UNIS NGIPS 8000[T1000-CN-G][T1000-E]系列入侵防御系统

日志信息参考

目 录

1 简介

本文档介绍设备日志信息，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 HOST 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
恶意URL日志	访问的恶意URL
应用控制日志	应用控制策略相关的日志
内容审计日志	审计出的流量的内容
安全日志	发生攻击的日志

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;managestyle=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。
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	系统正常运行时产生的信息，无需处理。

表项	说明	举例
	常运行的通知信息，用户无需处理。	

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 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。

2.1.5 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。

2.1.6 Portal Server 认证上下线通知

1. Portal Server 认证上线通知

日志内容	[$1: Portal Server] [$2:login]: [$3:USERNAME]@[$4:IPADDR]($5:MACADDR)
参数解释	$1：Portal Server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	Portal Server login: test@1.1.1.1(8c:34:fd:26:0f:50)
日志说明	Portal Server认证上线通知。
处理建议	无。

2. Portal Server 认证下线通知

日志内容	[$1: Portal Server] [$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：Portal Server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	Portal Server 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	Portal Server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。

2.1.8 IC 卡认证上下线通知

1. IC 卡认证上线通知

日志内容	[$1: IC_CARD] [$2:login]: [$3:USERNAME]@[$4:IPADDR]($5:MACADDR)
参数解释	$1：IC卡认证方式。 $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	IC_CARD login: test@1.1.1.1(8c:34:fd:26:0f:50)
日志说明	IC卡认证上线通知。
处理建议	无。

2. IC 卡认证下线通知

日志内容	[$1: IC_CARD] [$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：IC卡认证方式。 $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	IC_CARD logout: 123@1.1.1.1(8c:34:fd:26:0f:50) login at 2020-11-14 12:10:12, logout at 2020-11-14 12:10:41, duration is 28s, reason is logout
日志说明	IC卡认证下线通知。
处理建议	无。

2.1.9 POP3 认证上下线通知

1. POP3 认证上线通知

日志内容	[$1: POP3] [$2:login]: [$3:USERNAME]@[$4:IPADDR]($5:MACADDR)
参数解释	$1：POP3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	POP3 login: test@1.1.1.1(8c:34:fd:26:0f:50)
日志说明	POP3认证上线通知。
处理建议	无。

2. POP3 认证下线通知

日志内容	[$1: POP3] [$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：POP3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	POP3 logout: 123@1.1.1.1(8c:34:fd:26:0f:50) login at 2020-10-14 09:17:26, logout at 2020-10-14 09:18:52, duration is 85s, reason is logout
日志说明	POP3认证下线通知。
处理建议	无。

2.1.10 钉钉认证上下线通知

1. 钉钉认证上线通知

日志内容	[$1: Dingtalk] [$2:login]: [$3:USERNAME]@[$4:IPADDR]($5:MACADDR)
参数解释	$1：钉钉认证方式。 $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	Dingtalk login: test@1.1.1.1(8c:34:fd:26:0f:50)
日志说明	钉钉认证上线通知。
处理建议	无。

2. 短信认证下线通知

日志内容	[$1: Dingtalk] [$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：钉钉认证方式。 $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	Dingtalk logout: 123@1.1.1.1(8c:34:fd:26:0f:50) login at 2020-10-15 11:17:26, logout at 2020-10-15 11:18:52, duration is 85s, reason is logout
日志说明	钉钉认证下线通知。
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;1101033001171111310721344;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 系统状态日志

日志内容	[$1:STRING].
参数解释	$1：系统重启、接口UP/DOWN、升级版本、HA切换等系统状态信息。
日志等级	0~6
举例	<4>Nov 29 14:09:52 HOST;1101033001171111310721344;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。

2.4 健康日志

日志内容	CPU使用=[$1:UINT32];内存使用=[$2:UINT32];磁盘使用=[$3:UINT32];温度=[$4:UINT32];会话数=[$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;1101033001171111310721344;ipv4;3; device_health: CPU使用=10;内存使用=57;磁盘使用=1;温度=0;会话数=79
日志说明	每分钟发送一次。
处理建议	无。

2.5 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;1101033001171111310721344;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（单位为bit）。 $8：下行流量（单位为bit）。 $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;11010330011711131072134 4;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。

4 恶意 URL 日志

本节介绍恶意 URL 产生的日志信息。

4.1 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。

5 应用控制日志

本节介绍应用控制策略产生的日志信息。

5.1 应用控制日志

日志内容	user_name=[$1:STRING];user_group_name=[$2:STRING];term_platform=[$3:STRING];term_device=[$4:STRING];src_mac=[$5:STRING];src_ip=[$6:STRING]";"dst_ip=[$7:STRING];src_port=[$8:UINT16];dst_port=[$9:UINT16];pid=[$10:UINT32];pname=[$11:STRING];log_level=[$12:UINT32];handle_action=[$13:UINT32];act_name=[$14:STRING];";"app_name=[$15:STRING];app_cat_name=[$16:STRING];url_cate_name=[$17:STRING];url=[$18:STRING];account=[$19:STRING];content=[$20:STRING];ptype_desc=[$21:STRING]
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MAC地址。 $6：源IP地址。 $7：目的IP地址。 $8：源端口。 $9：目的端口。 $10：策略ID。 $11：策略名称：具体含义是策略类别，策略ID，子策略类别，子策略ID。其中策略类别的具体含义如表5-1所示。 $12：日志等级。 $13：处理动作。 $14：动作名称（接受还是拒绝）。 $15：应用名称。 $16：应用分类名称。 $17：URL分类名称。 $18：URL地址。 $19：账号。 $20：日志内容。 $21：策略描述。（包括应用控制、恶意URL控制、URL控制、邮件控制、搜索控制、HTTP上传控制、网页内容控制、虚拟帐号控制、应用审计）
日志等级	0~6
举例	Aug 31 16:11:28 10.0.53.205 Aug 31 16:17:36 HOST;11010020011908190911315 3;ipv4;3; app_filter: user_name=192.168.2.90;user_group_name=anonymous;term_platform=;term_device=未知类型;src_mac=00:21:cc:ca:39:25;src_ip=192.168.2.90;dst_ip=113.96.232.106;src_port=49908;dst_port=143;pid=1;pname=IPv4_policy_1_app_policy_1;log_level=0; handle_action=0;act_name=accept;app_name=IMAP邮件协议;app_cat_name=电子邮件;url_cate_name=;url=;account=;content=;ptype_desc=应用控制
日志说明	用户192.168.2.90使用了邮件协议。 其中“pname=IPv4_policy_1_app_policy_1”的含义为：策略类别为“IPv4应用控制策略”，策略ID是1，子策略为应用控制策略，子策略ID是1； “ptype_desc=应用控制”含义为：该策略类别为应用控制策略。
处理建议	接受放行

