SANGFOR_vAF8095_部署实施指导

For 阿里云

深信服智安全
SANGFOR SECURITY

2024 年 12 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	20241210			71980

目录

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。依托该需求深信服推出了基于公有云通用的搭建防火墙的解决方案，实现客户云数据安全化，解决客户痛点。

满足信创 PlatOS arm/x86、非信创 CentOS，并支持云化镜像部署。

vAF 特性描述：由于云防火墙部署在公有云上和物理墙功能上存在一些差异，版本针对云的特性针对性的做了一些适配

1. 网卡适配

- 支持 virtio_net 和 vmxnet3 的网卡驱动，e1000 驱动可用但存在性能不足
- 取消带外管理口的功能，公有云的 qcow2 镜像的 eth0 口默认为 dhcp 的模式，其他云平台 ETH0 口默认为静态 IP。eth0 口可以作为业务口；
- 物理口限制对于 mac 地址的修改

2. 双机部署

- 双机仅支持主备模式的配置，不支持主主及镜像模式的配置
- 双机默认关闭虚拟 mac 的配置，统一使用真实 mac 的转发

3.云防火墙隐藏的功能

- 隐藏了虚拟系统的功能
- 隐藏掉带外管理的配置
- 隐藏聚合口配置，不支持聚合口

4.云防火墙版本升级

- 新架构 vAF 支持版本升级，使用与硬件平台相同升级包，升级路线与硬件一致

第 2 章　部署环境概述

2.1 用前必读

深信服 vAF 是虚拟镜像方式存放在阿里云平台上，因此您需要先给 vAF 提供 ECS（Elastic Compute Service，阿里云服务器），您可以向阿里云购买等方式获得 ECS。

由于阿里云平台限制了“经典网络”的 ESC 用于部署防火墙，所以用于 vAF 的 ECS 必须采用“虚拟私有云”类型（VPC 网络），新购买的 ECS 用户手动选择“可用区”的时候，不要使用界面的默认配置，因为默认配置选择的是“经典网络”类型。

我们对 vAF 的 ECS 硬件配置分别为以下几种组合，因此您在购买的时候需要注意配置。

2C4G：2 核 CPU + 4G 内存

4C8G：4 核 CPU + 8G 内存

8C16G：8 核 CPU + 16G 内存

12C24G：12 核 CPU + 24G 内存

16C32G：16 核 CPU + 32G 内存

您在选购 ESC 时，请手动选择以上其中一种配置组合，若您已经购买了 ECS，请您检查下 ECS 配是否符合以上几种条件。

2.2 阿里云平台特性描述

- 底层架构为 KVM；
- 能够自定义上传镜像格式包括 Qcow2、VHD；
- 支持绑定弹性 IP，创建实例时，实例规格配置不同，所支持的网卡数量不同；

2.3 镜像获取

公有云 AF 提供支持信创/非信创场景 Qcow2、vmdk 等格式镜像文件

可联系深信服客服获取：售后服务热线：0755-23832091

获取链接：https://support.sangfor.com.cn/productSoftware/list?product_id=178

2.4 部署方式

在阿里云的 ECS 服务器上搭建 vaf8.0.95，支持网关模式部署/单臂模式部署（即三层部署）/旁路镜像（请查看阿里官网支持镜像流量区域）

https://help.aliyun.com/zh/vpc/user-guide/traffic-mirroring-overview

2.5 资源配置

1、性能在 200M 以内，云主机使用 2 核 4G 的配置；

2、性能在 400M 以内，云主机使用 4 核 8G 的配置；

3、性能在 800M 以内，云主机使用 8 核 16G 的配置；

4、性能在 1.5G 以内，云主机使用 12 核 24G 的配置；

5、性能在 2G 以内，云主机使用 16 核 32G 的配置；

产品	配置	吞吐量
云下一代防火墙（vAF8.0.95）	2C4G+120G 硬盘	5M-200M
	4C8G+120G 硬盘	300M-400M
	8C16G+120G 硬盘	500M-800M
	12C24G+120G 硬盘	900M-1G
	12C24G+120G 硬盘	1.5G
	16C32G+120G 硬盘	2G

