IPSec-tunnelflap tussen beveiligde toegang en C8000V's gehost in Azure/AWS

Inhoud

uitgeven

IPsec-netwerktunnels tussen C8000V / Cisco IOS-XE-routers en het Cisco Secure Access-netwerk in de regio US-East-2 zijn aan het flapperen.

Alle tunnelgroepen worden getroffen, waardoor tunnels worden afgesloten tussen de on-premise routers en het Cisco Secure Access-netwerk.

milieu

- Technologie: oplossingsondersteuning (SSPT - contract vereist)
- Subtechnologie: beveiligde toegang - netwerktunnels (IPSEC, site-to-site, private resource)
- Productfamilie: SECACS
- Routers: C8000V / Cisco IOS-XE-routers (on-premise)
- Extern eindpunt: Cisco Secure Access-netwerk (regio us-east-2)
- Softwareversie: niet opgegeven
- Foutberichten, logbestanden, foutopsporingen waargenomen
- Geen eindgebruikers getroffen tijdens de storing

resolutie

Van CNHE Splunk Logs

Poort = 1409

sourceIpAdr = x.x.x.x

Poort = 1408

sourceIpAdr = x.x.x.x

1. Verandering van extern eindpunt werd gedetecteerd (poort werd bijgewerkt)
2. Cortex triggert kindersleutel bij deze update
3. Geen reactie van client op rekeys met behulp van nieuwe poort, zodat cortex uitput en de tunnel opnieuw probeert te beëindigen
4. Kort na de herstart van de client met behulp van een nieuwe poort waar de tunnel komt

Van CSA Splunk logs.

2026-02-02T16:36:02.188+00:00 activeren van child rekey voor ike-update met lokale IP: x.x.x.x, ike_spi: new_datanode:

2026-02-02T16:36:04.207+00:00 opnieuw verzenden 1 van verzoek met bericht-ID 0

2026-02-02T16:36:08.207+00:00 opnieuw verzenden 2 van verzoek met bericht-ID 0

2026-02-02T16:36:16.207+00:00 opnieuw verzenden 3 van verzoek met bericht-ID 0

2026-02-02T16:36:32.207+00:00 opnieuw verzenden 4 van verzoek met bericht-ID 0

2026-02-02T16:37:04.207+00:00 opnieuw verzenden 5 van verzoek met bericht-ID 0

2026-02-02T16:38:08.208+00:00 opgeven na 5 heruitzendingen

2026-02-02T16:38:08.208+00:00 beëindigen IKE, kind SA rekey mislukt

Van het debug log 1769305781091_vJY_CENTRAL_R2.log:

Ongeldige SPI-fouten - Zeer vaak optredend:

*Jan 24 07:55:04.209: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC pakket heeft ongeldige spi voor destaddr=x.x.x.x prot=50, spi=, srcaddr=x.x.x.x, input interface=Tunnel12

*Jan 24 07:56:06.829: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC pakket heeft ongeldige spi voor destaddr=x.x.x.x, prot=50, spi=, srcaddr=x.x.x.x, input interface=Tunnel11

Tunnel Flapping - Meerdere gevallen van tunnels naar beneden / omhoog:

*Jan 24 08:33:12.069: %LINEPROTO-5-UPDOWN: Lijnprotocol op Interface Tunnel12, status gewijzigd in down

*Jan 24 08:33:14.459: %LINEPROTO-5-UPDOWN: Lijnprotocol op Interface Tunnel11, status gewijzigd in down

*Jan 24 08:33:15.275: %LINEPROTO-5-UPDOWN: Lijnprotocol op Interface Tunnel11, status gewijzigd in up

Oorzaak

Dit lijkt een schilferig klantprobleem als hun poort flappert.

Flapping lijkt voorlopig stabiel te zijn na het maken van een verandering in Azure.

Verwante inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.