FIREMON

FIREWALL CLEANUP RECOMMENDATIONS

Best practices for improved firewall efficiency, reduced complexity and better security.

Executive Summary

One of the fundamental functions of firewalls is **access control**. Because all access inherently entails risk, controlling access can help to control that risk and provide an **opportunity to evaluate the risk against business needs**. Firewall rule complexity, however, reduces the benefit of access control by **limiting visibility into the access you have granted**, eroding your ability to assess the business justification for that access, and increasing the cost associated with security management.

Firewall policy complexity results in unnecessary, dated, inapplicable or conflicting rules that enable overly permissive access, erroneously deny justified access, drive unnecessary risk and degrade network performance. Given that a recent survey found that **94%** of IT and security professionals **indicate that firewalls today are as critical as—or more critical than—they have ever been**, the status quo is clearly unacceptable.[1]

Remediating these firewall issues, however, requires short-term activities to improve the current state of the firewall and long-term activities to prevent future recurrence of the issues. This paper discusses the **implications of firewall policy complexity, why it remains a problem today, and how to resolve it**.

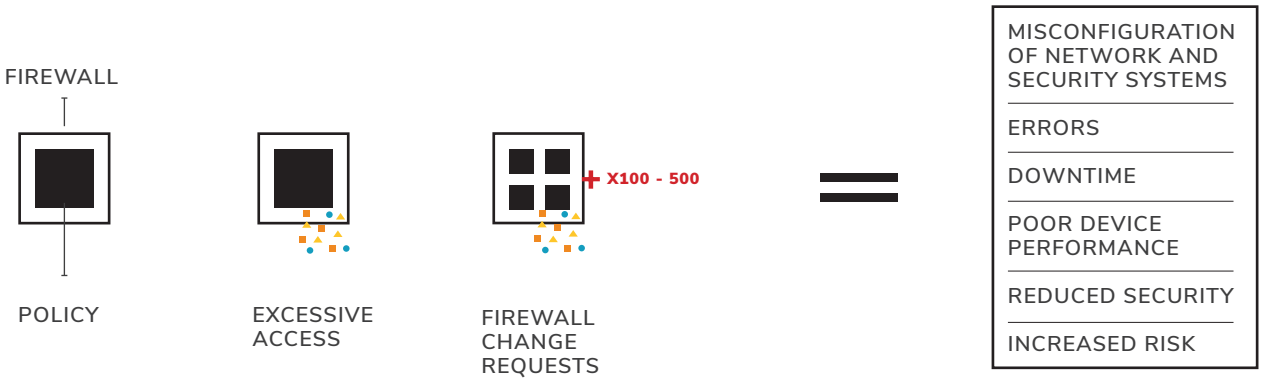
[1]FireMon. "2018 State of the Firewall." August 2018. http://content.firemon.com/resources/wp/firemon/2018-State-of-the-Firewall

Firewall Administration Challenges

One of the purposes of a firewall is 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, which is made up of rules that enforce access permissions**. Most firewalls employ a "positive security model," meaning that they deny access by default, and grant access only when a rule expressly requires it. By design, this model **should limit access only to what is necessary**, but in practice, the complexities of firewall management **often result in the granting of unnecessary or excessive access** that can increase an enterprise's exposure to risk.

