

腾讯云深信服 vSSLVPN 部署文档

目录

一、 产品介绍.....	1
二、 部署之前的网络规划和准备.....	2
三、 安装部署 vSSLVPN 服务器的方法.....	2
四、 登录深信服 vSSLVPN 的管理控制台并获取授权序列号.....	8
五、 vSSLVPN 的配置使用.....	10

一、产品介绍

- 1、深信服 vSSLVPN 产品是以软件镜像文件的方式存放在腾讯云上的，因此您需要先给 vSSLVPN 提供一台全新空闲的腾讯云 CVM 云主机来安装搭建深信服 vSSLVPN 服务器，安装后用来作为一台虚拟的 vSSLVPN 网关设备，对外提供 SSLVPN 和 IPSECVPN 服务
- 2、vSSLVPN 镜像文件不能下载到本地，只能用于安装于云服务器上。目前产品镜像文件全部免费使用，并提供一个月的免费试用序列号测试
- 3、vSSLVPN 产品在腾讯云上由三部分组成：腾讯云 CVM 虚拟机+深信服 vSSL 镜像文件+深信服 vSSLVPN 序列号

一、部署之前的网络规划和准备

1、产品功能介绍

vSSLVPN 产品是二合一的 vpn，既有 SSLVPN 功能，也有 IPSECVPN 功能

①、SSLVPN 功能通俗说就是客户端电脑或移动终端直接来拨入 vpn 的，支持的客户端操作系统有：win7、win8、win10、苹果 mac 电脑、安卓 4.0+、苹果 ios9.0+等

②、IPSECVPN 功能有两种连接模式：

其一、站点对站点的 ipsecvpn 隧道，是指云下本地机房的 vpn 硬件设备和腾讯云 VPC 网络里面部署的深信服 vSSLVPN 服务器来连接的 ipsecvpn 隧道

其二、站点对客户端，是指云下没有 vpn 硬件设备，只有移动办公用户，支持在移动办公 windows 客户端电脑上安装 pdlan 的 vpn 客户端软件来接入 ipsecvpn 隧道

2、产品部署网络规划

*注意事项：在腾讯云上部署深信服 vSSLVPN 服务器，请将 vSSLVPN 虚拟机部署在单独一个子网，不建议和云业务服务器部署在一个子网

①、SSLVPN 功能：支持部署于腾讯云的基础网络和 VPC 私有网络

②、IPSECVPN 功能：实现两个站点局域网内的相互访问，只支持部署在腾讯云 VPC 私有网络，不支持部署在基础网络（使用 ipsecvpn 功能 vSSLVPN 虚拟机必须和云业务服务器部署在同一个 VPC 内网的不同网段）

3、站点对站点的 ipsecvpn 隧道连接需满足的网络环境和条件

①、腾讯云上只能是 VPC 私有网络，不支基础网络，也就是云业务服务器和深信服 vSSLVPN 服务器要部署在腾讯云的同一个地域的同一个 VPC 私有网络名称里面

②、云下本地机房的 VPN 设备可以是我们的深信服的 VPN 设备，也可以是其他厂商的 VPN 设备，如果是其他厂商的 vpn 设备则必须得支持标准的 ipsecvpn 协议，支持 ikev1 版本才可以和我们深信服 vSSLVPN 连接标准的 ipsecvpn 隧道。暂时不支持 ikev2 版本

③、腾讯云 VPC 私有网络内网私有 ip 网段和云下本地机房内网私有 ip 网段不能相同，不能冲突

二、安装部署 vSSLVPN 服务器的方法

方法 1、事先没有准备好安装 vSSLVPN 镜像文件的独立空闲 CVM 服务器，全新购买搭建一台 vSSLVPN 服务器

1、首先在腾讯云市场搜索“深信服”，找到“深信服虚拟化 SSL / IPSEC VPN 镜像”或直接打开此链接：<https://market.cloud.tencent.com/products/5589#>，如下图所示



The screenshot shows the product page for '深信服虚拟化SSL / IPSEC VPN镜像' on the Tencent Cloud Marketplace. The page features a dark navigation bar with '腾讯云·云市场' and '云市场分类' links. Below the navigation bar, the breadcrumb path is '云市场 > 镜像服务 > 安全高可用 > 深信服虚拟化SSL / IPSEC VPN镜像'. The product title is '深信服虚拟化SSL / IPSEC VPN镜像', provided by '深信服科技股份有限公司'. The operating system is 'CentOS 7.1 64位', and the integrated software is 'centos7.1等'. The version is 'M7.6.1', and it has no dependencies. The price is '免费' (Free). There is a checkbox for '《腾讯云云市场用户协议》' which is checked. An orange '立即购买' (Buy Now) button is at the bottom.

