GETVPN KEY重新生成密钥行为崔凡吉莱

目录

简介

本文描述GETVPN Key Encryption Key (KEK)重新生成密钥行为更改。它包括Cisco IOS版本15.2(1)T)和Cisco IOS XE 3.5版本15.2(1)S)。本文解释在它导致的行为和可能性互操作性问题上的此变化。

贡献用温张， Cisco TAC工程师。

旧有行为

在Cisco IOS版本15.2(1)T之前， KEK重新生成密钥由关键服务器(KS)发送，当当前KEK超时时。组成员(GM)不维护计时器记录KEK的剩余寿命。只有当KEK重新生成密钥接收时，当前KEK由一新的KEK替换。如果GM不接收KEK请重新生成密钥在预计KEK终止，不触发再登记对KS，并且将保持现有KEK，无需让它超时。这能导致在其已配置的寿命以后使用的KEK。并且，作为副作用，有no命令在显示剩余的KEK寿命的GM。

新的行为

新的KEK重新生成密钥行为包括两更改：

- 在KS - KEK重新生成密钥在当前KEK终止前发送，很象流量Exchange密钥(TEK)重新生成密钥。
- 在GM -，如果KEK重新生成密钥没有接收， GM维护计时器记录剩余的KEK寿命并且触发再登记。

KS新建的行为

使用新请重新生成密钥行为， KS开始KEK在当前KEK终止前重新生成密钥根据此公式。

注意：在上述计算，红色选中项目部分只与单播一起使用重新生成密钥。

至少200秒，在当前KEK超时前，凭此行为， KS开始重新生成密钥KEK。在重新生成密钥发送后，KS开始使用新的KEK所有随后的TEK/KEK重新生成密钥。

GM新建的行为

新的GM行为包括两更改：

1. 它通过添加计时器记录KEK剩余寿命强制执行KEK寿命终止。当该计时器超时时， KEK在GM删除，并且再登记被触发。
2. GM预计KEK重新生成密钥发生在当前KEK终止之前的至少200秒(请参阅KS行为更改)。另一个计时器被添加，以便在事件新的KEK没有接收在当前KEK终止前的至少200秒， KEK删除，并且再登记被触发。此KEK删除和再登记事件在计时器间隔发生(KEK终止- 190秒， KEK终止- 40秒)。

与功能更改一起，也修改GM **show命令输出**相应地显示KEK剩余寿命。

```
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
```

互操作性问题

使用此KEK请重新生成密钥行为更改，代码互操作性问题需要考虑，当KS和GM也许不运行有此更改的两个IOS版本。

在GM运行更旧的代码的案件中，并且KS运行更新的代码， KS派出KEK在KEK之前重新生成密钥终止，但是没有其他值得注意的功能影响。然而，如果运行更新的代码的GM向运行更旧的代码的KS登记， GM可能导致解释(GDOI)再登记两组域为了接收新的KEK每KEK重新生成密钥周期。当这发生，事件顺序出现：

1. GM在当前KEK终止前再注册，因为KS只将发送KEK重新生成密钥，当当前KEK超时。GM接收KEK，并且它是和一样那个它当前有与少于190秒寿命余留的KEK。这告诉GM注册与KS，不用KEK重新生成密钥更改。

```
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. GM删除KEK在其寿命终止，并且设置再登记计时器(KEK终止， KEK终止+ 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. 当再登记计时器超时时，GM再注册和接收新的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
```

建议

在GETVPN部署，如果其中任一个GM Cisco IOS代码升级到其中一个与新的KEK的版本请重新生成密钥行为，思科建议KS代码升级避免互操作性问题。