

虚拟Web应用防火墙（vWAF）部署手册

Version 3.0



Copyright 2022 Hillstone Networks. 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 .

Hillstone Networks

本文档禁止用于任何商业用途。

联系信息

北京

苏州

地址：北京市海淀区宝盛南路1号院20号楼5层 地址：苏州市高新区科技景润路181号

邮编：100192

邮编：215000

联系我们：https://www.hillstonenet.com.cn/about/contact_Hillstone.html

关于本手册

本手册介绍山石网科的vWAF的部署方法。

获得更多的文档资料，请访问：<https://docs.hillstonenet.com.cn>

针对本文档的反馈，请发送邮件到：TechDocs@hillstonenet.com

山石网科

<https://www.hillstonenet.com.cn>

TWNO: TW-DPL-vWAF-3.0-CN-V1.0-6/20/2022

目录

目录	1
介绍	1
文档内容	1
目标读者	1
产品信息	1
VMware Tools的功能	2
Cloud-init的功能	2
许可证	3
许可证机制	3
平台类许可证	3
订阅类许可证	4
功能服务类许可证	4
申请许可证	4
安装许可证	5
许可证校验	5
在KVM上部署vWAF	8
系统要求	8
vWAF的工作原理	8
准备工作	8
安装步骤	9
步骤一：获取vWAF软件包	9

步骤二：导入脚本和系统文件	9
步骤三：首次登录vWAF	11
将vWAF联网	11
步骤一：查看接口的信息。	12
步骤二：连接接口	12
其他操作	13
查看vWAF	13
启动vWAF	14
关闭vWAF	14
升级vWAF	14
重启vWAF	14
卸载vWAF	14
访问vWAF的WebUI界面	15
在Openstack上部署vWAF	16
系统要求	16
安装步骤	16
步骤一：导入镜像文件	16
步骤二：创建云主机类型（Flavor）	18
步骤三：创建网络	20
步骤四：启动实例	20
访问vWAF	22
在VMware ESXi上部署vWAF	24
支持的部署场景	24

系统要求和限制	24
部署vWAF	26
安装vWAF	26
通过OVA模板安装vWAF	26
通过VMDK文件安装vWAF	28
第一步：导入VMDK文件	28
第二步：创建虚拟机	29
第三步：添加硬盘	30
启动和访问vWAF	31
在Xen平台上部署vWAF	32
系统要求	32
部署vWAF	32
步骤一：获取防火墙软件包	32
步骤二：导入镜像文件	32
步骤三：首次登录防火墙	34
访问vWAF的WebUI界面	35
升级vWAF	35
在Hyper-V上部署vWAF	35
系统要求	36
虚拟Web应用防火墙的工作原理	36
准备工作	37
安装步骤	37
步骤一：获取vWAF软件包	37

步骤二：创建虚拟机	37
步骤三：首次登录vWAF	40
访问虚拟Web应用防火墙的WebUI界面	41
升级虚拟Web应用防火墙	41
在微软云Azure上部署vWAF	42
组网设计	42
部署虚拟Web应用防火墙	43
第一步：创建容器	43
第二步：上传安装包	44
第三步：创建映像	45
第四步：创建虚拟机	46
第五步：查看IP	48
第六步：从外网访问vWAF	49
使用SSH2远程登录vWAF:	49
使用HTTPS远程登录vWAF:	50
第七步：购买并申请许可证	50
在AWS上部署vWAF	51
AWS介绍	51
位于AWS的vWAF	52
准备您的VPC	52
第一步：登录AWS账户	53
第二步：为VPC添加子网	53
第三步：为子网添加路由	54

在亚马逊云AWS上部署vWAF	55
创建vWAF实例	55
第一步：创建EC2实例	55
第二步：为实例选择Amazon系统镜像（AMI）	56
第三步：选择实例类型	57
第四步：配置实例详细信息	57
第五步：添加存储	57
第六步：标签实例	58
第七步：配置安全组	58
第八步：启动实例	59
配置子网和接口	60
分配弹性IP地址	60
在主控制台查看实例	60
购买并申请许可证	61
访问vWAF	61
使用PuTTY访问CLI管理界面	61
步骤一：使用PuTTYgen转换密钥对	61
步骤二：使用PuTTY访问CLI界面	62
访问WebUI界面	64
在亚马逊云AWS上进行vWAF的HA部署	66
组网设计	66
部署步骤	66
第一步：创建VPC及子网	67

第二步：创建及启用Internet网关	67
第三步：创建策略	68
第四步：创建IAM角色	70
第五步：创建EC2实例	72
第六步：创建网络接口	72
第七步：连接并配置vWAF	74
第九步：在AWS上配置云服务器的路由	80
第十步：在vWAF配置站点及策略	81
配置结果	82
在阿里云AliCloud上部署vWAF	83
系统要求	83
准备工作	83
部署虚拟Web应用防火墙	83
步骤一：创建对象存储	84
步骤二：导入镜像	85
步骤三：创建ECS实例	85
步骤四：为VPC设置默认路由	86
步骤五：访问vWAF	86
使用HTTPS远程登录vWAF:	87
在阿里云上进行vWAF的HA部署	87
组网设计	87
部署步骤	88
第一步：创建RAM角色	88

第二步：创建交换机	89
第三步：创建vWAF实例	91
第四步：新增弹性网卡并配置辅助私网IP	92
第五步：购买弹性公网IP并绑定到弹性网卡	93
第六步：申请AccesKey	93
第七步：在vWAF上进行HA相关配置	94
第八步：在vWAF配置站点及策略	99
配置结果	100
在腾讯云上部署vWAF	101
系统要求	101
安装步骤	101
步骤一：创建VPC	101
步骤二：创建子网	102
步骤三：创建对象存储	103
步骤四：导入镜像	103
步骤五：创建云服务器	104
步骤六：访问vWAF	107
使用HTTPS远程登录vWAF	108
在腾讯云上进行vWAF的HA部署	109
组网设计	109
部署步骤	109
步骤一：创建VPC及子网	110
步骤二：创建vWAF云主机	110

步骤三：创建弹性网卡	111
步骤四：申请高可用虚拟IP	112
步骤五：在vWAF上进行HA相关配置	113
步骤六：验证HA结果	118
步骤七：在vWAF配置站点及策略	119
配置结果	119
在腾讯云上通过辅助IP进行vWAF的HA部署	121
组网设计	121
部署步骤	121
步骤一：创建VPC及子网	122
步骤二：创建vWAF云主机	122
步骤三：创建弹性网卡并配置辅助IP	123
步骤四：创建访问密钥	124
步骤五：在vWAF上进行HA相关配置	124
步骤六：验证HA结果	129
步骤七：在vWAF配置站点及策略	130
配置结果	131
在华为云上部署vWAF	132
系统要求	132
安装步骤	132
步骤一：创建虚拟私有云	132
步骤二：创建云服务器/部署vWAF	133
步骤三：绑定弹性公网IP	135

