SANGFOR_vSSL7.6.8R2_部署实施指导

for 阿里云

深信服智安全
SANGFOR SECURITY

2021 年 8 月

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

■ 版权声明

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	编写	20210828			71980

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

目录

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

第 1 章　产品简介

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 推出了基于阿里云的安全远程接入解决方案，实现移动办公、混合云互联、分支与阿里云互联、APP 安全接入等场景需求，解决客户痛点。

第 2 章　部署环境概述

阿里云平台特性描述

- 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；

镜像获取

1、通过 vSSL 镜像已经上传阿里云镜像市场，用户直接在阿里云镜像市场搜索“深信服 SSLVPN”就可以获取相应镜像。

2、通过手动下载上传自定义镜像，镜像获取可联系深信服客服 4006306430 转 3

部署方式

1、vSSL VPN 支持单臂部署，不支持双机部署

授权方式

1、支持独立在线授权

2、支持 vLS 统一在线授权-（需要搭建 vLS 授权服务器）

3、支持多云安全平台在线授权

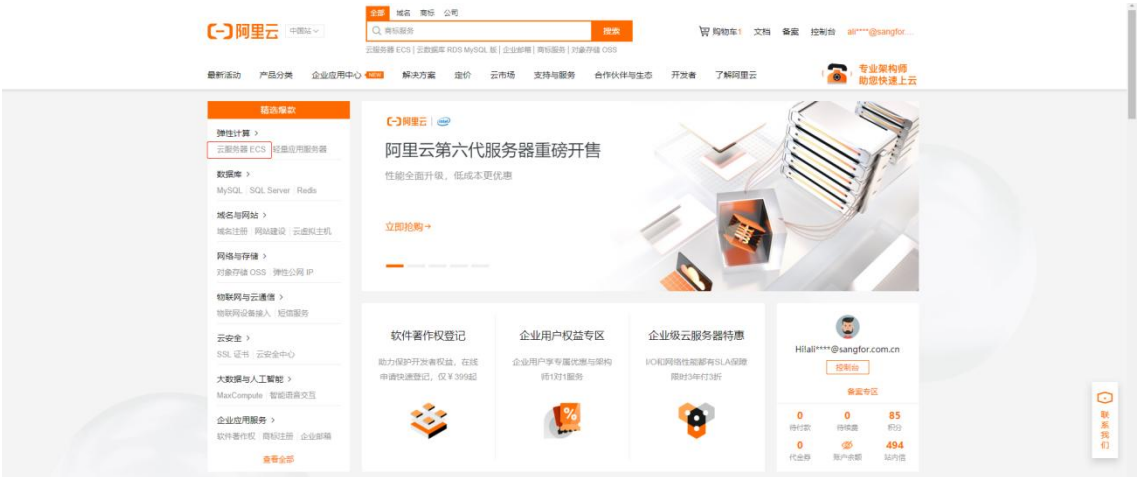
资源规格配置

产品	配置（推荐）	并发用户数
SSL VPN（vSSL）	2C4G+40G 硬盘	5-1000 并发
	4C4G+40G 硬盘	1000-2000 并发
	4C8G+40G 硬盘	2000-5000 并发
	8C8G+40G 硬盘	5000-7000 并发
	8C16G+40G 硬盘	7000-20000 并发

