

腾讯云 vSSL 部署实施指导书



深信服科技股份有限公司

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	腾讯云 vSSL 部署实施指导书	20191030	1.0	1.0	Qjj

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属深信服所有，受到有关产权及版权法保护。任何个人、机构未经深信服的书面授权许可，不得以任何方式复制或引用本文的任何片断。

目录

第 1 章 需求背景.....	4
第 2 章 部署概述.....	4
2.1 腾讯云平台特性描述.....	4
2.2 镜像获取.....	4
2.3 部署方式.....	4
2.4 资源配置.....	4
2.5 授权方式.....	5
第 3 章 部署指导.....	5
3.1 云平台配置.....	5
3.1.1 创建 CVM 虚拟机.....	5
3.1.2 主机设置.....	8
3.1.3 登录 vSSL.....	9
3.2 云组件授权配置.....	10
3.2.1 在线授权.....	11
3.2.2 申请试用.....	11
3.2.3 vSSL 授权说明.....	13
3.3 云组件配置.....	15
3.3.1 SSL 功能配置.....	15
3.3.2 IPSEC 功能配置.....	20
.....	20
第 4 章 常见问题.....	25

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 推出了基于腾讯云的安全远程接入解决方案，实现移动办公、混合云互联、分支与腾讯云互联、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 腾讯云平台特性描述

- ◆ 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 镜像已经上传腾讯云镜像市场，用户直接在腾讯云镜像市场搜索“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

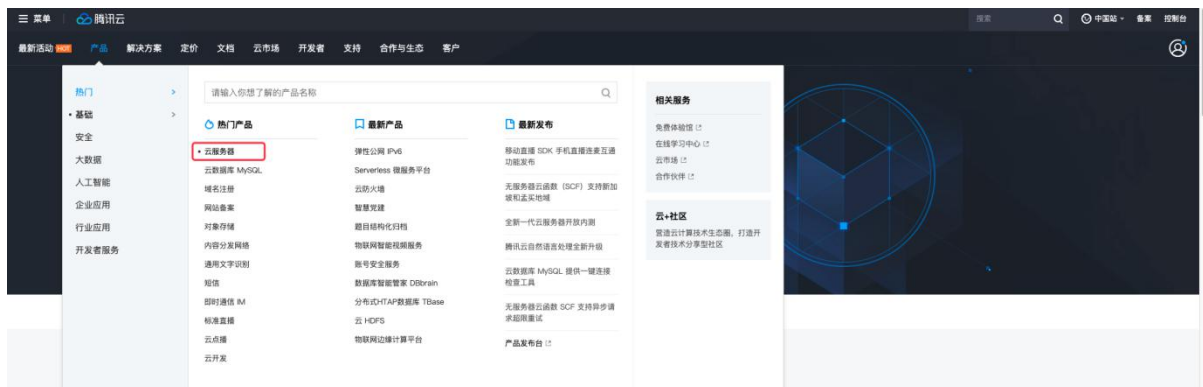
第3章 部署指导

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 CVM 虚拟机

登录腾讯云中国站, 点击购买 CVM 云服务器。



出现以下选择页面

快速配置
自定义配置

1.选择机型
2.设置主机
3.确认配置信息

计费模式: 包年包月 按量计费 竞价实例 [详细对比](#) 用户根据腾讯云特性结合实际情况自行选择

地域: 华南地区 华东地区 华北地区 西南地区 港澳台地区 亚太东南

广州 上海 北京 成都 重庆 中国香港 新加坡 曼谷

亚太南部 亚太东北 美国西部 美国东部 北美地区 欧洲地区

孟买 首尔 东京 硅谷 弗吉尼亚 多伦多 法兰克福 莫斯科 [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

网络: [子网剩余可用IP4093个](#)

如有私有网络/子网不符合您的要求, 可以去控制台 [新建私有网络](#) 或 [新建子网](#)。云主机购买后可以通过控制台切换私有网络完成私有网络/子网的切换

网络需要选择专有网络, 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。

可用区: 随机可用区 广州三区 广州四区

网络: [子网剩余可用IP4093个](#)

