中兴通讯 Elastic VPN 解决方案技术白皮书

1 概述：

随着 SDN 和 NFV 技术的迅猛发展，企业和运营商开始将眼光瞄准了 SDN 和 NFV 联合部署。中兴通讯深度融合 SDN 技术和 NFV 技术，并结合自身产品特点，提出 Elastic VPN 解决方案。Elastic VPN 解决方案是面向企业新型专线互联的网络解决方案。方案具有以下特点：

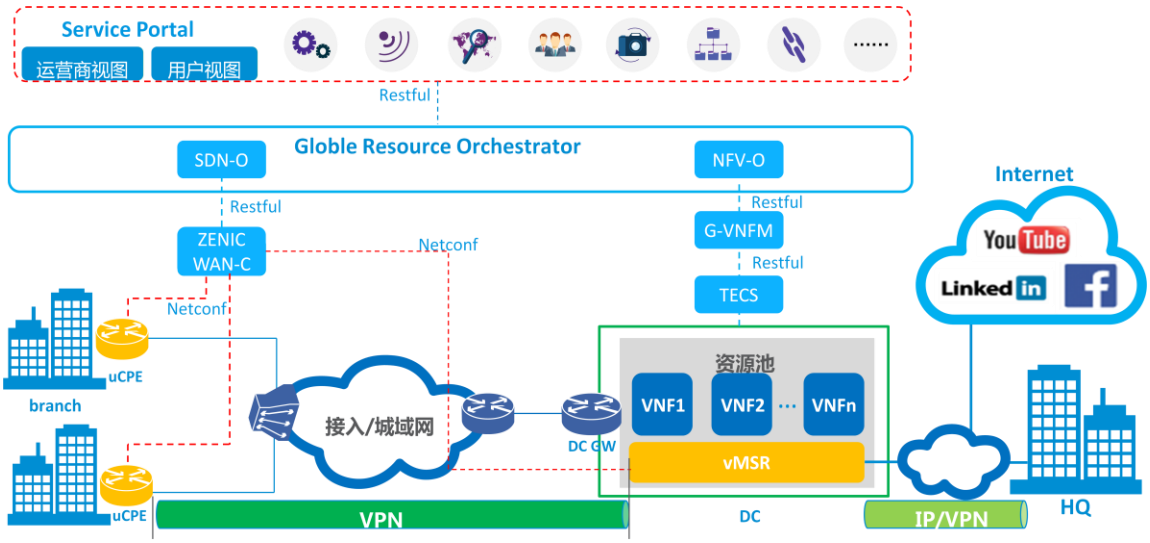
- 通过自平台自助选购 uCPE 设备，uCPE 即插即用，实现 uCPE 设备零配置部署；
- 通过业务自选购平台自助选购业务，实现网络业务即视即所得，即买即用；
- 业务虚拟化，将企业的 CPE 核心功能迁移至数据中心内，减少企业投资成本和运维成本，由服务提供商统一运维，同时减少服务提供商上门次数，缩减人力成本；
- 业务统一编排，一键式自动化部署，缩减业务开通时间，加速业务上线，提升用户体验；
- 统一的 ICT 运维平台，实现 ICT 云网一体化服务。

1.1 Elastic VPN 方案架构概述

Elastic VPN 方案主要包括业务电商 portal 层，资源编排管理层，业务管理控制层和基础设施层四个部分。业务电商 portal 层分为两种视图，用户视图和运营商视图，主要是面向终端用户业务自选购和运营商管理员网络维护；资源编排管理层主要负责网络资源、云资源的编排管理以及 CPE 设备的认证和管理；业务管理控制层主要负责网络自动化开通和业务自动化开通两个部分；基础设施层则是 CPE、服务器、存储池等组成的基础设施。

Elastic VPN 解决方案由业务 portal、编排器、管理系统、SDN 控制器、NFV 管理系统、转发设备等组成，构成端到端业务选购、开通、维护、撤销等操作的端到端的解决方案。

图 **错误！文档中没有指定样式的文字。**-1 Elastic VPN 方案总体架构图



1.2 Elastic VPN 方案组件概述

1.2.1 业务 portal

业务 portal 提供统一图形化界面，实现企业站点 Site to Internet、Site to Site、Site to DC 三种业务场景的业务配置界面。

可分为租户 portal 和管理 portal 两类：

管理 Portal。为管理员提供随选的策略配置、站点及设备管理、流量监控、租户监控界面等。

租户 Portal。为租户管理员提供随选的业务管理和资源、流量监控界面。

1.2.2 全局资源编排器

全局资源编排器 GRO 负责 Elastic VPN 相关的网络资源、NFVI 资源、网络业务的管理、编排等工作。GRO 内包含三个主要模块：SDNO、NFVO 和云编排。SDNO 主要负责网络连接相关业务的编排工作，如连接建立、业务 QOS、流量重定