第 3 章　部署实施

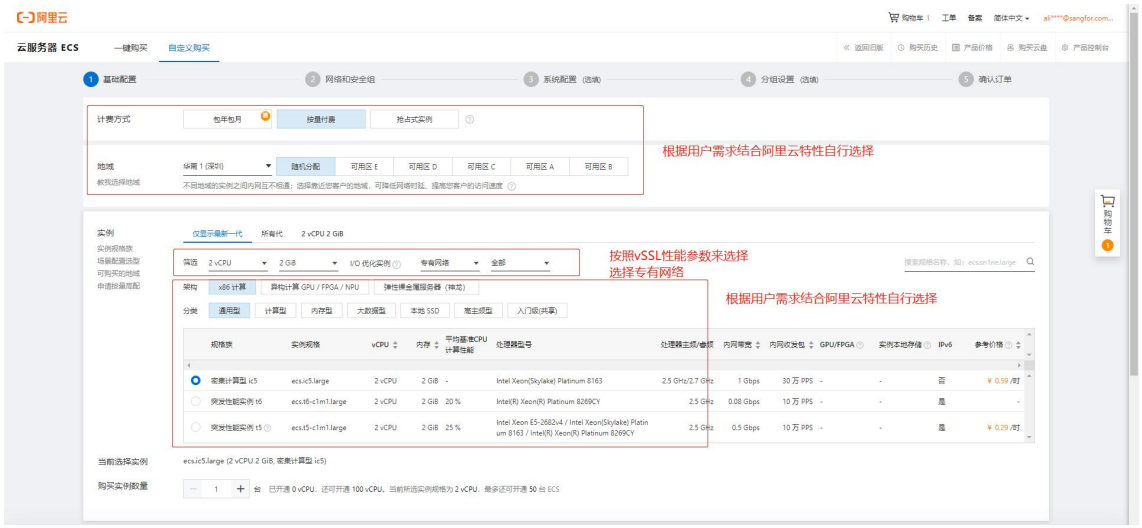
3.1 购买云服务器

登录阿里云中国站 www.aliyun.com，点击购买云服务器



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

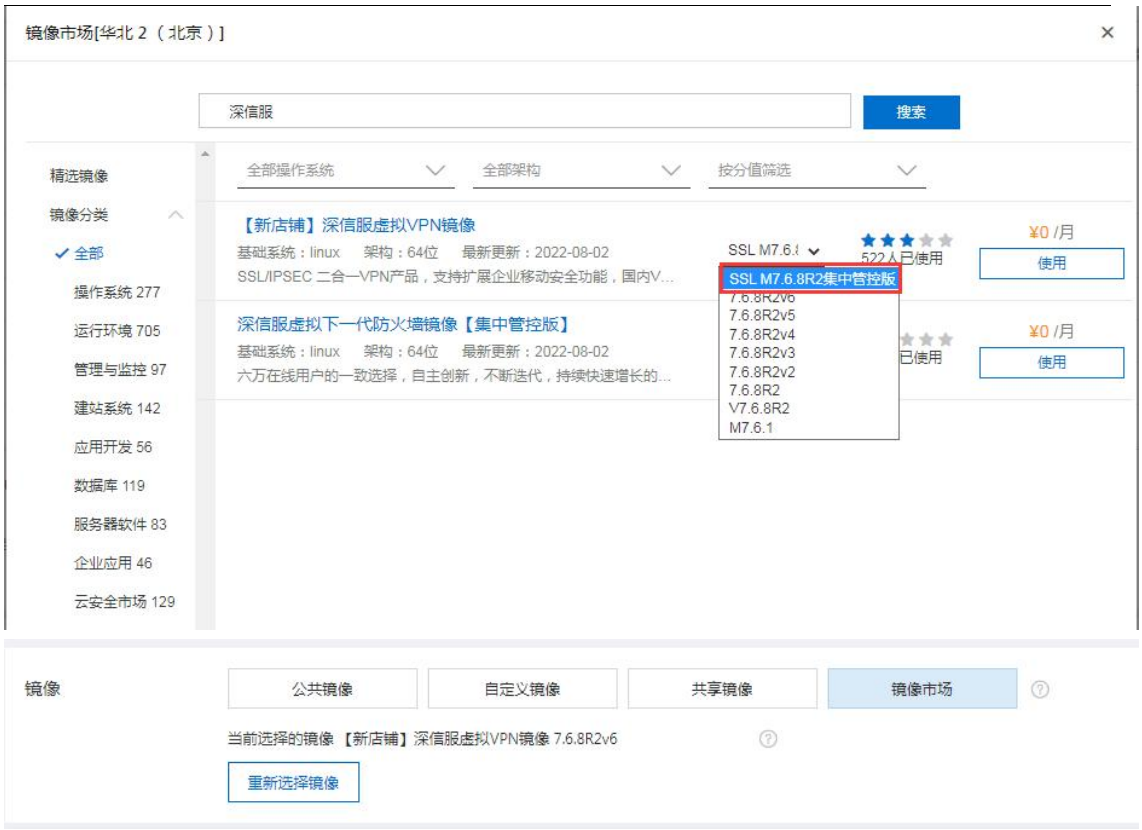
出现以下选择页面，参考上述章节中的资源规格配置，按照实际需求选择对应的服务器，例如选择 2 核 CPU、4G 内存的云服务器。注意“地域”一定要选择和云业务服务器在同一个地域



镜像在“自定义镜像”/共享镜像中选择已上传或其他账号共享到云平台的 vSSL7.6.8R2 的镜像，或者在“镜像市场”中搜索使用深信服 SSLVPN，选择最新 SSL M7.6.8R2 版本即可。