2.6 授权方式

1、多云安全中心平台在线授权（网络可达）多云平台地址：https://csc.sangfor.com.cn

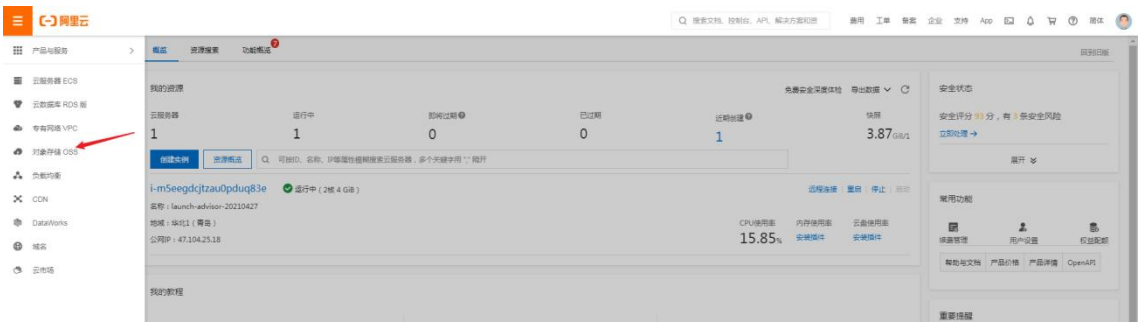
2、授权中心离线授权

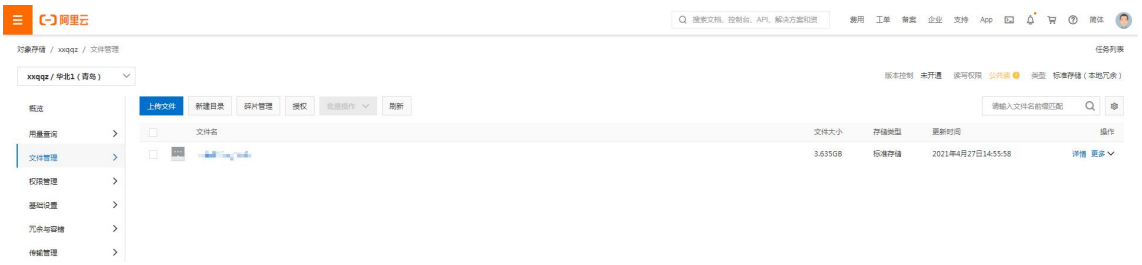
第 3 章　部署指导

3.1 镜像上传/制作：

镜像上传：

登陆阿里云中国站 www.aliyun.com 打开对象存储 OSS，将获取到的镜像上传至平台



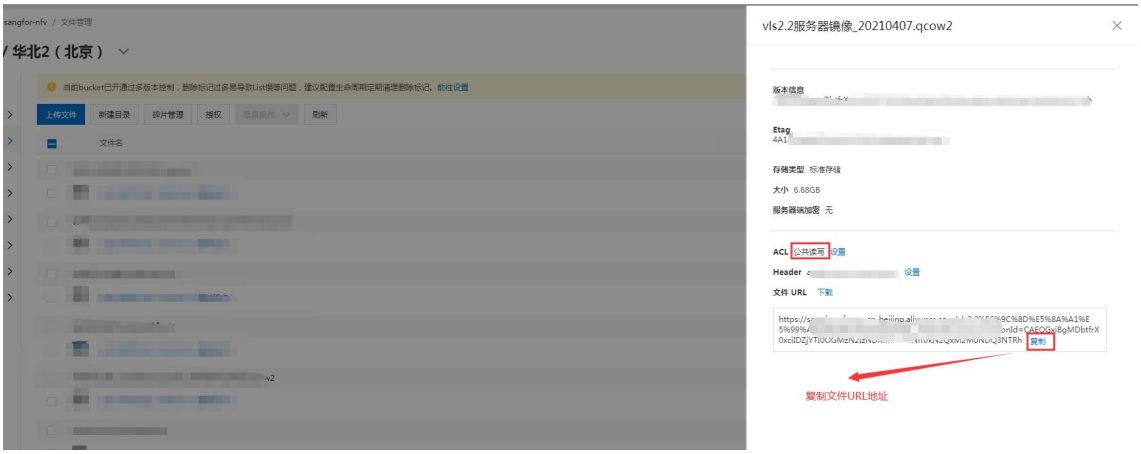


PS：如镜像大小超过平台网页传输大小限制，可使用图形化工具 OSS Browser+客户端上传，使用步骤参考深信服社区：

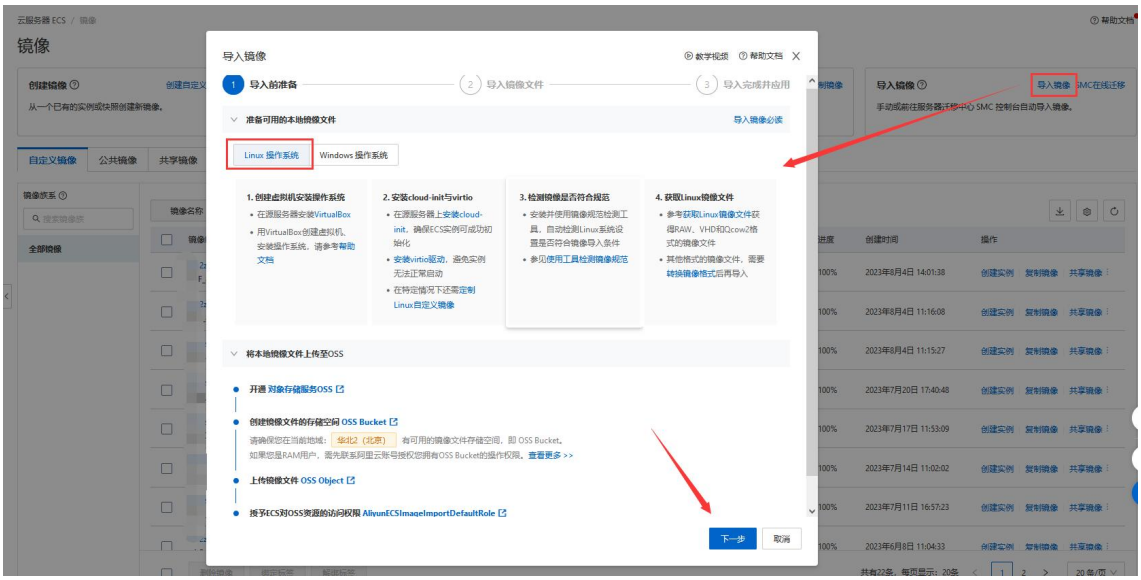
https://support.sangfor.com.cn/productDocument/read?product_id=178&version_id=1025&category_id=282786

