SD-WAN 网络及设备

用户使用手册

南京未来网络产业创新有限公司

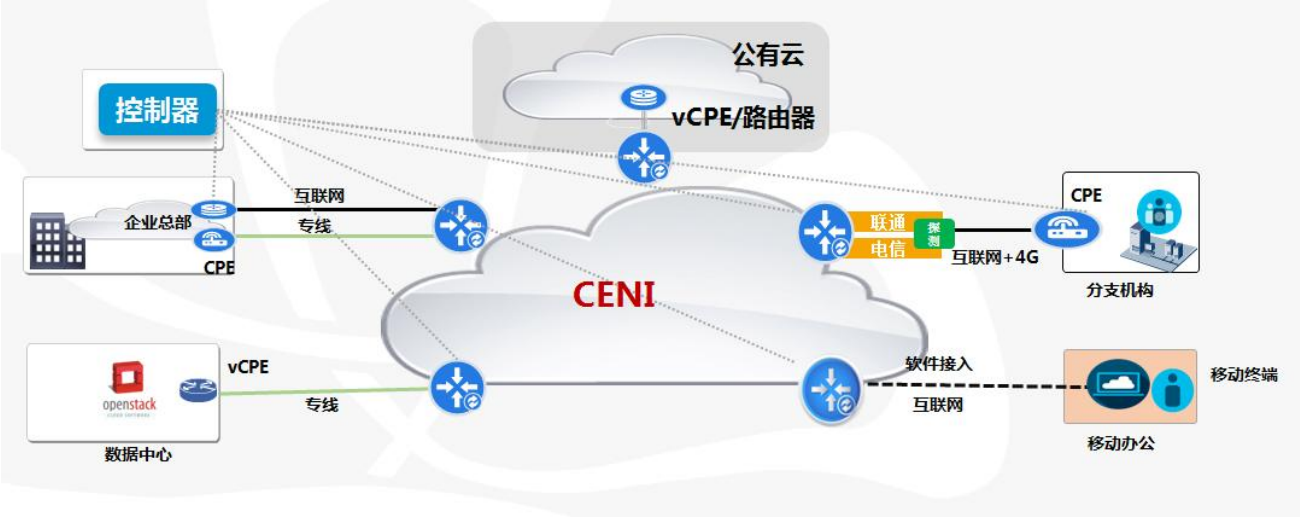
版权声明和保密须知
本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属南京未来网络产业创新有限公司所有，受到有关产权及版权法保护。任何单位和个人未经南京未来网络产业创新有限公司的书面授权许可，不得复制或引用本文件的任何片断，无论通过电子形式或非电子形式。
Copyright © 2020 南京未来网络产业创新有限公司

目 录

1、SDWAN 简介

SD-WAN，即软件定义广域网络，是将 SDN 技术应用到广域网场景中所形成的一种服务，这种服务用于连接广阔地理范围的企业网络、数据中心、互联网应用及云服务。这种服务的典型特征是将网络控制能力通过软件方式“云化”，支持应用可感知的网络能力开放。

所有的设备都在控制器的统一控制下运转，由控制器统一配置、统一管控，得到业务最优化。



SDWAN 组网拓扑图

1.1 名词解释

1.1.1 CPE

- 说明：全称为用户前端设备（Customer Premise Equipment），是指放在用户侧的 SDWAN 网络接入设备；
- 用途：作为“用户站点”去往 SDWAN 骨干网的“网关”，如果一个用户有多个分支机构接入 SDWAN 骨干网，则每个站点至少需要 1 台 CPE；部分重要站点，如数据中心、总部，则需要部署 2 台 CPE，一主一备。

1.1.2 PE/vPE

- 说明：全称为服务商边缘（Provider Edge），指 SDWAN 部署在骨干网边缘，提供用户“接入骨干网”的设备；
- 用途：用来提供用户网络接入，由于经常部署在虚拟化的环境中，故又称其为 VPE（Visual Provider Edge）。

1.1.3 POP 点

- ✧ 说明：全称为 SDWAN 骨干网覆盖的接入点（point of presence），指 SDWAN 骨干提供用户接入的节点，POP 点分布越多，则代表网络接入能力越强；
- ✧ 用途：用来提供用户的网络接入，通常一个 POP 里面会部署多个 VPE 及其配套的网络设备。

1.1.4 CPE HA

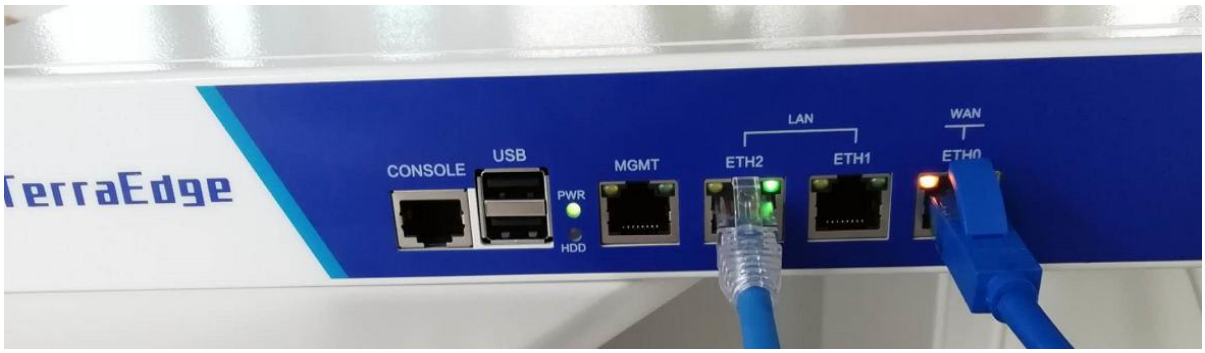
- ✧ 说明：全称为 CPE 高可用（CPE High Available），指用户某些重要的站点同时部署 2 台 SDWAN CPE，形成一主一备的模式；
- ✧ 用途：保障网络的高可靠，HA 模式下，主 CPE 提供网络转发，当主 CPE 出现故障时，备份 CPE 接管主 CPE 的职能，因此网络的正常通信不受影响。

2、CPE 初始配置

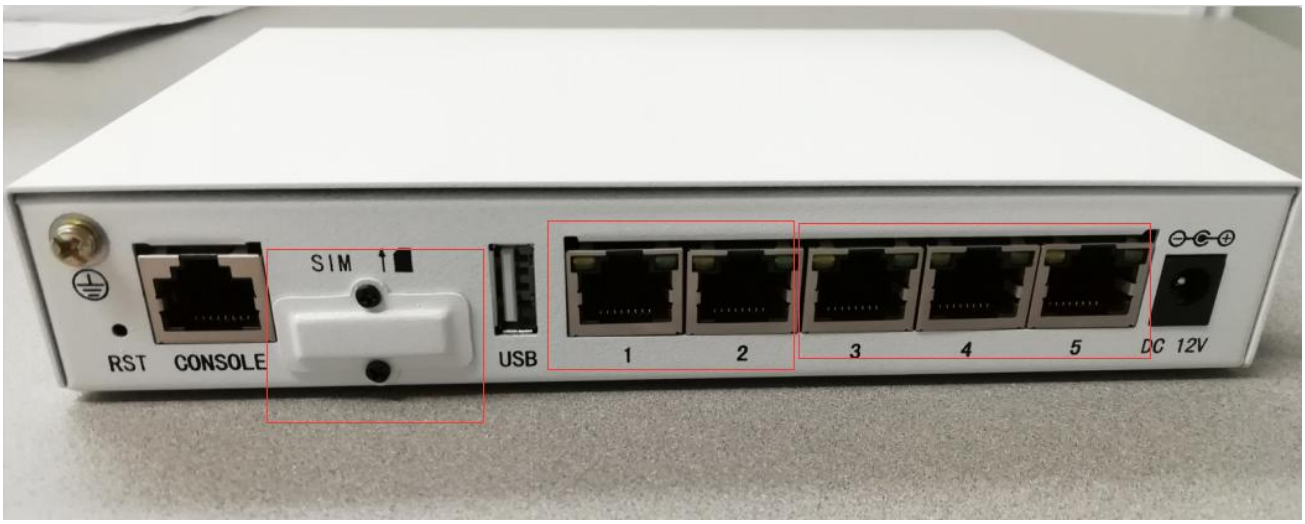
用户接收到的 CPE 都是已经做过本地配置的，默认 WAN 口是自动获取 IP 地址。若用户本地网络为自动获取 IP 地址或采用 4G 卡接入网络，可以直接插网线或插卡入网使用，请忽略本章节的配置。只有在用户网络环境是静态分配 IP 地址的情况，才需要按照本章节的操作步骤重新设置 WAN 口配置后再接入网络。

2.1 CPE 介绍

CPE 支持有线和无线两种接入方式，背面外观如下图（以两种最常用的型号为例）：



本型号没有 WIFI，不支持无线接入，只能通过有线接入网络。最右侧插口 ETH0 为 WAN 口，连接外部网络（出口路由器、机房交换机、工位网线等）。右侧第二口 ETH1、第三口 ETH2 为 LAN，连接内部网络设备（交换机、用户电脑等）。

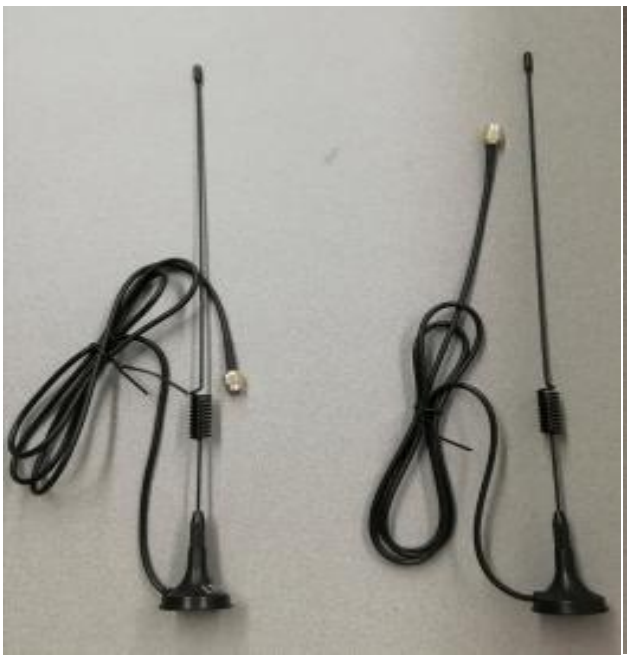


本型号有 WIFI，有卡槽支持手机卡/物联网卡等无线接入，也可以通过有线接入网络。SIM 卡槽用自带小螺丝刀拆卸盖片后安装，采用大卡。1 口和 2 口为 WAN 口，连接外部网络。3、4、5 口为 LAN 口，连接内部网络。

Sim 卡外保护罩可以使用包装盒内自带的小螺丝刀拆卸，如下图：

设备侧面外观如下图：

可以接上铁质 4G 天线和塑料 WIFI 天线，天线分别如下：

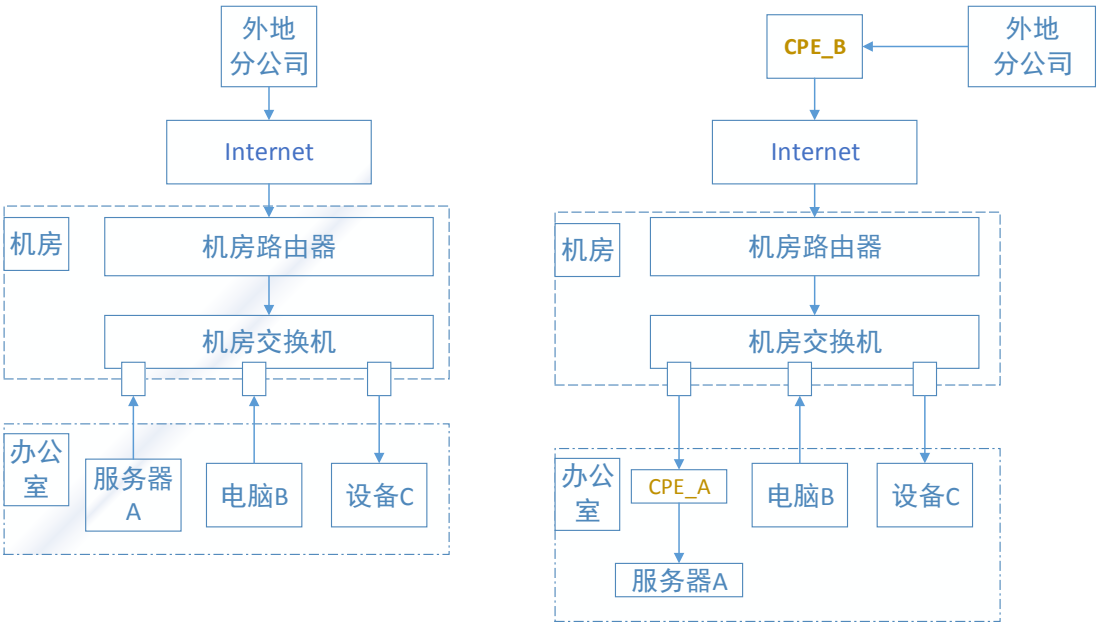


2.2 CPE 布放位置

CPE 布放位置由用户的网管根据业务需要来确定。原则上，CPE 就近安装在需要接入工业专网的设备旁边。根据用户网络实际情况，可以接在路由器和交换机上，也可以接在办公室工位上，只要 CPE 的 wan 口能够连通 Internet 就可以。

1、 简易部署模式

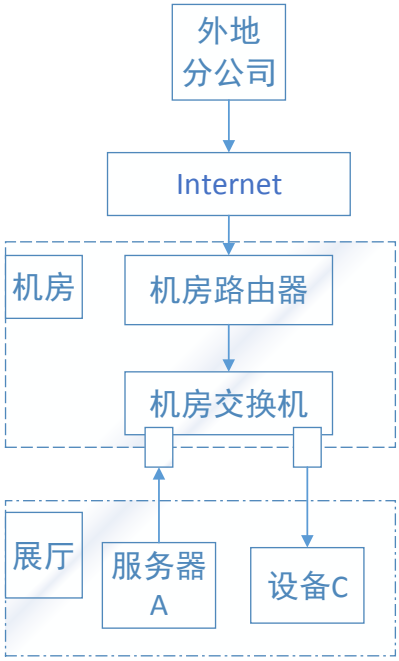
这种部署模式适用于设备较少的情况，如：有一台服务器需要对外提供服务，允许外地办事处通过工业专网接入。只要把设备接在 CPE 的 LAN 口，CPE 的 WAN 口能够连 Internet，就满足接入工业专网的条件，示意图如下（左图为客户原有网络，右图为 CPE 的部署位置）：

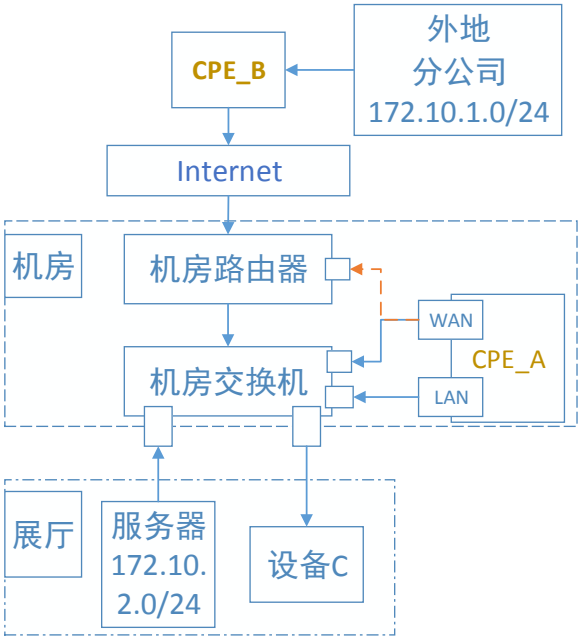


2、 旁挂部署模式

这种部署模式适用于设备较多的情况，如：整个部门或整个公司都需要和外地分公司通过工业专网互联或接入公有云。CPE 部署在机房，旁挂在交换机上，LAN 口接交换机，WAN 口视情况可以接交换机，也可以接路由器。对应的 IP 地址由客户的网管人员根据实际情况来划分。

部署示意图如下（左图为客户原有网络，右图为 CPE 的部署位置）：



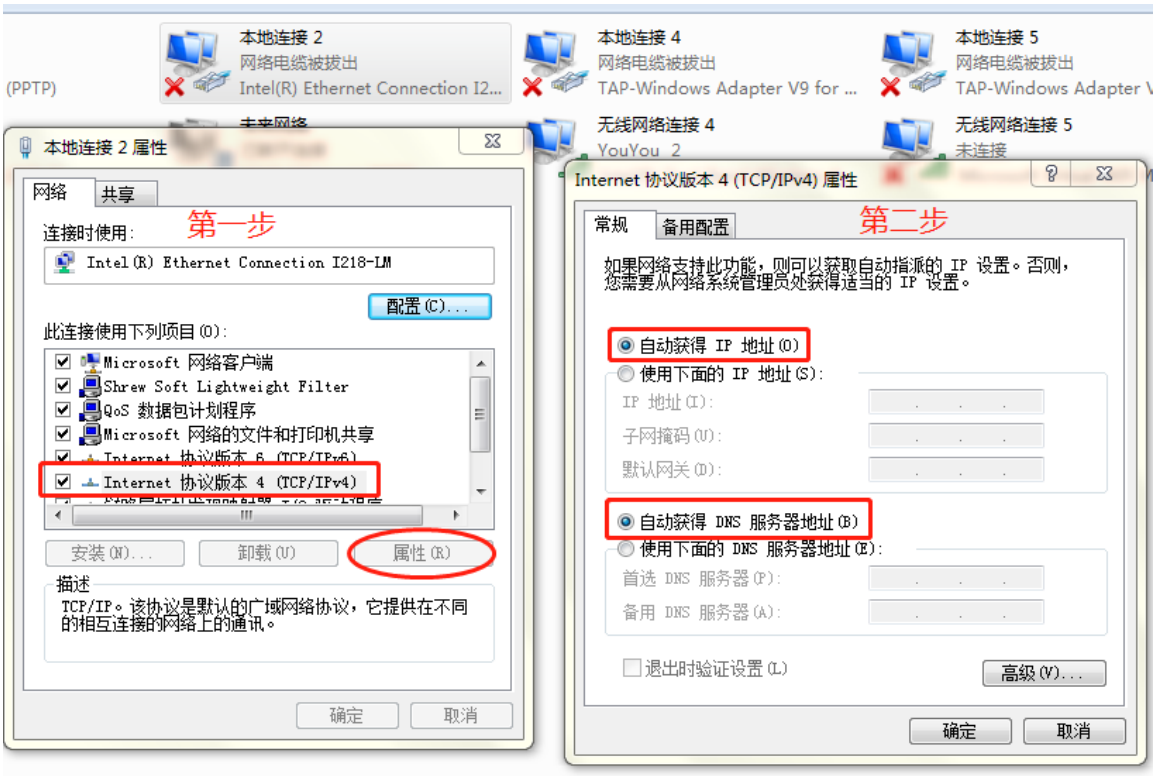


这种模式下，需要客户网管在交换机上加一条静态路由，将前往分支机构 CPE_B 的网段报文的下一跳指向 CPE_A 的 LAN 口网关即可。

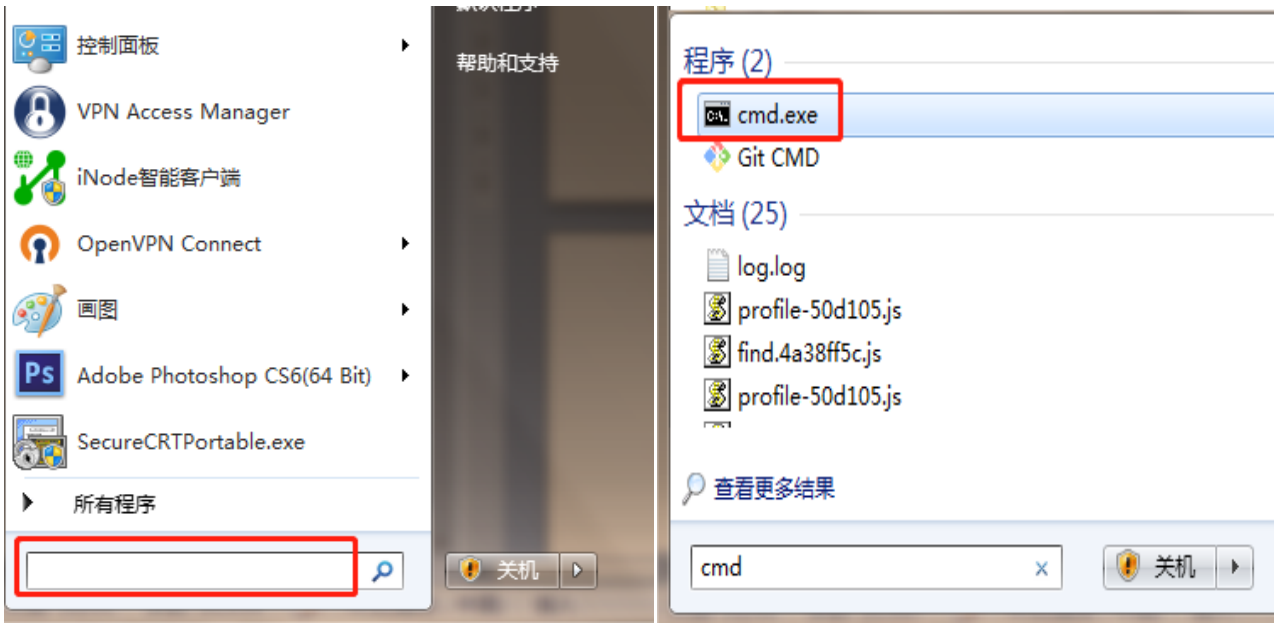
2.3 CPE 初始配置

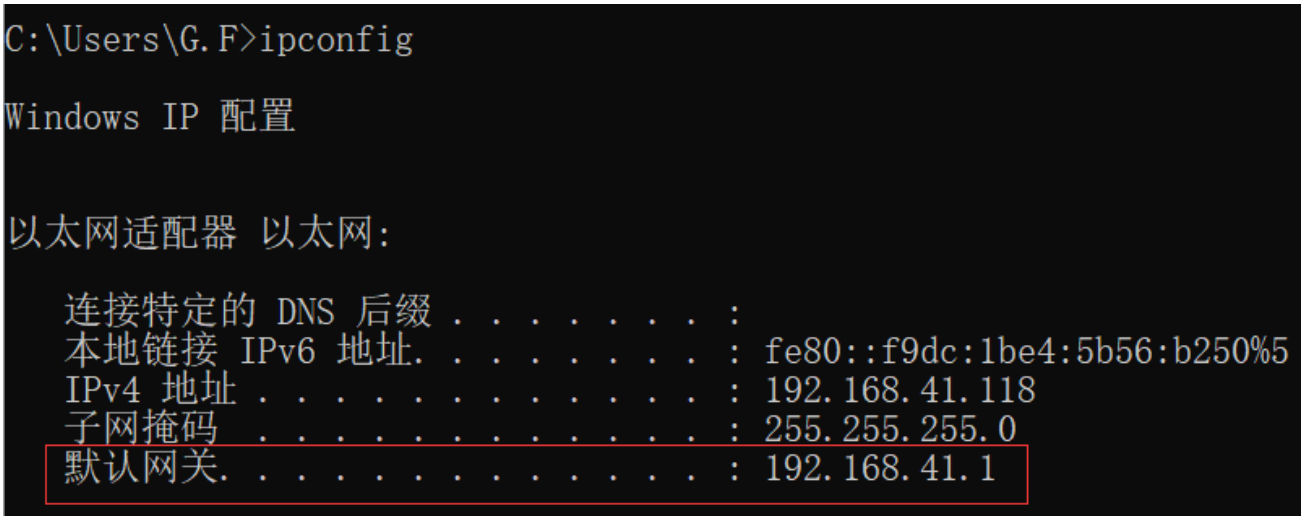
1、电脑配置为自动获取 IP，电脑通过网线连 CPE 的任意一个 LAN 口，把连接 internet 的网线连接到 CPE 的 WAN 口。打开电脑的网络连接，待网络连接成功后，点击网络连接，查看网络信息中的网关地址。