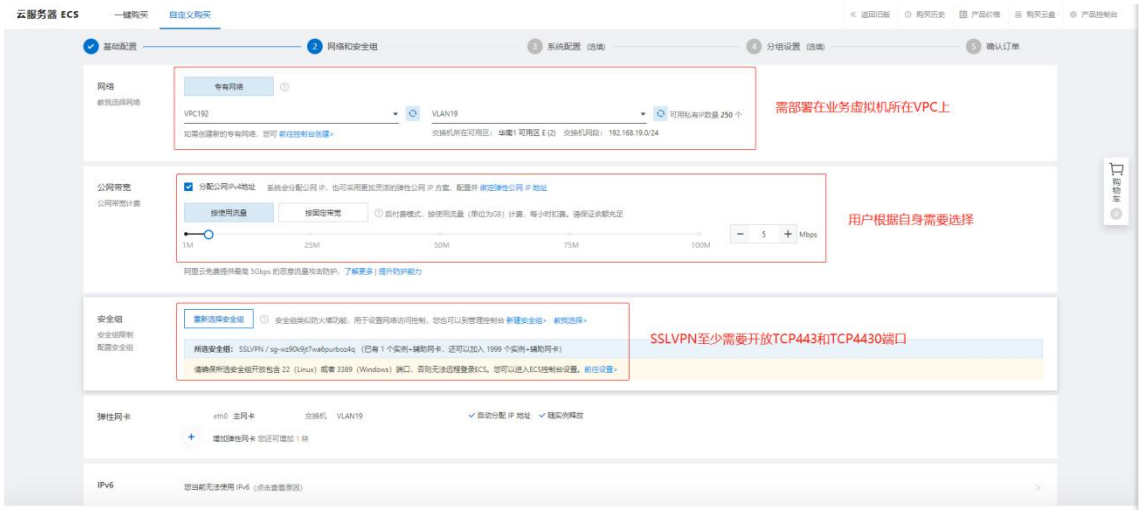
目前镜像市场在【华北 1/2/3/5、华南 1、华东 1/2、香港】等区域上线

【说明】国外阿里云市场没有深信服 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效云盘或者 SSD 云盘，存储选择最低 40G 即可，不需要选择额外的数据盘。可根据需求向上扩容系统盘

