La CLAVE GETVPN reintroduce el cambio del comportamiento

Contenido

Introducción

Este documento describe la clave de encripción de claves GETVPN (KEK) reintroduce los cambios del comportamiento. Incluye la versión 15.2(1)T del ® del Cisco IOS) y la versión 15.2(1)S del Cisco IOS XE 3.5). Este documento explica este cambio en los problemas de interoperabilidad del comportamiento y del potencial causados por él.

Contribuido por Wen Zhang, ingeniero de Cisco TAC.

Viejo comportamiento

Antes del Cisco IOS Release 15.2(1)T, el KEK reintroduce es enviado por el servidor dominante (KS) cuando expira el KEK actual. El miembro del grupo (GM) no mantiene un temporizador para no perder de vista el tiempo de vida restante del KEK. El KEK actual es substituido por un nuevo KEK solamente cuando se recibe un KEK reintroduce. Si el GM no recibe un KEK reintroduzca en el vencimiento previsto KEK, no acciona un reregistration al KS, y guardará el KEK existente sin dejarlo expirar. Esto podía dar lugar al KEK que era utilizado después de su curso de la vida configurado. También, como efecto secundario, no hay comando en el GM que muestra la vida útil de KEK restante.

Nuevo comportamiento

El nuevo KEK reintroduce el comportamiento incluye dos cambios:

- En el KS - El KEK reintroduce se envía antes del vencimiento actual KEK, como una clave del intercambio del tráfico (TEK) reintroduce.
- En el GM - El GM mantiene un temporizador para no perder de vista la vida útil de KEK

restante y acciona un reregistration si el KEK reintroduce no se recibe.

Nuevo comportamiento KS

Con el nuevo reintroduzca el comportamiento, el KS comienza un KEK para reintroducir antes del vencimiento actual KEK según esta fórmula.

$$KEK\_rekey\_time = KEK\_lifetime - (200 + (\#\_of\_retran * retran\_interval) + (5 * (1 + \frac{\#\_of\_registered\_GMs}{50})))$$

Nota: En el cálculo antedicho, el rojo porción resaltada se utiliza solamente con un unicast reintroduce.

De acuerdo con este comportamiento, un KS comienza a reintroducir un KEK por lo menos 200 segundos antes de que expira el KEK actual. Después de que se envíe la reintroducción, el comienzo KS para utilizar el nuevo KEK para todo el TEK/KEK subsiguiente reintroduce.

Nuevo comportamiento GM

El nuevo comportamiento GM incluye dos cambios:

1. Aplica un vencimiento de la vida útil de KEK agregando un temporizador para no perder de vista el tiempo de vida restante KEK. Cuando expira ese temporizador, el KEK se borra en el GM y se acciona un reregistration.
2. El GM espera que un KEK reintroduzca para ocurrir por lo menos 200 segundos antes el vencimiento actual KEK (véase el cambio del comportamiento KS). Se agrega se borra otro temporizador para en el evento no recibir el nuevo KEK por lo menos 200 segundos antes del vencimiento actual KEK, el KEK y se acciona un reregistration. Este evento de la cancelacíon y del reregistration KEK sucede en el intervalo del temporizador de (vencimiento KEK - 190 segundos, vencimiento KEK - 40 segundos).

Junto con los cambios funcionales, modifican a las **salidas del comando show** GM también para visualizar el tiempo de vida restante KEK por consiguiente.

```
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
```

Problemas de interoperabilidad

Con este KEK reintroduzca el cambio del comportamiento, el problema de interoperabilidad del código necesita ser considerado cuando el KS y el GM no pudieron funcionar con ambas versiones de IOS que tienen este cambio.

En el caso donde el GM está funcionando con el más viejo código, y el KS está funcionando con el más nuevo código, el KS envía el KEK reintroduce antes del vencimiento KEK, pero hay el no otro impacto funcional notable. Sin embargo, si un GM que funciona con el más nuevo código se registra con un KS que funciona con el más viejo código, el GM puede incurrir en el dominio de dos grupos de los reregistrations de la interpretación (GDOI) para recibir el nuevo KEK por el KEK reintroduce el ciclo. Una Secuencia de eventos ocurre cuando sucede ésta:

1. El GM reregistra antes del vencimiento actual KEK, puesto que el KS enviará solamente el KEK reintroduce cuando expira el KEK actual. El GM recibe el KEK, y es el mismo KEK que el él actualmente tiene con menos del permanecer del curso de la vida de 190 segundos. Esto dice a GM que está registrada con un KS sin el KEK reintroduce el cambio.

```
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. El GM borra el KEK en su vencimiento del curso de la vida, y fija un temporizador del reregistration de (vencimiento KEK, vencimiento 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. Cuando expira el temporizador del reregistration, el GM reregistra y recibirá el nuevo 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
```

Recomendaciones

En un despliegue GETVPN, si el código del Cisco IOS un de los GM se ha actualizado a una de las versiones con el nuevo KEK reintroduzca el comportamiento, Cisco recomienda que el código KS esté actualizado también para evitar el problema de interoperabilidad.