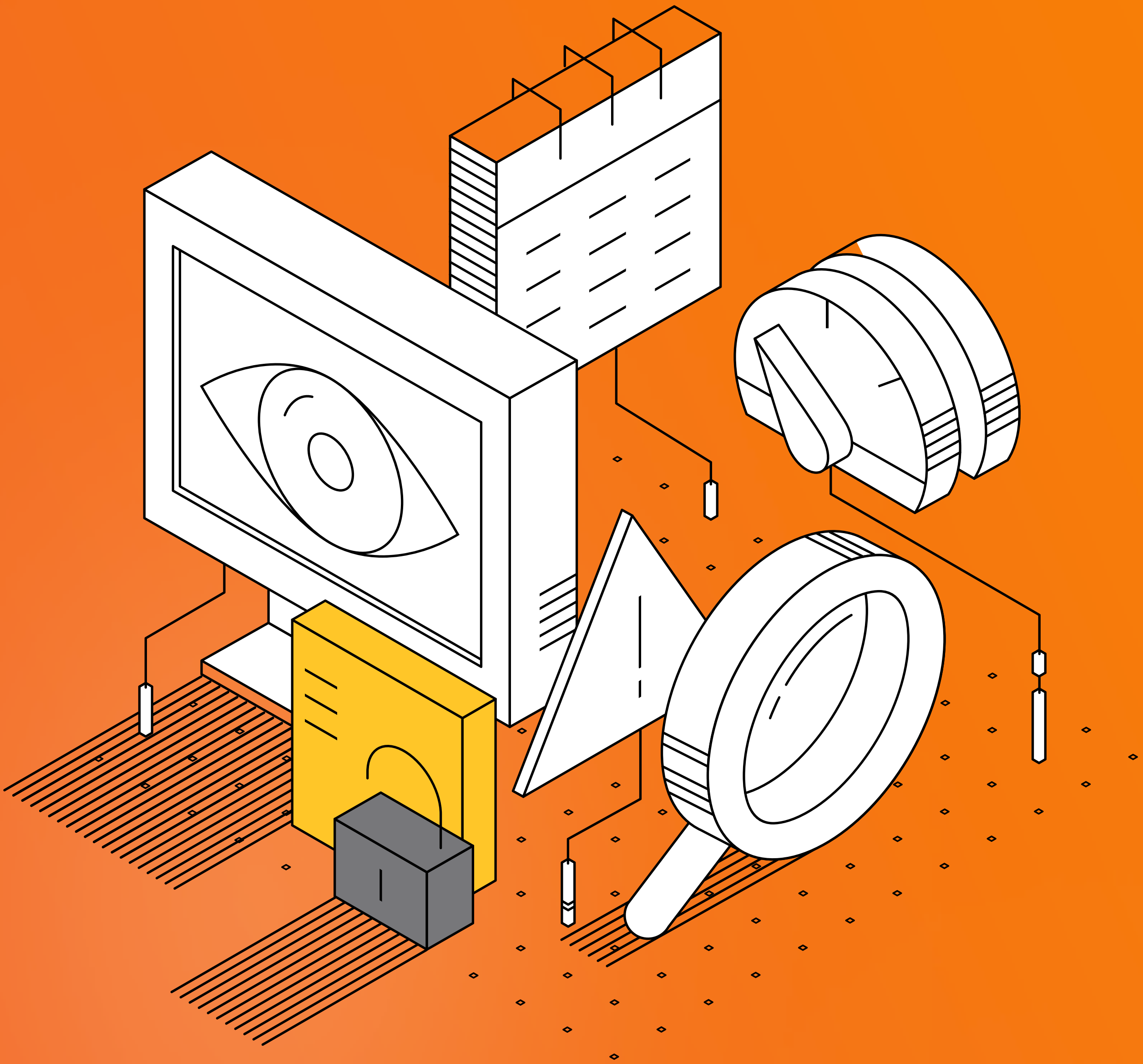
