阿里云 vNGAF4.0 版本配置指南

目录

<i>—`</i> ,	用前必读	2
<u> </u>	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、购买镜像	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。错误!	未定义书签。
	3.3、购买 vNGAF 授权错误!	未定义书签。
	3.3.1、购买 vNGAF 授权错误!	未定义书签。
	3.3.2、选择合适的付费方法。错误!	未定义书签。
	3.4、添加默认路由	11
	3.5、建立私网 IP 组	21
	3.6、配置 SNAT 策略	21
	3.7、配置 DNAT 策略	
	3.8、配置应用控制策略	23
四、	注意事项	24

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。

④ 计费方式	包年包月 😑	按量付费	0		首先需要选持 网络所在的可	爭您的 VPC 闭区
♀ 地域	44alt 1 🥯	华北 2	华北 3 📀	华东 1	华东 2	华南 1
		随机分配 ~	随机分配 ~	随机分配 ~	随机分配 ~	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)
	随机分配	随机分配 ~	随机分配 ~	美国东部1 可用区A ~	随机分配 ~	随机分配
	中东东部 1 (迪拜)	亚太东南 2 (悉尼)				
	随机分配。	随机分配 ~				
	【武礼/pc-94694c02g 如葉使用其他考有网络,講述相当前起树交換机所在可用区为: 公网 IP 地址: 分配 分配的公网IP地址不能和ECS杂化 交配的公网IP地址不能和ECS杂化 安全组:sg-w294gqh3l7rr6v6 清确保比交全组开放包含 22 (L 二前新法将安全组 ③	 【武人)vsv-949h (武人)vsv-949h (日有专有网络,也可以自行到: 却南1可用区 A 学編翰娜定关系,如要更加灵活 fy5e / sg-wz94ggh3l7rr6v6tl nux)或者 3389 (Windows) 	p8m0 空制台创建>> 的静态公阿P方案,建议选择 y5e(已有0个实例,还可以加入 端口,否形行先选择登录ECS。	有 IP 4091 个 不分配"公列IP地址,配置并 1000个实例 您可以进入 ECS控制台 设置。	综定单性公网 IP 地址>>	
	安全組織以附以總功船,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>> 約3	<u>弐</u> 売 ♀ > >	vNGAF 支	持 1C2G,
实例	系列Ⅱ	系列Ⅲ	⑦ 1/0 优化实例 ()		2C4G,及更	高 ECS 配置
	도列之间不能互相升降部 共享计算型 n1 1 校 1GB ecs.n1.tiny	共家通用型 n2 1 核 2GB ecs.n1.small	共享内存型 e2 2 核 4GB ecs.n1.medium	计算型(原独字) sn1 4 核 8G8 ecs.n1Jarge	通用型(原独字) sn2 8 核 16GB ecs.n1.xlarge	16核32GB ecsa1.3xlarge
	32 核 64GB ecs.n1.7xlarge					

(**) 带宽	按固定带宽	按使用流量	0	
后付盡模式,带宽费用合并在ECS实例中收取				
	ii.	50M 100M	200M	20 Mbps
	带宽值 0M。			
	阿里云免费提供最高 5Gbps 的)恶意流量攻击防护, 了解更多	>> 提升防护能力>>	
信 像	公共镜像	自定义镜像	共享镜像	镜像市场 ②
	₿ 从镜像市场选择(含)	操作系统)	使用平台 数据盘	默认值:40,不支持外加
🗟 存储	系统盘: 高	效云盘 🗸 40	GB 1240 IOPS	系统盘设备名:/dev/xvda
	如何选择 SS 数据盘: + 增加	D云盘 / 高效云盘 / 普通云盘 数据盘 您还可选配 4 块;	请看 详细说明 > >	vNGAF 暂时不支持扩展 数据盘,请选择不要添加