操作流程如下图（截图网络信息仅供示例）：

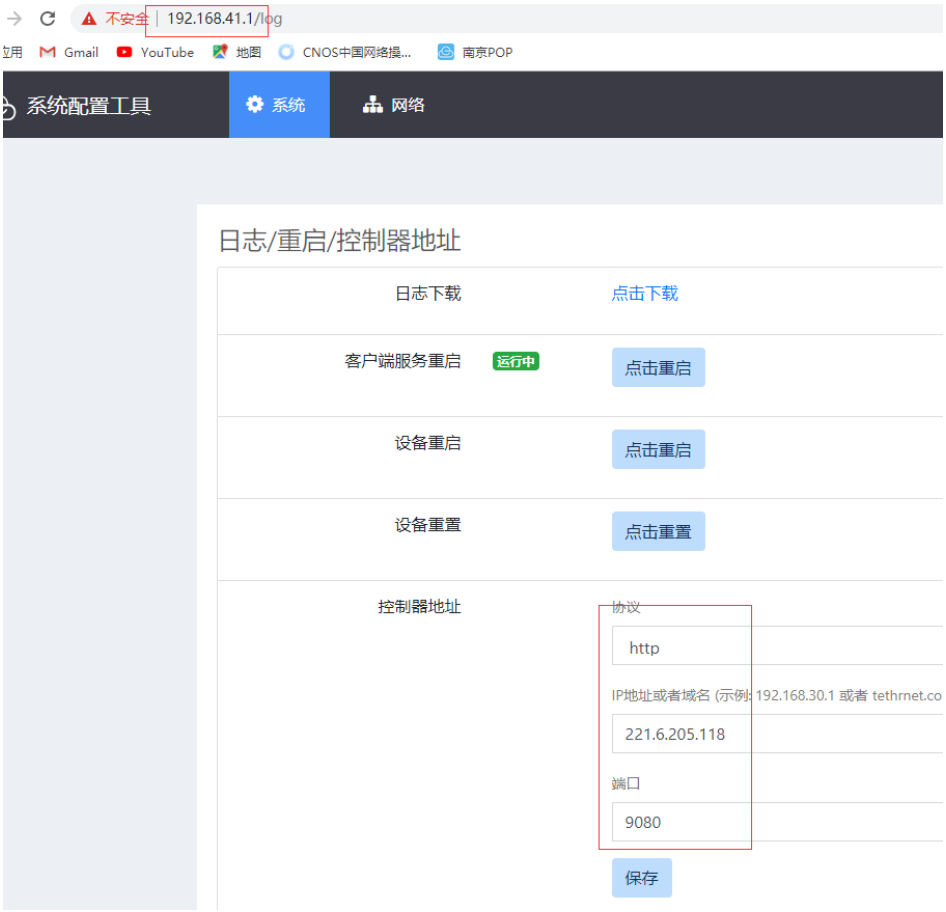


也可以在电脑开始菜单的搜索框中打开 cmd，输入 ipconfig，查看电脑的对应网络连接的网关配置，如下图：

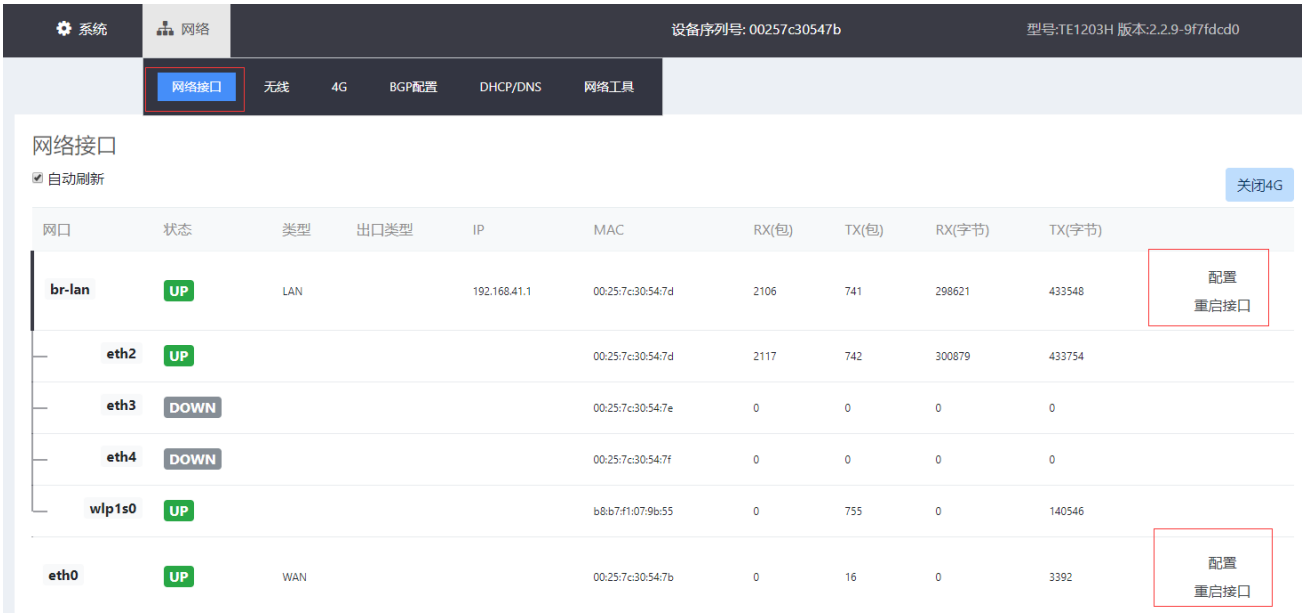




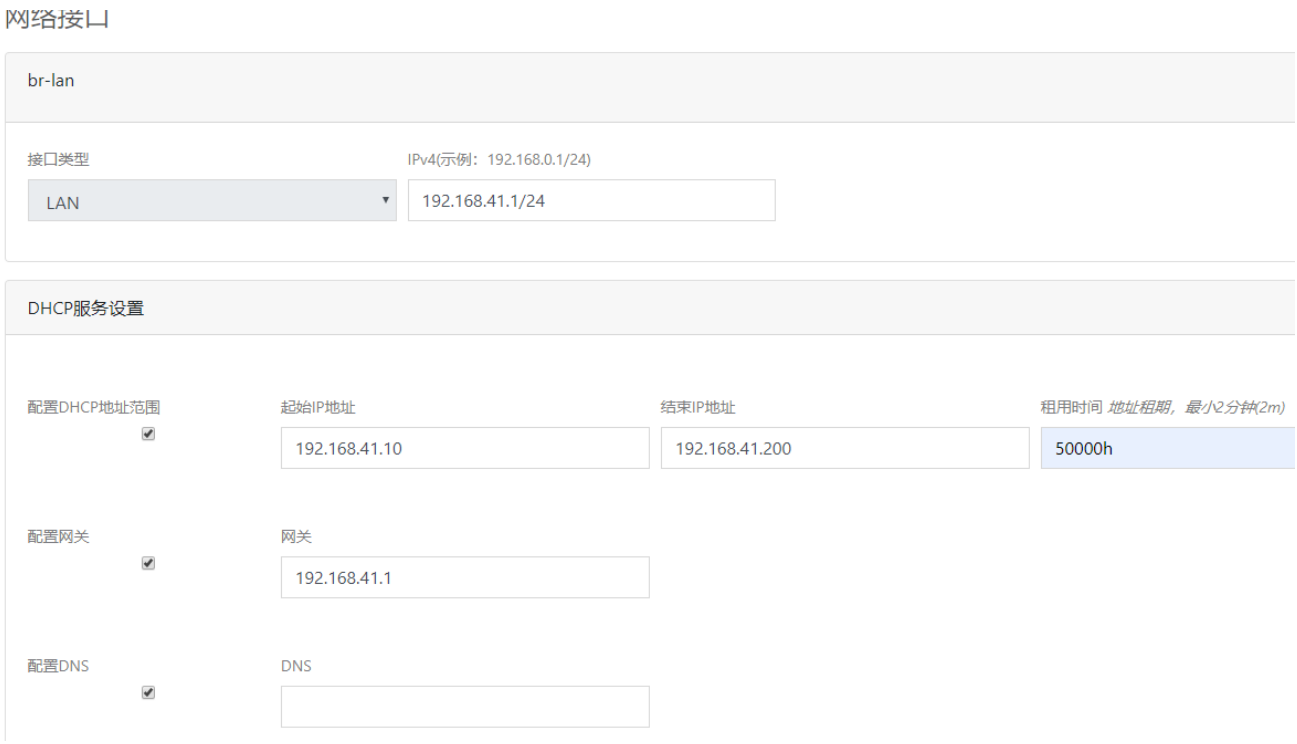
2、电脑打开浏览器，输入网关地址，用户名和密码均为 admin，进入本地管理页面。在系统菜单中核对管理员事先配置好的控制器地址和端口，如下图：



3、切换到网络页面，配置网络接口（绿色、状态为 up 的接口），如下图：



LAN 口 br-lan 的网关配置默认已经启用 DHCP，可以自动为用户的电脑和其他联网设备分配 IP。若用户无特殊的网段规划，则无需更改。若用户需要指定 LAN 口网关并划分网段，则点击 LAN 口，根据用户网络规划配置内网参数（网段、网关为必填项），如下图所示：



保存配置，点击重启接口，重启 br-lan。

由于修改 LAN 网关，会重新给电脑分配地址，需要将对应的电脑连接禁用再启用，获得新的网关地址。参考前述步骤一再次查看网络信息，输入新的网关地址，才可以再次进入本地配置页面。

4、CPE 的 WAN 口默认配置为 DHCP 自动获取 IP 地址，若用户公司的网络为自动获取 IP，则无需更改。若用户公司的网络为静态分配的 IP，则需要更改配置。由用户公司的网管为 CPE 分配一个固定 IP，点击在线的 WAN 口，填写地址和网关（必填），如下图：

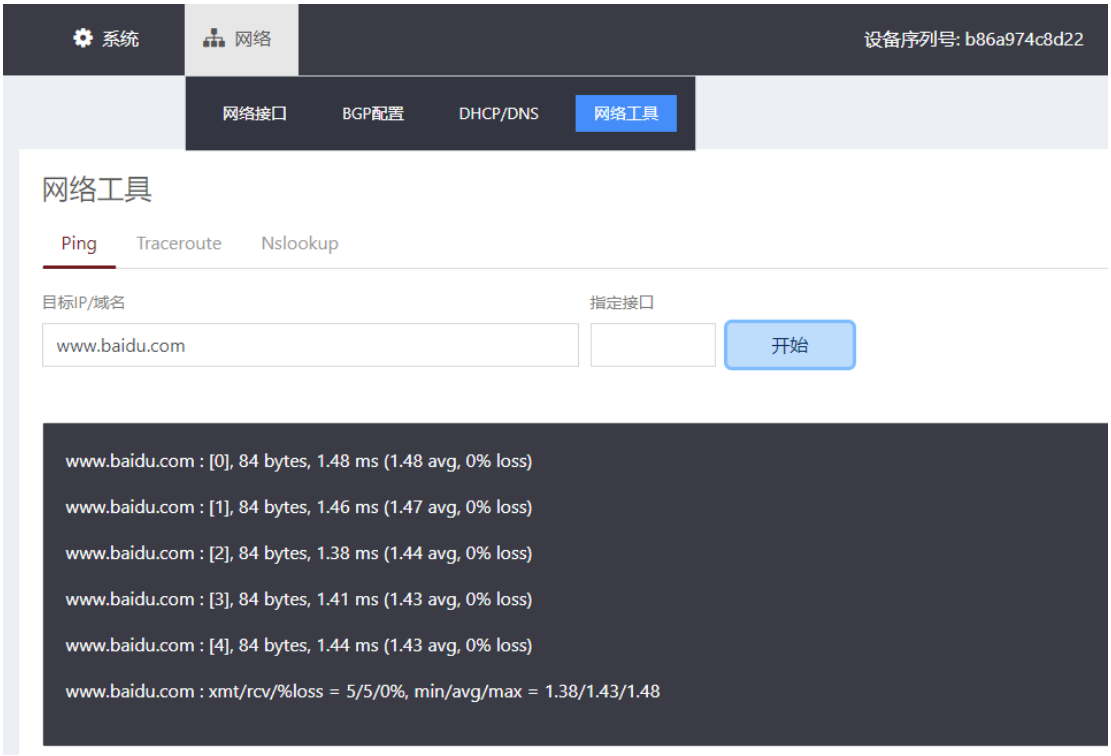
保存配置后，点击重启接口，重启 wan 口，让配置生效。

5、如果通过手机卡或者物联网卡上网，需要在断电状态下插入手机卡。CPE 默认已开启 4G 功能，不需要进行任何额外的手动配置，APN 参数会根据卡自动选择运营商 APN。插卡上电后，打开 4G 页面查看手机卡信息，查看连接状态，如下图：

其中，物联网卡需要具备访问 sdwan 网络的权限，即在运营商的指导下将 SDWAN 控制器和 VPE 服务器地址写入白名单，或单独增加一个 sdwan 网络的 APN。

6、 CPE 支持 WIFI 功能，可以配置无线名称和密码提供移动接入，如下图：

7、配置完成，网线连接完毕，可以在 CPE 上测试一下外网连通性，如下图：



8、通知未来网络管理员，由管理员将 CPE 与用户 ID 绑定。用户管理员登陆控制器，

http://221.6.205.118:9080，输入预先分配的用户账户和密码，即可查看和远程配置 CPE。

3、 CPE 基本配置

SDWAN 的其中一个核心功能是统一配置管理，即通过控制器统一管理所有的 CPE 设备，因此我们可以通过控制器下发配置给用户侧 CPE，来修改 CPE LAN 侧信息，例如 IP 地址、DHCP、路由、QOS 等等。控制器在上电后通过网络接入控制器，所有的配置均可以由控制器来处理。

CPE 的配置在控制器的“配置”->“接入”->“CPE”页面中，如下图所示：

3.1 CPE LAN 配置

1 在主菜单中选择“**配置 > CPE**”，打开 CPE 配置面板，选择需要配置的 CPE，点击“**编辑设备**”；

图 17

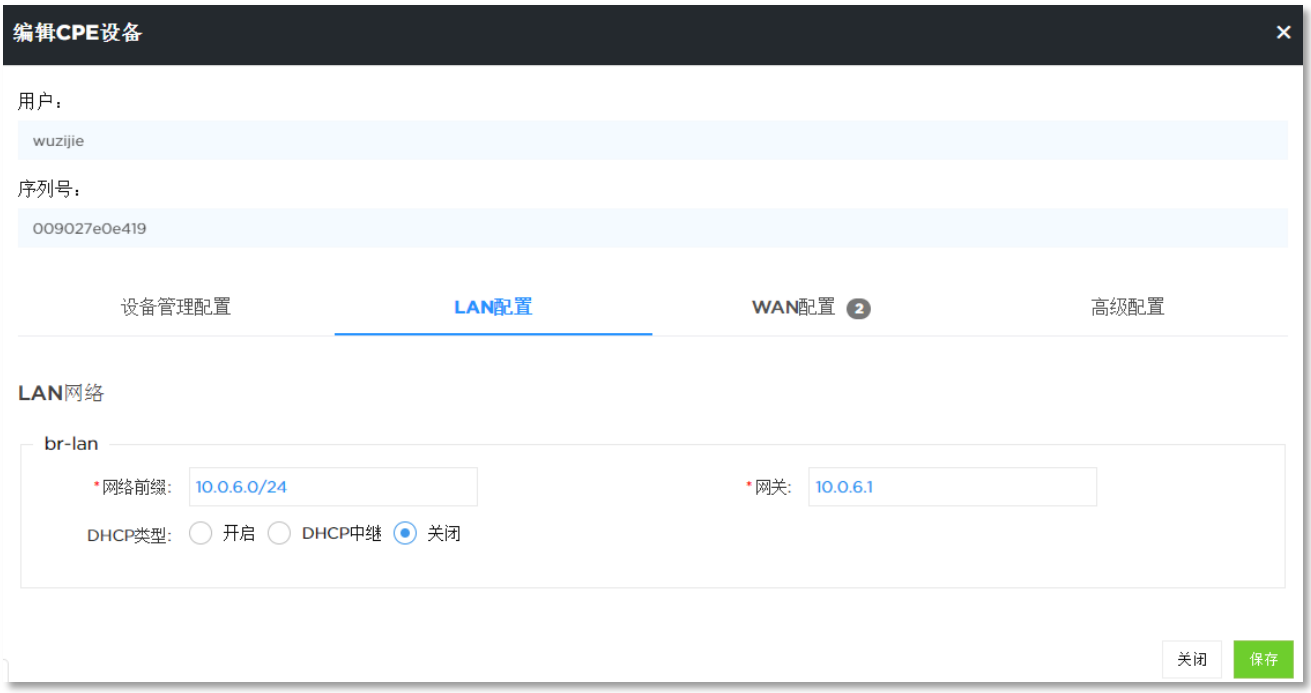
2 在 LAN 配置选项卡中，填写 IP 地址信息；

- **网络前缀**：CPE LAN 口子网号
- **网关**：CPE LAN 口的 IP 地址
- **DHCP**：开启动态主机配置协议

LAN IP 地址修改的操作说明：

a) CPE 通常有多个 LAN 物理接口，所有的 LAN 物理接口属于同一个名为 br-lan 的三层接口，因此本操作实质上是修改 br-lan 接口的 IP 地址；

b）默认情况下，当 CPE 第一次连接 VPE 后，控制器会为每个 CPE 下发一个随机且不和其它 CPE 冲突的子网，长度为/24，同时会把该子网的首个可用 IP 地址作为 CPE LAN 口的 IP 地址。（用户也可以通过主菜单“**配置 > 全局配置**”进行全局设置，指定一个地址池，指定后控制器会按照地址池为每个 CPE 分配 LAN 的 IP 地址）



3.2 CPE WAN 口配置

1 在主菜单中选择“配置 > CPE”，打开 CPE 配置面板，选择需要配置的 CPE，点击“编辑设备”，点击 WAN 配置选项；

注意：如果只有一条 WAN 链路，请谨慎修改 CPE 的 WAN IP，如果修改完成后 CPE 无法连接控制器，会造成该站点的网络中断。

✧ **优先级：**

作用：用来控制流量的转发接口；

描述：如果有多个 WAN 口，流量通过较低优先级的接口转发，如果优先级一致，则流量通过两个接口转发。

✧ **权重：**

作用：用来控制接口转发流量的比重；

描述：在优先级一致的情况下，可以配置指定 WAN 口承载流量的比重，比如 eth0 口链路的带宽是 100Mbps，而 eth1 口带宽是 10Mbps，则可以把 eth0 的权重配成 100，eth1 的权重配置成 10。

✧ **跟踪 IP：**

作用：用来判断 WAN 链路的可用性；

描述：配置跟踪 IP 后，如果该接口在 3 次“跟踪检查间隔内”无法 ping 通“跟踪 IP”，则认为该线路中断。

✧ **开启 NAT：**

作用：对去往 internet 的流量执行 NAT；

描述：去往 internet 的流量数据包，源 IP 地址将被转换成为该接口的 IP 地址。

✧ **是否为 4G 接口：**

作用：减少接口的管理流量，节约流量开销；

描述：打开该功能以后，控制器会降低对该接口的检查频率，从而减少流量的开销，与此同时带来的副作用是接口的敏感度和监控颗粒度会变差。

✧ **MTU：**

作用：可以调整 WAN 口的最大传输单元；

描述：当 Internet 上网模式为 adsl 时，需要调整 mtu 为 1492，因为 pppoe 会占 2 层 8 个字节。

✧ **禁用到 POP 的 IPsec 隧道：**

作用：选中后此 WAN 口将不会和 POP 建立 IPsec 隧道；

描述：WAN 口强制不与 POP 建立 IPsec 隧道，如果是双 WAN 的 CPE,可以实现 WAN1 走 Internet，WAN2 建立 IPsec 走隧道流量。

✧ **接入类型：**

作用：控制 CPE-VPE 的连接类型，三种模式可以选择（IPsec，GRE 专线和其它专线）；

描述：

a) IPSec 模式（**默认模式**），CPE-VPE 采用 GRE over IPsec 的方式连接，链路通过 AES 算法进行加密；

b) GRE 专线模式，CPE-VPE 采用 GRE 方式连接，CPE-VPE 之间通常是基于三层可达的专线连接；

c) 其它专线模式，CPE-VPE 直接通过 2 层点到点链路连接，比如 LAN，MSTP 或者 SDH 的方式。

3.3 CPE 与用户内网的路由配置

1 编辑 CPE 设备，点击“高级配置”选项，选择“可达网络”，进入 CPE 的路由配置面板；

✧ **LAN 路由通告**（默认开启）：

作用：将 CPE LAN 的路由发布给 SDWAN 骨干网的其它节点；

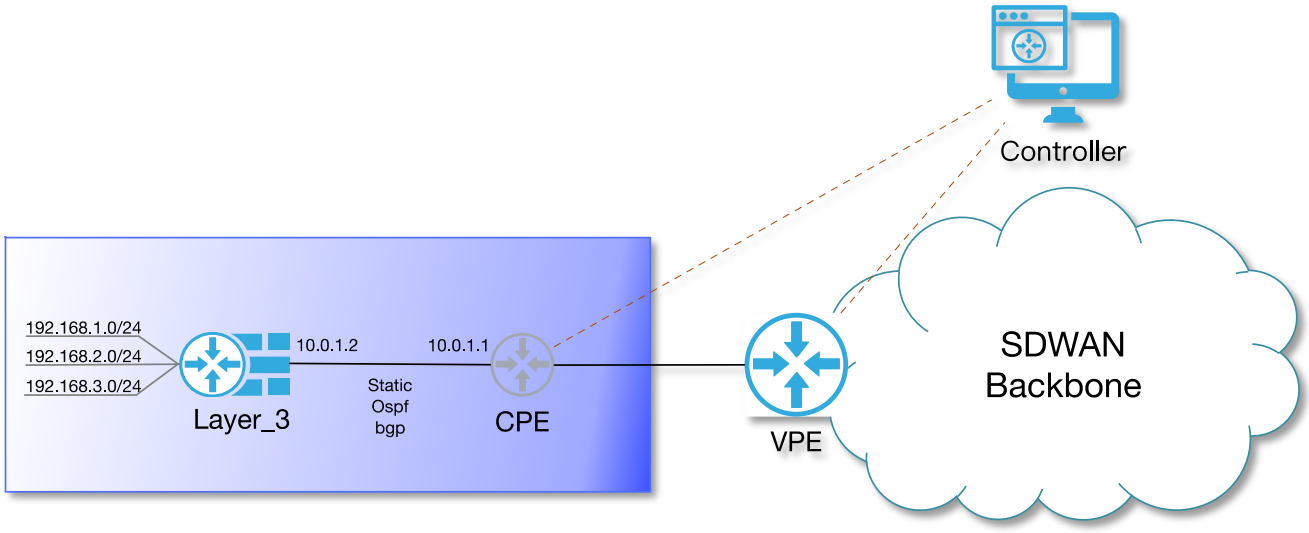
描述：一个客户通常会有多个站点，当站点连接到 SDWAN 以后，CPE 默认会把 LAN 接口所在的子网路由对外发布，以便其它站点能够访问该 CPE 所在的 LAN。同一个用户的多个 CPE 的 LAN 口网段不能重叠。

✧ **WAN 路由通告**（默认关闭）：

作用：将 CPE WAN 的路由发布给 SDWAN 骨干网的其它节点；

描述：在某些极端特殊的情况下，需要将 CPE WAN 接口所在的子网路由发布给其它站点，以便其它站点能否访问位于该 CPE WAN 口子网内的资源，这是一个非常危险且通常不必要的操作，发布以后该 WAN 接口自动关闭 NAT 功能，会导致 CPE LAN 内的设备无法正常访问互联网。

✧ **第三方路由器对接：**



CPE 与客户内网 3 层设备路由对接示意图

作用：CPE 与客户站点的现有内网进行路由对接；

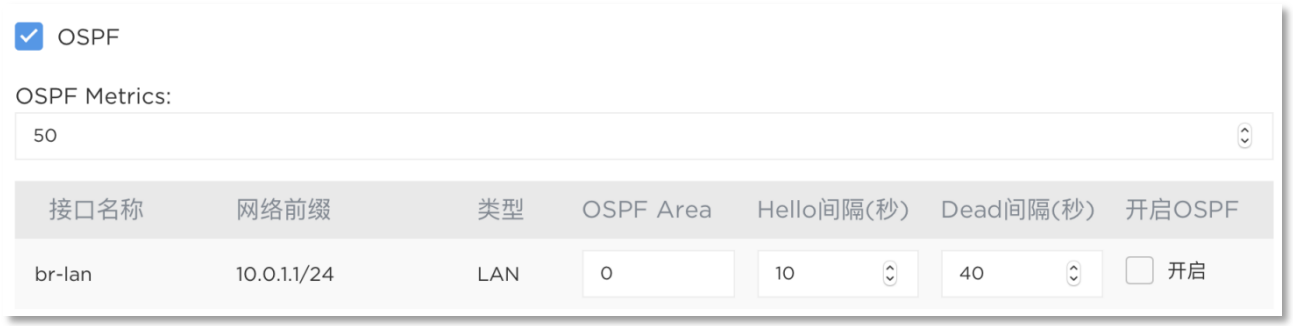
描述：在一些情况下，用户内网并不直接连接 CPE，而是通过一个“网关”设备连接，网关设备可能是路由器、防火墙或者 3 层交换机，此时 CPE 需要和“网关”进行路由对接，SDWAN 目前支持以下的路由方式：

a）静态路由

备注：用户侧内网子网不经常改变的情况下，建议使用静态路由的方式对接

b）OSPF 动态路由

备注：OSPF 属于动态路由协议，配置简单但机制复杂，如果用户内网的子网经常改变，且用户对路由协议有深刻的理解，则可以使用该功能与内网做网路由对接



c）BGP 动态路由

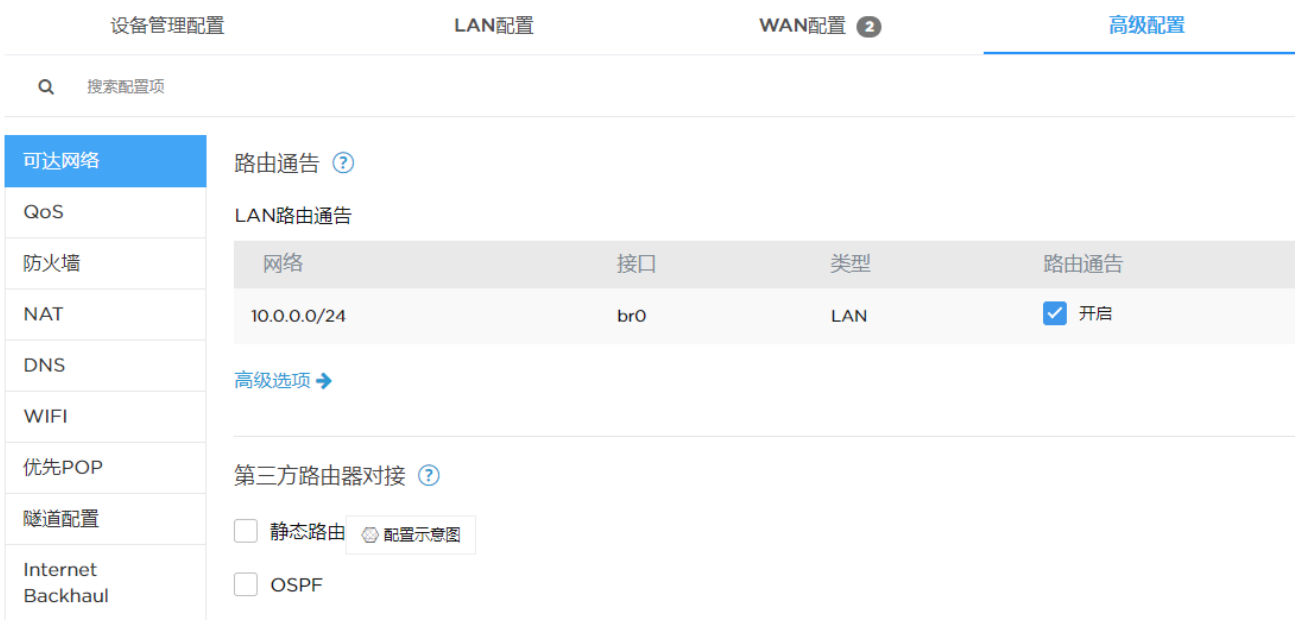
3.4 标识 CPE 设备

1、在“编辑设备”的选项卡中，设备名称可以给设备起个别名，自定义排序，填写数字越大，版面上越靠上；

4 、CPE 高级功能配置

高级功能是 SDWAN 最核心的部分，它使 SDWAN 有区别于传统的 MSTP 和 MPLS VPN 专网，通过使用这些高级功能，用户可以灵活的控制网络流量。

CPE 高级配置在 CPE 列表中选中一个目标 CPE，点击“编辑 CPE”，在页面中切换到“高级配置”页面，如下图所示：



4.1 应用定义

4.1.1 应用定义功能介绍

- ✧ 作用：对指定的网络流量，通过五元组规则，即基于源 IP 地址，源端口，目的 IP 地址，目的端口，和传输层协议这 5 个元素的组合，进行流量分类；
- ✧ 描述：应用定义是所有高级功能的基础，比如定义了视频、语音、ERP 等应用，就可以根据应用部署高级功能，如 QOS、防火墙、负载均衡和链路优化等。