如有私有网络/子网不符合您的要求, 可以去控制台 [新建私有网络](#) 或 [新建子网](#)。云主机购买后可以通过控制台切换私有网络完成私有网络/子网的切换

实例: 参考 vSSL 选型选择

全部机型: 标准型 高IO型 内存型 计算型 GPU机型 大数据型 根据业务需求选择

全部实例类型: 标准型S5 标准型S4 标准网络优化型SN3ne 标准型S3 标准型SA1 标准型S2 标准型S1

机型	规格	vCPU	内存	处理器型号(主频)	内网带宽	网络收发包	支持可用区	备注	费用
<input type="radio"/> 标准型S2	S2.MEDIU...	2核	2GB	Intel Xeon E5-2680 v4(2.4 GHz)	1.5Gbps	25万PPS	14个可用区	无	0.47元/小时
<input checked="" type="radio"/> 标准型S1	S1.MEDIU...	2核	2GB	-	1.5Gbps	-	3个可用区	无	0.46元/小时

共2项 只显示广州三区支持机型 < 上一页 1 下一页 >

存储选择按照需求选择高效云盘或者 SSD 云盘, 存储选择 40G 即可, 不需要选择额外的数据盘。

镜像 公共镜像 自定义镜像 共享镜像 镜像市场 ② 从镜像市场中选择深信服 SSL 镜像
从镜像市场选择

系统盘 高性能云硬盘 50 GB ② 选购指引 系统盘保持默认50G即可, 不要扩大或缩小
购买成功后, 系统盘不支持更换介质 根据业务需求选择高性能云硬盘或 SSD 磁盘
无需添加数据盘

数据盘 + 新建云硬盘数据盘 还可增加20块数据盘 ②

公网带宽 免费分配独立公网IP ② 若有其他云主机绑定了公网IP做了端口映射可不用分配独立的公网IP, 若无, 则需分配独立的公网IP用作接入。
按带宽计费 按使用流量 ② 详细对比 根据业务需求选择计费方式和带宽/流量大小

1Mbps 5Mbps 20Mbps 100Mbps - 1 + Mbps ②

公共网关 用作公网网关 ② 若设备做公共网关可勾选, 可以理解为内网的出口设备。

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 免费使用 按钮。

【说明】国外腾讯云市场没有深信服 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。

选择镜像 ×

服务市场

运行环境

操作系统

开发者工具

安全

应用镜像

建站系统

容灾与高可用

数据与存储

网络组件

运维工具

深信服虚拟SSL / IPSEC VPN一体化镜像 免费使用

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

同意用户协议

深信服虚拟化数据库安全审计镜像 (VDAS) 免费使用

操作系统: CentOS 7.0 64位

集成软件: CentOS 7.1

提供商家: 深信服科技股份有限公司

同意用户协议

上一页
1
下一页

Q

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。

已选机型 S1.MEDIUM2 (标准型S1, 2核2GB) 配置费用 0.51元/小时 (费用明细)

数量 - 1 + 带宽费用 0.06元/小时

下一步: 设置主机

3.1.2 主机设置

安全组未配置默认入站和出站方向都是拦截的, 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。

1.选择机型
2.设置主机
3.确认配置信息

安全组 新建安全组 已有安全组 ?

sg-dhvc02o7 | ssl 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](#)

安全组可以理解成防火墙, 腾讯云默认入站出站都是全拒绝
入站需放通以下端口, 出站根据需求决定是否放通
也可以购买时不做配置, 购买完成后再配置。

安全组规则 ? 入站规则 出站规则

来源	协议端口	策略	备注
0.0.0.0/0	TCP:80	允许	放通Web服务HTTP (80), 如 Apache、Nginx
0.0.0.0/0	TCP:443	允许	放通Web服务HTTPS (443), 如 Apache、Nginx
0.0.0.0/0	TCP:22	允许	放通Linux SSH登录
0.0.0.0/0	ICMP	允许	支持Ping服务
0.0.0.0/0	TCP:4430	允许	控制台
0.0.0.0/0	TCP:51111	允许	升级客户端
0.0.0.0/0	ALL	拒绝	-