Step3 从"镜像市场"选择镜像(vNGAF4.0*)。

镜像市场[华南 1]		×
	9、深信服虚拟化下一代防火墙 搜索	
精选镜像	 ▲ 全部操作系统 ✓ 全部操作系统 	
镜像分类 へ	深信服虏拟化下一代防火墙(包含50M吞叶量榜权)	00.0/8
✔ 全部	基础系统:linux 架构:64位 vNGAF 18人已使用	购买
操作系统	深信服vNGAF是为云环境设计的下一代防火墙产品,智能融合了防	
运行环境	深信服虚拟化下一代防火墙(包含200M吞吐量授权)	20.0/月
管理与监控	基础系统:linux 架构:64位 VNGAF VIGAF 31人已使用 31人已使用 31人已使用	购买
建站系统	深信服度划化下一代防火墙(句会5M吞叶量接权)	
应用开发	基础系统:linux 架构:64位 ✓NGAF ▲24	80.0/月 10平
数据库	深信服vNGAF是为云环境设计的下一代防火墙产品,智能融合了防	
服务器软件	深信服虚拟化下一代防火墙	<mark>0.0</mark> /月
企业应用	基础系统:linux 架构:64位 vNGAF → 412人已使用 家信服vNGAF是为云环境设计的下一代防火墙产品。智能强合了防止, 4404540,0017550	购买
云安全市场	VNGAF2.0 2010023	
已订阅的镜像	vNGAF2.0_20160302	
已购买的镜像	vNGAF2.0_20160127	
	VNGAF2.0 大有4条	1
< >	vNGAF2.0	

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。

云市场 ^{云计算的 AppStore}	在此编入参赛要的服务 手机网站建设企业网站建设PHP运行环境JAA运行环境全能环境	28全部 或者 发布定制要求▼ 第 linux研結調査 数据迁移 清除木马	灭家中心▼
云市场分类	必BUY软件 网站建设 安全 企业应用 API服务	开发者软件 品牌馆 🦷	校订 商品资讯
搜索 深信	系下一代的比喻 ×		
产品分类:	软件市场 服务市场 建站市场 云安全市场 企业应用 解决方案 API市场		
价格:	金誌 免機 1-98 99-198 199-1998 1999-2998 2998以上		
默认排序	上朝时间章 价格章 评分章		为您找到 3条结果
VNGAF	深信服虚拟化下一代防火墙(包含200M吞吐量授权) 🗟 阿里云代的 交付方式: 議會 基礎系統: sangfor OS 深信服MHOAF是为云场级设计的下一代的火墙产品,普髓融合了的火墙、WAF、IPS、APT的油产每户 服务者: 深信服料技能台有限公司 的火墙 NOFW 安全风关 IPS APT改击防护	体现保障: ⑥ ⑨ ₪ 产品评分: ★★★★★ 使用人致: 47	¥ 2720/月 + Ecs使用處用
VNGAF	深信服虚拟化下一代防火墙(包含5M吞吐量授权) ⑧ 阿里云代第 交付方式: 鏡像 基础系统: sanfor OS 深信服-MGAF显为云环境设计的下一代劲火墙产品,智能融合了防火墙、WAF、IPS、APT劲炉、僵户 服务病: 深信服料线股合有限公司 企业 安全 防火墙 NGFW IPS 一体化变全防护 网络边界安全	体现保障: ⑧ ⑨ № ⑧ 产品评分: ★★★★★ 使用人数: 49	¥ 280/月 + ECS使用夔用

Step2 进入"购买页面"

云安全市场 > 网络安全	云安全市场 > 网络安全 > 防火墙							
VNGAF	深信服虚拟化下一代防火墙(包含 深信服WNGAF是为云环境设计的下一代防火墙产品 里云相户VPC网络二到七层全面的安全防护。	200M吞吐量授权) ,智能给了防火墙、WAF、IPS、APT防	护、僵尸网络监测等多项安全功能,实现阿					
	¥ 2720 /月 续费:¥ 2720/月 按量价格:¥ 0/小时		用户评分:★★★★★ 使用人数:47人					
	立即购买							
(保)交易过程担保	· · · · · · · · · · · · · · · · · · ·	(监) 服务全程监管	优 优质服务商					

