GETVPN金鑰重新生成金鑰行為更改

目錄

簡介

本檔案將說明GETVPN金鑰加密金鑰(KEK)金鑰行為更改。它包括Cisco IOS®版本15.2(1)T)和Cisco IOS-XE 3.5版本15.2(1)S)。 本檔案將說明行為上的變更以及由此導致的潛在互通性問題。

作者：Wen Zhang，思科TAC工程師。

舊行為

在Cisco IOS版本15.2(1)T之前，KEK金鑰在當前KEK到期時由金鑰伺服器(KS)傳送。組成員(GM)不維護計時器來跟蹤KEK的剩餘壽命。只有在收到KEK重新金鑰時，當前的KEK才會被新的KEK替換。如果GM在預期的KEK到期時沒有收到KEK重新金鑰，其不會觸發對KS的重新註冊，並且其將保留現有的KEK而不使其到期。這可能導致KEK在其配置的生命週期之後被使用。此外，作為副作用，GM上沒有任何命令顯示剩餘的KEK生存期。

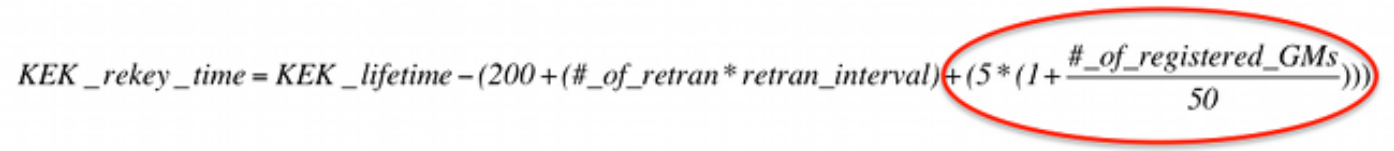
新行為

新的KEK重新生成金鑰行為包括兩個更改：

- 在KS上 — KEK重新金鑰在當前KEK到期之前傳送，很像流量交換金鑰(TEK)重新金鑰。
- 在GM上 — GM維護計時器以跟蹤剩餘的KEK生存期，並在未收到KEK重新金鑰時觸發重新註冊。

KS新行為

使用新的金鑰重新生成行為，KS根據此公式在當前KEK到期之前啟動KEK重新生成金鑰。



附註：在上述計算中，紅色突出顯示部分僅與單播金鑰一起使用。

基於此行為，KS在當前KEK到期之前，至少開始為KEK重新建立金鑰200秒。重新生成金鑰後，KS開始對所有後續的TEK/KEK重新生成金鑰使用新的KEK。

GM新行為

GM的新行為包括兩項改變：

1. 它通過新增計時器來跟蹤KEK剩餘壽命來強制實施KEK生存期到期。當該計時器到期時，在GM上刪除KEK並觸發重新註冊。
2. GM預期KEK重新金鑰將在當前KEK到期之前至少200秒發生（請參閱KS行為更改）。 增加另一個計時器，以便在當前KEK到期之前至少200秒沒有收到新KEK的情況下，刪除KEK並觸發重新註冊。此KEK刪除和重新註冊事件發生在計時器間隔（KEK到期 — 190秒，KEK到期 — 40秒）內。

隨著功能的改變，GM **show**命令輸出也相應修改以顯示KEK剩餘壽命。

```
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
```

互通性問題

由於此KEK金鑰重定行為更改，當KS和GM可能未同時運行具有此更改的兩個IOS版本時，需要考慮代碼互操作性問題。

在GM運行舊代碼且KS運行較新的代碼的情況下，KS在KEK到期之前傳送KEK重新金鑰，但是沒有其他顯著的功能影響。但是，如果運行較新代碼的GM向運行較舊代碼的KS註冊，則GM可能會發生兩個組解釋域(GDOI)重新註冊，以便在KEK重新金鑰週期中接收新的KEK。發生以下情況時會發生一系列事件：

1. GM在當前KEK到期之前重新註冊，因為KS僅在當前KEK到期時傳送KEK重新金鑰。GM收到KEK，它與GM當前具有的KEK相同，剩餘壽命少於190秒。這告知GM它向KS註冊，而沒有KEK金鑰更改。

```
%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. GM在其生存期到期時刪除KEK，並且設定重新註冊計時器（KEK到期，KEK到期+ 80）。

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

3. 當重新註冊計時器到期時，GM重新註冊並將接收新的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
```

建議

在GETVPN部署中，如果任何GM Cisco IOS代碼已升級到具有新KEK金鑰行為的某個版本，Cisco建議同時升級KS代碼以避免互操作性問題。