Hillstone Networks, Inc.

SG6000-VM 虚拟防火墙安装手册

Version 5.5R1P1



Copyright 2015Hillstone Networks, Inc.. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Hillstone Networks, Inc..

Hillstone Networks, Inc.

联系信息

公司总部(北京总部): 地址:北京市海淀区王庄路一号清华同方科技广场D座6层 邮编: 100083 联系我们:<u>http://www.hillstonenet.com.cn/about/contact_Hillstone.html</u>

关于本手册

本手册介绍Hillstone Networks, Inc. 公司的虚拟防火墙系统的安装方法。 获得更多的文档资料,请访问:<u>http://www.hillstonenet.com.cn/service/documentation.html</u> 针对本文档的反馈,请发送邮件到:<u>hs-doc@hillstonenet.com</u>

Hillstone Networks, Inc.

www.hillstonenet.com.cn

TWNO: TW-VFW-UNI-5.5R1P1-CN-V1.0-6/17/2015

发布日期: Wednesday, June 17, 2015

目录

日会	1
山水 介辺	1
11日	1
又怕內谷	1
日 你 佚 白	1
迫用功 <u>京</u>	T
产品列表	1
虚拟防火墙的功能	2
许可证	3
许可证机制	3
平台类许可证	3
功能服务类许可证	3
申请许可证	4
安装许可证	4
在KVM上部署SG6000-VM	6
系统要求	6
虑拟防火墙的工作原理	6
准备工作	6
(作用工)「・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	7
	7
少骤─ · 须取购入恒铁什也 · · · · · · · · · · · · · · · · · · ·	7
び振二・守八卿平和余筑乂十 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	0
	0
	9
	9
步骤→: 注	10
具他操作	10
查看虚拟防火墙	10
启动虚拟防火墙	11
关闭虚拟防火墙	11
升级虚拟防火墙	11
重启虚拟防火墙	12
卸载虚拟防火墙	12
访问虚拟防火墙的WebUI界面	12
在Openstack上部署SG6000-VM	13
系统要求	13
安装步骤	13
步骤一:导入镜像文件	13
步骤二:创建云主机类型(Flavor)	14
步骤三:创建云硬盘	16
步骤四:创建网络	17
步骤五:启动实例	18
访问SG6000-VM虚拟防火墙	18
在VMware ESXi上部署SG6000-VM	20

支持的部署场景	
系统要求和限制	
部署防火墙	
安装防火墙	
第一步:导入ISO文件	
第二步:创建虚拟机	
第三步:选择ISO文件	23
第四步:加入网络	
启动和访问虚拟防火墙	
防火墙初始配置	
在AWS上部署SG6000-VM	
AWS介绍	
位于AWS的SG6000-VM	
场景介绍	
vFW作为互联网网关	
vFW作为VPN网关	
服务器负载均衡	
准备您的VPC	
第一步: 登录AWS账户	
第二步:创建私有云(VPC)	
第三步:为VPC添加子网	
第四步:为子网添加路由	
安装虚拟防火墙	
创建防火墙实例	
第一步:创建EC2实例	
第二步:为实例选择AMI模板	
第三步:选择实例类型	
第四步:配置实例详细信息	
第五步:添加存储	
第六步:标签实例	
第七步:配置安全组	
第八步:启动实例	
配置子网和接口	40
分配弹杆IPmt	<u>م</u> ا
	۰۰- ۸۵
示用波山叭凉/ 口叭心址や狭	

	在主控台查看实例	. 41
ì	前回虚拟防火墙	. 41
	通过SSH访问CLI界面	.42
	访问WebUI界面	. 42
	配置虚拟防火墙	43
测	式	. 46
Ê	J建测试用虚拟机(Windows)	. 46
	第一步:创建VPC子网	. 46
	第二步:修改路由表	. 46
	第三步:创建EC2实例。	. 47
	第四步:连接测试实例	. 48
	第五步:创建DNAT规则	. 49
	(可选)第六步:创建SNAT规则	.49
Ŧ	开始测试	50
	测试一:远程连接虚拟服务器	. 50
	测试二:虚拟服务器访问公网	. 52
	测试三:查看防火墙进出站流量	. 52

山石网科的虚拟防火墙产品,简称为SG6000-VM(Virtual Firewall),是一个纯软件形态的产品,是运行在虚拟机上的StoneOS系统。

文档内容

本手册介绍如何将SG6000-VM虚拟防火墙部署到不同的环境中,包括KVM、Openstack、AWS和VMware中。本文仅讲述安装防火墙和 初始的联网操作,StoneOS系统本身的功能将不做讲解。

如果您需要了解StoneOS系统的详细功能,请参考StoneOS的相关文档(<u>点击此处</u>)。

目标读者

本文的目标读者为企业的网络管理员或对山石网科虚拟化感兴趣的读者。部署之前,根据不同的部署场景,用户需要相应地熟悉KVM、 Openstack、AWS或VMware的组件及使用。本手册以读者已经掌握虚拟化知识为前提,将只介绍与部署虚拟防火墙有关的操作。

适用场景

- 1. 在单台硬件设备上部署虚拟防火墙,建议使用KVM部署方式。请参考"在KVM上部署SG6000-VM"在第6页。
- 2. 使用Openstack的方式为企业已有的私有云部署虚拟防火墙,请参考"在Openstack上部署SG6000-VM"在第13页。
- 3. 如果企业需要在亚马逊云服务(AWS)的VPC子网构建虚拟防火墙,请参考"在AWS上部署SG6000-VM"在第29页。
- 4. 在ESXi Server主机上的部署虚拟防火墙,请参考"在VMware ESXi上部署SG6000-VM"在第20页。

产品列表

SG6000-VM系列虚拟防火墙共包含两款产品:SG-6000-VM01和SG-6000-VM02,他们的性能和参数列表如下:

性能参数	SG6000-VM01	SG6000-VM02
内核(最低/最高)	1/1	2/2
内存 (Gbps)	1 G	2 G
防火墙吞吐量(1518 Bytes)	2 Gbps	4 Gbps
最大会话	100 K	500 K
每秒新建会话	10 K	20 K
IPS吞吐量(1280 Bytes)	200 Mbps	400 Mbps
接口最大数	10 x virtual nics	10 x virtual nics
IPSEC VPN 隧道最大数/隧道接口最大数	50	500
SSL VPN用户数(默认/最大)	5/50	5/250

性能参数	SG6000-VM01	SG6000-VM02
安全域最大数量	16(包括8个预定义安全域)	16(包括8个预定义安全域)
策略规则最大数量	1000	1000
地址簿对象最大数量	512	512

虚拟防火墙的功能

SG6000-VM支持以下防火墙功能:

- ≫ 基本防火墙(策略、安全域、NAT等基础防火墙功能)
- ≫ 应用识别
- » 攻击防护(AD)
- ≫ 入侵防御(IPS)
- >> VPN (IPSec VPN、SSL VPN)
- » 用户管理
- ≫ 访问控制
- ≫ 高可用性(HA)
- » LLB负载均衡
- » 管理功能
- » _{日志}
- [≫] 统计集
- » iQoS

SG6000-VM虚拟防火墙产品的性能,由许可证的控制。只有购买并安装了相应的许可证,才能使产品达到其标称的数值。购买许可证, 请与销售人员联系。

许可证机制

与Hillstone Networks, Inc.的硬件防火墙产品类似,虚拟防火墙的许可证机制也分为平台许可证和功能服务类许可证。平台许可证是功能服务类许可证运行的基础。

平台类许可证

>>> 平台试用许可证(Platform Trial)

安装平台试用许可证后,支持的功能和性能与正式许可证相同,但是使用期限较短。具体可用时长,根据申请时协议决定。 到期后,已有的配置不能修改,若设备重启,防火墙恢复到默认许可证(default)控制的状态,受限的性能将重新受限。

≫ 平台正式许可证(Platform Base)

设备正式销售后,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和VPN功能,并且防火墙性能可达到标称数值。 到期后,设备恢复到默认许可证的状态,此后设备仍可正常使用,但不能升级到期后的OS版本。

≫ 默认许可证(Default)

虚拟防火墙预装了一个免费的默认许可证(default license),无需申请。该许可证长期有效。 使用默认许可证,系统功能的种类与使用正式许可证相同,只是性能受限,如下:

- ≫ 防火墙吞吐(1518 Bytes):100 Mbps
- ≫ 防火墙吞吐(64 Bytes):10 Mbps
- 最大会话:1K
- » 每秒新建会话:1K
- ≫ IPSec 吞吐量 512 包: 10 Mbps
- » IPSec VPN 隧道数:0
- » SSL VPN用户数:0
- » 最大策略数量:50
- » 最大地址簿数量:100

功能服务类许可证

只有购买并安装了各个功能服务类许可证,用户才能使用相应的功能,并能够获取特征库更新。

SSL VPN 许可证

授权SSL VPN的最大接入数量。多个SSL VPN许可证可以叠加允许接入用户的最大数量。没有单独的使用期限,过期时间与vFW所使用的平台许可证相同。

》 QoS许可证

开启QoS功能。没有单独的使用期限,过期时间与vFW所使用的平台许可证相同。

» 入侵防御(IPS) 许可证

提供入侵防御功能和IPS特征库升级。具有单独的使用期限。过期后,不能升级IPS特征库,入侵防御功能正常使用。

APP DB 许可证

提供APP库升级功能。APP DB许可证不需要单独申请,随平台许可证一同发放,有效期也同平台类许可证。 过期后,不能升级APP 特征库。



Note: URL DB功能和边界流量过滤(PTF)功能在界面上可见,但这两个功能暂时不生效,后续版本将支持。



Note:除了上面列出的许可证外,硬件防火墙所支持的其他许可证(如StoneShield),vFW暂不支持。

申请许可证

申请许可证,需要登录StoneOS系统。按照您的部署场景的不同,请参考不同的防火墙安装方法(<u>KVM</u>、<u>Openstack</u>、<u>AWS</u>或<u>VMware</u> <u>ESXi</u>)。

部署好虚拟防火墙后,访问StoneOS的WebUI界面,然后按照以下步骤生成许可证申请:

- 1. 登录StoneOS系统。
- 2. 选择"系统 > 许可证",进入许可证页面。
- 3. 在"许可证申请"中,填写生成许可证请求所需要的信息。
- 4. 点击"生成",出现一串代码。
- 5. 将生成的代码发送给销售人员,由其获取许可证再返回给您。

安装许可证

获得许可证后,用户需要将其装载到设备上使其生效。安装许可证,请按照以下步骤进行操作:

- 1. 选择"系统 > 许可证",进入许可证页面。
- 2. 在"许可证申请"中,用户可根据需要,以下以下两种方式中的一种导入许可证。
 - 上传许可证文件:选中"上传许可证文件"单选按钮,点击"浏览"按钮,并且选中许可证文件(许可证为纯文本.txt文件)。
 - >> 手动输入:选中"手动输入"单选按钮,然后将许可证字符串内容粘贴到文本框中。
- 3. 点击"确定"按钮保存所做配置。

在KVM上部署SG6000-VM

使用基于内核的虚拟机(Kernel-based Virtual Machine,缩写为KVM)部署山石网科虚拟防火墙,是在单机上创建虚拟防火墙的主要方 法。

系统要求

在KVM上部署山石网科的虚拟防火墙,需要宿主机满足以下要求。

- ≫ 支持Intel VT 或者 AMD-V
- >>> 至少能够分配2个虚拟网卡
- ≫ 64位CPU, CPU能虚拟两个内核
- Linux操作系统(推荐使用Ubuntu 14.04版本)
- 使用单机KVM环境:系统已安装软件KVM、qumu、bridge-utils、uml-utilities、libvirt、virtinst、virt-viewer和virt-manager。 (安装命令:sudo apt-get install kvm qemu bridge-utils uml-utilities libvirt-bin virtinst virt-manager virt-viewer)

虚拟防火墙的工作原理

将虚拟防火墙的虚拟网卡对应的tap接口连接到宿主机中的虚拟交换机(ovs或者Linux bridge),虚拟机把虚拟防火墙设置为默认网关, 虚拟防火墙就可以转发来自不同虚拟机或者物理网卡的流量。



准备工作

安装山石网科虚拟防火墙之前,用户已经具有Linux主机,且已经安装KVM和KVM的管理组件(包括qemu、bridge-utils、uml-utilities、libvirt、virtinst、virt-viewer和virt-manager)。

在Linux系统中输入以下安装命令安装这些组件:

sudo apt-get install kvm qemu bridge-utils uml-utilities libvirt-bin virtinst virt-manager virt-viewer.

安装步骤

在KVM主机上创建虚拟防火墙,按照下面的步骤进行操作:

步骤一:获取防火墙软件包

- 1. 联系客服人员获取下载防火墙软件包的地址。
- 2. 下载以下文件:
 - » 脚本文件(名称为"hsvfw")。脚本文件包含一些针对vFW系统文件的操作,例如安装、升级、重启vFW等。
 - >>> vFW系统文件(后缀名为iso的镜像文件,例如 "SG6000-VFW02-V6-r1230.iso")。

步骤二:导入脚本和系统文件

该步骤以使用Windows系统访问KVM主机为例介绍如何导入脚本文件和系统文件。

1. 在Windows系统下,登录KVM,输入以下命令,系统打开对话框窗口。

rz

2. 在对话框中浏览本地PC,选择脚本文件和防火墙的系统文件,将其上传到KVM服务器的根目录上。

例如:

hillstone@vfw:~\$ rz	
rz waiting to receive.	
Starting zmodem transfer. Press Ctrl+C to a	cancel.
Transferring SG6000-MX_MAIN-VFW02-V6-r1230.	iso
100% 78180 KB 3127 KB/s 00:00:25) Errors

3. 输入以下命令,查看根目录的文件列表。

ls

4. 如果出现脚本文件和系统镜像文件,说明已经上传成功。

例如:

hillsto	one@vfw:~\$	ls
hsvfu	SG6000-MX_	MAIN-VFW02-V6-r1230.iso

5. 输入以下命令,安装系统文件。

sudo ./hsvfw install ./vfw_iso [vm01|vm02] vm_name if_num

sudo	代表该命令使用管理员权限。
./hsvfw install	执行位于根目录的脚 本文件 (hsvfw) 的安装命 令。

./vfw_iso	安装位于根目录的系统文件。vfw_iso是系统镜像
	文件的全名,包括后缀名.iso。
vm01 vm02	虚拟防火墙的产品型号,vm01代表SG-6000 VM01
	型号, vm02代表SG-6000-VM02型号。
vm_name	为当前安装的虚拟防火墙指定一个名称。
if_num	为当前安装的虚拟防火墙分配接口数量,最多可划
	分出10个接口。

例如,输入以下命令,创建产品类型为VM02,名称为vfwname,具有2个接口的虚拟防火墙。

hillstone@vfw:~* <u>sudo</u> ./hsvfw_install/SG6000-VFW00-5.0R0-D0203.iso_vm02_vfwname_2
[sudo] password for hillstone:
1+0 records in
1+0 records out
1048576 bytes (1.0 MB) copied, 0.00199942 s, 524 MB/s
Network vfwname-eth0 defined from /var/lib/vfw/vfwname/vfwname-eth0
Network vfwname-eth0 marked as autostarted
Network vfwname-eth0 started
Network vfwname-ethl defined from /var/lib/vfw/vfwname/vfwname-ethl
Natural Communication and an extension
Network VfWname-etni marked as autostarted
Network ufuname-eth1 started
Starting install
Creating domain
error: XDG_RUNTIME_DIR not set in the environment.
Cannot open display:
Run 'virt-viewerhelp' to see a full list of available command line options
Domain creation completed. You can restart your domain by running:
virshconnect gemu:///system start vfwname
vFW vfwname installed.
Console access: telnet localhost 7014
SSH access: ssh_hillstone@192.168.144.2
hillstone@vfw:~≉ ■

6. 执行上一个命令后,Linux界面将输出Console接口的端口号,如上例中的7014。

步骤三:首次登录防火墙

刚安装的防火墙默认只开启了Console口的访问权限,可以通过访问该Console口,登录防火墙。

按照以下的步骤初次登录防火墙。

1. 在Linux中输入以下命令,连接防火墙。

telnet localhost port_num

port_num

例如,连接上一步骤创建的Conosole端口为7014的虚拟防火墙,输入以下命令。

```
hillstone@vfw:~$ telnet localhost 7014
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is ´^]´.
login:
```

2. 输入防火墙默认的用户名和密码。

```
login: hillstone
password: hillstone
```

3. 至此,你可以使用命令行界面对防火墙系统进行操作。建议您及时修改用户名和密码。

将vFW联网

当虚拟防火墙创建后,虚拟防火墙的每个接口自动成为一个虚拟网桥,并且该接口自动与KVM的一个vnet接口连接。若要将防火墙的与其 他网络(如私网或互联网)连接,将防火墙的vnet接口与其他网络的接口放置于同一个虚拟网桥下,即可以实现连接。

以下图为例,介绍如何将虚拟防火墙的vnet0接口与物理网络的90-eth0口连通。



步骤一:查看接口的信息。

本例中,一个物理网络(比如公司内网)与KVM宿主机的物理接口连接。您可以首先查看KVM宿主机的接口和vFW的接口信息。

1. 在Linux中,使用命令ifconfig查看接口,宿主机的物理接口为90-eth0:

	<u>illsto</u> pe@vfw:~≉ ifconfig
(0-eth0 Link encap:Ethernet HWaddr 52:54:00:ed:3e:e6
	inet addr:192.168.221.1 Bcast:192.168.221.255 Mask:255.255.255.0
	UP BROADCAST MULTICAST MTU:1500 Metric:1
	RX packets:0 errors:0 dropped:0 overruns:0 frame:0
	TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:0
	RX butes:0 (0.0 B) TX butes:0 (0.0 B)

2. 在Linux中输入命令brctl show查看虚拟网桥和接口。

该信息中,虚拟防火墙的"eth0"接口自动对应KVM的vnet接口"vnet74",并自动属于同一个网桥"vfwname-eth0"。物理接口自动从属于网桥"90-eth0"。

步骤二:连接接口

将防火墙接口与物理网络的接口设置为从属于同一个虚拟网桥下,这两个网络即可以互相通信。

按照以下步骤,将虚拟防火墙的 "vnet74" 接口与物理网络的 "90-eth0" 接口连接:

- 在Linux中,输入以下命令,将 "vnet74" 接口从原虚拟网桥 "vfwname-eth0" 中删除。 sudo brctl delif vfwname-eth0 vnet74
- 将刚刚被删除网桥的接口,添加到另一个接口所属的网桥下。 sudo brctl addif 90-eth0 vnet74
- 3. 输入命令brctl show,确认两个接口属于同一个虚拟网桥。

hillstone@vfw:~* brctl show bridge name 90-eth0 8000,525400ed3ee6	STP enabled yes	interfaces 90-eth0-nic vnet74
--	--------------------	-------------------------------------

4. 至此,这两个接口所连接的网络可以互相通信。

其他操作

查看虚拟防火墙

查看防火墙信息,使用以下命令:

sudo ./hsvfw show vm_name

./hsvfw show	执行脚本文件 (hsvfw)的查看命令。	
vm_name	虚拟防火墙的名称。	

例如,在Linux中查看名称为"vfwname"的虚拟防火墙:

hillstone@vfw:~≉ ./hsvfw show vfwname				
VFW instanc	e: 14			
VFW instanc	e name: vf⊍	name		
Version: SG	6000-VFW00-	-5.0R0-D0203	3.iso	
Status: run	ning			
Console por	t: 7014			
VNC port: :	16			
Mgmt address: 192.168.144.2				
Interface c	ount: 2			
Interface d	etail:			
Interface	Туре	Source	Model	MAC
vnet74 vnet75	network network	vfwname-et vfwname-et	nO virtio n1 virtio	52:54:00:0e:12:00 52:54:00:0e:12:01

启动虚拟防火墙

将已经安装在KVM系统中的防火墙启动,使用以下命令:

sudo ./hsvfw start vm_name

./hsvfw start	执行脚本文件 (hsvfw) 的启动命令。
vm_name	虚拟防火墙的名称。

关闭虚拟防火墙

要关闭虚拟防火墙,输入以下命令:

sudo ./hsvfw shutdown vm_name

./hsvfw shutdown	执行脚本文件(hsvfw)的关闭命令。
vm_name	虚拟防火墙的名称。

升级虚拟防火墙

升级防火墙的系统,按照以下步骤:

- 1. 上传新的镜像文件。
- 2. 输入以下命令开始升级。

```
sudo ./hsvfw upgrade vm_name ./new_vfw_iso
```

./hsvfw upgrade	执行脚本文件(hsvfw)中的升级命令。	
vm-name	被升级的虚拟防火墙的名称。	
./new_vfw_iso	新的系统镜像文件名称,包括.iso后缀名。	