3.2 配置网络和安全组



网络需要选择专有网络，需要选择业务虚拟机所在的 VPC，VLAN 可以是跟业务虚拟机同一个，也可以是独立的 VLAN；

公网带宽根据实际情况选择；

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。

点击 新建安全组 跳转到新窗口设置安全组；

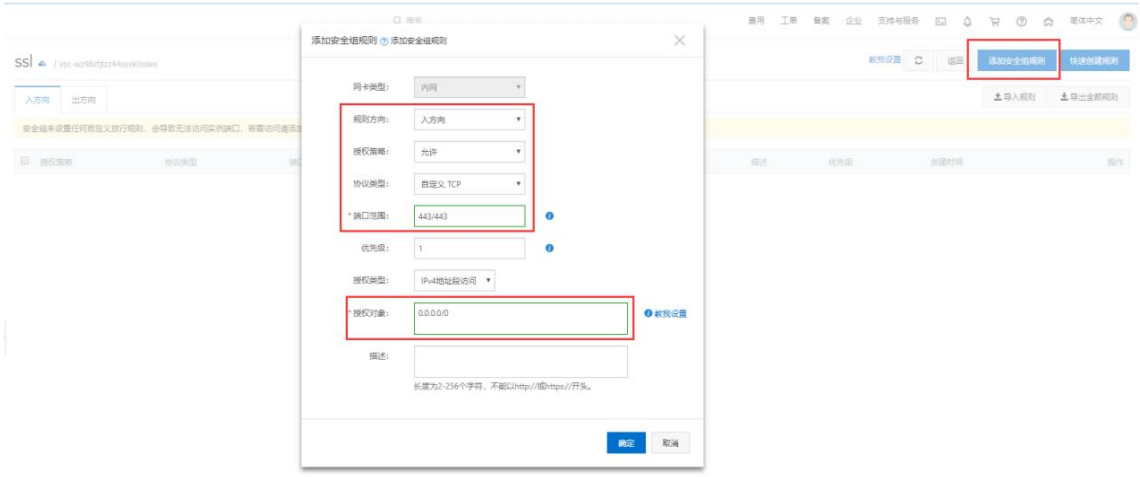
在新弹出的网页中点击 创建安全组 按钮；

模板选择自定义，名称按照实际情况填写，最后点击 确定 按钮保存。

创建完成后，点击 配置规则 按钮添加规则；

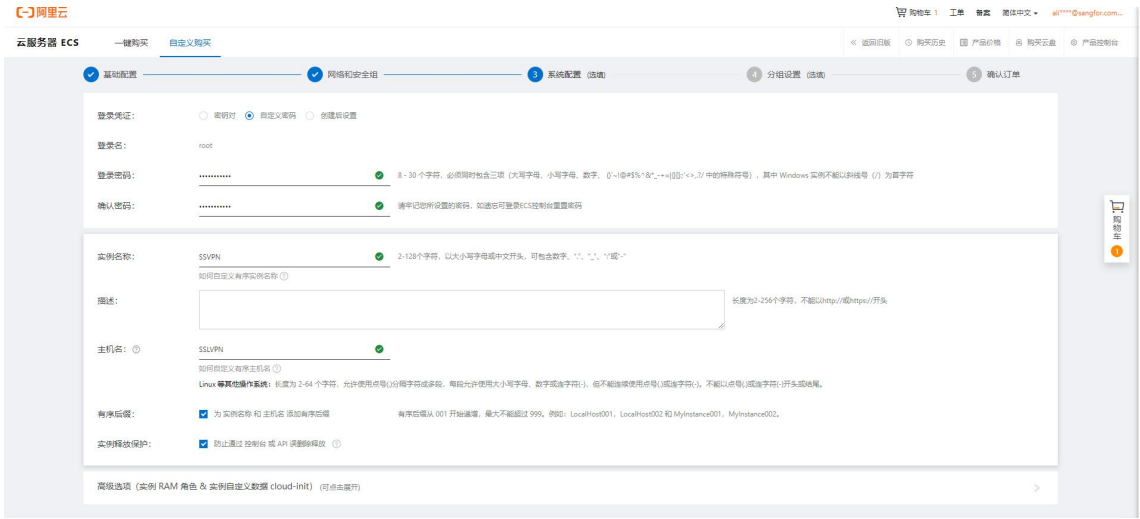
跳转到配置页面后，点击 添加安全组规则 按钮，然后在弹出的网页中逐个添加 TCP4430、TCP51111、TCP22 端口。