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。

选择配置





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

 管理控制合 	产品 与服务 🗸	Q.她发 🖡 🔁 幽闭 工業 敏振 支持 songór_cs 徽和中文
▼ 云计算器机报告	PHINISULA	▶ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
■ 元統のHA ECS	弹性公网印	ションでは、「などのない」では、「などのない」では、「などのない」では、「などのない」では、「などのない」では、「などのない」では、「などのない」では、「ない」」では、「ない」では、「ない」では、「ない」では、「ない」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「ない」」では、「は、」」では、「は、」」では、「は、」」では、「は、」」では、「は、」」では、「は、」」、」」では、「は、」」、」、」」、」
❤ 云数据库RDS 版		Melonpole V Salvecondersigner at
👶 负载均衡		C RMU PAL AL RR (1982)(201 Vol(20) - Vol(20) - RRAN RR
の 专有网络 VPC 同 云教講岸 Reds 版		© 沒有直得到的合条件的记录 从此处进入
分 弹性公用 P		由语硝性ID
 大敗据(敗加) 		
▶ 安全(云山) ▶ 時名日間(1/17)	-	
 → 云市场 		

3.2.2 购买弹性 IP

用户按需要选择购买弹性 IP 的方式

预付费	按量付费	
EIP只能绑定到VPC	下的ECS,且要求购买ECS时不要为其分配公网IP	
地域: 带宽峰值:	华北2(比売) 华东1(杭州) 华北1(倩岛) 香港 华西1(元初) 华东2(上海) 亚太东南和(倚加坡) 美西(建合) 美东(俾吉尼亚) 亚太东北1(日本) 欧州中部1(法二完高) 中东东部1(迪邦) 亚太东南2(張市) 华北3(张京口)	当前配置 地域: 华南1(深圳) 市効は信: 1 市窓计表方式: 技使用流量计费 计感明: 1/147 eip服务: 星 计频项: 配置規用(1P規用)+流量規 用 明天致温: 1 配置規用: 1 配置規用: 1
带宽计费方式:	按使用流量计数 	¥ 0.02 ///bf 公務流機規用: ¥ 0.80 /GB 立即购买

3.2.3 绑定弹性 ip

□ <mark>i-94piv4h44 爱 </mark>	🏻 10.0.3.3 (私有) 🌑 运行中	专有网络	CPU: 4核 内存: 4096 MB	包年包月 15-11-17 00:00到期	管理 变配 续费 <u>更多</u> →
□ 启动 停止 重启 重置密码	续费 释放设置 更多-			共有2条 ,每页显示:20条	启动
					重启
					重置密码
					修改信息
					连接管理终端
					连接帮助
		占土山	あませ) 知 空 诫 赴 T	р. μ Ξ	重新初始化磁盘
		从市此	处进入绑走弹性1	P 孙国,	更换系统盘
		选择刚	刚购买的弹性 IP	即可。	编辑标签
					安全组配置
					修改私网IP
					绑定弹性IP
			し 伝統 日子	-17 Linix -	
绑定弹性IP				×	
FCSको/ब्रो	WIGAE			-	
LCO X (/)	MORI -				
*2单M+TD 。	法许权				
5年1王16 :	明儿中				
-				-	
,A	112.74.38.4 / eip-9	94nc	at R	12世	
-	L		HILE B		

3.2.4 弾性 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

SANGFOR			这里用户名默 认为 admin.
技术服务先线 400-630-6430	接奈 深信服徒未服务性区 政策多支持 SUPPのRT 用深信設产品	下一代防火墙管理 用户名 密码 登录 使用隔值登录/0面	^{孫第} 为购买镜像时 设置的密码
● 2011-2017 读信解公司訴权所有			

