SANGFOR_vAF8032R1R1_部署实施指导 for 阿里云

深信服智安全
SANGFOR SECURITY

2021 年 1 月

■ **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	20210123			

目录

产品简介

深信服 vAF8032R1R1 以软件镜像文件的形式安装部署在阿里公有云平台上，需要先购买阿里云 ECS 云服务器来安装搭建 vAF，并同时购买 vAF 授权序列号来组合使用。

vAF8032R1R1 版本是在 AF8032 版本基础上支持在阿里云、腾讯云、华为云等公有云环境部署。AF8032R1 版本优化内容：

1、授权优化：

支持 VLS 和离线授权两种授权方式

支持灵活授权（只能在 VLS 服务器后台灵活授权）

解决授权 500M 问题

2、CSSP 对接需求：CSSP 单点登录，支持多 greep ip

3、公有云需求

网关 ID 由一张网卡生成

Eth0 口 dhcp/static 切换

支持磁盘动态扩容（只能在原有系统盘基础上扩容）

支持解密、高级配置（双因素）、EDR 联动

4、各公有云平台驱动适配

5、修复已知问题：解决已知安全问题与严重问题

目前公有云部署 vAF8032R1R1 版本与硬件防火墙 AF8032 版本，在功能上主要差异：不支持短信猫告警功能、光口 bypass 功能、恢复默认配等功能，其余功能与物理设备正式版本保持一致。

部署环境要求

1. vAF8032R1 虚拟机只能部署在阿里云 VPC 专有网络，不支持部署在经典网络（即云业务虚拟机和 vAF8032R1 虚拟机必须在同一个地域同一个 VPC 专有网络名称里面）

2. vAF8032R1 虚拟机部署在 VPC 专有网络中是作为一台虚拟的防火墙设备使用，是作为VPC专有网络中的逻辑上的出口设备，数据必须经过vAF8032R1虚拟机才可以做安全防护；

并且 VPC 内需要被安全防护的应用服务器不能绑定公网 IP，并且用来安装 vAF8032R1 的虚拟机必须是空闲的，不能有安装其他的业务服务

3. 如果 VPC 专有网络中没有使用其他 NAT 网关设备或阿里云 slb 负载设备做出口，vAF8032R1 虚拟机作为唯一的出口设备需要绑定弹性公网 IP（即 EIP）。如果客户的 VPC 专有网络中已经使用了其他 NAT 网关设备或阿里云 slb 负载设备，还需要同时部署 vAF 防火墙，请根据 VPC 专有网络环境拓扑提前做好网络设计规划

4. 部署 vAF8032R1 服务器必须准备另外一台虚拟机搭建 vls 授权服务器，用来授权序列号使用，vAF8032R1 需要和 vls 授权服务器可以相互通信，vls 授权服务器的搭建请参考 vls 部署手册

5. 阿里云镜像市场目前还没有 vAF8032R1 的镜像文件，需要通过上传或共享的方式将镜像上传到阿里云平台上使用，具体操作见镜像上传，共享操作文档

6. vAF8032R1 虚拟机推荐配置请参考如下截图：

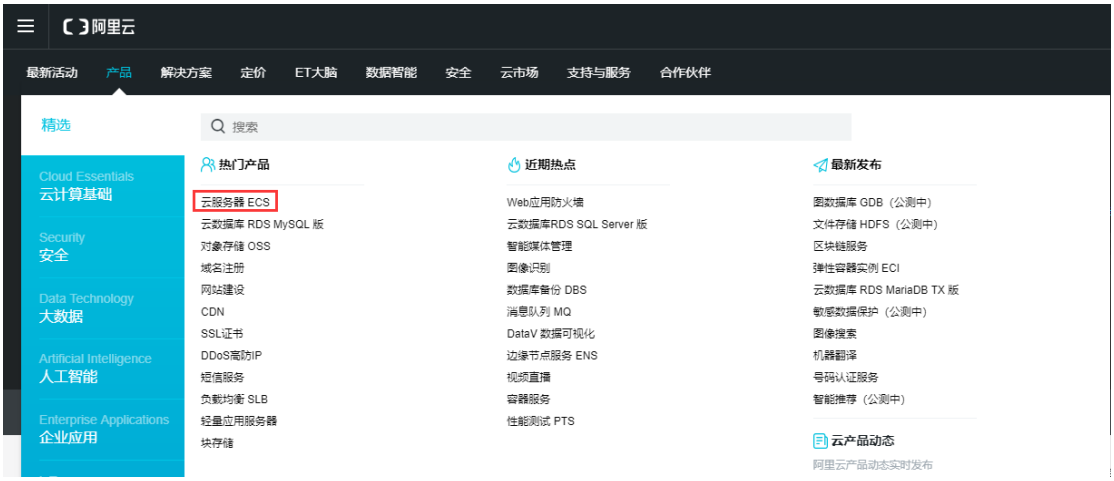
系统磁盘默认 80G（客户根据需求扩容），不需要数据盘，虚拟机机型无要求建议选择适合搭建服务器的机型

