Dépannage de l'enregistrement rejeté d'un membre du groupe GETVPN pour l'incompatibilité de longue SA

Contenu

Introduction

Ce document décrit comment résoudre le problème de rejet d'inscription pour l'incompatibilité à vie de Long Security Association (SA) entre le serveur de clés (KS) Group Encrypted Transport Virtual Private Network (GETVPN) et le membre de groupe (GM).

Contribué par Daniel Perez Vertti Vazquez, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- GM exécutant une version antérieure à IOS (Internetwork Operating System) 15.3(2)T qui ne prend pas en charge la fonctionnalité longue durée de vie.
- GM exécutant une version antérieure à IOS XE 15.3(2)S qui ne prend pas en charge la fonctionnalité de durée de vie longue durée de vie.

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

La fonctionnalité Longue durée de vie de l'SA est incluse dans les plates-formes IOS depuis la version 15.3(2)T et XE3.9 (15.3(2)S) dans les périphériques IOS XE. Il permet de prolonger la durée de vie de la clé de cryptage du trafic (TEK) et de la clé de cryptage de clé (KEK) de 24 heures à 30 jours. Lorsque la fonction de durée de vie de l'association de sécurité longue durée est utilisée dans le serveur de clés ; C'est à ce moment que la durée de vie dans la configuration de groupe GDOI a été modifiée à plus d'un jour, GETVPN KS vérifie la version logicielle de tous les GM et bloque l'enregistrement pour ceux qui ne prennent pas en charge la fonctionnalité.

> **Note**: L'utilisation de la durée de vie de l'association de sécurité longue (Long of SA) nécessite le chaînage de blocs AES-CBC (Advanced Encryption Standard-Galois/Counter Mode) avec une clé AES de 128 bits ou plus.

La fonctionnalité de durée de vie de l'association de sécurité longue durée est configurée dans le groupe Domaine d'interprétation de groupe (GDOI) du serveur de clés.

Les périphériques peuvent terminer le tunnel ISAKMP et s'authentifier mutuellement.

```
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
```

Cependant, lorsque GM essaie d'obtenir des clés de chiffrement, KS détecte que la version IOS de GM n'inclut pas la prise en charge de la durée de vie de l'SA longue et génère un message d'erreur pour supprimer la connexion.

```
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 essaie de créer un nouveau tunnel ISAKMP mais n'est pas en mesure de finir avec le processus d'enregistrement. À ce stade, vous pouvez remarquer plusieurs instances de la même négociation.

```
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:
```

Pour effectuer un examen plus approfondi de la compatibilité des fonctionnalités, exécutez la commande **show crypto gdoi feature long-sa-life** dans le KS. Ce résultat montre un exemple de deux GM, le premier exécute déjà une image IOS avec la prise en charge de cette fonctionnalité et le second est le GM affecté.

```
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
```

Solution

- Le problème peut être résolu par une mise à niveau de la GM vers IOS 15.3(2) ou version ultérieure. Un mappage entre les versions GDOI et IOS/IOS-XE se trouve dans le guide de conception GETVPN.
- Une deuxième solution de contournement peut être de remplacer la durée de vie de la nouvelle clé dans le groupe GDOI par moins de 86 400 secondes. Cette modification de configuration ne perturbe pas les membres du groupe de travail, car elle ne déclenche aucune

nouvelle clé.