深信服 vSSL VPN 部署实施指导书

深信服科技股份有限公司

2021 年 10 月

版权声明

深信服科技股份有限公司版权所有，并保留对本文档及本声明的最终解释权和修改权。

本文档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，除另有特别注明外，其著作权或其它相关权利均属于深信服科技股份有限公司。未经深信服科技股份有限公司书面同意，任何人不得以任何方式或形式对本文档内的任何部分进行复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部分用于商业用途。

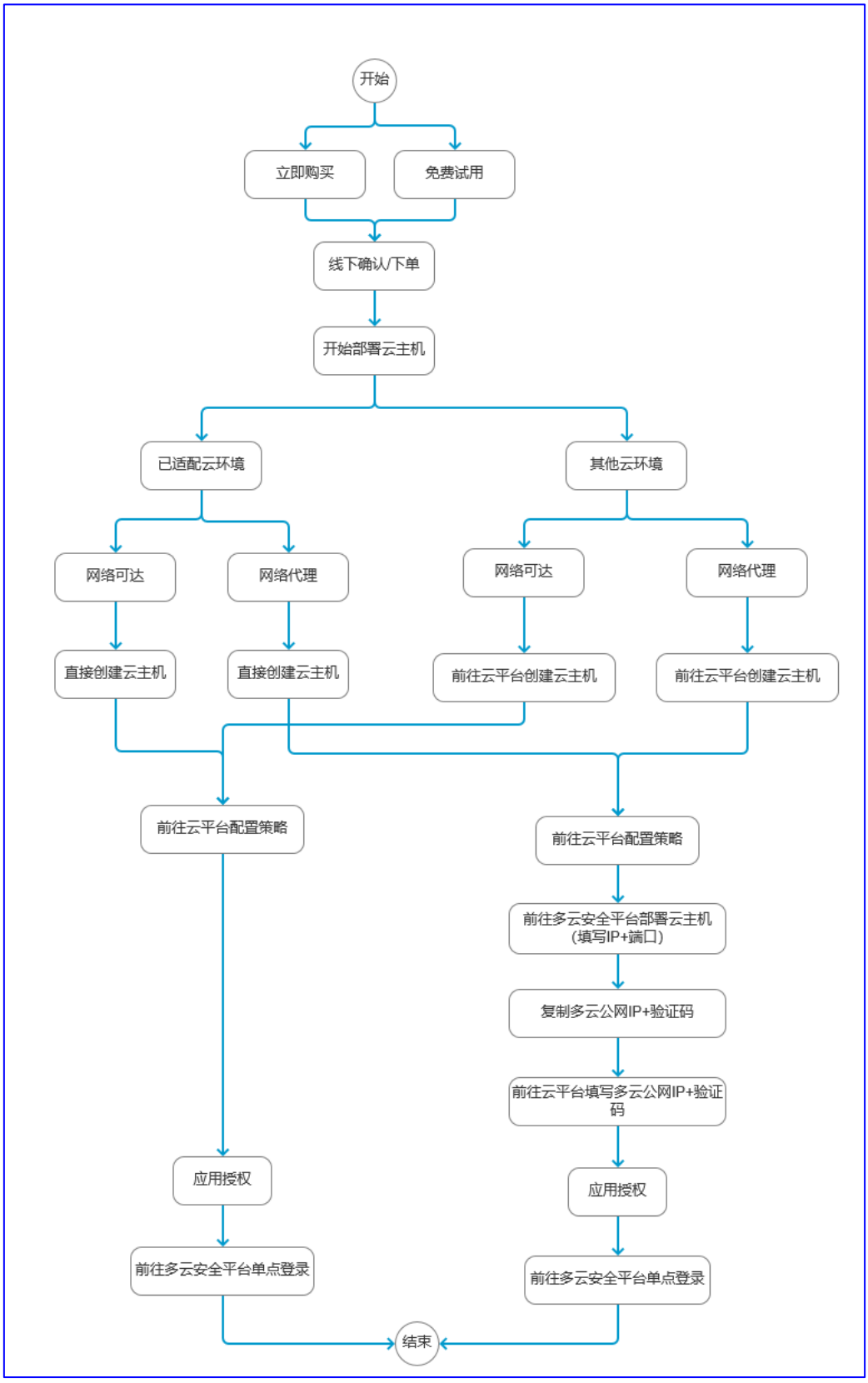
免责条款

本文档仅用于为最终用户提供信息，其内容如有更改，恕不另行通知。

深信服科技股份有限公司在编写本文档的时候已尽最大努力保证其内容准确可靠，但深信服科技股份有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

