|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| sihuatech   |  |  | | --- | --- | | 产品名称 | 密级 | | 快线网关 |  | | 产品版本 | 共 8 页 | | V1.00 | |
| 快线网关功能说明书 |
| ——V1.0版 |
|  |
| **葛巍峰** |
| **2014/6/10** |

|  |  |  |  |
| --- | --- | --- | --- |
| 拟制人： | 葛巍峰 | 日期： | 2014-6-10 |
| 评审人： |  | 日期： |  |
| 批准人： |  | 日期： |  |

修订记录

| 日期 | 版本 | 修改章节 | 修改描述 | 作者 |
| --- | --- | --- | --- | --- |
| 2014-6-10 | V1.00 |  | 初稿 | 葛巍峰 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

修订记录 1

1 引言 4

1.1 编写目的 4

1.2 背景 4

1.3 术语定义 5

2 系统需求分析 6

2.1 系统整体功能 6

2.2 总体需求分析 7

2.3 系统运行环境特征描述 8

2.3.1 网络边界 8

2.3.2 服务代理和转发 8

2.3.3 VPN接入点 8

2.3.4 周边系统描述 9

3 功能场景描述 10

3.1 状态管控 10

3.2 输出日志 10

3.2.1 日志格式的定义 10

3.2.2 日志输出方式 10

3.3 VPN业务场景 11

3.4 WEB加速场景 12

3.5 IP数据转发场景 13

3.6 7层协议代理场景 14

4 功能性说明 15

4.1 快线网关管控功能 15

4.1.1 权限管理 15

4.1.2 设备管理 16

4.1.3 日志管理 16

4.1.4 接口管理 16

4.1.5 应用管理 16

4.1.6 应用路径定义 16

4.2 对外接口定义 17

4.2.1 人机管控界面（WEB，Terminal） 17

4.2.2 日志上报接口（SYSLOG） 17

4.2.3 设备状态查询接口（SNMP） 17

4.2.4 应用状态查询接口（HTTP XML ） 17

4.2.5 设备配置接口（SSH+HTTP XML+IPMI） 17

4.2.6 应用路径同步接口（HTTP XML） 18

4.3 应用识别和匹配 18

4.4 IP/PORT转发功能 18

4.5 HTTP/HTTPS加速功能 20

4.5.1 UDP协议传输功能 20

4.5.2 HTTP协议版本转换 22

4.5.3 HTTPS协议代理功能 23

4.6 七层协议加速功能 23

4.7 VPN功能接入 24

4.7.1 VPN的用户鉴权和网络划分 24

4.7.2 VPN的数据传输通道 24

4.7.3 内部数据传输数据格式 24

4.8 功能支持列表 25

5 非功能性说明 25

5.1 可靠性要求 25

5.1.1 冗余性要求 25

5.1.2 心跳和健康上报机制 26

5.2 性能和稳定性要求 26

5.2.1 性能要求 26

5.2.2 稳定性要求 26

5.3 网络兼容性要求 26

5.4 安全性要求 26

5.5 可测试性/可调试 26

6 时间和计划 27

6.1 演示系统目标和时间 27

6.1.1 目标标志 27

6.1.2 时间安排 27

6.2 最终系统目标和时间 27

6.2.1 目标标志 27

6.2.2 时间安排 27

1. 引言

快线网关是快线服务系统的一部分，担负着快线系统用户服务的功能，本文从功能，接口，业务场景等方面对快线网关的功能进行描述。

* 1. 编写目的

本文的编写目的是描述快线网关的功能，业务要求。功能说明书是设计的基础,在日后的功能的细化设计中可以使设计及开发人员明确所开发的系统功能的目的，并在在日后的测试发布中可以作为编写测试用例的依据。

* 1. 背景

当前CDN产品的核心思想是将内容缓存到用户侧，让内容就近为用户服务，这个设计可以满足大部分内容为主的业务的加速，但是随着移动办公，网络游戏等各种交互业务的产生，传统的内容缓存为主的内容加速服务就很难满足新的业务要求，动态内容加速成为CDN迫切需要的功能。