向等；NFVO 负责网络业务和 NFVI 资源的管理、编排；云编排负责云资源的管理、分配等。

1.2.3 管理系统

管理系统主要负责设备合法性认证和基础设备配置下发，用户从运营商或者供应商处得到 uCPE 设备后，管理系统首先需要对 uCPE 的合法性进行认证，只有确保设备的合法性的前提下才会向设备下发相应的网络配置。

1.2.4 G-VNFM

G-VNFM 负责 VNF 生命周期管理（安装和初始化、查询、扩容减容、拆卸等）。每个 VNF 实例都有一个关联的 VNFM。一个 VNFM 可能指派管理一个单独的 VNF 实例，也可能管理多个相同类型的 VNF 实例甚至不同类型 VNF。

目前主要基于 VNFM 对 VNF 网元进行生命周期管理。中兴的 VManager 产品通过云端部署的 VNF 网元实现业务的整体互联和协同。北向通过 RESTful 与 Orchestrator 对接，获取 VNF 的按需创建、删除、修改命令。南向通过 RESTful 与 VIM 对接，执行 VNF 及网络环境的创建和关联。

1.2.4 SDN 控制器

SDN 控制器负责创建企业和云端的 overlay 网络，并进行管理和维护。中兴的 IPSDN 控制器聚焦 IP/MPLS WAN 网络的 SDN 需求，致力于构建弹性 IP 网络，实现 IP 网络的集中控制、业务开通及流量优化，提供面向用户的 IP 网络 SDN 演进解决方案。其对应的产品 ZENIC IPSDN 控制器基于标准层次化、组件化设计；通过南向支持多种标准接口实现与不同厂商设备的互通，通过北向 RESTCONF 和 NETCONF 接口提供满足用户需求的多种应用场景的 APP，实现网络的集中控制、流量优化、快速部署和业务创新。另外，通过北向 RESTCONF 接口，实现和传统网管的协作和互通。

ZENIC IPSDN 控制器基于先进的 OpenDayLight 开源框架，根据用户需求实现业务快速创新，平滑满足不断扩张的业务发展需要，构建弹性、智能、开放的统

一承载网络。

1.2.4 虚拟资源管理(VIM)

虚拟资源管理器 VIM 可以使用 VMWARE 平台,也可以使用 Openstack 平台。中兴的 TECS 云管平台以 OpenStack 开源云管理平台为基础, 融合电信 NFV 架构，采用虚拟计算、虚拟存储、虚拟网络等技术，完成计算资源、存储资源、网络资源的虚拟化。同时通过统一的接口，对这些虚拟资源进行集中调度和管理，从而降低业务的运行成本，保证系统的安全性和可靠性，是可以同时满足 IT 和 CT 云计算需求的 ICT 融合云管理平台。

1.2.4 转发设备

- 企业侧 uCPE

企业侧物理的小盒子，实现简单的用户接入功能，连接企业用户并通过企业专线接入远端的 POP 节点实现企业自身的虚拟化业务；或者接入企业的分支机构，实现企业虚拟专线连接。北向提供 Netconf 接口，满足控制器的连接和管理。

- 云化 vMSR

基于 X86 实现的虚拟 CPE，提供与物理 CPE 相匹配的网络功能，并实现虚拟业务的业务链功能。提供虚拟业务的快速自动添加和删除。同时提供北向的 netconf 接口，便于控制器对虚拟 CPE 进行的连接和管理。

