华为云 vSSL 部署实施指导书

深信服智安全
SANGFOR SECURITY

深信服科技股份有限公司

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

修订历史					
编号	**修订内容简述**	**修订日期**	**修订前版本号**	**修订后版本号**	**修订人**
1	华为云 vSSL 部署实施指导书	20191030	1.0	1.0	Qjj

目录

第 1 章 需求背景

目前大量用户为了减轻运维和数据不落地的需求采用了公有云托管业务，但是一直以来公有云架构的安全防护方面一直处于劣势，需要借助第三方安全虚拟化组件来补齐短板。依托该需求 SSL 推出了基于华为云的安全远程接入解决方案，实现移动办公、混合云互联、分支与华为云互联、APP 安全接入等场景需求，解决客户痛点。

第 2 章 部署概述

2.1 华为云平台特性描述

- 底层架构为 KVM；
- 能够自定义安全规则；
- 支持绑定浮动 IP；
- 支持添加多块网卡；

2.2 镜像获取

vSSL 镜像已经上传华为云镜像市场，用户直接在华为云镜像市场搜索“深信服”就可以获取相应镜像。

2.3 部署方式

vSSL 支持单臂模式部署，不支持集群部署，支持分布式集群部署。

2.4 资源配置

规格	配置参数	并发连接数	磁盘
vSSL-100	2 CPU,2G RAM	500	50G
vSSL-200	2 CPU,4G RAM	1000	50G
vSSL-400	4 CPU,4G RAM	2000	50G
vSSL-800	4 CPU,8G RAM	5000	50G
vSSL-1000	8 CPU,8G RAM	10000	50G

