Incident INC-20847 — IPsec Phase 2 DOWN

Tunnel HQ ↔ Berlin · fw-ber-01 · 23. Juni 2026

Incident-ID	INC-20847	**Schweregrad**	**KRITISCH**
Erkannt	23.06.2026 · 14:02:11 CEST	**Status**	**GESCHLOSSEN**
Quittiert	23.06.2026 · 14:05:02 CEST	**MTTD**	12 Sekunden
Recovery	23.06.2026 · 14:11:39 CEST	**MTTR**	9 min 28 s
Operator	M. K. (Bereitschaft NOC)	**Tenant**	Kunde A · DE-Süd
Quelle	BCSO Health-Check Engine v0.9	**Auto-Recovery**	Ja

Zusammenfassung

Am 23.06.2026 um 14:02:11 CEST meldete die BCSO Health-Check Engine den IPsec-Tunnel **„HQ-Berlin“** auf der Firewall **fw-ber-01** (pfSense+ 24.03) nach drei aufeinanderfolgenden negativen Polls als **DOWN**. Auslöser war ein temporärer WAN-Latenz-Spike (Ø 22 ms → 78 ms) verbunden mit einer Routen-Änderung des Carriers über AS3320. Der Tunnel re-etablierte sich nach erneuter Phase-2-Aushandlung selbstständig um 14:11:39 CEST. Es gab keine SLA-Verletzung und keinen Vor-Ort-Einsatz.

Betroffene Systeme

System	Typ	Rolle	Auswirkung
fw-ber-01	pfSense+ 24.03	Branch-Firewall Berlin	Tunnel-Endpunkt DOWN
fw-hq-01	OPNsense 24.7	Headquarter-Firewall (MASTER)	Tunnel-Gegenstelle
IPsec „HQ-Berlin“	Site-to-Site VPN	Produktionsverkehr DE-Süd ↔ HQ	Vollständiger Ausfall 9 m 28 s
WAN-Uplink Berlin	Carrier AS3320	Internet-Anbindung	Latenz-Spike + Routen-Wechsel

Timeline (Ereignis-Verlauf)

Zeit (CEST)	Ereignis	Quelle
14:02:11	Alert ausgelöst: IPsec Phase 2 DOWN nach 3 negativen Polls (Anti-Flapping aktiv).	Health-Check Engine
14:02:12	Eskalation Stufe 1: Teams #noc-alerts, E-Mail an Bereitschaft. SMS-Trigger gesetzt (T+5 m).	Notification-Router
14:03:47	Kontext beigefügt: WAN-Latenz fw-ber-01 seit 13:58 auf 78 ms (Baseline 22 ms). BGP-Route über AS3320.	Time-Series + Topology
14:05:02	Quittiert durch Operator M. K. · Ticket #INC-20847 eröffnet. Maintenance-Window nicht aktiv.	RBAC / Audit-Log

14:08:13	Automatischer Re-Init der Phase 1 nach Backoff-Window. Phase 2 noch nicht etabliert.	API-Connector pfSense
14:11:39	Recovery: Tunnel UP, Re-Key erfolgreich. Health-Check grün. Alert automatisch geschlossen.	Health-Check Engine
14:12:04	Post-Incident-Report generiert und an Tenant-Verteiler ausgeliefert.	BCSO Reporting

Ursachenanalyse (Root Cause)

Die Ursache lag nicht auf den beteiligten Firewalls, sondern auf der WAN-Strecke. Ein Routen-Wechsel des Carriers (AS3320) führte zu einem kurzzeitigen Anstieg der Round-Trip-Time auf 78 ms. In Folge schlugen drei aufeinanderfolgende IKE-Keepalives fehl, woraufhin pfSense die Security-Association abbaute. Der ausgehende Dead-Peer-Detection-Timer wurde anschließend regulär neu ausgehandelt.

Klassifikation: externe Ursache (Carrier-Routing) · keine Fehlkonfiguration auf BCSO-verwalteten Systemen festgestellt.

Kennzahlen (24-Stunden-Fenster)

Health-Checks ausgeführt	**24.812**
Davon abgewiesen (Anti-Flapping)	**47**
Alerts ausgelöst (alle Schweregrade)	**3**
Automatisch recovered	**2**
Eskaliert an Operator	**1**
SLA-Verletzungen	**0**
Mean Time to Detect (MTTD)	**12 Sekunden**
Mean Time to Resolve (MTTR)	**9 Minuten 28 Sekunden**

Handlungsempfehlungen

Priorität	Maßnahme	Beschreibung
Sofort	Korrelations-Alert anlegen	Kombi-Trigger „WAN-Latenz > 60 ms UND IPsec-Down“ als Provider-Eskalation klassifizieren — verhindert Operator-Eskalation bei externer Ursache.
Sofort	DPD-Timer verkürzen	Dead-Peer-Detection auf fw-ber-01 von 30 s auf 15 s setzen, damit Re-Key-Aushandlung früher startet.
Kurzfristig	Zweite WAN-Strecke evaluieren	Failover-Uplink über alternativen Carrier prüfen — eliminiert die Single-Source-Abhängigkeit von AS3320.
Kurzfristig	Reporting an Carrier	Latenz-Spike + Routen-Change als Ticket an Carrier-NOC, Referenz Zeitfenster 13:58–14:12 CEST.
Mittelfristig	Synthetic-Monitoring	End-to-End-Probe (ICMP + TCP/443) aus Berlin-Standort gegen HQ-Service einrichten — misst Anwender-Erlebnis statt nur Tunnel-Status.
Dokumentation	Runbook aktualisieren	Runbook RB-IPSEC-007 um Carrier-Routing-Szenario ergänzen, inkl. Eskalationspfad an Provider statt interner Bereitschaft.

Audit & Compliance

Sämtliche Ereignisse dieses Incidents wurden append-only im BCSO-Audit-Log persistiert (Hash-Kette, manipulationssicher). Der Vorgang erfüllt die Dokumentations-Anforderungen nach NIS2 Art. 21 („Vorfallbehandlung“) sowie ISO/IEC 27035. Keine personenbezogenen Daten von Endnutzern wurden verarbeitet — der Tunnel-Ausfall betraf ausschließlich Infrastruktur-Telemetrie.