目 录

1 流程介绍


开始
立即购买
免费试用
线下确认/下单
开始部署云主机
已适配云环境
其他云环境
网络可达
网络代理
网络可达
网络代理
直接创建云主机
直接创建云主机
前往云平台创建云主机
前往云平台创建云主机
前往云平台配置策略
前往云平台配置策略
前往多云安全平台部署云主机（填写IP+端口）
复制多云公网IP+验证码
前往云平台填写多云公网IP+验证码
应用授权
应用授权
前往多云安全平台单点登录
前往多云安全平台单点登录
结束

2 操作步骤

2.1 部署云主机

1、多云安全平台已适配“阿里云”“腾讯云”“华为云”，支持直接创建并部署云主机。

2、其他云环境需先联系多云安全平台客户经理分享镜像，通过该镜像在云平台创建云主机并配置 SNAT 后，再选择“其他云环境”并填写公网/私网 IP 和端口信息。

说明：可前往云平台查看 NAT。查看阿里云 NAT 说明文档

2.1.1 已适配云环境

在深信服多云安全平台-云安全能力中心-应用中心找到待部署的应用，点击“部署云主机”进行部署。

说明：登录深信服多云安全平台请联系店铺客服。

1、选择云环境与应用授权方式

选择云环境：支持选择“阿里云”“腾讯云”“华为云”。

选择云帐号：选择已接入的云帐号。若没找到合适的云帐号请先接入。接入说明请查看《连接云环境说明文档》

主帐号 ID：选择“阿里云”“腾讯云”时，需提供所选云帐号的主帐号 ID 用于创建云主机。可前往云平台-帐号信息复制主帐号 ID。

说明：主帐号 ID 填写错误会导致镜像分享失败。

（1）获取阿里云主帐号 ID，主帐号登录阿里云控制台时，鼠标悬浮 hover 用户头像并复制下图的账号 ID 即可。

（2）获取阿里云主帐号 ID，子帐号登录阿里云控制台时，鼠标悬浮 hover 用户头像并复制下图的企业别名即可。

（3）获取阿里云主帐号 ID，主帐号登录腾讯云控制台时，鼠标悬浮 hover 用户头像并复制下图的账号 ID 即可。

（4）获取阿里云主帐号 ID，子帐号登录腾讯云控制台时，鼠标悬浮 hover 用户头像并复制下图@后的主账号 ID 即可。

应用授权方式：包括网络可达、网络代理。

网络可达表示多云安全平台主动连接应用的公网 IP。

网络代理表示应用连接多云安全平台的公网 IP。

2、创建云主机

付费模式：可选包年包月、按量付费，建议选择和应用一致的付费模式。

购买时长：建议购买和应用一致的时长。免费试用结束的应用重新购买后，请前往云平台将云主机的到期时长更改成与应用一致或更长。

地域：选择业务所在私有网络的地域。

网络：选择业务所在的私有网络及子网。

项目 ID：云环境选择“华为云”时，需要填写项目 ID。

性能参数：多云安全平台根据应用选型自动计算出对应的实例规格、存储。

公网 IP：选择网络可达方式需提供公网 IP，如应用的防护带宽大于 100Mbps 或使用了 DNAT 方案，建议先不分配公网 IP，在主机创建完成并进行 DNAT 网关相关配置后，再前往多云安全平台找到应用填写绑定在 DNAT 上的公网 IP。

