Les tunnels IPSec basculent entre l'accès sécurisé et les C8000V hébergés dans Azure/AWS

Table des matières

Problème

Les tunnels réseau IPsec entre les routeurs C8000V / Cisco IOS-XE et le réseau d'accès sécurisé Cisco dans la région us-east-2 sont instables.

Tous les groupes de tunnels sont affectés, ce qui entraîne l'interruption des tunnels entre les routeurs sur site et le réseau d'accès sécurisé Cisco.

Environnement

- Technologie : Assistance pour les solutions (SSPT - contrat requis)
- Sous-technologie : accès sécurisé - tunnels réseau (IPSEC, site à site, ressource privée)
- Famille de produits : SECACS
- Routeurs : routeurs C8000V / Cisco IOS-XE (sur site)
- Terminal distant : réseau d'accès sécurisé Cisco (région us-east-2)
- Version du logiciel : non spécifiée
- Messages d'erreur, journaux, débogages observés
- Aucun utilisateur final affecté pendant la panne

Résolution

À partir des journaux Splunk CNHE

port = 1409

AdresseIPsource = x.x.x.x

port = 1408

AdresseIPsource = x.x.x.x

1. Modification du point de terminaison distant détectée (le port a été mis à jour)
2. Cortex déclenche une nouvelle clé enfant sur cette mise à jour
3. Aucune réponse du client sur les clés utilisant le nouveau port, de sorte que le cortex épuise les tentatives et termine le tunnel

4. Peu de temps après la réinitialisation du client en utilisant un nouveau port où le tunnel est activé

Provient des journaux de liaison Splunk CSA.

2026-02-02T16:36:02.188+00:00 déclenchement d'une nouvelle clé enfant pour mise à jour ike avec IP locale : x.x.x.x, ike_spi:new_datanode:

2026-02-02T16:36:04.207+00:00 retransmettre 1 de la requête avec l'ID de message 0

2026-02-02T16:36:08.207+00:00 retransmettre 2 de la requête avec l'ID de message 0

2026-02-02T16:36:16.207+00:00 retransmettre 3 de la requête avec l'ID de message 0

2026-02-02T16:36:32.207+00:00 retransmettre 4 de la requête avec l'ID de message 0

2026-02-02T16:37:04.207+00:00 retransmettre 5 de la requête avec l'ID de message 0

2026-02-02T16:38:08.208+00:00 abandon après 5 retransmissions

2026-02-02T16:38:08.208+00:00 terminaison IKE, échec de la nouvelle clé de l'association de sécurité enfant

À partir du journal de débogage 1769305781091_vJY_CENTRAL_R2.log :

Erreurs SPI non valides - Se produisant très fréquemment :

*Jan 24 07:55:04.209: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps : le paquet IPSEC reçu a un spi non valide pour destaddr=x.x.x.x port=50, spi=, srcaddr=x.x.x.x, input interface=Tunnel12

*Jan 24 07:56:06.829: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps : le paquet IPSEC reçu a un spi non valide pour destaddr=x.x.x.x, port=50, spi=, srcaddr=x.x.x.x, input interface=Tunnel11

Blocage de tunnel : plusieurs instances de tunnels descendant/montant :

*Jan 24 08:33:12.069: %LINEPROTO-5-UPDOWN: Protocole de ligne sur l'interface Tunnel12, état modifié en down

*Jan 24 08:33:14.459: %LINEPROTO-5-UPDOWN: Protocole de ligne sur l'interface Tunnel11, état modifié en down

*Jan 24 08:33:15.275: %LINEPROTO-5-UPDOWN: Protocole de ligne sur l'interface Tunnel11, état modifié à up

Motif

Cela semble être un problème de client instable si leur port est instable.

Le battement semble être stable pour l'instant après avoir effectué un changement dans Azure.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.