INTEGRATION BRIEF

FireMon + Sophos

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. Sophos customers need to comprehensively manage network policies across mixed-vendor firewall and cloud environments. Through the partnership between Sophos and FireMon, customers can manage policy through a single interface—across Sophos, traditional and cloud-based firewalls, and security groups.

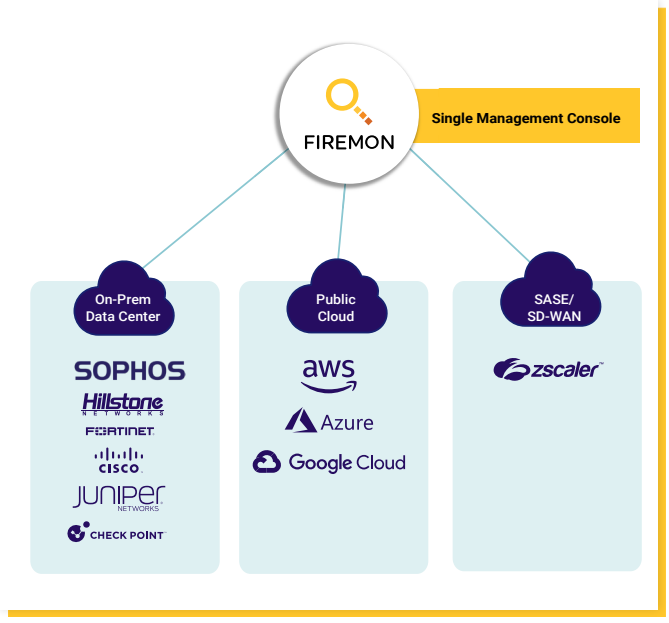
Challenges of Managing Mixed-Vendor Environments

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 rules across distributed heterogeneous environments and multi-vendor estates. At a time when enterprise priorities demand a flexible 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-Sophos partnership enables companies to simplify policy management across heterogeneous networks to:

- Improve the security and compliance posture by ensuring alignment between Sophos policies and all enterprise standards
- Visualize and analyze policy behavior 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
- Ensure continuous compliance by monitoring network access paths and with alerts to potentially risky policy changes
- Simplify migration to Sophos with a comprehensive view of existing firewall policies
- Monitor and identify rule changes that impact the security posture, compliance, or business continuity



FireMon and Sophos: How the Integration Works

Sophos Networks provides innovative and accessible cybersecurity solutions that reshape enterprise security, enabling cyber resilience. FireMon compliments Sophos Networks in multi-vendor firewall environments. By providing visibility and control of the Sophos 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 Sophos to be used in FireMon's Network Security Policy Management platform. FireMon collects and aggregates Sophos 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 Sophos network devices as part of their overall network map in relation to the hybrid network security topology.

Security Policy Management Use Cases

With the Sophos 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 and policy 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 best practices.

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 Sophos firewall data into an abstracted model that provides a network map visualization.

Rule Review: Analyze firewall configurations to identify hidden, 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.

SOPHOS

Sophos evolves to meet every new challenge, protecting millions of users and over 500,000 organizations of all sizes in more than 150 countries from today's most advanced cyber threats.

We now bring that same always-evolving belief to home users. At Sophos, we want to make sure the same level of protection we provide businesses is available to everyone. Sophos Home brings our powerful, business-grade protection to personal Macs and PCs. You're online all the time, at work and at home. Your security should be as well.

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 firewall policy-related risk. Only FireMon delivers complete visibility and control across an organization's entire IT landscape. Firemon.com

SB0314-EN-20231102-00