FIREMON
POLICY PLANNER

FIREMON

Improving Firewall Operations by Automating Change

The increasingly complex device configurations interwoven from today's firewall policies are challenging to implement at any point in time. Factor in the reality of ever-changing demands on network access and security, and manual upkeep of these systems has become nearly impossible.

Even more important than the sheer amount of time it takes to analyze the potential impact on performance and protection, configuration changes themselves must be carried out correctly. Policy Planner for FireMon® Security Manager™ automates this entire process while documenting the purpose and ownership of all rules and decisions.

What is Policy Planner?

FireMon Policy Planner is a firewall-intelligent workflow solution that transforms security infrastructure management by automating the change process and giving firewall administrators the specific hands-on tools necessary to evolve policy and protection over time. This web-based system collects user requirements, recommends rule changes, provides detailed risk assessment of requested changes, and empowers full system audit and verification.

Task	Resolution	Date/Time	Notes
Verify Solution	Verify	Wednesday 11:44AM	
Implement Change	Complete	Wednesday 12:03AM	done with install.... Tested successfully
Approve Design	Approve	Tuesday 4:32PM	it's good to go
Design Solution	Complete	Tuesday 12:20PM	Hey, please do this tonight
Provide More Info	Complete	Tuesday 9:37AM	
Design Solution	Need More Info	Monday 4:15PM	These destinations and services do not seem accurate. Please update
Request Ticket	Submitted	Monday 3:03PM	

Quickly audit that changes followed appropriate validation and verification procedures

Policy Planner works alongside existing business-process automation tools and integrates everywhere necessary to ensure critical firewall enhancements. FireMon's approach drastically advances the change process regardless of whether organizations employ sophisticated enterprise business process software or home-grown change management tools, whether communication involves attaching spreadsheets to emails, even when they have no dedicated tools at all.

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 - BEFORE changes are made

▪ Capture 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

Policy Planner software integrates with existing business-process systems without affecting performance of those systems or requiring changes to user behavior by providing engineering tools that specify accurate and compliant rules that leverage existing workflow.

Why Policy Planner?

FireMon Policy Planner ensures that the right firewall changes are made with less time and effort.

Use Policy Planner to:

▪ Quickly assess the risk of requested access

▪ Proactively analyze proposed changes for policy compliance

▪ Reduce the cost of documenting compliance

▪ Improve the firewall administrator's efficiency

▪ Enable business, technical and compliance change review

Features:

▪ Provides firewall-specific functionality that augments the IT change workflow

▪ Integrates with existing business process systems without affecting performance

▪ Prevents risky access requests from being implemented, documenting approvals

Solution Overview

RAPID RISK ASSESSMENT

In today's enterprise, security operations are driven by the need to satisfy new connectivity requirements while maintaining protection. The pace of change and complexity in network configuration make it increasingly difficult to assess and communicate any added risk exposed by new access.

Policy Planner solves this challenge.

By fully understanding any proposed modifications to firewall alignment before implementation using its patented risk assessment engine, Policy Planner

provides all the security analytics and visibility necessary to prevent introduction of problematic settings.

Policy Planner can:

- Detect when new access will uncover a vulnerable system
- Streamline approval for access that doesn't affect the risk profile

Model effect of requested changes - BEFORE implementation
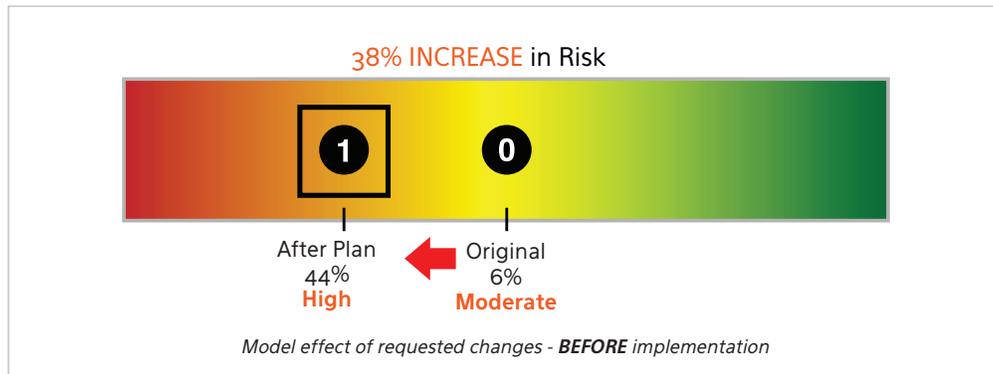
ADVANCED BUSINESS PROCESS INTEGRATION

Every organization has unique network security parameters and established management procedures. At the same time, further incorporation of industry standards builds operational consistency, streamlining critical processes to deliver crucial intelligence to numerous decision makers.

