algosec

Secure application connectivity.
Anywhere.



Technical blueprint: Attack path & rulebase hygiene

A practitioner's guide to dismantling risk in the hybrid fabric

Executive summary

In most environments, security teams are overloaded with alerts while the actual attack surface remains cluttered with legacy rules and temporary fixes from years ago. This blueprint argues that hygiene is your best defense. By cleaning up your rulebase and closing lateral movement paths before they are used, you stop reacting to threats and start preventing them.

This guide provides a clear, two-part playbook: a Remediation Workflow to close active risks and a Hygiene Framework to safely decommission dirty rules. Following these steps can help you cut Any/Any rules by half within 12 weeks and replace manual audit spreadsheets with automated proof.

Note from Iris

If you're like me, you're tired of being told that you have a problem without being given the steps to fix it. We've all inherited rulebases that look like digital archaeology - layers of old rules no one is brave enough to touch. This blueprint is designed to give you that confidence. I've focused on the logic you need to log into a console, verify a path, and fix it without breaking the apps the business depends on. No fluff; just the runbook.

The pathway to hybrid security

1. The hybrid manifesto:
   Establishing the architectural truths of hybrid security. Coming soon;
2. Cutting the kill chain:
   Shifting from alerts to visual, cross-estate risk mapping.
3. Attack path blueprint:
   Tactical steps for remediating hybrid vulnerabilities.
4. AI prompt playbook:
   Putting natural language automation to work for your team.
5. The trinity demo:
   A live masterclass in unified execution.
6. Migration mapping blueprint:
   The final framework for secure application mobility.

1. The reality: Complexity is the attack surface

In 2026, we don't just have a security problem; we have a hygiene problem. An attacker doesn't need a fancy exploit if they can walk through an overly permissive firewall rule you forgot about.

The goal is simple: move from a permissive state to a defensive one. We have to treat our on-premise core and cloud accounts as one single, connected fabric.

2. The remediation workflow

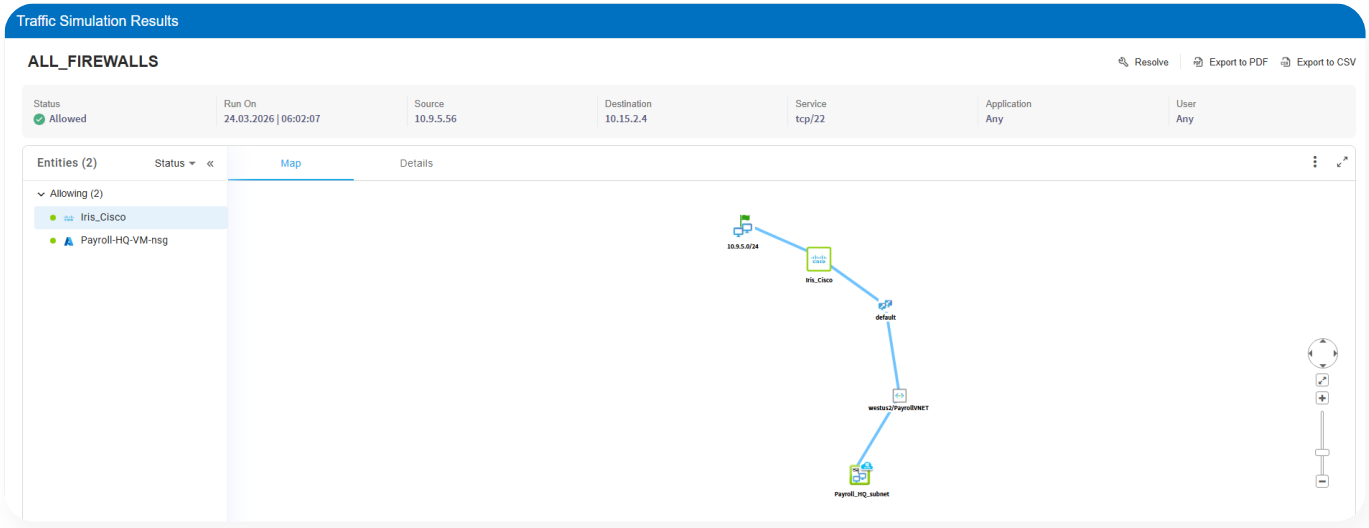
Remediation must be surgical. We never guess; we simulate.

