GETVPN KEY Rekey Behavior Change

Document ID: 116737

Contributed by Wen Zhang, Cisco TAC Engineer.

Nov 26, 2013

Contents

Introduction
Old Behavior
New Behavior
KS New Behavior
GM New Behavior
Interoperability Issues
Recommendations

Introduction

This document describes the GETVPN Key Encryption Key (KEK) rekey behavior changes. It includes the Cisco IOS® Release 15.2(1)T) and Cisco IOS−XE 3.5 Release 15.2(1)S). This document explains this change in behavior and potential interoperability issues caused by it.

Contributed by Wen Zhang, Cisco TAC Engineer.

Old Behavior

Prior to Cisco IOS Release 15.2(1)T, the KEK rekey is sent by the Key Server (KS) when the current KEK expires. The Group Member (GM) does not maintain a timer to keep track of the remaining lifetime of the KEK. The current KEK is replaced by a new KEK only when a KEK rekey is received. If the GM does not receive a KEK rekey at the expected KEK expiry, it does not trigger a reregistration to the KS, and it will keep the existing KEK without letting it expire. This could result in the KEK being used after its configured lifetime. Also, as a side effect, there is no command on the GM that shows the remaining KEK lifetime.

New Behavior

The new KEK rekey behavior includes two changes:

- On the KS − KEK rekeys are sent before the current KEK expiry, much like a Traffic Exchange Key (TEK) rekey.
- On the GM − The GM maintains a timer to keep track of the remaining KEK lifetime and triggers a reregistration if the KEK rekey is not received.

KS New Behavior

With the new rekey behavior, the KS starts a KEK rekey before the current KEK expiry according to this formula.

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

Note: In the above calculation, the red highlighted portion is only used with a unicast rekey.

Based on this behavior, a KS starts to rekey a KEK at least 200 seconds before the current KEK expires. After the rekey is sent, the KS starts to use the new KEK for all subsequent TEK/KEK rekeys.

GM New Behavior

The new GM behavior includes two changes:

1. It enforces a KEK lifetime expiry by adding a timer to keep track of the KEK remaining lifetime. When that timer expires, the KEK is deleted on the GM and a reregistration is triggered.
2. The GM expects a KEK rekey to occur at least 200 seconds prior to the the current KEK expiry (see KS behavior change). Another timer is added so that in the event the new KEK is not received at least 200 seconds before the current KEK expiry, the KEK is deleted and a reregistration is triggered. This KEK deletion and reregistration event happens in the timer interval of (KEK expiry − 190 seconds, KEK expiry − 40 seconds).

Along with the functional changes, the GM ***show*** command outputs are also modified to display the KEK remaining lifetime accordingly.

```
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
       Succeded 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
```

Interoperability Issues

With this KEK rekey behavior change, the code interoperability issue needs to be considered when the KS and GM might not run both of the IOS versions that have this change.

In the case where the GM is running the older code, and the KS is running the newer code, the KS sends out the KEK rekey prior to the KEK expiry, but there is no other notable functional impact. However, if a GM running the newer code registers with a KS running the older code, the GM may incur two Group Domain of Interpretation (GDOI) reregistrations in order to receive the new KEK per KEK rekey cycle. A sequence of events occur when this happens:

1. The GM reregisters before the current KEK expiry, since the KS will only send the KEK rekey when the current KEK expires. The GM receives the KEK, and it is the same KEK as the one it currently has with less than 190 seconds lifetime remaining. This tells the GM that it is registered with a KS without the KEK rekey change.

   ```
   %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. The GM deletes the KEK at its lifetime expiry, and sets a reregistration timer of (KEK expiry, KEK expiry + 80).

   ```
   %GDOI-5-GM_DELETE_EXPIRED_KEK: KEK expired for group G1 and was deleted
   ```
3. When the reregistration timer expires, the GM reregisters and will receive the new 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
```

Recommendations

In a GETVPN deployment, if any of the GM Cisco IOS code has been upgraded to one of the versions with the new KEK rekey behavior, Cisco recommends that the KS code be upgraded as well to avoid the interoperability issue.

Updated: Nov 26, 2013 Document ID: 116737