表5-1 策略类别详细说明

参数	含义
app_policy	应用控制
malware_policy	恶意URL控制
url_policy	URL控制
mail_policy	,邮件控制
search_policy	搜索控制
http_post_policy	HTTP上传控制
web_content_policy	网页内容控制
virtual_count_policy	虚拟帐号控制
Audit_policy	应用审计

6 内容审计日志

本节介绍内容审计产生的日志信息。

6.1 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;11010330011711131072134 4;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= 其它;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。

6.2 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;11010330011711131072134 4;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。

6.3 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;11010330011711131072134 4;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。

6.4 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。

6.5 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;11010330011711131072134 4;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。

6.6 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。

6.7 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;11010330011711131072134 4;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。

6.8 其它应用

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：其它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。

7 安全日志

本节介绍安全防护产生的日志信息。

7.1 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;11010330011711131072134 4;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。

7.2 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;11010330011711131072134 4;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。

7.3 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;11010330011711131072134 4;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。

7.4 IP-MAC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 16:47:55 HOST;11010330011711131072134 4;ipv4;3; security_ipmac: user_name= ;src_ip=192.168.5.95;src_port=1863;dst_ip=121.10.215.99;dst_port=1863;name=ip-mac-bind;type=arp-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。

7.5 IPS日志

日志内容	user_id=[$1:UINT32];user_name=[$2:STRING];policy_id=[$3:UINT32];src_mac=[$4:MACADDR];dst_mac=[$5:MACADDR];src_ip=[$6:IPADDR];dst_ip=[$7:IPADDR];src_port=[$8:UINT32];dst_port=[$9:UINT32] ;X-Forwarded-For=[$10:IPADDR];app_name=[$11:STRING];protocol=[$12:STRING];app_protocol=[$13:STRING];event_id=[$14:UINT32];event_name=[$15:STRING];event_type=[$16:STRING];level=[$17:STRING];ctime=[$18:STRING];action=[$19:STRING]
参数解释	$1：用户ID。 $2：用户名称。 $3：策略id。 $4：源MAC地址。 $5：目的MAC地址。 $6：源IP地址。 $7：目的IP地址。 $8：源端口。 $9：目的端口。 $10：HTTP代理IP。 $11：应用名称。 $12：协议名称。 $13：应用协议名称。 $14：事件ID。 $15：事件名称。 $16：事件类型。 $17：日志等级。 $18：日志时间。 $19：动作名称。
日志等级	1，4，5，6
举例	<6>Nov 28 16:48:13 HOST;00000080011708140090479 7;ipv4;3; ips: user_id=2;user_name=10.0.0.160;policy_id=1;src_mac=02:1a:c5:01:00:00;dst_mac=02:1a:c5:02:00:00;src_ip=10.0.0.160;dst_ip=10.0.0.200;src_port=25141;dst_port=4318;X-Forwarded-For=;app_name=全部应用;protocol=TCP;app_protocol=TCP;event_id=24639;event_name=PROTOCOL-RPC端口映射CA BrightStor ARCserve tcp过程122无效的函数调用尝试 ;event_type=拒绝服务;level=notice;ctime=2020-08-18 09:09:37;action=drop
日志说明	控制策略引用IPS模板，流量匹配到模板下的某条规则，且规则配置了记录日志。
处理建议	建议去检查确认内网用户是否存在异常的网络行为。

7.6 AV日志

日志内容	virus_name=[$1:STRING64];file_name=[$2:STRING256];user_name=[$3:STRING32];user_id=[$4:UINT32];policy_id=[$5:UINT32];src_mac=[$6:MACADDR];dst_mac=[$7:MACADDR];src_ip=[$8:IPADDR];dst_ip=[$9:IPADDR];src_port=[$10:UINT32];dst_port=[$11:UINT32];app_name=[$12:STRING32];app_name_en=[$13:STRING32];protocol=[$14:STRING32];app_protocol=[$15:STRING32];level=[$16:STRING];ctime=[$17:STRING];action=[$18:STRING]
参数解释	$1：病毒名称。 $2：文件名称。 $3：用户名称。 $4：用户ID。 $5：策略ID。 $6：源MAC。 $7：目的MAC。 $8：源IP。 $9：目的IP。 $10：源端口。 $11：目的端口。 $12：应用名称。 $13：应用英文名称。 $14：协议类型。 $15：高层协议类型。 $16：日志级别。 $17：发生时间。 $18：策略动作。
日志等级	4
举例	<4>Nov 28 16:48:13 HOST;00000080011708140090479 7;ipv4;3; AV: virus_name=avvirus;file_name=0823bdf784007435fc0741b270866a3c; user_name=192.168.8.90;user_id=2; policy_id=1;src_mac=00:01:7a:e1:63:0e;dst_mac=00:21:45:c7:00:c8;src_ip=192.168.8.90;dst_ip=119.147.194.95;src_port=19760;dst_port=8000;app_name=SMTP邮件协议; app_name_en=SMTP;protocol=TCP;app_protocol=SMTP; level=info;ctime=2017-11-28 16:48:13;action=pass
日志说明	检查到病毒。
处理建议	建议安装杀毒软件进行病毒查杀。

7.7 防暴力破解日志

日志内容	occur_time=[$1:STRING];src=[$2:IPADDR];dst=[$3:IPADDR];service=[$4:STRING]; action=[$5:STRING];
参数解释	$1：发生时间。 $2：源IP地址。 $3：目的IP地址。 $4：服务。 $5：动作。
日志等级	0~6
举例	<6>Nov 28 16:45:18 网关HA主; 1900011001160507437176 53; ipv4; 3; bfd: occur_time=2018-07-02 17:19:52;src=192.168.1.82;dst=192.168.1.65;service=pop3;action=blist
日志说明	匹配到防暴力破解规则。
处理建议	建议检查源地址对应用户是否存在异常行为。

7.8 非法外联日志

日志内容	time=[$1:STRING]; policy_name =[$2:STRING]; server_addr =[$3:IPADDR]; out_addr=[$4:IPADDR]; proto =[$5:STRING]; action=[$6:STRING];
参数解释	$1：发生时间。 $2：服务器非法外联策略名称。 $3：服务器IP地址。 $4：外联地址IP地址。 $5：协议。 $6：动作。
日志等级	1
举例	<1>Jul 12 14:59:18 D12;53000000011905134201075 1;ipv4;3; servconn_policy: time=2019-07-12 14:59:18;policy_name=out;server_addr=192.168.24.80;out_addr=192.168.24.255; proto=UDP;port=137;action=1
日志说明	匹配到非法外联防护策略。
处理建议	无。

