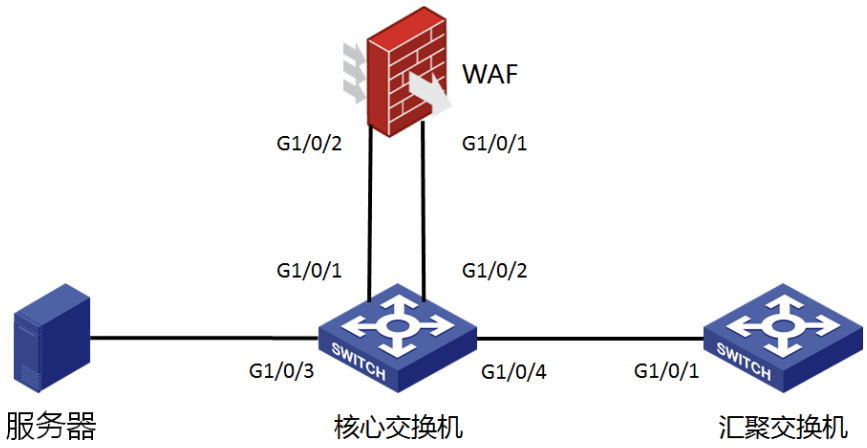
某据点核心交换机旁挂VPN实例流量不通问题处理案例

策略路由 王鸿渐 2018-12-12 发表

组网及说明

拓扑如下：



问题描述

现场有一台核心交换机（S7510）旁挂一台第三方WAF设备，核心交换机上联外部流量，下联服务器区，现有如下需求：外部流量网关和服务器网关均在核心交换机上，外部流量需要通过第三方WAF设备安全审计再回到交换机后转发给服务器，全程保证来回路径一致。

组网说明：

G1/0/4：permit trunk VLAN 3011　VLAN-interface 3011：10.223.53.1 / 24

G1/0/2：access VLAN 3183　VLAN-interface 3183：10.223.53.26 / 30

G1/0/1：access VLAN 3184　VLAN-interface 3184：10.223.53.30 / 30

以上接口都绑定VPN实例wangzha

G1/0/3：access VLAN 2000　VLAN-interface 2000：10.255.255.1 / 30

以上接口绑定VPN实例server

测试外部网络终端地址：10.223.53.2 / 30

测试服务器地址：10.255.255.2 / 30

现场首先在核心交换机上配置了PBR将外部流量引入第三方WAF设备，流量经过WAF静态路由回到核心交换机，但是经过测试发现，外部终端无法正常PING通服务器，说明流量转发出现了问题。

过程分析

1.首先我们检查交换机上的PBR配置是否正确?

配置如下：

policy-based-route 11 permit node 1

if-match acl 3000

apply next-hop vpn-instance wangzha 10.223.53.25

Advanced IPv4 ACL 3000, 1 rule, ACL's step is 5

rule 0 permit ip vpn-instance wangzha source 10.223.53.2 0 destination 10.255.255.2 0

interface Vlan-interface3011

ip binding vpn-instance wangzha

ip address 10.223.53.1 255.255.255.252

ip policy-based-route 11

检查PBR配置没有问题，在终端上tracert核心交换机与WAF互联端口地址发现流量按照PBR的路径到核心交换机。

2.检查WAF到核心交换机的回包是否正常

在核心交换机与WAF互联的下行端口（G1/0/1）做流量统计确认流量已到核心交换机

<XXXXXX>dis qos policy interface inbound

Interface: Ten-GigabitEthernet2/11/0/8

Direction: Inbound

Policy: test

  Classifier: test

  Operator: AND

    Rule(s) : If-match acl 3016

  Behavior: test

Accounting enable:

20 (Packets)

流量统计有包产生，说明流量已到核心交换机。

3.确认流量上送到核心交换机后如何转发：

检查路由配置及路由表

ip route-static vpn-instance server 10.223.53.0 30 vpn-instance wangzha 10.223.53.29

ip route-static vpn-instance wangzha 10.255.255.0 30 vpn-instance server 10.255.255.2

[XXXX]dis ip routing-table vpn-instance wangzha

Destinations : XXX Routes : XXX

10.255.255.0/30 Static 60 0 10.255.255.2 Vlan2000

[XXXX]dis ip routing-table vpn-instance server

Destinations : XXX Routes : XXX

10.223.53.0/30 Static 60 0 10.223.53.29 Vlan3184

确认路由均配置正常而且路由表生效，此时我们在核心和WAF之间互联端口抓包检查。

452 850.9717…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=253 (no respo
453 850.9721…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=251 (no respo
454 850.9725…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=249 (no respo
455 850.9730…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=247 (no respo
456 850.9734…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=245 (no respo
457 850.9737…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=243 (no respo
458 850.9741…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=241 (no respo
459 850.9746…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=239 (no respo
460 850.9749…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=237 (no respo
461 850.9752…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=235 (no respo

572 851.0270…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=13 (no respon
573 851.0275…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=11 (no respon
574 851.0280…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=9 (no respons
575 851.0284…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=7 (no respons
576 851.0290…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=5 (no respons
577 851.0295…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=3 (no respons
578 851.0299…	10.223.53.2	10.255.255.2	ICMP	98	Echo (ping) request id=0x00c1, seq=0/0, ttl=1 (no respons

此时我们抓包发现PING包的ttl值从253变到0，可以确认流量在核心交换机和WAF之间产生了环路。

解决方法

此时我们发现流量在核心和WAF之间产生路由环路，流量在经过WAF后回到交换机后又命中了PBR导致。

为了避免路由环路我们做如下配置修改：

将WAF与核心交换机互联的上行端口VPN实例改为SERVER，并配置回程流量的PBR保证来回路径一致，删除原本的静态路由。

interface Vlan-interface3184

ip binding vpn-instance server

ip address 10.223.53.30 255.255.255.252

policy-based-route 12 permit node 1

if-match acl 3001 apply

next-hop vpn-instance server 10.223.53.29

Advanced IPv4 ACL 3001, 1 rule, ACL's step is 5

rule 0 permit ip vpn-instance server source 10.255.255.2 0 destination 10.223.53.2 0

interface Vlan-interface2000

ip binding vpn-instance server

ip address 10.255.255.1 255.255.255.252

ip policy-based-route 12