SecPath F1000-AK1342(V7) 日志主机收不到快速日志

其他 于宛盈 2023-08-04 发表

问题描述

现场配置完快速日志输出后，日志主机收不到SSL VPN用户接入日志以及SSL VPN访问资源日志。

过程分析

现场配置如下：

customlog format packet-filter

customlog format session

customlog format dpi ips

customlog format dpi anti-virus

customlog host 10.10.10.10 export packet-filter session dpi ips anti-virus

customlog timestamp localtime

customlog character-encoding utf-8

1、customlog快速日志支持的模块输出有限，且 SSL VPN用户接入日志以及SSL VPN访问资源日志属于SSLVPN模块，customlog日志并不支持发送SSLVPN模块。

2、现场改成info-center 方式发送SSLVPN模块到日志主机。

注意点如下：

关键配置：info-center source { module-name | default } loghost { deny | level severity }

第一、配置日志信息的输出规则，module 选择SSLVPN模块， 可通过display info-center source module ?命令，通过帮助信息可获得module的设备所支持的模块。

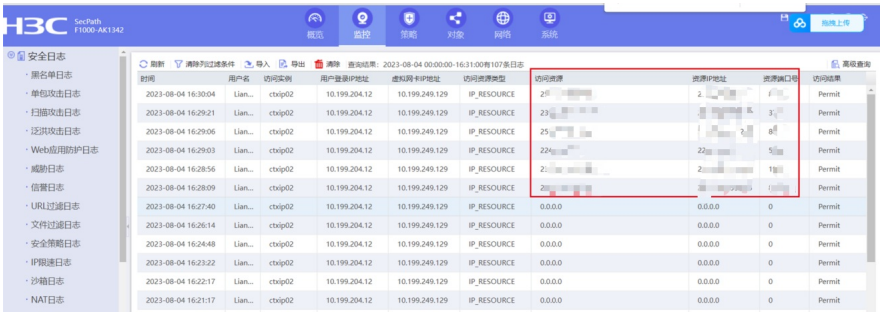
第二、 SSL VPN用户接入日志为SSL VPN用户的登入登出，在level选择中，对应着是数值5、信息级别为 notification。而 SSL VPN访问资源日志，对应着是比5更高级别，所以level 可以选择7。

第三、要注意的是，用户上下线日志生产功能和用户访问资源日志生产功能处于关闭状态，我们必须手动在 SSL VPN访问实例视图下开启。

1）log resource-access enable命令用来开启用户访问资源日志生成功能。

2） log user-login enable命令用来开启用户上下线日志生成功能。

未开启 log resource-access enable brief下，会出现访问资源及资源IP、端口号全0的情况



解决方法

总结：

1、 SSL VPN用户接入日志以及SSL VPN访问资源日志属于SSLVPN模块，我们需要配置info-center loghost x.x.x.x指定以info-center方式发送日志到日志主机，以及 info-center source命令用来配置日志信息的输出规则。

2、 SSL VPN用户接入日志以及SSL VPN访问资源日志生成的前提是，我们必须开启对应日志生成功能。

3、 info-center source命令用来配置日志信息的输出规则中的level，输送到日志主机调至6以上。

4、在display logbuffer或者more sslvpn.log时看不到SSLVPN对应日志时，可以通过 display info-center source module SSLVPN，来查看日志缓冲区（logbuffer）和日志文件（ logfile ）的level是否为很低的参数。