

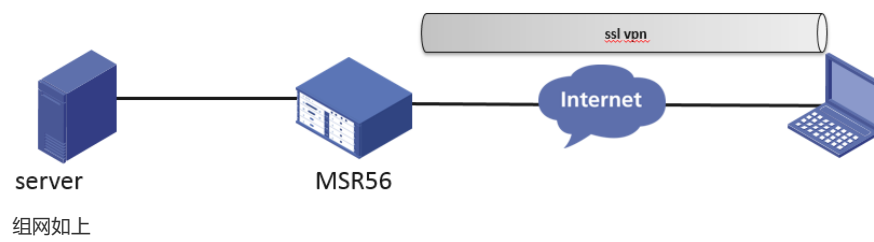
知 SSL VPN 拨入MSR56无法使用内网口地址telnet

SSL VPN

郭尧

2022-11-30 发表

组网及说明



问题描述

在PC上拨SSL VPN能够正常建立隧道，现场想在PC上通过MSR56的内网口地址登录设备WEB或者命令行，但测试无法进行登陆。

```
sslvpn ip address-pool sslvpnpool 192.120.1.2 192.120.1.50
```

```
#
```

```
sslvpn gateway ssl
```

```
ip address x.x.x.x port 9943
```

```
service enable
```

```
#
```

```
sslvpn context ssl
```

```
gateway ssl
```

```
ip-tunnel interface SSLVPN-AC1
```

```
ip-tunnel address-pool sslvpnpool mask 255.255.255.0
```

```
uri-acl uriacl
```

```
rule 1 permit uri tcp://10.19.1.0/24
```

```
rule 2 permit uri http://10.19.1.0/24
```

```
file-policy ssl
```

```
ip-route-list ssl
```

```
include 10.19.1.0 255.255.255.0
```

```
policy-group ssl
```

```
filter ip-tunnel acl 3000
```

```
filter web-access acl 3000
```

```
filter tcp-access acl 3000
```

```
filter ip-tunnel uri-acl uriacl
```

```
ip-tunnel access-route ip-route-list ssl
```

```
service enable
```

过程分析

进行如下步骤测试与信息排查

1. 内网口地址能可以ping通, telnet或者SSH失败, WEB无法打开。访问公网口地址是正常的。
2. telnet的时候设备上debug只有收, 看不到发, 尝试修改AC口的MTU值, 无效果。
3. 终端抓包发现, telnet的时候, PC与设备tcp建立不成功, PC发出了SYN,没有收到SYN ACK, 之后超时断连。

2022-04-24 18:31:05.110173	1 143.120.1.2	10.19.1.4	66 TCP	58458 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-04-24 18:31:06.111058	2 143.120.1.2	10.19.1.4	66 TCP	[TCP Retransmission] 58458 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-04-24 18:31:06.112184	3 143.120.1.2	10.19.1.4	66 TCP	[TCP Retransmission] 58458 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-04-24 18:31:12.112959	4 143.120.1.2	10.19.1.4	66 TCP	[TCP Retransmission] 58458 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-04-24 18:31:20.113729	5 143.120.1.2	10.19.1.4	66 TCP	[TCP Retransmission] 58458 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-04-24 18:35:47.459676	42 143.120.1.2	10.19.1.4	66 TCP	58679 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-04-24 18:35:47.459832	43 143.120.1.2	10.19.1.4	66 TCP	58688 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-04-24 18:35:47.459923	44 143.120.1.2	10.19.1.4	66 TCP	58697 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

4. debug tcp看, 平台是有发出syn ack的。

TCP Input(vrf = 0, state = LISTEN):

TCP packet: src = 143.120.1.2/64532, dst = 10.19.1.4/23

seq = 2288982862, ack = 0, flag = **SYN**

window = 64240, checksum = 0x38a5, datalen = 0, headlen = 32

*Apr 25 13:50:32:579 2022 MSR5620 SOCKET/7/TCP:

TCP Synrespond(vrf = 0, state = SYN_RCVD):

TCP packet: src = 10.19.1.4/23, dst = 143.120.1.2/64532

seq = 2590124407, ack = 2288982863, flag = **SYN ACK**

window = 4096, checksum = 0x60b1, datalen = 0, headlen = 32

5. 由于终端没收到, 需要排查驱动是否发出, debug physical可以看到我们没有发送SYN ACK, 因此问题出现在设备上。

2022-04-25 14:01:31.000533	534 60.191.99.139	61.240.144.70	64 TCP	46150 → 9943 [SYN] Seq=3909974160 Win=64240 MSS=1200 WS=256 [RstLen=0]
2022-04-25 14:01:31.000535	536 60.191.99.139	61.240.144.70	60 TCP	35006 → 23 [ACK] Seq=1 Ack=201795 Win=512 Len=0
2022-04-25 14:01:31.000536	537 60.191.99.139	61.240.144.70	60 TCP	35006 → 23 [ACK] Seq=1 Ack=204195 Win=515 Len=0
2022-04-25 14:01:31.000537	538 60.191.99.139	61.240.144.70	60 TCP	[TCP ACKed unseen segment] 35006 → 23 [ACK] Seq=1 Ack=205667 Win=515 Len=0
2022-04-25 14:01:31.000553	554 60.191.99.139	61.240.144.70	60 TCP	46150 → 9943 [RST] Seq=1 Win=0 Len=0
2022-04-25 14:01:31.000555	556 60.191.99.139	61.240.144.70	60 TCP	[TCP ACKed unseen segment] 35006 → 23 [ACK] Seq=1 Ack=206431 Win=515 Len=0

