阿里云 vNGAF4.0 版本配置指南

目录

一、用前必读

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

2、由于阿里平台限制了“经典网络”的 ECS 用于部署防火墙，所以用于装 vNGAF 的 ECS 必须采用“专有网络”类型（VPC 网络），新购买 ECS 用户手动配置选择“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。

3、我们对 vNGAF 的 ECS 硬件配置做了约定，分别为为以下几种组合，因此您在购买的时候需要注意配置。

2C2G：2 核 CPU+2G 内存

2C4G：2 核 CPU+4G 内存

4C4G：4 核 CPU+4G 内存

4C8G：4 核 CPU+8G 内存

您在选购 vNGAF 的 ECS 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 配置是否符合以上几种条件。

4、当前我们的 vNGAF 还不支持数据盘扩展，请您在选购 vNGAF 的 ECS 时不要附加选购数据盘。

二、网络场景

2.1 场景描述

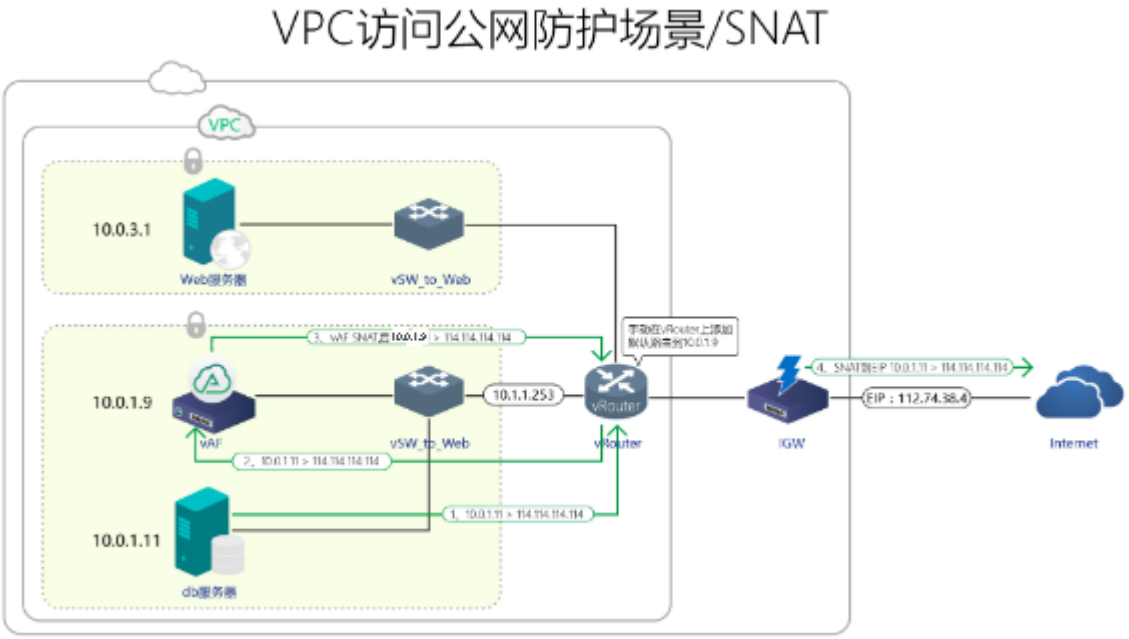
目前 vNGAF 支持两种场景：

SNAT 场景：VPC 私网子网中的实例通过 vNGAF 实现源地址转换访问互联网。

DNAT 场景：VPC 私网子网中的实例通过 vNGAF 实现端口映射为互联网提供服务。

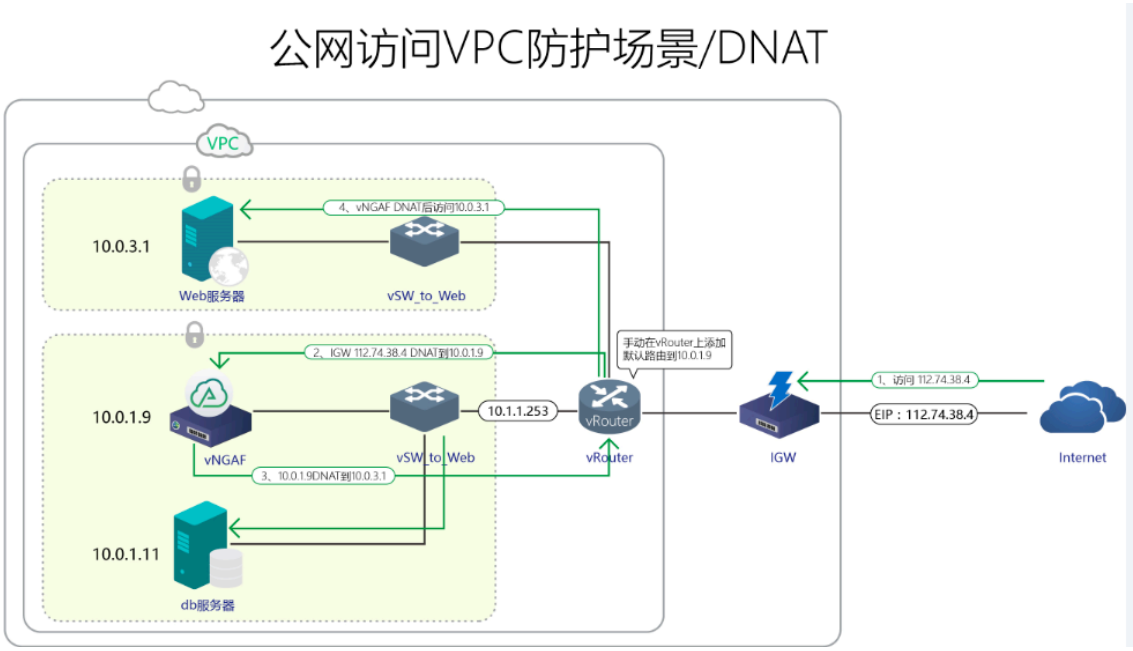
2.2 SNAT 场景

下图为 db 服务器通过 vNGAF 访问 intetnet 场景的数据流图。



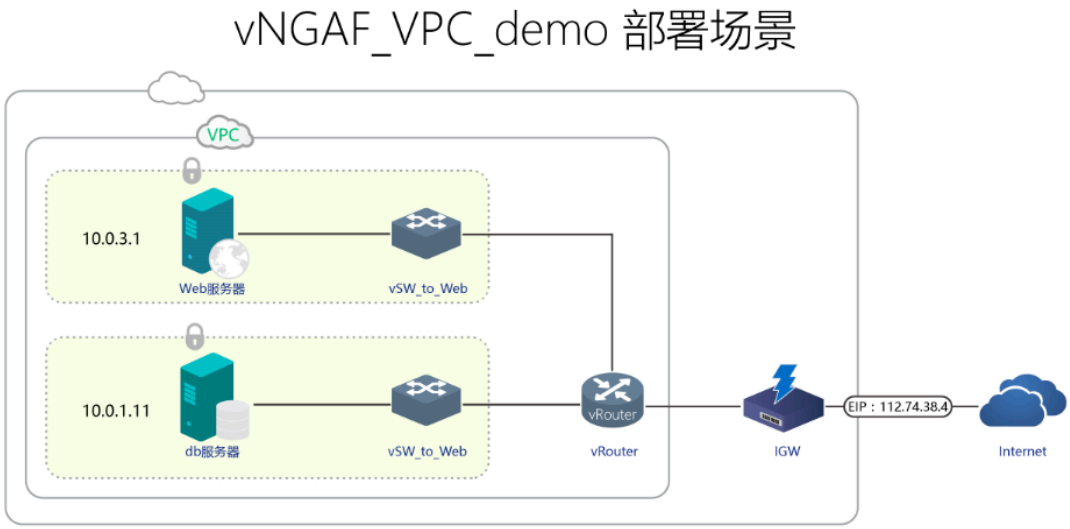
2.3 DNAT 场景

下图为 web 服务器通过 vNGAF 进行端口映射发布业务的数据流图。



三、环境搭建

本文使用如下 VPC 网络来进行环境配置演示。
创建一个 vNGAF_VPC_demo 网络
划分了两个子网： 10.0.3.0 和 10.0.1.0
每个子网部署一台 web 服务器(10.0.3.1)和 db 服务器(10.0.1.11)。



3.1、获得 vNGAF 的 ECS

因为深信服虚拟化下一代防火墙 vNGAF 需要部署在阿里云的 ECS 实例上进行使用，所以您首先需要为 vNGAF 购买 ECS，这里简单介绍一下 ECS 的购买方法。阿里云提供两个入口（管理控制台和阿里云市场）来购买 vNGAF 的 ECS。

3.1.1 入口一：从管理控制台购买

Step1 选择 vNGAF 放置的子网。

