algosec

Secure application connectivity.
Anywhere.

An application-centric approach to firewall rule recertification: Challenges and benefits

An AlgoSec Whitepaper

Introduction

Firewall rules support applications or processes that require network connectivity to and from specific servers, users, and networks. As part of ongoing security best practices, these rules must be reviewed and recertified on a regular basis.

The rationale for firewall rule recertification includes:

Security: Retaining unused or unnecessary firewall rules exposes the network to potential attacks.

Compliance: Industry regulations such as PCI-DSS recommend periodic reviews of firewall rules as a best practice.

Optimization: As rule sets grow, they impact firewall performance and increase management complexity. Excessive or outdated rules contribute to firewall bloat, making policies harder to manage and maintain.

Historically, rule recertification was performed by manually reviewing the comments field in each firewall rule. At minimum, this field should include the original requester and the rule's purpose. Even when properly documented, this approach is time-consuming, error-prone, and difficult to scale.

A more efficient and effective method is to adopt an application-centric approach. This approach identifies the business applications supported by each firewall rule, allowing teams to review and validate rules in the context of the applications they serve.

If the application still exists and has not changed, its associated rules can be recertified. If the application has been modified or decommissioned, its rules can be reviewed and removed as necessary.

This paper outlines the rule recertification process from both the firewall rule perspective and the application perspective. It also explains how to implement an application-centric approach and highlights its key benefits.

Why firewall rules become redundant

Firewall rules may become redundant for several reasons:

Application decommissioning

When an application is retired, its supporting firewall rules are often left in place even though they are no longer needed.

Application upgrades

For example, a desktop application may be upgraded to a web-based application using a different port (such as port 8080). Instead of modifying the existing rule, a new rule is created, and the original rule remains unnecessarily in the rule base.

Endpoint relocation

Servers or endpoints may be moved due to data center consolidation, cloud migration, upgrades, or hardware refresh projects. New rules are created to support updated connectivity, while legacy rules remain in place.

Managing and removing unnecessary firewall rules

Organizations typically approach rule recertification in one of two ways:

Ongoing review via expiration dates

Some organizations assign expiration dates to firewall rules. Each week, administrators review rules that are nearing expiration and either extend them or remove them. This makes recertification an ongoing operational process.

In less mature processes, expired rules are only reviewed after an application fails and a user reports an issue.

Project-based periodic review

Other organizations conduct rule recertification as a periodic project. Administrators review and validate all firewall rules across the environment at the same time.

The recertification process generally includes four steps:

1. Review firewall logs to determine when the rule was last used.
2. Check the rule comments to identify the requester and associated application.
3. Validate with the relevant business contact that the application is still in use.
4. Remove the rule or extend its expiration date.

Regardless of the chosen approach, automation significantly improves efficiency and reduces errors. An effective network security management solution should provide:

- Centralized visibility into firewalls, rules, network objects, and configurations
- Reports identifying unused rules
- Automated expiration tracking and alerts
- Change management capabilities to safely remove rules
- Rollback functionality in case of error
- A complete audit trail documenting all activities

