Túneles IPSec inestables entre Secure Access y C8000V alojados en Azure/AWS

Contenido

Problema

Los túneles de red IPsec entre los routers C8000V / Cisco IOS-XE y la red Cisco Secure Access en la región us-east-2 están inestables.

Afecta a todos los grupos de túneles, lo que provoca la caída de túneles entre los routers en las instalaciones y la red Cisco Secure Access.

Entorno

- Tecnología: Asistencia para soluciones (SSPT, contrato necesario)
- Subtecnología: Acceso seguro: túneles de red (IPSEC, de sitio a sitio, recurso privado)
- Familia de productos: SECACCS
- Routers: C8000V / routers Cisco IOS-XE (en las instalaciones)
- Terminal remoto: red Cisco Secure Access (us-east-2 region)
- Versión del software: no especificada
- Mensajes de error, registros, depuraciones observados
- Ningún usuario final afectado durante la interrupción

Resolución

Desde registros de Splunk CNHE

puerto = 1409

sourceIpAddr = x.x.x.x

puerto = 1408

sourceIpAddr = x.x.x.x

1. Se detectó un cambio en el terminal remoto (el puerto se actualizó)
2. Cortex activa la regeneración de claves secundarias en esta actualización
3. No hay respuesta del cliente en las regeneraciones de claves usando el nuevo puerto así que la corteza agota los reintentos y termina el túnel
4. Poco después del reinicio del cliente mediante un nuevo puerto donde aparece el túnel

Desde los registros de CSA Splunk.

2026-02-02T16:36:02.188+00:00 Activación de la regeneración de claves secundarias para la actualización de ike con IP local: x.x.x.x, ike_spi:new_datanode:

2026-02-02T16:36:04.207+00:00 retransmitir 1 solicitud con ID de mensaje 0

2026-02-02T16:36:08.207+00:00 retransmitir 2 de solicitud con ID de mensaje 0

2026-02-02T16:36:16.207+00:00 retransmitir 3 de solicitud con ID de mensaje 0

2026-02-02T16:36:32.207+00:00 retransmitir 4 de solicitud con ID de mensaje 0

2026-02-02T16:37:04.207+00:00 retransmitir 5 de solicitud con ID de mensaje 0

2026-02-02T16:38:08.208+00:00 renunciar después de 5 retransmisiones

2026-02-02T16:38:08.208+00:00 IKE de terminación, la regeneración de claves SA de hijo falló

Desde el registro de depuración 1769305781091_vJY_CENTRAL_R2.log:

Errores SPI no válidos: ocurren con mucha frecuencia:

*24 de enero de 2007:55:04.2009: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: el paquete IPSEC de rec'd tiene un spi no válido para destaddr=x.x.x.x prot=50, spi=, srcaddr=x.x.x.x, interfaz de entrada=Tunnel12

*24 de enero de 07:56:06.829: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: el paquete IPSEC de reconocimiento tiene un spi no válido para destaddr=x.x.x.x, port=50, spi=, srcaddr=x.x.x.x, interfaz de entrada=Tunnel11

Inestabilidad de túneles: varias instancias de túneles que se activan o desactivan:

*24 de enero 08:33:12.069: %LINEPROTO-5-UPDOWN: Protocolo de línea en el túnel de interfaz 12, estado cambiado a inactivo

*24 de enero 08:33:14.459: %LINEPROTO-5-UPDOWN: Protocolo de línea en el túnel de interfaz 11, estado cambiado a inactivo

*24 de enero 08:33:15.275: %LINEPROTO-5-UPDOWN: Protocolo de línea en el túnel de interfaz11, estado cambiado a activo

Causa

Esto parece ser un problema de cliente irregular si su puerto está inestable.

El aleteo parece ser estable por ahora después de hacer un cambio en Azure.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).