7.9 行为模型日志

日志内容	src_ip=[$1:IPADDR];st_ip=[$2:IPADDR];src_port=[$3:UINT32];dst_port=[$4:UINT32];src_mac=[$5:MACADDR];dst_mac=[$6:MACADDR];protocol=[$7:STRING];behavior_name_cn=[$8:STRING];behavior_name_en=[$9:STRING];behavior_detail=[$10:STRING];behavior_desc=[$11:STRING];level=[$12:STRING];action=[$13:STRING];
参数解释	$1：源IP地址。 $2：目的IP地址。 $3：源端口。 $4：目的端口。 $5：源MAC地址。 $6：目的MAC地址。 $7：协议类型。 $8：行为中文名称。 $9：行为英文名称。 $10：行为详情。 $11：行为描述。 $12：日志等级。 $12：动作。
日志等级	0~6
举例	<4>Jul 11 19:03:49
日志说明	2.208-2039-master;530000500119032974562668;ipv4;3;behavior_model:src_ip=172.16.22.61;dst_ip=172.17.1.95;src_port=21833;dst_port=53;src_mac=02:1a:c5:01:15:3b;dst_mac=68:91:d0:d5:7f:7d;protocol=UDP;behavior_name_cn=DNS 隧道;
处理建议	behavior_name_en=DNStunnel;behavior_detail=dnscat.27d5012b62965cbe1376c70aec84b1856d;behavior_desc=Dns traffic is too large,level=warning;action=拒绝

8 安全日志（探针）

8.1 入侵检测日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcMAC=[$4:MACADDR] DestMAC=[$5:MACADDR] SrcDeviceType=[$6:CHAR] SrcOS=[$7:CHAR] AttackTime=[$8:UINT64] SrcIPAddr=[$9:IPADDR] SrcPort=[$10:UINT16] DstIPAddr=[$11:IPADDR] DstPort=[$12:UINT16] Protocol=[$13:UCHAR] Application=[$14:CHAR] AttackType=[$15:UINT8] AttackName=[$16:CHAR] ProtectSubject=[$17:CHAR] SubProtectSubject=[$18:CHAR] CriticalLevel=[$19:UINT16] AttackDirection=[$20:UINT16] HttpPayload=[$21:CHAR] HttpRequestLine=[$22:CHAR] HttpResponseLine=[$23:CHAR] HttpHost=[$24:CHAR] ResponseCode=[$25:UINT16] AttackResult=[$26:UINT16] XForwarded=[$27:CHAR] CVE=[$28:CHAR] CNNVD=[$29:CHAR] BID=[$30:CHAR] MSB=[$31:CHAR] PackageName=[$32:CHAR] RuleId=[$33:UINT16] PolicyName=[$34:CHAR] SrcZoneName=[$35:CHAR] DestZoneName=[$36:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：源MAC地址。 $5：目的MAC地址。 $6：终端类型。 $7：终端操作系统。 $8：攻击时间。 $9：源IP地址。 $10：源端口号。 $11：目的IP地址。 $12：目的端口号。 $13：协议。 $14：应用类型。 $15：攻击分类。 $16：攻击名称。 $17：保护对象。 $18：保护子对象。 $19：严重级别。 $20：特征命中方向。 $21：攻击载荷。 $22：HTTP请求头。 $23：HTTP响应头。 $24：HTTP HOST。 $25：响应码。 $26：攻击结果。 $27：X-Forwarded-For。 $28：CVE编码 $29：CNNVD编号。

	$30：BID。 $31：MSB。 $32：取证报文名称。 $33：规则id。 $34：策略名称。 $35：源安全域。 $36：目的安全域。
日志等级	1，4，5，6
举例	<6>4 2020-11-06 18:07:01 HOST 11010040011508075469051l ipv4 Msgid=ips UserName=100.1.1.2 UserGroup= SrcMAC=00:50:56:b8:c8:e7 DestMAC=00:50:56:b8:4a:76 SrcDeviceType= SrcOS= AttackTime= SrcIPAddr=100.1.1.2 SrcPort=7847 DstIPAddr=100.2.1.3 DstPort=8500 Protocol=TCP Application=HTTP文件上传 AttackType=用户提权 AttackName= SERVER-OTHER Adobe ColdFusion未经身份验证的文件上传尝试 ProtectSubject= SubProtectSubject= CriticalLevel=2 AttackDirection=0 HttpPayload= HttpRequestLine= HttpResponseLine= HttpHost= ResponseCode= AttackResult=0 XForwarded= CVE= CNNVD= BID= MSB= PackageName= RuleId=1 PolicyName= SrcZoneName= DestZoneName=
日志说明	
处理建议	无。

8.2 病毒防护日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcMAC=[$4:MACADDR] DestMAC=[$5:MACADDR] SrcDeviceType=[$6:CHAR] SrcOS=[$7:CHAR] AttackTime=[$8:UINT64] SrcIPAddr=[$9:IPADDR] SrcPort=[$10:UINT16] DstIPAddr=[$11:IPADDR] DstPort=[$12:UINT16] Protocol=[$13:UCHAR] AppType=[$14:CHAR] VirusType=[$15:CHAR] VirusName=[$16:CHAR] VirusFamilyName=[$17:CHAR] AttackDirection=[$18:UINT16] XForwarded=[$19:CHAR] CriticalLevel=[$20:UINT16] FileName=[$21:CHAR] FileType=[$22:UINT16] FileHash=[$23:CHAR] FileSize=[$24:UINT64] RuleId=[$25:UINT64] PolicyName=[$26:CHAR] SrcZoneName=[$27:CHAR] DestZoneName=[$28:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：源MAC地址。 $5：目的MAC地址。 $6：终端类型。 $7：终端操作系统。 $8：攻击时间。 $9：源IP地址。 $10：源端口号。 $11：目的IP地址。 $12：目的端口号。 $13：协议。 $14：应用类型。 $15：病毒类型。 $16：病毒名称。 $17：病毒家族名称 $18：传输方向。 $19：X-Forwarded-For。 $20：严重级别。 $21：文件名。 $22：文件类型。。 $23：文件HASH。 $24：文件大小。 $25：规则id $26：策略名称。 $27：源安全域。 $28：目的安全域。
日志等级	4

举例	<4>4 2020-11-09 10:49:56 HOST 11010040011508075469051l ipv4 Msgid=av UserName=100.1.1.4 UserGroup=anonymous SrcMAC=00:50:56:b8:c8:e7 DestMAC=00:50:56:b8:4a:76 SrcDeviceType= SrcOS= AttackTime= SrcIPAddr=100.1.1.4 SrcPort=60263 DstIPAddr=100.2.1.2 DstPort=25 Protocol=TCP AppType=SMTP VirusType=adware VirusName=eicar.com VirusFamilyName= AttackDirection=0 XForwarded= CriticalLevel=2 FileName=poc%n%n.com FileType= FileHash= FileSize=68 RuleId=1 PolicyName= SrcZoneName= DestZoneName=
日志说明	
处理建议	无。