vSSL-1200	8 CPU,16G RAM	20000	50G

2.5 授权方式

1、支持在线试用
2、支持在线授权

第 3 章　部署指导

3.1 云平台配置

深信服 vSSL VPN 是以系统镜像的方式提供的，部署深信服 vSSL VPN 需要先提供一台独立的 ECS 主机来安装 vSSL VPN 镜像。

3.1.1 创建 ECS 虚拟机

登录华为云中国站，点击购买 ECS 云服务器。

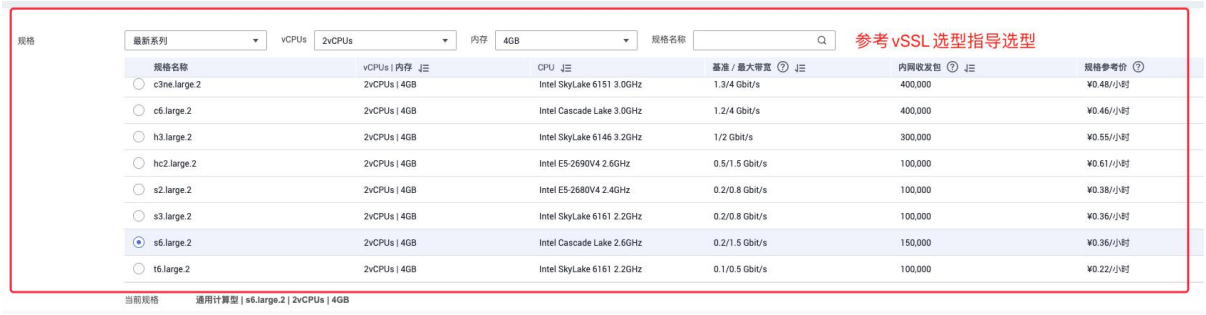
出现以下选择页面。

计费方式根据实际的业务需求选择，暂不支持按需计费的方式。

深信服 vSSL 镜像仅上架到以下三个区域：华南-广州、华东-上海二、华北-北京四。根据实际情况选择区域。

需要选择业务虚拟机所在的 VPC。vCPU、内存参考【2.4 资源配置】，按照实际需求选择对应的服务器，例如选择 2 核 CPU、2G 内存的云服务器。

注：镜像市场的镜像不支持入门型主机实例。



镜像在镜像市场中搜索“深信服”即可看到，选择“深信服虚拟 SSL/IPSec VPN 一体化镜像”，点击 确定 按钮。

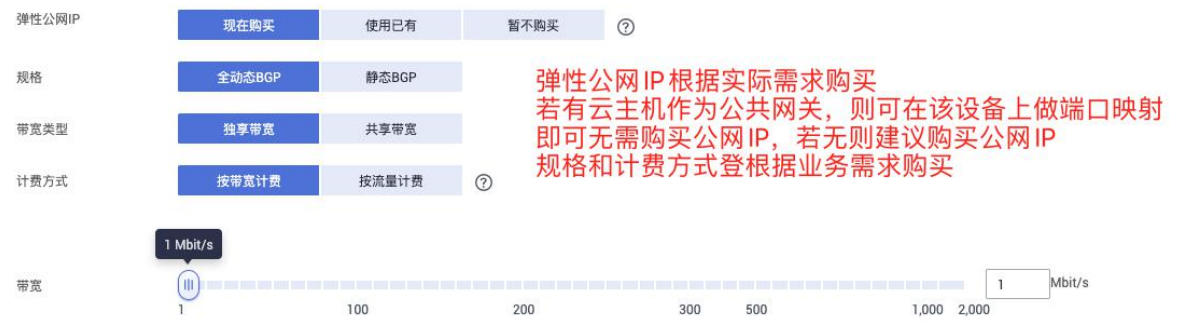
【说明】国外华为云市场没有深信服 SSLVPN 镜像，需要联系深信服工程师通过共享镜像的方式来提供。

存储选择按照需求选择高 IO、普通 IO、或是超高 IO，存储选择 40G 即可，不需要选择额外的数据盘。

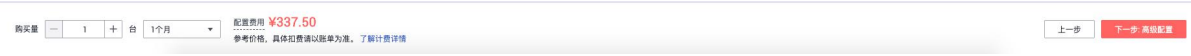
选择完成后，确认数量和费用，点击 下一步 按钮进入下一步配置。

3.1.2 网络设置

网络需要选择专有网络，安全组未配置默认进方向都是拦截，出方向都是放行的，若未定义则会导致创建好云主机后无法访问的情况。所以需要在安全组中放通 TCP443 端口（https 接入）、TCP4430 端口（控制台管理）、TCP51111 端口（升级使用）、TCP22 端口（后台维护），若有 http 接入需求也需放通 TCP80 端口。



选择完成后，确认数量和费用，点击 下一步 按钮进入下一步配置。



3.1.3 高级设置

为云主机命名，登录凭证设置一个密码密码即可，实际上后续无需使用此处密码，若有云备份需求可以购买云备份服务，若没有可不购买。

选择完成后，确认数量和费用，点击 下一步 按钮进入下一步配置。

最后再一次确认配置信息，点击 立即购买 按钮创建 vSSL。

3.1.4 登录 vSSL

部署完成后，在华为云的实例控制台可以看到创建好的 vSSL。

通过分配的公网 IP，例如 https://139.9.213.232:4430，即可登录到控制台，控制台帐号密码默认为 admin/admin。

3.2 云组件授权配置

vSSL 授权分以下为三种，使用云主机只需关注“在线授权”和“申请试用”即可。

- 在线授权：需要先购买获得序列号，然后将序列号信息填写到对应的位置
- 本地授权服务器授权：需要在本地搭建一个授权服务器（VLS），使用授权服务器对 vSSL 来授权。
- 申请试用：只要填写申请信息即可通过短信方式获得授权序列号，把序列号填入【在线授权】即可，使用此序列号可以**免费试用 30 天**。

【在线授权】与【申请试用】都需要 vSSL 能够连接互联网，与 vls.sangfor.com.cn 的 443 端口保持通信。

3.2.1 在线授权

在线授权需要填写授权 ID 和序列号，请联系当地销售或致电 400-806-6868 进行咨询购买。
点击控制台的在线授权，将购买的授权序列号填写到对应位置，提交后等待设备进程重启后即可变为授权状态。