注意: 来源为0.0.0.0/0 表示所有IP地址都可以用于访问, 建议填写您常用的IP地址

登录方式选择自动生成密码即可, 也可以设置密码, 但是此处设置的密码实际上用不上。其他设置保持默认即可。

实例名称 支持批量连续命名或指定模式串命名, 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 ? 选择自动生成密码即可, 实际上用不到此处的密码。

注: 创建后, 自动生成的密码将通过站内信发送给您。也可登录CVM控制台重置密码。

安全加固 免费开通 ?
安装组件免费开通DDoS防护和云镜主机防护 [详细介绍](#)

云监控 免费开通 ?
免费开通云产品监控、分析和实施告警, 安装组件获取主机监控指标 [详细介绍](#)

定时销毁 开启定时销毁 ?
开启定时销毁后, 系统将在设定时间点自动销毁机器

其他的保持默认即可

▶ 高级设置

设置完成后, 确认好数量和价格, 点击 下一步 按钮进入下一步。

已选机型 S1.MEDIUM2 (标准型S1, 2核2GB)

配置费用 **0.51**元/小时 (费用明细)

数量

带宽费用 **0.06**元/小时

[上一步](#)

[下一步: 确认配置信息](#)

最后再一次确认配置信息, 点击 **开通** 按钮创建 vSSL。

快速配置
自定义配置

1.选择机型
2.设置主机
3.确认配置信息

请确保当前选择安全组开放 22 端口和 ICMP 协议, 否则无法远程登录和 PING 云服务器。 [查看](#)

您没有设置主机密码, 系统将自动为您分配, 创建后, 自动生成的密码将通过站内信发送给您。您也可登录CVM控制台重置密码。 [查看](#)

地域和机型 广州三区: S1.MEDIUM2 (标准型S1, 2核2GB) [编辑](#)

镜像 镜像市场: 深信服虚拟SSL / IPSEC VPN一体化镜像 [编辑](#)

存储和带宽 50GB系统盘; 按带宽计费: 1Mbps [编辑](#)

安全组 sg-dhvc02o7 | ssl [编辑](#)

设置信息 密码登录 (系统自动生成) [编辑](#)

高级设置 [编辑](#)

已选机型 S1.MEDIUM2 (标准型S1, 2核2GB)

数量

配置费用 **0.51**元/小时 (费用明细)

带宽费用 **0.06**元/小时

[上一步](#) [开通](#)

3.1.3 登录 vSSL

部署完成后, 在腾讯云的实例控制台可以看到创建好的 vSSL。

ID/实例名	规格	状态	可用区	主机类型	配置	公网地址	实例计费模式	网络计费模式	操作
ins-gvnxp18 未命名	标准型S1	运行中	广州三区	标准型S1	2核 2 GB 1 Mbps 系统盘: 高性能云硬盘 网络: Default-VPN	134.175.27.48 (公网) 172.16.16.16 (私网)	预付费 2019-10-30 20:55:11	按带宽使用时长计费	登录 更多

通过分配的公网 IP, 例如 <https://134.175.27.48:4430>, 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。