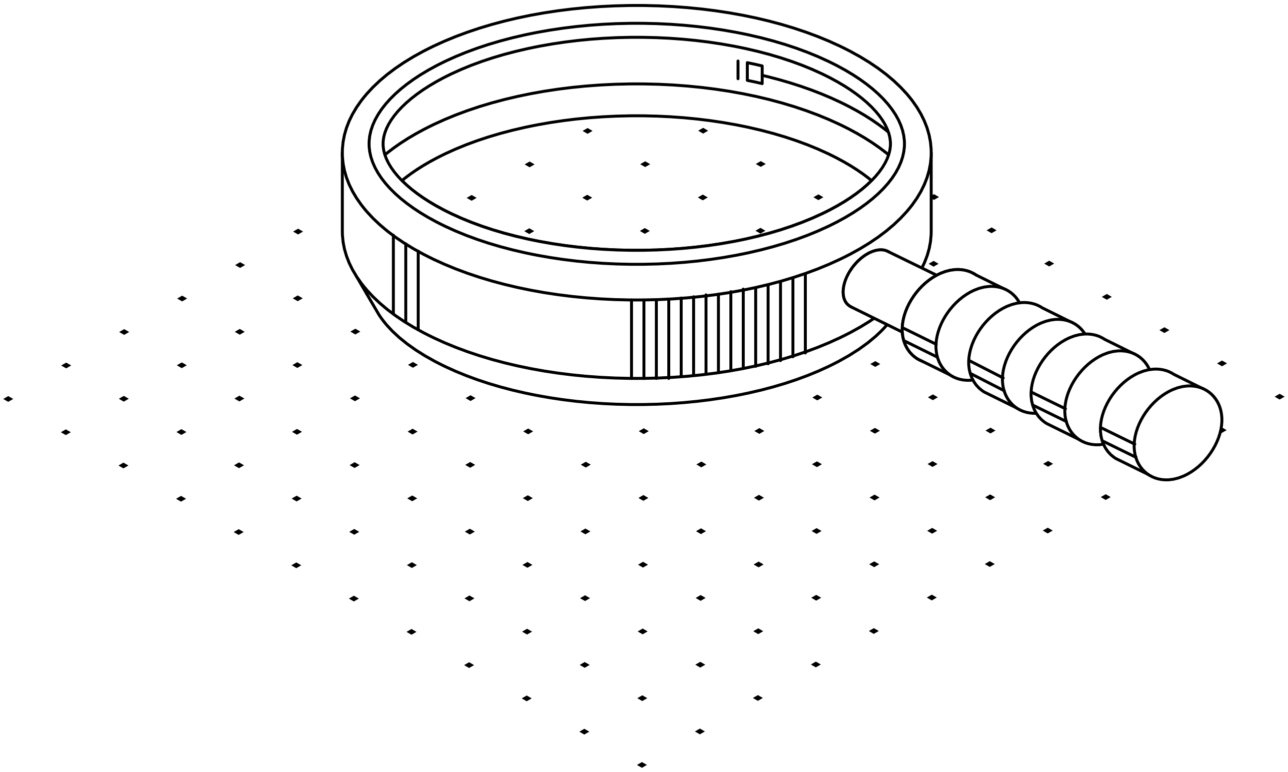


