**自建SD-WAN攻略——中神通大地云控篇**

在线文档： http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=2129

Word文档：https://www.trustcomputing.com.cn/help/zst\_build\_sdwan.docx

## SD-WAN介绍



**图1 SD-WAN SaaS架构示意图**

SD-WAN即软件定义广域网，通过混合链路实现企业分支、总部和分支互联，从而简化部署、集中管理和降低成本。由于SD-WAN的复杂性，加上没有合适的自建SD-WAN软件，目前SD-WAN应用的话语权被SaaS服务商所把持，SD-WAN SaaS架构示意图如图1所示，从图中可以看到SD-WAN有以下几个部件组成：

1、Orchestrator

Orchestrator 即中心控制器/网络控制器，面向多租户（Multi-tenant），为每个企业用户提供独享的集中式管理及信息展示页面，统一管理和配置部署在企业用户分支的用户端接入设备（CPE）。

Orchestrator 是软件定义网络（SDN）中的概念，属于控制平面（SaaS中的概念），SDN一开始用于内网LAN网络管理，后来这一架构用于外网WAN管理，就形成了SD-WAN。

2、POP

POP (Point of Presence) 即聚集器，是服务提供商在特定地理位置部署的网络接入点，通常是数据中心或公有云上的节点。它们是SD-WAN网络中实现全球覆盖、智能路由和优化连接的关键组成部分。

POP是实际网络流量的中转站，属于数据平面（SaaS中的概念），接收控制器下发的组网策略，与CPE一起构成SD-WAN网络。

3、CPE

CPE（Customer Premises Equipment）是指部署在企业分支机构或远程办公地点的硬件设备，用于连接企业内部网络和外部广域网，与传统防火墙等边界网关相比，CPE只专注于VPN路由，而且是接收控制器下发的组网策略，与POP一起构成SD-WAN网络。另外还有个人版的CPE/VPN软件，用于个人的远程接入，起码有Windows、安卓、iOS、Mac、Linux等五种OS版本。

4、Tunnel隧道

Tunnel隧道即VPN隧道，用于连接POP、CPE，普通SD-WAN使用有限几个VPN协议，例如：IPSec、PPTP、L2TP、OpenVPN，最新VPN协议还有IKEv2、AnyConnect、WireGuard等，有部分厂家使用非标准、私有的VPN协议，例如：lightWAN基于TCP的LTT，Panabit基于UDP的iWAN等。

值得注意的是，单一TCP/UDP隧道协议（LTT、iWAN）或固定端口的隧道协议（IPSec、PPTP、L2TP）在被运营商阻拦或QoS限速后，无法自我修复，容易被套牢。

5、网络资源

SD-WAN服务商的网络资源主要是遍布全球数据中心和公有云的POP节点，由于大多数公有云提供按需付费、后付费的支付方式，SD-WAN服务商可以无需建设自己的数据中心，而只是在有用户购买SD-WAN服务后，在公有云上开通云主机，安装自己的POP网关软件，再为最终用户提供SD-WAN服务，即所谓的羊毛出在羊身上。

总而言之，SD-WAN SaaS服务是一种集中管理的分布式VPN系统，主要为了给多个用户提供统一的管理平台，特点是集中可视化管理和零接触策略（ZTP）的部署方式。对于SD-WAN服务商而言，SD-WAN服务的基础网络设施（Underlay）提供者是第三方电信运营商和公有云巨头，控制器是才是其主要资产，POP、CPE都是为控制器而服务的（Overlay）。对于SD-WAN用户来说，购买SD-WAN服务后，因为组网策略都在控制器上，不容易转移到其它服务商，存在厂家绑定的问题，而且CPE设备功能不全，无法取代传统UTM防火墙等全功能边界网关，存在一定的投资风险。

## 中神通大地云控介绍

**1、基本介绍**

中神通大地EDR&DNS&URL&VPN云控管系统（简称大地云控/TrustGate）是一套专业的终端网络安全防护及互联互通网络应用增值软件，可将硬件、虚拟化平台打造为IPv4/IPv6双栈分布式云路由器/云原生安全接入网关（DNS/WEB/VPC/NAT/VPN/WAF/EDR/负载均衡/CASG/SASE/SD-WAN），为线上线下OS应用软件/SaaS/PaaS提供全面防护、互联互通的数字化安全网络底座。