vAF 防火墙授权序列号规格	虚拟机推荐规格
5M 吞吐量序列号	2 核，4G，80G
10M 吞吐量序列号	2 核，4G，80G
50M 吞吐量序列号	2 核，4G，80G
100M 吞吐量序列号	2 核，4G，80G
200M 吞吐量序列号	2 核，4G，80G
400M 吞吐量序列号	4 核，8G，128G
800M 吞吐量序列号	8 核，16G，256G
1.6G 吞吐量序列号	8 核，16G，256G

部署实施

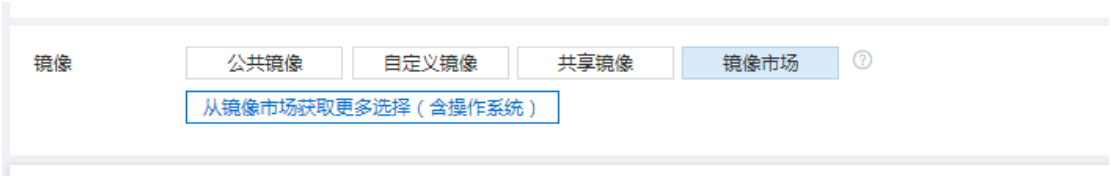
3.1 购买云服务器

登录阿里云中国站 www.aliyun.com，点击购买云服务器

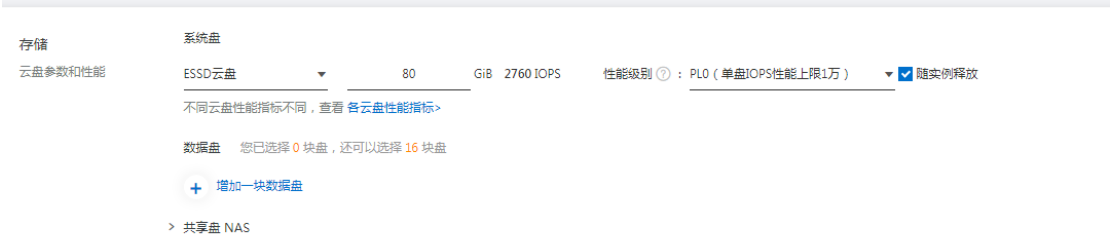


出现以下选择页面，参考上述章节中的选型要求，按照实际需求选择对应的服务器，例如选择 2 核 CPU、4G 内存的云服务器。注意“地域”一定要选择和云业务服务器在同一个地域

镜像在“自定义镜像”中选择已上传或其他账号共享到云平台的 vAF8032R1 的镜像即可



存储选择按照需求选择高效云盘或者 SSD 云盘，存储选择默认值 80G 即可，不需要选择额外的数据盘。



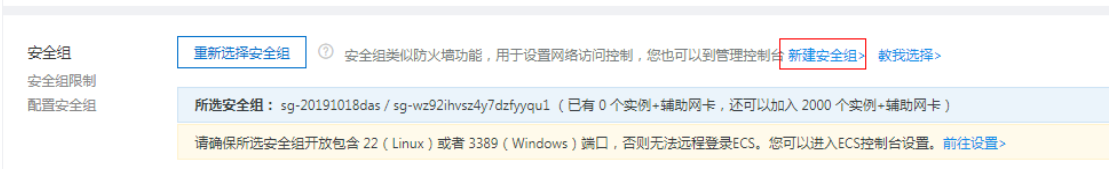
3.2 配置网络和安全组

网络选择专有网络，一定要选择云业务服务器所在的 VPC 专有网络名称；

公网带宽根据实际情况选择；

安全组默认情况入方向都是拦截，出方向都是放行的，若入方向未添加规则放通则会导致创建好云主机后从公网无法访问的情况。所以需要在安全组入方向放通 TCP443 端口（控制台管理）