2、点击“立即购买”，购买一台全新的 CVM 服务器，选择 vSSLVPN 镜像来购买搭建一台 vSSLVPN 服务器，如下图所示

1.选择地域与机型 2.选择镜像 3.选择存储和带宽 4.设置安全组和主机 5.确认配置信息

计费模式: 包年包月 按量计费 ② 详细对比

地域: 华南地区: 广州 深圳金融 华东地区: 上海 上海金融 华北地区: 北京 西南地区: 成都 重庆 NEW 香港 新加坡 东南亚地区: 新加坡

亚大地区: 首尔 北美地区: 曼谷 NEW 多伦多 美国西部: 硅谷 欧洲地区: 法兰克福 美国东部: 弗吉尼亚 NEW ② 更多地域

不同地域云产品之间内网不互通; 选择最靠近您客户的地域, 可降低访问时延, 创建成功后不支持切换地域。 [查看我的云服务器地域](#) [详细对比](#)

可用区: 随机可用区 广州三区 广州四区 ①

网络类型: 基础网络 私有网络 ②

基础网络与私有网络不能互通, 购买后不能更换网络类型, 请谨慎选择

网络: ② 共253个子网IP, 剩253个可用

云主机购买成功后, 网络类型不能更换。如现有的网络不合适, 您可以去控制台 [新建私有网络](#) 或 [新建子网](#)

用作公网网关 ① Windows 操作系统不能作为公网网关

实例: [重新选择](#) ①

下一步: 选择镜像

- ①、计费模式: 指这台 CVM 虚拟机购买的付费方式
- ②、地域: 首先明确云业务服务器是在什么地域, 那么部署 vSSLVPN 的 CVM 虚拟机就选择相同的地域, 注意一定要选择相同的地域
- ③、网络类型: 首先明确云业务服务器是在什么网络类型, 那么部署 vSSLVPN 的 CVM 虚拟机就选择相同的网络类型, 注意一定要选择相同的网络类型

3、选择后, 点击下一步选择镜像, 如下图所示

腾讯云 选购其他云产品 搜索 备案

云服务器 CVM [购买记录](#)

快速配置 自定义配置

1.选择地域与机型 2.选择镜像 3.选择存储和带宽 4.设置安全组和主机 5.确认配置信息

镜像: 公共镜像 自定义镜像 共享镜像 镜像市场 ②

[从镜像市场选择](#)

[上一步](#) [下一步: 选择存储和带宽](#)



①、选择镜像：点击“镜像市场”，点击“从镜像市场选择”选择“深信服虚拟化 SSL / IPSEC VPN 镜像”，点击“免费使用”

4、选择后，点击下一步选择存储和带宽，如下图所示

1.选择地域与机型 2.选择镜像 **3.选择存储和带宽** 4.设置安全组和主机 5.确认配置信息

系统盘 普通云硬盘 高性能云硬盘 SSD云硬盘 [? 选购指引](#)

购买成功后，系统盘不支持更换介质

0GB 50 GB

数据盘 [+ 新建云硬盘数据盘](#)

还可添加 10 云硬盘 [?](#)

网络计费模式 按带宽计费 按使用流量 [? 详细对比](#)

带宽 1 Mbps

分配免费公网IP [?](#)

费用 **配置费用**

查询失败，请重试

[上一步](#) [下一步：设置安全组和主机](#)

- ①、系统盘：默认选择 50G 即可
- ②、数据盘：不需要添加
- ③、网络计费模式：选择的是 vSSLVPN 的虚拟机外网所绑定的公网 IP 地址带宽大小，客户根据自己业务量自己选择带宽大小即可

5、选择后，点击下一步设置安全组和主机，如下图所示

快速配置 **自定义配置**

1.选择地域与机型 2.选择镜像 3.选择存储和带宽 **4.设置安全组和主机** 5.确认配置信息

所属项目 [?](#)

安全组 新建安全组 已有安全组 [?](#)

[? 使用指引](#)

如您有业务需要放通其他端口，您可以 [新建安全组](#)

实例名称 你还可以输入60个字符 [?](#)

登录方式 设置密码 立即关联密钥 自动生成密码 [?](#)

费用 **配置费用**

查询失败，请重试

[上一步](#) [下一步：确认配置信息](#)

- ①、安全组里面需要放通 vSSLVPN 所用到的端口

vSSLVPN 控制台管理页面默认端口: tcp4430

vSSLVPN 客户端拨入默认端口: tcp443

Sangforvpn 连接默认端口: tcp 和 udp4009

Ipsecvpn 拦截默认端口: udp4500 和 udp500

②、实例名称: 设置 vSSLVPN 的 CVM 虚拟机的名称和设置密码

6、选择后, 点击下一步确认配置信息, 如下图所示, 检查一遍配置信息后点击“立即购买”

