KRIZIA TECHNOLOGIES

Enterprise Cloud & SAP Migration Services

From Factory Floor to the Cloud. SAP S/4HANA on AWS with Multi-Firewall Security & DR.

A confidential automotive manufacturer moved SAP ECC to S/4HANA on AWS — keeping Check Point and FortiGate in the loop, with a cross-region disaster recovery site.

Document	End-to-End Case Study & Delivery Process
Prepared by	Indresh Pratap Singh, Krizia Technologies
Year	2026
Scope	SAP S/4HANA on AWS · Check Point + FortiGate · DR
Confidentiality	Customer case study anonymized

Email: contact@krizia.in · Web: www.krizia.in · WhatsApp: +91-93197-07938

KRIZIA TECHNOLOGIES

From Factory Floor to the Cloud. SAP S/4HANA on AWS with Multi-Firewall Security & DR.

A confidential automotive manufacturer moved SAP ECC to S/4HANA on AWS — keeping Check Point and FortiGate in the loop, with a cross-region disaster recovery site.

SAP S/4HANA on AWS · Multi-Firewall (Check Point + FortiGate) · Disaster Recovery · 2026

Why Move a Hybrid SAP Landscape to the Cloud

Our customer is a confidential **automotive manufacturer with two production plants**. For 14 years they ran **SAP ECC 6.0** entirely on-premises — SAP GUI clients, SAP MII shop-floor integration, and a mix of legacy interfaces talking to Oracle EBS and their MES/SCADA systems. Security at the edge was handled by two different firewall vendors: a **Check Point cluster** for the north-south perimeter and a **FortiGate HA pair** for east-west traffic between the office network and the plant IT/OT segments.

The decision to move was driven by four pressures:

- **SAP ECC 6.0 end-of-support deadline** (December 2027) approaching fast
- **Disaster recovery meant a tape backup** in another building — RPO of 8 hours, no testable failover
- A factory that runs 6 days a week — even one lost production day costs roughly **$50,000**
- No cloud skills in-house; the entire IT team was three people

This document shows the **before and after architecture** — and the two real incidents we solved during and after the migration, exactly as they happened.

> **The hard part was not the migration itself.** It was keeping two firewall ecosystems, plant OT traffic, and a future DR site working together — without ever stopping the factory.

Before the Cloud — The On-Premises Landscape

Before any cloud work, the entire SAP landscape lived inside the corporate data centre. SAP GUI and Fiori clients reached SAP ECC through the **Check Point perimeter**, while the shop floor connected through **FortiGate** into MES and SCADA. Every plant talked to head office over **MPLS**, with 45–180 ms latency between sites.

