华智达ANP 2.0 SD-WAN技术白皮书

文档名称	华智达ANP 2.0 SD-WAN技术白皮书
版本号	V2.0
拟制人	
发布日期	2020-9-1

1. 术语和缩略语

本文档所使用通用术语、缩略语请参见下表。

序号	术语/缩略语	英文含义	中文含义
1	ANP	Autonomous Network Platform	自治网络平台
2	ASG	Access Security Gateway	安全接入网关
3	CPE	Customer Premise Equipment	用户前置设备
4	gRPC	google Remote Procedure Call	谷歌远过程调用
5	LAN	Local Area Network	局域网
6	LCA	Local Control Agent	本地控制面代理
7	NAT	Network Address Translation	网络地址翻译
8	NVE	Network Virtualized Edge	网络虚拟化边缘
9	POP	Point Of Presence	入网点
10	RPC	Remote Procedure Call	远过程调用
11	SDN	Software defined Networking	软件定义网络
12	SD-WAN	Software defined WAN	软件定义广域网
13	VPC	Virtual Private Cloud	虚拟私有云，一般指公有云的一个租户网络
14	VPN	Virtual Private Network	虚拟专用网
15	VXLAN	Virtual Extensible LAN	虚拟可扩展局域网
16	ZTP	Zero Touch Provisioning	零接触部署

2. 背景

企业的业务发展内在需求、商业环境变化和技术的发展三种力量驱动了企业广域网的持续演进。

- 企业因业务发展需要快速地在特定区域乃至全球范围内扩展门店和分支机构。企业自身专注于主营业务的拓展，包括将企业的IT系统快速延伸到分支，而不希望受运营商网络接入条件的限制，甚至希望在没有专业的网络维护人员的情况下，也可以支撑企业广域网像局域网一样无缝延伸到分支机构，从而将企业的IT能力交付到分支机构。
- 远程办公、线上会议等新形式的工作方式兴起，有效提升了企业内部跨地域部门、和外部客户沟通效率，也大幅降低了差旅成本，新冠病毒疫情客观上也使得这一趋势加速发展。这就使得企业需要一种低成本的在任何地点、任何区域都可以安全接入企业私网的网络连接方案。
- SD-WAN(软件定义广域网)是一种提供企业广域网便捷连接技术，并且随着时间的推进，不断演进、深化。从最初的自动化的企业虚拟专网连接，演进到包含虚拟专网连接、边界安全防护、广域网络优化的三位一体解决方案。

3. 华智达ANP SD-WAN系统

3.1 华智达 ANP 系统的设计理念和客户价值

华智达ANP SD-WAN的愿景是将企业专有网络延伸到全球范围内任何有网络连接的地方，构建无边界的企业网络，并保证足够可靠、安全。所以ANP系统可以充分利用一切已有的连接技术接入企业私有网络，包括MSTP/OTN专线、MPLS线路、有线上网宽带、4/5G移动网络，乃至卫星线路，支持按应用需求的多链路按质量择优选路、QoS优化来保证关键应用的体验。同时支持通过集中管控的微分段安全策略在无边界的网络上构建安全防护边界。

华智达ANP产品诞生之初就是一个完全面向SD-WAN场景化设计、优化的产品，采用了大量的创新技术来保证SD-WAN的客户体验，而不仅仅是已有产品、开源组件的拼凑。ANP的设计理念包括：

