**运用Mesh VPN自建去中心化网络基础设施服务**

**武汉中神通信息技术有限公司**

在线链接：http://trustcomputing.com.cn/cn/index.php/support/techdocs/122-p2p-mesh-vpn

本文下载：http://trustcomputing.com.cn/help/p2p\_mesh\_vpn.docx

本文从分析现有VPN的类型、用途和问题入手，提出了由P2P VPN（点对点通讯、对等式网络）和Mesh VPN（网状VPN）构建去中心化网络基础设施服务/去中心化云计算/ Decentralized Infrastructure as a Service（DeIaaS）/ Decentralized Network的解决方案，对于“应用接入”、“内网穿透”、“客户端互联互通”、“云游戏视频串流”等应用场景有很好的优化作用。

**一、VPN的类型、用途和存在的问题**

**1.1 VPN类型**

现有VPN主要有两大类型：

1. **站点到站点/网关到网关/Site to Site/S2S VPN**

主要用于通讯双方角色对等（既是客户端又是服务器）、数量相同，且IP地址一般固定的场合，主要有IPSEC VPN等，VPN网关的网络拓扑一般是星型/Hub & Spoke模式和网状/Mesh模式，示意图如下图1所示。

****

**图1**站点到站点/网关到网关/Site to Site/S2S VPN示意图

**2）端点到站点/Point to Site/P2S VPN**

又称为拨号VPN/移动VPN/Road Warrior VPN、远程访问VPN/远程接入VPN/Access VPN、客户端服务器模式VPN等，用于多个客户端连接一个服务器，且客户端IP地址不固定的场合，主要有IKEv2 VPN（第二代IPSEC VPN）、OCSERV VPN、PPTP VPN、L2TP VPN、OpenVPN、SSLVPN、WireGuard VPN、SoftEther VPN、SSTP VPN等，VPN客户端&网关的网络拓扑一般是星型/Hub & Spoke模式，示意图如下图2所示。

把VPN客户端做成VPN路由器，可以使端点到站点/Point to Site/P2S VPN实现与站点到站点/网关到网关/Site to Site/S2S VPN相同的目的。

 ****

**图2**端点到站点/Point to Site/P2S VPN示意图

**1.2 VPN用途**

现有VPN主要有四大用途：

**1）应用接入**

 为了使用内部信息系统，在网络边界或公有云上架设VPN网关，用户登录VPN，就可使用内部信息系统。例如：企业Intranet信息系统（Email、OA、进销存、ERP等）、大学图书馆借阅系统等。除VPN外，零信任、SASE等也有类似的用途。

**2）异地上网**

 为了浏览域内外信息，在域内外某处架设VPN网关，用户登录VPN，就可浏览域内外信息。例如：隐私防护系统、大学国际教育浏览系统等。除VPN外，SD-WAN等也有类似的用途。

**3）内网穿透**

 在没有边界网关管理权限的情况下，为了在外部使用内部资源，在公有云上架设VPN网关，在内部资源处安装VPN客户端，外部用户可以通过公有云VPN网关，间接连接使用内部资源。例如：RDP远程桌面办公系统、家庭NAS远程管理等。

**4）客户端互联互通**

为了将分散各地的PC、服务器等网络设备组成虚拟局域网，在公有云或网络边界处架设VPN网关，在各PC、服务器等网络设备处安装VPN客户端，用户登录VPN，就可使用其它用户处的网络资源。

**1.3 VPN网关存在的问题**

从以上分析可以看出，VPN系统中VPN网关既处于控制层面/Control Plane，又处于数据层面/Data Plane，如果用户要连接所需资源或其他VPN客户端，必须经过VPN网关的中转才能到达最终目的地，由此带来与VPN网关/VPN服务器有关的五大问题：

**1）硬件瓶颈**

VPN网关承担进出数据的加密和连接，需要使用足够的CPU、内存、硬盘等资源。

**2）带宽瓶颈**

VPN网关承担进出数据的加密和连接，需要足够的接入带宽、抗DDoS攻击资源。

**3）单点故障**

VPN网关承担进出数据的加密和连接，需要防止VPN网关出现单点故障。

**4）隐私泄露**

VPN网关可能对VPN数据流进行监听审计，若相关信息保持不当，存在泄密的风险。CS/BS架构的服务器也有相同的风险。

**5）延时高、性能低**

VPN客户端连接远程网络资源必须先通过VPN网关，即使某些VPN客户端与所需资源距离近，仍要绕道VPN网关才能连接所需资源，存在延时高、性能低的问题。

**二、对现有VPN进行P2P VPN/Mesh VPN升级改造**

 为了摆脱对VPN网关高可用性的要求，实现去中心化的目的，可以对端点到站点/Point to Site/P2S VPN进行升级改造，将VPN网关的控制层面/Control Plane和数据层面/Data Plane分离，VPN网关仍然在控制层面/Control Plane，而数据层面/Data Plane由VPN客户端承担，示意图如下图3所示。