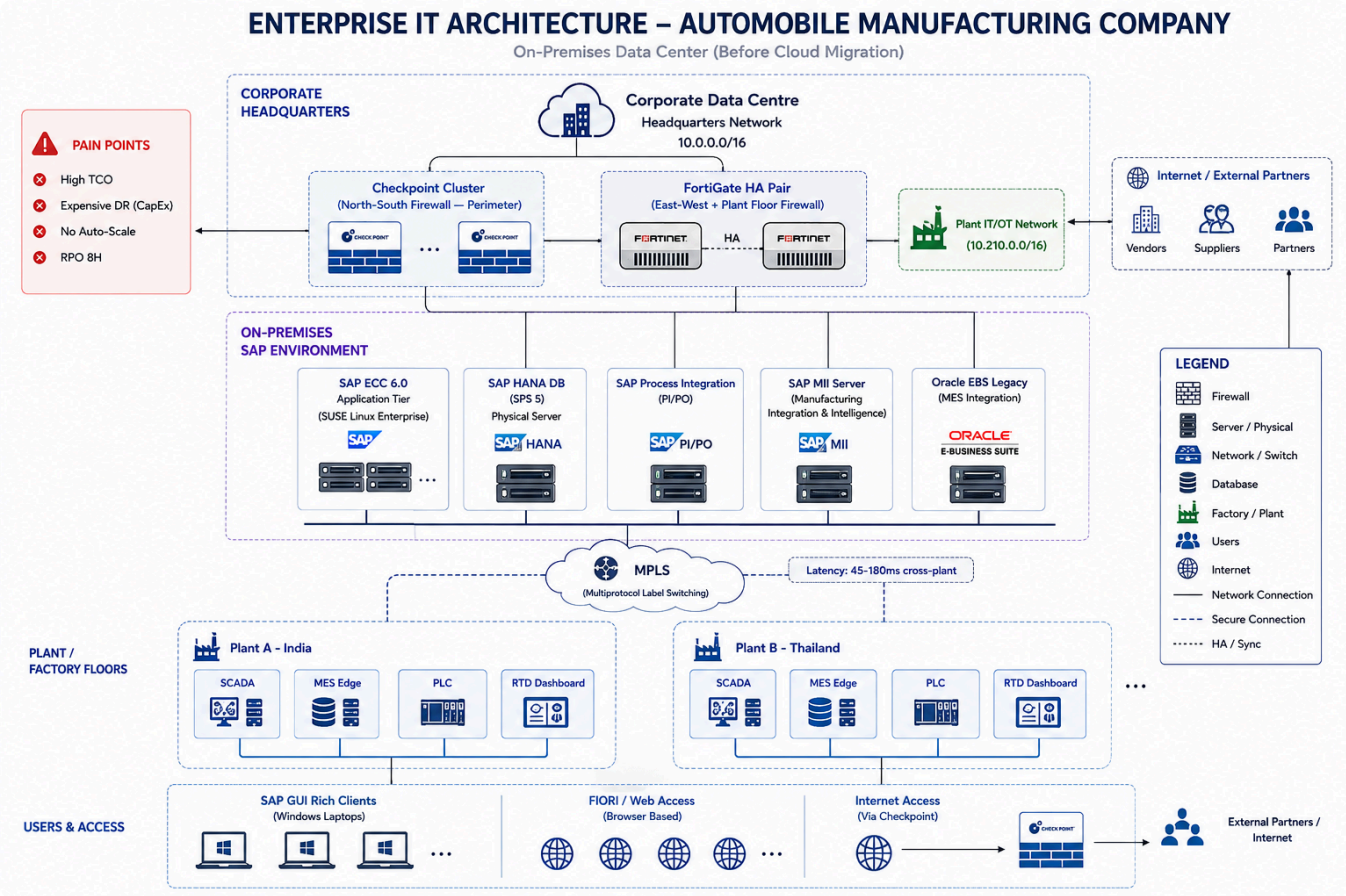

Figure 1 — On-premises SAP ECC 6.0 landscape: Check Point north-south firewall, FortiGate east-west segmentation, and MPLS-connected plants.

- **Check Point cluster:** internet / partner perimeter, HTTPS inspection enabled
- **FortiGate HA pair:** office ↔ plant IT/OT segmentation (10.210.0.0/16)
- SAP ECC 6.0 + SAP PI/PO + SAP MII, HANA database on physical servers
- MPLS WAN between Plant A and Plant B
- **DR = tape backup.** RPO 8 hours, RTO unmeasured

> **Every layer worked — but none of it could fail over.** The real risk was not a hardware failure; it was a site-level disaster with no testable recovery path.

Our Plan — Hybrid, Not Rip-and-Replace

We did not propose a full rip-and-replace. The plants, the OT segment, and the two firewall ecosystems were serving the business well. Our recommendation was a **hybrid model**:

- **SAP ECC 6.0 → SAP S/4HANA on AWS** (eu-west-1) via brownfield conversion, preserving all 14 years of data
- **Check Point and FortiGate stay in place** at the edge — the cloud connects to them, not around them
- Primary connectivity: **AWS Direct Connect 10 Gbps**. Backup: site-to-site IPSec VPN 1 Gbps

- **Transit Gateway hub** to connect the SAP VPC, shared-services VPC, and the DR region
- Cross-region **DR (eu-central-1) with HANA System Replication** — RPO 15 min, RTO 1 hour
- Plant OT traffic stays on-prem and reaches SAP through the firewall estate — controlled and audited

> **The key architectural decision:** cloud adoption must not create a firewall bypass. Every route from plant to cloud still crosses either Check Point or FortiGate, so the security team keeps full visibility.

After the Cloud — The New Hybrid Landscape

Post-migration, SAP S/4HANA runs in **AWS eu-west-1** with the DR copy in **eu-central-1**. The on-premises footprint shrank to the plant OT layer and the firewall estate. Direct Connect and the VPN feed into a **Transit Gateway**, which attaches the SAP VPC, shared services, and the DR VPC. HANA System Replication keeps the DR region warm at RPO 15 minutes.