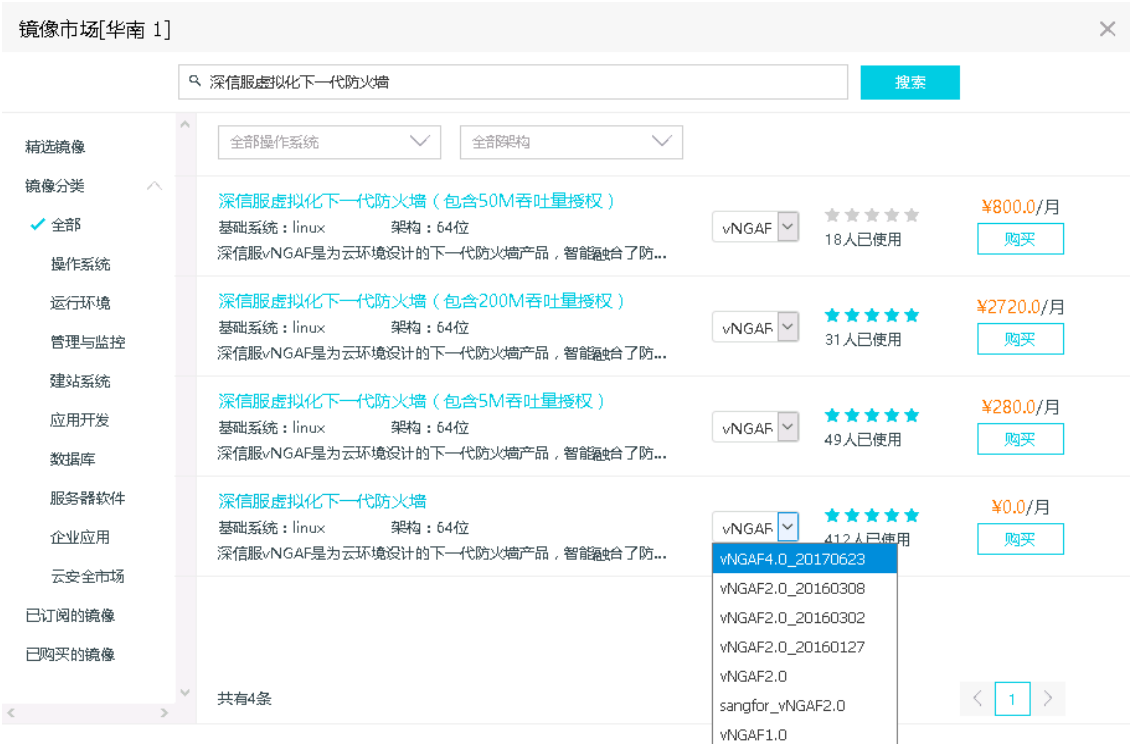
进入到管理控制台，选择 vNGAF 放置的子网，vNGAF 可以放置在 VPC 网络中的任意虚拟交换机（也可以单独放置在一个交换机）上，对该 VPC 的所有流量进行安全防护。这里连接在“vpc_94694c02g”上。点击“创建 ECS”进入到购买页面。

Step2 选择 ECS 配置

用户按需选择配置 ECS 配置，但需要注意图中几点。


计费方式
包年包月
按量付费
首先需要选择您的 VPC 网络所在的可用区
地域
华北 1
华北 2
华北 3
华东 1
华东 2
华南 1
华南 1 可用区 A
香港
亚太东南 1 (新加坡)
美国西部 1 (硅谷)
美国东部 1 (弗吉尼亚)
亚太东北 1 (东京)
欧洲中部 1 (法兰克福)
中东东部 1 (迪拜)
亚太东南 2 (悉尼)
随机分配
不同地域的实例之间内网互不相通；选择靠近您客户的地域，可降低网络时延、提高您客户的访问速度，教我选择>>
网络
经典网络
专有网络
这里必须要选择专有网络
经典网络与专有网络不能互通，购买后不能更换网络类型，请谨慎选择
[默认]vpc-94694c02g
[默认]vsw-949ltp8m0
可用私有 IP 4091 个
如需使用其他专有网络，请选择已有专有网络，也可以自行到 控制台创建>>
当前虚拟交换机所在可用区为：华南 1 可用区 A
公网 IP 地址：
分配
分配的公网IP地址不能跟ECS实例解除绑定关系，如需更加灵活的静态公网IP方案，建议选择 "不分配" 公网IP地址，配置并 绑定弹性公网 IP 地址>>
安全组：sg-wz94gqh3l7rr6v6tfy5e / sg-wz94gqh3l7rr6v6tfy5e (已有0个实例 还可以加入1000个实例)
请确保此安全组开放包含 22 (Linux) 或者 3389 (Windows) 端口，否则无法远程登录ECS。您可以进入 ECS控制台 设置。
重新选择安全组
安全组类似防火墙功能，用于设置网络访问控制，您也可以到管理控制台 新建安全组>> 教我选择>>
实例
系列 II
系列 III
I/O 优化实例
系列之间不能互相升降配
vNGAF 支持 1C2G，2C4G，及更高 ECS 配置
共享计算型 n1
共享通用型 n2
共享内存型 e2
计算型(原独享) sn1
通用型(原独享) sn2
1 核 1GB
ecs.n1.tiny
1 核 2GB
ecs.n1.small
2 核 4GB
ecs.n1.medium
4 核 8GB
ecs.n1.large
8 核 16GB
ecs.n1.xlarge
16 核 32GB
ecs.n1.3xlarge
32 核 64GB
ecs.n1.7xlarge

