FIREMON

BUYER'S GUIDE: CHANGE AUTOMATION

Automating Firewall Security Policy Changes

How to select a network security policy management (NSPM) solution to improve operational efficiency and reduce costs with firewall policy management automation

Sponsored by

FIREMON

Contents

Introduction

Making changes to firewall rules and security policies may seem routine, yet the stakes are exceptionally high. A single misconfiguration can disrupt access for legitimate users to mission-critical services or, worse, allow unauthorized individuals to breach the system, exposing the organization to significant security threats. Effective management of these configurations is crucial to maintaining robust security postures and ensuring operational continuity. In this buyer's guide, we will explore best practices and advanced tools designed to streamline and fortify the process of managing firewall rules and security policies.

Staying ahead of evolving threats is paramount in the world of cybersecurity. One key aspect of this proactive defense is to ensure enterprises have efficient management of their firewall policies. However, manual policy changes are time-consuming and error prone, creating an untenable environment for operations teams to manage. To keep up with business needs, manual policy changes are often made in haste, introducing countless opportunities for error. These sloppy changes expose organizations to unplanned outages and vulnerabilities that can be exploited by attackers.

Change automation, facilitated by Network Security Policy Management (NSPM) solutions, has emerged as a crucial tool in this endeavor, offering enterprises a streamlined approach to enhance operational efficiency and reduce overall costs. Change automation refers to the process of automating modifications and updates to firewall policies, ensuring a prompt and uniform response to access requests. Firewall policies act as the gatekeepers of network security, regulating traffic to prevent unauthorized access and protect sensitive data. Manual updates to firewall rules are time-consuming and error-prone, with the average enterprise network team making more than 100 firewall changes a week, many taking up to 2 weeks or more to complete.

The importance of change automation in relation to firewall policies is multifaceted. A simple misconfiguration can block legitimate users to mission critical services or can let wrong users in, exposing the organization to attack. By automating the implementation of necessary changes, organizations can swiftly adapt to evolving cybersecurity landscapes, reducing the window of vulnerability. This flexibility is crucial in mitigating potential security incidents and safeguarding against cyber threats.

Operational efficiency is another key benefit to change automation. Manual management of firewall policies can be resource-intensive and prone to human errors. NSPM solutions equipped with change automation capabilities offer a centralized platform for policy management, streamlining the process and ensuring changes are applied consistently across the network. This not only minimizes the risk of misconfiguration but also allows network teams to focus on strategic tasks rather than routine maintenance.

Cost reduction is a compelling reason for enterprises to invest in an NSPM solution, as they provide a cost-effective alternative by optimizing resource utilization. Automated processes reduce the workload on network security teams, allowing them to allocate resources more efficiently and avoid potential financial losses associated with security incidents.

We at FireMon understand the challenges of firewall policy changes. We are an industry leader in solutions that improve speed and reduce the cost of policy changes to achieve business SLAs while improving security and availability.

EDUCATION

The Challenges of Manual Policy Changes

- **Complex Configurations:** Modern networks are intricate, comprising numerous devices, applications, and users, making manual handling of firewall policy changes prone to misconfigurations.
- **Error Prone:** Each modification introduces the risk of human errors, potentially opening security loopholes or disrupting essential services, leading to vulnerabilities.
- **Time Sensitivity:** Swift responses to emerging threats or changes in business requirements are crucial. Manual processes are often time-consuming, delaying the adaptation to new challenges and exposing networks.
- **Communication Breakdowns:** Manual changes may require coordination between different teams, leading to misunderstandings, conflicting modifications, or oversights that result in inconsistent policies.
- **Scalability Issues:** As organizations grow, the workload associated with manual policy changes becomes overwhelming. Human limitations hinder the ability to efficiently scale manual processes across large and complex infrastructures.
- **Inconsistent Policies:** Lack of seamless communication and coordination can result in inconsistent policies, weakening the organization's overall security posture.
- **Resource Intensive:** Manual handling of firewall policy changes demands significant time and resources, impacting the efficiency of security teams.
- **Limited Visibility:** Real-time monitoring and visibility are compromised with manual processes, making it challenging to promptly identify and respond to suspicious activities.
- **Human Resource Challenges:** The human-centric nature of manual processes poses challenges in terms of expertise, availability, and the potential for turnover affecting policy consistency.
- **Audit and Compliance Risks:** The delayed feedback loop associated with manual processes increases the risk of non-compliance and makes audits more challenging to conduct effectively.

