

FIREMON SOLUTION BRIEF

FireMon + Fortinet

Real-Time Visibility and Unified Policy Management Across Entire Hybrid Estate

As organizations turn to digital transformation initiatives to accelerate their businesses, reduce costs, and improve customer experience, their network complexity and rates of change have both skyrocketed. To ensure security, compliance, and agility, Fortinet customers need to comprehensively manage network policies across heterogeneous firewalls and cloud environments. Through the partnership between Fortinet and FireMon, customers can manage policy through a single interface—across Fortinet, traditional and cloud-based firewalls, and cloud security groups.

Challenges of Managing Heterogeneous Environments

As networks become more complex and firewall rulesets continue to grow, it is increasingly difficult to identify and quantify the risk that is introduced by misconfigured or overly permissive firewall rules across distributed heterogeneous environments and multi-vendor firewall estates. At a time when enterprise priorities demand an agile approach to network security, organizations that do not have an integrated way to manage security policies across heterogeneous networks struggle with:

- Lack of visibility across all devices and gaps with insight into policies and routing paths across cloud and on-prem networks
- Lack of interoperability and integration resulting in manual security and compliance checks across systems
- Changes in the environment leading to increased risk of misconfigurations and an inability to keep pace with DevOps processes
- Inability to scale policy management and sustain intent across the entire multi-vendor network
- Expanding attack surface that makes it harder to maintain security and compliance

The FireMon-Fortinet partnership enables companies to simplify and automate policy management across heterogeneous networks to:

- Improve the security and compliance posture by ensuring alignment between Fortinet policies and all enterprise standards
- Visualize and analyze all network traffic to identify security and compliance risks
- Increase security agility and efficiency by managing network policies centrally across the entire hybrid network, including firewalls and cloud security groups
- Automate and streamline workflows for policy creation and management
- Ensure continuous compliance by monitoring network access paths and with alerts to potentially risky policy changes
- Simplify migration to Fortinet with a comprehensive view of existing firewall policies
- Monitor and identify rule changes that impact the security posture, compliance, or business continuity

FireMon and Fortinet: How the Integration 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 agile 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 in multi-vendor firewall environments. By providing visibility of the Fortinet firewall implementations within a single pane of glass, FireMon enables customers to manage policies from multiple firewall vendors along a common source of truth and enforce security and compliance across a range of network devices.

The integration allows FireMon users to collect information from Fortinet FortiManager to be used

in FireMon's Network Security Policy Management platform and FireMon Automation.

FireMon collects and aggregates Fortinet policy information directly into the FireMon platform and builds it into the FireMon network model that includes network topology, security controls, and assets. Customers can visualize the Fortinet network devices as part of their overall network map in relation to the hybrid network security topology.

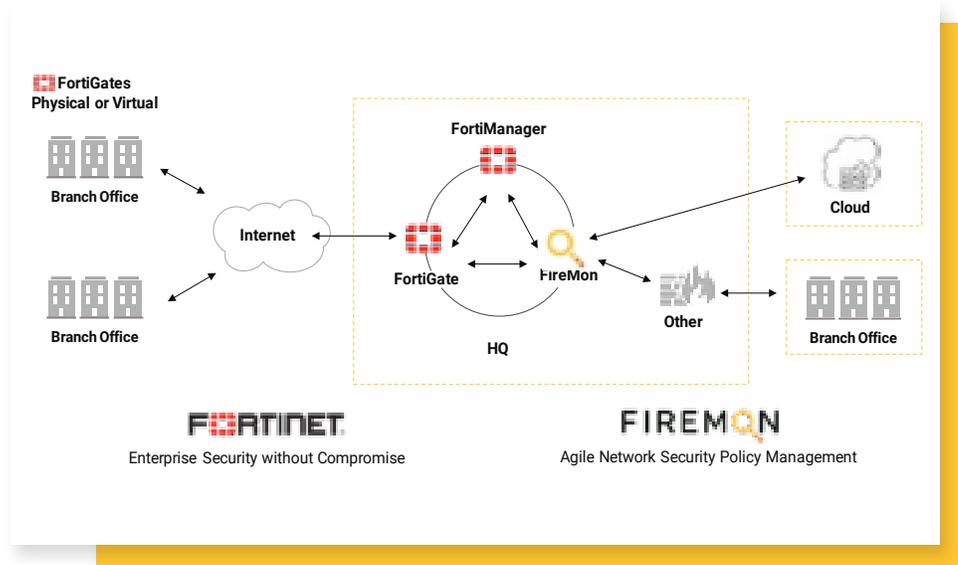


Figure 1. Real-time Visibility and Unified Policy Management Across the Entire Hybrid Estate

Security Policy Management Use Cases

With the Fortinet policy information available, FireMon applies real-time policy analysis to ensure the desired security policy enforcement is in place. Joint customers will be able to visualize configuration, policy, and rule usage statistics across all network security enforcement points and address the following use cases:

Policy Management Normalize and manage policies across firewalls, next-generation firewalls, and cloud environments from various vendors from a single pane of glass.