4.1.2 应用定义的配置

假设把所有分公司 172.20.0.0/16 去往 DC，访问 10.0.0.100 这台视频服务器的流量单独分类出来，可以通过如下操作完成。

1 在主菜单中选择在“配置 > 用户配置 > 应用定义”，去增加一种应用分类；

2 选择“应用定义”选项卡下面添加新的应用；

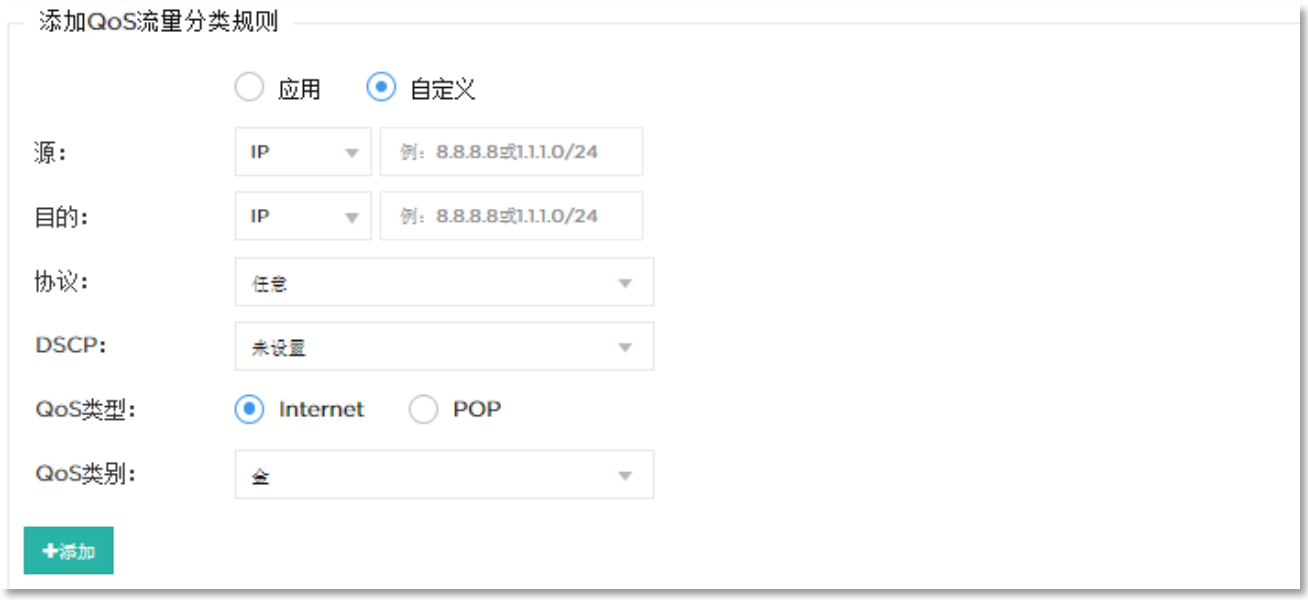
3 输入应用名称，通过五元组匹配应用。

4.2QOS 策略配置

1 在编辑设备的选项卡中，点击“高级配置”选项，选择“QOS”，进入 CPE 的 QOS 配置面板；

2 在 QOS 配置面板中，定义流量分类规则；

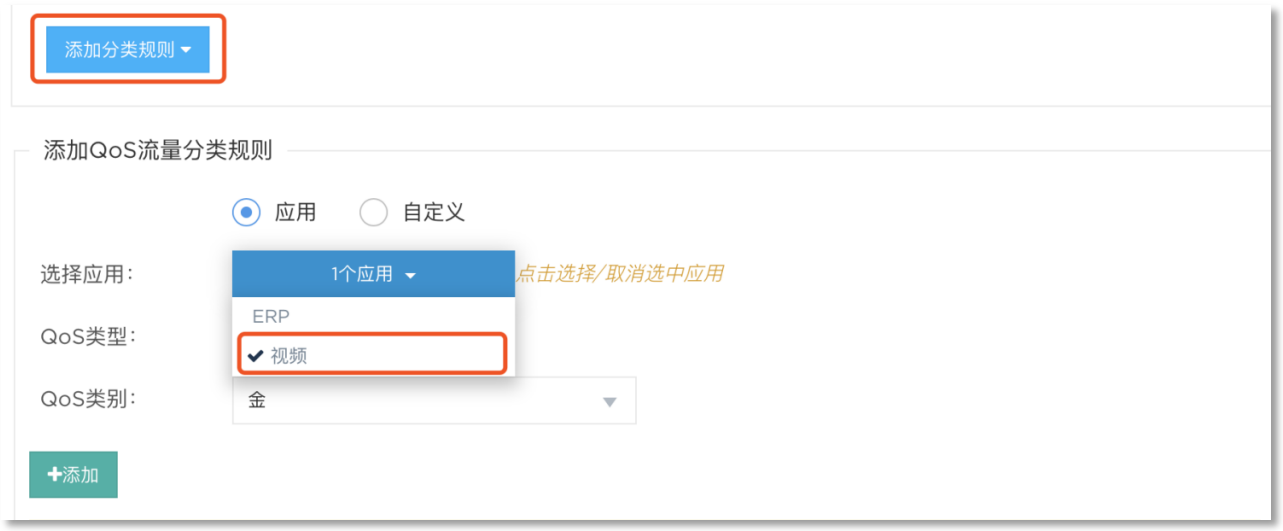
流量分类的规则可以读取预先定义的“应用”，或者通过自定义的方式，通过五元组，即基于源 IP 地址，源端口，目的 IP 地址，目的端口，和传输层协议这 5 个元素的组合，新建一条规则，如下所示；



举例说明：把所有分公司 172.20.0.0/16 去往 DC，访问 10.0.0.100 这台视频服务器的流量单独分类出来，可以通过以下 2 种方式完成流量分类：

- ✧ **基于应用定义分类**
- ✧ **新建五元组规则分类**

a)采用应用定义分类的方式，定义好应用以后，回到 QOS 配置面板，点击添加“分类规则”，在选择应用的下拉列表中，选择刚刚建立的应用，并指定相应的 QOS 级别“金”。

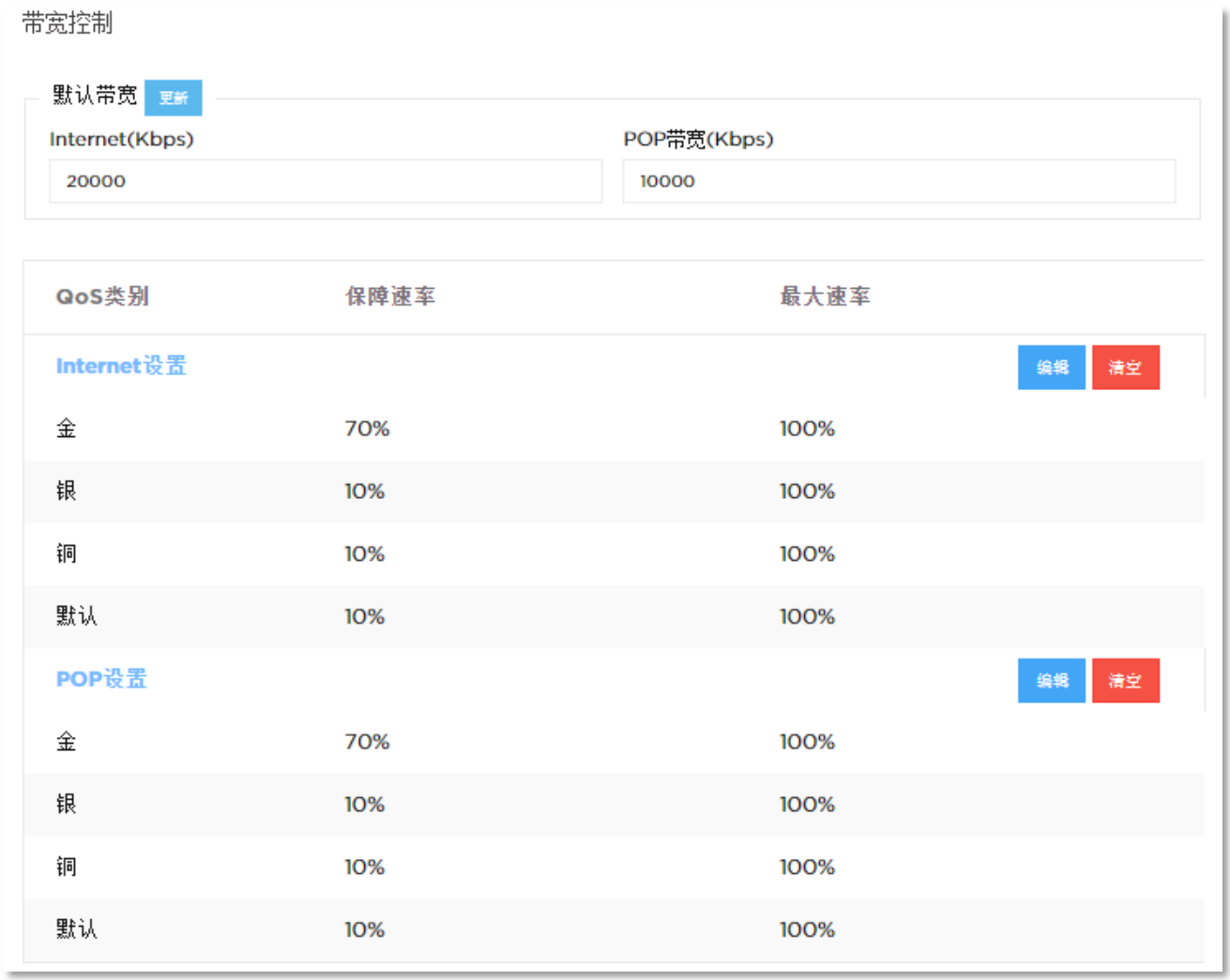


QOS 类型：可以指定去互联网的流量或者是去 SDWAN POP 的流量；

QOS 类别：可指定金、银、铜三个级别中的一种，不指定则为默认；

点击“添加”按钮之后，则将定义的“视频”应用划分到“金”这个 QOS 级别。

b) 在 QOS 的带宽控制面板下，为 QOS 通道划分带宽比例，其中 Internet 带宽总容量由用户自己根据实际情况填写，而 POP 带宽总容量由 SDWAN 根据订单分配。



4.3CPE 防火墙功能配置

4.3.1 防火墙

- ✧ 作用：防火墙基于五元组规则，即基于源 IP 地址，源端口，目的 IP 地址，目的端口，和传输层协议这 5 个元素的组合，在 CPE 上控制 Inbound 和 Outbound 的数据转发；
- ✧ 说明：使用 SDWAN 组网后，默认会把各地站点通过 3 层网络实现互通互访。在一些情况下，为了数据的安全，需要对访问权限做一些限制。此时我们可以通过包过滤防火墙规则去控制。

注意：SDWAN 的防火墙也可以配置模板或者单个 CPE 配置，应用了配置模板后则使用配置模板中的策略，单个 CPE 的配置不再生效。

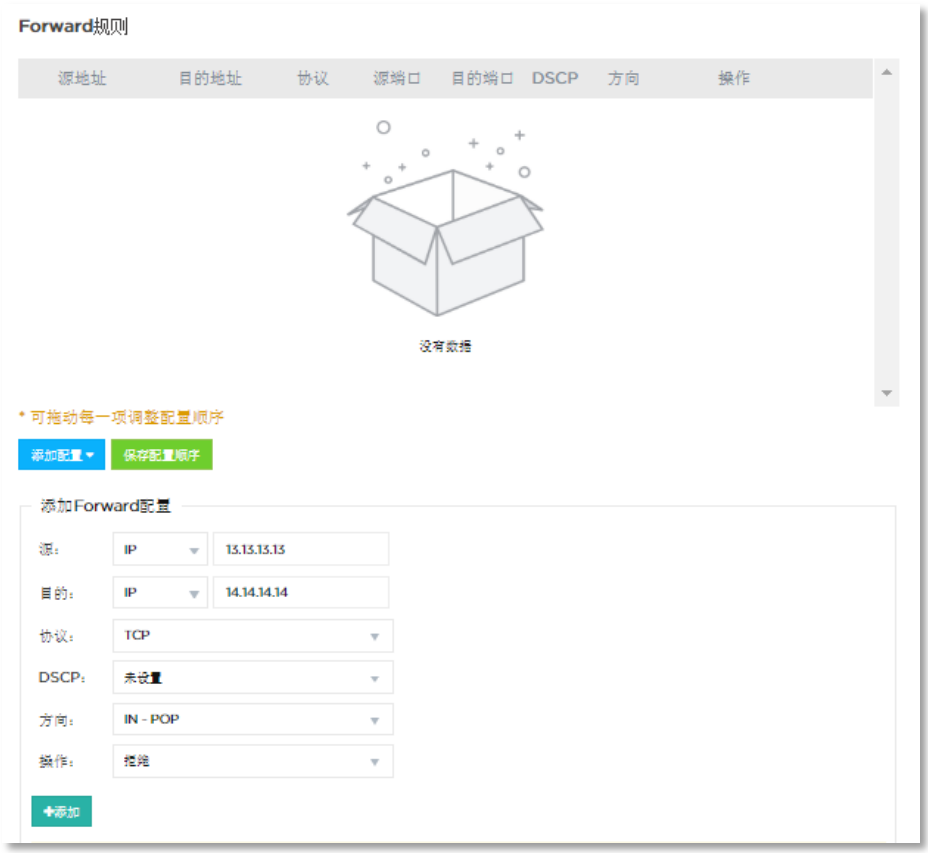
✧ Forward：针对经由 CPE 转发的流量，方向可以是 POP 的 IN/OUT 或则 Internet 的 IN/OUT；

✧ Input：只针对到 CPE 本身的流量，方向只能是 Internet 的 IN 方向。

4.3.2 基于单 CPE 的防火墙配置

1 在编辑设备的选项卡中，点击“高级配置”选项，选择“防火墙”，进入 CPE 的防火墙配置面板；

2 在 Forward 规则下点击添加配置按钮，写入五元组信息后点击添加按钮完成操作。



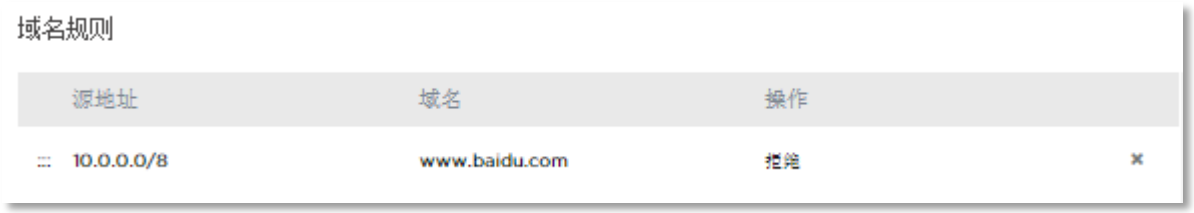
4.3.3 URL 防火墙

- ✧ 作用：URL 防火墙基于域名规则，即基于域（例如 qq.com）或者域名(例如 www.qq.com)，在 CPE 上控制 DNS 解析来实现访问控制；
- ✧ 说明：使用 SDWAN 组网后，站点除了去往数据中心的专网流量，您也许也想让一些分支机构站点通过 CPE 去访问互联网，同时希望能实现 WEB 的访问控制，比如禁止用户通过公司互联网访问视频网站 youku.com，此时我们可以通过域名防火墙去控制。

注意：CPE 后面的 Host 必须用 CPE 的 Lan 口 IP 作为 DNS，否则此功能不生效。

4.3.4 URL 防火墙配置

1 在防火墙配置，域名规则下点击添加配置按钮，写入 URL 信息后点击添加按钮完成操作。



4.4NAT 功能

4.4.1 DNAT 规则

✧ 作用：目的地址转换，可以是一对一，也可以多对多；

✧ 说明：当 CPE 的 LAN 内有应用要对外发布（对 Internet/POP 皆可）可使用此功能。

4.4.2 DNAT 配置

1 在 NAT 配置，DNAT 规则下点击添加配置按钮，映射关系信息后点击添加按钮完成操作。

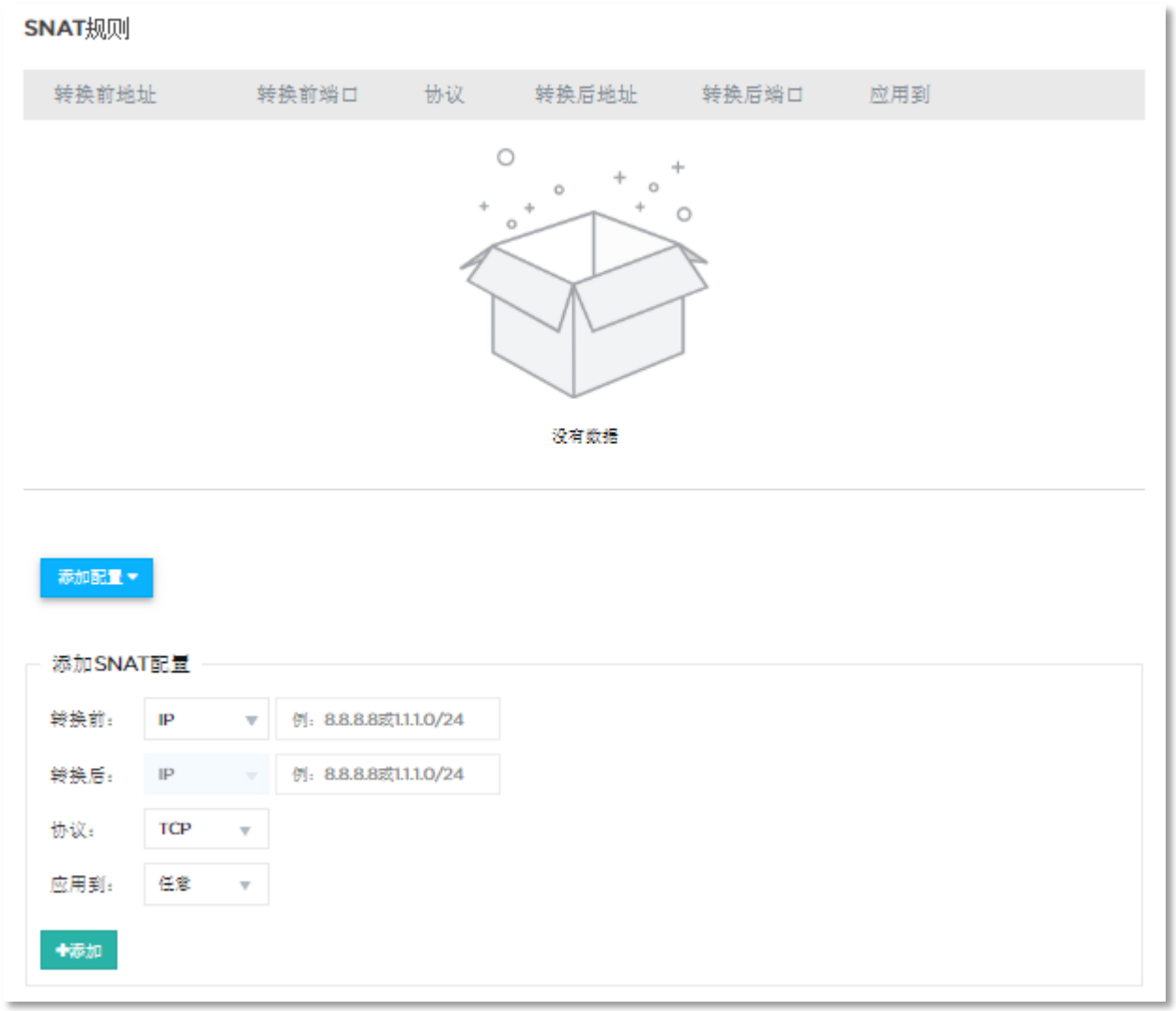
4.4.3 SNAT 规则

✧ 作用：原地址转换，可以是一对一，也可以多对多；

✧ 说明：当全局网络中存在 IP 地址段冲突可使用此功能。

4.4.4 SNAT 配置

1 在 NAT 配置，SNAT 规则下点击添加配置按钮，映射关系信息后点击添加按钮完成操作。



4.5优选 POP

✧ 作用：指定某些 POP 作为优选节点；

✧ 说明：不指定 POP 会从所有 POP 中选择接入链路质量最好的建立 IPsec。

1 在优选 POP 下选择指定接入的 POP 点，通过优先级还可以设定优选次选顺序。

4.6隧道配置

✧ 作用：通过此功能可以修改 VPN 类型（IPsec/OPENVPN）和端口号；

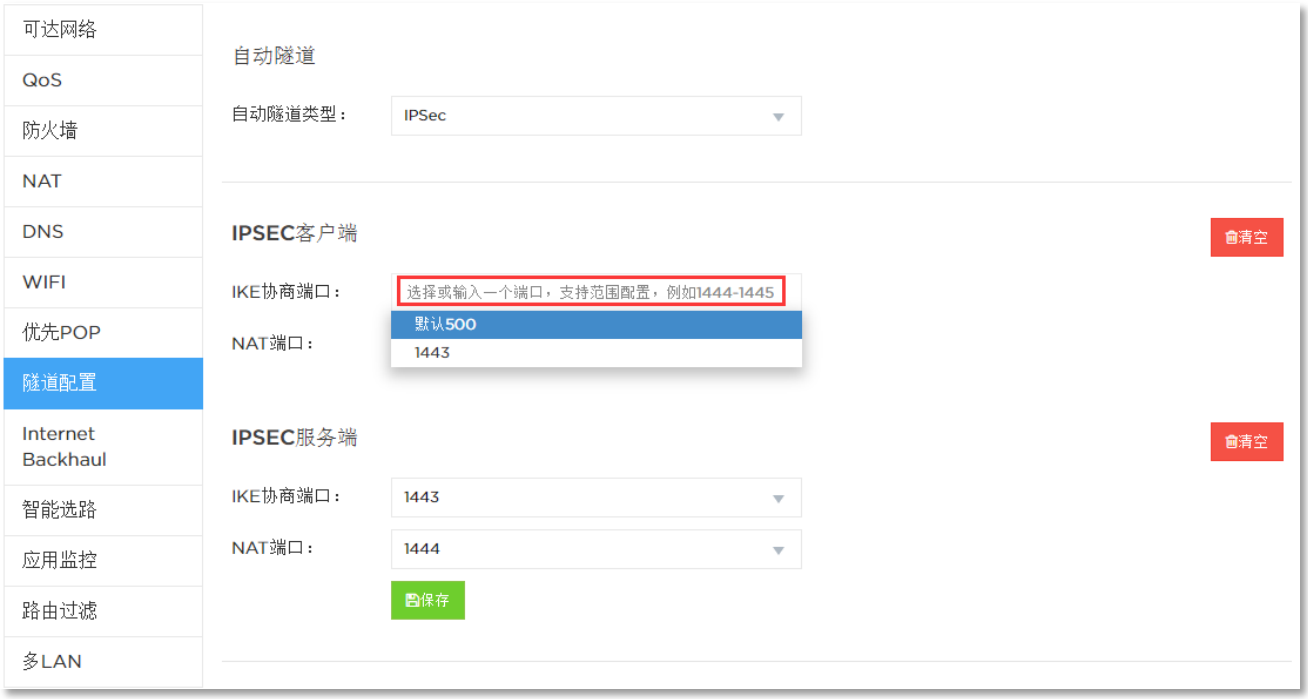
✧ 说明：IPsec 客户端端口指 CPE 发出的原端口，可以是**一个或者一段范围**的端口；

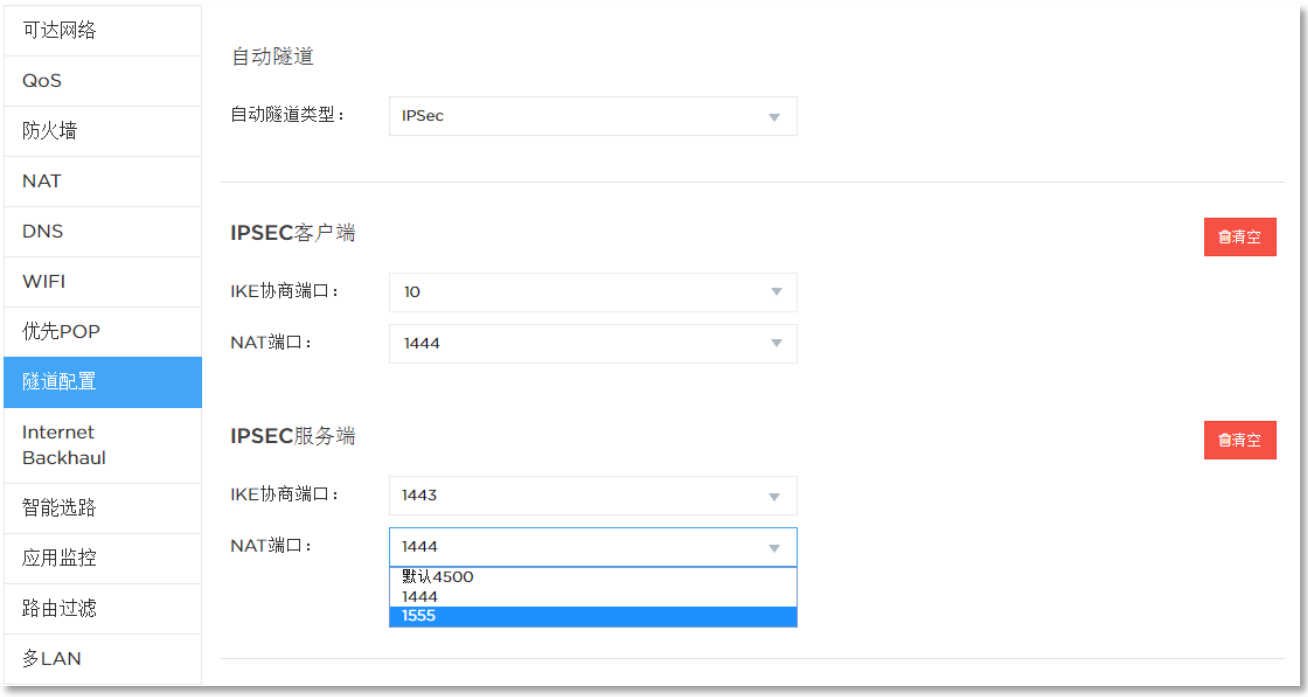
IPsec 服务端端口指 VPE 的接收端口；IKE 协商端口和数据传输端口默认分别为 1443 和 1444；

IPsec 端口可以针对单个 CPE 配置，也可以在全局配置下发所有 CPE，在单个 CPE 上的配置优先于全局配置。

4.6.1 IPsec 端口配置

1 在 CPE 设备编辑，隧道配置下配置 IPsec 端口，IPsec 客户端可以一个或者一段范围的端口，IPsec 服务端端口可以选择之前在系统管理中定义过的端口；





