奇安信虚拟化下一代防火墙 部署阿里云指导手册

奇安信集团

2020年4月

1

目录

第一章 概述	3
1.1. 产品介绍	3
1.2. 安装要求及其注意事项	3
第二章 设备介绍	4
2.1 设备列表	4
第三章 上线购买说明	4
3.1. 如何购买奇安信 vNGFW	4
3.2. 方法 1 云市场购买	4
3.3. 方法 2 管理控制台购买	7
第四章 许可证	
4.1. 许可证作用	10
4.2. 许可证类型	10
4.3.获得许可证	
第五章 部署案例	12
5.1. DNAT 网络部署	12
5.2. SNAT 网络部署	15
5.3. IPSEC VPN 网络部署	17
5.4. SSL VPN 网络部署	21

第一章 概述

1.1. 产品介绍

"奇安信虚拟化下一代防火墙"简称为vNGFW,它是一个纯软件形态的产品,是运行在 虚拟机上的完全自主知识产权的SecOS操作系统之上。奇安信vNGFW是虚拟机镜像方 式存放在阿里云平台上,所以您必须为它提供一个存储介质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,奇安信 vNGFW会自动安装成功。

1.2. 安装要求及其注意事项

● 阿里平台上用于安装部署奇安信vNGFW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"可用区域"的时候,需要修改成"专有网络" 类型。

- 安装的配置要求必须选择2个vCPU,内存最低是2G。
- 奇安信vNGFW只能在阿里云"I/O优化"的实例/虚拟机上运行。
- 启动实例以后您必须在控制台重置密码才能正常使用(新密码包括字母,数 字,特殊字符,至少12位)。

 产品授权方式分为试用版本和正式版本,镜像本身默认提供给用户30天的试用 期,在此期间所有的功能都可以正常试用,提前15天会有到期告警信息,试用期过 后如果没有新的授权,所有的功能均不能使用。正式版本需要您购买相应的许可服 务,购买了正式版本则所有的功能均可用,如果没有购买相关的特征的升级则该功 能特征库升级不可用,但是功能仍可使用。

第二章 设备介绍

2.1 设备列表

编号	类型	单位	数量	备注
				一台 ECS 需要安装 vNGFW, 另一台需要安装被保
1	云服务器 ECS	台	2	护的云服务器(如 WEB 服务器)
				阿里云会为每个 VPC 网络分配一个路由器,这
2	V_Router	台	1	个不需要用户单独购买,可以配置静态路由拓
				展用户的需求
				阿里云会为每个 VPC 网络默认分配一个交换机,
3	V_Switch	台	1	这个不需要用户单独购买,可以在交换机下购
				买 ECS 服务器
4	公网 IP 地址	个	1	需要在阿里云租用一个公网 IP 地址供用户访问
				使用
5	360 网神 vNGFW	套	1	绑定 ECS 服务器一起购买
6	WEB 服务器(示例)	套	1	绑定 ECS 服务器一起购买

第三章 上线购买说明

3.1. 如何购买奇安信 vNGFW

奇安信vNGFW需要部署在阿里云的ECS实例上进行使用,所以您必须购买ECS,我 们这里简单的介绍一下ESC的购买方法,阿里云为我们提供了两种购买方法。

3.2. 方法1云市场购买

一、 首先, 使用阿里云账号正常登陆阿里云系统中。

二、 进入云市场->网络安全在搜索栏输入"奇安信虚拟化下一代防火墙"点击进入 购买界面。如图1所示:

全速重构暖春助力包 期力各行各业第二第产	加速入口) ×
C→)阿里云 云市场 C→)阿里云 云市场 C→1000 C→1	E 文档 备案 控制台 360网神_gateway
云市场分类 服务 建站 API 力公软件 基础软件 新零售 容器 安全 IoT 阿里云心透 用所	□案例 新手专区 买家中心▼ 素家中心▼
云安全市场 > 网络安全 > 防火増	
う安信虚拟化下一代防火塩系统(I/O优化) う安信虚拟化下一代防火塩系统是专门为虚拟化环境安全需求设计的网络安全产品,产品功能主要包含安全策略、 访问控制,基础路由功能、NAT、LLB、HA、CoS、IPS、AV、URL过速、内容过速等功能 ¥ 0.01/月 按量价格:¥ 0.01/小时 按数:¥ 0.01/月 按量价格:¥ 0.01/小时	服务育: 閃時信息沈木(北京)股份有限公 可 取業客報: @ 7月1902 同酷处理: <u>推交工単</u> 在线时间:周一到周五9:30-18:30 电话: 4009030002は10928 18923391323 都相: ketu@b.360.cn
服务保障 请勿线下交易!90%的欺诈、纠纷、资金盗取均由线下交易导致。	

三、 点击"360网络虚拟化下一代防火墙系统(I/O优化)"->立即购买

	全速重构暖春助力	〕 1 助 力各行各业复工复产 4月21-4月24	加速入口 🕥 🛛 🗙
(一) 阿里云 云市场	在此編入怨黑要的服务 证书配置 短信 印刷文字识别 人脸识别	搜索 发布定制需求 冒购物车 身份证实名认证 视频直播 图片	E 文档 备案 控制台 360网神_gateway
云市场分类	服务 建站 API 办公软件 基础软件	牛 新零售 容器 安全 loT 阿里云心选 用/	□案例 新手专区 天家中心 ▼ 東家中心 ▼
云安全市场 > 网络安全 > 防火墙			
 う 安信虚拟(4 奇安信虚拟(4 访问控制,基础 ¥ 0.0	化下一代防火墙系统(I/O优化) 一代防火墙系统是专门为虚拟化环境安全需求设计 路由功能、NAT、LLB、HA、QOS、IPS、AV、UF 1 _{/月}	的网络安全产品,产品功能主要包含安全策略、 21过速、内容过速等功能 用户评分:★★★★★★	服务商 阿仲信息技术(北京)設份有限公 可 取系客級: ●阿特02 阿蜀处理: 程文工単] 在接时间:周一列両五9:30-18:30 电话: 4009030002转10928
续要:¥ 0. 立即购买	01/月 按量价格:¥ 0.01/小时	近180天成交:3笔	18923391323 館種: kefu@b.360.cn
服务保障 请勿线下交易!90%的欺诈、约	盼、资金盗歌均由线下交易导致。	(R) (B) (C)	
产品详情 产品价格	评论详情(2) 使用指南		

