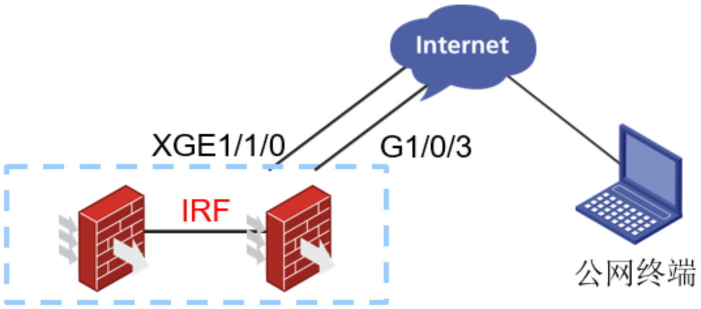
某局点SecPath F5000-M(V7) SSH备接口地址失败故障排查经验案例

IRF 保存上一跳 **王周华** 2021-09-30 发表

组网及说明

现场两台防火墙做了IRF，两个运营商出口配置了主备路由，想要实现无论通过主接口地址还是备接口地址，都可以实现SSH到设备上进行管理。大致拓扑如下：



本次涉及设备的型号以及版本：SecPath F5000-M(V7)   Version 7.1.064, Release 9616P39

问题描述

XG1/1/0是主链路，G1/0/3是备用链路，两条默认路由是优先级不同的主备关系，测试Ping G1/0/3的接口IP可以通，但是通过备接口地址无法使用SSH以及HTTPS的方式登录到设备上。

过程分析

1、查看会话表，看是否收到了公网终端发来的对应的SSH或者是HTTPS报文。由于公网地址涉及客户隐私，所以这边采用1.1.1.1代替G1/0/3地址，2.2.2.2代替XG1/1/0地址，3.3.3.3代替公网终端地址。现场将HTTPS端口通过ip https port 58443配置成58443端口，通过备接口地址访问HTTPS端口时收集了会话信息，替换地址后的会话表如下：

```
<CHQY-F5000M-1&2>dis session table ipv4 source-ip 3.3.3.3 destination-port 58443 verbose
Slot 1:
Initiator:
  Source      IP/port: 3.3.3.3/4305
  Destination IP/port: 1.1.1.1/58443
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/3
  Source security zone: DC_MSE
Responder:
  Source      IP/port: 1.1.1.1/58443
  Destination IP/port: 3.3.3.3/4305
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: TCP_SYN_RECV
Application: GENERAL_TCP
Rule ID: 2
Rule name: rz_wg
Start time: 2021-09-28 14:09:35  TTL: 17s
Initiator->Responder:         4 packets        208 bytes
Responder->Initiator:         8 packets        416 bytes

Initiator:
  Source      IP/port: 3.3.3.3/4306
  Destination IP/port: 1.1.1.1/58443
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/3
  Source security zone: DC_MSE
Responder:
  Source      IP/port: 1.1.1.1/58443
  Destination IP/port: 3.3.3.3/4306
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: TCP_SYN_RECV
Application: GENERAL_TCP
Rule ID: 2
Rule name: rz_wg
Start time: 2021-09-28 14:09:50  TTL: 25s
Initiator->Responder:         1 packets         52 bytes
Responder->Initiator:         4 packets        208 bytes
Total sessions found: 2

Slot 2:
Initiator:
  Source      IP/port: 3.3.3.3/4305
  Destination IP/port: 1.1.1.1/58443
  DS-Lite tunnel peer: -
```

解决方法

1、将堆叠主设备切到1框。

2、配置本地策略路由匹配源地址为G1/0/3接口地址，下一跳为G1/0/3的接口地址，让流量通过G1/0/3口转发。

```
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/3
  Source security zone: huiyi
Responder:
  Source      IP/port: 1.1.1.1/58443
  Destination IP/port: 3.3.3.3/4305
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: TCP_ESTABLISHED
Application: GENERAL_TCP
Rule ID: 2
Rule name: rz_wg
Start time: 2021-09-28 14:09:35  TTL: 3587s
Initiator->Responder:          0 packets          0 bytes
Responder->Initiator:          7 packets        364 bytes

Initiator:
  Source      IP/port: 3.3.3.3/4306
  Destination IP/port: 1.1.1.1/58443
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/3
  Source security zone: huiyi
Responder:
  Source      IP/port: 1.1.1.1/58443
  Destination IP/port: 3.3.3.3/4306
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: TCP_ESTABLISHED
Application: GENERAL_TCP
Rule ID: 2
Rule name: rz_wg
Start time: 2021-09-28 14:09:50  TTL: 3594s
Initiator->Responder:          0 packets          0 bytes
Responder->Initiator:          3 packets        156 bytes
Total sessions found: 2
```

可以看到主备框上都有会话，说明报文已经发送到设备上了，且来回方向都是有报文的。

2、于是让现场分别收集ICMP和HTTPS访问时的DEBUG信息作比较分析。ICMP的DEBUG信息如下：

```
<CHQY-F5000M-1&2>debugging ip packet acl 3105
This command is CPU intensive and might affect ongoing services. Are you sure you want to
continue? [Y/N]:y
<CHQY-F5000M-1&2>t d
The current terminal is enabled to display debugging logs.
<CHQY-F5000M-1&2>t m
The current terminal is enabled to display logs.
<CHQY-F5000M-1&2>*Sep 28 14:07:10:019 2021 CHQY-F5000M-1&2 IPFW/7/IPFW_PACKET: -C
Ontext=1-Slot=1;
```

Receiving, interface = GigabitEthernet1/0/3

```
version = 4, headlen = 20, tos = 72
pktlen = 60, pktid = 33482, offset = 0, ttl = 116, protocol = 1
checksum = 22521, s = 223.104.65.143, d = 119.131.211.58
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/3.
Payload: ICMP
  type = 8, code = 0, checksum = 0xd698.
```

```
*Sep 28 14:07:10:019 2021 CHQY-F5000M-1&2 IPFW/7/IPFW_PACKET: -COntext=1-Slot=1;
Delivering, interface = GigabitEthernet1/0/3
```