Failure is Not an Option

- **Fines and Lost Revenue:** Fines, costs, and lost revenue incurred from manual policy misconfigurations that can lead to data breaches and unplanned outages.
- **Operational Inefficiency:** Wasted time and resources manually managing hundreds of change requests per week.
- **Lack of Growth:** Missing change SLAs for applications hinders company expansion and risks competitive edge.
- **Shadow IT:** The business looks to bypass security teams to meet their deadlines.
- **Burnout:** Teams become frustrated and burned out trying to manage the tangle of firewall policies.

The challenges of manually handling firewall policy changes encompass a range of issues, from the inherent complexity of configurations to the limitations of human resources and the need for swift responses in a rapidly evolving threat landscape. Automated solutions offer a way to mitigate these challenges, providing efficiency, consistency, and scalability in managing firewall policies.

Empowering Your Enterprise:
Key Stakeholders in Purchasing a Network Security Policy

Networks from the backbone of enterprises, enabling seamless communication, streamlined operations, and enhanced productivity. As your organization grows and evolves, ensuring the smooth function of your network becomes paramount. This is where Network Security Policy Management (NSPM) solutions come into play. However, the decision to invest in an NSPM solution involves multiple stakeholders within your enterprise. Let's explore the key players involved in this transformative journey.

1. **IT Leadership –** Guiding the Vision: The IT leadership, including the Chief Information Officer (CIO) and Chief Technology Officer (CTO), play a pivotal role in shaping the strategic vision for the enterprise's technology infrastructure. They identify the need for an NSPM solution, align it with business goals, and define the outcomes expected from its implementation. Their insight ensures that the NSPM solution aligns with the organization's overarching IT strategy, security requirements, compliance standards, and budgetary considerations.

2. **Network Operations Teams –** Keeping the Network Afloat: The network operations team, comprising network engineers and administrators, are at the forefront of managing and maintaining your network. These experts are responsible for day-to-day network operations, troubleshooting issues, optimizing performance, and ensuring network availability. Their intimate knowledge of the network's intricacies is essential in evaluating NSPM solutions, as they can provide invaluable insights into the specific challenges faced and the desired capabilities needed to address them effectively.

3. **Security Team –** Safeguarding Your Assets: The security team is tasked with protecting your enterprise's digital assets from cyber threats, ensuring data confidentiality, integrity, and availability. In the context of NSPM solutions, they focus on identifying vulnerabilities, detecting intrusions, and monitoring network traffic for any suspicious or malicious activities. The security team's involvement in purchasing an NSPM solution ensures that it aligns with the organization's security policies, allows for real-time threat detection and response, and integrates with existing security infrastructure.

4. **Finance and Procurement –** Maximizing ROI: The finance and procurement department plays a crucial role in evaluating the financial implications of investing in an NSPM solution. They assess the total cost of ownership, return on investment (ROI), and negotiate pricing and licensing agreements. By collaborating closely with IT leadership and other stakeholders, they ensure that the chosen NSPM solution delivers tangible business value while adhering to budgetary constraints.

5. **Compliance and Legal –** Meeting Regulatory Requirements: In industries governed by strict regulations, such as healthcare, finance, or government, compliance and legal teams are vital stakeholders in NSPM solution procurement. They evaluate whether the solution meets industry-specific compliance requirements, data privacy standards, and regulatory mandates. Their involvement ensures that the NSPM solution aligns with legal obligations, protects sensitive data, and enables effective audit trails for regulatory purposes.

6. **User Representatives –** Advocating for User Experience: User representatives, such as department heads or end-users, provide critical input based on their firsthand experience with the existing network infrastructure. Their insights are invaluable in identifying pain points, understanding usability requirements, and assessing the impact of implementing an NSPM solution on workflow and productivity. By involving user representatives, you can ensure that the selected NSPM solution seamlessly integrates into daily operations and enhances the end-user experience.

Purchasing an NSPM solution requires collaboration and alignment amount various enterprise stakeholders. The IT leadership sets the strategic direction, while the network operations, security finance, compliance, legal, and user representatives provide essential perspectives. By harnessing the collective expertise of these key stakeholders, you can make an informed decision, select the NSPM solution, and empower your enterprise to unlock the full potential of its network infrastructure.

INTERNAL BUSINESS CASE DEVELOPMENT

How to Build a Business Case for a Network Security Policy Management Solution

While investing in security tools can be expensive, having a policy management tool is crucial for maximizing security investments, managing compliance and risks, and quickly making rule changes. As business justification is necessary for any large investment, this section will help outline our recommendations to build a strong case for investing in an NSPM solution.