3 全局下也可以进行配置，“配置 > 全局配置”；

4.6.2 OPENVPN 配置

1 在 CPE 设备编辑，隧道配置中可切换 VPE 类型，IPsec/OPENVPN。

4.7 Internet Backhaul

✧ 作用：此功能开启后会，其他站点上网的流量将会从此 CPE 出口出去；

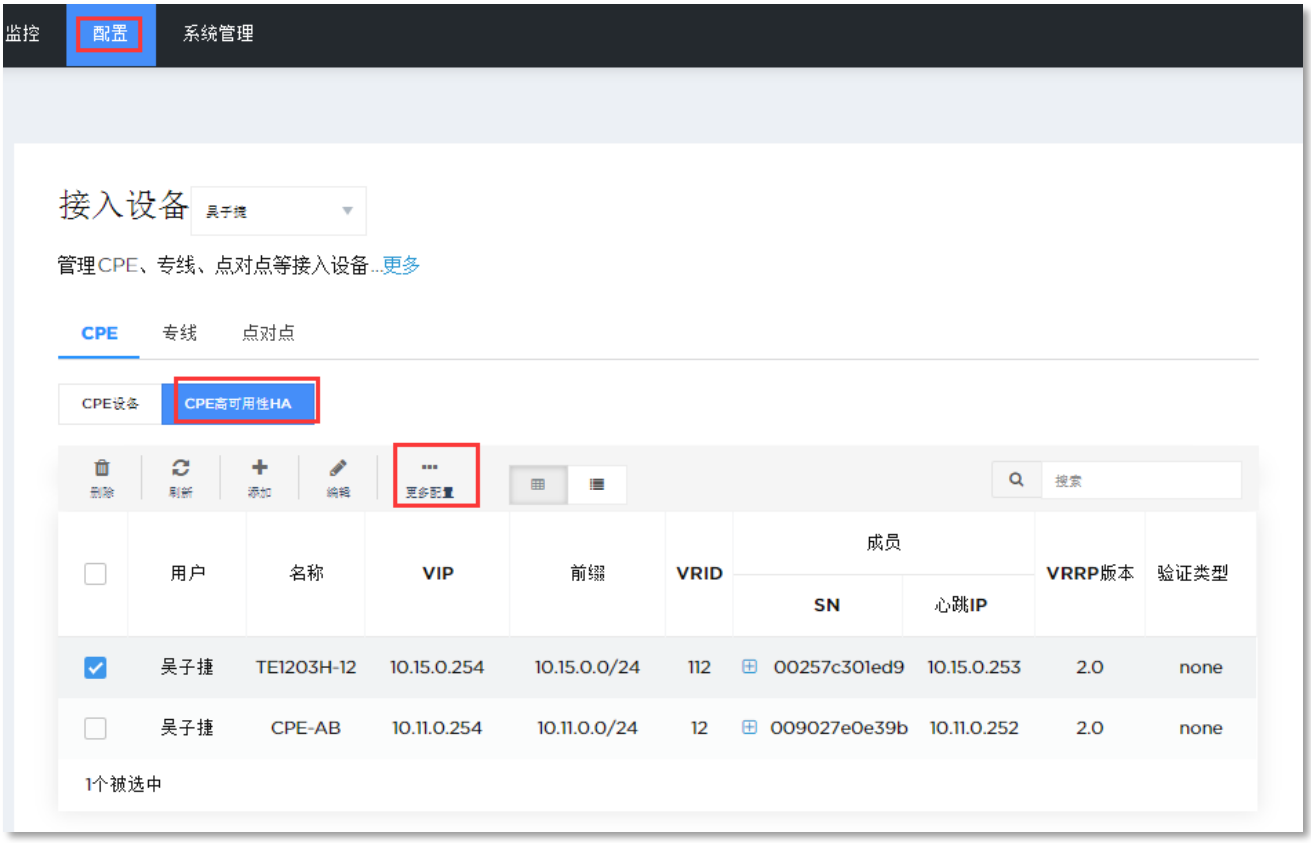
✧ 说明：此功能开启后 CPE 会发出由两条路由组成的默认路由 0.0.0.0/1 & 128.0.0.0/1；

如有特殊目标 IP 依然想从本地 Internet 出去访问，在**可达网络**中的**本地互联网路由**里进行添加。

注意：Internet Backhaul 可以在两个地方开启，CPE 本地或者 CPE 高可用 HA 配置面板。

1 CPE 在 Internet Backhaul 中打开即可；

2 如果是高可用 HA 模式，则需要在 HA 模式下开启；“配置 > CPE 高可用性 HA > 更多配置”；



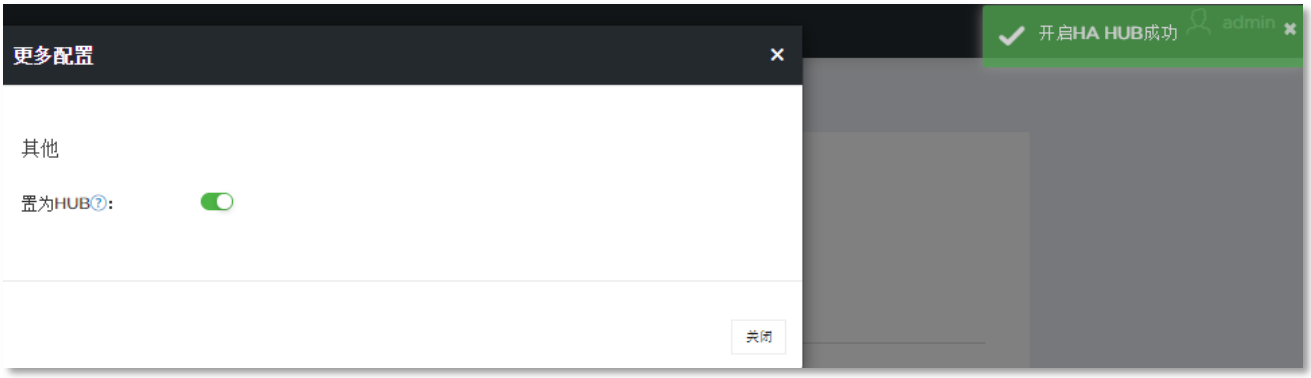


图 54

3 如有特殊目标 IP 依然想从本地 Internet 出去访问，在可达网络中的本地互联网路由里进行添加，可以匹配目的 IP，也可以匹配源 IP。

4.8配置模板

✧ 作用：生成配置模板，把需要相同配置的 CPE 与之关联，可继承模板里的配置策略，以提高配置部署效率；

✧ 说明：一些高级的功能必须在有配置模板的前提下才能使用，配置模板也是 3.0 版本最为推荐的配置方式。

配置模板中可以使用的高级功能如下：

a）可以调用多条专线，不用配置模板只能调用一条专线；

b）自定义 PPPOE 重新拨号时间，可以在凌晨设置一个重拨，避免在工作时间发生重拨导致隧道重建影响业务；

c）路由策略，app 选路，ECMP；

d）安全组策略

4.8.1 创建配置模板

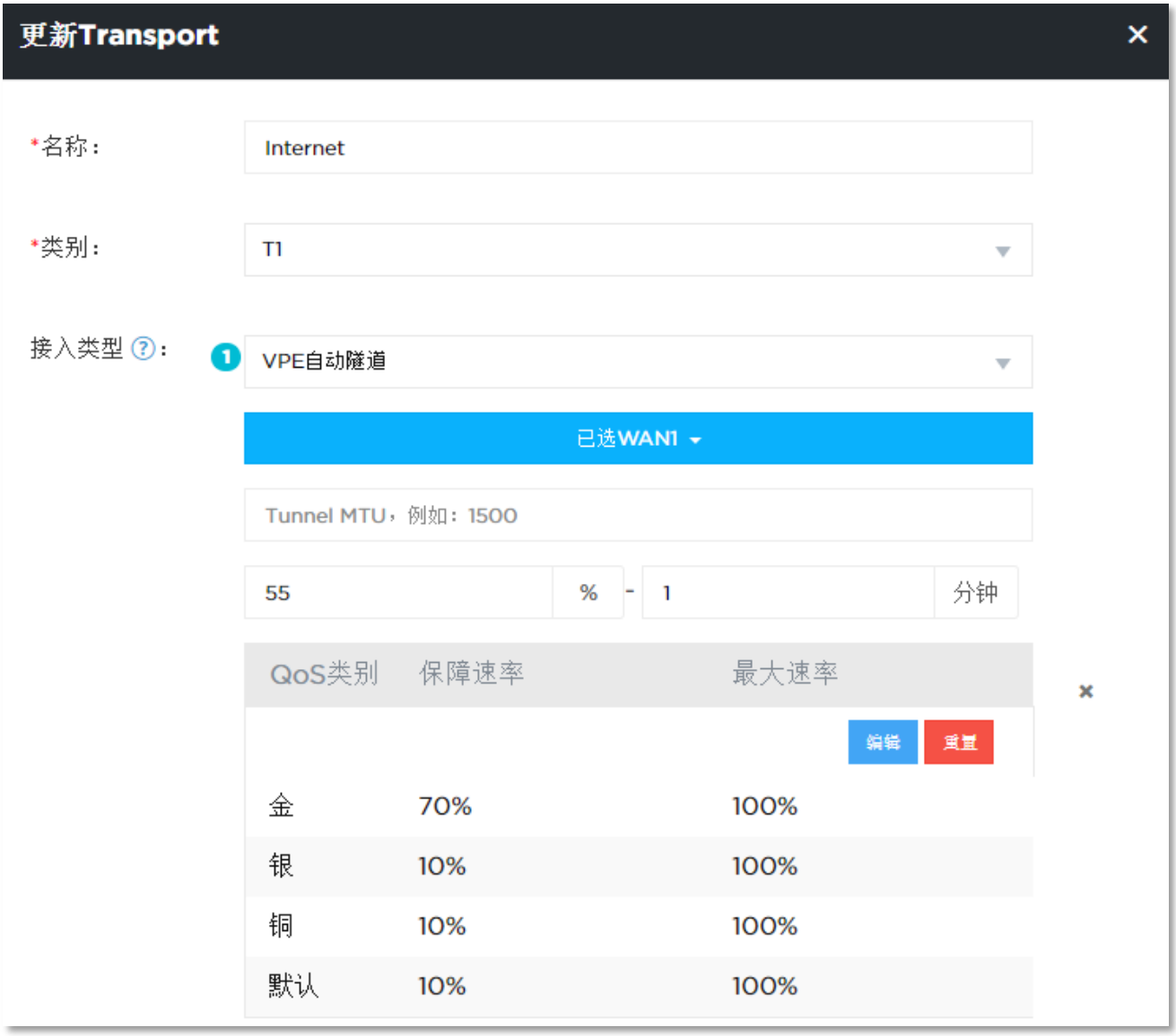
1 进入如下菜单“配置 > 配置模板 > 添加”；

2 可以给配置模板起个名称，并添加一个描述；

3 在策略中，必须创建 transport 才能保存配置模板，这里可以创建一个“T1”的 Transport，使用 IPsec VPE 的接入类型，关联 WAN1；

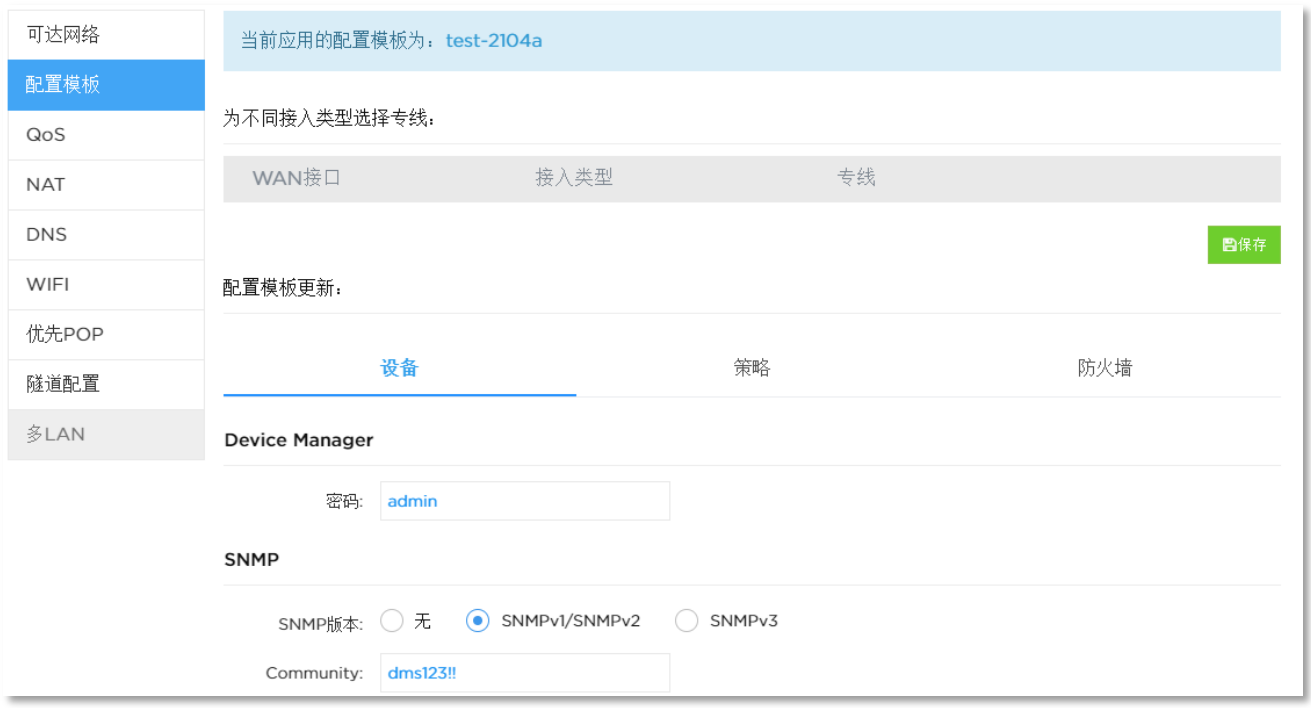
注意：VPE 自动隧道只能属于一个 Transport，且可以关联多个 WAN 口。


更新配置模板
基本信息
配置模板名称:
test-2104a
描述:
设备
策略
防火墙
流量分类
自定义规则:
源地址
目的地址
协议
源端口
目的端口
QoS类别
DSCP
类型
应用规则:
应用
QoS类别
类型
app0
pop
pop
添加分类规则
Transport
名称
类别
接入类型
Internet
Internet
VPE自动隧道
点对点IPSec隧道
Direct
无


更新Transport
*名称：
Internet
*类别：
T1
接入类型：
1
VPE自动隧道
已选WAN1
Tunnel MTU，例如：1500
55
%
-
1
分钟
QoS类别
保障速率
最大速率
编辑
重置
金
70%
100%
银
10%
100%
铜
10%
100%
默认
10%
100%

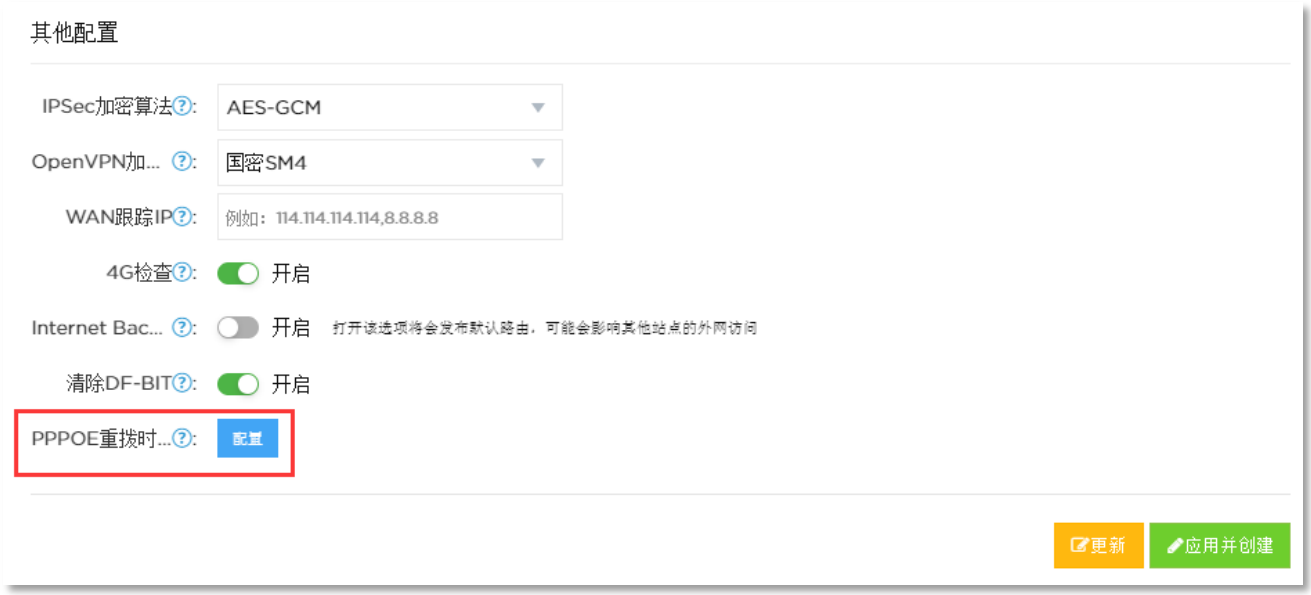
4 将配置模板与 CPE 管理

5 回到 CPE 编辑版面，选择“高级配置”，会发现原来菜单中的 QOS、防火墙、Internet Backhaul、智能选路、应用监控、路由过滤全都没有了，取而代之的是配置模板；



4.8.2 设置 PPPOE 重拨时间

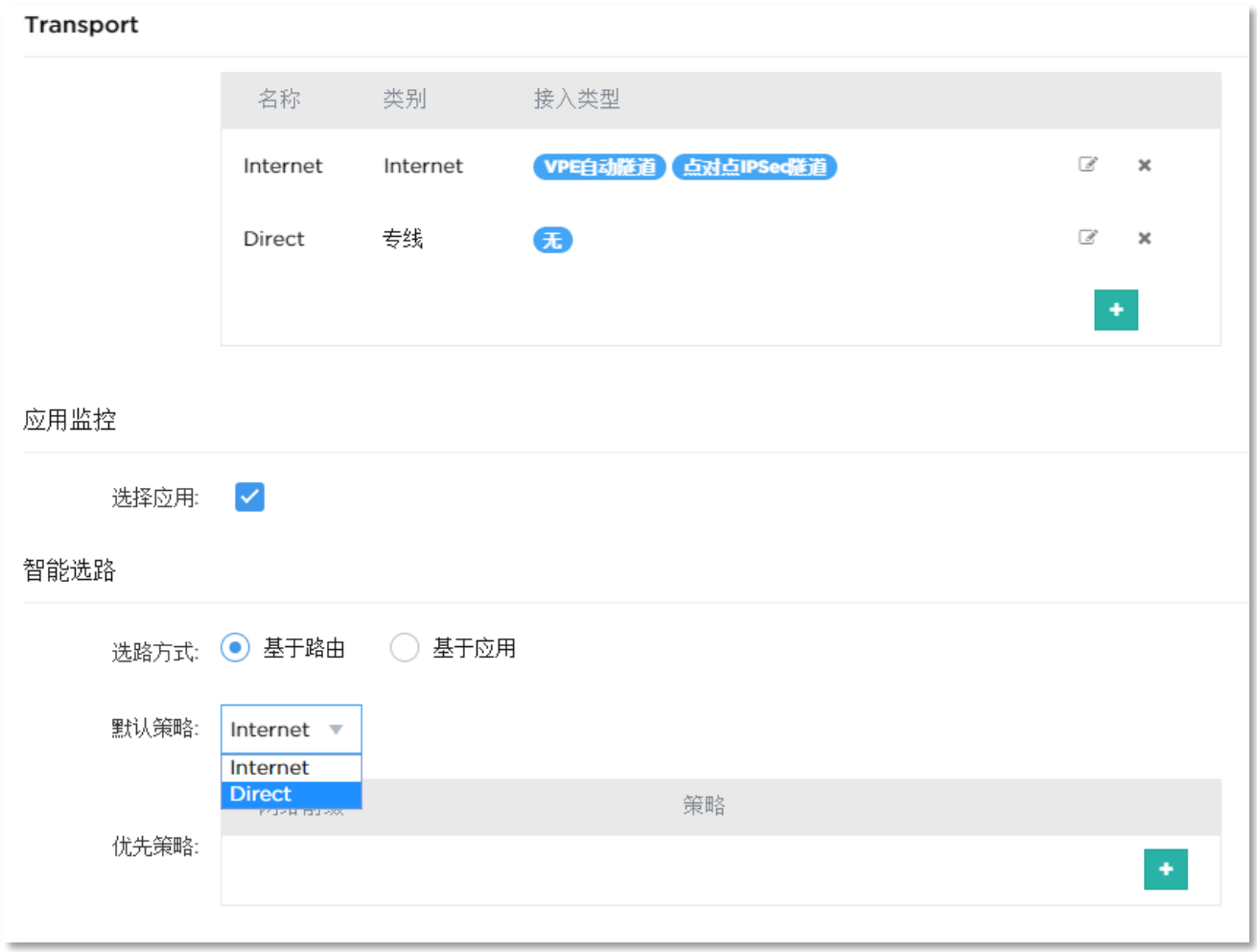
1 在配置模板中设备，其他配置里，设置一个 PPPOE 重拨时间；



2 如果希望每天凌晨 1 点执行，可在“时”这一列选择“1 时”，如果希望每小时的第 10、第 20、第 30 分钟执行，可按住 CRTL 键同时选择 10 分、20 分、30 分。

4.8.3 基于路由的选路

1 在配置模板中“策略”属性页中，智能选路中的默认策略主备模式，如果当前 CPE 是双 WAN，可以选择优先转发的 Transport；



4.8.4 基于应用的选路

1 在配置负载均衡规则之前，需要把流量按照五元组的规则，即基于源 IP 地址，源端口，目的 IP 地址，目的端口，和传输层协议这 5 个元素的组合，先把流量定义成“应用”；

2 定义 Overlay 网络，进入“配置 > 全局配置”；

配置 Overlay 网络会使 CPE 与 CPE 之间直接建立隧道，根据流量模型可以是 fullmesh 也可以是 hubspoke，其他选项还有 ipsec/gre，强制与非强制几种模式。

3 为各个级别 QOS 的应用打上 DSCP 标签，依然在**全局配置**，Overlay 网络下面；

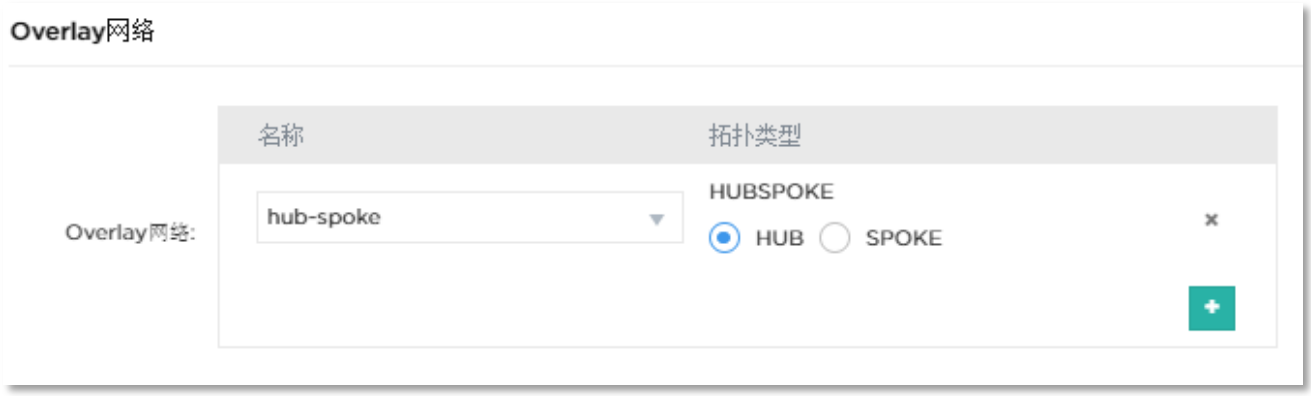
4 在智能选路中选择基于应用；

5 选择需要放入指定链路的应用；

6 故障切换机制可以是“自动切换”或者“不切换”

7 剩余其他应用除了选择另外一个 Transport 以外还可以将流量进行负载分担“ECMP”；

8 调用 Overlay 网络，如果是 HUB & SPOKE 模型，还需要定义角色为 HUB 或者 SPOKE。



4.8.5 路由过滤

✧ 作用：通过路由更新的控制来限制站点间某些网段的访问；

✧ 说明：路由过滤策略可以作用于不同的 Transport 或者本地的 Lan 测，支持 IN/OUT 两个方向；黑名单即表示不收或者不通告，白名单即表示接受或通告，通常的用法是设置大段的黑名单，再设置白名单允许某些特殊网段。

注意：14.14.14.0/24 表示‘14.14.14.0/24 le 32’，如果勾选严格匹配则表示为‘14.14.14.0/24’

4.8.6 路由 Master 模式

✧ 作用：Master 模式可以使 CPE 向 VPE 通告的路由带有更高的优先级；

✧ 说明：Master 模式仅在单个 Transport 前提下使用，开启后将通高优先级更高的路由给 VPE，以实现选路需求。

1 配置模板 Transport 中开启。

4.8.7 安全组

✧ 作用：安全组是一个或多个网段的集合，防火墙中调用安全组可以提高配置效率；

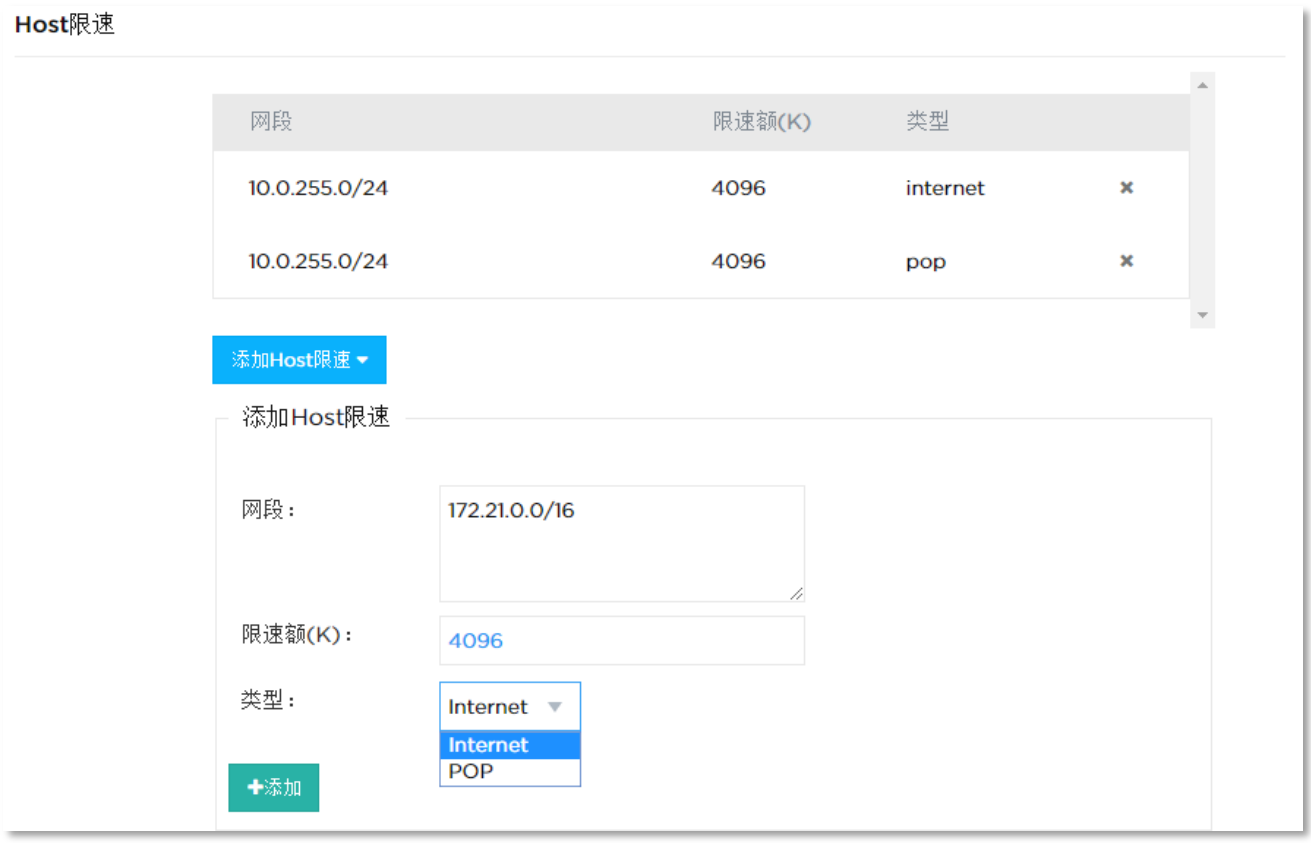
✧ 说明：例如 192.168.1.0/24 192.168.2.0/24，最多一万条。

1 配置模板防火墙中添加安全组。

4.8.8 Per Host Police

- 作用：基于主机 IP 做上下行限速，可以有效控制某个主机占用过多带宽；
- 说明：单臂模式启用此功能的时候要注意不能把自身 WAN 口的 IP 纳入限速的目标 IP 中。

