FireMon Policy Planner is a change workflow solution that automates the change process and gives firewall administrators the tools they need to evolve policy and protection over time. This web-based module collects user requirements, recommends rule changes, provides detailed risk assessment of requested changes, verifies that the correct change was made and supports full system audits and verification. Policy Planner works alongside existing business-process automation tools and enables communication throughout the change process.

FireMon Policy Planner augments network security change workflow with firewall-specific functions that:

• Define device-specific compliance policies and ensure that proposed changes will not violate those standards prior to implementation.

• Capture and validate firewall fields including source, destination, service and justification.

• Eliminate engineering for requirements already satisfied by firewall policy.

• Provide technical recommendations for all necessary firewall changes.

• Assess risk exposure for new access requests prior to implementation.

• Document rule changes in FireMon Security Manager.

FEATURES:

01 RAPID RISK ASSESSMENT Assess and communicate risk associated with new access requests while keeping pace with the change and complexity happening in the network.

• Detect when new access will uncover a vulnerable system.

• Scope proposed changes prior to implementation.

• Streamline approval for access that doesn’t affect the risk profile.

• Provide analytics and visibility necessary to prevent introduction of problematic settings

02 ADVANCED BUSINESS PROCESS INTEGRATION Integrate Policy Planner with existing process management solutions while adhering to Business Process Model and Notation (BPMN) best practices. Using the BPMN standard, multiple teams, including business and technical users, can utilize workflows, queue-specific templates and ticketing flows specific to their request. In addition to full-text search capabilities, Policy Planner writes ad-hoc queries based on any ticketing requirements-related fields. Users can monitor open tickets via dashboard widgets or manage the engineering force using a list of open items, assignees and time-in-queue.

03 RULE RECOMMENDATION FireMon Policy Planner Rule Recommendation analyzes the current behavior of rule sets and determines any necessary changes instantly. It also assists with common scenarios including: • No Change Necessary – Policy Planner will identify when a new requirement duplicates access that is already accounted for in the standard firewall policy before the engineer proceeds with implementation. • Similar Access Exists – Policy Planner will find rules that allow similar access to a new request to avoid creation of extraneous rules and complexity.

04 PROACTIVE COMPLIANCE CHECK Ensure that newly added rules or configuration changes meet existing compliance policies and best practices during the rule planning stage. Different checks for different device groups may be configured. For example, applying corporate audit checks to all devices and adding PCI audit checks only to devices in a PCI data environment. Audit results are displayed before the rule changes are approved, showing whether or not to implement policies as currently designed.

WHY POLICY PLANNER? Ensure that the right firewall changes are made at the right time using fewer resources. USE POLICY PLANNER TO: • Assess risk of requested access. • Proactively analyze proposed changes for policy compliance. • Reduce cost of documenting compliance. • Improve firewall administrator’s efficiency. • Enable business, technical and compliance change review. FEATURES: • Intelligent Rule Design - find out if access already exists or isn’t necessary • Proactive Compliance Checks - verify new rules or changes meet compliance requirements prior to implementation. • Full Customization - customize change request forms and controls to fit the needs of the organization. • Workflow Integration/Automation - each stage of the change request can be automated and integrated into third party management systems such as Remedy and ServiceNow.

**Why Not to Use Policy Planner?**

While Policy Planner offers a multitude of benefits, it's essential to consider potential limitations:

1. **Complexity vs. Simplicity:** For organizations with relatively simple and straightforward firewall policies, the level of automation offered by Policy Planner might be more robust than needed.
2. **Resource Allocation:** Implementing a new system requires time and resources. If your organization lacks the capacity to adopt and integrate Policy Planner effectively, it might not yield the desired results.
3. **Customization Needs:** If your organization's policies require frequent and unique customizations that deviate from industry standards, Policy Planner's automated recommendations might not align perfectly.

This is where the FireMon Policy Optimizer steps in, offering a comprehensive and innovative solution to streamline network security policy management, enhance efficiency, and fortify your organization's defenses.

**Why It's Needed:** Network security policies serve as the cornerstone of an organization's defense against cyber threats. However, as networks grow in complexity and scale, policy management becomes a time-consuming and error-prone process. Overly complex and redundant policies can lead to security gaps, compliance issues, and operational inefficiencies. The FireMon Policy Optimizer addresses these challenges head-on, empowering security teams to regain control over their policies, optimize their configurations, and bolster their overall security posture.

**Main Features:**

1. **Policy Analysis and Optimization:** The FireMon Policy Optimizer employs advanced algorithms to analyze and optimize existing network security policies. It identifies redundant rules, shadowed policies, and potential conflicts, allowing security teams to streamline and refine their policies for maximum efficiency.
2. **Risk Assessment and Compliance:** This solution provides real-time risk assessment by simulating policy changes before implementation. It helps organizations ensure compliance with industry regulations and internal security standards, minimizing the potential for policy violations and data breaches.
3. **Visual Policy Mapping:** With a user-friendly graphical interface, the FireMon Policy Optimizer offers a visual representation of your network security policies. This intuitive mapping enables quick identification of policy interdependencies, simplifying troubleshooting and reducing the risk of misconfigurations.
4. **Change Management:** Stay in control of policy changes with automated change management workflows. The FireMon Policy Optimizer helps organizations track, review, and approve policy modifications, ensuring a systematic approach to policy adjustments while minimizing disruptions.
5. **Real-time Monitoring and Reporting:** Gain insights into policy usage and effectiveness through real-time monitoring and customizable reporting. Identify underutilized or high-risk policies and take informed actions to optimize your network's security posture.
6. **Integration and Collaboration:** Seamlessly integrate the FireMon Policy Optimizer with existing security infrastructure, including firewalls, intrusion detection systems, and vulnerability management tools. Foster collaboration among security teams, enabling them to work cohesively to enhance policy management.