8.3 防暴力破解日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcMAC=[$4:MACADDR] DestMAC=[$5:MACADDR] SrcDeviceType=[$6:CHAR] SrcOS=[$7:CHAR] AttackTime=[$8:UINT64] SrcIPAddr=[$9:IPADDR] SrcPort=[$10:UINT16] DstIPAddr=[$11:IPADDR] DstPort=[$12:UINT16] Protocol=[$13:UCHAR] AppType=[$14:CHAR] BruteForceUserName=[$15:CHAR] AttackName=[$16:CHAR] BruteForceResult=[$17:UINT16] CriticalLevel=[$18:UINT16]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：源MAC地址。 $5：目的MAC地址。 $6：终端类型。 $7：终端操作系统。 $8：攻击时间。 $9：源IP地址。 $10：源端口号。 $11：目的IP地址。 $12：目的端口号。 $13：协议。 $14：应用类型。 $15：暴破用户名。 $16：攻击名称。 $17：暴破结果。 $18：严重级别。
日志等级	0~6

举例	<6>4 2020-11-09 10:48:05 HOST 11010040011508075469051l ipv4 Msgid=brute_attack UserName=100.1.1.59 UserGroup=anonymous SrcMAC=00:50:56:b8:c8:e7 DestMAC=00:50:56:b8:4a:76 SrcDeviceType= SrcOS= AttackTime= SrcIPAddr=100.1.1.59 SrcPort=4135 DstIPAddr=100.2.1.5 DstPort=14357 Protocol=TCP AppType=postgres BruteForceUserName= AttackName=postgres BruteForceResult= CriticalLevel=3
日志说明	
处理建议	无。

8.4 非法外联防护日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcMAC=[$4:MACADDR] DestMAC=[$5:MACADDR] SrcDeviceType=[$6:CHAR] SrcOS=[$7:CHAR] AttackTime=[$8:UINT64] SrcIPAddr=[$9:IPADDR] SrcPort=[$10:UINT16] DstIPAddr=[$11:IPADDR] DstPort=[$12:UINT16] Protocol=[$13:UCHAR] Application=[$14:CHAR] ReqPktCount=[$15:UINT8] ResPktCount=[$16:UINT8] ReqByteCount=[$17:UINT8] ResByteCount=[$18:UINT8] Result=[$19:UINT8]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：源MAC地址。 $5：目的MAC地址。 $6：终端类型。 $7：终端操作系统。 $8：发生时间。 $9：源IP地址。 $10：源端口号。 $11：目的IP地址。 $12：目的端口号。 $13：协议。 $14：应用名称。 $15：请求报文数。 $16：响应报文数。 $17：请求流量大小。 $18：响应流量大小。 $19：外联结果。
日志等级	1

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcMAC=[$4:MACADDR] DestMAC=[$5:MACADDR] SrcDeviceType=[$6:CHAR] SrcOS=[$7:CHAR] AttackTime=[$8:UINT64] SrcIPAddr=[$9:IPADDR] SrcPort=[$10:UINT16] DstIPAddr=[$11:IPADDR] DstPort=[$12:UINT16] Protocol=[$13:UCHAR] Application=[$14:CHAR] ReqPktCount=[$15:UINT8] ResPktCount=[$16:UINT8] ReqByteCount=[$17:UINT8] ResByteCount=[$18:UINT8] Result=[$19:UINT8]
举例	<1>4 2020-11-09 11:00:50 HOST 11010040011508075469051 1 ipv4 Msgid=outreach UserName=100.1.1.2 UserGroup=anonymous SrcMAC= DestMAC= SrcDeviceType= SrcOS= AttackTime= SrcIPAddr=100.1.1.2 SrcPort=62867 DstIPAddr=100.2.1.3 DstPort=80 Protocol=TCP Application= ReqPktCount= ResPktCount= ReqByteCount= ResByteCount= Result=
日志说明	
处理建议	无。

8.5 行为模型日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcMAC=[$4:MACADDR] DestMAC=[$5:MACADDR] SrcDeviceType=[$6:CHAR] SrcOS=[$7:CHAR] AttackTime=[$8:UINT64] SrcIPAddr=[$9:IPADDR] SrcPort=[$10:UINT16] DstIPAddr=[$11:IPADDR] DstPort=[$12:UINT16] Protocol=[$13:UCHAR] Application=[$14:CHAR] TunnelType=[$15:CHAR] CriticalLevel=[$16:UINT8] TunnelTime=[$17:UINT64]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：源MAC地址。 $5：目的MAC地址。 $6：终端类型。 $7：终端操作系统。 $8：发生时间。 $9：源IP地址。 $10：源端口号。 $11：目的IP地址。 $12：目的端口号。 $13：协议。 $14：应用名称。 $15：隧道类型。 $16：严重等级。 $17：隧道时间。
日志等级	0~6

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcMAC=[$4:MACADDR] DestMAC=[$5:MACADDR] SrcDeviceType=[$6:CHAR] SrcOS=[$7:CHAR] AttackTime=[$8:UINT64] SrcIPAddr=[$9:IPADDR] SrcPort=[$10:UINT16] DstIPAddr=[$11:IPADDR] DstPort=[$12:UINT16] Protocol=[$13:UCHAR] Application=[$14:CHAR] TunnelType=[$15:CHAR] CriticalLevel=[$16:UINT8] TunnelTime=[$17:UINT64]
举例	<4>4 2020-11-09 11:04:39 HOST 11010040011508075469051 1 ipv4 Msgid=secret_tunnel UserName=192.168.1.1 UserGroup=anonymous SrcMAC=38:22:d6:30:38:7f DestMAC=68:91:d0:d5:66:77 SrcDeviceType= SrcOS= AttackTime= SrcIPAddr=192.168.1.1 SrcPort=25839 DstIPAddr=114.114.114.114 DstPort=53 Protocol=UDP Application=DNS 隧道 TunnelType= CriticalLevel=2 TunnelTime=
日志说明	
处理建议	无。