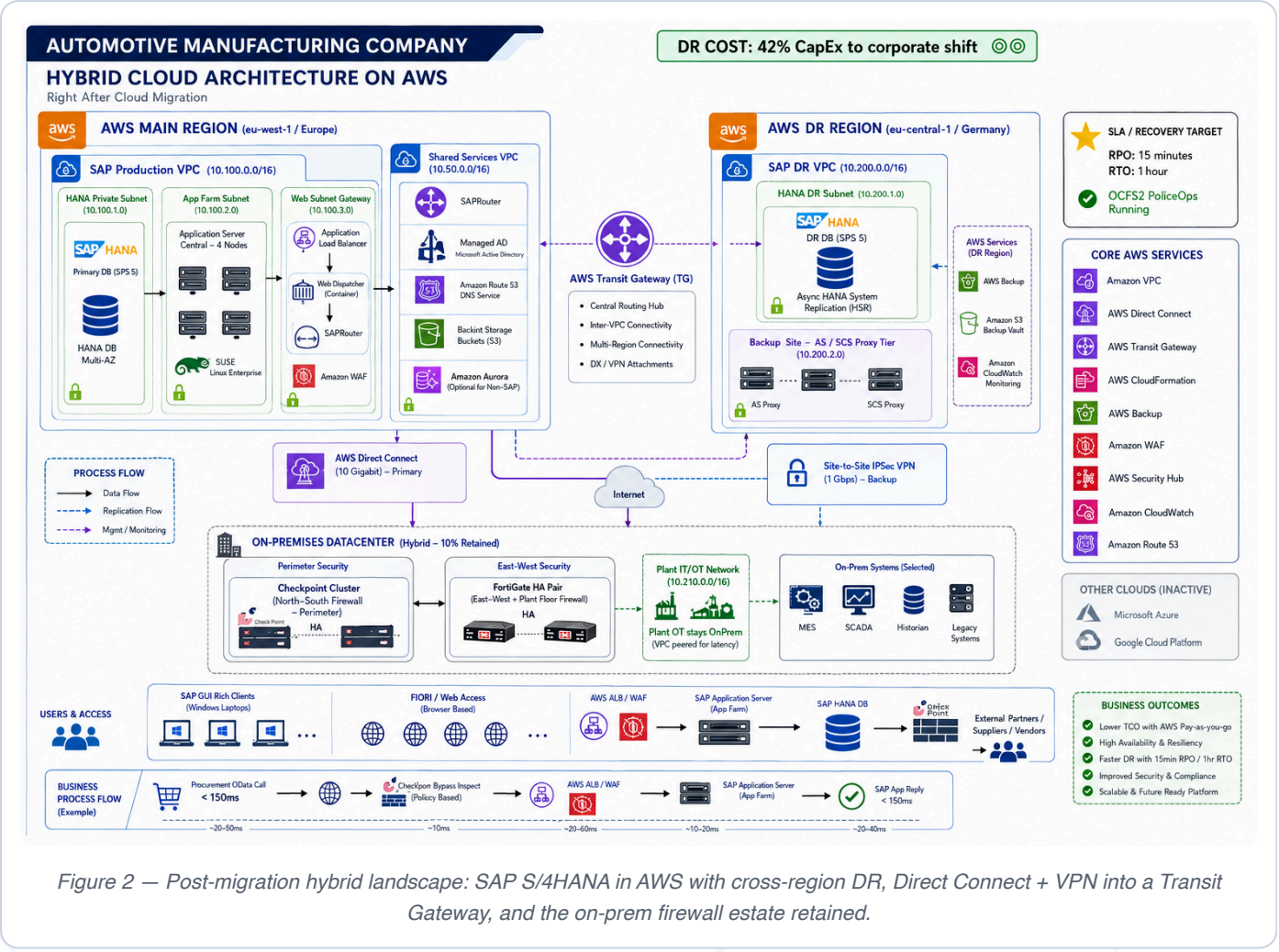

Figure 2 — Post-migration hybrid landscape: SAP S/4HANA in AWS with cross-region DR, Direct Connect + VPN into a Transit Gateway, and the on-prem firewall estate retained.

- **SAP Production VPC (10.100.0.0/16):** HANA, App Servers, Web Dispatcher, ALB
- **Shared Services VPC (10.50.0.0/16):** SAP Router, AD/DNS, backup buckets
- **DR VPC (eu-central-1, 10.200.0.0/16):** HANA standby via async System Replication
- **Transit Gateway hub:** DX + VPN attachments, VPC-to-VPC routing
- On-prem: Check Point + FortiGate retained, now terminating Direct Connect/VPN

Case Study — Two Real Incidents We Solved

> *"Everyone told us the cloud would be simpler. Nobody told us the firewall rules would be the hardest part. Krizia kept both our Check Point and FortiGate in the loop — and when things broke, they found the root cause in hours, not weeks." — **Program Lead, confidential automotive manufacturer (name changed for confidentiality)***

📌 Incident #1 — SAP OData Timeouts at the Check Point

Three weeks after go-live, the procurement team reported a repeating failure: SAP MII transactions to the legacy order system returned **"Connection to partner broken"** after roughly five minutes. OData calls from SAP to the Oracle EBS API were timing out with **HTTP 503** — at exactly 120 seconds, every time.

🔍 Diagnosis

Ping and routing were fine — so this was not a network outage. The timing pattern (a flat 120-second timeout) pointed at an intermediary terminating the TLS session and holding the payload. That intermediary was the **Check Point perimeter cluster running HTTPS deep inspection**.