步骤四：访问vWAF	136
步骤五：通过外网访问vWAF	136
使用SSH2远程登录	136
使用HTTPS登录vWAF	137
在华为云上进行vWAF的HA部署	138
组网设计	138
部署步骤	138
步骤一：创建虚拟私有云VPC及子网	139
步骤二：创建vWAF云服务器	139
步骤三：申请虚拟IP	140
步骤四：在vWAF上进行HA相关配置	141
步骤五：验证HA结果	146
步骤六：在vWAF配置站点及策略	147
配置结果	147
在H3C CAS上部署vWAF	148
系统要求	148
安装步骤	148
步骤一：创建虚拟交换机	148
步骤二：创建vWAF虚拟机	149
步骤三：登录vWAF进行相关配置	151
访问vWAF	152
使用SSH2远程登录	152
使用HTTPS远程登录	153

介绍

山石网科的虚拟Web应用防火墙，简称为vWAF（Virtual Web Application Firewall），是一个纯软件形态的产品，是运行在虚拟机上的WAF系统。

文档内容

本手册介绍如何将vWAF部署到不同的环境中，包括KVM、Openstack、Vmware环境中。本文仅讲述vWAF和初始的联网操作，WAF系统本身的功能将不做讲解。

如果您需要了解WAF系统的详细功能，请参考WAF的相关文档（[点击此处](#)）。

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、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vWAF有关的操作。

产品信息

vWAF系列虚拟Web应用防火墙产品包含多种型号，每种型号的产品要求虚拟机的最低配置如下：

产品型号	最低配置	推荐磁盘大小	可保护站点的数量
SG-6000-WV02	2个vCPU，4G内存	100GB及以上	16个站点
SG-6000-WV04	4个vCPU，8G内存	100GB及以上	32个站点
SG-6000-WV08	8个vCPU，16G内存	100GB及以上	128个站点
SG-6000-WV12	12个vCPU，24G内存	100GB及以上	256个站点



注意：虚拟Web应用防火墙的型号是由CPU许可证授权数和实际虚拟机配置的规格（CPU和内存）共同确定，以两者中较低的数值最终确定虚拟Web应用防火墙的型号。若实际安装环境未达到上述要求的最低配置，将无法启动对应型号的虚拟Web应用防火墙。

VMware Tools的功能

vWAF集成了VMware Tools，因此可以在Vmware虚拟化平台中实现自动化部署。vWAF部署完成后，在vCenter中打开其所在的虚拟机的电源，然后点击该虚拟机的摘要页面，可以查看vWAF的管理接口的IP地址、CPU、内存、接口流量等基本信息。

Cloud-init的功能

Cloud-init是专为云环境中虚拟机的初始化而开发的工具，它能从各种数据源读取相关数据（目前支持URL和configdrive两种获取方式）并据此对虚拟机进行配置。当cloud-init获取数据信息后，开始对虚拟机进行配置，常见的配置包括：用户名密码，路由等。vWAF中集成了cloud-init，使得cloud-init能够伴随vWAF的启动而运行，因此可以在虚拟化环境中实现vWAF的自动化部署。



注意:

- Cloud-init配置文件注入vWAF虚拟机会存在延迟，可等待几分钟后再次查看虚拟机的配置。若等待10分钟后仍未注入，可重启虚拟机再查看。
- 如果某条命令注入不成功，请检查命令是否拼写错误或使用了单词简写形式。

许可证

vWAF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

vWAF的许可证机制分为平台许可证、订阅类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。

平台许可证安装后，设备的SN号将进行变更，即变为虚拟SN（简称“vSN”）。若用户想继续获取功能服务类或订阅类许可证，可通过该vSN号进行申请。vWAF重新安装后，许可证不依赖于原系统的SN号，故原先申请的许可证仍可继续使用。同时，Hillstone提供公网和局域网LMS许可证服务器，对许可证进行校验及许可证的管理，保证许可证的安全。

平台类许可证

vWAF系统初始预装有一个免费的默认许可证（default license），无需申请。用户可根据需求申请平台订阅许可证和平台正式许可证。

- **默认许可证（Default）**

vWAF预装了一个免费的默认许可证（default license），无需申请。装有默认许可证的系统支持所有的功能，但是性能受限，例如系统仅支持创建1个站点，HTTP会话连接数仅支持500个等等。该许可证的有效期为30天。到期后，系统的所有功能将不能使用，且系统版本和所有的特征库将不能升级。

- **平台订阅许可证（Platform Sub）**

安装平台订阅许可证后，系统支持的功能和性能与正式许可证相同，但是使用期限较短。具体使用时间，根据申请时协议决定，该使用时间指的是绝对时间，例如2017年3月1日到2017年3月31日。到期后，已有的配置不能修改，重启后仅平台的功能可用，且性能受限。

- **平台正式许可证（Platform Base）**

产品正式销售后，可以安装平台正式许可证。正式许可证提供基础Web应用防火墙功能，并且防火墙性能可达到标称数值。到期后，系统仍可正常使用，但不能升级到到期后的系统版本。



注意:

平台许可证过期时，系统安装的订阅许可证和功能服务类许可证仍然有效，但不能升级到到期后的系统版本。

订阅类许可证

订阅类许可证能够控制相关功能是否开启及其使用期限。

- **CPU订阅许可证**

授权vWAF可配置的CPU的最大数量。CPU许可证有正式和试用两种类型，正式CPU许可证不会过期。试用许可证过期后，系统将会立即重启，重启后将恢复到最低型号SG-6000-WV02的配置，即2vCPU。

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。

- **WAF规则库许可证**

提供vWAF规则库升级功能。过期后不能升级系统的WAF规则库。已加载的WAF规则库正常工作。

- **反爬虫服务许可证**

提供vWAF的站点上的反爬虫服务。过期后，不能使用反爬虫服务功能。

- **WAF IP信誉库许可证**

提供vWAF的IP信誉库升级功能。到期后，系统会自动删除IP信誉特征库，且IP信誉防护功能将不能使用。

申请许可证

申请许可证，需要登录vWAF系统。

部署好vWAF后，访问其WebUI界面，然后按照以下步骤生成许可证申请：

1. 登录vWAF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。
4. 选择“系统 > 设备管理”，然后点击<设置及操作>标签页。
5. 点击“重启设备”，然后在提示对话框点击“确定”。
6. 等待系统重启。启动后，许可证将生效。