说明：SSL VPN 需配置的公网 IP 网络带宽请参考 2.4 应用组件规格及资源消耗表。

端口：默认选择 4430。

安全组：第一次连通必须将 4430 端口的访问策略设置为允许多云安全平台（42.193.174.234）访问。

2.1.2 其他云环境

1、选择云环境与应用授权方式

说明：多云安全平台已适配“阿里云”“腾讯云”“华为云”，其他云环境请前往对应的云平台通过多云安全平台分享的镜像创建云主机。

应用授权方式：包括网络可达、网络代理。

网络可达表示多云安全平台主动连接应用的公网 IP，需用户提供公网 IP 及端口信息。

网络代理表示应用连接多云安全平台的公网 IP，需用户前往云平台登录云主机填写多云安全平台公网 IP 及验证码信息。

2、创建云主机

付费模式：可选包年包月、按量付费，建议选择和应用一致的付费模式。

购买时长：建议购买和应用一致的时长。免费试用结束的应用重新购买后，请前往云平台将云主机的到期时长更改成与应用一致或更长。

地域：选择业务所在私有网络的地域。

网络：选择业务所在的私有网络及子网。

性能参数：根据多云安全平台提供的应用选型选择云主机规格及存储。点击查看应用组件规格及资源消耗表

公网 IP：选择网络可达方式需提供公网 IP。若应用的防护带宽大于 100Mbps 或使用了 DNAT 方案，建议先不分配公网 IP，在主机创建完成进行 DNAT 网关相关配置后，再前往深信服多云安全平台-云安全能力中心-应用中心找到应用填写绑定在 DNAT 上的公网 IP。

说明：SSL VPN 需配置的公网 IP 网络带宽请参考 2.4 应用组件规格及资源消耗表。

端口：默认选择 4430。

安全组：第一次连通必须将 4430 端口的访问策略设置为允许多云安全平台（42.193.174.234）访问。

2.2 配置策略及授权

2.2.1 网络可达方式一：云主机绑定公网 IP 方案

2.2.1.1 配置策略

确认安全组策略：云主机绑定的安全组 4430 允许多云安全平台（42.193.174.234）访问。

说明：

1、若云主机所关联的安全组不符合要求，请前往云平台-安全组创建安全组并绑定云主机。

2、若需换成其他的端口，请在第一次授权成功后再修改。

2.2.1.2 应用授权

网络可达模式配置正确，会自动发起第一次授权，请前往深信服多云安全平台-云安全能力中心-应用中心查看，当应用状态更新为“正常”即为授权成功。后续应用离线后需您主动“发起连接”才能再次连通。

说明：云环境为“其他云环境”时，完成以上配置后请前往深信服多云安全平台-云安全能力中心-应用中心找到该应用，点击“部署云主机”填写云主机的公网 IP 及端口信息，当应用状态更新为“正常”即为授权成功。

（1）填写公网 IP 及端口并点击立即部署

（2）查看应用状态

2.2.2 网络可达方式二：使用 DNAT 方案

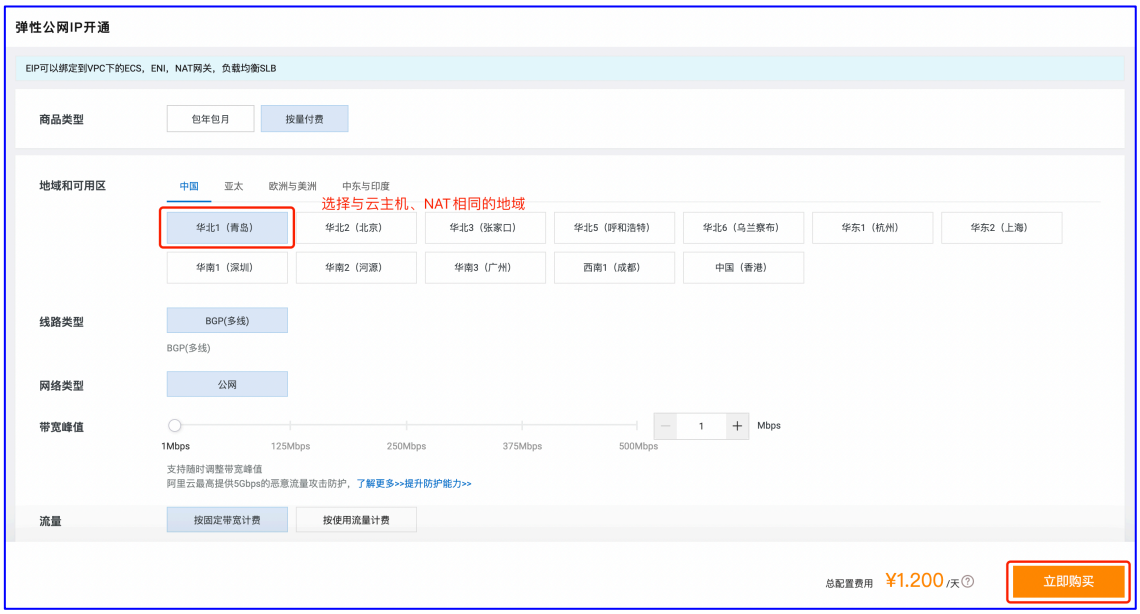
选择网络可达方式需提供公网 IP，如应用的防护带宽大于 100Mbps 或使用了 DNAT 方案，建议先不分配公网 IP，在主机创建完成并进行 DNAT 网关相关配置后，再前往深信服多云安全平台-云安全能力中心-应用中心找到应用填写绑定在 DNAT 上的公网 IP。

