TITAN AI · CONDUIT · CHANGE REQUEST

CHG0030107 — [TITAN] Critical — network on nsg-telco-5g-core

Severity	Critical	Priority	1 - Critical
Cloud	Azure	State	Assigned
Resource	nsg-telco-5g-core	Group	network_operations
Resource type	Microsoft.Network/networkSecurityGroups	Change type	Emergency
Opened	2026-04-22 19:37:25	Closed	2026-04-22 19:37:25
CAB required	Yes	Close code	—

Security Finding

```
5G core NSG allows any-any between N6/N9 interfaces — control-plane and user-plane traffic
improperly separated. 3GPP TS 33.501 and NIST SP 800-207 (Zero Trust) deviation.
```

Justification

```
Critical: 5G core NSG allows any-any between N6/N9 interfaces — control-plane and user-plane
traffic improperly separated. 3GPP TS 33.501 and NIST SP 800-207 (Zero Trust) deviation.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
az network nsg rule create --resource-group rg-telco-5g --nsg-name nsg-telco-5g-core --name
allow-n6-only --priority 100 --source-address-prefixes 10.5.0.0/16 --destination-port-ranges 2152
--access Allow --protocol Udp
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 (nsg-telco-5g-core).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: 5G core NSG allows any-any between N6/N9 interfaces — control-plane and user-plane
traffic improperly separated. 3GPP TS 33.501 and NIST SP 800-207 (Zero Trust) deviation.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of nsg-telco-5g-core 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 nsg-telco-5g-core 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 nsg rule create --resource-group rg-telco-5g --nsg-name nsg-telco-5g-core --name allow-n6-only --priority 100 --source-address-prefixes 10.5.0.0/16 --destination-port-ranges 2152 --access Allow --protocol Udp
```

Compliance Mapping

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

AI Close Notes

```
TITAN CONDUIT opened this critical network change request and assigned it to the regulatory_affairs group for review. STATE: ASSIGNED — awaiting human action. Per TITAN AI policy (and Kazmi rule, 2026-04-22), configuration changes are NEVER auto-applied and change tickets are NEVER auto-closed by TITAN. The assigned group reviews the recommended fix, schedules a CAB-approved change window, applies the fix manually, validates via SCOUT rescan, and closes this ticket themselves. TITAN documents and routes — the human owns the change from here.
```