Palo Alto Networks ML-Powered Next-Generation Firewall and FireMon

Ground-to-Cloud Unified Multivendor Security Policy Management

Benefits

- Total support for access and compliance at the user and app layer
- APIs for integration with Palo Alto Networks, non-Palo Alto Networks devices, and the Panorama™ management platform
- Real-time monitoring for instant network awareness and remediation steps
- Sub-second rule and policy checks across 350+ controls for continuous compliance
- Comprehensive change analysis with scoring rules for risk and compliance
- Attack simulation based on vulnerabilities and network policy
- End-to-end orchestration from request to design and from implementation to decommissioning

The Challenge

As networks become more complex and policy rule sets continue to multiply, it becomes increasingly difficult to manage compliance, implement rule changes, prevent outages, and address vulnerabilities before they're exploited. Without an integrated way to manage policies across multivendor, highly distributed environments, organizations struggle with time-consuming and error-prone manual compliance reporting, extended response times to business owners, and lack a clear view of risk across their entire environment.

Security Manager from FireMon

FireMon Security Manager is a comprehensive security policy management platform that helps organizations quickly adapt to change, manage risk, and achieve continuous compliance. By standardizing and consolidating firewall, cloud security groups, and other network policy device rule sets into a single management console, Security Manager gives network teams visibility and control over even the most complex hybrid networks with ease. Designed with enterprise needs in mind, Security Manager is highly scalable and highly customizable with the industry's only API-first approach that exposes every control for quick and reliable integrations.

Palo Alto Networks NGFWs

Palo Alto Networks NGFWs offer a prevention-focused architecture that's easy to deploy and operate. The machine learning-powered 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, focus on what matters most, and enforce consistent protection everywhere. The user, application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies and write rules that are easy to understand and maintain.

Palo Alto Networks and FireMon

FireMon solutions help you accelerate the adoption of Palo Alto Networks firewalls and maximize the value of your investment within a mixed-vendor network. You can work smarter with the necessary tools to see through your network complexity and be more proactive with your security.

FireMon gives Palo Alto Networks users a fusion of security process automation, vulnerability management, continuous compliance and policy orchestration capabilities that can help speed migration to the latest firewall technologies. FireMon makes it easy to add Palo Alto Networks firewalls into an existing mixed-vendor environment, ensuring that organizations can make the most out of their firewall deployments without losing comprehensive visibility and management capabilities. With real-time visibility and control into user and application settings connected to firewall policies, changes, compliance and configurations, FireMon gives you airtight security controls across your entire environment.

Use Case 1: Maintaining Compliance Across Complex Multivendor Environments from the Data Center to the Cloud

Challenge

Compliance is about more than avoiding failed audits and violations. It's about ensuring that security is continually meeting the standards that an organization has set out for itself. Maintaining compliance across complex multivendor environments is challenging at the best of times and impossible with manual processes.

Solution

FireMon makes sure you're always audit-ready with sub-second compliance checks across a library of 350+ controls. Automatically verify each network change to stay ahead of the auditors and detect when compliance starts to drift. Optimize all the capabilities of Palo Alto Networks devices, including application and user details through the same interface that you're managing any other firewalls through, ensuring rules conform to your industry requirements and security best practices across your entire network.

Use Case 2: Automating Enterprise Change Management to Increase Speed and Minimize Errors

Challenge

Manual change management is a dangerous business. It slows the business down, hinders agility, and introduces countless opportunities for errors. Firewall and cloud group security misconfigurations can open vulnerabilities and expose critical data and workflows to attack.

Solution

FireMon gives you speed and confidence with end-to-end orchestration for Palo Alto Networks devices. Complete visibility into the effects of rules helps uncover shadowed, redundant, hidden and overly permissive rules. Changes happen in seconds for the entire rule lifecycle—request, design, risk scoring, implementation, monitoring and decommissioning—all from a single FireMon console. You can create rule checks, track changes, remediate security failures, and monitor traffic with total automation.

Use Case 3: Automate the Discovery and Remediation of Policy Issues by Integrating FireMon with Cortex XSOAR

Challenge

The complexity of enterprise network infrastructure can make security incidents related to network security policies difficult to detect and manage. Once the incident is uncovered, manual remediation is often time-consuming and error-prone. Policy management needs to be integrated across the entire ecosystem, with automated tools to evaluate policy changes and implement changes.

Solution

FireMon integrates fully with Cortex® XSOAR, adding automated policy management to the orchestration platform. FireMon analyzes the policy-related event data it receives directly from Cortex via API, determines any changes that need to be made to address it and can enact those changes automatically with admin approval. This allows for the automated discovery and remediation of policy-related issues with a suite of rule assessment tools to detect vulnerabilities, misconfigurations, and traffic paths.

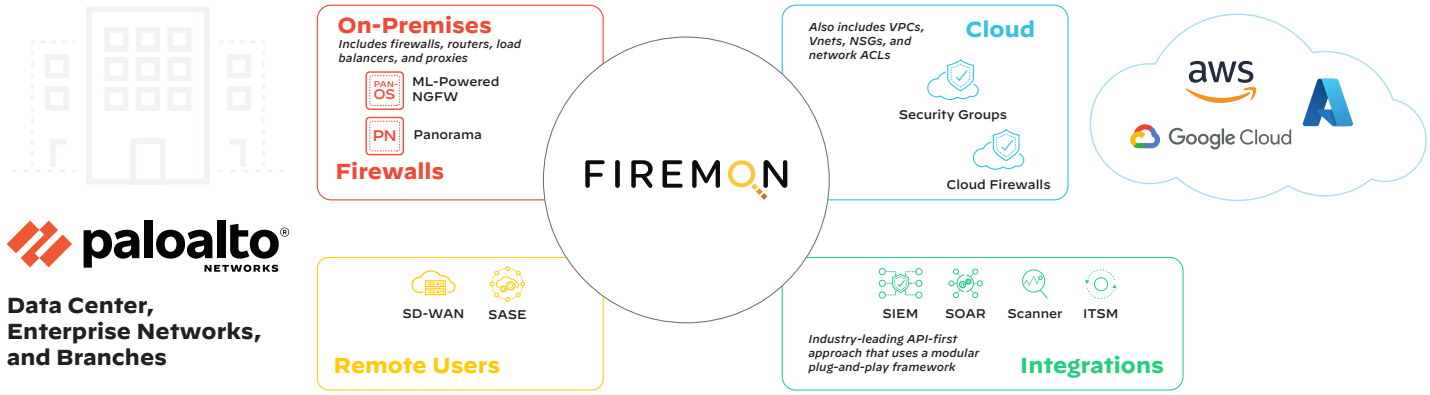

Figure 1: FireMon security policy management

About FireMon

FireMon is the only real-time security policy management solution built for multi-vendor hybrid enterprise environments. FireMon provides policy automation for the latest network security technologies helping organizations achieve continuous compliance while minimizing policy-related risk. Only FireMon delivers complete visibility and control across an organization's entire IT landscape.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. 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