注：规则方向选择入方向；授权动作选择允许；授权对象填写 0.0.0.0/0（代表任意 IP，若有其他需求则按需填写）

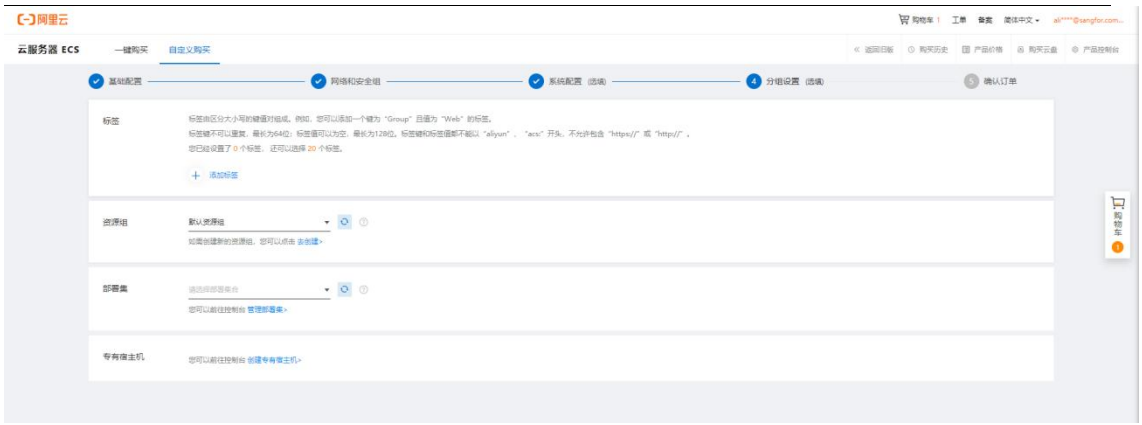


填写完成后回到配置云服务器的页面，点击重新选择安全组的按钮，选择刚刚创建的安全组，然后选择下一步；

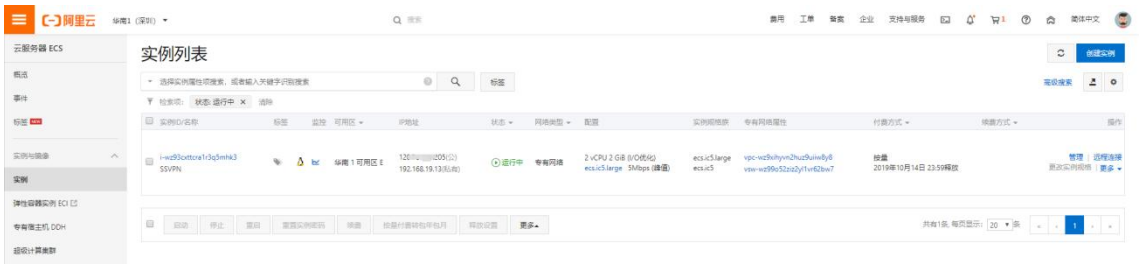
后面的配置按照实际情况选择即可。一般默认



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



最后确认订单支付即可完成 vSSLVPN 云主机的创建。创建完成后可以在实例列表里看到新建的 vSSL VPN 主机的相关信息，包括运行状态、内网 IP 地址、EIP 地址、配置信息等，如下图。



3.3 设备登录

因为 vSSLVPN 默认是支持 DHCP 功能的，所以无需进后台配置 IP 地址和路由，既云主机购买部署成功后，便可以使用 IE 浏览器打开如下 vSSLVPN 的控制台，地址：https://IP:4430，默认用户名和密码为：admin/admin。管理登录界面如下所示：

第 4 章　设备授权

4.1 独立在线授权

4.1.1.测试授权申请：

联系测试授权或交付人员获取测试授权序列号

可致电深信服客服询问：售后服务热线：400-630-6430 （中国大陆）

序列号如下所示：


```
[global]
vendor =                        SANGFOR TECHNOLOGIES INC.
licno =                         7C41EE41743779AC878D
aid =                           A4076-2C0C-C6B9-F3C1-D64C-FEDF-E74D-94B9
customer_name =                 深信服测试专用
license_type =                  test
license_date =                  2021-08-13 17:43:29
license_version =               7.5
customer_company =              unknow_company
yuntu_account =                 unknow_yuntu_account
sflicense_version =             1.0.0
trial_date =                    1636646399
active_modules =                SSL

[SSL]
sn =                            3FB8-96C7-CC33-F0C5-7CF3-C227-26DC-EA20
```

