SecCenter上看不到防火墙发过来的域间访问日志的处理方法

李树兵　2018-03-18 发表

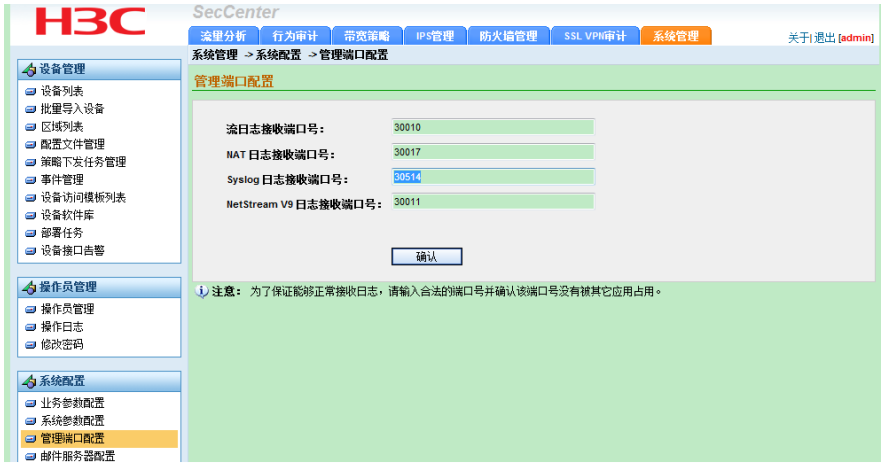
在处理SecCenter问题的时候经常会遇到看不到设备发过来的日志信息，比如常见的看不到防火墙发过来的域间访问控制日志，如下图：

本文将简单介绍处理此类问题的思路。

导致看不到的原因比较多，有如下几个常见原因：①防火墙设备没产生日志。②设备产生日志了但是syslog报文没有发送到SecCenter服务器上③发到服务器上但是由于SecCenter接收服务器异常导致入库失败④数据库表中无数据⑤设备上的时间和服务器所在时间不一致导致查询相应时间点无数据。

对于原因①需要查看防火墙上的遇见策略的配置以及查看防火墙自身页面上是否有日志产生。

原因②SecCenter默认接收syslog日志的端口号是UDP的30514，确保设备上配置syslog主机的时候地址是SecCenter服务器的IP地址，端口号和SecCenter上接收syslog日志的端口号相同。还有就是确保中间有没有经过安全产品，是否可能将日志报错过滤了，可以在服务器上使用抓包软件（比如wireshark）看服务器是否收到设备发过来的udp 30514 的syslog包。



原因③查看SecCenter的接收服务器是否正常，如果不正常，可以重启此服务器。

原因④ SecCenter上域间访问日志对应的数据表是tb_firewall_filter_detail，可以使用数据库管理工具登录到服务器上的MySQL数据库，推荐Navicat Premium 版本，下载链接：http://www.navicat.com.cn/d

ownload，默认的登录端口号是3308，登录的用户名是root，密码是123456，登录进去之后查看tb_firewall_filter_detail这个表里面是否有数据。如果没有数据查看是否服务器上开了防火墙或者运行了其他安全软件，关闭他们进行测试。

原因⑤如果表中有数据但是在页面里面显示没有数据，需要确定设设备上的地址和服务器上的地址是否一致，因为日志发过来的时候是带上了设备的时间，而在SecCenter页面上查的时候是使用的服务器本地的时间，如果时间不一致会导致查看在对应的时间点上查看的时候无数据。如果时间差8小时，有可能是差8个时区导致，可以修改SecCenter上增加设备的时间访问参数。