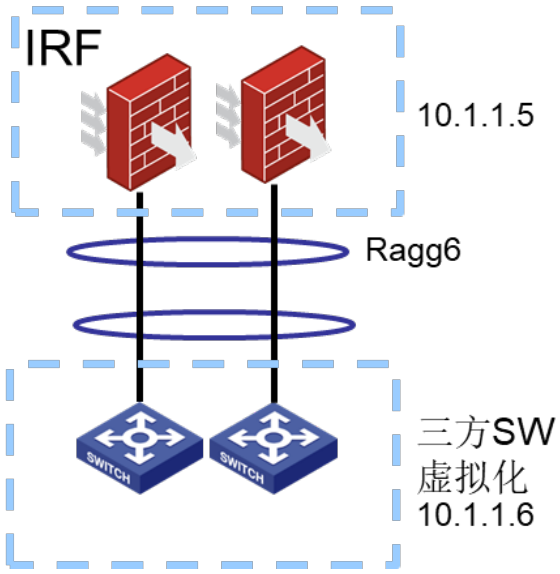
排查某局点防火墙不通对端交换机案例

ASPF 链路聚合 吴川云 2022-02-28 发表

组网及说明

防火墙IRF主备冗余组三层部署，与对端第三方交换机三层聚合口互联；防火墙使用三层聚合口的子接口进行终结vlan；

防火墙接口互联地址为10.1.1.5，交换机接口互联地址为10.1.1.6；



问题描述

防火墙ping交换机的互联地址10.1.1.6，不通，防火墙slot1生成会话，单向计数：

<xxx>ping 10.1.1.6
Ping 10.1.1.6 (10.1.1.6): 56 data bytes, press CTRL+C to break
Request time out
Request time out
Request time out
Request time out
Request time out

```
dis session table ipv4 source-ip 10.1.1.5  ver
Slot 1:
Initiator:
  Source      IP/port: 10.1.1.5/3166
  Destination IP/port: 10.1.1.6/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: InLoopBack0
  Source security zone: Local
Responder:
  Source      IP/port: 10.1.1.6/3166
  Destination IP/port: 10.1.1.5/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Route-Aggregation6.1018
  Source security zone: Untrust
State: ICMP_REQUEST
Application: ICMP
Rule ID: 15
Rule name: permit-any
Start time: 202xxx  TTL: 45s
Initiator->Responder:            4 packets          224 bytes
Responder->Initiator:            0 packets          0 bytes

Slot 2:
Total sessions found: 0
```

交换机ping防火墙的互联地址10.1.1.5，可通，防火墙slot2生成会话；

```
dis session table ipv4 source-ip 10.1.1.6  ver
Slot 1:
Total sessions found: 0

Slot 2:
Initiator:
  Source      IP/port: 10.1.1.6/5265
  Destination IP/port: 10.1.1.5/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Route-Aggregation6.1018
  Source security zone: Untrust
Responder:
  Source      IP/port: 10.1.1.5/5265
  Destination IP/port: 10.1.1.6/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: ICMP_REPLY
Application: ICMP
Rule ID: 15
Rule name: permit-any
Start time: 202XXX  TTL: 20s
Initiator->Responder:            4 packets          224 bytes
Responder->Initiator:            4 packets          224 bytes
```

过程分析

收集debug ip packet、debug security-policy、debug aspf-policy进行分析：

*XXX FILTER/7/PACKET: -COntext=13; The packet is permitted. Src-ZOne=Local, Dst-ZOne=Untrust;If-In=InLoopBack0(348), If-Out=Route-Aggregation6.1018(354); Packet Info:Src-IP=10.1.1.5, Dst-IP=10.1.1.6, VPN-Instance=, Src-MacAddr=0000-0000-0000,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), SecurityPolicy=permit-any, Rule-ID=15.

```
*xxx IPFW/7/IPFW_PACKET: -Context=13;
Sending, interface = Route-Aggregation6.1018
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 24033, offset = 0, ttl = 255, protocol = 1
checksum = 16741, s = 10.1.1.5, d = 10.1.1.6
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet from local at interface Route-Aggregation6.1018.
Payload: ICMP
  type = 8, code = 0, checksum = 0x0ac8.


*xxx IPFW/7/IPFW_PACKET: -Context=13-Slot=2;
Receiving, interface = Route-Aggregation6.1018
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 27140, offset = 0, ttl = 64, protocol = 1
checksum = 62530, s = 10.1.1.6, d = 10.1.1.5
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface Route-Aggregation6.1018.
Payload: ICMP
  type = 0, code = 0, checksum = 0x12c8.


*xxx IPFW/7/IPFW_PACKET: -Context=13-Slot=2;
Delivering, interface = Route-Aggregation6.1018
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 27140, offset = 0, ttl = 64, protocol = 1
checksum = 62530, s = 10.1.1.6, d = 10.1.1.5
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Forwarding IP packet to upper layer.
Payload: ICMP
  type = 0, code = 0, checksum = 0x12c8.
```

*XXX FILTER/7/PACKET: -COntext=13-Slot=2; The packet is permitted. Src-ZOne=Untrust, Dst-ZOne=Local;If-In=Route-Aggregation6.1018(354), If-Out=InLoopBack0(348); Packet Info:Src-IP=10.1.1.6, Dst-IP=10.1.1.5, VPN-Instance=, Src-MacAddr=300d-9e42-ad1e,Src-Port=0, Dst-Port=0, Protocol=ICMP(1), Application=invalid(0), SecurityPolicy=permit-any, Rule-ID=15. //**安全策略匹配的any放通所有的规则，允许报文转发**

*Feb 11 19:45:49:427 2022 nsp-c776a1b1 ASPF/7/PACKET: -COntext=13-**Slot=2**; The first packet was dropped by ASPF for invalid status. Src-ZOne=Untrust, Dst-ZOne=Local;If-In=Route-Aggregation6.1018(354), If-Out=InLoopBack0(348); Packet Info:Src-IP=10.1.1.6, Dst-IP=10.1.1.5, VPN-Instance=none, Src-Port=3291, Dst-Port=0. Protocol=ICMP(1) //**ASPF提示首包丢弃，查看debug，发现答复的应答报文从slot2的接口上来，主备组网环境中，当出现非对称路径流量时，需要将会话状态机的模式配置为宽松模式，可以避免异常会话丢包。**

结合测试的会话发现两端分别ping的时候生成会话的框不同，对端ping本侧防火墙，回包都在本框处理，流量可以放行；本端ping交换机时，icmp-request从slot 1发出，交换机回应icmp-reply在直连防火墙slot2的链路上，导致本侧防火墙检测到非对称路径流量，将报文丢弃；开启会话宽松后可以避免此类异常丢包；

解决方法

配置会话宽松模式后可以通信；

session state-machine mode { compact | loose }

缺省情况下，会话状态机为严格模式。