SCENARIO 6: "FRIENDLY FIRE"

Network Incident Investigation & Crisis Response

North Coast International Airport (NCIA)
Tabletop Exercise — Player Briefing Packet
Exercise Duration: 2 Hours
EXERCISE — FOR TRAINING USE ONLY

EXERCISE — EXERCISE — EXERCISE

1. SITUATION BRIEF

It is 9:47 AM on a Wednesday. The morning departure rush is winding down. Then every point-of-sale terminal in the airport goes dead. Simultaneously.

Every card reader in every restaurant, coffee shop, gift shop, and duty-free store — from Concourse A to Concourse B, landside to airside — is showing the same thing: **"TRANSACTION FAILED — UNABLE TO REACH PAYMENT GATEWAY."** The terminals are powered on. The screens are working. But they cannot process a single transaction.

Within three minutes, the airport's Retail VLAN monitoring dashboard shows **zero active connections** between the Retail VLAN (VLAN 40) and the Server VLAN (VLAN 10), where the payment gateway appliance sits. That pathway — which handled an average of 4,200 transactions per hour — is now carrying exactly zero packets.

At the same time, the FIDS displays in the Concourse B food court flicker and go dark. Gate management terminals on Concourse B report intermittent connectivity. The airline shared-use check-in kiosks on the landside are timing out.

Nothing else is affected. The PACS system is up. Cameras are recording. Radios work. The AODB is online. Email works. It is a targeted, surgical disruption — and it hit at the worst possible time, in the most visible possible way.

YOUR MISSION: Determine the cause of the outage. Is this a cyberattack, a system failure, or something else? Restore payment processing. Manage vendors, airlines, passengers, and media. And figure out who — or what — did this.

System	Status	Impact
POS Terminals (All Concessions)	DOWN — Cannot reach payment gateway	All 47 retail tenants. Cash only. Lines building.
Payment Gateway (VLAN 10)	ONLINE — server is up and responding to local pings	Gateway is healthy. It's not receiving traffic from the Retail VLAN.
FIDS Displays (Concourse B food court)	DOWN — Screens dark	4 displays in the food court area. Other FIDS working.

Gate Mgmt Terminals (Concourse B)	INTERMITTENT — slow, timeouts	Airlines reporting delays in boarding processes.
Check-in Kiosks (Landside)	INTERMITTENT — session timeouts	Passengers unable to complete self-check-in.
PACS / Cameras	NORMAL	No impact. VLAN 30 unaffected.
AODB / Core Ops	NORMAL	Flight data, scheduling, ops — all working.
Email / Admin	NORMAL	VLAN 20 unaffected.

2. NCIA NETWORK ARCHITECTURE (SIMPLIFIED)

All NCIA systems are segmented into VLANs (Virtual Local Area Networks). Traffic between VLANs passes through the core firewall (Palo Alto PA-850), which enforces access control rules between segments.

VLAN	Name	Key Systems	Status
10	Server	Payment Gateway, AODB, FIDS Server, Domain Controller, DNS, DHCP	ONLINE — all servers responding
20	Admin	Workstations — Ops, Finance, HR, IT, Executive	NORMAL
30	Security	CCTV, NVR, PACS Controller	NORMAL
40	Retail	POS terminals (47 tenants), vendor workstations	■ DOWN — no connectivity to VLAN 10
50	Passenger	FIDS displays, check-in kiosks, gate mgmt, airline CUTE	■ DEGRADED — intermittent connectivity
60	Baggage / OT	BHS, gate readers, ramp systems	NORMAL
99	Management	Switch/router management, firewall admin	NORMAL

Key fact: The POS terminals (VLAN 40) must reach the Payment Gateway (VLAN 10) to process any transaction. If traffic between VLAN 40 and VLAN 10 is blocked — for any reason — every card reader in the airport goes dark.

3. INITIAL INTELLIGENCE — THREE THEORIES

Your IT team has gathered the following preliminary information. Three theories are on the table. Each has supporting evidence. Only one is correct. You need to figure out which.

THEORY A: EXTERNAL CYBERATTACK	
The outage is surgical and simultaneous. It hit a specific VLAN pair. The pattern — Retail VLAN severed from Server VLAN — is consistent with a targeted denial-of-service or firewall manipulation attack. If someone gained access to the firewall management interface, they could create a rule that blocks specific VLAN traffic without touching anything else.	**Supporting Evidence:** • The POS vendor (RetailLink) reported "unusual API query patterns" against their cloud management portal from an unrecognized IP address yesterday afternoon. • The SIEM logged 3 failed SSH login attempts against the firewall management IP (10.1.99.1) last night between 2:00 and 2:15 AM from external IP 185.220.101.34. • The outage is too precise to be a random hardware failure.

