

ML-Powered Next-Generation Firewalls and AlgoSec Security Management Suite

Automate Firewall Security Policy Management

Benefits of the Integration

- Gain holistic visibility across next-generation firewalls (NGFWs), on-premises and in the cloud.
- Eliminate guesswork and misconfigurations in NGFW change management.
- Risk assessment and optimization for traditional and NGFW policies.
- Automatically implement policy creation and changes on target devices.
- Get continuous regulatory compliance reports, reducing prep time and costs by 80%.

The Challenge

Today's business environment is always changing, as are the business needs of various company departments. In this dynamic and rapidly evolving business environment, IT often struggles to gain adequate visibility or precise enough control to ensure compliance with security policies and regulatory guidelines. Effective policy management that accommodates the dynamic nature of today's organizations is a key challenge for many IT departments.

The Solution

Companies need comprehensive visibility across their networks and more effective policy management to keep pace with today's organizations without compromising their networks or introducing security risk. Unfortunately, many companies still rely on manual processes for change management, risk analysis, auditing, and other security policy management tasks, which can introduce mistakes, slow down operations, and put their business at risk.

Fragmented policy management and manual security change processes are no longer acceptable in today's environment. Transitioning to centralized policy management not only helps track changes for compliance requirements but also offers automation tools to reduce human errors. This improved visibility allows companies to have a comprehensive view of their security policies, enabling better risk analysis. Automation features streamline changes to existing policies,

making them more efficient and accelerating the delivery of new business applications.

AlgoSec Security Management Suite

AlgoSec provides a range of powerful features designed to simplify, automate, and enhance your network security. AlgoSec solutions enhance policy management, provide centralized visibility, offer in-depth network security insights, and streamline network security management across your hybrid network. By integrating AlgoSec into your network security strategy, you can achieve improved visibility, centralized policy management, enhanced security, and better compliance management.

AlgoSec empowers organizations to securely accelerate application delivery by automating application connectivity and security policy, anywhere. With AlgoSec you'll gain visibility, reduce risk, and process changes at zero touch across the hybrid network.

Palo Alto Networks ML-Powered Next-Generation Firewall

Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFWs) offer a prevention-focused architecture that's easy to deploy and operate. The machine learning NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations and enforce consistent protection everywhere. Panorama network security management empowers you with easy-to-implement, consolidated policy creation and centralized management features. Manage your network security with a single security rulebase for firewalls, threat prevention, URL filtering, application awareness, user identification, sandboxing, file blocking, access control, and data filtering. This crucial simplification, along with App-ID technology-based rules, dynamic security updates, and rule usage analysis, reduces administrative workload and improves your overall security posture.

Palo Alto Networks ML-Powered NGFW and AlgoSec Security Management Suite

AlgoSec integrates seamlessly with Palo Alto Networks NGFW to automate application and user-aware security policies. The integration covers the full policy management lifecycle, from discovery to compliance, reducing complexity, risks, costs, and manual efforts while enhancing security and business agility.

This integration simplifies network management, enhances security, and provides a single pane of glass for unified visibility, streamlining the monitoring of Palo Alto Networks NGFW and cloud security controls. It encompasses a wide range of features, including support for Panorama, App-ID, and User-ID technology.

Using intelligent, highly customizable workflows, AlgoSec automates the entire security policy change process—from planning and design through submission, proactive risk analysis, implementation on the device, validation, and auditing. With AlgoSec, you can also generate prepopulated, audit-ready compliance reports for most industry regulations, as well as customized corporate policies—which help reduce audit preparation efforts and costs by as much as 80%.

Use Case 1: Unified Management for the Hybrid Environment

Challenge

Companies are embracing public cloud platforms, such as Google Cloud Platform (GCP), Amazon Web Services (AWS), or Microsoft Azure; as well as private cloud and software-defined networking (SDN) platforms, such as VMware NSX, Nutanix Flow, or Cisco ACI. This shift requires companies to manage security policy in a unified manner across the multicloud hybrid environment and different security technologies, including all form factors of the Palo Alto Networks NGFWs, Panorama, and cloud security groups.

Solution

AlgoSec unifies security policy management across traditional and Palo Alto Networks NGFWs deployed on-premises as well as security controls deployed on public and private clouds. AlgoSec provides a single pane of glass, to seamlessly manage your entire security policy—including change management, policy provisioning, network and cloud security control visualization and traffic simulations, policy and risk analysis, auditing, and compliance reporting.

Use Case 2: Security Policy Change Management

Challenge

Manual change management processes for network security policies often lead to misconfiguration, introducing unnecessary risks and causing outages that disrupt business operations.

Solution

Using intelligent, highly customizable workflows, AlgoSec automates the entire security policy change process—from planning and design through submission, proactive risk analysis, implementation on the device, validation, and auditing. With AlgoSec, you can avoid guesswork and manual errors, reduce risk, and enforce compliance.

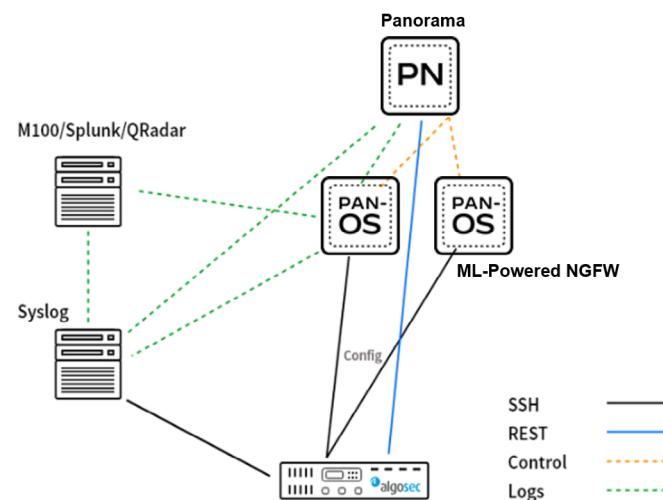


Figure 1: Palo Alto Networks Panorama managed NGFWs centrally managed by ASMS or remote agent

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to secure application connectivity by automating connectivity flows and security policy, anywhere.

AlgoSec lives at the intersection of the infrastructure, security policy and the applications that run your business, enabling greater visibility, reduced risk and zero-touch change automation across the entire hybrid network.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. Our next-gen security solutions, expert services, and industry-leading threat intelligence empower organizations across every sector to transform with confidence. For more information, visit www.paloaltonetworks.com.



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000

Sales: +1.866.320.4788

Support: +1.866.898.9087

www.paloaltonetworks.com

© 2023 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
parent_pb_algosec_112023