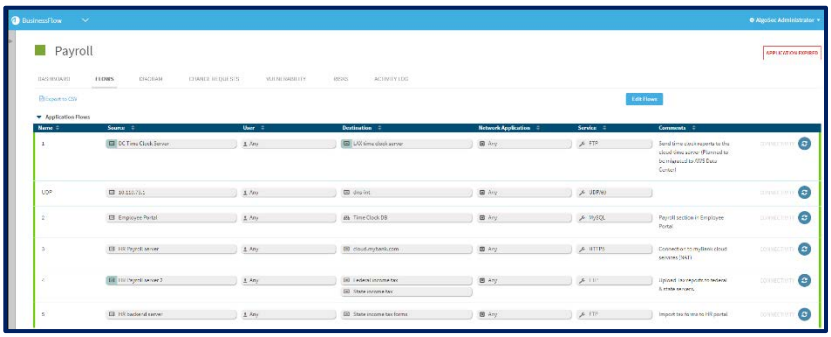
Security Policy Management Automation Across the Entire Cisco Environment

AlgoSec manages network security policies throughout their lifecycle, from discovering application connectivity requirements through ongoing change management and proactive risk analysis, to secure decommissioning. Delivering complete visibility into firewalls and cloud security controls from a unified console, AlgoSec simplifies, automates and orchestrates security policy management for Cisco physical, virtual and cloud devices to accelerate application delivery while ensuring security and continuous compliance across the enterprise.

Provision Application Connectivity

AlgoSec makes it easy to securely provision, maintain and decommission connectivity required by business applications. By automatically mapping application-connectivity requirements to the underlying network/cloud infrastructure, AlgoSec accelerates application delivery and minimizes outages while enforcing security and compliance across the hybrid data center/cloud environment.



See and Understand Complex Network Security Policies

AlgoSec provides visibility and analysis of complex network security policies across virtual, cloud and physical environments to simplify security operations, including policy cleanup, troubleshooting, auditing and risk analysis. Security and operations teams can simply and automatically optimize the configuration of Cisco firewalls, routers and SDN solutions to ensure security and compliance.

Automate Security Policy Change

AlgoSec automates the security policy change management process and delivers hands-free policy push for Cisco Firepower and ASA firewalls, IOS routers, Layer-3 switches and Cisco ACI.

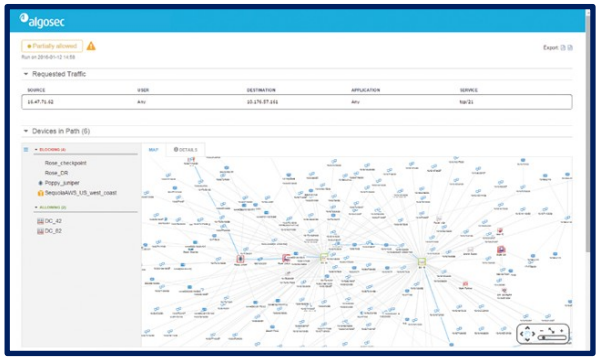
By eliminating guesswork though intelligent change management workflows—from design and submission to proactive risk analysis, implementation, validation and auditing—AlgoSec helps operations and security teams save time, avoid manual errors and reduce risk.

Key Benefits

- **Quick discovery and provision of required connectivity** to accelerate application delivery and minimize outages.
- **Zero-touch, intelligent workflows** for policy changes on Cisco firewalls, routers and ACI to eliminate misconfigurations and rework.
- **Proactive assessment of risk** of change requests, routing only potentially risky changes through manual review.
- **Cleanup and optimization of firewall and router policies** quickly and efficiently.
- **Simplified, automated internal and regulatory firewall audits** that reduce time and cost by as much as 80%.
- **Every security policy rule and change request tied to respective business application** to prioritize policy changes and threat-mitigation based on impact to the business.

Get the Most out of Your ACI Investment

AlgoSec's uniform security policy management transcends legacy networks, cloud and WAN all the way to your ACI fabric, delivering full security visibility across the different estates that comprise your network. AlgoSec brings firewalls and the ACI fabric into a single-pane-of-glass for comprehensive management and automated workflow to execute and assess the impact of changes. AlgoSec enables zero-touch changes end to end by automatically creating contracts on ACI and updating security policies on firewalls in the data center and at its perimeter.



Micro-Segmentation and Policy Enforcement

AlgoSec leverages Cisco Tetration as well as other data sources and sensors to discover application flows by quickly learning how application use the network. AlgoSec automatically generates whitelist policies based on discovered connectivity, and pushes them to various security constructs (firewalls, ACI contracts) to enforce east-west filtering. AlgoSec also enhances security by ensuring consistent and continuous end-to-end implementation of micro-segmentation policy across the entire network.

Ease the Migration to Firepower

With the AlgoSec solution, you can easily migrate existing firewall rule-sets to Cisco Firepower. The solution maps and cleans the existing network security policy rule-set, automatically translates the rules to Firepower, and pushes them with zero-touch to Firepower devices (via FMC). As part of the migration process AlgoSec also performs what-if risk analysis and provides full documentation of changes.

Supported Cisco Products and Services

- Cisco Firepower Management Center
- Cisco ASA Series Firewalls (including virtual versions for Amazon Web Services, VMware, Microsoft Azure and Firepower Services)
- Cisco PIX Security Appliance
- Cisco Firewall Services Module (FWSM)
- Cisco Layer-3 Switches
- Cisco Security Manager
- Cisco IOS, IOS-XR and Nexus Routers (5K, 7K, 9K), including ACLS and complex VRF architectures with VRF leakage
- Cisco Application Centric Infrastructure (ACI)
- Cisco Tetration Analytics
- Cisco Identity Services Engine (ISE)

Comprehensive Support for Heterogeneous Environments

AlgoSec seamlessly integrates with all leading brands of traditional and next-generation firewalls and cloud security controls as well as SIEM solutions, routers, load balancers and web proxies, to deliver unified security policy management across any heterogeneous cloud, SDN or on-premise network.

algosec

Cisco Partner

AlgoSec.com