CHG0030010 — [TITAN] High — security on fw-allow-all-ingress

Severity	High	Priority	2 - High
Cloud	Multi	State	New
Resource	fw-allow-all-ingress	Group	network_operations
Resource type	compute.googleapis.com/Firewall	Change type	Normal
Opened	2026-04-21 14:36:44	Closed	2026-04-21 14:36:44
CAB required	Yes	Close code	—

Security Finding

```
GCP firewall rule 'fw-allow-all-ingress' allows any protocol from 0.0.0.0/0 to all VMs tagged
'default' — every compute instance is exposed to the internet.
```

Justification

```
GCP firewall rule 'fw-allow-all-ingress' allows any protocol from 0.0.0.0/0 to all VMs tagged
'default' — every compute instance is exposed to the internet.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
gcloud compute firewall-rules update fw-allow-all-ingress
--source-ranges=10.0.0.0/8,172.16.0.0/12,192.168.0.0/16
3. TITAN FORGE verifies the fix was applied.
4. Post-change rescan by TITAN SCOUT — finding must no longer appear.
5. Close ticket with Successful close_code.
```

Risk & Impact Analysis

```
Risk level: MEDIUM-HIGH risk — misconfiguration with realistic exploit path.
Business impact if unremediated: Increases attack surface; auditor finding likely.
Scope: single resource (fw-allow-all-ingress).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: GCP firewall rule 'fw-allow-all-ingress' allows any protocol from 0.0.0.0/0 to all
VMs tagged 'default' — every compute instance is exposed to the internet.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of fw-allow-all-ingress before change (baseline:
titan-live-demo-20260421T213642Z).
2. If post-change rescan still shows the finding OR a new issue appears within 15 min:
a. TITAN FORGE fires rollback automatically using stored snapshot.
b. Incident reopens and escalates to on-call.
3. Manual rollback command path (human override) is documented in close notes.
```

Test Plan

```
1. TITAN SCOUT rescans fw-allow-all-ingress immediately after FORGE applies the change.
2. PASS criteria: the specific finding no longer appears in SCOUT results.
3. PASS criteria: no new CRITICAL or HIGH findings introduced by the change.
```

```
4. Automated compliance check: HIPAA/PCI/SOC2 controls re-evaluated.
5. If any check fails, backout plan fires automatically.
```

Recommended Fix Command

```
gcloud compute firewall-rules update fw-allow-all-ingress
--source-ranges=10.0.0.0/8,172.16.0.0/12,192.168.0.0/16
```

Compliance Mapping

```
CIS Azure 6.2, NIST SC-7, PCI DSS 1.2.1
```

AI Close Notes

```
(empty)
```