Step3 从“镜像市场”选择镜像(vNGAF4.0*)。

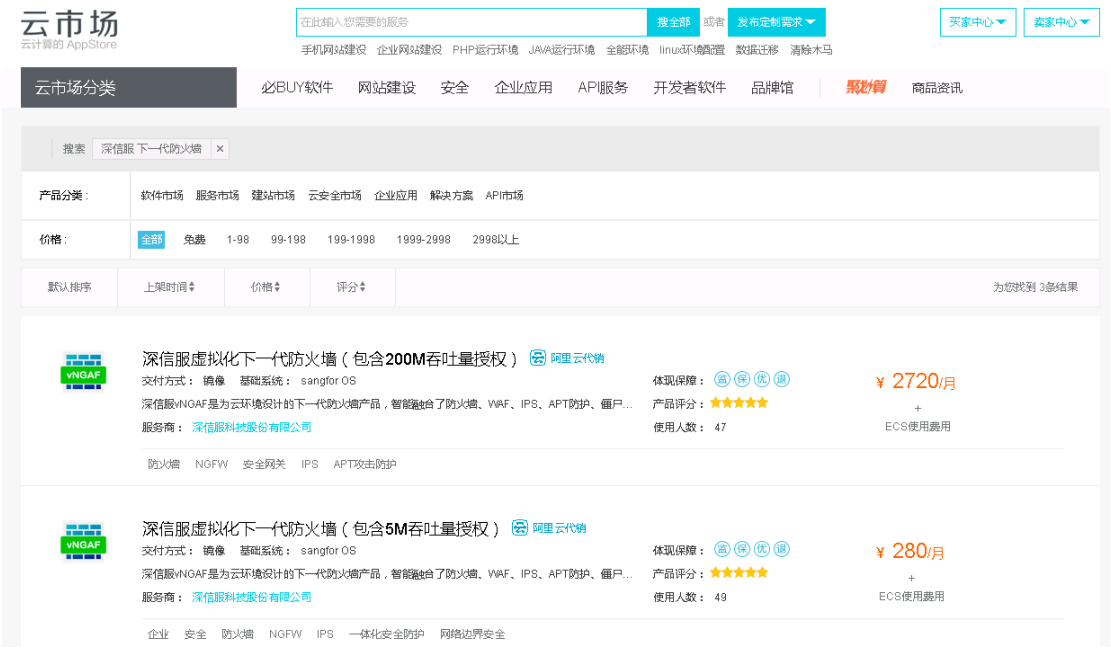


Step4 选好镜像后，付款即成功购买。

3.1.2 入口二：从阿里云市场购买

Step 1：搜索“防火墙”。

从阿里云市场搜索“深信服虚拟化下一代防火墙”，点击进入购买界面。



Step2 进入“购买页面”

Step3 进行 ECS 配置选择

此处必须要进行自选 ECS 配置，默认配置会导致 vNGAF 无法工作。这是由于阿里的平台分为经典网络和专用网络，而默认选择的是经典网络，目前经典网络还无法支持 vNGAF。

在这一步选择支持“专有网络”的可用区，并且选择 ECS 的 cpu 和内存配置必需符合 1.2 中的要求（满足 2C2G，2C4G，4C4G，4C8G 其中之一）。 这里选择的是“2C4G”。

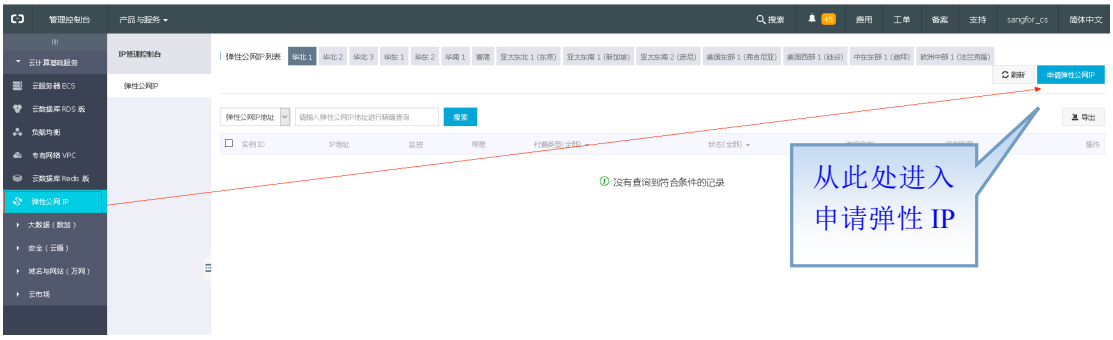
这一步还需要关联用户的 VPC 网络，选择实例放置的位置。这里选择的是之前创建好的 vpc 专用网络，放到“vpc_94694c02g”虚拟交换机所在子网。