8.6 Dos防护日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcMAC=[$4:MACADDR] DestMAC=[$5:MACADDR] SrcDeviceType=[$6:CHAR] SrcOS=[$7:CHAR] AttackTime=[$8:UINT64] SrcIPAddr=[$9:IPADDR] SrcPort=[$10:UINT16] DstIPAddr=[$11:IPADDR] DstPort=[$12:UINT16] Protocol=[$13:UCHAR] Application=[$14:CHAR] FloodType=[$15:CHAR] CriticalLevel=[$16:UINT16] AttackName=[$17:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：源MAC地址。 $5：目的MAC地址。 $6：终端类型。 $7：终端操作系统。 $8：攻击时间。 $9：源IP地址。 $10：源端口号。 $11：目的IP地址。 $12：目的端口号。 $13：协议。 $14：应用名称。 $15：拒绝服务类型。 $16：严重级别。 $17：攻击名称。
日志等级	4

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcMAC=[$4:MACADDR] DestMAC=[$5:MACADDR] SrcDeviceType=[$6:CHAR] SrcOS=[$7:CHAR] AttackTime=[$8:UINT64] SrcIPAddr=[$9:IPADDR] SrcPort=[$10:UINT16] DstIPAddr=[$11:IPADDR] DstPort=[$12:UINT16] Protocol=[$13:UCHAR] Application=[$14:CHAR] FloodType=[$15:CHAR] CriticalLevel=[$16:UINT16] AttackName=[$17:CHAR]
举例	<4>4 2020-11-09 11:09:01 HOST 11010040011508075469051 1 ipv4 Msgid=security_flood UserName= UserGroup= SrcMAC=00:50:56:b8:c8:e7 DestMAC= SrcDeviceType= SrcOS= AttackTime= SrcIPAddr=100.1.1.6 SrcPort=10000 DstIPAddr=100.2.1.11 DstPort=53 Protocol=UDP Application= FloodType=udpflood CriticalLevel=2 AttackName=flood-attack
日志说明	
处理建议	无。

8.7 恶意URL日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcMAC=[$4:MACADDR] DestMAC=[$5:MACADDR] SrcDeviceType=[$6:CHAR] SrcOS=[$7:CHAR] AttackTime=[$8:UINT64] SrcIPAddr=[$9:IPADDR] SrcPort=[$10:UINT16] DstIPAddr=[$11:IPADDR] DstPort=[$12:UINT16] AppType=[$13:CHAR] Application=[$14:CHAR] CriticalLevel=[$15:UINT16] URLType=[$16:CHAR] URL=[$17:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：源MAC地址。 $5：目的MAC地址。 $6：终端类型。 $7：终端操作系统。 $8：发生时间。 $9：源IP地址。 $10：源端口号。 $11：目的IP地址。 $12：目的端口号。 $13：协议类型。 $14：应用名称。 $15：严重级别。 $16：URL分类。 $17：URL。
日志等级	0

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcMAC=[$4:MACADDR] DestMAC=[$5:MACADDR] SrcDeviceType=[$6:CHAR] SrcOS=[$7:CHAR] AttackTime=[$8:UINT64] SrcIPAddr=[$9:IPADDR] SrcPort=[$10:UINT16] DstIPAddr=[$11:IPADDR] DstPort=[$12:UINT16] AppType=[$13:CHAR] Application=[$14:CHAR] CriticalLevel=[$15:UINT16] URLType=[$16:CHAR] URL=[$17:CHAR]
举例	<0>4 2020-11-09 11:39:22 HOST 11010040011508075469051l ipv4 Msgid=malicious_url UserName=10.10.1.2 UserGroup=anonymous SrcMAC=00:50:56:b8:73:5f DestMAC= SrcDeviceType=PC SrcOS=PC(Windows) AttackTime= SrcIPAddr=10.10.1.2 SrcPort=52344 DstIPAddr=112.80.248.75 DstPort=80 AppType=TCP Application= CriticalLevel=2 URLType= URL=http://www.baidu.com/
日志说明	
处理建议	无。

9 审计日志（探针）

9.1 DNS日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Domain=[$11:CHAR] ResponseContent=[$12:CHAR] Protocol=[$13:UINT16] ReqByteCount=[$14:UINT64] ResByteCount=[$15:UINT64] ReqPktCount=[$16:UINT64] ResPktCount=[$17:UINT64] ResponseCode=[$18:UINT4] RequestID=[$19:UINT16] ResponseID=[$20:UINT16] ReqType=[$21:UINT16] Direction=[$22:UINT16] ResFristAnswerTTL=[$23:UINT32]

参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：域名。 $12：返回内容。 $13：协议。 $14：请求流量。 $15：响应流量。 $16：请求报文数。 $17：响应报文数。 $18：应答的RCODE字段。 $19：请求标识。 $20：应答标识。 $21：请求报文查询问题中的类型。 $22：方向。 $23：应答报文中Answers域里的第一个记录的TTL。
日志等级	6
举例	<6>4 2020-11-10 09:23:03 HOST 11010040011508075469051l ipv4 Msgid=dns UserName=10.10.1.2 UserGroup=anonymous SrcDeviceType=未知类型 SrcOS=未知类型 SrcMAC=00:50:56:b8:73:5f SrcIPAddr=10.10.1.2 SrcPort=63562 DstIPAddr=8.8.8.8 DstPort=53 Domain=www.baidu.com ResponseContent=14.215.177.38 Protocol=UDP ReqByteCount= ResByteCount= ReqPktCount= ResPktCount= ResponseCode=0 RequestID=0x0 ResponseID=0x126c ReqType=0 Direction=1 ResFristAnswerTTL=365
日志说明	
处理建议	无。

9.2 FTP日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Account=[$12:CHAR] CMD=[$13:CHAR] FileName=[$14:CHAR] FileHashCode=[$15:UINT16]

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Account=[$12:CHAR] CMD=[$13:CHAR] FileName=[$14:CHAR] FileHashCode=[$15:UINT16]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议类型。 $12：帐号。 $13：命令。 $14：文件名。 $15：文件hash值。
日志等级	6
举例	<6>4 2020-11-06 10:46:06 HOST 11010040011508075469051l ipv4 Msgid=ftp UserName=10.10.1.2 UserGroup=anonymous SrcDeviceType=PC SrcOS=PC(Windows) SrcMAC=00:50:56:b8:73:5f SrcIPAddr=10.10.1.2 SrcPort=58710 DstIPAddr=192.168.0.253 DstPort=21 Protocol=TCP Account=anonymous CMD=get FileName=20191123add.wxfj FileHashCode=
日志说明	
处理建议	无。

9.3 TELNET日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Account=[$12:CHAR] CMD=[$13:CHAR]

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Account=[$12:CHAR] CMD=[$13:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议类型。 $12：帐号。 $13：命令。
日志等级	6
举例	<6>4 2020-11-06 10:53:49 HOST 11010040011508075469051l ipv4 Msgid=telnet UserName=10.10.1.2 UserGroup=anonymous SrcDeviceType=PC SrcOS=PC(Windows) SrcMAC=00:50:56:b8:73:5f SrcIPAddr=10.10.1.2 SrcPort=58736 DstIPAddr=192.168.203.129 DstPort=23 Protocol=TCP Account= CMD=
日志说明	
处理建议	无。