授权成功后在授权信息页面会有【更改授权】、【删除授权】和【授权服务器授权】三个选项。【删除授权】和【授权服务器授权】都是删除掉当前的授权信息，使设备变为初始化状态；【更改授权】则是将新的序列号覆盖掉当前的，授权 ID 不会更改。

3.2.2 申请试用

点击 申请试用， 填写对应信息。

【姓名】、【手机号码】、【短信验证码】、【公司名称】和【产品用途】是必填项，提交申请后，会有审核人审批，审批完成后，会收到授权 ID 和授权序列号，把授权 ID 和授权序列号填入【在线授权】，填写成功后控制台会有提示：您还可以免费试用 30 天，您可以使用【在线授权】或【本地授权服务器授权】。

重新登录 vSSL 控制台，系统就会显示可以免费试用 30 天。

3.2.3 vSSL 授权说明

授权成功后，vSSL 控制台有授权客户和授权有效期的提示。

查看【系统设置】-【系统配置】-【授权信息】页面，即可显示授权信息

若因为某种原因（网络不可达等），连续 7 天未收到授权服务器的心跳信息，此时 vSSL 从授权切换到非法状态，非法状态时控制台不可配置业务，但原有的业务还可以继续使用。非法状态的设备登录后在首页头部有非法状态的提示。

导致非法状态的原因有序列号过期、授权资源与实际资源不匹配、序列号被禁用、序列号失效等，在控制台头部都会有对应的提示信息。

如果非法状态的设备经过 30 天还是没有收到正确的授权则都会变为初始化状态。由于设备是由已经授权过的设备转变为初始化状态，因此将不会再有免费试用的选项。

3.3 云组件配置

3.3.1 SSL 功能配置

3.3.1.1 用户环境与需求

A 公司在华为云上部署了若干业务服务器，公司内部的业务人员需要访问其中的销售系统，公司内部的运维人员需要访问数据库服务器。

3.3.1.2 设备配置步骤

配置步骤如下：

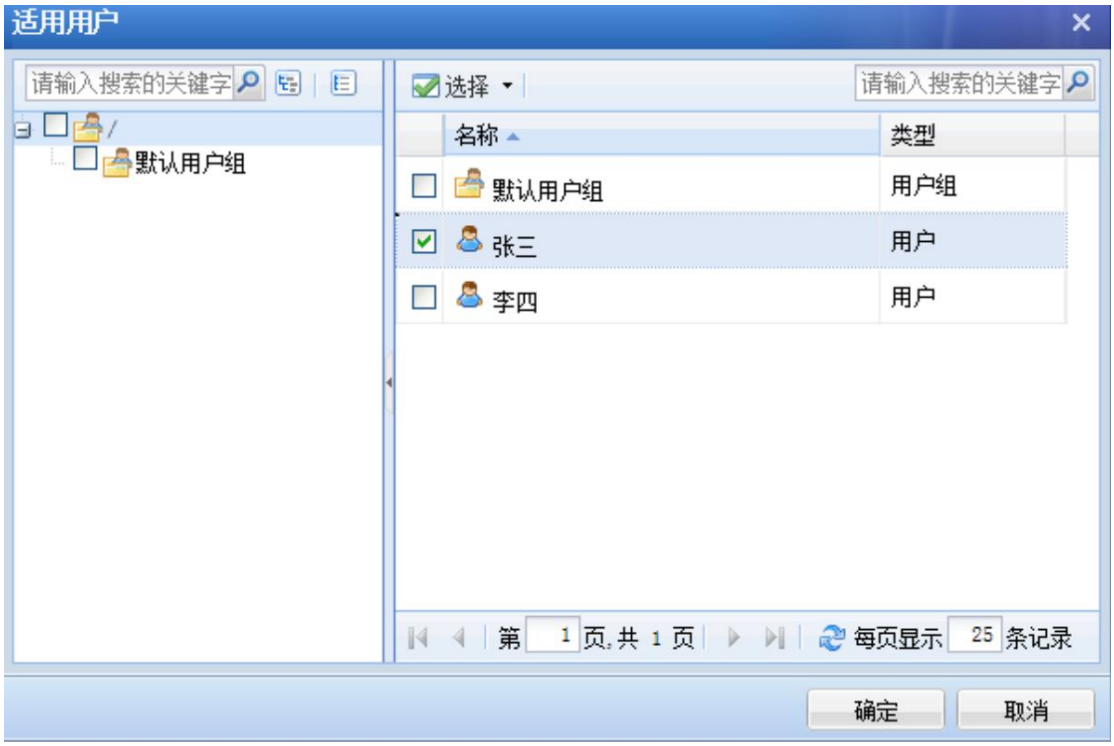
第一步：进入『SSL VPN 设置』→『用户管理』，点击新建，新建两个 SSL 接入用户，配置完以后点保存，本案例配置界面如下：

