防火墙和国网日志对接的配置方法和日志格式

Syslog日志 info-center 张春光 2023-10-23 发表

组网及说明

1、国家电网支持的日志类型如下：

日志列表	助记符
用户登录成功	LOGIN
用户退出	LOGOUT
用户登录失败	LOGIN_FAILED
CPU利用率	CPU_EXCEED_THRESHOLD
内存利用率	MEM_EXCEED_THRESHOLD
防火墙电源故障	POWER_ABSENT
防火墙风扇故障	FAN_RECOVERED
防火墙温度异常	TEMPERATURE_WARNING
网口状态异常	PHY_UPDOWN
网口状态恢复	PHY_UPDOWN
不符合安全策略访问	FILTER_ZONE_IPV4_EXECUTION
攻击告警	ATK_IP4_SYN_FLOOD_SZ ATK_IP4_UDP_FLOOD_SZ ATK_ICMP_FLOOD_SZ
入侵保护事件	IPS_IPV4_INTERZONE

2、国家电网日志格式：：

1、支撑组日志：

1	用户登录成功	内容：用户名<空格>源地址
		<5> 2006-03-12 20:12:23 fw01 FW 0 1 **admin 10.1.1.1**
2	用户退出	内容：用户名<空格>源地址
		<5> 2006-03-12 20:12:23 fw01 FW 0 2 **admin 10.1.1.1**
3	用户登录失败	内容：用户名<空格>源地址
		<4> 2006-03-12 20:12:23 fw01 FW 0 3 **shtest 10.1.1.1**
4	修改策略	内容：用户名<空格>源地址<空格>修改内容（包含策略ID）
		<4> 2006-03-12 20:12:23 fw01 FW 0 4 **admin 10.1.1.1 Rule 20 added, permit tcp packets from 10.10.10.0/24 to 20.20.20.0/24**
5	CPU利用率	<5> 2006-03-12 20:12:23 fw01 FW 1 1 **80%**
6	内存利用率	<5> 2006-03-12 20:12:23 fw01 FW 1 2 **80%**
7	防火墙电源故障	<1> 2006-03-12 20:12:23 fw01 FW 1 3 **Power_Supply_Error**
8	防火墙风扇故障	<1> 2006-03-12 20:12:23 fw01 FW 1 4 **Fan_Error**
9	防火墙温度异常	<2> 2006-03-12 20:12:23 fw01 FW 1 5 **Temperature_Over_Limit 65°C**
10	网口状态异常	<4> 2006-03-12 20:12:23 fw01 FW 1 7 **Eth1 Link down**
11	网口状态恢复	<4> 2006-03-12 20:12:23 fw01 FW 1 8 **Eth1 Link up**

2、FW组日志：

1	不符合安全策略访问	内容：协议<空格>源IP地址<空格>源端口<空格>目的IP地址<空格>目的端口
		<2> 2006-03-12 20:12:23 fw01 FW 3 1 **TCP 10.1.1.1 4099 10.2.2.2 80**

3、安全策略组日志：

1	攻击告警	内容：协议<空格>攻击类型<空格>攻击源IP地址<空格>攻击源端口<空格>攻击目标IP地址<空格>攻击目标端口
		<1> 2006-03-12 20:12:23 fw01 FW 3 2 **UDP dos-attack 192.168.2.200 8081 192.168.2.214 80** <1> 2006-03-12 20:12:23 fw01 FW 3 2 **TCP ddos-attack 192.168.2.200 8081 192.168.2.214 80** <1> 2006-03-12 20:12:23 fw01 FW 3 2 **ICMP port-scan-attack 192.168.2.200 8081 192.168.2.214 80**

4、DPI组日志：

1	入侵保护事件	内容：事件描述<空格>源ip地址<空格>源端口<空格>目的ip地址<空格>目的端口
		<0> 2006-03-12 20:12:23 kemel IDS 0 **PPLive 在线流媒体 192.168.10.244 138 192.168.10.255 138**

配置步骤

info-center format sgcc
info-center loghost 127.0.0.1 port 3301 format default
info-center loghost 1.1.1.1 format sgcc
info-center source CFGLOG loghost level informational
customlog format keepalive sgcc
customlog format packet-filter sgcc
customlog format security-policy sgcc
customlog host 1.1.1.1 export security-policy packet-filter
monitor memory-usage logging slot 1 cpu 0 interval 60
monitor cpu-usage logging slot 1 cpu 0 interval 60

配置关键点
info-center配置发送所有系统类日志、DPI日志、ATK日志 customlog快速日志发送安全策略、安全策略配置日志；