1 配置模板防火墙中添加需要限速的 IP 网段。



4.9CPE-VPE 链路优化

在一些客户的网络环境中，用户最后一公里通过 Internet 的方式接入 SDWAN，由于 Internet 品质不稳定，经常造成延时敏感型应用访问不正常，比如 IP 语音，在丢包率超过 0.5%的情况下通话就有明显的卡顿，链路优化功能可以改善这类情况，功能开启后，CPE-VPE 之间指定的应用会把原始的数据包复制一份副本数据进行传输，从而降低了网络丢包率（仅在 Ipsec 隧道上生效）。

SDWAN 链路优化功能需要在 QOS 功能基础上配置，配置过程分为以下步骤：

1 定义应用

2 将应用绑定 QOS 级别

3 为指定的 QOS 级别开启链路优化功能

开启 QOS 策略后，在 CPE 设备管理中找到链路优化；

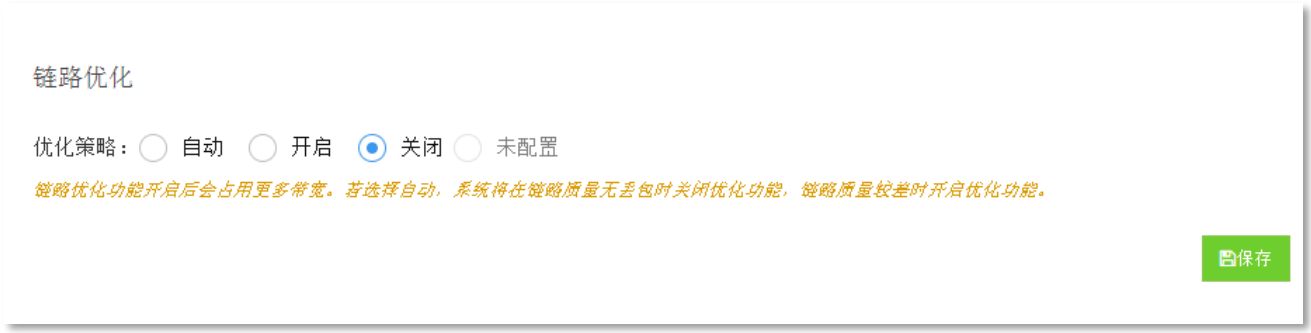


图 84

图 85

优化策略

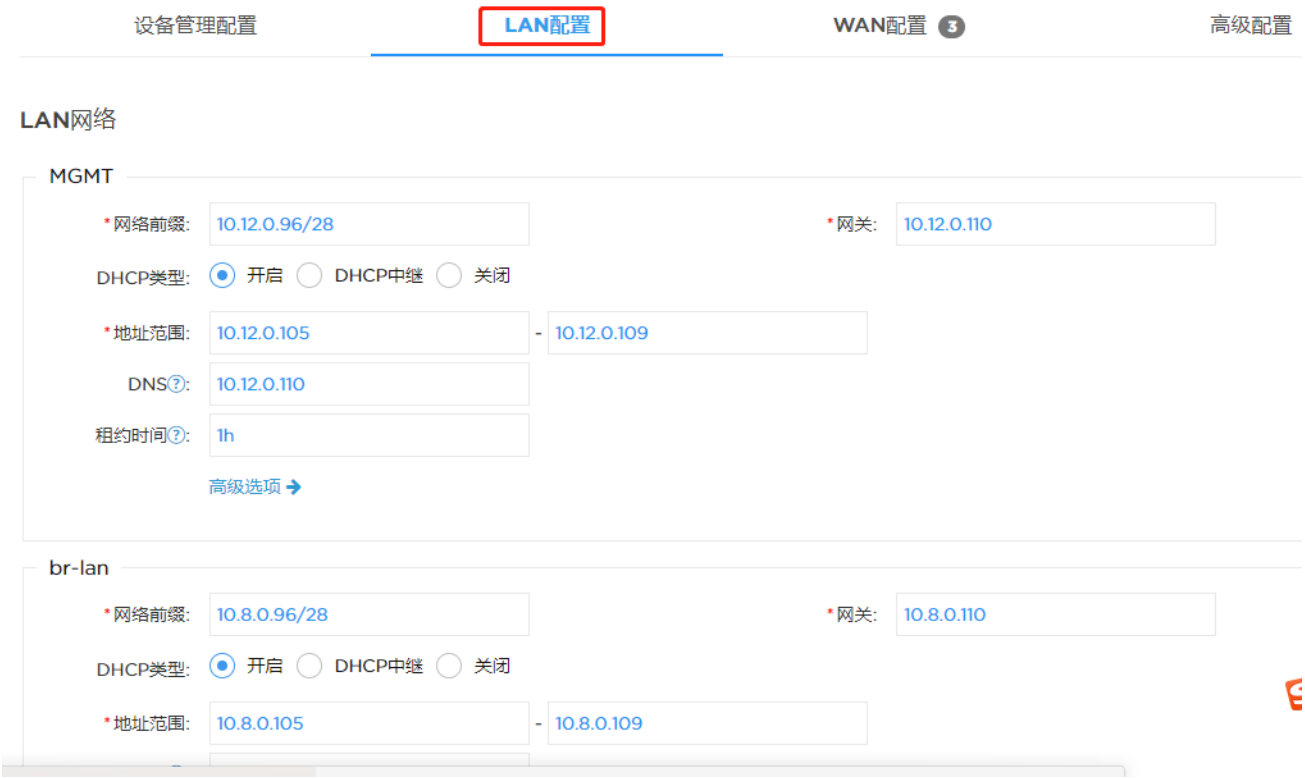
功能：开启（永久开启链路优化），自动（根据链路状态自动开启链路优化）或者关闭（关闭链路优化）

4.10 CPE 多 LAN 配置

CPE 有多个 LAN 口，部分类型的 CPE 支持自由定义逻辑 LAN 口，把不同的物理 LAN 口划归到不同的逻辑 LAN 口，实现分组使用。如划分成管理 LAN 口和传输 LAN 口。

操作如下图：

返回 LAN 配置，可以看到出现了两个逻辑 LAN 网络，根据实际网络需要配置对应的信息。

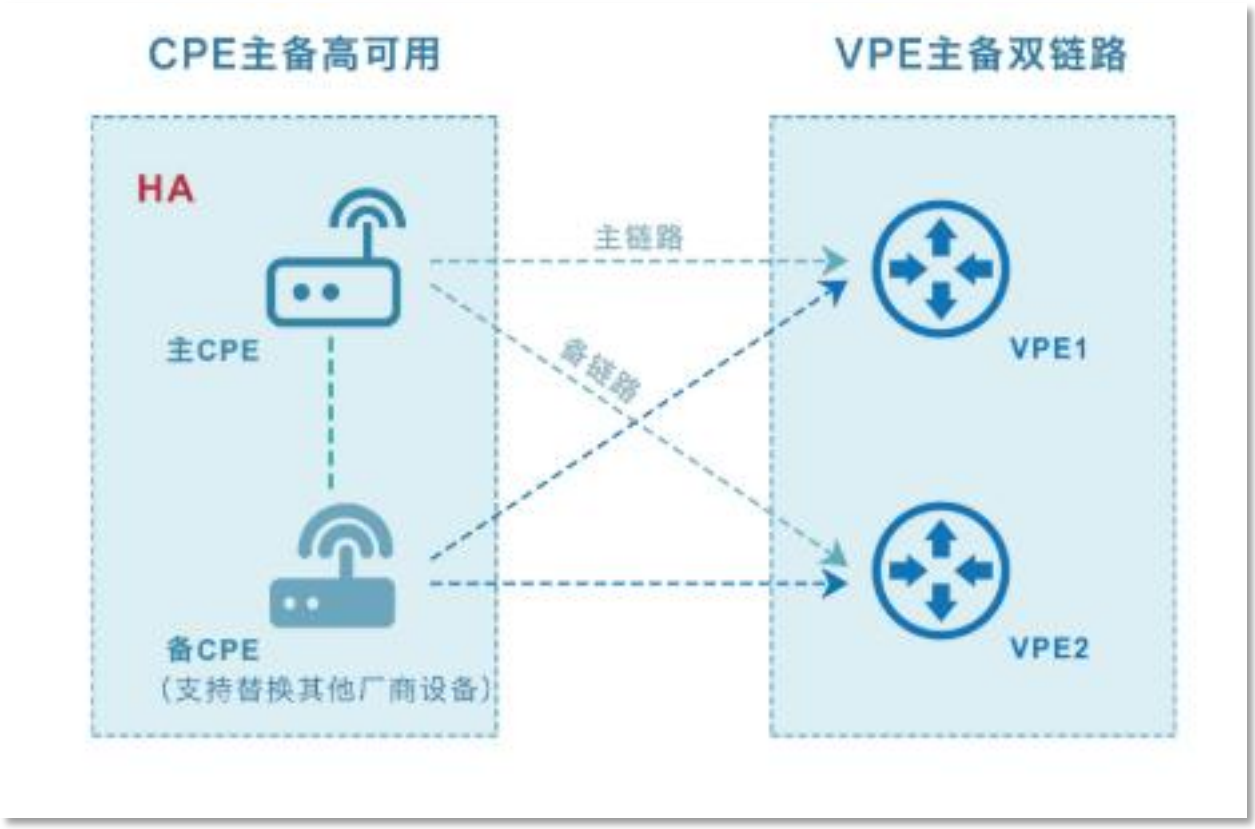


在高级配置中可以看到，LAN 路由通告中出现了对应的两个逻辑 LAN 口。将两个逻辑 LAN 口的路由通告都启用，把路由发布到对端。

5 、CPE 高可用配置（HA）

5.1CPE HA 功能介绍

- ✧ 作用：通过双 CPE 接入 SDWAN，避免设备单点故障
- ✧ 说明：对于一些重要的站点，需要 2 台 CPE 做 HA，当 1 台 CPE 发生故障，另外一台 CPE 能保障网络的正常运行。SDWAN CPE 的 HA 采用标准的 VRRP，将两台 CPE 划分到一个 VRRP 组，对内提供一个 Visual IP 与用户 LAN 对接，对外主备 2 台 CPE 均同时保持与 SDWAN 骨干连接，当出现以下情况，CPE 将发生主备切换：
  - a) 主 CPE WAN 接口 Down
  - b) 主 CPE 无法连接 POP
  - c) 主 CPE 无法联系“跟踪 IP”

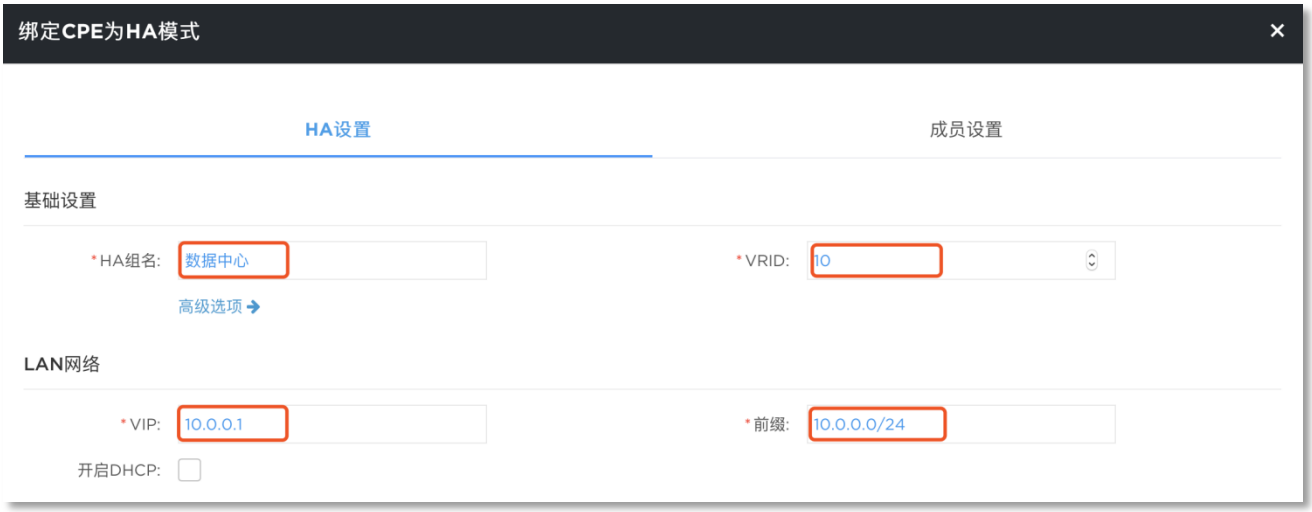


HA 模型示意图

5.2CPE HA 功能配置

1 在主菜单中选择配置 > CPE，打开 CPE 配置面板，选择 CPE 高可用性 HA 选项卡，点击添加打开 HA 配置面板；

2 在 HA 配置面板中，输入 HA 组的配置信息；



✧ **HA 组名**

作用：HA 组的标识

描述：可以是中文或者英文

✧ **VRID**

作用：VRRP 组的唯一标识

描述：数值为 0~255 之间的任意整数，只在本地有意义，不同 VRRP 组之间配置相同的 VRID 不会冲突

✧ **VIP**

作用：VRRP 对 LAN 提供的虚拟 IP 地址

描述：VIP 默认由主 CPE 接管，当主 CPE 故障，则由备份 CPE 接管

✧ **前缀**

作用：确定 VRRP LAN 的子网长度

描述：与接口子网掩码功能类似

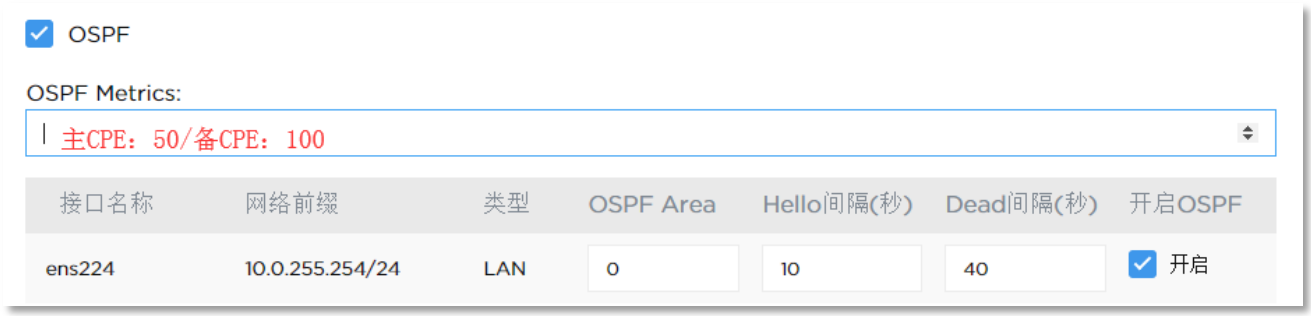
3 在 HA 的**成员设置**面板中，输入 CPE 成员信息后完成配置。

5.3基于路由的主备模式

说明：配置模板中的路由 Master 模式也可以实现主备高可用，配置方式如下

1 主 CPE 配置模板中开启 Master 模式，备 CPE 不要开启，开启方式参考 4.8.7 章节；

2 Lan 侧 OSPF 与客户内网对接，主 CPE 的 OSPF 配置 Metrics 为 50，备为 100。



6 、点对点线路

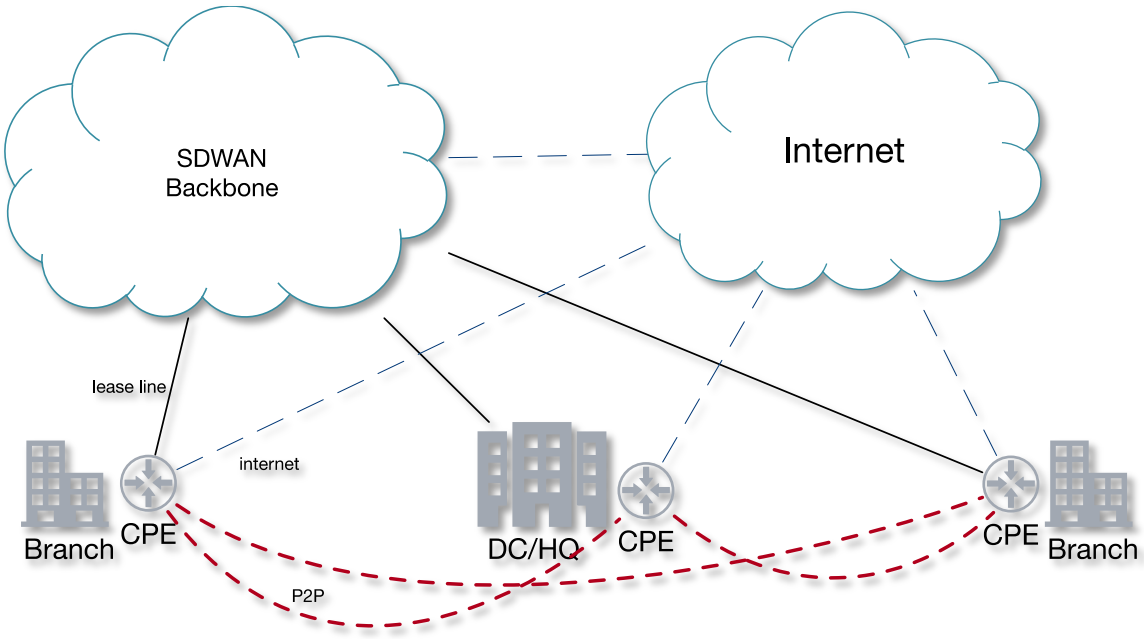
6.1点对点功能介绍

- ✧ 作用：CPE 与 CPE 直接建立 IPsec/GRE 连接，或者基于二层专线直连，不经过 SDWAN 骨干网络；
- ✧ 说明：这种组网有两种模式：FULL MESH / HUB SPOKE

FULL MESH：CPE 与 CPE 全互联模式（此模式不支持 GRE）

HUB SPOKE：找一个 CPE 作为 HUB 点，其他 CPE 与之建立隧道

注意：CPE 与 CPE 点对点建立隧道必须确保至少一端是固定公网 IP 地址。



HA 混合组网模型示意图

6.2CPE P2P 功能配置

1 在主菜单中选择“配置 > 点对点配置”面板，选择好用户之后点击添加打开 P2P 配置面板；

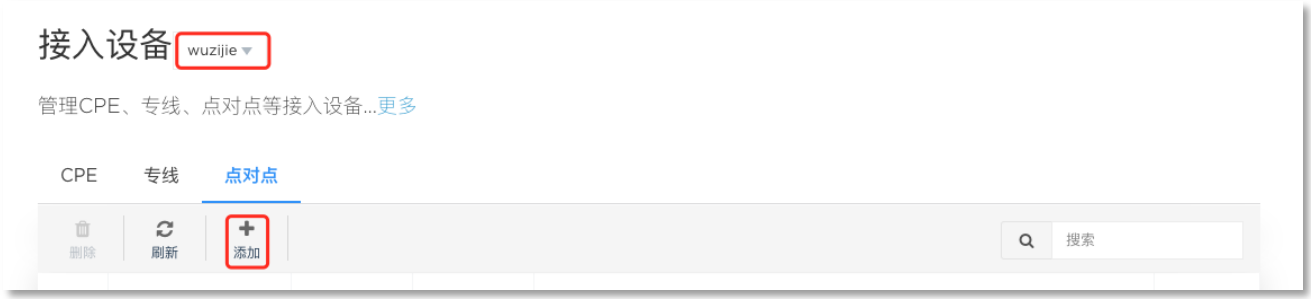
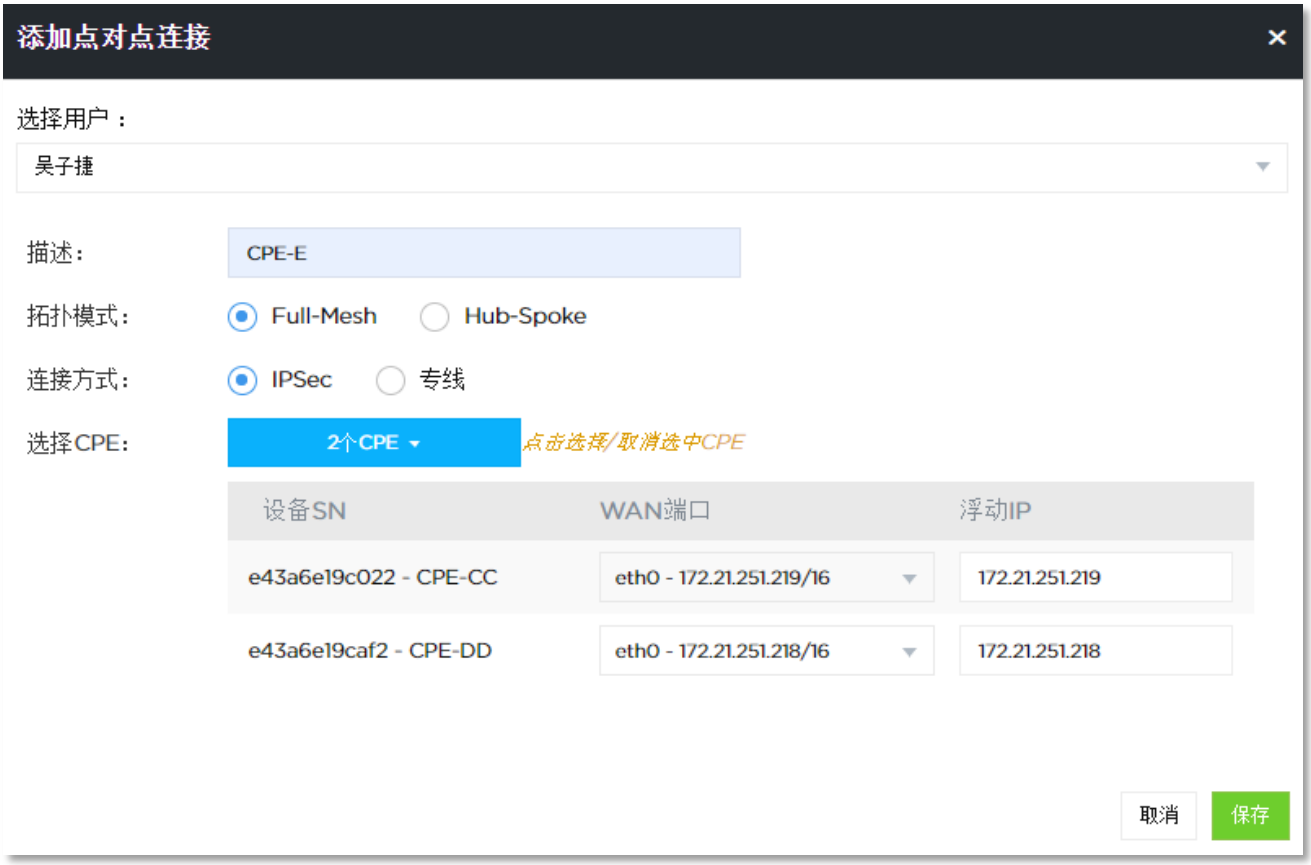
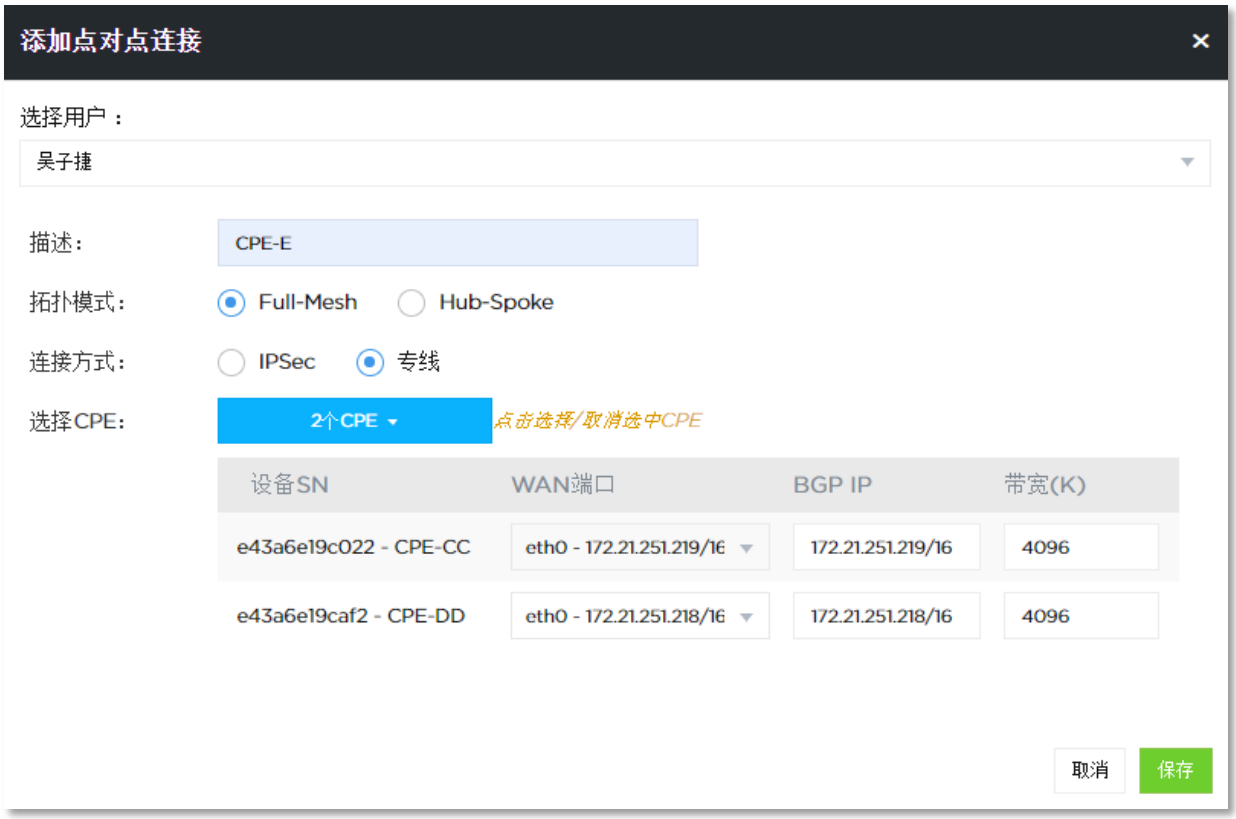
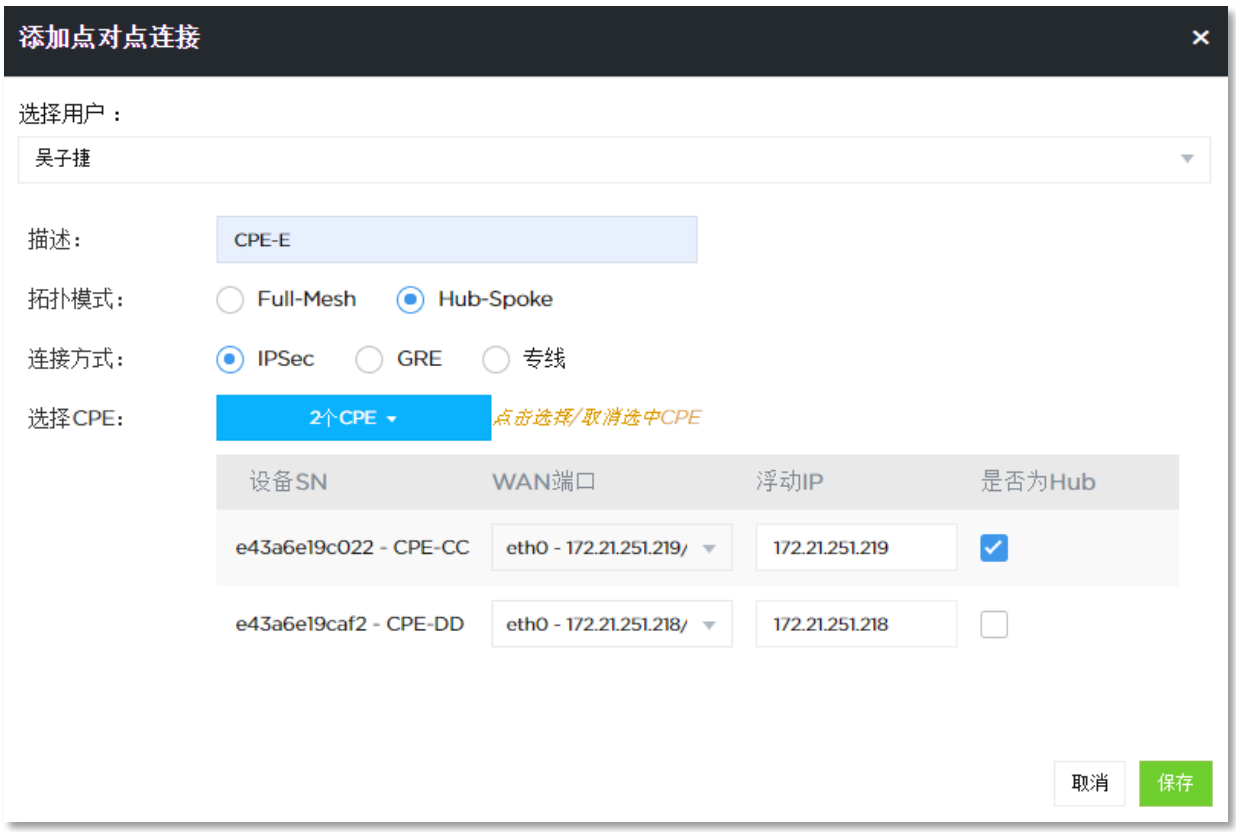


