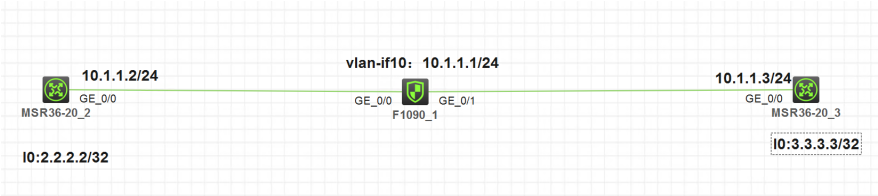
防火墙ASPF丢包典型案例分析

会话 包过滤 **孔凡安** 2022-03-30 发表

组网及说明



如图所示：防火墙配置了vlan-interface接口，地址为10.1.1.1/24. GE0/0和GE0/1均属于vlan1.
R2和R3起环回口模拟业务流量，2.2.2.2访问3.3.3.3.

问题描述

此类组网下常见的丢包的一种原因为正向的流量和反向的流量转发方式不同。

正向三层，反向二层；亦或者是正向二层，反向三层。

这种情况会导致反向报文关联不上原来的会话，从而导致丢包。

过程分析

正向二层，反向三层情况举例如下：

会话信息：

```
Slot 1:
Initiator:
  Source      IP/port: 2.2.2.2/10961
  Destination IP/port: 3.3.3.3/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/10/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/0
  Source security zone: Trust
Responder:
  Source      IP/port: 3.3.3.3/10961
  Destination IP/port: 2.2.2.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/10/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
State: ICMP_REQUEST
Application: ICMP
Rule ID: 0
Rule name: any
Start time: 2022-03-30 15:09:10  TTL: 53s
Initiator->Responder:            5 packets        510 bytes
Responder->Initiator:            0 packets          0 bytes
```

通过会话可以看出，入方向创建二层会话，携带vlan标签10.

查看debug信息：

回包没有关联之前的会话，而是重新匹配安全策略，最后被ASPF丢弃。

```
*Mar 30 15:13:57:230 2022 H3C IPFW/7/IPFW_PACKET: -Context=1;
Receiving, interface = Vlan-interface10
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 47, offset = 0, ttl = 255, protocol = 1
checksum = 45424, s = 3.3.3.3, d = 2.2.2.2
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
vsysID = 1
prompt: Receiving IP packet from interface Vlan-interface10.
Payload: ICMP
  type = 0, code = 0, checksum = 0x495c.
```

*Mar 30 15:13:57:230 2022 H3C FILTER/7/PACKET: -COntext=1; The packet is permitted. Src-ZOne =Trust, Dst-ZOne=Trust;If-In=Vlan-interface10(1286), If-Out=Vlan-interface10(1286); Packet Info:Src-IP=3.3.3.3, Dst-IP=2.2.2.2, VPN-Instance=, Src-MacAddr=ac37-90ec-0305,Src-Port=0, Dst-Port=0, Protocol=ICMP(1), Application=invalid(0),Terminal=invalid(0), SecurityPolicy=any, Rule-ID=0.

*Mar 30 15:13:57:230 2022 H3C ASPF/7/PACKET: -COntext=1; The first packet was dropped by AS PF for invalid status. Src-ZOne=Trust, Dst-ZOne=Trust;If-In=Vlan-interface10(1286), If-Out=Vlan-inte rface10(1286); Packet Info:Src-IP=3.3.3.3, Dst-IP=2.2.2.2, VPN-Instance=none, Src-Port=10962, Dst -Port=0. Protocol=ICMP(1).

注意事项：二层转发debug不会打印ip packer的信息，security-policy可以打印出来。

可以根据安全策略的打印判断报文是二层转发还是三层转发，出入接口为Vlan-interface代表三层转发，出入接口为GigabitEthernet（bridge类型）或者BAGG并携带vlan标签代表为二层转发。

解决方法

明确防火墙二层转发还是三层，出入方向保持一致即可。

建议防火墙三层转发，更好的发挥其性能。