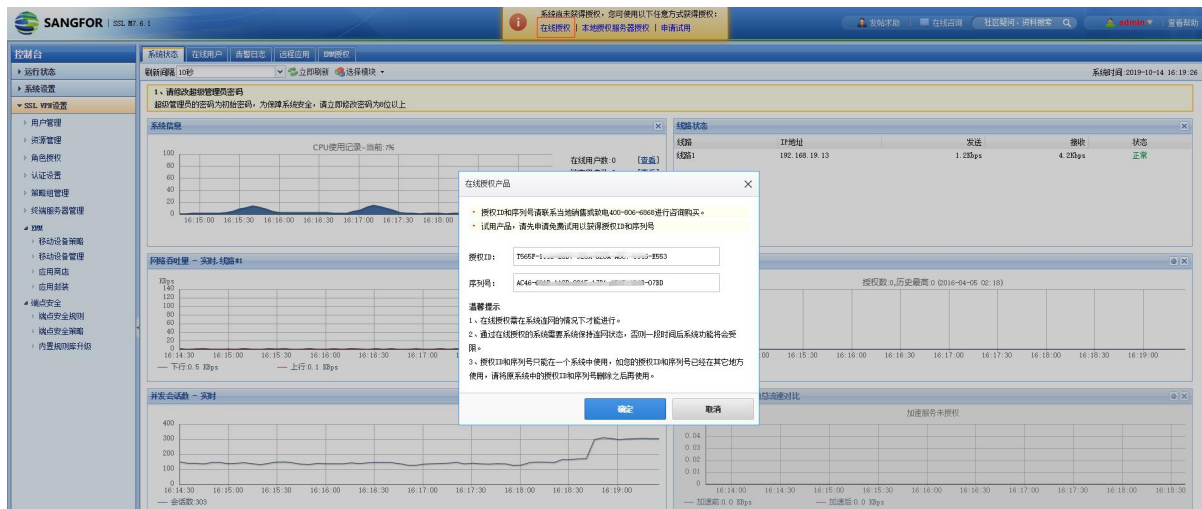
- 在线授权: 需要先购买获得序列号, 然后将序列号信息填写到对应的位置
- 本地授权服务器授权: 需要在本地搭建一个授权服务器 (VLS), 使用授权服务器对 vSSL 来授权。
- 申请试用: 只要填写申请信息即可通过短信方式获得授权序列号, 把序列号填入【在线授权】即可, 使用此序列号可以**免费试用 30 天**。

【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: *

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
产品用途不能为空

推荐人:

推荐人电话:

我们会优先处理填写有推荐人信息的试用申请

【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

授权信息
日期与时间
控制台配置
外置数据中心
设备证书
邮件服务器
SysLog
SNMP

基本信息

授权类型： 授权服务器授权
 授权用户： 许文锋
 软件使用有效期至： 2018-04-20
 切换到“在线授权”

VPN授权模块

SSL VPN 用户总数：	10	✓	
IPSec VPN 移动用户数：	0	✗	<input type="button" value="设置"/>
线路数：	4	✓	
分支机构数：	4	✓	
远程应用用户数：	20	✓	
跨运营商：	已授权	✓	
单点登录：	已授权	✓	
短信认证：	已授权	✓	
流缓存：	已授权	✓	
单边加速：	已授权	✓	
集群：	已授权	✓	

EMM授权模块

版本： EMM高级版
 授权数： 10

功能：	✓ SSL VPN安全接入	✓ EasyApp-SDK接入	✓ 自动封装SSLVPN接入
	✓ 落地文件加密	✓ 应用统一入口	✓ 双域安全隔离
	✓ 单点登录	✓ 安全数据删除	✓ 设备行为管控

