Änderung des Verhaltens von GETVPN KEY-Neuschlüsseln

Inhalt

Einführung

In diesem Dokument werden die Änderungen am Verhalten des GETVPN Key Encryption Key (KEK)-Schlüssel beschrieben. Sie umfasst Cisco IOS® Release 15.2(1)T und Cisco IOS-XE 3.5, Version 15.2(1)S. In diesem Dokument werden diese Verhaltensänderung und mögliche Interoperabilitätsprobleme, die durch diese Änderungen verursacht werden, erläutert.

Mitarbeiter: Wen Zhang, Cisco TAC Engineer.

Altes Verhalten

Vor der Cisco IOS-Version 15.2(1)T wird der KEK-Schlüssel vom Key-Server (KS) gesendet, wenn die aktuelle KEK abläuft. Das Gruppenmitglied (GM) unterhält keinen Timer, um die verbleibende Lebensdauer des KEK zu verfolgen. Der aktuelle KEK wird nur dann durch einen neuen KEK ersetzt, wenn ein KEK-Schlüssel empfangen wird. Wenn der GM beim erwarteten Ablaufdatum des KEK keinen KEK-Schlüssel erhält, wird keine Neuregistrierung für den KS ausgelöst, und der vorhandene KEK bleibt unverändert, ohne dass er abläuft. Dies kann dazu führen, dass der KEK nach seiner konfigurierten Lebensdauer verwendet wird. Außerdem gibt es als Nebeneffekt keinen Befehl auf dem GM, der die verbleibende KEK-Lebensdauer anzeigt.

Neues Verhalten

Das neue KEK-Schlüssel-Verhalten umfasst zwei Änderungen:

- Auf dem KS - werden die KEK-Schlüssel vor dem aktuellen Ablaufdatum des KEK gesendet, ähnlich wie bei einem TEK-Schlüssel (Traffic Exchange Key).
- Auf dem GM - Der GM behält einen Timer, um die verbleibende KEK-Lebensdauer

nachzuverfolgen, und löst eine erneute Registrierung aus, wenn der KEK-Schlüssel nicht empfangen wird.

KS Neues Verhalten

Mit dem neuen Schlüsselverhalten startet der KS einen KEK-Schlüssel vor dem aktuellen KEK-Ablauf gemäß dieser Formel.

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

Hinweis: In der obigen Berechnung wird der rot hervorgehobene Teil nur mit einem Unicast-Schlüssel verwendet.

Basierend auf diesem Verhalten beginnt ein KS, einen KEK mindestens 200 Sekunden vor Ablauf des aktuellen KEK erneut zu aktivieren. Nachdem der Schlüssel gesendet wurde, beginnt der KS, den neuen KEK für alle nachfolgenden TEK/KEK-Schlüssel zu verwenden.

Neues Verhalten von GM

Das neue GM-Verhalten umfasst zwei Änderungen:

1. Er erzwingt ein KEK-Lebenszeitlimit, indem ein Timer hinzugefügt wird, um die verbleibende Lebensdauer des KEK zu überwachen. Wenn dieser Timer abläuft, wird der KEK auf dem GM gelöscht, und eine erneute Registrierung wird ausgelöst.
2. Der GM geht davon aus, dass ein KEK-Schlüssel mindestens 200 Sekunden vor dem aktuellen KEK-Ablauf eintritt (siehe KS-Verhaltensänderung). Ein weiterer Timer wird hinzugefügt, sodass im Falle, dass der neue KEK nicht mindestens 200 Sekunden vor dem aktuellen Ablaufdatum des KEK empfangen wird, der KEK gelöscht wird und eine erneute Registrierung ausgelöst wird. Das Löschen und erneuten Registrieren der KEK erfolgt im Zeitgeberintervall von (KEK-Ablauf - 190 Sekunden, KEK-Ablauf - 40 Sekunden).

Neben den Funktionsänderungen werden auch die GM **show**-Befehlsausgaben so geändert, dass die verbleibende Lebensdauer des KEK entsprechend angezeigt wird.

```
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
```

Interoperabilitätsprobleme

Bei dieser Änderung des KEK-Schlüssel-Verhaltens muss das Problem der Codeinteroperabilität beachtet werden, wenn KS und GM möglicherweise nicht beide IOS-Versionen ausführen, die diese Änderung aufweisen.

Wenn der GM den älteren Code ausführt und der KS den neueren Code ausführt, sendet der KS den KEK-Schlüssel vor dem Ablauf des KEK-Ablaufs aus, aber es gibt keine weiteren nennenswerten funktionalen Auswirkungen. Wenn jedoch ein GM, der den neueren Code ausführt, bei einem KS registriert wird, der den älteren Code ausführt, kann der GM zwei Group Domain of Interpretation (GDOI)-Neuregistrierungen vornehmen, um den neuen KEK pro KEK rekey-Zyklus zu erhalten. In folgenden Fällen tritt eine Reihe von Ereignissen auf:

1. Die GM-Registrierer werden vor dem aktuellen KEK-Ablaufdatum registriert, da der KS den

KEK-Schlüssel nur dann sendet, wenn die aktuelle KEK abläuft. Der GM empfängt das KEK und ist mit weniger als 190 Sekunden Lebensdauer der gleiche KEK wie der aktuelle. Dies weist den GM darauf hin, dass er bei einem KS registriert ist, ohne dass die KEK rekey-Änderung vorgenommen wurde.

```
%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. Der GM löscht die KEK bei Ablauf der Lebensdauer und setzt einen Wiederregistrierungs-Timer von (KEK-Ablauf, KEK-Ablauf + 80).

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

3. Nach Ablauf des Registrierungs-Timers registriert GM die neue KEK-Nummer und wird diese erhalten.

```
%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
```

Empfehlungen

Wenn in einer GETVPN-Bereitstellung ein GM-Cisco IOS-Code auf eine der Versionen mit dem neuen KEK-Schlüssel-Verhalten aktualisiert wurde, empfiehlt Cisco, den KS-Code ebenfalls zu aktualisieren, um Interoperabilitätsprobleme zu vermeiden.