UNIS ACG1000 日志信息参考

目 录

1 简介 1
1.1 日志格式说明 1
1.2 如何获取日志信息 2
1.2.1 将日志信息保存到日志文件 2
1.2.2 将日志信息发送到日志服务器 3
1.3 日志模块列表 3
1.4 文档使用说明 3
2 系统管理日志 4
2.1 用户上下线日志 4
2.1.1 Imc 认证上下线通知 4
2.1.2 免认证上下线通知 5
2.1.3 APP 认证上下线通知 6
2.1.4 微信认证上下线通知 7
2.1.5 本地 WEB 认证上下线通知 8
2.1.6 短信认证上下线通知 9
2.1.7 单点登录上下线通知 10
2.2 系统操作日志 11
2.3 事件日志 12
2.4 系统状态日志 12
2.5 健康日志 12
2.6 整机转发流量日志 13
3 流量日志 13
3.1 流量日志 13
3.2 流阻断日志 14
3.3 NAT 日志 14
3.3.1 Nat44 日志 14
3.3.2 Nat 日志 15
4 策略匹配日志 16
4.1 策略匹配日志 16
5 网站访问日志 16
5.1 网站访问日志 17

6 恶意 URL 日志 17
6.1 恶意 URL 日志 18
7 内容审计日志 18
7.1 IM 上报内容 19
7.2 博客、微博、论坛、社区上报内容 20
7.3 搜索引擎上报内容 21
7.4 邮件上报 22
7.5 文件传输上报内容 23
7.6 娱乐/股票上报内容 24
7.7 其他应用 25
8 防攻击日志 25
8.1 防异常包攻击日志 26
8.2 防扫描攻击日志 27
8.3 防 DOS 攻击日志 28
9 IPSec_traffic 日志 29
9.1 IPSec_traffic 日志 29
9.2 VPN 告警日志 29

1 简介

本文档介绍 UNIS ACG1000 日志信息，包含日志的参数介绍、产生原因、处理建议等，为用户进行系统诊断和维护提供参考。

本文假设您已具备数据通信技术知识，并熟悉 UNIS 网络产品。

1.1 日志格式说明

缺省情况下，日志采用如下格式：

```
<pri>time name msg
```

表1-1 日志头字段说明

字段	描述
pri	PRI部分由尖括号包含的一个数字构成，这个数字包含了程序模块（Facility）、严重性（Severity），这个数字是由Facility乘以 8，然后加上Severity得来
time	时间紧跟在PRI后面，中间没有空格，格式必须是“Mmm dd hh:mm:ss”，不包括年份。“日”的数字如果是1～9，前面会补一个空格（也就是月份后面有两个空格），而“小时”、“分”、“秒”则在前面补“0”。月份取值包括：Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec
name	设备名称或IP，注意，name字段一定要包含sn，格式是： device_name;sn;ipversion;msgversion Ipversion包括：ipv4,ipv6
msg	该日志的具体内容，包含事件或错误发生的详细信息。

日志信息按严重性可划分为如表 1-2 所示的八个等级，各等级的严重性依照数值从 0～7 依次降低。

表1-2 日志等级说明

级别	严重程度	描述
0	Emergency	表示设备不可用的信息，如系统授权已到期
1	Alert	表示设备出现重大故障，需要立刻做出反应的信息，如流量超出接口上限
2	Critical	表示严重信息，如设备温度已经超过预警值，设备电源、风扇出现故障等
3	Error	表示错误信息，如接口链路状态变化，存储卡拔出等
4	Warning	表示警告信息，如接口连接断开，内存耗尽告警等
5	Notification	表示正常出现但是重要的信息，如通过终端登录设备，设备重启等
6	Informational	表示需要记录的通知信息，如通过命令行输入命令的记录信息，执行ping命令的日志信息等
7	Debug	表示调试过程产生的信息

本文使用表 1-3 定义的方式表示日志描述字段中的可变参数域。

表1-3 可变参数域

参数标识	参数类型
INT16	有符号的16位整数
UINT16	无符号的16位整数
INT32	有符号的32位整数
UINT32	无符号的32位整数
INT64	有符号的64位整数
UINT64	无符号的64位整数
DOUBLE	有符号的双32位整数，格式为：[INT32].[INT32]
HEX	十六进制数
CHAR	字节类型
STRING	字符串类型
IPADDR	IP地址
MAC	MAC地址
DATE	日期
TIME	时间

1.2 如何获取日志信息

缺省情况下，设备的日志功能处于开启状态，并允许向控制台（console）、WEB 页面、日志服务器（loghost）和本地日志文件（logfile）方向输出日志信息。您可以在 WEB 页面上实时看到系统输出的日志信息，也可以通过 **display log event** 命令查看事件日志信息。

通过 **log** 命令可以设置日志信息的输出规则，通过输出规则可以指定日志的输出方向以及对哪些特性模块或信息等级的日志信息进行输出。所有信息等级高于或等于设置等级的日志信息都会被输出到指定的输出方向。例如，输出规则中如果指定允许等级为 6（informational）的信息输出，则等级 0～6 的信息均会被输出到指定的输出方向。

说明

- 监视终端是指以 AUX、VTY、TTY 类型用户线登录的用户终端。
- 配置日志服务器后，日志服务器也可以实时监控日志信息。
- 本地日志文件可以记录日志信息，但仅能通过 WEB 页面查看。

1.2.1 将日志信息保存到日志文件

缺省情况下，系统根据通过 **log** 命令配置的日志过滤条件，将需要记录的日志实时记录到日志文件当中。日志文件中的内容可以通过 WEB 页面中的日志查询实时查看。