FIREMON

Firewall Cleanup Recommendations

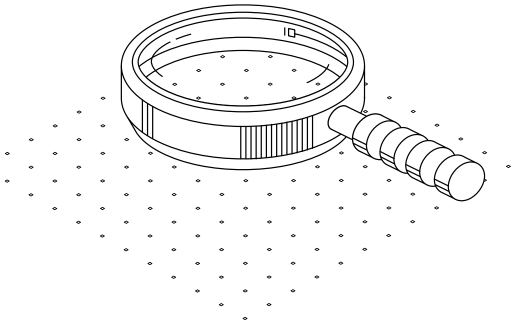
Considerations for Improved Firewall Efficiency, Reduced Complexity and Better Security

TABLE OF CONTENTS



01

Executive Summary



Firewalls are designed to provide access control. Although there is risk associated with any access, by limiting what access is permitted the risk is limited and understood and can be evaluated against business need to effectively justify the risk. However, poor firewall management defeats this purpose by ineffectively controlling access and limiting visibility into what access is actually permitted; poor management also increases the cost associated with security management.

The result of poor management is a firewall policy with unnecessary rules that result in excessive complexity, overly permissive access, unnecessary risk and performance degradation, all of which lead to higher costs that can be avoided. These problems can be addressed with both short-term and long-term activities to clean up the firewall now and prevent this situation from returning. This paper discusses the implications of firewall policy complexity, why it remains a problem today and how to resolve it.

02

Firewall Administration Challenges

Firewalls are designed and implemented to control access, whether that access is inbound or outbound, restricted as to source or destination, or a limitation on available services. At the core of the firewall is the policy, made up of rules, that enforces what access is permitted. Nearly all firewalls are designed with a "positive security model," meaning that unless a rule expressly permits access, that access is denied. This design should limit access only to what is necessary, but in practice, firewall management is very complicated, and significantly more access is permitted than is necessary. Traditional firewall administration typically results in mistakes, unnecessary complexity, excessive access and substantial risk.

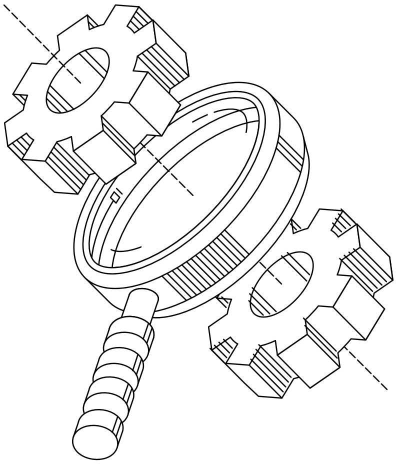
Managing firewalls configured with thousands of rules places a considerable burden on organizations to make sure that their firewall policies are implemented correctly. Large organizations have deployed hundreds of firewalls to control access, and the configurations of these devices are constantly changing. Firewall policies quickly become complex as the number of rules and objects grows from hundreds to thousands. In addition, organizations often have a mix of firewall vendors and different administrators for different business units within the organization. Too often organizations are faced with poor-quality policies and unused rules, resulting in misconfiguration of network and security systems, errors, downtime, poor device performance, reduced security and increased risk.

This is a severe problem that affects nearly every enterprise. A recent survey of hundreds of enterprises discovered that 73 percent of all respondents considered their firewall policies ranged from "somewhat complex" to "out of control." The impact of these issues is even worse. The firewalls that should provide confidence by exposing only an accepted amount of access and related risk have become so difficult to manage that most administrators accept that security gaps exist in the firewall policy due to complexity and lack of visibility.

03

Causes of Firewall Policy Mistakes

> The scope and severity of improperly configured firewalls necessitates action. To understand what must be done, it is first important to understand how the problem is created. There are two primary issues that necessitate policy cleanup: complexity and excessive access.



Policy Complexity

Complexity by itself is not a security issue. In large complex enterprises, the firewalls that control access will necessarily have complex firewall policies. However, excessive complexity has implications that are a problem. Not surprisingly, there is a strong correlation between the complexity of the firewall and the number of mistakes in the policy. As complexity increases, mistakes increase. Unfortunately, each mistake adds unnecessary complexity, resulting in even further mistakes. Over the years, these problems compound upon one another, resulting in an unmanageable policy, deteriorated firewall performance, increased risk and increased management costs.

The effort required to manage a firewall significantly increases as the complexity of a policy increases. The cost to correctly administer the firewall increases exponentially as well. Increased costs are associated with creating new rules due to the time it takes to identify where and how to meet the change requirement. Management costs are also associated with annual audits of these exceedingly complex policies.