与之同时的网宿，蓝汛，AKAMAI等CDN运营商纷纷提出了自己的动态内容加速的解决方案，在此背景下提出了快线网络的产品概念，力求解决最终用户到SP的中间一公里的网络加速，并兼容现有的高级应用协议，通过减少用户端到SP端网络延迟和传输效率提高用户的服务体验，创造服务价值。

总体来说快线系统由于不涉及到大量的内容的存储业务，因此相对于CDN具备了去中心化的特点，即没有逻辑上的中心和边缘的概念，没有控制上的核心和分支的概念，全局服务在任何一个或一组组件异常的情况下都可以正常容错。

相对于面向应用和服务的加速用户而言，所加速都是http协议族的业务，一大部分企业用户也有面向网络加速的要求，当企业，企业的分支机构，企业的在外办事人员人员，企业的IT系统所托管的机房分布在各地的时候，此时企业往往需要将四者网络进行打通，建立高速的企业内部虚拟网络，此时快线系统可以利用其自身的内部传输网络，通过四者的的接入点的用户接入到快线网络中完成虚拟企业内网的创建。

基于上述的多方面需求的背景，快线网关被提出和设计，用于快线系统中的用户接入，应用接入，数据处理的功能。

* 1. 术语定义
* LinEx：思华科技用户网络加速的快线系统的标识；
* 快线网关：快线系统中用于用户服务的组件。
* 应用路径信息：在快线系统中用于标识一个应用到达目标网络所经过的路径的描述；
* NAT：NAT（Network Address Translation，网络地址转换）是将IP 数据包头中的IP 地址转换为另一个IP 地址的过程。在实际应用中，NAT 主要用于实现私有网络访问公共网络的功能。
* Syslog：syslog发送端会传送出一个小的文字讯息到syslog接收端。接收端通常名为“syslogd”、“syslog daemon”或[syslog服务器](http://zh.wikipedia.org/w/index.php?title=Syslog%E4%BC%BA%E6%9C%8D%E5%99%A8&action=edit&redlink=1)。系统日志讯息可以被以[UDP](http://zh.wikipedia.org/wiki/UDP)协定及╱或[TCP](http://zh.wikipedia.org/wiki/TCP)协定来传送。
* SNMP：简单网络管理协议（SNMP），由一组网络管理的标准组成，通常用于获得网络端的设备的运行情况，传递当前的运行指标。
* SNMP TRAP：使SNMP被管设备主动通知SNMP管理器的一种程序接口。
* AAA服务器：AAA是验证、授权和记账（Authentication、Authorization、Accounting ）三个英文单词的简称。
* RADIUS协议：RADIUS（Remote Authentication Dial In User Service）协议是在IETF的RFC2865和2866中定义的。RADIUS 是基于 UDP 的一种客户机/服务器协议。
* Diameter协议：被IETF的AAA工作组作为下一代的[AAA协议](http://baike.baidu.com/view/64087.htm)标准，是RADIUS的增强版本，最新一代的AAA协议标准。
* HTTP：超文本传输协议 (HTTP-Hypertext transfer protocol) 是一种详细规定了浏览器和万维网服务器之间互相通信的规则，通过因特网传送万维网文档的数据传送协议。
* HTTPS：在http(超文本传输协议)基础上提出的一种安全的http协议，因此可以称为安全的超文本传输协议。http协议直接放置在TCP协议之上，而https提出在http和TCP中间加上一层加密层。从发送端看，这一层负责把http的内容加密后送到下层的TCP，从接收方看，这一层负责将TCP送来的数据解密还原成http的内容。
* SSL(Secure Socket Layer)：是Netscape公司设计的主要用于WEB的安全传输协议。
* 数字证书：一种文件的名称，好比一个机构或人的签名，能够证明这个机构或人的真实性。其中包含的信息，用于实现上述功能。
* 加密和认证：加密是指通信双方为了防止铭感信息在信道上被第三方窃听而泄漏，将明文通过加密变成密文，如果第三方无法解密的话，就算他获得密文也无能为力；认证是指通信双方为了确认对方是值得信任的消息发送或接受方，而不是使用假身份的骗子，采取的确认身份的方式。