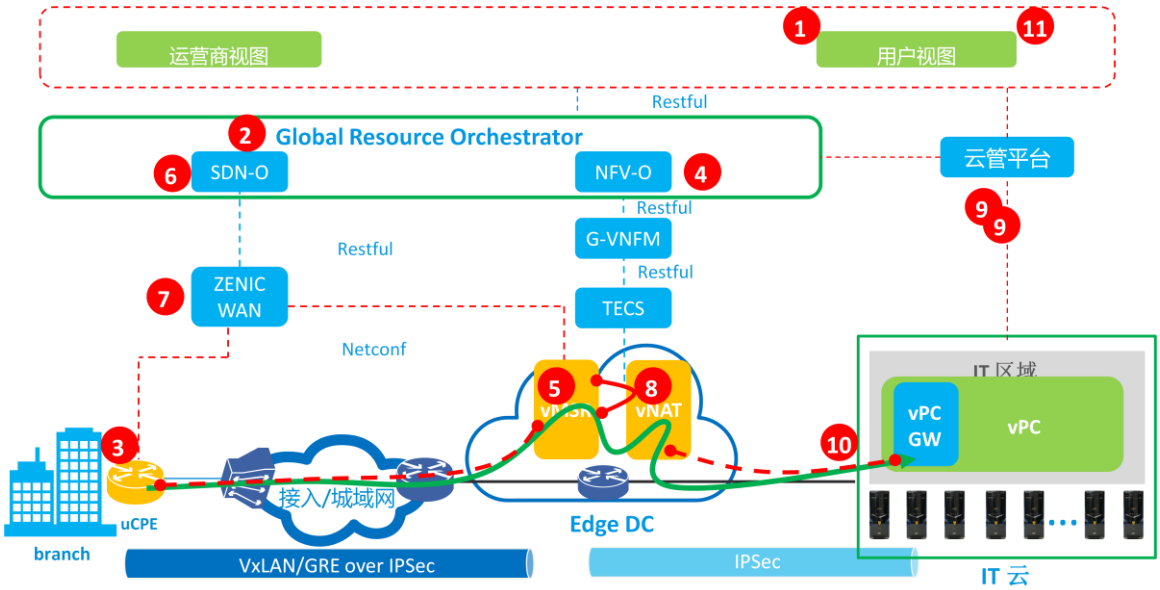
- VPC GW

DC 侧网关设备，提供 DC 与外界的互联。

2 中兴通讯 Elastic VPN 解决方案

2.1 云网一体化协同自动化部署

图 **错误！文档中没有指定样式的文字。**-2 网一体化协同自动化部署



通过 service portal 的用户视图，实现企业 vMSR、增值业务、DC 的一键协同自动化部署，缩短业务开通时间，提高用户体验，具体的业务流程如下：

1. 租户通过用户视图 portal 选购 vMSR 业务，业务 portal 将请求传递给 GRO；

2. GRO 将业务进行拆分给 SDNO 和 NFVO，等待用户设备上线认证通过信息；

3. 用户连接设备，设备自动发送认证信息；

4. 用户设备认证上线后，NFVO 通过 G-VNFM 为用户创建 vMSR 网元；

5. vMSR 上线后，自动向 SDN 控制器发送注册信息，加入到 SDN 控制域；

6. SDNO 向控制器发送命令，建立用户 uCPE 到云内 vMSR 的 VPN 隧道；

7. 控制器执行 VPN 建立过程；

8. SDNO 编排 vMSR 内业务链路径，通过控制器下发到 vMSR 内转发设备上；

9. GRO 编排 vMSR 到 VPC 的网络连接，将其拆分为 SDNO 和智能云管平台的

指令，分别下发给 SDNO 和智能云管平台，SDNO 下发控制器，由控制器将指令下发给 vMSR，智能云管平台下发给 VPC GW；

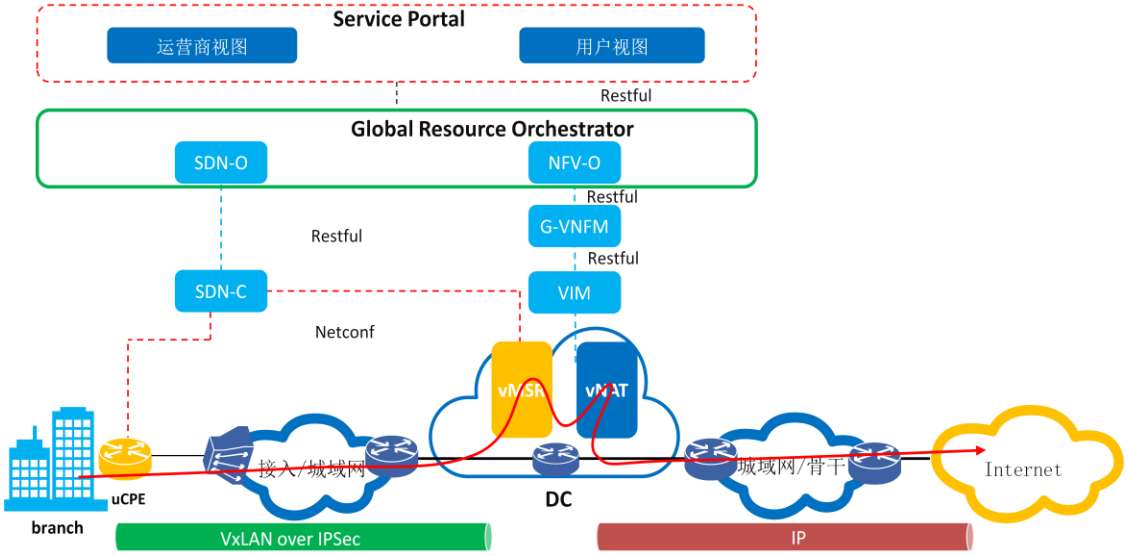
10.建立 vMSR 到 VPC GW 的 VPN 连接；

11.租户在 portal 上管理已经创建的 vMSR 网元。

2.2 企业专线 Internet 访问

2.2.1 L2 uCPE 专线 Internet 访问实现