Step4 关联好网络类型后，付款即成功购买。

3.2、设置 vNGAF 弹性 IP

已经弹性 IP 的用户请路过 3.2.1、3.2.2 章节，直接从 3.2.3 开始阅读。

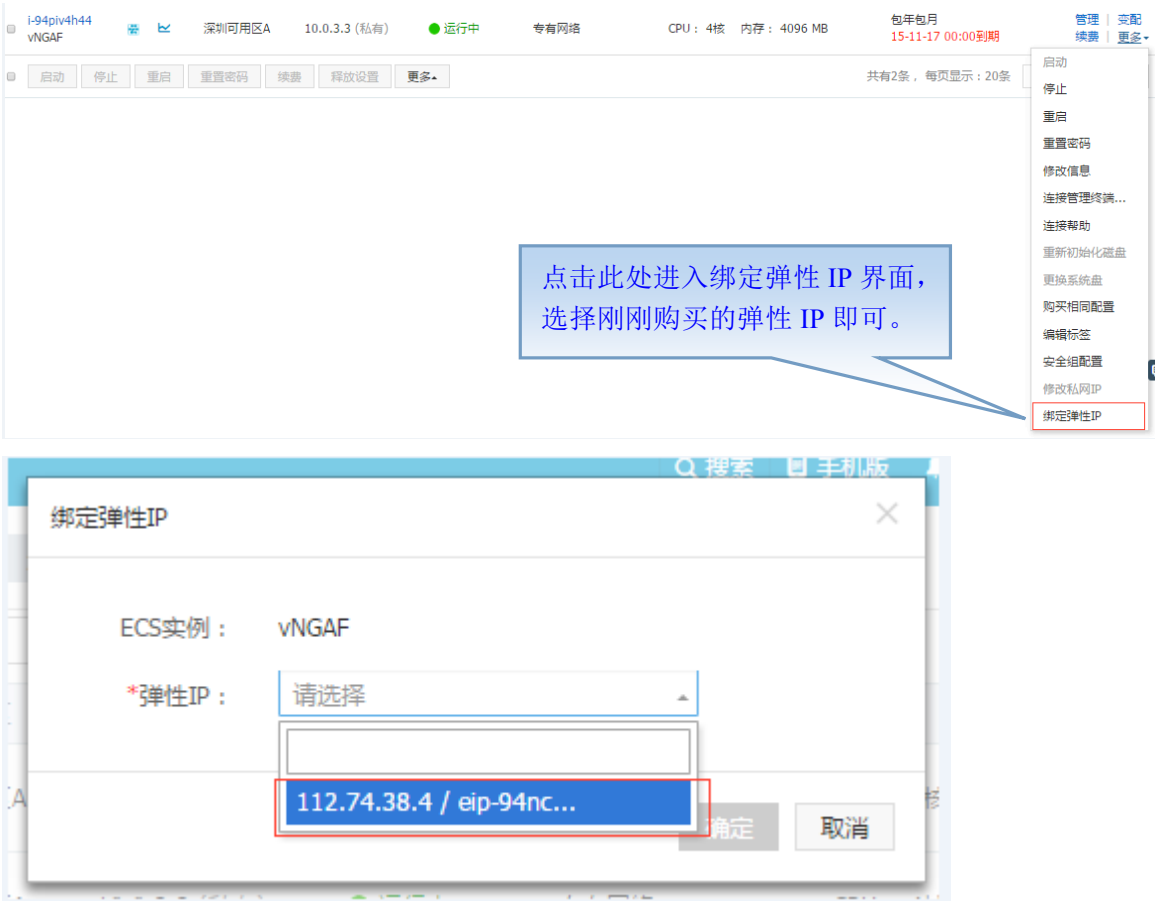
3.2.1 申请弹性 IP



3.2.2 购买弹性 IP

用户按需要选择购买弹性 IP 的方式

3.2.3 绑定弹性 ip

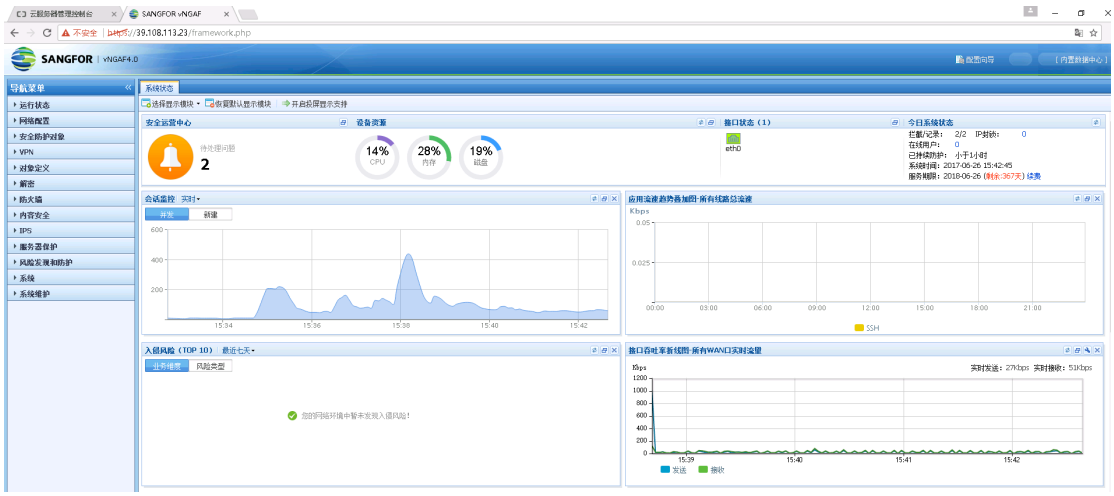


3.2.4 弹性 IP 登录

弹性 IP 绑定成功后，便可以使用 IP112.74.38.4 登录我们首页了。
在 VPC 网络中使用 https://私有 IP　也可以登录我们的防火墙

3.2.5 登录成功首页

使用正确的用户名和密码登录成功后，便可以看到 vNGAF 的系统状态首页了。

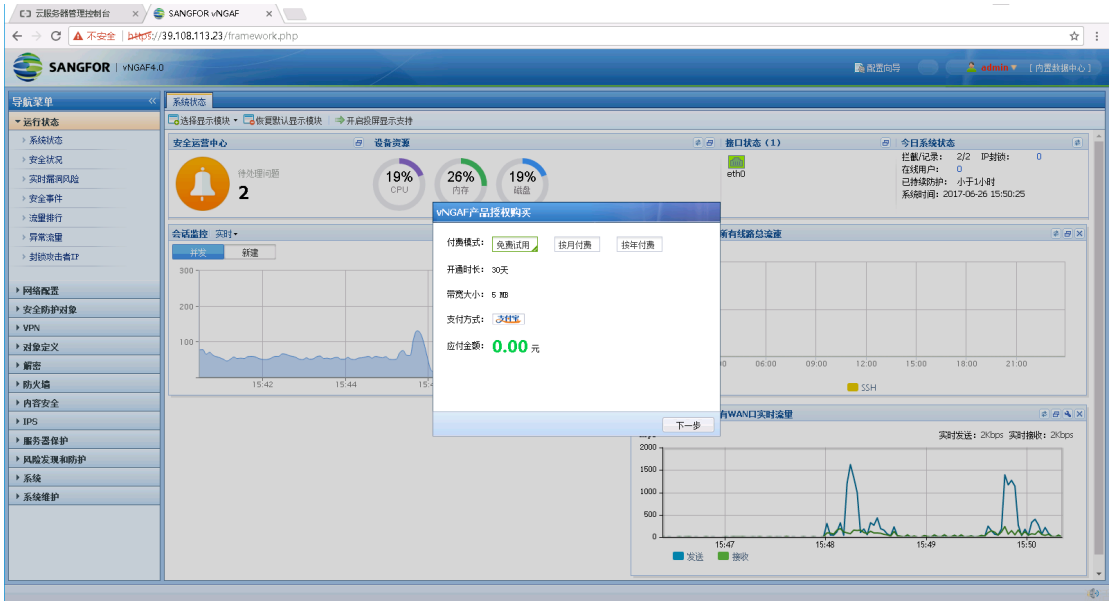


3.4 vNGAF 产品授权购买

购买 vNAGF 产品授权，需要通过支付宝完成支付，其中支付宝使用的 SSL 数字证书的签名算法是 SHA256，IE6、IE7 和部分 IE8 不支持该算法。因此，购买 vNGAF 产品授权时，请使用谷歌、火狐和 IE9 以上（包括 IE9）浏览器。
通过配置的公有 IP 可以登录 vNGAF 的控制台。
用户名：admin, 初始密码为：admin；

