SKYBOX SECURITY

Six steps to firewall hygiene with optimized rulesets

Analyze firewall rule sets and automate change management workflows to improve cyber hygiene and reduce risk

Challenges

Fifty-five percent of 603 IT security decision-makers recently polled by Akamai and Ponemon Institute[1] expressed concerns about the agility of their organizations' security postures, citing that firewall rule changes took longer than three weeks to implement. A root cause is firewall rule bloat and complexity. Firewall rulesets become unwieldy and unmanageable over time with superfluous, overly permissive, obsolete, or orphan rules, expanding the attack surface of an organization and enabling easy access for threat actors.

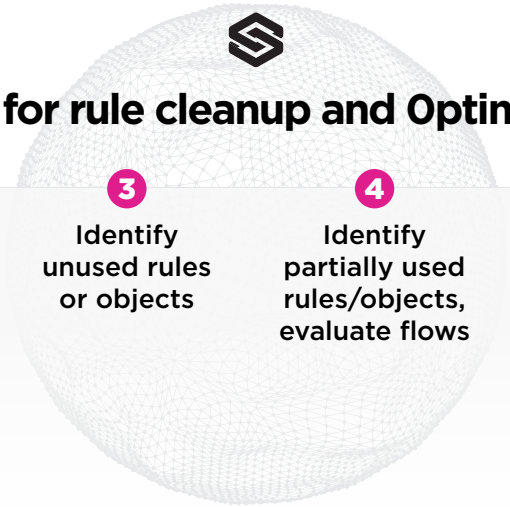
Removing unnecessary rules and objects reduces firewall policy complexity, increases manageability, and reduces misconfigurations, service disruptions, and rollbacks. A simpler ruleset facilitates easier documentation of business justification and ownership for each rule. A clear, intelligible ruleset combined with effective rule lifecycle management processes enables organizations to comply with internal policies and external regulatory frameworks continuously. Rule optimization is particularly beneficial in industries where periodic rule recertification is mandatory.

Use cases

- **Increased risk from large rulesets**
- **Rule logic analysis to identify shadowed/redundant rules**
- **Identification of duplicate and orphaned objects**
- **Unutilized rules flagged by traffic flow analysis**
- **Traffic flow analysis at source, destination, and service levels**
- **Automated workflows for removing and modifying rules/objects**
- **Seamless integration with 3rd party ticketing systems**

[1] Rethink Firewalls: Security and Agility for the Modern Enterprise, Ponemon Institute and Akamai, 2020

However, without automated operational workflows, rule optimization can be daunting even for seasoned administrators when managing complex mixed-vendor environments. Therefore, administrators should combine rule optimization with automated ticketing and change orchestration processes for seamless provisioning of optimized rulesets.



6 steps for rule cleanup and Optimization

1. **Identify shadowed, redundant, expired, or disabled rules**
2. **Identify duplicate or orphaned objects**
3. **Identify unused rules or objects**
4. **Identify partially used rules/objects, evaluate flows**
5. **Create tickets for rule/object deletion/ modification**
6. **Automated provisioning of rule/object changes on firewalls**

Solution

Security operations teams should optimize firewall rulesets annually or every 2 years for continuous cyber hygiene. At a minimum, teams should undertake the exercise before firewall migration or rule recertification projects.

1 Identify shadowed, redundant, expired, or disabled rules

In Figure 1 on page 3, Rule number 12 (app0 and app1 in Destination Objects/FTP in Service Objects), is shadowed by the more permissive Rule number 3 (any in Destination Objects/any in Service Objects), which appears above it in the firewall rule set. Because of how the firewall evaluates traffic, it will always match rule 3 first, and rule 12 remains unutilized. Similarly, a redundant rule has its scope entirely covered by other rules with the same action below it in the rule chain and should be eliminated. The Skybox Firewall Assurance module analyzes the rule base to identify shadowed, redundant, administratively disabled or expired rules.

2 Identify duplicate or orphaned objects

Duplicate objects have the same scope but different unique names. Administrators can eliminate the inconsistency of firewall rules that use duplicate objects by reconfiguring all rules to use one object and deleting the extra objects. Orphaned objects exist within the firewall configuration but are unutilized in any firewall rule. These objects can be pre-existing or newly created due to the elimination of duplicate objects. The Skybox Firewall Assurance module can flag duplicate or orphaned objects for elimination.