许可证校验

对于虚拟化产品vWAF安装许可证后，需要连接到许可证服务器，进行合法性校验，以防止许可证被克隆盗版。

目前系统支持两种校验方式，分别是通过互联网连接到公网许可证服务器校验和通过局域网连接到内网LMS(虚拟许可证管理系统)校验，用户可根据需要选择其中的一种方式。

- 互联网：适用于小型私有云或公有云场景。vWAF连接到公网服务器后，服务器将提供许可证的合法性校验（目前公网服务器暂不提供许可证的分发和管理）。若发现克隆许可证的行为或vWAF未连接服务器进行校验，设备将会在30天后重启。

- 局域网：适用于大型私有云或行业云场景。vWAF连接到LMS后，LMS不仅提供许可证的校验，还提供许可证的自动分发和管理。若发现克隆许可证的行为，服务器将回收克隆或被克隆的其中一台vWAF设备的全部许可证并重启该设备；若设备不连接服务器进行校验，将会在30天后重启。

连接许可证服务器，请按照以下步骤进行操作：

1. 选择“系统 > 许可证 > 许可证校验”，进入许可证校验页面。



The screenshot displays the 'License' configuration window, divided into two main sections: 'License 服务器状态' (License Server Status) and 'License 校验配置' (License Verification Configuration). The status section shows '连接状态' (Connection Status) as '连接失败' (Connection Failed), '服务器地址' (Server Address) as '0.0.0.0', '服务器端口' (Server Port) as '0', and '校验方式' (Verification Method) as '局域网' (Local Area Network). The configuration section has '校验方式' (Verification Method) with radio buttons for '互联网' (Internet) and '局域网' (Local Area Network), where '局域网' is selected. Below this are input fields for '服务器地址' (Server Address) and '服务器端口' (Server Port), with a hint '(1 - 65535)' next to the port field. At the bottom are '确定' (OK) and '取消' (Cancel) buttons.

2. 在“License服务器状态”中，显示服务器的连接状态、Session ID 和校验方式。

在“License校验配置”中，用户可根据需要，使用以下两种方式中的一种进行许可证校验

- **互联网**：选中“互联网”单选按钮，点击“确定”按钮，保存配置。vWAF将通过公网服务器进行许可证校验。
- **局域网**：选中“局域网”单选按钮，并指定“服务器地址”和“服务器端口”后，点击“确定”按钮，保存配置。vWAF将通过局域网LMS进行许可证校验、分发和管理。

3. 选择“系统 > 设备管理”，然后点击<设置及操作>标签页。
4. 点击“重启设备”，然后在提示对话框点击“确定”。
5. 等待系统重启。启动后，许可证将生效。



注意: 通过公网服务器进行许可证验证时，请保证连接公网服务器的接口可以访问互联网。关于LMS(许可证管理系统)的更多资料，请参阅《LMS许可证管理系统使用手册》。

在KVM上部署vWAF

使用基于内核的虚拟机（Kernel-based Virtual Machine，缩写为KVM）部署山石网科vWAF，是在单机上创建vWAF的主要方法。

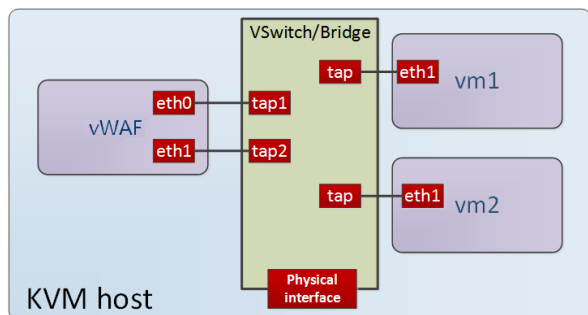
系统要求

在KVM上部署山石网科的vWAF，需要宿主机满足以下要求。

- 要求至少能够提供2个CPU、4 GB内存。
- 使用单机KVM环境：系统已安装软件KVM、qemu、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`）

vWAF的工作原理

将vWAF的虚拟网卡对应的tap接口连接到宿主机中的虚拟交换机（Open Switch或者Linux bridge），虚拟机把vWAF设置为默认网关，vWAF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vWAF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vWAF，按照下面的步骤进行操作：

步骤一：获取vWAF软件包

1. 请登录如以下ftp路径获取并下载vWAF软件包的地址。

下载路径：<ftp://release@release.hillstonenet.com/WAF/hsvwaf>

用户名/密码：hillstonenet/hillstonenet

2. 下载以下文件：

- 脚本文件（名称为“hsvwaf”）。脚本文件包含一些针对vWAF系统文件的操作，例如安装、升级、重启、关闭、查看vWAF等。需要注意的是，该脚本并不适用于所有KVM环境。
- vWAF系统文件（后缀名为.qcow2的镜像文件）。

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vWAF的系统文件，将其上传到KVM服务器的根目录上。
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：

```
root@pxe74867aee16bc:~/cma# ls
hsvwaf  SG6000-VW-5.5R6-2.3-v6.qcow2
```

5. 输入以下命令，安装系统文件。

```
sudo ./hsvwaf install ./vwaf_qcow2 [wv02|wv04|wv08|wv12] vm_name -n if_num
```

<code>sudo</code>	代表该命令使用管理员权限。
<code>./hsvwaf install</code>	执行位于根目录的脚本文件（hsvwaf）的安装命令。
<code>./vwaf_qcow2</code>	安装位于根目录的系统文件。 <code>vwaf_qcow2</code> 是系统镜像文件的全名，包括后缀名.qcow2。
<code>wv02 wv04 wv08 wv12</code>	vWAF的产品型号，如wv02代表SG-6000-WV02型号，具体参考 产品信息 。
<code>vm_name</code>	为当前安装的vWAF指定一个名称。
<code>if_num</code>	为当前安装的vWAF分配接口数量，最多可划分出10个接口,执行上述安装命令不填写该参数，默认自动安装4个接口。

例如，输入以下命令，创建产品类型wv02，名称为vwaf_test，具有3个接口的vWAF。

```
root@pxe74867aee16bc:~/cma# ./hsvwaf install SG6000-VW-5.5R6-2.3-v6.qcow2 wv02 vwaf_test -n 3
1+0 records in
1+0 records out
1048576 bytes (1.0 MB) copied, 0.00140776 s, 745 MB/s
Network vwaf_test-br0 defined from /var/lib/vwaf/vwaf_test/vwaf_test-br0
Network vwaf_test-br0 marked as autostarted
Network vwaf_test-br0 started
Network vwaf_test-br1 defined from /var/lib/vwaf/vwaf_test/vwaf_test-br1
Network vwaf_test-br1 marked as autostarted
Network vwaf_test-br1 started
Network vwaf_test-br2 defined from /var/lib/vwaf/vwaf_test/vwaf_test-br2
Network vwaf_test-br2 marked as autostarted
Network vwaf_test-br2 started

Starting install...
Creating domain...
Domain creation completed. You can restart your domain by running:
  virsh --connect qemu:///system start vwaf_test
vFW vwaf_test installed.
Console access: telnet localhost 7007
SSH access: ssh hillstone@192.168.133.4
```

