阿里云 vNGAF1.0 版本配置指南

目录

一、用前必读.....2
二、网络场景.....2
2.1 场景描述.....2
2.2 SNAT 场景.....2
2.3 DNAT 场景.....3
三、环境搭建.....3
3.1、获得 vNGAF 的 ECS.....4
3.1.1 入口一：从管理控制台购买.....4
3.1.2 入口二：从阿里云市场购买.....6
3.2、绑定弹性 ip.....8
3.2.1 vNGAF 绑定弹性 ip.....8
3.3、获得 vNGAF 授权.....8
3.3.1、获得 vNGAF 授权.....8
3.3.2、选择合适的付费方法。.....9
3.4、添加默认路由.....9
3.5、建立私网 IP 组.....9
3.6、配置 SNAT 策略.....10
3.7、配置 DNAT 策略.....11
3.8、配置应用控制策略.....12
四、注意事项.....13

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

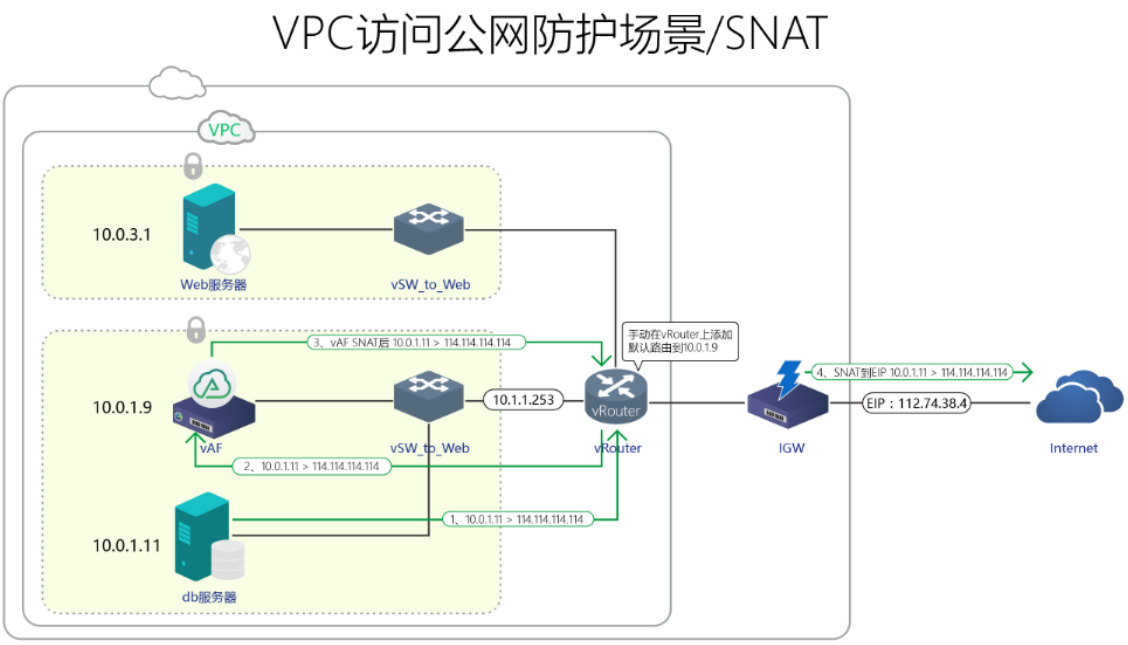
