Inestabilidad intermitente de grupo de túnel de red de acceso seguro con gateway VPN de Azure durante eventos de regeneración de claves IKE

Contenido

Problema

Un grupo de túnel de red recién configurado entre Cisco Secure Access y Azure VPN Gateway experimenta intermitencia intermitente del túnel aproximadamente cada 4 horas durante los eventos de regeneración de claves IKE.

Se observan estos síntomas y mensajes de error específicos:

- Análisis BGP inactivo, temporizador de espera caducado
- Alerta: rekey IKE fallido
- Túnel IKE desconectado

La inestabilidad del túnel provoca interrupciones periódicas, errores de regeneración de claves IKE, errores de comprobación de integridad, desconexiones del túnel y caídas de iguales BGP, lo que afecta a la conectividad estable con los recursos de Azure. Los fallos de autenticación se observan durante las negociaciones de regeneración de claves.

Entorno

- Grupo de túnel de red de Cisco Secure Access (CSA) configurado en Azure VPN Gateway
- Túneles VPN de sitio a sitio IPsec que utilizan IKEv2
- Azure VPN Gateway con cifrado AES-GCM-256 configurado en políticas de modo principal

(MM)

- NAT-T (NAT transversal) habilitada en ambos lados mediante el puerto 4500
- Peering BGP configurado entre los puntos finales
- Duración de SA IKE predeterminada de 4 horas (28800 segundos)
- Configuración de duración inicial de SA IPsec, modificada posteriormente a 10800 segundos
- PFS (Confidencialidad directa perfecta) no habilitada en el lado de Azure

Resolución

El problema se resolvió mediante un cambio de configuración para evitar los cifrados AES-GCM en las políticas de modo principal, según la identificación de un error en el gateway VPN de Azure.

Paso 1: Azure VPN Gateway Debug Analysis

Las depuraciones IKE se recopilaron del lado de Azure VPN Gateway, lo que revela este comportamiento durante los intentos de regeneración de claves:

```
SESSION_ID :{} Remote x.x.x.x:500: Local x.x.x.x:500: [SEND]Sending IPSec policy Payload for tunnel Id
SESSION_ID :{} Remote x.x.x.x:4500: Local x.x.x.x:4500: [SEND][CHILD_SA MM_REKEY] Sending IKE rekey res
SESSION_ID :{} Remote x.x.x.x:4500: Local x.x.x.x:4500: [LOCAL_MSG] IKE Tunnel closed for tunnelId x3 w
```

Paso 2: Identificación de causa raíz

El soporte técnico de Azure investigó los errores de regeneración de claves. El análisis de Azure identificó que cuando Azure inicia un MM-REKEY usando AES-GCM-256, el paquete de regeneración de claves está mal formado. El dispositivo local no responde a la solicitud de regeneración de clave incorrecta, lo que provoca la desconexión del túnel.

Paso 3: Implementación de solución alternativa de configuración

Basándose en las recomendaciones de Azure, esta mitigación se implementó:

- Elimine los cifrados AES-GCM de las políticas de modo principal (MM) en la configuración del grupo de túnel de red.
- Configure métodos de encriptación alternativos que no utilicen el modo GCM.

Consulte el paso 17 en https://securitydocs.cisco.com/docs/csa/olh/121327.dita.

Paso 4: Opciones de mitigación alternativas

Azure también proporcionó estrategias de mitigación adicionales que se pueden considerar:

- Configure la duración de MM en las instalaciones para que sea superior a 28800 segundos, de modo que Azure siempre inicie rekey.
- Establezca Azure VPN Gateway en modo de solo respondedor con una duración de SA en las instalaciones menor que la de Azure.

Causa

La causa raíz es un error en la puerta de enlace VPN de Azure que afecta a las operaciones de regeneración de claves AES-GCM. Cuando Azure inicia un MM-REKEY mediante AES-GCM-256, el paquete de regeneración de claves está mal formado, lo que hace que el dispositivo Cisco Secure Access local no responda a la solicitud de regeneración de claves mal formada. Esto da lugar a fallas de regeneración de claves IKE, errores de autenticación y desconexiones subsiguientes del túnel.

Azure ha confirmado esto como un error existente y ha documentado una solución planeada en una futura versión de gateway prevista para mediados de 2026.

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).