9.4 网站访问日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Domain=[$12:CHAR] URL=[$13:CHAR] WebCategory=[$14:CHAR] Method=[$15:CHAR] Title=[$16:CHAR]

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Domain=[$12:CHAR] URL=[$13:CHAR] WebCategory=[$14:CHAR] Method=[$15:CHAR] Title=[$16:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议。 $12：网址域名。 $13：用户访问的完整URL。 $14：网站分类名称。 $15：GET或POST。 $16：网页标题。
日志等级	6
举例	<6>4 2020-11-06 11:16:26 HOST 11010040011508075469051 1 ipv4 Msgid=website UserName=10.10.1.2 UserGroup=anonymous SrcDeviceType=PC SrcOS=PC(Windows) SrcMAC=00:50:56:b8:73:5f SrcIPAddr=10.10.1.2 SrcPort=58836 DstIPAddr=60.174.240.3 DstPort=443 Protocol=TCP Domain=www.jd.com URL=https://www.jd.com WebCategory=其它 Method=GET Title=京东商城
日志说明	
处理建议	无。

9.5 社区日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Application=[$12:CHAR] ApplicationGroup=[$13:CHAR] Account=[$14:CHAR] Action=[$15:CHAR] Subject=[$16:CHAR] Content=[$17:CHAR]

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Application=[$12:CHAR] ApplicationGroup=[$13:CHAR] Account=[$14:CHAR] Action=[$15:CHAR] Subject=[$16:CHAR] Content=[$17:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议。 $12：应用名称。 $13：应用分类名称。 $14：帐号。 $15：应用行为名称。 $16：主题。 $17：内容。
日志等级	6
举例	<6>4 2020-11-06 13:47:14 HOST 11010040011508075469051l ipv4 Msgid=social_bbs UserName=10.10.1.2 UserGroup=anonymous SrcDeviceType=PC SrcOS=PC(Windows) SrcMAC=00:50:56:b8:73:5f SrcIPAddr=10.10.1.2 SrcPort=59734 DstIPAddr=49.7.40.133 DstPort=443 Protocol=TCP Application=新浪微博_登录 ApplicationGroup=微博 Account=5175171222 Action=登录 Subject= Content=
日志说明	
处理建议	无。

9.6 邮件日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Application=[$12:CHAR] ApplicationGroup=[$13:CHAR] Account=[$14:CHAR] Action=[$15:CHAR] Sender=[$16:CHAR] Receiver=[$17:CHAR] Subject=[$18:CHAR] Content=[$19:CHAR] FileName=[$20:CHAR] FileSize=[$21:UINT32] FilesHashCode=[$22:UINT16] FileType=[$23:CHAR]

参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议。 $12：应用名称。 $13：应用分类名称。 $14：帐号。 $15：应用行为名称。 $16：发送地址。 $17：接收地址。 $18：主题 $19：邮件内容。 $20：文件名。 $21：文件大小。 $22：文件hash值。 $23：文件类型。
日志等级	6
举例	<6>4 2020-11-14 11:22:48 HOST 11010040011508075469051 1 ipv4 Msgid=mail UserName=100.1.1.6 UserGroup=anonymous SrcDeviceType=未知类型 SrcOS=未知类型 SrcMAC=00:50:56:b8:c8:e7 SrcIPAddr=100.1.1.6 SrcPort=54441 DstIPAddr=100.2.1.3 DstPort=110 Protocol=TCP Application=POP3邮件协议 ApplicationGroup=电子邮件 Account=azYWNolVBxhjNu Action=收邮件 Sender=Ie8UXzGzUKkWWiNvrdjM@KkGPNWROfxtsPEmuGsfgs.edu Receiver=MZBCMk6JHXdQ3vzgTWM1gQD5XQzop@IwUNZf.gov Subject=no3TJtRUyMJY Content= FileName=pOGD.PdF FileSize= FilesHashCode= FileType=
日志说明	
处理建议	无。

9.7 搜索引擎日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Application=[$12:CHAR] ApplicationGroup=[$13:CHAR] Account=[$14:CHAR] Action=[$15:CHAR] Content=[$16:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议。 $12：应用名称。 $13：应用分类名称。 $14：帐号。 $15：应用行为名称。 $16：内容。
日志等级	6
举例	<6>4 2020-11-06 14:08:43 HOST 11010040011508075469051l ipv4 Msgid=search_engine UserName=10.10.1.2 UserGroup=anonymous SrcDeviceType=PC SrcOS=PC(Windows) SrcMAC=00:50:56:b8:73:5f SrcIPAddr=10.10.1.2 SrcPort=60104 DstIPAddr=14.215.177.38 DstPort=443 Protocol=TCP Application=百度 ApplicationGroup=搜索引擎 Account= Action=搜索 Content=mei
日志说明	
处理建议	无。

9.8 文件传输日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Application=[$12:CHAR] ApplicationGroup=[$13:CHAR] Account=[$14:CHAR] Action=[$15:CHAR] FileName=[$16:CHAR] FileSize=[$17:UINT32] FileHash=[$18:CHAR] FileType=[$19:CHAR]

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Application=[$12:CHAR] ApplicationGroup=[$13:CHAR] Account=[$14:CHAR] Action=[$15:CHAR] FileName=[$16:CHAR] FileSize=[$17:UINT32] FileHash=[$18:CHAR] FileType=[$19:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议。 $12：应用名称。 $13：应用分类名称。 $14：帐号。 $15：应用行为名称。 $16：文件名。 $17：文件大小。 $18：文件hash值。 $19：文件类型。
日志等级	6
举例	<6>4 2020-11-06 14:13:04 HOST 11010040011508075469051l ipv4 Msgid=file UserName=10.10.1.2 UserGroup=anonymous SrcDeviceType=PC SrcOS=PC(Windows) SrcMAC=00:50:56:b8:73:5f SrcIPAddr=10.10.1.2 SrcPort=60163 DstIPAddr=14.18.245.237 DstPort=443 Protocol=TCP Application=QQ邮箱_上传 ApplicationGroup=电子邮件 Account=990419869 Action=上传 FileName=20201106/1413020009-ldap日志.pcap FileSize= FileHash= FileType=
日志说明	
处理建议	无。

9.9 娱乐/股票日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Application=[$12:CHAR] ApplicationGroup=[$13:CHAR] Account=[$14:CHAR] Action=[$15:CHAR]