第二步：进入『SSL VPN 设置』→『资源管理』，新建一个 TCP 应用。点击新建，选择 TCP 应用，设置资源名称，选择资源类型，配置界面如下：

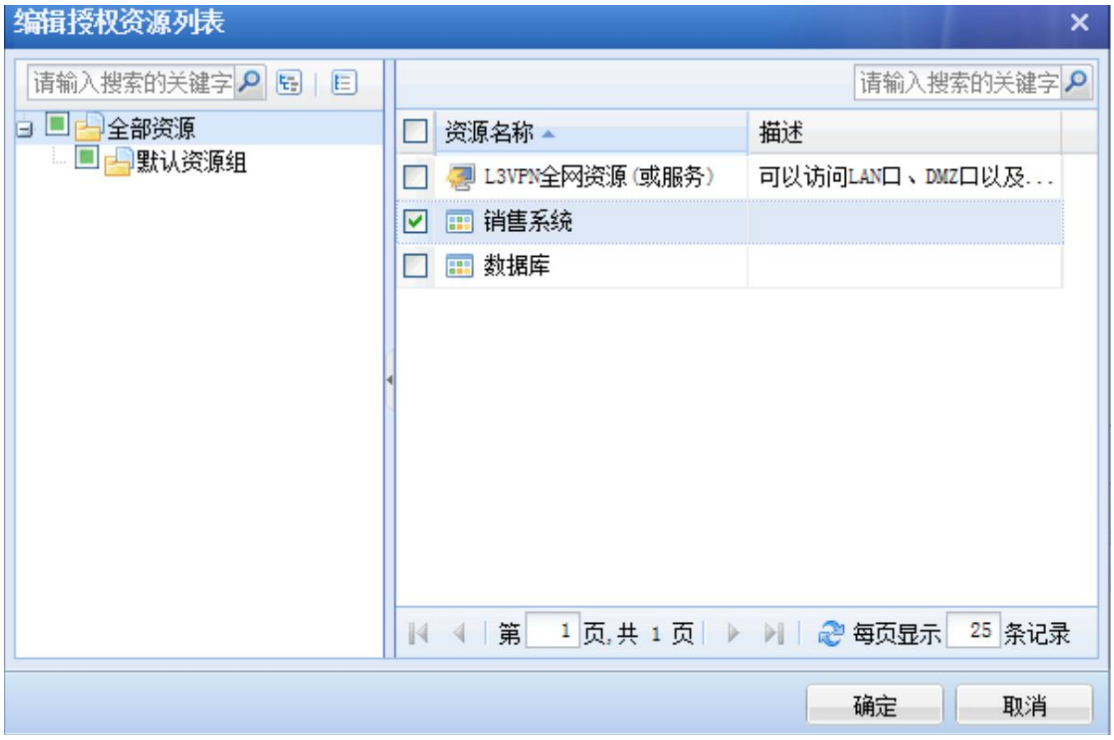
配置资源地址，点击后面的添加按钮，配置完后点击确定，配置界面如下：

第三步：角色关联，即将资源和用户关联，进入『SSL VPN 设置』→『角色授权』，点击新建，选择新建角色，配置角色名称，选择关联用户，界面如下：

关联用户，点击后面的选择授权用户按钮，配置完后点击确定，配置界面如下：



进入『编辑授权资源』页面，选择关联资源，界面如下：



配置完以后点保存。

第四步：配置完成后点击【立即生效】，使配置生效。

第五步：用户在浏览器上输入 SSL 的登录地址，登录界面如下：

第六步：输入用户名密码登录 SSL，便可以看到资源列表，界面如下：

这时，用户就可以访问被关联的资源了。

3.3.2 IPSEC 功能配置

3.3.2.1 用户环境与需求

A 公司在华为云 VPC 专有网络里部署了一个灾备中心，希望通过公司总部内网部署的深信服 VPN 设备与华为云上的深信服 VPN 设备建立一个 IPSec VPN 隧道，将公司内部机房的数据同步到灾备中心。

3.3.2.2 设备配置

公司总部防火墙上的配置

由于公司总部的深信服 VPN 设备接在内网，且该设备做 VPN 连接时是以总部部署，所以需要在前置防火墙上将公网 IP 的 TCP/UDP 的 4009（默认端口）端口映射给 VPN 设备。

公司总部三层交换机上的配置

添加到华为云 VPC 专有网络网段的路由，下一跳指向深信服 VPN 设备，将数据交由深信服 VPN 设备进行封装处理。

总部 VPN 设备上的配置

第一步：配置 WEBAGENT，进入『IPSEC VPN 设置』→『基本设置』，设置好主 webagent 信息，MTU 和最小压缩值默认即可，监听端口采用默认值，其中，主 webagent 配置成“防火墙映射的公网 IP 地址:4009”。