点击 新建安全组 跳转到新窗口设置安全组；



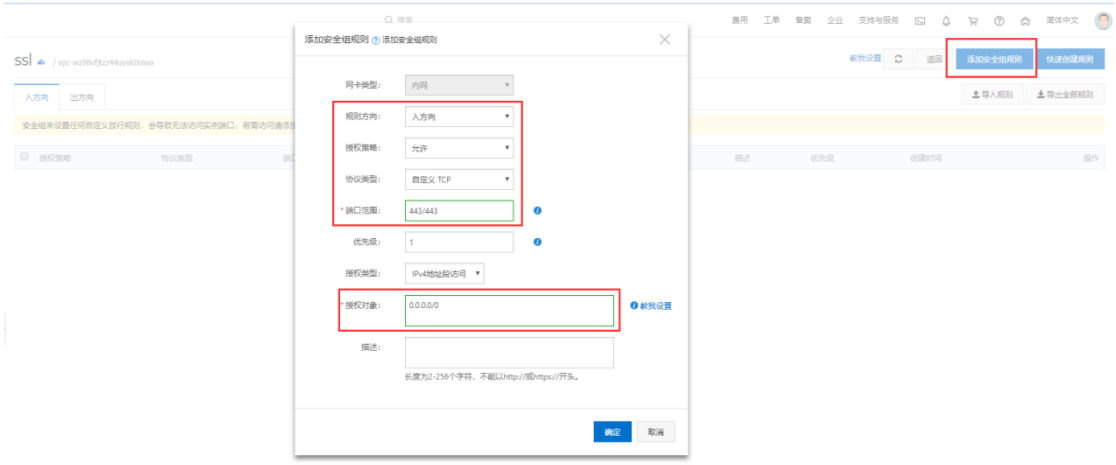
在新弹出的网页中点击 创建安全组 按钮；

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 TCP443、TCP51111 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。

最后确认订单支付即可完成 vAF8032R1 云主机的创建。

3.3 设备登录

因为 vAF8032R1 是支持 DHCP 功能的，所以无需进后台配置 IP 地址和默认路由，既云主机购买部署成功后，便可以使用 IE 浏览器打开如下 vAF8032R1 的控制台，地址：https://IP，默认用户名和密码为：admin/admin。vAF8032R1 管理登录界面如下所示：

在未授权情况下，输入用户名和密码无法登陆，显示如下：

设备授权

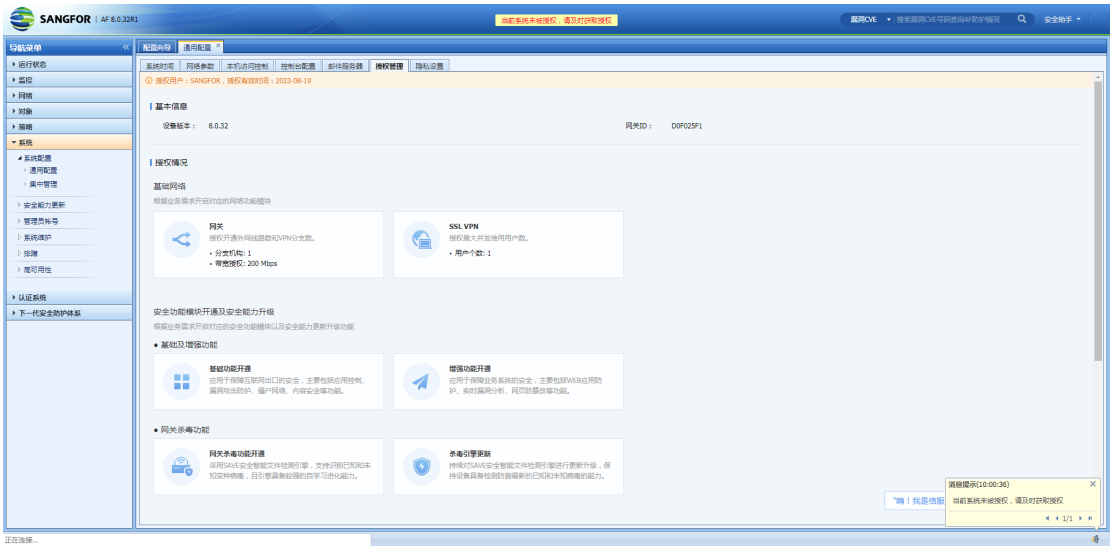
对 vAF8032R1 授权，有 VLS 授权与离线授权两种方法。

4.1 VLS 授权

对 vAF8032R1 授权，必须搭建 vls 授权服务器给 vAF8032R1 服务器授权序列号，vls 授权服务器的搭建请参考 vls 授权服务器部署手册，填写序列号到 vls 授权服务器，然后分配授权个数给 vAF8032R1 服务器

