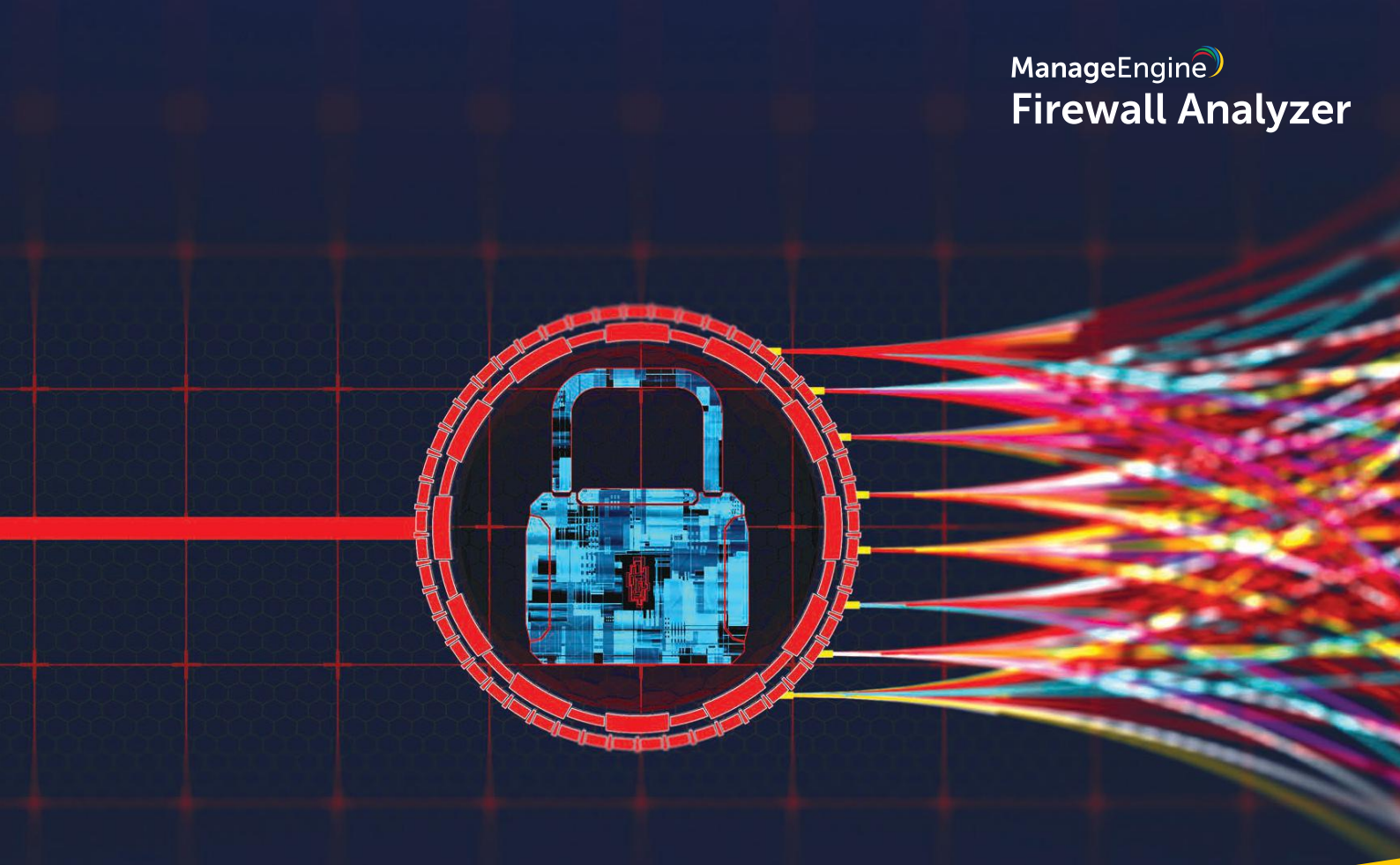
ManageEngine
Firewall Analyzer



FREE E-BOOK

10 FIREWALL BEST PRACTICES FOR NETWORK SECURITY ADMINS

CONFIGURE FIREWALL TO MAXIMIZE EFFECTIVENESS

-Mouli Srinivasan

WWW.FWANALYZER.COM

Firewall best practices

Table of content

10 firewall best practices for network security admins

Introduction

You shall not pass!

