NERC | FIREMON

Mapping of NERC CIP to Essential Network Security Controls

Tasked with providing critical safeguards by the North American Electrical Reliability Corporation Critical Infrastructure Protection (NERC CIP), Utilities, Oil & Gas, and Power Companies face a daunting challenge. Network engineers may be required to develop and use various controls like network segmentation, Demilitarized Zone (DMZ), firewalls, and anomaly detection based IDS to secure their infrastructures.

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 NERC CIP requirements.

Essential Network Security Controls	NERC CIP v5 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 NERC CIP. **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	CIP-007-5 R2 - Security Patch Management CIP-010-5 R3 - Configuration Change Management and Vulnerability Assessments
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	CIP-007-5 R4 - Systems Security Management
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 NERC CIP standards • Automatically identifying rules that require immediate analysis based on real-world events • Documenting rule recertification and justification to aid in compliance audits	CIP-005-5 R1 - Electronic Security Perimeter(s) CIP-007-5 R2 - Security Patch Management

Essential Network Security Controls	NERC CIP v5 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	CIP-005-5 R1 - Electronic Security Perimeter CIP-005-5 R2 - Interactive Remote Management CIP-007-5 R4 - Security Event 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	CIP-008-5 R1 - Cyber Security Incident Response Plan Specifications CIP-008-5 R2 - Cyber Security Incident Response Plan Implementation and Testing CIP-008-5 R3 - Cyber Security Incident
Incident Response and Management Preempt breaches through continuous adaptive enforcement. Complete policy life-cycle 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	CIP-007-5 R2 - Security Patch Management CIP-010-5 R3 - Vulnerability Assessments

FireMon is the only agile network security policy platform for firewalls and cloud security groups.

FireMon is the fastest way to streamline network security policy management, which is one of the biggest impediments to IT and enterprise agility. Only FireMon offers Continuous Policy Automation, including the full range of capabilities to dynamically secure firewall and cloud security group policies – and increase enterprise agility. Since creating the first-ever network security policy management solution, FireMon has delivered command and control over complex network security infrastructures for more than 1,700 customers located in nearly 70 countries around the world. To learn more, request a demo today.