GETVPN KEY 키 다시 키 동작 변경

목차

소개

이 문서에서는 KEK(GETVPN Key Encryption Key) 키 재설정 동작 변경에 대해 설명합니다.여기에는 Cisco IOS® Release 15.2(1)T) 및 Cisco IOS-XE 3.5 Release 15.2(1)S가 포함됩니다. 이 문서에서는 이러한 동작의 변화 및 이로 인한 잠재적인 상호 운용성 문제에 대해 설명합니다.

기고자: Wen Zhang, Cisco TAC 엔지니어

이전 동작

Cisco IOS Release 15.2(1)T 이전에는 현재 KEK가 만료되면 KS(Key Server)에서 KEK rekey를 전송합니다.GM(Group Member)은 KEK의 남은 수명을 추적하기 위한 타이머를 유지하지 않습니다.KEK rekey를 받은 경우에만 현재 KEK가 새 KEK로 교체됩니다.GM이 예상 KEK 만료에 KEK rekey를 수신하지 않을 경우, KS에 재등록을 트리거하지 않으며, 만료되지 않고 기존 KEK를 유지합니다.그러면 구성된 수명 후에 KEK가 사용될 수 있습니다.또한, 부작용으로, GM에 대해 나머지 KEK 수명을 보여주는 명령이 없습니다.

새 동작

새로운 KEK 키 재설정 동작에는 두 가지 변경 사항이 포함됩니다.

- KS에서 - KEK rekeys는 TEK(Traffic Exchange Key) rekey와 마찬가지로 현재 KEK 만료 전에 전송됩니다.
- GM에서 - GM은 나머지 KEK 수명을 추적하기 위한 타이머를 유지 관리하고 KEK rekey가 수신되지 않을 경우 재등록을 트리거합니다.

KS 새로운 행동

새 키 재설정 동작을 사용하면 KS는 이 공식에 따라 현재 KEK 만료 전에 KEK 키 재설정을 시작합니다.

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

참고:위의 계산에서 빨간색으로 강조 표시된 부분은 유니캐스트 키 리키에만 사용됩니다.

이 동작을 기반으로 KS는 현재 KEK가 만료되기 200초 전에 KEK를 재키하기 시작합니다.rekey가 전송되면 KS는 모든 후속 TEK/KEK rekey에 새 KEK를 사용하기 시작합니다.

GM의 새로운 행동

새로운 GM 동작에는 두 가지 변경 사항이 포함됩니다.

1. KEK 남은 수명을 추적하기 위해 타이머를 추가하여 KEK 수명 만료가 시행됩니다.타이머가 만료되면 KEK가 GM에서 삭제되고 재등록이 트리거됩니다.
2. GM은 현재 KEK 만료 200초 전에 KEK rekey가 발생할 것으로 예상합니다(KS 동작 변경 참조). 현재 KEK 만료 200초 전에 새 KEK를 받지 못할 경우 KEK가 삭제되고 재등록이 트리거되도록 또 다른 타이머가 추가됩니다.이 KEK 삭제 및 재등록 이벤트는 타이머 간격(KEK 만료 - 190초, KEK 만료 - 40초)에 발생합니다.

기능 변경과 함께 GM **show** 명령 출력도 수정되어 KEK 잔여 수명을 적절하게 표시합니다.

```
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
```

상호 운용성 문제

이 KEK 키 재설정 동작 변경으로 인해 KS와 GM이 이 변경 사항이 있는 IOS 버전 둘 다를 실행하지 않을 경우 코드 상호 운용성 문제를 고려해야 합니다.

GM에서 이전 코드를 실행하고 있고 KS에서 최신 코드를 실행하는 경우 KS는 KEK 만료 전에 KEK rekey를 전송하지만 다른 주목할 만한 기능적 효과는 없습니다.그러나 최신 코드를 실행하는 GM이 이전 코드를 실행하는 KS에 등록하면 GM은 KEK 키 재키당 새 KEK를 받기 위해 2개의 GDOI(Group Domain of Interpreventing) 재등록이 발생할 수 있습니다.다음과 같은 경우 일련의 이벤트가 발생합니다.

1. 현재 KEK가 만료될 때만 KEK rekey가 전송되므로 GM은 현재 KEK 만료 전에 다시 등록됩니다.GM은 KEK를 수신하며, 190초 미만의 수명이 남아 있는 KEK와 동일한 KEK입니다.이는 GM에 KEK 키 변경 없이 KS에 등록되었음을 알려줍니다.

   ```
   %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. GM은 KEK를 수명 만료에 삭제하고 (KEK 만료, KEK 만료 + 80)의 재등록 타이머를 설정합니다.

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

3. 재등록 타이머가 만료되면 GM은 재등록하고 새 KEK를 받게 됩니다.

```
%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
```

권장 사항

GETVPN 구축에서 GM Cisco IOS 코드 중 하나가 새로운 KEK 키 재설정 동작으로 버전 중 하나로 업그레이드된 경우 상호 운용성 문제가 발생하지 않도록 KS 코드를 업그레이드할 것을 권장합니다 .