Beyond the management costs, there are also system costs to complexity. The larger a security policy, the more taxing it is for the firewall to evaluate new access attempts against the policy. In one extreme example, average CPU usage of a firewall was reduced by 30 percent when the unused rules were removed from the policy.

Excessive Access

Excessive access, on the other hand, is a problem in its own right. By definition, excessive access violates the purpose of the firewall, which is to control access. However, it is extremely common and most often unintentional. There are three primary causes for this issue:

Ineffective Change Management

Unnecessary changes are made in several ways. Some are made without considering how best to implement them based on the current policy. Changes are made without considering the potential risk to the business. In worst-case scenarios, rogue changes are made that compromise all security.

Poor Definition of Business Requirements

Business is demanding. Changes are requested and must be implemented quickly. Often, these requests provide limited information about what is necessary to permit access. A simple request such as "permit access to this server from my network" does not provide sufficient information to limit access to only necessary access. What part of the network truly needs the access? What services are needed to permit necessary access? The result is often the creation of broad access rules. Well-intentioned security administrators will do their best to limit access, but without good information, it is very difficult. Often rules are created with "ANY" objects to enable the access in a timely fashion to meet the business demand.

But how do you determine whether a change is "low risk"? This definition varies by organization and sometimes even by sub-groups within an organization. IPA allows this definition to be easily configured according to the needs and regulatory constraints of the environment – e.g. check changes on PCI firewalls against PCI standards, check all changes (including those on the PCI devices) against the corporate standard. Systems should, wherever possible, determine the right mix of analysis required and apply them as needed to the designed changes.

Lack of "Aging" Strategy

There is an old riddle about firewall management: What goes in but never comes out? Answer: A firewall rule! Most organizations have well-established methods and procedures for adding rules into a firewall, but very few organizations have strategies for removing rules that no longer serve a legitimate business purpose. In fact, 63 percent of the respondents in a recent survey identified unused rules as a primary cause of policy complexity, while 59 percent cited the lack of vendor-supplied tools to assist in policy analysis as preventing them from addressing the problem. Over time, unnecessary rules result in excessive complexity, overly permissive access, unnecessary risk and performance degradation, all of which lead to higher costs that can be avoided.

04

The Firewall Cleanup Process

Maintaining an effective, efficient and correct firewall policy is a continual process. But in most cases, the existing firewall infrastructure is in dire need of an initial cleanup to address years of abuse and neglect. This section addresses this one-time or potentially periodic process of firewall cleanup. However, a more effective firewall management strategy should be considered to prevent the recurrence of this problem. This topic is briefly addressed at the end of this paper.

There are two key items to consider when cleaning up a firewall:

- Time / Effort / Cost: These are all essentially different measurements of the same issue. With limited time and resources to perform daily responsibilities, care and concern must be paid to how to reduce the effort necessary to achieve the goal of cleaning up the firewall policy. An efficient process must be followed to reduce this effort as much as possible.
- Business Impact / Risk: Over 80 percent of all network outages are caused by change. Firewall change is particularly risky and has the potential to both open a network up to excessive risk and negatively impact business continuity. Any changes made to the policy must take into consideration the risk of the change and the impact to the business.

The process outlined below takes these items into account by laying out a process that first attacks the quickest and least risky changes to immediately reduce complexity, then follows up with low-risk, high-value changes, and finally addresses the more time-consuming but high-value changes. This process most efficiently addresses the complexity and accuracy issues of a firewall policy.

Remove Technical Mistakes

Technical mistakes in a firewall policy can be identified as ineffective or incorrect no matter what the firewall is protecting. Two primary examples of technical mistakes are redundant and shadowed hidden rules. These two mistakes are very similar in that they are both examples of rules (or portions of rules) that the firewall will never evaluate because a prior rule will match the incoming traffic. The difference between the two is that a redundant rule has the same action as the rule that hides it, and a shadowed rule has an opposite action.

