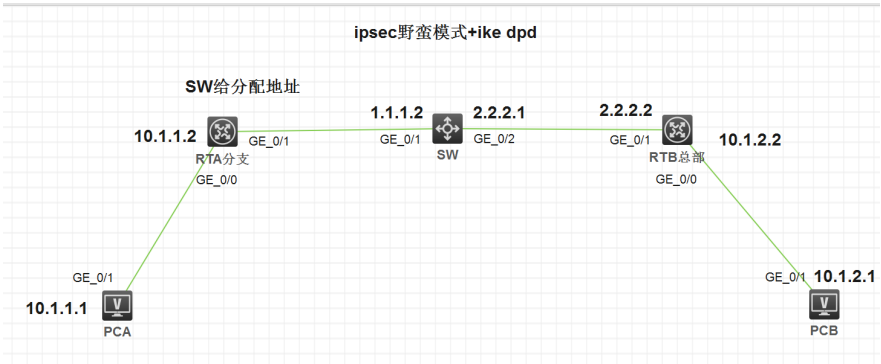
某局点 MSR设备 ipsec野蛮模式 配置ike dpd协商不起来

IPSec VPN 苏清秀 2020-02-21 发表

组网及说明



组网介绍：

RTA的G0/1口地址是动态获取的，由SW分配，SW是dhcp server，RTA与RTB通过ike 野蛮模式建立ipsec隧道。

相关设备配置：PCA和PCB的配置，以及各接口的IP地址自己配置上。

问题描述

MSR设备与第三方防火墙对接，在两个设备上面配合IKE DPD（注意模式要一致）

测试在第三方防火墙侧点击“隧道拆除（即等同于手动添加reset ike sa reset ipsec sa这两个命令）”，MSR不能感知，只能手动删除ike sa和ipsec sa才行，也就是说ike dpd没有生效。

过程分析

在第三方防火墙上点击“隧道拆除”，ike dpd没有效果，有两种可能性：

（1）我司MSR设备没有回包给第三方防火墙；

（2）回包了，但是对端没有收到。

模拟器的实验效果Ike dpd是可以生效的：

ipsec隧道能够正常建立，两端私网也能通，并且能够看到dpd报文的交互：

```
    98 15180.699558  1.1.1.1             2.2.2.2             ESP          150 ESP (SPI=0x0d1b092b)
    99 15180.706078  2.2.2.2             1.1.1.1             ESP          150 ESP (SPI=0xec8839b2)
   100 15180.909240  1.1.1.1             2.2.2.2             ESP          150 ESP (SPI=0x0d1b092b)
   101 15180.911669  2.2.2.2             1.1.1.1             ESP          150 ESP (SPI=0xec8839b2)
   102 15181.115089  1.1.1.1             2.2.2.2             ESP          150 ESP (SPI=0x0d1b092b)
   103 15181.117836  2.2.2.2             1.1.1.1             ESP          150 ESP (SPI=0xec8839b2)
   104 15181.322360  1.1.1.1             2.2.2.2             ESP          150 ESP (SPI=0x0d1b092b)
   105 15181.324765  2.2.2.2             1.1.1.1             ESP          150 ESP (SPI=0xec8839b2)
   106 15182.507868  6c:45:1a:f3:01:04    Broadcast           0xb003        22 Ethernet II
   107 15182.593993  6c:45:3f:9a:03:04    Broadcast           0xb003        22 Ethernet II
   108 15184.547894  6c:45:1a:f3:01:04    Broadcast           0xb003        22 Ethernet II
   109 15184.674529  6c:45:3f:9a:03:04    Broadcast           0xb003        22 Ethernet II
   110 15186.594935  6c:45:1a:f3:01:04    Broadcast           0xb003        22 Ethernet II
   111 15186.754105  6c:45:3f:9a:03:04    Broadcast           0xb003        22 Ethernet II
   112 15188.690599  6c:45:1a:f3:01:04    Broadcast           0xb003        22 Ethernet II
   113 15188.863260  6c:45:3f:9a:03:04    Broadcast           0xb003        22 Ethernet II
   114 15189.573089  2.2.2.2             1.1.1.1             ISAKMP       126 Informational
   115 15189.574323  1.1.1.1             2.2.2.2             ISAKMP       126 Informational
   116 15189.580061  1.1.1.1             2.2.2.2             ISAKMP       126 Informational
   117 15189.582522  2.2.2.2             1.1.1.1             ISAKMP       126 Informational
   118 15190.787172  6c:45:1a:f3:01:04    Broadcast           0xb003        22 Ethernet II
```