3.2.5 登录成功首页

	SANGFOR VNGAF ×	Δ - σ
	/39.108.113.23/framework.php	陶 ☆
	.0	Razos (Azhe-o
导航菜单	系统状态	
→ 运行状态	- 通接量示模块 •	
> 网络配置	安全営営中心 母 後着淡瀬	# @ 擁口狀态(1) Ø 今日系统状态
・安全防护対象 ・VPN	代表の語 14% 28% 19% 16	主観记录: 2/2 UP技術: 0 在54月中: 0 已計解助性: 小子以有:
→ 对象定义		系統時間: 2017-05-25 15:42-45 服务期期: 2018-06-26 (軌余:367天) 体表
) 前密		
防火端	雪橇重整 火打▼	- 版用電理超時費加降值時間高級電理 Kbps
/ 内容安王 - 100		0.05
1 85.3.610		
→ 展然変要加株的	400	0.025
▶ 系统		
>系绕维护	200	
		00.00 03:00 06:00 09:00 12:00 15:00 18:00 21:00
	15:34 15:36 15:30 15:40 15:42	SSH
	入銀风险(TOP 10) 最近七天・ 2 伊 ×	▲口吞吐革新线图·所有WAN口实时注题 0 日 N ×
	业务组成 风险类型	Maps 英时发送: 270cps 英时接版: 51kbps
		1200
		800-
	⊘ 您的网络环境中暂未发现入团风险!	em
		400
		15:39 15:40 15:41 15:42
	l	

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;

CJ 无能器储密理控制台 x / 彙 SANGFOR iNGAF x							
← → C ▲ 不安全 bHp5;//	← → C ▲ 不安全 ▶#が//39.108.113.23/framework.php 文 :						
				副部語句号 🔷 🔔 admin 🔻 [内置数据中心]			
导航菜单	系统状态						
▼ 运行状态	□ 选择显示模块 • □ 恢复默认显示模块 > 开启投屏显示支持						
> 系统状态	安全运营中心 🛛 设备资源		● 母 接口状态 (1)	 今日系统状态 			
> 安全状況		26% 10%	ethO	拦截/记录: 2/2 IP封锁: 0 在线用户: 0			
 > 安全事件 	2 CPU	内存 磁盘		已持续防护: 小于1小时 系统时间: 2017-06-26 15:50:25			
> 流量排行		vNGAF产品授权购买					
> 昇常流量	会话监控 英时•		所有线路总流速	* 8 ×			
→ 封锁攻击者IP	并发系建	光面山时 光面山时 技用问题 按年问题					
	300 -	开通时长: 30天					
▶ 网络配置		带宽大小: 5 108					
◆ 安全防护对象	200-	支付方式: 341%					
▶ VPN ▶ 対象曲以	100-	应付金额· 0 00 -					
· Л≱上入 → 留家		121711 KK, 0.00 7	0 06:00 09:00	12:00 15:00 18:00 21:00			
→ 防火墙	15:42 15:44 1	8		H22			
→ 内容安全	L						
→ IPS			有WAN口实时流量	¢ 8 % ×			
▶ 服务器保护		2000 -		实时发送:2Kbps 实时接收:2Kbps			
▶ 风险发现和防护		1500					
→ 系統				M			
▶ 系绕维护		1000 -					
		500 -	A A	In a hilling			
		0	15:47 15:48	15:49 15:50			
			■ 发送 🔲 接收				

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

vNGAF产量	- 授权购买			
付费模式:	免费试用	按月付费	按年付费	
开通时长:	30天			
带宽大小:	5 MB			
支付方式:	支付宝			
应付金额:	0.00 元			
			(下一步

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。

vNGAF产品	授权购买
联系人:	请输入姓名
电话号码:	请输入电话号码
公司名称:	请输入公司名称
电子邮箱:	请填写正确邮箱地址以便获得序列号
推荐人:	请输入推荐人姓名 (选填)
温蓉提示:	电子邮箱用于接收产品序列号,请务必填写有效邮箱。
	上一步下一步

以下是样例:

vNGAF产品	授权购买
联 系 人:	张三
电话号码:	0755-86627888
公司名称:	sangfor
电子邮箱:	xx@xx.com
推荐人:	深信服
温馨提示: :	电子邮箱用于接收产品序列号,请务必填写有效邮箱。
	上一步下一步

