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

1、SDWAN 简介1
1.1 名词解释
1.1.1 CPE
1.1.2 PE/vPE
1.1.3 POP 点
1.1.4 CPE HA
2、CPE 初始配置
2.1 CPE 介绍
2.2 CPE 布放位置
2.3 CPE 初始配置6
3、 CPE 基本配置12
3.1 CPE LAN 配置
3.2 CPE WAN 口配置14
3.3 CPE 与用户内网的路由配置16
3.4 标识 CPE 设备19
4 、CPE 高级功能配置
4.1 应用定义21
4.1.1 应用定义功能介绍21
4.1.2 应用定义的配置

4.2	QOS 策略配置	23
4.3	CPE 防火墙功能配置	26
4.3.	1 防火墙	. 26
4.3.	2 基于单 CPE 的防火墙配置	. 27
4.3.	3 URL 防火墙	. 29
4.3.	4 URL 防火墙配置	. 29
4.4	NAT 功能	30
4.4.	1 DNAT 规则	. 30
4.4.	2 DNAT 配置	. 30
4.4.	3 SNAT 规则	. 30
4.4.	4 SNAT 配置	. 30
4.5		21
4.5	优选 POP	51
4.5 4.6	优选 POP	. 32
4.5 4.6 <i>4.6.</i>	优选 POP 隧道配置	. 31 . 32 . <i>32</i>
4.5 4.6 <i>4.6.</i> <i>4.6.</i>	优选 POP 隧道配置 <i>1 IPsec 端口配置</i>	. 32 . <i>32</i> . <i>34</i>
 4.5 4.6 4.6. 4.7 	优选 POP 隧道配置 <i>1 IPsec 端口配置</i>	. 32 . <i>32</i> . <i>34</i> . 35
 4.5 4.6 4.6. 4.7 4.8 	优选 POP 隧道配置 <i>1 IPsec 端口配置</i>	. 32 . <i>32</i> . <i>34</i> . 35 . 37
 4.5 4.6 4.6. 4.7 4.8 4.8. 	 优选 POP	. 32 . <i>32</i> . <i>32</i> . <i>34</i> . 35 . 37 . <i>38</i>
 4.5 4.6 4.6. 4.7 4.8 4.8. 4.8. 4.8. 	 优选 POP	. 32 . <i>32</i> . <i>32</i> . <i>34</i> . 35 . 37 . <i>38</i> . <i>44</i>
 4.5 4.6 4.6. 4.7 4.8 4.8. 4.8. 4.8. 4.8. 4.8. 	 优选 POP 隧道配置 <i>1 IPsec 端口配置</i> <i>2 OPENVPN 配置</i> INTERNET BACKHAUL 配置模板 <i>1 创建配置模板</i> <i>2 设置 PPPOE 重拨时间</i>	. 32 . <i>32</i> . <i>34</i> . <i>35</i> . <i>37</i> . <i>35</i> . <i>37</i> . <i>35</i> . <i>37</i> . <i>37</i>
 4.5 4.6 4.6. 4.7 4.8 4.8. 4.8. 4.8. 4.8. 4.8. 4.8. 4.8. 4.8. 	 优选 POP	. 32 . 32 . 32 . 32 . 32 . 32 . 32 . 32

	4.8.6	路由 Master 模式5	50
	4.8.7	安全组	50
	4.8.8	Per Host Police	51
	4.9	CPE-VPE 链路优化5	2
	4.10	CPE 多 LAN 配置5	3
5	、CP	PE 高可用配置(HA)5	4
	5.1 0	CPE HA 功能介绍5	4
	5.2	CPE HA 功能配置5	5
	5.3	基于路由的主备模式5	7
6	、点	对点线路5	7
	6.1	点对点功能介绍5	7
	6.2	CPE P2P 功能配置5	8
7	、远和	程办公6	2
	7.1	远程办公功能介绍6	2
	7.2	远程办公信息查看	2
	7.3	远程办公客户端接入6	4
	7.3.1	Windows	<i>55</i>
	7.3.2	MacOs	<i>;9</i>
	7.3.3	IPhone7	71
	7.3.4	Android	73
8	网络	监控7	'4

8.1	CPE 详情列表	4
8.2	CPE-POP 的网络品质监控70	6
8.3	CPE-POP 的流量监控7	7
8.4	CPE-ANY 的网络品质监控73	8
8.5	CPE WAN 口流量监控	0
8.6	应用流量监控	1
8.7	远程办公监控	3
0.0 8.0	扣升监控	0
8 10	4 心血注	׳ 8
0.10		0

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

南京未来网络产业创新有限公司

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:

	**(*(11))·	100
2 空制面板 ▶	帮助和支持	程序 (2)
VPN Access Manager		🔤 cmd.exe
iNode智能客户端		Git CMD
OpenVPN Connect		
💕 BE 🔸		grofile-50d105.js
PS Adobe Photoshop CS6(64 Bit)		find.4a38ff5c.js profile-50d105 is
SecureCRTPortable.exe		
▶ 所有程序		₽ 查看更多结果
<u>م</u>	● 关机 ▶	cmd × 义 义 关机 >
C:\Users\G.F>ipconfig		
Windows IP 配置		
以太网适配器 以太网:		
连接特定的 DNS 后缀		
本地链接 IPv6 地址.		. : fe80::f9dc:1be4:5b56:b250%5
IPv4 地址		. : 192.168.41.118
子网掩码		. : 255. 255. 255. 0
默认网关		. : 192.168.41.1

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:

→ C ▲ 不安全 192.1	68.41.1/løg	
如 M Gmail 🖸 YouTube	2 地图 〇 CNOS中国网络提 南京POP	
● 系统配置工具	🗘 系统	
	日志/重启/控制器地址	
	日志下载	点击下载
	客户端服务重启 运行中	点击重启
	设备重启	点击重启
	设备重置	置重击点
	控制器地址	协议 http
		IP地址或者域名 (示例: 192.168.30.1 或者 tethrnet.co 221.6.205.118
		端口
		9080
		保存

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:

🌻 系统	📥 网络				设备序	列号: 00257c3054	47b		型号:TE1203H 版本:2.2.9-9f7fdcd0		
	网络接口	无线	4G BGP配置	DHCP/DNS	网络工具						
网络接口											
☑ 自动刷新										关闭4G	
	状态	类型	出口类型	IP	MAC	RX(包)	TX(包)	RX(字节)	TX(字节)		
br-lan	UP	LAN		192.168.41.1	00:25:7c:30:54:7d	2106	741	298621	433548	配置 重启接口	
eth2	UP				00:25:7c:30:54:7d	2117	742	300879	433754		
eth3	DOWN				00:25:7c:30:54:7e	0	0	0	0		
eth4	DOWN				00:25:7c:30:54:7f	0	0	0	0		
wlp1s0	UP				b8:b7:f1:07:9b:55	0	755	0	140546	[]	
eth0	UP	WAN			00:25:7c:30:54:7b	0	16	0	3392	配置 重启接口	

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: 南京未来网络产业创新有限公司

网络接口			
br-lan			
接口类型	IPv4(示例: 192.168.0.1/24)		
LAN	▼ 192.168.41.1/24		
DHCP服务设置			
配置DHCP地址范围	起始IP地址	结束IP地址	租用时间 <i>地址租期,最小2分钟</i> (2m)
∠	192.168.41.10	192.168.41.200	50000h
配置网关	网关		
×	192.168.41.1		
配置DNS	DNS		

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<mark>禁用再启用</mark>,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(<u>必填</u>),如下图:

eth0		
接口类型 WAN 参数列表	接口协议 ▼ 静态地址	Y
IPv4	172.161.1.185/20	
IPv4网关(选填)	172.161.0.1	
DNS Server	221.6.4.66	

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:

🗰 无规则							以闰户列号.00237C303470		空与.10120.	эп дүхх.2.9-91	nacao
	网络接口	无线	4G	BGP配置	DHCP/DNS	网络工具					
4G基本信息											
4G功能:	开启				SIM卡状态:			连接状态:	未连接		
运营商:					信号质量:			APN:	3GNET		
IMSI:					网络注册:						
									关闭4G	<u>重置</u> 4G	刷新
4G设置											
APN					4G自动重连 开启后。	会每15分钟检查4G	状态,如果4G为离线状态则自动重置4G模块				
					□ 开启						
											保存

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。

南京未来网络产业创新有限公司

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:

🌻 系统	🛔 网络						设备序列号: 00257c30547b		
	网络接口	无线	4G	BGP配置	DHCP/DNS	网络工具			
无线设置									
SSID					加密方式			密码 ●	
dadi					WPA2		v	•••••	
频道					状态				
11(2.4G)				•	开启		v		

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:

奈	🛔 网络					设备序列号: b86a974c8d22
	网络接口	BGP配置	DHCP/DNS	网络工具		
网络工具						
Ping Tracer	route Nsloo	kup				
目标IP/域名				指定接口		
www.baidu.com	1				开始	
www.baidu.coi	m : [0], 84 bytes	, 1.48 ms (1.48	avg, 0% loss)			
www.baidu.co	m : [1], 84 bytes	, 1.46 ms (1.47 a	avg, 0% loss)			
www.baidu.co	m : [2], 84 bytes	, 1.38 ms (1.44 a	avg, 0% loss)			
www.baidu.coi	m : [3], 84 bytes	, 1.41 ms (1.43 a	avg, 0% loss)			
www.baidu.coi	m : [4], 84 bytes	, 1.44 ms (1.43 a	avg, 0% loss)			
www.baidu.coi	m : xmt/rcv/%lo	ss = 5/5/0%, m	in/avg/max = 1.3	38/1.43/1.48		

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。

	监控	配置	系统管理	₽						
		接入 CPE		🗲 专线	③ 点对点					
接入设	备	用戶配直	<u>الا</u>	。远程办公	◎ 全局配置	2 配置模板				
管理CPE、	专线等接入	设备更多								
CPE	专线 点	讨点								
CPE设备	CPE高可用	性HA								
創除	C 刷新 约	+ #定设备	₩ 扁韻设备	○ 自动刷新				序列号 🔻	搜索	
	序列号 (全部) ▼			最近在线时间	激活状态 (全部) ▼	POP (?)	VPE	?	连	接状态
	b86a974c8 (ceni_合肥)	d10 •		17秒前	●已激活	南京POP 广州POP	njvpe gzvpe	2		34 58

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";

④ 详情	面 删除		▶ 设备 ● 自	目动刷新			序列号 ▼ 搜索	
	用户	序列号	所属HA组	最近在线时间	激活状态 (全部) ▼	POP ?	VPE ?	连接状态 ⑦
	wuzijie	009027e0ae73 (CPE-A) ¹	(主)CPE-AB	2秒前	● 已激活	漕河泾1	wanda-vpeA	# ®

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)

编辑CPE设备			×
用户: wuzijie 序列号:			
009027e0e419			
设备管理配置	LAN配置	WAN配置 2	高级配置
LAN网络			
br-lan • 网络前缀: 10.0.6.0/24 DHCP类型: 开启 DHCF	中继 💿 关闭	* 网关: 10.0.6.1	
			关闭 保存

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。

Internet类型					
接口名	参数				接入类型
	优先级:	4	•权重:	1	
160	跟踪IP⑦:	114.114.114.114,8.8.8.8	跟踪检查间隔(秒):	例如: 10	
ensioo 10.10.0.13/24	开启NAT:		MTU:	例如: 1500	IPSec 🔻
(STATIC) 🕜 🗹	是否为4G接口⑦:		禁用到POP的Ⅰ⑦:		
	NON-Internet :		带宽(M):		
选中后控制器将无法配置 CPE的WAN口!!!	优先级:	4	•权重:	1	
	跟踪IP⑦:	114.114.114.114,8.8.8.8	跟踪检查间隔(秒):	例如: 10	
ens192 192.168.30.212/24	开启NAT:	~	MTU:	例如: 1500	IPSec v
(DHCP) 🕜 🗹	是否为4G接口⑦:		禁用到POP的Ⅰ⑦:		IPSec GRE考线 其他类体
	NON-Internet :		带宽(M):		泉池市政
专线类型					
接口名	参数				接入类型
					关闭 保存

◆ 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。

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:

南京未来网络产业创新有限公司

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;

可达网络	路由通告 ⑦			
QoS	LAN路由通告			
防火墙	网络	接口	类型	路由通告
NAT	10.0.6.0/24	br-lan	LAN	🖌 开启
DNS	高级选项 🗲			
WIFI				
优先POP	第三方路由器对接 🕜			
隧道配置	静态路由 💿 எ愛示意图			
Internet Backhaul	OSPF			
智能选路	BGP			
应用监控	本地互联网访问策略 ?			
路由过滤	兀酚目的IP			
多LAN				
	· 例如: 192.168.1.0/24. 输入一个或多个网络相当	(1947一个), 数多5000条		ĥ

◆ 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。

路由通告 ?				
LAN路由通告				
网络	接口	类型	路由通告	
10.0.1.0/24	br-lan	LAN	✔ 开启	

◆ 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。

高级选项 🕹			
WAN路由通告			
网络	接口	类型	路由通告
10.10.0.0/24	ens160(STATIC)	WAN	开启
192.168.30.0/24	ens192(DHCP)	WAN	一 开启
▪ 不推荐开启WAN路由透告。会自动关(▪ PPP类型接口不支持开启WAN路由透	闭此WAN接口的NAT功能,并且可能造成网 告	络故障	

♦ 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

✔ 静态路由 💿 配置示意图		
网络前缀	网关	是否通告
192.168.1.0/24 192.168.2.0/24 192.168.3.0/24	10.0.1.2	✓ 开启 ¥
		+

b) 0SPF 动态路由

备注: 0SPF 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

SPF						
OSPF Metrics:						
50						٢
						\
接口名称	网络前缀	类型	OSPF Area	Hello间隔(秒)	Dead间隔(秒)	开启OSPF
br-lan	10.0.1.1/24	LAN	0	10 🗘	40 🗘	一 开启

c) BGP 动态路由

BGP						
*Peer AS	Local AS	*BGP Peer	存活时间 (秒)	保持时间 (秒)	BGP密码	操作
Peer AS	Local AS	例如: 192.168.1.1	60	180		×
						+

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;

编辑CPE设	备
用户:	
layer_3	
序列号:	
005056b8f8	Bbf
设备名称:	
vCPE-8	
自定义排序:	根据设置的优先级排序,越大越靠前,例如:1
8888	

CPE设备 CPE	高可用性HA					
 ① 〕 □ □	2 + // 刷新 绑定设备 编编设备	● 自动刷新			序列号 ▼ 携	索
□ 用户	序列号	最近在线时间	激活状态 (全部) ▼	POP ?	VPE ?	连接状态 ⑦ (፲록) ▼
layer_3	005056b87c39 (vCPE-11) ¹⁰⁰⁰⁰⁰	20秒前	●已激活			1 î • C
layer_3	005056b8f7b9 (vCPE-10) ⁹⁹⁹⁹⁹	17秒前	●已激活			
layer_3	005056b8a35d (vCPE-9) ⁹⁹⁹⁹	21秒前	● 已激活			
layer_3	005056b8f8bf (vCPE-8 <mark>) ⁸⁸⁸⁸</mark>	28秒前	●已激活	漕河泾1 漕河泾3	wanda-vpeA wanda-vpeE	1 1

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:

设备管理配	置	LAN配置	WAN配置 2	高级配置
Q 搜索配置项				
可达网络 QoS	路由通告 ⑦ LAN路由通告			
防火墙	网络	接口	类型	路由通告
NAT	10.0.0/24	br0	LAN	✔ 开启
DNS	高级选项 🗲			
WIFI				
优先POP	第三方路由器对接 ?			
隧道配置	静态路由 💿 配置示意			
Internet Backhaul	OSPF			

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;

监控	配置系统管	锂				
	接入 🖸 CPE	🖌 专线	🔘 点对点			
用户配置	用户配置	远程办公		企 配置模板		
设置用户的应用定义	,远程办公,全局;	配置,配置模板…」	多			
应用定义 远程力	公 全局配置	配置模板				
2 + 刷新 添加					Q 搜索	

2 选择"应用定义"选项卡下面添加新的应用;

应用定	义 远程办公	全局配置 配置模	扳	
	+ 			
	app1	app2	app3	
A	1条规则	A 1条规则	A	

3 输入应用名称,通过五元组匹配应用。

▪应用名称:				
服务器地址 服务	器端口 协议	客户端地址	客户端端口	DSCP
以上规则满足任意一	·条即匹配该应用	∃	增加	识别规则 🔻
增加识别规则——				
服务器:	IP v	例: 8.8.8.8或1.1.1	0/24	
协议:	任意		*	
DSCP:	未设置		•	
		高	级 →	
添加				
配置需符合以下几 1.客户端或服务器 2.客户端、服务器 3.客户端和服务器 4.客户端和服务器 例:111.0/	山个条件: 器的IP不能为0.0 器、协议或方向函 器地址不能相同 器地址为子网时, /24(正确),1.1.1	.0.0,整个网络司 查少填一项 网络前缀为起始 I/24(不正确)]用O.O.O.O/O表; 地址	⊼
			×	闭保存
客户瑞地址 服务	·器地址 协议	客户瑞骑口 服	务器端口 DSCF	
	тср	52	01	
A app1 1条规则		app2 1条规则 孑		app3 1条规则

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; 南京未来网络产业创新有限公司

可达网络	流量分类
QoS	源地址 目的地址 协议 源端口 目的端口 应用 QoS类别 DSCP 类型
防火墙	
NAT	° , + , +
DNS	* * * 0
WIFI	
优先POP	
隧道配置	
Internet Backhaul	没有数据
智能选路	
应用监控	添加分类规则▶
路由过滤	
多LAN	

2 在 QOS 配置面板中, 定义流量分类规则;

添加QoS流量	量分类规则
	● 应用 ○ 自定义
选择应用:	可选择多个应用 → 点击选择/取消选中应用
QoS类型:	Internet OPOP
QoS类别:	金 ▼
+添加 QoS分类规则 1. 源或目的 2. 源、目的 3. 源和目的	则需符合以下几个条件: 到P不能为0.0.0.0,整个网络可用0.0.0.0/0表示 约或协议至少填一项 约地址不能相同
4. 源和目的 例:	3地址为子网时,网络前缀为起始地址 1.1.1.0/24(正确),1.1.1.1/24(不正确)

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;

- 添加QoS流量分:	类规则	
	🔾 应用 💿 自定义	
源:	IP v 例: 8.8.8.8或1.1.1.0/24	
目的:	IP ▼ 例: 8.8.8.或1.1.1.0/24	
协议:	任意	•
DSCP:	未设置	•
QoS类型:	Internet OPOP	
QoS类别:	±	•
+添加		

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"。

添加分类规则 🗸	
添加QoS流量分	类规则
	 应用 自定义
选择应用:	1个应用 → 点击选择/取消选中应用
QoS类型:	ERP ✔ 视频
QoS类别:	金 •
+ 添加	

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。

南京未来网络产业创新有限公司

带宽控制		
默认带宽 王新		
Internet(Kbps)		POP带费(Kbps)
QoS类别	保障速室	最大速率
internet设置		编辑 清空
金	70%	100%
银	10%	100%
铜	10%	100%
默认	10%	100%
POP设置		编辑 清空
金	70%	100%
银	10%	100%
铜	10%	100%
默认	10%	100%

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。

南京未来网络产业创新有限公司

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;





Input 规则								
源地址	目的地址	协议	源端口	目的端口	DSCP	方向	操作	<u></u>
			0 + + +	+ ° +				
* 可拖动每一项调	整配置顺序							Ψ.
添加配置 ▶ 保存	宇記置顺序							

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。

源地址	: 目的	地址	协议	源端口	目的端口	DSCP	方向	操作	
			2		+ • +				
					1 10-10				
				0.1	9 34 30				
				a.	1 34.70				
可拖动每−	-项调整配置顺	序		43	9 36.70				
可拖动每- ^{森加配置▼}	-项调整配量顺 保存配量顺序	序		a,	9 96 30				
可拖动每- ^{森加配置} ▼	-项调整配量顺 保存配量顺序 ward配置	序		a,	1 34 32				
可拖动每- ^{森加配量} ▼ 添加For	- 项调整配量顺 保存配量顺序 ward配量	序 		đ	20.30				
可拖动每- ^{藤加配置 ▼} 添加For 源:	-项调整配量顺 保存配量师并 ward配量 IP ▼	序 13.13.13.13		a.	90.10				
可拖动每一 ^{pp} 加配量~ 添加For 源: 目的:	- 项调整配置顺 保存配置顺序 ward配置 IP ▼ IP ▼	序 13.13.13.13 14.14.14.14	1	a,					
可拖动每一 赫加配重▼ 添加For 源: 目的: 协议:	- 项调整配量顺 保存配量顺序 ward配量 IP v IP v TCP	序 13.13.13.13 14.14.14.14	:						
可拖动每一 麻加配量 添加Fon 源: 目的: 力议: DSCP:	- 项调整配置顺 保持配置师 IP ▼ IP ▼ TCP 未设置	13.13.13.13 14.14.14.14	1						
可拖动每一 麻加BCE▼ 添加For 源: 目的: 日 文 に 方向:	- 项调整配置顺 保存配置顺序 ward配置 IP ▼ IP ▼ TCP 未设置 IN - POP	* 13.13.13.13	1						

Forward规则								
源地址	目的地址	协议	源端口	目的端口	DSCP	方向	操作	
13.13.13.13	14.14.14.14	TCP				IN - POP	拒绝	×
15.15.15.15	16.16.16.16	UDP				OUT - POP	拒绝	×
* 可拖动每一项调	整配量顺序							

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。

可达网络	本地 DNS 解析		Q 搜索	╋ ◆本地DNS解析
QoS	市 之	ID		品作
防火墙	+34-12	Ir		JA IF
NAT				
DNS				
WIFI				
优先POP				
隧道配置	代理 DNS 服务器解析		Q 搜索	+ 代理DNS解析
Internet Backhaul	域名	DNS服务器IP		操作
智能选路	• + ++파 뿌ᄜù \\ 65 등 1,627년 대 성 명	口店。如何要要的时间头融出的。	ᄵᅶᅂᄜᇂᇾᅠᆹᇑᆍᇰᇰ	
应用监控	"文持配直款认的DNS牌们版分态,	只填DNS版务器IP时即内默认的DNS,	<u>胖</u> 妍服分器,也配旦多余	
路由过滤				
多LAN				

域名规则			
源地址	域名	操作	
10.0.0/8	www.baidu.com	拒绝	×

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。

可达网络	DNAT规则				
QoS	转换后地址 转换后端口 协议 转换前地址 转换前端口 应用到				
防火墙					
NAT	° + • +				
DNS					
WIFI					
优先POP					
隧道配置					
Internet Backhaul	没有数据				
智能选路					
应用监控	添加配置▶				
路由过滤					
多LAN	SNAT规则				