目前 vNGAF 支持两种场景：

SNAT 场景：VPC 私网子网中的实例通过 vNGAF 访问互联网。

DNAT 场景：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。

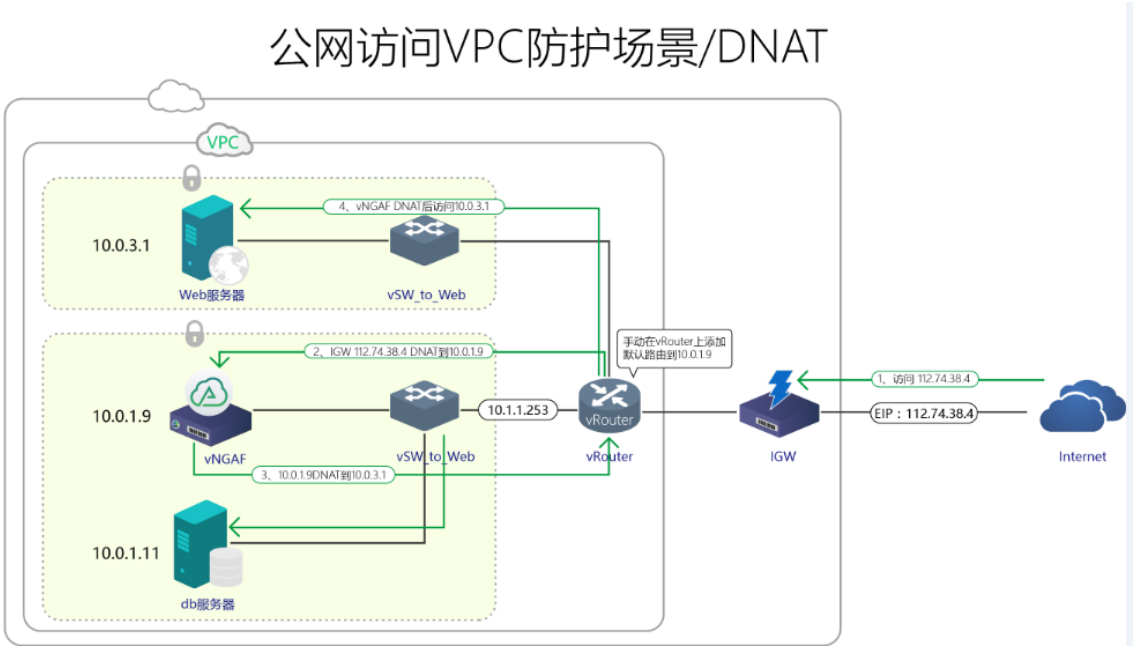
2.2 SNAT 场景

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



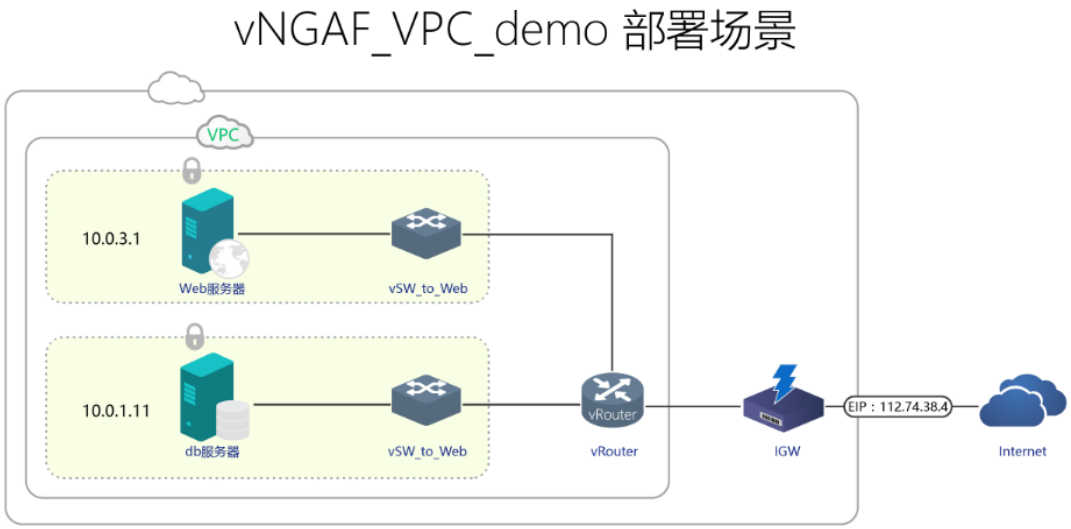
2.3 DNAT 场景

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“vSW_to_db”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。

Step3 从“镜像市场”选择镜像。

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“深信服防火墙”，点击进入购买界面部署选用页面。

Step2 进入“自选 ECS 配置”