我们这里在【华南1】里创建,在这个区域里网络类型只有"专有网络",如果您是 在别的区域创建的ECS,发现默认的网络类型是"经典网络"请您修改成"专有网 络",**奇安信vNGFW**只支持"专有网络"。

● 公网IP是为vNGFW分配一个公网的IP地址,您可以通过这个地址访问管理 vNGFW设备,(这个公网IP并不是配置在防火墙上的,它实际是一个出口的NAT 地址映射)。

● 需要选择ECS所属于的VPC和交换机,阿里云会默认为您创建VPC网络和交换机,它们分别是vpc-wz90di3zp;vsw-wz9s0r7z.如果您手动创建了VPC和交换机在这里更改即可。

● 不同的实例配置的如系列I,II,III,它们的资源规格和价格都是不一样的,这里可

以根据您的需求购买,但要满足:必须2个vCPU,内存最低是2G。如图2所示。

CD网络	重合	
选择	配置	
地域	地域 可用区	华东1 华北1 华市1 华东2 随机分配 ▼
镜像	镜像名称 镜像版本	奇安信/虚拟化下一代励火境系统(I/O优化) ▼4.0 ▼
	网络类型	
	实例系列	ক মান ক মান ক মান
		28771 29071 11 29071 11
	I/O优 化	I/O 优化实例 ②
云服务器	实例规格:	(默认配置) 2 核 4GB : 标准型 s2,ecs.s2.large 更多实例规格
	公网带器	物因金带来
	带宽	50M 100M 150M 1 Mbps
		—————————————————————————————————————
	系统盘	高效元用 ▼ 40 GB 1240 IOPS 系統盘设备名:/dev/xvda
	数据盘	如何选择 SSD云盘 / 高观云盘 / 音通云盘 , 谓首 译明说明 >> + 增加一块 您还可选配 4 块;
购买	付费方式	包月套督 拉量

四、 点击立即购买->去支付, 如图3

COMED	C	阿	Ŧ	5
-------	---	---	---	---

确认订单						
确认订单	支付		\rightarrow		Яi	和成功
产最各种		优惠券	付费方式	购买周期	数量	促销
服务商: 阿里云计算有限公司						
 云服务器ECS(包全包月) 地域: 柴南1 可用区: 柴南1可用区A 实例规治: 2枚408 VO优化实例: 1/0 优化实例 VO优化实例: 1/0 优化实例 研究技術: 1/0 优化实例 瑞売: 1Mbps(設固定完意) 操作系统: Aliyun Customized Linux 联成曲: 400,高双云曲 数成晶: 云圈: 是 霍码: 未设置 		无	包年包月	1个月	1	无
服务商: 阿神信息技术(北京)股份有限公司						
奇安信应拟化下一代防火墙系统(I/O优化) V4.0		Ŧ	包年包月	1个月	1	无
12586: 1426頁 1 185本: V4.0		~~	按量付费	-	1	无

五、 购买成功以后您可以返回阿里云首页进入->控制台->云服务器**ECS->**华南1云 服务器查看是否创建成功。所下图4所示:

2	利列表 4荷1 亚太东南1(新加坡)	综合:1	华北 2	华北 3 华东 2	美国东部 1 (弗吉尼亚) 雪港	中东东部1(迪拜)	亚太东南 2 (孫尼)	紫东 1	欧洲中部 1 (決当	(売福)	亚太东北 1 (东京)
央	▲公共例告告接接查问			披东 •	• 标签							
	实例四/名称		動物	所在可用区	卫地址		状态(全部)	 同時建型(全) 	18) +	配量		
	i-wz9ip23m39afyi0arvf0 iZwz9ip23m39afyi0arvf0	• •	×	华裔 1 可用区 4	A 172.18.220.11	4(私有)	● 运行中	专有网络		CPU: 1核	内存:	1024 MB (I/O(行化)
	i-wz9engm2s3ka1hhyvemn IZwz9engm2s3ka1hhyvemn	•	¥	华南 1 可用区 4	A 119.23.20.79 172.18.220.11	公) 3(私有) 、	● 這行中	专有网络		CPU:2檢 1Mbps	内存:	4096 MB (I/O优化)
0	873 停止 重合 重	警察員	续费	拉服特包年短期	月 释放设置	±%.		v NGFW 的	实例	则安装成	功	

172.18.220.113 这个 IP 地址是真实的防火墙地址,119.23.20.79 是出口设备的地址, 实际上是一个 119.23.20.79->172.18.220.113 地址映射。在公网可以通过 *https://119.23.20.79* 登录 vNGFW 的 WEBUI 控制台,对设备进行配置管理,在私网可 以通过 *https://172.18.220.113* 登录 vNGFW 的 WEBUI 控制台,对设备进行配置管 理。

3.3. 方法 2 管理控制台购买

一、如果您想通过管理控制台方式购买,您必须曾经创建过VPC网络和交换机。 例如:返回阿里云首页->控制台->专有网络VPC->华南1->交换机。如图5所示:

1000144

阿里云-vNGFW上线指导手册

华南 1				
专有网络: 2 译性公网IP: 0				
专有网络: vpc-wz90di3zpjvs42irzn93l		网段:172	2.18.0.0/16	
路由器	1			
交换机	1		ECS	2
安全组	1	市 一 一 二	一交换机1,	进入配置页面

图 5

二、 进入交换机列表->创建实例->创建ECS实例, 如图6所示:

服 件 *						Qas	4 💴	an:	I.	82	**	1.00 C	1 8 4.92
文操作列表									-14	电对电电子	R8884147 R34	Gite	622981
SMAD . WAASADASWAAR	-												
交换机 四/省积	0.0563932	Ro	秋志	100E	可用私有中間	包織町口	影动动机	3	ΠE				10月
vm-uzhitr?z=4k18kv2kq8 -	2	172.18.208.0(20	सम	\$1801 可用区 A	4093	2016-11-15 20:00:39	-	-	System creat	el defeu			মর i হাণ তাইনাগ-
										光和译	· 4727: 0		1
									点	击"包	建实例	v	



- 三、按照下列要求创建ECS实例
- 区域选择【华南1】。
- 网络选择专用网络。
- VPC和交换机需要选择【华南1】下的需要查看名字是否正确。
- 公网IP地址如果使用不分配,后续可以通过弹性公网IP的形式绑定。

● 安全组需要创建一个策略,全通即可,可在ECS实例中引用,默认安全组没有选型是空,需要更改。如图7所示:

阿里云-vNGFW上线指导手册

0 telet	经北 1	spat 2	1941£ 3 🤷	华东1	华东 2	. ≄m i1
	华北1可用区8	制机分配	联机分配	段族1可開区E -	随机分配	\$週1可用区A →
	御湯	亚太东南1(新加坡)	美国西部 1 (社会)	美国东部 1 (美吉尼亚)	亚太东北1(东京)	欧洲中部 1 (法兰克福)
	1880.00 mile -	- 346.949	- 30005001 可用区8 -	美国加超1月用EA -	期机分配	messie -
	中东东部 1 (道理)	亚大东湾 2 (悪尾)				
	网络马驼 一	- BROAR				
网络 网络 ·····················	经共同语	TANKS	Ø			
G 1948	经共同结构实际	V ANS.	0			
C 1988	经共同场。 初天后不适应场内的中国 (第5人)+pc-wc90d3zgjvs42	TANKS im93~ (Million-webt	© Dr?cofk1Blwv1	满 IP 4050 个		
C 1988	经费网络 和来后不能是场积热度型 【图从】+pc-wz9063zg/w42 如高份规制也+4和问情,通知	TANKA Imga (Millow-west 岡和本和阿爾,也可以同行的)	් 0r?colk108wv1 ~ දැනය දුන්නැමැති2> ~	- 洞 IP 4050 个		
C 1985	日本時時名 期代日本建築時間時期 (第5人)+pc-wz90d3zgjvs42 如高後現現他中和時間、通信別 公司ド 地道) 不分配	TANKA (1993) [[Hil].www.chi IChatania (1911)[179]	② 0/7cc4k118w1* 司用w 全时后的道>>	W IP 4050 个		
C 1988	经数期3名 购买后不能图场网络类型 图示()+pc-wc90d325jvs42 如面他用用他争构问道,通信M 公网 IP 始起 (不分配 不分配例分数)。网络线 1 12	TANKS (2093) (Rid):www.wc9d 1284w44Rin (ERid):sou-wc9d 1284w44Rin (ERid):sou-wc9d 1284w44 1284w44 1284w44 1284w44 1284w4 1284w4 1284w4 1284w4 1284w4 1284w4 1284w4 1284w4 1284w4 1284w4	① 0n7colk108wo1~ 200669建>~ 20069建>~	満 IP 4050 个		
P045	日本期間48 初天后不必至於死時完型 「「新人」・pc・ws90di3agiv42 如高後月期告申時間、通信が 公局 P 始星) 不分配 不分配 、ののP 始星) 不分配 、ののP 始星) 不分配 なののP 始星) 本分配 なのののP 始星) 本分配 なのののP 始星) 本分配 なのののP 始星) 本分配 なのののP 始星) 本分配 なのののP 始星) 本分配 本分配 なのののP 始星) 本分配 本分の 本 本 本 本 本 本 本 本 本 本 本 本 本	でのかれる (1874)/www.we9d 日本やお月前、色戸に日子列と (18月の2月、首和日子 非正式のた) (18月の2月、首和日子 非正式のた) (18月の2月、首和日子 非正式のた)	② 0/?cofk188wv1。 包約約8%>> 公開 IP 地址>> (已有1/1大約6 还可以加入068	(第19-4050 个 (本の))		
P045	日本時時名 約天日不過型が約回於型 「新人」。pc-wz90di3zgjv042 如面は日期他を有時間、「新日常 公司 P 始星) 不力成(用合約)の(PP8世) こ22 なうwz920440hd7a33390m8) 「新年間にたまを形形があまえ」()	でかかれる につりうか。 「おいしいい・いとう」 日本からの時間、他同じに同行時日 の の の の の の の の の の の の の	② 0.72cx14188w1。 可用 空時后部連>> 公用 IP 地理>> (日和2115月96 正可以加入の8 第日、 副新天体合理教育に5。	満 (F 4050 个 ? 今時) 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
Files	日本地理研究 田水の中本会社 マッション マッション ロー ロー	FANKIS (1514)/www.w2941 (1514)/www.w2941 (1514)/www.w2941 (1514)/mwww2941 (1514)/mwwwa941 (1514)/mwww2941 (1514)/mwww2941 (1514)/mwww2941 (1514)/mwww2941 (1514)/mwww2941 (1514)/mwwwa941 (1514)/mwwwa941 (1514)/mwwwa941 (1514)/mwwa941 (1	① 077c0%10%wy1~ 支約6分通>~ 公明 IP 转把>~ (日本145分 任可以加入の)3 第日、回到天法百姓被承托CS。	満 IP 4050 个 11年90 12月以進人 ECS技術会 役望。		