4.1.2.测试授权激活：

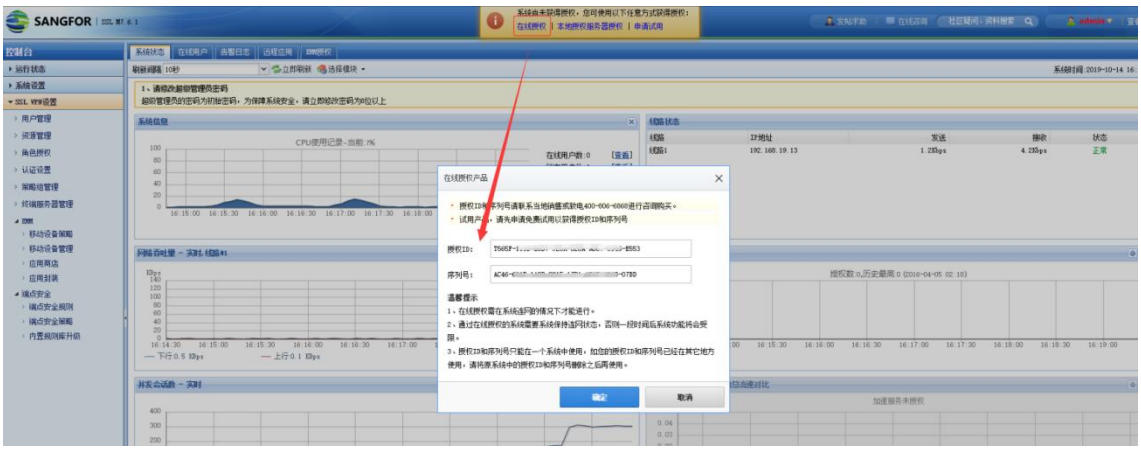
使用浏览器打开 vSSLVPN 的控制台，地址：https://IP:4430

默认用户名和密码为：admin/admin。

点击上方系统提示-在线授权，将 aid 填入授权 ID：，将 sn 填入序列号：

授权信息点击左树菜单栏-系统设置-系统配置-授权信息查看

注意：在线授权需要 SSL 设备联网，能与授权中心域名 vls.sangfor.com.cn 保持通讯



4.1.3.正式授权申请：

联系销售或交付人员获取正式授权序列号

可致电深信服客服询问：售后服务热线：400-630-6430 （中国大陆）

4.1.4.正式授权激活：

激活步骤与 4.1.2 相同

授权成功后在授权页面会有【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。

4.2 多云安全平台在线授权

深信服 SSL VPN 使用多云安全平台在线授权：

4.2.1.测试授权申请：

自注册并登陆多云安全平台地址：https://mcsp.sangfor.com.cn

在【云安全能力中心】-【应用市场】中立即购买/申请试用 SSL 应用，提交待审核完毕

审核结果在【云安全能力中心】-【应用中心】中查看

可致电深信服客服询问：售后服务热线：400-630-6430 （中国大陆）

4.2.2.测试授权激活：

审核通过后在【云安全能力中心】-【应用中心】中点击部署应用

由于 SSL 实例已经创建完成，此时只需激活授权，选择【其他云环境】，上线方式选择网络可达以及网络代理，具体详情可参考说明文档

点击立即部署之后大约 2-5min 内可以完成授权，在应用中心查看在线情况，并登陆防

火墙

4.2.3.正式授权申请：

可联系销售或者商务，根据正式购买订单开通多云安全平台账号以及防火墙应用

4.2.4.正式授权激活：

激活步骤与 4.2.2 相同

第 5 章 SSL 组件功能配置

5.1 SSL 功能配置

1 用户环境与需求：

A 公司在阿里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。

2 配置步骤如下：

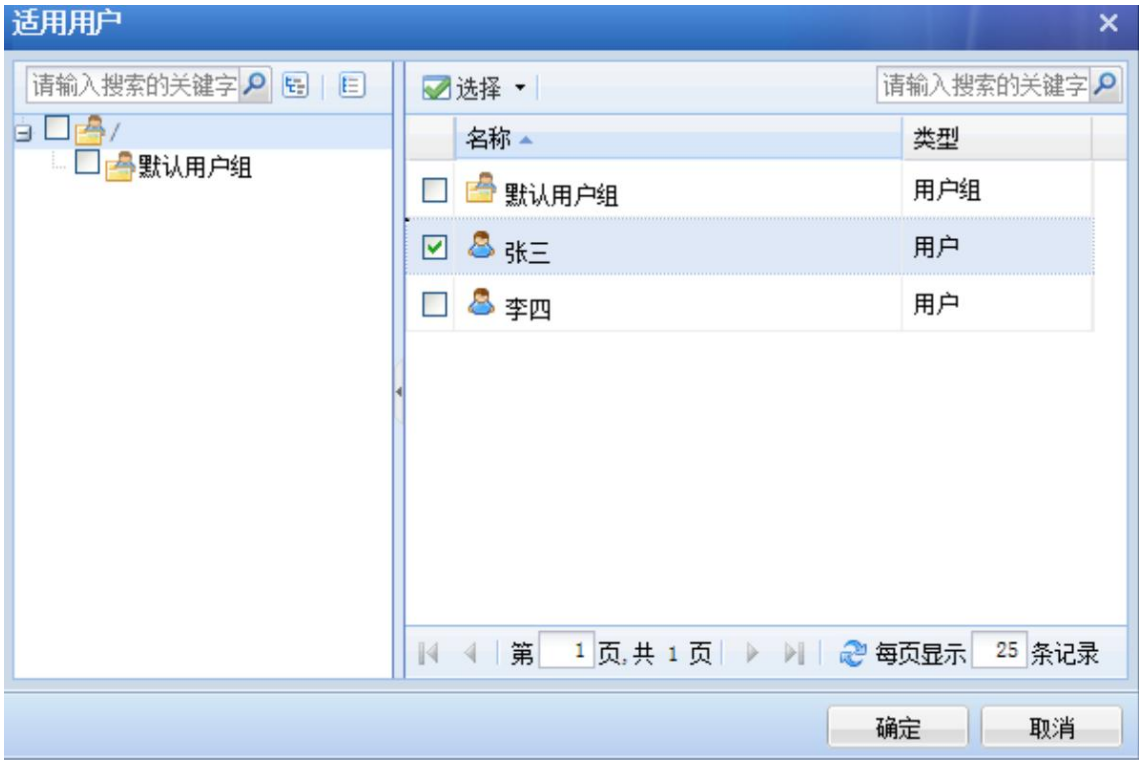
第一步：进入『SSL VPN 设置』→『用户管理』，点击新建，新建两个 SSL 接入用户，配置完以后点保存，本案例配置界面如下：