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。

Step3 进行 ECS 配置选择

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“4C4G”。

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“vNGAF_VPC_demo”专用网络，放到“vSW_to_db”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、绑定弹性 ip

3.2.1 vNGAF 绑定弹性 ip

本示例中我们约定绑定弹性公网 ip 为 112.74.38.4。了解阿里云弹性 ip，可参考如下相关文档：

http://help.aliyun.com/knowledge_detail/5974922.html?spm=5176.6883001.0.0.ze4Ijm

配置好弹性 ip 后，用户就有两种方法可以登录 vNGAF 了。

在公网可以通过 https://112.74.35.4 登录 vNGAF WEBUI 控制台，对设备进行配置管理

在私网可以通过 https://10.0.1.9 登录 vNGAF WEBUI 控制台，对设备进行配置管理

3.3、获得 vNGAF 授权

3.3.1、获得 vNGAF 授权

通过配置的弹性 ip 可以登录 vNGAF 的控制台。

用户名为 admin，密码为购买 ECS 用户自己设置的密码。

进入到“系统配置→序列号→购买序列号”。

3.3.2、选择合适的付费方法。

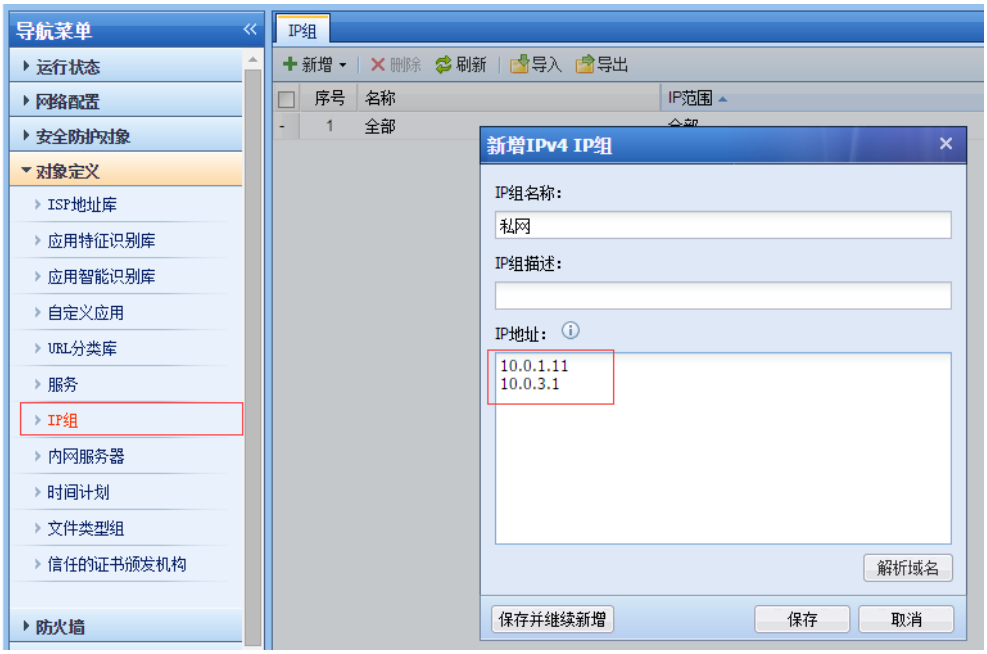
跳转到购买页面提交个人信息填写点击提交后将获得序列号，将序列号输入到 2.4.1 的图中。就可以愉快地使用 vNGAF 了。（此处内容比较简单，我们省略购买页面截图说明）。

3.4、添加默认路由

添加一条默认路由指向 vNGAF，目的在于把 VPC 网络的流量引流到 AF

3.5、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。



3.6、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)

3.7、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　　：TCP

目的端口　　：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)

3.8、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

在阿里控制台修改 vNGAF 私网 IP，当 vNGAF 恢复默认配置时，密码恢复为 admin。在阿里控制台重置 vNGAF 密码，当 vNGAF 恢复默认配置时，密码恢复为阿里控制台所设密码。