Keep your network safe from hackers.

Your firewall is the first line of defense against security threats, but as you may already know, simply adding firewall devices and security modules to your network doesn't ensure your network is more secure. You need to regularly watch and analyze your firewall's syslogs and configurations, and optimize its performance to protect your network. The heart of any firewall's performance is its rules and policies. If not managed properly, these can leave your network vulnerable to attacks.

Gartner predicts that 99 percent of exploited vulnerabilities will continue to be ones known by security and IT professionals for at least one year. Gartner concludes that the best and cheapest way to mitigate cyberattacks caused by known vulnerabilities is by removing them altogether with regular patching.

“

Gartner predicts that 99% of exploited vulnerabilities will continue to be ones known by security and IT professionals for at least one year.

For many security admins, maintaining optimal rule performance is a daunting task. Businesses are demanding that networks perform faster, leaving security admins balancing on the thin line separating speed and security. With these challenges in mind, here are some firewall best practices that can help security admins handle the conundrum of speed vs. security.

Firewall best practices

1. Document firewall rules and add comments to explain special rules.

It's critical for everyone in an IT team to have visibility over all the rules that have been written. Along with the list of rules, it's important to record:

- The purpose of a rule.
- The name of the security admin who wrote the rule, along with date of creation.
- The users and services affected by the rule.
- The devices and interfaces affected by the rule.
- Rule expiration date.

You can record this information as comments when creating a new rule or modifying an existing rule. The first thing you should do, if you haven't already, is review all the existing rules, and document the above information wherever possible. Though this might be a time-consuming task, you'll only have to do it once, and it'll end up saving you a lot of time when auditing and adding new rules in the long run.

2. Reduce over-permissive rules and include "deny all or deny rest" wherever necessary.

It's better to be safe than sorry; it's good practice to start off writing firewall rules with a "deny all" rule. This helps protect your network from manual errors. After testing and deploying the rules, it's a good idea to

include a "deny rest" at the bottom. This ensures that your firewall allows only the required traffic and blocks the rest. You'll also want to avoid using over-permissive rules like "allow any" as this can put your network at risk.

Permissive rules give users more freedom, which can translate into granting users access to more resources than they need to perform business-related functions. This leads to two types of problems:

- Under or overutilized network bandwidth.
- Increased exposure to potentially malicious sites.

Restrict over-permissive rules, and avoid these issues altogether.

3. Review firewall rules regularly. Organize firewall rules to maximize speed and performance.

As years go by and new policies are defined by different security admins, the number of rules tends to pile up. When new rules are defined without analyzing the old ones, these rules become redundant and can contradict each other, causing anomalies that negatively affect your firewall's performance. Cleaning up unused rules on a regular basis helps avoid clogging up your firewall's processor, so it's important to periodically audit rules as well as remove duplicate rules, anomalies, and unwanted policies.

Placing the most used rules on top and moving the lesser-used rules to the bottom helps improve the processing capacity of your firewall. This is an activity that should be performed periodically, as different types of rules are used at different times.

4. Check the health of your rules with a penetration test.

A penetration test is a simulated cyberattack against your computer system that checks for exploitable vulnerabilities. Just like how cars undergo crash tests to detect holes in the safety design, periodic penetration tests on your firewall will help you identify areas in your network's security that are vulnerable.