2.2.2.1 配置策略

2.3.2.1.1 创建弹性公网 IP

1、前往弹性公网 IP 控制台-创建公网 IP。如您已创建请直接往下配置 DNAT。

2、填写相关信息，其中地域需选择与云主机、NAT 相同的地域。



2.2.2.1.2 配置 DNAT

1、前往专有网络控制台-NAT 网关-进入 NAT 网关详情

说明：若创建新的 NAT 网关，需选择与主机相同的地域及 VPC。

2、在“DNAT”页面创建 DNAT

3、填写 DNAT 条目信息并点击确定创建

选择公网 IP 地址：选择弹性公网 IP，该公网 IP 需在多云安全平台填写

选择私网 IP 地址：选择刚刚创建云主机的私网 IP。

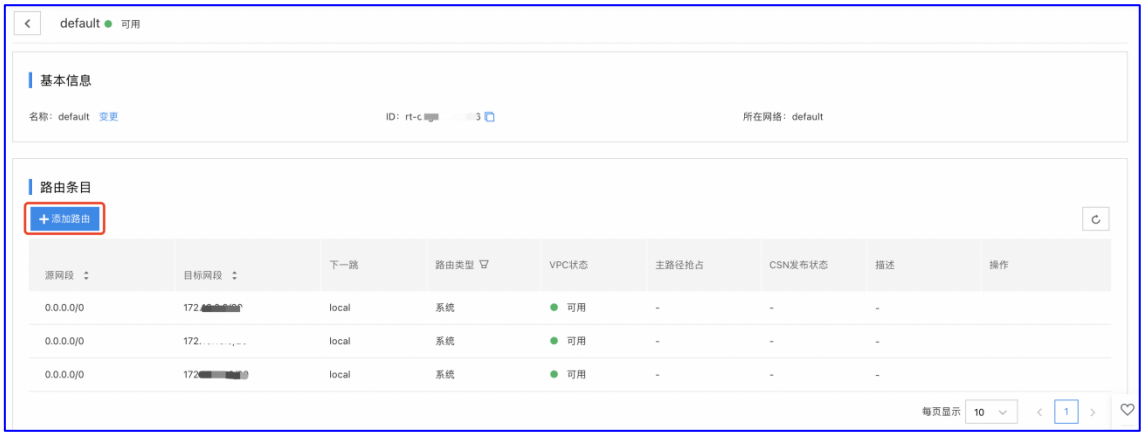
端口设置：公网端口可自定义，该端口需在多云安全平台填写；第一次授权时 SSL VPN 公网端口、私网端口必须填写 4430。

2.2.2.1.3 配置路由表

说明：阿里云不需要配置路由表，腾讯云、华为云、百度云需要配置路由表。

1、选择路由表并点击进入路由表详情页

2、添加路由



3、填写路由信息并点击确定

源网段：当前云主机所在的网段

目标网段：云主机需要访问的网段

路由类型：选择“NAT 网关”

下一跳实例：选择刚刚配置的“DNAT 实例”

