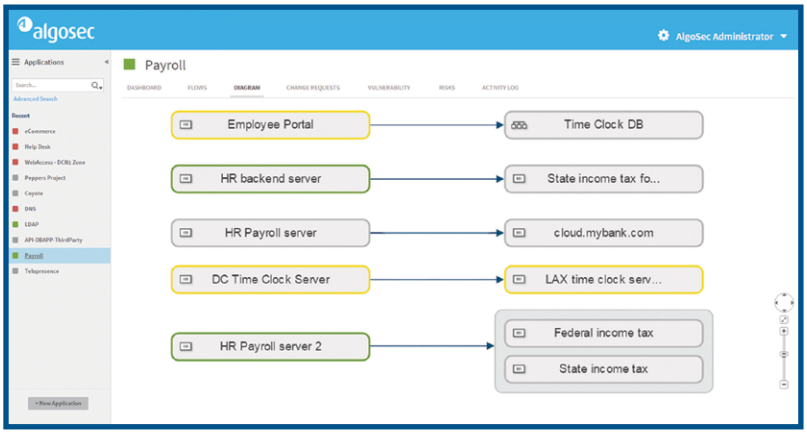
PARTNER SOLUTION BRIEF:
ALGOSEC & CISCO

Security Policy Management for Your Cisco Environment

AlgoSec manages complex network security policies throughout their lifecycle — from discovering application connectivity requirements, through ongoing change management and proactive risk analysis, to secure decommissioning. With powerful visibility across firewalls and cloud security controls, AlgoSec simplifies, automates and orchestrates security policy management for Cisco 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 infrastructure, AlgoSec accelerates application delivery, minimizes outages and enforces security and compliance across the entire hybrid data center.



Visualize and Analyze 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. Using AlgoSec, security and operations teams can simply and automatically optimize the configuration of Cisco firewalls and routers, as well as related network infrastructure, to ensure security and compliance.

AlgoSec Security Management for Cisco

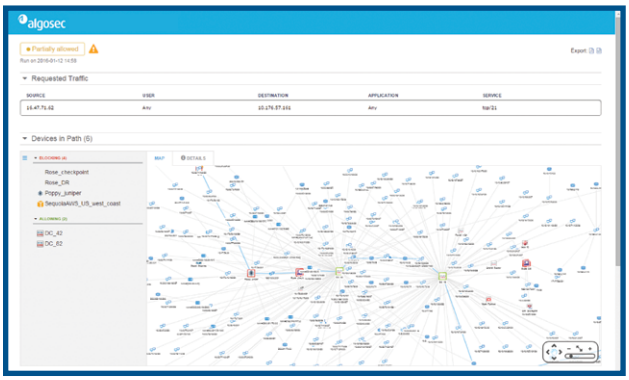
- Easily discover and provision required connectivity to accelerate application delivery and minimize outages.
- Get zero-touch intelligent workflows for policy changes on Cisco firewalls, routers and APIC — to eliminate misconfigurations and rework.
- Proactively assess risk for change requests, and route only risky changes through a manual review.
- Cleanup and optimize firewall and router policies quickly and efficiently.
- Simplify and automate internal and regulatory firewall audits, and reduce time and costs by as much as 80%.
- Tie every firewall rule and change request to their respective business applications to prioritize policy changes and threat mitigation based on the impact to the business.

cisco
Preferred Solution Partner

Automate Security Policy Changes

AlgoSec automates the entire security policy change management process and delivers hands-free policy push for Cisco ASA firewalls and PIX appliances, Firewall Services Module (FWSM) as well as IOS routers and Cisco APIC.

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.



Supported Cisco Devices	
Device	**Version**
Cisco Firepower Management Center	v6.1 and higher
Cisco Firepower Threat Defense	4xxx, 8xxx series FX-OS 2.0 and higher
Cisco ASA Series Firewalls (including virtual versions for Amazon Web Services, VMware, and Microsoft Azure, as well as FirePOWER Services)	v4.4 and higher
Cisco PIX Security Appliance	v4.4 and higher
Cisco Firewall Services Module (FWSM)	v1.0 and higher
Cisco Layer-3 Switches	All versions
Cisco Security Manager	v4.3
Cisco IOS, IOS-XR and Nexus Routers (5K, 7K, 9K), including ACLS and complex VRF architectures with VRF leakage	All versions
Cisco Application Centric Infrastructure (ACI)	v1.0 and higher
Cisco Identity Services Engine (ISE)	All versions

Comprehensive Support for Heterogeneous Environments

In addition to Cisco devices, 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 enterprise network.

amazon web services, AVAYA, BLUE COAT, BROCADE, Check Point SOFTWARE TECHNOLOGIES LTD., cisco, DELL SONICWALL, f5, FORCEPOINT, FORTINET, Hillstone NETWORKS, HUAWEI, IBM, JUNIPER NETWORKS, Microsoft Azure, paloalto, splunk>, vmware, WatchGuard

algosec

AlgoSec.com