

Keeping your firewall rule documentation up to date in the face of multiple changes

Using Athena's new Firewall Rule Tracker

Abstract

When firewall rules become obsolete, referring to documented business justification is essential for considering whether or not to remove a particular rule. Firewall audits look at the rules to understand the security posture of the network, and maintaining up to date documentation for every firewall rule is also necessary for complying with PCI DSS 1.1.5 and NERC R2.2. This paper looks at the various approaches to rule documentation, how changes complicate the ability to keep documentation current, and how FirePAC's Rule Tracker addresses the weaknesses in other approaches.

Why is Rule documentation important?

Retaining knowledge of the rule base as business needs and people change:

When business lines and partners change, become obsolete, or replaced over time, firewall engineers tend to forget the business justification for the rules they have added. As engineers change and new people transition into the role, this problem is compounded even further. To have any semblance of control over the rule bases, it is therefore essential that rules are added to the firewall in an organized manner, documenting the business need, and the end user that requested the change. Without this knowledge, it becomes very difficult to justify why rules exist and determine what rules may no longer be needed.

Security Benefits:

Providing access to business services increases the risk of potential network exploits. Exposed assets and business services need to be constantly monitored and analyzed for application vulnerabilities. When access is no longer needed for certain business services, disabling the access avoids the overhead of steps that need to be taken in safeguarding against the attacks. Documenting the business justification for each rule that is added, and keeping it up to date in the face of changes, is an important aspect of accepting and managing risk.

Moreover, the first step in complying with requirements of security standards and frameworks like PCI DSS or NERC is to provide documentation for each rule and the safeguards in place when the rules are allowing dangerous services. A rule documentation system explaining the history of changes and their business justification goes a long way in convincing auditors that you are monitoring your rule bases and keeping good control over them.

Cleaning up obsolete rules:

On implementation, firewall engineers know why they are adding rules, but they are not usually notified when the business need for the rules they have added becomes obsolete. As a result, rule bases are not generally optimized until the firewall rules grow too large and messy. In the absence of complete rule documentation, firewall engineers must turn to rule usage analysis, which involves reams of log data potentially running into hundreds and thousands of giga bytes, to identify the rules that are no longer needed by users. Rule documentation helps firewall engineers short circuit the review of the business purpose with users before removing the rules as part of the firewall optimization process.

How is rule documentation performed?

Firewall Rule Comments:

Firewall management consoles, or the firewall CLI interface used for making changes to the rules, do not support the capture of detailed documentation for each rule. The rule comments field is the only way to specify the rule purpose in the firewall. However this comment field is not the appropriate place for detailed documentation. If the comment field is used, it is often used to provide a short description for the rule.

Change Ticketing Systems:

Medium to large enterprises use change ticketing systems to document the change requests coming in from end users. A separate help desk team often interfaces with the end users to enter these change requests into the ticketing systems documenting the request. These change ticketing systems are good at capturing documentation from the end user and are often preliminary in nature. Firewall engineers perform more analysis of what is involved to satisfy the change request. A change request might require changes in more than one firewall and more than one rule in a given firewall. Also one or more rules together could handle one or more change requests. When these tickets are finally closed in the change ticketing systems, the resolution might not have any description of the rules that were changed. As a result, when it is time to clean up rules or do a rule audit for PCI or other security requirements, it is difficult to locate up to date documentation that can be associated with specific rules.

Some firewall engineers use the practice of keeping the change ticketing id within the firewall rule comment. However generating a rule documentation report requires integration with the change ticketing system either from the firewall management console, or in the form of separate tools that can take the rules from the firewall and get the rule documentation from the ticketing system. However, this adds firewall management burden, and might not be accurate when an engineer has to make changes in an emergency. For this reason, it is almost impossible to keep real-time documentation consistent and constantly up to date.

Homegrown CMDB systems:

This is another approach where the firewall operations or review team maintain their own configuration management database storing the rules, network and service objects along with the business justification. The CMDB could be a self contained system containing the full documentation for the rules. If a change ticketing system is being used to capture the change requests, then the change ticketing ID is stored in the CMDB. They could be integrated with the change ticketing systems to pull the detailed documentation. This approach works well with CLI based firewall configurations where parsing the configurations and rules is some what easier. However identifying rules that have been modified because of changes in object groups requires a more thorough understanding of object groups. This approach also breaks down in mixed firewall environments that contain non CLI firewall configurations. Some of the other challenges with this approach involve: Identifying the rules that did not change so that the documentation is retained but with the updated line and rule numbers in the face of additions and deletions, identifying rules that have been modified so that the documentation can be updated and finally identifying rules that have been added so that documentation can be added are some of the other challenges in this approach.