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Application=[$12:CHAR] ApplicationGroup=[$13:CHAR] Account=[$14:CHAR] Action=[$15:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议。 $12：应用名称。 $13：应用分类名称。 $14：帐号。 $15：应用行为名称。
日志等级	6
举例	<6>4 2020-11-06 17:52:15 HOST 11010040011508075469051l ipv4 Msgid=releax_stock UserName=192.168.1.85 UserGroup=anonymous SrcDeviceType=未知类型 SrcOS=未知类型 SrcMAC=28:d2:44:3d:42:af SrcIPAddr=192.168.1.85 SrcPort=57691 DstIPAddr=43.250.14.39 DstPort=80 Protocol=TCP Application=优酷_土豆视频_登录 ApplicationGroup=P2P流媒体 Account=1003057311 Action=登录
日志说明	
处理建议	无。

9.10 IM日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Application=[$12:CHAR] ApplicationGroup=[$13:CHAR] Account=[$14:CHAR] Action=[$15:CHAR] Content=[$16:CHAR]

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Application=[$12:CHAR] ApplicationGroup=[$13:CHAR] Account=[$14:CHAR] Action=[$15:CHAR] Content=[$16:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议。 $12：应用名称。 $13：应用分组名称。 $14：帐号。 $15：应用行为名称。 $16：聊天内容。
日志等级	6
举例	<6>4 2020-11-06 17:43:48 HOST 11010040011508075469051 1 ipv4 Msgid=im UserName=192.168.207.2 UserGroup=anonymous SrcDeviceType=未知类型 SrcOS=未知类型 SrcMAC=38:22:d6:30:38:7f SrcIPAddr=192.168.207.2 SrcPort=37252 DstIPAddr=114.221.144.160 DstPort=80 Protocol=TCP Application=QQ(移动端)_登录_收发消息 ApplicationGroup=即时通讯 Account=615275810 Action=登录_收发消息 Content=
日志说明	
处理建议	无。

9.11 LDAP日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Account=[$12:CHAR] Action=[$13:CHAR] Result=[$14:CHAR]

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Account=[$12:CHAR] Action=[$13:CHAR] Result=[$14:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议类型。 $12：登录名。 $13：动作。 $14：结果。
日志等级	6
举例	<6>4 2020-11-06 15:00:07 HOST 11010040011508075469051l ipv4 Msgid=ldap UserName=10.10.1.2 UserGroup=anonymous SrcDeviceType=PC SrcOS=PC(Windows) SrcMAC=00:50:56:b8:73:5f SrcIPAddr=10.10.1.2 SrcPort=60763 DstIPAddr=192.168.203.189 DstPort=389 Protocol=TCP Account= Action=操作 Result=
日志说明	
处理建议	无。

9.12 SSL证书日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:CHAR] Application=[$12:CHAR] CertSubject=[$13:CHAR] CertExpireDate=[$14:CHAR] CertInst=[$15:CHAR] CertPKI=[$16:CHAR] CertVersion=[$17:CHAR] CertID=[$18:CHAR] CertSignID=[$19:CHAR] CertLength=[$20:UINT32] ClientSHLength=[$21:UINT32] ClientSHVersion=[$22:CHAR] ClientSessionID=[$23:CHAR]

	ClientSHSuitCount=[$24:UINT32] ClientSHSuit=[$25:CHAR] ClientSHExtCount=[$26:UINT32] ClientSHExtLength=[$27:UINT32] ServerName=[$28:CHAR] ServerSHLength=[$29:UINT32] ServerSHVersion=[$30:CHAR] ServerSelectedSuit=[$31:CHAR] ServerSHExtCount=[$32:UINT32] ServerSHExtLength=[$33:UINT32] CertVerify=[$34:] CertChain=[$35:] SNI=[$36:]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议。 $12：应用名称。 $13：证书主题。 $14：证书有效期。 $15：证书颁发机构。 $16：证书公钥。 $17：证书版本号。 $18：证书唯一编号。 $19：证书签名算法标识。 $20：证书长度。 $21：Client握手长度。 $22：Client握手通信版本。 $23：Client会话ID。 $24：Client握手加密套件数量。 $25：Client握手加密套件。 $26：Client握手扩展数量。 $27：Client握手扩展长度。 $28：Server名称。 $29：Server握手长度。 $30：Server握手通信版本。 $31：Server选择握手加密套件。 $32：Server握手扩展数量。 $33：Server握手扩展长度。 $34：证书校验。 $35：证书链。 $36：SNI。
日志等级	6

举例	<6>4 2020-11-10 09:45:04 HOST 11010040011508075469051 1 ipv4 Msgid=ssl UserName=10.10.1.2 UserGroup=anonymous SrcDeviceType=未知类型 SrcOS=未知类型 SrcMAC=00:50:56:b8:73:5f SrcIPAddr=10.10.1.2 SrcPort=51031 DstIPAddr=192.168.203.129 DstPort=443 Protocol=TCP Application=安全传输层协议(TLS) CertSubject= CertExpireDate= CertInst= CertPKI= CertVersion= CertID= CertSignID= CertLength=0 ClientSHLength=508 ClientSHVersion=TLS 1.2 ClientSessionID=5f7df99831c432c14b72cdb30fcb8534deb876dfc686f18a96c440038bd3b2e7 ClientSHSuitCount=16 ClientSHSuit=5a5a130113021303c02bc02fc02cc030cca9cca8c013c014009c009d002f0035 ClientSHExtCount=16 ClientSHExtLength=403 ServerName= ServerSHLength=0 ServerSHVersion=TLS 1.2 ServerSelectedSuit=0 ServerSHExtCount=0 ServerSHExtLength=0 CertVerify= CertChain= SNI=
日志说明	
处理建议	无。

9.13 加密流量日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] BeginTime=[$12:CHAR] EndTime=[$13:CHAR] SrcPacketsMax=[$14:CHAR] SrcPacketsMin=[$15:CHAR] SrcTimesMax=[$16:CHAR] RrcTimesMin=[$17:CHAR] DstPacketsMax=[$18:CHAR] DstPacketsMin=[$19:CHAR] DstTimesMax=[$20:CHAR] DstTimesMin=[$21:UINT32] ReqByteCount=[$22:UINT32] ResByteCount=[$23:UINT32] ReqPktCount=[$24:UINT32] ResPktCount=[$25:UINT32] BD=[$26:CHAR] PacketState=[$27:UINT32] TimeState=[$28:UINT32] CipherSuites=[$29:UINT32] Selected=[$30:CHAR] ClientExtension=[$31:CHAR] ServerExtension=[$32:UINT32] ClientKeyExchangeLength=[$33:UINT32] ServerKeyExchangeLength=[$34:] CertDuration=[$35:] SelfSigned=[$36:] SAN=[$37:] CertNumsLength=[$38:] IsCA=[$39:]