制作成自定义镜像：

获取 OSS 对象地址：



云服务器 ECS-实例与镜像-镜像、导入镜像



防火墙镜像 X86 架构参数要求：

操作系统类型：　　Linux

操作系统版本：　　Kylin

操作系统架构：　　64 位操作系统 x86_64

系统盘大小：　　120G

镜像格式：　　Qcow2（可不填自动检测）

防火墙镜像 ARM 架构参数要求：

操作系统类型：　　Linux

操作系统版本：　　Kylin

操作系统架构：　　ARM64 位操作系统 arm64

系统盘大小：　　120G

镜像格式：　　Qcow2（可不填自动检测）

3.2 创建实例（ECS）：

第一步：

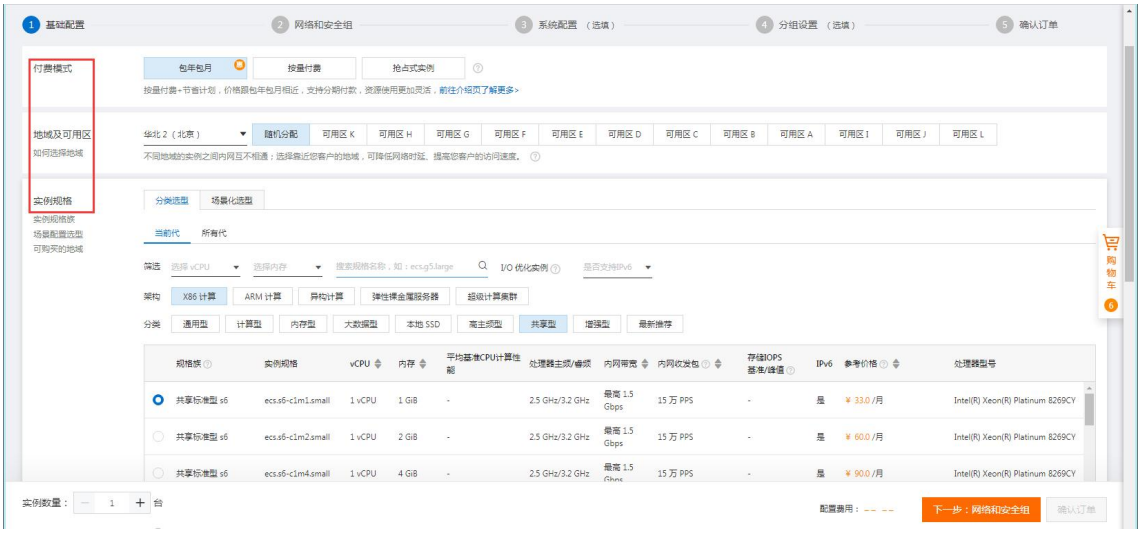
登陆阿里云中国站进入-【云服务器 ECS】-【实例与镜像】-实例，创建实例

第二步：

根据实际需求选择付费方式、地域、规格大小（规格选择请参考上述资源配置要求）

注意：推荐使用实例规格族：经济型、通用算力型 u1、计算型 c7、网络增强型 c7nex 等。

「不支持 C8i、C9i 实例规格」



镜像选择自定义镜像-上述步骤制作的镜像

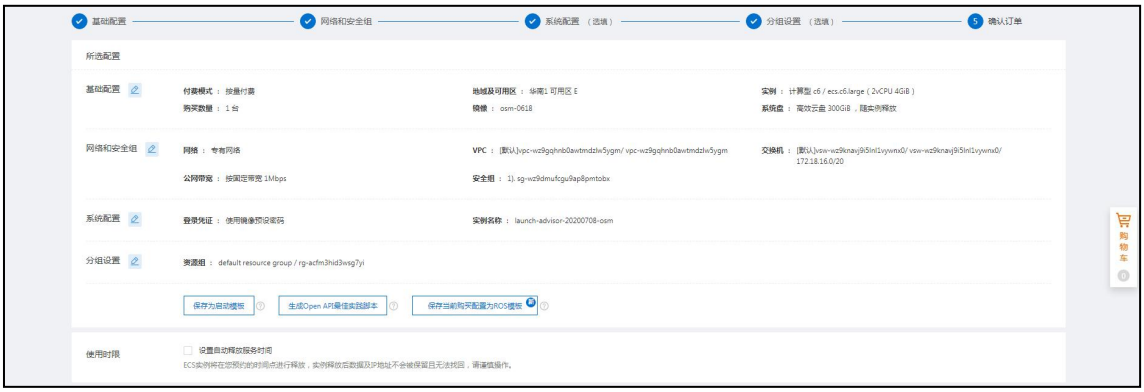
磁盘大小需 120G 以上，可不添加数据盘

第三步：

配置网络以及安全组，需要注意放通 443 端口+7443 端口（默认控制台端口为 443，7443 端口使用 csc 在线授权时使用）。

公网 IP 请根据实际需求购买

注意：登录凭证只能选用镜像密码，所有组件均只能使用镜像自身密码。此处可随意设置密码，该设置密码对于防火墙不生效

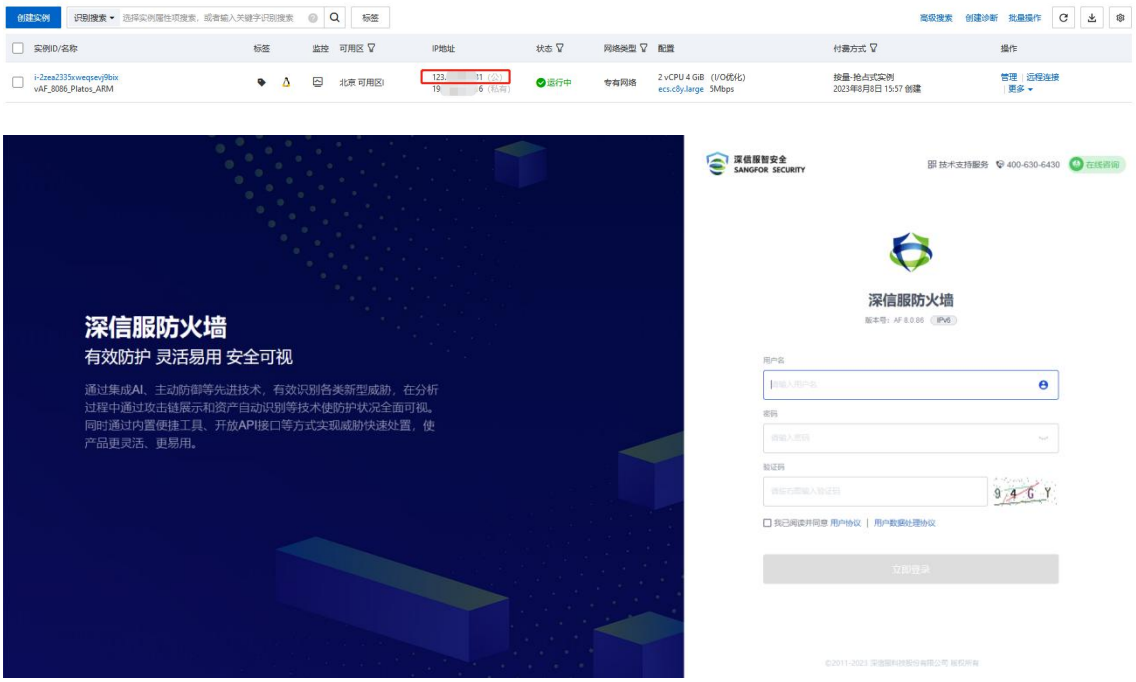


查看实例列表，创建成功

3.3 设备登陆：

使用公网地址登录 vAF，登陆方式：https://x.x.x.x、默认登陆密码 admin/admin

注意：8095vAF 未授权无法登录 WEBUI 控制台



第 4 章　设备授权

4.1 公有云安全组件授权平台在线授权：

深信服云下一代防火墙使用云安全中心在线授权：

4.1.1.测试授权申请：

①、注册云图账号(如已有云图账号可跳过步骤 1，前往步骤 2 登陆)