THEORY B: VENDOR COMPROMISE (SUPPLY CHAIN)	
RetailLink — the SaaS vendor that manages remote configuration for all 47 POS terminals — pushed a firmware update to all terminals at 9:30 AM this morning. If that update was corrupted or compromised, it could have bricked the terminals' ability to reach the gateway.	**Supporting Evidence:** • RetailLink confirmed they pushed a scheduled firmware update at 9:30 AM. • The outage started 17 minutes after the update (9:47 AM). • The terminals themselves are online — they just can't reach the gateway. Could a misconfigured update have changed the default gateway or DNS settings on the terminals?

THEORY C: INTERNAL SYSTEM ERROR	
An authorized change to the firewall or network infrastructure — a routine maintenance action — may have unintentionally blocked the wrong traffic. This would explain the surgical precision of the outage: it's not an attack, it's a mistake.	**Supporting Evidence:** • IT's change management log shows a firewall rule change was executed at 9:45 AM this morning — two minutes before the outage. • The change was listed as: "Block inbound traffic from known malicious IP range 185.220.0.0/16 per threat intel advisory TI-2026-0312." • A routine threat mitigation rule shouldn't affect internal VLAN traffic... unless it was written wrong.

4. TEAM ASSIGNMENTS & STANDING ORDERS

TEAM A: AIRPORT OPERATIONS (COMMAND)	
Role: 47 retail tenants can't process card transactions. Passengers are standing in lines with no way to pay. Airlines are reporting check-in kiosk failures. You need to manage the operational fallout while IT figures out the cause.	**Standing Orders:** Triage: Which systems are down and what's the passenger impact? Communicate: Tenant liaison, airline ops, passenger messaging. Cash Ops: Coordinate with tenants on cash-only procedures and ATM availability.

TEAM B: IT & CYBERSECURITY (LEAD — YOUR INVESTIGATION)	
Role: Three theories. One answer. The evidence is in the firewall logs, the SIEM, the change management system, the vendor communication, and the network traffic data. You need to eliminate two theories and confirm one. Then you need to fix it.	**Standing Orders:** Investigate: Firewall rule analysis, SIEM log review, vendor contact, change log audit. Contain: If it's an attack, isolate. If it's a vendor issue, roll back. If it's internal, revert. Communicate: Keep the room informed. Don't disappear into the logs — translate for the non-IT teams.

TEAM C: PUBLIC INFORMATION (PIO)	
Role: Passengers are already posting on social media: "NCIA card readers down — can't buy coffee." One person has tweeted "Are we under cyberattack??" You don't know the answer yet. You need to say something without saying the wrong thing.	**Standing Orders:** Monitor: Track social media in real time. Draft: Prepare statements for three scenarios (attack, vendor failure, internal error). Hold: Do NOT confirm a cyberattack until IT has confirmed it. Premature disclosure is irreversible.

TEAM D: SECURITY, LEGAL & COMPLIANCE	
Role: If this is a cyberattack, PCI-DSS notification requirements may be triggered. TSA may need to be informed depending on scope. If payment card data was compromised, the state Attorney General's office has a 72-hour notification window. But if it's NOT an attack... none of that applies. You need to be ready for both.	**Standing Orders:** Assess: Is there any indication that payment card data was accessed or exfiltrated? Standby: Prepare notification templates for TSA, PCI council, state AG — but do NOT send. Coordinate: If law enforcement is needed, what's the trigger?

5. RULES OF ENGAGEMENT

- **"This is an Exercise":** Begin and end all simulated communications with this phrase.
- **Real-World Emergencies:** Use **"REAL WORLD — REAL WORLD"** to halt.
- **This Is a Whodunit:** Three theories. One answer. Red herrings are real. Some evidence will point you in the wrong direction. Your job is to follow the data — not your gut.
- **Two Clocks Running:** You are simultaneously investigating the cause AND managing the operational impact. Every minute the POS terminals are down costs the tenants money and the airport credibility. The investigation matters, but the passengers don't care why it's broken — they care that it's fixed.
- **Don't Jump to Conclusions:** If you declare this a cyberattack and you're wrong, the consequences are severe: unnecessary breach notifications, stock panic if NCIA is publicly traded, loss of vendor and airline confidence, and media embarrassment. If you declare it an internal error and you're wrong, a real attacker continues operating on your network. Get it right before you commit.

6. INVESTIGATION WORKSHEET

THEORY TRACKER

Theory	Supporting Evidence	Contradicting Evidence	Status
A: External Cyberattack			■ Active ■ Eliminated
B: Vendor Compromise			■ Active ■ Eliminated
C: Internal Error			■ Active ■ Eliminated

TIMELINE

09:30 — RetailLink pushes firmware update to POS terminals
09:45 — Firewall rule change executed by IT (Change #CM-2026-0087)
09:47 — POS terminals lose connectivity to payment gateway
09:48 — FIDS displays in Concourse B food court go dark
09:50 — Gate management terminals report intermittent connectivity
09:52 — First tenant calls AOC to report POS failure

Continue building the timeline as you receive new information...