Identify the Problems: Identify gaps, redundancies, and inefficiencies in an organization's current network security. This helps begin identifying the problems at hand.

Define the Solution: Research NSPM tools that will help solve the problems identified in the first bullet. FireMon offers a centralized platform for firewall management with advanced analytics and reporting tools, providing complete visibility and quick identification and mitigation for security risks for organizations.

Outline the Benefits: Outlining the benefits of instituting an NSPM solution to the affected teams demonstrates the value it would have for the organization. With FireMon, users can expect a decrease in operational costs, reduced time spent on manual tasks, fewer security related risks, and more.

Calculate the ROI: Calculate the ROI to demonstrate the financial benefit of implementing an NSPM solution like FireMon. Start by calculating the ROI for Audits & Compliance, Change Management, and Risk Reduction.

Present the Business Case: When presenting the business case for NSPM, ensure to emphasize its benefits and how it can address the identified problem, using data and metrics to support the case, including the ROI calculations discovered in the previous bullet.

Calculate the ROI for Change Automation with FireMon:

1. How many firewalls are in the environment? ___
2. How much time is spent manually changing firewall policies? ___
3. What is the average weighted cost of staff responsible for manually updating firewall policies? ___

With this information, begin the ROI calculation by:

4. Multiplying the number of firewalls by the number of hours spent on each firewall: ___
5. Then multiply the weighted cost of staff responsible for performing these manual tasks by the total number of hours spent working on each firewall: ___

Keep in mind, this is just the ROI for automating firewall policy changes with FireMon. There are other ROI calculations that can be added if the NSPM solution is used for maintaining compliance and risk reduction.

FireMon customers regularly report seeing up to a 90% reduction in the amount of time and resources it takes to create and update firewall policies, saving days, if not weeks, in the overall policy change process. They also see policy misconfigurations drop off significantly depending on how they use the platform, with some customers reporting no policy misconfigurations since they deployed FireMon.

What to Look for in a Policy Automation Solution

When searching for the perfect policy automation solution for your business, the decision should never be made lightly. The right platform can streamline operations, enhance compliance, and significantly reduce manual labor, transforming your policy management into a seamless, efficient process. There are a handful of key features and benefits to look for, ensuring you choose a solution that aligns perfectly with your organization's needs:

1. **Comprehensive Integration Capabilities:** Your ideal policy automation tool should effortlessly integrate with existing systems within your organization. This ensures a smooth workflow and eliminates the need for manual data entry, thereby enhancing efficiency and reducing the risk of human error.
2. **User-Friendly Interface:** A solution is only as effective as its usability. Look for a platform with an intuitive design that allows users to easily create, manage, and enforce policies without requiring extensive training or technical knowledge.
3. **Flexible Customization Options:** Every business has unique needs. A top-tier policy automation solution offers customizable templates and workflows that can be tailored to meet specific operational requirements, ensuring that the platform serves your organization in the most effective manner possible.
4. **Robust Reporting and Analytics:** Insightful data is the foundation of informed decision-making. Opt for a solution that provides comprehensive reporting and analytics capabilities, allowing you to monitor compliance, track the effectiveness of your policies, and identify areas for improvement.
5. **Stellar Customer Support:** Even with the most user-friendly solution, questions and challenges will arise. Ensure that your selected platform is backed by responsive and knowledgeable customer support, ready to assist you every step of the way.

Choosing the right policy automation solution is pivotal for operational success. By prioritizing integration capabilities, user experience, flexibility, analytics, and support, you're not just investing in a tool—you are investing in the future of your organization.

NAVIGATING THE BUYING JOURNEY

What to Consider When Looking to Perform a Technical Evaluation of an NSPM Solution for Policy Automation

Similar to many IT-related projects, an NSPM solution for firewall policies may require a technical evaluation depending on the complexity of the organization's environment and firewall policy structure.

If required, here's our three-step process for conducting a comprehensive technical evaluation for an NSPM solution:

1. **Define Objectives:** Identify the organization's network security objectives and requirements such as achieving continuous compliance, risk reduction strategies, improving operational efficiencies, and reducing costs.
2. **Develop Success Criteria:** Work with the vendor's sales engineering team to build a list of success criteria that helps assess its technical capabilities.
3. **Conduct a Proof-of-Concept (PoC):** This critical step in the evaluation process enables testing the solution in the environment and provides valuable insights into its fit within the organization.