The reason for making this distinction is that shadowed rules present a second problem beyond unnecessary complexity; they also can cause significant confusion. An administrator analyzing a policy may see the shadowed rule and make an incorrect assumption about the firewall's behavior on the matching traffic. For this reason, shadowed rules are seen as a more severe issue in a firewall policy. Hidden rules are a very good example of unnecessary complexity. The rules serve no business function.

Removing these hidden rules is a very low-risk change, since after removal there is no change in firewall behavior. Hidden rules, by definition, were never going to be evaluated by the firewall, so removing them will have no effect on the policy behavior

However, identifying hidden rules is not a trivial task. Manual evaluation of a policy to find hidden rules is very difficult. In a small policy of tens of rules, it may be possible to spot these mistakes, but in a policy with hundreds, or even thousands, of rules, this is a very difficult task. Beyond just policy size, individual rule complexity caused by multiple objects, nested groups and poor naming conventions can all lead to difficulty in identifying hidden rules.

Although removing a hidden rule is considered low risk, this assumes that the hidden rules are correctly identified. For accurate and complete identification of hidden rules, use of an automated analysis is suggested. The sheer size and complexity of a typical enterprise firewall makes this step in the process too difficult to perform manually.

Review Rules & Refine Access

Rule review is an absolute necessity to ensure the firewall policy is effectively controlling access. Removing mistakes is a great first step. Removing unused access is a great next step. However, the simple determination that a rule is used does not mean it is necessary. A review of the business need and an acceptance of risk are necessary to fully justify the necessity of any remaining rule. Rule review is a complicated effort, and one that should be undertaken. However, that topic is beyond the scope of this paper, as it addresses a larger business decision and the process of justifying risk

Significant improvements can be made to the firewall policy in a technical rule-review process. In particular, refining broad access rules to include only necessary access is an improvement. This type of analysis will apply to any broad access rule, but is most commonly associated with rules where “ANY” is defined. Generally these rules are created with excessive access due to poorly defined business requirements. For example, access to a server is requested, but it is not known what protocol or port is used in that access. As a result, a service of “ANY” is defined. Refining that access from “ANY” to a narrowly defined list of services will greatly enhance the security of the protected networks.

The correct way to solve this problem is through business analysis to identify what is justified and necessary. But this can be extremely difficult to accomplish because necessity is not understood. One very effective way to solve this problem is to evaluate usage of the rule. Once it is understood what access is being used, it is possible to refine the broad access rule with a much more narrowly defined access rule.

Flow analysis is used to evaluate usage. A flow is a quadruple data record defining the source, destination, protocol and port of traffic flowing through the monitored rule. By building up a history of all the witnessed activity, it is possible to document what is necessary. Unfortunately, flow analysis is not easy to do manually, and it is not provided by firewall vendors. However, tools are available to assist with this process, and they should be investigated when attempting to perform this step of policy cleanup.

05

Benefits of a Proper Firewall Policy

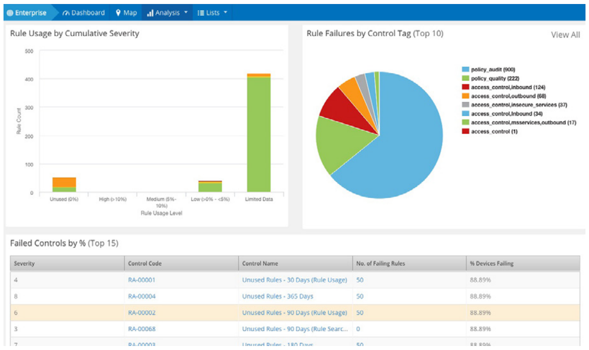
There are many and significant benefits to cleaning up a firewall policy.