中神通大地云控的OS应用模型如图2所示。



**图2 中神通大地云控OS应用模型示意图**

**2、功能组成**

中神通大地云控集安全及效率于一身，包括终端网络安全防护、网络服务器、网络客户端、网络路由器服务、日志留存及WEB管理面板，具体功能有EDR/XDR/EPP安全防护全家桶（防火墙、防病毒、HIDS入侵检测、WAF、数据库防火墙、主机安全加固、蜜罐、弱点扫描等），IPv6、VXLAN、GRE、WARP等网络连接，DNS&DDNS权威智能域名解析及代理过滤服务，WebDAV/WEB在线代理/WEB服务器及WEB代理服务器，IKEv2、WireGuard等多种S2S/P2S 全栈VPN服务器及全栈VPN路由客户端，SS/TJ/SSH/V2/Nginx/Stunnel/TLSProxy/KMS/BT客户端/NFS/CIFS应用服务，网桥/TCP转换/NAT/路由/流量统计，ServerStatus/SNMP/Netflow等状态监控。全部功能都配有图形界面输入、IP可视化、状态查询、日志留存、源IP控制、目的IP控制、时间控制、流量控制、在线帮助、视频演示等WEB管理界面。

中神通大地云控的功能应用示意图如图3所示。



**图3 中神通大地云控功能应用示意图**

## 三、自建SD-WAN攻略

**3.1 自建SD-WAN的由来**

目前流行的SD-WAN应用方式是购买并使用SD-WAN SaaS/MSP托管服务，使用这种服务意味着必须和其他用户共享控制器、POP节点和网络资源，对于那些只想为自家应用提供SD-WAN网络，不想成为服务商，不想把敏感数据托管在第三方平台，不想和其他用户共享网络资源的客户，自建SD-WAN是唯一可行的途径。

事实上，WEB、CDN、DNS、邮件等服务都经历了从只能第三方服务商购买并使用SaaS/MSP托管服务，到有能力自建的过程。以WEB服务为例，以前建站的主力是基于虚拟主机的WEB服务，一台主机为多个用户提供计算、存储、网络、后台面板等共享服务，随着云计算和建站面板软件的普及，在独享云主机上安装管理WEB及数据库服务成为了主流，中神通大地云控就是为了在独享主机上安装管理SD-WAN服务，与建站面板软件有着类似的定位。

**3.2 自建SD-WAN的技术分析**

目前，市面上可供选择的自建SD-WAN途径除了华为等大厂昂贵的SD-WAN设备外，还有几款简易的SD-WAN/VPN软件，其隧道协议单一且非标准，容易被运营商阻拦或QoS限速。

中神通公司针对现状的不足，提供一种轻量化、非SaaS服务、基于大地云控的自建SD-WAN软件解决方案，用户自己准备硬件设备、云服务器和接入带宽，与SD-WAN SaaS/MSP托管服务相同的是都提供集中可视化管理、零接触策略（ZTP）部署，与SD-WAN SaaS/MSP托管服务的不同在于自建自管自用、去中心化、免SD控制器、增强型CPE以及标准全栈隧道协议。

中神通大地云控有着全栈VPN服务器、全栈VPN客户端/路由器、智能路由、智能DNS、IP可视化、管理员原子化等功能，根据启用功能的不同，可以胜任SD-WAN架构中的控制器、POP、CPE、隧道等角色功能，具体分析如下表1所示。