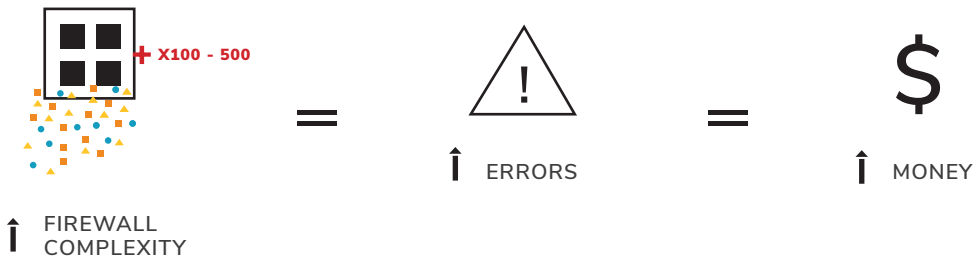
Here's why. An individual firewall's configurations can incorporate thousands of rules, and large organizations may deploy hundreds of firewalls. Moreover, the configurations of the **devices that the firewalls protect change constantly**. The 2018 State of the Firewall survey showed that many organizations receive as many as 100 firewall change requests a week, with some receiving as many as 500 firewall change requests each week.[2] Firewall policies **proliferate as the number of rules and devices increases**. In addition, organizations often have a mix of firewalls from different vendors, and different administrators for different business units. As well, eight out of ten companies report[3] that they are implementing, or planning to implement, technologies such as containerization, virtualization, microsegmentation, Zero Trust environments and software-defined networking, **all of which extend the traditional firewall domain**.

These factors combine to create an environment in which **poor-quality policies and rules abound**, resulting in misconfiguration of network and security systems, errors, downtime, poor device performance, reduced security and increased risk. Not surprisingly, IT and security professionals cite **complexity of firewall rules and policies as their greatest firewall challenge**.[4] The firewall that should provide confidence by exposing only an accepted amount of access and related risk has become so difficult to manage that some administrators simply accept that security gaps exist. In this paper, we will show you **practical, proven ways to clean up your firewalls to reduce complexity and enhance security**.



[2] FireMon. "2018 State of the Firewall." August 2018. http://content.firemon.com/resources/wp/firemon/2018-State-of-the-Firewall
[3] FireMon. "2018 State of the Firewall." August 2018. http://content.firemon.com/resources/wp/firemon/2018-State-of-the-Firewall
[4] FireMon. "2018 State of the Firewall." August 2018. http://content.firemon.com/resources/wp/firemon/2018-State-of-the-Firewall

©2018 FireMon, LLC. All rights reserved. 101118



Causes of Firewall Policy Errors

Cleaning up your firewalls reduces complexity and improves security. But to understand how to approach firewall cleanup, it is helpful to understand first how your current firewall environment developed.

EXCESSIVE POLICY COMPLEXITY

Firewall policy complexity is inevitable, but it is not inherently an error or a security issue. In large enterprises, the firewalls that control access will necessarily have complex associated policies. However, excessive complexity can be both an error and a security issue.

Not surprisingly, there is a strong correlation between excessive complexity of a firewall and the number of errors in the policy. As **complexity becomes excessive, errors increase**. Worse still, the issue compounds itself, with each error resulting in even more errors.

Excessive complexity has measurable impacts. The effort and the cost required to **manage a firewall significantly increases as firewall policy complexity increases**. Increased costs, for example, can result from the need for **new rule development and implementation**, and from the ongoing need for **annual audits** of these complex policies.

There are also system costs that add to firewall complexity. **The larger a security policy, the more taxing it is for a firewall to evaluate new access attempts against the policy**. In one extreme example, removing the unused rules from a policy **reduced average CPU usage by 30 percent**.

©2018 FireMon, LLC. All rights reserved. 101118

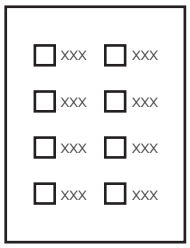
EXCESSIVE ACCESS

Excessive access negates the benefit of, and purpose for, using a firewall. Unfortunately, excessive access is all too common. Three of the primary causes for this are ineffective change management, poor definition of business requirements, and lack of an aging strategy.

