Modification de comportement de rekey de CLÉ GETVPN

Contenu

Introduction

Ce document décrit les modifications de comportement de rekey de la clé de chiffrement à clé GETVPN (KEK). Il inclut la release 15.2(1)T de Cisco IOS®) et release 15.2(1)S du Cisco IOS XE 3.5). Ce document explique ce changement des problèmes d'interopérabilité de comportement et de potentiel provoqués par lui.

Contribué par Wen Zhang, ingénieur TAC Cisco.

Vieux comportement

Avant la Cisco IOS version 15.2(1)T, le rekey KEK est envoyé par le serveur principal (KS) quand le courant KEK expire. Le membre du groupe (GM) ne met pas à jour un temporisateur pour maintenir la vie restante du KEK. Le courant KEK est remplacé par un nouveau KEK seulement quand un rekey KEK est reçu. Si le GM ne reçoit pas un rekey KEK à l'échéance prévue KEK, il ne déclenche pas un reregistration au KS, et il gardera le KEK existant sans le permettre d'expirer. Ceci a pu avoir comme conséquence le KEK étant utilisé après sa vie configurée. En outre, comme effet secondaire, il n'y a aucune commande sur le GM qui affiche la vie restante KEK.

Nouveau comportement

Le nouveau comportement de rekey KEK inclut deux modifications :

- Sur le KS - Des rekeys KEK sont envoyés avant l'échéance du courant KEK, tout comme un rekey de la clé d'échange du trafic (TEK).
- Sur le GM - Le GM met à jour un temporisateur pour maintenir la vie restante KEK et déclenche un reregistration si le rekey KEK n'est pas reçu.

Nouveau comportement KS

Avec le nouveau comportement de rekey, le KS commence un rekey KEK avant l'échéance du courant KEK selon cette formule.

> Remarque: Dans le calcul ci-dessus, la partie mise en valeur rouge est seulement utilisée avec un rekey d'unicast.

Basé sur ce comportement, les débuts KS pour réintroduire un KEK au moins 200 secondes avant le courant KEK expire. Après que le rekey soit envoyé, les débuts KS pour utiliser le nouveau KEK pour tous les rekeys ultérieurs TEK/KEK.

Nouveau comportement GM

Le nouveau comportement GM inclut deux modifications :

1. Il impose une échéance de vie KEK en ajoutant un temporisateur pour maintenir la vie restante KEK. Quand ce temporisateur expire, le KEK est supprimé sur le GM et un reregistration est déclenché.
2. Le GM s'attend à ce qu'un rekey KEK se produise au moins 200 secondes avant la l'échéance du courant KEK (voir la modification de comportement KS). Un autre temporisateur est ajouté de sorte qu'en cas le nouveau KEK ne soit pas reçu au moins 200 secondes avant l'échéance du courant KEK, le KEK est supprimé et un reregistration est déclenché. Cet événement de suppression et de reregistration KEK se produit en intervalle de compteur de (échéance KEK - 190 secondes, échéance KEK - 40 secondes).

Avec les modifications fonctionnelles, les **sorties de commande show** GM sont également modifiées pour afficher la vie restante KEK en conséquence.

```
GM#show crypto gdoi
GROUP INFORMATION

Group Name : G1
Group Identity : 3333
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 0
IPSec SA Direction : Both

Group Server list : 10.1.11.2

Group member : 10.1.13.2 vrf: None
Version : 1.0.4
Registration status : Registered
Registered with : 10.1.11.2
Reregisters in : 81 sec     <=== Reregistration due to TEK or
KEK, whichever comes first
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 0.0.0.0
Last rekey seq num : 0
Unicast rekey received: 0
Rekey ACKs sent : 0
Rekey Received : never
```

```
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 0
After latest register : 0
Rekey Acks sents : 0

ACL Downloaded From KS 10.1.11.2:
access-list deny ospf any any
access-list deny eigrp any any
access-list deny udp any port = 848 any port = 848
access-list deny icmp any any
access-list permit ip any any

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 56     <=== Running timer for remaining KEK
lifetime
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
Serial1/0:
IPsec SA:
spi: 0xD835DB99(3627408281)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (2228)
Anti-Replay(Time Based) : 10 sec interval
```

Problèmes d'interopérabilité

Avec cette modification de comportement de rekey KEK, le problème d'interopérabilité de code doit être considéré quand le KS et le GM ne pourraient pas exécuter chacun des deux versions IOS qui ont cette modification.