- 内置公有云兼容的多租户网络架构，从SD-WAN编排模型到控制器、POP设备、CPE设备都原生支持多租户架构，转发平面采用VXLAN或者VXLAN Over IPSec封装，以支持大规模SD-WAN运营场景以及大型企业客户的多网络平面隔离和分权分域管理需求。同时华智达将云网络的"微分段"安全架构引入到了SD-WAN中，通过基于安全组的微分段模型，实现了细颗粒度的安全隔离以及安全策略的集中管控。
- 极致的轻量级、易用性设计，裁减掉不必要的特性，让系统在绝大多数场景下足够用且好用，让系统消耗更少的IT硬件资源、更少的人力维护成本。
- 将研发、生产流程的软件灌装、上线运行和业务开通统一拉通考虑，参照移动网络的终端安全模型设计CPE的安全接入和上线流程，使得CPE的安装调试就和手机一样方便：插上SIM卡即可用接入网络。华智达为每个CPE颁发唯一的证书，用证书公钥的Hash值作为CPE的认证标识(DeviceId相当于SIM卡的IMSI号)，CPE上电后根据证书查询注册服务器，注册服务器中登记CPE对应的控制器，最终和控制器完成基于证书的认证，并下载配置数据，从而完成真正的"零配置"上线。
- 轻量化的All-In-One设计。即使是数百元的低端CPE上，也包含了多租户的VPN连接、微分段安全防护/基本上网行为管理和应用识别优化功能。就如同智能机内置拍照、摄像、导航等功能一样，和专业设备相比有差距，但是足够好用。并且一台设备可以替代几台完全不同的设备，不仅减少了购买成本，更重要的是ANP系统可以全面支持集中的网络及安全策略管控，大大降低IT人员的运维难度。
- 控制器和CPE/POP之间采用高效的gRPC接口，统一支持配置、监控和路由通告等功能，从而可以支持数以十万计的CPE组网场景。并且我们将源自于P2P大规模分布式系统中的Merkle树对账机制引入到ANP中，并通过gRPC接口原生支持Merkle树的对账流程。

3.2 ANP 2.0 SD-WAN **系统构成**

3.2.1 **网络架构及产品简介**

ANP 2.0 SD-WAN系统内置了IPSec VPN加密、安全防护和广域网优化能力，全面支持IPv4/v6双栈组网。其系统架构如图 3.1所示，包含了如下组件：

- ANPC控制器，负责全网设备的接入认证和业务控制，北向开放全部gRPC和REST API。南向采用自定义的gRPC协议控制CPE/vCPE/vPOP设备，也支持NetConf和第三方设备对接。支持三节点集群部署。
- ANPM管理器，负责全网设备的管理、监控，一般和ANPC合一部署，也可以分离部署。支持多租户管理，支持账户的分权分域权限管理。
- ASG1200系列接入CPE设备，用于门店、分支的接入，全面支持Wi-Fi和4G，其中部分款型支持5G。软件功能支持L2/L3转发、多VRF隔离、OSPF/BGP动态路由协议、SNAT/DNAT、VXLAN&VXLAN Over IPSec、安全组微分段隔离、PBR、链路质量检测、基于应用识别的QoS调度/SLA链路选择/上网行为管理等等。支持HA双机部署。
- ANP SD-WAN客户端软件，用于PC客户端的拨号接入。
- ASG2000，总部硬件接入和汇聚设备，和ASG1200的功能基本一致，并且性能更加强大、网络接口更加丰富。
- ASG2000v，其充当两种角色：1）vCPE软件，以虚机形式部署，用于接入企业的私有云或者公有云VPC网络。2）vPOP软件，部署在专门的汇聚数据中心或者公有云上，提供全网的连接汇聚。

