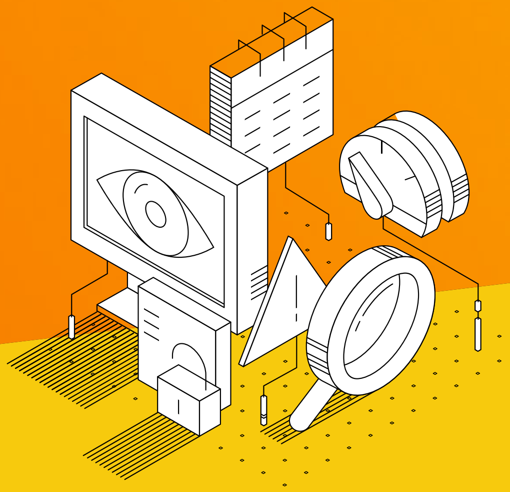
FIREMON

Intelligent Policy Automation

Orchestrating change management with speed and security



The Challenge: Balancing business needs with security/compliance

Firewall teams are under immense pressure to balance the needs of both the business and the security and compliance groups. If an access request is denied, even for security reasons, and it prohibits business, they get noticed – and not in a good way. Conversely, access request approvals that violate security may go ignored or unnoticed, because in many cases, business productivity trumps security.

Specific challenges include:

- Time-consuming change requests, averaging 2-3 weeks to complete
- Managing multiple de-centralized systems that increase management complexity
- Compromising security to meet Service Level Agreements (SLAs)
- Lack of understanding of the total impact of the change request

Faster isn't always better

The pressure to open up access to meet SLAs combined with limited security resources can lead to incorrect changes being implemented, negating the work and increasing unnecessary risk to the business. Introducing workflow automation into the change process helps reduce time and increase productivity, but it can also introduce security holes that allow cyber attackers to gain a foothold in an organization. Turnkey automation solutions miss an important piece of the automation puzzle – the context of the environment it is automating.

The Solution: Intelligent Policy Automation

When automating policy change management, one size does not fit all. Each step in establishing an automated process and utilizing it in practice should be context-aware to ensure changes are not simply implemented quickly but also correctly. FireMon is the first to effectively address this dilemma with its framework for Intelligent Policy Automation (IPA).

WHY INTELLIGENT POLICY AUTOMATION?

- Balances the needs of both business and security/compliance groups
- De-risks a "one-size-fits-all" solution

95% of the change management process is planning to ensure the best rule is implemented.

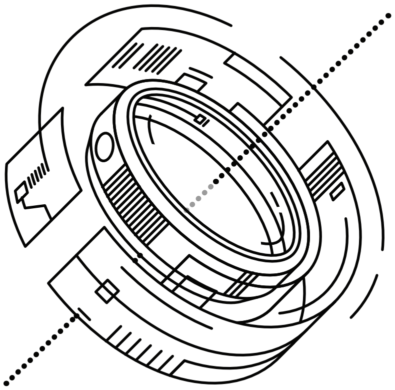
What is Intelligent Policy Automation?

Intelligent Policy Automation (IPA) is the industry's only firewall policy change management solution that safely and effectively ensures policy automation needs are met while reducing an organization's risk posture. Fully flexible workflows ensure organizational requirements and processes are maintained during change automation. IPA lets you decide where automation should enter the workflow and where it might be better to keep things manual.

- **Request** – Integrate with existing ticketing systems to enable new requests to filter directly into FireMon's change automation platform. Customize request forms to ensure all relevant change information is captured upfront.
- **Design** – Verify that new access is required to meet the request. If a change already exists or an existing rule can be modified to allow the requested access, then a new rule isn't necessary. Fewer unnecessary rules, means longer device life and less risk.
- **Analyze** – Run a pre-change analysis on proposed rules to determine the impact to security and compliance.
- **Review** – Establish criteria during the analysis phase that, when met, kicks off automated review, implementation, and verification or a mix of the three.
- **Implementation** – Get the necessary contextual, device-specific assistance for implementing rules or automate implementation as it fits your organization's established process (for supported devices).
- **Verification** – Manually or automatically verify that the change meets the plan and followed the appropriate process for implementation.
- **Monitor/Review** – Review, amend, and decommission policies as business needs and threats demand using FireMon's suite of security management products.

Who is FireMon?

FireMon solutions deliver continuous visibility into and control over network security infrastructure, policies, and risk. Using the FireMon Security Intelligence Platform, today's enterprise organizations, government agencies, and managed services providers dramatically improve effectiveness of network defenses, optimizing investments and speeding response to changing business demands.



Pre-Change Impact Analysis FireMon's proprietary Security Concern Index to determine the level of risk introduced by a proposed change.

Automated Change Verification confirms the right change was made and followed the correct process.

FULLY FLEXIBLE CONFIGURATION OPTIONS:

- Standards-based workflow engine
- Pre-change impact assessments
- Workflow development that integrates into complex enterprise environments
- Flexible approval mechanisms based on risk of change

IMPLEMENTATION SUPPORT FOR:

- Cisco ASA 8.3 (Syntax)
- Palo Alto Networks v7+ (through Panorama)

Learn more about our solutions: www.firemon.com

FIREMON

8400 W. 110th Street, Suite 500
Overland Park, KS 66210 USA