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。

南京未来网络产业创新有限公司



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。
| 可达网络 | 当前POP: | 漕河泾3(wanda | a-vpeE) | 轲径2(wanda-vpeD) |
|----------------------|--------|---------------------------------------|-----------|-----------------|
| QoS | 选择POP: | ·
漕河泾1, 漕河泾2 | 2, 漕河泾3 👻 | 点击选择/取消选中POP |
| 防火墙 | | POP名称 | 优先级 | VPE端口 |
| NAT | | 漕河泾1 | 高 🔻 | 所有 🕜 |
| DNS | | 漕河泾2 | 高 🔻 | 所有 🕜 |
| WIFI | | · · · · · · · · · · · · · · · · · · · | ÷ | |
| 优先POP | |)曹泂)全 3 | | 所有 🗹 |
| 隧道配置 | | 保存 | | |
| Internet
Backhaul | | - C | | |
| 智能选路 | | | | |
| 应用监控 | | | | |
| 路由过滤 | | | | |
| 多LAN | | | | |

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;

司法网络			
山辺岡路	自动隧道		
QoS			
防火墙	自动隧道类型:	IPSec	
NAT			
DNS	IPSEC客户端		
WIFI	IKE协商端口:	选择或输入一个端口,支持范围配置,修	刘如1444-1445
优先POP	NAT端口:	默认500 1443	
隧道配置			
Internet Backhaul	IPSEC服务端		
智能选路	IKE协商端口:	1443	•
应用监控	NAT端口:	1444	•
路由过滤		■保存	
多LAN			

可达网络	14 14 17分2分		
QoS	日功隧道		
防火墙	自动隧道类型:	IPSec	•
NAT			
DNS	IPSEC客户端		
WIFI	IKE协商端口:	10	•
优先POP	NAT端口:	1444	
隧道配置			
Internet Backhaul	IPSEC服务端		
智能选路	IKE协商端口:	1443	•
应用监控	NAT端口:	1444	•
路由过滤		1444 1555	
多LAN			

3 全局下也可以进行配置, "配置 > 全局配置";

监控 配置 系统管理	
用户配置 layer_3 🔹	置模板,VPE-PE子接口连接,VPE路由,云加速…更多
应用定义 远程办公 全局配置 配 置	置模板 VPE-PE VPE路由 云加速
CPE全局配置	
IPSec :	
- IPSEC客户端	保存
IKE协商端口: <i>支持范围配量。例如</i> 1444-1445 1443	NAT端口: <i>支持范围配置,例如111-1115</i> 1444
IPSEC服务端	
IKE协商端口:	NAT端口:
1554 💌	1555 🔹

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。

可达网络	白动隧道	
QoS	口均规但	
防火墙	自动隧道类型:	IPSec v
NAT		OpenVPN
DNS	IPSEC客户端	創造室
WIFI	IKE协商端口:	1443 📼
优先POP	NAT _{端口} :	1444 👻
隧道配置		
Internet	IPSEC服务端	自清空
Backhaul	IKE协商端口:	1443 🔻
智能选路	NATHE	1444 -
应用监控	1001/101	
路由过滤		· 告保存
多LAN		
	OpenVPN 配置	
	服务器端口:	₩146234 系统管理隧道端口可以自定义端口
	协议:	TCP TCP/UDP ▼

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;

可达网络	置为HUB⑦:	
QoS	1	打开该选项将会发布默认路由,可能会影响其他站点的外网访问
防火墙		
NAT		
DNS		
WIFI		
优先POP		
隧道配置		
Internet Backhaul		
智能选路		
应用监控		
路由过滤		
多LAN		

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";

Ŷ	配置	系统管理	里							
ł	妾入设	法备 具开机								
管理CPE、专线、点对点等接入设备…更多										
	CPE	专线	点对点							
	CPE设备	CPE高可	用性HA							
	前 刑除	C 利新	+ / / / / / / / / / / / / / / / / / / /	 更多配量				Q	搜索	
		5 35		26/22		成员			ひ チャー	
		用户	-名称	VIP	HU 538	VRID	SN	心跳IP	₩ККР₩Ф	短虹尖型
		吴子捷	TE1203H-12	10.15.0.254	10.15.0.0/24	112	⊞ 00257c301ed9	10.15.0.253	2.0	none
		吴子捷	CPE-AB	10.11.0.254	10.11.0.0/24	12		10.11.0.252	2.0	none
	1个被选	中								

更多配置			>	:	🗸 开启	HA HUB成功 🔍 admin 🗙
其他						
置为HUB⑦:						
			关闭			
			জিয়া দ 4			
			图 54			
_	009027e0e419			漕河径3	wanda-vpeE	
吴子捷	(CPE-E) ⁹⁴	19秒前	● 已激活	漕河径2	wanda-111	/ î 🗹
				漕河泾3	wanda-vpeE	

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。

本地互联网访问策略 ?		
匹配目的IP		
例如: 192.168.1.0/24,输入一个或多个网络前缀(每行一个),最多5000条		1
匹配源IP		
例如 :192.168.1.0/24, 输入一个或多个网络前缀(每行一个),最多 5000 条		1,
		_
	关闭	保存

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";

	监控 配置	系统管理			
用户间	<u> 配置 gr</u> 捷	•			
设置用户	9的应用定义,远程办公,	全局配置,配置模板,VPE-PE子接口	连接,VPE路由,云加速	≢更多	
应用定	2义 远程办公 全局	配置 配置模板 VPE-PE VPE	路由 云加速		
前 制除	2 + _{刷新} 添加			Q	搜索
	名称	描述	已应用 CPE 数	创建时间	
	test-2104a		1	2020-04-20 1	9:32:35
	test-TE1203H01		1	2020-03-13 13	:12:53

更新配置模板			×						
基本信息									
配量模板名称: test -	2104a	描述:							
设备		策略	防火墙						
Device Manager									
密码:	admin								
SNMP									
SNMP版本:	○ 无	2 SNMPv3							
Community:	dms123!!								
CPE密钥									
CPE密钥⑦:	粘贴公明,通常包含在文件'~/.ssh/id	rsa.pub'中,以'ssh-rsa'开头。							
其他配置									
IPSec加密算法⑦:	AES-GCM	v							
OpenVPN加密算法⑦:	因密SM4	*							
WAN跟踪IP⑦:	例如: 114.114.114.114,8.8.8.8								
4G检查(?):	● 开启								
Internet Backhaul?:	开启 打开该送动将会发布就认为	5亩。可能会影响其他站点的外网访问	9						
·◎◎DF-BH(): PPPOE重投时间():	E ^L								

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										
配量模板名称:	test-2104a				描述	:				
	投备			策略	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	Ž	<u> 1 전</u>			
	app0				全	p	ор		×	
					银	P	ор		×	
	添加分类规则									
Transport										
	名称	类别	接入粪	型						
	Internet	Internet	VPE	aneat an	点IPSec 建波			Z	×	
	Direct	辛线	无					Z	×	
								+		

更新Transport						×		
*名称:	Internet							
*类别:	ті							
接入类型 🝞: 🛛 🕦	VPE自动隧道				~			
			已选 WANI 、					
	Tunnel MTU,	Tunnel MTU,例如:1500						
	55		% - 1		分钟			
	QoS 类别	保障速率		最大速率		×		
				编辑	重量			
	金	70%		100%				
	银	10%		100%				
	铜	10%		100%				
	默认	10%		100%				

Transport							
	名称	类别	接入类型				
	Internet	Internet	VPE自动隧道	点对点IPSec能	道	ľ	×
	Direct	Tunnel MTU: 专 带宽告警阈值: 告警持续时间: WAN: WAN1	: 55% : 1分钟			a	×
应用收款		QoS类别	保障速率	最大速率			
		金	70	100			
选择应用:	~	 银	10	100			
安田台长3 <u>年</u> 回初			10	100			
笛 尼 匹 哈		默认	10	100			
选路方式:	● 基于路由						

