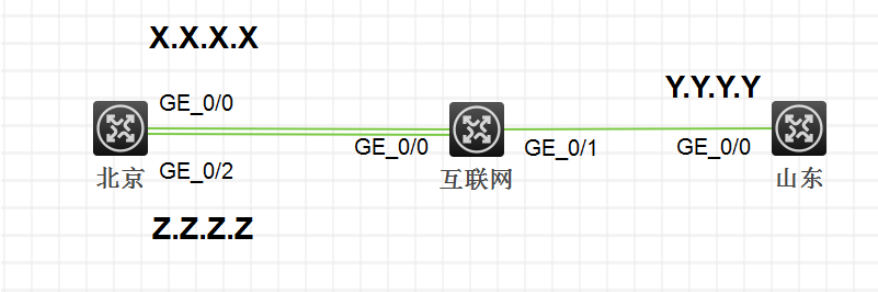
MSR3610在负载分担的情况下两端ipsec建立不起来

IPsec 王喆兴 2018-02-26 发表

组网如图北京侧双出口与山东侧互联，X.X.X.X与Y.Y.Y.Y之间建立ipsec连接。北京侧的两个口均配置了NAT地址转换。
两侧ipsec一直建立不起来。



在两侧设备上debug ike all，山东侧触发连接。发现山东侧发出去了ike协商报文。
[10:00:26]Sending packet to X.X.X.X remote port 500, local port 500.
[10:00:26]*Feb 23 09:48:22:223 2018 SSGM-JN IKE/7/PACKET: vrf = 0, src = Y.Y.Y.Y, dst = X.X.X.X /500
[10:00:26]
[10:00:26] I-COOKIE: 9aa32a24f774818f
[10:00:26] R-COOKIE: 0000000000000000
[10:00:26] next payload: SA
[10:00:26] version: ISAKMP Version 1.0
[10:00:26] exchange mode: Main
[10:00:26] flags:
[10:00:26] message ID: 0
[10:00:26] length: 176
北京侧也收到了此协商报文。
[10:00:26]Received packet from Y.Y.Y.Y source port 500 destination port 500.
[10:00:26]*Feb 23 09:45:27:196 2018 SSGM-BJ IKE/7/PACKET: vrf = 0, local = X.X.X.X, remote = Y.Y.Y.Y/500
[10:00:26]
[10:00:26] I-COOKIE: 9aa32a24f774818f
[10:00:26] R-COOKIE: 0000000000000000
[10:00:26] next payload: SA
[10:00:26] version: ISAKMP Version 1.0
[10:00:26] exchange mode: Main
[10:00:26] flags:
[10:00:26] message ID: 0
[10:00:26] length: 176
但是北京侧没有给予回应，而是发起了新的IKE协商，达到山东侧后发现地址为北京侧G0/2口的地址。
[10:00:29]Sending packet to Y.Y.Y.Y remote port 500, local port 500.
[10:00:29]*Feb 23 09:45:30:662 2018 SSGM-BJ IKE/7/PACKET: vrf = 0, local = X.X.X.X, remote = Y.Y.Y.Y/500
[10:00:29]
[10:00:29] I-COOKIE: 1645329acca28453
[10:00:29] R-COOKIE: 0000000000000000
[10:00:29] next payload: SA
[10:00:29] version: ISAKMP Version 1.0
[10:00:29] exchange mode: Main
[10:00:29] flags:
[10:00:29] message ID: 0
山东侧收到的报文。
[10:00:30]Received packet from Z.Z.Z.Z source port 1 destination port 500.
[10:00:30]*Feb 23 09:48:25:707 2018 SSGM-JN IKE/7/PACKET: vrf = 0, src = Y.Y.Y.Y, dst = Z.Z.Z.Z/1
[10:00:30]
[10:00:30] I-COOKIE: 1645329acca28453

[10:00:30] R-COOKIE: 0000000000000000
[10:00:30] next payload: SA
[10:00:30] version: ISAKMP Version 1.0
[10:00:30] exchange mode: Main
[10:00:30] flags:
[10:00:30] message ID: 0
[10:00:30] length: 196

检查北京侧的ipsec相关配置，没有发现异常。

```
#
ipsec transform-set ssgmjn
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy ssgmjn 1 isakmp
 transform-set ssgmjn
 security acl 3333
 local-address X.X.X.X
 remote-address Y.Y.Y.Y
 ike-profile ssgmjn
#
ike profile ssgmjn
 keychain ssgmjn
 match remote identity address Y.Y.Y.Y 255.255.255.255
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain ssgmjn
 pre-shared-key address Y.Y.Y.Y 255.255.255.255 key cipher
$c$3$6meEvo5vu6k8y74sY34caa7qZAgkXVZQ4lcj
#
```

查看端口配置，发现两个端口下均有nat outbound 3000 的配置。

```
 #
interface GigabitEthernet0/2
 port link-mode route
 ip address Z.Z.Z.Z 255.255.255.252
 ip address 124.207.69.82 255.255.255.252 sub
 ip last-hop hold
 nat outbound 3000
 nat server protocol tcp global 124.207.69.82 80 inside 172.16.4.50 8080
 nat server protocol tcp global 124.207.69.84 62221 inside 10.10.10.212 80
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address X.X.X.X 255.255.255.252
 tcp mss 1024
 ip last-hop hold
 nat outbound 3000
 nat server protocol tcp global X.X.X.X 443 inside 10.10.10.215 443
 nat server protocol tcp global X.X.X.X 1195 inside 10.10.10.39 1195
```

检查acl 3000，发现其中有一条permit ip。

```
acl advanced 3000
 rule 0 deny ip source 172.16.4.0 0.0.0.255 destination 10.10.11.0 0.0.0.255
 rule 1 deny ip source 172.16.4.0 0.0.0.255 destination 172.16.8.0 0.0.0.255
 rule 2 deny ip source 10.10.10.0 0.0.0.255 destination 10.10.11.0 0.0.0.255
 rule 3 deny ip source 10.10.10.0 0.0.0.255 destination 172.16.8.0 0.0.0.255
 rule 4 deny ip source 172.16.1.0 0.0.0.255 destination 172.16.8.0 0.0.0.255
 rule 5 deny ip source 172.16.1.0 0.0.0.255 destination 10.10.11.0 0.0.0.255
 rule 10 permit ip
```

由于北京侧设备两个口走的是负载分担。当流量选择走G0/2口后，nat outbound 3000将其转换为自己

接口地址Z.Z.Z.Z与山东侧进行协商。而ipsec配置中没有此地址，因此两台设备一直无法协商成功。

在acl 3000中加一条deny ip source X.X.X.X 0 destination Y.Y.Y.Y 0，不让NAT 对ipsec的相关协商报文进行地址转换。这样无论触发的流量走哪个口，均不会影响到ipsec的协商报文。

遇到ipsec的相关问题，先检查哪一阶段协商不成功，debug ike all或ipsec all进行定位。检查ipsec相关配置时也要留心协商报文出接口的配置。