GETVPN KEY キー再生成の動作変更

内容

概要

このドキュメントでは、GETVPN の Key Encryption Key（KEK）のキー再生成の動作の変更について説明します。これには、Cisco IOS® リリース 15.2(1)T と Cisco IOS-XE 3.5 リリース 15.2(1)S が含まれます。 このドキュメントでは、この動作の変更とそれによって発生する相互運用性の潜在的な問題について説明します。

著者：Cisco TAC エンジニア、Wen Zhang

古い動作

Cisco IOS Release 15.2(1)T より前は、現在の KEK が期限切れになると、KEK のキー再生成がキー サーバ（KS）によって送信されます。グループ メンバー（GM）では、KEK の残りのライフタイムを追跡するためにタイマーを保持しません。KEK のキー再生成を受信した場合にのみ、現在の KEK が新しい KEK に置き換えられます。GM が予期される KEK の期限が切れたときに KEK のキー再生成を受信しなかった場合、GM は KS の再登録を開始せず、既存の KEK を期限切れにせずにそのまま保持します。これにより、KEK がそれに設定されたライフタイムの後に使用される可能性があります。また、副次的な悪影響として、GM で KEK の残りのライフタイムを表示するコマンドがありません。

新しい動作

新しい KEK のキー再生成の動作には、次の 2 つの変更があります。

- KS での変更 - Traffic Exchange Key（TEK）のキー再生成のように現在の KEK が期限切れになる前に、KEK のキー再生成が送信されます。
- GM での変更 - GM が KEK のキー再生成を受信しなかった場合、GM は KEK の残りのライフタイムを追跡するためにタイマーを保持し、再登録を開始します。

KS の新しい動作

新しいキー再生成の動作では、KS は次の式に従って現在の KEK が期限切れになる前に KEK のキー再生成を開始します。

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

注：上記の計算では、赤色で強調表示された部分のみがユニキャストのキー再生成で使用されます。

この動作に基づいて、KS は現在の KEK が期限切れになる少なくとも 200 秒前に、KEK のキー再生成を開始します。キー再生成が送信された後、KS は以降のすべての TEK/KEK のキー再生成用に新しい KEK の使用を開始します。

GM の新しい動作

新しい GM の動作には、次の 2 つの変更があります。

1. KEK の残りのライフタイムを追跡するためにタイマーを追加することで、KEK のライフタイムの期限切れが強制的に適用されます。そのタイマーが期限切れになると、GM で KEK が削除され、再登録が開始されます。
2. GM では、現在の KEK が期限切れになる少なくとも 200 秒前に、KEK のキー再生成が発生することを想定します（KS の動作の変更を参照）。 別のタイマーが追加され、現在の KEK が期限切れになり、KEK が削除され、再登録が開始される少なくとも 200 秒前にイベントで新しい KEK を受信しないようにします。この KEK の削除と再登録のイベントは、タイマー インターバル（KEK の期限切れ - 190 秒、KEK の期限切れ - 40 秒）で発生します。

機能変更とともに、KEK の残りのライフタイムを適宜表示する GM の **show コマンド出力も変更されています。**

```
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
```

相互運用性の問題

この KEK のキー再生成の動作の変更により、KS と GM がこの変更が適用されている両方の IOS バージョンを実行していない可能性がある場合、コードの相互運用性の問題を考慮する必要があります。

GM が古いコードを実行し、KS が新しいコードを実行している場合、KS は KEK が期限切れになる前に KEK のキー再生成を送信しますが、その他の留意すべき機能への影響はありません。ただし、新しいコードを実行している GM が古いコードを実行している KS に登録する場合、GM では、KEK のキー再生成のサイクルごとの新しい KEK を受信するために 2 つの Group Domain of Interpretation (GDOI) 登録が発生する可能性があります。これが発生した場合、次の一連のイベントが発生します。

1. 現在の KEK が期限切れになった場合、KS は KEK のキー再生成のみを送信するため、GM は現在の KEK が期限切れになる前に再登録します。GM は KEK を受信します。この KEK は残りのライフタイムが 190 秒未満である現在の KEK と同じです。これにより、KEK が KEK のキー再生成を変更せずに KS に登録されていることが GM に通知されます。

```
%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 はライフタイムの期限が切れたときに KEK を削除し、再登録のタイマー (KEK の時間切れ、KEK の時間切れ + 80) を設定します。

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

3. 再登録のタイマーが期限切れになると、GM は新しい KEK を再登録し、受信します。

```
%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
```

推奨事項

GETVPN の展開では、GM の Cisco IOS コードのいずれかが新しい KEK のキー再生成の動作を実装するいずれかのバージョンにアップグレードされた場合は、相互運用性の問題を回避するため、KS コードもアップグレードすることを推奨します。