- Reducing firewall administration overhead has a direct impact on the bottom line. Efficiencies gained through proper automation will produce a positive ROI. FireMon commissioned an excellent research report on firewall management ROI as a way to reduce cost. Be sure to visit the FireMon website and download your copy of "Firewall Economics – Spire Security Research Report."
- An optimized firewall policy will significantly reduce CPU load and may actually extend the life of the firewall platform. Understanding how rules are processed inside the policy is a key aspect of efficient firewall operation.
- Equally important to understanding how rules are used is to identify rules that are not being used. The identity and removal of unused rules not only reduces policy complexity but also will increase the overall security posture of an organization and aid in compliance initiatives.
- While identifying unused rules is an important aspect of policy optimization, it is also important to gain an understanding of how the actual objects inside a rule are being used (or not used). Removing unused objects not only helps reduce policy complexity but will also benefit the security posture of the firewall policy.
- Reduction in policy complexity through better firewall policy optimization will decrease the probability of and susceptibility to human error when making policy and configuration changes.
- The reduction of policy complexity will make firewall troubleshooting easier and accelerate restoration times, thus minimizing service impact during times of outages.
- Identifying overly permissive rules that allow greater access than the business requires can significantly increase the overall corporate security posture and provide better support for compliance initiatives.
- Alongside policy optimization comes good rule documentation. Having a well-optimized policy that is also complemented by thorough, centralized rule documentation further enhances firewall management and compliance provisions.

06

FireMon Security Manager

The cleanup and optimization of a firewall policy can be a daunting challenge weighted by different variables. What is the size of the rulebase? How well has it been managed over time? Is there available rule documentation to aid in remediation of unused rules? FireMon created Security Manager to help address these very challenges. If you've been tasked with optimizing your company's firewalls, Security Manager can help. Moreover, once you've invested the time and energy to achieve the optimization of firewall policies, FireMon can help you keep it that way. FireMon provides a full suite of utilities designed specifically to aid in the cleanup, optimization and ongoing maintenance of a firewall rulebase.


Enterprise
Dashboard
Map
Analysis
Lists
Rule Usage by Cumulative Severity
500
400
300
200
100
0
Rule Count
Unused (0%)
High (>10%)
Medium (5%-10%)
Low (>0% - <5%)
Limited Data
Rule Usage Level
Rule Failures by Control Tag (Top 10)
View All
policy_audit (900)
policy_quality (222)
access_control,inbound (124)
access_control,outbound (68)
access_control,insecure_services (37)
access_control,Inbound (34)
access_control,msservices,outbound (17)
access_control (1)

Failed Controls by % (Top 15)

Severity	Control Code	Control Name	No. of Failing Rules	% Devices Failing
4	RA-00001	Unused Rules - 30 Days (Rule Usage)	50	88.89%
8	RA-00004	Unused Rules - 365 Days	50	88.89%
6	RA-00002	Unused Rules - 90 Days (Rule Usage)	50	88.89%
3	RA-00068	Unused Rules - 90 Days (Rule Searc...	0	88.89%
7	RA-00003	Unused Rules - 180 Days	50	88.89%

More than just a cleanup tool, Security Manager is a real-time security management and event monitoring solution for firewalls, switches, routers and loadbalancer devices. Security Manager monitors for changes to policies and configurations, automatically compares a new policy to the previous policy and reports the difference (Who, What, When and Where). In addition, when the new policy is stored on the Security Manager server, it can perform an automatic, real-time audit against corporate requirements and report on it. Security Manager can readily achieve continual compliance monitoring – not just monitoring once or twice a year!

Security Manager's "Policy Test" lets you virtually verify current firewall policy connectivity or analyze results of a proposed "what if" data model.

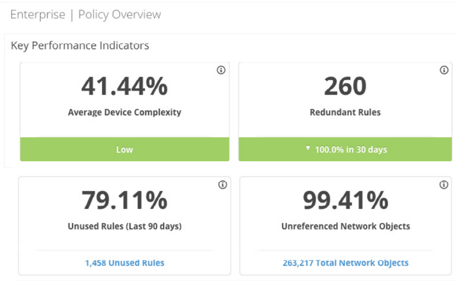
Remove Technical Mistakes with Hidden Rules Report

Security Manager provides a standard report for identifying redundant and shadowed rules with the exact details that indicate the portion of the rule causing the redundancy. This automated analysis can be run immediately after FireMon is installed and configured on the network. Within minutes of deploying Security Manager, you can have a prioritized list of actions to begin cleaning up a firewall policy.