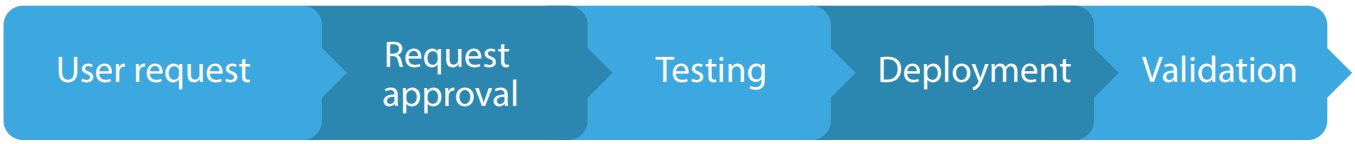
5. Automate security audits.

A security audit is a manual or systematic measurable technical assessment of the firewall. Given that it consists of a combination of manual and automated tasks, auditing and recording the results of these tasks on a regular basis is essential. You need a tool that can both automate tasks and record results from manual tasks. This will help track how configuration changes impact the firewall.

6. Implement an end-to-end change management tool.

The key to efficient policy management is an end-to-end change management tool that can track and record requests from start to finish. A typical change procedure might involve the following steps:

End-to-end configuration change monitoring



- A user raises a request for a particular change.
- The request is approved by the firewall or network security team, and all the details on who approves the request are recorded for future reference.
- After approval, the configuration is tested to confirm whether changes in the firewall will have the desired effect without causing any threat to the existing setup.
- Once the changes are tested, the new rule is deployed into production.

- A validation process is performed to ensure that the new firewall settings are operating as intended.
- All changes, reasons for changes, time stamps, and personnel involved are recorded.

7. Lay out an extensive, real-time alert management plan.

A real-time alert management system is critical for efficient firewall management. You need to:

- Monitor the availability of the firewall in real time. If a firewall goes down, an alternate firewall needs to immediately go up so all traffic can be routed through this firewall for the time being.
- Trigger alarms when the system encounters an attack so that the issue can be quickly rectified.
- Set alert notifications for all the changes that are made. This will help security admins keep a close eye on every change as it happens.

8. Retain logs as per regulations.

You need to retain logs for a stipulated amount of time depending on which regulations you need to comply with. Below are some of the major compliance standards along with the retention period required for each regulation.

Regulation	Retention requirement
PCI DSS	1 year
ISO 27001	3 years
NIST	3 years
NERC CIP	3 years
HIPAA	7 years
FISMA	3 years
GLBA	6 years
SOX	7 years

Different countries have different regulations on how long logs need to be stored for legal and auditing purposes. You should check with your legal team on which regulations your business needs to comply with.

9. Periodically check for security compliance.

Regular internal audits, combined with compliance checks for different security standards, are important aspects of maintaining a healthy network. Every company will follow different compliance standards based on the industry that business is in. You can automate compliance checks and audits to run on a regular basis to ensure you're meeting industry standards.

10. Upgrade your firewall software and firmware.

No network or firewall is perfect, and hackers are working around the clock to find any loopholes they can. Regular software and firmware updates to your firewall help eliminate known vulnerabilities in your system. Not even the best set of firewall rules can stop an attack if a known vulnerability hasn't been patched.

How can Firewall Analyzer help in adhering to these firewall best practices?

