防火墙如何拦截某些DNS请求报文

IPS防攻击 **彭钦** 2022-07-25 发表

组网及说明

无

告警信息

无

问题描述

现场要求只能访问内部域名，而这些域名不存在.com或.com.cn之类的，但监控端发现终端有这种DNS请求（域名带有.com和.com.cn的请求），现场需要在防火墙侧将其拦截阻断。

过程分析

（1）IPS自定义特征库:

drop udp any any -> any 53 (msg:"DNS Query for *.com"; content:"|03|com"; classtype:bad-unknown; sid:7002821; rev:1;)

drop udp any any -> any 53 (msg:"DNS Query for *.com.cn"; content:"|03|com|02|cn"; classtype:bad-unknown; sid:7002822; rev:1;)

上述信息放在一个txt，然后命名后缀改成.rules

（2）入侵防御--特征--导入snort特征库

（3）新增配置文件

（4）安全策略下选择该入侵防御配置文件。

解决方法

参考上面分析