INEFFECTIVE CHANGE MANAGEMENT

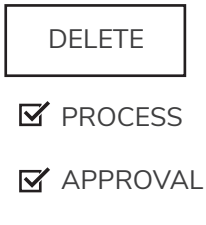
Formal, structured change management processes ensure that you **implement changes only when they are required**, in an optimized way with the appropriate approvals. The use of ineffective change management processes, or the failure to use even minimal processes, has several consequences. One is the implementation of unnecessary changes, such as **granting or limiting access** that has already been granted or limited in other ways. Another consequence is that **changes may not function as effectively as they could, or fail completely when interacting with existing policies**. Additionally, some changes made without fully considering the potential risk to the business, or accidentally allowing rogue changes, can **compromise security on a much larger scale**.

POOR DEFINITION OF BUSINESS REQUIREMENTS



The very nature of a digital enterprise means you will often receive last-minute change requests that require fast implementation. Often, these requests provide limited information about what is necessary to permit access. A request such as "permit access to this server from my network" does not **provide sufficient information to ensure that you limit access to only the necessary minimum**. This does not necessarily signal inattention or insufficient effort on the part of the requester. The simple fact is that optimized rules require a reasonably thorough **understanding of network conditions**, which may exceed the requestor's expertise. The result is often the creation of **overly-broad access rules**. Firewall administrators can do their best to limit access, but without specific, detailed business requirements, it is very difficult.

LACK OF AN "AGING" STRATEGY



An old riddle about firewall management asks "What goes in, but never comes out?" The answer is "A firewall rule." Even organizations that have established procedures for adding firewall rules may not have **strategies in place for removing them**. Optimally, a strategy should include: removing rules that no longer serve a legitimate business purpose, defining reasonable intervals at which to review rules for possible obsolescence, and a process for determining who needs to approve rule removal. Without such a strategy in place, **aging rules can lead to excessive access that degrades security** or unnecessary access limitations that hamper productivity.

Maintaining an effective and efficient firewall policy is a continual process. Often, existing firewall infrastructures require an initial cleanup to address previous inattention. This section addresses one-time and/or periodic firewall cleanup processes, and a later section addresses strategies to promote ongoing firewall hygiene.

©2018 FireMon, LLC. All rights reserved. 101118

The Firewall Policy Cleanup Process

There are two key items to consider when planning a firewall cleanup:

1. Time / Effort / Cost
   The limited time and resources available to most businesses constrain the time IT and security staff can spend performing daily responsibilities and special projects alike. As such, a firewall cleanup project should be as efficient as possible.

2. 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 firewall cleanup approach outlined below shows how to begin with 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.

REMOVE TECHNICAL ERRORS

Two technical errors that commonly occur in firewall policies are the presence of **redundant and shadowed hidden rules**. These mistakes are similar in that they are both examples of rules (or portions of rules) that the firewall will never evaluate because a preceding rule will match the incoming traffic. The difference between the two is that a redundant rule would result in the same action as the rule that hides it, while a shadowed rule would result in a different, and possibly opposite, action.

This distinction matters because shadowed rules present a second problem beyond redundancy, which is that they also 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** have the potential to be a **more severe issue**.

Identifying hidden rules is not a trivial task. Manual evaluation of a policy to find hidden rules is time-consuming. In a small policy of tens of rules, it may be possible to spot these errors rapidly. In a policy with hundreds, or even thousands of rules, the task is more challenging. In addition to the sheer number of policy rules, obstacles to analysis include the presence of multiple objects, nested groups, and poor naming conventions.

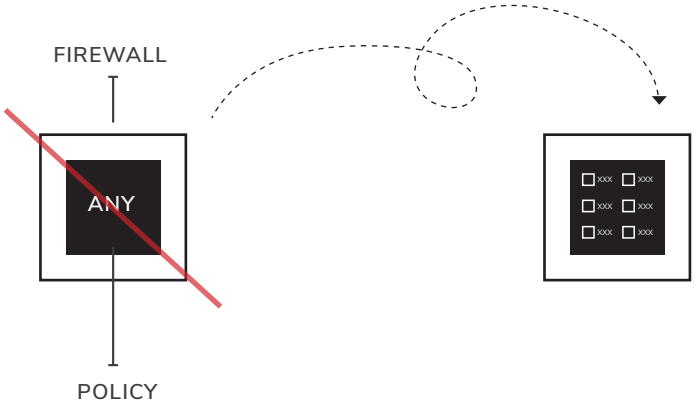
Removing hidden rules is low-risk, since there will be no change in firewall behavior post-removal. The firewall was never going to evaluate the hidden rules, so removing them not affect policy behavior. **But that is true only if a rule is correctly identified as being hidden in the first place.** The size and complexity of a typical enterprise firewall makes this step in the process too difficult to perform manually. For accurate and complete identification of hidden rules, automated analysis is a significantly better option.

