# 思华快线网关应用日志格式定义

**v1.0**

jqhuang@fortinet.com

2014-7-10

目录

# 1．概述

快线网关日志格式针对不同的模块具有不同的格式定义，本文档用于描述快线网关输出的应用日志的格式。日志格式定义以满足用户需求为目标，依据《快线网关功能说明书-V1.0》中的 3.2 节输出日志中的需求描述为基础，定义本文内容。

在 3.2 节中，定义了快线网关两种日志类型：运行日志和应用日志，其中应用日志格式具有明确的规定，本文即以此定义应用日志的格式。在开发内部我们习惯将此类型日志称之为流量日志（Traffic log），所以在本文中可能交叉使用两种说法，但概念相同。

# 2．syslog 格式定义

应用日志输出方式采用标准 syslog 格式，syslog 格式如下：

| <PRI> *data time* [*hostname*] *message* |
|---|

其中 PRI 遵循标准 syslog 定义方式，计算方法为：

| Facility levels * 8 + Severity levels |
|---|

这里应用日志的 Facility levels 为 0（kernel messages），Severity levels 为 6（Informational），所以应用日志的 PRI 为 6。

data time 使用 syslog 标准格式如下（24 小时计时格式）：

| date=YYYY-MM-DD time=HH:MM:SS |
|---|

hostname 部分使用盒子的 hostname，根据用户配置不同而不同。

message 部分为日志内容，此部分为三部分，第一部分为盒子的 SN 号码，第二部分为 message_content 类型，第三部分为真正的日志内容。格式如下：

| device_id=XXX… message_type message_content |
|---|

其中 messgae_type 分为三种：

http-proxy

vpn

nat-route

综上，总体的格式如下：

| <6> date=YYYY-MM-DD time=HH:MM:SS [hostname] device_id=XXXXXXX message_type message_content |
|---|

举例：

| <6> date=2014-07-10 time=13:33:56 [LinEx-beijing1] device_id=093833EF6CB1332 http-proxy 1.1.1.1 2.2.2.2 80 GET www.163.com /index.html 200 2033 68 web-netease 5.5.5.5 10 |
|---|

message_content 的格式根据不同业务分为三种，HTTP 业务，VPN 业务和直接路由转发业务。下面根据不同业务进行分别说明。

# 3．HTTP 日志内容格式

HTTP 格式日志用户要求符合 W3C 日志格式要求，W3C 日志格式为可扩展自定义格式，这里我们在第一阶段暂时不能提供可以配置的日志格式，本节暂定一种固定格式。

基本定义参考 W3C 标准和用户需求，我们给出如下格式定义：

*c-ip s-ip s-port cs-method cs-host cs-uri-stem sc-status sc-bytes cs-bytes app-id nexthop-ip nexthop-delay*

下表针对字段进行了说明：

| 字段 | 说明 |
|---|---|
| c-ip | W3C 标准字段，client 的 ip |
| s-ip | W3C 标准字段，server 的 ip（需确认这里是 proxy 的服务地址还是 SP 地址？） |
| s-port | W3C 标准字段，server 的 port（需确认同上） |
| cs-method | W3C 标准字段，请求方法 |
| cs-host | W3C 标准字段，请求 host 字段值 |
| cs-uri-stem | W3C 标准字段，请求 uri，不包含参数部分 |
| sc-status | W3C 标准字段，服务返回码（如 200、404 等） |
| sc-bytes | W3C 标准字段，返回内容字节数 |
| cs-bytes | W3C 标准字段，请求字节数 |
| app-id | 非 W3C 标准字段，识别应用业务标识 |
| nexthop-ip | 非 W3C 标准字段，下一跳 IP（这里基本上为下一快线网关或者 SP 服务器） |
| nexthop-delay | 非 W3C 标准字段，下一跳延迟 |

举例：

<6> date=2014-07-10 time=13:33:56 [LinEx-beijing1] device_id=093833EF6CB1332 http-proxy 1.1.1.1 2.2.2.2 80 GET www.163.com /index.html 200 2033 68 web-netease 5.5.5.5 10

# 4．VPN 日志内容格式

要求针对 VPN 的业务，要记录用户的登录 ID，用户 VPN 网络标识，客户端的 IP 地址，客户端的分配的 VPN 内网 IP 地址，用户连接时长，总的传输数据，峰值流量，记录到应用路径的下一个节点等。

第一阶段只实现一个 IPsec VPN，所以无法做到到 AAA 认证，只能做本地认证。

需要看对端 VPN 产品的支持情况，以 IP/domain name/ email 等来做用户 ID

格式定义如下：

*event user-id vpn-id client-ip remote-ip life-time last-time total-byte max-rate*

| 字段 | 说明 |
|---|---|

| | |
|---|---|
| event | ESTABLISH,DELETE,EXPIRE,REKEY |
| type | VPN 类型 IPsec/pptp/l2tp 等 |
| user-id | 用户 ID |
| vpn-id | VPN ID |
| client-ip | Client IP |
| remote-ip | 分配给移动接入用户的内网地址 |
| life-time | SA 生命周期，可以为时间或传输字节数 |
| last-time | 连接时长 |
| total-byte | 传输字节数 |
| max-rate | 峰值流量 |

下一跳 LinEx 地址 VPN 模块无法得到，应该放到应用路由出输出。

举例：

```
<6> date=2014-07-10 time=13:33:56 [LinEx-beijing1] device_id=093833EF6CB1332 vpn
ESTABLISH IPsec root sihua-1 2.2.2.2 4.4.4.4 3600 59 1774333 13043
```

# 5．NAT 路由日志内容格式

路由转发业务格式如下：

```
protocol orig_sip orig_dip orig_sport orig_dport reply_sip reply_dip reply_sport reply_dport
inbytes outbytes appname sgateway dgateway
```

字段说明：

| 字段 | 说明 |
|---|---|
| protocol | 四层协议（TCP、UDP） |
| orig_sip | 源 IP(original direction) |
| orig_sport | 源端口(original direction) |
| orig_dip | 目的 IP(original direction) |
| orig_dport | 目的端口(original direction) |
| reply_sip | 源 IP(reply direction) |
| reply_sport | 源端口(reply direction) |
| reply_dip | 目的 IP(reply direction) |
| reply_dport | 目的端口(reply direction) |
| inbytes | 进栈字节数(original direction) |
| outbytes | 出栈字节数(reply direction) |
| appname | 识别应用业务标识 |
| sgateway | 源快线网关 |
| dgateway | 目标快线网关 |

举例：

<6> date=2014-07-10 time=13:33:56 [LinEx-beijing1] device_id=093833EF6CB1332 type=nat-route protocol=TCP orig_sip=1.1.1.1 orig_dip=2.2.2.2 orig_sport=2334 orig_dport=80 reply_sip=4.4.4.4 reply_dip=1.1.1.1 reply_sport=2334 reply_dport=80 inbytes=2003 outbytes=100 appname=web-taobao sgateway=LinExA dgateway=LinExB