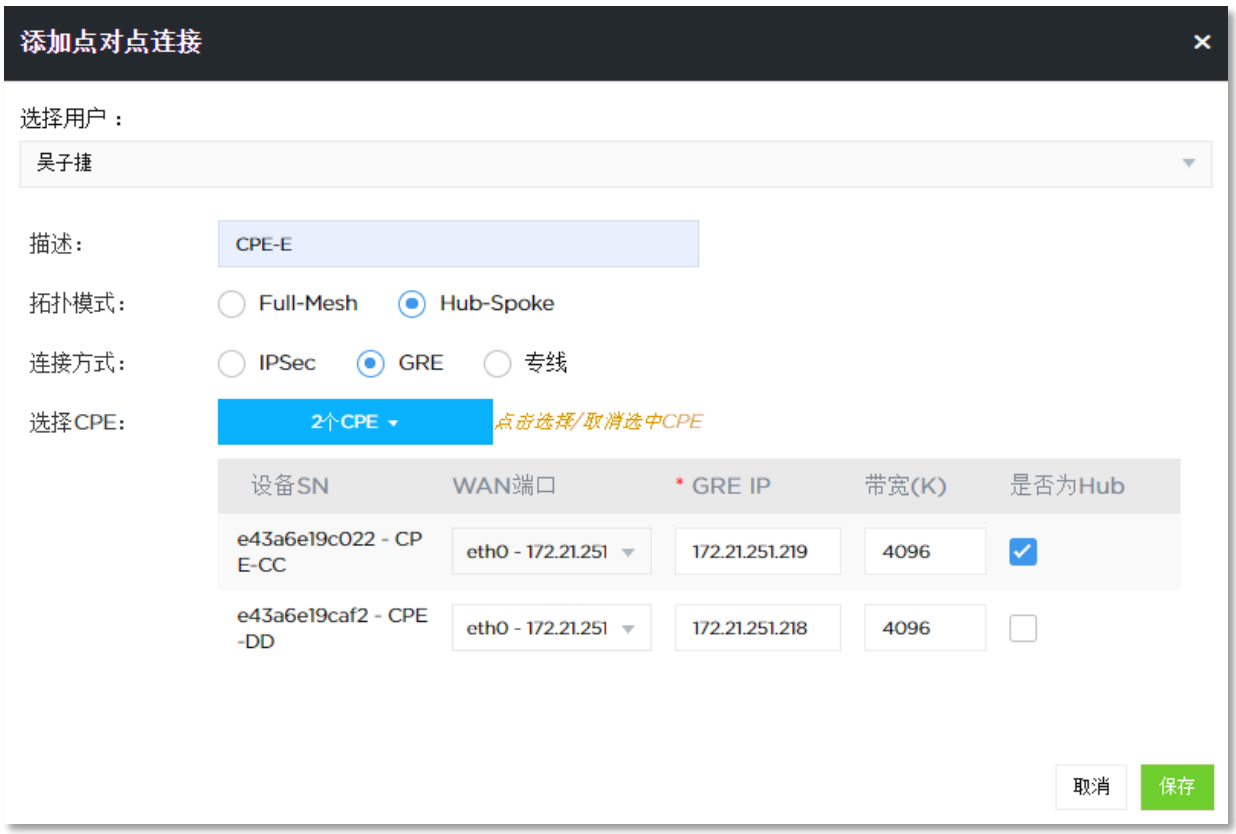
图 94

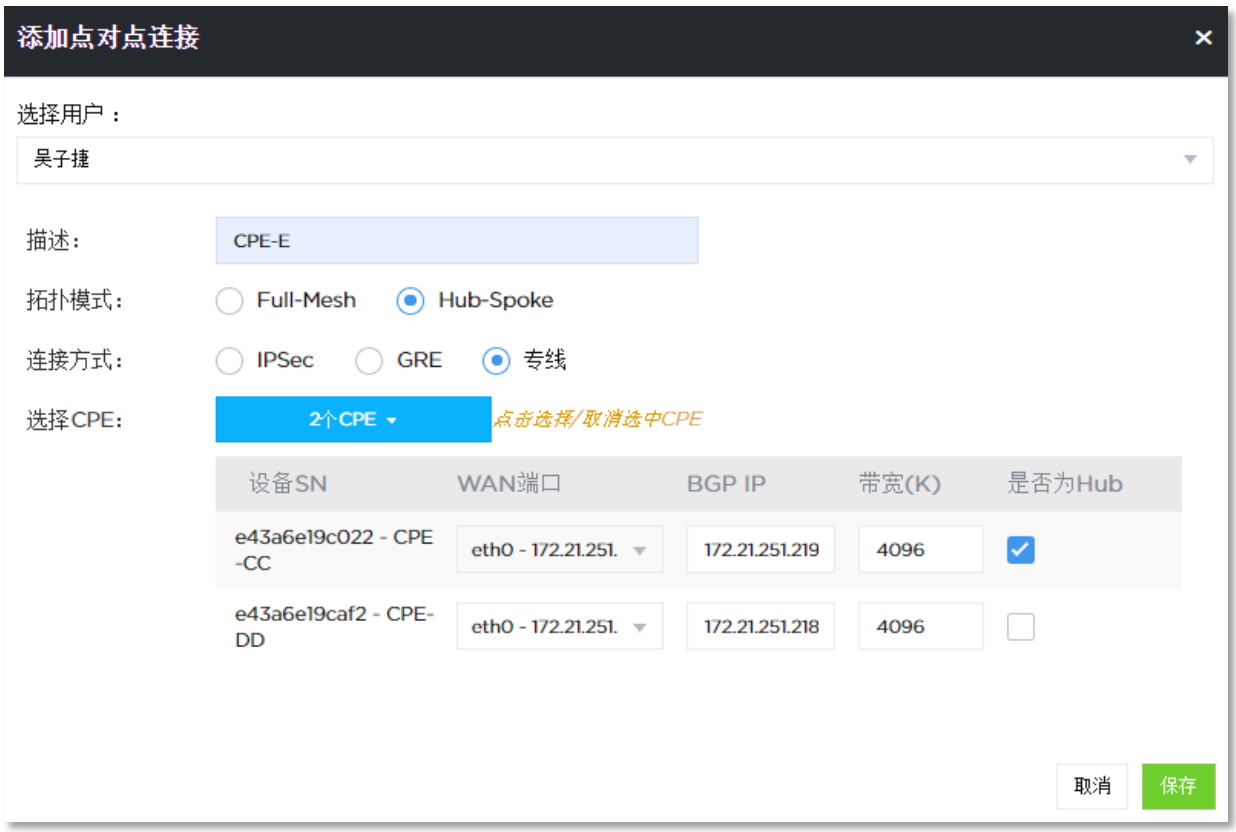
2 在 P2P 配置面板中，输入配置信息；


添加点对点连接
选择用户：
吴子捷
描述：
CPE-E
拓扑模式：
Full-Mesh
Hub-Spoke
连接方式：
IPSec
专线
选择CPE：
2个CPE
点击选择/取消选中CPE
设备SN
WAN端口
浮动IP
e43a6e19c022 - CPE-CC
eth0 - 172.21.251.219/16
172.21.251.219
e43a6e19caf2 - CPE-DD
eth0 - 172.21.251.218/16
172.21.251.218
取消
保存


添加点对点连接
选择用户：
吴子捷
描述：
CPE-E
拓扑模式：
Full-Mesh
Hub-Spoke
连接方式：
IPSec
专线
选择CPE：
2个CPE
点击选择/取消选中CPE
设备SN
WAN端口
BGP IP
带宽(K)
e43a6e19c022 - CPE-CC
eth0 - 172.21.251.219/16
172.21.251.219/16
4096
e43a6e19caf2 - CPE-DD
eth0 - 172.21.251.218/16
172.21.251.218/16
4096
取消
保存


添加点对点连接
选择用户：
吴子捷
描述：
CPE-E
拓扑模式：
Full-Mesh
Hub-Spoke
连接方式：
IPSec
GRE
专线
选择CPE：
2个CPE
点击选择/取消选中CPE
设备SN
WAN端口
浮动IP
是否为Hub
e43a6e19c022 - CPE-CC
eth0 - 172.21.251.219/
172.21.251.219
e43a6e19caf2 - CPE-DD
eth0 - 172.21.251.218/
172.21.251.218
取消
保存


添加点对点连接
选择用户：
吴子捷
描述：
CPE-E
拓扑模式：
Full-Mesh
Hub-Spoke
连接方式：
IPSec
GRE
专线
选择CPE：
2个CPE
点击选择/取消选中CPE
设备SN
WAN端口
* GRE IP
带宽(K)
是否为Hub
e43a6e19c022 - CPE-CC
eth0 - 172.21.251
172.21.251.219
4096
e43a6e19caf2 - CPE-DD
eth0 - 172.21.251
172.21.251.218
4096
取消
保存



✧ **连接类型**

作用：选择全互联还是 Hub Spoke

描述：如果是 Hub Spoke 模式必须确定一个 Hub 点

✧ **连接方式**

作用：三种不同的连接方式 GRE/IPsec/二层专线

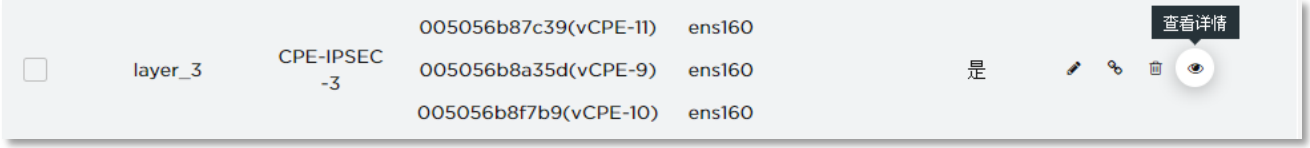
描述：专线模式一般用于 2 层专网，GRE/IPsec 一般用于互联网

✧ **浮动 IP**

作用：表示外网 IP

描述：如果 Wan IP 就是工网 IP，那么浮动 IP 与 Wan IP 一致，如果 Wan IP 是内网 IP，浮动 IP 填写外网 IP 地址

3 查看 P2P 链路状态。



7 、远程办公

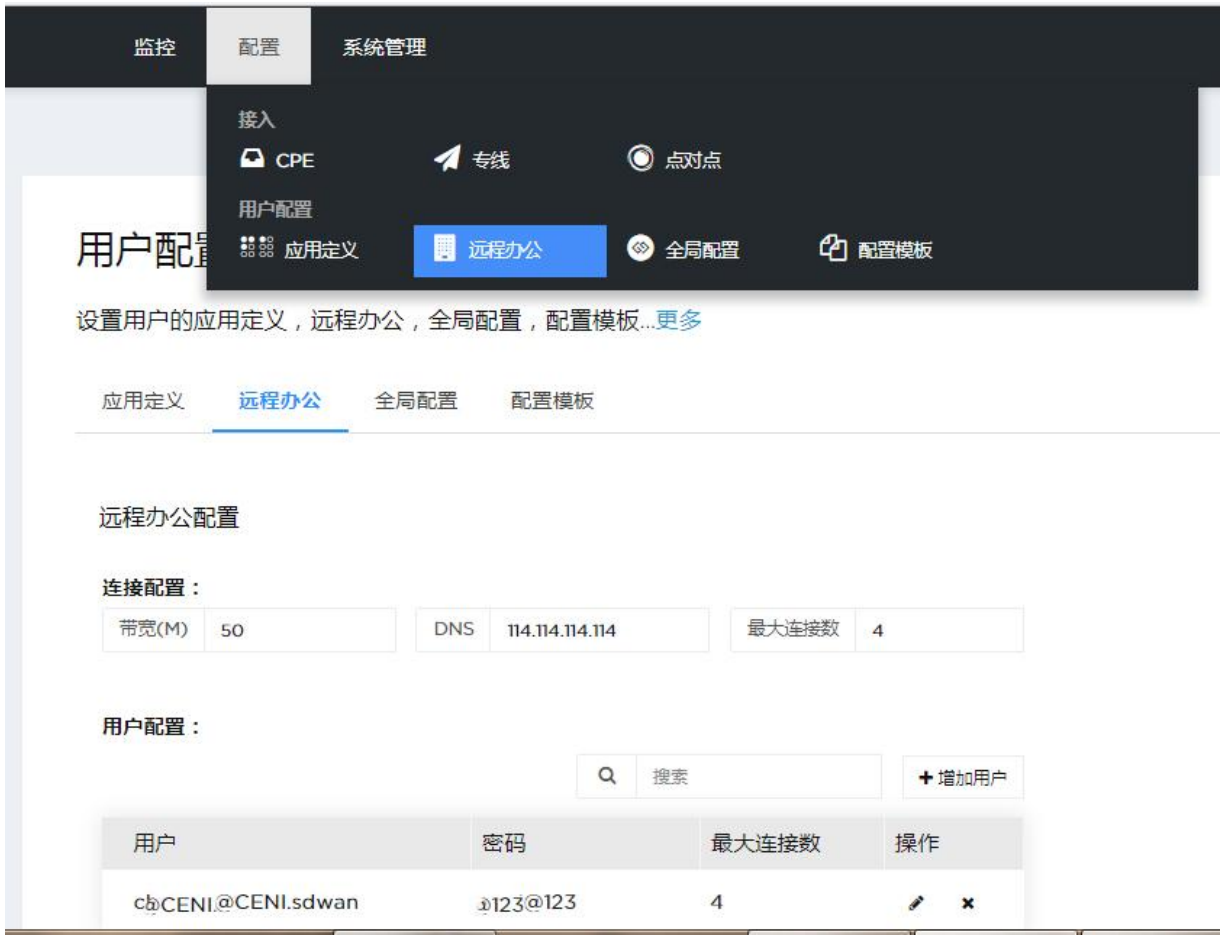
7.1远程办公功能介绍

- ✧ 作用：移动端拨号 VPN，远程连接；
- ✧ 说明：远程办公的客户端可以采用 PPTP、IPsec 和 OPENVPN 三种拨入方式，微软、苹果、安卓操作系统均可使用。(这里我们首推 OPENVPN,OPENVPN 拨号成功后自动实现本地与隧道的路由分离)。

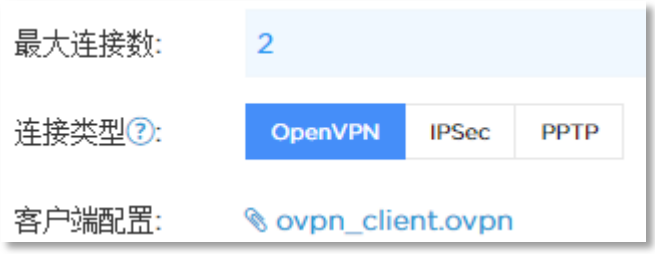
7.2远程办公信息查看

系统管理员会为购买了远程办公业务的用户开通办公账号，分配用户名和密码。同时设置最大连接数、带宽、client IP。

用户进入远程办公页面即可以查看相关信息，如下图：


监控
配置
系统管理
接入
CPE
专线
点对点
用户配置
应用定义
远程办公
全局配置
配置模板
用户配置
设置用户的应用定义，远程办公，全局配置，配置模板...更多
应用定义
远程办公
全局配置
配置模板
远程办公配置
连接配置：
带宽(M)
50
DNS
114.114.114.114
最大连接数
4
用户配置：
搜索
+增加用户
用户
密码
最大连接数
操作
cb@CENI.@CENI.sdwan
123@123
4

远程办公的三种用户接入信息和配置如下图：



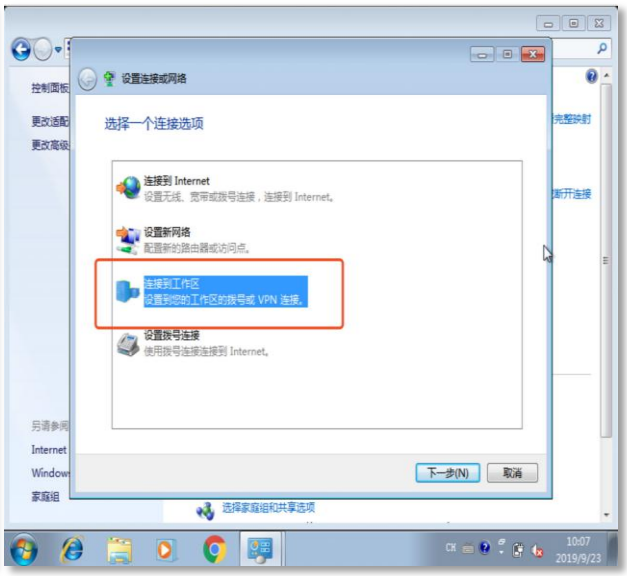
7.3 远程办公客户端接入

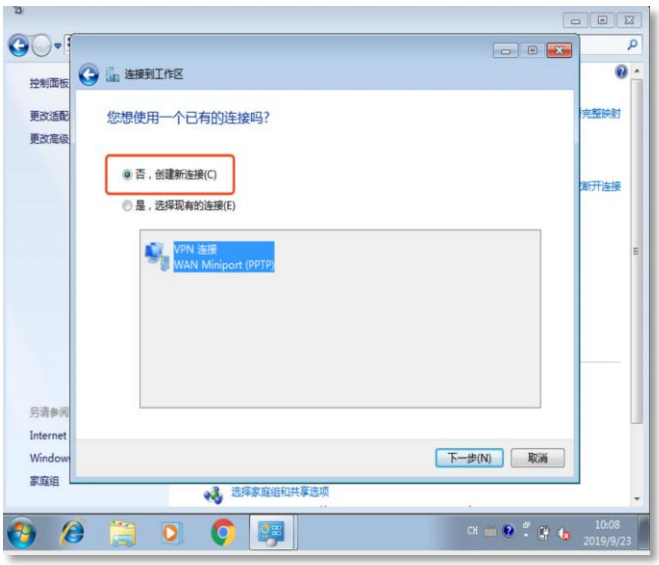
7.3.1 Windows

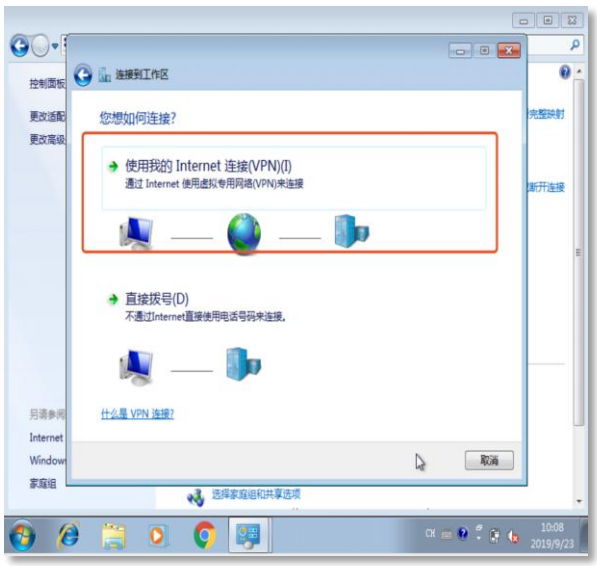
✧ Windows 原生客户端

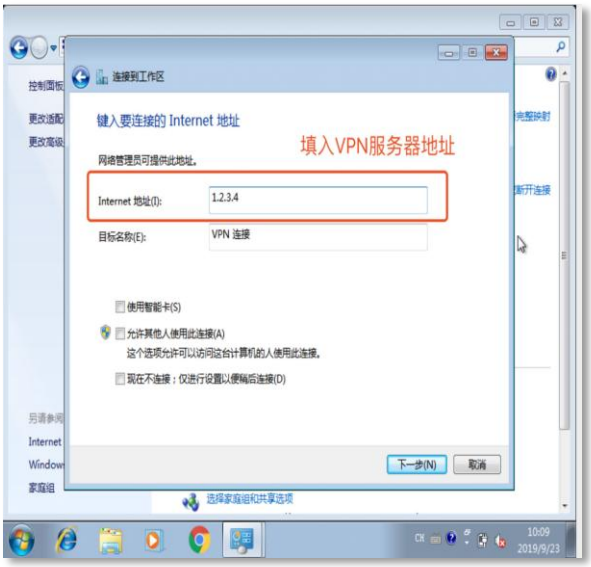
支持使用 Windows 原生客户端通过 PPTP 协议拨 VPN 连接 SDWAN 骨干网。该方式的优点在于不需要额外安装软件，使用方便。缺点在于有些网络环境对 PPTP 协议不友好，会导致 PPTP 拨号失败。

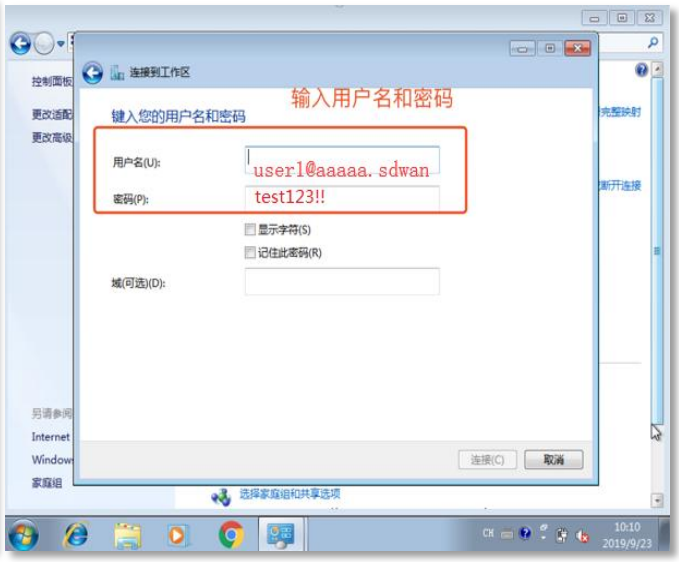
配置步骤如下：











✧ 第三方 IPSec 客户端

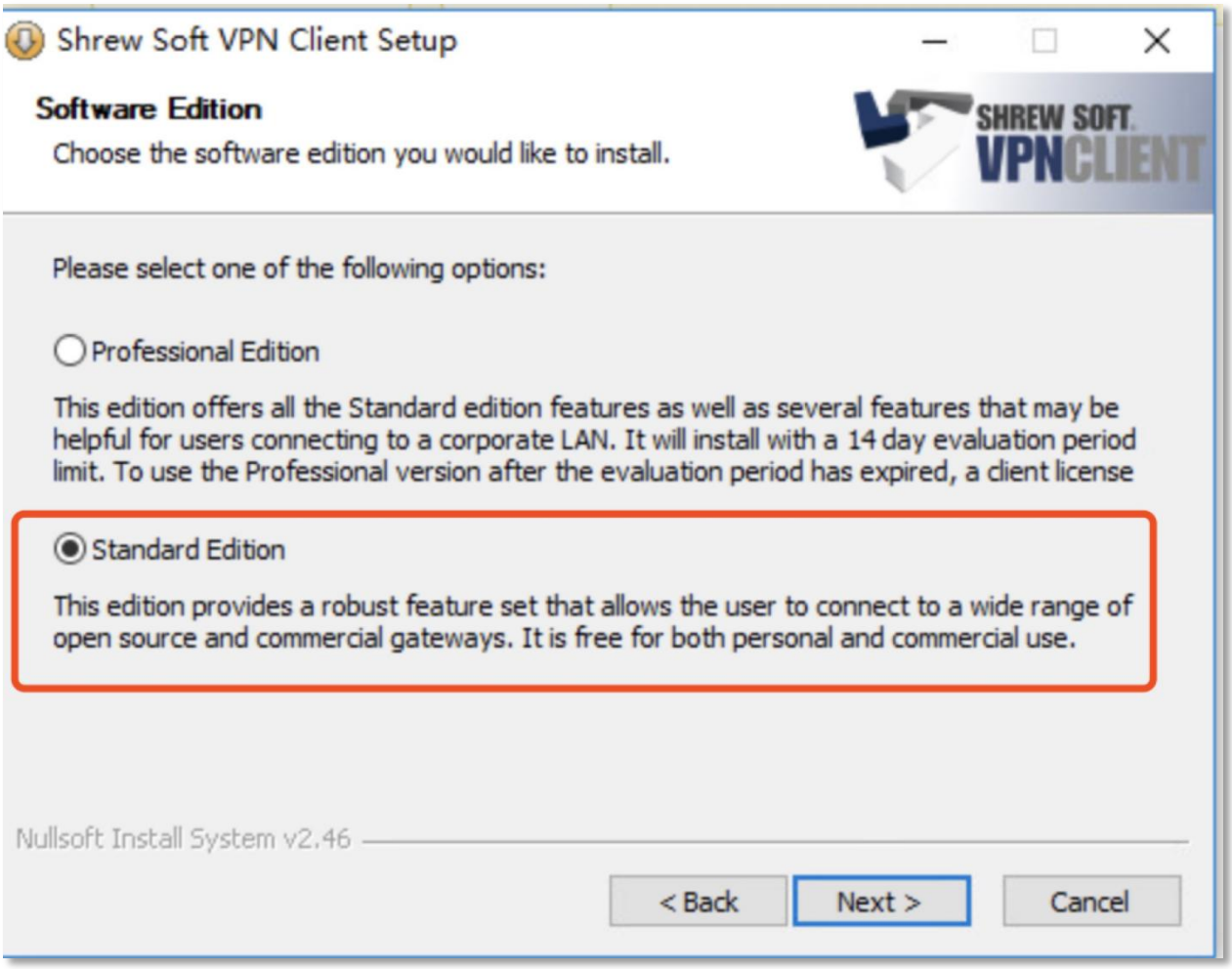
支持标准的 IPSec 接入。可以通过安装第三方 IPSec 客户端，通过 IPSec 协议接入骨干。该方式的优点在于稳定性高于 PPTP，缺点在于需要额外安装第三方软件，略显不方便。