Policy Planner 3.0 combines automated analysis of network enforcement with support for the Object Management Group's (OMG) Business Process Model and Notation (BPMN) standard, leveraging FireMon's integrated work flow to facilitate integration with existing business process management solutions.

Via inclusion of BPMN (Version 2.0) best practices throughout analysis and rules recommendation, Policy Planner provides targeted results crucial to both business and technical users, addressing one of today's IT security workforce management challenges.

Multiple teams including audit staff can also create customized workflows using Policy Planner BPMN 2.0-compliant task templates – including forks for parallel approval paths, resulting decisions, status notifications, pre-set timers to escalate delayed tickets, and related user inputs. Workflow is delivered in industry-standard modeling notation with queue-specific templates and, customized ticketing flows, providing the ability to submit requests based on the nature of proposed changes, current enforcement, or user access level.

Spearheaded by technology leaders including Accenture, IBM, Oracle, SAP and Unisys, support for BPMN methodologies permit rapid deployment of Policy Planner alongside those companies' solutions, among many others.

In addition to full-text search capabilities, FireMon Policy Planner Version 3.0 is also tightly integrated with ties directly into FireMon's Insight platform, lending native ability to write ad-hoc queries based on any ticketing requirements-related fields. Use Policy Planner 3.0 to author queries and create dashboard widgets displaying the count of open tickets by status, or manage your engineering force using a list of open items, assignees, and time in the queue.

Integration with Existing Processes


Assess Potential Design Changes
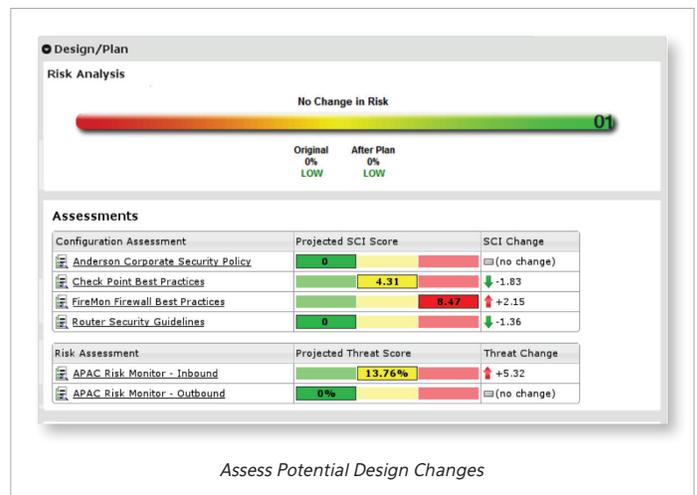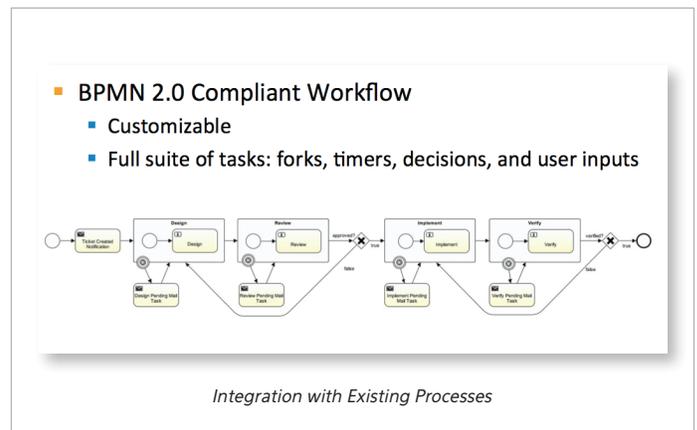
RULE RECOMMENDATION

FireMon Policy Planner 3.0 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** – A firewall's standard policy often allows for necessary business services but also mandates submitting any new requirements to the security team. When the involved access already exists, Security Manager shortens the change process by identifying that no change is required before the proposed engineering proceeds.

▪ **Similar Access Exists** – Creating new rules can be a knee-jerk reaction to any new request, but this often generates surplus rules that increase the policy's complexity. Rule Recommendation finds rules that allow access similar to the new request so additional modifications are limited.

