Organizations rely on firewall technology as a primary solution to limit unnecessary risk, manage access and decide on what traffic to allow or deny. Unfortunately, firewalls have traditionally suffered from one common problem — rulesets are created without the notion of proactive management. This results in rulesets that continually grow, slowing firewalls down and making compliance and management tasks burdensome or impossible.

To keep firewall rulesets clean and optimize performance, Skybox provides the centralized solution you need to:

- Unify management of a multi-vendor firewall estate spanning geographic locations, business units, etc.
- Automate cleanup and optimization processes to ensure management matches the speed of your business
- Orchestrate tasks intelligently based on the context of the environment and policy requirements
- Handle foundational tasks like optimization and cleanup, as well as policy compliance, firewall changes and rule life cycle management — all from one platform

**Skybox Best Practice Approach**

When transitioning from unmanaged firewalls that have grown organically to proactively managed firewalls that are in compliance with internal security policies or external regulations, the first step in the process is often to “clean up” the firewall ruleset. This is needed because investigating compliance of rules that shouldn’t exist due to irrelevancy or ineffectiveness is a waste of time. To streamline policy management, Skybox follows the best-practice process outlined in this brief.
Identify Shadowed Rules and Optimization Opportunities

Many administrators instinctively pursue “unused rules” as their first step for cleanup. This approach can falsely assume that an unused rule is a rule that should be deleted. It’s possible the exact opposite is true.

Before unused rules can be deleted, we need to understand why the rule isn’t being used. Assuming that the destination addresses have been decommissioned or the rule is no longer needed by the organization can ignore a common situation: a broader rule higher up the rule chain is passing traffic once destined for this rule. This overlapping rule situation is typically described as a “shadowed rule pair.” It could be that the smaller, shadowed (and unused) rule is really the one we want to keep.

1. Investigate shadowed rules
2. Remove shadowed rules where the broader rule will be kept
3. For shadowed rules you want to keep, move the broader, more permissive rules to the bottom of rule chain to allow more prescriptive rules to pass appropriate traffic
4. Explore trace data on these overly permissive rules to investigate ports and IP addresses; this is in order to reduce the scope of apps, services or source/destination network groups
5. Place the modified, narrower rule in its proper place in the rule chain
6. Continue cleanup efforts by investigating your unused rules
7. Move rules with higher hit-count up the rule chain

Exploring Shadowed Rules

Skybox explores shadowed rules to provide the information needed to decide which rule to keep: the broader rule on top or the smaller rule being shadowed. For example, if the larger rule on top is overly permissive, move it to the bottom of the rule chain so that the narrow rules pass all specific traffic. What traffic remains will then pass by the broader rule.

Analyzing Trace Data

Skybox examines trace data along with the broader rule of ports and IP addresses associated with the traffic that the rule passes. This data helps guide decisions on how to tailor a rule to an appropriate level, and it informs where — in terms of apps, service groups, source/destination networking groups — it’s appropriate to place that rule back in the rule chain.

The cleanup process continues by exploring unused rules and moving more prominently used rules up the rule chain.
Eliminate Redundant Rules

Another opportunity for rule optimization is to minimize redundant rules. These are rules that are used, but another rule lower in the chain matches the same traffic. It’s common for a redundant rule to have a smaller scope than the higher-ranking rule.

Skybox provides insight to these redundant rules, some of which are displayed as “poor usage.” The classification of “poor” means that one or more of their elements (e.g., source, destination or services) is larger than the actual usage of the element, rendering the rule less effective than desired. For example, a rule may display “any” as the source object, but the traffic passed by this rule comes from only a few sources. The destination element may have less than one percent usage; but as the destination for this rule is the “any” object, there can billions of possible destination addresses.
Support Compliance Readiness Strategy

Skybox’s automated solutions enable security personnel to manage a high volume of firewall rules more efficiently to bring their firewall into compliance and reduce the amount of overhead involved in managing compliance policies.

In addition, Skybox’s automated approach to rule life cycle management harnesses visibility and context-aware intelligence to streamline rule reviews and cleanup, transforming a project-based activity to a business-as-usual process. Using Skybox® Change Manager also provides integration between the built-in workflow and analytics engine, helping to avoid overlapping rules when processing new access requests.

Learn More

Optimization and cleanup is just one element of Skybox capabilities for firewall and security policy management. Learn more about our solutions in the links below:

- Skybox® Firewall Assurance Datasheet
- Skybox® Security Suite Overview

About Skybox Security

Skybox provides the industry’s broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 130 networking and security technologies, the Skybox® Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.

“Skybox has optimized our existing information security tools and provided a new, high-level, proactive approach to security management.”

—Oleg Volkov, CISO, United Card Services