TERMS

REDUNDANT RULE
Results in the same action as the rule that hides it

SHADOWED RULE
Results in a different, and possibly opposite, action, causing significant confusion

©2018 FireMon, LLC. All rights reserved. 101118



REVIEW RULES AND REFINE ACCESS

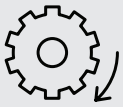
Once you have corrected the technical errors, the next step is to **remove unused and unnecessary access rules through a technical rule-review process**. One example of this process is refining broad access rules to include only necessary access. This type of analysis will apply to any broad access rule but is commonly associated with rules that utilize "ANY". Such rules are generally the result of change requests that provided poorly defined business requirements.

To illustrate, consider a change request that asks for access to a server, but fails to specify the protocol or port to use for that access. In this case, the rule may incorporate "ANY" to compensate for the lack of input. **Refining access from "ANY" to a narrowly defined list of services could significantly enhance security**. The question then becomes how to go about selecting the specific services.

One effective approach is to evaluate usage of a given rule. Once you establish a pattern that shows precisely the access that is being used when the rule is applied, you can **revise the rule to allow only that access**. You can perform this usage evaluation using flow analysis. A **flow is a quadruple data record defining the source, destination, protocol and port of traffic flowing through the monitored rule**. Building up a history of all the observed activity provides the specifics you need to define access narrowly and remove the generic "ANY" from the rule. Performing flow analysis manually would be prohibitively difficult, but various tools provide automation for the process.

©2018 FireMon, LLC. All rights reserved. 101118

8 BENEFITS
OF CLEAN FIREWALL POLICIES








Benefits of Clean Firewall Policies

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

1. Administration Efficiencies
   Reducing firewall administration overhead has a direct impact on the bottom line. **Efficiencies gained through proper automation will contribute to a positive ROI.**

2. Increase in Performance
   An optimized firewall policy will significantly reduce CPU load and could help to **extend the life of the firewall platform**. Understanding how rules are processed inside the policy is a key aspect of **efficient firewall operation**.

3. Rule Simplification
   Identifying and **removing unused rules** reduces policy complexity, enhances an organization's overall security posture, and aids in compliance initiatives.

4. Object Reduction
   Identifying and **removing unused objects** also helps reduce policy complexity and improve an organization's security posture.

5. Decreased Human Error
   Reducing policy complexity through better firewall policy optimization **decrease the probability of and susceptibility to human error when making policy and configuration changes**.

6. Easier Troubleshooting
   Reducing policy complexity can make firewall **troubleshooting easier** and **reduce restoration times, minimizing service impact** during outages.

7. Enhanced Security
   Identifying overly permissive rules can enhance an organization's overall **corporate security posture and provide better support for compliance initiatives**.

8. Improved Firewall Manageability
   A **well-optimized policy** complemented by thorough, centralized rule documentation further **enhances firewall management** and compliance provisions.

FIREMON

©2018 FireMon, LLC. All rights reserved. 101118

FireMon Security Manager

The cleanup and optimization of an organization's firewall policy can be a daunting challenge. To understand the full scope of the challenge, you need to know certain parameters. What is the size of the rule base? How well has it been managed over time? Is rule documentation available to aid in remediation of unused rules?

