Comware V7 NGFW如何快速判断DPI IPS策略是否生效

IPS防攻击 金山 2016-04-21 发表

Comware V7 平台自B64版本起支持DPI特性，包含IPS入侵防御检测功能。
现场工程师完成DPI域间策略配置后，观察一段时间，未发现设备产生IPS攻击防范日志，希望能通过一个简单方法快速判断IPS策略是否已经生效，以及能否产生日志。

无

无

首先确认FW墙IPS特征库是否已经更新，DPI功能特性及域间策略已经配置完成，且DPI功能已经通过inspect activate命令激活。
本案例在V7 IPS特征库1.0.15版本上验证有效，策略规则保持默认值即可。
在客户端侧任意访问一个HTTP服务，可以是一个网站首页，也可以是一台设备的Web配置页面。
要保证这个HTTP访问的双向流量要经过开启DPI特性的NGFW设备转发，关于这一点可以利用防火墙会话表项详细信息及报文收发数统计进行确认。
然后，在浏览器地址栏中，
将原有的URL路径 http://a.b.c.d/x
保持HOST、端口不变，修改为 http://a.b.c.d/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
修改完成后回车再次访问

随后浏览器中通常会显示无法找到该页面等信息，防火墙上应该当产生如下日志：
%Apr 21 11:54:58:136 2016 F1020 IPS/4/IPS_IPV4_INTERZONE: -Context=1; Protocol(1001)=TCP; Application(1002)=http; SrcIPAddr(1003)=172.20.30.254; SrcPort(1004)=49225; DstIPAddr(1007)=172.20.10.2; DstPort(1008)=80; RcvVPNInstance(1042)=--; SrcZoneName(1025)=Trust; DstZoneName(1035)=Untrust; PolicyName(1079)=ips_policy; AttackName(1088)=Web_Server_Arbitrary_Command_Execution_Vulnerability; AttackID(1089)=23566; Category(1090)=Vulnerability; Protection(1091)=WebServer; SubProtection(1092)=Any; Severity(1087)=MEDIUM; Action(1053)=Permit & Logging.

如果设备确实可以产生该日志，则说明DPI IPS模块工作正常。
若未产生日志，请再次检查设备配置是否正确，包括info-center工作状态是否正常；检查客户端与NGFW设备之间是否还有其它应用层安全设备已经阻断该攻击行为。