017.3 and higher	Cisco Adaptive Security Appliance (ASA), Cisco Firepower® Threat Defense (FTD), Palo Alto Networks, Fortinet, Check Point Firewalls, and cloud-native security devices. Please refer to the link below for a complete list of supported devices: https://www.algosec.com/supported-devices/
AlgoSec FireFlow (AFF)		
AlgoSec AppViz		
AlgoSec AppChange		
ActiveChange (for AFF)	v2018.1 and higher	

Summary

Integrating Cisco ACI with AlgoSec lets you do the following:

- **Automatically design and push security policy changes** to Cisco ACI by creating contracts and filters to enforce the data center allowed list policy, and also changes to firewalls connected to the ACI fabric and to other network security controls in a multicloud environment
- **Proactively assess risk** in Cisco ACI contracts and recommend changes needed to eliminate misconfigurations and compliance violations both while making policy changes and, periodically, for the entire multicloud environment
- **Application policy** reflection of the data center's underline security policies as implemented on firewalls and other security devices

Product availability

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.

For more information

1. Cisco Application Centric Infrastructure https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html.
2. The AlgoSec Connectivity and Compliance App on ACI App Center https://aciappcenter.cisco.com/connectivitycompliance-2-2-1a.html.
3. AlgoSec and Cisco https://www.algosec.com/cisco-algosec/.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C22-738043-02 11/19