第二步：进入『SSL VPN 设置』→『资源管理』，新建一个 L3VPN。点击新建，选择 L3VPN，设置资源名称，选择资源类型，配置界面如下：

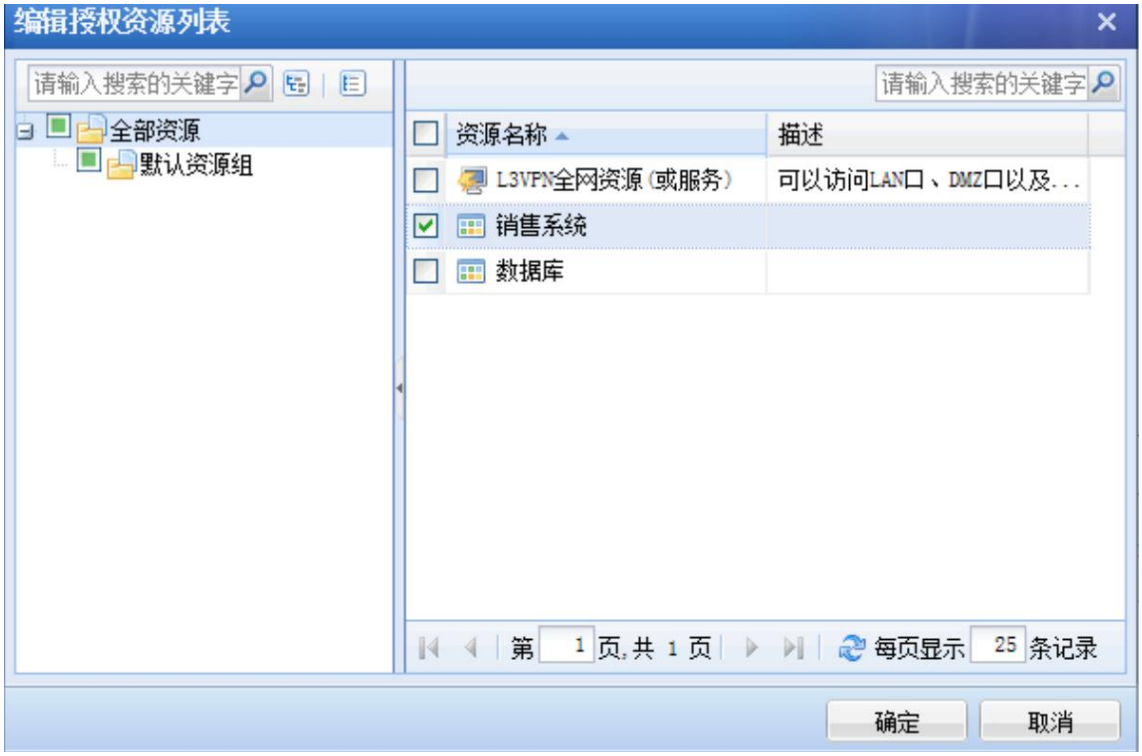
配置资源地址，点击后面的添加按钮，配置完后点击确定，配置界面如下：

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：



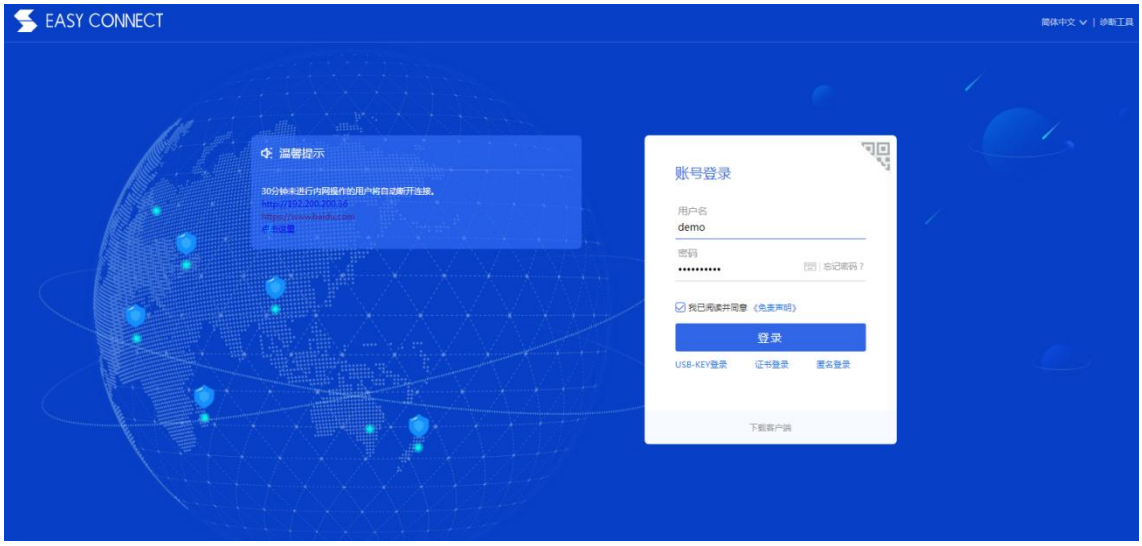
进入『编辑授权资源』页面，选择关联资源，界面如下：配置完以后点保存。

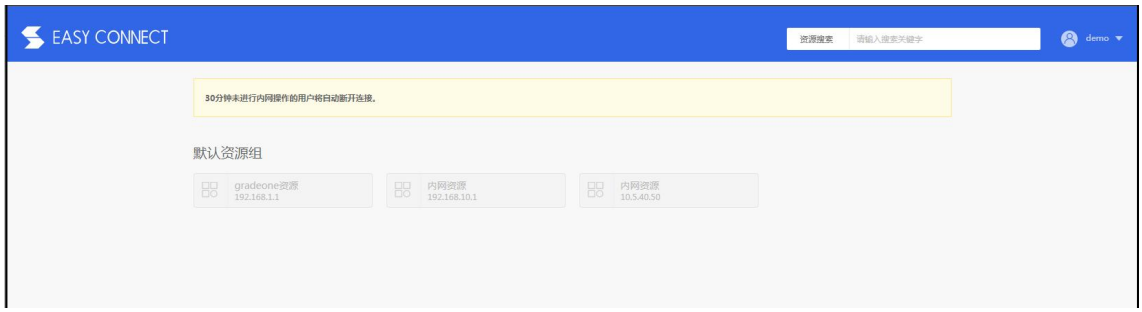


第四步：配置完成后点击【立即生效】，使配置生效。

第五步：用户在浏览器上输入 SSL 的登录地址：https://sslIP

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：





5.2 IPSEC 功能配置

1 用户环境与需求：

A 公司在阿里云 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 设备与阿里云上的深信服 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。

2 配置步骤如下：

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：

添加到阿里云 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：

阿里云深信服 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，阿里云 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——在阿里云 VPC 虚拟路由器上配置路由。