1.2.2 将日志信息发送到日志服务器

您可以通过配置日志服务器向指定的 IP 地址发送设备的日志信息，还可同时配置日志服务器接收日志信息的端口号（该值需要和日志主机侧的设置一致，缺省为 514）。如果设备侧配置的日志服务器接收日志信息的端口号与日志服务器侧不一致，则日志服务器将无法接收日志信息。

您可以指定多个不同服务器同时接收设备产生的日志信息。但最多可指定 3 个。

1.3 日志模块列表

表 1-4 列出了所有可能生成日志信息的日志模块。

表1-4 日志模块列表

模块名	说明
系统管理日志	包括系统操作日志和系统状态日志
流量日志	与流量相关的日志
网站访问日志	所有访问过的网站
恶意URL日志	访问的恶意URL
内容审计日志	审计出的流量的内容
防攻击日志	发生攻击的日志
系统事件日志	系统事件，比如接口up/down

1.4 文档使用说明

本文将系统日志信息按照日志模块分类。

本文以表格的形式对日志信息进行介绍。有关表中各项的含义请参考表 1-5。

表1-5 日志信息表内容说明

表项	说明	举例
日志内容	显示日志信息的具体内容	ACL [$1:UINT32] [$2:STRING] [$3:COUNTER64] packet(s).
参数解释	按照参数在日志中出现的顺序对参数进行解释。 参数顺序用“$数字”表示，例如“$1”表示在该日志中出现的第一个参数。	$1：ACL编号 $2：ACL规则的ID和内容 $3：与ACL规则匹配的数据包个数
日志等级	日志严重等级	6
举例	一个真实的日志信息举例。	operator_name=admin; operate_ip=192.168.1.105; create_time=2014-07-22 17:56:32;level=notice;reason=mod;result=success;manage style=WEB;content=mod syslog configuration
日志说明	解释日志信息和日志生成的原因	匹配一条ACL规则的数据包个数。该日志会在数据包个数发生变化时输出。

表项	说明	举例
处理建议	建议用户应采取哪些处理措施。级别为6的“Informational”日志信息是正常运行的通知信息，用户无需处理。	系统正常运行时产生的信息，无需处理。

2 系统管理日志

本节介绍系统管理输出的日志。

2.1 用户上下线日志

2.1.1 Imc 认证上下线通知

1. IMC 认证上线通知

日志内容	[$1:Imc] [$2:login]: logname=[$3:USERNAME] realname=[$4:REALNAME] groupname=[$5:GROUPNAME]@[$6:IPADDR]($7:MACADDR)
参数解释	$1：Imc认证。 $2：认证上线。 $3：认证用户名字。 $4：用户真实名称。 $5：用户组名称。 $6：用户IP地址。 $7：用户MAC地址。
日志等级	5
举例	Imc login:logname=123 realname=321 groupname=test @1.1.1.1(8c:34:fd:26:0f:50)
日志说明	Imc认证上线通知。
处理建议	无。

2. IMC 认证下线通知

日志内容	[$1:Imc] [$2:logout]: logname=[$3:USERNAME] realname=[$4:REALNAME] groupname=[$5:GROUPNAME]@[$6:IPADDR]($7:MACADDR) login at [$8:TIME], logout at [$9:TIME], duration is [$10:TIME], reason is [$11:logout/kickoff]
参数解释	$1：Imc认证。 $2：认证下线。 $3：认证用户名字。 $4：用户真实名称。 $5：用户组名称。 $6：用户IP地址。 $7：用户MAC地址。 $8：登录时间。 $9：退出时间。 $10：登录时常。 $11：logout/kickoff退出/强制下线。
日志等级	5
举例	Imc logout:logname=test realname=testabc groupname=test@1.1.1.1(8c:34:fd:26:0f:50) login at 2016-05-25 09:17:26, logout at 2016-05-25 09:18:52, duration is 85s, reason is logout
日志说明	Imc认证下线通知。
处理建议	无。

2.1.2 免认证上下线通知

1. 免认证上线通知

日志内容	[$1:Free] [$2:login]: [$3:USERNAME]@[$4:IPADDR]($5:MACADDR)
参数解释	$1： 免认证方式。 $2：认证上线。 $3：认证用户名字。 $4：用户IP地址。 $5：用户MAC地址。
日志等级	5
举例	Free login: test@1.1.1.1(8c:34:fd:26:0f:50)
日志说明	免认证上线通知。
处理建议	无。

2. 免认证下线通知

日志内容	[$1:Free] [$2:logout]: logname=[$3:USERNAME]@[$4:IPADDR]($5:MACADDR) login at [$6:TIME], logout at [$7:TIME], duration is [$8:TIME], reason is [$9:logout/kickoff]
参数解释	$1： 免认证方式。 $2：认证下线。 $3：认证用户名字。 $4：用户IP地址。 $5：用户MAC地址。 $6：登录时间。 $7：退出时间。 $8：登录时常。 $9：logout/kickoff退出/强制下线。
日志等级	5
举例	Free logout:logname=123@1.1.1.1(8c:34:fd:26:0f:50) login at 2016-05-25 09:17:26, logout at 2016-05-25 09:18:52, duration is 85s, reason is logout
日志说明	APP认证下线通知。
处理建议	无。

2.1.3 APP 认证上下线通知

1. APP 认证上线通知

日志内容	[$1:APP] [$2:login]: logname=[$3:USERNAME] realname=[$4:REALNAME] groupname=[$5:GROUPNAME]@[$6:IPADDR]($7:MACADDR)
参数解释	$1：APP认证。 $2：认证上线。 $3：认证用户名字。 $4：用户真实名称。 $5：用户组名称。 $6：用户IP地址。 $7：用户MAC地址。
日志等级	5
举例	APP login:logname=123 realname=321 groupname=APPgroup@1.1.1.1(8c:34:fd:26:0f:50)
日志说明	APP认证上线通知。
处理建议	无。