登陆 vls 授权服务器给 vAF8032R1 授权序列号：

分配授权个数给 vAF8032R1 后，登陆 vAF8032R1 的 web 管理页面查看序列号页面就显示序列号个数出来了，如下所示：



授权完成之后进入授权管理页面可看到如下显示，当前显示未被授权是正常现象，AF 已可用，等待最多半小时之后系统进入正常授权状态：

4.2 离线授权

同《深信服云图 XCentral 授权中心操作手册_V2.0.docx》中章节“2.2.2.2.AF 离线激活”中指导步骤授权。

请联系客服获取。

第 5 章　AF 安全功能配置

5.1 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　　：L3_manage

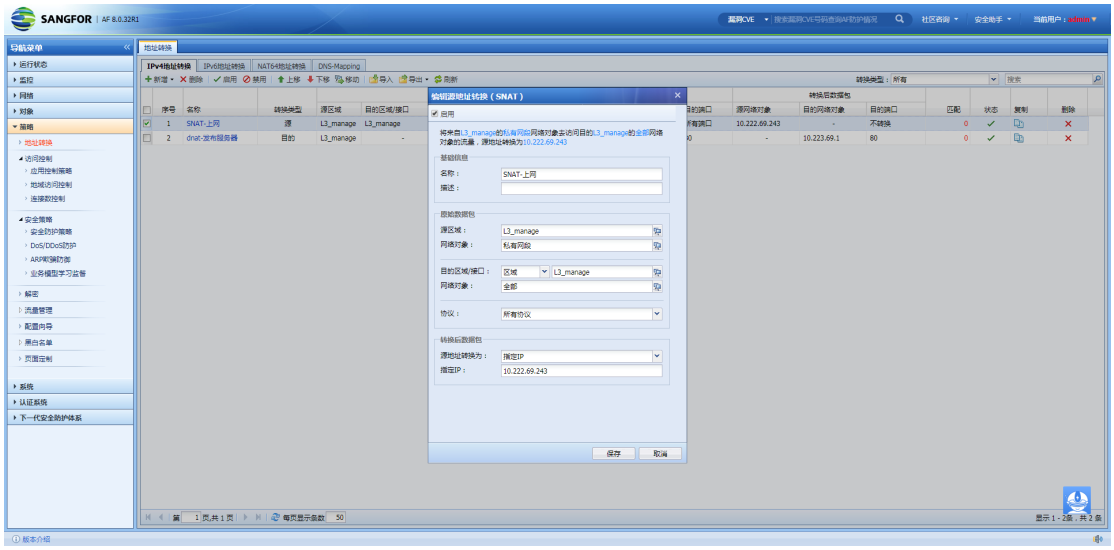
源 IP 组　　：私有网段

目的区域　　：L3_manage

目的 IP 组　：全部

协议　　：所有

源地址转换　：指定 IP 10.223.69.243　　(eth0 接口 IP)