Using automated and detailed analysis, Security Manager provides accurate reports of hidden rules in the policy. These results are actionable; prioritized remediation steps with the lowest risk and the highest impact are identified at the top of the report.

Remove Unused Access with Usage Analysis

Identifying unused access in a policy is impossible by static review alone. Identifying actual usage on the network requires historical or real-time log analysis. Using an innovative and unique matching analysis, Security Manager is able to perform real-time analysis and provide an unlimited history for rule and object usage in a policy. As a result, you can perform usage analysis to identify unused and most used rules and objects in all policies. This actionable information permits quick remediation of unused access.



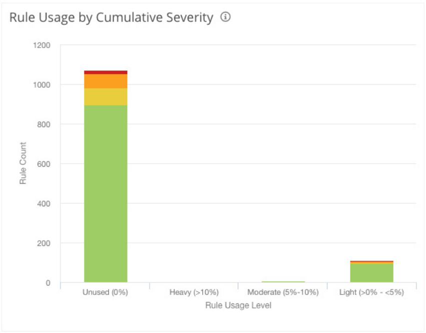
Enterprise | Policy Overview

Key Performance Indicators

41.44% Average Device Complexity Low	260 Redundant Rules ˄ 100.0% in 30 days
79.11% Unused Rules (Last 90 days) 1,458 Unused Rules	99.41% Unreferenced Network Objects 263,217 Total Network Objects

RULE USAGE ANALYSIS

Using real-time log monitoring, Security Manager provides graphical "Rule Usage" reporting that automatically identifies how rules and objects are being used so you can easily determine what changes need to be made to reduce policy complexity. In addition, Security Manager provides the data necessary to optimize the policy.



UNUSED RULE ANALYSIS

Security Manager clearly identifies which rules have seen no activity at all to help chart a remediation path for the removal of unused rules. This further aids the reduction of policy complexity while improving the corporate security posture.

UNUSED OBJECT ANALYSIS

Firewall vendors handle network and service objects differently. Some provide a robust editor for placing many objects in a rule, and others rely on group objects to represent a single identity. Some vendors require that objects have a saved definition before being placed in a rule, while others allow standard network and service definition directly in the rule. Regardless of the management approach, oftentimes network and service objects become stagnant inside of a rule, which adds inefficiencies to the security policy.

Objects inside of security rules that serve no purpose potentially allow unwanted access to resources. Security Manager's Rule Usage Analysis Report shows the hit count of security rules and the objects inside the rules. In addition, the report has a dedicated section for "Rules with Unused Objects," giving administrators the data necessary to reduce the scope of rules that are in use.

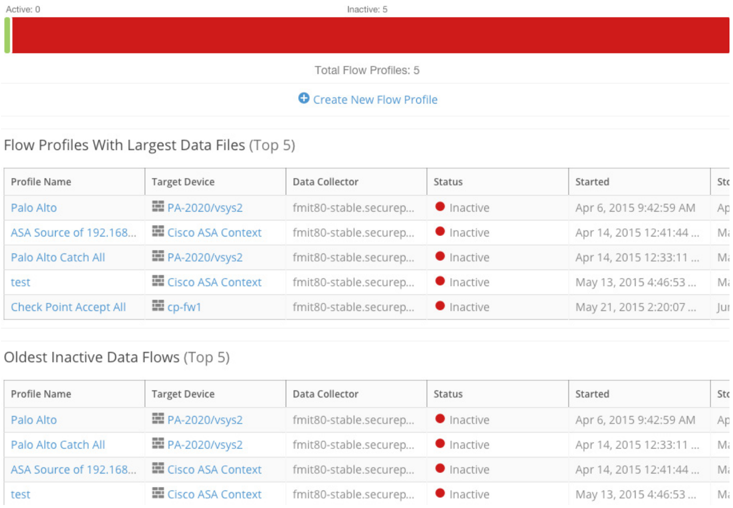
Sometimes objects are not hidden inside any rule or policy on the firewall. In those cases, Security Manager's global Object Usage Report details the usage of network and service objects regardless of their position in a policy.