**图3** 控制层面/Control Plane和数据层面/Data Plane示意图

由两个VPN客户端承担数据层面/Data Plane的VPN系统，即构成**P2P VPN**，我们称之为**直线计算**；由N个VPN客户端承担数据层面/Data Plane的VPN系统，即构成**Mesh VPN**，我们称之为**NS计算**（No Server Computing，不是Serverless计算）或星月计算，简称**星计算**（Star Computing），在Mesh VPN系统中，每一个VPN客户端均与其它VPN客户端直接相连并传输数据，均系彼此之间最短网络距离。

实际使用中，各VPN客户端（星）首先要登录VPN网关（月亮），再进行P2P VPN/Site to Site VPN/Mesh VPN组网，VPN网关的作用是提供各VPN客户端IP地址、监听端口、公钥认证数据等信息，作用类似STUN Server + PGP Key Server，供VPN客户端在第二阶段连接其它端点时使用，数据传输在各VPN客户端中进行，而且无需在各自的出口路由/边界网关上做修改。由各客户端组成的Mesh VPN示意图如下图4所示：



**图4** Mesh VPN示意图

除了VPN节点之间的直接连接外，各个VPN节点还可以为相连的外部网络提供DNAT端口映射服务连接其它VPN节点（CDN、应用加速等），~~或者为相连的内部网络提供SNAT服务连接其它VPN节点及其外部网络（SD-WAN等），~~或者VPN节点自身提供正向、反向代理服务进而延伸Mesh网络。

P2P VPN/Mesh VPN系统在数据层面/Data Plane实现了去中心化，对于“异地上网”意义不大，但对“应用接入”、“内网穿透”和“客户端互联互通”有显著的改善效果，可完美解决VPN网关带来的五大问题，其优越性具体表现在：**联网设备直接互联，绕过VPN网关，减轻了VPN网关的负担，不受VPN网关接入带宽的限制，降低了VPN网关的单点故障，免受VPN网关的监听审计，同时大幅减小延时、提高性能**。

P2P VPN/Mesh VPN系统作用如下表1所示：

|  |  |  |
| --- | --- | --- |
| **项目** | **P2P/Mesh VPN系统的作用** | **说明** |
| 应用接入零信任、SASE | 解决问题1（硬件瓶颈）、问题3（单点故障）、问题5（延时高、性能低）；一定条件下解决问题2（带宽瓶颈）、问题4（隐私泄露） | 如果只接入一个应用系统则对带宽缓解作用不大，如果同时接入多个异地应用系统则有明显的优化作用；如果不信任VPN网关，可以选择不经过VPN网关，但需要管理员同意 |
| 异地上网SD-WAN | 没解决问题 | 远程网络资源不可能都安装VPN客户端 |
| 内网穿透 | 解决全部问题 | 对应P2P VPN |
| 客户端互联互通 | 解决全部问题 | 对应Mesh VPN |

**表1** Mesh VPN系统的作用

Mesh VPN在“客户端互联互通”领域的用途主要表现在：所有局域网/P2P的网络应用都可升级为基于互联网的去中心化的网络应用（自建去中心化网络应用/Self-hosting DApp），包括但不限于远程桌面、虚拟办公、视频会议、视频监控、视频直播、隐私保护/隐私计算、文件共享/远程连接NAS、网络备份/灾备、网络打印、CDN、去中心化VoIP点对点通讯/文件传输、RTC音视频通信、云通讯、多云应用、企业专网专线、SD-WAN、网络游戏对战、Kubernetes集群、区块链、电子货币交易、边缘计算、物联网、Ad-Hoc网络等。

**三、运用中神通大地云控系统进行P2P VPN/Mesh VPN组网**

要实现P2P VPN/Mesh VPN组网，首先要选择一款既能当VPN网关又能当VPN客户端的软件，对于普通VPN（IKEv2 VPN/IPSEC VPN/OpenVPN/SSLVPN/PPTP VPN/L2TP VPN等）或内网穿透代理软件而言，这两个角色只能选择其一，故普通VPN或内网穿透代理软件均无法方便快捷的实现P2P VPN、Mesh VPN组网。