确认信息后,请点击【提交订单】

vNGAF产品	品授权购买
订单编号 :	F30346B8E75D4AA90A479DC74B5A101B
订购人:	张三
购买时长:	30天
带宽大小:	5 MB
电子邮箱:	xx@xx. com
订单总额 :	0.00 元
	「「二方」「「近父り早」
vNGAF产品	品授权购买
授权	恭喜您,产品授权成功! 序列号已经发至 xx@xx.com 邮箱,请注意查收邮件!
	开始使用

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】

vNGAF产品	授权购买		
付费模式:	免费试用 按月付费 🧹	按年付费	
 开通时长:	1个月 💌		
带宽大小:	5 MB 💌		
支付方式:	定时定		
应付金额:	280.00 元		
		下一步	

确认信息无误后,【提交订单】

vNGAF产品	授权购买	×
订单编号 :	AFFC6E46739B7BE5843E5C73B3F19B4A	
订购人:	张三	
购买时长:	1个月	
带宽大小:	5 MB	
电子邮箱:	xx@xx.com	
订单总额:	280.00 元	
	上一步 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:

恭喜您,购买成功!
购买清单已发至xx@xx.com邮箱,请注意查收邮件!
订 单 编 号: AFFC6E46739B7BE5843E5C73B3F19B4A
产品序列号: [199555455117]。 NFGGG62ZHVTH3VDWNIN117
5N过期时间: 2 10
点击复制序列号

【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。

vNGAF产品授权购买	×
请输入有效的序列号:	
请将序列号串码填写在此处	
温馨提示: 1. 产品授权序列号购买成功后可在邮箱查收获取。	
2. 请检查浏览器是否拦截了支付页面。	
3. 或者通过'系统'->'系统酉置'->'序列号'->'修改序列号'输入序列号。	
重新购买 提交验证	

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:

C3 云服务器管理控制台 ×	SANGFOR UNGAF X) ×
	/39.108.113.23/framework.php	☆ :
	0 🔓 印度向导 🔷 admin * [內里和	据中心]
导航菜单	Réstine Résting Réstin	
→ 运行状态	系統相同 网络参数 控制面积置 序列号	
▶ 网络配置		^
▶ 安全防护对象	四天が今:10209414 当前前外码:	
▶ VPN	UHPSSQMv2L2VY2ZJSHFW3STN562ZHVTH3VDWNP6OHK4JATMZEQHXV6AXPTYX03VWZBPA5ZOT907Q	
▶ 对象定义		
) 順密		
/ 防火垣) 由安定会		
→ IPS	田坦远大,填气起源大利印度刘玉	
▶ 服务器保护		
▶ 风险发现和防护		
▼系統		
> 系統配置		
> 管理员帐号		
> 日志设置		
> 邮件服务器		
→ 邮件告警		
> 全局放行与封堵		
1. 无弦镜的		
' 永靖准丁		
		alla

(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:

CD 云服务器管理控制台 ×	SANGFOR VNGAF ×		×
	/39.108.113.23/framework.php	\$:
	0	副 部語句导 💦 🔷 🌰 admin 🔻 (内置共振中心	D
导航菜单	系统状态 安全状况 *		
▶ 运行状态			
▶ 网络配置	安全运营中心 🔗 设备资源		1 -
 > 安全防护対象 > VPN > 対象定义 > 留本 	Филипона 22% 27% 19% 4 СРО 27% 19%	11 載记录:22 [P545]:0 石鉄周下:0 已持時時時:1/9引 月前時時時:2017-0-75-26 (純余:07天) 終売	
→ 防火墙		应用流速趋势叠加图·所有线路总流速 # G ×	
▶ 内容安全	并发 新建	Kbps 由此进入【续费】,延长您的开通时长	1
→ IPS	300	0.05	
▶ 服务器保护			
▶ 风险发现和防护	200 -	0.025 -	
▼系統			
> 系统配置			
> 管理员帐号		00:00 03:00 06:00 09:00 12:00 15:00 18:00 21:00	
> 日志设立	16:40 16:42 16:44 16:46 16:48	SSH	1
> 即任服务益	入侵风险(TOP 10) 最近七天・ ● ○ ×	接口吞吐率折线图•所有WAN口实时流量	4
 / 即任日要) 全局執行与封援 	业务维度 风险类型	Kbps 实时发送: 32Kbps 实时接收: 45Kbps	
· 32950711-93074		400	
▶ 系统维护		300 -	
	◆ 定的可能环境中基本发现入强和脸!	200 0 0 发送 一 规论 16:46 16:47 16:48	Ļ

