A CHAVE GETVPN Rekey a mudança do comportamento

Índice

Introdução

Este documento descreve a chave de criptografia chave GETVPN (KEK) rekey mudanças do comportamento. Inclui a liberação 15.2(1)T do ® do Cisco IOS) e liberação 15.2(1)S do Cisco IOS XE 3.5). Este documento explica esta mudança nas questões de interoperabilidade do comportamento e do potencial causadas por ele.

Contribuído por Wen Zhang, engenheiro de TAC da Cisco.

Comportamento velho

Antes do Cisco IOS Release 15.2(1)T, o KEK rekey é enviado pelo server chave (KS) quando o KEK atual expira. O membro do grupo (GM) não mantém um temporizador para manter-se a par da duração restante do KEK. O KEK atual está substituído por um KEK novo somente quando um KEK rekey é recebido. Se o GM não recebe um KEK rekey na expiração prevista KEK, não provoca um reregistration ao KS, e manterá o KEK existente sem deixá-lo expirar. Isto podia conduzir ao KEK que está sendo usado após sua vida configurada. Também, como um efeito secundário, não há nenhum comando no GM que mostra o tempo de vida de KEK restante.

Comportamento novo

O KEK novo rekey o comportamento inclui duas mudanças:

- No KS - O KEK rekeys é enviado antes da expiração atual KEK, bem como uma chave da troca do tráfego (TEK) rekey.
- No GM - O GM mantém um temporizador para manter-se a par do tempo de vida de KEK restante e provoca um reregistration se o KEK rekey não é recebido.

Comportamento novo KS

Com o novo rekey o comportamento, o KS começa um KEK rekey antes da expiração atual KEK de acordo com esta fórmula.

> Nota: No cálculo acima, a parcela destacada vermelha é usada somente com um unicast rekey.

Baseado neste comportamento, um KS começa rekey um KEK pelo menos 200 segundos antes que o KEK atual expire. Depois que o rekey é enviado, os começos KS para usar o KEK novo para todo o TEK/KEK subsequente rekeys.

Comportamento novo GM

O comportamento novo GM inclui duas mudanças:

1. Reforça uma expiração do tempo de vida de KEK adicionando um temporizador para manter-se a par da duração restante KEK. Quando esse temporizador expira, o KEK está suprimido no GM e um reregistration é provocado.
2. O GM espera que um KEK rekey para ocorrer pelo menos 200 segundos antes o da expiração atual KEK (veja a mudança do comportamento KS). Um outro temporizador é adicionado de modo que no evento o KEK novo não seja recebido pelo menos 200 segundos antes da expiração atual KEK, o KEK é suprimido e um reregistration é provocado. Este evento do supressão e do reregistration KEK acontece no intervalo de temporizador de (expiração KEK - 190 segundos, expiração KEK - 40 segundos).

Junto com as mudanças funcionais, os **show command outputs (resultado do comando show)** GM são alterados igualmente para indicar em conformidade a duração restante KEK.

```
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
```

Questões de interoperabilidade

Com este KEK rekey a mudança do comportamento, a questão de interoperabilidade do código precisa de ser considerada quando o KS e o GM não puderam executar ambas as Versões do IOS que têm esta mudança.

No caso onde o GM está executando o código mais velho, e o KS está executando o código mais novo, o KS manda o KEK rekey antes da expiração KEK, mas há o não outro impacto funcional notável. Contudo, se um GM que executa o código mais novo se registra com um KS que executa o código mais velho, o GM pode incorrer o domínio de dois grupos de reregistrations da interpretação (GDOI) a fim receber o KEK novo pelo KEK rekey o ciclo. Uma sequência de evento ocorre quando esta acontece:

1. O GM registra-se novamente antes da expiração atual KEK, desde que o KS enviará somente o KEK rekey quando o KEK atual expira. O GM recebe o KEK, e é o mesmo KEK que esse ele tem atualmente com menos do que permanecer de uma vida de 190 segundos. Isto diz ao GM que está registrado com um KS sem o KEK rekey a mudança.

   ```
   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
```

2. O GM suprime do KEK em sua expiração da vida, e ajusta um temporizador do reregistration de (expiração KEK, expiração KEK + 80).

```
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
```

3. Quando o temporizador do reregistration expira, o GM registra novamente e receberá o KEK novo.

```
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
```

Recomendações

Em um desenvolvimento GETVPN, se algum do código do IOS Cisco GM foi promovido a uma das versões com o KEK novo rekey o comportamento, Cisco recomenda que o código KS esteja promovido também para evitar a questão de interoperabilidade.