



Network Security Assurance

Find and Fix Network Security Control Weaknesses Before AI Adversaries Exploit Them



FINDING
Overly permissive rule allows unrestricted traffic
PA NGFW > acme-tsg-001 > NA-East-Prod > pan-fw-nyc-01 > Allow-All-NYC

[Remediate](#) [Create ticket](#) [Accept risk](#) [Export](#) [...](#)

Overview Rule Detail Remediation

Severity

IMPACT

#3
of 287 rules

#2
rules shadowed

87%
HTTPS, HTTP, DNS

This rule is positioned at #3 in a 287-rule policy and allows all traffic from trust to untrust. It renders 3 more specific rules below it useless. 83% of its traffic is just HTTPS, HTTP, and DNS — services that could each have their own granular rule with proper logging and rate limiting.

SEVERITY
High

FINDING TYPE
Any/any rules

STATUS
Open

FIRST DETECTED
Apr 2, 2026

DAYS OPEN
48 days

LAST SCANNED
3 min ago

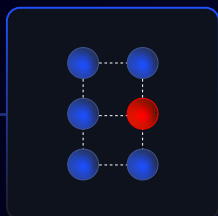
The Challenge

Bad rules stay live. Teams find out too late.

Modern network security environments change faster than teams can manually validate them. Over time, as rules are altered, network security controls quietly drift away from security baselines. Risk gets buried in the rulebase. Stale rules stay live, shadowed rules obscure true exposure, and overly permissive any/any rules sneak in, leaving hidden paths to breach for AI-powered attackers.

Security teams are unable to easily see these network security control gaps when they materialize. How could they? They're juggling 10 to 100 firewalls and hundreds of weekly rule changes as it is. Periodic manual rule reviews don't help. They rarely instill confidence and fail to validate live enforcement posture. Months pass between audits, widening the gap for AI adversaries to exploit weaknesses.

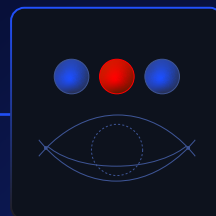
Legacy network security policy management tools also fail to deliver assurance. These tools were built to administer firewall rules, document compliance, and orchestrate change requests. Those workflows don't reliably answer the most pressing question: are live controls across firewalls, SASE, and adjacent network security tools actually enforcing the security posture the business intended?



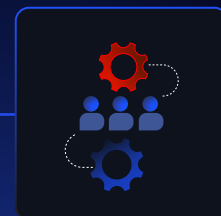
Network security controls drift.



Risk gets buried in the rulebase, leaving hidden paths to breach.



Manual defensive workflows can't keep pace with AI-speed attacks



Periodic manual reviews fail to validate live enforcement posture.



The Solution

Continuously find and fix network security control weaknesses

Reach Network Security Assurance is AI-driven defense for the network security controls that AI-powered adversaries target. Security teams get continuous visibility into how network security controls are configured, enforced, and drifting across your firewall, SASE, and adjacent network security enforcement points. Reach identifies rule issues, misconfigurations, unintended access paths, and drift at the speed of AI, then prioritizes what matters most and remediates gaps before attackers can exploit them.

Detected issues are tied back to actual exposure, guiding remediation down to the exact rule, firewall, or configuration that created the risk. Reach turns quarterly, days-long rule reviews into continuous, threat-informed rule analysis and remediation, automatically validating every change and fixing risky controls as they appear.

1



Continuously validate network security intent.

Live controls drift hourly. Reach validates network security intent continuously across firewalls and SASE so security policy and live enforcement never separate.

2



Detect network security drift and hidden exposure.

Reach surfaces stale, shadowed, redundant, and overly permissive rules, and reads the rulebase the way an attacker would, prioritizing what adversaries actively exploit.

3



Constantly harden and realign network security controls

Quarterly cleanup projects become AI-speed remediation. Reach guides remediation with step-by-step instructions to close gaps and reduce attack surface.

FINDING

Overly permissive rule allows unrestricted traffic

PA NGFW > acme-tsg-001 > NA-East-Prod > pan-fw-nyc-01 > Allow-All-NYC

[Remediate](#) [Create ticket](#) [Accept risk](#) [Export](#) [...](#)

Overview Rule Detail Remediation

Step-by-step remediation

- 1 Locate the rule**
In Panorama, open [Policies → Security](#) and locate [Allow-All-NYC \(#3\)](#) in the Branch-Security policy on pan-fw-nyc-01.
- 2 Analyze traffic patterns**
Review the traffic log for the past 30 days to identify the actual source/destination/service patterns (83% is HTTPS, HTTP, DNS).
- 3 Create granular replacements**
Create granular replacement rules for each identified traffic pattern with specific source subnets, destination zones, and service ports.
- 4 Demote the broad**
Move Allow-All-NYC to a lower position or disable it, and monitor for breakage over 7 days.
- 5 Finalize and commit**
Once validated, delete the original any-any rule and commit the config.