中低端防火墙IPsec不定时中断问题处理案例分享

IPSec VPN　孔凡安　2023-11-10 发表

组网及说明

现场的情况为总部（FW）采用IPsec安全策略模板方式与分支（AP）建立基于IKEv的IPsec隧道

告警信息

不涉及

问题描述

现场的故障现象为AP侧和FW的IPsec隧道不定时断开，自动重连失败。需要手工清除IPsec隧道后才能重新连接成功。

AP侧分析故障时收到了FW侧的断开请求，重连隧道失败。要求FW侧同步分析。

```
Wed, 2023-11-01 01:23 14[IKE] <1|21> IKE_SA 1[22] rekeyed between 192.168.1.100[test]...183.203.181.185[183.203.181.185]
Wed, 2023-11-01 01:23 14[IKE] <1|21> rescheduling reauthentication in 0s after rekeying, lifetime reduced to 120s
Wed, 2023-11-01 01:23 14[IKE] <1|21> IKE_SA 1[21] state change: ESTABLISHED => REKEYED
Wed, 2023-11-01 01:23 14[ENC] <1|21> generating CREATE_CHILD_SA response 4 [ SA No KE ]
Wed, 2023-11-01 01:23 14[NET] <1|21> sending packet: from 192.168.1.100[4500] to 183.203.181.185[4500] (300 bytes)
Wed, 2023-11-01 01:23 15[IKE] <1|21> unable to reauthenticate in REKEYED state, delaying for 12s
Wed, 2023-11-01 01:23 10[NET] <1|21> received packet: from 183.203.181.185[4500] to 192.168.1.100[4500] (76 bytes)
Wed, 2023-11-01 01:23 10[ENC] <1|21> parsed INFORMATIONAL request 5 [ D ]
Wed, 2023-11-01 01:23 10[IKE] <1|21> received DELETE for IKE_SA 1[21]
Wed, 2023-11-01 01:23 10[IKE] <1|21> deleting IKE_SA 1[21] between 192.168.1.100[test]...183.203.181.185[183.203.181.185]
Wed, 2023-11-01 01:23 10[IKE] <1|21> IKE_SA 1[21] state change: REKEYED => DELETING
Wed, 2023-11-01 01:23 10[IKE] <1|21> IKE_SA deleted
Wed, 2023-11-01 01:23 10[ENC] <1|21> generating INFORMATIONAL response 5 [ ]
Wed, 2023-11-01 01:23 10[NET] <1|21> sending packet: from 192.168.1.100[4500] to 183.203.181.185[4500] (76 bytes)
Wed, 2023-11-01 01:23 10[IKE] <1|21> IKE_SA 1[21] state change: DELETING => DESTROYING
Wed, 2023-11-01 01:25 10[IKE] <1|22> queueing IKE_DELETE task
Wed, 2023-11-01 01:25 10[IKE] <1|22> activating new tasks
Wed, 2023-11-01 01:25 10[IKE] <1|22>   activating IKE_DELETE task
Wed, 2023-11-01 01:25 10[IKE] <1|22> deleting IKE_SA 1[22] between 192.168.1.100[test]...183.203.181.185[183.203.181.185]
Wed, 2023-11-01 01:25 10[IKE] <1|22> IKE_SA 1[22] state change: ESTABLISHED => DELETING
Wed, 2023-11-01 01:25 10[IKE] <1|22> sending DELETE for IKE_SA 1[22]
Wed, 2023-11-01 01:25 10[ENC] <1|22> generating INFORMATIONAL request 0 [ D ]
Wed, 2023-11-01 01:25 10[NET] <1|22> sending packet: from 192.168.1.100[4500] to 183.203.181.185[4500] (76 bytes)
Wed, 2023-11-01 01:25 13[NET] <1|22> received packet: from 183.203.181.185[4500] to 192.168.1.100[4500] (76 bytes)
Wed, 2023-11-01 01:25 13[ENC] <1|22> parsed INFORMATIONAL response 0 [ D ]
Wed, 2023-11-01 01:25 13[IKE] <1|22> IKE_SA deleted
Wed, 2023-11-01 01:25 13[IKE] <1|22> IKE_SA 1[22] state change: DELETING => DESTROYING
Wed, 2023-11-01 01:25 13[CHD] <1|22> CHILD_SA 1[478] state change: INSTALLED => DESTROYING
```

```
Fri, 2023-11-03 01:20 13[IKE] <1|9> IKE_SA 1[9] state change: ESTABLISHED => REKEYED
Fri, 2023-11-03 01:20 13[ENC] <1|9> generating CREATE_CHILD_SA response 0 [ SA No KE ]
Fri, 2023-11-03 01:20 13[NET] <1|9> sending packet: from 192.168.1.100[4500] to 183.203.181.185[4500] (300 bytes)
Fri, 2023-11-03 01:20 07[NET] <1|9> received packet: from 183.203.181.185[4500] to 192.168.1.100[4500] (76 bytes)
Fri, 2023-11-03 01:20 07[ENC] <1|9> parsed INFORMATIONAL request 1 [ D ]
Fri, 2023-11-03 01:20 07[IKE] <1|9> received DELETE for IKE_SA 1[9]
Fri, 2023-11-03 01:20 07[IKE] <1|9> deleting IKE_SA 1[9] between 192.168.1.100[test]...183.203.181.185[183.203.181.185]
Fri, 2023-11-03 01:20 07[IKE] <1|9> IKE_SA 1[9] state change: REKEYED => DELETING
Fri, 2023-11-03 01:20 07[IKE] <1|9> IKE_SA deleted
Fri, 2023-11-03 01:20 07[ENC] <1|9> generating INFORMATIONAL response 1 [ ]
Fri, 2023-11-03 01:20 07[NET] <1|9> sending packet: from 192.168.1.100[4500] to 183.203.181.185[4500] (76 bytes)
Fri, 2023-11-03 01:20 07[IKE] <1|9> IKE_SA 1[9] state change: DELETING => DESTROYING
Fri, 2023-11-03 01:22 09[IKE] <1|10> queueing IKE_DELETE task
Fri, 2023-11-03 01:22 09[IKE] <1|10> activating new tasks
Fri, 2023-11-03 01:22 09[IKE] <1|10>   activating IKE_DELETE task
Fri, 2023-11-03 01:22 09[IKE] <1|10> deleting IKE_SA 1[10] between 192.168.1.100[test]...183.203.181.185[183.203.181.185]
Fri, 2023-11-03 01:22 09[IKE] <1|10> IKE_SA 1[10] state change: ESTABLISHED => DELETING
Fri, 2023-11-03 01:22 09[IKE] <1|10> sending DELETE for IKE_SA 1[10]
Fri, 2023-11-03 01:22 09[ENC] <1|10> generating INFORMATIONAL request 0 [ D ]
Fri, 2023-11-03 01:22 09[NET] <1|10> sending packet: from 192.168.1.100[4500] to 183.203.181.185[4500] (76 bytes)
Fri, 2023-11-03 01:22 15[NET] <1|10> received packet: from 183.203.181.185[4500] to 192.168.1.100[4500] (76 bytes)
Fri, 2023-11-03 01:22 15[ENC] <1|10> parsed INFORMATIONAL response 0 [ D ]
Fri, 2023-11-03 01:22 15[IKE] <1|10> IKE_SA deleted
Fri, 2023-11-03 01:22 15[IKE] <1|10> IKE_SA 1[10] state change: DELETING => DESTROYING
```