阿里云 VPC 路由表路由配置：

在阿里云 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。

第 6 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. **组建集群问题**

   答：需要以下两个条件才可以组集群，（分布式部署不需要以下两个条件）

   A. 云平台的网络需要支持组播。

   B. 云平台中的 IP 能够被云主机里面的系统自由的切换和使用。因为 SSL VPN 的集群方案需要一个 CIP，这个 CIP 最初是绑定在主机上，一旦主机挂了，VPN 系统会在备机上启用这个 CIP，但是很多云平台不支持虚拟机里面的系统自由绑定 IP，而是需要人工手动在云平台上面操作，把 IP 绑定到虚拟机上。

如果以上两个条件支持，那么可以组集群，组集群的一些注意事项如下：

A. 只开 EMM 序列号，可以组集群。

B. 组集群时，两台或者多台设备开通的功能必须一致，数量可以不一致。

C. 组集群后，两台或者多台设备的授权数量是叠加的。比如 vpn1 有 10 个 ssl vpn 授权用户数，vpn2 有 20 个 ssl vpn 授权用户数，那么组集群后，就总共有 30 个 ssl vpn 授权用户数。EMM 授权用户数也是如此。

D. 如果集群在异常或者正常情况下拆了，60 天内没有重新组起来，那么授权数将会回到这台设备最初申请的授权用户数。

附： 联系方式

深圳市南山区学苑大道 1001 号南山智园 A1 栋

售前咨询热线：400-806-6868

手机用户请拨打：0755-86627830

售后服务热线：400-630-6430

Email:master@sangfor.com.cn

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