重启虚拟防火墙

要重启虚拟防火墙,使用以下命令:

sudo ./hsvfw reboot vm_name

./hsvfw reboot	执行脚本文件 (hsvfw) 的重启命令。
vm_name	虚拟防火墙的名称。

卸载虚拟防火墙

要卸载已经安装的虚拟防火墙系统,使用以下命令:

sudo ./hsvfw uninstall vm_name

./hsvfw uninstall	执行脚本文件(hsvfw)的卸载命令。
vm_name	虚拟防火墙的名称

访问虚拟防火墙的WebUI界面

虚拟防火墙的第一个虚拟接口(eth0/0)默认开启DHCP,如果防火墙连接到启动了DHCP的网络,eth0/0口将自动获得IP地址。通过浏 览器访问eth0/0的地址,即可打开WebUI界面。

具体步骤如下:

- 1. 参考上述""在KVM上部署SG6000-VM"在第6页"的方法,使用Telnet命令登录防火墙。
- 2. 登录后,输入以下命令,查看eth0/0接口的IP地址。

show interface ethernet0/0

- 3. 打开浏览器(建以使用Chrome浏览器), 输入上面显示的IP地址。
- 4. 输入用户名密码(默认为hillstone/hillstone)
- 5. 点击"登录"按钮,进入虚拟防火墙的WebUI管理界面。
- 6. 关于如何使用StoneOS系统,参考StoneOS的配置文档(<u>点击此处</u>)。

在Openstack上部署SG6000-VM

系统要求

在Openstack上部署山石网科的虚拟防火墙,需要宿主机满足以下要求。

- ≫ 支持Intel VT 或者 AMD-V
- >>> 至少能够分配2个虚拟网卡
- » 64位CPU, CPU能虚拟两个内核
- Linux操作系统(推荐使用Ubuntu 14.04版本)
- PE经安装Openstack (icehouse版本),及其组件Horizon, Nova, Neutron, Glance和Cinder。(Openstack的安装方法按照 http://docs.openstack.org/icehouse/install-guide/install/apt/content/)

安装步骤

步骤一:导入镜像文件

- 1. 输入以下命令,对话框自动打开,选取防火墙的系统文件,将其上传到您的Linux终端的根目录中。 rz。
- 2. 输入以下命令,将防火墙系统文件导入到Openstack中作为一个镜像。

glance image-create --name=image-name --property hw_vif_model=virto --disk-format=iso --container-format=bare --is-public=true <vfw iso</pre>

glance image-create	将文件导入到Openstack中。
name=image-name	自定义镜像名称。
property	镜像文件的属性。
hw_vif_model=virtio	限定网卡的类型定义为virtio。
disk-format=iso	导入文件的格式为iso。
container-format=bare	指不对镜像做封装。
is-public=true	对所有租户可见。
vfw_iso	虚拟防火墙系统文件的全名,包括后缀名.iso。

例如,创建名为"image-vfw"的镜像,输入命令:

glance image-create --name=image-vfw --property hw_vif_model=virtio --disk-format=iso --container-form-

at=bare --is-public=true <SG6000-MX_MAIN-VFW02-V6-r1230.iso

返回结果如下:

Property	Value
Property 'hw_vif_model'	+
checksum	a1c764edc703654e230ca04f1b4ddc73
container_format	l bare
created_at	2015-01-08T08:59:37
deleted	I False
deleted_at	I None
disk_format	liso
id	4d1e1c30-4eec-4b67-9072-686a1ac24fd9
is_public	l True
min_disk	10
min_ram	10
name	l image-vfw
owner	l a925cd9e37e0496fb5e535ad4bbf99c4
protected	False
size	1 80056320
status	l active
updated_at	2015-01-08T08:59:39
virtual_size	I None

步骤二:创建云主机类型(Flavor)

一般情况下,非管理员不能直接修改实例的属性参数(例如内核、内存等信息),只有通过将实例与一个云主机类型(Flavor)绑定,才 能继承云主机类型的属性。

使用管理员账户,创建云主机类型:

1. 使用管理员帐户,登录Openstack的Web管理界面。

орепятаск			
Log In			
User Name			
Password			
Sign In			

2. 从左侧导航栏选择 "管理员 > 系统面板 > 云主机类型 (Admin > System Panel > Flavors)"。



3. 点击右上角"创建云主机类型(Create Flavor)"按钮。

Filter + Crainte Flavor	💼 Delete Flavors
-------------------------	------------------

4. 在弹出的 < 创建云主机类型 > 对话框,进行设置。

Create Flavor		ж
Flavor Info * Flavor Access		
Name *	From here you can create a new flavor to organize instance resources.	
ID		
auto		
VCPUs *		
RAM MB *		
Root Disk GB *		
Ephemeral Disk GB *		
Swap Disk MB *		
	Cancel Create Fla	vor

在<云主机类型信息>标签页设置基本信息。

Name	自定义云主机名称。
ID	ID号码由Openstack自动生成。
VCPUs	指定该主机的CPU虚拟内核的数量。对于VM01型号的虚拟防火墙,内核数量指定 为1;VM02型号的虚拟防火墙,内核数量为2。
RAM MB	主机的内存大小,单位为MB。对于VM01型号的虚拟防火墙,内存最小值为 1024MB;对于VM02,内存最小值为2048MB。

Root Disk	指定根磁盘分区所需容量。单位为GB。建议根磁盘最小值为2GB。
Ephemeral Disk	临时磁盘大小。单位为GB,使用默认值(0),表示不使用临时磁盘。
Swap Disk	指定交换空间大小。单位为MB , 使用默认值 (0) , 不需要使用交换空间。

5. 点击右下角"创建云主机类型(Create Flavor)"按钮,完成配置。

步骤三:创建云硬盘

云硬盘用于存储G6000-VM虚拟防火墙的配置文件和许可证。如果不设置云硬盘,虚拟防火墙重启后,防火墙的系统配置将丢失,除非通过配置文件的导入导出功能做过手动备份,否则在没有存储硬盘的情况下,防火墙不能恢复重启前的配置。

虚拟防火墙需要最小为2048 MB的云硬盘作为存储硬盘。

下面步骤介绍如何创建存储硬盘。

1. 创建一个磁盘文件。

dd if=/dev/null of=diskname seek=block_num bs=bs_size

dd if=/dev/null	将/dev/null作为初始化文件的设备。	
of= <diskname< th=""><th>为磁盘文件命名。</th></diskname<>	为磁盘文件命名。	
seek=block_num	指定区块数量。	
bs=bs_size	设定读入/输出的区块的大小。建议设定每一个区块为1M。	

例如 , 创建一个名为"test"的2G磁盘文件 :

dd if=/dev/zero of=<test> seek=2048 bs=1M

2. 输入以下命令,格式化磁盘文件,使其成为可用的存储硬盘。

mke2fs -t ext4 -qF <diskname

mke2fs -t ext4 -qF	将磁盘文件格式化为ext4格式。
diskname	被格式化的磁盘文件的名称,上一步创建的磁盘文件。

例如,将上述的test磁盘文件格式化:

mke2fs -t ext4 -qF <test

3. 将格式化的磁盘作为镜像文件导入到Openstack。

glance image-create --disk-format raw --container-format bare --name image-name< diskname

glance image-create	在Openstack中创建一个镜像。
disk-format raw	指定磁盘格式为RAW。

container-format bare	指定不为磁盘进行封装。
name image-name	
< diskname	上一步中的磁盘文件名称。

例如,将上述名为"test"磁盘作为镜像文件导入,作为名为"image1"的镜像:

glance image-create --disk-format raw --container-format bare --name image1 <test

返回的结果如下:

, I Property	Value
<pre>I checksum I container_format I created_at I deleted I deleted_at I disk_format I id I is_public I min_disk I min_ram I name I owner I protected I size I status I updated_at I virtual_size</pre>	<pre> d62c4f44d79a2368be3468d6ed0d781f bare 2015-01-08T07:30:44 False none raw d1385a5c-aa9e-42bf-b82b-17d153470fd1 False 0 0 image1 4280f63e5f6d4ec8a362c8ba2a6e5932 False 2147483648 active 2015-01-08T07:31:35 None </pre>

4. 输入以下命令,将镜像文件转换为云硬盘:

cinder create --display-name volume-name --image-id \$(glance image-list | awk '/vfw-flash-image/{print \$2}

') size-num

cinder createdisplay-name volume-name	创建存储,为存储命名。display-那么为
<pre>image-id \$(glance image-list awk '/vfw-flash- image/{print \$2}')</pre>	通过glance命令查找到上一步中的磁盘文件对应的ID号码,将该 磁盘文件作为云硬盘。
size-num	硬盘的容量大小,默认单位为GB。要求最小值设为2,表示2GB 硬盘。

例如,将上述名为"image1"镜像文件转为容量为2 GB的云硬盘,命名为"volumetest":

cinder create --display-name volumetest --image-id \$(glance image-list | awk '/image1/{print \$2}') 2

步骤四:创建网络

Openstack的网络服务为Openstack云部署提供了可扩展的网络连接服务,通过Openstack的WebUI界面,就可以实现网络的创建和修改。

由于不同用户的组网需求不同,且创建网络属于Openstack的基础操作,本文档不再描述如何创建网络,请参考Openstack的帮助文档中 有关创建网络的章节(http://docs.openstack.org/user-guide/content/dashboard_create_networks.html)

步骤五:启动实例

输入以下命令,创建虚拟防火墙。

nova boot --image image-name --flavor flavor-name --nic net-id=\$(neutron net-list | awk '/net1-name/{print \$2} ') --nic net-id=\$(neutron net-list | awk '/net2-name/{print \$2}') --nic net-id=\$(neutron net-list | awk '/net3-name/{print \$2}') --block-device-mapping vdb=\$(cinder list | awk '/ volume-name/ {print \$2})

'):volume::False instance-name

nova boot	启动命令。
image image-name	指定启动防火墙时,要启动的镜像。image-name为虚 拟防火墙系统文件的镜像名称。
flavor flavor-name	指定云主机类型(flavor)。
nic net-id=\$(neutron net-list awk	为防火墙连接网络。net-name是网络名称。
<pre>'/net-name/{print \$2}')</pre>	根据组网规划,重复输入该命令可连接多个网络。
block-device-mapping vdb=\$(cinder list	指定云硬盘的名称。
awk '/ volume-name/ {print \$2}	
'):volume::False	
instance-name	自定义实例名称。

访问SG6000-VM虚拟防火墙

完成上一步的创建实例后,按照以下步骤访问防火墙:

1. 登录Openstack的Web管理界面。

	openstack	
Log In		
User Name		
Password		
		Sign In

- 2. 使用以下方法中的一种:
 - ≫ 如果您使用普通用户身份登录,从左侧导航栏,选择"项目 > Compute > 实例"。
 - >>> 如果您使用管理员身份登录,从左侧导航栏选择"管理员>系统面板>实例"。
- 3. 在列表中,点击虚拟防火墙的名称。



4. 在跳转的界面中,点击"控制台(**Console**)",即可在嵌入的命令行界面中访问虚拟防火墙。 Instance Details: FW02



5. 关于如何操作防火墙,参考StoneOS的配置文档(<u>点击此处</u>)。

在VMware ESXi上部署SG6000-VM

SG6000-VM虚拟防火墙通过ISO格式封装,可以安装在任意一台支持VMware ESXi虚拟机的X86设备上。

虚拟防火墙的部署,要求您必须已经熟悉VMware的vSpere Hypervisor架构、ESXi主机设置、VMware虚拟机部署等知识。

支持的部署场景

根据您的网络设计,您可以部署单个或多个SG6000-VM虚拟防火墙。



系统要求和限制

SG6000-VM的使用要求和限制:

- » VMware ESXi 的版本为5.0或5.5。
- » VM01要求最少使用1个vCPU、内存最小为1GB; VM02要求最少使用2个vCPU、内存最小为2GB。
- 建议每个虚拟防火墙的接口(vmNIC)数量至少为3个,一个作为管理接口,一个作为数据入口,一个作为数据出口。
- ≫ 网卡类型为E1000或vmxnet3。

部署防火墙

将SG6000-VM系列虚拟防火墙部署在ESXi服务器上,我们建议您使用vCenter和vSphere Client相结合的方式进行安装和管理。

安装防火墙

在部署虚拟防火墙之前,请先申请试用版本或联系销售人员,获取SG6000-VM虚拟防火墙的ISO镜像文件。

第一步:导入ISO文件

- 1. 将虚拟防火墙的ISO镜像文件保存在本地。
- 2. 在vSphere Client中,点击"主页 > 清单 > 主机和集群",然后在左侧列表中点击vFW所在的ESXi主机。
- 3. 在右侧页面点击"配置"标签页,选择左侧导航栏的"存储器",然后右键点击数据存储,选择"浏览数据存储"。



4. 在弹出的 <数据存储浏览器 > 中,点击上传按钮" 💜",将保存在本地的SG6000-VM的ISO镜像文件上传到数据存储中。

第二步:创建虚拟机

- 1. 打开vSphere Client,输入vCenter的IP地址、用户名和密码,点击"登录"。
- 2. 选择"主页 > 清单 > 虚拟机和模板",在右侧页面点击"创建新虚拟机"。



- 3. 在弹出虚拟机向导中,选择"自定义(Custom)"配置类型,点击"下一步"。
- 4. 在 < 名称和位置 > 选项卡中,输入虚拟机的名称并选择数据中心,然后点击"下一步"。
- 5. 在 <存储器 >选项卡中,选择目标存储,点击"下一步"。
- 6. 在 < 虚拟机版本 > 选项卡中,选择"虚拟机版本:8",点击"下一步"。
- 7. 在 < 客户机操作系统 > 选项卡中,选择"Windows",点击"下一步"。
- 在<CPU>选项卡中,根据您要创建的虚拟防火墙类型进行选择。如果您创建的是SG6000-VM01,选择1个CPU和1个核;如果您创建 SG6000-VM02,选择2个CPU和2个核,然后点击"下一步"。
- 在 < 内存 > 选项卡中,根据防火墙类型进行选择。对于SG6000-VM01类型的防火墙,至少选择1G内存;对于VM02类型的防火墙,选择2G内存,然后点击"下一步"。
- 10. 在<网络>选项卡中,建议至少选择3个网卡,一个用于管理接口,一个用于数据入口,一个用于数据出口。网卡类型为E1000或 VMNET3。
- 11. 在<SCSI控制器>选项卡中,可以保留默认选项,或者选择"VMware准虚拟"。(vFW只支持读取IDE类型的磁盘作为系统启动磁盘,但是,如果您希望使用SCSI类型的磁盘启动防火墙(见下面步骤14),需要选择"VMware准虚拟(VMware

paravirtual)",采用VMware准虚拟的方式读取SCSI类型的磁盘。)然后,点击"下一步"。



- 12. 在 <选择磁盘 >选项卡中,选择"创建一个新的磁盘",点击"下一步"。
- 13. 在 < 创建磁盘 > 选项卡中,为虚拟防火墙分配磁盘空间(最小值设置为2G),点击"下一步"。
- 在<高级选项>选项卡中,选择"IDE"类型的磁盘节点。vFW支持通过读取IDE类型的磁盘进行启动。(如果已经选择了"VMware 准虚拟"类型作为SCSI控制器(见步骤11),也可以直接选择"SCSI"类型磁盘。否则,需要务必选择IDE类型磁盘。)然后,点击 "下一步"。
- 15. 点击"完成",系统将生成虚拟机。

第三步:选择ISO文件

1. 在vSphere Client中,点击"主页 > 清单 > 虚拟机和模板",点击左侧列表中的虚拟防火墙,点击右侧页面的"编辑虚拟机设置"。



 在弹出的<虚拟机属性>对话框中,选中"CD/DVD驱动器",选择"数据存储ISO文件"单选按钮,点击"浏览",找到上一步骤中 上传到数据中心的ISO文件。同时,选中"启动时连接"。

Ø	vFW-01 - Virtual N	1achine Properties 🛛 🗕 🗖 🗙
Hardware Options Resources Profiles vServices Virtual Machine Version: 8		
Show All Devices	Add Remove	Device Status
Hardware	Summary	Connect at power on
Memory CPUs CPUs VidCl device VidCl device ScStoncoller 0 Co/ovo drive 1 (cdited) Troppy drive 1 Network adapter 1 Network adapter 2	2048 MB 1 Video card Restricted Peravirua (datastore1) vFW/S Cherk Device vfwll dvPortGroup_trunk1 (d	Device Type Client Device Net: To connect the device, you must power on the Vitual machine and then dick the Connect CD/DVD button in the toobar. C Hoot Device C Datastore ISO File [datastore 1] vFW/S66000 vFW01-5. Browse Mode C Pastbrough IDE (recommended) C Emulate IDE Vitual Device Node C IDE (1:0) CD/DVD drive 1
Help		OKCancel

3. 点击"确定"。

第四步:加入网络

- 1. 在vSphere Client中,点击"主页 > 清单 > 主机和集群",然后在左侧列表中点击vFW所在的ESXi主机。
- 在右侧页面点击"配置"标签页,选择左侧"硬件"下的"网络",然后在"vSphere标准交换机"下,点击右上角的"添加网络"。

说明:vSphere标准交换机(VSS)网络适用于在单台ESXi主机上添加虚拟防火墙,如果在多台ESXi主机上部署虚拟防火墙,需要使

用vSphere Distributed Switch 分布式交换机(在"主页 > 清单 > 网络"目录下,可以添加或配置VDS的网络和端口组)。

192.168.1.6 VHware ESQ, 55.0, 1331820 诒(综务 9天)				
	116 NB (新学) 新学 (新学) Wile (2011) Mill (Hardware Status)			
硬件	查道: [InSphere 現:違交換稅] JrSphere Distributed Switch			
处理器	「「「」「「」」「」「」」「「」」「」」「「」」「」」「」」「「」」」「「」」」	刷新 添加网络 】 闢性		
内存				
	标准交换机: vSwtch0 称称 国性			
(* 1415) (*				
网络通数器	VVN Network 2			
高级设置	2 1728/W3.			
电源管理				

3. 在弹出的 <添加网络向导 >对话框中,选中"虚拟机",点击"下一步"。

4. 选择防火墙的接口所属的vSwtich交换机,点击"下一步"。

5. 在"网络标签"文本框,为防火墙接口所属的端口输入一个名称,根据需要,选择VLAN或不选择,点击"下一步"。

6. 点击"确定"。

- 7. 重复步骤2至步骤6,为防火墙的所有接口创建vSwtich的端口。
- 8. 返回"主页 > 清单 > 虚拟机和模板",点击左侧列表中的虚拟防火墙,然后点击右侧页面的"编辑虚拟机设置"。
- 在弹出的<虚拟机属性>对话框中,选中"网络适配器",然后在右侧的"网络标签"下拉菜单中,选择该接口所属的vSwtich交换机端口,然后点击"确定"。

8	vFW-01 - J	差拟机属性 - □ ×
硬件 送项 资源	配置文件 vService	虚拟机版本: 8
□ 显示所有设备	添加 移除	
 硬件 ● 内存 ○ CPU ● 显卡 ● VMCI设备 ○ SCSI技制器 ○ CO/POUNED ○ CO/POUNED<th>補費 2048 MB 1 夏卡 受限制 LSI Logit SAS 1 (datatoret])FW/SG60 虚抑組盤 文白地治路 文白地治路 文白地治路 diffortGroup_trank1 (d</th><th>▶ 引力电源的连接 通配器类型 当前适配器: WHONET 3 ▶ 100:50:56:87:c5:e8 ● 自动 手动 ▶ 100:c5:08:10: 非运动 東波古 DirectPath I/O: 非运动 東波古 Transference 非运动 ● 自动 事运动 ● Pathered 非运动 ● Pathered 非运动 ● Pathered 非运动 ● Pathered 東波动 ● Pathered ・ ● Pathered ● ● Pathered ● ● Pathered ● ● Pathered ● ● Pathered ● <</th>	補費 2048 MB 1 夏卡 受限制 LSI Logit SAS 1 (datatoret])FW/SG60 虚抑組盤 文白地治路 文白地治路 文白地治路 diffortGroup_trank1 (d	▶ 引力电源的连接 通配器类型 当前适配器: WHONET 3 ▶ 100:50:56:87:c5:e8 ● 自动 手动 ▶ 100:c5:08:10: 非运动 東波古 DirectPath I/O: 非运动 東波古 Transference 非运动 ● 自动 事运动 ● Pathered 非运动 ● Pathered 非运动 ● Pathered 非运动 ● Pathered 東波动 ● Pathered ・ ● Pathered ● ● Pathered ● ● Pathered ● ● Pathered ● ● Pathered ● <
帮助(出)		

10. 重复上一步,为防火墙上的所有接口分配交换机端口。如果在创建虚拟机时,没有添加足够的接口,可以点击"添加"按钮,为防火 墙添加更多的网络接口。

启动和访问虚拟防火墙

完成上面的所有配置之后,就可以启动防火墙的虚拟机了。

- 1. 在vShpere Client中,点击"主页 > 清单 > 虚拟机和模板"。
- 2. 右键单击防火墙,选择"打开控制台",vSphere Client弹出新的对话框,连接防火墙的Console口。
- 3. 点击绿色电源按钮。