2.2.2.1.4 确认安全组策略

云主机绑定的安全组 4430 允许多云安全平台（42.193.174.234）访问。

说明：

1、若云主机所关联的安全组未符合要求，请前往云平台-安全组创建安全组并绑定云主机。

2、若需换成其他的端口，请在第一次授权成功后再修改。

2.2.2.2 应用授权

网络可达模式配置正确，会自动发起第一次授权，请前往多云安全平台-云安全能力中心-应用中心查看，当应用状态更新为“正常”即为授权成功。后续应用离线后需您主动“发起连接”才能再次连通。

说明：云环境为“其他云环境”时，完成以上配置后请前往深信服多云安全平台-云安全能力中心-应用中心找到该应用点击“部署云主机”或“更改信息”并填写 DNAT 绑定的公网 IP 及端口信息，当应用状态更新为“正常”即为授权成功。

（1）填写公网 IP 及端口并点击立即部署

（2）查看应用状态

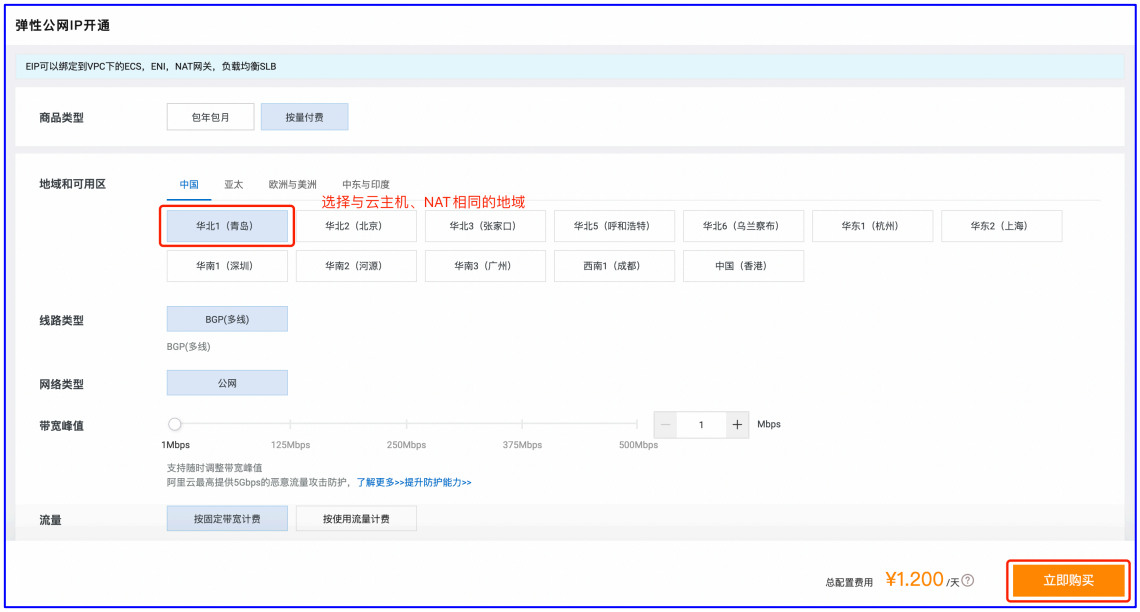
2.2.3 网络代理方式：使用 SNAT 方案

2.2.3.1 配置策略

