某局点V7防火墙升级后无法看到攻击防范日志问题处理案例

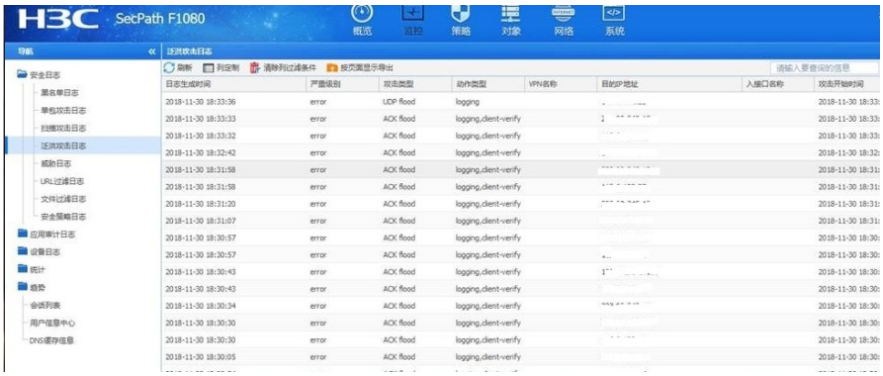
Syslog日志 王鸿渐 2018-12-11 发表

组网及说明

不涉及

问题描述

检查web中的攻击防范日志日志发现仅停留在升级版本的当天，后未一直更新。



过程分析

V7防火墙缺省日志输出规则如下：

输出方向	日志信息来源	开关	等级
控制台	所有支持的模块	开	debugging
监视终端	所有支持的模块	关	debugging
日志主机	所有支持的模块	开	informational
日志缓冲区	所有支持的模块	开	informational
日志文件	所有支持的模块	开	informational

也就是说默认开启info-center enable命令后日志均会产生于日志缓存区和日志文件中。

此时我们在web界面上查看攻击防范日志并没更新，检查日志缓存区和日志文件上有没有生产对应的日志信息，可以通过收集诊断信息和logfile文件进行检查。

检查诊断信息中的save-configruration配置发现

undo info-center enable

升级重启后读取的为保存配置，导致日志信息中心并没有打开。

此时我们开启info-center enable 后发现WEB日志中的攻击防范行为还是没有更新，此时我们做如下检查：

logbuffer中能正常显示攻击防范日志

%Dec XXXXXX F1080 ATK/3/ATK_IP4_ACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=XXXXX; RcvVPNInstance(1042)=; UpperLimit(1049)=1000; Action(1053)=logging; BeginTime_c(1011)=XXXXXX

将设备上的攻击防范信息记录清空做统计，显示正常增长：

display attack-defense statistics security-zone trust

Attack policy name: 1

Slot 1:

Scan attack defense statistics:

AttackType AttackTimes Dropped

No scanning attacks detected.

Flood attack defense statistics:

AttackType AttackTimes Dropped

ACK flood 5 0

UDP flood 1 0

Signature attack defense statistics:

AttackType AttackTimes Dropped

Traceroute 13 13

解决方法

由于现场设备开了安全策略记录日志，生产的大量信息都将攻击防范日志冲散后，导致在web日志中无法正常查看攻击防范日志。关闭安全策略日志记录功能后问题解决，建议配置安全策略时优化配置仅记录关键日志或者将日志发送到日志主机上记录。


H3C SecPath F1080
概览
监控
策略
对象
网络
系统
导航
泛洪攻击日志
安全日志
黑名单日志
单包攻击日志
扫描攻击日志
泛洪攻击日志
威胁日志
URL过滤日志
文件过滤日志
安全策略日志
应用审计日志
设备日志
刷新
列定制
清除列过滤条件
按页面显示导出
请输入要查询的信息
日志生成时间 严重级别 攻击类型 动作类型 VPN名称 目的IP地址 入接口名称 攻击开始时间
2018-12-05 15:43:15 error ACK flood logging 2018-12-05 15:43:15
2018-12-05 15:43:02 error ACK flood logging 2018-12-05 15:43:02
2018-12-05 15:43:02 error ACK flood logging 2018-12-05 15:43:02