1. 系统需求分析

根据快线网络的业务需求，总结出快线网络所应该支持的功能，以满足系统整体运行的需要。

* 1. 系统整体功能

快线系统总体上业务功能分为：多点对多点的VPN网络，点对面的服务加速，点对点的VPN通道。其中多点对多点的VPN网络一般用于企业及分支结构，数据中心的互联，也适用于VPN的游戏加速业务服务；点对面的服务加速用于HTTP/HTTPS等应用交付网络的业务加速；点对点的VPN通道是多点VPN的极端情况，用于数据安全传输，远程数据同步等业务。



* 1. 总体需求分析

根据整个系统的业务功能，快线网关的业务功能被定义成几个方面：

1. 支持根据用户访问的目的IP和端口进行应用判断，对用户数据NAT转发到目标网络；
2. 支持HTTP协议的动态网页加速功能；
3. 支持对HTTP协议的7层数据匹配进行应用判断；
4. 支持HTTPS代理加速的功能；
5. 支持灵活的业务路径配置的定义和生效；
6. 支持日志定义，日志打印，日志可配置的输出的功能；
7. 对未来的IPV6网络的兼容性；
8. 支持RADIUS和Diameter协议的VPN用户认证/鉴权功能；
9. 支持IPSEC，OpenVPN，PPTP，L2TP协议的VPN服务，及多个VPN接入点的网络汇聚；

* 1. 系统运行环境特征描述
     1. 网络边界

快线网关系统在大部分情况下需要接入在两个网络之间，即面向互联网的接入和面向内部传输网络的接入，通过快线网关的内部功能，将接收到公网的用户请求通过内部传输网络传输到用户的目的网络中的快线网关上，终点的快线网关将请求最终投放到目的网络中。并将用请求的服务的返回数据原路传输给用户。

* + 1. 服务代理和转发

快线网关需要根据用户请求行为的特定标志位判断用户的请求目标，根据用户请求的目标对用户服务进行代理或者对用户IP数据进行转发。

典型的两种情况是：根据用户请求的HTTP/HTTPS协议的Hostname字段，根据用户请求的目的IP或者端口字段。当出现对其他应用协议进行支持的时候可能涉及到识别指定的应用层标志字段来判断用户所请求的应用。

* + 1. VPN接入点

快线网关作为VPN接入点的时候，需要通过分布在网络边缘的多个快线网关接入多个用户，并最终将所有具备相同VPN属性的用户汇聚成一个内部VPN，各个接入点的用户请求数据都会通过在内部VPN中得到处理和转发。用户数据通过快线网关进入内部网络，通过内部网络达到目标网络，通过目标网络的快线网关进入用户目标网络。

* + 1. 周边系统描述



周边系统包括：

* 用户调度系统：用于将互联网用户导向到快线网关；
* 日志采集系统：用于将快线网关的服务日志采集到中心节点的HDFS的文件系统上；
* AAA系统：用于记录VPN注册用户信息，包校验用户登录VPN的密码和状态，决定用户是否可以登录；
* 日志处理系统：对采集下来的日志进行数据处理，计算出分析结果上报报表系统；
* 路由管理系统：对全网的应用路径信息进行维护，根据网关设备的健康情况，压力情况，调度策略，应用策略等信息维护应用路径表，并做全网的网关和路径管理网元同步；
* OSS：通过分布式系统对全网的各个硬件设备进行管理和维护；
* 报表系统：获取日志处理系统给出的原始数据，展示业务的承载的报表；
* 网络感知平台：通过分布于网络中得大量的探针对服务进行播测，判断服务的可用性，为调度系统提供调度依据；