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

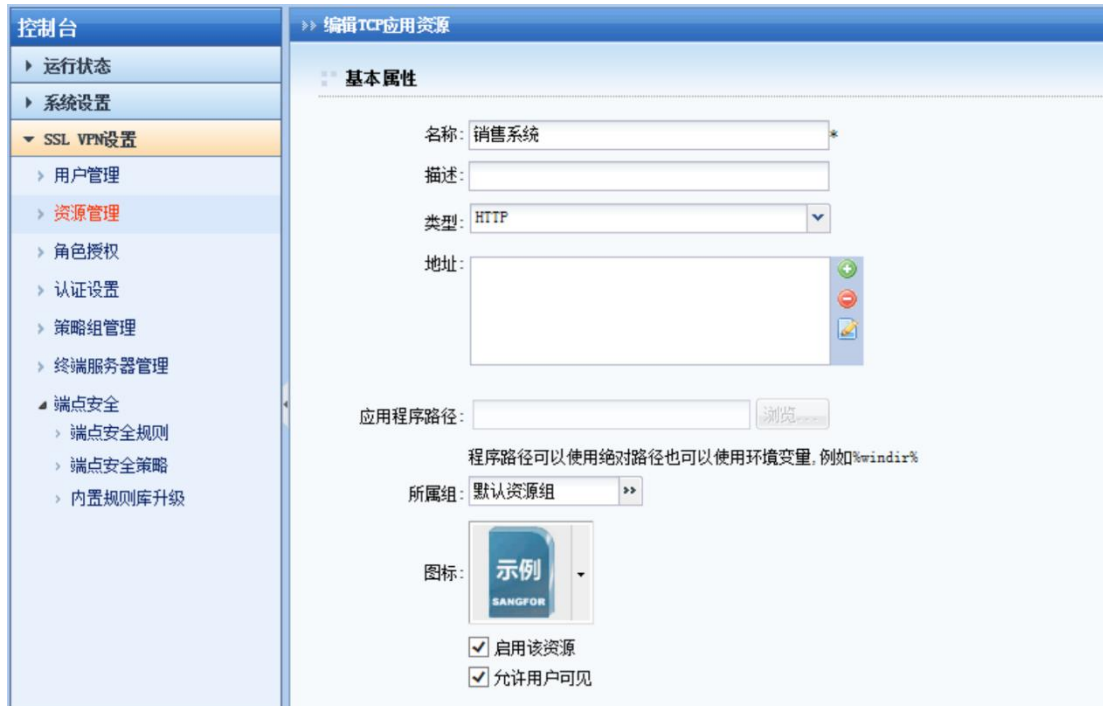
A 公司在腾讯云上部署了若干业务服务器, 公司内部的业务人员需要访问其中的销售系统, 公司内部的运维人员需要访问数据库服务器。

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：



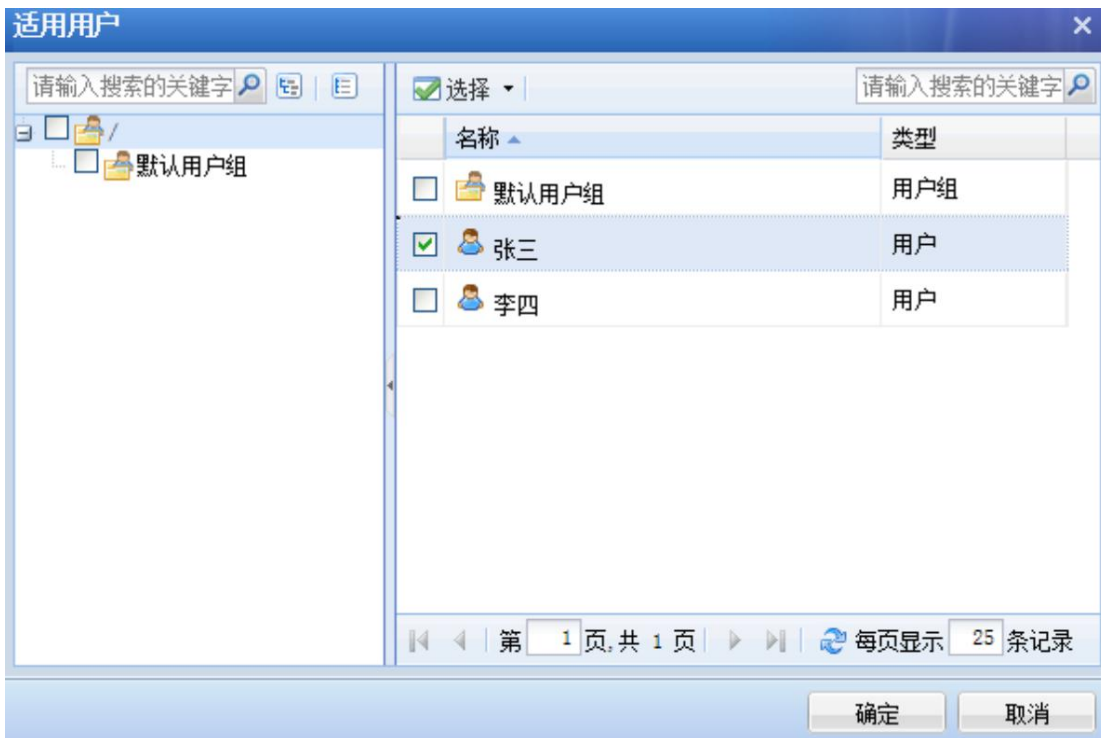
配置资源地址，点击后面的**添加**按钮，配置完后点击**确定**，配置界面如下：



