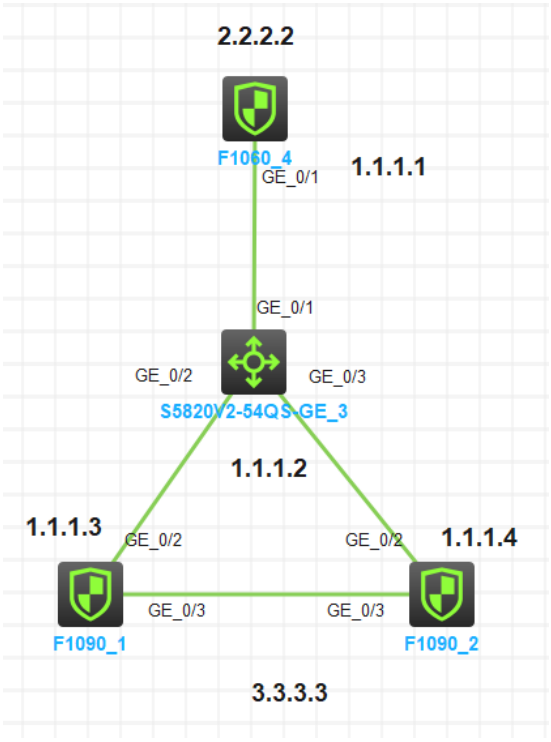
RBM切换后ipsec不通

VRRP 李超 2022-08-23 发表

组网及说明



F1060和F1090建立主模式ipsec，两台F1090做RBM+vrrp主备部署，防火墙起环回地址作为ipsec保护的数据流

问题描述

RBM没有发生切换时，ipsec隧道正常，业务正常，当RBM发生切换后，ipsec出现中断，重置两边的ike sa和ipsec sa之后，可以建立ipsec隧道。

过程分析

当RBM发生主备切换后，出现ping不通的情况

```
56 bytes from 3.3.3.3: icmp_seq=40 ttl=255 time=2.000 ms
56 bytes from 3.3.3.3: icmp_seq=41 ttl=255 time=2.000 ms
56 bytes from 3.3.3.3: icmp_seq=42 ttl=255 time=15.000 ms
Request time out
Request time out
Request time out
Request time out
```

debug显示没有ike sa报文被丢弃

```
RBM_S<H3C>%Aug 23 15:42:42:734 2022 H3C VRRP4/6/VRRP_STATUS_CHANGE: -Context=1;
The status of IPv4 virtual router 1 (configured on GigabitEthernet1/0/2) changed from Backup to Master: Controled by RBM.

*Aug 23 15:42:42:735 2022 H3C IKE/7/EVENT: -Context=1; Received message from ipsec, message type is 8.
*Aug 23 15:42:42:856 2022 H3C IKE/7/EVENT: -Context=1; Received message from ipsec, message type is 6.
*Aug 23 15:42:42:856 2022 H3C IKE/7/ERROR: -Context=1; vrf = 0, local = 1.1.1.2, remote = 1.1.1.1/500
Receive invalid SPI message from IPsec, but no IKE SA exists.
*Aug 23 15:42:45:782 2022 H3C IKE/7/EVENT: -Context=1; Received packet successfully.
*Aug 23 15:42:45:782 2022 H3C IKE/7/PACKET: -Context=1; vrf = 0, local = 1.1.1.2, remote = 1.1.1.1/500
Received packet from 1.1.1.1 source port 500 destination port 500.
*Aug 23 15:42:45:782 2022 H3C IKE/7/PACKET: -Context=1; vrf = 0, local = 1.1.1.2, remote = 1.1.1.1/500

  I-Cookie: c341cec17ec350e0
  R-Cookie: a7aa81bc4a10f75d
  next payload: HASH
  version: ISAKMP Version 1.0
  exchange mode: Info
  flags: ENCRYPT
  message ID: 148774b
  length: 84
*Aug 23 15:42:45:782 2022 H3C IKE/7/EVENT: -Context=1; IKE thread 3051461584 processes a job.
*Aug 23 15:42:45:782 2022 H3C IKE/7/EVENT: -Context=1; Info packet process started.
*Aug 23 15:42:45:782 2022 H3C IKE/7/EVENT: -Context=1; Received informational exchange packet, but IKE SA is inexistent or incomplete.
*Aug 23 15:42:49:135 2022 H3C IKE/7/EVENT: -Context=1; Received packet successfully.
*Aug 23 15:42:49:135 2022 H3C IKE/7/PACKET: -Context=1; vrf = 0, local = 1.1.1.2, remote = 1.1.1.1/500
Received packet from 1.1.1.1 source port 500 destination port 500.
*Aug 23 15:42:49:135 2022 H3C IKE/7/PACKET: -Context=1; vrf = 0, local = 1.1.1.2, remote = 1.1.1.1/500
```

因为F1090是用vrrp虚地址与F1060建立ipsec的，F1090发生RBM切换后，对于F1060是无感知的，所以，从F1060去ping 3.3.3.3时依然匹配与原RBM主协商的ipsec sa发出去，没有重新走ipsec 协商流程，导致对端F1090因为没有ike sa出现不通 的情况。此处从F1090侧重新触发一下ipsec协商后既可以通信。

解决方法

需要在F1060和F1090上都配置dpd检测，DPD（Dead Peer Detection，对等体存活检测）用于检测对端是否存活。本端主动向对端发送DPD请求报文，对对端是否存活进行检测。如果本端在DPD报文的重传时间间隔（retry seconds）内未收到对端发送的DPD回应报文，则重传DPD请求报文，若重传两次之后仍然没有收到对端的DPD回应报文，则删除该IKE SA和对应的IPsec SA。

配置dpd之后RBM切换后，重新触发ipsec协商，协商完成后ping能够正常通信

ike dpd interval 3 retry 3 periodic