中神通大地云控使用了最新VPN技术，实现了VPN网关的对P2P VPN/Mesh VPN组网的控制功能，任何兼容的VPN客户端软件均可实现P2P VPN/Mesh VPN组网。

 P2P VPN/Mesh VPN与大家熟知的P2P下载、Mesh WiFi有类似之处，以下以P2P、BT、PT下载为例，说明中神通大地云控P2P VPN/Mesh VPN的运行原理，相关比较如下表2所示：

|  |  |  |
| --- | --- | --- |
| **比较项目** | **P2P、BT、PT下载** | **中神通大地云控P2P VPN/Mesh VPN** |
| 控制层面/Control Plane | BT Tracker服务器 | VPN网关 |
| 数据层面/Data Plane | BT客户端软件 | VPN客户端软件 |
| 客户端软件的作用 | 既可下载又可上传，均不通过Tracker服务器 | 既可访问其他VPN客户端，也可选择接受其他VPN客户端的访问，均不通过VPN网关，但也可配置为通过VPN网关访问 |
| 用户获取信息途径 | BT、PT种子站 | WEB用户门户 |
| 运行流程 | 1）在BT客户端软件上加载BT、PT种子；2）得到Tracker服务器信息，查询Tracker服务器得到其它BT客户端的IP、端口、下载率等信息；3）BT客户端连接其它BT客户端进行下载 | 1）用户登录WEB门户下载VPN配置文件，在VPN客户端软件上加载配置文件；2）连接到VPN网关后，用户在WEB门户中，查询得到自己的连接信息，再与其他VPN客户端用户交换组网连接信息。另外，管理员可直接得到每个用户的组网信息；3）VPN客户端使用组网信息，连接其它VPN客户端进行组网 |

**表2** 中神通大地云控P2P VPN/Mesh VPN与P2P、BT、PT下载的对比表

**四、P2P VPN/Mesh VPN应用举例**

以下以一个简单的内网穿透应用为例，对比三种不同的组网方式，说明使用P2P VPN/Mesh VPN的效果和优越性。

**用户需求：**客户办公室互联网由所在楼宇统一接入，客户没有楼宇边界网关/防火墙的管理权限，由于疫情的发作，需要从外部连接客户办公室内部网络的PC进行居家办公，主要是Windows自带的RDP远程桌面等，最好能自建服务而不是使用第三方服务。也适用于使用Parsec、Moonlight等软件在两台PC之间进行云游戏视频串流。

**4.1 使用frp中转**

使用内网穿透代理软件frp（或SSH端口映射等）进行TCP方式组网，示意图如下图5所示。

**设置步骤：**在公有云上安装frp服务器软件，在内网RDP远程桌面PC及外部PC上安装frpc客户端软件，针对每个服务端口手工编写配置文件，再通过各种方法使其成为Windows服务，做到能够随机启动。

**数据传输：**如此这般，①外部用户就可以连接公有云上的frp服务器，②再间接连接上内网的RDP远程桌面PC，数据流的方向是单向的。

从以上描述可以看出，与中间服务器有关的问题1（硬件瓶颈）、问题2（带宽瓶颈）、问题3（单点故障）、问题4（隐私泄露）、问题5（延时高、性能低）等都存在。



**图5**使用内网穿透代理软件frp进行TCP方式组网

frp连接后，外部PC连接内网PC的远程桌面示意图如下图6所示，“计算机”栏IP地址为frp服务器的公网IP。



**图6** frp连接建立后的远程桌面连接配置

**4.2使用传统拨号VPN连接**

使用传统拨号/客户端服务器模式VPN进行连接，示意图如下图7所示。



**图7**使用传统拨号/客户端服务器模式VPN连接

**设置步骤：**在公有云上安装VPN服务器软件，在内网RDP远程桌面PC及外部PC上安装VPN客户端软件，分别加载配置文件并拨号连接。

**数据传输：**如此这般，①外部用户就可以连接公有云上的VPN服务器，②再间接连接上内网的RDP远程桌面PC，而数据流可以是双向的，即③内网PC也可以连接外部PC。

VPN连接后，从外部PC（虚拟IP：10.9.0.11）到内网PC（虚拟IP：10.9.0.10）需要经过VPN服务器（虚拟IP：10.9.0.1），反之亦然，其traceroute信息如下图8所示，延时很大，路由有2跳/Hop。