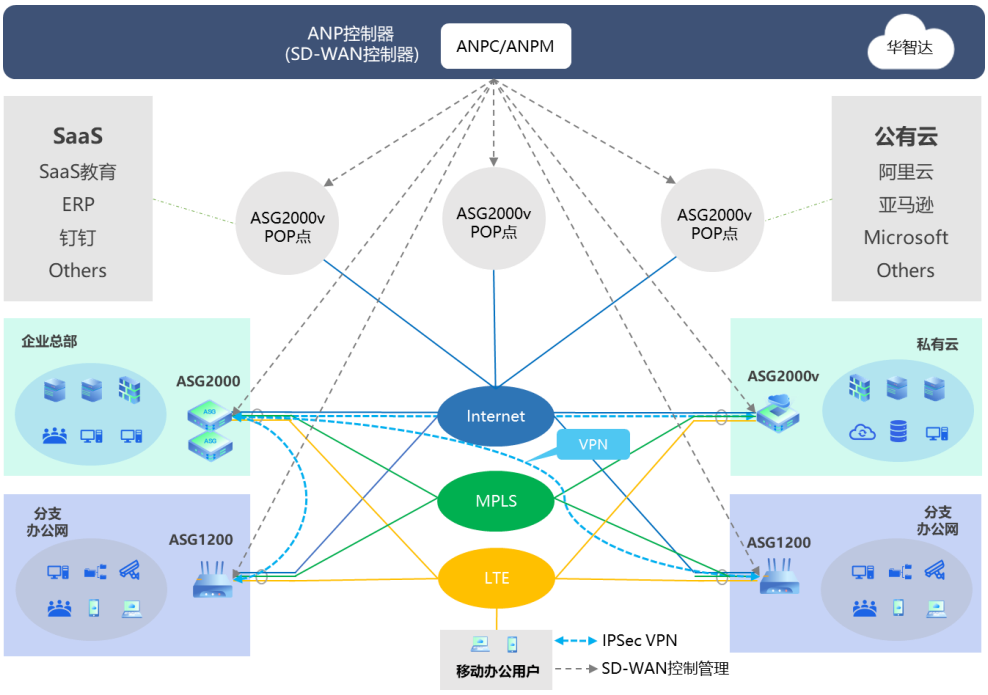

图 3.1

3.2.2 ANP 软件架构

ANP系统软件架构见图 3.2所示，自上而下由ANPM(管理及编排器)、ANPC控制器、ANP-OS软转发平台构成。其中ANPC+ANPM可以合一部署，在200个CPE的网络规模下，消耗系统资源不超过4核vCPU+8G内存，最低可以在2vCPU+4GB RAM的系统下运行。

ANP-OS可以运行在全系列的基于ARM、x86 CPU的CPE硬件上，也可以部署在虚拟机中。最小资源消耗仅为2vCPU、512MB RAM。ANP-OS已经适配了产业链内多家ODM厂商硬件，并且对于任意一款新硬件，在驱动及Linux小系统已经就绪的情况下，1周时间内完成适配。