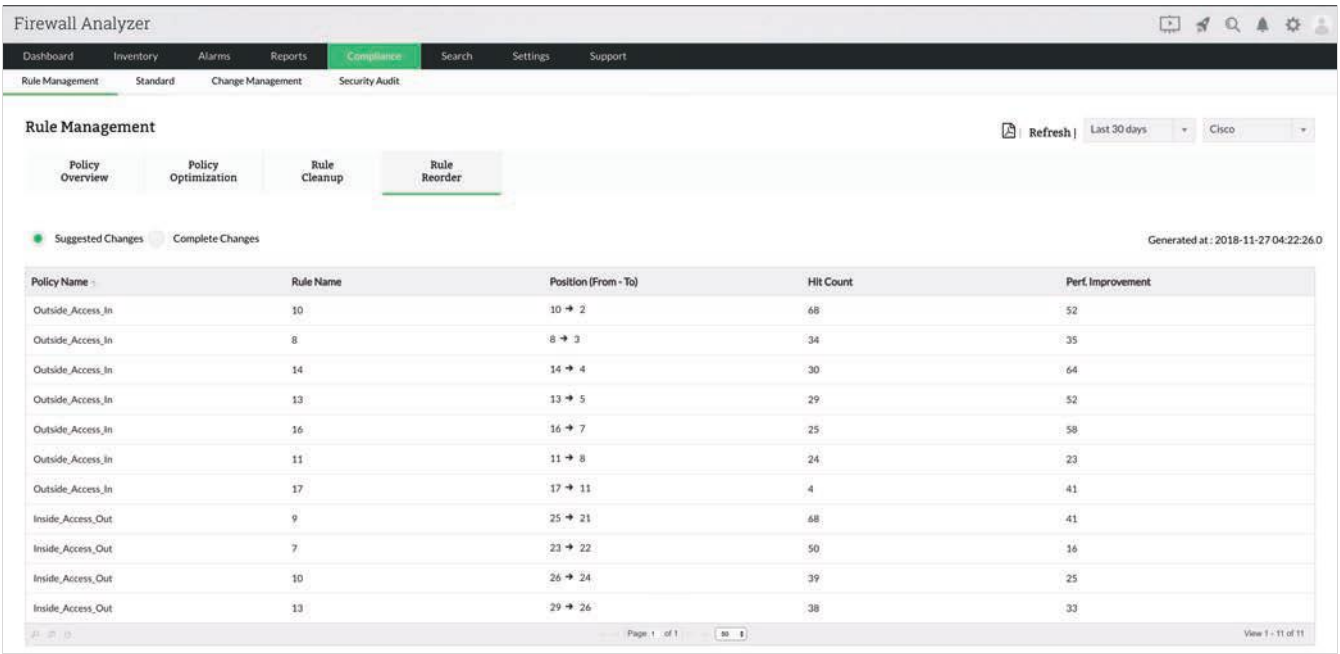
1. Rule Management:

Policy Overview: Manually documenting all firewall rules and reviewing them on a regular basis is an arduous and time-consuming task. To solve this issue, you can use Firewall Analyzer to fetch the entire set of rules written for your firewall. To simplify review, you can also filter rules on the following criteria:

- Allowed and denied rules.
- Inbound and outbound rules.
- Inactive rules.
- Rules with logging disabled.
- Over-permissive, any-to-any rules.

Policy Optimization: Firewall Analyzer's Policy Optimization feature identifies shadow rules, redundancy, generalization, correlation, and grouping anomalies. These anomalies negatively impact firewall performance, and removing them will help you optimize rule efficiency.

Rule Reorder: Firewall Analyzer provides suggestions on rule position by correlating the number of rule hits with rule complexity and anomalies. It can estimate the performance improvement for a suggested change.