图 7

镜像点击镜像市场,从镜像市场中搜索"奇安信虚拟化下一代防火墙系统(I/O优化)"如图8所示:

参 実例	系列Ⅰ	5911	系列 Ⅲ	⑦ 1/0 优化实例 ()	Ð	
	系列之间不能互相升降配					
	通用型 n1	遍用型 n2	内存型 e3	独享型 sn1	独享型 sn2	
	1核1GB 通用型 n1tiny	1枝2GB 通用型 n1.small	2 核 4GB 週用型 n1.medium	4 核 8GB 通用型 n1.large	8 锿 16GB 通用型 ril.xlarge	16 核 32GB 通用型 n1.3slarge
	32 袂 64GB 通用型 n1.7xlarge					
					使用"镱	意像市场"
	公共掩御	自定义镜像	共亨镜像	鏡像市场	٢	
	₿₿ 从機能市场选择(含)	秦作系统)	人镜像市	场中搜索		
			图 8			

四、 进行搜索->购买

镜像市场[华南 1]	×
	选择使用所需镜像,将跳转云市场购买包月套餐(含云服务器),享受镜像优惠价格!	
全部 运行环境	奇安信/虚拟化下一代防火墙系统(I/O优化) Q 筛选 X	
管理与监控 建站系统 应用开发	奇安信虚拟化下一代防火墙系统(I/O优化) V4.0 ▼ 40.01 /月 来源 网神信息技术(北京)股份有限公司 988 360网油虚拟化下一代防火墙系统是专门为虚拟化环境完全要求设。	
数据库 服务器软件 企业应用		
云安全市场 已购买的镜像		
	上一页 1 下一页	

图 9

五、 后面的操作请参照云市场安装使用说明。

第四章 许可证

4.1. 许可证作用

奇安信vNGFW产品是否可以正常使用由产品的许可证控制,只有购买并安装了相应的许可证以后,用户才能够正常使用产品的相关功能。

4.2. 许可证类型

● 试用许可证:

成功安装③奇安信vNGFW⑨实例以后,它默认自带试用许可证,有效期为30天,支 持的功能和性能与正式许可证相同,功能相关的特征库(IPS、AV、App、URL 等)都可以正常升级,但是使用到期后,vNGFW功能不可用,流经vNGFW的流量 会立即中断,功能相关的特征库不能升级,导入正式许可证后恢复流量通讯。 试用许可证下支持的IPSEC VPN并发用户数是5,SSL VPN并发用户数是5,虚拟

系统是1

● 正式许可证:

成功安装"奇安信vNGFW"实例以后,您可以安装平台正式许可证。正式许可证提供

基础防火墙功能授权、IPS特征库升级授权、AV特征库升级授权、应用识别特征库升级授权、URL过滤库升级授权,正式许可到期后设备所有功能均可用,经过防火墙的流量正常转发,但是功能相关的特征库会无法正常升级。

正式许可证下支持的IPSEC VPN并发用户数是1000, SSL VPN并发用户数是 1000, 虚系统是8

4.3.获得许可证

通过配置的公网IP地址用https的方式登录vNGFW的WEB控制台,默认的用户 名是admin,密码为购买ECS用户自己设置的密码。如图10所示:



图 10

拷贝产品序列号申请正式的许可证。

进入云市场->网络安全在搜索栏输入"奇安信虚拟化下一代防火墙系统-License" 点击进入购买界面,如下图11所示:

DIGI 118	全速重构暖春助力包 %为\$55\$\$\$11\$F 加速入口》 ×
[-] 阿里云 云市场	在北瓜人思惑罪的服务 技会 技会 たがの ための たがの たがの <
云市场分类 云安全市场 > 网络安全 > 防火噴	服务建始API办公软件基础软件新零售容器。安全loT 阿里元心选用户室例新手专区 英家中心▼ 家家中心▼
	下一代防火填系统(1/0优化) 代防火填系统(1/0优化) 代防火填系统是每门为虚拟化环境会全需求设计的网络安全产品,产品功能主要包合安全策略、 指助功能、NAT、LLB、HA、GoS、IPS、AV、URL过速,内容过速等功能 1月 用户评分:★★★★★★ 1月
服务保障 诸勿城下交易!90%的欺诈、剑	8. 资金温歇均由线下交易导致。 保 退 低 优
产品详情 产品价格	· 评论详情(2) 使用指离

图11

在线申请后,许可授权会通过在线方式提供,如有问题可以寻求在线客服、 400电话或售后邮箱咨询。获取许可证后,进入->系统->许可证-导入

导航菜单	許可证	
04 莱纳	■ 見入	
▶ 设定	库名 <u>支持最大</u> 数	导入时间
▶ 管理员	1 56mm 导入正式许可证	2017-03-09 23:07:04
▶ 管理主机	2 应用识别库升级	2017-03-09 23:07:04
▶ 管理证书	3 IPS(WAF)	2017-03-09 23:07:04
► SNMP	4 IPS库升级	2017-03-09 23:07:04
▶ 許可证	5 AV功能	2017-03-09 23:07:04
▶ 升級	6 AV库升级	2017-03-09 23:07:04
▶ 配置文件	7 URL库升级	2017-03-09 23:07:04
▶ 虚拟系统	8 IPsed能道教 5	
▶ 高可用性	9 井炭注接数 1000000	
	10 SSL VPN并发用户数 5	
	11 虚拟系统功能 1	2017-04-08 23:07:04