FireMon regularly helps many organizations successfully conduct technical evaluations and even offers a managed POC program. Contact us for more details.

Here are the recommended critical requirements to consider when purchasing an NSPM solution to manage firewall policies:

Policy Change Automation: An NSPM should be able to fully automate the deployment of policy change with automation tools, along with the option to execute changes manually as well.

Real-Time Compliance Violation Monitoring and Detection: A solution should be constantly monitoring the entire environment for violations created by planned or unplanned rule changes and alert teams in real-time.

Rule Lifecycle Management: Essential to maintaining compliance with various frameworks including PCI DSS, are periodic rule reviews that should be automated with dedicated workflows built into the NSPM platform.

Compliance Reviews of Proposed Changes Prior to Deployment: An NSPM solution should be able to scan any proposed rule or policy change for compliance violations to ensure no new violations are accidentally injected into the environment.

Compatibility: NSPM solutions should be compatible with an organization's network infrastructure, support managing devices/vendors from a single pane of glass and streamline network security policies without disrupting existing network operations.

Scalability: An NSPM solution should scale with the organization's growing network infrastructure and support multi-tenancy to manage multiple networks from a single platform.

Integration with Third-Party Solutions: An API-first approach that can integrate with third-party solutions, such as vulnerability scanners, SIEM, SOAR, threat intelligence platforms, ITSM integrations, and incident response systems, to quickly detect and respond to potential security threats.

Ease of Use: Ensure the solution offers a user-friendly interface with a centralized dashboard for managing network security policies and real-time data access, contextual help, and support to troubleshoot issues and perform tasks.

Support and Maintenance: A proven and time-tested NSPM solution that provides world-class reliable support and maintenance services, including regular updates, patches, and bug fixes, as well as training, certification programs, and ongoing education keeps users in the organization up to date with the latest features and capabilities.

Ease of Business/Customer Experience: Ensuring that your NSPM vendor is easy to work with and professional essential, as it ensures timely support, effective issue resolution, and ongoing assistance, which are crucial for maintaining network security and minimizing disruptions to business operations.

Expectations in Deploying an NSPM Solution

As we know, all deployments are unique, and the process varies between vendors. In this section, we will share how FireMon's Professional Services team can help guide customers through the implementation process efficiently and with a focus on delivering outcomes and optimizing time to value.

Initiation: FireMon will provide a technical consulting session to review, provide guidance, and assist in planning the installation in the deployment environment.

Environment Prep: FireMon will provide an Implementation Readiness Checklist in advance of this phase. For distributed architectures, the deployment environment will need to be provisioned in accordance with FireMon's requirements.

Install Software: FireMon will review the self-installation to verify core functionality of the software such as retrieving, normalizing, and receiving usage data, verifying change detection and authentication configurations, defining user group permissions, validating SMTP, and importing zones and network segments.

Demo and Deploy: FireMon offers an additional session to review the configuration and demonstrate prioritized use cases to ensure desired outcomes are achieved, along with technical consulting sessions for configuring and operating the software as needed.

Closeout: FireMon offers a health and architecture review and a FireMon Runbook, which provides a snapshot of the current deployment's health/configuration and outlines tasks and troubleshoots to ensure FireMon and device health.

Operational Transition: Once fully up and running, our team will ensure a smooth transition to FireMon's customer support team.

NSPM Implementation Milestones: Ensuring a Smooth Transition for Enterprises

Network Security Policy Management (NSPM) solutions have become indispensable in today's fast-paced digital landscape. As enterprises invest in NSPM solutions to bolster their security infrastructure, a well-structured implementation plan is crucial for a seamless transition. This section outlines essential NSPM implementation milestones to guide enterprises in preparing for this critical phase.

1. Pre-Implementation Assessment

Before diving into NSPM implementation, conduct a comprehensive pre-implementation assessment. This phase should include:

- Network Audit: Analyze your existing network infrastructure, policies, and configurations. Identify gaps, redundancies, and areas for improvement.
- Stakeholder Engagement: Involve key stakeholders, including IT teams, network administrators, and security personnel, to gather insights and requirements.
- Risk Assessment: Evaluate potential risks and vulnerabilities that the NSPM solution aims to mitigate.