注册链接：https://xaasauth.sangfor.com.cn/?source=xcentral#/register

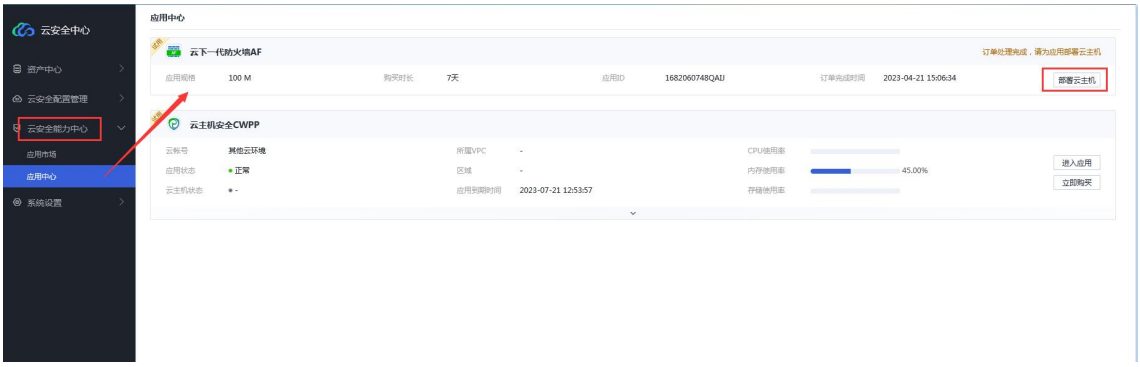
②、使用云图账号登陆云安全平台(一定需要登陆)

访问链接：https://csc.sangfor.com.cn

在【云安全能力中心】-【应用市场】中立即购买/申请试用防火墙应用，提交后待审核完毕

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）

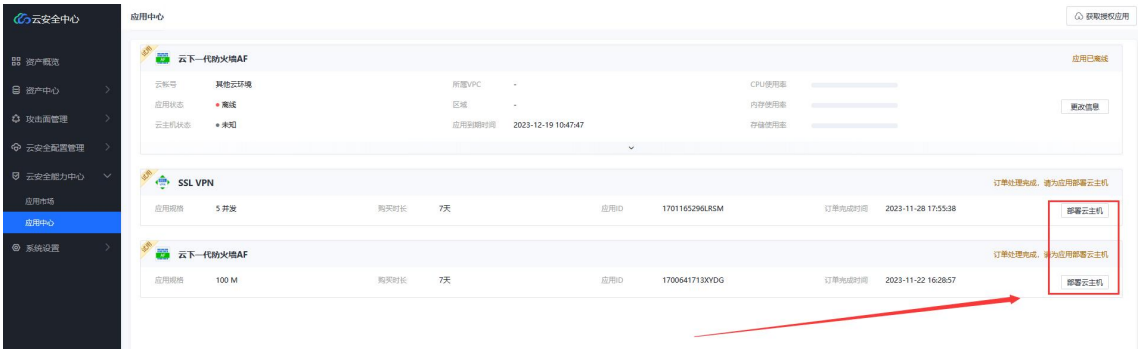


4.1.2.测试授权激活：

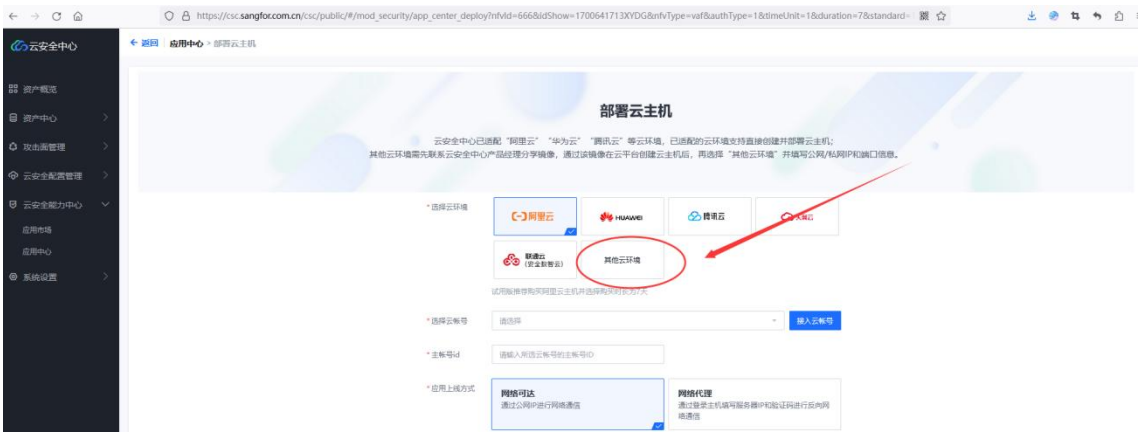
审核通过后在【云安全能力中心】-【应用中心】中点击部署应用

网络可达：

①、登陆云安全授权平台-【云安全能力中心】-【应用中心】-[部署云主机]



②、选择【其他云环境】选项



③、选择【其他云环境】-以授权防火墙组件为例：

选择【其他云环境】

云主机模式：不选择

应用组件版本号选择：【8090】（8090 及以上版本）

方式选择：【网络可达】

填写防火墙设备的公网 IP 和端口以及设备超级管理员登录的管理员账号密码

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

网络代理详细步骤可以参考深信服社区：

https://support.sangfor.com.cn/productDocument/read?product_id=178&version_id=1025&category_id=282791

4.1.3.正式授权申请：

①、注册云图账号(如已有云图账号可跳过步骤 1，前往步骤 2 登陆)

注册链接：https://xaasauth.sangfor.com.cn/?source=xcentral#/register

②、使用云图账号登陆云安全中心(一定需要登陆)

