FIREMON

PROACTIVE SECURITY INTELLIGENCE

www.firemon.com

FORTINET INTEGRATION

Manage change, clean up legacy policies and archive ongoing compliance.

Changes affecting multi-purpose devices that unify separate security functions must absolutely be correct. Yet the simple act of running your business makes device configurations and firewall policies more complex, which makes it more likely that busy firewall administrators will make some incorrect changes.

FireMon Security Manager helps keep Fortinet firewalls running smoothly with its complete configuration management solution, including full support for the Fortigate line of network security platforms and appliances. FireMon monitors each appliance, capturing event and traffic logs in real time. All change events trigger a full configuration capture including detailed change history and a full audit trail of operations.

SECURITY MANAGER & FORTINET

PLAN CONFIGURATION CHANGES

With Security Manager's Policy Planner, you can make the correct changes more efficiently, based on real data, and model what the effect will be on your overall risk score *before* implementation.

CLEAN UP POLICIES

Use Security Manager's suite of cleanup tools to simplify overly complex policies and keep your firewall configurations clean despite the numerous changes that happen every day. Monitor configuration changes as they happen, communicate those changes to the right people at the right time and ensure that the rules are strictly enforced.

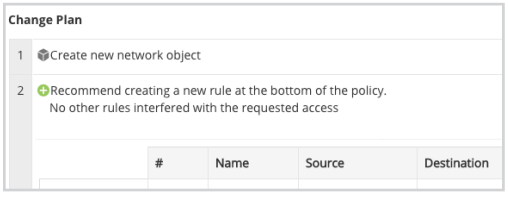
STAY IN COMPLIANCE

Because access requirements are central to most compliance program reviews, you must know and demonstrate what access is allowed and why. Security Manager tracks the business justification for a policy alongside its configuration elements for easy entry and reporting.

CHANGE MANAGEMENT

FIREWALL-SPECIFIC REQUESTS

Improve the efffectiveness of changes by getting better information from your users. Learn more about what access they need - and why they need it - with a firewall-specific change request form.



FireMon view of recommended modification to a normalized rule.

RULE RECOMMENDATION

Once the requirement is submitted, Rule Recommendation determines how the firewall is currently behaving and recommends appropriate changes to improve firewall security.

AUDIT LOG

Security Manager keeps a record of every change to the firewall, allowing you to track who made it, what was modified and when it occurred in an easy-to-use, line-by-line format.

ADVANCED FIREWALL MANAGEMENT

- Plan Configuration Changes
- Clean Up Policies
- Stay In Compliance

TRY FIREMON IN YOUR FORTINET ENVIRONMENT

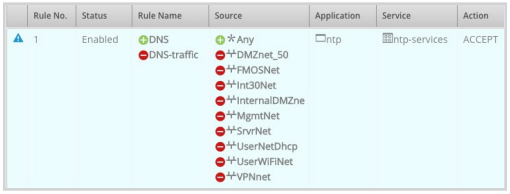
FIREMON.COM/TRIAL

CHANGE CONTROL TRACKING
Track the change control number alongside the technical implementation for the change. Once you start tracking the numbers, you will find changes that lack proper documentation quickly and easily.

CHANGE CONTROL REPORT
Search and report instantly on implementation details for any change control number. This report includes information on who implemented change, when it was implemented and on which firewalls.

GRAPHICAL CHANGE REPORT
Know immediately what changes have occurred and see what has changed with one glance.

IMMEDIATE CHANGE NOTIFICATION
Make changes at any time of the day or night. Security Manager monitors your firewalls 24x7 to capture all changes - planned or not, malicious or innocent - and alerts the right people via email or monitoring systems.



Changes to rules are normalized and displayed in the FireMon client.

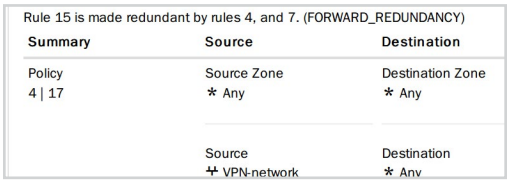
FIREWALL CLEANUP

DAILY ACTIVITY REPORT
Stay on top of the data Security Manager collects with the Daily Activity Report, which gets you started whether you need to know if the firewalls had a busy day or you need to troubleshoot why response seems slow.

HIDDEN RULES REPORT
Knowing when the policy contains conflicts is a great way to stay on top of rules that need to be cleaned up. Security Manager's Hidden Rules Report analyzes your rules and provides specific, concrete recommendations for cleaning them up.

RULE USAGE ANALYSIS
Proactively reduce risky or unnecessary access by monitoring which rules are being used and removing unused ones as needed.

OBJECT USAGE ANALYSIS
Even when a rule is used, Security Manager drills down and determines which objects in that rule are unused, so you can further celan up the rule and limit unnecessary access.



Normalized rules as shown in FireMon hidden rules report.

FIREWALL COMPLIANCE

TRAFFIC FLOW ANALYSIS
Auditors often find rules that are too broad for their purpose. Security Manager's Traffic Flow Analysis allows you to watch traffic on a single rule and shows you how to more narrowly define it. Use Traffic Flow Analysis to remove all unnecessary "Any" objects from your accept rules.

PCI ASSESSMENT
Security Manger's knowledge of the rule base can help you comply with PCI DSS Requirement 1. Because it knows the zones that affect PCI DSS requirements, it can find and report on any failures.

CUSTOM COMPLIANCE REPORTING
Security Manager supports extensions for the unique compliance requirements of each organization and industry.

FIREMON

8400 W. 110th Street, Suite 500
Overland Park, KS 66210 USA
P: 1.913.948.9570 E: info@firemon.com

Learn more about our solutions:
www.firemon.com

REV 071615