某局点 SecPath W2010-G2(三代)透明代理模式部署监控信息中出现169保留地址

WAF 刘文粟 2023-05-25 发表

问题描述

透明代理模式部署，访问正常
但出现了一个169的地址

协议类型	源IP	目标IP	源端口	目标端口	源端口	目标端口	序列号	标志	发送字节数	接收字节数	操作
TCP	192.168.1.1	192.168.1.2	2	80	80	80	000029	ESTAB	2371	3059	详细 删除
TCP	192.168.1.1	192.168.1.25	7	80	80	80	000029	ESTAB	52	52	详细 删除
TCP	192.168.1.1	192.168.1.208	2082	3180	80	80	000029	ESTAB	2617	31287	详细 删除
TCP	192.168.1.1	192.168.1.77	77	80	80	80	000004	SYN_SENT	44	0	详细 删除
TCP	192.168.1.1	192.168.1.11	11	80	80	80	000000	SYN_SENT	40	0	详细 删除
TCP	192.168.1.1	192.168.1.25	4	80	80	80	000000	SYN_SENT	40	0	详细 删除
TCP	192.168.1.1	192.168.1.105	10517	3101	80	80	000001	SYN_SENT	44	0	详细 删除

过程分析

TCP日志也是正常的

日志详情

日志详情

时间: 2023-05-12 17:27:34	源IP: 119.28.11.11	目的IP: 119.28.11.11
目的端口: 80	资产名称: VNC	源地域: 中国
攻击类型: 协议合规检测	防护策略: 监控	攻击域: HTTP请求头
严重级别: 中级	处理动作: 通过	修改动作: 无
协议类型: HTTP	客户端设备类型: PC端	客户端浏览器类型: 谷歌浏览器
客户端操作系统类型: WINDOWS	CDN IP:	XFF IP:

解决方法

经研发确认，169是内置的地址，用于透明代理交互