2. APP 认证下线通知

日志内容	[$1:APP] [$2:logout]: logname=[$3:USERNAME] realname=[$4:REALNAME] groupname=[$5:GROUPNAME]@[$6:IPADDR]($7:MACADDR) login at [$8:TIME], logout at [$9:TIME], duration is [$10:TIME], reason is [$11:logout/kickoff]
参数解释	$1：APP认证。 $2：认证下线。 $3：认证用户名字。 $4：用户真实名称。 $5：用户组名称。 $6：用户IP地址。 $7：用户MAC地址。 $8：登录时间。 $9：退出时间。 $10：登录时常。 $11：logout/kickoff退出/强制下线。
日志等级	5
举例	APP logout:logname=test realname=testabc groupname=APPgroup@1.1.1.1(8c:34:fd:26:0f:50) login at 2016-05-25 09:17:26, logout at 2016-05-25 09:18:52, duration is 85s, reason is logout
日志说明	APP认证下线通知。
处理建议	无。

2.1.4 微信认证上下线通知

1. 微信认证上线通知

日志内容	[$1:Wechat] [$2:login]: [$3:USERNAME]@ [$4:IPADDR]($5:MACADDR)
参数解释	$1： 微信认证方式。 $2：认证上线。 $3：认证用户名字。 $4：认证用户地址。 $5：用户MAC地址。
日志等级	5
举例	Wechat login: oWW9-t4_wnLcLNS2kgcQL09QJRfY@192.168.8.62(74:e5:43:16:cc:26)
日志说明	微信认证上线通知。
处理建议	无。

2. 微信认证下线通知

日志内容	[$1:Wechat] [$2:logout]: logname=[$3:USERNAME]@[$4:IPADDR]($5:MACADDR) login at [$6:TIME], logout at [$7:TIME], duration is [$8:TIME], reason is [$9:logout/kickoff]
参数解释	$1： 微信认证方式。 $2：认证下线。 $3：认证用户名字。 $4：用户IP地址。 $5：用户MAC地址。 $6：登录时间。 $7：退出时间。 $8：登录时常。 $9：logout/kickoff退出/强制下线。
日志等级	5
举例	Wechat logout:logname=owIrqtxgUPUiaBntthMX5csEOr7c@192.168.6.69(80:ed:2c:8a:2d:be) login at 2016-05-25 09:17:26, logout at 2016-05-25 09:18:52, duration is 85s, reason is logout
日志说明	微信认证下线通知。
处理建议	无。

2.1.5 本地 WEB 认证上下线通知

1. 本地 WEB 认证上线通知

日志内容	[$1: Local authentication] [$2:login]: [$3:USERNAME]@[$4:IPADDR]($5:MACADDR)
参数解释	$1：本地WEB认证方式。 $2：认证上线。 $3：认证用户名字。 $4：用户IP地址。 $5：用户MAC地址。
日志等级	5
举例	Local authentication login: test@1.1.1.1(8c:34:fd:26:0f:50)
日志说明	本地WEB认证上线通知。
处理建议	无。

2. 本地 WEB 认证下线通知

日志内容	[$1: Local authentication] [$2:logout]: [$3:USERNAME]@[$4:IPADDR]($5:MACADDR) login at [$6:TIME], logout at [$7:TIME], duration is [$8:TIME], reason is [$9:logout/kickoff]
参数解释	$1： 本地WEB认证方式。 $2：认证下线。 $3：认证用户名字。 $4：用户IP地址。 $5：用户MAC地址。 $6：登录时间。 $7：退出时间。 $8：登录时常。 $9：logout/kickoff 退出/强制下线。
日志等级	5
举例	Local authentication logout: 123@1.1.1.1(8c:34:fd:26:0f:50) login at 2016-05-25 09:17:26, logout at 2016-05-25 09:18:52, duration is 85s, reason is logout
日志说明	本地WEB认证下线通知。
处理建议	无。

2.1.6 短信认证上下线通知

1. 短信认证上线通知

日志内容	[$1:Sms] [$2:login]: [$3:USERNAME]@[$4:IPADDR]($5:MACADDR)
参数解释	$1：短信认证方式。 $2：认证上线。 $3：认证用户名字。 $4：用户IP地址。 $5：用户MAC地址。
日志等级	5
举例	Sms login: test@1.1.1.1(8c:34:fd:26:0f:50)
日志说明	短信认证上线通知。
处理建议	无。

2. 短信认证下线通知

日志内容	[$1:Sms] [$2:logout]: [$3:USERNAME]@[$4:IPADDR]($5:MACADDR) login at [$6:TIME], logout at [$7:TIME], duration is [$8:TIME], reason is [$9:logout/kickoff]
参数解释	$1：短信认证方式。 $2：认证下线。 $3：认证用户名字。 $4：用户IP地址。 $5：用户MAC地址。 $6：登录时间。 $7：退出时间。 $8：登录时常。 $9：logout/kickoff退出/强制下线。
日志等级	5
举例	Sms logout: 123@1.1.1.1(8c:34:fd:26:0f:50) login at 2016-05-25 09:17:26, logout at 2016-05-25 09:18:52, duration is 85s, reason is logout
日志说明	短信认证下线通知。
处理建议	无。

2.1.7 单点登录上下线通知

1. 单点登录上线通知

日志内容	[$1:SSO] [$2:login]: [$3:USERNAME]@[$4:IPADDR]($5:MACADDR)
参数解释	$1：单点登录方式。 $2：认证上线。 $3：认证用户名字。 $4：用户IP地址。 $5：用户MAC地址。
日志等级	5
举例	SSO login: test@1.1.1.1(8c:34:fd:26:0f:50)
日志说明	单点登录上线通知。
处理建议	无。