5.2 配置 DNAT 策略

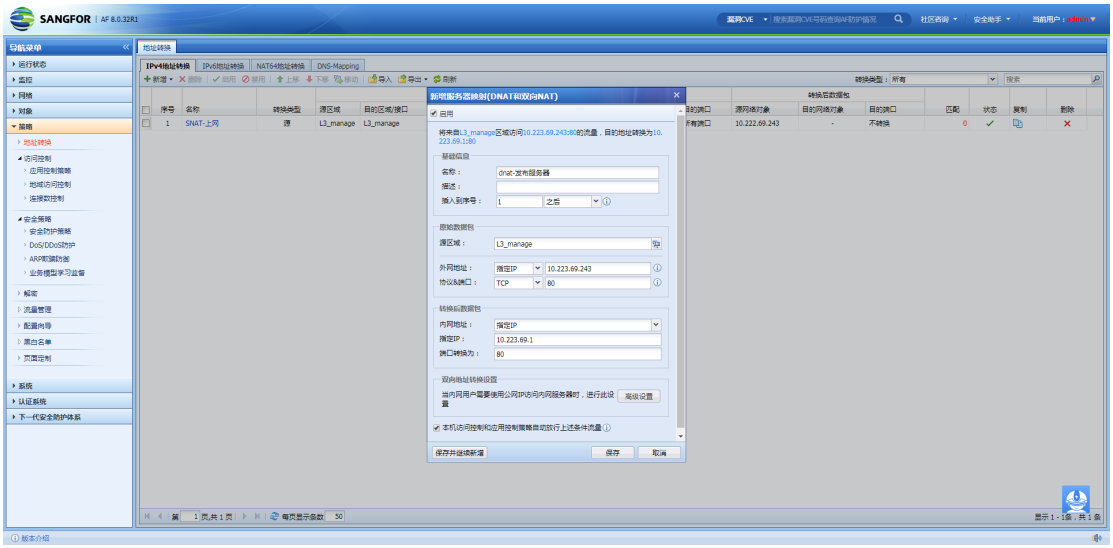
目的地址转换 DNAT：公网客户端可通过 EIP 访问私网服务,如开放的 80 端口 web 服务

源区域　　：L3_manage

目的 IP　　：指定 IP 10.223.69.243　　#　(eth0 接口 IP)

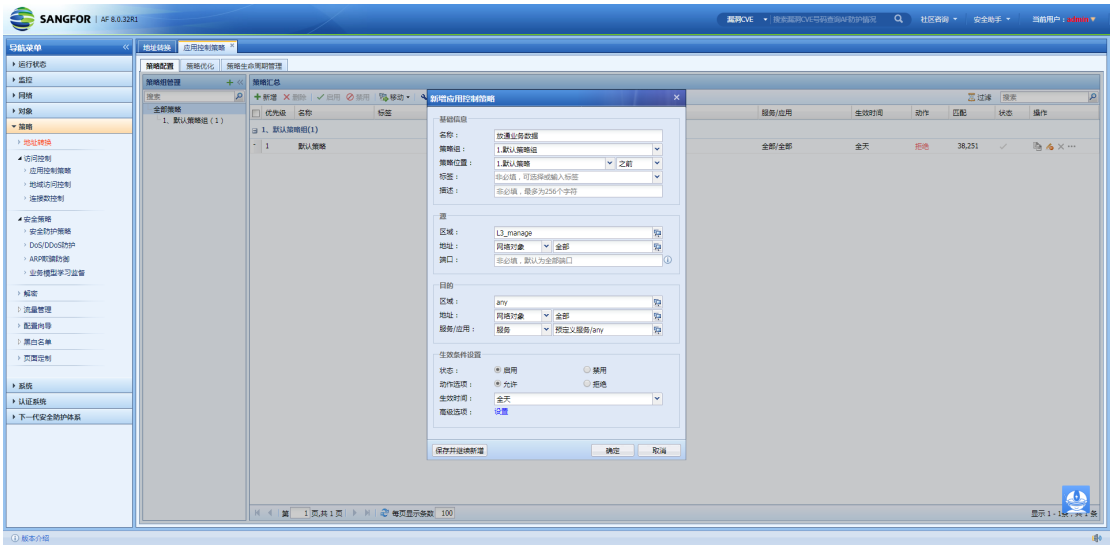
协议类型　　：所有协议（或者可以指定 TCP 协议类型，端口：80）

目的地址转换：指定 IP 10.223.69.1　　#　(需要映射提供访问服务的私网服务器 IP)



5.3 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 vAF 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

5.4 添加默认路由

在 VPC 专有网络的虚拟路由表中添加默认路由指向 vAF 的 ECS 实例，目的在于把 VPC 中内网服务器的的流量引流到 vAF。

注意：需要 vNGAF 防护的 ECS 实例，不可以绑定弹性 IP。

第 6 章　vAF 升级

vAF8032R1 暂时不支持升级到更高的软件版本。也不支持公有云低版本 vAF 升级到此版本。

第 7 章　常见问题

1. vAF8032R1 服务器和 vLS 授权的时候要满足什么条件？

答：vAF8032R1 需要和 vls 授权服务器相互通信，并且 vLS 授权服务器给 vAF8032R1 授权时必须联网上网（VLS 需要连通授权服务器 VLS.sangfor.com.cn 的 TCP443 端口）

2.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。