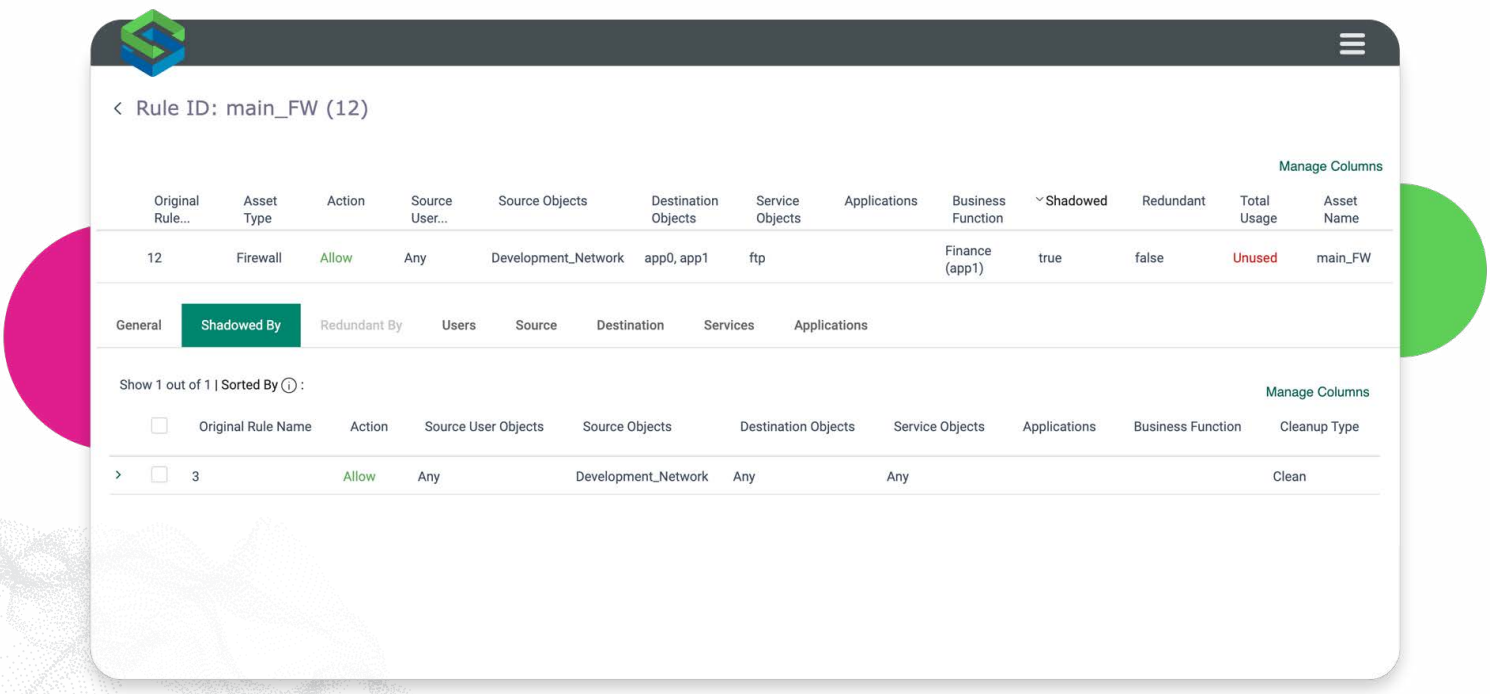


Figure 1: Example of a shadowed rule

3 Identify unused rules/objects

By analyzing firewall hit counters and traffic logs, Firewall Assurance identifies unused rules & objects that can be safely removed from the firewall. Firewalls must be configured to forward the correctly formatted Syslog data to the Skybox Collector, where usage metrics are calculated. Administrators must conduct the analysis over a sufficiently long period before altering firewall rules. Rules that are unutilized during the analysis period are flagged for either deletion or disabling.

4 Identify partially used rules/objects, evaluate flows

The **Skybox Firewall Assurance** module provides detailed, granular visibility into partial usage of rules and objects by delineating the exact utilization of sources, destinations, and services within a rule or object. Thus, the solution can identify overly permissive rules and objects. It can also map individual flows documenting communication between source, destination, and service tuples.

5 Create tickets for rule/object deletion/modification

The next step in the workflow is to submit tickets in Firewall Assurance for relevant rules and objects identified for deletion, deactivation, or modification. Administrators can manage the tickets in the **Skybox Change Manager** module, which fully automates firewall change management workflows for continuous network security, availability, and compliance while integrating seamlessly with popular 3rd party ITSMs and ticketing systems. During the risk assessment phase of the workflow, the Change Manager module ensures that proposed changes do not inadvertently expose vulnerabilities

or violate the compliance requirements codified in Firewall Assurance. This ability to de-risk proposed changes against unintentional vulnerability exposure is a unique Skybox differentiator and a critical capability for organizations interested in maintaining a fortified security posture.

6 Automated provisioning of rule/object changes on firewalls

Change Manager orchestrates the changes on supported firewalls through integrations with PAN Panorama, Fortinet FortiManager, Check Point Security Management, and Cisco Firewall Management Center. Tickets are closed after the changes are successfully implemented and verified. An optional step is to recertify the firewall rule set in Change Manager following automated de-provisioning of rules/objects and provisioning of modified rules/objects.

Benefits

- **Reduce attack surface by eliminating risky rules**
- **Improve business agility through faster firewall rule provisioning**
- **Increase network resiliency and ease of troubleshooting**
- **Free up personnel time through automated rule optimization**
- **Improve audit readiness and stay continuously compliant**
- **De-risk proposed changes by leveraging Skybox threat intelligence**

Want to learn more? Get a demo or talk to an expert:

skyboxsecurity.com/request-demo

ABOUT SKYBOX SECURITY

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. Our Security Posture Management Platform delivers complete visibility, analytics, and automation to quickly map, prioritize, and remediate vulnerabilities across your organization.