Comware V7 NGFW如何快速判断DPI AV策略是否生效

AV防病毒 金山 2016-04-21 发表

Comware V7 平台自B64版本起支持DPI特性，包含AV(anti-virus)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 AV特征库1.0.15版本上验证有效，策略规则保持默认值即可。
准备一个病毒文件 Email-Worm.Win32.Agent.mk ，在本案例附件中已经提供，使用WinRAR压缩，密码为123456
将该文件解压并上传到HTTP或FTP服务器，注意为反病毒程序添加例外处理动作，以避免被删除。
在客户端侧使用HTTP或FTP方式，尝试上传下载这个文件，注意要保证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。
在执行文件传输动作时，会发现传输不正常，同时可以在NGFW设备上观察到如下日志产生：
%Apr 21 18:24:26:566 2016 F1020 ANTI-VIR/4/ANTI_IPV4_INTERZONE: -Context=1; Protocol(1001)=TCP; Application(1002)=ftp-data; SrcIPAddr(1003)=172.20.30.254; SrcPort(1004)=49838; DstIPAddr(1007)=172.20.10.2; DstPort(1008)=2364; RcvVPNInstance(1042)=--; SrcZoneName(1025)=Trust; DstZoneName(1035)=Untrust; PolicyName(1079)=untrust_trust; VirusName(1085)=Email-Worm.Win32.Agent.mk; VirusID(1086)=34267; Severity(1087)=MEDIUM; Action(1053)=Reset & Logging.

如果设备确实可以产生该日志，则说明DPI AV(anti-virus)模块工作正常。
若未产生日志，请再次检查设备配置，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文件传输行为。