INC0010100 — [TITAN] Critical — network on fw-telco-core-edge

Severity	Critical	Priority	1 - Critical
Cloud	Azure	State	Closed
Resource	fw-telco-core-edge	Group	network_operations
Resource type	Microsoft.Network/firewalls	Change type	Emergency
Opened	2026-04-22 20:19:25	Closed	2026-04-22 20:33:25
CAB required	Yes	Close code	Successful

Security Finding

```
Azure Firewall telco-core-edge has 'Allow Any/Any' rule permitting all inbound from internet to SS7/Diameter signaling subnet. CTIA security guidelines and 3GPP TS 33.210 violation — possible SS7 exploitation path.
```

Justification

```
Critical: Azure Firewall telco-core-edge has 'Allow Any/Any' rule permitting all inbound from internet to SS7/Diameter signaling subnet. CTIA security guidelines and 3GPP TS 33.210 violation — possible SS7 exploitation path.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
az network firewall policy rule-collection-group collection remove --policy-name fw-telco-core-edge-policy --rule-collection-group-name network --name allow-any-any
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: HIGH business risk — active exposure; fix required immediately.
Business impact if unremediated: Potential data exfil, privilege escalation, or compliance breach.
Scope: single resource (fw-telco-core-edge).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Azure Firewall telco-core-edge has 'Allow Any/Any' rule permitting all inbound from internet to SS7/Diameter signaling subnet. CTIA security guidelines and 3GPP TS 33.210 violation — possible SS7 expl
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of fw-telco-core-edge before change (baseline: titan-telecom-demo-20260422T201925Z).
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-telco-core-edge 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

```
az network firewall policy rule-collection-group collection remove --policy-name
fw-telco-core-edge-policy --rule-collection-group-name network --name allow-any-any
```

Compliance Mapping

```
CIS 1.x IAM, NIST AC-2, SOC 2 CC6.1, CIS Azure 6.2
```

AI Close Notes

```
TITAN CONDUIT orchestrated end-to-end: SCOUT detected the critical network incident, FORGE applied
the consent-gated fix automatically (incident class), SCOUT rescan confirmed the finding cleared,
and CONDUIT closed this ticket with a Successful close_code. Pre-change snapshot retained for 30
days for rollback.
```