过程分析

首先查看现场配置比较简单，使用的IPsec策略模板的方式建立IPsec隧道。

```
#
 ikev2 dpd interval 20 on-demand
#
ikev2 keychain 1
 peer 2
  identity fqdn test
  pre-shared-key ciphertext $c$3$ea+tyrkuRMjsjkahglajgd/XVc43xMIrmGk=
#
ikev2 profile 1
 authentication-method local pre-share
 authentication-method remote pre-share
 keychain 1
 identity local address X.X.X.X
 match remote identity fqdn test
#
ikev2 proposal 1
 encryption aes-cbc-128
 integrity sha1
 dh group2
#
ikev2 policy 1
 proposal 1
#
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address X.X.X.X 255.255.255.240
 manage https inbound
 manage ping inbound
 manage ssh inbound
 undo dhcp select server
 ipsec apply policy GE0/1
 gateway 183.203.181.177
#
ipsec transform-set 1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec policy-template 1 1
 transform-set 1
 local-address X.X.X.X
 ikev2-profile 1
#
ipsec policy GE0/1 2 isakmp template 1
#
```

针对此类不定时断开的问题，由于输出日志等级的原因，有时仅从记录的logfile信息无法看出异常。因此，需要收集中断前的debug信息方可定位问题。
对应命令如下：

```
RBM_S<F1090_S>debugging ikev2 all remote-address x.x.x.x
```

实际情况是现场隧道很多，且断开的隧道比较随机。因此尝试对所有的隧道开启debug，即不加对端地址。实际如果能在确定对端地址的情况下建议针对性debug，有的放矢。
根据收集信息发现，故障时候FW重传DPD报文没有得到回应，后续删除隧道。

```
*Nov  8 02:36:03:634 2023 H3C IKEV2/7/DPD-MESSAGE: -COntext=1; vrf = 0, src =
```

183.203.181.185, dst = 120.208.142.17/8192

Retransmit DPD packet.

*Nov 8 02:36:03:634 2023 H3C IKEV2/7/DPD-MESSAGE: -COntext=1; vrf = 0, src = 183.203.181.185, dst = 120.208.142.17/8192

Sending packet to 120.208.142.17 remote port 8192, local port 4500.