3.4.1 vNGAF 产品授权方式

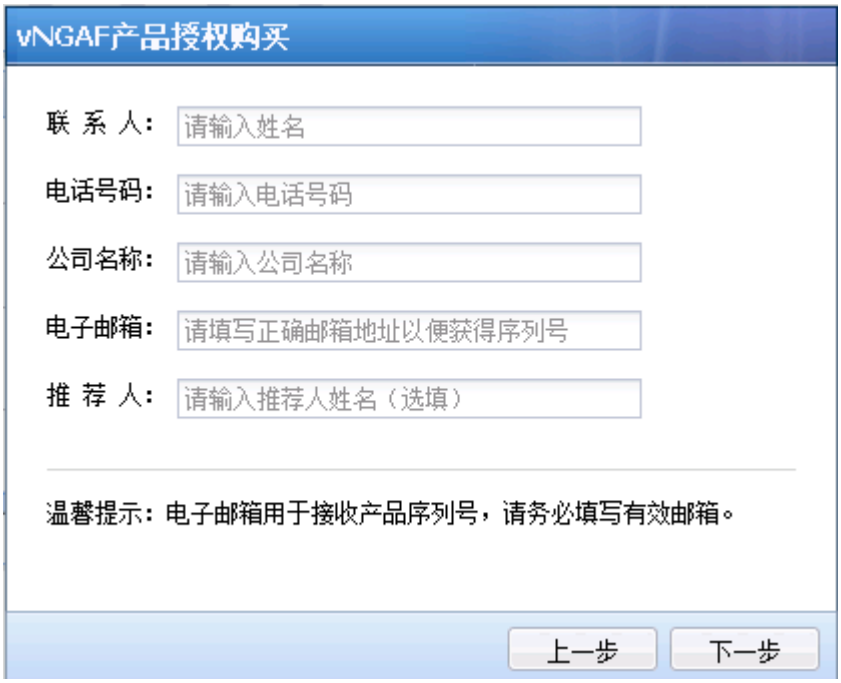
vNGAF 目前有三种付费模式：
（1）免费试用：开通时长为 30 天，宽带大小为 5M，应付金额为 0.00 元；
（2）按月付费：
（3）按年付费：
这两种是有偿的付费模式，根据选择开通时长和宽带大小收费；