1. 功能场景描述

本章描述了快线网关的的功能运行的场景，包括网络，业务形态，协议处理的要求。

* 1. 状态管控

能够对快线网关进行基础配置，业务配置，日志配置，安全性配置。

管控方式包括人机界面管控，接口管控，终端登录控制。

* 1. 输出日志
     1. 日志格式的定义

针对各种不同的业务日志要求的字段不一致，需要能够对各种不同的服务进行日志字段，日志格式，日志是否压缩，日志分隔符等的控制。

针对HTTP/HTTPS协议的业务：需要满足W3C的日志字段的要求，同时记录，判断出来的用户所属业务标识，到应用路径的下一个节点（网关，SP服务，用户）的标识和延迟，自身返回的数据的延迟；

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；

针对IP/PORT转发的业务，需要定义用户IP，用户的所属业务，应用路径的下一个节点（网关，SP服务，用户）的标识和延迟，以及应用层指定的字段（比如FTP协议中的下载URL）

* + 1. 日志输出方式

日志输出方式包括应用日志的输出和运行日志的输出。

其中运行日志级别自定义分为Debug，INFO，WARN，ERROR，FATAL；应用日志的输出遵循3.2.1节所定义的日志格式和字段。

有两种方式进行输出：

本地磁盘打印：支持日志打印到本次磁盘的目录用于问题调试；

SYSLOG协议的日志输出：支持UDP方式和TCP方式的SYSLOG协议网络输出。

* 1. VPN业务场景

VPN的业务形态是：企业或者个人用户通过网络设备，定制客户端，通用VPN客户端等手段，从多个网络中向提供VPN服务的快线网关发起VPN请求，快线网关根据用户传递进来的特定字段，用户名密码，密钥信息判断用户请求的合法性，和授权用户建立VPN连接，并将多个快线网关接入到同一个VPN网络的请求进行处理，将用户请求通过内部的网络传输到用户请求目标就近的接入快线网关，利用已有的内网高速网络，满足用户对网络加速的需求。

对该业务同时提出来一些附加的VPN功能，包括：

定时检测用户信息，对用户的VPN连接进行关闭操作；

通过RADIUS或者Diameter协议，向AAA系统发送用户认证鉴权指令，根据返回结果确认用户是否可以上线；

根据用户属性判断用户所归属的VPN网络；

对用户VPN内网中的网络路由进行维护，保证VPN网络可以根据用户访问的目标网络判断目标的用户接入网关；

对多个节点的VPN网络中分配出去分配IP地址列表进行维护确保VPN网络中没有IP地址冲突的情况；

各VPN接入点之间的数据通道的传输方式进行优化，确保接入点之间VPN隧道高效传输；

对接入点之间数据通讯进行控制，减少无效数据穿越内部的VPN通道；

一般的业务逻辑图如下：



* 1. WEB加速场景

WEB加速的场景包括HTTP协议和HTTPS协议的WEB服务加速的应用，区别是后者需要进行证书分发和部署。

面向的服务目标是传统CDN无法承载的动态内容的加速和交互内容的加速，交互内容包括用户上传数据，用户指令提交，服务动态数据交付等，代表业务有：内容上传加速，网页游戏加速，用户订单数据提交。

其中为了明显的提高内部网络加速效能，针对内部传输网络的网络质量包括延迟，丢包率，带宽等指标明显更优的情况，内网的HTTP数据传输建议采用UDP方式进行传输，减少TCP协议所带来的延迟。

每个网关在网络中是没有层级关系和功能区分的，一个网关即要充当用户接入的WEB服务，又要充当回SP源站的代理服务器。

Web加速场景逻辑图如下：



* 1. IP数据转发场景

在部分不是HTTP业务的加速场景中，网关无法根据请求的标志字段判断用户的业务，也就无法判断用户真正访问的目标网络。此时网关可以根据用户访问的目标IP或者端口判断用户请求的所属的业务类型，根据业务的路径定义将用户请求的IP数据包进行NAT/PAT处理，追加业务标志后通过隧道转发到目标网络的网关入口，目标网络的网关根据已经判断的用户业务标志将IP数据请求NAT/PAT到目标网络。