2. Solution Selection and Customization

Selecting the right NSPM solution is paramount. Consider the following factors:

- Vendor Evaluation: Choose a reputable vendor with a track record of successful NSPM implementations.
- Customization: Tailor the NSPM solution to align with your specific network and security requirements.
- Integration: Ensure seamless integration with existing network and security tools.

3. Policy Definition and Optimization

Define and optimize network security policies to enhance security and streamline operations:

- Policy Review: Evaluate and update existing policies to align with business objectives and regulatory compliance.
- Policy Automation: Implement automated policy enforcement to minimize human errors and enhance efficiency.
- Policy Documentation: Create comprehensive documentation for all policies and procedures to aid in auditing and troubleshooting.

4. Training and Skill Development

Invest in training and skill development for your IT and security teams:

- Training Programs: Enroll team members in training programs offered by the NSPM vendor to gain expertise.
- Cross-Training: Encourage cross-training to ensure knowledge transfer and skill redundancy within the team.
- Certifications: Consider certifications like CISSP, CCSP, or vendor-specific certifications for your team members.

5. Testing and Validation

Before deploying the NSPM solution in a live environment, thorough testing and validation are essential:

- Functional Testing: Ensure that all NSPM features and policies are functioning as intended.
- Security Testing: Conduct penetration testing and vulnerability assessments to identify and address any weaknesses.
- User Acceptance Testing (UAT): Allow end-users to test the system to ensure it meets their requirements.

6. Pilot Deployment

Implement the NSPM solution in a controlled pilot environment to gather valuable information and address any issues:

- Select a Subset: Start with a subset of your network or user base to minimize potential disruptions.
- Gather Feedback: Encourage pilot users to provide feedback on usability and performance.
- Refinement: Refine the implementation based on feedback and lessons learned during the pilot phase.

NSPM Implementation Milestones: Ensuring a Smooth Transition for Enterprises

7. Full Deployment

Once the pilot is successful, proceed to full deployment:

- Phased Approach: Deploy the NSPM solution in phases to manage any unforeseen issues.
- Monitoring and Support: Continuously monitor the implementation and provide support to users and administrators.
- Assess Value: Once devices are imported, shift focus to assess the immediate value of the NSPM solution for your use cases in your production environment.

8. Post-Implementation Evaluation

After the full deployment, conduct a post-implementation evaluation:

- Performance Analysis: Assess how the NSPM solution has impacted network security, efficiency, and compliance.
- Customer Success: Partner with the NPSM vendor's Customer Success team to leverage best practices for adoption and usage of the NSPM solution.
- Feedback Gathering: Continue to gather feedback from users and administrators for ongoing improvements.
- Documentation Updates: Update documentation based on lessons learned during the implementation.

Implementing a Network Security Policy Management solution is a critical step in fortifying an enterprise's cybersecurity posture. By following these NSPM implementation milestones, enterprises can significantly reduce the challenges and risks associated with the transition. A well-planned and executed NSPM implementation ensures that network security policies are efficiently managed, leading to improved security, compliance, and operational efficiency.

Buying Journey Obstacles & Risks When Implementing an NSPM

Implementing a network security policy management solution is a critical step for enterprises in safeguarding their digital assets, managing firewall policies, and ensuring regulatory compliance. However, the journey to acquire and deploy such a solution is fraught with obstacles and risks that demand careful consideration.

Complex Vendor Landscape: The market is flooded with options, each claiming to be the best, making the selection process overwhelming. The risk here is that selecting the wrong solution can result in wasted resources and missed opportunities to enhance security.

Ensuring Compatibility: Enterprises must carefully assess how the new solution will integrate with their current network environment. Failing to do so can lead to disruptions, costly modifications, and reduced overall efficiency.

Identifying Comprehensive Needs: It is vital to identify the comprehensive security needs of the organization. Sometimes, enterprises tend to focus on immediate issues without considering long-term requirements. Inadequate planning in this regard can lead to gaps in security coverage.

Budget Constraints: Budget limitations can be a significant obstacle in the buying journey. Enterprises must find a solution that fits their financial parameters without compromising on security. There's a risk of either overspending or settling for an inadequate solution if budget constraints are not carefully managed.

User Training and Adoption: Implementing a network security policy management solution involves training users and ensuring they effectively adopt the new system. Resistance to change can slow down the implementation process, affecting overall security posture.

Scalability: Enterprises need to consider the scalability of the chosen solution. As the organization grows or experiences changes, the solution should be flexible enough to adapt without the need for a complete overhaul. The risk lies in selecting a solution that can't grow alongside the enterprise's requirements.