2. 单点登录下线通知

日志内容	[$1:SSO] [$2:logout]: [$3:USERNAME]@[$4:IPADDR]($5:MACADDR) login at [$6:TIME], logout at [$7:TIME], duration is [$8:TIME], reason is [$9:logout/kickoff]
参数解释	$1：单点登录方式。 $2：认证下线。 $3：认证用户名字。 $4：用户IP地址。 $5：用户MAC地址。 $6：登录时间。 $7：退出时间。 $8：登录时常。 $9：logout/kickoff退出/强制下线。
日志等级	5
举例	SSO logout: 123@1.1.1.1(8c:34:fd:26:0f:50) login at 2016-05-25 09:17:26, logout at 2016-05-25 09:18:52, duration is 85s, reason is logout
日志说明	单点登录下线通知。
处理建议	无。

2.2 系统操作日志

日志内容	operator_name=[$1:STRING];operate_ip=[$2:IPADDR];create_time=[$3:TIME];level=[$4:STRING];reason=[$5:STRING];result=[$6:STRING];managestyle=[$7:STRING];content=[$8:STRING]
参数解释	$1：操作员名字。 $2：操作IP地址。 $3：操作时间。 $4：事件级别。 $5：操作原因。 $6：操作结果。 $7：管理类型。 $8：操作内容。
日志等级	0~6
举例	<6>Nov 29 14:09:52 host;110103300117111310721344;ipv4;3; operate: operator_name=admin;operate_ip=172.16.0.2;create_time=2017-11-29 14:09:52;level=notice;reason=add;result=success;managestyle=WEB;content=add ipv6_policy configuration
日志说明	管理员执行操作。
处理建议	无。

2.3 事件日志

日志内容	[$1:STRING].
参数解释	$1：系统重启、接口UP/DOWN、升级版本、HA切换等信息。
日志等级	0~6
举例	admin@192.168.1.105 logout from ssh.
日志说明	系统状态变化。
处理建议	无。

2.4 系统状态日志

日志内容	[$1:STRING].
参数解释	$1：系统健康检查信息等。
日志等级	0~6
举例	<4>Nov 29 14:09:52 host;110103300117111310721344;ipv4;3; system_state: 健康检查 tcp 探测成功
日志说明	系统状态变化。
处理建议	无。

2.5 健康日志

日志内容	cpu_used=[$1:UINT32];mem_used=[$2:UINT32];disk_used=[$3:UINT32];temperature=[$4:UINT32];session_num=[$5:UINT32]
参数解释	$1：CPU使用率。 $2：内存使用率。 $3：硬盘使用率。 $4：温度。 $5：会话数。
日志等级	6
举例	<6>Nov 29 14:09:52 host;110103300117111310721344;ipv4;3; device_health: cpu_used=10;mem_used=57;disk_used=1;temperature=0;session_num=79
日志说明	每分钟发送一次。
处理建议	无。

2.6 整机转发流量日志

日志内容	up=[$1:UINT64];down=[$2:UINT64]
参数解释	$1：设备一分钟内上行平均流速（bps）。 $2：设备一分钟内下行平均流速（bps）。
日志等级	6
举例	<6> Nov 29 14:09:52 host;110103300117111310721344;ipv4;3;device_traffic: up=167559;down=2258504
日志说明	每分钟发送一次。
处理建议	无。

3 流量日志

本节介绍系统流量产生的日志信息。

3.1 流量日志

日志内容	user_name=[$1:STRING];ugname=[$2:STRING];umac=[$3:MAC];uip=[$4:IPADDR];appname=[$5:STRING];appg_name=[$6:STRING];up=[$7:UINT64];down=[$8:UINT64];create_time=[$9:UINT64];end_time=[$10:UINT64]
参数解释	$1：用户名称。 $2：用户组名称。 $3：用户MAC地址。 $4：用户IP地址。 $5：应用名称。 $6：应用组名称。 $7：上行流量。 $8：下行流量。 $9：开始统计时间。 $10：结束统计时间。
日志等级	6
举例	<6> Nov 29 14:09:52 host;110103300117111310721344;ipv4;3;statistic_traffic: user_name=刘晓林;ugname=root;umac=60:0B:03:AD:12:14;uip=192.168.8.82;appname=UDP;appgname=网络协议;up=720;down=0;create_time=1511859600;end_time=1511859660
日志说明	每分钟发送一次。
处理建议	无。

3.2 流阻断日志

日志内容	src_ip=[$1:IPADDR];dst_ip=[$2:IPADDR];protocol=[$3:STRING];src_port=[$4:UINT32];dst_port=[$5:UINT32];in_interface=[$6:STRING];out_interface=[$7:STRING];policyid=[$8:UINT32];action=[$9:STRING];Content=[$10:STRING];
参数解释	$1：源IP。 $2：目的IP。 $3：协议。 $4：源端口。 $5：目的端口。 $6：入接口。 $7：出接口。 $8：策略id。 $9：动作。 $10：内容。
日志等级	6
举例	<6> Nov 29 14:09:52 host;1101033001171111310721344;ipv4;3; policy_detail: src_ip=1.1.1.5;dst_ip=2.2.2.2;protocol=TCP;src_port=4056;dst_port=5006;in_interface=ge0;out_interface=ge1;policyid=2;action=deny;Content=;
日志说明	匹配到deny策略，且配置日志时发送。
处理建议	无。