2.2.3.1.1 创建弹性公网 IP

1、前往弹性公网 IP 控制台-创建公网 IP。如您已创建请直接往下配置 DNAT。

2、填写相关信息，其中地域需选择与云主机、NAT 相同的地域。



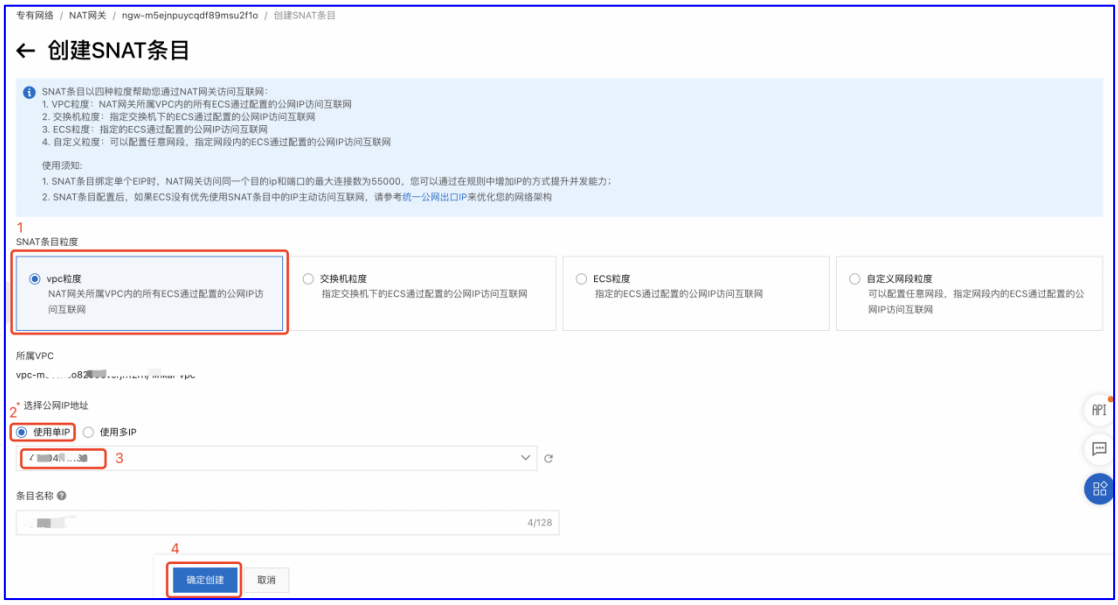
2.2.3.1.2 配置 SNAT

1、前往专有网络控制台-NAT 网关-进入 NAT 网关详情

说明：若创建新的 NAT 网关，需选择与云主机相同的地域及 VPC。

2、在“SNAT”页面创建 SNAT

3、选择 vpc 粒度及刚刚创建的公网 IP 并点击“确定创建”



2.2.3.2 填写验证码

第一步：前往深信服多云安全平台-云安全能力中心-应用中心查看应用的验证码

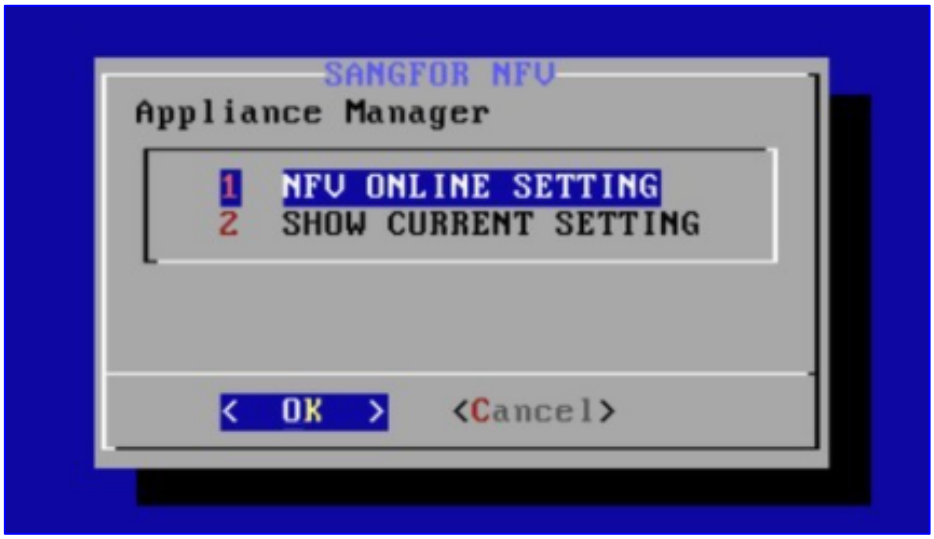
说明：云环境选择其他云环境时，在云平台创建云主机后，需在深信服多云安全平台-云安全能力中心-应用中心找到该应用订单点击“部署云主机”，填写云主机的私网 IP 及端口信息，部署完成应用同步成功即可查看验证码。

