DNS服务器端口复用导致防火墙域名拦截不定时失败

应用审计 李瑞 2023-01-03 发表

组网及说明

串联部署，我们墙做转发，转发内网的所有DNS报文，并Snort配置了自定义的域名拦截特征，用于拦截指定的黑域名

drop udp any any -> any 53 (msg:"DNS Query for each.tenchier.com";content:"|04|each|08|tenchier|03|com"; classtype:bad-unknown; sid:7002809; rev:1;)

告警信息

不涉及

问题描述

现场出现不定时域名拦截失败的问题

过程分析

查看防火墙上有源端口53的会话，说明DNS服务器存在端口复用的情况，即请求其它域名的DNS应答报文新建了会话，这个报文的五元组恰好与黑域名的请求DNS报文一致，导致黑域名的DNS请求报文被会话放通，无法走DNS过滤流程，导致黑域名被放通。

解决方法

利用安全策略阻断源端口为53的流量，阻止源端口53的报文在防火墙上新建会话