步骤如下：

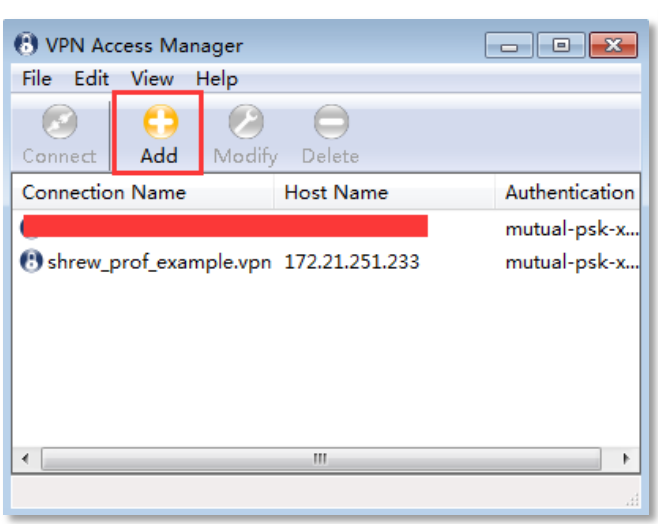
下载并安装开源 Shrew IPSec client,

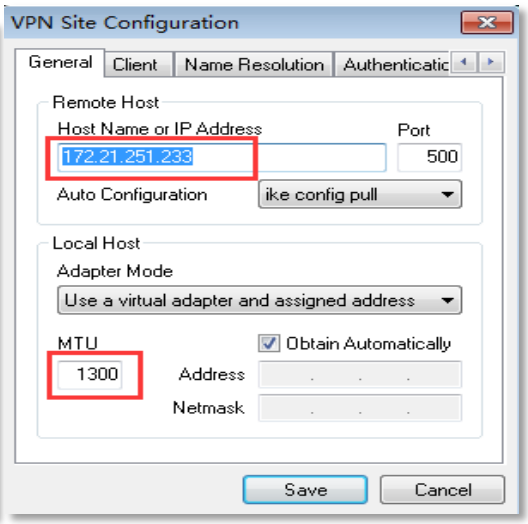
https://www.shrew.net/download/vpn/vpn-client-2.2.2-release.exe

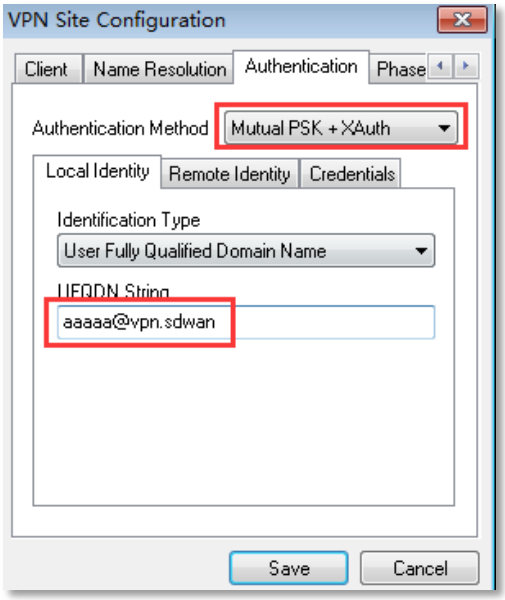
1 安装时，选择标准版；

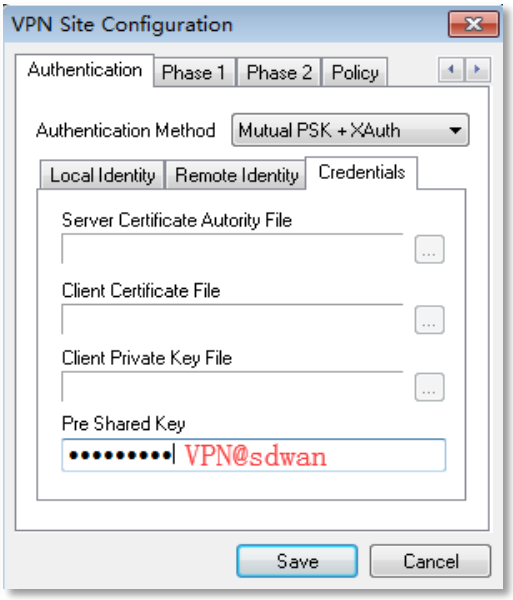


2 安装后，添加配置文件，配置文件中要填写 VPE 的 IP 地址、MTU、认证方式、组名和预共享密钥；

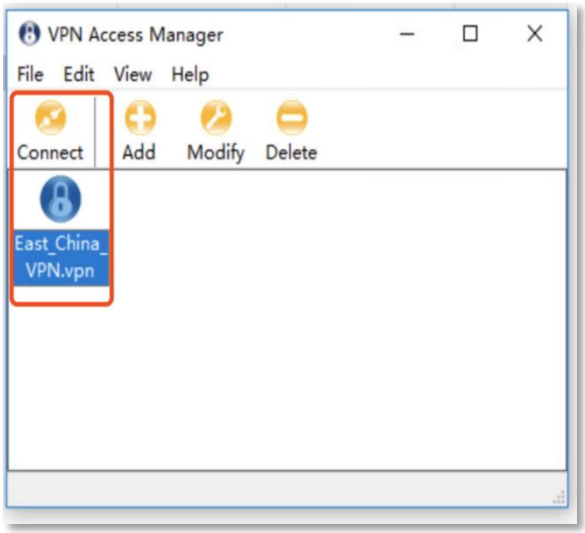


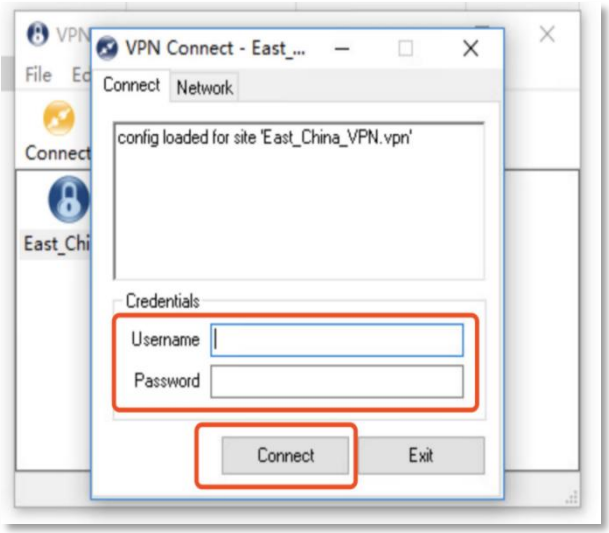






3 选中 VPN 配置，并点击“Connect”按钮，输入服务商提供的用户名和密码：





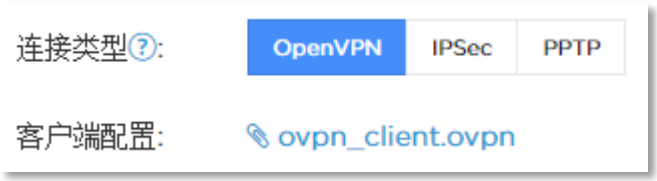
✧ 第三方 OPENVPN 客户端

OPENVPN 为最推荐的远程拨号 VPN，拨号连通后自动实现隧道分离。步骤如下：

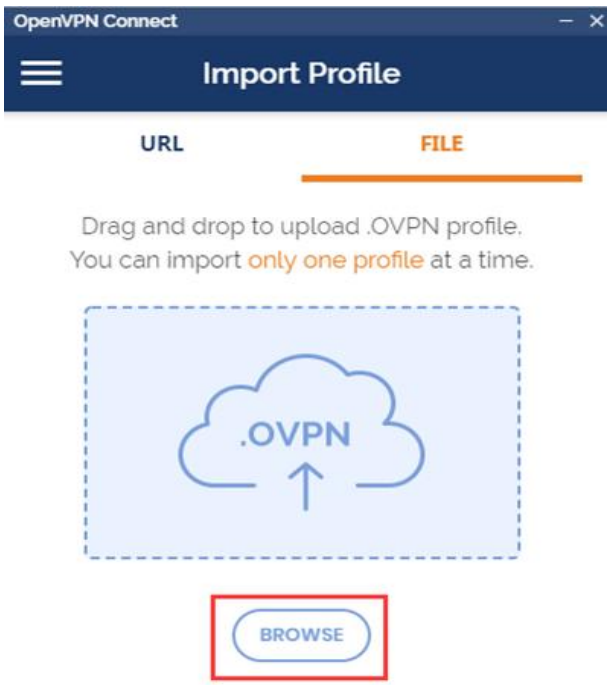
下载并安装开源 Open VPN Connect，

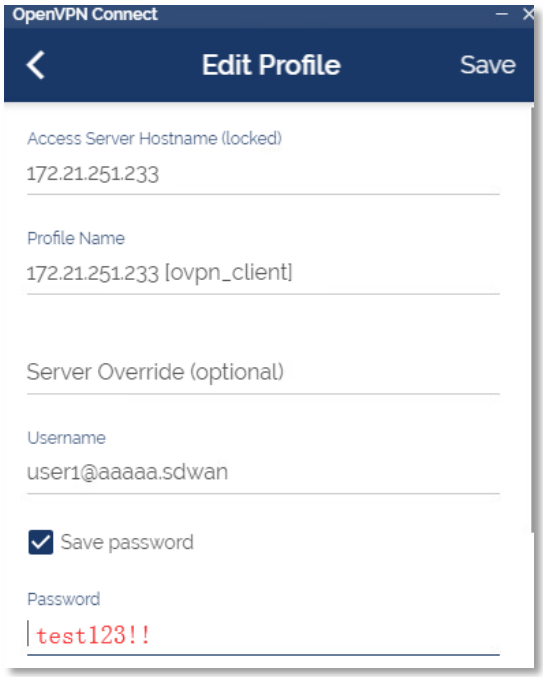
https://openvpn.net/client-connect-vpn-for-windows/

1 安装客户端软件，下载配置模板；

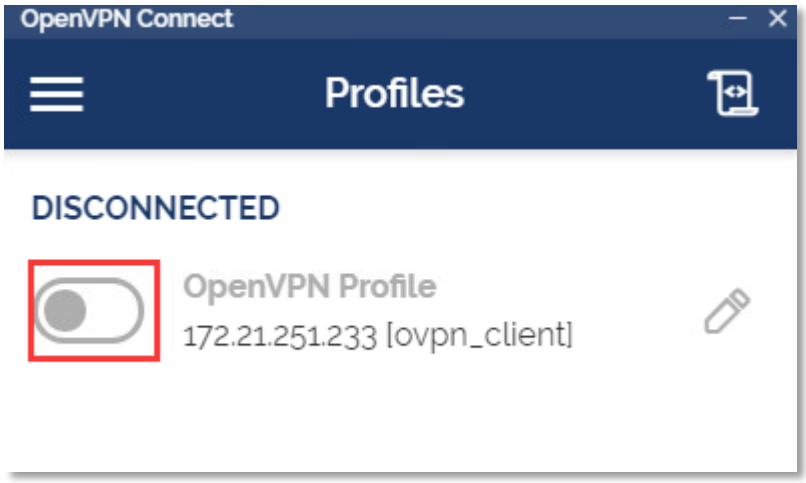


2 打开以安装好的客户端软件，导入下载好的配置模板；并输入用户名密码保存。





3 连接 VPN

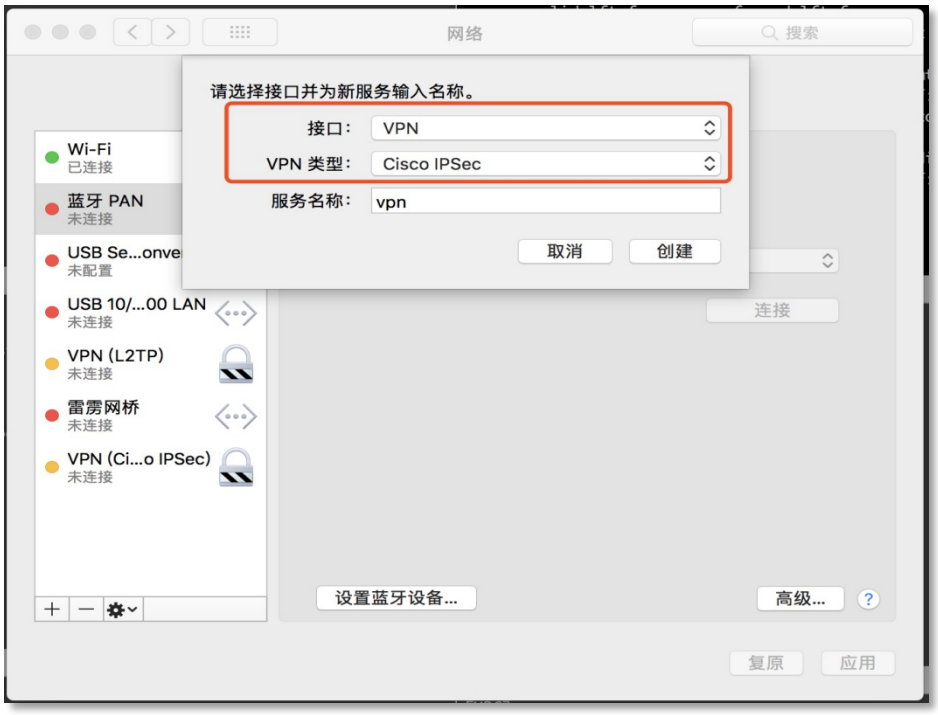


7.3.2 MacOs

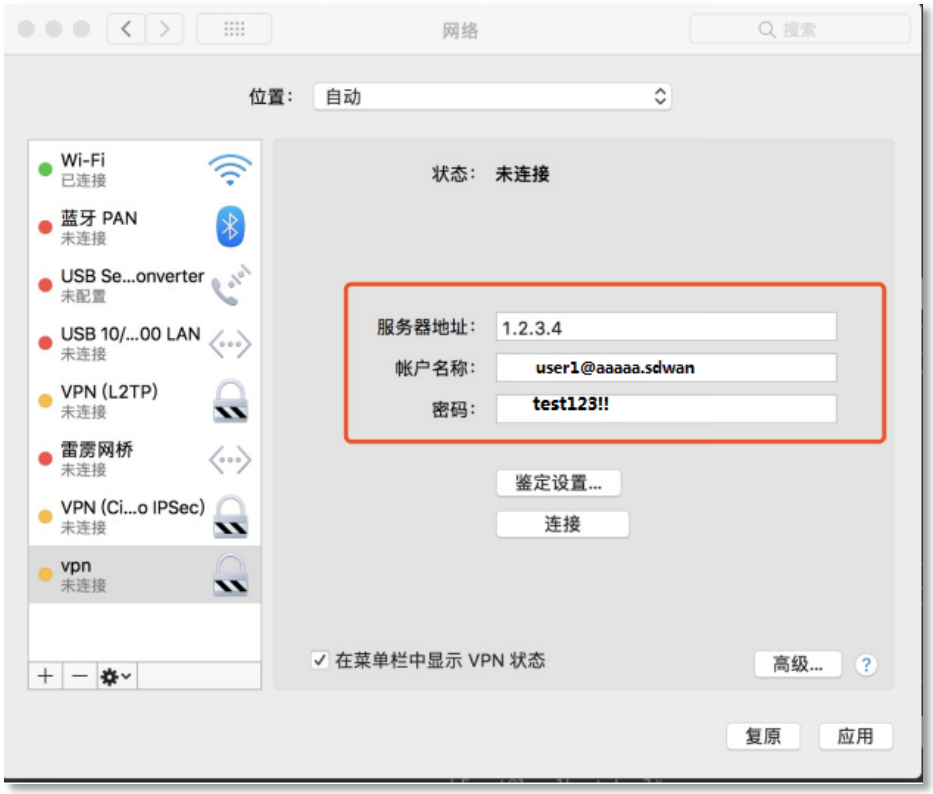
对于 MacOs，可以使用系统原生的 VPN 客户端，通过 IPSec 拨号，也可使用 OPENVPN 连接骨干网络（OPENVPN 操作方式与 Windows 客户端相同这里就不再重述）。

步骤如下：

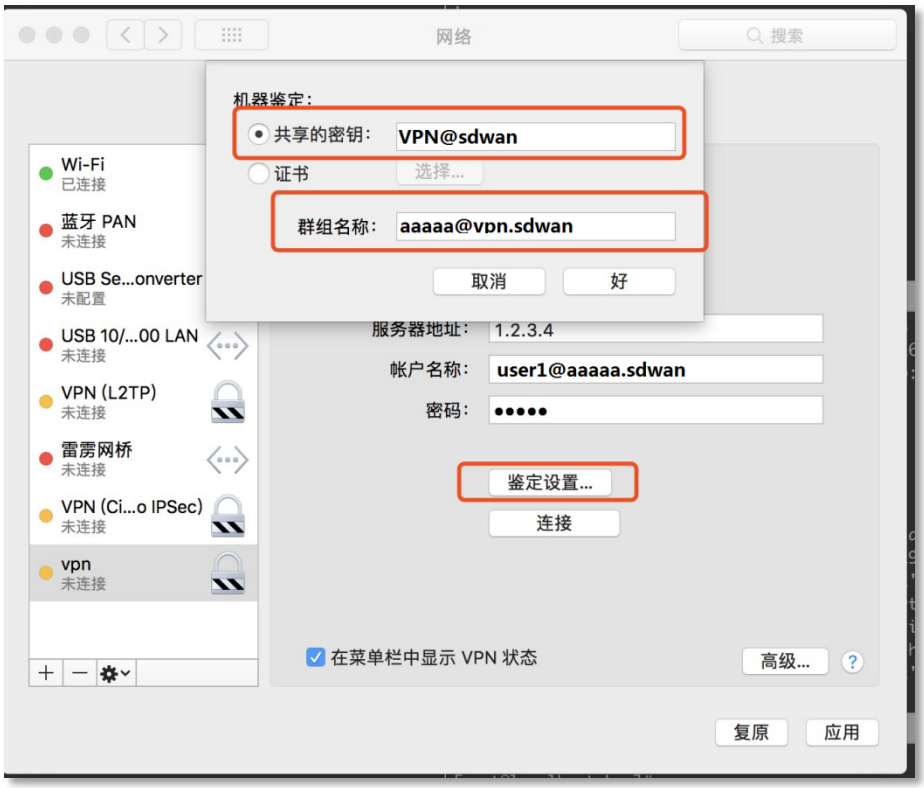
1 打开网络配置页面，添加新的 VPN，选择 Cisco IPSec 类型；



2 填入服务商提供的服务器地址，用户名，密码等信息；



3 点击“鉴定设置”按钮，填入服务商提供的共享密钥和群组名称；



4 点击“连接”按钮。

7.3.3 IPhone

对于 IPhone，可以使用系统原生的 VPN 客户端，通过 IPSec 协议连接骨干。步骤如下：

1 在“通用”配置页面，选中 VPN 管理，并添加 VPN 配置；

2 VPN 类型选择 IPSec，填入服务商提供的服务器，账户，密码，群组名称，密钥等信息；

3 选中新建立好的 vpn，并点击连接按钮。

7.3.4 Android

对于 IPhone，可以使用系统原生的 VPN 客户端，通过 IPSec 协议或者 PPTP 协议连接骨干。

✧ IPSec

在“无线和网络”设置页面里添加 VPN 配置，类型选择 “IPSec Xauth PSK”， 填入服务商提供的服务器地址，IPSec 标识符，IPSec 预共享密钥，用户名，密码等信息。

✧ PPTP

在“无线和网络”设置页面里添加 VPN 配置，类型选择 “PPTP”， 填入服务商提供的服务器地址，用户名，密码等信息。

8 网络监控

系统提供了网络监控功能，包括用户信息、拓扑信息、日志信息和告警信息。

8.1 CPE 详情列表

在主菜单中选择监控 > 大屏视图 > 租户，打开 CPE 监控面板，就可以看到 CPE 的详细列表。如下图所示：

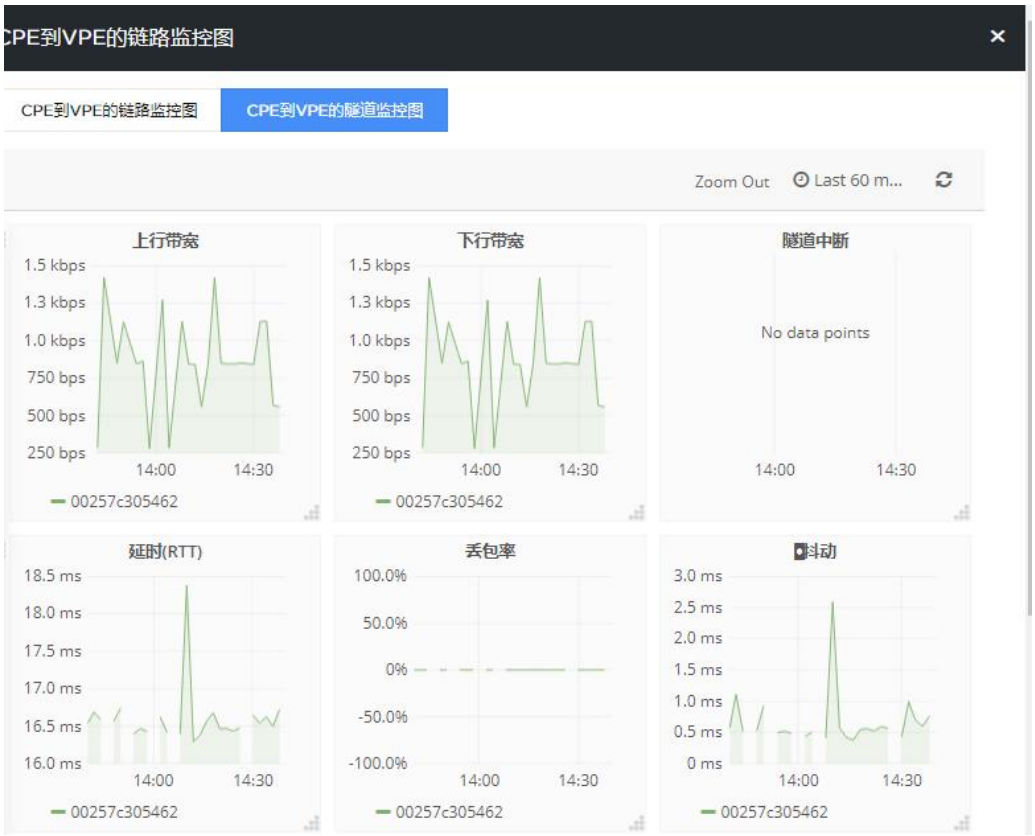
点击 CPE 的序列号，可以进入 CPE 详情页面：

点击 CPU 或内存的使用率，打开性能监控面板，可以自定义时间查看该站点 CPE 性能的历史情况，监控数据保存 3 年；

8.2 CPE-POP 的网络品质监控

在 CPE 详情列表中，可以查看 CPE 到 VPE 的延时、抖动和丢包率统计信息。点击 CPE 对应的 VPE 名称，即可进入 CPE 链路品质监控页面。可以查看 CPE—VPE 的链路质量、隧道带宽和质量。