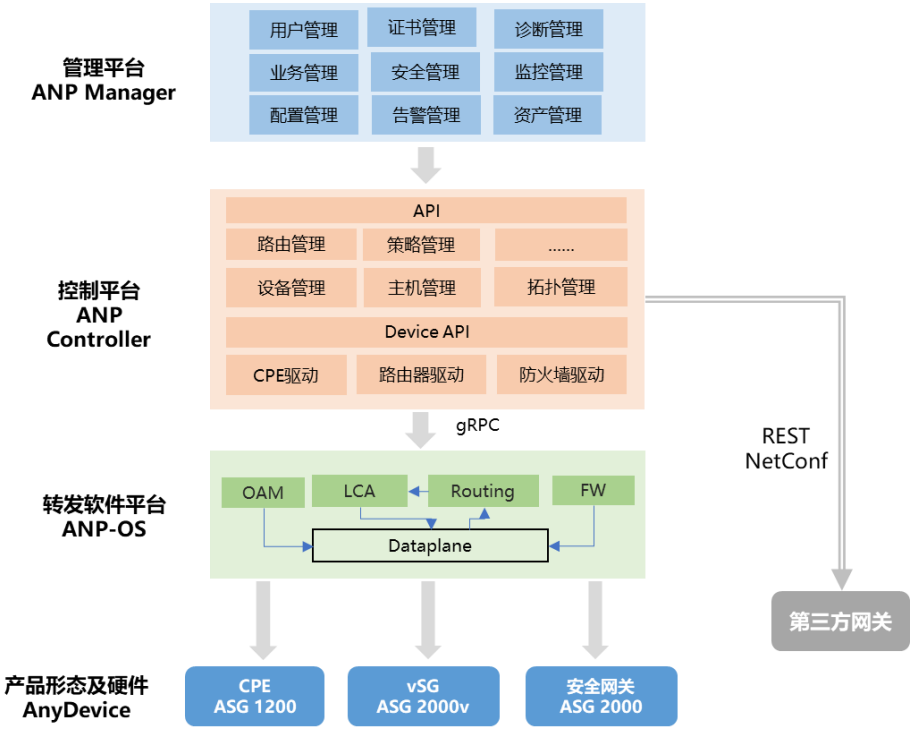

图 3.2

3.3 ANP 支持的组网模式

ANP 2.0支持如下的组网场景：

3.3.1 统一POP汇聚的Hub-Spoke/星型组网方式

- vPOP充当Hub节点，汇聚所有的CPE流量，vPOP本身完全是多租户架构，采用VRF做租户流量隔离，单个POP最大支持4000个VRF。
- CPE/vCPE充当Spoke节点，Internet流量默认本地出口，私网流量通过VXLAN Over IPSec隧道发送到vPOP节点进行路由。也可以配置PBR策略路由或应用识别策略，将Internet流量也通过私网统一出口。CPE支持和企业内部网络运行OSPF/BGP路由协议，接收路由通告，并通过控制器发布到其它分支机构，同时对于控制器通告的路由表项，也支持通过路由协议通告给企业局域网内的路由/交换设备，即使企业出口位于NAT之后，动态路由的能力也不受影响。

华智达ANP也支持POP的多跳、层次化组网，控制器支持POP之间的最短路径计算。

3.3.2 总部CPE直接汇聚分支的星型组网方式

ANP SD-WAN架构支持CPE和POP能力的合一，既可以汇聚流量，也可以处理正常的广域网出口流量业务。因而在SD-WAN私有化部署的情况下，可以无需部署专门的流量汇聚POP/vPOP设备，而是直接采用总部出口的CPE硬件来汇聚分支机构的VPN连接。

3.3.3 一跳入云组网模式

对于企业上云场景，可以通过在公有云侧的VPC中部署一个华智达ASG2000v虚机作为vCPE，企业总部、分支的CPE直接通过IPSec VPN连接到VPC中的ASG 2000v vCPE，从而打通企业私网和公有云的VPC网络，使得访问公有云就像访问本地服务器资源一样便捷。

如果希望VPC和企业私网可以双向互访，那么就需要将企业私网的路由注入VPC，将企业私网路由下一跳指向vCPE的接口。如果仅仅需要企业私网访问VPC中的业务，则可以通过ANP控制器编排启用vCPE连接VPC侧的反向SNAT，从而无需在VPC中注入明细私网路由。

3.3.4 Full-Mesh组网方式

ANP支持两种Full-Mesh组网:

- 不加密VXLAN直接互联方式，适用于MPLS专网全互联的场景。可以通过将CPE配置为NVE，自动在租户内的NVE节点间建立Full-Mesh的VXLAN连接。
- VXLAN Over IPSec Full-Mesh互联，通过将租户内部的节点编排为对等的客户节点&服务节点合一角色，从而支持Full-Mesh的互联。

3.3.5 SD-WAN客户端软件接入组网

在ANP架构下，SD-WAN客户端就是一个轻量级的vCPE，其帐号开通、认证由ANP控制器统一

负责，同时需要安装专门的华智达客户端软件。

华智达SD-WAN客户端软件拨号时，首先和控制器联系，控制器为其指派合适的POP点进行接入。在SD-WAN客户端接入的情况下，POP点同样支持多租户。

4. ANP SD-WAN的创新特色

4.1 基于数字证书的 ZTP 零部署和设备安全认证架构

如 图 4.1所示，华智达CPE出厂时即分配唯一的序列号(SN)，并灌装唯一的证书(以证书的公钥的Hash值作为DeviceId，用于认证时识别身份)，这些信息通过生产文件提供给硬件工厂生产和灌装软件，同时录入官网注册服务器anp.huastart.com。当客户开通时，在官网登记客户的实际控制器地址。CPE发货到客户处上电，只要DHCP可以获得地址，其自动查询华智达官网的DNS，并向官网查询本CPE的实际归属控制器，官网返回结果，CPE再和实际的ANP SD-WAN控制器联系，认证通过后进行配置数据的下载。下载完成后即可以正常运行。

这些设计保证了在Underlay可以访问Internet的情况下，ANP SD-WAN是真正的ZTP免配置部署，在分支端，装维人员唯一要做的事情就是连接正确的网线、将CPE上电。