访问链接：https://csc.sangfor.com.cn

③、联系销售或者商务，根据正式购买订单添加防火墙应用

4.1.4.正式授权激活：

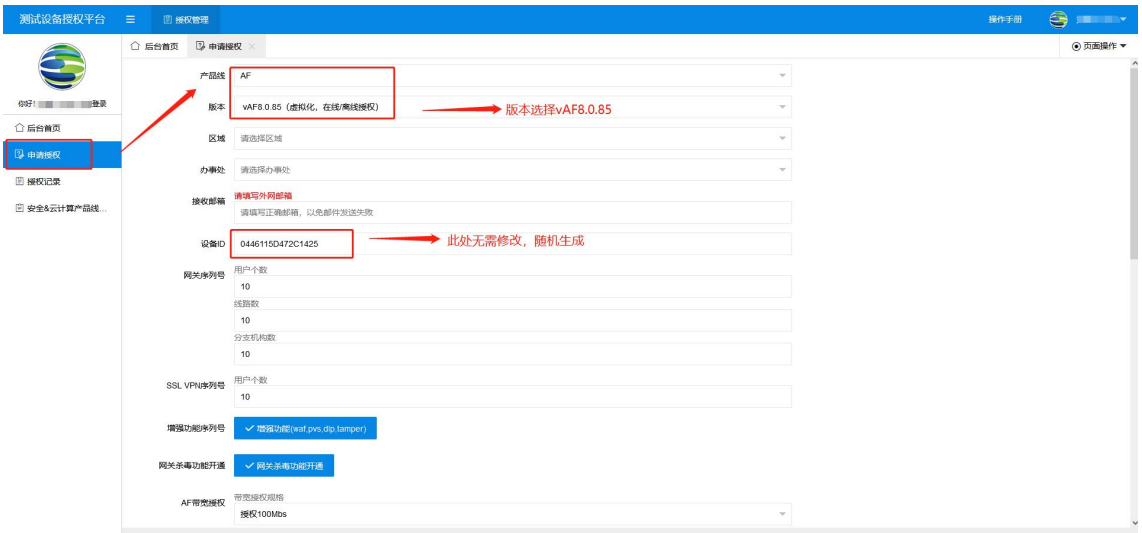
激活步骤与 4.1.2 相同

4.2 授权中心离线授权：

使用授权中心离线授权：license.sangfor.com.cn

4.2.1.测试授权申请：

联系深信服技术支持申请：提供设备 ID/硬件信息



4.2.2.授权激活：（按提示进行激活）

条件：8095 未授权无法登录控制台，需后台创建离线标志文件

授权激活指引：

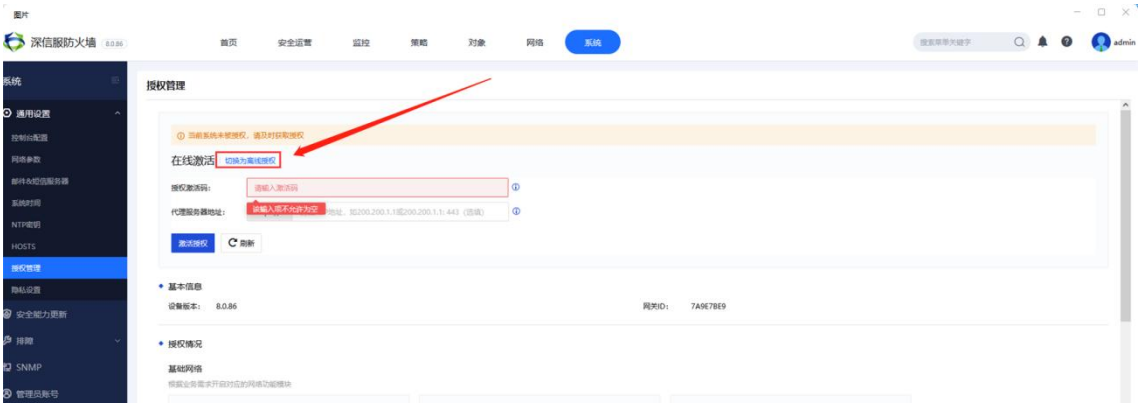
①触发离线授权条件：

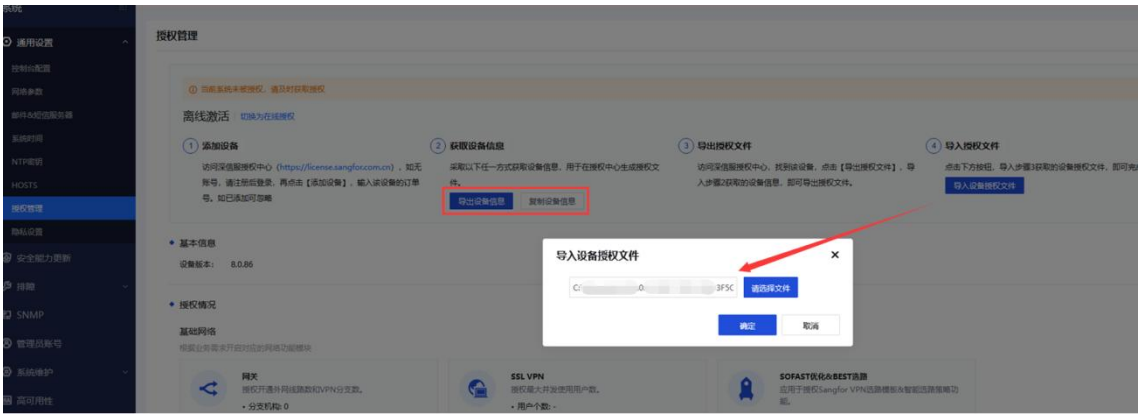
进入 vAF 后台创建标志文件：

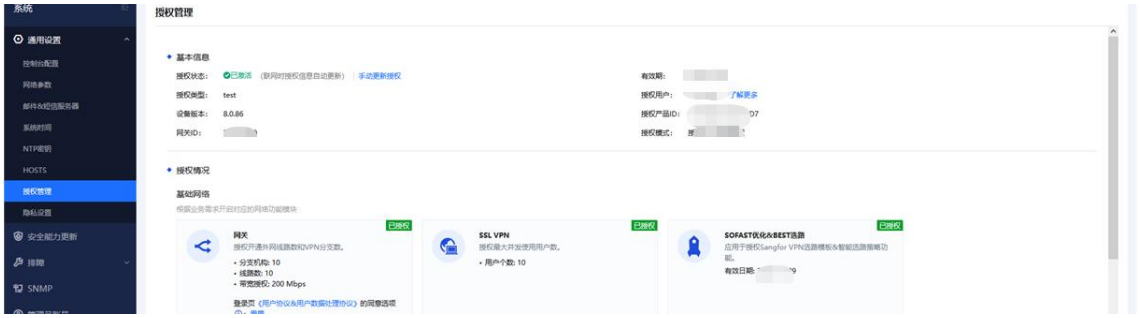
touch /sfos/system/etc/af/auth_mode_flag