4 将配置模板与 CPE 管理

应用定	2义 远程办公	全局配置 配置模板	VPE-PE VP	E路由 云加速	
節 删除	2 + _{刷新} 添加				Q 搜索
	名称	描述		已应用 CPE 数	创建时间 应用到CPE
	test-2104a			1	

应用配置模板到CPE		×
选择CPE:		
下拉选择CPE,可选择多个		
005056b87cf6 - vCPE-2 005056b8b2a8 - vCPE-3 8cea1b004e54 - awifi-1 005056b8fb1f - vCPE-7		
005056b8f8bf - vCPE-8 005056b8a35d - vCPE-9 005056b8f7b9 - vCPE-10	选择需要管理的CPE	01
005056b87c39 - vCPE-11		

应用定	义 远程办公	全局配置	配置模板	VPE-PE	VPE路由	云加速		
<mark>面</mark> 删除	2 + _{刷新} 添加							Q 搜索
	名称	描述			已应月	用CPE数	创建时间	已应用的CPE
	test-2104a				1		e 🗋 1	

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;

可达网络	
QoS	
防火墙	
NAT	
DNS	可达网络
WIFI	可に変換す
优先POP	
隧道配置	QoS
Internet	NAT
Backhaul	DNS
智能选路	WIFI
应用监控	优先POP
路由过滤	隧道配置
多LAN	多LAN

可达网络	当前应用的配置模板为: te	est-2104a						
配置模板	为不同接入类型洗择专线.							
QoS								
NAT	WAN接口	接入类型		专线				
DNS					日保存			
WIFI	配置模板更新.							
优先POP								
隧道配置	设备		策略		防火墙			
多LAN	Device Manager							
	密码: admin							
	SNMP							
	SNMP版本: 〇 无	SNMPv1/SNMPv2	SNMPv3					
	Community: dms123!!							

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;

其他配置	
IPSec加密算法??:	AES-GCM 🔻
OpenVPN加 ?):	国密SM4
WAN跟踪IP?):	例如: 114.114.114.8.8.8.8
4G检查?):	● 开启
Internet Bac ?:	○ 开启 打开该选项将会发布默认路由,可能会影响其他站点的外网访问
清除DF-BIT?):	● 开启
PPPOE重拨时…?:	配置
	☞更新

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;

Transport					
	名称	类别	接入类型		
	Internet	Internet	VPE自动隧道(点对点IPSed隧道)	ľ	×
	Direct	专线	无	ľ	×
应用收纳					
应用面征					
选择应用:					
智能选路					
选路方式:	● 基于路由	○ 基于应用			
默认策略:	Internet 🔻				
	Direct		策略		
优先策略:					+

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";

监控 配置 系统管理			Я
接入 CPE	🖌 专线 🛛 💿 点对点		
	🗐 远程办公 🎯 全局配置	29 配置模板	
设置用户的应用定义,远程办公,全局配置, 应用定义 远程办公 全局配置 配	, 配置模板更多 置模板		
CPE全局配置			
IPSec :			
IPSEC客户端		保存	
IKE协商端口:支持范围配置,例如444-1445 1443	NAT端山: <i>支持范围配置,例如444-14</i> 1444	145	

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。

Overlay网络 Overlay网络			
名称	拓扑类型		
hub-spoke	HUB-SPOKE	×	
full-mesh	FULL-MESH	×	
			+ 増加

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;

DSCP 设置DS	CP										
金	未设置	•	银	未设置	铜	未设置	•	默认	未设置	•	保存

4 在智能选路中选择基于应用;

Transport					
	名称	类别	接入类型		
	Internet	Internet	VPE自动隧道(点对点IPSed隧道)	I	×
	Direct	专线	无	(B)	×
应田监控					
选择应用:	\checkmark				
智能选路					
选路方式:	🦳 基于路由	 基于应用]		
	可配置: 1. 指定的 2. 当指定 3. 非指定	的应用走 Interne E路径断掉后,可 E的应用走默认题	■t或专线 可配置每个应用是否自动切换到另外一条路径 路径		

5 选择需要放入指定链路的应用;

智能选路 选路方式:	◯ 基于路由 ● 基于应用	3				
	可配置: 1. 指定的应用走Interne 2. 当指定路径断掉后,可 3. 非指定的应用走默认路	t或专线 可配置每个应用是否自动切换到 格径	则另外	一条路径		
指定应用:	4个应用 ▼	点击选辑/取消选中应用				
	应用名称	路径		故障切换机制 🕐		
	test2	Internet	•	自动切换	•	
	test4	Internet	•	自动切换	•	
	TCP5201	Internet	•	自动切换	-	
	аррО	Direct	Ψ.	不切换	-	
	▪其他应用	ECMP	•	不切换	▼	
	Internet 50	% Direct 50		%		

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。

Overlay网络			
	名称	拓扑类型	
Overlay网络:	hub-spoke	HUBSPOKE	×
			٠

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'

路由过滤				
白名单策略:	网络前缀	策略	方向	严格匹配⑦
	网络前缀	策略	方向	严格匹配②
黑名单策略:	14.14.14.0/24 15.15.15.0/24	本地 🔻	IN v	×
				+

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。

Transport				
	名称	类别	接入类型	
	Internet	Internet	VPE自动隧道	ĭ ×
	高级选项 ↓ 是否为I	Master		•

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。

安全组			
			*
	安全组名	网段	
	添加安全组▼		*
	- 添加安全组		
	安全组名称:		
	网段:	例如: 192.168.1.0/24 ,输入一个或多个网 络前缀(每行一个),最多 10000 条	
	◆ 添加		

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。

Host 限速						
						•
	网段		限速额 (K)	类型		
	10.0.255.0/24		4096	internet	×	
	10.0.255.0/24		4096	рор	×	
	添加Host限速 ▼					*
	- 添加Host限速					
	网段:	172.21.0.0/16				
	限速额 (K) :	4096				
	类型:	Internet V				
	╋添加	POP				

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;

左右	史女	任	12
τĿ	ĿЦ	1/1-1	1

优化策略: 自动 开启 • 关闭 未配置 链路优化功能开启后会占用更多带宽。若选择自动,系统将在链路质量无差包时关闭优化功能,链路质量较差时开启优化功能。

□保存

链路优化	图 84
优化策略: 自动 • 开启 关闭	
QoS类别	链路优化
金	
银	
铜	
默认	
	吉保 谷

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:

可达网络	多LAN		+ 添加
QoS	LAN名称	物理端口(多选)?	
防火墙 NAT	br-lan(默认)	eth3, eth2	∂ X
DNS	MGMT	eth4, wlp1s0	ð ×
WIFI	例如:lan1	eth4 ^ eth3 wh3c0	✓ Ø

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。

设备管理	理配置	LAN配置	WAN	配置 3	高级配置
LAN网络					
MGMT					
*网络前缀:	10.12.0.96/28		*网关:	10.12.0.110	
DHCP类型:	 ● 开启 ○ DHCP中继 ○ ; 	关闭			
*地址范围:	10.12.0.105	- 10.12.0.109			
DNS?:	10.12.0.110				
租约时间?:	lh				
	高级选项 🗲				
br-lan					
*网络前缀:	10.8.0.96/28		*网关:	10.8.0.110	
DHCP类型:	 ● 开启 ○ DHCP中继 ○ # 	关闭			
*地址范围:	10.8.0.105	- 10.8.0.109			
-					

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。

可达网络	路由通告 ?			
QoS	LAN路由通告			
防火墙	网络	接口	类型	路由通告
NAT	10.8.0.96/28	br-lan	LAN	✓ 开启
DNS	10.12.0.96/28	MGMT	LAN	✓ 开启
WIFI	高级选项 →			
优生DOD				

