**快线网关功能部分测试**

# 应用路由CLI说明

应用路由相关CLI包括2个部分: gateway 和route：

## Gateway

Gateway用来定义快线内部数据网络中其他快线网关。

CLI如下：

|  |
| --- |
| **# config application-route gateway**  **# edit** *<name>*  **# set description** *<desc>*  **# set address** *<ip>*  **# exit** |

注意：

1. 快线网关有一个预定义为GW\_SELF的 gateway，表示本快线网关；
2. 在快线内部网络中，每个网关都需要定义其他跟本网关有数据往来的gateway；
3. 目前只支持IPv4的address；

## Route

Route用来定义快线内部数据应用路由，包括L4, L7和VPN三种类型，将匹配的流量路由到指定快线网关上。

CLI如下：

|  |
| --- |
| **# config application-route route**  **# edit** *<id>*  **# set description** *<desc>*  **# set type** *<L4|L7|VPN|forward>*  // L4 match  **# set protocol** *<tcp/udp/any>*  **# set destination-address** *<ip>*  **# set destination-port** *<port>*  // L7 match  **# set application-signature** *<name>*  // VPN match  **# set vpnid** *<vpnid>*  **# set destination-network** *<ip/netmask>*  // next hop gateway settings, for L4/L7/VPN  **# set nexthop-gateway** *<gateway-name>*  **# set forward-gateway** *<tunnel|fullnat>*  // L4 & L7 server settings  **# set server-address** *<ip>*  **# set server-port** *<ip>*  **# set forward-server** *<snat | clientip>*  // L7 server settings  **# set server-type** *<http/https>*  // cascade topology only  **# set forward-mark** *<mark>*  **# exit** |

其中各项参数定义如下：

**id** - 应用路由id；

**description** - 应用路由描述（可选）；

**type** - 应用路由类型，目前包括L4/L7/VPN/Forwad四类，其中:

L4 指通过ip/proto/port来进行匹配;

L7 根据应用层识别分类来进行匹配;

VPN 指VPN流量，通过VPNID来指定；

Forward 指流量在本地进行中转，比如报文需要通过3个快线网关A->B->C时，中间网关B上需要配置该forward类型路由，通过forward-mark进行匹配；

**protocol** - 指定L4应用路由中protocol匹配条件，包括tcp/udp/any三类;

**destination-address** - L4应用路由中报文目的地址，目前只支持IPv4；

**destination-port** - L4应用路由中报文目的端口，在protocol为TCP, UDP时生效；

**application-signature** - 参见L7 proxyd命令行定义，用来指定应用层匹配识别类型；

**vpnid** - 接入的VPN流量，会通过本地或者第三方认证服务器进行认证，认证完 成之后会生成对应VPNID，用来标识VPN网络；

**destination-network** - 指定VPN网络内目的网段，同一VPN网络内不同网段可以对应到不同的gateway，需要定义不同的应用路由；

**nexthop-gateway** - 下一跳快线网关，可以指定其他网关或者本地网关；

**forward-gateway** - 数据报文传输给下一跳快线网关的方式，包括tunnel和fullnat两种(目前只支持tunnel)

**forward-mark** - 对于级联场景，报文需要通过3个或者3个以上快线网关，比如 A -> B ->C，在A上配置正常L4/L7/VPN路由之后，需要额外设置forward-mark，在B上配置forward类型路由，指定forward-mark来进行匹配，并配置nexthop-gateway来指定下一跳网关;

*对于非级联场景，该值不需要配置；*

**server-address** - 对于L4/L7类型应用路由，指定报文真实server地址；

**server-port** - 对于L4/L7类型应用路由，指定报文真实server 端口；

**server-type** - 对于L7类型的HTTP类应用路由，指定后端访问server是通过HTTP/HTTPS访问；

**forward-server** - 对于L4/L7类型应用路由，输出网关将报文输出给server时，采用保留原clientip，还是SNAT访问方式；

注意：

1. 应用路由采用first match匹配方式，即一个报文如果同时匹配多条应用路由的话，会第一条匹配路由生效；(暂时未支持调整顺序操作)
2. 对于普通非级联场景，只需要在接入网关上配置应用路由即可，输出网关不需要配置对应的应用路由，但是输出网关上需要配置接入网关的gateway定义，否则回应方向报文可能无法返回到原接入网关；
3. 对于L7/VPN类型路由，需要先配置VPN或者L7 proxy相关配置，参见对应相关文档；