Review & Refine Access

OVERLY PERMISSIVE RULES AND USE OF “ANY”

Security Manager includes a “Traffic Flow Analysis” feature that shows unique traffic patterns that exist in a rule and clearly reports on what data is flowing across a broadly defined address range. This analysis also shows what traffic is flowing across the use of “ANY” in a source, destination or service field.

With the output from this report, it is possible to refine an existing rule and replace the broadly defined access with a more correct and narrowly defined rule.



Flow Profiles With Largest Data Files (Top 5)

Profile Name	Target Device	Data Collector	Status	Started	Sto
Palo Alto	PA-2020/vsys2	fmit80-stable.securep...	● Inactive	Apr 6, 2015 9:42:59 AM	Ap
ASA Source of 192.168...	Cisco ASA Context	fmit80-stable.securep...	● Inactive	Apr 14, 2015 12:41:44 ...	Ma
Palo Alto Catch All	PA-2020/vsys2	fmit80-stable.securep...	● Inactive	Apr 14, 2015 12:33:11 ...	Ma
test	Cisco ASA Context	fmit80-stable.securep...	● Inactive	May 13, 2015 4:46:53 ...	Ma
Check Point Accept All	cp-fw1	fmit80-stable.securep...	● Inactive	May 21, 2015 2:20:07 ...	Jur

Oldest Inactive Data Flows (Top 5)

Profile Name	Target Device	Data Collector	Status	Started	Sto
Palo Alto	PA-2020/vsys2	fmit80-stable.securep...	● Inactive	Apr 6, 2015 9:42:59 AM	Ap
Palo Alto Catch All	PA-2020/vsys2	fmit80-stable.securep...	● Inactive	Apr 14, 2015 12:33:11 ...	Ma
ASA Source of 192.168...	Cisco ASA Context	fmit80-stable.securep...	● Inactive	Apr 14, 2015 12:41:44 ...	Ma
test	Cisco ASA Context	fmit80-stable.securep...	● Inactive	May 13, 2015 4:46:53 ...	Ma

A WORD ABOUT RULE DOCUMENTATION

Policy cleanup is a very important project, but a good firewall management strategy also includes a solid rule review process based on business justification. Security Manager provides the ability to automatically document device policies stored in the policy repository for that device. Rule documentation is the meta-data that explains a rule. Both automated and manual entry methods exist for the rule meta-data as values for specified attributes. The meta-data is uniquely associated with the rule for its lifetime, so when the policy or rule is modified, the metadata is not subject to modified rule numbers or other transient data changes.

Rule documentation can support your most important firewall administration tasks. For example, rule documentation is critical for certain regulatory compliance standards. Rules that don’t meet a particular standard’s specifications must be justified. Security Manager’s rule documentation features can act as the centralized repository for that justification.

Rule documentation includes the following attributes: Owner, Business Unit, Created on, Expires on, Justification

AUDIT CHANGE LOG

Security Manager's Audit Change Log feature captures and records the detail of every change event in the context of the firewall policy.

It appears in the GUI as a collection of incremental policy comparisons at the rule, object and policy levels that is updated in real time as revisions are retrieved. This provides the ability to produce detailed reports on the life history of rule and object changes in context of a policy. Documentation is the meta-data that explains a rule. Both automated and manual entry methods exist for the rule meta-data as values for specified attributes. The meta-data is uniquely associated with the rule for its lifetime, so when the policy or rule is modified, the meta-data is not subject to modified rule numbers or other transient data changes.

FIREMON

Learn more about our solutions: www.firemon.com

8400 W. 110th Street, Suite 500
Overland Park, KS 66210 USA