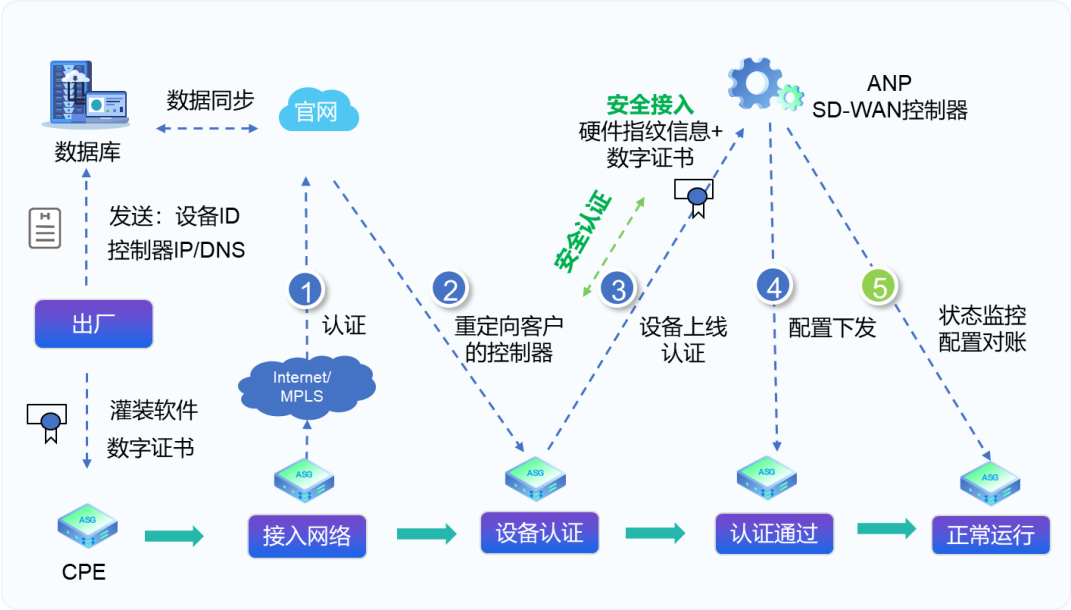

图 4.1

4.2 全面的多租户架构

ANP从ANPM/ANPC控制器到POP设备、CPE，均原生支持多租户架构，兼容OpenStack Neutron的网络模型，转发采用VRF隔离。也支持单租户多VRF，方便同一个租户采用不同的网络平面隔离不同的内部业务系统。

控制器在多租户的基础上，支持基于角色/资源的授权，从而支持灵活的分权分域管理方式，以满足客户复杂的网管权限控制要求。

4.3 All-In-One 的轻量级 CPE

华智达采用统一的轻量级转发面软件系统ANP-OS，将VXLAN/VXLAN Over IPSec、微分段安全/基本上网行为管理、应用识别、WAN QoS优化作为基本功能，路由协议可以裁减。从而可以在数百元的低端ARM平台上也可以支持全面的企业广域网边缘功能，并且这些功能都可以通过控制器进行集中的策略管理。

4.4 远程办公和 SD-WAN 统一架构

华智达是唯一的一家实现SD-WAN和PC远程拨号统一架构支持的SD-WAN厂商。客户需要下载专门的SD-WAN客户端软件，并申请帐号才能接入网络。ANP系统可以统一管理远程办公的帐号、密码，也支持客户端软件在界面上本地修改密钥。客户端软件和vCPE接入一样，也支持多租户接入网络。

客户端软件下载后需要激活，ANP系统可以配置限定远程办公帐号和PC客户端硬件的绑定关系，以确保即使远程拨号帐号泄露，也不会造成安全泄密事件发生。

4.5 创新的控制面和转发面配置对账技术

分布式系统中数据的一致性是个难题，尤其是对于SD-WAN这样的管理通道不稳定的广域网系统，问题更加突出。传统领先厂商的SDN系统均实现了较为简单的配置对账功能，也就是周期性把配置数据全部读取到控制器上进行对比，这个方式极其消耗时间和带宽，对于成千上万的SD-WAN系统

以及CPU较弱的CPE系统而言，这个方法难以实际实施。华智达通过引入将类似于Merkle树的对账机制引入到系统中来，对每个数据记录原生设计携带UUID和更新的时间戳，对这两个字段的Hash构建完整的Merkle树。最终可以支持无论多少条记录，纠正错误的配置数据可以在秒级完成。