Firewall Change Monitoring Systems:

The new generation of Firewall Rule Analytic and repository systems extend the capabilities of a home grown CMDB system to commercial grade capabilities. They are very sophisticated in that they understand the firewall configurations similar to the management consoles and only lack in the deployment capabilities. They handle mixed firewall environments and can talk to the firewall devices to retrieve the firewall configuration elements using a terminal channel controller interface, or the firewall vendor provided API. These solutions differ from the traditional text based firewall configuration repository systems in that they understand the actual rules and the network and service objects being used in the rules, not just the CLI text in the firewall configuration.

Most of these systems provide a capability to store documentation along with the rules, making it easier to generate reports with rule documentation, or query business justification for rules. Some of these integrate with the change ticketing systems to automatically get the documentation from the ticketing systems using the ticketing id, if it is available. as part of rule comments.

Some of these systems provide an integrated approach to rule documentation in that they provide capabilities to create change requests within the same system, and then associate them with the rules that were created or modified because of the change requests. Some of these systems track the rules through out their life cycle; including identifying changes being made to the rules and the users making the changes. They look at the firewall configurations for the changes while using the firewall log messages to correlate the changes to the users who made them. All these systems however require a tight integration with the firewalls; often direct connection to the firewall devices using SSH/Telnet channels to collect firewall configurations or rule bases and syslog, SNMP messages. The interface through which rule documentation can be updated is also limited. It is not possible to collaborate on rule documentation in an offline mode using spread sheets and then import it into the database. Working with the firewall configurations in an offline mode to document the rules is also very difficult. The team responsible for the rule documentation might be different from the team making the changes and hence might not have permissions to access the device. Most of these systems are also some what limited in terms of identifying which rules have not changed when rules are moved around or new rules are inserted when rules do not have rule IDs to identify the rule. This is essential in carrying over the documentation for rules that have not changed.

How is FirePAC's Rule Tracker different?

Athena's Rule Tracker is based on the firewall analytics capabilities in Athena FirePAC. It extends the excellent Rule and Object Search and comparison features in Athena FirePAC to track rule life cycle, and document business justification for rules. Rule Tracker was designed to solve the following major problems:

- Accurate Rule tracking and recognition of rule modifications requires an understanding of the context in which the rule is used (access list names, policy packages, Zone to Zone policies), the content of the rule (Source, Destination, Service objects and object groups), the content of the network and service object and object groups used in the rules. It is not enough to track rules by using only the line number or the rule number or the CLI text. This understanding is essential to identifying: rules that have not changed so that documentation is retained even if line or rule numbers have changed, rules that have been modified and the rule portions that are modified so that it is easy to identify if the rule's documentation has to be updated, and finally new rules that have been added so that new documentation can be added. You bring in updated configurations and Rule tracker will flag all rules requiring documentation updates.
- The team that is documenting the rules might be different from the team making the changes and hence they might not have access to the devices or the firewall management systems that have access to the devices. But they can get the firewall configurations from the operations team. You bring in the configuration into Rule Tracker and the rule tracker automatically flags all rules that need documentation. Rule tracker keeps track of the history of modifications to the rules as you bring in incremental changes to the firewall configuration.
- Users are very familiar with the Excel spreadsheets for documenting rules. All you need is list of the rules that need documentation. Using Rule tracker, you can update the documentation using the spread sheet type UI or export the rules in a spreadsheet, communicate the spreadsheet to the stake holders and import the finalized documentation back into the Rule tracker database.
- When it is time for a Security Audit or rule clean up, users need the latest rule documentation and the rule modification history in the form of a report for the audit period. With Rule Tracker, you can generate the latest rule documentation and the history of rule modifications that have happened during a given time interval. After establishing a base line review, reviewers might want to look at the rule modification history only for the last several months since the last audit and review only those modifications. Rule Tracker facilitates this with the Rule modification history and the documentation for those modifications.

- While a tabular view of the rules helps non technical and non CLI users to understand the rules, CLI text of the actual rule will be useful for the firewall engineers to track the rule in the firewall configuration and understand its purpose. Rule Tracker provides a tabular presentation of the rules along with the CLI text of the rule from the firewall configuration to help managers and technical users.

For more information about Athena's Firewall Rule Tracker, see:

<http://www.athenasecurity.net/ruletracker.html>.