An application-centric approach to firewall rule recertification

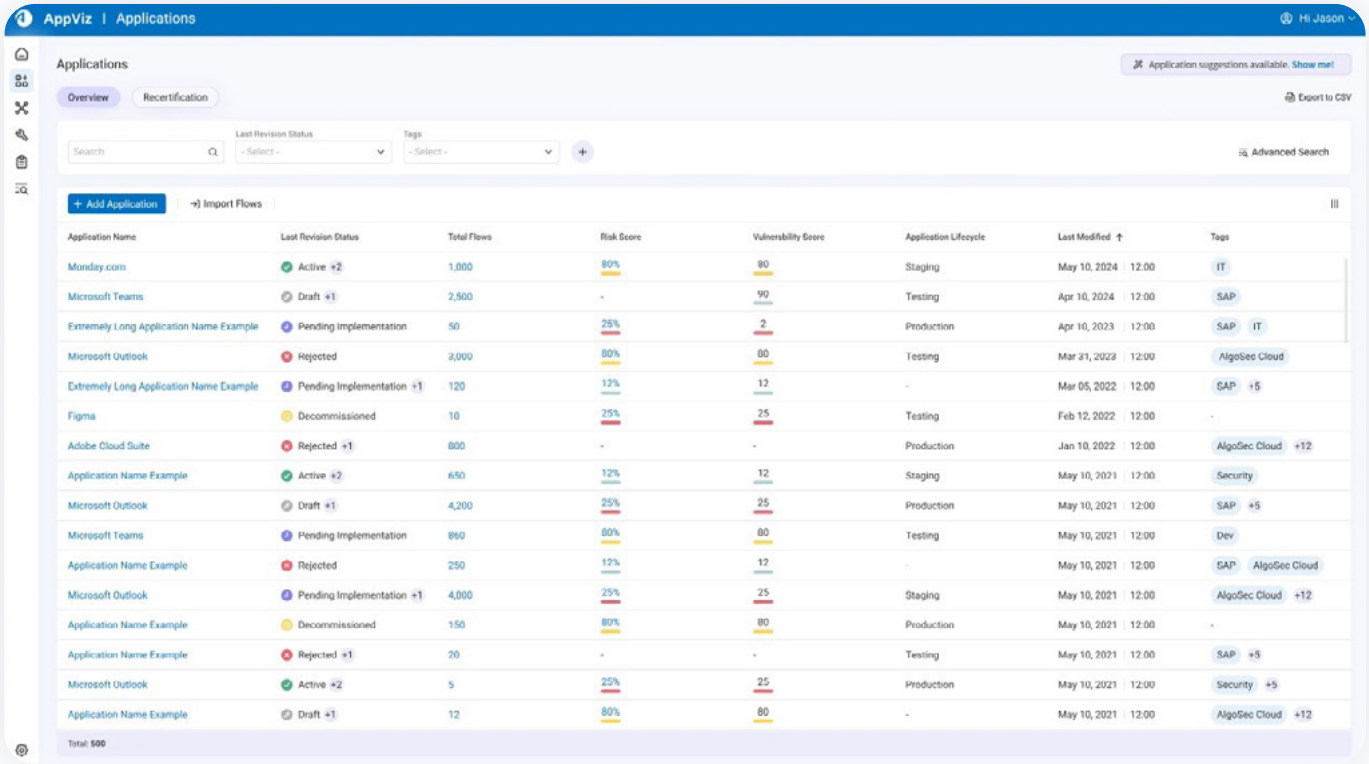
AlgoSec Horizon makes recertification fast, practical and auditable by shifting the work from low-value firewall rules to the business objects your teams actually care about: applications and their logical flows. Instead of forcing owners to read hundreds or thousands of technical rules, AppViz packages the flows that implement an application and gives owners a simple, flow-by-flow workflow to attest what's still required.

How the process looks:

- **Discover (Greenfield or Brownfield)**
  - **Greenfield:** start clean — create applications and flows directly in AppViz.
  - **Brownfield:** bring existing knowledge: AI discovery, cloud application discovery (AWS/Azure/GCP), micro-segmentation integrations, or a CSV import wizard so teams can import discovered applications and flows.
- **Map & package**

  AppViz can begin from a seed asset, suggest application membership, correlate flow telemetry with policy data, aggregates "thin" flows to comprehensive application flows, and enumerate the firewall/cloud rules that implement each flow. AppViz then packages those flows into a single recertification task for the application owner.
- **Certify & audit**

  The Application Grid shows owner, certification status, expiry date, and progress (percentage of flows certified). Admins can set application expiry dates and AppViz automatically notifies owners as recertification is due. AppViz records certification decisions and can write certification/comments back into the AlgoSec policy record for audit and change-management workflows.



Summary

Certifying applications and flows is X15 faster and business-relevant than a rule-by-rule audit. AlgoSec horizon reduces audit effort by aggregating intent, linking flows to rules, and automating owner notifications and reporting. This is particularly relevant for companies that need a repeatable, auditable recertification program as regulations and internal policies require periodic attestation.

"The key is understanding your applications; if you don't understand your applications fully, you can't manage them, and you can't reduce the risk around them."

Nationwid

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to securely accelerate application delivery up to 100 times faster by automating application connectivity and security policy across the hybrid network environment.

With two decades of expertise securing hybrid networks, over 2300 of the world's most complex organizations trust AlgoSec to help secure their most critical workloads.

Learn how AlgoSec enables application owners, information security experts, SecOps and cloud security teams to deploy business applications faster while maintaining security at www.algosec.com.