IPS设备的web页面的报文示踪显示“对报文执行阻断动作，建议查看DPI监测信息”但是安全策略里边并未调用DPI

域间策略/安全域 **张帅杰** 2022-04-21 发表

组网及说明

外网---出口防火墙----IPS(堆叠)------核心----------服务器

问题描述

现场在用web页面的报文示踪构造一个外网访问内网的数据流，发现已经匹配到一条安全策略，并且已经检查通过，但是下一步报文提示被阻断，请检查DPI检测信息，策略里边并没有调用DPI，需要知道原因。

过程分析

1. 登录命令行页面收集如下信息：
debugging security-policy
debugging ip packet
debugging aspf packet
debugging ip info
2. 发现有如下阻断提示：
*Mar 25 13:28:37:010 2022 xxx IPFW/7/IPFW_INFO: -Chassis=1-Slot=2.1; MBUF was intercepted! Phase Num is 8(post routing beforefrag), Service ID is 3(interzone), Bitmap is 1040000000000000, return 1(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)! Interface is Route-Aggregation31.31, s= 1.1.1.1, d= 2.2.2.2, protocol= 17, pktid = 10736.
因为interzone原因导致报文被丢弃。
3，debugging ip packet 信息有如下显示：
说明从防火墙上发过来的入方向的报文进入的是1框
*Mar 25 13:29:02:533 2022 xxx IPFW/7/IPFW_PACKET: -Chassis=1-Slot=2.1;
Receiving, interface = Route-Aggregation10
version = 4, headlen = 20, tos = 224
pktlen = 489, pktid = 60054, offset = 0, ttl = 244, protocol = 17
checksum = 44129, s = 1.1.1.1, d = 2.2.2.2
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0
prompt: Receiving IP packet from interface Route-Aggregation10.
Payload: UDP
source port = 5060, destination port = 5060
checksum = 0xe8ef, length = 469.

4.查看会话信息，也是建立在1框上。
并且建立的回程的会话的入口是Route-Aggregation30.30
CPU 1 on slot 2 in chassis 1:
Initiator:
Source IP/port: 1.1.1.1/5060
Destination IP/port: 2.2.2.2/5060
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)
Inbound interface: Route-Aggregation10
Source security zone: Untrust
Responder:
Source IP/port: 2.2.2.2/5060
Destination IP/port: 1.1.1.1/5060
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)
Inbound interface: Route-Aggregation30.30
Source security zone: Trust
State: UDP_READY
Application: SIP

5. 通过安全策略的debug信息，以及路由表看，出接口应该是31.31，并且出口是在2框上。
Dst-ZOne=Trust;If-In=Route-Aggregation10(6996), If-Out=Route-Aggregation31.31(7002); Packet Info:Src-IP=103.20.113.10, Dst-IP=192.168.148.100,
6.所以根据如上信息判断：流量是从1框进去2框出去，有跨框情况，并且由于会话建立的出口错误导致此问题产生。

解决方法

开启会话同步功能：session synchronization enable