防火墙输出配置日志到日志主机

Syslog日志 **孔凡安** 2021-11-10 发表

组网及说明

不涉及

问题描述

防火墙是否支持配置日志外发到日志主机

过程分析

通常配置日志的存储路径在 flash:/logfile/cfglog.log，可以直接在命令行读取。
也可以在web界面的设备日志-配置日志查看。
说明如下：

配置日志的存储

日志类型	日志格式	存储位置	
配置日志	NTOP日志(分保分支)	优先级顺序	硬盘 /mnt/hda0/ntop_database/syslog_optlog/
			U盘 和硬盘路径类似
			内存数据库
	系统日志	日志缓冲区	display logbuffer module CFGLOG
		Flash	logfile\cfglog.log

- 分保分支中的配置日志
  - ✓ 支持NTOP格式存储到数据库
  - ✓ 如果没有操作则不生成db文件
  - ✓ 若有日志，每天生成一个db文件，每个文件最大3.5G
- 助记符 CFGLOG_CFGOPERATE

```
%Dec 26 14:06:13:847 2018 NGFW CFGLOG/6/CFGLOG_CFGOPERATE: -Client=WEB-User=admin-IPAddr=10.152.36.134-Role=level-3 network-admin ne
twork-operator; Config in system changed: -Old setting=default -New setting=userlog flow export source-ip 10.152.36.21.
```

解决方法

可以根据日志输出等级进行配置，如下：

[FW1]info-center source CFGLOG loghost level ?

alert Action must be taken immediately (severity=1)

critical Critical conditions (severity=2)

debugging Debug-level messages (severity=7)

emergency System is unusable (severity=0)

error Error conditions (severity=3)

informational Informational messages (severity=6)

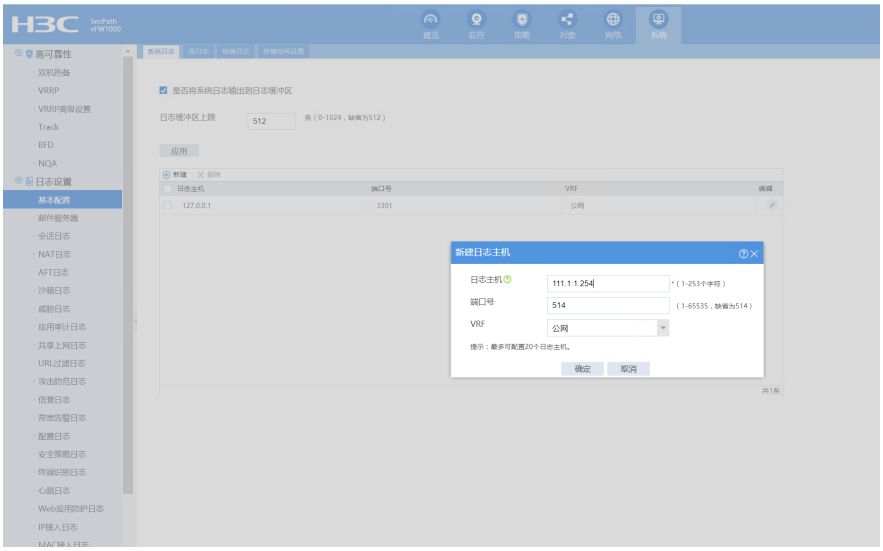
notification Normal but significant conditions (severity=5)

warning Warning conditions (severity=4)

同时Web界面配置syslog日志外发功能。

系统-日志设置-基本配置

新建日志主机



这样，配置日志就可以发送到日志主机了。

抓包发现有CFGLOG.log日志外发：