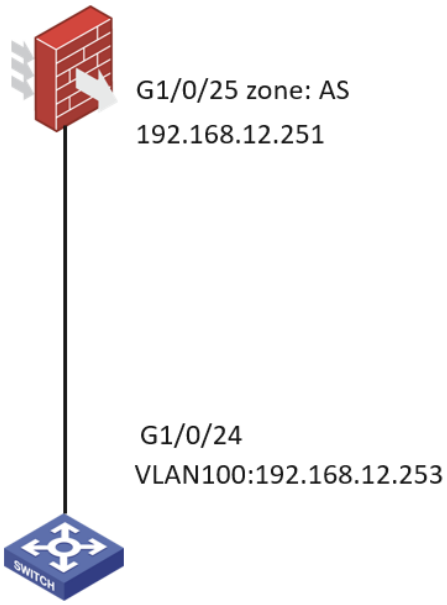
F1000-AI-15对接交换机直连不通的经验案例

域间策略/安全域 徐玉娟 2022-08-19 发表

组网及说明



问题描述

防火墙和交换机直连ping测试不通，防火墙接口为1/0/25，安全域为AS，防火墙地址为192.168.12.251，直连交换机地址为192.168.12.253

[SW13]ping -a 192.168.12.253 -c 100 192.168.12.251

Ping 192.168.12.251 (192.168.12.251) from 192.168.12.253: 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

过程分析

1，检查配置，安全策略均放通了

```
security-policy ip
  rule 185 name any_to_local
    action pass
    source-zone AS
    destination-zone Local
security-zone name AS
  import interface GigabitEthernet1/0/25
```

2，查看路由表也正常

```
===============display ip routing-table===============
 Destination/Mask   Proto   Pre Cost        NextHop         Interface
192.168.12.128/25   Direct  0   0           192.168.12.251   GE1/0/25
```

3，查看会话匹配了对应的安全策略rule185，但是会话中接口安全域不对，怀疑是来回路径不一致导致

```
<FW1000>display session table ipv4 source-ip 192.168.12.253 verbose
Slot 1:
Initiator:
  Source      IP/port: 192.168.12.253/41249
  Destination IP/port: 192.168.12.251/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/25
  Source security zone: Trust
Responder:
  Source      IP/port: 10.16.120.251/41249
  Destination IP/port: 10.16.120.253/0
  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: 185
Rule name: any_to_local
Start time: 2022-08-14 09:56:58  TTL: 29s
Initiator->Responder:           41 packets       3444 bytes
Responder->Initiator:           41 packets       3444 bytes
```

4，收集debug进一步确认，查看有如下异常，收包接口是1/0/25，回包接口是1/0/23，接下来排查路径不一致的原因

```
Delivering, interface = GigabitEthernet1/0/25
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 32962, offset = 0, ttl = 255, protocol = 1
checksum = 13518, s = 192.168.12.253, d = 192.168.12.251
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
VsysID = 1
prompt: Forwarding IP packet to upper layer from FastForward.
Payload: ICMP
  type = 8, code = 0, checksum = 0x2c5d.

*Aug  14 15:14:18:934 2022 FW1000 IPFW/7/IPFW_PACKET:
Sending, interface = GigabitEthernet1/0/23
version = 4, headlen = 20, tos = 0
pktlen = 84, pktid = 32422, offset = 0, ttl = 255, protocol = 1
checksum = 14058, s = 192.168.12.251, d =192.168.12.253
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
VsysID = 1
```

prompt: Sending IP packet from local at interface GigabitEthernet1/0/23.

Payload: ICMP

type = 0, code = 0, checksum = 0x345d.

5，查看fib表项，发现防火墙根据192.168.12.253的路由表项对数据报文进行了转发，发到了接口1/0/23

解决方法

==========display fib==========

Destination/Mask Nexthop Flag OutInterface/Token Label

192.168.12.128/25 192.168.12.251 U GE1/0/25 Null

192.168.12.253/32 192.168.12.253 UH GE1/0/23 Null

将静态路由的下一跳和出接口修改为一致解决

经确认，现场配置了另外几条下一跳地址与出接口不一致的静态路由，导致形成了错误的fib表项

ip route-static 192.168.121.0 24 GigabitEthernet1/0/23 192.168.120.253

ip route-static 192.168.122.0 24 GigabitEthernet1/0/23 192.168.120.253