Vendor Reputation and Support: Choosing a reputable vendor is crucial. The risk of opting for an unknown or unreliable vendor includes inadequate customer support, potential security vulnerabilities, and the possibility of the vendor going out of business, leaving the enterprise without updates or support.

Project Management: Effective project management is vital for a smooth implementation. Failing to allocate the right resources, set clear objectives, and manage the project efficiently can lead to delays, increased costs, and a suboptimal solution.

Navigating these challenges requires careful planning, comprehensive assessment, and a commitment to finding the right solution for the organization's unique needs. Enterprises that successfully address these obstacles and manage these risks will be well-positioned to fortify their network security and protect their digital assets now, and in the future.

EVALUATING MARKET OFFERINGS

Key Features and Functionality to Consider when Purchasing an NSPM Solution

FEATURES AND FUNCTIONALITY	VENDORS	IMPORTANCE	SCORE
Intelligent Rule Recommendations			
Rule Creation Workflows			
Real-time Change Monitoring Across the Environment			
Complete Network Visibility			
Rule Lifecycle Management			
Compliance Reviews of Proposed Changes Prior to Deployment			
Performance Optimization			
Scalability			
Centralized Management			
Integration with Third-Party Solutions			
Reporting and Analytics			
Support and Training			
Compatibility			
Ease of Use			
Support and Maintenance			

Unlocking Network Excellence: Key Questions to Ask an NSPM Vendor

At FireMon, we understand the importance of selecting the right Network and Security Performance Management (NSPM) solution for your enterprise. As you embark on this transformative journey, it is crucial to ask the right questions to ensure that the chosen vendor aligns with your unique requirements and delivers optimal results. Here are the key questions to ask an NSPM vendor when considering purchasing their solution:

1. **What is Your Solution's Core Functionality?** Start by understanding the core functionality of the NSPM solution. Ask the vendor about the specific features and capabilities it offers. Does it provide real-time network monitoring, performance analytics, and security insights? Can it detect anomalies, optimize network traffic, and identify potential bottlenecks? A comprehensive NSPM solution should encompass a range of functionalities that address your organization's specific needs.
2. **How Will Your Solution Integrate with Existing Infrastructure?** Compatibility with your existing network infrastructure is crucial to avoid disruptions and ensure a seamless integration process. Inquire about the vendor's expertise in integrating their NSPM solution with various hardware, software, and network technologies. Discuss any potential challenges or limitations that may arise during the integration process and seek clarification on how the vendor plans to overcome them. Compatibility with your existing network infrastructure is crucial to avoid disruptions and ensure a predictable integration process.
3. **How Does Your Solution Address Network Security?** Network security is paramount in today's cyber landscape. Engage the vendor in a discussion about how their NSPM solution addresses network security concerns. Does it offer robust threat detection and response capabilities? Can it monitor and analyze network traffic for potential security breaches? A comprehensive NSPM solution should empower your organization to proactively safeguard its digital assets.
4. **How Does Your Solution Provide Insights and Analytics?** Data-driven insights are vital for optimizing network performance and making informed decisions. Inquire about the analytics capabilities of the NSPM solution. Does it provide real-time dashboards, customizable reports, and predictive analytics? Can it identify patterns, trends, and anomalies that impact network performance? The ability to leverage actionable insights is essential to unlock the full potential of your network infrastructure.
5. **What Level of Customization and Scalability Does Your Solution Offer?** Every enterprise has unique requirements and growth aspirations. Ensure that the NSPM solution can be customized to meet your specific needs. Inquire about the vendor's scalability capabilities. Can their solution adapt to the evolving network demands of your organization as it grows? A flexible and scalable NSPM solution will future proof your network infrastructure investment.
6. **How Does Your Solution Support Compliance and Regulatory Requirements?** In industries governed by strict regulations, ensuring compliance is non-negotiable. Discuss with the vendor how their NSPM solution supports compliance and regulatory requirements. Does it offer functionalities to assist in meeting industry-specific standards? Can it generate audit trails and reports for regulatory purposes? A compliant NSPM solution will help you navigate complex regulatory landscapes with ease.
7. **What is Your Approach to Customer Support and Training?** Customer support and training are vital components of a successful NSPM implementation. Ask the vendor about their customer support offerings. Do they provide ongoing technical assistance, software updates, and maintenance services? Inquire about their training programs to ensure that your team receives the necessary knowledge and skills to maximize the value of the NSPM solution.
8. **Can You Provide Case Studies or Testimonials from Satisfied Customers?** To gauge the effectiveness of the NSPM solution, ask the vendor for case studies or testimonials from satisfied customers. Real-life examples and success stories will provide valuable insights into how the solution has benefited other organizations. Look for evidence of improved network performance, enhanced security, and increased operational efficiency.