第二步：为分支建一个 VPN 账号，进入『IPSEC VPN 设置』→『用户管理』，新增一个 VPN 账号，选择类型为分支，配置界面如下：

第三步：新增本地子网，宣告总部需要进行 VPN 互连的网段，进入『系统设置』→『网路配置』→『本地子网』，新增总部需要进行 VPN 互连的网段，配置界面如下：

以上步骤结束，总部配置完成。

华为云深信服 VPN 设备的配置：

建立 VPN 连接，进入『IPSEC VPN 设置』→『连接管理』，新建一个连接，填写总部设置的 WEBAGNET，总部建的 VPN 账号，界面如下：

以上配置结束后，华为云 VPN 设备与公司总部的 VPN 设备就能够建立 IPSec VPN 隧道，但是此时两边的服务器通信还是无法实现的，还需要进行下一步的配置——在华为云 VPC 虚拟路由器上配置路由。

在华为云 VPC 虚拟路由器上配置路由

在华为云 VPC 虚拟路由器上添加目的网段是公司总部内网网段的路由，下一跳指向深信服 VPN，目的在于把 VPC 网络指定目的 ip 组的流量引流到深信服 VPN 上，将数据交由深信服 VPN 进行封装处理。

至此，公司总部内网的服务器就可以与华为云上的服务器进行通信，实现数据的同步。

第 4 章 常见问题

1. **vSSL 授权不成功怎么办**

   答：先查看提示信息。检查项主要包括：网络是否可达，授权的序列号信息与设备资源是否匹配、序列号是否已经导入授权服务器数据库表等。

2. **为什么 vSSL 使用一段时间后授权失败了**

   答：可检查下网络是否可达，授权是否被删除，或授权有效时间是否已过期等。

3. **vSSL 开机非常慢怎么办**

   答：通常情况下是主机的内存和 CPU 不足导致。

4. **授权成功、删除授权、切换授权后登录控制台，头部显示不全、提示断网怎么办**

   答：授权的状态在切换的时候后台会有很多进程进行重启，控制台登录后有些进程可能还没有重启完成导致，可以在设备切换状态后等待一段时间再登录，如果头部显示不全可以刷新几次。

5. **是否包含 EMM 功能**

   答：包含

6. **是否能够升级**

   答：可以