## 典型示例

环境中有A, B, C三个快线网关，其内部网络接口IP地址分别为：

|  |  |  |
| --- | --- | --- |
| 快线网关 | 内部网络接口地址 | 服务网络接口地址 |
| A | 10.0.1.1/16 | 100.100.1.1/24 |
| B | 10.0.2.1/16 | 100.100.2.1/24 |
| C | 10.0.3.1/16 | 100.100.3.1/24 |

### 需求1

在快线网关A上，

1. 将TCP, 目的地址为100.100.1.1, 目的端口为80的报文，通过tunnel方式路由到快线网关B，并输出到快线网关B的服务网络中HTTP server 100.100.2.10:8080上；
2. 将UDP，目的地址为100.100.1.1, 目的端口为53的报文，通过tunnel方式路由到快线网关C，并输出到快线网关C的服务网络中DNS server 100.100.3.10:53上；

Gateway配置:

A:

|  |
| --- |
| **# config application-route gateway**  **# edit B**  **# set address 10.0.2.1**  **# exit**  **# config application-route gateway**  **# edit C**  **# set address 10.0.3.1**  **# exit** |

B:

|  |
| --- |
| **# config application-route gateway**  **# edit A**  **# set address 10.0.1.1**  **# exit**  **# config application-route gateway**  **# edit C**  **# set address 10.0.3.1**  **# exit** |

C

|  |
| --- |
| **# config application-route gateway**  **# edit A**  **# set address 10.0.1.1**  **# exit**  **# config application-route gateway**  **# edit B**  **# set address 10.0.2.1**  **# exit** |

Route配置(只需要在A上配置route):

|  |
| --- |
| **# config application-route route**  **# edit 1**  **# set type L4**  **# set protocol tcp**  **# set destination-address 100.100.1.1**  **# set destination-port 80**  **# set nexthop-gateway B**  **# set forward-gateway tunnel**  **# set server-address 100.100.2.10**  **# set server-port 8080**  **# set forward-server snat**  **# exit**  **# config application-route route**  **# edit 2**  **# set type L4**  **# set protocol udp**  **# set destination-address 100.100.1.1**  **# set destination-port 53**  **# set nexthop-gateway C**  **# set forward-gateway tunnel**  **# set server-address 100.100.3.10**  **# set server-port 53**  **# set forward-server snat**  **# exit** |

### 需求2(级联)

级联场景，在A上，将TCP, 目的地址为100.100.1.1, 目的端口为80的报文，通过tunnel方式路由到快线网关B，由B中转到C，并输出到快线网关C的服务网络中HTTP server 100.100.2.10:8080上；(A -> B -> C)

Gateway配置如需求1；

Route配置(需要在A，B上配置)

A配置如下：

|  |
| --- |
| **# config application-route route**  **# edit 1**  **# set type L4**  **# set protocol tcp**  **# set destination-address 100.100.1.1**  **# set destination-port 80**  **# set nexthop-gateway B**  **# set forward-gateway tunnel**  **# set server-address 100.100.2.10**  **# set server-port 8080**  **# set forward-server snat**  **# set forward-mark 100**  **# exit** |

B配置如下

|  |
| --- |
| **# config application-route route**  **# edit 1**  **# set type forward**  **# set forward-mark 100**  **# set nexthop-gateway C**  **# set forward-gateway tunnel**  **# exit** |

其中

1. forward-mark用来标记该类型的流量，可以任意指定，保证A和B上相同，不和其他forward-mark重复即可；
2. 输出网关C不需要配置；