售后服务热线：400-630-6430 （中国大陆）联系深信服 400 协调工程师切换离线授权

②登录 web 点击切换离线授权，并根据当前设备硬件信息开出授权文件导入激活





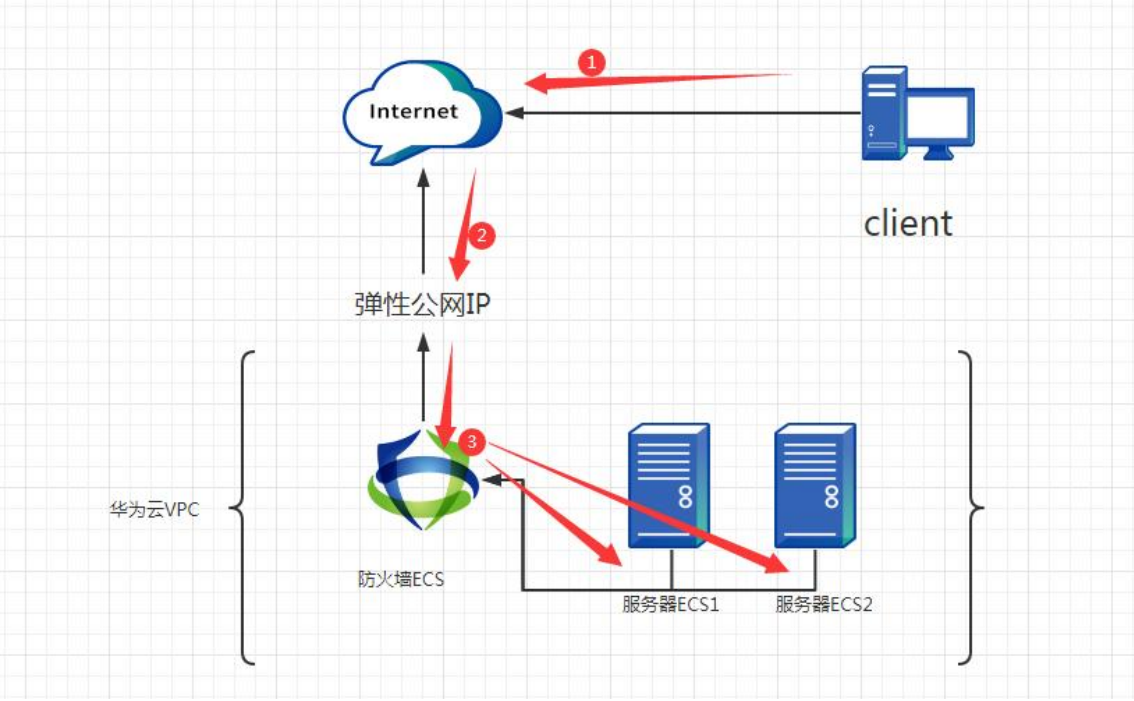


第 5 章　防火墙基本配置

5.1 单网卡单公网 IP 部署场景：

5.1.1.需求背景：

客户在阿里云部署了一台、或者多台业务服务器系统，需求要通过防火墙进行等保安全防护，实现通过防火墙映射访问业务系统，并通过防火墙代理上网，达到上下行流量经过防火墙安全防护。



5.1.2.需求分析：

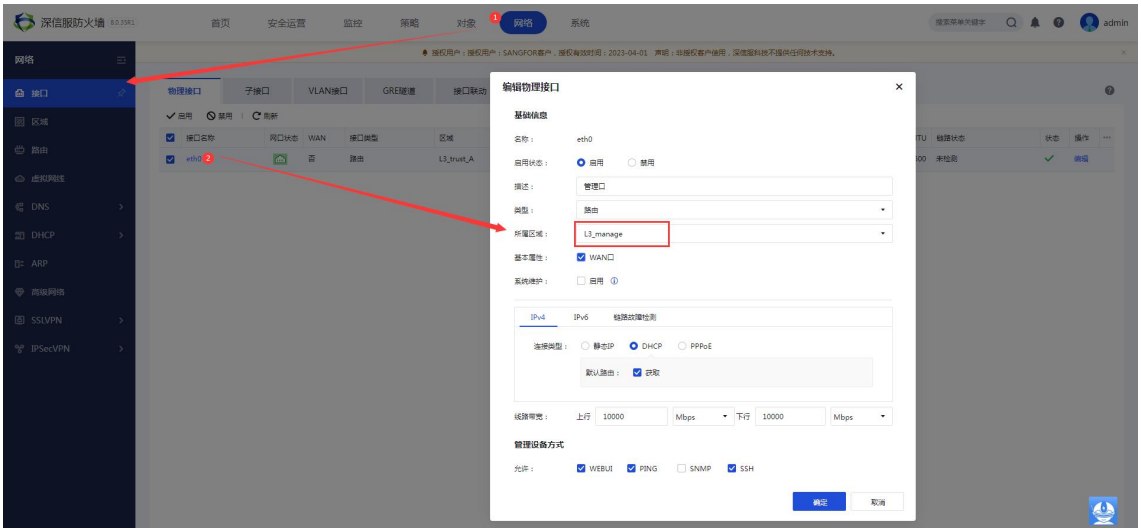
客户阿里云部署了一台或者多台业务系统，对外提供服务的只有一个公网 IP，并且无重复端口，将防火墙部署在与业务系统相同的 VPC 子网中，并将业务系统的公网 IP 绑定给防火墙使用，从而达到业务发布通过防火墙映射访问，通过调整 vpc 子网路由表实现业务系统通过防火墙代理上网，

5.1.3.配置步骤：

业务发布配置：

防火墙配置 DNAT：发布业务系统

步骤 1：进入接口配置区域



步骤 2：进入策略-地址转换-新增目的地址转换

新增 NAT：选择[目的地址转换]

[源区域]：eth0 口所在区域

[源地址]：全部

[目的地址]：eth0 口 IP 地址　　注意：此处 IP 地址需要填写防火墙接口私网 IP 地址

[服务]：80 端口/其他

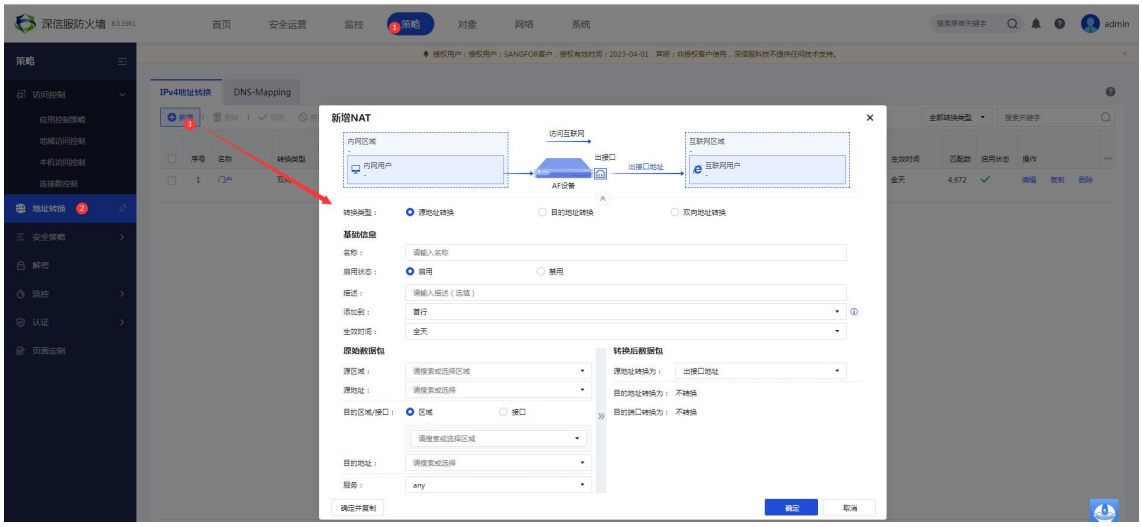
[目的地址转换]：指定 IP 服务器 IP

注意：新增服务端口时，源端口需填写全部（0-65535）

代理上网配置：

防火墙配置 SNAT：代理业务系统上网

步骤 1：进入策略-地址转换-新增源地址转换



新增 NAT：默认选择[源地址转换]

