某局点MSR 5620 SSL VPN无法通过内网口地址登录设备

SSL VPN　陈阳　2022-04-28 发表

组网及说明

终端—公网—MSR5620—内网

告警信息

无

告警信息

问题描述

终端通过SSL VPN拨号后，无法通过MSR 5620的内网口地址登录设备WEB或者telnet，通过公网口地址登录正常。

过程分析

终端SSL VPN拨号之后，ping内网口地址能通，说明网络正常，通过公网口地址telnet设备或者登录WEB正常，说明设备的服务是开启的。

终端ping设备内网口地址时，debug信息收发均正常

<MSR5620>*Apr 24 15:16:14:193 2022 MSR5620 IPFW/7/IPFW_PACKET: -Slot=2;
Receiving, interface = SSLVPN-AC1
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 44283, offset = 0, ttl = 64, protocol = 1
checksum = 12853, **s = 1.1.1.1, d = 1.1.1.2**
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface SSLVPN-AC1.
Payload: ICMP
  type = 8, code = 0, checksum = 0x4c99.

*Apr 24 15:16:14:193 2022 MSR5620 IPFW/7/IPFW_PACKET: -Slot=2;
Delivering, interface = SSLVPN-AC1
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 44283, offset = 0, ttl = 64, protocol = 1
checksum = 12853, **s = 1.1.1.1, d = 1.1.1.2**
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Forwarding IP packet to upper layer.
Payload: ICMP
  type = 8, code = 0, checksum = 0x4c99.

*Apr 24 15:16:14:193 2022 MSR5620 IPFW/7/IPFW_PACKET: -Slot=2;
Sending, interface = SSLVPN-AC1
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 56115, offset = 0, ttl = 255, protocol = 1
checksum = 17660, **s = 1.1.1.2, d = 1.1.1.1**
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet from local at interface SSLVPN-AC1.
Payload: ICMP
  type = 0, code = 0, checksum = 0x5499.

通过内网口地址telnet登录时，debug看到设备只有收，没有发

*Apr 24 15:16:24:562 2022 MSR5620 IPFW/7/IPFW_PACKET: -Slot=2;
Receiving, interface = SSLVPN-AC1
version = 4, headlen = 20, tos = 0
pktlen = 52, pktid = 44287, offset = 0, ttl = 128, protocol = 6
checksum = 45619, **s = 1.1.1.1, d = 1.1.1.2**
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface SSLVPN-AC1.
Payload: TCP
  source port = 30822, destination port = 23
  sequence num = 0x8b536aeb, acknowledgement num = 0x00000000, flags = 0x2
  window size = 64240, checksum = 0x69d2, header length = 32.

*Apr 24 15:16:24:562 2022 MSR5620 IPFW/7/IPFW_PACKET: -Slot=2;
Delivering, interface = SSLVPN-AC1
version = 4, headlen = 20, tos = 0
pktlen = 52, pktid = 44287, offset = 0, ttl = 128, protocol = 6
checksum = 45619, **s = 1.1.1.1, d = 1.1.1.2**
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Forwarding IP packet to upper layer.
Payload: TCP
  source port = 30822, destination port = 23
  sequence num = 0x8b536aeb, acknowledgement num = 0x00000000, flags = 0x2
  window size = 64240, checksum = 0x69d2, header length = 32.

*Apr 24 15:16:25:572 2022 MSR5620 IPFW/7/IPFW_PACKET: -Slot=2;
Delivering, interface = SSLVPN-AC1
version = 4, headlen = 20, tos = 0

解决方法

MSR 56设备不支持这种场景的使用。

pktlen = 52, pktid = 44288, offset = 0, ttl = 128, protocol = 6
checksum = 45618, **s = 1.1.1.1, d = 1.1.1.2**
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Forwarding IP packet to upper layer from FastForward.
Payload: TCP
source port = 30822, destination port = 23
sequence num = 0x8b536aeb, acknowledgement num = 0x00000000, flags = 0x2
window size = 64240, checksum = 0x69d2, header length = 32.

*Apr 24 15:16:27:586 2022 MSR5620 IPFW/7/IPFW_PACKET: -Slot=2;
Delivering, interface = SSLVPN-AC1
version = 4, headlen = 20, tos = 0
pktlen = 52, pktid = 44289, offset = 0, ttl = 128, protocol = 6
checksum = 45617, **s = 1.1.1.1, d = 1.1.1.2**
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Forwarding IP packet to upper layer from FastForward.
Payload: TCP
source port = 30822, destination port = 23
sequence num = 0x8b536aeb, acknowledgement num = 0x00000000, flags = 0x2
window size = 64240, checksum = 0x69d2, header length = 32.

后续确认本地登录（包括telnet和WEB）会话需要走slot 0，而根据debug信息可以看到SSL VPN会话发生在slot 2上，所以出现了无法登录设备的情况。

对于SSL VPN场景在分布式设备和IRF环境下会出现部分流量不通的情况，原因在于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，所以部署SSL VPN时，需要保证流量在一个转发板上。

现场使用的MSR 5620设备转控分离，从而触发了SSL VPN流量登录本机不通的问题，如果通过SSL VPN访问内网设备，此时会话不走slot 0，所以访问内网没有问题。