某局点MSR3660路由器和天融信防火墙建立GRE over IPSec VPN不通的经验案例

GRE VPN IPSec VPN 李聪 2018-06-28 发表

组网及说明

无

问题描述

某局点使用MSR3660路由器和天融信防火墙建立GRE over IPSec VPN不通，现场反馈IPSec VPN和GRE隧道都是建立起来的，但是数据不通。接下来针对这个问题进行分析。

过程分析

1、搜集配置进行分析

现场反馈建立IPSec VPN和GRE隧道都是使用的公网地址进行配置的，IPSec VPN保护的感兴趣流也是源目公网地址。具体配置如下（公网地址不是客户真实地址）：

```
#配置感兴趣流
acl advanced 3107
 rule 0 permit gre source 111.111.111.111 0 destination 222.222.222.222 0
#配置ike keychain
ike keychain wuhan_1
 pre-shared-key address 222.222.222.222 255.255.255.255 key cipher $c$3$+z622GBHXswjD77qm7wlcjGMKTIVYmB/TGI=
#配置ike profile
ike profile wuhan_1
 keychain wuhan_1
 local-identity address 111.111.111.111
 match remote identity address 222.222.222.222 255.255.255.255
#配置IPSec提议
ipsec transform-set wuhan_1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#配置IPSec policy策略
ipsec policy policy1 7 isakmp
 transform-set wuhan_1
 security acl 3107
 local-address 111.111.111.111
 remote-address 222.222.222.222
 ike-profile wuhan_1
```

最后需要将IPSec policy策略调用在外网接口。

```
#创建tunnel接口，并且协议为GRE：
interface Tunnel7 mode gre
 ip address 10.16.253.9 255.255.255.252
 source 111.111.111.111
 destination 222.222.222.222
 keepalive 6 3
```

通过上面的配置并没有看出问题，GRE建立和IPSec VPN建立都使用公网地址也是按理来说是可行的。现场也搜集display ike sa以及display ipsec sa信息发现IPSec VPN都是建立成功的。

2、分析问题原因

发现执行命令reset ike sa和reset ipsec sa之后ping测试依然可以成功建立IPSec隧道和GRE隧道。接下来通过执行ping测试，并且观察display ipsec statistics信息进行分析。

（1）当我们设备终端主动往对方发包时，执行display ipsec statistics看到我们设备有发送的报文，但是没有收到对方的回复报文：

```
[H3C]display ipsec statistics

  IPsec packet statistics:

    Received/sent packets: 0/15

    Received/sent bytes: 0/1320
```

Dropped packets (received/sent): 15/0

Dropped packets statistics

No available SA: 0

现场和天融信工程师确认之后，天融信并没有收到我们发过去的报文。于是我们设备开启debugging ip packet acl观察报文的处理过程，发现我们的报文已经发出，并且是发出去的接口是tunnel 7的GRE隧道接口，说明我们设备处理没有问题。

（2）天融信设备往我们路由器发包，执行display ipsec statistics看到我们设备有接收到报文，并且也有回复报文：

[H3C]display ipsec statistics

IPsec packet statistics:

Received/sent packets: 15/15

Received/sent bytes: 1320/1320

Dropped packets (received/sent): 0/0

Dropped packets statistics

No available SA: 0

但是对方设备抓包还是没有看到我们设备的回包。同样在我们设备debugging ip packet acl进行分析也没有发现问题，我们设备从tunnel 7接口收到报文处理之后也将报文发往tunnel隧道。

（3）定位问题

通过测试发现我们设备发往天融信的方向出现了问题，怀疑是外网原因导致的。外网原因一般就是网络质量不好或者外网运营商设备不能通过比较大的报文。因此尝试在外网接口修改mtu也没有解决问题。

但是从上面的配置我们可进一步分析，发现终端的报文进入GRE隧道之后今天公网地址封装，然后再次进行IPSec封装。这样的话对于一个建立隧道使用的公网地址进行了两次封装，怀疑是公网地址封装报文层数导致的，因此建议两边的设备配置GRE隧道协商的地址改为私网地址进行协商，然后IPSec再保护这个建立GRE隧道的私网地址。

于是，我们设备的配置修改了以下几点地方进行测试：

a、创建loopback接口，配置为私网地址，用来协商GRE使用的。

b、将IPSec VPN保护的感兴趣流改为本地loopback地址到对方设备的loopback接口地址。

具体配置如下：

```
#创建loopback接口：
interface LoopBack1
 ip address 192.168.1.1 255.255.255.255
#配置感兴趣流为loopback接口地址
acl advanced 3107
 rule 0 permit gre source 192.168.1.1 0 destination 192.168.1.2 0
#配置ike keychain
ike keychain wuhan_1
 pre-shared-key address 222.222.222.222 255.255.255.255 key cipher $c$3$+z622GBHXswjD77qm
7wlcjGMKTIVYmB/TGI=
#配置ike profile
ike profile wuhan_1
 keychain wuhan_1
 local-identity address 111.111.111.111
 match remote identity address 222.222.222.222 255.255.255.255
#配置IPSec提议
ipsec transform-set wuhan_1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#配置IPSec policy策略
ipsec policy policy1 7 isakmp
 transform-set wuhan_1
 security acl 3107
 local-address 111.111.111.111
```

remote-address 222.222.222.222
ike-profile wuhan_1
最后需要将IPSec policy策略调用在外网接口。
#创建tunnel接口，并且协议为GRE：
interface Tunnel7 mode gre
ip address 10.16.253.9 255.255.255.252
source 192.168.1.1
destination 192.168.1.2
keepalive 6 3
通过上面配置之后，现场IPSec VPN和GRE隧道正常协商，通过ping测试之后业务正常。说明一点，在复杂的公网环境中，建议协商GRE隧道的地址使用内网地址协商，IPSec VPN封装保护GRE隧道协商地址即可。避免了复杂的公网环境导致的异常情况。

解决方法

1、建loopback接口，配置为私网地址，用来协商GRE使用的。
2、IPSec VPN保护的感兴趣流改为本地loopback地址到对方设备的loopback接口地址。
通过上面的配置可以避免复杂的公网环境对报文封装的影响。