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7007。

步骤三：首次登录vWAF

刚安装的vWAF默认只开启了Console口的访问权限，可以通过访问该Console口，登录vWAF。

按照以下的步骤初次登录vWAF。

1. 在Linux中输入以下命令，连接vWAF。

telnet localhost port_num

port_num	管理端口号，是步骤二的第6步输出的端口号。
----------	-----------------------

例如，连接上一步骤创建的Conosole端口为7007的vWAF，输入以下命令。

```
root@pxe74867aeel6bc:~/cma# telnet localhost 7007
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

login: █
```

2. 输入vWAF默认的用户名和密码。

login: hillstone

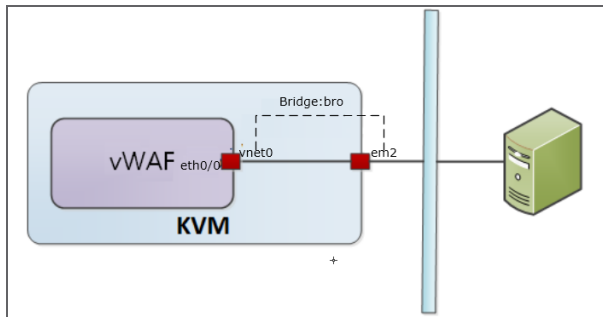
password: hillstone

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

将vWAF联网

当vWAF创建后，vWAF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vWAF的与其他网络（如私网或互联网）连接，将vWAF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vWAF的vnet0接口与物理网络的em2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vWAF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em2：

```
root@pxe74867aee16bc:~/cma# ifconfig
br0      Link encap:Ethernet  HWaddr 74:86:7a:ee:16:bd
         inet6 addr: fe80::7686:7aff:feee:16bd/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:2173361 errors:0 dropped:1693498 overruns:0 frame:0
         TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:100088021 (100.0 MB)  TX bytes:1936 (1.9 KB)
```

2. 在Linux中输入命令**brctl show**查看虚拟网桥和接口。

该信息中，vWAF的“eth0/0”接口自动对应KVM的vnet接口“vnet0”，并自动属于同一个网桥“testvwaf-br0”。物理接口自动从属于网桥“br0”。

```
root@pxe74867aee16bc:~/cma# brctl show
bridge name      bridge id                STP enabled  interfaces
br0               8000.74867aee16bd        no           em2
testvwaf-br0     8000.5254002b1fa3        yes          testvwafbr0-nic
                                                         vnet0
```

步骤二：连接接口

将vWAF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vWAF的“vnet0”接口与物理网络的“em2”接口连接：

1. 在Linux中，输入以下命令，将“vnet0”接口原虚拟网桥testvwaf-br0中删除。

```
sudo brctl delif testvwaf-br0 vnet0
```

2. 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 br0 vnet0
```

3. 输入命令brctl show，确认两个接口属于同一个虚拟网桥。

```
root@pxe/486/aeel6bc:~/cma# brctl show
bridge name      bridge id        STP enabled      interfaces
br0               8000.74867aeel6bd  no               em2
                  vnet0
```

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vWAF

查看vWAF信息，使用以下命令：

```
sudo ./hsvwaf show vm_name
```

./hsvwaf show	执行脚本文件（hsvwaf）的查看命令。
vm_name	vWAF的名称。

例如，在Linux中查看名称为“vwaf_test”的实例：

```
root@pxe74867aeel6bc:~/cma# ./hsvwaf show vwaf_test
vWAF instance: 2
vWAF instance name: vwaf_test
Version: SG6000-VW-5.5R6-2.3-v6.qcow2
Status: running
Console port: 7002
VNC port: :2
Mgmt address: 192.168.133.4
Interface count: 3
Interface detail:
Interface  Type      Source      Model      MAC
-----
vnet6     network  vwaf_test-br0 virtio     52:54:00:f8:3a:d5
vnet7     network  vwaf_test-br1 virtio     52:54:00:e1:f2:e4
vnet8     network  vwaf_test-br2 virtio     52:54:00:16:8f:b1
```

启动vWAF

将已经安装在KVM系统中的vWAF启动，使用以下命令：

```
sudo ./hsvwaf start vm_name
```

./hsvwaf start	执行脚本文件（hsvwaf）的启动命令。
<i>vm_name</i>	vWAF的名称。

关闭vWAF

要关闭vWAF，输入以下命令：

```
sudo ./hsvwaf shutdown vm_name
```

./hsvwaf shutdown	执行脚本文件（hsvwaf）的关闭命令。
<i>vm_name</i>	vWAF的名称。

升级vWAF

vWAF支持在线升级，用户可以直接通过vWAF WebUI界面的“系统 > 升级管理”页面进行系统升级，建议您选择这种方法。具体操作方法请参考《vWAF WebUI用户手册》。

重启vWAF

要重启vWAF，使用以下命令：

```
sudo ./hsvwaf reboot vm_name
```

./hsvwaf reboot	执行脚本文件（hsvwaf）的重启命令。
<i>vm_name</i>	vWAF的名称。

卸载vWAF

要卸载已经安装的vWAF系统，使用以下命令：