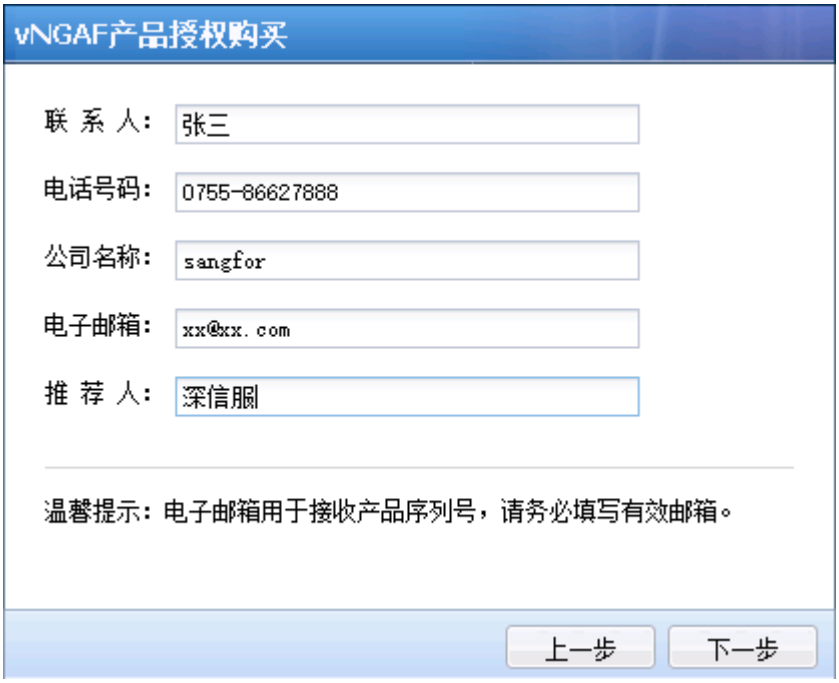
3.4.2 免费试用方式

选择免费试用模式【免费使用】
开通时长为 30 天，宽带大小为 5M，应付金额为 0.00 元

根据提示填写您的信息，其中电子邮箱用于接收产品序列号，请务必填写有效邮箱。



以下是样例：



确认信息后，请点击【提交订单】

至此，您已经成功获得 vNGAF 免费授权，免费试用时长为 30 天，宽带大小为 5M。
现在点击【开始使用】，您的 vNGAF 已经可以正常使用。

3.4.3 付费使用方式

如果您需要延长您的开通时长，有以下两种方式供您参考。

(1)您还不是 vNGAF 免费试用客户，可以直接购买序列号授权；
　如下图，您可以选择【按月付费】和【按年付费】

确认信息无误后，【提交订单】

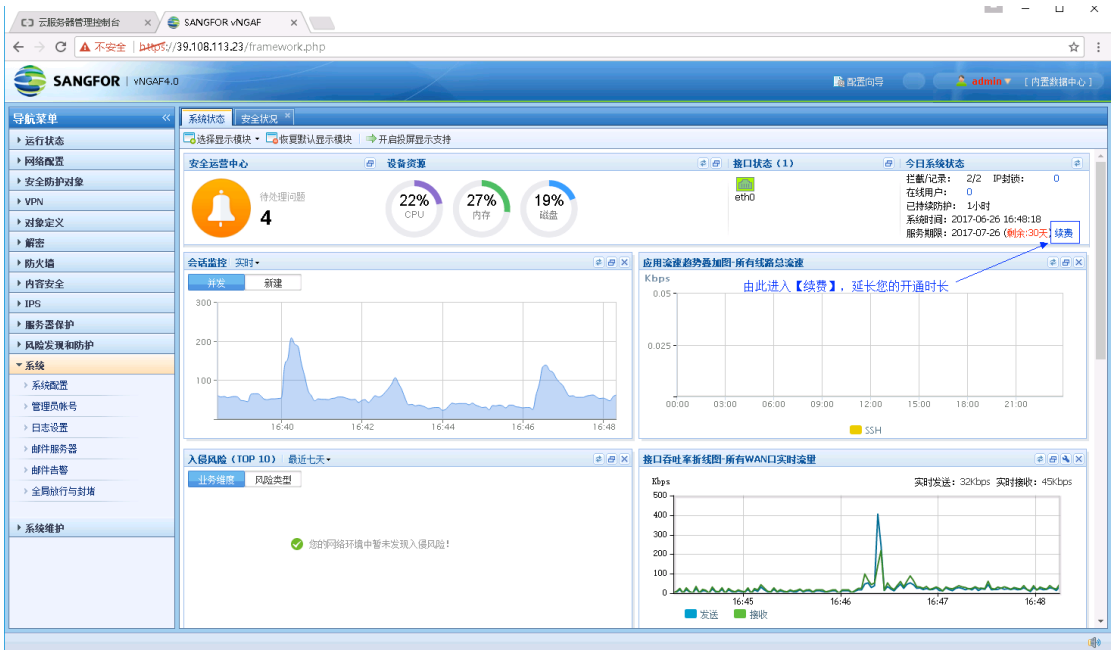
在【支付宝】支付成功后，服务器返回您购买的序列号，如下图：

【点击复制序列号】，粘贴到 vNGAF 的序列号输入框，如下图；
由于浏览器设置问题，可能会复制不成功，请再次【点击复制序列号】，或者选中上图中产品序列号，右键复制。

如果没有找到如上图的序列号输入框，您可以在【系统—>系统设置—>序列号】输入序列号，如下图：

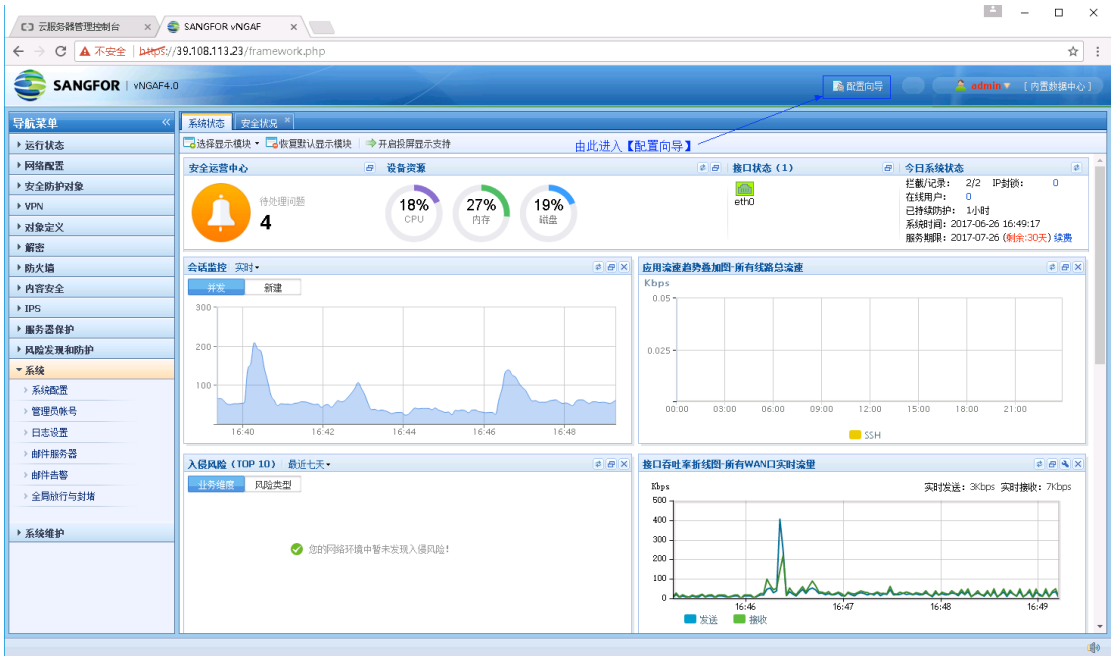
(2)您已经是 vNGAF 免费使用客户；

登录 vNGAF 后，您可以在【系统状态】中找到【续费】按钮，如下图：



3.5 配置向导

如下图，登录 vNGAF 后，从右上角进入【配置向导】
配置向导可以快速便捷对外发布私网中的云服务器。
目前只支持快速配置单个云服务器，需要发布多个不同云服务器，请移步到 3.6 至 3.9 节。



【配置向导】有两种部署场景：

DNAT 场景

私网中的云服务器通过端口映射为互联网提供服务

SNAT 场景

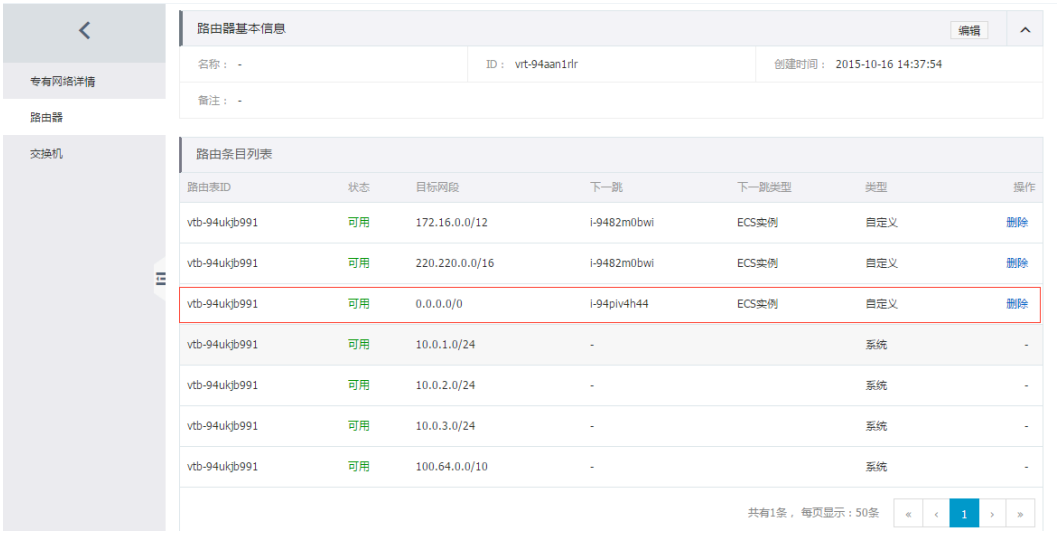
私网中的云服务器通过源地址转换访问互联网


配置向导
1.场景选择
2.实例配置
3.访问控制
4.防护配置
5.完成配置
DNAT场景
未配置
私网中的云服务器通过端口映射为互联网提供服务
SNAT场景
未配置
私网中的云服务器通过源地址转换访问互联网
下一步