3.3 NAT日志

3.3.1 Nat44 日志

日志内容	BIND:user [$1:IPADDR], nat_range:[$2:IPADDR] [$3:UINT32]-[$4:UINT32] ,ifdesc=[$5:STRING]
参数解释	$1：用户IP。 $2：转换IP。 $3：起始端口。 $4：终止端口。 $5：接口名字。
日志等级	6
举例	<6>Nov 28 16:46:03 host;1101033001171111310721344;ipv4;3; nat: BIND:user 192.168.5.36, nat_range:220.249.52.178 12224-12323 ,ifdesc=ge16
日志说明	匹配到NAT44规则，且规则里和日志过滤中均配置发送日志。
处理建议	无。

3.3.2 Nat 日志

日志内容	src_ip=[$1:IPADDR];src_port=[$2:UINT32];dst_ip=[$3:IPADDR];dst_port=[$4:UINT32];before_trans_ip=[$5:IPADDR];after_trans_ip=[$6:IPADDR];protocol=[$7:STRING];before_trans_port=[$8:UINT32];after_trans_port=[$9:UINT32];type=[$10:STRING]
参数解释	$1：源IP。 $2：源端口。 $3：目的IP。 $4：目的端口。 $5：转换前的IP。 $6：转换后的IP。 $7：协议。 $8：转换前的端口。 $9：转换后的端口。 $10：类型。
日志等级	6
举例	<6> Dec 1 16:44:16 host;110103300117111310721344;ipv4;3; nat: src_ip=172.16.0.2;src_port=60081;dst_ip=140.207.119.140;dst_port=80;before_trans_ip=172.16.0.2;after_trans_ip=192.168.3.9;protocol=TCP;before_trans_port=60081;after_trans_port=60081;type=snat
日志说明	匹配到NAT规则，且规则里和日志过滤中均配置发送日志。
处理建议	无。

4 策略匹配日志

4.1 策略匹配日志

日志内容	src_ip=[$1:STRING];dst_ip=[$2:STRING];protocol=[$3:STRING];src_port=[$4:INT];dst_port=[$5:INT];in_interface=[$6:STRING];out_interface=[$7:STRING];policyid=[$8:INT];action=[$9:STRING];Content=[$10:STRING]
参数解释	$1：源IP。 $2：目的IP。 $3：协议。 $4：源端口。 $5：目的端口。 $6：内网接口。 $7：外网接口。 $8：策略ID。 $9：策略动作。 $10：。
日志等级	6
举例	<6>Nov 28 16:45:18 host;1101033001171113107213 44;ipv4;3; policy_detail: src_ip=192.168.10.209;dst_ip=106.120.168.93;protocol=TCP;src_port=60051;dst_port=80;in_interface=ge10;out_interface=ge17;policyid=11;action=permit;Content=
日志说明	匹配到NAT规则，且规则里和日志过滤中均配置发送日志。
处理建议	无。

5 网站访问日志

本节介绍网站访问产生的日志信息。

5.1 网站访问日志

日志内容	user_name=[$1:STRING];user_group_name=[$2:STRING];term_platform=[$3:STRING];term_device=[$4:STRING];src_ip=[$5:STRING];dst_ip=[$6:STRING];url_domain=[$7:STRING];url=[$8:STRING];url_cate_name=[$9:STRING];handle_action=[$10:UINT32];msg=[$11:]
参数解释	$1：用户名称。 $2：用户组名称。 $3：终端平台。 $4：终端设备。 $5：源IP地址。 $6：目的IP地址。 $7：网站域名。 $8：用户访问的完整URL。 $9：网站分类名称。 $10：策略配置的处理动作。 $11：预留字段，不填充内容。
日志等级	0~6
举例	<6>Nov 28 16:55:48 host;110103300117111310721344;ipv4;3; web_access: user_name=192.168.4.223;user_group_name=root;term_platform=windows;term_device=PC;src_ip=192.168.4.223;dst_ip=125.88.193.243;url_domain=www.haosou.com;url=http://www.haosou.com/brw?w=1&v=7.1.1.558&u=http%3A%2F%2Fchurch-group-discounts.com%2F;url_cate_name= 其他;handle_action=0;msg=
日志说明	匹配到URL审计策略，且规则和日志过滤均配置发送日志。
处理建议	无。

6 恶意 URL 日志

本节介绍恶意 URL 产生的日志信息。

6.1 恶意URL日志

日志内容	user_name=[$1:STRING];user_group_name=[$2:STRING];term_platform=[$3:STRNG];term_device=[$4:STRING];src_ip=[$5:IPADDR];dst_ip=[$6:IPADDR];web_name=[$7:STRING];url=[$8:STRING];msg=[$9:]
参数解释	$1：用户名称。 $2：用户组名称。 $3：终端平台。 $4：终端设备。 $5：源IP地址。 $6：目的IP地址。 $7：网站域名。 $8：用户访问的完整URL。 $9：预留字段，不填充内容。
日志等级	4
举例	user_name=192.168.4.223;user_group_name=root;term_platform=windows;term_device=PC;src_ip=192.168.4.223;dst_ip=61.155.222.136;web_name=009blog.com;url=http://009blog.com/favicon.ico;msg=
日志说明	匹配到过滤恶意URL策略，且规则和日志过滤均配置发送日志。
处理建议	无。