```
sudo ./hsvwaf uninstall vm_name
```

./hsvwaf uninstall	执行脚本文件（hsvwaf）的卸载命令。
---------------------------	----------------------

<code>vm_name</code>	vWAF的名称
----------------------	---------

访问vWAF的WebUI界面

vWAF的第一个虚拟接口（eth0/0）默认开启DHCP，如果vWAF连接到启动了DHCP的网络，eth0/0口将自动获得IP地址，查看方法参见[查看WAF](#)。打开浏览器，通过HTTPS的方式访问eth0/0的地址，即可打开WebUI界面。

具体步骤如下：

1. 打开浏览器（推荐使用Chrome浏览器），输入上面eth0/0的IP地址。
2. 输入用户名密码（默认为hillstone/hillstone）
3. 点击“登录”按钮，进入vWAF的WebUI管理界面。
4. 关于如何使用WAF系统，参考WAF的使用手册（[点击此处](#)）。

在Openstack上部署vWAF

系统要求

在Openstack上部署山石网科的vWAF，需要宿主机满足以下要求。

- 要求至少能够提供2个CPU、4GB内存。
- 已经安装Openstack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

将vWAF镜像文件导入到Openstack平台中作为一个镜像：

1. 使用创建的账户，登录Openstack的Web管理界面。



- 2. 从左侧导航栏选择“项目 > 计算 > 镜像”。
- 3. 点击页面右上角的“创建镜像”按钮。
- 4. 在弹出的<创建镜像>对话框中进行设置。

创建镜像

名称 *

描述

镜像源

镜像文件

镜像文件 ⓘ

选择文件

未选择任何文件

镜像格式 *

选择格式

说明:

指定镜像上传到镜像服务

目前镜像URL只支持HTTP/HTTPS，且要求镜像服务能够访问到镜像地址。

请注意：镜像地址必须是有效的直接指向镜像二进制文件的URL。URL被重定向或者服务器返回错误页面将导致镜像不可用。

在标签页设置基本信息。

选项	说明
名称	自定义镜像的名称。
描述	指定镜像的描述信息。
镜像源	在下拉菜单中选择“镜像文件”类型。
镜像文件	点击“选择文件”按钮，从本地PC的文件系统中找到要上传到Openstack的vWAF镜像文件。
镜像格式	在下拉菜单中选择“QCOW2-QEMU模拟器”格式。

- 5. 点击右下角的“创建镜像”按钮，完成配置。新创建的镜像将会显示在镜像列表中。

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。
2. 从左侧导航栏选择 “管理员> 系统> 云主机类型 ”。
3. 点击右上角 “创建云主机类型” 按钮。
4. 在弹出的<创建云主机类型>对话框，进行设置。

创建云主机类型

主机类型信息 *

云主机类型访问

名称 *

云主机类型定义RAM和磁盘的大小、核数，以及其他资源，在用户部署实例的时候使用。

ID ⓘ

auto

虚拟内核 *

内存 (MB) *

根磁盘(GB) *

临时磁盘(GB)

0

Swap磁盘(MB)

0

取消

创建云主机类型

在<云主机类型信息>标签页设置基本信息。

名称	自定义云主机名称。
ID	ID号码由Openstack自动生成。
虚拟内核	指定该主机的CPU虚拟内核的数量。对于vWAF，内核数量指定为2。
内存（MB）	主机的内存大小，单位为MB。对于vWAF，内存最小值为

	4096MB。
根磁盘（GB）	指定根磁盘分区所需容量。单位为GB。建议根磁盘最小值为100GB。
临时磁盘（GB）	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磁盘（GB）	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”按钮，完成配置。

步骤三：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）

步骤四：启动实例

使用创建的账户，创建云主机实例：

1. 使用创建的帐户，登录Openstack界面。
2. 从左侧导航栏选择“项目 > 计算 > 实例”。