图 12

第五章 部署案例

5.1. DNAT 网络部署

一、 DNAT模式场景描述

● DNAT全称是目标IP地址或端口转换,vNGFW设备会把原始数据报的目标IP地址 修改成身后所保护服务器的IP地址或端口,起到一个远程接入和安全性保护的作 用。

● VPC网络内的WEB服务器实例只有内网IP地址没有公网地址, Internet用户是无法访问WEB服务器。(见图13所示)

● VPC网络内的vNGFW实例既有公网IP地址,又有内网IP地址。(见图十三所示)

- vNGFW采用IP端口映射的方式为互联网用户提供服务
- 二、 网络拓扑及其数据流



图 13

三、 具体配置

(一) 使用https登录"奇安信vNGFW"进入->网络->NAT->DNAT创建一条名字为"dnat-

http-port80"如图14所示:

SNAT		4764
常規信息		
	名称	dnat-http-port80 (1-63字符)
	描述	(0-127字符)
	日志	8
	启用	8
转换前匹配		
	源地址	● 対象选择 ◎ 輸入IP
		any ·
	目的地址	[◎] 刘翰兹释 ◎ 氟λ P VNGFW 接口地址
		172 . 18 . 220 . 113
	服务	• •
	入接口	gel 🗸 🖌
转换后匹配		所保护的服务器地址
	IP地址	IPv+Httht ▼ 172 . 18 . 220 . 114
	端口	不特殊 💙
		竊定 取消

图 14

Internet用户访问的原始IP地址是119.23.20.79,这个数据报经过IGW设备后它会 修改目的地址119.23.20.79->172.18.220.113,所以在vNGFW的"转换前匹配"的"目的 13 地址"是172.18.220.113而不是公网IP地址。

为了防止vNGFW管理的80端口和DNAT规则的80端口冲突,所以请您把管理防火墙的80端口修改成其他。

(二)进入->安全->安全规则,添加一条安全规则策略放行所需要的数据报,由于 是测试所以添加的是全通的安全规则。如图15所示:

常规信息

名称	any			•	(1-63字符)
描述				(0-	-127字符)
艺力作用	●允许 ● 摺	色 □ 安全连接(隧道)			
启用	V				
源安全域	any		· · · · · · · · · · · · · · · · · · ·	4	
目的安全域	any			× +	
源用户					添加
源地址	◉ 源IPv4	◎ 源IPv6	◎ 源区域		
	any		×	× +	<u>透加</u>
目的地址	◉ 目的IPv4	○ 目的IPv6	◎ 目的区域		
	any		1	× +	<u>27840</u>
服务	any		1	1.	添加
应用	any		1	× *	<u> 选择</u>
入侵防护			1	1	
URL过渡			1	1	
病毒检测				1	
来自隧道			1	1	
时间			1	1	
内容过滤			×	1	
文件过滤			· · · · · · · · · · · · · · · · · · ·	1	
邮件过滤			· · · · · · · · · · · · · · · · · · ·	-	
网络行为管理			· · · · · · · · · · · · · · · · · · ·	1	
VLAN				(8	0值范围0-4094,格式: 1,3,5-10,12)
日志	×				
启用长连接					

图 15

全通安全规则是存在安全隐患的,所以在您实际部署的环境中请您根据具体的需 求,细化安全规则。

(三)进入->阿里云控制台->专有网络VPC->华南1->路由器中添加一条默认路由,下一跳是vNGFW实例,它的作用是把VPC的流量引流到vNGFW上。具体的配置如下图 16所示:

14

虚拟路由列表			
路由醫基本信息			
名称: mm		ID : vrt-wz9q5	b8p7)ysk3aheinma
備注: -			
路由条目列表			添加默认路由
DI専由規	状态	目标网段	T-2
vtb-wz9waxo6cvwjtbjkub55f	可用	0.0.0.0/0	i-wa9enqm2s3ka1 hhyvenin
vtb-wz9waxo6cvwjibpkub55f	可用	172.18.208.0/20	
vtb-wz9waxo6cvwjibpkub55f	可用	100.64.0.0/10	
		图 16	

5.2. SNAT 网络部署

一、 SNAT模式场景描述

● SNAT全称源IP地址转换,即内网地址向外访问时,发起访问的内网IP地址转换为指定的IP地址(可指定具体的服务以及相应的端口或端口范围),这可以使内网中使用保留IP地址的主机访问外部网络,即内网的多部主机可以通过一个有效的公网IP地址访问外部网络。

● 在VPC中WEB服务器是无法主动访问Internet的,所以如果想让VPC中的服务器 实例访问Internet的资源,必须要把流量引入vNGFW中并且匹配SNAT规则,源地 址发生改变后方可访问。(如下图17所示)。

● 引流采用DNAT引流方式,路由器中添加一条默认路由,下一跳是vNGFW实例。

二、 SNAT网络拓扑及其数据流



图 17

15

三、 具体配置

(一) 使用https登录"奇安信vNGFW"进入->网络->NAT->SNAT创建一条名字为"SNAT"

具体配置如下图18所示:

SNAT		AT64	
常规信息			
	名称	snat	★ (1-63字符)
	描述		(0-127字符)
	日志		
	启用		填入web服务器IP
转换前匹配			
	源地址	◎ IPv4对象 ◎ IPv6对象	● 输入IP
		172 . 18 . 220 . 114 🔹	
	目的地址	● 对象选择 ● 输入IP	
		any	✓ +
	服务	any	✓ +
	出接口	any	✓ +
转换后四部			
	地址模式	◉ 动态地址 ── 静态地址	根据路由判断出口。转换出口IP
	类型	BY ROUTE	
		确定 取消	

