GETVPN密钥密钥重新生成行为更改

目录

简介

本文档介绍GETVPN密钥加密密钥(KEK)重新生成密钥的行为更改。它包括Cisco IOS®版本15.2(1)T)和Cisco IOS-XE 3.5版本15.2(1)S)。 本文档说明行为的变化以及由此引起的潜在互操作性问题。

作者：思科TAC工程师Wen Zhang。

旧行为

在Cisco IOS版本15.2(1)T之前，当当前KEK过期时，密钥服务器(KS)会发送KEK密钥。组成员(GM)不维护计时器以跟踪科索沃能源公司的剩余寿命。只有收到新的KEK密钥时，才会取代现有的KEK。如果通用汽车在预期的科索沃公司到期时没有收到科索沃公司的返点，它就不会触发对克兰群岛的重新注册，它将保留现有科索沃公司，而不会让其过期。这可能导致KEK在其配置的生命期后使用。此外，作为副作用，GM上没有显示剩余KEK寿命的命令。

新行为

新的KEK密钥更新行为包括两个变化：

- 在KS - KEK密钥在当前KEK到期之前发送，与流量交换密钥(TEK)密钥类似。
- 在GM上 — GM维护一个计时器以跟踪剩余的KEK寿命，并在未收到KEK密钥时触发重新注册。

KS新行为

根据此公式，KS在当前KEK到期之前启动KEK重新密钥。

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

注意：在上述计算中，红色突出显示部分仅与单播密钥一起使用。

根据此行为，KS至少在当前KEK过期之前200秒开始对KEK重新键入。重新密钥发送后，KS开始对所有后续TEK/KEK重新密钥使用新的KEK。

转基因新行为

新的转基因行为包括两个变化：

1. 它通过添加计时器来跟踪KEK剩余寿命，从而强制KEK生存期到期。当该计时器过期时，GM上的KEK将被删除，并触发重新注册。
2. 通用汽车预计，KEK返点至少在当前KEK到期前200秒发生（参见KS行为更改）。 添加另一个计时器，以便在当前KEK到期前至少200秒未收到新KEK时，删除KEK并触发重新注册。此KEK删除和重新注册事件发生在计时器间隔（KEK到期 — 190秒，KEK到期 — 40秒）内。

随着功能的改变，GM **show命**令输出也被修改以相应地显示KEK剩余寿命。

```
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
```

互操作性问题

通过此KEK重新生成密钥的行为更改，当KS和GM可能不运行具有此更改的两个IOS版本时，需要考虑代码互操作性问题。

在GM运行较旧代码，KS运行较新代码的情况下，KS在KEK到期前发送KEK密钥，但没有其他显着的功能影响。但是，如果运行较新代码的GM向运行较旧代码的KS注册，则GM可能会产生两个组解释域(GDOI)重新注册，以便根据KEK重新密钥周期接收新的KEK。发生以下情况时会发生一系列事件：

1. 由于KK只在当前KEK到期时发送KEK密钥，因此GM在当前KEK到期前重新注册。GM接收KEK，它与它目前拥有的KEK相同，剩余寿命不到190秒。这告诉通用汽车，它在KS上注册，而没有KEK密钥更改。

```
%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KEK的有效期到期时删除KEK，并设置重新注册计时器（KEK到期，KEK到期+ 80）。

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

3. 当重新注册计时器到期时，GM重新注册并将接收新的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
```

建议

在GETVPN部署中，如果任何GM Cisco IOS代码已升级到具有新KEK密钥重新生成行为的某个版本，思科建议升级KS代码，以避免互操作性问题。