FireMon's NSPM Solution for Change Automation

FireMon's Policy Manager is an NSPM platform that automates firewall and cloud security policy management to minimize policy-related risk, facilitate quick and accurate rule changes, and ensure compliance with internal and external regulations. By providing real-time visibility and control, Policy Manager enables organizations to save time and resources while eliminating the risks caused by misconfigurations.

Real-Time Change Monitoring: Real-time change monitoring is crucial to stay ahead of problems before they start. FireMon monitors policy changes across the entire environment, on any device; on premises or in the cloud. If a policy changes, you'll know about it – and our custom alerts mean you'll find out about it in the way you want.

Efficient Change Workflows: FireMon workflows take the complicated, messy, and time-consuming processes of new rule creation and changes to existing policies then streamlines them. FireMon evaluates each request for its impact across the environment. It identifies all firewalls and other devices in its path to create a recommendation for how the rule should be created, what objects can be reused, and how to enforce it. All of this is performed through a workflow process that dramatically reduces the time It takes to deploy and do it accurately.

Policy Change Automation: FireMon can fully automate the deployment with our automation tools. Once a rule is ready to go, the changes can be made manually or the FireMon platform can deploy them automatically to the affected devices immediately or schedule them during approved change windows. Once sent, the changes can be fully implemented in minutes.

FireMon NSPM is Built for Change Automation

FireMon improves operational efficiency and reduces costs to achieve business SLAs while improving security and availability. Without FireMon's automation capabilities, enterprises face unmanageable, complex environments where rule creation/change is a time consuming, error prone process which in turn introduces costly outages, increased security risk, and loss of productivity. However, once implemented, enterprises can expect the following with FireMon:

Enhanced Capabilities for Effective Security Policy Management: Built-in reports use a wide range of controls to identify and remediate policies, while over 500 included controls can be customized using SiQL query language. Customize controls and assessments to specific needs while utilizing minimal professional services with highly customizable workflows that can be tailored to meet the needs of any organization.

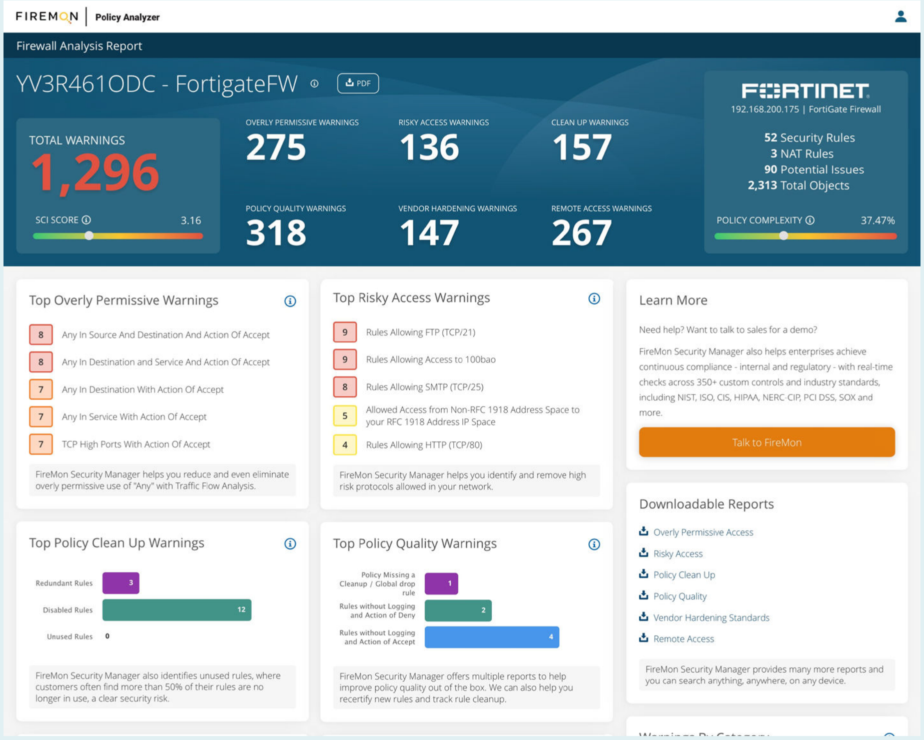
Integration: FireMon's API-first approach makes integrations easy into SIEM, SOAR, vulnerability scanners, and ITSM tools. Optimized rule creation workflows seamlessly integrate into broader ITSM tools and can make calls to any FireMon platform function using API.