购买数量

购买时长 2 3 ^{88折}半年 ^{83折}1年 ^{7折}2年 ^{5折}3年 其他时长

自动续费 账户余额足够时, 设备到期后按月自动续费

费用 **配置费用**
查询失败, 请重试

至此, vSSLVPN 服务器就搭建好了。

方法 2、事先已准备好安装 vSSLVPN 镜像文件空闲全新的 centos 系统的 CVM 服务器

注意：1、事先准备好的 CVM 虚拟机必须是全新独立的，就是虚拟机里面没有安装过其他业务服务，否则更换系统盘安装其他镜像文件，之前安装的业务服务软件和数据配置都会丢失的；2、并且这台 CVM 虚拟机是需要和业务服务器是在同一个地域的同一个网络类型名称里面的；3、这台 CVM 服务器的操作系统只能是 centos 系统

1、首先打开腾讯云市场控制台页面，点击“云主机”，找到事先准备好的空闲全新的 CVM 虚拟机，如下图所示



2、点击 CVM 虚拟机的“更多”-“虚拟机状态”-点击“关机”，然后再点击“更多”-“重装镜像”，如下图所示



3、在重装系统页面，点击镜像来源的“服务市场”，点击镜像的“安全高可用”，搜索“深信服”，选择“深信服虚拟化 SSL / IPSEC VPN 镜像”的镜像文件，然后点击“开始重装”，如下图所示

您已选 1 台云主机，[查看详情](#) ▾

No.	主机名	主机ID	系统盘大小	操作系统
1	vSSL7.6	ins-013919t2	50GB	CentOS 7.1 64位

注意：重装后，服务器系统盘内的所有数据将被清除，恢复到初始状态；服务器数据盘的数据不会丢失，但需要手动挂载才能使用，具体请参看 [操作指引](#)

镜像来源：

镜像：

系统盘：云锁安全防护镜像linux版

深信服

深信服虚拟化下一代防火墙镜像 (VAF) (50GB)
操作系统：CentOS 6.0 64位
集成软件：防火墙、WAF、IPS、APT防护、僵尸网络监测等
提供商家：深信服科技股份有限公司

深信服虚拟化SSL / IPSEC VPN镜像 (50GB)
操作系统：CentOS 7.1 64位
集成软件：centos7.1等
提供商家：深信服科技股份有限公司

登录设置

用户名

4、重装系统后，CVM 虚拟机会自动开机的

三、登录深信服 vSSLVPN 的管理控制台并获取授权序列号

注意：在登录 vSSVPN 的 web 控制台之前，先给 vSSLVPN 服务器的安全组的入方向规则放行 tcp4430 端口，并且 vSSLVPN 服务器需要放行安全组正常上网

1、打开腾讯云市场控制台页面，点击“云主机”，找到已安装 vSSLVPN 镜像的虚拟机，查看公网 IP 地址，然后打开电脑浏览器，地址栏输入：<https://ip:4430> (ip 地址是 vSSLVPN 虚拟机的公网 ip 地址)，打开后，默认管理员账号：admin、默认密码：admin 如下图所示中的 vSSL7.6 虚拟机公网 ip 地址：203.195.205.102，然后输入 <https://203.195.205.102:4430> 即可打开 vSSLVPN 管理控制台页面





2、输入默认管理员账号和密码 admin/admin，登录进去后，点击“申请试用”来申请30天的免费测试vpn序列号



3、点击“申请试用”后，填写*必填的选项和填写有效的手机号码

APPLY FOR TRIAL

请填写您的联系方式以及需求，我们会第一时间响应您的需求！

姓名: *

手机号码: *

短信验证码: *

公司名称: *

产品用途: *

我们会优先处理填写有真实产品用途的试用申请

- 4、填写信息后，点击“提交申请”，大概 20 分钟内手机短信上会收 30 天的免费 vpn 序列号
- 5、然后在 vSSLVPN 管理控制台页面，点击“在线授权”，复制填写授权 ID 和序列号进去激活后 vpn 的功能就可以测试使用了
- 6、使用 vSSLVPN 的 30 天的免费测试 vpn 序列号测试好了后，如果要正式购买 vpn 序列号，请在腾讯云市场搜索“深信服”找到深信服售后人员电话或 qq 联系正式购买即可

五、vSSLVPN 的配置使用

- 1、在 <https://ip:4430> 页面—SSLVPN 配置—配置用户管理、资源管理、角色授权这些基本配置选项，具体配置方法可以参考 vSSLVPN 快速配置文档
- 2、客户端电脑上打开网页地址栏输入 <https://ip> 去接入的 SSLVPN 隧道（ip 地址就是腾讯云深信服 vSSLVPN 服务器公网 IP 地址），前提是 vSSLVPN 服务器的安全组入方向规则也需要放通 tcp443 端口。