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。SDWANCPE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VisualIP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;

CPE设备	备CPE高可用性	ĚΗΑ						
<mark>面</mark> 删除	2 刷新 添加	▲ 編辑 更多酯	em 🖷			Q	搜索	
			成员			心江米刊		
	 山小	VIP	日山均和	VRID	SN	SN 心跳IP		验证关望

2 在 HA 配置面板中, 输入 HA 组的配置信息;

绑定CPE为HA模式	×
HA设置	成员设置
基础设置	
• HA组名: 数据中心 高级洗面 ▲	*VRID: 10
LAN网络	
* VIP: 10.0.0.1 开启DHCP:	*前缀: 10.0.0.0/24

♦ HA 组名

作用: HA 组的标识

描述:可以是中文或者英文

\diamond 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

\diamond 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。

	HA设置		成员设置	
设备号	参数			
000c29f0a229 - 数据中心-主	*优先级: *心跳IP: ▼ WAN跟踪接口: LAN接口:	 ✓ 是否为Master 高级 → 10.0.0.2 eth0 マ br-lan 	▼	×
000c29af244c - 数据中心-备	 ・优先级: ・心跳IP: ▼ WAN跟踪接□: LAN接□: 	 是否为Master 高级 → 10.0.0.3 eth0 ▼ br-lan 	▼	×
				+ 取消 保存

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。

OSPF						
OSPF Metrics:						
主CPE: 50/名	똛CPE: 100					\$
接口名称	网络前缀	类型	OSPF Area	Hello间隔(秒)	Dead间隔(秒)	开启OSPF
ens224	10.0.255.254/24	LAN	0	10	40	🖌 开启

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 O Hub-Spoke					
连接方式:	● IPSec ○ 专线					
选择CPE:	2个CPE → 点击选;	释/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-S	òpoke			
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	

沃山	노고	나는	本 幸
邻川	尻刃	13.	比按

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↑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 🛛 💿 I	Hub-Spoke				
连接方式:	IPSec 💿 GRE	○ 专线				
选择CPE:	2∱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 - CP E-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

添	加点	对点	ī连	倿
_				

选择用户:						
吴子捷						•
描述:	CPE-E					
拓扑模式:	Full-Mesh 💿 H	lub-Spoke				
连接方式:	IPSec GRE	● 专线				
选择CPE:	2个CPE ▼	点击选择/取消选中0	CPE			
	设备SN	WAN端口	BGP 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

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。

		005056b87c39(vCPE-11)	ens160				查看详情	
layer_3	CPE-IPSEC -3	005056b8a35d(vCPE-9)	ens160	是	ø	ø	i •	
		005056b8f7b9(vCPE-10)	ens160					

本端配置	对端配置	连接状态
设备SN: 005056b8f7b9(vCPE-10) 端口: ens160 隧道IP: any 隧道接口IP: 100.69.58.81/30 ☑	设备SN: 005056b8a35d(vCPE-9) 端口: ens160 隧道IP: 192.168.30.89 隧道接口IP: 100.69.58.82/30 ☑ <u>点击可查看流量</u>	● 成功 延时:0.36ms 丢包:0%
设备SN: 005056b87c39(vCPE-11) 端口: ens160 隧道IP: any 隧道接口IP: 100.69.58.93/30	设备SN: 005056b8a35d(vCPE-9) 端口: ens160 隧道IP: 192.168.30.89 隧道接口IP: 100.69.58.94/30 ☑	● 成功 延时:O.37ms 丢包:O%

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	★ 专线 (
	. 远程办公	◎ 全局配置	2 配置模板	
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	久 4	
用户配置:				
用户配置:	Q	搜索	+ 增加用户	
用 户配置: 用户	Q 密码	_{搜索} 最大连接数	+ 增加用户 操作	

应用到VPE:

将上述连接配置、用户配置应用到指定的一个或多个VPE

VPE名称	VPE IP	配置
		Client IP? : 100.70.0.4
njvpe (南京)	221.6.205.122-ens160 (中国联通/网通)	限速(M): 50
		DNS? :
		114.114.114
gzvpe1 (广州)	210.21.33.126-ens160 (中国联通/网通)	

远程办公信息

基本信息:

	✔ 开启	🖌 开启	公网IP	运营商	所属POP	
服労蓄地址:		~	221.6.205.122	中国联通/网通	南京远程办公	

远程办公的三种用户接入信息和配置如下图:

	:	最大连接数:		2				
	:	连接类型?:		OpenVPN	IPSec	PPT	Р	
		客户端配置:	Q	⊗ ovpn_clie	ent.ovpn			
最大连接数:	2							
连接类型?:	OpenVP	N IPSec	PPTP					
预共享密钥:	VPN@s	dwan		IPSe	ec标识 🤇	?: a	aaaaa@vpn.sdwan	

£.

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:

	网络和 Internet > 网络和共享中心 + 4 接卖控制面板	P	00-T	0	۹ 💌
		20 -	お利用店	(二) 肇 设置连接或网络	0 -
江朝國政主义	查看基本网络信息并设置连接		TTATATOC		
更改适配器设置	i 🙀 —— 🎐 —— 🌒 🏛	完整映射	更改适配	选择一个连接选项	完整映射
更改高级共享设置	WXLI-PC 多重网络 Internet		更成微级		
	(此计算机)				採开生培
	查看活动网络 连接或	断开连接		● 议直无线、范市到335号连续,连续到 internet。	AND LODIE
	词上,网络 访问类型: Internet			· 设置新网络 和图新的路由图成注闭点	N
	正作网络 连接: ↓本地连接	-			- 5
		=		ま 接到工作区 各番単物的工作区的提号或 VPN 法接	
	「「」 M 3 访问単型: デ法法接到 Internet				
	正作网络 连接: ↓本地连接 2			つ 後置接号连接 伸用提号连接连接到 Internet.	
	更改网络设置				
	2 设置新的连接或网络		另请参阅		
另请参阅	设置无线、宽带、拨号、临时或 VPN 连接;或设置路由器或访问点。		Internet		
Internet 选项	★ 注接到网络		Window	頭 (N)也一可	ř.
Windows 防火墙	连接到或重新连接到无线、有线、拨号或 VPN 网络连接。		家庭组	选择家庭组和共享选项	
家庭组	" 法探索或识和共享许师				10:07
	W REFERENCE AND A REFERENCE AN	•	😏 😕) 📑 🔍 😲 📴 👘 👘	2019/9/23
20			1		
00-1			00	- T	
			0		
控制面板 😏 🕍 建接到上	LTER		控制	動版 🤤 🔐 建規則工作区	- Vil
更改适配 您想使用	一个已有的连接吗?	完整映射	更改這	an 您想如何连接?	完整映射
更改高级			更改推	音级	וו ו
●否, 台	创建新连接(C)			→ 使用我的 Internet 连接(VPN)(I)	
◎是,ÿ	先爆现有的连接(E)	進行十座接		通过 Internet 使用器纵专用网络(VPN)未通接	断开连接
	VPN 连接	E			
				and the second sec	
				→ 直接拨号(D)	
				AVELUINE INCLUSION SATATION.	
另请参阅			另请任	参河 <u>什么思 VPN 连接</u> 2	
Internet			Interr	net	
Window	下一步(N) 取消		Wind	wot	X
家庭组	· 选择家庭组和共享违项	-	家庭的	目 通道 选择家庭组织共享选项	
			and the second s		
A M		10:08			10:08