3. 点击右上角“启动云主机”按钮。
4. 在弹出的<启动云主机>对话框，进行设置。

启动云主机

详情 *

访问 & 安全

网络 *

创建后

高级选项

可用域

nova

云主机名称 *

test

云主机类型 * ?

SG-6000-WV02_flavor

云主机数量 * ?

1

云主机启动源 * ?

从镜像启动

镜像名称 *

test (104.2 MB)

指定创建云主机的详细信息

详细说明启动云主机的情况,下面的图表显示此项目所使用的资源和关联的项目配额。

方案详情

名称	SG-6000-WV02
虚拟内核	2
根磁盘	2 GB
临时磁盘	0 GB
磁盘总计	2 GB
内存	2,048 MB

项目限制

云主机数量10 中的 2 已使用

虚拟CPU数量20 中的 4 已使用

内存总计51200 中的 4096 MB已使用

取消

运行

在<详情>标签页设置基本信息。

可用域	指定为默认域。
云主机名称	自定义实例名称。
云主机类型	指定云主机类型（flavor）。

云主机数量	指定云主机数量。
云主机启动源	指定云主机启动源为“从镜像启动”
镜像名称	选择步骤一中配置的镜像名称。

在<网络>标签页点击”+“按钮选择网络。



5. 点击右下角“运行”按钮，完成配置。

访问vWAF

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。
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 > 计算 > 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“云主机名称”。

☐	云主机名称	镜像名称	IP 地址	配置	值对	状态	可用域	任务	电源状态	从创建以来	动作
☐	test_hillstone	test									

4. 打开浏览器（推荐使用Chrome浏览器），系统默认开启HTTPS管理方式，输入云主机的浮动IP地址，如“https://浮动IP”。
5. 输入用户名密码（默认为hillstone/hillstone）
6. 点击“登录”按钮，进入vWAF的WebUI管理界面。
7. 关于如何操作vWAF，参考山石网科的Web应用防火墙的使用手册（[点击此处](#)）。

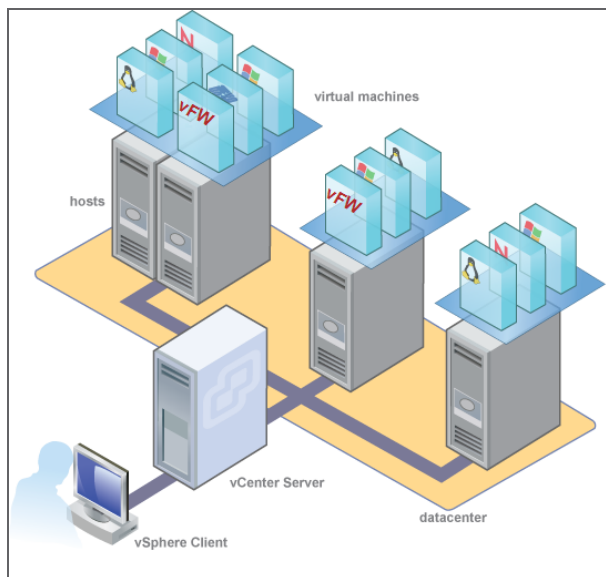
在VMware ESXi上部署vWAF

vWAF通过VMDK格式或OVA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。

vWAF的部署，要求您必须已经熟悉VMware的vSphere 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vWAF虚拟Web应用防火墙。



系统要求和限制

vWAF的使用要求和限制：

- VMware ESXi 的版本为5.0、5.5或6.0。
- 虚拟机要求最少使用2个vCPU、内存最小为4GB。
- 建议每个vWAF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VMXNET-3。建议每台虚拟机只安装同一类型的网卡，不要同时安装E1000网卡和VMXNET-3网卡。

部署vWAF

将vWAF部署在ESXi服务器上，我们建议您使用vCenter和vSphere Client相结合的方式安装和管理。

用户可以通过导入OVA模板和导入VMDK文件两种方式进行部署，推荐用户使用通过OVA模板的方式。部署完成后，后续用户可使用img文件进行在线升级。如果您的ESXi版本为6.0，建议使用OVA模板进行部署。

安装vWAF

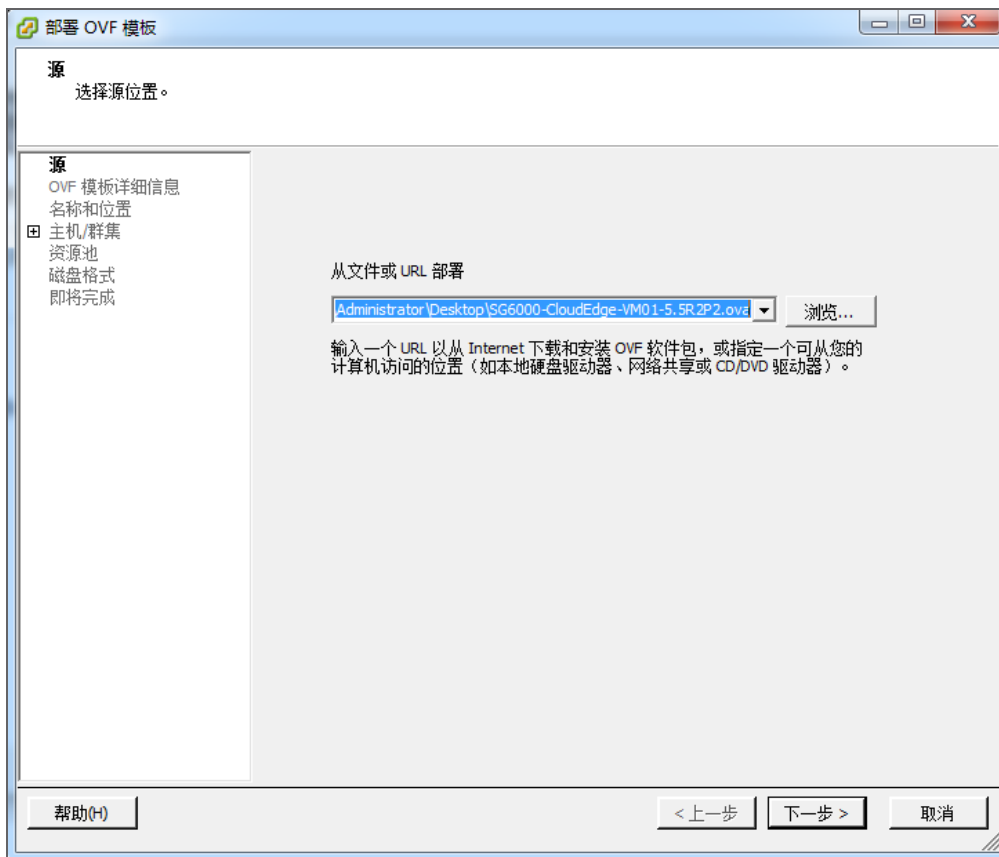
通过OVA模板安装vWAF

在安装vWAF之前，请先设置好ESXi Server主机、vCenter Server主机和vSphere Client主机，并获取OVA文件。

安装vWAF请按照以下步骤进行操作：

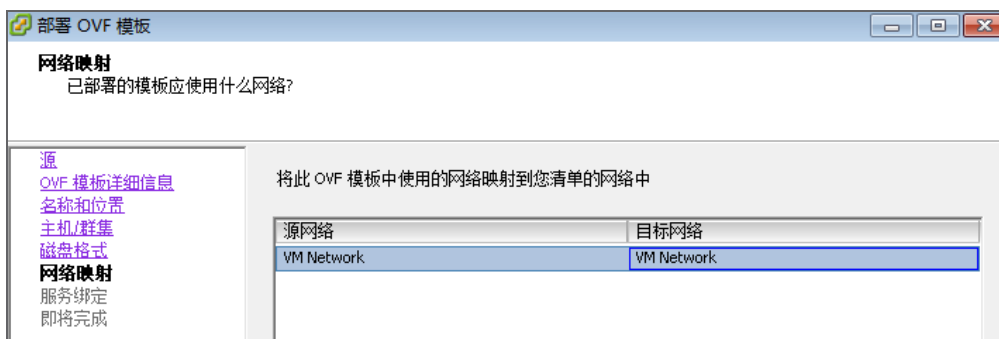
1. 将OVA文件保存在本地。
2. 双击vSphere Client客户端，在登录页面中输入vCenter Server的IP地址或名称，然后输入用户名和密码，点击“登录”。
