Flap dei tunnel IPSec tra Secure Access e C8000Vs ospitati in Azure/AWS

Sommario

Problema

I tunnel di rete IPsec tra i router C800V / Cisco IOS-XE e la rete Cisco Secure Access nell'area U.S.A.-East-2 stanno lampeggiando.

Il problema interessa tutti i gruppi di tunnel e di conseguenza i tunnel non sono attivi tra i router locali e la rete Cisco Secure Access.

Ambiente

- Tecnologia: supporto per la soluzione (SPPT - contratto obbligatorio)
- Sottotecnologia: accesso sicuro - tunnel di rete (IPSEC, da sito a sito, risorsa privata)
- Famiglia di prodotti: SECACS
- Router: C800V / Cisco IOS-XE router (in sede)
- Endpoint remoto: rete Cisco Secure Access (regione us-east-2)
- Versione del software: non specificata
- Messaggi di errore, log, debug rilevati
- Nessun utente finale interessato durante l'interruzione

Risoluzione

Da registri Splunk CNHE

porta = 1409

sourceIpAddr = x.x.x.x

port = 1408

sourceIpAddr = x.x.x.x

1. È stata rilevata una modifica remota dell'endpoint (porta aggiornata)
2. Cortex attiva la reimpostazione della chiave figlio in questo aggiornamento
3. Nessuna risposta dal client alle richiavi tramite una nuova porta, quindi la cortex esaurirà i tentativi e terminerà il tunnel
4. Subito dopo il riavvio del client utilizzando una nuova porta in cui viene attivato il tunnel

Dai log Splunk CSA.

2026-02-02T16:36:02.188+00:00 attivazione della chiave figlio per l'aggiornamento di ike con IP locale: x.x.x.x, ike_spi:new_datanode:

2026-02-02T16:36:04.207+00:00 ritrasmette 1 richiesta con ID messaggio 0

2026-02-02T16:36:08.207+00:00 ritrasmette 2 della richiesta con ID messaggio 0

2026-02-02T16:36:16.207+00:00 ritrasmette 3 della richiesta con ID messaggio 0

2026-02-02T16:36:32.207+00:00 ritrasmette 4 della richiesta con ID messaggio 0

2026-02-02T16:37:04.207+00:00 ritrasmette 5 della richiesta con ID messaggio 0

2026-02-02T16:38:08.208+00:00 rinuncia dopo 5 ritrasmissioni

2026-02-02T16:38:08.208+00:00 terminazione di IKE. Reimpostazione chiave SA figlio non riuscita

Dal log di debug 1769305781091_vJY_CENTRAL_R2.log:

Errori SPI non validi - Si verificano molto di frequente:

*24 gen 07:55:04.209: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: pacchetto IPSEC registrato con spi non valido per destaddr=x.x.x.x.x prot=50, spi=, srcaddr=x.x.x.x, interfaccia di input=Tunnel12

*Gen 24 07:56:06.829: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: pacchetto IPSEC registrato con spi non valido per destaddr=x.x.x.x, prot=50, spi=, srcaddr=x.x.x.x, interfaccia di input=Tunnel11

Tunnel Flapping - Istanze multiple di tunnel che vanno verso l'alto o il basso:

*24 gen 08:33:12.069: %LINEPROTO-5-UPDOWN: protocollo di linea sul tunnel di interfaccia12, stato modificato in giù

*24 gen 08:33:14.459: %LINEPROTO-5-UPDOWN: protocollo di linea sul tunnel di interfaccia11, stato modificato in giù

*24 gen 08:33:15.275: %LINEPROTO-5-UPDOWN: protocollo di linea sul tunnel di interfaccia11, stato modificato su up

Causa

Questo sembra un problema del client difettoso se la porta lampeggia.

Dopo aver apportato una modifica in Azure, il flapping sembra per ora stabile.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).