Detailed Rule Recommendations
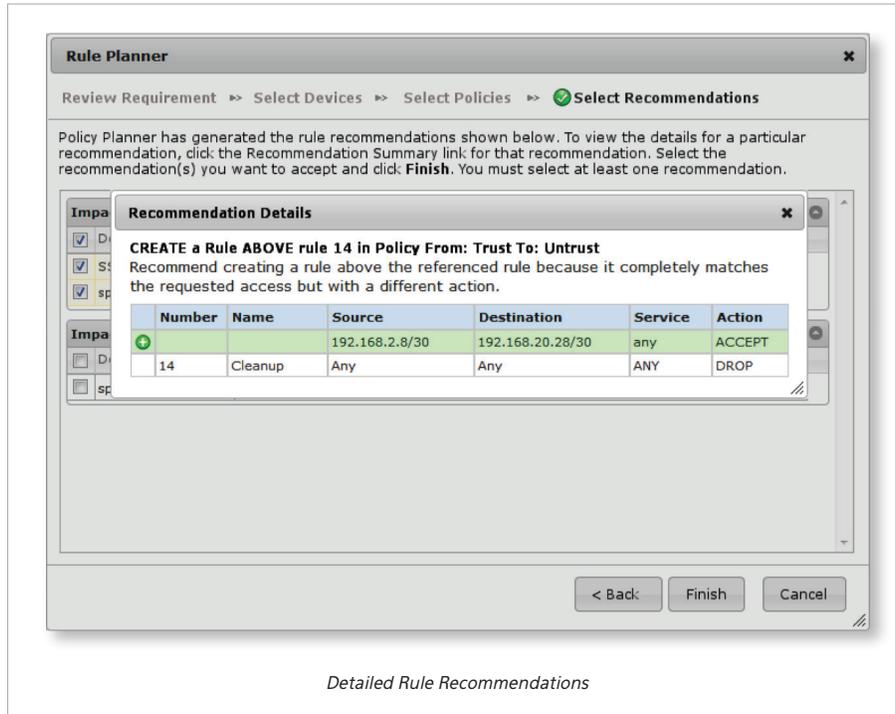
PROACTIVE COMPLIANCE CHECKING

Do newly added rules or configuration changes violate existing compliance policies and best practices? Having used Security Manager to clean up broad access, limit access to critical assets, and ensure that existing configurations meet corporate and regulatory guidelines, how do organizations ensure that new rules adhere to established standards?

With Policy Planner, choose those compliance checks that must be applied during the rule planning stage. Configure different checks for different device groups –applying, for example, corporate audit checks to all devices and adding PCI audit checks only to devices in a PCI compliant data environment. Audit results are displayed before the rule changes are approved, highlighting whether or not to implement policies as currently designed.

Policy Planner identifies and highlights proposed rules
which would violate existing compliance policies.
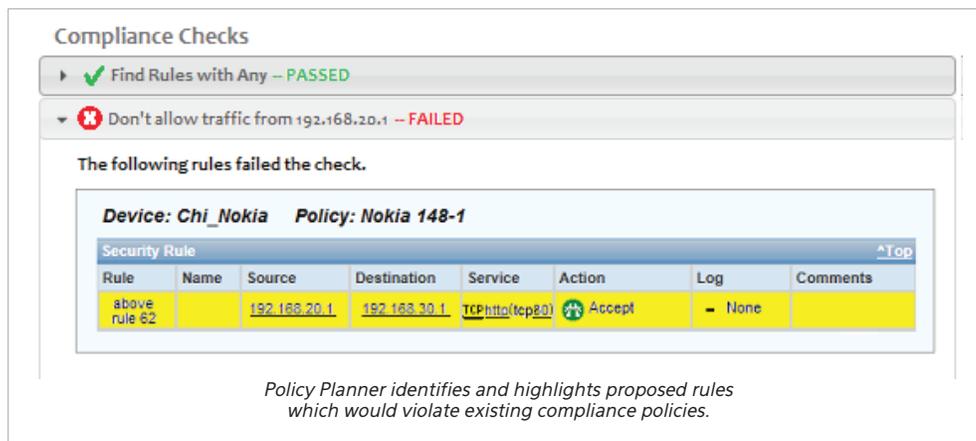
F I R E M O N

Ready to Try Policy Planner? http://www.firemon.com/demo

Follow us on Twitter @FireMon

Like us on Facebook: www.facebook.com/firemon

8400 W. 110th Street, Suite 400 · Overland Park, KS 66210 USA · Phone: 1.913.948.9570
E-mail: info@firemon.com · www.firemon.com