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。

C3 云服务器管理控制台 ×	SANGFOR VNGAF X	— —	- X
	/39.108.113.23/framework.php		☆ :
		副 政策向导	据中心]
导航菜单	系统状态 安全状况 *		
→ 运行状态	□ 选择显示模块 • □ 恢复默认显示模块 ⇒ 开启投屏显示支持 由此进入 【	【配置向导】	
▶ 网络醌匮	安全运营中心	# Ø 接口状态(1) Ø 今日系统状态	\$
▶ 安全防护对象			1
▶ VPN	待处理问题 18% 27% 19%	etho 在SARAF: 3 已持续防护: 1小时	
→ 对象定义		系統时间: 2017-06-26 16:49:17 服务期限: 2017-07-26 (如今:30天)((2 7 8
▶ 解密		······································	_
▶ 防火墙	会話监控 实时▼ # # X	应用流速趋势叠加图·所有线路总流速 *	8×
▶ 内容安全	并发 新建	Kbps 0.05-	
→ IPS	300		
▶ 服务器保护			
▶ 风险发现和防护	200-	0.025 -	
▼系統			
> 系統配置			
> 管理员帐号		00:00 03:00 06:00 09:00 12:00 15:00 18:00 21:00	
> 日志设置	16:40 16:42 16:44 16:46 16:48	SSH	
> 邮件服务器	入侵风险(TOP 10) 長近七天▼ # @ ×	接口吞吐案拆线图-所有WAN口实时按键 # P	4×
> 邮件告警	小谷维度 网络类型	Khas 空时发送,36has 空时接收,7k	hns
> 全局放行与封堵		500	1
		400 -	
▶ 糸鏡維护	🔗 你的网络环播山顿未安福入傅风险!	300 -	-
	YOH RUDRY LARTE HARRANDA	200 -	
		0 16:46 16:47 16:48 16:49	
		📕 炭送 📕 搬收	-
			da

【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



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。

<	路由器基本信息						编	辑 へ
专有网络洋梧	名称: -			ID: vrt-94aan1rlr 创建时间: 2015-10-16 14:37:54				
2 10 10 10 10 10 10 10 10 10 10 10 10 10	备注: -							
海田縣								
交换机	路由条目列表							
	路由表ID	状态	目标网段		下一跳	下一跳英型	类型	操作
	vtb-94ukjb991	可用	172.16.0.0/12		i-9482m0bwi	ECS实例	自定义	删除
=	vtb-94ukjb991	可用	220.220.0.0/16		i-9482m0bwi	ECS实例	自定义	删除
	vtb-94ukjb991	可用	0.0.0.0/0		i-94piv4h44	ECS实例	自定义	删除
	vtb-94ukjb991	可用	10.0.1.0/2	4			系统	-
	vtb-94ukjb991	可用	10.0.2.0/2	4			系统	-
	vtb-94ukjb991	可用	10.0.3.0/2	4	-		系统	-
	vtb-94ukjb991	可用	100.64.0.0	/10			系统	
						共有1条,每页显	示:50条 《 〈 1	> »