**图8**传统拨号VPN建立后的traceoute信息

从以上描述可以看出，与VPN服务器有关的问题1（硬件瓶颈）、问题2（带宽瓶颈）、问题3（单点故障）、问题4（隐私泄露）、问题5（延时高、性能低）等都存在。

VPN连接后，外部PC（虚拟IP：10.9.0.11）连接内网PC（虚拟IP：10.9.0.10）的远程桌面示意图如下图9所示，“计算机”栏IP地址为内网PC的虚拟IP。VPN连接后，PC的默认路由没有改变，不影响已有的上网路径。



**图9** 传统VPN建立后的远程桌面连接配置

**4.3使用P2P VPN/Mesh VPN连接**

使用P2P VPN/Mesh VPN进行连接，示意图如下图10所示。



**图10**使用P2P VPN/Mesh VPN连接

**设置步骤：**在公有云上安装中神通大地云控系统，在内网RDP远程桌面PC及外部PC上安装VPN客户端软件，分别加载配置文件并拨号连接；都与VPN服务器连接后，双方再查询VPN服务器得到自身连接信息，并告知对方（管理员可直接得到每个终端所需的其它终端的连接信息），再分别加载对方的直接连接信息。

**数据传输：**如此这般，①外部用户就可以直接连接内网的RDP远程桌面PC，数据流可以是双向的，即②内网PC也可以直接连接外部PC。

VPN连接后，外部PC（虚拟IP：10.9.0.11）连接内网PC（虚拟IP：10.9.0.10）的远程桌面示意图如上图9所示，和采用传统客户端服务器模式VPN连接一样，“计算机”栏IP地址为内网PC的虚拟IP。P2P/Mesh VPN连接后，PC的默认路由没有改变，不影响已有的上网路径。

P2P VPN/Mesh VPN建立后，从外部PC（虚拟IP：10.9.0.11）到内网PC（虚拟IP：10.9.0.10）不需要经过VPN服务器（虚拟IP：10.9.0.1），反之亦然（例如：内网PC直接连接外部PC/NAS），其traceroute信息如下图11所示，可以看到延时从客户端服务器模式VPN的几百ms减少到了几十ms，且路由只有1跳/Hop。



**图11** P2P VPN/Mesh VPN建立后的traceoute信息

从以上描述可以看出，由于数据传输阶段绕过了VPN服务器，所以与VPN服务器有关的5个问题都得到了解决。

就P2P VPN而言，带来了以下的改善：

* 由于数据传输不在VPN/应用服务器上进行，数据传输不受VPN/应用服务器接入带宽限制，只和传输双方的接入带宽有关，服务器成本大大降低
* 由于数据传输不在VPN/应用服务器上进行，传输数据不受VPN/应用服务器的监听审计，双方可以放心使用，不存在第三方信息泄露
* 由于数据传输不在VPN服务器上进行，双方使用最优网络路径进行连接，延时大大降低，性能大大增加；突破NAT的限制自由互联互通
* 建立P2P VPN无需在各自的出口路由/边界网关上做修改；建立P2P VPN后，即使VPN服务器出故障短期也不影响现有P2P VPN连接；新建P2P VPN仍然需要VPN服务器

就Mesh VPN而言，除了上述P2P VPN的改善外，还有以下好处：

* 由于数据传输不在VPN服务器上进行，且有内核级VPN服务器特性加持，普通性能、普通接入带宽的云服务器/VPS加装中神通大地云控后，可为成千上万用户提供P2P VPN/Mesh VPN组网服务
* VPN服务器安装位置没有特殊要求，可以安装在任意公有云上；数量也没有限制，任意一台VPN服务器作用都是相同的

 武汉中神通信息技术有限公司已经建立了让每个联网终端都能成为服务器的星计算SaaS服务（用户也可以用大地云控自建），用户不必购买昂贵的（云）服务器、带宽即可实现VPN组网并对外提供服务，具体请见公司公告：http://trustcomputing.com.cn/bbs/viewthread.php?tid=1829

**参考资料：**

1、运用中神通大地云控组建Mesh VPN网络

http://trustcomputing.com.cn/cn/index.php/support/techdocs/123-zst\_mesh\_vpn

2、中神通大地EDR&DNS&URL&VPN云控管系统（简称大地云控）

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