INTERNAL

Scalable Microsegmentation

When Manifest-State Meets Reality

Vincent Phelan
Head of Infrastructure Architecture
Standard Chartered Bank • Singapore

Ross Draper
Head of Global Network Platforms
Standard Chartered Bank • Singapore

INTERNAL

The Problem With Firewall Rules as Segmentation



Nobody remembers the /24

That subnet was split and moved 3 times before the next renewal cycle. The intent is lost — only the data remains.



Perimeter thinking on internal networks

Partner IPs and NATs are static and traceable. Internal apps evolve, move, and never stay the same.



10,000 rules, zero provenance

Which rules map to which business need? Who approved them? Are the approvals still valid? Nobody knows.

INTERNAL

Manifest-Driven Intent

Abstract the network. Declare application-to-application intent.

BEFORE: Firewall Rules

```
permit tcp 10.42.16.0/24 10.53.8.0/24 eq 443
permit tcp 10.42.16.0/24 10.53.9.0/24 eq 8080
permit tcp 10.42.16.0/24 10.61.3.0/24 eq 443
# why? who? when? still needed?
# subnet moved in 2023, re-NATed 2024
# approved by... someone, probably
```

AFTER: Application Manifest

```
consumer: app-a
publisher: app-b
protocol: https
contract: DCH-2024-0847
owner: APP-TEAM-PAYMENTS
# IP resolution from IPAM at deploy time
```

INTERNAL

Contention Points — The Messy Reality

"If the system doesn't stop it, it must be allowed"

Show an app team an "out" to bypass — they will take it. RDP enabled to your reverse proxy because someone wanted to skip management access restrictions.

Every application is special

Allow one exception and you allow everyone's. The gatekeeper role is thankless — you continuously explain the "why" while teams push for the "but".

The approval lapse

Is your manifest still what's configured? Did the contract expire? Make the approval step visible in the pipeline — incident calls will simply bypass it.

Operations needs an out

Without a rollback or emergency bypass for operations, you cannot blame them for going around the system. But every bypass is a policy hole.

INTERNAL

Where Segmentation Hits Its Limits

Diminishing Returns

- Ever-growing rule sets create fatigue and misconfiguration risk
- Where does network segmentation yield to identity-based controls?
- Demanding unique LB entry points per consumer sounds great — creates operational overhead

What Is Good Enough?

- Consumer/publisher model — app teams understand it
- Going beyond creates complexity that causes more risk than it mitigates
- The goal is provable, auditable segmentation — not maximum granularity

INTERNAL

Multi-DC and Non-Prod — The Hidden Debt



Same app, different DCs — different rules?

If the same application deployed across multiple data centers has different segmentation rules — they are simply not the same application. The manifest should enforce parity.



Non-prod rules ≠ prod rules = go-live debt

Making non-prod easier by relaxing rules creates technical debt at go-live. "Why is this so hard? It worked in non-prod" — because non-prod had no rules. Equal rules test prod through non-prod.

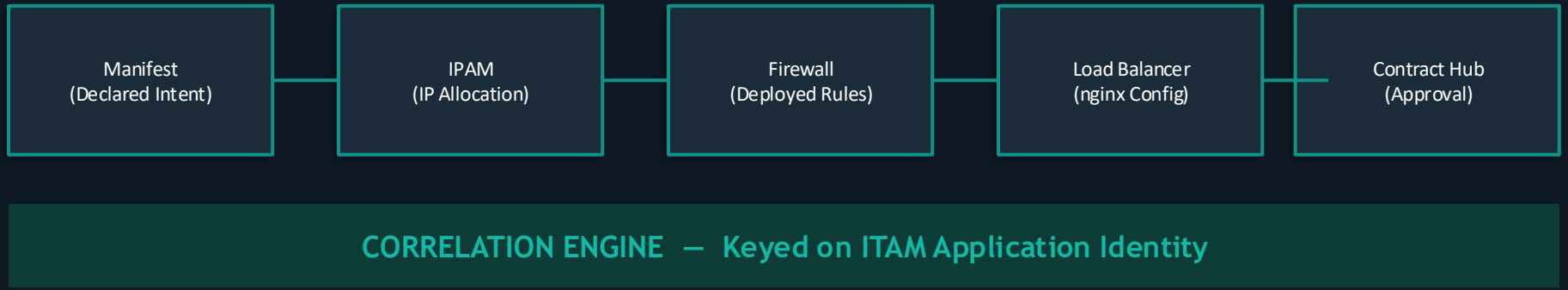


Cross-environment by default

App A consumes App B — valid in non-prod and prod immediately. Rules persist across environments. Address it at first instance in non-prod; prod is pre-validated.

INTERNAL

Continuous Validation — Catching the Drift



What drift looks like:

- Manifest declares HTTPS — nginx config shows HTTP on port 8080
- Contract approved 14 months ago — auto-renewal never triggered
- IPAM shows /24 allocation — firewall rule references old /22 pre-migration
- Team A updated NTP standard — Teams B, C, D failing compliance

INTERNAL

Takeaways



Declare segmentation as application intent, not IP rules. Abstract the network layer.



Validate continuously — daily, automated, against every enforcement layer. Not quarterly audits.



Non-prod and prod must have equal rules. Cross-environment by default, not by request.



Good enough segmentation > perfect segmentation that creates fatigue and misconfiguration.



Make drift visible. When the dashboard is public, people fix things before you ask.

INTERNAL

Questions & Discussion

How does your organisation validate that segmentation intent matches reality?