- 4. 稍等片刻,该防火墙即可启动。
- 5. 当显示如下的命令行界面时,输入默认的用户名和密码(hillstone/hillstone),登录防火墙。

		Welcоме	
n Navot svi i na doarod skor na doarod skor na doarod	Hillst	one Netwo	rks
Hillstone StoneOS Software Copyright (c) 2006-2015 by change_monitor_stat, can no login: hillstone password: SG-6000# _	Version 5.5 Hillstone Ne ot find the r	et⊌orks, Inc. Moni_appinfo_t object	t for appid 66

防火墙初始配置

经过上面的配置后,就能够通过vSphere Client对防火墙虚拟机进行管理。但是,需要首先对防火墙的管理接口进行配置,才能使用WebUI界面,方便后续使用StoneOS系统。

对防火墙进行初始配置,按照以下步骤进行操作:

- 1. 从网络管理员处获取配置管理接口所需的信息,包括IP地址、子网掩码、网关IP地址。
- 2. 配置管理口IP地址并开启访问权限。系统默认的管理接口为eth0/0。由于接口eth0/0默认开启了DHCP,需要手动关闭DHCP,才能 分配静态IP地址。登录Console口之后,输入以下命令配置管理接口:

SG-6000(config-if-eth0/0)# exit				
SG-6000(config-if-eth0/0)# manage http https telnet snmp ssh				
<pre>SG-6000(config-if-eth0/0)# ip address a.b.c.d/netmask</pre>				
SG-6000(config)# no ip address dhcp				
SG-6000(config)# interface ethernet0/0				
SG-6000# config				

ip address a.b.c.d/netmask	为该接口分配一个静态IP地址和子网掩码。		
manage {http https telnet snmp	开启接口的管理功能,包括http、https、telent、		
ssh ping}	snmp、SSH和ping。		

3. 添加静态路由。使用以下命令,为防火墙接口添加下一跳为网关的目的路由。

SG-6000(config) # ip vrouter trust-vr

SG-6000(config)# ip route a.b.c.d/netmask A.B.C.D

SG-6000 (config) #

a.b.c.d/netmask	指定目的地址。任意目的地请输入0.0.0.0/0。
A.B.C.D	下一跳的地址,输入网关的IP地址。

4. 保存设置。使用以下命令,将设置保存。

SG-6000# save

5. 测试网关的连通性。

SG-6000(config-	if-eth0/0)# ping 192.168.1.6
Sending	ICMP pa	ckets to 192.168.1.6
Seq	tt1	time(ms)
1	64	4.28
2	64	10.0
3	64	10.0
4	64	9.96
5	64	10.1

6. 在浏览器输入管理接口的IP地址,访问WebUI管理界面(确认已经使用manage http命令开启WebUI访问权限)。

在AWS上部署SG6000-VM

AWS介绍

亚马逊网络服务系统(英语:Amazon Web Services,简称为AWS),是亚马逊公司所创建的云计算平台,提供许多远程Web服务。

AWS提供的多种组件中,与虚拟防火墙直接相关的是VPC和EC2。

- 虚拟私有云(英语: Virtual Private Cloud,简称为VPC)是一个逻辑隔离的虚拟网络,用户可以在VPC中创建自有的IP地址范围和 子网,配置路由表和网关。
- ➢ EC2(英语:Elastic Compute Cloud,简称为EC2)提供云中的计算容量,用户可以将EC2简单的看成虚拟机服务。EC2与VPC结合,就能够为计算资源提供强大的联网功能。



位于AWS的SG6000-VM

SG6000-VM虚拟防火墙(英语:Virtual Firewall,简称为vFW),作为EC2实例安装在AWS上,通过VPC的联网能力,为VPC子网中的服 务器提供防火墙业务。



场景介绍

vFW作为互联网网关

SG-6000-VM系列虚拟防火墙作为VPC网关部署在租户的网络出口处,通过检测流量发现攻击为何和异常行为,有效的保护VPC网络、 EC2实例和租户的应用。AWS平台上的vFW能够实现动态部署,在EC2实例发生船舰、启动、迁移、撤销等状态变化时,也可以同步更新 vFW的配置信息和安全策略。

vFW作为VPN网关

SG-6000-VM系列可以提供IPSec和SCVPN连接方式,满足不同的VPN场景。在混合云模式下,企业的本地系统及分支系统能够与AWS上的企业服务建立标准的点到点的VPN连接,并通过基于应用、用户和内容的访问控制功能保证通信的合法性和流畅性。

服务器负载均衡

SG-6000-VM可以将网络流量平均分配给同样服务的不同EC2实例上。当一个EC2实例的负载达到上限时,服务器负载均衡功能会将新的连接请求转发给其他EC2实例以防止连接请求被丢弃。支持的负载均衡的算法包括加权散列、加权最小连接数和加权轮询。

本手册的组网设计

本手册以vFW作为互联网网关的部署场景为例,介绍在AWS上安装和使用vFW的操作方法。为了方便对照和理解,手册中的步骤和截图 与组网图中的子网、接口和IP地址完全一致,仅供用户参考,用户不应拘泥于本示范。在您配置您的实际场景中,需要将子网、接口和IP 地址等元素替换为您的真实场景。

在这个组网设计中,AWS用户的VPC将包括三个子网,其中一个放置私网服务器,另外两个对应vFW的两个接口。通过vFW,私网服务器 与互联网网关隔离,访问私网服务器的流量都要进出vFW。

vFW的管理接口eth0和业务接口eth1均连接到VPC的互联网网关(Internet Gateway,简称IGW)。当访问eth1的公网地址时,如果为 eth1添加DNAT规则,那么互联网用户就能够访问位于Subnet 1 的私网服务器了。并且,在接口eth0上配置了SNAT规则,使私网服务器 能够访问互联网。



- >> VPC : 10.0.0/16.
- Subnet 0 (Manage): 10.0.0.0/24。Subnet 0 和Subnet 2 代表防火墙的两个接口所在的VPC子网。接口eth0属于Subnet 0, 它 是防火墙的管理接口。
- Subnet 1 (Private): 10.0.1.0/24。企业的虚拟服务器(即EC2实例)所在的子网,可以看作是企业放置Web、FTP、Mail 服务器等提供业务的服务器所在的私网。
- Subnet 2 (Public): 10.0.2.0/24。防火墙的业务接口eth1属于Subnet 2。eth1接口的公网地址将作为私网服务器的IP地址,用于 互联网访问私网服务器时使用。

准备您的VPC

使用AWS服务的前提是拥有一个AWS账户。申请AWS账户,需要准备一张信用卡和手机号码,在AWS的中国区网站申请(<u>点击此处</u>)。 更多关于如何配置VPC,请查看AWS的入门文档(<u>点击此处</u>)。

在本手册的组网设计中,我们假定用户还未创建过VPC网络。本部分的操作就是介绍如何创建VPC和子网。如果您已经有自己的VPC,可以忽略这部分操作。

完成这部分后,我们将会得到以下网络:

- >>> VPC : 10.0.0/16
- Subnet 0 (Manage) : 10.0.0.0/24
- Subnet 2 (Public) : 10.0.2.0/24

第一步: 登录AWS账户

- 1. 拥有AWS账号之后,登录AWS管理控制台(Console)。
- 2. 要进入VPC界面,在控制台点击"VPC"。



3. 进入VPC页面。



第二步:创建私有云(VPC)

在VPC控制面板(VPC Dashboard),通过VPC配置向导(VPC Wizard)创建一个VPC。

1. 点击"启动VPC向导"按钮,开始使用向导。



2. 在"带单个公有子网的VPC"标签页下,点击"选择"。



3. 为VPC输入名称"VPC",其他选项保留默认设置,然后点击"创建VPC"。

步骤 2:带单个公有子网的 VPC					
IP CIDR 块:*	10.0.0/16	(65531 个可用 IP 地址)			
VPC 名称:	VPC	D			
公有子网:*	10.0.0/24	(251 个可用 IP 地址)			
可用区:*	无首选项 ▼				
子网名称:	公有子网				
	AWS 创建 VPC 以后,您可以添	加更多子网。			
启用 DNS 主机名:*	● 是 □ 否				
硬件租赁:*					

4. VPC创建成功。



5. 该VPC默认包含一个子网,即公有子网,它具有一条默认路由,连接互联网网关(IGW)。在后面的操作中,我们将会把防火墙eth0 接口绑定到该子网中,作为防火墙的管理接口,用于访问StoneOS系统。

为了便于标识,将公有子网的名称修改为"Manage"。(操作方法:点击左侧导航栏的"子网",在列表中找到与VPC绑定的子网,点击"名称"所在的文本框编辑。)

日本	Ŧ	子网 ID	-	状态	-	VPC
Manage) [edf486		available	• (vpc-041d0366 (10.0.0.0/16) VPC
		😢 🛇 eff113		available	•	vpc-56100f34 (81.1.0.0/16) performance
perform	ancep	subnet-eea3bd8c		available		vpc-56100f34 (81 1 0 0/16) performance

第三步:为VPC添加子网

在本示例的设计中,防火墙的接口eth0作为管理接口,用于访问管理vFW,另一个接口eth1作为防火墙的业务口,是互联网访问私网服务 器的入口。管理接口所在子网已经默认生成了("Subnet 0 (Manage)"),下面介绍如何创建业务子网(接口eth1)。

要实现上面的子网配置,请按照以下步骤进行操作:

1. 在VPC控制面板,点击"子网",然后点击"创建子网"。

VPC 控制面板 ■ VPC 馏选	创建子网)删除子际	修改自动分配公有	j ip	
无 •	Q,搜创建子网具属	± ×		
Virtual Private Cloud	名称	子网ID 🗸	状态 -	VPC
您的 VPC	Manage	subnet-e4edf486	available	vpc-041d0366 (10.0.0.0/16) VPC
子网	xqxu-net2	subnet-62f5eb00	available	vpc-0b918e69 (172.16.0.0/16) xqxu-vpc
影山泰	xqxu-net3	subnet-61f5eb03	available	vpc-0b918e69 (172.16.0.0/16) xqxu-vpc
Internet RIX	xqxu-net1	subnet-9cf4eafe	available	vpc-0b918e69 (172.16.0.0/16) xqxu-vpc
Internet MX	DB	cubnot baabb8d8	available	Vinc 36312264 (172 31 0 0/16) LMvVPC

