某局点SecPath F5060(V7) 过设备的DNS回包被设备拒绝问题处理经验案例

ASPF 徐猛 2019-10-31 发表

组网及说明

现场设备做了IRF，现场的异常流量拓扑如下：
10.10.10.101-------------------------BGG10 （F5060）BGG30----------------211.137.191.**（DNS服务器）

问题描述

现场设备做了IRF，会有部分经过设备的DNS解析流量，无法正常转发的情况，经过查看日志，有大量回程流量被拦截的日志记录。

%Oct 30 11:16:36:102 2019 SDFI_Server_FW-F5060 FILTER/6/FILTER_ZONE_IPV4_EXECUTION: -Slot=2; SrcZoneName(1025)=Untrust;DstZoneName(1035)=Trust;Type(1067)=ACL;SecurityPolicy(1072)=any_TO_Server;RuleID(1078)=10;Protocol(1001)=UDP;Application(1002)=general_udp;SrcIPAddr(1003)=211.137.191.**;**SrcPort(1004)=53**;SrcMaAddr(1021)=441a-fa74-dc01;DstIPAddr(1007)=10.10.10.101;DstPort(1008)=8528;MatchCount(1069)=1;Event(1048)=Deny;

2019-10-30 17:38:23	Untrust	Trust	any_TO_Server	10	UDP	general_udp	211.137.191	53	10.10.10.101	8067	1	Deny
2019-10-30 17:37:17	Untrust	Trust	any_TO_Server	10	UDP	general_udp	211.137.191	53	10.10.10.101	64711	1	Deny
2019-10-30 17:36:59	Untrust	Trust	any_TO_Server	10	UDP	general_udp	211.137.191	53	10.10.10.101	53107	1	Deny
2019-10-30 17:36:55	Untrust	Trust	any_TO_Server	10	UDP	general_udp	211.137.191	53	10.10.10.101	24263	1	Deny

过程分析

（1）因为现场日志中报错，都是回包的被拒绝的日志记录，同时现场设备还是台做了IRF的设备，所以开始怀疑是会话同步的问题。但是检查设备配置发现，现场设备的会话同步是开启了的。
session synchronization enable asymmetric
session synchronization dns http

（2）查看会话，显示是没有回包：
Initiator:
Source IP/port: 10.10.10.101/37248
Destination IP/port: 211.137.191.**/53
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/2010/-
Protocol: UDP(17)
Inbound interface: Bridge-Aggregation30
Source security zone: Trust
Responder:
Source IP/port: 211.137.191.**/53
Destination IP/port: 10.10.10.101/37248
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/2010/-
Protocol: UDP(17)
Inbound interface: Bridge-Aggregation10
Source security zone: Untrust
State: UDP_OPEN
Application: DNS
Rule ID: 40
Rule name: out_9999_可访问校外网地址
Start time: 2019-10-30 17:05:26 TTL: 22s
Initiator->Responder: 1 packets 104 bytes
Responder->Initiator: 0 packets 0 bytes

（3）由于通常没有回程会话记录的情况下，是没有回包导致的，但是由于设备日志中有报错，所以我们收集了下debug信息这边看下：
Debug中查看确实有发包和回包记录：
*Oct 30 17:13:13:744 2019 SDFI_Server_FW-F5060 FILTER/7/PACKET: -COntext=1; The packet is permitted. Src-ZOne=Trust, Dst-ZOne=Untrust;If-In=Bridge-Aggregation30(155), If-Out=Bridge-Aggregation10(151), VLAN-In=2010, VLAN-Out=2010; Packet Info:Src-IP=10.10.10.101, Dst-IP=211.137.191.**, VPN-Instance=, Src-MacAddr=0016-31e7-466c,Src-Port=44935, Dst-Port=53, Protocol=

UDP(17), Application=dns(574), SecurityPolicy=out_9999_可访问校外网地址, Rule-ID=40.
但是对于回包，debug中显示报文被丢弃：
*Oct 30 17:13:16:431 2019 SDFI_Server_FW-F5060 FILTER/7/PACKET: -COntext=1-Slot=2;**The packet is denied.** Src-ZOne=Untrust, Dst-ZOne=Trust;If-In=Bridge-Aggregation10(151), If-Out=Bridge-Aggregation30(155), VLAN-In=2010, VLAN-Out=2010; Packet Info:Src-IP=211.137.191.**, Dst-IP=10.10.10.101, VPN-Instance=, Src-MacAddr=441a-fa74-dc01,Src-Port=53, Dst-Port=44935, Protocol=UDP(17), Application=general_udp(2087), SecurityPolicy=any_TO_Server, Rule-ID=10.

（4）根据debug和会话情况，可以确认，该问题确实是由于我们设备的问题导致的。但是结合日志中查看的情况，只有DNS的回包流量会被拒绝，正常情况下，DNS的请求流量经过我们设备转发出去后，设备上会有相应的会话，然后回程流量会匹配会话做回程的转发，DNS请求的流量已经正常转发出去了，那么回包被拒绝就应该不是安全策略的原因导致了的。

所以怀疑是否设备上的DNS会话，在DNS应答报文还没到设备上的时候，就已经老化了，所以拒绝了收到的DNS应答报文。

我们的DNS应用老化时长默认是1秒的，后续让现场将后来让现场将配置session aging-time application DNS 5测试，故障依旧。

（5）后续经产品线工程师建议，修改为session aging-time application DNS 30后，测试正常

解决方法

（1）设备上开启会话同步功能：
session synchronization enable asymmetric
session synchronization dns http
（2）同时修改设备上的DNS会话默认老化时长为1秒，将老化时长修改为30秒使用
session aging-time application DNS 30