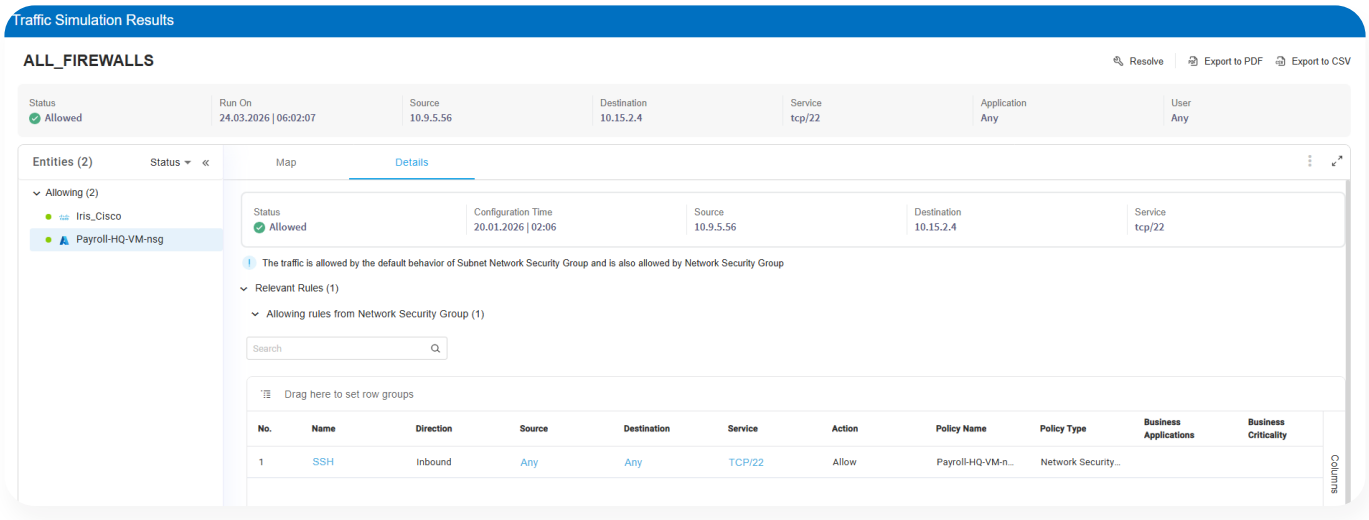
Step 1: Trace the path

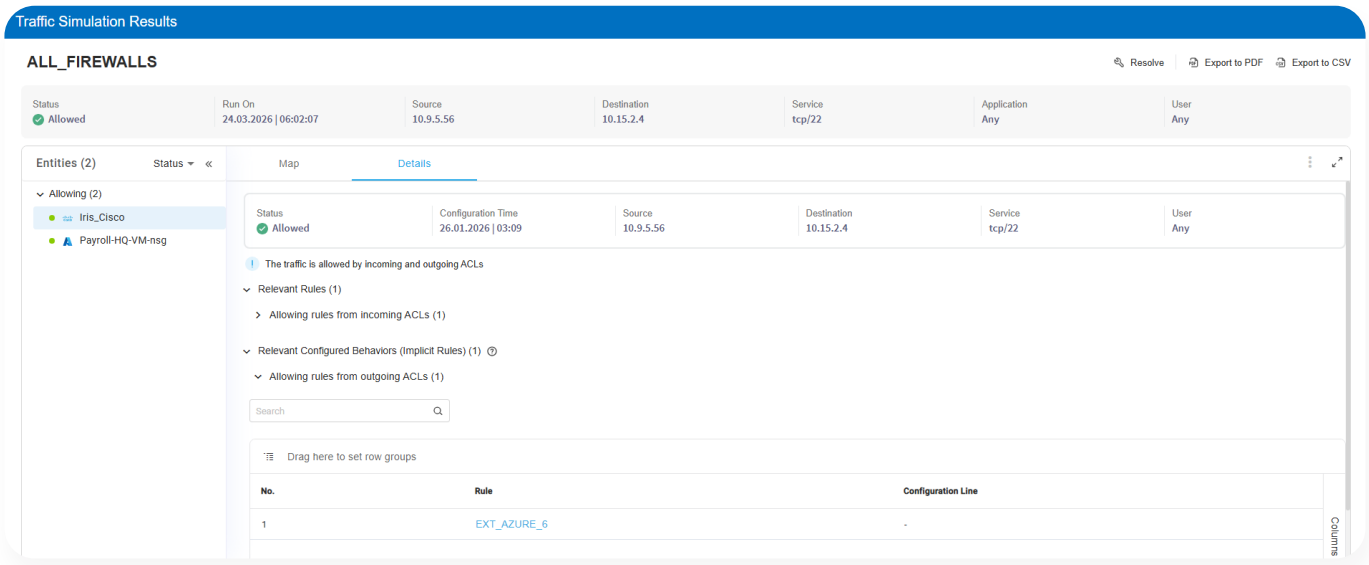
Ignore the alert text for a second and look at the graph. You need to see how traffic actually flows from your cloud frontend to your on-premise core. Identify every hop - every security group, router, and firewall in the way.