具体的NAT/PAT策略包括：

根据用户请求数据，修改目标IP成最终的服务IP，将请求发送到和目标网通讯的数据隧道中；

目标网关从隧道获取数据后，将源IP改成自身的出口IP，将请求发送给目标服务网络；

服务返回数据后根据Session记录，将目标IP改成用户IP，数据发送到和源网关的数据隧道中；

源网关从隧道中将数据取出后，将源IP改成网关IP发送给用户。

IP数据转发场景的逻辑图如下：



* 1. 7层协议代理场景

非HTTP业务同时系统没有足够的IP地址用于业务区分，此时需要对请求的应用层的字段进行识别并判断请求所关联的应用，根据应用的类型使用应用代理的功能进行服务。

和WEB加速基本类似，只是在应用判断的字段，应用代理的方式所有不同。

业务场景逻辑结构如下：



1. 功能性说明

本章对快线网关的功能模块的子功能进行列举和说明，并对部分数据处理流程细节进行描述。

* 1. 快线网关管控功能

* + 1. 权限管理

定义对设备进行管理的用户ID和密码，对设备管理权限进行分权，包括查看权限，应用修改权限，设备修改权限等。

对管理用户登陆进行用户名密码验证，对可操作的IP地址段进行限制。

* + 1. 设备管理

对设备的硬件情况进行查看和管理，包括查看CPU，内存，网卡，IO，磁盘空间使用情况进行查看和管理，对网络情况进行配置，包括IP地址配置，路由配置。

在设备操作系统出现异常的时候，使用支持IPMI接口的BMC芯片对硬件进行检查和故障排除。

* + 1. 日志管理

对日志进行管理包括日志字段协议，日志的格式定义，日志的输出方式定义，日志SYSLOG输出情况下的输出目标IP地址+端口和协议，需要本地磁盘进行存放的日志需要定义轮训策略，压缩策略。

* + 1. 接口管理

定义系统对外的各种接口参数，包括接口的验证策略，主动接口的目标地址，被动接口受信任IP，接口类型，接口传递的参数。

具体的接口类型参见4.2章节所描述的接口。

* + 1. 应用管理

对应用进行配置定义应用的识别标志，应用的允许列表，应用的回源方式，应用数据传输方式，HTTPS的证书文件，VPN的诸多协议的参数，AAA服务器配置，鉴权协议配置等。

* + 1. 应用路径定义

对每一个应用定义路径信息进行定义，定义每一种应用到达目标网络的路径，在每一段网络的对数据的处理方式。

对于WEB服务加速，7层协议代理，IP数据转发业务来讲包括应用识别标志位（URL，HOSTNAME，Header，Refer等），应用服务接入点的网关标识，备份回源接入点列表配置，应用回源方式，应用层协议描述，用户请求处理方式。

