INTEGRATION BRIEF

FIREMON

FORTINET

Manage change, clean up legacy policies and achieve ongoing compliance on Fortinet devices

When changes affect multi-purpose devices that unify separate security functions into a single management point, they absolutely positively must be correct. Yet just running your business every day makes device configurations and firewall policies more complex and harder to understand. This complexity makes it more likely that busy firewall administrators will make some incorrect changes.

FireMon helps keep Fortinet firewalls running smoothly with a 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. Fortinet devices can be monitored directly or indirectly if another event collection system is in place.

With Security Manager, organizations can:

PLAN CONFIGURATION CHANGES

The best time to ensure that configuration changes are correct and won't have unintended consequences is before you implement them. 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.

CLEAN UP POLICIES

A simple firewall policy is best. Use Security Manager's suite of cleanup tools to simplify overly complex policies. Security Manager keeps your firewall configuration clean despite the numerous changes that happen every day. Its change detection and reporting functions monitor configuration changes as they happen and communicate those changes to the right people on the team at the right time. Use Security Manager to maximize firewall performance with features such as Usage Analysis to ensure that highly used rules are placed properly in the ruleset for maximum performance and Traffic Flow Analysis to ensure that rules are strictly defined.

STAY IN COMPLIANCE

As access requirements are central to the review of most compliance programs, you must know and be able to demonstrate what access is allowed and why that access is in place. Security Manager tracks the business justification for a policy alongside its configuration elements for easy entry and reporting.

Advanced Firewall Management

Change Management

Configuration Cleanup

Regulatory Compliance

FORTINET™
REAL TIME NETWORK PROTECTION

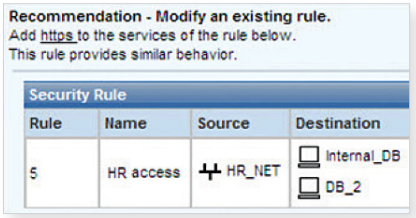
Change Management

FIREWALL-SPECIFIC REQUESTS

You can improve change effectiveness 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.

RULE RECOMMENDATION

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



FireMon view of recommended modification to normalized Fortinet rule

AUDIT LOG

Security Manager's data repository keeps a record of every change to the firewall, including who made it, what was modified, and when it occurred. Track who changed what with an easy-to-use interface that shows you what you need to see in a line-by-line format.

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 the change, when it was implemented, and on which firewalls.

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

GRAPHICAL CHANGE REPORT

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

IMMEDIATE CHANGE NOTIFICATION

Team members can make changes at any time of the day or night. Security Manager monitors your firewall continuously to capture all changes, planned or not, malicious or innocent, and alerts the right people. Notifications can be sent to team members in easy-to-read emails, or to monitoring systems via syslog.

Firewall Cleanup

DAILY ACTIVITY REPORT

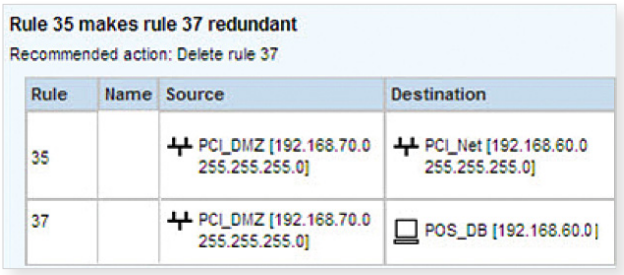
Security Manager collects a lot of data every day and you need to stay on top of it. The Daily Activity Report gets you started whether you need to know if the firewalls had a busy day or you're troubleshooting why response seems slow.

FIREWALL COMPLEXITY REPORT

With Security Manager, it's easy to identify which firewalls are the most complex and which need cleanup because their rule base has become overly complex. A single view across all firewalls quickly shows if access is defined too broadly and which specific rules are the primary causes. Firewall complexity affects not only performance but operational management as well. The less complex you can make the ruleset, the faster traffic will be evaluated by the system and the easier it will be for network engineers to manage access on a day-to-day basis.

HIDDEN RULES REPORT

Rule sets are large and complex. But knowing when the policy contains conflicts is a great way to stay on top of the 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 35 makes rule 37 redundant

Recommended action: Delete rule 37

Rule	Name	Source	Destination
35		PCI_DMZ [192.168.70.0 255.255.255.0]	PCI_Net [192.168.60.0 255.255.255.0]
37		PCI_DMZ [192.168.70.0 255.255.255.0]	POS_DB [192.168.60.0]

Normalized Fortinet rules as shown in FireMon hidden rules report

RULE USAGE ANALYSIS

Once access has been requested and granted, removing it can be difficult. You can tackle this problem pro-actively by monitoring which rules are being used and removing the unused ones when needed.

OBJECT USAGE ANALYSIS

Even when a rule is used, Security Manager's analysis engine drills down and determines which objects in that rule are unused. This empowers you to further clean up the rule and limit unnecessary access.

Firewall Compliance

TRAFFIC FLOW ANALYSIS

Auditors often find rules that are too broad for their purpose—and you must fix them after the fact. Security Manager's Traffic Flow Analysis keeps you on top of things by watching the traffic on a single rule and showing how you can more narrowly define it. Use Traffic Flow Analysis to remove all unnecessary "Any" objects from your accept rules.

PCI ASSESSMENT

Security Manager'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

Compliance is different for each organization and industry. Security Manager supports extensions for unique compliance requirements. FireMon encourages you to participate in our Nexus firewall management community and share your best practices for addressing compliance and other challenges.

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

rev 052013