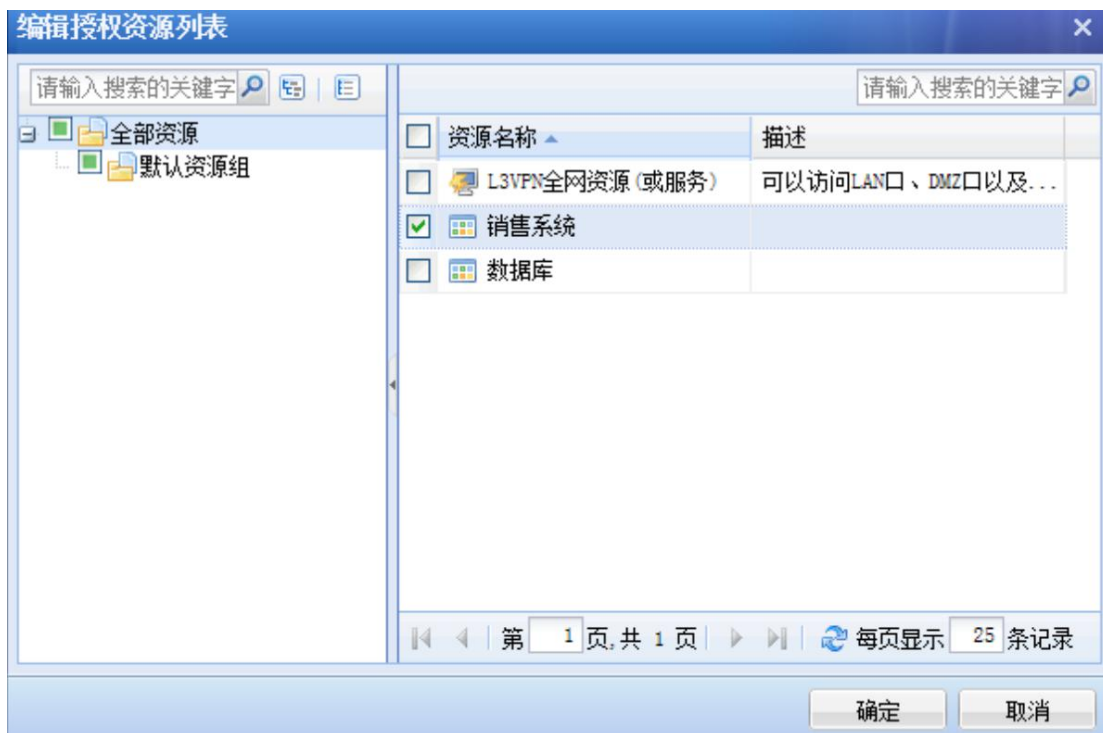
第三步：角色关联，即将资源和用户关联，进入『SSL VPN 设置』→『角色授权』，点击**新建**，选择新建角色，配置角色名称，选择关联用户，界面如下：



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：



登录SSL VPN

用户名: 密 码: 其它登录方式: [证书登录](#) [USB-Key登录](#)[下载USB-Key驱动](#) [手动安装组件](#) [下载svpnntool工具](#)

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：



test11 设置 | 加速效果 | 开机登录设置 | 注销

默认资源组

● [FTP\(FTP\)](#)