*Nov 8 02:36:03:634 2023 H3C IKEV2/7/PACKET: -COntext=1; vrf = 0, src = 183.203.181.185, dst = 120.208.142.17/8192

I-SPI: 0a786923a4221b30

R-SPI: ff1ba72b42ed8c98

Message ID: 0

Exchange type: INFORMATIONAL

Flags: REQUEST

Next payload: ENCRYPTED, Length: 76

*Nov 8 02:36:03:634 2023 H3C IKEV2/7/DPD-MESSAGE: -COntext=1; vrf = 0, src = 183.203.181.185, dst = 120.208.142.17/8192

Sending an IPv4 packet.

*Nov 8 02:36:03:634 2023 H3C IKEV2/7/ERROR: -COntext=1; vrf = 0, src = 183.203.181.185, dst = 183.202.198.192/22016

Liveness check timeout.

*Nov 8 02:36:03:634 2023 H3C IKEV2/7/EVENT: -COntext=1; vrf = 0, src = 183.203.181.185, dst = 183.202.198.192/22016

Send delete SA to IPsec, the reason is dpd fail.

%Nov 8 02:36:03:634 2023 H3C IPSEC/6/IPSEC_SA_TERMINATE: -COntext=1; The IPsec SA was deleted.

Reason: An IKE SA deletion message was received.

SA information:

Role: responder

Local address: 183.203.181.185

Remote address: 183.202.198.192

Sour addr: 192.168.100.0/255.255.255.0 Port: 0 Protocol: IP

Dest addr: 172.16.19.0/255.255.255.0 Port: 0 Protocol: IP

Inside VPN instance:

Outside VPN instance:

Inbound AH SPI: 0

Outbound AH SPI: 0

Inbound ESP SPI: 3865425843

Outbound ESP SPI: 3491711361

ACL number:

*Nov 8 02:36:03:634 2023 H3C IKEV2/7/FSM: -COntext=1; vrf = 0, src = 183.203.181.185, dst = 183.202.198.192/22016

Child SA(ESP SPI 0xb3b765e6) deleted.

解决方法

针对此类问题涉及到NAT穿越场景，一般会配置DPD检测，检测失败后，设备删除IKEv2 SA和IPsec SA之后发起完整重协商。

ikev2 dpd命令用来配置全局IKEv2 DPD功能。

undo ikev2 dpd命令用来关闭全局IKEv2 DPD功能。

【命令】

ikev2 dpd interval interval [retry seconds] { on-demand | periodic }

undo ikev2 dpd interval

【缺省情况】

IKEv2 DPD探测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

interval interval：指定触发IKEv2 DPD探测的时间间隔，取值范围为10～3600，单位为秒。对于按需探测模式，指定经过多长时间没有从对端收到IPsec报文，则发送报文前触发一次DPD探测；对于定时探测模式，指触发一次DPD探测的时间间隔。

retry seconds：指定DPD报文的重传时间间隔，取值范围为2～60，单位为秒，缺省值为5秒。

on-demand：指定按需探测模式，即根据流量来探测对端是否存活，在本端发送IPsec报文时，如果发现当前距离最后一次收到对端报文的时间超过指定的触发IKEv2 DPD探测的时间间隔（即通过interval指定的时间），则触发DPD探测。

periodic：指定定时探测模式，即按照触发IKEv2 DPD探测的时间间隔（即通过interval指定的时间）定时探测对端是否存活。

【使用指导】

IKEv2 DPD有两种模式：按需探测模式和定时探测模式。一般若无特别要求，建议使用按需探测模式，在此模式下，仅在本端需要发送报文时，才会触发探测；如果需要尽快地检测出对端的状态，则可以使用定时探测模式。在定时探测模式下工作，会消耗更多的带宽和计算资源，因此当设备与大量的IKEv2对端通信时，应优先考虑使用按需探测模式。

如果IKEv2 profile视图下和系统视图下都配置了DPD探测功能，则IKEv2 profile视图下的DPD配置生效，如果IKEv2 profile视图下没有配置DPD探测功能，则采用系统视图下的DPD配置。

配置的interval一定要大于retry，保证在重传DPD报文的过程中不触发新的DPD探测。

【举例】

配置根据流量来触发IKEv2 DPD探测的时间间隔为15秒。

<Sysname> system-view

[Sysname] ikev2 dpd interval 15 on-demand

配置定时触发IKEv2 DPD探测的时间间隔为15秒。

<Sysname> system-view

[Sysname] ikev2 dpd interval 15 periodic

【相关命令】

- dpd（IKEv2 profile view）

```
*Nov  8 02:36:03:634 2023 H3C IKEV2/7/EVENT: -COntext=1; vrf = 0, src = 183.203.
181.185, dst = 183.202.198.192/22016

 [IKE->IPsec] Send delete DPD request.

*Nov  8 02:36:03:634 2023 H3C IKEV2/7/FSM: -COntext=1; vrf = 0, src = 183.203.18
```