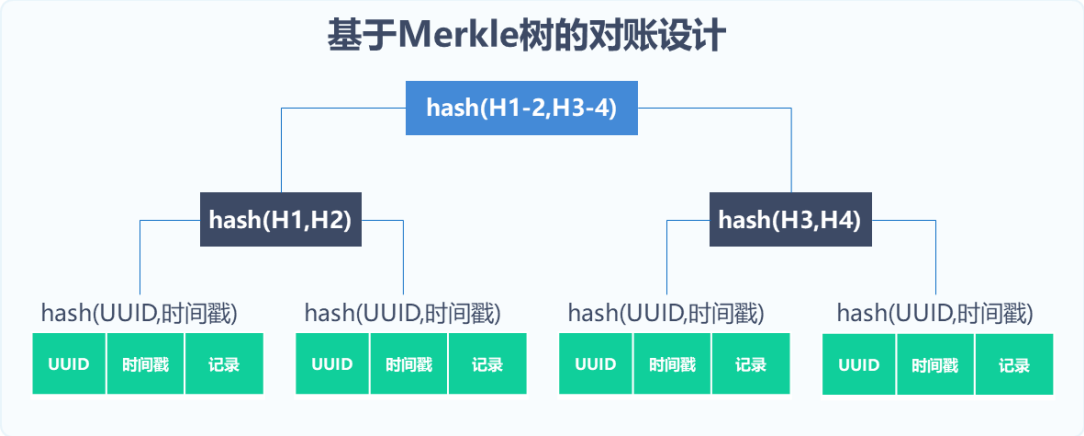

图 4.2

4.6 广域网大二层支持

华智达ANP系统转发面采用VXLAN或VXLAN Over IPSec封装形式，支持跨地域的大二层组网，支持同一个租户下二层和三层混合组网。

为了降低大二层组网时的广播风暴问题，ANP系统支持Anycast网关，对ARP进行代答，避免ARP广播穿越广域网。

4.7 支持 NAT 出口企业网的动态路由接入

如果客户站点网络规模较大，则需要和CPE通告动态路由协议，并且SD-WAN系统也必须将每个站点的动态路由通告到同租户下的其它站点，在专线组网的情况下，部分厂商采用了部署BGP/EVPN RR(Route Reflector，路由反射器)的方式，需要CPE和RR通告路由，这种方式的缺陷非常明显：

1） BGP协议不支持穿越NAT，如果客户站点不是专线，也没有公网IP地址，则此方案不可行。

2） RR方案支持的网络规模非常有限，一般就在几百的节点，并且对于CPE这样的低端设备，RR的路由通告不区分租户/VRF进行全反射，在不稳定的广域网下是否能够正常运行都是问题

华智达ANP解决方案通过CPE和控制器之间的gRPC通道通告路由，即使CPE没有公网地址也可以正常进行路由通告。同时控制器维护虚拟拓扑，将路由只通告到同一个虚拟拓扑(一个VRF)下的相关CPE设备上，大大减少了控制面的负担。进一步地，ANP还采取了延迟撤销路由等技术，使得动态路由即使在超大规模组网、不稳定的广域网上也可以稳定商用。

4.8 微分段安全

ANP微分段安全和AWS、OpenStack的安全组机制类似，支持租户定义多个安全组，每个安全组可以配置一组安全策略，简单地将安全组成员加入到安全组，ANP系统就可以自动查找安全组成员所在的位置，并下发安全过滤策略到指定的CPE或中心站点。安全组规则默认是白名单机制的有状态防火墙规则。

ANP 2.0支持的安全组成员类型包括两种：CPE设备、IP地址段，后一种情况用于控制同一个分支下不同主机、部门的不同网络访问权限。

4.9 量子加密 SD-WAN 方案

如图 4.3所示，华智达ASG1200-A系列CPE支持国密加密算法以及量子密钥冲注功能，并支持和EQC量子密管通信进行量子密钥的分发，以替代IKE的密钥分发机制，从而支持量子密钥加密的安全VPN通道。其中EQC是华智达子公司易科腾研发的量子密管系统。