图 18

● 因为只有一个服务器需要访问Internet资源,所以在"转换前匹配"的IP中填入 172.18.220.114这个32位的主机地址,如果您想让一个地址段访问公网,那么请在 IPV4对象中配置地址段,它需要引用一个地址对象。

● 由于访问Internet资源的多样性,所以在目标地址和服务中选择any,表示所有。

● 类型使用BY_Route的意思是根据路由来判断出接口,源IP地址转成出

接口的IP地址,在vNGFW里能匹配的路由是缺省路由即:0.0.0.0/0.0.0.0网关 172.18.223.253,所以源IP地址转换成和这个网关一个网段的IP地址即: 172.18.220.113

(二)进入->安全->安全规则,添加一条安全规则策略放行所需要的数据报,由于 是测试所以添加的是全通的安全规则。如图十四所示

(三)进入->阿里云控制台->专有网络VPC->华南1->路由器中添加一条默认路由,下一跳是vNGFW实例,它的作用是把VPC的流量引流到vNGFW上。具体的配置如下图19

阿里云-vNGFW上线指导手册

虚拟路由列表

路由醫基本信息			
名称: mm		ID : vit-wz9	15b8p7jysk3aheinma
偏注: -			
路由条目列表			添加默认路由
跳曲地口	扶志	目标网段	₩
vtb-wz9waxo6cvwjitojkub55f	可用	0.0.0.0/0	i-wz9engm2s3ka1hhyvemn
vtb-wz9waxo6cvwjitejkub55f	可用	172.18.208.0/20	-
vtb-wz9waxo6cvwjtojkub55f	可用	100.64.0.0/10	-
		图 19	

5.3. IPSEC VPN 网络部署

一、 IPSEC VPN模式场景描述

● IPSEC VPN作为一项成熟的技术,广泛应用于组织总部和分支机构之间的组网 互联,其利用组织已有的互联网出口,虚拟出一条"专线",将组织的分支机构和总 部连接起来,组成一个大的局域网,既提供了远程接入访问,又通过数据包的加密 形式保障了数据的安全性,已经被广泛使用。

● vNGFW支持IPSEC VPN功能,可以使用这种技术在公司内部网络,或者数据中心和奇安信vNGFW之间建立一个安全的隧道,实现内网之间的资源的安全访问。(如下图20所示)

● 另一种应用场景是通过IPSEC VPN技术在两个或者多个VPC网络间建立安全隧 道实现资源的访问。(如下图21所示)

● Internet用户是通过DNAT技术访问到vNGFW的,如果您使用IPSEC VPN技术被 封装的ESP报文经过NAT设备会有很多问题,vNGFW支持"NAT穿越"技术,可以 解决这一问题。

二、 IPSEC VPN应用拓扑







三、 具体配置

(一) 进入->隧道->IPSec-VPN->IKE网关创建一个IKE网关策略,如下图22所示:

IKE网关	IKE提议	拨号用户组		
基本设置				
	名称	ipsec-to-360		* (1-63字符)
	接口	ge1		*
	本端IP地址	172.18.220.11	3	*
	协商模式	●主模式	◉ 野蛮模式	
网络设置				无法确定对方IP,所以使用动态
	地址模式	◎ 静态地址	◉ 动态地址	◎拨号用户组
	本端ID	○ NULL	U-FQDN	FQDN ASN1DN
	本端ID值	234567		* (1-255字符) 電西本面对古语久
	对端ID	○ NULL	U-FQDN	● FQDN ● ASN1DN 而女须取刈刀以笛
	对端ID值	123456		* (1-255字符) 的1D
IKE提该	(<mark>P1</mark> 提议)	psk-aes128-sha	1-g2	➤ * (网关协商模式为野蛮模式时,只支持1个DH组算法)
	预共享密钥	123456		* (6-31字符)
高级设置				
	连接类型	• 双向	◎ 发起者	◎ 响应者
	NAT穿越		- 一定要	要勾选NAT穿越,否则无法通讯
7	揣存活检测			
		确定	取消	

图22

● 由于无法确定请求者的IP地址,它可能是一个ADSL拨号设备,所以在地址模式中使用了动态IP地址,vNGFW作为被动响应设备。

● 身份标示才有FQDN形式,所以要求您必须知道对方VPN的设备的ID值是多少。

● NAT穿越在当前的网络环境下需要使用。

当vNGFW实例使用NAT穿越时,需要对端的VPN设备也同样的开启NAT穿越功能。 (二)进入->隧道->IPSec-VPN->IPSec隧道,添加一条规则,如下图23所示:

IPSec隧道 IPSec提	й į
基本设置	
名称	ipsec-to-360 * (1-63字符)
IPSec(p2)提议	esp-aes128-sha1-g0
IKE网关	ipsec-to-360
启用	
高级设置	
ID模式	 ● 自动 ● 手动
防重放	●关闭 ○ 32 ○ 64 ○ 128 ○ 256 ○ 512
自动连接	□ ← 由于是被动响应,所以不使用
DHCP over IPSec	
	确定取消

(三)进入->安全->安全规则,添加一条安全规则策略放行所需要的数据报,由于 是测试所以添加的是全通的安全规则。如图24所示。

(四) 配置对端VPN设备,请参照相应产品的操作手册进行配置。

以上配置仅实现当公司内网或者数据中心主动发起流量的互通,如果您在VPC的服务器中主动发起访问公司内网是不通的,原因是流量不是感性数据流不能做到VPN流程。如果您有VPC内网主动访问的需求,请加一条匹配VPN的安全规则,如下图二十四所示:

安全策略	会话设置	策略冗余分析				
常规信息						
	名称	ipsec-to-ipsec			*	(1-63字符)
	描述				(0-	127字符)
	动作	● 允许 ● 拒约	色 💿 安全连接(隧道	i) 👉	_	
	隧道(VPN)	ipsec-to-360	使用VPN隙	道并引用	*	
	启用					
	源安全域	any		~	*	
	目的安全域	any		~	*	
	源用户					添加
	源地址	◉ 源IPv4	◎ 源IPv6	◎ 源区域		
		172.18.220.114		~	*	添加
	目的地址	◉ 目的IPv4	○ 目的IPv6	◯ 目的区域		
		192.168.10.2		~	*	添加
	服务	any		~	*	添加
	应用	any		~	*	<u>洗择</u>
	· ·····					

图24

新添加的VPN规则需要移动顺序到全通安全规则之前,否则无法匹配。

(五)进入->阿里云控制台->专有网络VPC->华南1->路由器中添加一条默认路由,下一跳是vNGFW实例,它的作用是把VPC的流量引流到vNGFW上。具体的配置如下图25所示:

虚拟路由列表				
路由器基本信息				
名称: mm		ID : vrt-wz9q5b	8p7jysk3ahelnma	1
备注: -				
路由条目列表			添加默认路由	
路由表ID	状态	目标网段	下一部	
vtb-wz9waxo6cvwjitqkub55f	可用	0.0.0/0	i-wz9enqm2s3ka1hhyvemn	
vtb-wz9waxo6cvwjitqkub55f	可用	172.18.208.0/20	-	
vtb-wz9waxo6cvwjitqkub55f	可用	100.64.0.0/10	-	
		团 25		

图25

5.4. SSL VPN 网络部署

一、 SSLVPN模式场景描述

● SSL VPN比较适合用于移动用户的远程接入(Client-Site), IPsec VPN多用于 "网—网"连接, SSL VPN用于"移动客户—网"连接。SSL VPN用户需安装客户端程 序,即可通过SSL VPN隧道接入内部网络,且对客户端设备要求低,因而降低了配 置和运行支撑成本。很多企业用户采纳SSL VPN作为远程安全接入技术,主要看重 的是其方便的接入能力。

● 奇安信vNGFW实例的SSL VPN功能只需要维护中心节点的网关设备,客户端 免维护,降低了部署和支持费用。

● 奇安信vNGFW的SSL VPN功能更容易提供细粒度访问控制,支持本地用户认证外,还与第三方认证系统(如: Radius、AD等)结合更加便捷。

● 奇安信vNGFW获取SSL VPN客户端的形势简单快捷,您只需要在浏览器输入 *https://IP:64443*。安装客户端即可。

二、 SSLVPN应用拓扑及其数据流





三、 具体配置

(一) 进入->用户认证->认证用户,添加一个认证用户,如下图27所示:

认证用户	认证用户组	认证用户角色	
基本设置			
	名称	test	◆ (1-63字符)
	密码	*******	* (1-31字符)
	确认密码	********	• (1-31字符)
	有效日期	2017/03/31 10:08	<u> </u>
	描述		
		确定 取消	在该时间内有效
		确定	



有效日期必须和当前的系统时间匹配。

(二)进入->用户认证->认证服务器->local,编辑本地认证服务器,增加"test"这个用户,如下图28所示:

认证服务器							
基本设置							
22044 OCEA	名称	local			•	(1-63字符)	
	**#	🔍 च्ह्रेन्स्रेस् क्रि	Podius				<u>ि स</u> 1941 स
	突出。 (表表:n田 合	◎ 用合		aa		~ NU	- NETPIKNE
	xxIII.E.P	© д ,⊢	○ HI/THE	▽用巴			
		▲ 批重绑定	1) 批量辭除炯定				
		- 名称	~ 使用绯	『 定功能		状态	
		1 🗌 wangli				已绑定	
		2 🗹 test				绑定成功	
		20 -		#4 .	1.00		
		20 4	「黒」」の	жир 💌 М	0		第1余皇弟(余)共(余)

图 28

(三)由于在SSL协议交互的时候需要使用到非对称加密技术-数字证书,奇安信 vNGFW支持自签发数据证书:

1. 自签发CA根证书

进入->PKI->本地CA->本地CA,使用"生成自签发CA"功能,如下图29所示:

本地CA	CRL
------	-----

配置信息	
版本	V3
序列号	CCBB5E996436E711
主题信息	C=CN, ST=beljing, L=beljing, O=360, OU=qa, CN=360-lengedsec, emailAddress=
颁发者	C-CN, ST-beijing, L-beijing, O-360, OU-qa, CN-360-lengedsec, emailAddress-
签发时间	2017-03-11 00:24:50
过期时间	2027-03-09 00:24:50
签名算法	sha1WithRSAEncryption
MD5指纹值	27:DD:90:5B:31:99:48:46:1C:11:C4:79:32:B2:1D:F3
SHA1指纹值	34:20:78:56:28:2C:13:81:79:ED:25:A8:90:EC:D5:57:8D:99:1E:67
	异出PEM格式 异出DER格式

图 29

2. 生成"一般证书"

这个证书生成后系统会使用CA证书为这个"一般证书"签名,这个过程是系统自动完成,不需要您手工配置。

进入->PKI->本地CA->一般证书,生成一般证书,如下图30所示:

一般证书		
配置信息		
	名称	8888
	版本	V3
序	列号	CCBB5E996436E712
主题	信息	C=CN, ST=beijing, L=beijing, O=360, OU=tiandi, CN=8888, emailAddress=
颔	发者	C-CN, ST-beijing, L-beijing, O-360, OU-qa, CN-360-lengedsec, emailAddress-
盗发	时间	2017-03-11 00:26:55
过期	时间	2017-09-07 00:26:55
签名	算法	sha1WithRSAEncryption
MD5指	統值	D6:79:8C:A2:72:7A:14:F1:16:58:AA:0C:60:29:D3:A8
SHA1措	纹值	F9:65:35:8A:25:32:F7:E7:C7:F2:28:EB:85:3C:00:11:3F:7D:E7:90