参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议。 $12：开始时间。 $13：结束时间。 $14：TCP连接过程中发送的所有包的最大负载长度。 $15：TCP连接过程中发送的所有包的最小负载长度。 $16：TCP连接过程中发送的所有有负载的包的间隔时间(毫秒)的最大值。 $17：TCP连接过程中发送的所有有负载的包的间隔时间(毫秒)的最小值。 $18：TCP连接过程中接收的所有包的最大负载长度。 $19：TCP连接过程中接收的所有包的最小负载长度。 $20：TCP连接过程中接收的所有有负载的包的间隔时间(毫秒)的最大值。 $21：TCP连接过程中接收的所有有负载的包的间隔时间(毫秒)的最小值。 $22：请求流量。 $23：响应流量。 $24：请求报文数。 $25：响应报文数。 $26：TCP负载中的字节分布情况（0-255出现的次数列表） $27：TCP连接过程中有负载的前20个包的包长转移概率矩阵 $28：TCP连接过程中有负载的前20个包的间隔时间转移概率矩阵 $29：TLS客户端支持加密套件列表 $30：TLS服务器端选择的加密套件 $31：TLS客户端支持的extension列表 $32：TLS服务器端选择的extension列表 $33：TLS握手过程中ClientKeyExchange消息的负载长度 $34：TLS握手过程中ServerKeyExchange消息的负载长度 $35：服务器证书的有效期(单位天) $36：服务器证书是否为自签名证书 $37：服务器证书中的SAN数量 $38：服务器证书链长度 $39：是否是CA证书
日志等级	6

举例	<6>4 2020-11-10 16:41:35 HOST 11010040011508075469051 1 ipv4 Msgid=encrypted_traffic UserName=100.2.1.10 UserGroup=anonymous SrcDeviceType= SrcOS= SrcMAC= SrcIPAddr=100.2.1.10 SrcPort=47873 DstIPAddr=100.1.1.32 DstPort=4135 Protocol=TCP BeginTime=1604997673 EndTime=1604997694 SrcPacketsMax= SrcPacketsMin= SrcTimesMax= RrcTimesMin= DstPacketsMax= DstPacketsMin= DstTimesMax= DstTimesMin= ReqByteCount=1380 ResByteCount=1026 ReqPktCount=3 ResPktCount=4 BD= PacketState= TimeState= CipherSuites= Selected= ClientExtension= ServerExtension= ClientKeyExchangeLength= ServerKeyExchangeLength= CertDuration= SelfSigned= SAN= CertNumsLength= IsCA=
日志说明	
处理建议	无。

9.14 登录日志

日志内容	Msgid=[$1:CHAR] UserName=[$2:CHAR] UserGroup=[$3:CHAR] SrcDeviceType=[$4:CHAR] SrcOS=[$5:CHAR] SrcMAC=[$6:MACADDR] SrcIPAddr=[$7:IPADDR] SrcPort=[$8:UINT16] DstIPAddr=[$9:IPADDR] DstPort=[$10:UINT16] Protocol=[$11:UCHAR] Application=[$12:CHAR] Account=[$13:CHAR] Action=[$14:CHAR] Result=[$15:CHAR]
参数解释	$1：日志类型。 $2：用户名称。 $3：用户组名称。 $4：终端类型。 $5：终端系统。 $6：源MAC地址。 $7：源IP地址。 $8：源端口号。 $9：目的IP地址。 $10：目的端口号。 $11：协议类型。 $12：应用。 $13：登录名。 $14：动作。 $15：结果。
日志等级	6
举例	<6>4 2020-11-06 17:23:37 HOST 11010040011508075469051 1 ipv4 Msgid=login UserName=10.10.1.2 UserGroup=anonymous SrcDeviceType=PC SrcOS=PC(Windows) SrcMAC=00:50:56:b8:73:5f SrcIPAddr=10.10.1.2 SrcPort=61304 DstIPAddr=192.168.210.32 DstPort=139 Protocol=TCP Application=NETBIOS会话服务 Account= Action=Logon Result=
日志说明	
处理建议	无。

10 会话日志（探针）

10.1 会话日志

日志内容	Msgid=[$1:CHAR] SrcMAC=[$2:MACADDR] DstMAC=[$3:MACADDR] UserName=[$4:CHAR] UserGroup=[$5:CHAR] SrcIPAddr=[$6:IPADDR] SrcPort=[$7:UINT16] DstIPAddr=[$8:IPADDR] DstPort=[$9:UINT16] Protocol=[$10:UCHAR] Application=[$11:CHAR] ApplicationGroup=[$12:CHAR] ReqByteCount=[$13:UINT64] ResByteCount=[$14:UINT64] ReqPktCount=[$15:UINT64] ResPktCount=[$16:UINT64] ReqPayloadByteCount=[$17:UINT64] ResPayloadByteCount=[$18:UINT64] ReqPayloadPktCount=[$19:UINT64] ResPayloadPktCount=[$20:UINT64] BeginTime=[$21:UINT64] EndTime=[$22:UINT64] Status=[$23:UINT8] SrcDeviceType=[$24:CHAR] SrcOS=[$25:CHAR] BrowserType=[$26:CHAR]
参数解释	$1：日志类型。 $2：源MAC地址。 $3：目的MAC地址。 $4：用户名称。 $5：用户组名称。 $6：源IP地址。 $7：源端口号。 $8：目的IP地址。 $9：目的端口号。 $10：协议类型。 $11：应用。 $12：应用组。 $13：上行字节数。 $14：下行字节数。 $15：上行数据包数。 $16：下行数据包数。 $17：上行字节数（有效载荷）。 $18：下行字节数（有效载荷）。 $19：上行数据包数（有效载荷）。 $20：下行数据包数（有效载荷）。 $21：会话开始时间。 $22：会话结束时间。 $23：会话状态。 $24：终端类型。 $25：终端操作系统。 $26：浏览器类型。
日志等级	6

举例	<6>4 2020-11-09 14:19:24 HOST 11010040011508075469051 1 ipv4 Msgid=flow_session SrcMAC= DstMAC= UserName=10.10.1.2 UserGroup=anonymous SrcIPAddr=10.10.1.2 SrcPort=32461 DstIPAddr=119.100.50.31 DstPort=20480 Protocol=TCP Application=百度 ApplicationGroup=搜索引擎 ReqByteCount=1856 ResByteCount=11947 ReqPktCount=15 ResPktCount=13 ReqPayloadByteCount= ResPayloadByteCount= ReqPayloadPktCount= ResPayloadPktCount= BeginTime=1604902721 EndTime=1604902762 Status=2 SrcDeviceType= SrcOS= BrowserType=Chrome Browser
日志说明	
处理建议	无。