图 4.3

5. 标准应用场景

5.1 标准的企业分支组网

无论是普通的企业分支组网、工厂互联、门店互联，都可以归属到本类下，区别是不同场景、不同站点的流量大小、成本约束不同，需要选择不同规格的硬件设备。

- 如果企业区域相对集中，可以采用私有的POP进行汇聚。如果企业有私有云资源，可以将基于ASG2000v的POP部署在私有云中，采用标准的CPE+POP的Hub-Spoke方式组网；如果企业没有私有云，也可以在总部部署硬件CPE作为流量的汇聚点，CPE接入到
- 如果企业是全球化组网，可以在公有云或租用IDC资源部署POP点，分支机构就近入网，POP点间Full-Mesh组网，进行不同区域之间的流量中转。

在企业分支组网场景下可以充分利用ANP的微分段安全能力做好分支总部的安全防护，同时可以启用基于应用识别的上网行为管理功能，控制分支机构对Internet、核心业务系统的访问权限，并保证带宽用于承载企业的核心应用。

5.2 SD-WAN 专业运营商组网

- 无骨干网方式，运营商可以租用公有云或者IDC资源作为POP，POP之间可以按租户虚拟拓扑配置POP间VXLAN隧道，处理区域间中转流量，构建一个虚拟骨干网。每个POP都可以为最多4000个租户共享，每个租户都可以配置相应的配额。
- 有骨干网方式，采用ANP ASG2000/2000v建设POP点，汇聚就近CPE，同时POP设备和骨干网的连接有两种方式：
  - ✓ 精细化VPN组网，SD-WAN POP和PE以BGP OptionA的方式组网，将每个租户的VRF映射到VLAN子接口，在PE上进入相应的骨干网MPLS VPN。此方案的好处是骨干网可以看到每个

SD-WAN租户，可以做精细化带宽和流量工程。缺点是开通复杂、骨干网需要对接的信息也过多。

- ✓ 骨干网作为Overlay方式。SD-WAN POP点就近接入骨干网，但是POP点间直接建立VXLAN隧道，无需将租户信息和骨干网VPN进行映射。如果需要QoS保证，POP设备应将相应的租户的VXLAN外层打上不同等级的DSCP标签，骨干网信任DSCP，并匹配DSCP标签进入相应的MPLS TE隧道。

5.3 企业远程办公场景

可以在标准的企业分支组网或SD-WAN运营的基础上叠加企业远程办公。在ANP的体系架构下，任何一个POP点，或总部CPE设备都可以作为远程办公的接入点。在控制器上为特定的租户配置启用远程办公，则控制器会在租户对应的服务节点(POP和总部CPE节点)上使能远程办公功能，同时需要创建远程办公的帐号密码、导入客户端软件的证书。客户下载客户端软件并安装激活后就可以拨号接入企业的私网。

ANP的SD-WAN客户端目前仅支持Windows客户端。

5.4 企业入云和多云互联场景

华智达 ANP 系统中的 ASG2000v 支持公有云部署，目前也已经适配主流的公有云平台。企业可以将 ASG2000v 当作 vCPE 以虚机方式部署在公有云的企业 VPC 中，而无需租用公有云的 VPNaaS 服务。

在 ANP 系统中，受 ANPC 控制的 vCPE 可以像 CPE 一样自动连接到 POP 汇聚设备，如果企业在多个云上租户了 VPC 资源，则可以统一规划私网地址，通过 ANP 的 vCPE 将多个云的 VPC 连接到企业的 SD-WAN 汇聚 POP 设备上，从而实现了局域网内一样的访问体验。

如果希望云端的应用一样能够主动访问企业的内网应用，则需要在公有云的 VPC 中注入企业私网的明细路由，并将其下一跳地址指向 vCPE 的接入端口 IP 地址。如果无需互访，则启用 vCPE 的 LAN 口 (连接 VPC 内网接口) 的 SNAT 功能，这样只允许企业访问云 VPC 资源，而不能反向访问。

关于华智达

400-056-9328
sales@huastart.com
http://www.huastart.com/

南京华智达网络技术有限公司，企业使命是"让企业网络更加简单、安全和智能"，其中研发人员占比70%以上。

产品方向以软件定义为中心，以ANP自治网络软件平台为基础，提供SD-WAN、开放网络和量子加密网络系列产品和解决方案。