3.6 添加默认路由

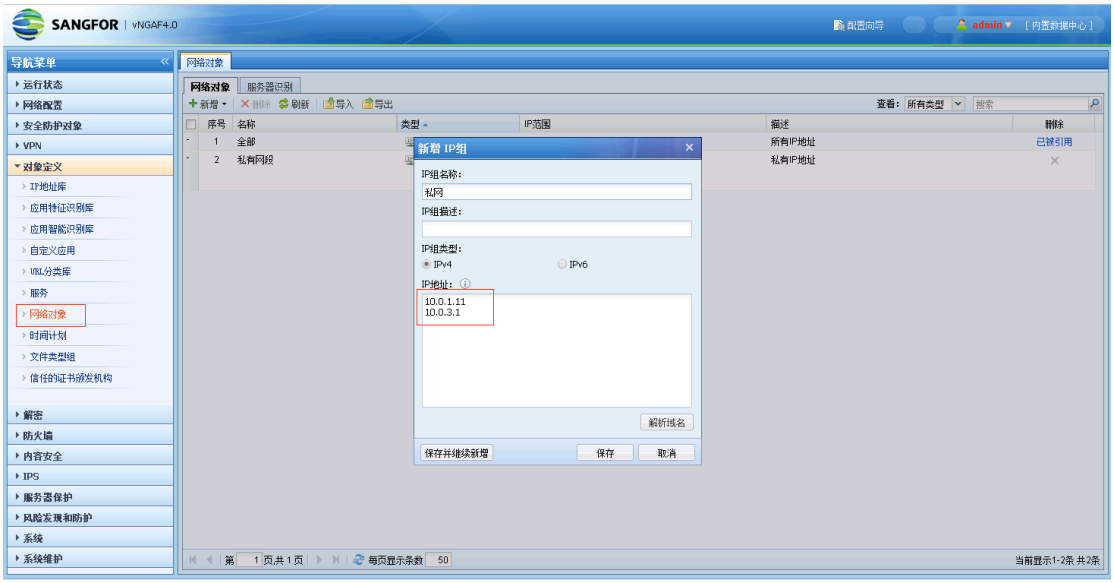
在 VPC 的路由器中添加默认路由指向 vNGAF 的 ECS 实例，目的在于把 VPC 网络的流量引流到 vNGAF。

