Cambio de comportamiento de clave nueva GETVPN

Contenido

Introducción

Este documento describe los cambios en el comportamiento de la clave de cifrado de clave GETVPN (KEK). Incluye Cisco IOS® versión 15.2(1)T) y Cisco IOS-XE versión 3.5 versión 15.2(1)S). Este documento explica este cambio en el comportamiento y los posibles problemas de interoperabilidad causados por él.

Colaborado por Wen Zhang, ingeniero del TAC de Cisco.

Comportamiento antiguo

Antes de la versión 15.2(1)T del IOS de Cisco, el servidor de claves (KS) envía la clave KEK cuando caduca el KEK actual. El miembro del grupo (GM) no mantiene un temporizador para realizar un seguimiento de la vida útil restante de la KEK. La KEK actual se reemplaza por una nueva KEK sólo cuando se recibe una nueva clave KEK. Si el MM no recibe una clave KEK al vencimiento esperado del KEK, no activa un nuevo registro en el KS, y mantendrá el KEK existente sin dejar que caduque. Esto podría hacer que el KEK se use después de su duración configurada. Además, como efecto secundario, no hay ningún comando en el GM que muestre la vida útil restante del KEK.

Nuevo comportamiento

El nuevo comportamiento de la clave KEK incluye dos cambios:

- En el KS: las llaves se envían antes del vencimiento del KEK actual, al igual que una nueva clave de intercambio de tráfico (TEK).
- En el GM - El GM mantiene un temporizador para realizar un seguimiento de la vida útil

restante del KEK y activa un nuevo registro si no se recibe la clave de clave KEK.

Comportamiento nuevo de KS

Con el nuevo comportamiento de nueva clave, el KS inicia una nueva clave KEK antes del vencimiento del KEK actual según esta fórmula.

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

Nota: En el cálculo anterior, la parte resaltada roja sólo se utiliza con una clave de unidifusión.

En base a este comportamiento, un KS comienza a volver a llaves al menos 200 segundos antes de que caduque el KEK actual. Después de enviar la nueva clave, el KS comienza a utilizar la nueva KEK para todas las nuevas claves TEK/KEK posteriores.

Nuevo comportamiento GM

El nuevo comportamiento GM incluye dos cambios:

1. Aplica un vencimiento de duración de KEK al agregar un temporizador para realizar un seguimiento del tiempo de vida restante de KEK. Cuando ese temporizador caduca, el KEK se elimina en el GM y se activa un nuevo registro.
2. El GM espera que se produzca una nueva clave KEK al menos 200 segundos antes de la expiración del KEK actual (consulte el cambio de comportamiento de KS). Se agrega otro temporizador para que, en el caso de que el nuevo KEK no se reciba al menos 200 segundos antes de la fecha de vencimiento del KEK actual, se elimine el KEK y se active un nuevo registro. Este evento de eliminación y registro KEK se produce en el intervalo del temporizador de (vencimiento de KEK - 190 segundos, vencimiento de KEK - 40 segundos).

Junto con los cambios funcionales, los resultados del comando **show** GM también se modifican para mostrar la vida útil restante del KEK en consecuencia.

```
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 cambio de comportamiento de reclave KEK, el problema de interoperabilidad del código debe ser considerado cuando el KS y el GM pueden no ejecutar ambas versiones del IOS que tienen este cambio.

En el caso de que el GM esté ejecutando el código más antiguo y el KS esté ejecutando el código más nuevo, el KS envía la clave KEK antes de la expiración del KEK, pero no hay otro impacto funcional notable. Sin embargo, si un GM que ejecuta el código más nuevo se registra con un KS que ejecuta el código más antiguo, el GM puede incurrir en dos registros de Group Domain of Interpretation (GDOI) para recibir el nuevo ciclo de clave KEK por KEK. Se produce una secuencia de eventos cuando esto ocurre:

1. El GM se vuelve a registrar antes del vencimiento del KEK actual, ya que el KS sólo enviará la clave KEK cuando venza el KEK actual. El MM recibe el KEK y es el mismo KEK que el

que tiene actualmente con menos de 190 segundos de vida. Esto le dice al MM que está registrado con un KS sin el cambio de clave KEK.

```
%GDOI-4-GM_RE_REGISTER: The IPSec SA created for group G1 may
have expired/been cleared, or didn't go through. Re-register to KS. %CRYPTO-5-GM_REGSTER:
Start registration to KS 10.1.11.2 for
group G1 using address 10.1.13.2 %GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to
Unicast Rekey. %GDOI-5-SA_KEK_UPDATED: SA KEK was updated %GDOI-5-SA_TEK_UPDATED: SA TEK
was updated %GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.11.2 complete
for group G1 using address 10.1.13.2 %GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS:
Installation of
Reg/Rekey policies from KS 10.1.11.2 for group G1 & gm identity 10.1.13.2
```

2. El GM elimina el KEK en el vencimiento de su vida útil y establece un temporizador de registro de (vencimiento del KEK, vencimiento del KEK + 80).

```
%GDOI-5-GM_DELETE_EXPIRED_KEK: KEK expired for group G1 and was deleted
```

3. Cuando venza el temporizador de registro, el GM vuelve a registrarse y recibirá el nuevo KEK.

```
%GDOI-4-GM_RE_REGISTER: The IPSec SA created for group G1 may
   have expired/been cleared, or didn't go through. Re-register to KS.
%CRYPTO-5-GM_REGSTER: Start registration to KS 10.1.11.2 for
group G1 using address 10.1.13.2 %GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to
Unicast Rekey. %GDOI-5-SA_KEK_UPDATED: SA KEK was updated %GDOI-5-SA_TEK_UPDATED: SA TEK
was updated %GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.11.2 complete for
group G1 using address 10.1.13.2 %GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation
of
Reg/Rekey policies from KS 10.1.11.2 for group G1 & gm identity
10.1.13.2
```

Recomendaciones

En una implementación de GETVPN, si alguno de los códigos GM de Cisco IOS se ha actualizado a una de las versiones con el nuevo comportamiento de la nueva clave KEK, Cisco recomienda que el código KS se actualice también para evitar el problema de interoperabilidad.