3. 登录vCenter Server后，点击左侧“localhost”根节点，然后点击“文件 > 部署OVF模板”。

- 从弹出的“部署OVF模板”对话框中点击“浏览”，从文件系统中选择OVA文件，然后点击“下一步”。



- 确认OVF模板详细信息后，点击“下一步”。
- 输入OVF模板的名称，并选择清单位置，点击“下一步”。
- 选择要在其上部署 OVF 模板的主机或群集，点击“下一步”。
- 选择要在其中运行 OVF 模板的资源池，点击“下一步”。
仅当群集包含资源池时，系统才会显示此页面。
- 数据存储已被默认选择，点击“下一步”。

10. 选择模板使用的网络，点击“下一步”。



11. 配置服务绑定，默认“vCenter Extension vService”即可，点击“下一步”。
12. 单击”完成“按钮，启动部署任务。

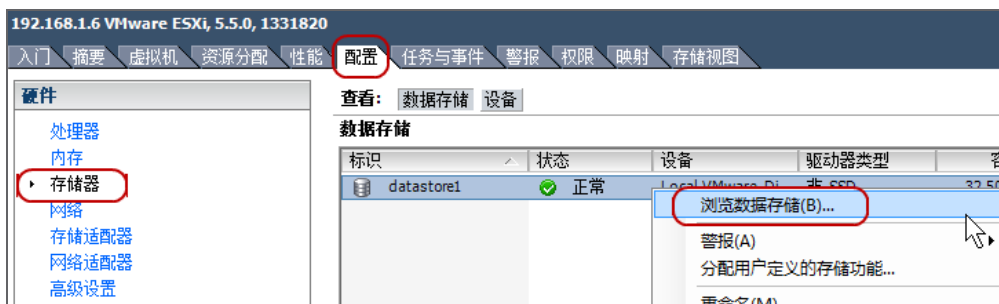
稍等片刻，即可部署成功。

通过VMDK文件安装vWAF

在部署vWAF之前，请先申请试用版本或联系销售人员，获取vWAF的VMDK文件。

第一步：导入VMDK文件

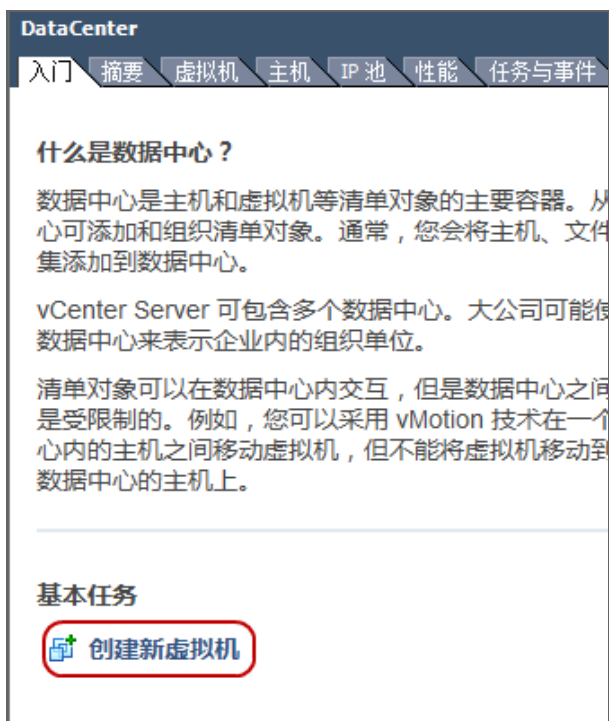
1. 将vWAF的VMDK文件保存在本地。
2. 在vSphere Client中，点击“主页 > 清单 > 主机和集群”，然后在左侧列表中点击vWAF所在的ESXi主机。
3. 在右侧页面点击“配置”标签页，选择左侧导航栏的“存储器”，然后右键点击数据存储，选择“浏览数据存储(B)...”。



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vWAF的VMDK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”。

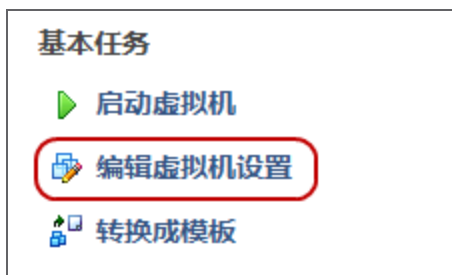


3. 在弹出虚拟机向导中，选择“自定义（Custom）”配置类型，点击“下一步”。
4. 在<名称和位置>选项卡中，输入虚拟机的名称并选择数据中心，然后点击“下一步”。
5. 在<存储器>选项卡中，选择目标存储，点击“下一步”。
6. 在<虚拟机版本>选项卡中，选择“虚拟机版本：8”，点击“下一步”。
7. 在<客户机操作系统>选项卡中，选择“Windows”，点击“下一步”。

8. 在<CPU>选项卡中, 根据您要创建的vWAF类型进行选择, 具体参照[产品信息](#)。选择完成, 然后点击“下一步”。
9. 在<内存>选项卡中, 根据vWAF类型进行选择。具体参照[产品信息](#), 选择完成后, 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, 保留默认选项, 点击“下一步”。
12. 在<选择磁盘>选项卡中, 选择“不创建磁盘”, 点击“下一步”。
13. 点击“完成”。

第三步：添加硬盘

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vWAF, 点击右侧页面的“编辑虚拟机设置”。

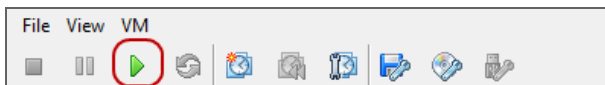


2. 在弹出的<虚拟机属性>对话框中, 点击“添加”按钮。
3. 在弹出的<添加硬件>对话框中选择<硬盘>, 点击“下一步”。
4. 选择“使用现有虚拟磁盘”, 点击“下一步”。
5. 找到第一步中上传到数据存储的VMDK文件, 点击“下一步”。
6. 保持默认选项, 点击“下一步”。
7. 点击“完成”, 系统将生成虚拟机。

启动和访问vWAF

完成上面的所有配置之后，就可以启动vWAF的虚拟机了。

1. 在vSphere Client中，点击“主页 > 清单 > 虚拟机和模板”。
2. 右键单击vWAF，选择“打开控制台”，vSphere Client弹出新的对话框，连接vWAF的Console口。
3. 点击绿色电源按钮。



4. 稍等片刻，该vWAF即可启动。vWAF的第一个虚拟接口（eth0/0）默认开启DHCP，如果vWAF连接到启动了DHCP的网络，eth0/0口将自动获得IP地址。
5. 打开浏览器（推荐使用Chrome浏览器），系统默认开启HTTPS的管理方式，输入eth0/0的IP地址，如“https://IP地址”。
6. 输入用户名密码（默认为hillstone/hillstone）