图 **错误！文档中没有指定样式的文字。**-3 L2 uCPE 专线 Internet 访问实现



企业 L2 uCPE 专线 Internet 访问方案，采用 VXLAN 技术构建面向企业专线 Internet 访问的网络软管道。uCPE 与 vMSR 之间建立 L2 的 VXLAN 隧道实现 L2 专线的承载。为了实现穿越 NAT 及安全保证，VXLAN 报文承载在公网 IPSec 隧道上。

对于 L2 专线，企业业务报文通过二层方式接 uCPE，uCPE 基于 Port/Port+vlan 进行 VXLAN 封装转换， uCPE 与 vMSR 间的 VXLAN 隧道承载租户的二层业务报文。

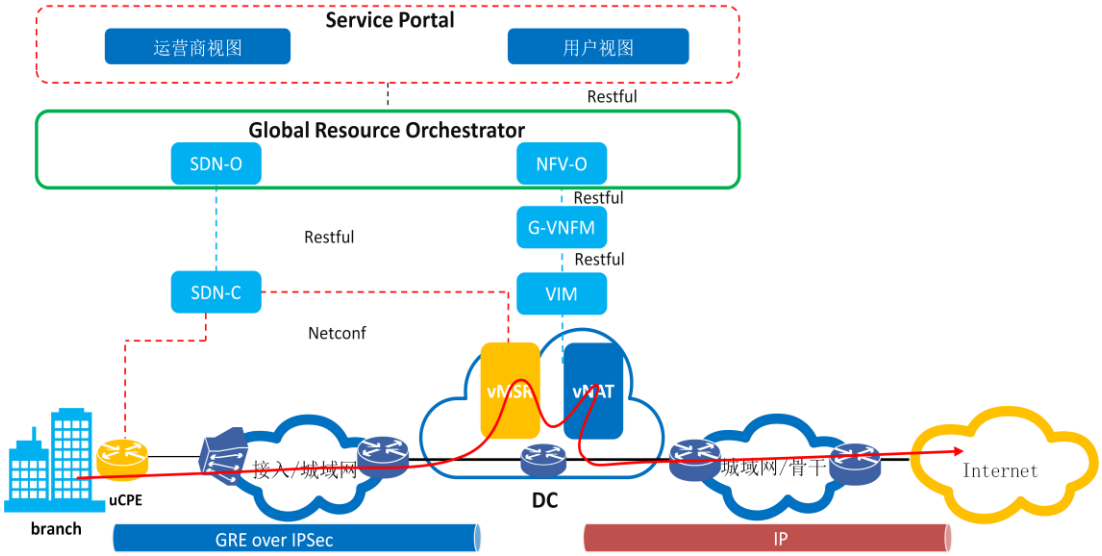
详细技术方案如下：

企业租户通过 Port/Port+vlan 接入 uCPE，uCPE 实现企业租户业务的 VXLAN 封装及相关 VNI 的映射，在 uCPE 的出口进行公网 IPSec 隧道的封装。

vMSR 终结公网的 IPSec，以及企业租户 VXLAN 的解封装，然后实现用户的上网业务。

2.2.2 L3 uCPE 专线 Internet 访问实现

图 **错误！文档中没有指定样式的文字。**-4 L3 uCPE 专线 Internet 访问实现



企业 L3 uCPE 专线 Internet 访问方案，采用 GRE 技术构建面向企业专线 Internet 访问的网络软管道。uCPE 与 vMSR 之间建立 L3 的 GRE 隧道实现 L3 专线的承载。为了实现穿越 NAT 及安全保证，GRE 报文承载在公网 IPSec 隧道上。

对于 L3 专线，企业业务报文通过三层方式接入 uCPE，uCPE 基于三层进行 GRE 封装转换，， uCPE 与云化 vCPE 间的 GRE 隧道承载租户的三层业务报文。详细技术方案如下：