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。

)									[内置数据中心	
导航菜单	网络对象										
▶ 运行状态	网络对象	服务器识别									
▶ 网络配置	+新増・	× 刪除 🗳 刷新 🕍 导入 🧯	导出					查看: 所有类型	! ▼ 搜索		P
▶ 安全防护对象	□ 序号	名称	类型	*	IP范围		描述			刪除	
▶ VPN	- 1	全部	4	新増 IP组		×	所有IP地址			已被引用	
▼ 对象定义	• 2	私有网段	말	IP组名称:			私有IP地址			×	
→ IP地址库				私网							
> 应用特征识别库				IP组描述:							
> 应用智能识别库											
> 自定义应用				IP组类型:							
› URL分类库				IPv4	IPv6						
> 服务			ſ	IP地址: (i)							
→ 网络对象				10.0.3.1							
> 时间计划											
> 文件类型组											
> 信任的证书颁发机构											
▶ 解密						解析域名					
▶ 防火墙											
▶ 内容安全				保存并继续新增	保存	取消					
→ IPS											
▶ 服务器保护											
风险发现和防护											
▶ 系鏡											
▶ 系绕维护	H - 1)	1 页井1 页 🕨 🗎 😂	每页显示条数	t 50					3	当前显示1-2条 共	+2条

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)

导航菜单	地址转换	
▶ 运行状态	IPv4地址转换 DNS-Mapping 新增源地址转换	×
▶ 网络配置	+新増→×⊪除↓✓启用 ⊘禁用↓★上∛ → 启用	
▶ 安全防护对象		
▶ VPN	□ 序号 名称 转换类型 源区域 描述・ 5NA 1	岩口
▶ 对象定义	100℃・ 插入到: 1 →前 ▼	_
→ 解密	·····································	
▼ 防火墙	区域: manage	5
> 地址转换	网络对象: 私网	<u>s</u>
> 连接数控制		
▶ 内容安全		
→ IPS	· · · · · · · · · · · · · · · · · · ·	1
▶ 服务器保护	eth0	\mathbf{v}
▶ 风险发现和防护	网络对象: 全部	<u>p</u>
▶系统		
▶ 系统维护		
	間に立め以、端口	
	源地址转换	
	转换为: 指定IP	~
	指定印: 10.0.1.9	
	保存并继续新增 保存	取消

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)

导航菜单	地址转换
▶ 运行状态	IPv4地址转换 DNS-Mapping 新增目的地址转换 ×
▶ 网络配置	+新増→×⊪除↓✓启用 ⊘禁用↓ ●上]
▶ 安全防护对象	
▶ VPN	序号名称 转换类型 源区域 石物・ DINA I 描述: 時間地(小) 四名第
▶ 对象定义	描入到: 1 →前 ▼
→ 解密	莱
▼防火墙	区域: manage 炉
▶ 地址转换	
> 连接数控制	目的
	IP: ●指定IP(i)
▶ 内容安全	10.0.1.9
→ IPS	请选择 短
▶ 服务器保护	
▶ 风险发现和防护	协议
▶ 系统	协议类型: 所有协议 💙
▶ 系统维护	日的他们转换
	指定叩: 10.0.3.1
	✔ 放通上述条件的数据,不受应用控制策略限制 ①
	高级设置
	保存并继续新增 保存 取消

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)。

导航菜单	应用控制策略	
▶ 运行状态	+新增 × 刪除 ✓ 启用 ⊘ 禁用 ↑ 上移 新増应用控制策略	×
▶ 网络配置	□ 优先级 名称 分组 源[月田	
▶ 安全防护对象	- 1 默认策略 - 全音	
→ VPN	名称: 放	(通业务数据
▶ 对象定义	7组: 默	
▶解密	- 第	
▶ 防火墙	网络对象:利	
▼ 内容安全		ianage 👳
▶ 应用控制策略	端口: •	全部
> 内容安全策略	•	指定端口()
→ 僵尸网络		
	目的	
→ IPS	网络对象: 4	
▶ 服务器保护		
▶ 风险发现和防护		
▶系统	服务/应用	
▶ 系统维护	服务/应用: ●	服务
		预定义服务/any 型
	U U U U U U U U U U U U U U U U U U U	
		旧应祥 望
	生效时间:	天 天
	志力作: .) 允许 💛 拒绝
	高级选项: 设	置
	<u></u>	
	▶ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	确定

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。