图 30

3. 导入可信CA

进入->**PKI-**>证书管理->可信**CA-**>导入,从本地CA中心导入CA证书,如下图31所示:

可信CA		
配置信息		
	名称	test * (1-63字符,例如 text-1_v1.0.txt)
	导入方式	● 从本地C4中心 ── 上传文件
		导入本地CA证书
		确定 取消

图 31

4. 导入本地证书

进入->**PKI**->证书管理->证书列表->导入,从本地CA中心导入**一般证书,如下图**32 所示:

证书列表		
配置信息		
	名称	test123 * (1-63字符,例如 text-1_v1.0.txt)
	导入方式	◎ 从本地CA中心 ◎ Lté文件 选择本地证书
	一般证书	8888
	可信CA	test
		选择根CA
		确定现消

图 32

(四)进入->隧道->地址池,创建一个用户SSL VPN的地址池,这个地址池地址就

是SSL VPN客户端的虚拟IP地址。如	日卜图3	3
----------------------	------	---

基本设置



确定 取消



进



SSLVPN									
基本设置									
	名称	ssl-vpn			*	(1-63字符)			
	接口	ge1			*				
	本端P地址	172.18.220.113			× *				
	演口	64443			*	(1025-65533	5)		
	客户湍地址池	ssl-vpn			× +	←引)	用地址沿	也	
	启用	•							
证书设置									
	服务器证书	test123			v *	← 引	用证书		
认证设置									
	认证方式	🖲 单因子认证 🔍 双因子认	证						
	认证服务器	local			× *	(当选择证书)。	\证服务器后, }	默认开启客户端	(证书认证)
网络设置									
	可访问网络	目的地址。	子网	网摘码		- 跃点数		(1-9999)	+
		目的地址		子阿掩码			跃点数	操作	
		172.18.220.114		32			1	Ċ	
					填入	服务器	IP地址		

图 34

(五)进入->安全->安全规则,添加一条安全规则策略放行所需要的数据报,由于 是测试所以添加的是全通的安全规则。如图十四所示。

(六) 进入->阿里云控制台->专有网络VPC->华南1->路由器中添加一条默认路由,

下一跳是vNGFW实例,它的作用是把VPC的流量引流到vNGFW上。具体的配置如下图35所示:

虚拟踏曲列表

路由醫基本信息				
名称: mm		ID : vrt-wz9q5b8p	7)ysk3aheInma	1
留注: -				
路由条目列表			添加默认路由	
加由寺田	状态	目标网段	下一款	
vtb-wz9waxo6crwjitqkub55f	可用	0.0.0.0/0	I-wz9engm2s3ka1hhyvemn	
vtb-wz9waxo6crwjtbgkub35f	可用	172.18.208.0/20	· ·	
vtb-wz9waxo6cvwjttqkub55f	可用	100.64.0.0/10		
		图 35		

(七)远程客户端操作:

1. 在客户端浏览器输入*https://119.23.20.79:64443*,后下载vNGFW的SSL VPN客户端程序,如下图36所示:

- Windows Internet Explorer		
🖉 https://119.23.20.79:64443/	▼ 😵 证书错误 🔝 <	ŝ,
👍 🔊 建议网站 🔻 💋 网页快讯军 🔻		Ī
5	🗋 🗝 t	5

下载		
	22FAh M 盐白噪	请下载
	点击下载	

图 36

2. 安装完成后运行客户端程序,输入IP地址和端口号,端口号默认为64443,如下 图37所示:

		×
地址	119.23.20.79	
端口	64443	
	连 接	

3. 连接成功后请输入用户名密码,验证成功后客户端会分配到虚拟的IP地址,如下图38所示:

〜 隧道信	; 浪	山山 流量统i	#	。 	×
公网信息			私网信息		
服务器地址	119.23.20.79		IP地址	192.168.4.10	
服务器端口	64443		子网掩码	255.255.255.0	
本地地址	172.24.203.10	1	DNS		
			WINS		
加密信息			用户信息		
密码组合	AES-256+SHA	1	用户名		

图 38

4. 在客户端上访问服务器测试连通性,如下图39所示:

🚾 C:{Windows\system32\cmd.exe	
正在 Ping 172.18.220.114 具有 32 字节的数据: 来自 172.18.220.114 的回复: 字节-32 时间-38ns TTL-64 来自 172.18.220.114 的回复: 字节=32 时间=38ns TTL=64 来自 172.18.220.114 的回复: 字节-32 时间=38ns TTL=64	*
172.18.220.114 的 Ping 统计信息: 数据包: 已发送 = 3, 已接收 = 3, 丢失 = 0 (6z 丢失), 往返行程的估计时间(以毫秒为单位): 最短 - 36ms, 最长 - 38ms, 平均 - 38ms Conteol-C	
^C C:\Users\ierruvang>ning 172.18.220.114	
正在 Ping 172.18.220.114 具有 32 字节的数据: 来自 172.18.220.114 的回复: 字节=32 时间=40ns TTL=64 来自 172.18.220.114 的回复: 字节-32 时间=36ns TTL=64 来自 172.18.220.114 的回复: 字节=32 时间=36ns TTL=64 来自 172.18.220.114 的回复: 字节=32 时间=36ns TTL=64	
172.18.220.114 的 Ping 统计信息: 数据包: 已发送 – 4, 已接收 – 4, 丢失 – 0 (0% 丢失), 往返行程的估计时间<以毫秒为单位>: 最短 – 36ms, 最长 – 40ms, 平均 – 37ms	
C:\Users\jerrywang}	-

图 39

如果您对奇安信vNGFW的使用还有任何疑问请联系在线客服、400电话或直接邮件售后咨询。