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 公司在腾讯云 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 设备与腾讯云上的深信服 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

添加到腾讯云 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”。



主 WEBAGENT:	200.11.22.33:4009	修改密码
备份WEBAGENT:		修改密码
MTU 值 (224-2000):	1500	共享密钥
最小压缩值 (99-5000):	100	
VPN监听端口 (默认为4009):	4009	
<input checked="" type="checkbox"/> 修改MSS (仅在UDP传输时有效)		
<input checked="" type="radio"/> 直连 <input type="radio"/> 非直连		

高级 测试 确定

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：

新增用户 -- 网页对话框

用户名:	<input type="text" value="test"/>	认证方式:	<input type="text" value="本地认证"/>
密码:	<input type="password" value="••••••"/>	算法:	<input type="text" value="AES"/>
确认密码:	<input type="password" value="••••••"/>	类型:	<input type="text" value="分支"/>
描述:	<input type="text"/>	用户组:	<input type="text" value="非组用户"/>

使用组属性

<input type="checkbox"/> 启用硬件绑定鉴权	硬件证书:	<input type="text"/>
<input type="checkbox"/> 启用DKEY	DKEY:	<input type="text"/>
<input type="checkbox"/> 启用虚拟IP	虚拟IP:	<input type="text" value="0.0.0.0"/>

有效时间:

启用过期时间 过期时间: : :

<input checked="" type="checkbox"/> 启用户户	<input type="checkbox"/> 启用网上邻居	<input checked="" type="checkbox"/> 启用压缩
<input type="checkbox"/> 接入总部后禁止该用户上网	<input type="checkbox"/> 启用多用户登录	<input type="checkbox"/> 禁止在线修改密码

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。

腾讯云深信服 VPN 设备的配置：

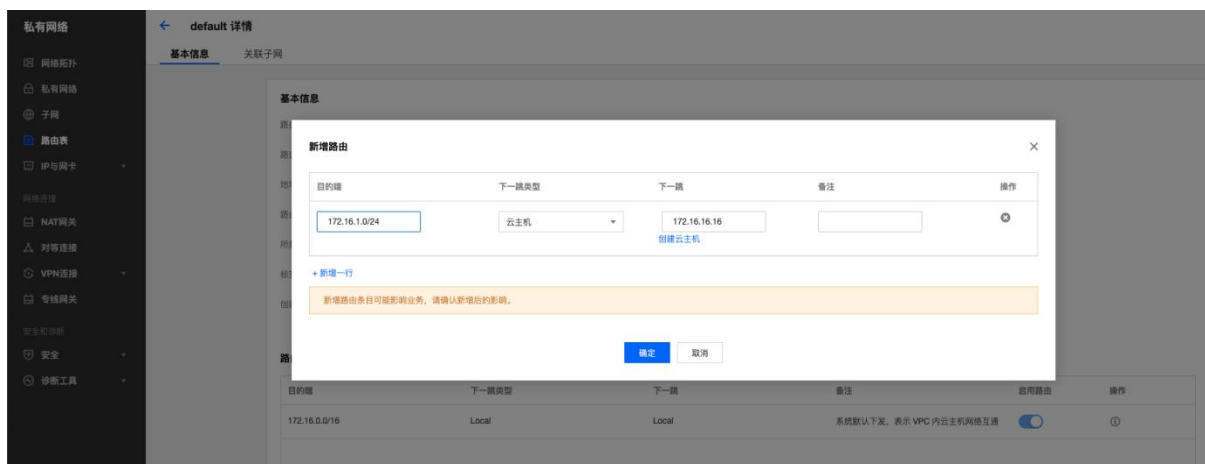
建立 VPN 连接，进入『IPSEC VPN 设置』→『连接管理』，新建一个连接，填写总部设置的 WEBAGNET，总部建的 VPN 账号，界面如下：



以上配置结束后，腾讯云 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——在腾讯云 VPC 虚拟路由器上配置路由。

在腾讯云 VPC 虚拟路由器上配置路由

在腾讯云 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腾讯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