INTEGRATION BRIEF

FireMon + Zscaler

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 Zscaler users to effectively manage policies to eliminate policy-related risk, accurately change rules, and meet internal and external compliance requirements.

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 Zscaler devices and the cloud
- Manage rules and policies that span Zscaler and devices from other vendors
- Centralize, normalize, and enforce network security policies across the entire hybrid estate, including firewalls, cloud security groups, and Secure Access Service Edge (SASE) platforms

Firewall Policy Management Challenges

Managing firewall policies poses several challenges for organizations, including high-risk vulnerabilities within the policies, reducing turnaround time for policy changes, and ensuring compliance with internal and external standards. Plus, with the adoption of cloud services, SaaS delivery models, and the turn to SD-WAN and Secure Access Service Edge (SASE) technologies, it's imperative for security teams to manage risk and ensure compliance across these highly complex networks. Additionally, organizations may need to migrate policies to Zscaler's Advanced Cloud Firewall to manage policies that span multiple devices from different vendors. Overcoming these challenges requires intelligent solutions that can tame the complexity to 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 Zscaler

FireMon's Security Manager network security policy management platform (NSPM) works in harmony with Zscaler's Zero Trust Exchange advance cloud firewall and enables organizations to manage the complexity of firewall policies.

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 risk

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 Zscaler Firewall

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

Multi-Vendor Firewall Policy Management

- Gather 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

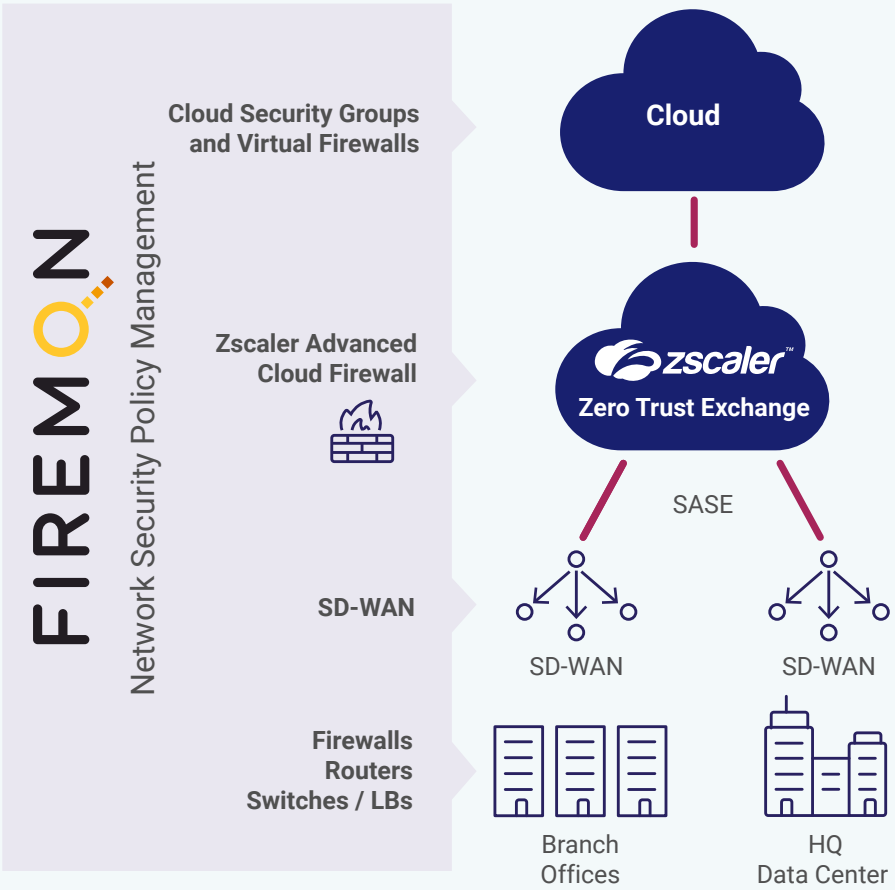
- A real-time centralized repository of firewalls, rules, and policies that spans the entire environment including the secure service edge and cloud
- Search for any device, policy, or rule with FireMon's proprietary Security Intelligence Query Language (SiQL)
- Consolidated compliance and risk assessments 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
- Strong API first support with over 100 native integrations
- Architected for scale and reliability in any size environment

FireMon + Zscaler: How it Works

Zscaler's FWaaS (firewall-as-a-service) is the only cloud-delivered firewall that can deliver zero trust. Their FWaaS safeguards web and non-web traffic for all users, applications, and locations with the industry's most comprehensive cloud native zero trust platform. Zscaler Firewall offers full protection for work-from-anywhere users, complete inspection to find hidden attacks, catches evasive web traffic on non-standard ports and more.

FireMon complements Zscaler Advance Cloud Firewall 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 of 100% Zscaler 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. Customers can visualize the Zscaler Firewall as part of their overall network map in relation to the hybrid network security topology, including local internet breakouts from the edge router outward to the Zscaler Firewall.

The 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 Zscaler

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 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're 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 Zscaler 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.

zscaler™

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyber attacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. For more information, visit www.Zscaler.com

SB0272-EN-20230705-01