IPSec-Tunnel-Flap zwischen sicherem Zugriff und in Azure/AWS gehosteten C8000Vs

Inhalt

Problem

IPsec-Netzwerktunnel zwischen C8000V-/Cisco IOS-XE-Routern und dem Cisco Secure Access-Netzwerk in der Region "us-east-2" flattern.

Alle Tunnelgruppen sind betroffen, sodass Tunnel zwischen den Routern vor Ort und dem Cisco Secure Access-Netzwerk nicht verfügbar sind.

Umwelt

- Technologie: Solution Support (SSPT - Vertrag erforderlich)
- Subtechnologie: Sicherer Zugriff - Netzwerktunnel (IPSEC, Site-to-Site, private Ressource)
- Produktfamilie: SECACCS
- Router: C8000V/Cisco IOS-XE-Router (vor Ort)
- Remote-Endgerät: Cisco Secure Access-Netzwerk (Region "us-east-2")
- Softwareversion: Nicht angegeben
- Fehlermeldungen, Protokolle, erkannte Debugging-Fehler
- Keine Auswirkungen auf Endbenutzer während des Ausfalls

Auflösung

Von CNHE Splunk Logs

Port = 1409

sourceIpAddr = x.x.x.x

Port = 1408

sourceIpAddr = x.x.x.x

1. Remote-Endpunktänderung wurde erkannt (Port wurde aktualisiert)
2. Cortex löst bei diesem Update den Kinderrekey aus
3. Keine Reaktion des Clients auf Neuschlüsseln mit neuem Port, sodass Cortex Wiederholungsversuche erschöpft und den Tunnel beendet
4. Kurz nach Neuinitiierung durch den Client über neuen Port, an dem der Tunnel gestartet wird

Aus CSA-Splunk-Protokollen.

2026-02-02T16:36:02.188+00:00 Auslösen von Child-rekey für IKE-Update mit lokaler IP: x.x.x.x, ike_spi:new_datanode:

2026-02-02T16:36:04.2027+00:00 Erneutes Senden von 1 Anforderung mit der Nachrichten-ID 0

2026-02-02T16:36:08.2027+00:00 Erneutes Übertragen von 2 der Anforderung mit der Nachrichten-ID 0

2026-02-02T16:36:16.2027+00:00 Erneutes Übertragen von 3 der Anforderung mit der Nachrichten-ID 0

2026-02-02T16:36:32.2027+00:00 Erneutes Übertragen von 4 der Anforderung mit der Nachrichten-ID 0

2026-02-02T16:37:04.2027+00:00 Erneutes Übertragen von 5 der Anforderung mit der Nachrichten-ID 0

2026-02-02T16:38:08.2008+00:00 Aufgeben nach 5 Neuübertragungen

2026-02-02T16:38:08.2028+00:00 IKE beenden, Child SA-Schlüssel fehlgeschlagen

Aus dem Debug-Protokoll 1769305781091_vJY_CENTRAL_R2.log:

Ungültige SPI-Fehler - treten sehr häufig auf:

*Jan 24 07:55:04.2009: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC-Paket hat ungültigen SPI für destaddr=x.x.x.x port=50, spi=, srcaddr=x.x.x.x, Eingabe interface=Tunnel12

*Jan 24 07:56:06.829: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC-Paket hat ungültigen SPI für destaddr=x.x.x.x, port=50, spi=, srcaddr=x.x.x.x, Eingabe interface=Tunnel11

Tunnel-Flapping - Mehrere Tunnelinstanzen nach unten/oben:

* Jan. 24 08:33:12.069: %LINEPROTO-5-UPDOWN: Leitungsprotokoll am Schnittstellentunnel12, Zustand geändert in "Down"

* Jan. 24 08:33:14.459: %LINEPROTO-5-UPDOWN: Leitungsprotokoll am Schnittstellentunnel11, Zustand geändert in "Down"

*Jan. 24 08:33:15.275: %LINEPROTO-5-UPDOWN: Leitungsprotokoll am Schnittstellentunnel11, Zustand geändert auf "up"

Ursache

Dies scheint ein fehlerhaftes Client-Problem zu sein, wenn der Port flattert.

Flapping scheint nach einer Änderung in Azure vorerst stabil zu sein.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.