配置dns snooping功能实现防火墙基于域名的安全策略原理分析

域间策略/安全域 孔凡安 2022-10-01 发表

问题描述

DNS Snooping功能适用于基于域名做策略的场景（如安全策略、带宽策略等）。设备使用基于域名的策略过滤用户流量时，需要获取域名对应的IP地址才能真正实现流量过滤。

过程分析

1. 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，使得策略可以基于此域名对应的IP地址实现流量过滤。如果DNS请求报文中的域名与过滤规则中的域名不同，设备不会记录域名解析结果。
2. DNS Snooping设备只有位于DNS客户端与DNS服务器之间，或DNS客户端与DNS代理设备之间时，DNS Snooping功能配置后才能正常工作。
3. 开启DNS Snooping功能对应命令为dns snooping enable，缺省情况下，防火墙上域名解析表项的有效时间为DNS响应报文中的TTL。如果现场dns老化时间过短，可以手工调整老化时间，对应命令为object-group dns-aging [time aging-time]

解决方法

display system internal dns snooping host命令用来显示DNS Snooping记录的域名解析信息。该命令需要在probe视图下使用。

详细介绍说明可参考V2.0版本：[配置dns snooping功能实现防火墙基于域名的安全策略原理分析](#)