A							
		0	2011 控制面板	3 🛄 连接到工作区			0
更改活配	键入要连接的 Internet 地址 	完整映射	更改适配	键入您的用户名和密码	输入用户名和密码		完整映射
	网络管理员可提供此地址。	斯开连接	SCIAIRING	用户名(U):	user1@aaaaa.sdwan		漸开连接
	Internet XBat(): 目标名称(E): VPN 连接			密码(P): [test123!!] 显示字符(S)		
				城(可选)(D):	记住此密码(R)		8
	□ (00号着船中(5) ● たド其他人使用応注款(A) ☆今夜近今年回じ次回次会+置前的人体用化法接。						
	□ 现在不连接:(仅进行设置以便陶后连接(D)						
另请参阅 Internet			另请参阅 Internet				4.
Windown 家庭组	下一步(N) 取消 3. 选择家庭组织共享选项]	Window 家庭组	31 . 洪	探索庭识和共享洗项	连接(C) 取满	
()) 🔅 💽 👰 🖉 👘	10:09 2019/9/23	👌 🙆			сн — 🤮 🐔 🛊 👍	10:10 2019/9/23

◆ 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;

O Shrew Soft VPN Client Setup			×
Software Edition Choose the software edition you would like to install.	T	SHREW SO	FT. LIENT
Please select one of the following options:			
O Professional Edition			
This edition offers all the Standard edition features as well as seve helpful for users connecting to a corporate LAN. It will install with a limit. To use the Professional version after the evaluation period ha	ral features 14 day eval as expired, a	that may b luation per client licer	e iod ise
Standard Edition This edition provides a robust feature set that allows the user to coopen source and commercial gateways. It is free for both personal	onnect to a v and commer	vide range cial use.	of
Nullsoft Install System v2,46	Next >	Can	cel

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;

		VPN Site Configuration
OVPN Access Manager		General Client Name Besolution Authenticatic
File Edit View Help		
		Remote Host
Connect Add Modify Delete		172.21.251.233 500
Connection Name Host Name	Authentication	Auto Configuration ike config pull
	mutual-psk-x	Local Host
🚯 shrew_prof_example.vpn 172.21.251.233	mutual-psk-x	Adapter Mode
		Use a virtual adapter and assigned address 🔹
		MTU 👽 Obtain Automatically
		1300 Address
		Netmask
< III	•	
	.#	Save Cancel
VPN Site Configuration	VPN Site Configuration	
-----------------------------------------------------------	--------------------------------------------	
Client Name Resolution Authentication Phase	Authentication Phase 1 Phase 2 Policy	
Authentication Method Mutual PSK + XAuth	Authentication Method Mutual PSK + XAuth	
Local Identity Remote Identity Credentials	Local Identity Remote Identity Credentials	
Identification Type User Fully Qualified Domain Name 👻	Server Certificate Autority File	
UEQDN String aaaaa@vpn.sdwan	Client Certificate File	
	Client Private Key File	
	••••••••••••••••••••••••••••••••••••••	
Save Cancel	Save Cancel	

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:

(i) VPN Access Manager File Edit View Help (i) (i) (ii) (iii) (iii) (iiii) (iiii) (iiii) (iiii) (iiiii) (iiiii) (iiiii) (iiiii) (iiiii) (iiiii) (iiiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) (iiii) <t< th=""><th>-</th><th>×</th><th>Image: Symplectic symple</th></t<>	-	×	Image: Symplectic symple
			Credentials Username Password Connect Exit

◆ 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;

连接类型?:	OpenVPN	IPSec	PPTP
客户端配置:	⊗ ovpn_clie	ent.ovpn	

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。

OpenVPN Connect		OpenVPN Conne	ct	– ×
	Import Profile		K Edit Profile Sav	
URL	FILE	Access Server 172.21.251.2	Hostname (locked) 33	
Drag and drop to upload You can import only one	d .OVPN profile. profile at a time.	Profile Name 172.21.251.2	33 [ovpn_client]	
	2	Server Over	rride (optional)	
	\supset	Username user1@aaaa	aa.sdwan	
		Save pas	sword	
BROWSE	\supset	Password test123!	!	

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;

		网络		٩	搜索
诸	选择接口并为新朋	服务输入名称。			
● Wi-Fi 已连接	接口: VPN 类型:	VPN Cisco IPSec		0	
● 蓝牙 PAN 未连接	服务名称:	vpn			
● USB Seonve 未配置			取消 创建		٢
● USB 10/00 LAN 未连接	>			连打	g
<mark>● VPN (L2TP)</mark> 未连接					
 ● 雷雳网桥 未连接 	>				
● VPN (Cio IPSec) 未连接					
+ - *~	设置	፤蓝牙设备		i	高级 ?
				复原	[应用

2 填入服务商提供的服务器地址,用户名,密码等信息;

$\bullet \bullet \bullet \checkmark \checkmark \blacksquare$	网络	Q. 搜索
位置:	自动	
 Wi-Fi 已连接 蓋牙 PAN 未连接 	状态: 未连接	
	服务器地址: 1.2.3.4 帐户名称: userl@aaaaa.sd 密码: test123!! 鉴定设置 连接	wan
朱连接 ▲▲ + - ◆	✓ 在菜单栏中显示 VPN 状态	高级 ? 复原 应用

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;

	网络	○ 搜索
● Wi-Fi 已连接 ● 蓝牙 PAN 未连接 ● USB Seonverter 未配置 ● USB 10/00 LAN	 ※定: 共享的密钥: VPN@sdwan 证书 选择 群组名称: aaaaa@vpn.sdwan 取消 好 服务器地址: 1.2.3.4 	
未连接 VPN (L2TP) 未连接 雷雳网桥 <···>	帐户名称: user1@aaaaa.sdwan 密码: ••••• 鉴定设置	
● VPN (CLo IPSec) 未连接 ● vpn 未连接	连接	
+ - *	☑ 在菜单栏中显示 VPN 状态	高级 ? 复原 应用

4 点击"连接"按钮。

	网络	Q 搜索
位置	t: 自动 🗘	
Wi-Fi 一 已连接 一 盛牙 PAN 未连接 USB Seonverter *和配置 USB 10/00 LAN *基接 VPN (L2TP) *走接 電雳网桥 *连接 VPN (Cio IPSec) 未连接 · vpn *连接	状态: 未连接 服务器地址: 1.2.3.4 帐户名称: user1@aaaaa.sdwar 密码: ・・・・・ 鉴定设置 连接	1
+ - &-	✓ 在菜单栏中显示 VPN 状态	高级 ?
		复原 应用

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;

5:46 🕫		#! ≎ ■
く通用	VPN	
VPN配置		
状态		未连接
✓ 公司 ^{未知}		í
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;

取消	添加配置	完成
	cisco	
类型		IPsec >
描述	test	
服务器	1.2.3.4	
帐户	user1@aaaaa.SdWaN	
密码	test123!!	
使用证书		
群组名称	aaaaa@vpn.sdwan	
密钥	VPN@sdwan	

3 选中新建立好的 vpn,并点击连接按钮。

5:5	50 V		::!! ? 🗩
く设置	ĩ	VPN	
VPN	配置		
状态	-		未连接
	公司 ^{未知}		í
\checkmark	test 未知		í
添加]VPN配置		

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。

\diamond 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。

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	÷
编辑VPN配直文件	
4.40	
test	
类型 IPSec Xauth PSK 服务器地址	•
1.2.3.4	
IPSec 标识符	
aaaaa®von.sdwan	
IPSec 预共享密钥	
VPN@sdwan	
□ 显示高级选项 ^{用户名}	
user1@aaaaa.sdwan	
密码	
test123!!	
□ 始终开启的 VPN 必须为始终开启的 VPN 指定 DNS 服务	22
ЦU Й	保存