Policy Validation Validate policies against regulatory requirements or custom-defined policies.

Access Analysis Confirm security controls enforce access, security, and compliance policies.

Rule Base Compliance Monitor and ensure security controls continuously maintain compliance with defined access and rule policies. Identify rules, access, and configuration compliance violations.

Network Mapping Automatically collect and build Fortinet firewall data into a visual and interactive model that provides network abstraction of access paths end-to-end with access path analysis and network map visualization.

Rule Review Analyze firewall configurations to identify hidden, unused, shadowed, or overly permissive rules that provide more access than necessary.

Change Tracking Track changes to firewall rules for compliance or rule review analysis. Ensure changes are certified. Identify when a change occurred, who made the change, and whether it was expected. Determine if the change has a negative impact.



Figure 2. The Overview Dashboard view of the Fortinet FortiGate firewall within FireMon Security Manager, showing rules identified for cleanup and improvement.

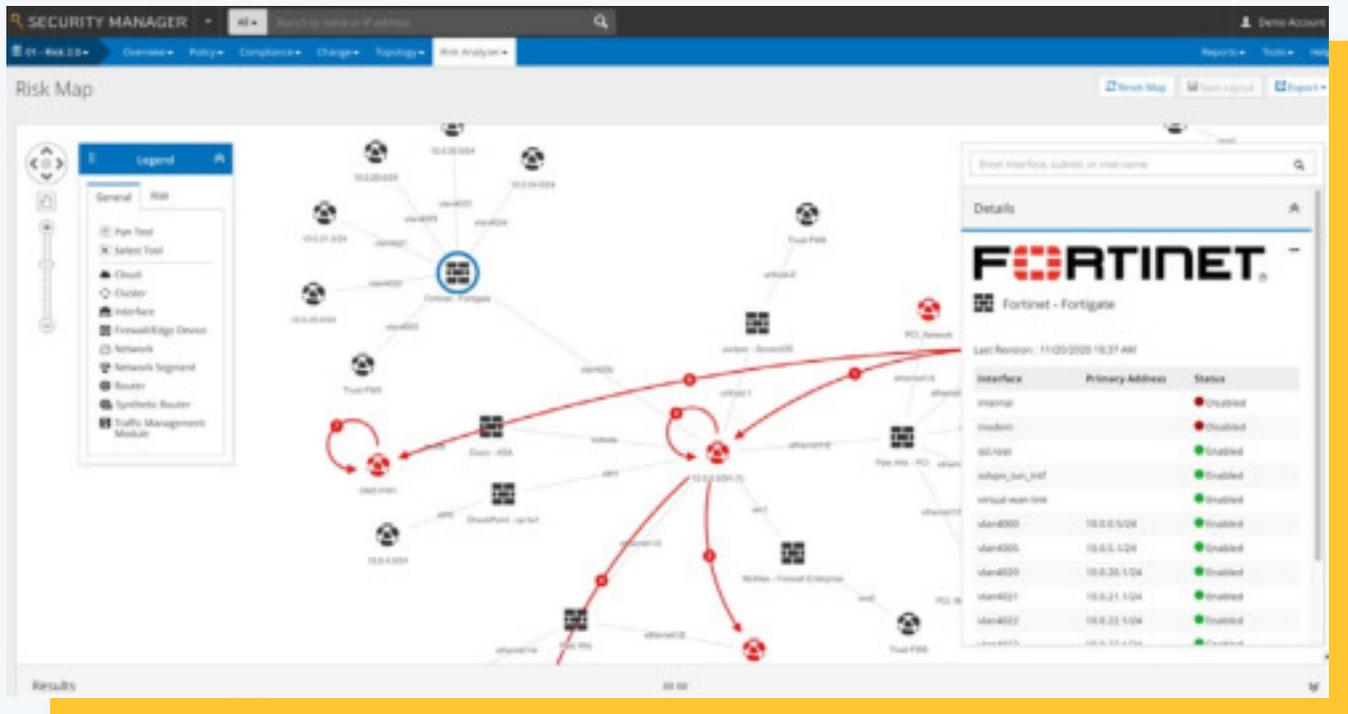


Figure 3. The Risk Analyzer dashboard view of the Fortinet FortiGate firewall within FireMon Security Manager, showing disabled devices.

FIREMON

FireMon is the only agile network security policy platform for firewalls and cloud security groups providing the fastest way to streamline network security policy management, which is one of the biggest impediments to IT and enterprise agility. Since creating the first-ever network security policy management solution, FireMon has delivered command and control over complex network security infrastructures for more than 1,700 customers located in nearly 70 countries around the world. For more information, visit www.firemon.com.

FORTINET®

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networked, application, multi-cloud or edge environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 465,000 customers trust Fortinet to protect their businesses. Both a technology company and a learning organization, the Fortinet Network Security Expert (NSE) Training Institute has one of the largest and broadest cybersecurity training programs in the industry. Learn more at www.fortinet.com, the Fortinet Blog, or FortiGuard Lab.