Solución de Problemas de Registro Rechazado del Miembro del Grupo GETVPN para Incompatibilidad de SA Larga

Contenido

Introducción

Este documento describe cómo resolver el problema de rechazo del registro para la incompatibilidad de vida de larga duración de la Asociación de seguridad larga (SA) entre el servidor clave (KS) de red privada virtual de transporte cifrado de grupo (GETVPN) y miembro de grupo (GM).

Colaborado por Daniel Perez Vertti Vazquez, Ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- GETVPN
- Internet Security Association and Key Management Protocol (ISAKMP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- GMs que ejecutan una versión anterior a Internetwork Operating System (IOS) 15.3(2)T que no admiten la función de larga duración.
- GMs que ejecutan una versión anterior a IOS XE 15.3(2)S que no soportan la función de larga duración.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

La función Long SA lifetime se incluye en las plataformas IOS desde la versión 15.3(2)T y desde XE3.9 (15.3(2)S) en los dispositivos IOS XE. Permite prolongar la duración de las claves de cifrado del tráfico (TEK) y de cifrado de claves (KEK) de 24 horas a 30 días. Cuando la función Long SA lifetime se utiliza en el servidor de claves; esto es cuando la duración en la configuración de grupo GDOI ha cambiado a más de un día, GETVPN KS verifica la versión de software de todos los GM y bloquea el registro para aquellos que no soportan la función.

> **Nota:** El uso de Long of SA lifetime requiere encadenamiento de bloques con cifrado estándar avanzado (AES-CBC) o modo de contador/estándar de cifrado avanzado (AES-GCM) con una clave AES de 128 bits o más.

La función de larga duración SA se configura en el grupo de servidores de claves de dominio de interpretación de grupo (GDOI).

Los dispositivos pueden completar correctamente el túnel ISAKMP y autenticarse entre sí.

```
208752: Jun 10 22:19:14.380: ISAKMP-PAK: (82124):sending packet to 10.40.10.10 my_port 848
peer_port 848 (R) MM_KEY_EXCH
208753: Jun 10 22:19:14.380: ISAKMP: (82124):Sending an IKE IPv4 Packet.
208754: Jun 10 22:19:14.380: ISAKMP: (82124):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
208755: Jun 10 22:19:14.380: ISAKMP: (82124):Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE

208756: Jun 10 22:19:14.380: ISAKMP: (82124):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
208757: Jun 10 22:19:14.380: ISAKMP: (82124):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
```

Sin embargo, cuando GM intenta obtener claves de cifrado, KS detecta la versión del IOS en GM no incluye soporte de la función de duración de SA larga y genera un mensaje de error para cerrar la conexión.

```
208758: Jun 10 22:19:14.433: ISAKMP-PAK: (82124):received packet from 10.40.10.10 dport 848
sport 848 Global (R) GDOI_IDLE
208759: Jun 10 22:19:14.433: ISAKMP: (82124):set new node 1548686329 to GDOI_IDLE
208760: Jun 10 22:19:14.433: ISAKMP: (82124):processing HASH payload. message ID = 1548686329
208761: Jun 10 22:19:14.433: ISAKMP: (82124):processing NONCE payload. message ID = 1548686329
208762: Jun 10 22:19:14.433: ISAKMP: (82124):GDOI Container Payloads:
208763: Jun 10 22:19:14.433:    ID
208764: Jun 10 22:19:14.433: ISAKMP: (82124):Node 1548686329, Input = IKE_MESG_FROM_PEER,
IKE_GDOI_EXCH
208765: Jun 10 22:19:14.434: ISAKMP: (82124):Old State = IKE_KS_LISTEN  New State =
IKE_KS_GET_SA_POLICY_AWAIT
208766: Jun 10 22:19:14.434: ISAKMP: (82124):GDOI Container Payloads:
208767: Jun 10 22:19:14.434:    SA
208768: Jun 10 22:19:14.434: ISAKMP-ERROR: (82124):GDOI processing Failed: Deleting node
208769: Jun 10 22:19:14.434: ISAKMP-ERROR: (82124):deleting node 1548686329 error TRUE reason
"GDOI QM rejected - failed to process QM"
208770: Jun 10 22:19:21.280: %GDOI-4-REJECT_GM_VERSION_REGISTER: Reject registration of GM
10.40.10.10(ver 0x1000001) in group MYGETVPN as it cannot support these GETVPN features enabled:
Long-SA
```

GM intenta crear un nuevo túnel ISAKMP pero no puede finalizar con el proceso de registro. En este punto, puede observar varias instancias de la misma negociación.

```
Router# sh crypto isakmp sa | i 10.80.127.20
10.80.127.20    10.40.10.10     MM_NO_STATE       2104 ACTIVE (deleted)

Router#show crypto gdoi
GROUP INFORMATION

    Group Name               : MYGETVPN
    Group Identity           : 1
    Rekeys received          : 0
    IPSec SA Direction       : Inbound Only

     Group Server list       : 10.80.127.20

    Group member             : 10.40.10.10      vrf: None
       Registration status   : Registering
       Registering to        : 10.80.127.20
       Re-registers in       : 44 sec
       Succeeded registration: 0
       Attempted registration: 3
       Last rekey from       : 0.0.0.0
       Last rekey seq num    : 0
       Multicast rekey rcvd  : 0
       allowable rekey cipher: any
       allowable rekey hash  : any
       allowable transformtag: any ESP

    Rekeys cumulative
       Total received        : 0
       After latest register : 0
       Rekey Received        : never

 ACL Downloaded From KS UNKNOWN:
```

Para realizar una revisión adicional de la compatibilidad de funciones, ejecute el comando **show crypto gdoi feature long-sa-lifetime** en el KS. Este resultado muestra un ejemplo de dos GM, el primero ya ejecuta una imagen IOS con soporte para esta funcionalidad y el segundo es el GM afectado.

```
Router# sh cry gdoi feature long-sa-lifetime
Group Name: GETVPN_GROUP
    Key Server ID       Version   Feature Supported
        10.80.127.20      1.0.18         Yes

Group Member ID Version Feature Supported 10.40.10.9 1.0.17 Yes          10.40.10.10       1.0.4
No
```

Solución

- El problema se puede solucionar con una actualización del GM a IOS 15.3(2) o posterior. Se puede encontrar un mapping entre las versiones de GDOI y las versiones de IOS/IOS-XE en la Guía de Diseño de GETVPN.
- Una segunda solución alternativa puede cambiar la duración de la nueva clave en el grupo GDOI a menos de 86400 segundos. Este cambio de configuración no causa ninguna interrupción para los miembros del grupo de trabajo, ya que no activa ninguna tecla de

reinicio.