2. 输入子网名称,在"VPC"下拉菜单选择刚刚创建的VPC,在"CIDR块"下拉菜单输入子网地址"10.0.2.0/24"。

创建子网	×
使用 CIDR 格式指定子网的 II /28 网络掩码之间。另请注意	P 地址块(例如 10.0.0.0/24)。请注意,块大小必须介于 /16 网络掩码和 ,子网的大小可与 VPC 的大小相同。
名称标签 VPC	Public vpc-041d0366 (10.0.0.0/16) VPC
可用区	无首选项 🔹 🗊
CIDR 块	10.0.2.0/24
	现消 是, 创建

3. 点击"是,创建"。

第四步:为子网添加路由

AWS VPC有隐式路由器,会自动生成主路由表,包含一条指向本地的路由。用户也可以创建自定义路由表。为了使刚刚创建的业务子网 ("Subnet 2 (Public)")的下一跳指向互联网网关(igw),需要将这条路由添加到它的路由表。

为子网添加路由,按照以下步骤进行操作:

- 1. 在VPC控制面板,点击"路由表"。
- 2. 为了便于标记,找到刚刚创建的子网对应的路由表,修改路由表名称为"IGW"。



3. 选中该路由表,点击下方的<路由>标签页,然后点击"编辑"。

4. 点击"添加其他路由",添加一条所有流量的目的为互联网网关的路由。

rtb-2b45a24e							
摘要	路由	子网关联	路日	由传播		标签	
取消 保存							
目的地	目标		状态	已传播	删除		
10.0.0/16	local		活跃的	否			
0.0.0/0	igw-9d4ea	abf8		否	8		
添加其他路由							

5. 点击"保存"。

安装虚拟防火墙

创建防火墙实例

vFW将作为一个EC2实例安装在AWS中。防火墙的管理接口(eth0)和业务接口(eth1)分别用于访问StoneOS系统和私网服务器。

下面介绍如何在AWS中安装vFW。在完成"安装虚拟防火墙"这部分的操作后,您将:

- » 拥有一个运行中的虚拟StoneOS系统
- » 看到管理接口eth0和业务接口eth1都获取到私网IP地址和公网IP地址
- ≫ 能够访问防火墙的CLI和WebUI界面

第一步:创建EC2实例

1. 在AWS管理控制台 (Console), 点击"EC2"。



2. 在EC2控制面板,点击"启动实例"。



3. 进入实例配置向导页面。

第二步:为实例选择AMI模板

AMI 是一种模板,它包含启动实例所需的软件配置(操作系统、应用程序服务器或应用程序)。

vFW的通过共享AMI模板的方式提供给用户。在您申请使用或购买了SG6000-VM之后,山石网科就会将虚拟防火墙镜像文件共享给您的AWS帐户。关于如何选择防火墙型号,参考产品介绍("在AWS上部署SG6000-VM"在第29页)。

得到共享的vFW的AMI模板后,按照以下步骤选择模板:

1. 接上步,在实例配置向导中,点击"我的AMI"。

1. 选择 AMI 2. 选择实例类型	3. 配置实例	4.32007944 5.4723次例 6.路图安全组 7.甲核	
步骤 1: 选择一个An AMI是一种模板,其中包含启动的	nazon 系统 _{《例所需的软件配置}	映 像 (AMI) 像作系统、应用程序都导着构态用程序, 意可以选择由 AWS 或统计的用户社区提供的 AMI,也可以选择自己的 AMI。	取消并退出
快速启动 (我的 AMI)	Q. 搜索 我的 A	an X	K < 1到3, 共3个AMI > >
社区 AMI	۵	vfe01.ami00246001 ಸಗುರ ಕಾರ್ಡಿಕಿ ಪ್ರಕ್ರಿತಿ ಕ್ಲೀತ್ರಿ ಹೆಸ್ಟ್ ಪ್ರಕ್ರಿ 17572465113	选择 64位
 ■ 未規有的 ■ 与我共享 ■ 架构 	۵	VMw2 - ami-48215371 小心2 優容高貴恵 (1) - 111111111111111111111111111111111	选择 64位
□ 32 位 □ 64 位 ▼ 根设备类型	۵	Hillstone vFW - am:dt/?Beaef hillstone vHual Revail 研合偏亮型 eloo 直接反映型 hvm 视频者 15/37-2455113	选择 64 位
 EBS 实例存储 			

2. 找到您需要的产品型号,点击"选择"。

第三步:选择实例类型

如果您购买的是SG6000-VM01产品,建议您选择1个CPU、1GB内存的实例;如果您购买的是SG6000-VM02产品,建议选择2个CPU、 4GB内存的实例。

1. 法择7	AMI 2. 选择实制绘型 3. 配置实例 4. 示加	g存储 5. 标至实例 6. j	12世史全地 7. 审核				
步骤	2: 选择一个实例类型	the state of the s	n 11 v - 6- et man de 25 de la compte 90 et	the second state of the second states			
Amazon	CONTRACTOR AND A REPORT OF A	A DECEMBER OF DESIGN	CONTINUES - C	2118 CPU, M45, (918409)993	(HOATHORDER, PLICE/CARD/CERLIN	《详述目的资源组合。 〕 雕塑多 有大头的头型。	(2)这些关键如何利益定的打算剩余的组度。
90.02.1911	₩1月头的天坐 載加一八 3	E-1 EE-MC-1					
=101x4	BRING WERE: IZ MICRO (Variable ECU, 1 VCPU,	2.5 GHZ, Intel Xeon Family, 1	GIB (447, 1)(187+ EBS)				
	系列	- 太型 -	vCPU () -	内存 (GiB) ~	実制存储 (GB) ① -	可用的优化 EBS ① -	网络性能 ① -
	道用型	t2.micro	1	1	仅限于 EBS		低到中等
	通用型	t2.small	1	2	仅限于 EBS		低利中等
	通用型	t2.medium	2	4	仅限于 EBS		低到中等
0	通用型	m1.small	1	1.7	1 x 160		帳
	通用型	m3.medium	1	3.75	1 x 4 (SSD) -		中等
	道用型	m3.large	2	7.5	1 x 32 (SSD)		中等
	通用型	m3.xlarge	4	15	2 x 40 (SSD)	是	中等
	通用型	m3.2xlarge	8	30	2 x 80 (SSD)	是	8
	计算优化	c3.large	2	3.75	2 x 16 (SSD)		中等
	计模优化	c3.xlarge	4	7.5	2 x 40 (SSD)	是	高
	计算优化	c3.2xlarge	8	15	2 x 80 (SSD)	是	*
	计算优化	c3.4xlarge	16	30	2 x 160 (SSD)	是	高
	计算优化	c3.8xlarge	32	60	2 x 320 (SSD)		10 Gb .
						取消 上-	-步 iii被和启动 下一步:配置实例详细信息

选中实例前面的单选按钮,点击"下一步:配置实例详细信息"进入下一步。

第四步:配置实例详细信息

为实例选择所属的VPC和VPC子网,按照以下步骤:

1. 在 "网络"下拉菜单选择部署vFW的VPC,在 "子网"下拉菜单选择管理接口eth0所属的子网(Subnet 0(Manage):10.0.0.0/24),其他选项保持默认值。

1. 选择 AMI 2. 选择实例类型 3. 概题	实例 4.添加存储 5.标签实例 6.配置安全	2组 7. 审核
步骤 3: 配置实例详细信, 配置实例以便满足您的需求。您可以从同- 实例的数量	 AMI 上启动多个实例,请求竞价型实例以利用其低 1 	价优势,向实例分配访问管理角色等等。
网络 子网 白动公祝人女 19	 (vpc-041d0366 (10.0.0.0/16) (subnet-e4edf486(10.0.0.0/24) cn-north 251小可用 IP 認知 	● 新建 VPC -1a ● 新建子网
日初月山之日 III IAM 角色	0 <u>F</u>	▼ C 创建新的 IAM 角色
关闭操作 烏用終止保护 监控	 (停止 (副時止意外终止 (副局用 CloudWatch 详细监控 将收取额外费用。 	v
租赁	 共享相期(多相户硬件) 将对专用租赁收取额外的费用。 	T

2. 为防火墙添加一个接口eth1,作为业务接口。点击"添加设备"。

ſ	▼ 网络	各接口			
	设备	网络接口	子网	主要 IP	辅助 IP 地址
	eth0	新网络接口 •	subnet-e4edf48€ ▼	自动分配	添加 IP
	添加设	a			

3. 在 "子网" 下拉菜单,选择与接口eth0不同的子网(Subnet 2 (Public): 10.0.2.0/24)。

▼ [0]	洛接口			
设备	网络接口	子网	主要 IP	辅助 IP 地址
eth0	新网络接□ ▼	subnet-e4edf48(•	自动分配	添加 IP
eth1	新网络接口 •	subnet-289f864; subnet-289f864a 10.	自动分配 0.2.0/24 cn-north-1a	添加 IP
	我们工计市头你的空间。	subnet-e4edf486 10.	0.0.0/24 cn-ntsth-1a	

4. 点击"下一步:添加存储"。

第五步:添加存储

1. 保留默认值。或者,如果您需要更大的存储空间,在"大小"文本框输入数字,获取更大的存储空间。

1. 选择 AMI 2	2. 选择实例类型 3. 配置实例		4.添加存储 5.标签实例		6. 監査安全组 7. 审核				
步骤 4: 添力 始的实例将使用以" 存储卷。了解更多	旧存储 F存储设备设置启 关于 Amazon EC	动。您可以将其 2 中的存储选项	他 EBS 卷和实 i。	例存储卷连接到	您的实例,或编辑	用根卷的设置。	您还可以在启动	1 实例后连接其他	EBS 卷而非
类型 ①	设备 ①	快照	1	大小 (GiB)	① 卷类型	0	IOPS ()	终止时删除(
类型 ① 相目录	设备 ① /dev/xvd	a snap-t	i) id6019b5	大小 (GiB) 1	 1 卷类型 通用型 	() (SSD) •	IOPS () 3/3000	终止时删除(〕 □	

2. 点击"下一步:标签实例"。

第六步:标签实例

标签用于生成密钥对。vFW可以不使用公钥和私钥的密钥对方式进行认证,而是直接使用用户名和密码。请忽略该步骤,直接点击"下一步:配置安全组"。

第七步:配置安全组

安全组是一组防火墙规则,它规定哪些类型的流量可以进出实例。EC2的安全组缺省具有一条允许SSH连接的规则,为了便于访问,我们 需要添加一条允许所有类型流量的规则。

