# 思华快线网关L7 proxy CLI参考

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

2014/09/11

Ver 1.0

|  |  |  |
| --- | --- | --- |
| 版本 | 描述 | 作者 |
| 0.9 | 初始版本 | jqhuang |
| 1.0 | 增加了log部分的system log配置，增加L7 approute单跳模式说明。 | jqhuang |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 概述

本文描述思华快线网关服务器L7 proxy功能相关的配置CLI描述。

L7 proxy功能提供了一个具有流量应用识别功能的方向代理服务器。用户流量接入后，网关对其进行应用内容识别，区分用户目的地并转发至不同链路。从而实现区分应用流量的网络加速功能。

现阶段，L7 proxy功能仅支持两种应用（HTTP和HTTPS），本功能针对HTTP流量的HOST字段和URI字段加以识别和区分，根据应用路由定义路径，将流量导入到不同链路中，达到加速功能。

## 功能关系

在快线网关系统中，L7 proxy以一个多项配置形式存在（可理解为表）。即一个快线网关可配置多个L7 proxy服务。一个服务需要指定服务开启服务的interface、IP、端口以及类型等参数。服务与服务之间的IP端口对不能重复。

L7 proxy依据快线网关的app route表进行应用的识别和路由，系统的app route 为多项配置形式，每项中需要指定识别应用特征、下一跳地址、服务器地址和端口等信息。关于app route的选项，请参考app route的CLI详细说明。

在app route中，应用识别特征和下一跳网关两个对象需要引用其他对象，其中应用识别特征（application-signature）给出了应用识别的依据，可以配置为域名或URI。而下一跳网关则为转发路由的下一跳信息，主要为IP地址，通常为下一个快线网关。这两个配置都以多项配置形式存在，在配置app route之前需要先配置好。

另外，如果打算使用https类型的L7 proxy，需要预先导入需要使用的证书和私钥配置，证书和私钥的批量时使用压缩包打包，使用CLI接口导入。导入到系统中后以本地证书形式存在，配置L7 proxy服务时可以需要引用相关证书。

## CLI

Fortinet CLI风格：

1. 多view层层递进风格，一个配置/配置条目在一个view中完成。
2. 每个view中配置完成后end进行提交，提交后才生效，使用abort放弃提交。
3. 多项配置形式，使用edit <条目标识>新增编辑配置表项条目，使用delete删除现有配置条目。
4. 独立的配置均可使用show/get进行查看，查看方法使用show/get + 配置节点即可。
5. 少数命令使用单条命令式形式，立刻生效，比如exec boot等。

## L7 proxy

L7 proxy为多项配置形式，可以配置多个，系统中以名称做区分，配置节点 config l7-proxy proxy，使用edit/delete <proxy-name>进行添加修改等操作。

语法：

**config l7-proxy proxy**

**edit <proxy-name>**

**set cert-list <SSL Certificates for proxy>**

**set default-cert <Default SSL Certificate>**

**set \*interface <interface name>**

**set \*listen-ip <proxy listen ip>**

**set listen-port <proxy listen port>**

**set status <proxy status>**

**set type <proxy type>**

说明：

|  |  |
| --- | --- |
| 表项 | 说明 |
| cert-list | https proxy使用的证书列表，当type为https时可见且必须配置，默认值为空。配置引用系统内本地证书。 |
| default-cert | https proxy 使用默认证书列表，为不支持SNI的客户端提供默认证书，当type为https时可见，非必须配置，默认值为空。配置引用系统内本地证书。 |
| interface | 开启proxy服务的接口，必须配置，默认为空。配置引用系统内接口。 |
| listen-ip | 开启proxy的服务IP，必须配置，默认为空。配置检测ipv4地址格式有效性。 |
| listen-port | 开启proxy的服务端口，非必须配置，默认为80。配置检测范围，整数1-65535。 |
| status | proxy服务状态，选项配置，选项为enable/disable，默认为enable。用以开启停止proxy服务。 |
| type | proxy类型，选项配置，选项为http/https，默认为http。 |