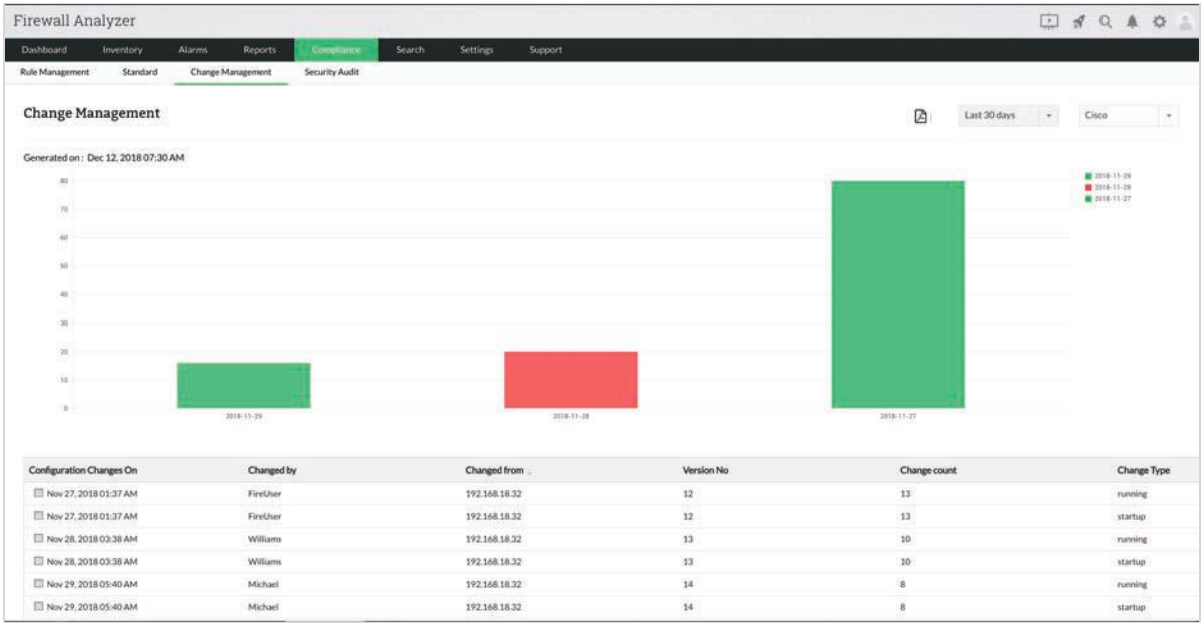


Rule Cleanup: Firewall Analyzer provides a detailed list of all unused firewall rules, objects, and interfaces. The Rule Cleanup feature gives you a high-level overview of which rules, objects, and interfaces can be removed or deactivated.

As you can see, Firewall Analyzer doesn't just provide visibility into firewall rules; its in-depth Rule Optimization and Rule Reorder reports help in removing rule anomalies and inefficiencies in rule performance. Together these reports help in:

- Documenting firewall rules.
- Reviewing firewall rules.
- Optimizing firewall performance.
- Organizing firewall rules to maximize speed.

2. Configuration Change Management: Firewall Analyzer fetches configuration changes from firewall devices and generates the following Change Management report.