1. 选择"创建一个新安全组",并添加名称。



2. 添加规则,允许所有流量。

Г	RE ()	192 ()	96-1328 ()	88 0
¢	804 • Krti 48 • Halton	icr kir	22 3 - 866.06	11月1日 - 10000 11月1日 - 1000
	A 第8 2世方 0.0.100 行承担的公共利用 P 地址的问题的第二 第13章	1955年全体和印度型为农大开动已知的 P 地址进行协同。		

3. 点击"审核和启动"。

第八步:启动实例

- 1. 在审核页面查看已配置的信息,然后点击"启动"。
- 2. AWS将弹出提示,确认是否需要密钥对,选择"在没有密钥对的情况下继续"。



3. 点击"启动实例"。AWS将启动防火墙,您可以点击"查看启动日志"查看启动过程。



4. 点击"查看实例",返回EC2实例列表,防火墙正在启动。

实例 ID	▼ 实例类型	- 可用区	▼ 实例状态	Ψ	状态检查	▼ 警报 状态	
i-4f70a577	t2.micro	cn-north-1a	running		🌋 正在初始化	Æ	70

配置子网和接口

分配弹性IP地址

ŧŀ

弹性 IP 地址(英语:Elastic IP,简称为EIP)是AWS分配给用户的静态公网 IP 地址。借助EIP,可以快速将公网地址映射到一个实例。 我们将申请两个弹性IP地址,分别分配给管理接口eth0和业务接口eth1。这样,vFW的两个接口都分别具有一个私网IP地址和一个公网IP 地址,这两个IP地址可以自动映射,不需要设置规则。

1. 在EC2控制面板,点击左侧导航栏的"弹性IP",进入弹性IP界面。

2. 点击"分配新地址",获取一个公网IP地址。



- 3. 重复上一步,申请第二个IP地址。
- 4. 选中一个弹性IP,点击"关联地址"。在弹出对话框中,输入eth0的接口ID号。这个弹性IP地址是防火墙的管理接口eth0的公网地

天联地址				
择要与此 IP 地址关联的实例s	或网络接口。 (54	.223.138.88)		
	实例	搜索实例 ID 或 名称 标签		
	网络接口	或者 eni-ef88ab8a		
	私有 IP 地址	10.0.0.97*	• (1)	
		□ 重新关联	1	

- 5. 重复上一步,将第二个弹性IP地址分配给接口eth1。这个弹性IP将是私网服务器的公网地址。
- 6. 返回列表,选中弹性IP地址,可以看到已经分配了公网IP地址和DNS服务器地址。



禁用接口的源/目的地址转换

为两个网络接口禁用源/目的转换。

- 1. 在EC2控制面板,点击"网络接口"。
- 2. 选中接口eth0,点击"操作>更改源/目的检查"。

3. 在弹出的对话框中,选择"已禁用",点击"保存"。



4. 重复上面的操作,禁用接口eth1的源/目标检查。

在主控台查看实例

返回EC2控制面板,点击左侧导航栏的"实例",选中防火墙实例,可以查看防火墙的详细信息。

启动实例	连接	操作 丶													Ð	•
Q, 按标3	6和属性辩选	或者接关键:	学授索											0 K	< 1到10,共	10 > >
	ID v	实例类型	▼ 可用区 *	实例状态 ~ 状	态检查 ~	警报 状态		公有 DNS 👻	公有 IP	×	密钥名称 -	蓋控	自动时间	- 安全组 -	VPC ID	- → F
i-4f7	'0a577	t2.micro	cn-north-1a	🥥 running 🛛 😋	2/2 的检查	ž	>	ec2-54-223	54.223.138.88			disabled	2015年4月23日 UTC+8上年	1 VPC	vpc-041d0366	subr
i-861	Bf40b3	t2.micro	cn-north-1a	stopped		ж.	6				performance	disabled	2015年4月10日 UTC+8下午	-5 launc	vpc-36312254	subr
< III	le9bc8	12 medium	cn-north-1a	🔵 running 🛛 🥝	2/2 的检查	无	6	ec2-54-223	54 223 169 59		hsvfw	disabled	2015年4月23日 UTC+8上4	-9 default	vpc-807e61e2	sito
突例:∎i-4	lf70a577	弹性 IP: 54	.223.147.156												_	
attab	distant Antonio	10-10-	4-100													
通逐	状态检查	2612	怀金													
		実例 ID 実例はす	1-4t/0a5//							公有し	NS ec2-54-223-1	38-88.cn-north-1.co	ompute.amazonaws.com.cn			
		次的状态 实例未用	12 micro							二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	IP 54 223 147	6				
		彩布DNS	ip-10-0-0-97 cn-north-1 compu	te internal						可用	IX cn-north-1a					
		私有IP	10.0.0.97							安全	相 VPC 電纜	LIN .				
		辅助私有 IP							i	机的准	件 无计划事件					
		VPC ID	vpc-041d0366							AMI	ID vfw01 (ami-0	624b63f)				
		子阿ID	subnet-e4edf486							귀	H -					
		网络推口	eth0							IAM 貿	色 -					
			网络榕口 eth0													
		源/目标检查								음祖对송	(称 -	-				
		500 @ @	接口に	eni-ef88ab8a						期刊	15/5/42651	13				
		EDS 現代 研究先会期	VPC IE	vpc-041d0366						111200	10 ZU15年4月Z3	E 01C+8E+11:0	0.35(小割1小时)			
		根で開発型	正接执行者 *****	15/5/4265113						マエロ	in normal					
		协能存得备	注 授 从 场 送 按 时 间	Thu Ang 23 11:00-3	5 CMT+800					14/	1 私本					
				2015												
			终止时期除	true						警报状	走 态					
			私有 IP 地址	10.0.0.97						内核	ID -					
			私有 DNS 名称	ip-10-0-97.cn-nort	h-				R/	AM 磁盘	ID -					
			2044 ID 4644	54 223 138 88						置放着	细 -					
			·····································	false						虚损	LIK hvm					
			#1	Primary network int	erface					B	r-p9fb0081					
			安全细	VPC					AM	1.111211	IRR U					

访问虚拟防火墙

vFW的缺省设置中,开启了管理接口eth0的访问权限,我们将首先使用SSH访问接口eth0,通过命令行界面对StoneOS进行配置。若要更 多关于如何StoneOS命令行操作指南,请参考《StoneOS命令行用户手册》(<u>点击此处</u>)。

通过SSH访问CLI界面

1. 打开一个SSH远程连接软件,这里以PuTTY为例,输入防火墙管理接口eth0的公网IP地址。



(注意:如果您也使用PuTTY,还需要将"Connection > SSH > Cipher"中的"3DES"调整到顶端,调整后才能成功连接。)

2. 界面将提示您输入用户名和密码, 敲入系统默认的 "hillstone"和 "hillstone" 作为用户名和密码。



3. 现在您可以使用远程的SSH连接,对vFW进行设置。

访问WebUI界面

由于HTTP连接的默认端口80和SSL VPN的默认端口4433在中国亚马逊禁用,所以,若要访问StoneOS的WebUI和SSL VPN,需要更换端口号。

访问StoneOS的WebUI界面,按照以下步骤:

1. 使用SSH连接登录CLI界面后,使用以下命令,修改HTTP端口为8888。

SG-6000# config

```
SG-6000(config)# http port 8888
```

(可选)若需要使用SSL VPN功能,使用以下命令修改SSL VPN的端口号为8889。
 SG-6000# conf

SG-6000(config)# tunnel scvpn test SG-6000(config-tunnel-scvpn)# https-port 8889

3. 开启eth0接口的http访问权限:

SG-6000# config SG-6000(config)# interface ethernet0/0 SG-6000(config-if-eth0/0)# manage http

4. 在一台连接互联网的PC上,打开浏览器,输入eth0对应的弹性IP地址和端口号8888,即可访问StoneOS WebUI界面。

VPC Management Cons × C HILLSTONE NETWORKS ×		Fintuaer
← → C fi 🗋 54.223.138.88:8888		☆ 🐵 🐔 ≡
← ○ C fi 54221138.88 5888	Hilstons + (n) Withins	<u>슈</u> (영 종 프
	mon beneral-like and the set of t	
	A MARY AND A MARY MARKANIA - MARKANIA	

5. 输入默认的用户名和密码"hillstone"和"hillstone",点击"登录"进入系统。

配置虚拟防火墙

获取DHCP

在StoneOS系统中,管理接口eth0默认开启了DHCP,所以已经获取了私网地址,而业务接口eth1需要开启DHCP后才能拥有私网地址。

- 1. 登录StoneOS的WebUI界面,选择"网络>接口"。
- 2. 选中接口ethernet0/1,点击"编辑"。

Hillstone					_
A RYWS RX'S VEWO1	首页	监控 策略	对象	网络 系统	
品 安全城	+ 新建 - 🦯 编辑 - 删除	🔿 RORF			
(山 接口	一 接口名称	状态	获取类型	IP/掩码	MAC
So VLAN	ethernet0/0		DHCP	10.0.0.97/24	02db.7646.3396
I DNS	ethernet0/1		静态	0.0.0.0/0	0262.2403.3912
DHCP	vswitchif1	ଜ୍ କ୍କୁ କୁ	静态	0.0.0.0/0	001c.150c.2f12

3. 在弹出的对话框中,选择"绑定三层安全域"。

在"IP配置"的"类型"部分,选中"自动获取"单端按钮,开启DHCP。

ernet 接口		
基本配置	基本 化 五 接口名称: ethernet0/1	
属性	描述: (0-63) 字符	
高级	绑定安全域: ◎ 二层安全域 ◎ 三层安全域 ◎ TAP ◎ 无绑定	
RIP	安全域: untrust V	
	IP配置 英型: ◎ 静态IP ⑧ 自动获取 ◎ PPPoE	
	☑ DHCP 服务器提供的网关信息设置为默认网关路由	
	高级选项 DDNS	
	管理方式 I Teinet III SSH III Ping III HTTP III HTTPS III SNMP	
	路由 逆向路由: ⑧ 点用 ◎ 关闭 ◎ 自动	
	WAP智能分流: 回 启用	
	确定 取:	肩

然后选中"DHCP服务器提供的网关信息设置为默认网关路由"单选按钮。

4. 点击"确定"返回接口列表,刷新一下,可以看到ethernet0/1已经获取到了AWS分配给eth1的子网IP地址。

+	★ 禁福 • √ 新盛 ■ 医尿 ○ 憂葉									
	接口名称	状态	获取类型	IP/掩码	MAC	安全域				
	ethernet0/0		DHCP	10.0.0.97/24	02db.7646.3396	trust				
	ethernet0/1		DHCP	10.0.2.88/24	0262.2403.3912	untrust				
	vswitchif1	ୟ ୧ ୟ ୟ	静态	0.0.0/0	001c.971e.c312	NULL				