## L7 proxy 使用 application route

关于application signature请参考相关说明部分，这里描述下l7 proxy与其引用关系。

系统中，L7 proxy只使用类型为L7的app route表项，且只有以下表项对L7 proxy有效：

|  |  |
| --- | --- |
| 表项 | 说明 |
| application\_signature | 路由识别应用特征，选项配置，引用系统中应用路由特征（application route signature） |
| forward-server | 服务器感知IP方式，此选项对L4/L7类型路由都生效。选项配置，选项为snat/clientip，snat时快速网关将流量进行snat，服务器SP不能感知client的IP。clientip时则使用clientip进行转发，服务器SP能够感知IP但是，此时需要SP服务器需要配置特殊路由，用以将回复包转发至快线网关。 |
| nexthop-gateway | 下一跳快线网关，此选项对L4/L7类型路由都生效。选项配置，引用引用路由网关配置（application route gateway）。注意：下一跳网关一般不配置为默认本地快线GW\_SELF。如果设置为本地转发，那么此时快线为单跳模式，单跳模式将导致L7 proxy不理会forward-server配置，而恒采用快线自己的出口IP作为源IP。因为转发后的源IP必须为快线自己的出口IP才能使SP回复数据包正常返回。 |
| server-address | 目的服务器SP的IP，当类型为L7时必须配置，默认为空，配置检测ip有效性。 |
| server-port | 目的服务器SP的端口，当类型为L7时有效，默认为80，配置检测范围，整数1-65535 |
| server-type | 目的服务器SP的类型，选项配置，可选项http/https，当类型为L7时有效，默认为http。 |
| type | application route类型，选项配置，可选项为L4/L7/VPN，L7proxy只使用类型为L7的应用路由条目。 |

## L7 proxy 使用 application signature

app route中需要配置application signature，L7 proxy根据此配置进行应用的识别。配置为多项配置形式，配置可被application route引用，可使用edit/delete进行添加删除。配置节点config application-route signature。

语法：

**config application-route signature**

**edit <application signature id>**

**set type <signature type>**

**set sig <signature content>**

说明：

|  |  |
| --- | --- |
| 表项 | 说明 |
| type | 特征类型，选项配置，可选项HOSTNAME/URI，默认选项HOSTNAME |
| sig | 特征内容，特征匹配内容，字符串类型，必须配置，长度1-1024。 |

## L7 proxy 使用 local certificate

L7 proxy的类型为https时，需要引用系统的本地证书配置，local certificate为多项配置形式，配置节点config system certificate local，可使用edit/delete进行添加删除。

语法：

**config system certificate local**

**edit <certificate name>**

**set certificate <certificate string>**

**set comments <certificate comments>**

**set csr <certificate signing request>**

**set password <certificate password>**

**set private-key <certificate private key string>**

说明：

|  |  |
| --- | --- |
| 表项 | 说明 |
| certificate | 证书字符串，必须配置 |
| comments | 注释，字符串类型，非必须配置 |
| csr | 证书对应的证书求字符串，非必须配置 |
| password | 私钥密码，如果有则必须配置 |
| private-key | 私钥字符串，必须配置 |

以上配置在CLI端只能查看，由于CLI端不能输入回车和特殊字符，过长的证书和私钥字符串无法在CLI端输入，需要在GUI端进行配置，或者使用CLI端的导入命令进行导入。

## local certificate batch import

系统本地证书的批量导入功能使用立即生效的exec命令方式，导入压缩包后在系统中生成相应的local certificate。有关压缩包和格式请参考文档《思华快线网关证书导入格式》。

语法：

exec certificate local batch-import tftp <zip file name> <tftp server ip>

使用后将立刻从指定ip下载指定压缩包文件，并将其导入系统中。

## 快线log

linex log针对三种不同的业务提供log，现阶段仅提供syslog形式，协议类型仅限于udp。快线log配置为单配置形式，系统中配置全局生效，配置节点config log setting linex

语法：

**config log setting linex**

**set http-log <http log status>**

**set nat-log <nat log status>**

**set protocol <syslog transfer protocol>**

**set server-ip <syslog server ip address>**

**set server-port <syslog server port>**

**set vpn-log <vpn log status>**

**set system-log <system log status>**

**set system-log-port <syslog server port for system log>**

**set system-log-protocol <syslog transfer protocol for system log>**

**set system-log-server-ip <syslog server ip address for system log>**

说明：

|  |  |
| --- | --- |
| 表项 | 说明 |
| http-log | http log开关，选项配置，可选项enable/disable |
| nat-log | nat log开关，选项配置，可选项enable/disable |
| vpn-log | vpn log开关，选项配置，可选项enable/disable |
| protocol | syslog协议，选项配置，可选项tcp/udp，现阶段tcp暂不支持 |
| server-ip | syslog服务器ip |
| server-port | syslog服务器端口 |
| system-log | 系统syslog日志开关，选项配置，可选项enable/disable |
| system-log-server-ip | 系统syslog日志服务器ip |
| system-log-port | 系统syslog日志服务器端口 |
| system-log-protocol | 系统syslog日志协议，选项配置，可选项tcp/udp，现阶段tcp暂不支持 |