

INTEGRATION BRIEF

FireMon + Fortinet

Comprehensive firewall rule management to reduce risk, manage change, and enforce compliance

Enterprise network environments are getting more and more complex every day with a steady stream of new devices, applications, and cloud services. Manual tools can't keep pace, leaving firewall and security policies nearly impossible to manage and open the door to compliance violations and misconfigurations that can lead to unplanned outages and data breaches.

FireMon Security Manager is an essential tool for FortiGate and FortiManager users to effectively manage policies to eliminate policy-related risk, accurately change rules, and meet internal and external compliance requirements.

Firewall Policy Management Challenges

Managing firewall policies poses several challenges for organizations, including identifying high-risk vulnerabilities within the policies, reducing turnaround time for policy changes, and ensuring compliance with internal and external standards. Additionally, organizations may need to migrate policies to Fortinet devices or the cloud and manage policies that span multiple devices from different vendors. Overcoming these challenges requires intelligent solutions that can tame the complexity of the entire firewall rulebase, giving network security teams the ability to effectively manage firewall policies ensuring they are up to date, properly configured, and secure from security threats.

The FireMon Solution for Fortinet

FireMon's Security Manager network security policy management platform (NSPM) enables organizations to effectively manage the complexity of firewall policies.

Highlights

- Find high-risk vulnerabilities embedded in firewall policies
- Avoid misconfigurations and reduce turnaround time for firewall policy changes
- Achieve and maintain compliance with internal and external standards
- Migrate firewall policies to Fortinet devices and the cloud
- Manage rules and policies that span Fortinet and devices from other vendors

Reduce Policy-Related Risk

- Real-time risk evaluation and alerts detect and immediately notify teams of policy vulnerabilities in the environment
- Risk and threat modeling evaluates the impact of exploits and displays recommended patches
- Risk guardrails review proposed policy changes to ensure new risks aren't introduced
- Vulnerability scanner integrations give deeper insight to policy-related risks

Manage Firewall Rule Changes

- Real-time change monitoring detects new policies and changes to existing policies
- Automated rule change workflows span the entire rule creation and change process
- Policy change automation recommends rules and optionally can deploy them to devices across the network

Achieve and Maintain Compliance of Firewall Policies

- Consolidated compliance reporting takes only minutes to produce accurate reports
- Built-in reports for standards including PCI-DSS, NERC-CIP, NIST, and GDPR
- Real-time violation detection identifies policy violations in existing rules and catches new ones before they are deployed
- Rule recertification workflows automate rule reviews and recertification

Firewall Policy Migration to Fortinet Devices or to the Cloud

- Transfer firewall rules and policies from existing firewalls to Fortinet devices and/or the cloud
- Centralized policy management simplifies rule review, cleaning, and staging for migration

Multi-Vendor Firewall Policy Management

- Gathers devices and policies across the entire environment with built-in support for over 80 vendors
- Translates multi-vendor policies into a consistent, centralized rule database
- Full visibility and control for reporting, audit tracking, and policy management

FireMon Security Manager Key Features

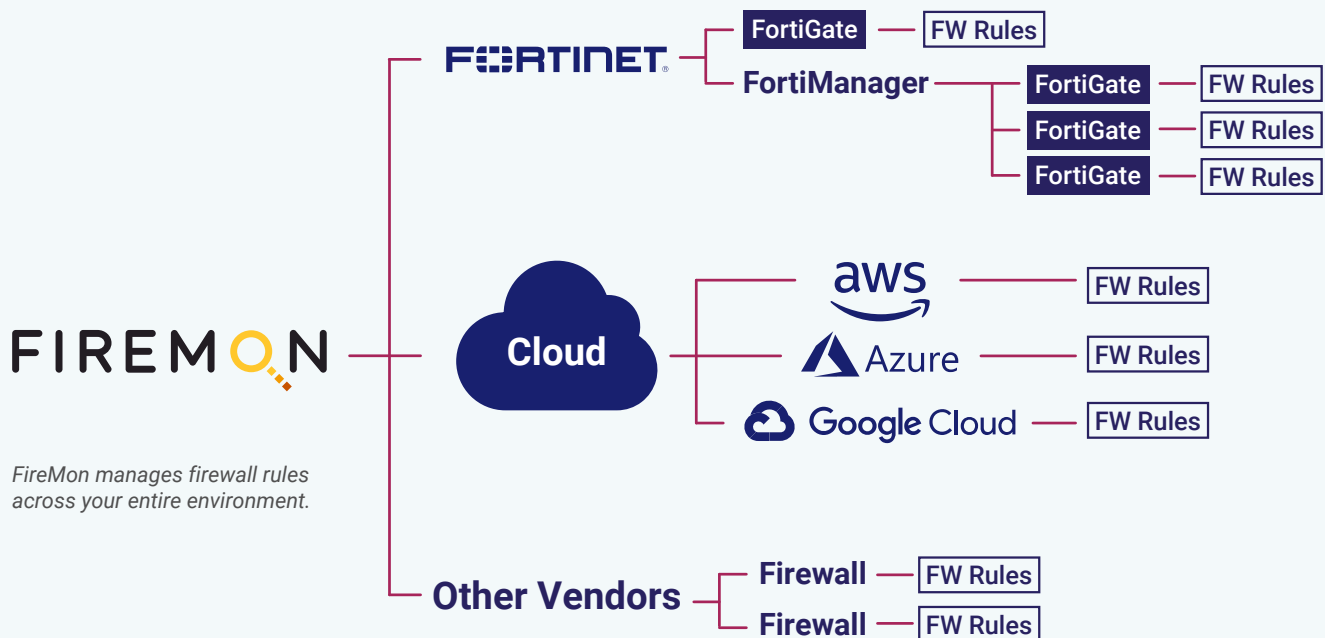
- A real-time centralized repository of firewalls, rules, and policies that spans the entire environment including the cloud
- Search for any device, policy, or rule with FireMon's proprietary Security Intelligence Query Language (SiQL)
- Consolidated compliance and risk assessments with over 20 preconfigured reports
- 500+ controls and ability to create new ones using custom queries
- Intelligent rule design and change workflows with optional ITSM integration
- Rule review and recertification for complete rule lifecycle management
- Every platform available via APIs and over 100 native integrations
- Architected for scale and reliability in any size environment