[源区域]：eth0 口所在区域

[源地址]：需要代理上网的内网网段

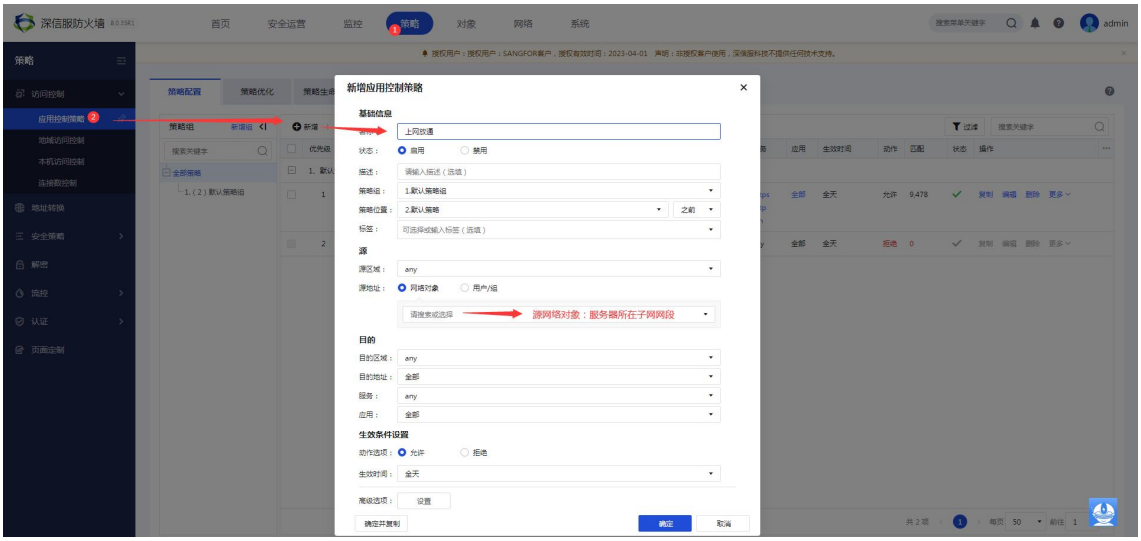
[目的区域/接口]：eth0 口所在区域

[目的地址]：全部

[服务]：any

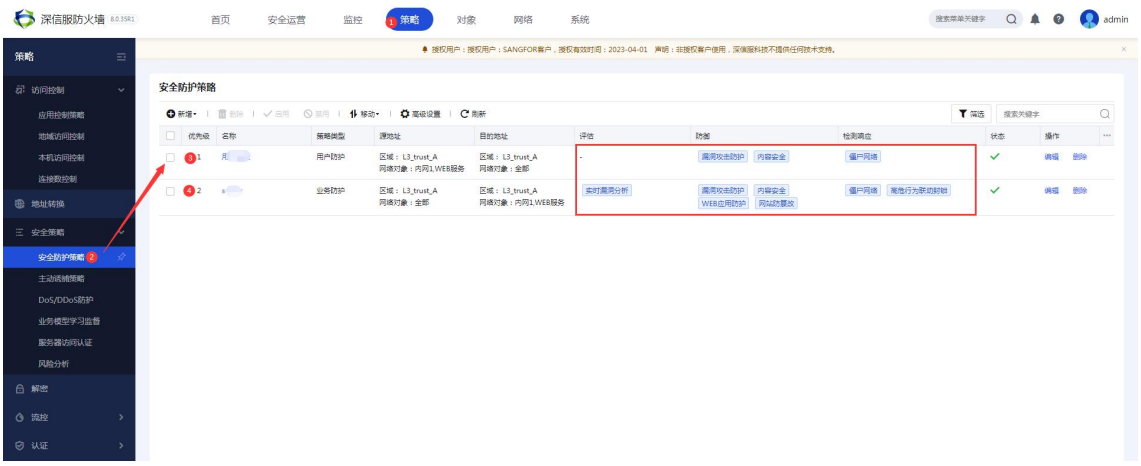
[源地址转换为]：出接口

步骤 2：进入策略-访问控制-应用控制策略-新增 ACL 放通上网流量



安全防护策略配置：

步骤 1：进入策略-安全策略-安全防护策略-新增业务安全与用户安全



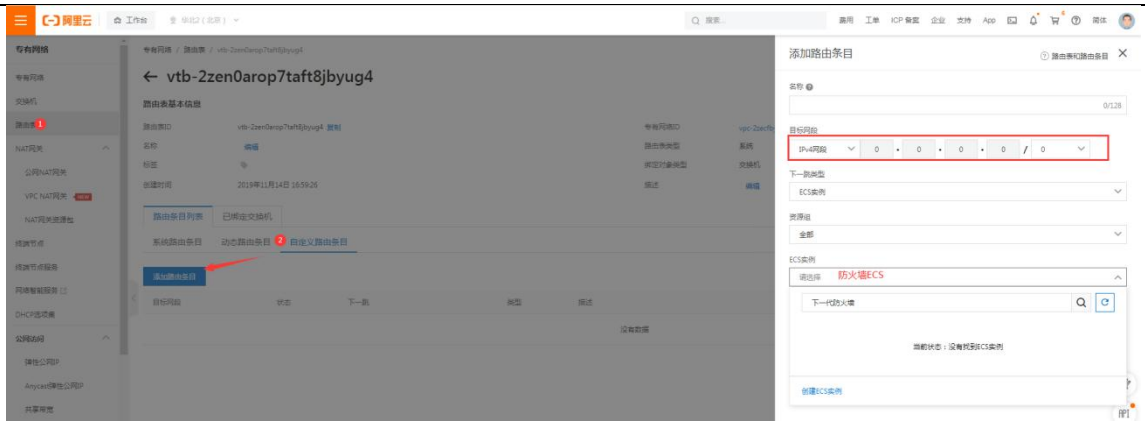
平台引流配置：

由于阿里云平台特性，服务器上网流量需要使用到路由表功能将上网流量引流至防火墙

步骤 1：登陆阿里云平台-虚拟私有云 VPC-路由表-新增自定义路由条目

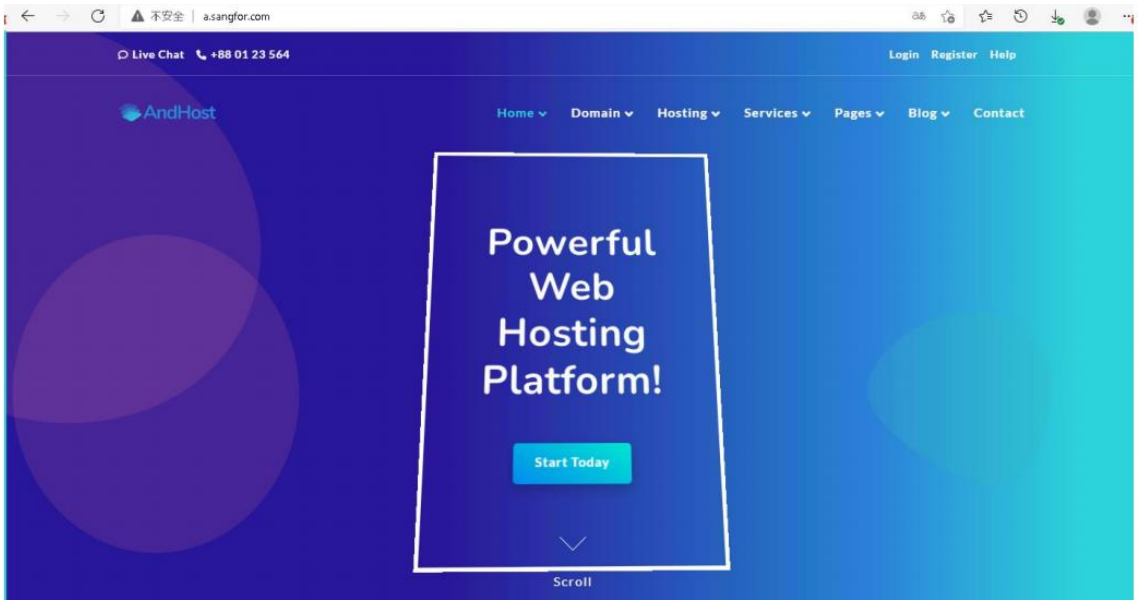
目的网段：0.0.0.0/0　　下一跳类型：实例　　ECS 实例：防火墙实例

注意：阿里云路由表分区域解耦，请添加路由时请选择关联业务系统所子网的路由表



5.1.4.效果展示：

使用防火墙公网 IP 访问业务系统：



服务器访问公网正常：

```
[root@ecs-01587956 ~]# wget www.baidu.com
--2021-11-17 16:31:59--  http://www.baidu.com/
Resolving www.baidu.com (www.baidu.com)... 39.156.66.14, 39.156.66.18
Connecting to www.baidu.com (www.baidu.com)|39.156.66.14|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2381 (2.3K) [text/html]
Saving to: 'index.html.1'

100%[======================================================================================>] 2,381       --.-K/s   in 0s

2021-11-17 16:31:59 (251 MB/s) - 'index.html.1' saved [2381/2381]

