# 思华快线网关应用日志格式定义

## v1.1

[jqhuang@fortinet.com](mailto:jqhuang@fortinet.com)

2014-7-14

目录

[思华快线网关应用日志格式定义 1](#_Toc392774117)

[v1.0 1](#_Toc392774118)

[1．概述 3](#_Toc392774119)

[2．syslog格式定义 3](#_Toc392774120)

[3．HTTP日志内容格式 4](#_Toc392774121)

[4．VPN日志内容格式 4](#_Toc392774122)

[5．NAT路由日志内容格式 4](#_Toc392774123)

## 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。

日志格式在第一阶段为固定格式，为基本syslog格式，字段不可配置。可以通过tcp，udp协议进行发送，用户可配置。

## 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）：

YYYY-MM-DD HH:MM:SS UTC +0800

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：

SN 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> YYYY-MM-DD HH:MM:SS UTC +0800 [hostname] SN message\_type message\_content

举例：

<6> 2014-07-10 13:33:56 UTC +0800 [LinEx-beijing1] 093833EF6CB1332 http-proxy 1.1.1.1 2.2.2.2 80 GET [www.163.com](http://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。

**这里需要说明的是，内容部分的格式通过空格进行区分间隔，如果内容字段中包含空格，则需要使用双引号（”）进行范围标注。如果在内容字段中出现双引号，则需要使用\进行转义，如果内容中出现\，则需要使用连续的两个\\进行转义。如下：**

字段1：My name is “Ming”

字段2：218.1.34.0\24

则内容体为：

“My name is \”Ming\”” 218.1.34.0\\24

## 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 c-useragent c-refer app-id nexthop-ip nexthop-delay trans-time*

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，proxy绑定的ip |
| s-port | W3C标准字段，proxy绑定的port |
| 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 |
| c-useragent | 非W3C标准字段，请求的头部的User-Agent字段 |
| c-refer | 非W3C标准字段，请求的头部的refer字段 |
| 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，第一阶段暂不支持 |
| trans-time | 非W3C标准字段，请求传输完成时间，第一阶段暂不支持 |

举例：

<6> 2014-07-10 13:33:56 UTC +0800 [LinEx-beijing1] 093833EF6CB1332 http-proxy 1.1.1.1 2.2.2.2 80 GET [www.163.com](http://www.163.com) /index.html 200 2033 68 “IE 8.0” <http://www.sina.com> web-netease 5.5.5.5 10 50

## 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 inbytes outbytes*

|  |  |
| --- | --- |
| 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 |
| inbytes | 进入VPN隧道字节数 |
| outbytes | 出VPN隧道字节数 |

由于VPN流量日志的需求，流量日志的发送时间间隔应该可以用户配置。

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> 2014-07-10 13:33:56 UTC +0800 [LinEx-beijing1] 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> 2014-07-10 13:33:56 UTC +0800 [LinEx-beijing1] 093833EF6CB1332 nat-route TCP 1.1.1.1 2.2.2.2 2334 80 4.4.4.4 1.1.1.1 2334 80 2003 100 web-taobao LinExA LinExB