Real-time network security policy management at scale: Architected for real-time reporting, change detection, and search in any size environment, FireMon's time-proven scalability is verified to support 15K devices and 25M rules. Meanwhile, up-to-date network understanding means accurate policy creation and recommendations.

Try FireMon with Policy Analyzer

Committing to any security solution can be time and resource intensive. This is why FireMon has created Policy Analyzer, our complimentary firewall security posture assessment solution that provides best practices and rule suggestions to reduce policy-related risks. Policy Analyzer is a perfect way to test out FireMon without any cost or commitment.

- **Assessment Results:** Available in minutes with no installation, setup, or dedicated hardware.
- **Key Results:** includes overly permissive, risky access, vendor hardening, and policy quality warnings.
- **Change Validation:** See if policy changes improve diagnostic scores.
- **Downloadable Reports:** Dive deeper into the results and share with others.
- **Top Remediation Recommendations:** Discover insights based on FireMon's 20+ years of experience.



FIREMON | Policy Analyzer

Firewall Analysis Report

YV3R461ODC - FortigateFW ⓘ PDF

TOTAL WARNINGS 1,296

SCI SCORE ⓘ 3.16

OVERLY PERMISSIVE WARNINGS 275

RISKY ACCESS WARNINGS 136

CLEAN UP WARNINGS 157

POLICY QUALITY WARNINGS 318

VENDOR HARDENING WARNINGS 147

REMOTE ACCESS WARNINGS 267

FORTINET

192.168.200.175 | FortiGate Firewall

52 Security Rules
3 NAT Rules
90 Potential Issues
2,313 Total Objects

POLICY COMPLEXITY ⓘ 37.47%

Top Overly Permissive Warnings ⓘ

8	Any In Source And Destination And Action Of Accept
8	Any In Destination and Service And Action Of Accept
7	Any In Destination With Action Of Accept
7	Any In Service With Action Of Accept
7	TCP High Ports With Action Of Accept

FireMon Security Manager helps you reduce and even eliminate overly permissive use of "Any" with Traffic Flow Analysis.

Top Risky Access Warnings ⓘ

9	Rules Allowing FTP (TCP/21)
9	Rules Allowing Access to 100bao
8	Rules Allowing SMTP (TCP/25)
5	Allowed Access from Non-RFC 1918 Address Space to your RFC 1918 Address IP Space
4	Rules Allowing HTTP (TCP/80)

FireMon Security Manager helps you identify and remove high risk protocols allowed in your network.

Learn More

Need help? Want to talk to sales for a demo?

FireMon Security Manager also helps enterprises achieve continuous compliance - internal and regulatory - with real-time checks across 350+ custom controls and industry standards, including NIST, ISO, CIS, HIPAA, NERC-CIP, PCI DSS, SOX and more.

Talk to FireMon

Top Policy Clean Up Warnings ⓘ

Redundant Rules	3
Disabled Rules	12
Unused Rules	0

FireMon Security Manager also identifies unused rules, where customers often find more than 50% of their rules are no longer in use, a clear security risk.

Top Policy Quality Warnings ⓘ

Policy Missing a Cleanup / Global drop rule	1
Rules without Logging and Action of Deny	2
Rules without Logging and Action of Accept	4

FireMon Security Manager offers multiple reports to help improve policy quality out of the box. We can also help you recertify new rules and track rule cleanup.

Downloadable Reports

- Overly Permissive Access
- Risky Access
- Policy Clean Up
- Policy Quality
- Vendor Hardening Standards
- Remote Access

FireMon Security Manager provides many more reports and you can search anything, anywhere, on any device.

Warnings By Category

Click here to try Policy Analyzer

Summary

Automating network security policies is essential for enterprises to efficiently manage their policies, adapt swiftly to cyber threats, and minimize human error. By automating these processes, organizations can enhance operational efficiency, reduce costs, and improve overall network security.

Through the information provided in this e-Book, we hope we've provided the resources to help research, select, and implement an NSPM solution to improve operational efficiency and reduce costs.

FIREMON

To learn more, please visit
FireMon.com or contact us by email at sales@firemon.com

FIREMON