FireMon created Security Manager to help address these challenges. If you've been tasked with **optimizing your company's firewall, we can help**. Once you've invested the time and energy to achieve that optimization, **FireMon can help you maintain it**. FireMon provides a full suite of utilities **designed specifically to aid in the cleanup, optimization and ongoing maintenance of a firewall rule base**.

More than just a cleanup tool, Security Manager is a **real-time security management and event monitoring solution for firewall switches, routers, load balancers, and other similar devices**. Security Manager monitors for changes to policies and configurations and automatically compare a new policy to the previous policy and report the differences.

In addition, when you store new policies on Security Manager, FireMon can perform an automatic, real-time audit against corporate requirements and report on it. **Our "Policy Test" lets you virtually verify current firewall policy connectivity or analyze results of a proposed "what if" data model** to help you achieve continual compliance monitoring.

REMOVE TECHNICAL ERRORS WITH HIDDEN RULES REPORT

FireMon provides a standard report for identifying hidden, redundant and shadowed rules, with the exact details that indicate the portion of the rule causing the redundancy or error. You can run this automated analysis immediately after installing and configuring FireMon on the network. **Within minutes, you can have a prioritized list of actions needed to begin cleaning up your firewall policies.**

REMOVE UNUSED ACCESS WITH USAGE ANALYSIS

Identifying unused access in a policy is impractical, if not impossible, by static review alone. Determining actual usage on the network requires historical or real-time log analysis. Using an innovative and unique matching analysis, **FireMon performs 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.

SECURITY MANAGER

RULE USAGE ANALYSIS

Using real-time log monitoring, FireMon provides graphical "Rule Usage" reporting that automatically identifies how rules and objects are being used so you can easily determine what changes you must make to reduce complexity. and optimize the policy.

UNUSED RULE ANALYSIS

FireMon clearly identifies which rules have seen no activity 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.

©2018 FireMon, LLC. All rights reserved. 101118

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. Similarly, 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. Regardlessof the management approach, network and service objects often become stagnant inside of a rule, which adds inefficiency to the security policy.

Objects inside of security rules that serve no current, legitimate purpose potentially allow unwanted access to resources. Our 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, FireMon's global Object Usage Report details the usage of network and service objects regardless of their position in a policy.

REVIEW AND REFINE ACCESS

OVERLY PERMISSIVE RULES AND USE OF "ANY"

FireMon's "Traffic Flow Analysis" feature shows unique traffic patterns that exist in a rule and clearly reports on the data 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. You can use the output from this report to refine an existing rule and replace the broadly defined access with a more narrowly defined rule.

RULE DOCUMENTATION

In addition to policy cleanup, a comprehensive firewall management strategy should include a rule review process focused on business justification. FireMon provides the ability to automatically document device policies stored in the policy repository for that device. Rule documentation is the metadata that explains a rule. The metadata 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. For example, you must justify rules that don't meet a particular standard's specifications. FireMon'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, and Justification.

AUDIT CHANGE LOG

FireMon's Audit Change Log feature captures and records the detail of every change event in the context of the firewall policy. The feature appears in the user interface as a collection of incremental policy comparisons at the rule, object and policy levels. FireMon updates these comparisons 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 the context of a policy.

©2018 FireMon, LLC. All rights reserved. 101118

Conclusion

Firewalls continue to play a **vital role in network security even as network technologies and architectures evolve**. To ensure a strong security posture, you must maintain firewalls in optimal condition, and the first step in that process is cleaning up current firewall policies and rules. FireMon provides the specialized tools and features you need to clean up firewalls enterprise-wide efficiently and thoroughly.

For more information, **visit www.firemon.com**.

About FireMon

The FireMon platform delivers continuous security for hybrid enterprises through a powerful fusion of vulnerability management, compliance and orchestration. Since creating the first-ever network security policy management solution, FireMon has continued to deliver visibility into and control over complex network security infrastructures, policies, and risk postures for more than 1,700 customers around the world. For more information, visit www.firemon.com.

©2018 FireMon, LLC. All rights reserved. 101118