阿里云 vNGAF1.0 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
Ξ,	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1	0
	3.7、配置 DNAT 策略1	1
	3.8、配置应用控制策略1	2
四、	注意事项1	3

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。

		交换机 ID/名称	ECS实例数	网段	状态	可用区	可用私有IP数	创建时间	描述	操作
交换机		vsw-94pyuorys vSW_to_web	1	10.0.3.0/24	可用	深圳可用区A	251	2015-10-17 10:32:54	连接web服务器	编辑 删除 创建实例 -
		vsw-94w6lzmh3 连接FTP服务器	1	10.0.2.0/24	可用	深圳可用区A	251	2015-10-16 16:26:17	连接FTP服务器	编辑 │ 删除 创建实例▼
	-	vsw-94qufwdlc vSW_to_db 🖌	3	10.0.1.0/24	可用	深圳可用区A	249	2015-10-16 14:39:47	连接数据库服务器	编辑 删除 创建实例▼
										创建ECS实例
								共有39	後, 毎贝显示:10条	创建RDS实例
										创建SLB实例

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。







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。

	产品与服务	s 解决方案	云市场	开发者中心	阿里云+	
深信服	防火墙	却 助中心(1)		论坛(1)	三古场(1)	♥ 搜索
	GAF	★ ★ ★ ★ ★)	的下一代网络安全产品	,智能融合了WAF、IPS、	APT防护、僵尸网 0元/次

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。

深信服下一代防火墙	
评分: ☆☆☆☆☆ 暫无	
基础系统:Gentoo-r8 64位 可用地域:杭州,青岛,北京 云服务器规格推荐:4G2C 漫持:ECS免费试用	:, 深圳 , 上
镜像版本: V1.0 ▼	
所在地域: 杭州 青岛 北京 深圳 上海 镜像只	能用于同地域的云服务器
是否购买ECS : 购买ECS 只购买镜像	
新购ECS配置	
推荐配置: 普及型1:2核CPU-2G内存-3M带宽 -	
购买时长: 单月 季度 半年 一年	
数量: 1 ♀ 台	
金额:¥219 (镜像0元+云服务器 219元)	这里请选择"自选 ECS",不 要直接点击"立即购买",否
交易过程担保 不满意全额退款 服务全程监管	则可能导致您的 ECS 不可用
立即购买 自选ECS配置 ⑧ 已订阅	
☑ 同意 《镜像市场用户使用协议》	
已有ECS的用户请前往 管理控制台 进行设置	

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

i-94p2b6r64 db服务器 ✔	4	Ľ	深圳可用区A	10.0.1.11 (利	有) 🔴 រ៉	四行中 专有网络	CPU: 1核	内存: 2048 MB	包年包月 15-11-17 00:00到期	管理 变配 续费 更多▼
i-94piv4h44 vNGAF			深圳可用区A	112.74.38.4 10.0.1.9 (私社	(弹性) 可)	四行中 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 更多▼
启动停止	重启	重	置密码 续	费释放设置	更多▲			共有3条 , 每页显	示:20条 « <	1 > >

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"。

← → C ★ bttps://112.74.38.4/framework.php							
	R4						
导航菜单	系统状态 系统配置 *						
→ 运行状态	系統时间网络参数 控制台配置 序列号						
▶ 网络配置							
▶ 安全防护对象	网关序列号						
▶ 对象定义	用作网关设备,可以连接外网线路与分支						
▶ 防火墙							
▶ 内容安全	状态:未激活 点击此处跳转到购买						
▶ 风险发现和防护	1. 分支机构:0 授权界面, 您可以洗择						
▼系统	3. 移动用户数:0 直接购买序列呈武者						
▶ 系统配置	修改序列号 购买序列号 选择 法用 WICAE						
> 管理员帐号	见评 试用 VNOAF						
	四月 购买成功后在						
	此输入序列号						