（1）部署云主机

（2）查看并复制验证码

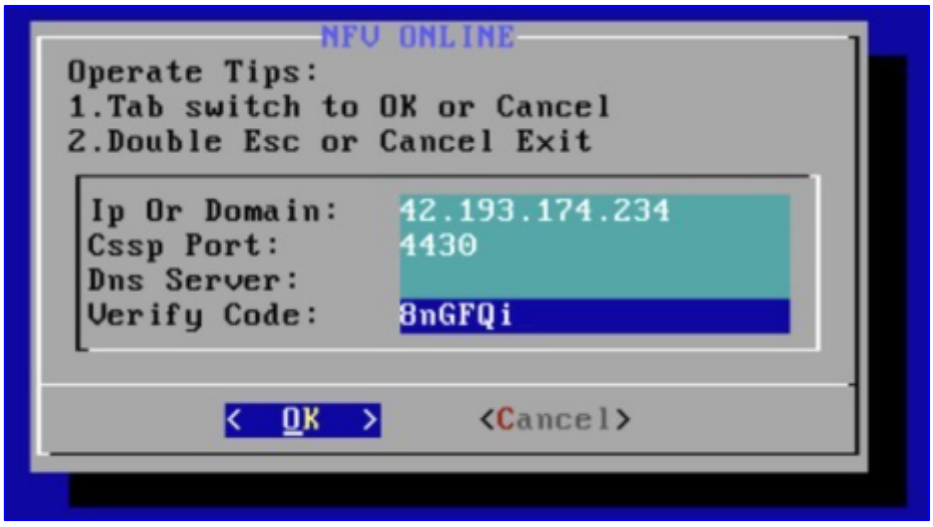
第二步：在云服务器-实例列表找到该主机，并登录/远程连接该主机

第三步：在“SANGFOR NFV”界面找到“NFV ONLINE SETTING”并点击“OK”



第四步：在“NFV ONLINE”界面的“Ip Or Domain”、“Uerify Code”分别填写多云安全平台的公网 IP（42.193.174.234）和应用的验证码。

说明：如未能正常打开“NFV ONLINE”界面，请按 alt+F8 或 option+F8。



2.2.3.3 应用授权

网络代理模式配置正确后将自动授权，请前往多云安全平台-云安全能力中心-应用中心查看，当应用状态更新为“正常”即为授权成功。

2.3 单点登录

前往云安全能力中心-应用中心，当应用状态为“正常”时，点击“进入应用”即可单点登录至应用的控制台。

2.4 应用组件规格及资源消耗表

产品名称	应用规格	所需要资源（虚拟核心数、内存、硬盘）	网络可达方式-主机绑定公网 IP 带宽性能
SSL VPN	最大理论并发用户数/EMM 授权数 50	2vCPU,4GiB，50G 系统盘	网络带宽性能 10Mbps
SSL VPN	最大理论并发用户数/EMM 授权数 100	2vCPU,4GiB，50G 系统盘	网络带宽性能 20Mbps
SSL VPN	最大理论并发用户数/EMM 授权数 200	2vCPU,4GiB，50G 系统盘	网络带宽性能 40Mbps
SSL VPN	最大理论并发用户数/EMM 授权数 300	2vCPU,4GiB，50G 系统盘	网络带宽性能 60Mbps
SSL VPN	最大理论并发用户数/EMM 授权数 500	2vCPU,4GiB，50G 系统盘	网络带宽性能 100Mbps
SSL VPN	最大理论并发用户数/EMM 授权数 1000	2vCPU,4GiB，50G 系统盘	网络带宽性能 200Mbps
SSL VPN	最大理论并发用户数/EMM 授权数 2000	4vCPU,8GiB，50G 系统盘	网络带宽性能 400Mbps
SSL VPN	最大理论并发用户数/EMM 授权数 5000	4vCPU,8GiB，50G 系统盘	网络带宽性能 1000Mbps
SSL VPN	最大理论并发用户数/EMM 授权数 7000	8vCPU,16GiB，50G 系统盘	网络带宽性能 1400Mbps

特殊要求说明：同时购买并发数、EMM 授权数时请按较高的一个应用规格数选择所需要资源及带宽性能。如购买并发数为 1000，EMM 授权数为 2000 时，需选择 2000 对应的所需要资源及带宽性能。

2.5 云平台链接汇总

云平台	分类	链接
阿里云	安全组	立即前往
阿里云	NAT 网关	立即前往
阿里云	弹性公网 IP	立即前往
阿里云	云服务器	立即前往