基于域名的安全策略 and DNS过滤 区别详解

域间策略/安全域 **李瑞** 2022-07-05 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

基于域名的安全策略和 DNS过滤 是有区别的，需要根据现场的需求进行选择配置

过程分析

1. DNS过滤：是指通过在DNS代理上开启DNS过滤功能，可以实现对用户通过域名进行的业务访问进行控制。开启DNS过滤功能后，DNS代理将会提取DNS客户端发送的DNS请求报文中的域名与本功能配置的白名单或黑名单进行匹配，根据匹配结果对DNS请求报文执行放行或丢弃动作。
2. dns snooping+基于域名的安全策略：不需要防火墙配置dns代理，只需要终端的DNS交互流量正反向经过防火墙即可。开启DNS Snooping功能后，设备会监听过路的DNS请求报文和DNS应答报文，如果DNS请求报文中的域名与策略中的域名相同，设备会在收到该域名的响应报文时记录域名解析结果，并上报给策略，安全策略就会根据配置动作进行放行或者阻断。这个要求防火墙和终端的dns服务器需要尽量保持一致。

效果上两者也有区别：
dns过滤可以实现终端无法解析黑名单中的域名，即终端无法获取到域名对应的IP地址，但是终端直接访问黑名单中的域名对应的IP地址，该功能是无法阻止的。
而dns snooping可以阻断黑名单域名对应的IP地址的业务流量，无法阻止终端的dns解析。

解决方法

按照分析过程，合理选择功能，实现现场的需求。