7 内容审计日志

本节介绍内容审计产生的日志信息。

7.1 IM上报内容

日志内容	user_name=[$1:STRING];user_group_name=[$2:STRING];term_platform=[$3:STRING];term_device=[$4:STRING];pid=[$5:UINT32];src_mac=[$6:STRING];src_ip=[$7:IPADDR];dst_ip=[$8:IPADDR];dst_port=[$9:UINT32];app_name=[$10:STRING];app_cat_name=[$11:STRING];handle_action=[$12:UINT32];account=[$13:UINT32];action_name=[$14:STRING];content=[$15:STRING];msg=[$16:]
参数解释	$1：用户名称。 $2：用户组名称。 $3：终端平台。 $4：终端设备。 $5：策略id。 $6：源MAC地址。 $7：源IP地址。 $8：目的IP地址。 $9：目的端口号。 $10：应用名称。 $11：应用分类名称。 $12：策略配置的处理动作。 $13：帐号。 $14：应用行为名称。 $15：聊天内容。 $16：预留字段，不填充内容。
日志等级	0~6
举例	<6>Nov 28 16:45:28 host;110103300117111310721344;ipv4;3; im: user_name= 靖娟娟;user_group_name=root;term_platform=;term_device=PC;pid=1;src_mac=68:91:d0:d0:0b:79;src_ip=192.168.1.69;dst_ip=223.167.104.149;dst_port=8080;app_name=微信;app_cat_name= 即时通讯;handle_action=0;account=2743413360;action_name=收消息;content=;msg=
日志说明	匹配到七元组策略或（如：即时通讯）应用过滤规则，且规则和日志过滤均配置发送日志。
处理建议	无。

7.2 博客、微博、论坛、社区上报内容

日志内容	user_name=[$1:STRING];user_group_name=[$2:STRING];term_platform=[$3:STRING];term_device=[$4:STRING];pid=[$5:UINT32];src_mac=[$6:STRING];src_ip=[$7:IPADDR];dst_ip=[$8:IPADDR];dst_port=[$9:UINT32;app_name=[$10:STRING];app_cat_name=[$11:STRING];handle_action=[$12:UINT32];account=[$13:UINT32];action_name=[$14:STRING];subject=[$15:STRING];content=[$16:STRING];msg=[$17:]
参数解释	$1：用户名称。 $2：用户组名称。 $3：终端平台。 $4：终端设备。 $5：策略id。 $6：源MAC地址。 $7：源IP地址。 $8：目的IP地址。 $9：目的端口号。 $10：应用名称。 $11：应用分类名称。 $12：策略配置的处理动作。 $13：帐号。 $14：应用行为名称。 $15：主题。 $16：内容。 $17：预留字段，不填充内容。
日志等级	0~6
举例	<5>Nov 28 17:00:29 host;11010330011711310721344;ipv4;3;social_log:user_name=192.168.4.223;user_group_name=root;term_platform=windows;term_device=PC;pid=1;src_mac=28:d2:44:37:6c:f0;src_ip=192.168.4.223;dst_ip=116.10.186.184;dst_port=80;app_name= 猫扑论坛;app_cat_name=网络社区;handle_action=0;account=sradish_xiaoxiao;action_name= 发表;subject= 灌水;content=测试发帖灌水;msg=
日志说明	匹配到七元组策略或（如：网络社区）应用过滤规则，且规则和日志过滤均配置发送日志。
处理建议	无。

7.3 搜索引擎上报内容

日志内容	user_name=[$1:STRING];user_group_name=[$2:STRING];term_platform=[$3:STRING];term_device=[$4:STRING];pid=[$5:UINT32];src_mac=[$6:STRING];src_ip=[$7:IPADDR];dst_ip=[$8:IPADDR];dst_port=[$9:UINT32];app_name=[$10:STRING];app_cat_name=[$11:STRING];handle_action=[$12: UINT32];account=[$13:STRING];action_name=[$14:STRING];content=[$15:STRING];msg=[$16:]
参数解释	$1：用户名称。 $2：用户组名称。 $3：终端平台。 $4：终端设备。 $5：策略id。 $6：源MAC地址。 $7：源IP地址。 $8：目的IP地址。 $9：目的端口号。 $10：应用名称。 $11：应用分类名称。 $12：策略配置的处理动作。 $13：帐号。 $14：应用行为名称。 $15：内容。 $16：预留字段，不填充内容。
日志等级	0~6
举例	<6>Nov 28 16:47:58 host;11010330011711131072134 4;ipv4;3; search_engine: user_name=车源;user_group_name=root;term_platform=;term_device=PC;pid=13;src_mac=68:f7:28:a0:3d:3e;src_ip=192.168.8.13;dst_ip=202.89.233.101;dst_port=443;app_name=必应;app_cat_name=搜索引擎;handle_action=0;account=;action_name=搜索;content={_t_:1,_cl_:_w_,_v_:_th_,_id_:_C11913ED7902462E8DFB3F820252E2C1_,_fz_:3210240,_q_:_houtianhu_,_app_:_*_,_kb_:_*_,_c_:5};msg=
日志说明	匹配到七元组策略或（如：搜索引擎）应用过滤规则，且规则和日志过滤均配置发送日志。
处理建议	无。

7.4 邮件上报

日志内容	user_name=[$1:STRING];user_group_name=[$2:STRING];term_platform=[$3:STRING];term_device=[$4:STRING];pid=[$5:UINT32];src_mac=[$6:STRING];src_ip=[$7:IPADDR];dst_ip=[$8:IPADDR];dst_port=[$9:UINT32];app_name=[$10:STRING];app_cat_name=[$11:STRING];handle_action=[$12:UINT32];account=[$13:STRING];action_name=[$14:STRING];send_addr=[$15:IPADDR];receive_addr=[$16:IPADDR];subject=[$17:STRING];content=[$18:STRING];file_name=[$19:STRING];file_size=[$20:UINT32];msg=[$21:]
参数解释	$1：用户名称。 $2：用户组名称。 $3：终端平台。 $4：终端设备。 $5：策略id。 $6：源MAC地址。 $7：源IP地址。 $8：目的IP地址。 $9：目的端口号。 $10：应用名称。 $11：应用分类名称。 $12：策略配置的处理动作。 $13：帐号。 $14：应用行为名称。 $15：发送地址。 $16：接收地址。 $17：主题。 $18：邮件内容。 $19：文件名称。 $20：文件大小。 $21：预留字段，不填充内容。
日志等级	0~6
举例	<5>Nov 28 16:45:33 host;11010330011711310721344;ipv4;3; mail: user_name=10.0.50.4;user_group_name=anonymous;term_platform=;term_device=PC;pid=2;src_mac=68:91:d0:d0:05:bd;src_ip=10.0.50.4;dst_ip=220.181.15.127;dst_port=1746;app_name=IMAP邮件协议;app_cat_name=电子邮件;handle_action=0;account=zhangqiang_zz@126.com;action_name= 接收邮件;send_addr=Amazon Web Services <aws-marketing-email-replies@amazon.com>;receive_addr=zhangqiang_zz@126.com;subject= Monday Announcements from AWS re:Invent 2017;content=;file_name=;file_size=0;msg=
日志说明	匹配到七元组策略或（如：电子邮件）应用过滤规则，且规则和日志过滤均配置发送日志。
处理建议	无。

