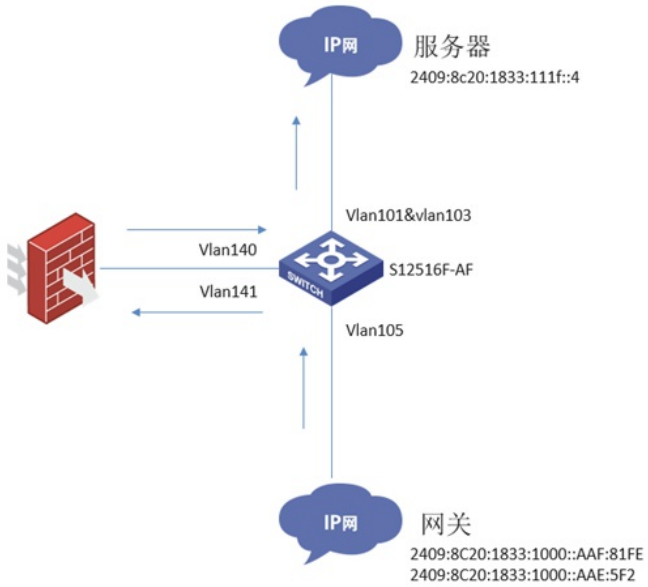
S12516F-AF交换机旁挂华为防火墙部分流量转发不通经验案例

OSPF IPv6 孙兆强 2020-03-30发表

组网及说明



上图组网为简化组网，网关为多个网段网关，图中以2个地址为例。华为防火墙旁挂在S12516F-AF上，交换机上通过策略路由将来回流量均重定向到防火墙上，使来回流量均经过防火墙。

问题描述

部分网段无法访问服务器地址，例如

```
<WG>ping ipv6 -t 10 -a 2409:8C20:1833:1000::AAF:81FE 2409:8c20:1833:111f::4
Ping6(56 data bytes) 2409:8C20:1833:1000::AAF:81FE --> 2409:8C20:1833:111F::4, press CTRL_C to break
56 bytes from 2409:8C20:1833:111F::4, icmp_seq=0 hlim=53 time=5.111 ms
56 bytes from 2409:8C20:1833:111F::4, icmp_seq=1 hlim=53 time=3.532 ms
56 bytes from 2409:8C20:1833:111F::4, icmp_seq=2 hlim=53 time=3.578 ms
56 bytes from 2409:8C20:1833:111F::4, icmp_seq=3 hlim=53 time=3.554 ms
56 bytes from 2409:8C20:1833:111F::4, icmp_seq=4 hlim=53 time=3.518 ms

--- Ping6 statistics for 2409:8c20:1833:111f::4 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 3.518/3.859/5.111/0.627 ms
<WG>ping ipv6 -t 10 -a 2409:8C20:1833:1000::AAE:5F2 2409:8c20:1833:111f::4
Ping6(56 data bytes) 2409:8C20:1833:1000::AAE:5F2 --> 2409:8C20:1833:111F::4, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
```

过程分析

查看防火墙配置，流量均已放通，来回路由均指到交换机。

查看交换机上行口和下行口策略路由配置，ACL匹配所有ipv6流量将上下行流量指到防火墙上。

```
acl ipv6 advanced 3000
 rule 5 permit ipv6
```

从网关上tracert服务器查看路径，发现路由存在环路。

```
<WG>tracert ipv6 2409:8c20:1833:111f::4
traceroute to 2409:8c20:1833:111f::4 (2409:8C20:1833:111F::4), 30 hops at most, 60 byte packets, press CTRL_C to break
 1  2409:8C20:1833:1000::AAE:5F1  1.418 ms  1.022 ms  0.982 ms
 2  2409:8C20:1833:1000::AAE:FE42  4.428 ms  4.135 ms  3.904 ms
```

3 2409:8C20:1833:1000::AAE:5F1 1.267 ms 1.121 ms 1.107 ms
4 2409:8C20:1833:1000::AAE:FE42 4.106 ms 3.988 ms
5 2409:8C20:1833:1000::AAE:5F1 1.271 ms 1.244 ms

在125上查看路由display ipv6 routing-table 2409:8c20:1833:111f::4发现有一条异常的路由将流量指回了防火墙。

为何会学习到此条路由呢？查看交换机及防火墙ospf路由配置。
交换机配置
interface Vlan-interface140
ip address 10.174.5.249 255.255.255.252
ospf cost 10
ospf timer hello 1
ospf network-type p2p
ospfv3 1 area 0.0.0.0
ospfv3 cost 10
ospfv3 timer hello 1
ospfv3 network-type p2p
ipv6 address 2409:8C20:1833:1000::AAE:5F9/126
#
interface Vlan-interface141
ip address 10.174.254.65 255.255.255.252
ospfv3 20 area 0.0.0.0
ospfv3 cost 10
ospfv3 timer hello 1
ospfv3 network-type p2p
ipv6 address 2409:8C20:1833:1000::AAE:FE41/126

防火墙配置
interface Eth-Trunk1.140
vlan-type dot1q 140
ipv6 enable
ip address 10.174.5.250 255.255.255.252
ipv6 address 2409:8C20:1833:1000::AAE:5FA/126
ipv6 mtu 1600
ospfv3 100 area 0.0.0.0
ospfv3 cost 10
ospfv3 network-type p2p
ospfv3 timer hello 1
ospf cost 10
ospf network-type p2p
ospf timer hello 1
ospf enable 100 area 0.0.0.0
undo service-manage enable
#
interface Eth-Trunk1.141
vlan-type dot1q 141
ipv6 enable
ip address 10.174.254.66 255.255.255.252
ipv6 address 2409:8C20:1833:1000::AAE:FE42/126
ipv6 mtu 1600
ospfv3 100 area 0.0.0.0
ospfv3 cost 10
ospfv3 network-type p2p
ospfv3 timer hello 1
ospf cost 10
ospf network-type p2p
ospf timer hello 1

ospf enable 100 area 0.0.0.0
undo service-manage enable

交换机上两个口为不同的ospf进程，防火墙上两个口为同一个ospf进程。

交换机通过vlan 101学习到这个路由。交换机vlan 140和fw建立ospfv3，这个路由fw学习到。交换机vlan 141和fw建立ospfv3，这个路由交换机又学习了一遍。又因为交换机vlan 140和vlan 141两个接口是调用的ospf进程不一样，一个是进程1一个是进程20，所以交换机会形成错误等价路由指向fw。部分源地址能通是因为等价路由是hash选择，部分地址正好hash到正确的路由上。

解决方法

Fw的两个口Eth-Trunk1.140和Eth-Trunk1.141调用不同的ospfv3进程，比如140口用ospfv3 100 area 0.0.0.0　另一个141口用ospfv3 200 area 0.0.0.0