FIREMON

SOLUTION BRIEF

The Dangers of DIY NSPM

The DIY approach to managing firewall and network security policies exposes organizations to increased risk, sluggish response to change requests, and compliance violations.

Network security is crucial for enterprises to protect sensitive data, combat cyber threats, and meet compliance standards. With specialized network security policy management (NSPM) solutions like FireMon, enterprises don't have to think twice about the security, compliance, or protection of their network infrastructure.

While some enterprises are tempted to build their own NSPM solution in-house, whether it be relying on spreadsheets, scripting tools, or open-source software, opting for this path often results in a slew of challenges.

The Challenges of Going it on Your Own

As firewall policies become increasingly more complex, most organizations start with spreadsheets to begin to wrap their arms around the task of managing them. It's easy to think that's it and move on, however spreadsheets are quickly overwhelmed by the millions of combinations of rules connecting devices, services, and ports across a network.

It's tempting to look at open-source tools, scripts, or even building a solution in-house that can manage the firewall policies. They may be inexpensive, but they lack the robustness and security needed for effective policy management.

These DIY solutions struggle to keep up with changes in the security environment. Established NSPM solutions provide a wide range of features to analyze policies, assess risks, report compliance, manage changes, and automate processes. Trying to replicate these with manual tools or DIY solutions is challenging and can slow down response times to cyber threats.

In-house NSPM solutions are often inefficient and costly, taking away valuable resources from core business initiatives. Developing and maintaining custom scripts or open-source tools can be labor-intensive and prone to errors. Investing in a ready-made solution offers swift deployment, saving time and reducing expenses for development, testing, and maintenance.

- **Opportunities for Mistakes:** A lack of expertise leads to mistakes, making established NSPM vendors such as FireMon, with years of honed solutions and field experience, preferable due to their understanding of security policy management complexities and the challenges of modern enterprises, while building in-house NSPM solutions demands significant expertise, research, and maintenance, which can be time-consuming and expensive.
- **Inability to React Quickly:** Established NSPM solutions offer a wide range of features such as policy analysis, risk assessment, compliance reporting, change management, and automation, which might be challenging for enterprises to replicate in a DIY solution due to resource and time constraints.
- **Time and Cost Inefficiency:** Building an NSPM solution requires significant resources and diverts attention from core business initiatives, whereas purchasing a ready-made solution enables swift deployment, saving time and reducing development, testing, and maintenance expenses.
- **Inability to Scale:** NSPM vendors prioritize scalability to meet the expanding needs of growing enterprises, whereas developing an in-house solution with similar scalability might result in inefficiencies and higher costs.
- **Inadequate Updates and Support:** Trusted NSPM vendors continuously update their solutions to protect against evolving threats, provide ongoing support, and save enterprises from the challenges of maintaining a DIY system with the same level of updates and support.
- **Lack of Integration and Compatibility:** NSPM solutions offer seamless integration with diverse security tools and devices, simplifying network security management, while building an in-house system that aligns with existing components can be complex and potentially cause compatibility problems.
- **Unproven Security and Reliability:** Established NSPM solutions undergo stringent testing and validation to meet industry security and reliability standards, prioritizing data protection, while developing an in-house system with equivalent standards can be

challenging, potentially risking severe consequences for the enterprise due to security lapses.

- **Time Consuming Training and Development:** The dynamic nature of talent within an organization necessitates constant training of new teams, and constructing a reliable NSPM solution requires a blend of expertise in network security, software development, and policy management; lacking these skills can result in vulnerabilities and inadequate security measures.

The FireMon Solution

Protecting your network from ever-evolving cyber threats is crucial for enterprises. That's why it's essential to choose a reliable and specialized Network Security Policy Management (NSPM) solution. By opting for a purpose-built solution like FireMon, organizations can ensure expert guidance, comprehensive features, seamless scalability, continuous updates, integration support, and robust security measures.

With FireMon, enterprises can confidently safeguard their networks while staying focused on their core business goals. Our purpose-built NSPM solution offers expertise, efficiency, and continuous support, empowering organizations to protect against emerging cyber threats and maintain continuous compliance.

Reduce Risk

FireMon reduces risk through real-time risk assessments, prioritizing rule violations, offering threat modeling, suggesting patches, and preventing potential attacks. FireMon Security Manager also continuously evaluates new rules and changes to prevent policy-related vulnerabilities.

Manage Change

FireMon efficiently manages change by continuously monitoring policy changes across all devices, both on-premises and in the cloud, promptly identifying potential impact on the organization. Additionally, it expedites the creation and modification of policy rules, ensuring accurate deployment while offering seamless automation for rapid implementation, taking just minutes to complete.

Enforce and Maintain Compliance

FireMon ensures organizations enforce and maintain compliance with customizable compliance reporting that generates in minutes. FireMon Security Manager also offers real-time violation detection for policy compliance, proactively alerting users, and automates firewall rule recertification, ensuring ongoing adherence to compliance, business, or security policies

Summary

In today's complex network landscape, building your own NSPM solution or relying on spreadsheets, custom scripts, or open-source software can put your organization at significant risk. Instead, investing in a time-tested NSPM solution like FireMon is the best way for enterprises to protect their network infrastructure. With its expertise, cost-effectiveness, scalability, and enhanced security, a professional NSPM solution is an essential investment for any organization looking to secure their network. Don't take the risk of building your own solution – choose FireMon and ensure that your network security policies are in safe hands.

FIREMON

FireMon improves 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.COM

SB0308-EN-20231019-01