FireMon + Fortinet: How it Works

Fortinet is accelerating digitization with solutions engineered for integrated security and networking. The Fortinet Security Fabric offers a broad portfolio of integrated and automated security tools to make real-time network security a reality. As part of the Fortinet Security Fabric, FortiManager provides full visibility and control of the Fortinet Security Fabric and enables management of Fortinet products and devices including FortiGate firewalls, through a single console.

FireMon complements FortiManager and FortiGate devices with a suite of specialized tools specifically designed to manage the complexity of firewall rules and policies. Once deployed, FireMon gathers rules and policies from every firewall across the environment and stores them in a centralized rule repository. Whether an entire network comprising 100% FortiGate and FortiManager devices, or a combination of various vendors, including the cloud, FireMon pulls it all together into a single platform for visibility and control of the entire rulebase.

This single source of truth powers a comprehensive network model that offers policy and rule mapping, security control evaluations, and consolidated compliance reporting. It also adds a layer of intelligence that proposes rule changes and automatically checks that new rules won't inject any additional risk in the environment or violate compliance requirements before they are deployed.



Results of Using FireMon with FortiGate and FortiManager

90% Less Time to Create Compliance Reports FireMon transforms compliance reporting from a year-round exercise to the click of a button. Reporting that would normally take audit teams weeks to collect and consolidate takes only minutes with FireMon.

90% Less Time to Create and Deploy New Firewall Rules Take the guesswork out of rule creation with FireMon's intelligent tools that find optimal routes between devices and provides accurate step-by-step instructions to create the rules manually or use the option to have Security Manager automatically deploy them across the environment.

100% Detection of High-Risk and Misconfigured Rules FireMon's visibility to every rule and policy enables it to find every overly permissive and unused rule, and those that inadvertently expose services to the possibility of being exploited. It also protects the environment from the accidental creation of new risks by checking rule changes for vulnerabilities before they are deployed.

90% Less Time to Migrate Firewalls Security Manager makes the job of migrations easier by helping security teams review firewall rules to ensure they are needed and functioning as intended. Once cleaned, the rules are ready to move from one vendor to another, or to the cloud. Migrations to Fortinet devices or cloud security groups can be performed quickly and accurately with simply the click of a button.

FIREMON

FireMon's mission is to improve security operations that will in turn lead to better security outcomes. FireMon delivers industry-leading security policy management, cloud security operations, and asset management solutions. Our platform is the only real-time solution that reduces firewall and cloud security policy-related risks, manages policy changes, and enforces compliance. FireMon's Cloud Defense solution (formerly DisruptOps) is the only distributed cloud security operations offering that detects and responds to issues in the fast-paced public cloud environments. Our cloud-based Asset Management solution (formerly Lumeta) scans entire infrastructures to identify everything in the environment and provide valuable insights into how it's all connected.

FORTINET

Fortinet (NASDAQ: FTNT) is a driving force in the evolution of cybersecurity and the convergence of networking and security. Our mission is to secure people, devices, and data everywhere, and today we deliver cybersecurity everywhere you need it with the largest integrated portfolio of over 50 enterprise-grade products. Well over half a million customers trust Fortinet's solutions, which are among the most deployed, most patented, and most validated in the industry. The Fortinet Training Institute, one of the largest and broadest training programs in the industry, is dedicated to making cybersecurity training and new career opportunities available to everyone. FortiGuard Labs, Fortinet's elite threat intelligence and research organization, develops and utilizes leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence. Learn more at <https://www.fortinet.com>, the Fortinet Blog, and FortiGuard Labs.