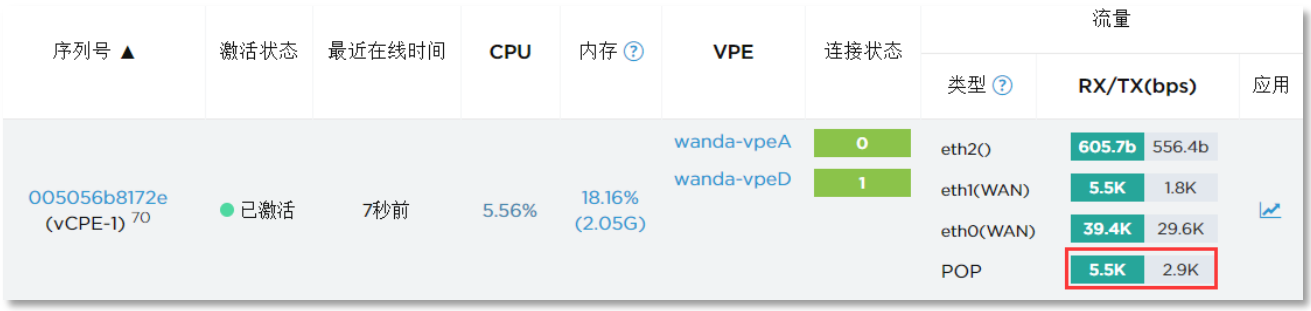
可以自定义时间查看指定 CPE-VPE 的网络品质情况，数据保存 3 年；



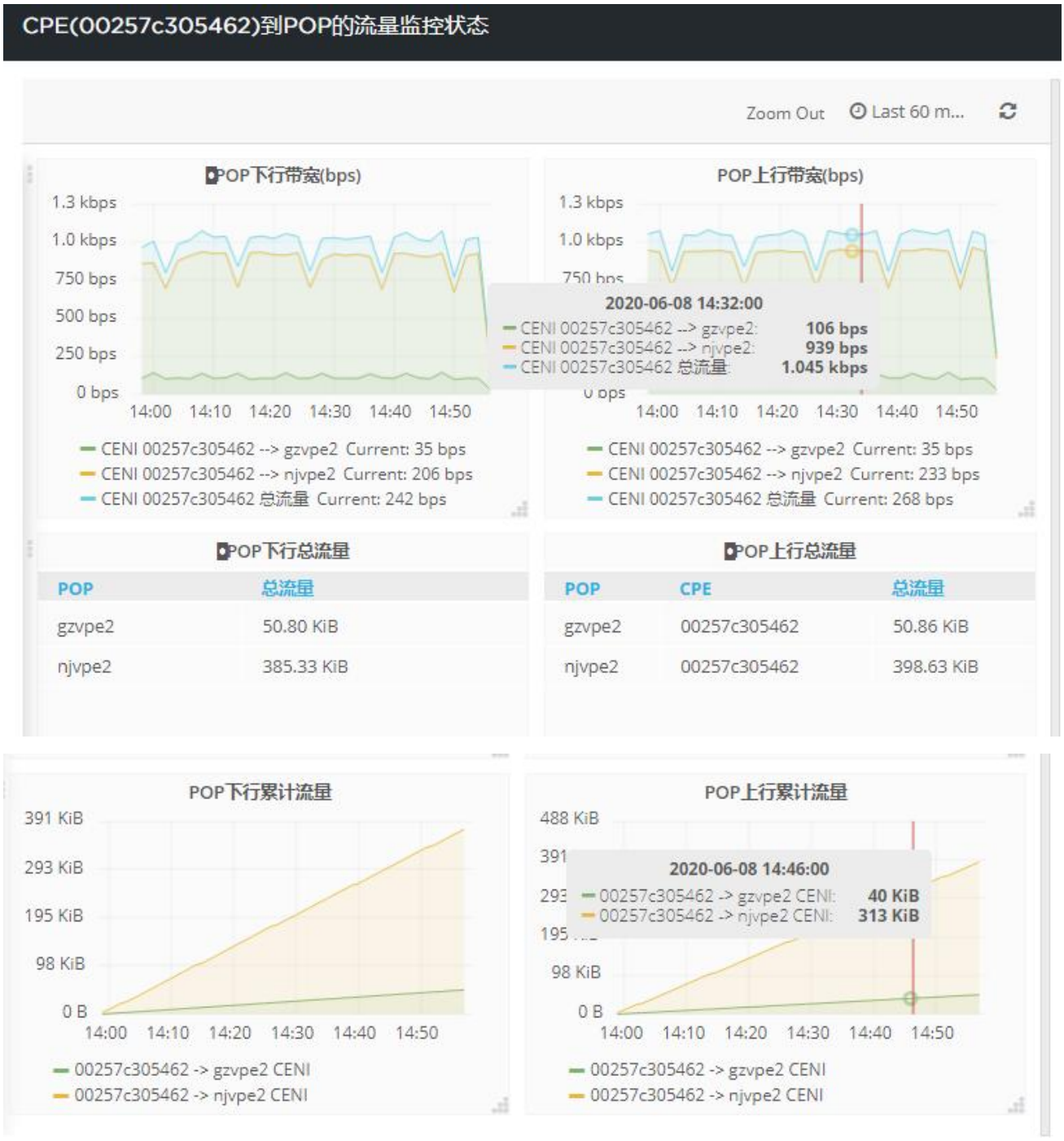
8.3 CPE-POP 的流量监控

可以监控 CPE-POP 的带宽使用率，用于确认为分支机构购买的骨干带宽是否够用，具体的操作如下：

在 CPE 监控面板，点击流量选项卡中 POP 的流量图表；



可以自定义时间查看指定 CPE-VPE 的网络带宽情况，包括上行和下行带宽的使用量，以及上行和下行带宽的数据包收发量，数据保存 3 年。

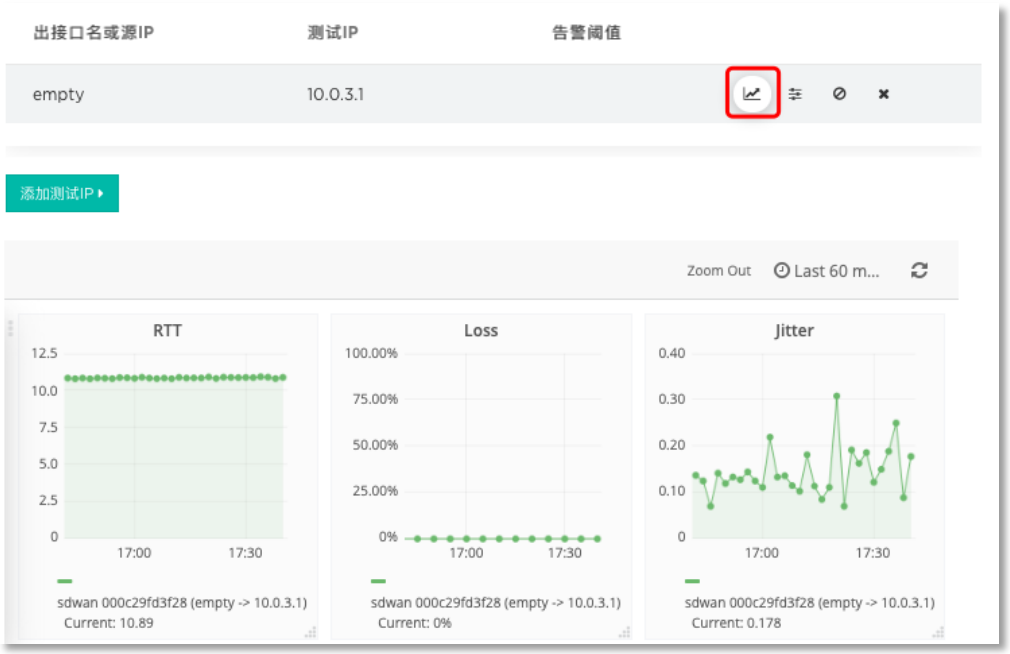


8.4 CPE-Any 的网络品质监控

可以检测指定 CPE 到任意一个指定目标的延时、抖动和丢包率，具体操作如下：

1、在 CPE 监控面板中点击相应的 CPE 序列号打开设备信息面板，并选择监控选项卡；

2 在监控面板下添加指定的目标 IP 地址信息；



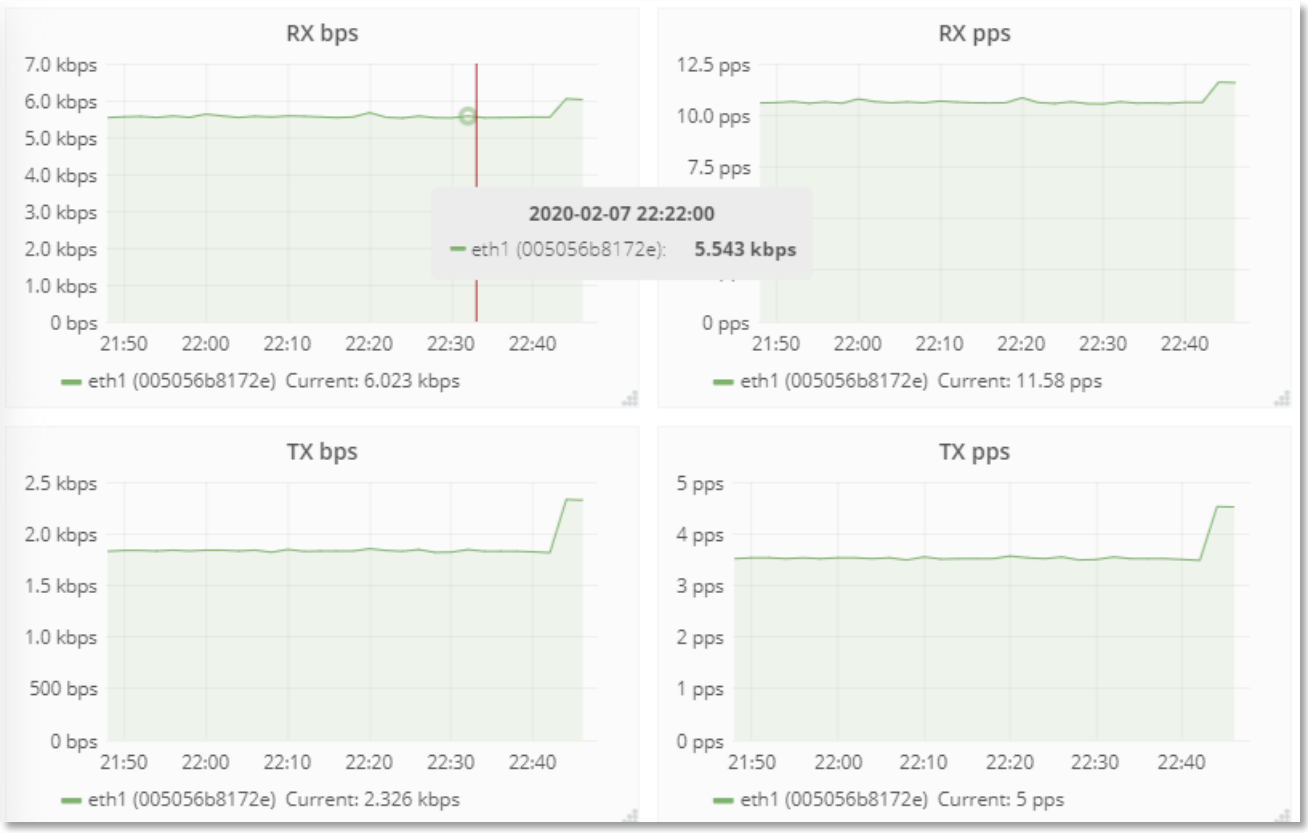
8.5 CPE WAN 口流量监控

可以监控 CPE 的 WAN 口带宽使用情况，具体操作如下：

1 在 CPE 监控面板，选择图表选项卡中 WAN 的流量图表；

图 157

2 您可以自定义时间查看指定 CPE 去往互联网的带宽情况，包括上行和下行带宽的使用量，以及上行和下行带宽的数据包收发量，数据保存 3 年。



8.6 应用流量监控

如果定义了应用，则可以查看对应 CPE 上指定应用的网络使用情况，具体操作如下：

1 首先在配置 > CPE 中选择指定 CPE，点击编辑设备开关进入编辑 CPE 设备面板，选择高级配置 > 应用监控，勾选需要监控的应用；

2 配置模板 > 策略中也可以开启应用监控；

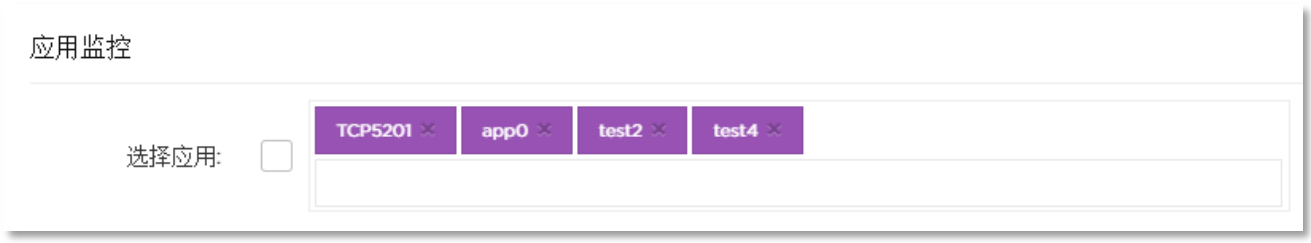
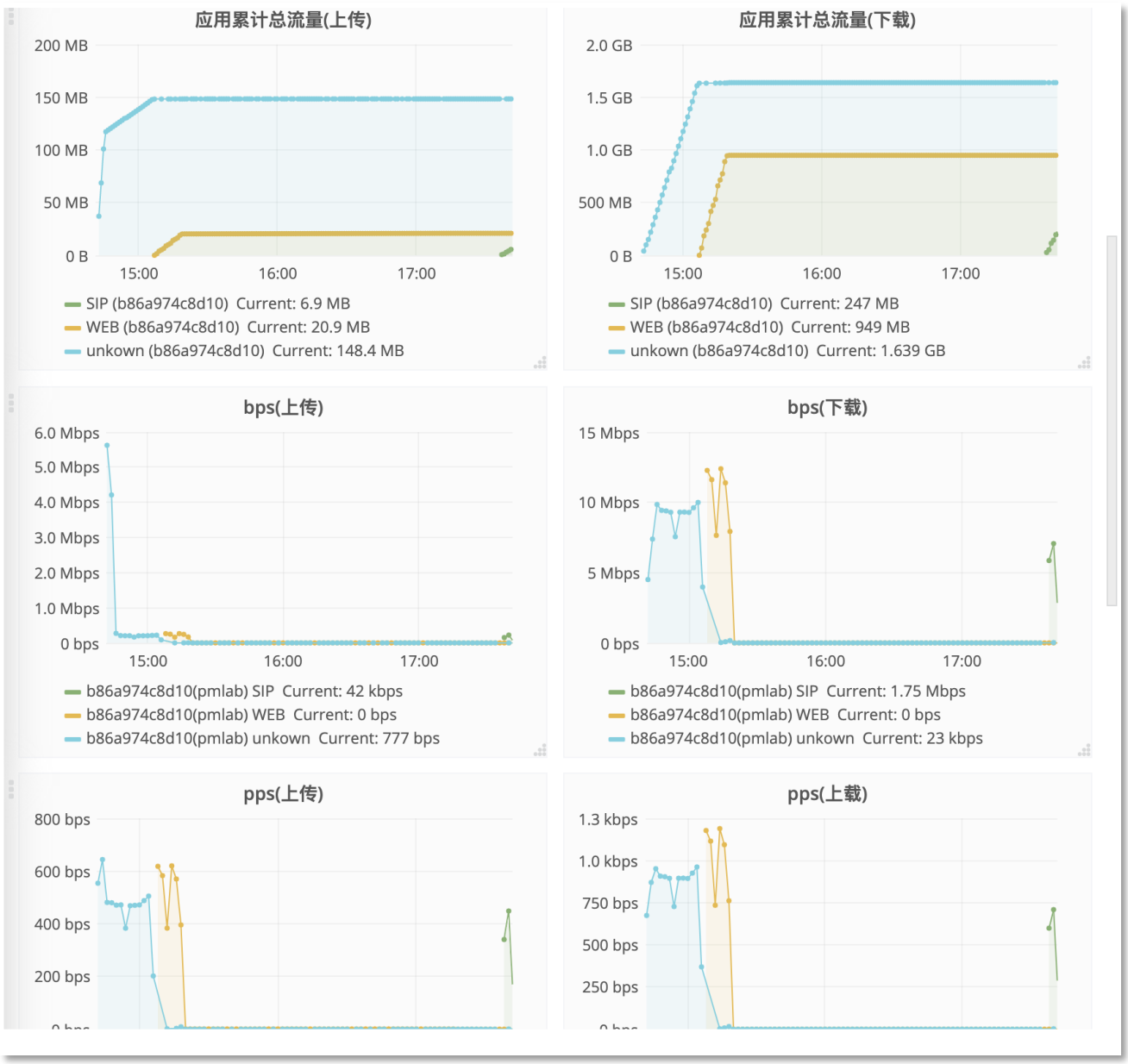


图 160

3 在主菜单中选择监控 > 大屏视图 > 租户，打开 CPE 监控面板，选择图表选项卡中应用的流量图表；

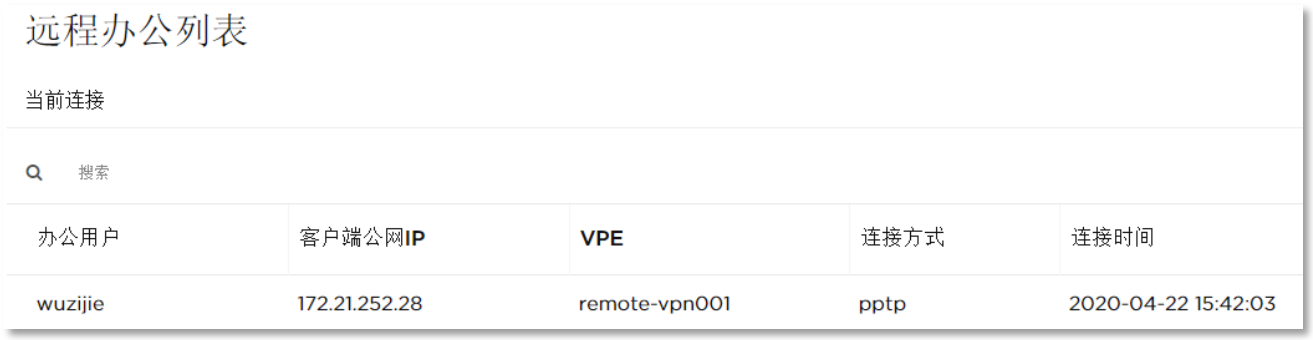
图 161

4 可以自定义时间查看指定 CPE 应用的带宽情况，包括上行和下行带宽的使用量，以及指定应用的总流量，数据保存 3 年。

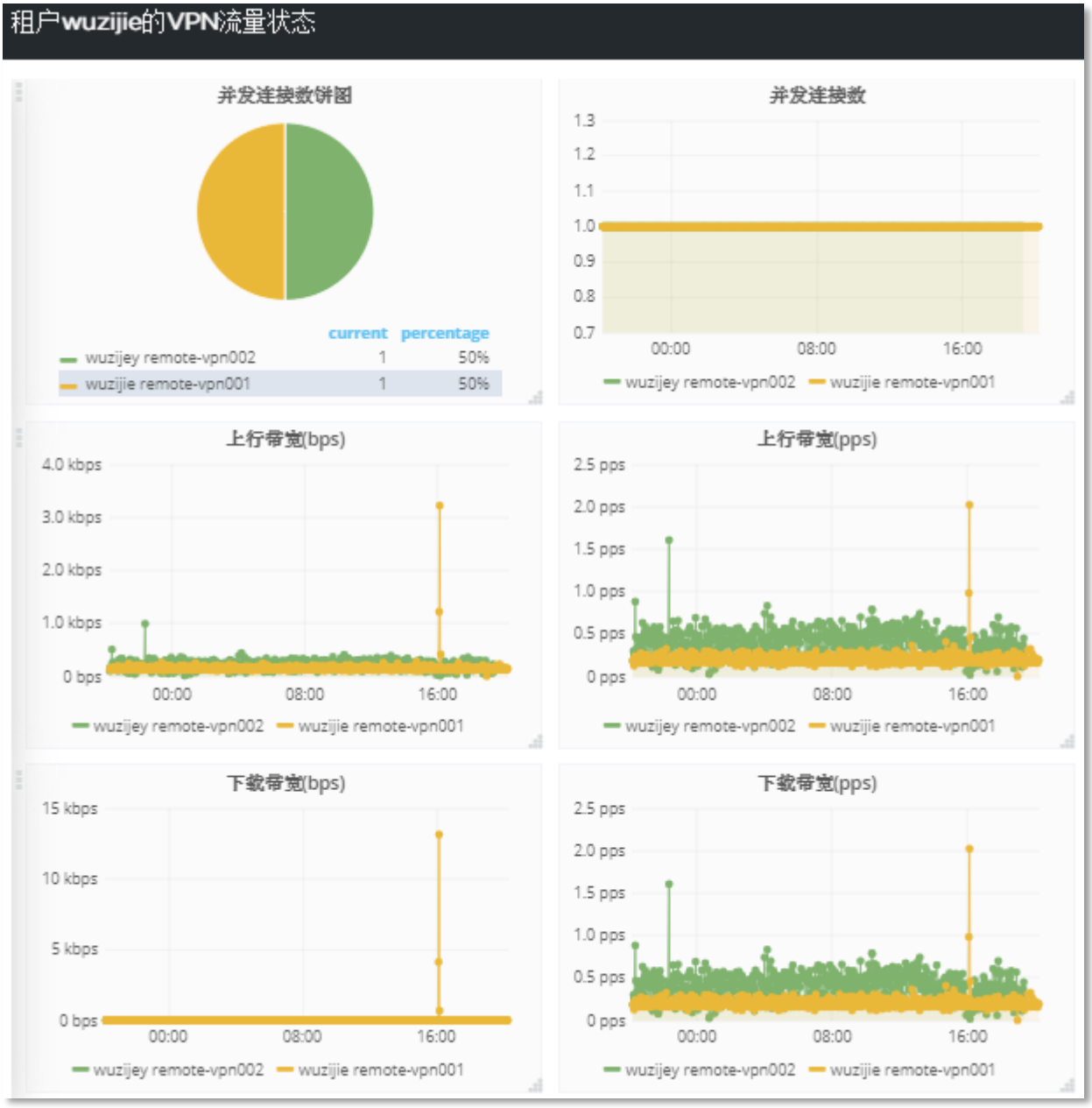


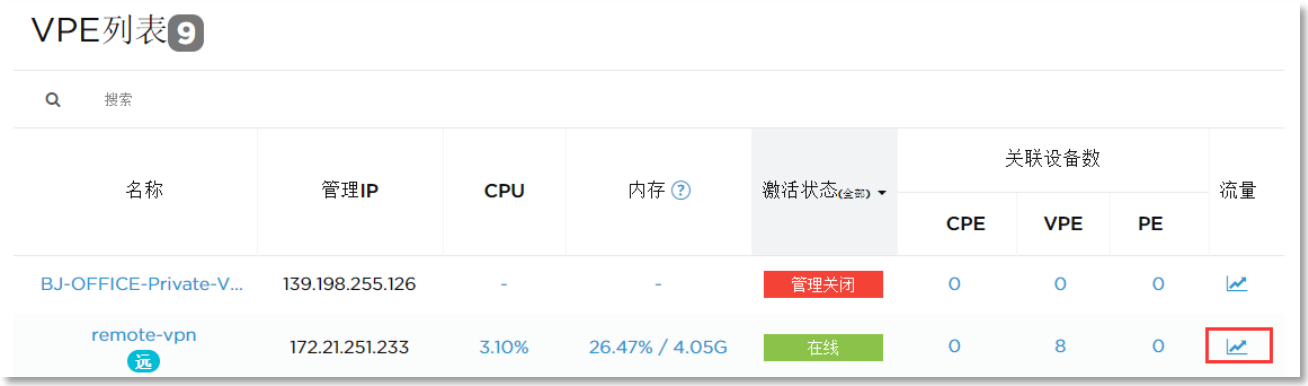
8.7 远程办公监控

开通了远程办公服务的用户，可以通过监控页面查看远程办公的并发、带宽以及操作日志等。进入监控页面，在页面下方可以看到远程办公列表信息，如下图：


远程办公列表
当前连接
搜索
办公用户
客户端公网IP
VPE
连接方式
连接时间
wuzijie
172.21.252.28
remote-vpn001
pptp
2020-04-22 15:42:03


连接日志
查看远程办公流量
搜索
2020-04-16 - 2020-04-23
办公用户
操作
时间
wuzijey
wuzijie名下的wuzijey位于POP点(remote-vpn002)的连接中断，接入方式是:openvpn, 源IP是192.168.200.85, 在线时长为:1h0m0s, 总下载流量为:0BB, 总上传流量为:91.9KB
2020-04-23 19:21:52
wuzijey
wuzijie名下的wuzijey通过POP点(remote-vpn002)连接成功，接入方式是:openvpn, 源IP是192.168.200.85
2020-04-23 18:21:52
wuzijey
wuzijie名下的wuzijey位于POP点(remote-vpn002)的连接中断，接入方式是:openvpn, 源IP是192.168.200.85, 在线时长为:1h0m0s, 总下载流量为:0BB, 总上传流量为:106.9KB
2020-04-23 18:21:46
wuzijey
wuzijie名下的wuzijey通过POP点(remote-vpn002)连接成功，接入方式是:openvpn, 源IP是192.168.200.85
2020-04-23 17:21:46


租户wuzijie的VPN流量状态
并发连接数饼图
current
percentage
wuzijey remote-vpn002 1 50%
wuzijie remote-vpn001 1 50%
并发连接数
1.3
1.2
1.1
1.0
0.9
0.8
0.7
00:00
08:00
16:00
wuzijey remote-vpn002
wuzijie remote-vpn001
上行带宽(bps)
4.0 kbps
3.0 kbps
2.0 kbps
1.0 kbps
0 bps
上行带宽(pps)
2.5 pps
2.0 pps
1.5 pps
1.0 pps
0.5 pps
0 pps
下载带宽(bps)
15 kbps
10 kbps
5 kbps
0 bps
下载带宽(pps)


VPE列表 9
搜索
名称
管理IP
CPU
内存
激活状态
关联设备数
CPE
VPE
PE
流量
BJ-OFFICE-Private-V...
139.198.255.126
-
-
管理关闭
0
0
0
remote-vpn
远
172.21.251.233
3.10%
26.47% / 4.05G
在线
0
8
0

8.8 拓扑监控

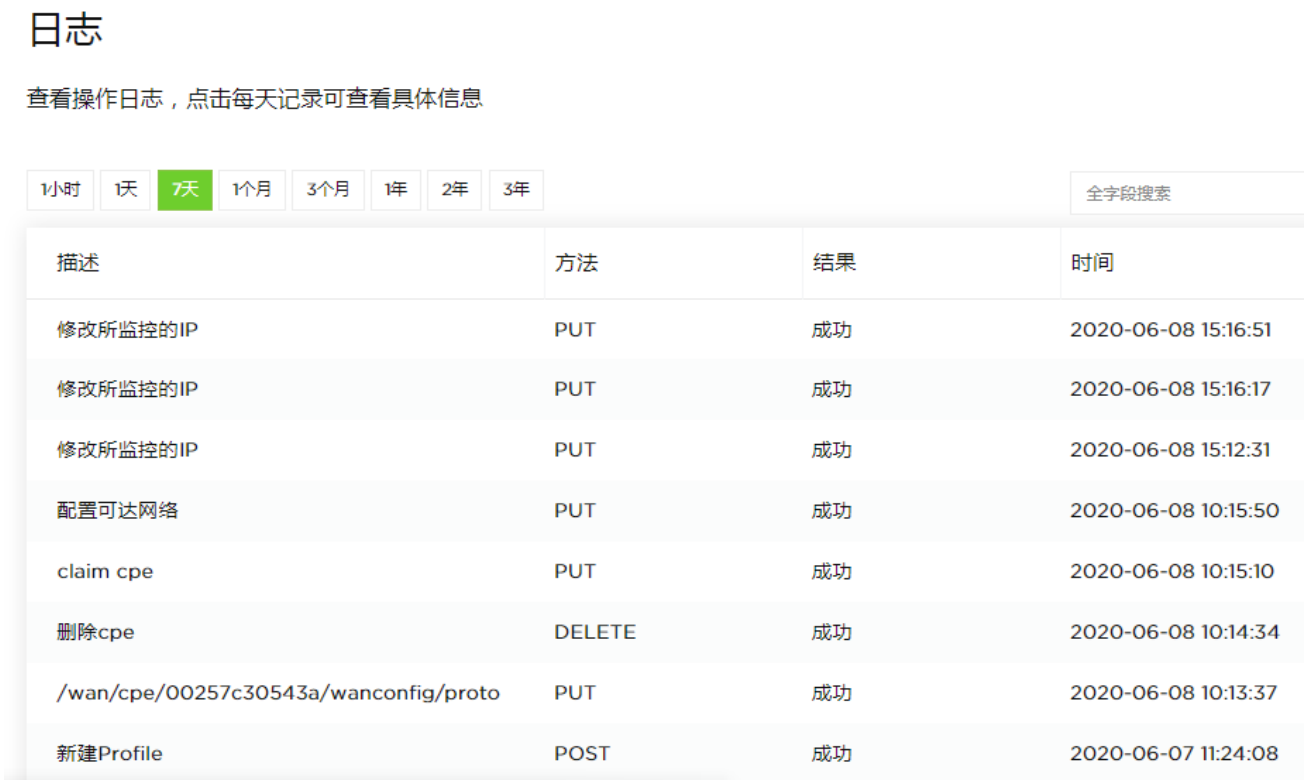
用户可以在监控列表中查看设备拓扑图，在页面中可以看到所有设备的整体关联图。若页面中默认的拓扑图是聚和的，则需要手动拖拽聚和后的拓扑图，把各个设备展开。

示例图如下：

点击每一个设备，能够展示设备的详情。

8.9 日志监控

系统提供了丰富的日志功能，最长保存三年。日志涵盖了各种操作类型，示意图如下：



8.10 告警监控

系统能够展示告警统计信息，按照告警的类别列出告警数量统计信息，还可以展示告警的详细信息，包括时间、用户、行为、级别、类型等。

告警详情

告警列表

1小时 1天 7天 1个月 3个月 1年 2年 3年

按子类别和设备序列号过滤： 所有

全字段搜索 刷新 配置告警

时间	类别	子类别	严重级别	关联ID	消息	状态	
2020-06-07 19:54:19	CPE	CPE上线	CRITICAL		CPE 00257c305453(ceni_无锡),所属租户:CENI, 上线, 该CPE 位于租户 CENI, 上线时间为 Sun Jun 07 19:54:19 CST 2020	未处理	解除告警
2020-06-05 16:10:12	CPE	CPE上线	CRITICAL		CPE 00257c305467(ceni_镇江),所属租户:CENI, 上线, 该CPE 位于租户 CENI, 上线时间为 Fri Jun 05 16:10:12 CST 2020	未处理	解除告警
2020-06-05 13:14:42	CPE	WAN□ DOWN	CRITICAL	[Fri Jun 5 13:14:35 CST 2020]cddf9b8f-225e-46d6-a443-1d01de062820	SN: 00257c30546c(ceni_常州),所属租户:CENI,LINK: eth0	未处理	解除告警
2020-06-05 13:09:51	CPE	WAN□UP	CRITICAL	[Fri Jun 5 13:09:50 CST 2020]629af222-fac6-46a9-bf51-ef00990a4b5b	SN: 00257c30546c(ceni_常州),所属租户:CENI,LINK: eth0	未处理	解除告警