POLICY OPTIMIZER: Continuous compliance with automated rule review, recertification and decommissioning THE CHALLENGE: Stay compliant, document everything, do it automatically. Rules get outdated. That’s just what they do. As networks change and access requirements shift, security controls have knock-on effects on other rules, policies and access controls. Security teams must detect these network dynamics and recertify rules to ensure airtight compliance. The manual process of decommissioning and recertification leaves enterprises with a bag full of outdated, redundant, overly permissive and risky rules that lead to compliance failures and increased risk. FireMon’s Policy Optimizer puts an end to the suffering

THE SOLUTION: Continuous Compliance through Automated Review and Change Management FireMon’s Policy Optimizer keeps firewalls squeaky clean by automating your review process and instantly decommissioning access that could lead to a compliance failure. Policy Optimizer communicates to everyone involved with the rules, giving you a central hub for security teams, policy owners, application admins and business teams to validate rules, check for compliance and recertify. Orchestration kicks into gear to decommission or recertify rules with complete documentation for every last statement in the rule syntax.

WHY POLICY OPTIMIZER? Automate review for all firewall rules and instantly document, recertify, decommission and report every policy. • Validate access with business and application teams • Find overly permissive rules, pull back compliance drift • Continuous compliance: PCI DSS, HIPAA, ISO, NIST, SOX and others • Automate workflows and communication for all teams • Instantly document all access policies and rules

FEATURES: Single-console, global visibility across the enterprise Event-driven rule review Custom workflows tailored to your compliance and audit requirements

AUTOMATED POLICY REVIEW Assign review based on rule and policy properties and dictate removal of troublesome, outdated or undocumented rules. The integrated policy review platform eliminates inefficient, error-prone manual processes and ensures network operations’ ability to improve protection and compliance. EVENT-DRIVEN ENROLLMENT Automatically identify rules that demand immediate analysis as determined by real-world events such as time-frame expiration, critical security control failure, periodic review or ad-hoc query. TARGETED INTELLIGENCE FOR RULE IMPROVEMENT Get detailed information regarding each reviewed rule with the option to approve or reject current rule configurations. It also assists with: • Best Practices Adoption – Quickly confer with business stakeholders and remove rules that are expired, undocumented, hidden or unused, as well as those that have been modified from their original purpose. • Performance Improvement – Avoid the service interruptions that can happen due to unnecessary rules reducing the productive life of a firewall. MAINTAIN COMPLIANT STATUS Interact directly with compliance and audit staff to ensure that any modifications retain alignment with required controls and maintain a repository of change documentation for use during mandated assessments and audits. CUSTOMIZED WORKFLOW Easily change the built-in workflow to meet your custom needs. Because it is built on BPMN 2.0 task types, you can utilize a workflow specific to your environment. When integrated with the FireMon Policy Planner module, Policy Optimizer can be extended to create change tickets for removable rules and invoke application-level recommendations. This integration closes the loop on the rule lifecycle in that rules are effectively removed when they’re at the end of their useful life.

Cisco DNA Center (Cisco Digital Network Architecture Center) is a modern network management solution that offers several advantages over the older CiscoWorks LAN Management Solution (LMS). Here are 10 reasons why Cisco DNA Center is considered superior:

1. **Automation and Orchestration:** Cisco DNA Center provides advanced automation and orchestration capabilities, allowing for streamlined provisioning, configuration, and management of network devices. LMS lacks the same level of automation.
2. **Intent-Based Networking (IBN):** DNA Center employs intent-based networking principles, enabling administrators to define high-level business objectives and policies, which the system translates into specific network configurations. LMS lacks this intelligent and context-aware approach.
3. **Centralized Control:** DNA Center offers centralized control over network operations, making it easier to manage and monitor network-wide changes, configurations, and policies. LMS is more device-centric and lacks the same centralized control.
4. **Analytics and Insights:** DNA Center provides advanced analytics and insights through its Assurance module, offering proactive monitoring, anomaly detection, and troubleshooting recommendations. LMS lacks robust analytics capabilities.
5. **Security Integration:** DNA Center integrates security features, including threat detection and mitigation, within the network management framework. This integration is more comprehensive than what LMS offers.
6. **User-Friendly Interface:** DNA Center boasts a modern and user-friendly interface that simplifies network management tasks, making it easier for administrators to navigate and perform tasks compared to LMS's sometimes clunky interface.
7. **Scalability:** DNA Center is designed to scale for larger and more complex networks, accommodating the growing demands of modern IT infrastructures. LMS might struggle to handle the same scale efficiently.
8. **APIs and Integrations:** DNA Center offers rich APIs that facilitate integration with third-party applications and tools, allowing for greater customization and extending its capabilities beyond traditional network management. LMS has limited API support.
9. **Software-Defined Networking (SDN) Integration:** DNA Center is closely tied to Cisco's SDN solutions, such as Cisco Application Centric Infrastructure (ACI) and Software-Defined Access (SD-Access), enabling more dynamic and agile network architectures. LMS lacks such deep SDN integration.
10. **Future-Proofing:** DNA Center is aligned with Cisco's vision of the future of networking, focusing on technologies like SDN, automation, and analytics. Investing in DNA Center ensures staying current with industry trends, while LMS might become increasingly outdated.

Cisco DNA Center is a more modern and comprehensive network management platform that emphasizes automation, intent-based networking, advanced analytics, and security integration. It's well-suited for organizations looking to embrace cutting-edge networking practices and manage complex, dynamic networks. On the other hand, Cisco LMS is more suitable for organizations with simpler network management needs who may prefer a more traditional approach to network management.