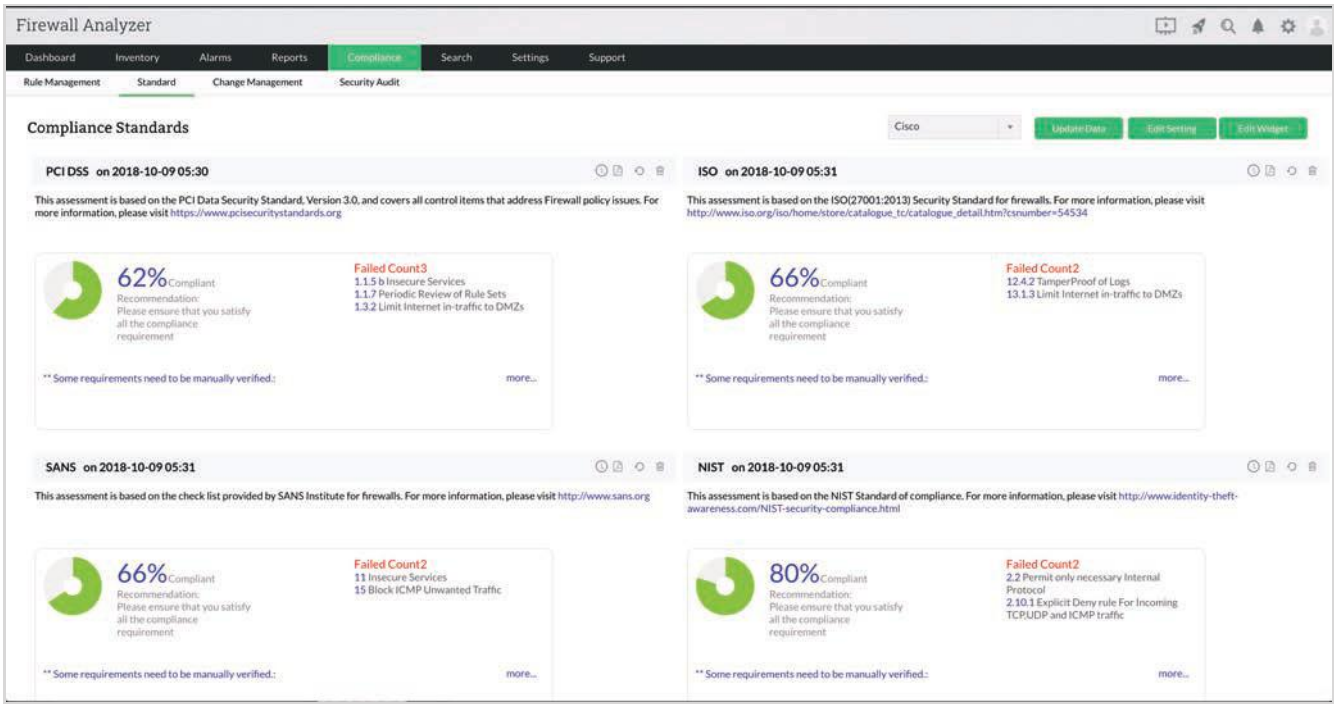


This report helps you find who made what changes, when, and why. Firewall Analyzer also sends real-time alerts to your phone when changes happen. This report ensures that all configurations and subsequent changes made in your firewall are captured periodically and stored in a database.

With a combination of ManageEngine's ServiceDesk Plus for ticketing and Firewall Analyzer for monitoring configuration changes, security admins gain end-to-end change monitoring. This type of end-to-end change monitoring system is critical for avoiding security events caused by human error.

3. Compliance Reports: Firewall Analyzer generates out-of-the-box compliance reports for the following industry standards:

- Payment Card Industry Data Security Standard (PCI DSS)
- ISO 27001:2013
- NIST Special Publication 800-53
- NERC's Critical Infrastructure Protection (CIP) Standards
- SANS Institutes' Firewall Checklist



With these reports, you can track your firewall devices' compliance status in terms of configurations.

4. Configuration Security Audits: Firewall Analyzer can perform security audits on the configuration setup of your firewall and provide detailed reports on any security loopholes. Firewall Analyzer also provides the severity of loopholes, ease of attack due to these loopholes, and a recommendation on how to fix reported issues.

5. Alarm Management: With Firewall Analyzer, you can set alarm notifications for both security and traffic incidents. Firewall Analyzer monitors syslogs, and sends out a notification whenever an alarm threshold trigger is passed. Alert notifications can either be sent via email or SMS. Firewall Analyzer's alarms help you identify security and traffic events as soon as they occur.

6. Log Retention: With Firewall Analyzer, you can either retain logs in the database or the archive. You can also set a time period for log retention to save disk space and improve performance; after all, disk space requirements can exceed 10TB if log data needs to be retained for a full year.

Summary

Continuously monitoring and reviewing your firewall rules, configuration and logs play an important role in securing your network.

With the ManageEngine's Firewall Analyzer, you can

- Document and review firewall rules.
- Organize firewall rules to maximize speed.
- Monitor all configuration changes made to the firewall.
- Perform forensic analysis on firewall logs.
- Set alarm notifications for traffic and security anomalies.
- Generate compliance reports and perform security audits.

With Firewall Analyzer, you can efficiently manage your firewall rules and adhere to the best practices.

About Firewall Analyzer

Firewall Analyzer is a rule, configuration and log analytics software that helps security administrators proactively detect and prevent network security threats. Firewall Analyzer supports all major commercial firewalls and open source security devices.

With Firewall Analyzer, you can efficiently manage your firewall rules and adhere to the best practices.

Download free trial **Request for a demo**