### ♦ 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。

Σ		202 K/s 🏹	1	00%	18:00
					+
0	编辑VPN函 ^{名称} test	習堂文件			1
¢	类型 PPTP 服务器地址 1.2.3.4				I
	✓ PPP加密 □ 显示高级 用户名 user1@aaaa	舒(MPPE) 及选项 ia.sdwan			I
	密码 test123!!				
	□ 始终开启 此VPN类型无法	目的 VPN 去随时保持连接			I
	Δ	0			

# 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:

CPE列表 🛃										
<b>序列号 -</b> 搜索										
序列号 ▲	潮活出太	最近在线时间	CDU	内友③	VDE			流量		
	1981日1人心。 - 政元1115341110			VPE	E12-Mas	类型 ?	RX/TX(bps)	应用		
005056b8172e (vCPE-1) ⁷⁰	● 己激活	10秒前	5.00%	18.16% (2.05G)	wanda-vpeA wanda-vpeD	1	eth2() eth1(WAN) eth0(WAN) POP	540.1b         527.1b           5.1K         1.7K           35.7K         28.7K           5.5K         3.2K	~	
005056b82238 (vCPE-4) ⁴⁰	● 己激活	3秒前	5.00%	22.98% (2.04G)	wanda-vpeE wanda-vpeD wanda-vpeE	0 0 专线0.15	ens224() ens192(WAN) ens160(WAN) POP	67.1b         68.8b           5.5K         4.1K           32.5K         24.7K           5.6K         5.7K	~	

点击 CPE 的序列号,可以进入 CPE 详情页面:

### 设备(b86a974c8d10)的信息



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;

PE到VPE的链路监控图		×
CPE到VPE的链路监控图 CPE到V	/PE的隧道监控图	
		Zoom Out 🛛 Last 60 m 😂
上行带宽 1.5 kbps	下行带宽 1.5 kbps	隧道中断
1.3 kbps 1.0 kbps 750 bps	1.3 kbps 1.0 kbps 750 bps	No data points
250 bps 14:00 14:30 - 00257c305462	250 bps 14:00 14:30 - 00257c305462	14:00 14:30
延时(RTT) 18.5 ms	<b>丢包率</b> 100.0%	<b>1</b> 約志力 3.0 ms
18.0 ms	50.0%	2.5 ms
17.0 ms	-50.0%	1.5 ms
16.0 ms 14:00 14:30	-100.0% 14:00 14:30	0 ms 14:00 14:30

## 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。

### CPE(00257c305462)到POP的流量监控状态



## 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;

序列号 ▲	谢话带本	最近在线时间	近在线时间 CDU 内存	内友 ②	VDE	连接带本	流量		
		政 过 11 \$34010	CPU	NJIT 🕕	r 313 🕔 🛛 VPE		类型 ?	RX/TX(bps)	应用
					wanda-vpeA	1	eth2()	<b>622.5b</b> 532.5b	
005056b8172e	<mark>72e</mark> 70 ● 已激活	の手小台の	E 0.0%	18.15%	wanda-vpeD	0	eth1(WAN)	<b>5.5K</b> 1.8K	1.4
(vCPE-1) ⁷⁰		の作り用り	5.69%	(2.05G)			eth0(WAN)	<b>39.2K</b> 29.5K	~
							POP	5.6K 3.0K	

## 2 在监控面板下添加指定的目标 IP 地址信息;

	设备信息			监控
连通性测试				度焊键通性
出接口名或源 IP	测试IP	描述	告警阈值(丢包%/抖动ms/延时ms)	
^{添加测试P} ▼ 添加测试IP -				
选择出接口或转	俞入源IP:			
不指定				v
⁺待测试IP:				
114.114.114.114				
○ 单次测试	💿 连续测试			
描述:				
維路測试				
提交测试				
* 连续测试的IF	<b>2</b> 会加入上述表中,可点	<b>〔击查看历史</b>	测试监控信息	



# 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;

序列号 ▲	谢活状态	最近在线时间	CPU 内存 ⑦		VPE	连接状态	流量		
			cro	F 3 I 3 💽	VI L	21 JA 10 10	类型 🝞	RX/TX(bps)	应用 ]
005056b8172e (vCPE-1) ⁷⁰	● 已激活	8秒前	5.60%	18.16% (2.05G)	wanda-vpeA wanda-vpeD	1	eth2() eth1(WAN) eth0(WAN) POP	467.7b         598.6b           5.3K         1.9K           36.0K         26.6K           5.4K         2.8K	]

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;

应用监控:	2个应用 🔸	点击选择/取消选中应用	
	应用名称	开启监控	
	ERP		
	视频		
	保存		

2 配置模板 > 策略中也可以开启应用监控;

应用监控		
选择应用:	TCP5201 ×         app0 ×         test2 ×         test4 ×	

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;

序列号 ▲	游迁伏太	最近在线时间 CDU 内容		内方③	为存⑦ VPF		流量		
		4X ///1123/2413103	CFU	1117 🕔	VFL	庄琅1八心	类型 🝞	RX/TX(bps)	应用
005056b8172e (vCPE-1) ⁷⁰	●已激活	13秒前	5.90%	18.25% (2.05G)	wanda-vpeA wanda-vpeD	0	eth2() eth1(WAN) eth0(WAN) POP	439.1b         620.7b           5.6K         2.1K           36.1K         26.5K           5.8K         3.0K	

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							
<b>Q</b> 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			查看远程办公流重
<b>Q</b> 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-vpnOO2)的连接中断,接入方式是:« 源IP是192.168.200.85, 在线时长为:1hOmOs, 总下载流量为:OBB, 总上传流量为:	openvpn, 2020-04-23 19:21:5 91.9KB	2
wuzijey	wuzijie名下的wuzijey通过POP点(remote-vpnOO2)连接成功,接入方式是:op IP是192.168.200.85	envpn, 源2020-04-23 18:21:5	2
wuzijey	wuzijie名下的wuzijey位于POP点(remote-vpnOO2)的连接中断,接入方式是: 源IP是192.168.200.85, 在线时长为:1hOmOs, 总下载流量为:OBB, 总上传流量为:	openvpn, 2020-04-23 18:21:4 106.9KB	6
wuzijey	wuzijie名下的wuzijey通过POP点(remote-vpnOO2)连接成功,接入方式是:op IP是192.168.200.85	envpn, 源2020-04-23 17:21:4	6



VILJUNE								
Q 搜索								
名称	管理ID	CPU	内存 ②	谢活状态。	È	(联设备数		法量
-11 1/1,		CFU	1 3 13	WITH POOLEDY -	CPE	VPE	PE	加重
BJ-OFFICE-Private-V	139.198.255.126	-	-	管理关闭	0	0	0	~
remote-vpn	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:

## 日志

#### 查看操作日志,点击每天记录可查看具体信息

1小时 1天 7天 1个月 3个月 1年 2年 3年	i .		全字段搜索
描述	方法	结果	时间
修改所监控的IP	PUT	成功	2020-06-08 15:16:51
修改所监控的IP	PUT	成功	2020-06-08 15:16:17
修改所监控的IP	PUT	成功	2020-06-08 15:12:31
配置可达网络	PUT	成功	2020-06-08 10:15:50
claim cpe	PUT	成功	2020-06-08 10:15:10
删除cpe	DELETE	成功	2020-06-08 10:14:34
/wan/cpe/00257c30543a/wanconfig/proto	PUT	成功	2020-06-08 10:13:37
新建Profile	POST	成功	2020-06-07 11:24:08

## 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	号过滤: 所有	有	Ŧ		全字段搜索	€刷新	☞ 配置告警
B	时间	类别	子类别	严重级别	关联ID	消息	状态	
2	2020-06-07 9:54:19	CPE	CPE <u>上</u> 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
2 1	2020-06-05 6:10:12	CPE	CPE <u>上</u> 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
2	2020-06-05 3:14:42	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	解除告答
2	2020-06-05 3:09:51	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	解除告答