某局点SecPath W2000-V(二代) 没有攻击日志和访问日志的经验案例

WAF 王燕 2021-05-19 发表

组网及说明

不涉及

问题描述

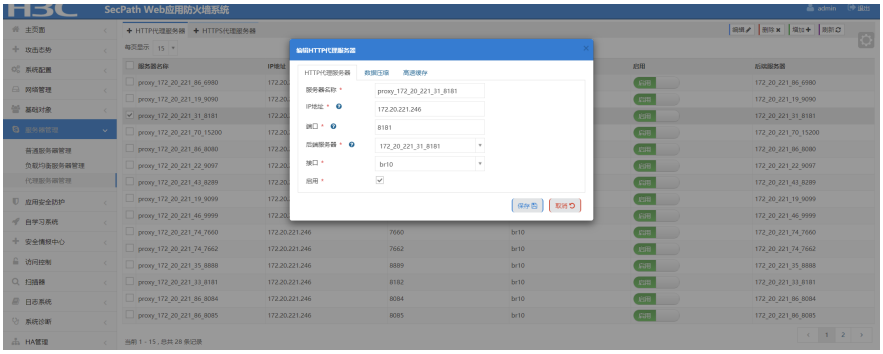
旁路反向代理，没有访问日志和攻击日志；访问方式为使用火狐浏览器访问waf代理IP地址http://172.20.221.246:8181

过程分析

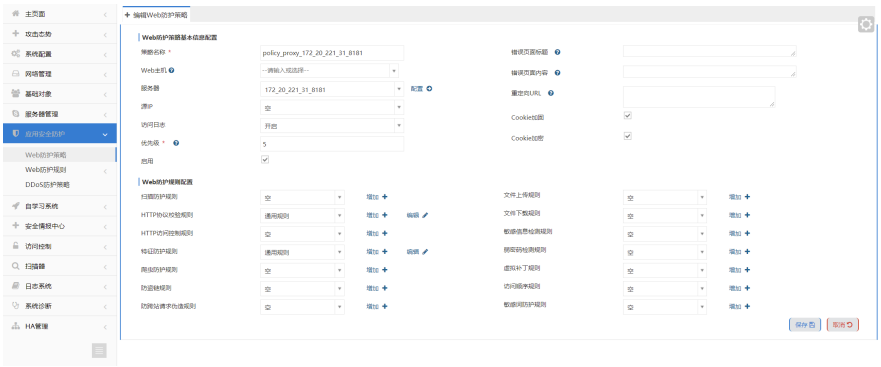
1、检查设备基础配置，本地日志记录已开启；

真实服务器，注意客户还原IP“否”

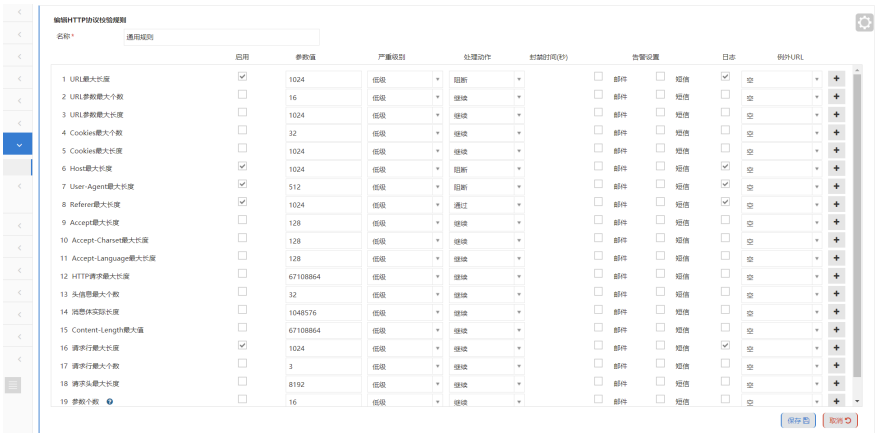
代理服务器配置：



防护规则调用：



检查“通用规则”的日志勾选情况；

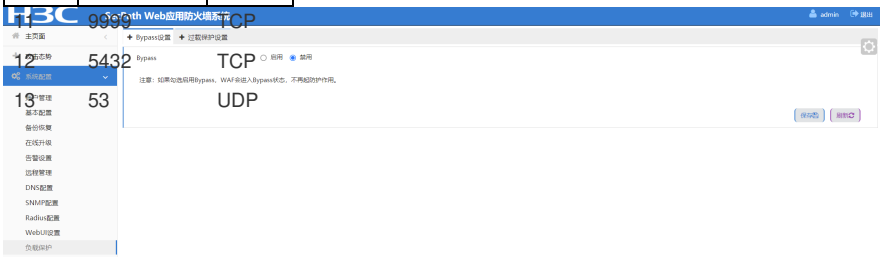


WAF内部端口如下，配置反向代理代时需要注意避开；

序号	目的端口	协议
1	22	TCP
2	443	TCP
3	1801	TCP
4	1081	TCP
5	1800	TCP
6	5081/5082	UDP
7	9996/9998	UDP
8	6379/6998/6999	TCP
9	8848	TCP
10	9997	TCP
11	9999	TCP
12	5432	TCP
13	53	UDP

检查完普通配置之后，注意以下两点：（该问题的处理不涉及，虚拟的waf不支持bypass，硬件WAF需要注意检查）

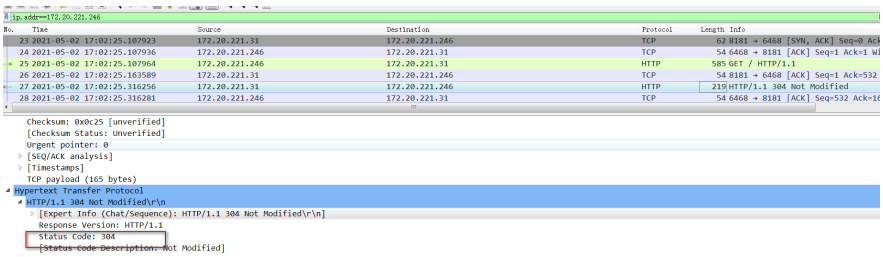
是否启用了bypass



开启过载保护，需要查询系统日志是否触发了软件bypass，然后没有自动恢复，这也是一个故障点；

官网原话：开启过载保护后，当设备超过半数的cpu利用率均超过80%或内存超过95%，WAF进入软件bypass状态，不再起防护作用。CPU的所有核使用率低于30%并且持续40S后就可退出bypass。

2、抓包bri10口，来回流量都有上waf设备，但错误代码304



3、后续研发定位，现场配置的反代端口里有9999端口，与系统内部端口冲突了，导致不产生日志，修改为其他端口后解决