INTEGRATION BRIEF

FireMon + Microsoft Azure

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

The network fabric of digital enterprises is in a rapid state of flux thanks to the growing adoption of cloud and edge computing. Research shows that enterprises seldom restrict themselves to a single cloud platform as competing cloud vendors offer hyper scalable, secure, and stable hosting environments. Add to this the complexity of migration, from a physical data center to the cloud, which makes securing the infrastructure, data, and applications that much more challenging.

Firewall Policy Management Challenges

Enterprises around the world are adopting Microsoft Azure cloud environments to gain the benefits of cost reduction and business agility. As the speed of business accelerates, unified network policy must remain secure. Businesses must be as vigilant about threats to their data in the cloud as they are to threats against traditional enterprise networks. While Microsoft Azure secures the cloud instance, ultimately it is the organization's responsibility to protect their data in the cloud. Protecting cloud environments requires visibility with a platform that delivers a common visualization, normalized data structures, unified policies, scalability, and control.

The FireMon Solution for Microsoft Azure

FireMon's Policy Manager network security policy management platform (NSPM) enables organizations to effectively manage the complexity of both their physical data centers and in public and private cloud environments.

Highlights

- Orchestrate network security across physical data centers, public and private clouds
- Manage native, embedded security infrastructure in public and private clouds (IaaS applications)
- Manage Azure NSGs that control access to SaaS applications
- Manage Azure firewall policies for basic, standard, and premium
- Single-pane-of-glass visibility and control cross hybrid environment
- Perform global policy analysis with a holistic view
- Engage in real-time, scalable, continuous change management
- Avoid misconfigurations and reduce turnaround time for firewall policy changes

Reduce Policy-Related Risk

- Attack policy complexity and reduce risk
- Reduce policy complexity that can lead to increased risk
- Eliminate high risk, overly permissive rules
- Ensure dormant unused rules are not available for potential exploitation
- Remove shadow rules that can be misleading if performing manual policy analysis

Manage Firewall Rule Changes

- Automated rule change workflows span the entire rule creation and change processes
- Policy change automation recommends rules and can optionally 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

FireMon Policy Manager Key Features

- A real-time centralized repository of firewalls, rules, and policies that spans the entire environment
- 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

Firewall Policy Migration to Microsoft Azure Devices

- Centralized policy management simplifies rule review, cleaning, and staging for migration

Multi-Vendor Firewall Policy Management

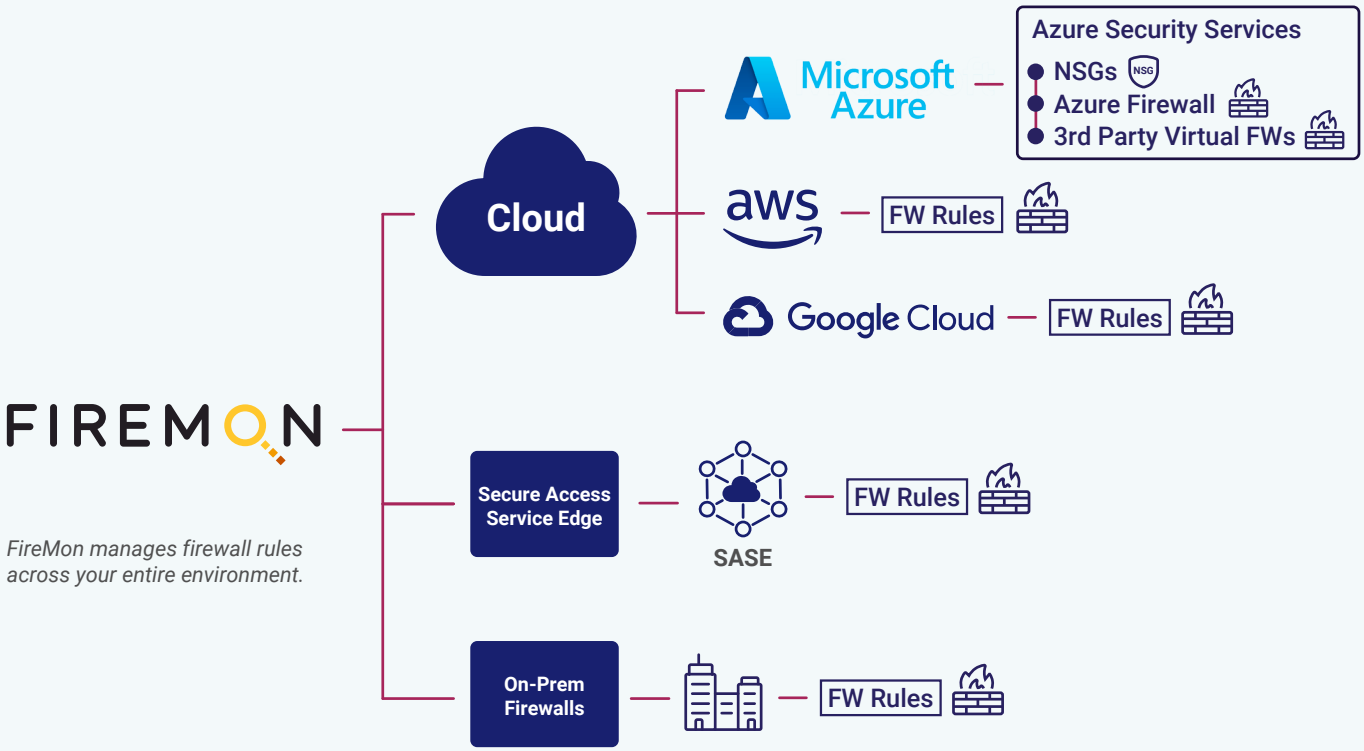
- Gathers devices and policies across the entire environment with built-in support for over 80 vendors
- Translates multi-vendor policies into a consistent, centralized rule database
- Full visibility and control for reporting, audit tracking, and policy management

FireMon + Microsoft Azure: How it Works

Microsoft Azure Firewall is a managed, cloud-based network security service that protects Azure Virtual Network resources. The stateful firewall services has built-in high availability and unrestricted cloud scalability to help you create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.

FireMon complements Microsoft Azure 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 composed of 100% Microsoft Azure devices, or a combination of various vendors, 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 interject any additional risk in the environment or violate compliance requirements before they're deployed.



Results of Using FireMon with Microsoft Azure

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 Policy 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 Policy 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 Microsoft Azure 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.

Microsoft

Microsoft (Nasdaq "MSFT" @microsoft) enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more.

SB0323-EN-20231218-01