- **Rule 17:** source = SAP MII server, destination = Oracle EBS API, service = https, action = Inspect
- Each inspected OData request added **~2,500 ms** of certificate-validating latency on a chatty 244 KB XML payload
- The SAP app server hit its **ICM receive-timeout** before the response arrived, and killed the session
- The result: 503s, "session aborted by server", and a blocked procure-to-pay process

🛠️ Fix

We created a **precise bypass rule** for this one integration — not a broad inspection exemption. Only the SAP MII server → Oracle EBS API HTTPS flow moved from "Inspect" to "Bypass", after the security team approved the exception and confirmed the endpoint was a trusted internal API.

Before	After
HTTPS deep inspection on MII → EBS API flow	Targeted bypass rule for MII → EBS API only
~2,500 ms added latency per OData call	18 ms handshake; requests complete in normal time
120-second ICM timeout aborts the session	No more 503s; procure-to-pay restored
All other inspection rules untouched	All other inspection rules untouched

> **SLA result:** 55 minutes to detect, ~1 hour to root-cause, 35 minutes to fix. Total restore time under 2 hours 30 minutes — within the agreed 99.95% availability target.

📌 Incident #2 — Asymmetric Routing Breaks DR Failover

During the first full disaster-recovery drill, HANA replication itself was healthy — but the **DR application tier could not be reached**. Plant users could ping the DR SAP instance (ICMP worked) yet TCP connections never completed. This is the classic signature of **asymmetric routing**.

🔍 Diagnosis

The forward path (plant → FortiGate → Direct Connect → Transit Gateway → DR VPC) used the primary 10 Gbps Direct Connect route. But the **return path** from the DR VPC was routed back over the backup IPSec tunnel —

which the FortiGate treated as a lower-priority but still valid path. TCP SYN travelled one way, SYN-ACK the other: **sessions never established**.

- FortiGate routing table: 10.200.0.0/16 reachable via BOTH Direct Connect and the IPSec backup tunnel
- **SD-WAN member priority was not pinned** for DR VPC destinations — the VPN won the return path
- Check: "get router info routing-table bgp" showed the wrong next-hop preference
- Fix location: FortiGate SD-WAN member priority + destination-based routing policy

🛠️ Fix

We pinned the DR VPC route to the **Direct Connect interface as priority 1**, demoted the IPSec tunnel to priority 10 for that destination, and added a **destination-based routing policy** so 10.200.0.0/16 always egresses the Direct Connect interface. The asymmetric path disappeared immediately.

Layer	Change
SD-WAN members	DC_eng1 (Direct Connect) set priority 1 for 10.200.0.0/16
SD-WAN members	Vpn_Backup demoted to priority 10 for the same destination
Destination policy	10.200.0.0/16 always routes out Direct Connect interface
Verification	BGP table re-checked; TCP 3-way handshake completes on both paths

> **Lesson codified into every future build:** whenever two redundant paths exist to the same destination, pin the preferred path per destination. Do not rely on priority alone — verify with a full TCP handshake test, not just ICMP.

The Results — Measured After 6 Months

15 min	1 hr	0	~40%	99.95%
RPO — cross-region DR	RTO — tested in live drill	Lost production days	Lower DR cost vs. physical site	Availability maintained

> **Program lead, post-drill review:** "The two firewall vendors are still on the network diagram — exactly where they should be. The difference is that the system they protect can now survive a site-level disaster and restore in under an hour."

Lessons for Your Migration

Lesson	Takeaway
Inspection breaks chatty APIs	Audit HTTPS inspection rules for every long-running integration before go-live; use targeted bypasses, not broad exemptions.
Two paths = asymmetric risk	Pin preferred routes per destination whenever redundant connectivity exists; test with TCP, not ping.
DR is only real after a drill	Schedule failover drills quarterly — the first drill is where the real problems surface.
Firewall estate is an asset	Keep existing security tools in the loop for hybrid traffic; cloud adoption should not bypass the perimeter.

Sizing must come from data	HANA sizing from real database metrics, not rule-of-thumb — it is what keeps the bill honest.

Ready to start your journey? Every engagement begins with a **free, no-obligation assessment**. Contact Krizia Technologies to book yours — and let's design your hybrid SAP journey the same way: one accountable partner, end to end.

Let’s Solve Your Problem Together

Every engagement starts with a **free, no-obligation assessment**. We will tell you exactly where you stand, what needs to change, and what it will cost.

Krizia Technologies

Enterprise Cloud & SAP Migration Services

Email: contact@krizia.in

Web: www.krizia.in

WhatsApp: +91-93197-07938

Prepared by Indresh Pratap Singh