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

<	路由器基本信息						编辑	-	^
专有网络关键	名称: -			ID : vrt-94aan1rlr	5-10-16 14:37:54				
で有からが用	备注: -								
交换机	路由条目列表								
	路由表ID	状态	目标网段		下—跳	下一跳类型	类型		操作
	vtb-94ukjb991	可用	172.16.0.0	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	>	»

3.5、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。

导航菜单	× IP组							
▶ 运行状态	▲ +新	増▼	★删除:	😂 刷新	í 🕍导入 / 📩 导出			
▶ 网络配置		序号	名称			IP范围 ▲		
) 安全防护对象	-	1	全部		新増IPv4 IP组	△侴		×
▼ 对象定义								
→ ISP地址库					IP组名称:			
▶ 应用特征识别库					私网			
> 应用智能识别库					IP组描述:			
→ 自定义应用								
▶ URL分类库					IP地址: ①			
▶ 服务					10.0.1.11 10.0.3.1			
→ IP组								
> 内网服务器								
▶ 时间计划								
> 文件类型组								
> 信任的证书颁发机构								解析域名
 ▶ 防火墙 					保存并继续新增		保存	取消

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)

导航菜单	地址转换			
・运行状态	「IPv4地	新增源地址转换	k.	×
・网络配置	+新增、	✓ 启用		<u>^</u>
▶ 安全防护对象				
▶ 对象定义	✓ …	名称:	SNAT	
▼ 防火墙		描述:		
> 地址转换		源		
) 连接数控制		⊠域:	manage	<u>P</u>
→ DoS/DDoS防护		IP组:	私网	聖
▶ 内容安全		目的	a	
→ IPS		区域/接口:	◎区域	
▶ 服务器保护			manage ○ 接口	垣
▶ 风险发现和防护			eth0	v
・系統		IP组:	全部	<u>50</u>
・系統曲				
		协议		
		配置协议、端		设置
		源地址转换		
		转换为:	指定IP	~
		指定IP:	10.0.1.9	
				
	H - I	保存并继续新出		保存取消

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)

导航菜单	地址转换			
・运行状态	「IPv4地	址转换	新增目的地址转	专换 ×
▶ 网络配置	+新增、	・×刪除		
▶ 安全防护对象				
▶ 对象定义	□ 序号	名称	名称:	DNAT
▼防火墙		SNAT	描述:	映射web服务器
> 地址转换			『記』	
> 连接数控制			区域:	manage 👳
→ DoS/DDoS防护			目的	
			TD.	● 指完 IP ①
▶ 内容安全			16.	
> IPS				○ IP组
▶服务器保护				请选择
▶ 风险发现和防护				
・系統			协议	
・系統曲			协议类型:	所有协议
			一目的地址转换	<u>م</u>
			IP转换为:	指定IP
			指定IP:	10.0.3.1
			☑ 放通上述条(牛的数据,不受应用控制策略限制 ① 高级设置 •
	H	第 1 3	【保存并继续新:	增 保存 取消

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)。

导航菜单	《 应用控制策略		
・运行状态	+新增 ×刪	余 ✓ 启用	⊘禁用 全上移 ♣ 下移 移动 盧导入 🏥
・网络配置	□ 序号 名	编辑应用控制	策略 ×
▶ 安全防护对象	☑ 1 放	名称:	放通业务数据
▶ 对象定义	- 2 黒	描述:	
▶ 防火墙		源	
▼ 内容安全		IP组:	私网
> 应用控制策略		区域:	manage 👳
> 病毒防御策略		端口:	● 全部
) 僵尸网络			◎ 指定端口 ①
→ WEB过滤			
> IPS		目的	
▶ 服务器保护		IP组:	全部 短
• 风险发现和防护		区域:	manage 😥
・系統		服务/应用	
・系統維护		服冬/应用,	 · · · · · · · · · · · · · · ·
		ימעמוימאיי	预定义服务/any 原
			◎ 应用 🗸
			「 · · · · · · · · · · · · · · · · · · ·

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。