7.5 文件传输上报内容

日志内容	user_name=[$1:STRING];user_group_name=[$2:STRING];term_platform=[$3:STRING];term_device=[$4:STRING];pid=[$5:UINT32];src_mac=[$6:STRING];src_ip=[$7:IPADDR];dst_ip=$8:[IPADDR];dst_port=[$9:UINT32];app_name=[$10:STRING];app_cat_name=[$11:STRING];handle_action=[$12:UINT32];account=[$13:STRING];action_name=[$14:STRING];file_name=[$15:STRING];msg=[$16:]
参数解释	$1：用户名称。 $2：用户组名称。 $3：终端平台。 $4：终端设备。 $5：策略id。 $6：源MAC地址。 $7：源IP地址。 $8：目的IP地址。 $9：目的端口号。 $10：应用名称。 $11：应用分类名称。 $12：策略配置的处理动作。 $13：帐号。 $14：应用行为名称。 $15：文件名称。 $16：预留字段，不填充内容。
日志等级	0~6
举例	<6>Nov 28 16:45:18 host;11010330011711131072134 4;ipv4;3; file_transfer: user_name=192.168.7.105;user_group_name=anonymous;term_platform=;term_device=Mac;pid=19;src_mac=7c:04:d0:c6:4f:22;src_ip=192.168.7.105;dst_ip=180.97.34.136;dst_port=49771;app_name= 百度网盘;app_cat_name=文件传输;handle_action=0;account=;action_name= 接收;file_name=89006A2E.AutodeskSketchBook_1.7.0.0_x64__tf1gferkr813w.Appx;msg=
日志说明	匹配到七元组策略或（如：文件传输类）应用过滤规则，且规则和日志过滤均配置发送日志。
处理建议	无。

7.6 娱乐/股票上报内容

日志内容	user_name=[$1:STRING];user_group_name=[$2:STRING];term_platform=[$3:STRING];term_device=[$4:STRING];pid=[$5:UINT32];src_mac=[$6:STRING];src_ip=[$7:IPADDR];dst_ip=[$8:IPADDR];dst_port=[$9:UINT32];app_name=[$10:STRING];app_cat_name=[$11:STRING];handle_action=[$12:UINT32];account=[$13:STRING];action_name=[$14:STRING];parent_info=[$15:STRING];msg=[$16:]
参数解释	$1：用户名称。 $2：用户组名称。 $3：终端平台。 $4：终端设备。 $5：策略id。 $6：源MAC地址。 $7：源IP地址。 $8：目的IP地址。 $9：目的端口号。 $10：应用名称。 $11：应用分类名称。 $12：策略配置的处理动作。 $13：帐号。 $14：应用行为名称。 $15：父协议信息。 $16：预留字段，不填充内容。
日志等级	0~6
举例	<6>Nov 28 16:45:38 host;110103300117111310721344;ipv4;3;relax_stock:user_name=张亮;user_group_name=root;term_platform=;term_device=PC;pid=1;src_mac=84:7b:eb:29:8d:a5;src_ip=192.168.1.100;dst_ip=150.138.174.36;dst_port=80;app_name=网络视频/语音;app_cat_name=流媒体;handle_action=0;account=;action_name=看视频;parent_info=;msg=parent_info=;
日志说明	匹配到七元组策略或（如：股票软件类，流媒体类）应用过滤规则，且规则和日志过滤均配置发送日志。
处理建议	无。

7.7 其他应用

日志内容	user_name=[$1:STRING];user_group_name=[$2:STRING];term_platform=[$3:STRING];term_device=[$4:STRING];pid=[$5:UINT32];src_mac=[$6:STRING];src_ip=[$7:IPADDR];dst_ip=[$8:IPADDR];dst_port=[$9:UINT32];app_name=[$10:STRING];app_cat_name=[$11:STRING];handle_action=[$12:UINT32];account=[$13:STRING];action_name=[$14:STRING];content=[$15:STRING];msg=[$16:]
参数解释	$1：用户名称。 $2：用户组名称。 $3：终端平台。 $4：终端设备。 $5：策略id。 $6：源MAC地址。 $7：源IP地址。 $8：目的IP地址。 $9：目的端口号。 $10：应用名称。 $11：应用分类名称。 $12：策略配置的处理动作。 $13：帐号。 $14：应用行为名称。 $15：内容。 $16：预留字段，不填充内容。
日志等级	0~6
举例	<6>Nov 28 16:45:18 host;11010330011711131072134 4;ipv4;3; other_app: user_name=192.168.10.209;user_group_name=anonymous;term_platform=;term_device=PC;pid=11;src_mac=28:56:5a:13:3f:ab;src_ip=192.168.10.209;dst_ip=106.120.168.93;dst_port=80;app_name= 360安全中心;app_cat_name=软件更新;handle_action=0;account=;action_name= 网页浏览;content=;msg=
日志说明	匹配到七元组策略或（如：其他应用类及各应用类的网页浏览行为）应用过滤规则，且规则和日志过滤均配置发送日志。
处理建议	无。