6. debug sslvpn 可以看出, 故障是因为主控上没有会话导致无法匹配, 而跨设备正常是因为包都在spu板子上进行交互。

内网口登陆设备-故障时候:

*Apr 26 14:28:56:800 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; SSLVPN-AC1 input packet:

*Apr 26 14:28:56:800 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0000 45 00 00 34 f b d 4 0 0 0 80 06 63 5e 8f 78 01 02

*Apr 26 14:28:56:800 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0010 0a 13 01 04 e d 37 00 17 9d 6b 62 a1 00 00 00 00

*Apr 26 14:28:56:800 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0020 80 02 fa f0 eb 32 00 00 02 04 05 b4 01 03 03 08

*Apr 26 14:28:56:800 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0030 01 01 04 02

*Apr 26 14:28:56:800 2022 MSR5620 SSLVPNK/7/SSLVPN_EVENT: -Slot=2; IPAC: Found peer 143.120.1.2.

*Apr 26 14:28:57:800 2022 MSR5620 SSLVPNK/7/SSLVPN_EVENT: -Slot=2; IPAC: The check result of the referenced address pool is 1.

*Apr 26 14:28:57:800 2022 MSR5620 SSLVPNK/7/SSLVPN_EVENT: -Slot=2; IPAC: Received 56 bytes of user traffic: cContextID=0x1, OnlineID=0x16

*Apr 26 14:28:58:290 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: SSLVPN-AC1 output packet:

*Apr 26 14:28:58:290 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: 0000 45 c0 00 34 df 2b 00 0 0 ff 06 40 47 0a 13 01 04

*Apr 26 14:28:58:290 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: 0010 8f 78 01 02 00 17 ed 37 bb a5 4d 0d 9d 6b 62 a2

*Apr 26 14:28:58:290 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: 0020 80 12 10 00 ce 65 00 00 02 04 05 b4 01 03 03 08

*Apr 26 14:28:58:290 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: 0030 04 02 00 00

*Apr 26 14:28:58:290 2022 MSR5620 SSLVPNK/7/SSLVPN_ERROR: IPAC: Failed to find peer 143.120.1.2 in VPN instance 0.

*Apr 26 14:28:58:290 2022 MSR5620 SSLVPNK/7/SSLVPN_ERROR: IPAC: Failed to get data of peer 143.120.1.2.

登陆内部服务器正常的时候:

*Apr 26 14:37:58:304 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; SSLVPN-AC1 input packet:

*Apr 26 14:37:58:304 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0000 45 00 00 32 e c a0 40 00 80 06 72 96 8f 78 01 02

*Apr 26 14:37:58:304 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0010 0a 13 01 02 e
e b0 00 17 bc 31 8f 9e 99 d4 97 8c

解决方法

*Apr 26 14:37:58:304 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0020 50 18 fa 5f 01

此问题的根本原因是因为会话跨板卡：SSLVPN会话起在slot2上，本机登陆telnet（也包括Web登录）

会话需要去slot0，这种场景下MSR5620设备不支持，而通过sslvpn后，直接在终端跨我们的设备去telnet/

web登录其他的内部服务器的时候，这样会话不会去slot0，因此现场可以成功登陆内部服务器。

注：在分布式设备和IRF环境下会出现部分流量不通的问题，此问题的根本原因是SSL VPN

的流量不支持跨板和跨板转发，求同流量只能在一个转发板上，因此部署SSL VPN的流量一定要

在一个转发板上。

*Apr 26 14:37:58:353 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0000 45 c0 00 28 8
2 bc 00 00 fe 06 9d c4 0a 13 01 02

*Apr 26 14:37:58:353 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0010 8f 78 01 02 0
0 17 ee b0 99 d4 97 8c bc 31 8f a8

*Apr 26 14:37:58:353 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0020 50 10 1f e1 8
8 61 00 00

*Apr 26 14:37:58:353 2022 MSR5620 SSLVPNK/7/SSLVPN_EVENT: -Slot=2; IPAC: Found peer
143.120.1.2.

*Apr 26 14:37:58:353 2022 MSR5620 SSLVPNK/7/SSLVPN_EVENT: -Slot=2; IPAC: The check res
ult of the referenced address pool is 1.