企业租户通过三层接入 uCPE，uCPE 实现企业租户业务的 GRE，在 uCPE 的出口进行公网 IPSec 隧道的封装。

vMSR 终结公网 IPSec 并实现企业租户 GRE 的解封装，然后实现用户的上网业务。

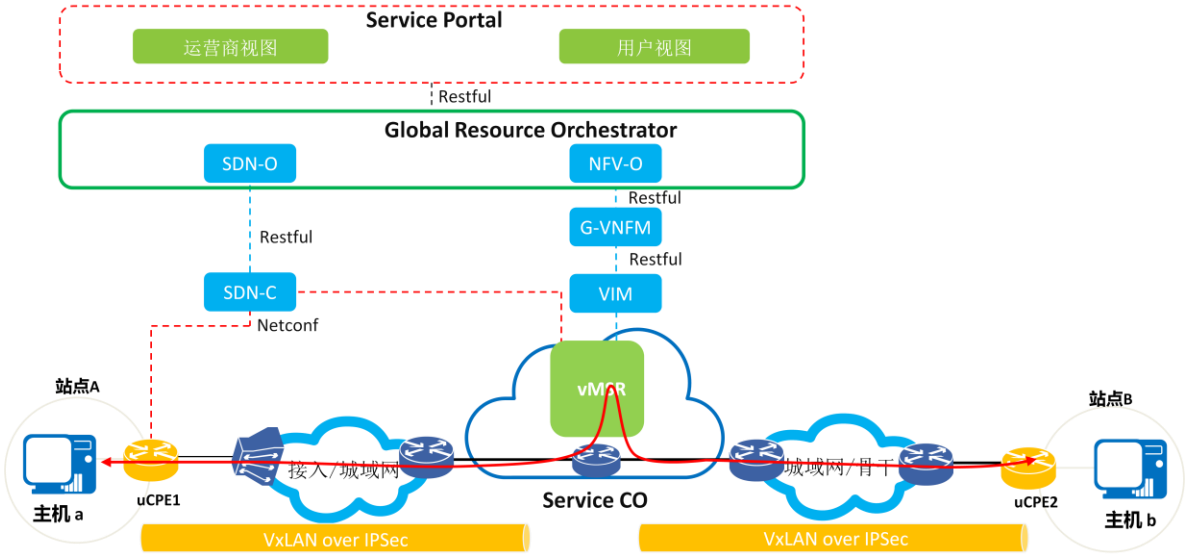
2.2.3 L3 uCPE 实现本地 Internet 访问

企业租户本地 Internet 访问方案采用 uCPE WAN 口 NAT 功能，实现站点流量本地直接上网业务。

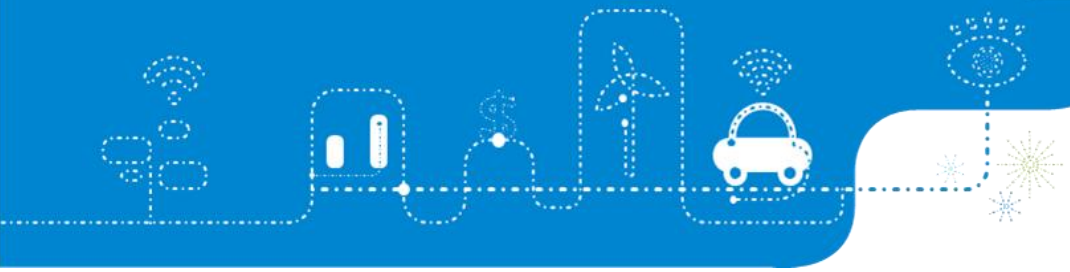
2.3 企业站点专线互访

2.3.1 L2 uCPE 专线站点互访

图 **错误！文档中没有指定样式的文字。**-5 L2 uCPE 专线站点互访



企业各站点之间二层专线互访采用 VXLAN 技术构建 overlay 虚机专线，uCPE 和 vMSR 之间通过内置的 VXLAN 网关建立 VXLAN 隧道，实现虚拟的二层专线承载。用户报文默认承载于 VxLAN over IPSec 隧



道上，实现 NAT 穿越 及安全加密功能。

对于二层虚拟专线，企业业务报文通过二层接入 uCPE，基于 Port 或 Port+VLAN 进行 VXLAN 隧道封装，uCPE 和 vMSR 间通过 VXLAN 隧道承载租户二层业务报文，并通过公网地址建立 IPSEC 隧道，保证用户报文穿越公网的安全性。详细技术方案如下：