注意：需要 vNGAF 防护的 ECS 实例，不可以绑定弹性 IP。



3.7 建立私网 IP 组

建立 IP 组对象：建一个“私网”IP 组，加入两台服务器的 ip。



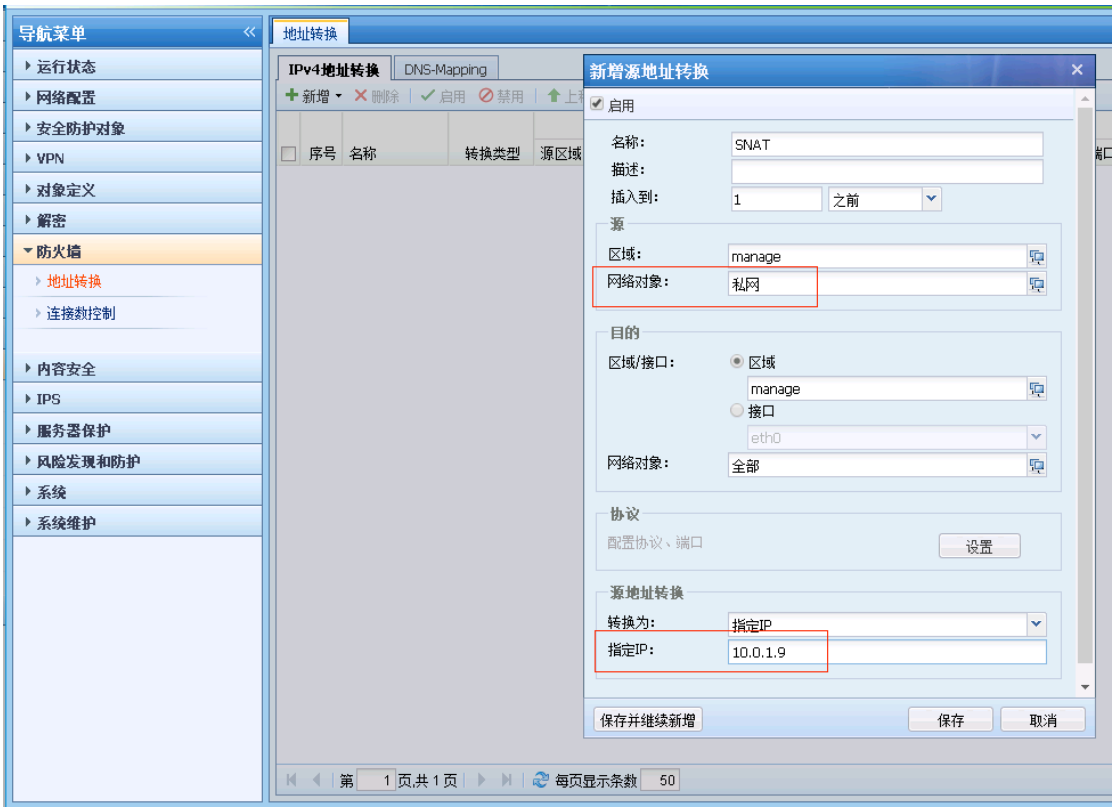
3.8 配置 SNAT 策略

源地址转换 SNAT：私网客户端可访问公网服务

源区域 ： manage

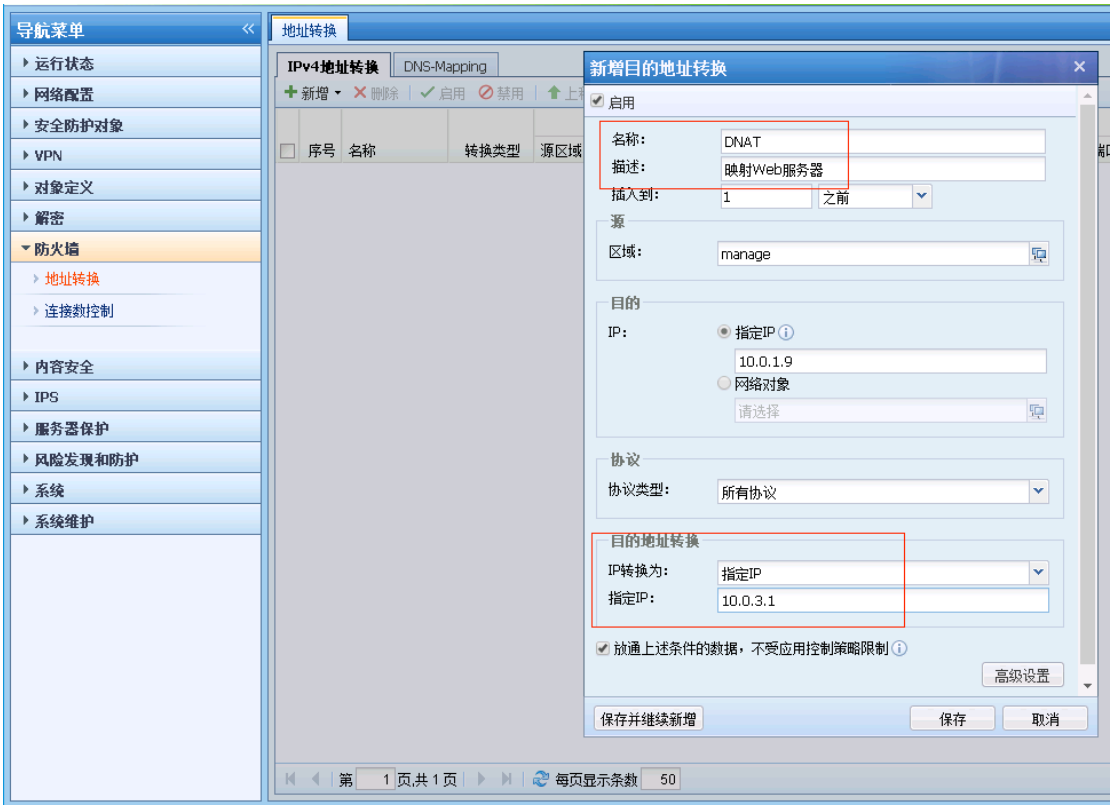
源 IP 组 ： 私网

目的区域　　：manage
目的 IP 组　：全部
协议　　：所有
源地址转换　：指定 IP 10.0.1.9　　(eth0 接口 IP)



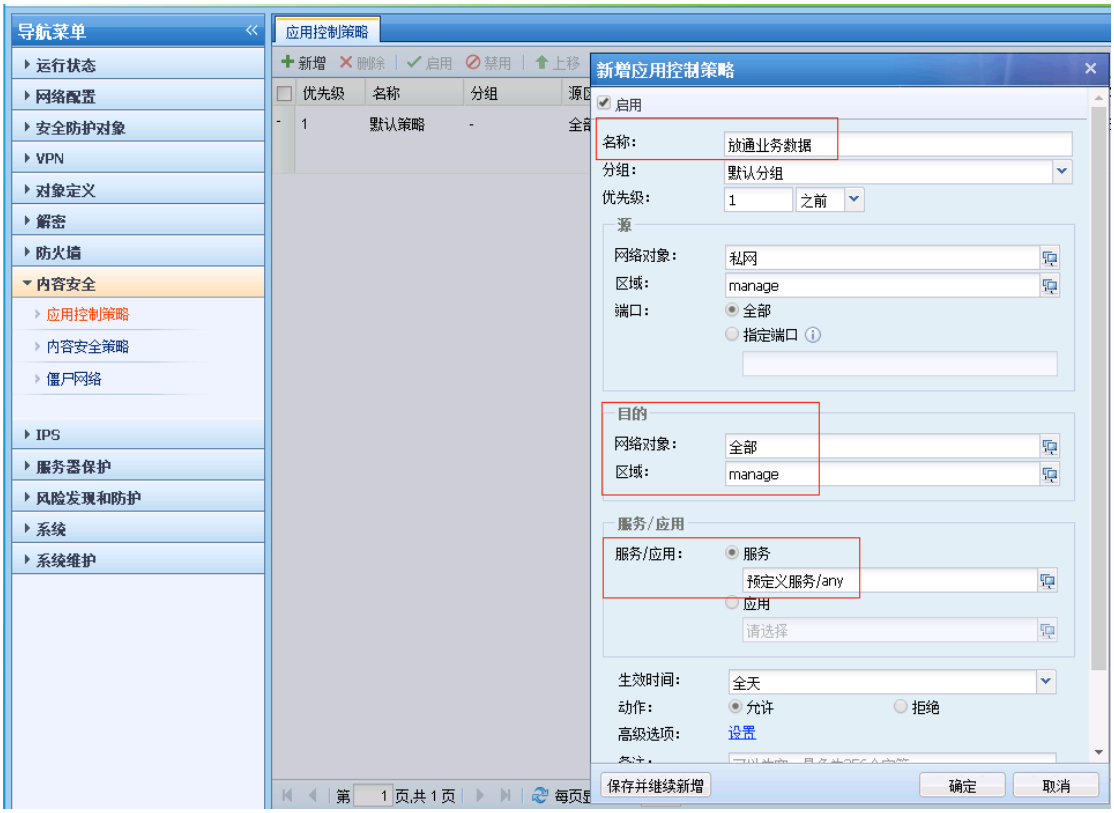
3.9 配置 DNAT 策略

目的地址转换 DNAT：公网客户端可通过 EIP 访问私网服务,如开放的 80 端口 web 服务
源区域　　：manage
目的 IP　　：指定 IP 10.0.1.9　　#　(eth0 接口 IP)
协议类型　　：所有协议（或者可以指定 TCP 协议类型，端口：80）
目的地址转换：指定 IP 10.0.3.1　　#　(需要映射提供访问服务的私网服务器 IP)



3.10 配置应用控制策略

配完 NAT 策略后网络配置已经完成，但由于 vNGAF 默认是阻拦所有数据包的，我们需要配置策略将客户需要的业务数据放通，这里放通 SNAT 场景（私网→公网）数据访问（用户可以根据自己的需要放通相应的业务）。



以上步骤完成后，基本网络配置完成，其它功能策略，客户按需配置

四、注意事项

1.在阿里控制台修改 vAF 私网 IP，当 vAF 恢复默认配置时，密码恢复为 admin。
2.在阿里控制台重置 vAF 密码，当 vAF 恢复默认配置时，密码恢复为阿里控制台所设密码。
3.由于支付宝用的 SSL 数字证书的签名算法是 SHA256，目前确定 IE6、IE7 和部分 IE8 不支持。
4.阿里云平台变换 ECS 配置后，请重启 vNGAF 使其生效。
5.序列号快过期时候，有邮件提醒，请务必填写正确的邮箱地址。
6.目前不支持外接数据盘。