对于VPN服务来讲，应用路径包括每一接入点所接入的网络的包含的地址列表，用户接入后为用户分配的地址资源，VPN网络内的默认路由。

* 1. 对外接口定义

本节描述了快线网关对外接口的定义。

* + 1. 人机管控界面（WEB，Terminal）

开放给系统管理员使用的管控接口，通过手工通过界面操作，命令输入的方式完成对快线网关的管理和配置。

Web界面是指通过图形化的Web界面来对快线网关的进行管理和控制，可以对块线网关进行4.1所描述的大部分管理功能；

Terminal方式是指通过SSH终端的方式登陆到快线网关的操作系统，使用通用的操作系统命令对快线网关进行调试，查看和配置文件修改生效。

* + 1. 日志上报接口（SYSLOG）

对用户服务日志通过syslog UDP的方式进行上报到指定的接收端API中。

* + 1. 设备状态查询接口（SNMP）

通过向设备发起的SNMP查询指令，获取设备当前的状态，包括不同的网卡的出入流量，磁盘使用情况，CPU内存占用情况，系统连接数等信息。

* + 1. 应用状态查询接口（HTTP XML ）

通过HTTP XML报文的形式向设备查询当前运行设备的应用列表，每一个应用的服务健康性，每个应用的南北向流量情况，每个应用的南北向连接数。

* + 1. 设备配置接口（SSH+HTTP XML+IPMI）

通过HTTP XML或者SSH的方式对设备进行配置，包括4.1.2，4.1.3，4.1.5章节所描述的配置和管理功能。

当设备操作系统出现故障的时候通过支持IPMI接口的BMC设备对设备的硬件，操作系统进行故障排除，软件重装等操作。

* + 1. 应用路径同步接口（HTTP XML）

通过HTTP XML的方式对快线网关的应用路径进行设置和同步，并实时平滑生效。

* 1. 应用识别和匹配

快线网关受到用户请求后，如果用户请求并非是VPN请求，怎需要逐步的对请求数据进行分析判断请求所属的应用，首先查看IP地址是否可以匹配出有效的应用，如果无法匹配则在TCP Session中查找是否包含相应的Session，如果没有相关的Session怎需要查看TCP端口字段是否是特殊端口，如果端口是通用端口无法匹配，则当端口是80，8080，3128端口时，进行HTTP协议分析，通过协议分析判断请求所属应用，如果不是HTTP端口则需要对应用层数据打开查看已有的标志规则寻找匹配项，如都不能匹配，则将数据丢弃。

示意图如下：



* 1. IP/PORT转发功能

用户请求到达后，通过IP和端口的形势判断出用户的请求的应用则可以通过IP地址NAT的方式对用户请求进行转发，一般来说快线网关内部的网络传输方式可以选择NAT方式和隧道方式，但在某些特定情况下只能选择隧道方式，比如SP需要获得用户的IP地址。



通常情况下的用户数据从发起者到服务端的变化，网关间的通讯全部采用隧道方式，优点是不需要做Session保持，用户源IP数据不会丢失，缺点是隧道封装需要消耗额外的资源：



当然也可以采用下述方式，优点是不需要消耗资源封装和接封装，缺点是用户源IP数据在传输过程中丢失，需要快线网关A保存用户源IP信息和Session的关系：



当SP需要用户的真实IP的时候，需要将快线网关部署在SP服务的内网/VPN内网做数据筛选：



当多个LinEx发起到LinExB的请求的时候，每一个请求到达时LinEx都临时保留到UserIP和源网关的关系，用于处理用户回包的时候数据返回时的策略。



当用户端使用VPN接入，SP接入端使用代理方式回源的情况：



* 1. HTTP/HTTPS加速功能
     1. HTTP/HTTPS工作模式描述

HTTP协议中包含两种工作模式，即SP需要最终用户访问IP和IP对用户访问IP没有要求的情况。





* + 1. UDP协议传输功能

发起请求网关动作：用户发起HTTP请求到快线网关，快线网关将请求应用层数据获取后，通过UDP协议的方式发送HTTP 命令到目标快线网关，开启计时器，如果在超时时间内收到UDP返回的HTTP报文，则将HTTP返回信息通过通常HTTP协议转发给用户，如果在超时时间内没有收到HTTP返回数据，则认为网络状况较差，使用常规的TCP协议重新向目标快线网关发起HTTP协议，此时的返回数据可以直接返回给用户。



接受请求网关动作：网关收到UDP协议传输的HTTP报文，将该报文的HTTP层数据解析，读取应用信息，根据应用路径信息判断目标的应用位置，发起常规的HTTP请求到目标网络，目标网络返回数据后，将数据通过UDP协议返回给请求发起网关。



* + 1. HTTP协议版本转换

针对HTTP1.0 到HTTP 1.1的版本转化，能够将低版本浏览器发起的HTTP1.0的请求转化成HTTP1.1版本代理返回源站，减少源站在处理改请求时的压力。