1. 企业的每个站点属于不同的网段，用户网关集中在 vMSR。

2. 站点 A 的主机 a 发送 ARP 请求网关 MAC，用户侧 uCPE 将 ARP 请求封装 VXLAN 透传至 VMSR，VMSR 解封装 VXLAN 报文，用户网关终结 ARP 请求并进行回应， ARP 回应经 VXLAN 隧道送给主机 a。

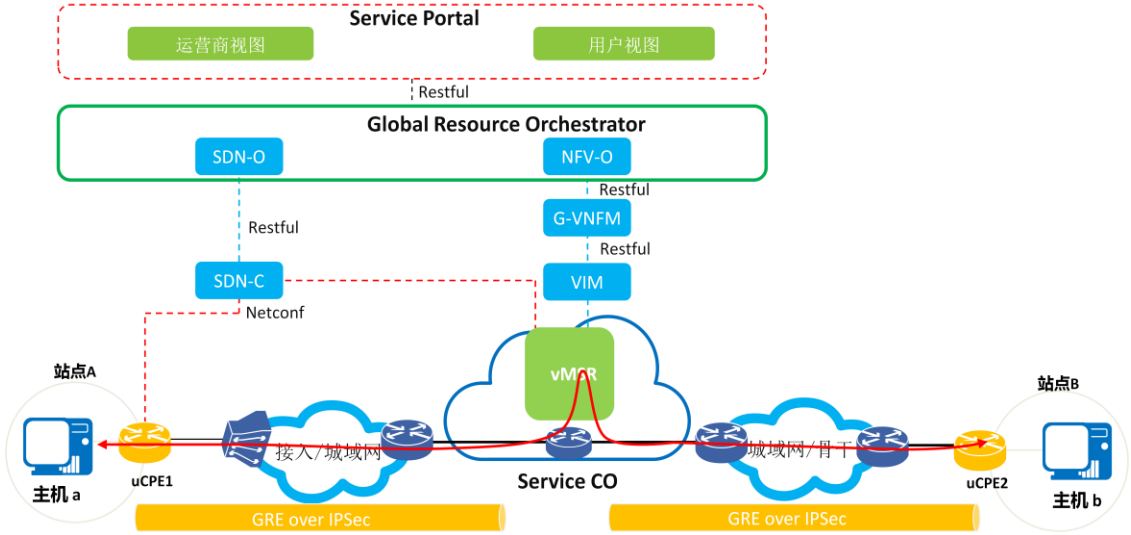
3. 主机 a 获取用户网关的 ARP 后，进行业务报文封装，发送业务报文。报文经 uCPE 封装 VxLAN over IPSEC 隧道头后发送给远端。

4. vMSR 收包用户报文后，先进行 IPSEC 解封装，再解封装内层 VxLAN 报文，还原主机 a 发送出来的报文，发现目的 MAC 为用户网关接口 MAC，则根据目的 IP 进行路由转发，查找路由得到出接口为主机 b 所属站点 B 的用户网关接口，查找 ARP 表项，如没有则发起 ARP 请求，得到回应后进行业务报文 VxLAN 隧道封装，转发业务报文。

5. vMSR 再对报文进行 IPSEC 封装，报文通过外层 IP 路由转发到目的站点 uCPE2，先进行 IPSEC 的解封装，再进行 VxLAN 隧道解封装，并根据内层原始报文，在本地 VLAN 内并将其发送给主机 b。