[root@ecs-01587956 ~]# ping www.qq.com
PING ins-r23tsuuf.ias.tencent-cloud.net (111.30.185.195) 56(84) bytes of data.
64 bytes from localhost (111.30.185.195): icmp_seq=1 ttl=47 time=9.72 ms
64 bytes from localhost (111.30.185.195): icmp_seq=2 ttl=47 time=8.70 ms
64 bytes from localhost (111.30.185.195): icmp_seq=3 ttl=47 time=8.61 ms
64 bytes from localhost (111.30.185.195): icmp_seq=4 ttl=47 time=8.60 ms
^C
--- ins-r23tsuuf.ias.tencent-cloud.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.604/8.911/9.726/0.485 ms
[root@ecs-01587956 ~]#
```

第 6 章　注意事项

① vAF8095 默认未授权，无法登录 webui 控制台，请授权后登录或切换离线授权登录。

② 授权过期 30 天内可以继续使用基础功能/安全功能，过期超过 30 天设备将处于 bypass 状态(安全功能失效)。授权中断/删除效果与过期超 30 天一致。

③ 使用多云安全平台授权时需要安全中心公网 IP：121.46.6.201 允许访问防火墙 WEBUI 端口和 7443 端口

④ 使用云图离线方式激活时需要触发离线授权条件或者设备后台创建标志文件

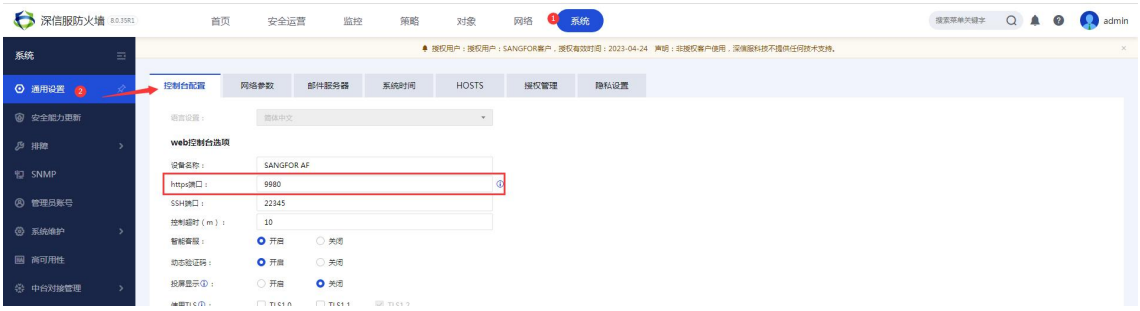
【后台创建文件可联系深信服技术支持协助（vAF 切换离线授权）】

⑤ 配置 vAF 之前需要先激活授权

⑥ 针对 https 的网站防护需要做 SSL 解密，需要将证书上传到 vAF 上

⑦ 使用多云安全平台授权时针对业务系统网站端口为 443 的需要提前修改下一代防火墙 WEB 管理端口为其他端口：

可在【系统】-【通用配置】-【控制台配置】中修改 https 端口



注意：下一代防火墙端口改变之后也需要在多云管理平台修改 vAF 端口（该端口用于下发授权）