* + 1. HTTPS协议代理功能



* 1. 七层协议加速功能

针对非HTTP协议请求，如果并非是VPN拨入的请求，无法通过IP地址和端口进行应用识别则需要使用七层协议加速功能进行处理。

* 1. VPN功能接入

VPN功能在业务接入分为企业VPN和个人VPN。企业VPN一般指企业总部，企业分支机构，企业数据中心多地网络通过快线网关接入到VPN系统，达到企业内部高速互联的目的；个人VPN一般面向个人用户对面向个人用户的游戏加速，点对点数据共享，安全数据通道进行VPN服务。快线网关在支持已有的L2TP，PPTP，IPSEC，OPENVPN的VPN协议拨入基础之上，需要的个性功能如下：

* + 1. VPN的用户鉴权和网络划分

快线网关需要根据AAA服务器的用户描述信息，通过RADUIS或者Diameter协议发送鉴权申请，返回成功后允许用户接入并根据VPN拨入的用户名判断用户所属的应用，并根据数据包的目标地址和应用路径的判断下一个网关，将用户请求的数据包中附加上应用标志字段，发送到内部网络中到下一跳网关的隧道中去。

* + 1. VPN的数据传输通道

VPN数据发送端网关



VPN数据接受端网关



* + 1. 内部数据传输数据格式

建议采用的内网传输隧道的数据格式，接受用请求的快线网关通过VPN通道建立的用户ID判断出VPN内部数据归属的应用，将数据从VPN封装取出，在IP数据的头上追加应用标识，将包含应用标识，用户请求数据的整个数据作为隧道IP封装的Payload，发送到目标的快线网关，目标快线网关根据将隧道中数据取出，读取应用标识字段后，将用户请求数据还原发送到用户请求的目的VPN网络中。



* + 1. 多VPN标识多路由功能

同一个快线网关可以介入多个不同VPN网络的用户，而不同的VPN网络是可能存在IP冲突的情况的，这就要快线网关的VPN路由中需要增加网络标识字段。



* 1. 功能支持列表

用户请求方式：VPN接入请求，通常的IP数据请求；

应用识别方式：根据AAA系统中记录的VPN的用户ID识别应用，根据用户请求的IP/端口，根据用户请求的HTTP协议的HOSTNAME/UA/Refer等Header字段，根据用户请求的其他应用层标志；

数据传输方式：SNAT（NAT，Proxy等），ppp tunnel，带有应用特征标识的tunnel，快线网关之间的级联传输。

1. 非功能性说明
   1. 可靠性要求
      1. 冗余性要求

要求两台以上的快线网关能够支持互为服务冗余。

允许多台下一条接入点的均衡负载策略。

* + 1. 心跳和健康上报机制

通过配置快线网关，可以使其自动给定时上报其设备的健康状态。

* 1. 性能和稳定性要求
     1. 性能要求

要求通过快线网关进行服务，单台设备对于VPN，HTTP代理，四层代理混合服务的情况下能够满足10Gbps流量的服务数据转发。

网络数据包在设备上的延迟不超过1ms。

* + 1. 稳定性要求

系统可用性高于99.99%。

* 1. 网络兼容性要求

对已有的IPV4网络和IPV6网络兼容，并且支持IPV4和IPV6的网络的转化，将IPV6的网络请求转发到IPV4的网络上，或者将IPV4的网络请求转发到IPV6的网络上。

适应快线网关的内网进公网出；内网出公网进，内网进内网出，公网进公网出的几种网络工作模式。

* 1. 安全性要求

可以通过控制指令和接口对某些用户进行用户踢出操作，对用IP地址进行禁用，对于鉴权多次失败的请求IP进行禁用。

* 1. 可测试性/可调试

能够通过系统的console等接口对系统的功能进行分析和故障排查，并能够对已知的功能进行测试。

1. 时间和计划
   1. 演示系统目标和时间
      1. 目标标志
      2. 时间安排
   2. 最终系统目标和时间
      1. 目标标志
      2. 时间安排