2.3.2 L3 uCPE 专线站点云端互访

图 **错误！文档中没有指定样式的文字。**-6 L3 uCPE 专线站点云端互访



当企业通过三层接入，网关部署在企业内部 uCPE 时，企业间跨子网互通通过企业内部网关完成。企业业务通过 IPSEC 隧道连接打通。相关业务交互流程如下：

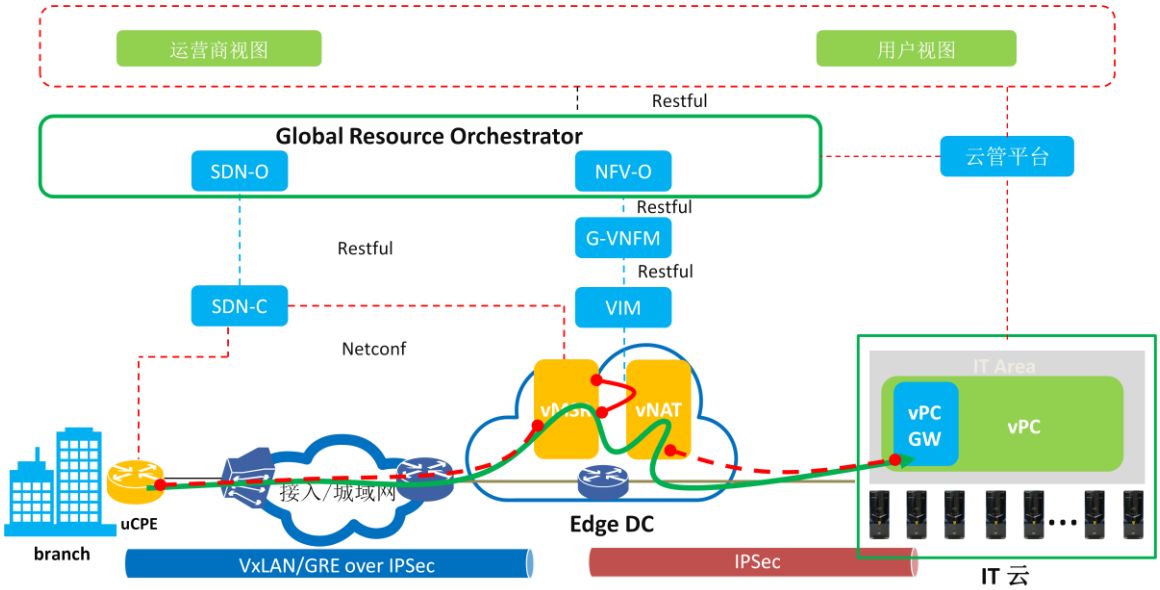
1. 主机 a 发送到主机 b 的业务报文，uCPE1 依据路由转发，执行 IPSec 隧道封装，然后从 uCPE 的 WAN 口发送报文到远端 vMSR。

2. 报文在 uCPE1 和 vMSR 间根据外层 IP 路由转发， vMSR 收到报文后，解封装 IPSEC 隧道，依据路由转发，再执行 IPSec 隧道封装，隧道目的端点为 uCPE2，报文在 vMSR 和 uCPE2 间根据外层 IP 路由转发。

3. uCPE2 收到报文后进行 IPSEC 隧道解封装，然后在本地根据路由转发到达主机 b。

2.3 云网一体化协同访问方案

图 **错误！文档中没有指定样式的文字。**-7 云网一体化访问方案



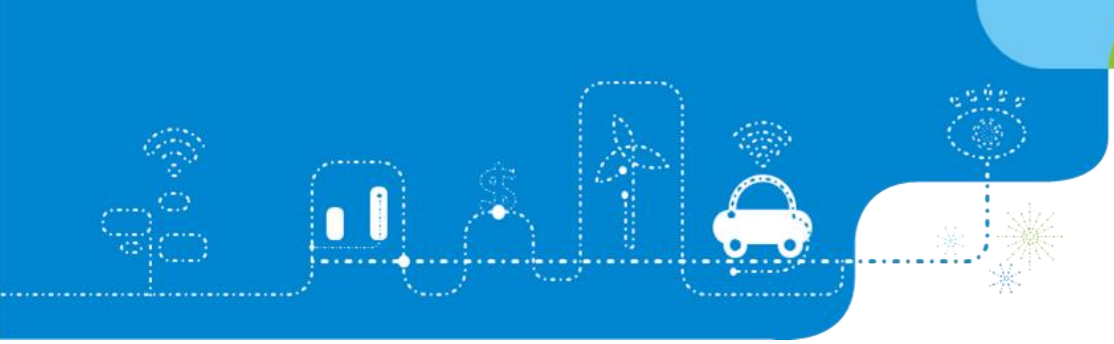
通过云网一体化协同，实现企业和 vPC 之间自动建立 VPN 连接，service portal 对外提供云网一体化服务界面。智能云管平台负责 vPC 资源分配及 vPC 内网络部署以及 vPC GW 对外连接 VPN 配置；GRO 负责实现企业是 VPC 之间 VPN 的建立。

终端用户通过在 service portal 上分别选择 vPC 业务和 vPC 连接业务，触发 vMSR 和 vPC GW 之间建立 VPN 业务，VPN 采用 IPSec 隧道，vMSR 作为 IPSec 的发起端，vPC GW 作为 IPSec 的相应端。

SDN 控制器向 vMSR 下发 IPSec 隧道的配置信息，包括用户指定兴趣流、IPSec 响应端 IP 地址、IKE 模式等，实现 IPSec 隧道自动创建。

1. 分支 uCPE 发起 vPC 资源访问的请求，其报文先转发至 vMSR，uCPE 和 vMSR 之间按照 uCPE 的转发模式进行隧道封装，二层转发采用 VxLAN over IPSec，三层转发采用 GRE over IPSec 的形式；