Dans le cas où le GM exécute le code plus ancien, et le KS exécute le code plus nouveau, le KS envoie le rekey KEK avant l'échéance KEK, mais il n'y a la pas autre incidence fonctionnelle notable. Cependant, si un GM exécutant le code plus nouveau s'inscrit à un KS exécutant le code plus ancien, le GM peut encourir le domaine de deux groupes des reregistrations de la traduction (GDOI) afin de recevoir le nouveau KEK par cycle de rekey KEK. Une séquence d'opérations se produisent quand ceci se produit :

1. Le GM reregisters avant l'échéance du courant KEK, puisque le KS enverra seulement le rekey KEK quand le courant KEK expire. Le GM reçoit le KEK, et c'est le même KEK que celui il a actuellement à rester de vie de moins de 190 secondes. Ceci indique au GM qu'il est inscrit à un KS sans modification de rekey KEK.

   ```
   GM#show crypto gdoi
   GROUP INFORMATION

   Group Name : G1
   Group Identity : 3333
   Crypto Path : ipv4
   Key Management Path : ipv4
   ```

```
Rekeys received : 0
IPSec SA Direction : Both

Group Server list : 10.1.11.2

Group member : 10.1.13.2 vrf: None
Version : 1.0.4
Registration status : Registered
Registered with : 10.1.11.2
Reregisters in : 81 sec     <=== Reregistration due to TEK or
KEK, whichever comes first
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 0.0.0.0
Last rekey seq num : 0
Unicast rekey received: 0
Rekey ACKs sent : 0
Rekey Received : never
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 0
After latest register : 0
Rekey Acks sents : 0

ACL Downloaded From KS 10.1.11.2:
access-list deny ospf any any
access-list deny eigrp any any
access-list deny udp any port = 848 any port = 848
access-list deny icmp any any
access-list permit ip any any

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 56     <=== Running timer for remaining KEK
lifetime
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
Serial1/0:
IPsec SA:
spi: 0xD835DB99(3627408281)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (2228)
Anti-Replay(Time Based) : 10 sec interval
```

2. Le GM supprime le KEK à son échéance de vie, et place un temporisateur de reregistration de (échéance KEK, échéance KEK + 80).

```
GM#show crypto gdoi
GROUP INFORMATION

Group Name : G1
Group Identity : 3333
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 0
IPSec SA Direction : Both
```

```
Group Server list : 10.1.11.2

Group member : 10.1.13.2 vrf: None
Version : 1.0.4
Registration status : Registered
Registered with : 10.1.11.2
Reregisters in : 81 sec     <=== Reregistration due to TEK or
KEK, whichever comes first
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 0.0.0.0
Last rekey seq num : 0
Unicast rekey received: 0
Rekey ACKs sent : 0
Rekey Received : never
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 0
After latest register : 0
Rekey Acks sents : 0

ACL Downloaded From KS 10.1.11.2:
access-list deny ospf any any
access-list deny eigrp any any
access-list deny udp any port = 848 any port = 848
access-list deny icmp any any
access-list permit ip any any

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 56     <=== Running timer for remaining KEK
lifetime
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
Serial1/0:
IPsec SA:
spi: 0xD835DB99(3627408281)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (2228)
Anti-Replay(Time Based) : 10 sec interval
```

3. Quand le temporisateur de reregistration expire, le GM reregisters et recevra le nouveau KEK.

```
GM#show crypto gdoi
GROUP INFORMATION

Group Name : G1
Group Identity : 3333
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 0
IPSec SA Direction : Both

Group Server list : 10.1.11.2

Group member : 10.1.13.2 vrf: None
```

```
Version : 1.0.4
Registration status : Registered
Registered with : 10.1.11.2
Reregisters in : 81 sec     <=== Reregistration due to TEK or
KEK, whichever comes first
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 0.0.0.0
Last rekey seq num : 0
Unicast rekey received: 0
Rekey ACKs sent : 0
Rekey Received : never
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 0
After latest register : 0
Rekey Acks sents : 0

ACL Downloaded From KS 10.1.11.2:
access-list deny ospf any any
access-list deny eigrp any any
access-list deny udp any port = 848 any port = 848
access-list deny icmp any any
access-list permit ip any any

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 56     <=== Running timer for remaining KEK
lifetime
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
Serial1/0:
IPsec SA:
spi: 0xD835DB99(3627408281)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (2228)
Anti-Replay(Time Based) : 10 sec interval
```

Recommandations

Dans un déploiement GETVPN, si code de Cisco IOS l'un des GM a été mis à jour à une des versions avec le nouveau comportement de rekey KEK, Cisco recommande que le code KS soit aussi bien mis à jour pour éviter le problème d'interopérabilité.