看debug结果，能够发现ike dpd就是RTA与RTB两端互相发送 R_U_THERE和R_U_THERE_ACK报文，相互交互的过程。

*Jan 19 13:29:08:073 2020 RTA IKE/7/EVENT: vrf = 0, src = 1.1.1.1, dst = 2.2.2.2/500Notification R_U_THERE is received.

*Jan 19 13:29:08:073 2020 RTA IKE/7/DPD: vrf = 0, src = 1.1.1.1, dst = 2.2.2.2/500DPD packet with sequence number 15775 is received.

*Jan 19 13:29:08:073 2020 RTA IKE/7/EVENT: Sending DPD packet of type R_U_THERE_ACK with sequence number 15775.

*Jan 19 13:29:08:073 2020 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.2/500Encrypt the packet.

*Jan 19 13:29:08:073 2020 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.2/500Construct notification packet: R_U_THERE_ACK.

*Jan 19 13:29:08:073 2020 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.2/500Sending packet to 2.2.2.2 remote port 500, local port 500.

*Jan 19 13:29:08:073 2020 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.2/500

解决方法

解决方案：
（1）建议两端同时抓包或者开debug看一下报文的交互过程；
（2）确保两端的ike dpd模式配置一致。
相关设备的配置如下：
RTA：

```
#
sys
ip route-static 10.1.2.0 24 1.1.1.2
int g 0/1
 ip add dhcp-alloc
qu
acl advanced 3000
  rule 0 permit ip source 10.1.1.0 0.0.0.255 dest 10.1.2.0 0.0.0.255
qu
ipsec transform-set t1
 enca-mode tunnel
 protocol esp
 esp encry 3des-cbc
 esp authen md5
qu
ike keychain k1
 pre-shared-key add 2.2.2.2 24 key simple h3c
qu
ike dpd interval 10 retry 5 periodic
ike profile p1
  keychain k1
 exchange-mode addressive
 local-identity fqdn rta
 match remote identity address 2.2.2.2
qu
ipsec policy m1 1 isakmp
  security acl 3000
 ike-profile p1
 transform-set t1
remote-add 2.2.2.2
qu
int g 0/1
 ipsec apply policy m1
qu
#
```

SW：

```
#
sys
dhcp enabledhcp server ip-pool 1
  network 1.1.1.0 mask 255.255.255.0
 gateway-list 1.1.1.2
qu
#
```

RTB:

```
#
sys
acl advanced 3000
  rule 0 permit ip source 10.1.2.0 0.0.0.255 dest 10.1.1.0 0.0.0.255
qu
ipsec transform-set t1
  enca-mode tunnel
  protocol esp
  esp encry 3des-cbc
  esp authen md5quike keychain k1
  pre-shared-key hostname rta key simple h3c
qu
ike profile p1
    keychain k1
   exchange-mode aggressive
```

```
    local-identity address 2.2.2.2
    match remote identity fqdn rta
qu
ike dpd interval 10 retry 5 periodic
ipsec policy-template tem1 1
     security acl 3000
     ike-profile p1
    transform-set t1
    local-address 2.2.2.2
qu
ipsec policy n1 1 isakmp template tem1  1
int g 0/1
  ipsec apply policy n1
qu
#
```