2. vMSR 接收到报文后，对报文解除封装，然后匹配兴趣流，对流量进行 IPSec 封装（采用隧道模式），IPSec 隧道



的外层源 IP 为 vMSR 的 IP 地址，外层目的 IP 为 vPC GW 的 IP 地址，然后通过 IP 路由转发 IPSec 流量至 vPC GW；

3. vPC GW 接收到数据报文后进行解封装，然后按照报文的转发信息将报文转发至目的资源。

2.4 高价值增值业务

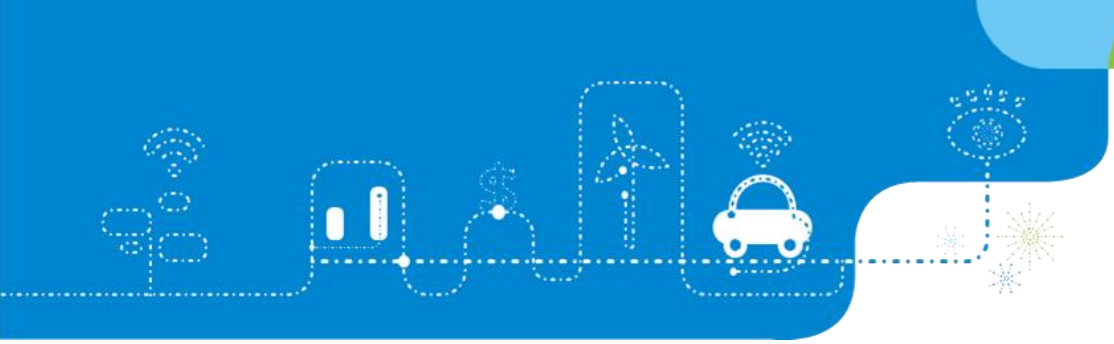
Elastic VPN 通过集中式的软件架构，带来一系列的高附加值功能，通过软件按需增加新的功能特性。新的功能特性不再需要通过专有的硬件实现，而是可以通过运行在 COTS 硬件上的软件实现该功能。简化了部署和维护的成本，并且可以通过灵活的商业模式实现"pay as you grow"，避免了前期高昂的投资成本。目前 Elastic VPN 支持的增值业务如下：

高性能防火墙：毫无疑问，企业网络安全一直是 CIOs 或者 IT 主管最为关注的事情。Elastic VPN 提供高性能防火墙，为企业网络安全保驾护航。企业通过定制安全策略来保证 WAN 链路的安全性。与此同时，为避免分支结构分别配置时犯错的风险，Elastic VPN 提供集中的控制平台允许企业设定集中的安全策略。

WAN 网络应用加速：随着云计算的深入，基于云平台的各类应用越来越丰富，这类应用也要求稳定、安全、高速率的网络连接。为了提升这类应用的体验，WAN 加速软件利用报文中特征字段提取该类应用数据，通过切片、索引、压缩等方式降低应用对带宽的要求，提升用户体验。

上网行为管理：对于企业来说，IT 部门会有对员工的上网行为进行监控，对某些网址禁止访问等需求，Elastic VPN 提供上网行为管理程序帮助互联网用户控制和管理对互联网的使用，包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计、用户行为分析。

IPPBX：为节省开支，许多公司将传统电话系统迁移到 IP 电话系统，利用公司的数据网络承载语音通信。为满足用户需求，Elastic VPN 提供 IPPBX 虚拟应用，完全将话音通信集成到公司的数据网络中，从而建立能够连接分布在全球各地办公地



点和员工的统一话音和数据网络。

3 总结

Elastic VPN 作为 SDN/NFV 综合解决方案，不仅达到了为用户节省开支、提高网络连接灵活性的目的，还提供安全的云接入通道，提升了用户数据在广域网传输的安全性，与此同时，通过云网一体化协同部署，实现 CT 云和 IT 云的无缝链接，使用户的 vCPE、网络增值业务、IT 云业务形成有机的统一体，整体提升了用户体验。中兴通讯可以提供整套解决方案中涉及的组件,也可以兼容第三方的组件.灵活、可靠、敏捷、简单的 Elastic VPN 网络解决方案凭借其连接灵活性、安全可靠性、业务部署实时性、ICT 一体化部署的能力不仅能为政企用户提供更方便网络使用、节省开支等好处，还能为运营商扩大营收，实现运营商和政企用户的双赢。

未 来，不 等 待

中兴通讯股份有限公司
ZTE CORPORATION

深圳市科技南路 55 号中兴通讯大厦

邮编: 518057

Web: www.zte.com

Tel: +86-755-26770000

Fax: +86-755-26771999