终端通过SSL VPN 拨入MSR5620后通过设备内网口无法登录WEB界面或者telent

SSL VPN 王科 2022-05-18 发表

组网及说明

MSR5620 Release 0809P33

PC—公网—MSR5620—内网

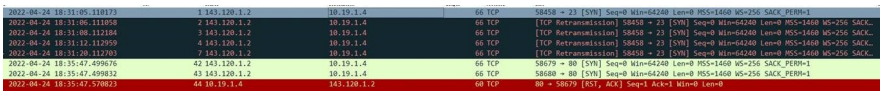
问题描述

设备在PC上拨SSL VPN，正常，现场想在PC上通过MSR5620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 143.120.1.2 143.120.1.50
#
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

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，telent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。



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:

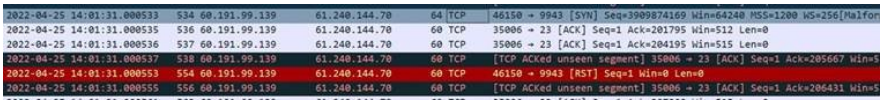
TCP Synrespond(vrf = 0, state = SYN_RCVD):

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。**



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 fb d4 40 00 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 ed 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: Reveived 56 bytes of user traffic: cOntextID=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 00 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 03

*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 ec 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

*Apr 26 14:37:58:304 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0020 50 18 fa 5f 01 57 00 00 ff fa 18 00 41 4e 53 49

*Apr 26 14:37:58:304 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0030 4 f f0

*Apr 26 14:37:58:304 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_PACKET: **-Slot=2; SSLVPN-AC1 output packet.**

*Apr 26 14:37:58:353 2022 MSR5620 SSLVPNK/7/SSLVPN_PACKET: -Slot=2; 0000 45 c0 00 28 82 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 00 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 88 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 result of the referenced address pool is 1.**

解决方法

1. 此问题的根本原因是因为：SSLVPN会话起在slot2上，本机登陆telnet（也包括Web登录）会话需要走slot0，这种场景下MSR56设备不支持。
2. 开通过sslvpn后，直接在终端跨我们的设备去telnt/web登录其他的内部服务器的时候，这样会话不会走slot0，因此现场可以成功登陆内部服务器。
3. sslvpn场景在分布式设备和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的流量不支持跨框和跨板转发，来回流量只能在一个转发板卡上，因此部署SSL VPN的流量一定要在一个转发板上。