或者,在命令行界面,使用以下命令:

SG-6000# config

SG-6000(config) # interface ethernet0/1

SG-6000(config-if-eth0/1) # ip address dhcp setroute

创建策略

创建一条允许所有方向流量通过的策略。

- 1. 选择"策略 > 安全策略",点击"新建"。
- 2. 配置一条允许所有方向的所有类型流量都通行的策略。

約配置								
基本配置		名称:		Permit				(0~95)字符
10-412/03平	源信息							
rap)delula.		安全域:		Any			~	
		地址:		Any			~	
		用户/用户组:					*	
	目的信息							
		安全域:		Any			~	
		地址:		Any			~	
	其它信息							
		服务/服务组:		Any			~	
		应用/应用组:		Any			~	
		时间表:					*	
	行为							
		④ 允许	◎拒	絶	◎安	全连接		
		WebikiE	~ 1	ocal	Y	Web认证只能	能在trust-vr	
				-		and take		
				确定		取消		

- 3. 点击"确定"。
- 或者,在命令行界面,使用以下命令:

SG-6000(config) # rule id 1 from any to any service any permit

测试

为了测试私网服务器的流量是否能通过虚拟防火墙,需要在私网中创建虚拟机。

创建测试用虚拟机 (Windows)

下面,以安装一个Windows2012 Server虚拟机为例,测试防火墙是否实现了连通私网与公网的作用。

第一步:创建VPC子网

- 1. 在VPC控制面板,点击"子网",然后点击"创建子网"。
- 2. 输入子网名称 "Private",在 "VPC" 下拉菜单选择您的VPC,在 "CIDR块" 输入子网地址 "10.0.1.0/24"。

创建子网 ×
使用 CIDR 格式指定子网的 IP 地址块(例如 10.0.0.0/24)。请注意,块大小必须介于 /16 网络掩码和 /28 网络撬码之间。另请注意,子网的大小可与 VPC 的大小相同。
名称标签 Private ①
VPC vpc-041d0366 (10.0.0.0/16) VPC •
可用区 无首选项 🔻 🚺
CIDR 块 10.0.1 0/24
取消 是,创建

3. 完成后,可以在子网列表中看到三个子网。

Q	搜索子网及其属性		×											
	名称	-	子网 ID	Ŧ	状态	+	VPC	•	CIDR	Ŧ	可用 IP	~	可用区	Ŧ
	Private		subnet-13e2fb71		available		vpc-041d0366 (10.0.0.0/16) VPC		10.0.1.0/24		251		cn-north-1a	
	Public		subnet-289f864a		available		vpc-041d0366 (10.0.0.0/16) VPC		10.0.2.0/24		250		cn-north-1a	
	Manage		subnet-e4edf486		available		vpc-041d0366 (10.0.0.0/16) VPC		10.0.0.0/24		249		cn-north-1a	

第二步:修改路由表

修改私网服务器的路由表,按照以下步骤:

1. 在VPC控制面板,点击"路由表"。为了便于查找,将主路由表名称更改为"VFW"。



2. 点击下方的"路由"标签页,点击"编辑",增加一条目标为虚拟防火墙eth0接口的路由。

rtb-2b45a24e VFV	v					
摘要	路由	子网关联	路E	由传播		标签
取消 保存						
目的地	目标		状态	已传播	删除	
10.0.0/16	local		活跃的	否		
0.0.0/0	eni-ef88a	b8a)	舌	8	
添加其他路由						

3. 点击"保存"。

第三步:创建EC2实例。

- 1. 在EC2控制面板,点击"启动实例"。
- 2. 从AWS的AMI社区资源中,选取Windows Server 2012版本,点击"选择"。



- 3. 在实例类型中,选择默认的实例类型即可,点击"下一步:配置实例详细信息"。
- 4. 选择VPC和私网服务器所在的 "Private" 子网 (Subnet 1: 10.0.1.0/24)。



- 5. 依次点击"下一步",在"添加存储"和"标签实例"均使用默认值。
- 6. 在"配置安全组"页面,添加一个允许所有流量的规则。

	分配安全组:	 创建一个新安全组 10.11/		
	安全组名称:	◎ 这样一个 现有时 安全组 Windows2012		
	描述:	Windows2012		
类型 ①		协议 ①	端口范围 ①	来源 ①
RDP	Y	TCP	3389	任何位置 • 0.0.0.0/0
所有流量	•	全部	0 - 65535	任何位置 • .0.0.0/0
添加规则				

- 7. 在审核页面查看已配置的信息,然后点击"启动"。
- 8. (重要)在弹出的对话框中,选择"创建新密钥对",输入任意名称,然后点击"下载密钥对",浏览器将自动下载私钥文件。将下载的私钥文件(.pem)保存到本地一个安全位置,留后续使用。



9. 点击"启动实例"。虚拟的Windows Server将开始启动。

第四步:连接测试实例

将私钥解密获取登录Windows的密码,按照以下步骤:

1. 在EC2实例中,右键单击刚刚创建的Windows实例,选择"连接"。

i-c360b5fb	t2.micro	连接,师
i-8b8f40b3	t2.micro	获取 Windows 密码
i-09589331	t2.medium	启动更多类似项
i-be6ebb86	t2.micro	实例状态 ▶
i-ad864f95	t2.micro	实例设置 ▶
i-c036f6f8	t2.medium	
i-4515d17d	t2.micro	CloudWatch 监控 ▶

2. 在弹出的对话框中,点击"获取密码",然后在弹出的对话框中,点击"选择文件",将下载的私钥(.pem)文件导入。

3. 点击"解密密码",界面显示密码。建议将此密码复制到一个文本文件中保存。



4. 关闭该对话框。

第五步:创建DNAT规则

创建一条目的NAT规则,将访问接口eth1的连接转换为私网服务器的地址。

- 1. 选择"策略 > NAT > 目的NAT",点击"新建"。
- 2. 在弹出的对话框中,"源地址"设置为Any;"目的地址"设置eth1接口的私网IP;"将地址转换为"输入私网服务器的IP地址。

目的NAT配置					
基本配置	当IP地址符合以下 虚拟路由器:	条件时 trust-vr	v		
更多配置	源地址:	地址条目	~	Any	~
	目的地址:	IP地址	×	10.0.2.88	
	服务:	Any	*		
	将地址转换为 动作:	● 转换	◎ 不转换	40.0.4.22	
	转换为IP:	IP地址	*	10.0.1.33	
	将服务端口转换为			(4.05.505)	
	转换端口: 会赴均衡。	□ 启用 转换端口:	1号按合约	(1-65,535) 新列太同的内网昭冬半	
	***		Call 10 2X POI	A1497111-1697197-90892100	
	共體 HA组:				
	描述:				(0-63) 字符
					确定取消

3. 点击"确定"。

或者,在命令行界面,使用以下命令:

SG-6000(config) # ip vrouter trust-vr

SG-6000 (config) # dnatrule from any to 10.0.2.88 trans-to 10.0.1.33

(可选)第六步:创建SNAT规则

SNAT规则使得私网服务器能够访问互联网。如果您的私网服务器只用作业务服务器,不需要主动访问互联网的,可以忽略该配置。

- 1. 选择"策略 > NAT > 源NAT",点击"新建"。
- 2. 创建将所有流量转换为出接口IP的SNAT规则。

甘本教學	当时兼计符合以下	下冬件时			
至少相位	虚拟路由器:	trust-vr	v		
更多配置	源地址:	地址条目	*	Any	~
	目的地址:	地址条目	v	Any	~
	出流量:	所有流量	v		
	服务:	Any	¥		
	将地址转换为				
	转换为:	 出接口IP 	⑤ 指定II	 ○ 不转换 	
	模式:	动态端口			
	Sticky:	□ 启用			
	启用Sticky后,	每一个源IP产生的所:	有会话将被	e映射到同一个固定的IP	地址
	11.44				
	HA组:	● 0 ○ 1			
	措述:				(0-63) 字符
	描述:				(0-63) 字符
	描述:				(0-63) 字符
	描述:				(0-63) 字符
	描述:				(0-63) 字符

3. 点击"确定"。

或者,在命令行界面,使用以下命令:

SG-6000(config) # ip vrouter trust-vr

SG-6000(config) # snatrule from any to any trans-to eif-ip mode dynamicport

开始测试

开始测试之前,确保vFW具有以下配置:

- >> 一条全通的安全策略("创建策略"在第44页)
- >>> 接口eth0和eth1均开启了DHCP并已经获得VPC私网地址("配置子网和接口"在第40页)
- 》 创建了DNAT规则("第五步:创建DNAT规则"在第49页)
- » 如果需要从私网服务器访问公网,需要已经创建SNAT规则("(可选)第六步:创建SNAT规则"在第49页)

测试一:远程连接虚拟服务器

在一个连接互联网的PC上,使用远程桌面程序登录虚拟服务器。

- 1. 在Windows系统的开始界面中,输入"mstsc"并敲回车键。
- 2. 系统启动Windows的远程桌面程序, 输入公网IP地址(接口eth1的公网地址)。

5	远程桌面连接 — — — — — — — — — — — — — — — — — — —
Vert and the second sec	远程桌面 连接
计算机(<u>C</u>):	54.223.147.156 v
用户名:	Administrator
当你连接时将	向你询问凭据。
💽 显示选项	(2) 连接(1) 帮助(1)

3. 点击"连接",复制粘贴通过解密私钥获得的密码。如果复制粘贴密码后,系统提示错误,请尝试手动输入密码。

Windows 安全	×
输入你的凭据 这些凭据将用于连接 54.223.147.156。	
Administrator	
使用其他帐户	
□ 记住我的凭据	
确定取消	۲.

4. 在弹出的证书错误提示中,点击"是",继续登录。

5. 成功登录到虚拟机的 Windows Server 系统。

E	7			▼ ₩ all	54.223.147.156	_ 8 × /		
24 24	284						Hostname : Instance ID : Private IP Address :	WIN-M28AE824VV3 1-c360b5fb 10.0.1.33
E	2						Availability Zone : Instance Size : Architecture :	cn-north-la t2.micro AMD64
Feed	back							
E Mic	2							
						- Windo	ows Server 2012 R2	
		2						10/48 10/48 2015/4/23

测试二:虚拟服务器访问公网

如果您在vFW中配置了SNAT规则,那么您的私网服务器也可以访问互联网。



测试三:查看防火墙进出站流量

登录防火墙,选择"监控 > 设备监控 > 概览",可以看到防火墙接口的进出站流量已经被监测到。

