



某局点comwareV7设备IPSEC内网不通

IPSec VPN

孔德飞

2022-06-18 发表

组网及说明

PC1-----核心SW1-----1/0/1出口FW1（ipsec 1/0/2）-----公网-----对端出口设备-----对端核心SW2-----PC2

告警信息

不涉及

问题描述

PC2无法访问PC1

过程分析

首先保证本端出口FW到对端IPSEC设备的IPSEC隧道的感兴趣流只有一条，最好指明源目IP，这样做的目的是为了排除干扰流量

PC2访问PC1的时候，通过查看内层会话，发现PC2-----PC1的报文有10个，PC1----PC2的报文也有10个

通过display ipsec statistics tunnel-id 0发现FW1发出的报文只有6个，说明FW没有将加密后的报文成功发出

首先将ipsec允许分片的命令打开

在接口GigabitEthernet1/0/2上设置IPsec封装后外层IP头的DF位。

```
[Sysname] interface gigabitethernet 1/0/2
```

```
[Sysname-GigabitEthernet1/0/2] ipsec df-bit clear
```

第二，开启ipsec支持加密后的报文分片

```
[Sysname] ipsec fragmentation after-encryption
```

debug显示加密前的报文没有发出，那就不用开启ipsec fragmentation after-encryption，因为默认就是允许IPSEC加密前的报文分片

将IPSEC隧道已经建立，但是内网不通的排查方法整理如下：

如果IPSEC已经建立，如果内网不通，按照如下思路排查：

1. 针对内网IP源目写一条ACL，首先debug ip packet、debug ip info、debug security-policy、debug aspf packet，看一下是否有策略阻断或者状态异常
2. 如果策略正常放通，那就查看内层会话，看一下会话是否正常，回程报文的地址是否是内网地址，如果是公网地址，说明命中了NAT，那就需要检测接口的NAT相关配置
display session table ipv4 destination-ip 10.0.0.1 protocol icmp verbose

接口的配置NAT outbound，带名字的ACL要优先匹配，字符靠前的优先匹配

其次是带数字的ACL匹配，最后是不带ACL的匹配，一条流量会遍历接口下的所有NAT配置，看能否做NAT

3. 如果进行前两步操作内网依然不通，那就在分支上将感兴趣流只保留一条内网服务器互访的时候，总部与分支分别查看ipsec统计以及内存会话查看ipsec统计的命令如下：

(1) 首先通过display ipsec sa确认ipsec sa的tunnel id

```
[H3C]display ipsec sa
```

```
Interface: GigabitEthernet0/2
```

```
IPsec policy: policy1
```

```
Sequence number: 1
```

```
Mode: ISAKMP
```

```
Tunnel id: 0
```

```
Encapsulation mode: tunnel
```

(2) 然后通过tunnel-id查看ipsec收发包统计

```
[H3C]display ipsec statistics tunnel-id 0
```

```
IPsec packet statistics:
```

```
Received/sent packets: 19/19
```

```
Received/sent bytes: 1672/1672
```

```
Dropped packets (received/sent): 0/0
```

```
Dropped packets statistics
```

```
No available SA: 0
```

```
Wrong SA: 0
```

```
Invalid length: 0
```

```
Authentication failure: 0
```

```
Encapsulation failure: 0
```

```
Decapsulation failure: 0
```

```
Replayed packets: 0
```

```
ACL check failure: 0
```

```
MTU check failure: 0
```

```
Loopback limit exceeded: 0
```

```
Crypto speed limit exceeded: 0
```