8 防攻击日志

本节介绍防攻击产生的日志信息。

8.1 防异常包攻击日志

日志内容	user_name=[$1:STRING];src_ip=[$2:IPADDR];src_port=[$3:UINT32];dst_ip=[$4:IPADDR];dst_port=[$5:UINT32];name=[$6:STRING];type=[$7:STRING];protocol=[$8:STRING];mac=[$9:MAC];count=[$10:UINT32];level=[$11:UINT32];in_if_name=[$12:STRING];create_time=[$13:UINT64];end_time=[$14:UINT64];extend=[$15];
参数解释	$1：用户名称。 $2：源IP地址。 $3：源端口号。 $4：目的IP地址。 $5：目的端口号。 $6：名称。 $7：类型。 $8：协议名称。 $9：MAC地址。 $10：计数。 $11：级别。 $12：入接口名称。 $13：创建时间。 $14：结束时间。 $15：预留字段，不填充数据。
日志等级	4
举例	<4>Nov 28 16:47:38 host;110103300117111310721344;ipv4;3;security_abnormal_pkt:user_name=test;src_ip=20.1.1.5;src_port=0;dst_ip=30.1.1.2;dst_port=0;name=jolt2;type=abnormal-packet;protocol=ICMP;mac=00:40:01:55:24:34;count=8268;level=4;in_if_name=ge6;create_time=1406279692;end_time=1406279702;extend=;
日志说明	检查到网络层攻击。
处理建议	无。

8.2 防扫描攻击日志

日志内容	user_name=[$1:STRING];src_ip=[$2:IPADDR];src_port=[$3:UINT32];dst_ip=[$4:IPADDR];dst_port=[$5:UINT32];name=[$6:STRING];type=[$7:STRING];protocol=[$8:STRING];mac=[$9:MAC];count=[$10:UINT32];level=[$11:UINT32];in_if_name=[$12:STRING];create_time=[$13:UINT64];end_time=[$14:UINT64];extend=[$15];
参数解释	$1：用户名称。 $2：源IP地址。 $3：源端口号。 $4：目的IP地址。 $5：目的端口号。 $6：名称。 $7：类型。 $8：协议名称。 $9：MAC地址。 $10：计数。 $11：级别。 $12：入接口名称。 $13：创建时间。 $14：结束时间。 $15：预留字段，不用填充数据。
日志等级	4
举例	<4>Nov 28 16:47:38 host;110103300117111310721344;ipv4;3; security_scan: user_name= ;src_ip=192.168.2.34;src_port=0;dst_ip=198.46.82.65;dst_port=0;name=ipsweep;type=scan-attack;protocol=ICMP;mac=00:21:45:c0:fa:00;count=1;level=4;in_if_name=ge2;create_time=1511858856;end_time=1511858856;extend=;
日志说明	检查到网络层攻击。
处理建议	无。

8.3 防DOS攻击日志

日志内容	user_name=[$1:STRING];src_ip=[$2:IPADDR];src_port=[$3:UINT32];dst_ip=[$4:IPADDR];dst_port=[$5:UINT32];name=[$6:STRING];type=[$7:STRING];protocol=[$8:STRING];mac=[$9:MAC];count=[$10:UINT32];level=[$11:UINT32];in_if_name=[$12:STRING];create_time=[$13:UINT64];end_time=[$14:UINT64];extend=;
参数解释	$1：用户名称。 $2：源IP地址。 $3：源端口号。 $4：目的IP地址。 $5：目的端口号。 $6：名称。 $7：类型。 $8：协议名称。 $9：MAC地址。 $10：计数。 $11：级别。 $12：入接口名称。 $13：创建时间。 $14：结束时间。 $15：预留字段，不用填充数据。
日志等级	4
举例	<4>Nov 28 16:47:55 host;110103300117111310721344;ipv4;3; security_flood: user_name= ;src_ip=192.168.5.95;src_port=1863;dst_ip=121.10.215.99;dst_port=1863;name=udpflood;type=flood-attack;protocol=UDP;mac=28:d2:44:7c:2e:51;count=1;level=4;in_if_name=ge5;create_time=1511858873;end_time=1511858873;extend=;
日志说明	检查到网络层攻击。
处理建议	无。

9 IPSec_traffic 日志

9.1 IPSec_traffic日志

日志内容	本地vpn名字=[$1:STRING]；上行带宽=[$2:INT64]；下行带宽=[$3:INT64]
参数解释	$1：本地VPN名称 $2：上行带宽。 $3：下行带宽。
日志等级	6
举例	<6>Nov 28 16:46:13 host;110103300117111310721344;ipv4;3; ipsec_traffic: 本地vpn名字=北京abt总部；上行带宽=68770；下行带宽=9163
日志说明	名称为“总部”的VPN上行带宽为68770，下行带宽为9163。单位：bit
处理建议	无。

9.2 VPN告警日志

日志内容	local_vpn_name=[$1:STRING64];peer_vpn_name=[$2:STRING64];local_vpn_ip=[$3:IPADDR];peer_vpn_ip=[$4:IPADDR];state=[$5:UINT32];line=[$6:STRING64]
参数解释	$1：本地VPN名称 $2：对端VPN名称 $3：本地VPN接口地址 $4：对端VPN接口地址 $5：状态，固定为0 $6：分支节点断开的线路名称，仅分支节点有。
日志等级	6
举例	-
日志说明	因对端网络不可达造成IPsec VPN断开。
处理建议	无。