GETVPN KEY gedragsverandering

Inhoud

Inleiding

Dit document beschrijft de KEK (GETVPN Key Encryption Key) gedragswijzigingen. Hij bevat de Cisco IOS® release 15.2(1)T en Cisco IOS-XE 3.5 release 15.2(1)S). In dit document wordt deze gedragsverandering en de mogelijke interoperabiliteitsproblemen toegelicht.

Bijgedragen door Wen Zhang, Cisco TAC Engineer.

Oud gedrag

Voorafgaand aan Cisco IOS release 15.2(1)T wordt de KEK rekey verzonden door de Key Server (KS) wanneer de huidige KEK verlopen. Het groepslid (GM) heeft geen timer om de resterende levensduur van de KEK bij te houden. De huidige KEK wordt alleen vervangen door een nieuwe KEK wanneer een KEK rekey wordt ontvangen. Indien de GM bij het verwachte verstrijken van de KEK geen KEK rekey ontvangt, brengt hij geen herregistratie aan bij de KS en behoudt hij de bestaande KEK zonder het te laten verlopen. Dit kan ertoe leiden dat de KEK wordt gebruikt na de ingestelde levensduur. Als neveneffect is er geen opdracht op de GM die de resterende KEK-levensduur toont.

Nieuw gedrag

Het nieuwe KEK rekey gedrag omvat twee veranderingen:

- Op de KS - KEK worden rekeys verstuurd vóór de huidige KEK expiratie, net zoals een Traffic Exchange Key (TEK) - start.
- Op de GM - De timer zorgt voor het bijhouden van de resterende KEK-levensduur en voor een herregistratie als de KEK-rekey niet wordt ontvangen.

KS nieuw gedrag

Met het nieuwe rekey-gedrag, begint de KS een KEK rekey voor het huidige KEK-verstrijken volgens deze formule.

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

Opmerking: In de bovenstaande berekening wordt het rode gemarkeerde gedeelte alleen gebruikt met een eenblaasrekkertje.

Op basis van dit gedrag begint een KS een KEK ten minste 200 seconden te rekken voordat de huidige KEK vervalt. Nadat de rekey is verstuurd, begint de KS de nieuwe KEK te gebruiken voor alle daaropvolgende TEK/KEK-rekeys.

GM New Gedrag

Het nieuwe GM-gedrag bevat twee veranderingen:

1. Het dwingt een KEK levenslange afloop door een timer toe te voegen om de resterende levensduur van KEK bij te houden. Als die timer afloopt, wordt de KEK op de GM verwijderd en wordt een herregistratie gestart.
2. De GM verwacht dat een KEK rekey ten minste 200 seconden voor het huidige KEK verlopen (zie KS gedragsverandering). Er wordt een andere timer toegevoegd, zodat in het geval dat de nieuwe KEK niet ten minste 200 seconden voor het huidige aflopen van KEK wordt ontvangen, de KEK wordt verwijderd en er een herregistratie wordt gestart. Deze KEK wissen en herregistratie gebeurtenis vindt plaats in het timer interval van (KEK expiratie - 190 seconden, KEK expiratie - 40 seconden).

Samen met de functionele veranderingen worden de GM **show**-opdrachtoutput ook aangepast om de resterende levensduur van KEK weer te geven.

```
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
```

Interoperabiliteitsproblemen

Door deze KEK gedragsverandering moet het probleem van de code interoperabiliteit worden overwogen wanneer de KS en GM geen van beide IOS versies die deze verandering hebben kunnen uitvoeren.

In het geval dat de GM de oudere code runt en de KS de nieuwere code runt, sturen de KS de KEK rekey uit vóór het verstrijken van de KEK, maar er is geen andere opmerkelijke functionele impact. Indien een GM de nieuwere code registreert bij een KS met de oudere code, mag de GM echter twee Groepsdomein van Tolken (GDOI)-registraties uitvoeren om de nieuwe KEK per KEK rekey-cyclus te ontvangen. Een opeenvolging van gebeurtenissen gebeurt wanneer dit gebeurt:

1. De genetisch gemodificeerde reregisters vóór het huidige KEK-verstrijken, aangezien de KS het KEK pas rekey zal sturen als de huidige KEK afloopt. De GV ontvangt de KEK en is dezelfde KEK als de GKE die momenteel nog niet 190 seconden in leven is. Dit vertelt de GM dat hij bij een KS is geregistreerd zonder de KEK rekey verandering.

```
%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. De GM schrapt de KEK bij het verstrijken van zijn levensduur en zet een reregistratie-timer van (KEK expiratie, KEK expiratie + 80).

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

3. Als de timer voor de herregistratie afloopt, worden de genetisch gemodificeerde reregisters gebruikt en wordt de nieuwe KEK ontvangen.

```
%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
```

Aanbevelingen

In een GETVPN-toepassing, als een van de GM Cisco IOS-code is bijgewerkt naar een van de versies met het nieuwe KEK rekey-gedrag, raadt Cisco aan om de KS-code ook te verbeteren om het interoperabiliteitsprobleem te voorkomen.