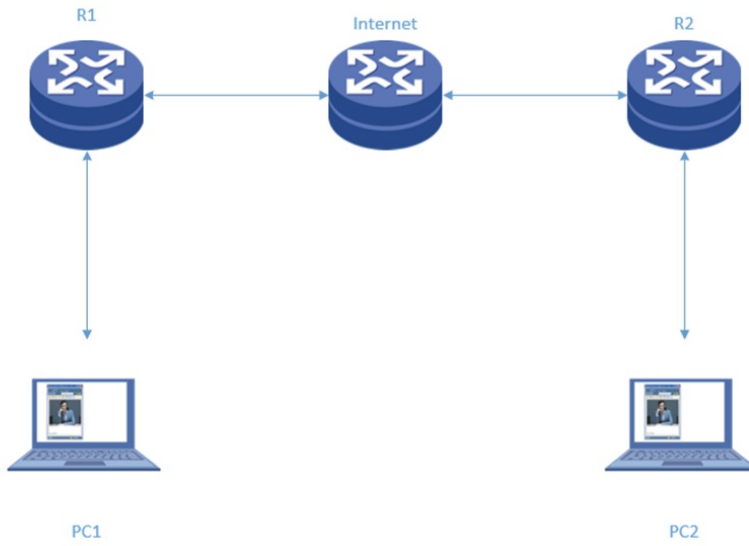


知 IPsec隧道正常建立, IPsec业务丢包

IPSec VPN 柳志翔 2023-06-29 发表

组网及说明



R1为我司MSR3610-X1,R2设备是其他厂商设备, 通过公网地址建立IPsec隧道。

告警信息

```
来自 [redacted].8 的回复: 字节=32 时间=31ms TTL=123
来自 [redacted].8 的回复: 字节=32 时间=44ms TTL=123
来自 [redacted].8 的回复: 字节=32 时间=31ms TTL=123
请求超时。
请求超时。
来自 [redacted].8 的回复: 字节=32 时间=48ms TTL=123
来自 [redacted].8 的回复: 字节=32 时间=43ms TTL=123
请求超时。
请求超时。
请求超时。
请求超时。
来自 [redacted].8 的回复: 字节=32 时间=31ms TTL=123
```

Ipssec隧道正常建立后ping对端PC2地址，发现有丢包。

问题描述

IPsec正常建立, IPsec业务有丢包。

过程分析

查看IPsec 隧道丢包数没有增长

Ping前

```
<H3C>display ipsec statistics
```

IPsec packet statistics:

Received/sent packets: 1645/158253

Received/sent bytes: 126464/12945256

Dropped packets (received/sent): 0/63598

Dropped packets statistics

No available SA: 63598

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

Ping后

```
<H3C>display ipsec statistics
```

IPsec packet statistics:

Received/sent packets: 1735/167518

Received/sent bytes: 132224/13714416

Dropped packets (received/sent): 0/63598

Dropped packets statistics

No available SA: 63598

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

接口流量也未打满

Eth-channel3/0/0

Current state: UP

Line protocol state: UP

Last 300 seconds input rate: 2910.07 bytes/sec, 23280 bits/sec, 33.16 packets/sec

Last 300 seconds output rate: 4522.48 bytes/sec, 36179 bits/sec, 36.91 packets/sec

GigabitEthernet0/0

Current state: UP

Line protocol state: UP

Description: LAN-interface

Bandwidth: 1000000 kbps

Maximum transmission unit: 1500

Allow jumbo frames to pass

Last 300 second input: 10 packets/sec 1059 bytes/sec 0%

Last 300 second output: 7 packets/sec 904 bytes/sec 0%

设备信号也正常

Current RSSI: -44 dBm

Current RSRQ: -8 dB

Current RSRP: -76 dBm

Current SNR: 10 dB

解决方法: -24 dBm

排查对端设备链路后恢复正常。
在路由器上做ipsec流统看下流量是否丢在路由器上

```
acl number 3333
```

```
rule 0 permit icmp source X.X.X.X 0 destination Y.Y.Y.Y 0
```

```
rule 1 permit icmp source Y.Y.Y.Y 0 destination X.X.X.X 0
```

```
#
```

```
traffic classifier 1 operator and
```

```
if-match acl 3333
```

```
traffic behavior 1
```

```
filter permit
```

```
qos policy 1
```

```
classifier 1 behavior 1
```

```
IPsec policy XXX 10 isakmp
```

```
qos pre-classify //QoS使用IPsec封装后报文的外层IP头信息来对报文进行分类
```

在内网接口和外网接口都应用

```
Interface G0/0
```

```
qos apply policy 1 outbound
```

```
qos apply policy 1 inbound
```

```
interface Eth-channel3/0:0
```

```
qos apply policy 1 outbound
```

```
qos apply policy 1 inbound
```

清除下设备接口计数

```
reset counters interface
```

ping完后收集

```
display qos policy interface
```

```
[H3C]display qos policy interface
```

```
Interface: Eth-channel3/0:0
```

```
Direction: Inbound
```

```
Policy: 1
```

```
Classifier: 1
```

```
Matched : 104 (Packets) 7696 (Bytes)
```

```
5-minute statistics:
```

```
Forwarded: 0/191 (pps/bps)
```

```
Dropped : 0/0 (pps/bps)
```

```
Operator: AND
```

```
Rule(s) :
```

```
If-match acl 3333
```

```
Behavior: 1
```

```
Filter enable: Permit
```

```
Interface: Eth-channel3/0:0
```

```
Direction: Outbound
```

```
Policy: 1
```

```
Classifier: 1
```

```
Matched : 147 (Packets) 18522 (Bytes)
```

```
5-minute statistics:
```

```
Forwarded: 0/460 (pps/bps)
```

```
Dropped : 0/0 (pps/bps)
```

```
Operator: AND
```

```
Rule(s) :
```

```
If-match acl 3333
```

```
Behavior: 1
```

```
Filter enable: Permit
```

Interface: GigabitEthernet0/0