SOLUTION BRIEF

Mapping of NIST 800-53 to Essential Network Security

Nearly every organization faces significant IT security compliance demands regardless of agency. Their intent is ensuring mandated controls are always in place and that they are performing assessments with prescribed regularity. And deciphering governmental regulations like FISMA, NIST, DISA STIG, or FEDRAMP can be a daunting task for network teams. Federal agencies and private enterprises alike are adopting frameworks like NIST 800-53 to enhance their security best practices.

Essential network controls are often steeped in process and interpretation, making them difficult to budget and implement. Isolating these controls enables IT and Security to have common ground to ensure their network policy meets compliance standards.

This mapping shows how FireMon's solutions deliver your essential network controls and how they map to your NIST requirements.

Essential Network Security Controls	NIST 800-53 rev4 Requirements
Inventory of Authorized and Unauthorized Devices Knowing what you have in your environment is a cornerstone of your network security strategy, and ultimately, successful compliance with NIST. FireMon helps you find more by: – Eliminating 100% of your blind spots and monitor changes and modifications to the environment – Discovering, mapping, and alerting on topology changes across the entire hybrid enterprise, including multi-cloud environments	CA-7 - Continuous Monitoring CM-8 - Information System Component Inventory IA-3 - Device Identification and Authentication SA-4 - Acquisition Process SC-17 - Public Key Infrastructure Certificates SI-4 - Information System Monitoring PM-5 - Information System Inventory
Continuous Vulnerability Assessment and Remediation The best way to combat unwarranted access is to preemptively identify areas of vulnerability. FireMon helps manage risk by: – Scoring attack simulations and policy updates for risk and impact and then re-scoring once you've made improvements – Integrating with your vulnerability management solutions (i.e., Qualys, Rapid7, and Tenable) to measure risk and identify potential attacks – Detecting in real-time to uncover vulnerable systems, scope proposed changes before implementation, and to streamline the approval process	CA-2 - Security Assessments CA-7 - Continuous Monitoring RA-5 - Vulnerability Scanning SC-34 - Non-Modifiable Executable Programs SI-4 - Information System Monitoring SI-7 - Software, Firmware, and Information Integrity
Maintenance, Monitoring, and Analysis of Audit Logs Continuous compliance requires the monitoring and analysis of logs and updates to network devices. FireMon helps you monitor by: – Providing out-of-the-box and customizable assessments to help you ensure compliance with NIST standards – Automatically identifying rules that require immediate analysis based on real-world events – Documenting rule recertification and justification to aid in compliance audits	AC-23 - Data Mining Protection AU-2 - Audit Events AU-3 - Content of Audit Records AU-4 - Audit Storage Capacity AU-5 - Response to Audit Processing Failures AU-6 - Audit Review, Analysis, and Reporting AU-7 - Audit Reduction and Report Generation AU-8 - Time Stamps AU-9c - Protection of Audit Information AU-10 - Non-repudiation AU-11 - Audit Record Retention AU-12 - Audit Generation AU-13 - Monitoring for Information Disclosure AU-14 - Session Audit CA-7 - Continuous Monitoring IA-10 - Adaptive Identification and Authentication SI-4 - Information System Monitoring

Essential Network Security Controls	NIST 800-53 rev4 Requirements
Secure Configurations for Network Devices Secure configuration for network devices starts with firewall policy and the specific management tools deployed. **FireMon helps you with security assessments and hygiene by:** – Eliminating duplicate or shadowed rules that adversely impact device performance – Performing real-time analysis and providing an extensive history for rule and object usage in a policy to help you easily identify unused rules – Showing unique traffic patterns that exist in a rule and report on what data is flowing across a broadly defined address range – Applying event-driven review and verification to help you keep and recertify the rules that are still needed and those that need to be decommissioned	AC-4 - Information Flow Enforcement CA-3 - System Interconnections CA-7 - Continuous Monitoring CA-9 - Internal System Connections CM-2 - Baseline Configuration CM-3 - Configuration Change Control CM-5 - Access Restrictions for Change CM-6 - Configuration Settings CM-8 - Information System Component Inventory MA-4 - Nonlocal Maintenance SC-24 - Fail in Known State SI-4 - Information System Monitoring
Boundary Defense Network security used to be about maintaining healthy boundaries at the perimeter, but mobile computing, cloud platforms, and digital transformation mean these boundaries are more porous and less defined. **FireMon helps you by:** – Connecting to all on-premises network devices and private public cloud instances to capture security policies, normalize data, and to display through a single pane of glass – Providing insight into any requests that duplicate access or any rules that allow similar access to a new request – Performing a pre-change impact analysis that simulates a potential rule change and analyzes its impact on compliance and security – Integrating with your existing ticketing systems to automate policy approval	AC-4 - Information Flow Enforcement AC-17 - Remote Access AC-20 - Use of External Information Systems CA-3 - System Interconnections CA-7 - Continuous Monitoring CA-9 - Internal System Connections CM-2 - Baseline Configuration SA-9 - External Information System Services SC-7 - Boundary Protection SC-8 - Transmission Confidentiality and Integrity SI-4 - Information System Monitoring
Incident Response and Management Preempt breaches through continuous adaptive enforcement. Complete policy lifecycle automation helps reduce the impact of breaches and proactively strengthens your security posture. **FireMon helps you proactively by:** – Eliminating 100% of your blind spots and monitor changes and modifications to the environment – Discovering, mapping, and alerting on topology changes across the entire hybrid enterprise, including multi-cloud environments – Automatically identifying rules that require immediate analysis based on real-world events, like a breach – Showing unique traffic patterns that exist in a rule and report on what data is flowing across a broadly defined address range	IR-1 - Incident Response Policy and Procedures IR-2 - Incident Response Training IR-3 - Incident Response Testing IR-4 - Incident Handling IR-5 - Incident Monitoring IR-6 - Incident Reporting IR-7 - Incident Response Assistance IR-8 - Incident Response Plan IR-10 - Integrated Information Security Analysis Team

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.

SB0080-EN-20200101-02