Example: HybridQuery Cisco Azure TSQ

This example showcases a hybrid TSQ that allows traffic from Azure and Cisco devices. It is an illustration of how to visualize and analyze the flow of traffic across a hybrid environment—from a cloud frontend to an on-premise core.







Step 2: Find the point of least resistance (PoLR)

The PoLR is the single change that breaks the attack chain with the least amount of work. In the example above, changing four AWS groups is a headache. Modifying rule 212 on your on-premise firewall is the PoLR. It's the kill switch for this specific threat.

Step 3: Run a what-if simulation

Before you hit Apply, use FireFlow to see the impact.

- **The goal:** Make sure blocking that port won't accidentally kill a legitimate backup job or a different app that shares that rule.
- **The check:** If the simulation shows no impact on known application traffic, you're good to go.

3. Rulebase hygiene: The cleanup

A clean rulebase is a fast, secure rulebase. We look for dirty rules in three categories:

- **Shadowed rules:** Rules that do nothing because a rule above them already handles the traffic.
- **Unused rules:** Rules that haven't seen a hit in 90+ days.
- **Overly permissive:** Those Any/Any rules that were meant to be temporary.

The ghost discovery method

How to delete rules without fear:

- **Identify:** Find rules with zero hits in Horizon.
- **Disable:** Turn the rule off in your next maintenance window. Do not delete it yet.
- **Monitor:** Use Horizon AppViz to watch the health of your applications.
- **Delete:** If the app stays green for 30 days, the rule is a ghost. Now you can safely delete it.

4. Technical deep-dive: Decoding unknown traffic

Unknown-TCP traffic is a huge blind spot. If you don't know what it is, you can't secure it properly.

Horizon ACE uses AI to look at traffic patterns and label them for you. For example, it might find Unknown-TCP between two clusters and label it web-to-database-sync. Once it's labeled, you can replace a broad Allow Any rule with a specific, tight rule for just that service.

5. Your daily routine

- **Daily:** Check your high-risk alerts and make sure Horizon AppViz shows your apps are healthy.
- **Weekly:** Run a shadowed rule report. These are easy wins for cleaning up your policy.
- **Monthly:** Run a full simulation of an attack from the public internet to your most sensitive data zones (PCI/PII).

Summary: Why this works

This blueprint works because it speaks your language — **hit-counts, VPCs, and shadowed rules.** It separates the emergencies (attack paths) from the maintenance (hygiene), and it gives you the tools to prove your work to auditors without opening a single spreadsheet.

Next Stop (Stop #4): Once you've mastered this manual cleanup, we'll move to the **AI Prompt Playbook**, where we show you how to use natural language to automate the whole Disable → Monitor → Delete process.

Welcome to the Fabric.

Iris AlgoSec

© AlgoSec Inc. All rights reserved. AlgoSec and the AlgoSec logo are registered trademarks of AlgoSec Inc.
All other trademarks used herein are the property of their respective owners.