|  |  |  |  |
| --- | --- | --- | --- |
| **部件** | **自建SD-WAN** | **SD-WAN SaaS服务** | **说明** |
| 控制器 | 无需专门的控制器，简化多用户管理及使用功能；与POP合二为一，在POP上做管理 | 必须有控制器，为多用户同时使用提供统一的管理平台 | 自建SD-WAN通过去中心化、简化多用户管理及使用功能达到自主可控、专一灵活的目的；SD-WAN SaaS服务通过复用控制器、POP网络资源达到利益最大化的效果 |
| POP | 代替控制器，设置可下发给CPE的组网策略，实现零接触策略（ZTP）；启用VPN服务器/VXLAN/GRE为CPE提供初级接入；启用VPN客户端/VXLAN/GRE连接其它POP，构成链式隧道 | 接收控制器下发的组网策略，与CPE一起构成SD-WAN网络 | 自建SD-WAN通过控制器与POP合二为一，达到自用、去中心化、免SD控制器的目的；SD-WAN SaaS服务通过将POP管理功能上移/集中至控制器，达到为多用户提供统一管理的效果 |
| CPE | 启用VPN客户端/VXLAN/GRE连接POP，接收下发的组网策略，实现零接触策略（ZTP）；启用智能路由、智能DNS功能，实现智能无感分流；提供丰富的网络管理、网络安全功能，为企业排忧解难；兼容第三方标准协议的个人版VPN软件APP | 接收控制器下发的组网策略，与POP一起构成SD-WAN网络；桥接第三方网络安全设备，由后者提供网络安全增值服务；非标准的个人版CPE/VPN软件 | 自建SD-WAN通过POP与CPE直接实现零接触策略（ZTP），达到简化部署的目的；SD-WAN SaaS服务通过将CPE管理功能上移/集中至控制器，达到为多用户提供统一管理的效果 |
| 隧道 | 全栈VPN服务器、全栈VPN客户端/路由器，避免被运营商阻拦或QoS限速；使用标准隧道协议，可以连接第三方VPN服务商分布在世界各地的庞大网络 | 传统的端口固定的VPN协议，或单一TCP/UDP的隧道协议，容易被运营商阻拦或QoS限速；私有隧道协议不兼容标准隧道协议，只能自用 | 自建SD-WAN通过提供全栈隧道协议，达到互联互通、不被控制的目的；SD-WAN SaaS服务通过使用私有协议，达到控制用户非法接入、厂家绑定的效果 |
| 网络资源 | 可以利用现有网络资源，可以使用优惠资格购买新的云服务器，可以自由选择全世界的云服务器供应商；只要资金到位，同样可以像SD-WAN头部服务商那样建立N台遍布世界各地的POP | SD-WAN服务商无需建设自己的数据中心，POP都是建立在公有云上，由于有后付费机制，理论上可以做到0投入建立几百台台遍布世界各地的POP网络资源；客户只能使用SD-WAN服务商的网络资源 | 自建SD-WAN可以有多种途径实现网络资源自由的目的；SD-WAN SaaS服务通过复用网络资源达到利益最大化的效果 |

**表1 自建SD-WAN技术分析对比表**

**3.3自建SD-WAN攻略**

 **1、下载试用**

最新中神通大地EDR&DNS&URL&VPN云控管系统下载信息：

https://trustcomputing.com.cn/bbs/viewthread.php?tid=1174

**2、参考资料**

1）中神通大地云控、VPN、SD-WAN、SASE比较

*Comparison of TrustComputing TrustGate, VPN, SD-WAN and SASE*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1763

2）云市场VPN商品比较

*Comparison of VPN products in cloud market*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1825

3）中神通大地云控——多WAN路由解析功能介绍

*TrustComputing TrustGate—Introduction to Multi WAN Routing Resolution Function*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=2125

4）中神通大地云控——IP可视化功能介绍

*TrustComputing TrustGate—Introduction to IP Visualization Function*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=2128

5）零信任VPN系统

*Zero trust VPN system*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1592

6）运用Mesh VPN自建去中心化网络基础设施服务

*Self built decentralized network infrastructure services using mesh VPN*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1820

7）运用中神通大地云控组建Mesh VPN网络

*Establish mesh VPN network by using TrustComputing TrustGate*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1821

8）运用WireGuard构建下一代内核级VPN

*Using wireguard to build the next generation kernel VPN*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1741

9）中神通大地云控全栈VPN服务器 vs OpenWrt全栈VPN客户端

*TrustGate Full Stack VPN Server vs OpenWrt Full Stack VPN Client*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1966

10）中神通大地云控IPv6说明

*Description of TrustComputing TrustGate’s IPv6 function*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1406

11）中神通大地云控的流量统计、控制、计费、运营功能介绍

*Introduction of traffic statistics, control, billing and operation functions of TrustComputing TrustGate*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1581

12）在Docker容器中安装使用中神通大地云控系统

*Installing and using TrustComputing TrustGate system in docker container*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1606

13）在公有云云市场中使用大地云控OS镜像的注意事项

Considerations for *Using TrustComputing TrustGate OS image in public cloud market*

http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=1540

## 四、总结

**大地云控系统 + 网络资源 = 自建自管SD-WAN系统**

本文分析了SD-WAN SaaS/MSP 托管服务的架构和优缺点，接着为用户提出一种轻量化、去中心化的自建SD-WAN方案，结论是使用中神通大地云控作为SD-WAN建设工具，可以代替实现第三方的SD-WAN SaaS服务作为自用服务，并有自主可控、灵活专一、性价比高等的优点。

## 联系方式

武汉中神通信息技术有限公司

联系人：胡先生

手 机：+86-13607188723

QQ号：390226588

QQ群：233482006

官 网：http://www.trustcomputing.com.cn/cn/index.php/product/dns-url

微信公众号名称：中神通信息

微信号：utmwall