7. 点击“登录”按钮，进入vWAF的WebUI管理界面。
8. 关于如何使用vWAF系统，参考vWAF的使用手册（[点击此处](#)）。

在Xen平台上部署vWAF

vWAF虚拟Web应用防火墙通过VHD格式封装，可以安装在XenServer服务器上。

在Xen平台上vWAF的部署，要求您必须已经熟悉Xen的Hypervisor 架构、XenServer主机设置和Xen虚拟机部署等知识。

系统要求

山石网科的vWAF可以安装在X86架构的XenServer物理服务器上。

XenServer主机需满足以下要求：

- 支持Intel VT 或者 AMD-V
- 至少能够分配2个虚拟网卡，网卡速度100MB/s及以上
- 64位CPU，主频1.5GHz及以上
- 2G内存及以上
- 100G硬盘及以上，硬盘类型可以是PATA、SATA和SCSI

部署vWAF

在安装vWAF之前，请先设置好XenServer主机和XenCenter客户端。

步骤一：获取防火墙软件包

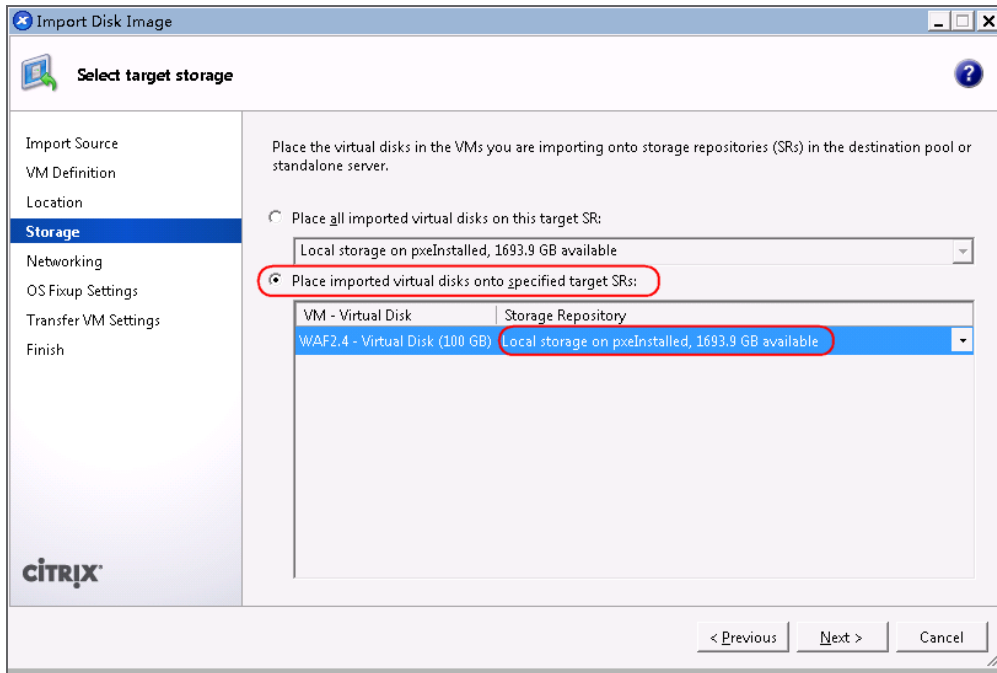
请联系客服人员获取下载防火墙软件包的地址，并将VHD镜像文件保存到管理主机的文件系统中。

步骤二：导入镜像文件

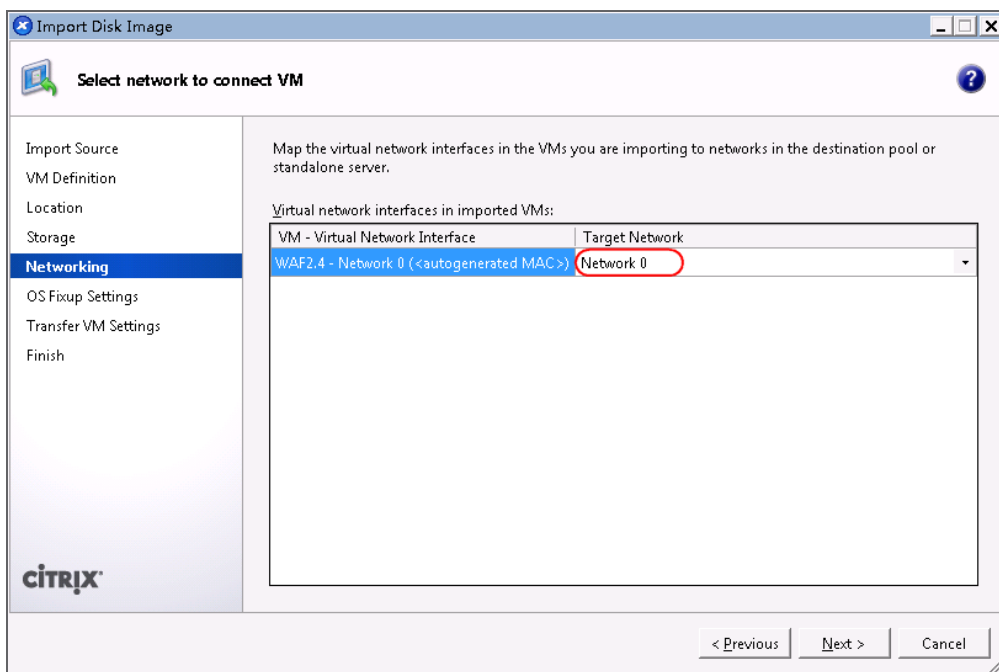
安装vWAF请按照以下步骤进行操作：

1. 双击XenCenter客户端，然后点击工具栏中的“Add new server”按钮，在弹出的对话框中输入一个XenServer的IP地址或名称，然后输入用户名和密码，点击“Add”。

2. 登录XenCenter后，点击“File > Import”，弹出导入向导对话框。
3. 点击“Browse”，选择将要部署的vWAFVHD镜像文件，然后点击“Next”。
4. 指定虚拟机的名称，并配置虚拟机的内存和CPU的数量（可参考[产品信息](#)），然后点击“Next”。
5. 选择虚拟机所在的资源池和宿主机，然后点击“Next”。
6. 配置VHD镜像文件上传到本地存储，然后点击“Next”。



7. 配置虚拟机的虚拟网卡（即vWAF的接口）所连接的外部网络，然后点击“Next”。



8. 选择“Don't use Operating System Fixup”单选按钮，然后点击“Next”。

9. 配置Transfer VM（临时VM）所连接的外部网络，然后点击“Next”。

- 如果您的网络中部署了DHCP服务，请选择“Automatically obtain network settings using DHCP”。
- 如果您的网络中未部署DHCP服务，请选择“Use these network settings”进行手动配置，该IP地址需和XenCenter客户端IP地址处于同一网段。

10. 确认配置信息后，点击“Finish”按钮，启动导入任务。

步骤三：首次登录防火墙

按照以下的步骤初次登录防火墙。

1. 在左侧虚拟机列表中，选中vWAF所在的虚拟机后，单击右键，选择“Start”。
稍等片刻，虚拟机即可启动成功。
2. 键入回车后，输入vWAF默认的用户名和密码。

login: hillstone

password: hillstone

- 至此，你可以使用命令行界面对vWAF系统进行操作。建议您及时修改用户名和密码。

访问vWAF的WebUI界面

vWAF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：

- 参考上述步骤三的方法，登录防火墙。
- 登录后，输入以下命令，查看eth0/0接口的IP地址。
show interface ethernet0/0
- 打开浏览器（建议使用Chrome浏览器），输入上面显示的IP地址。
- 输入用户名密码（默认为hillstone/hillstone）。
- 点击“登录”按钮，进入vWAF的WebUI管理界面。
- 关于如何使用WAF系统，参考WAF的使用手册（[点击此处](#)）。

升级vWAF

vWAF支持使用img镜像文件在线升级。用户可以直接通过WebUI界面的“系统 > 升级管理”页面进行系统升级。具体操作方法请参考《Web应用防火墙 WebUI手册》。

在Hyper-V上部署vWAF

Hyper-V是微软的一款基于hypervisor技术的虚拟化产品，vWAF能够在Hyper-V中部署是在微软Azure云中部署的前提条件。

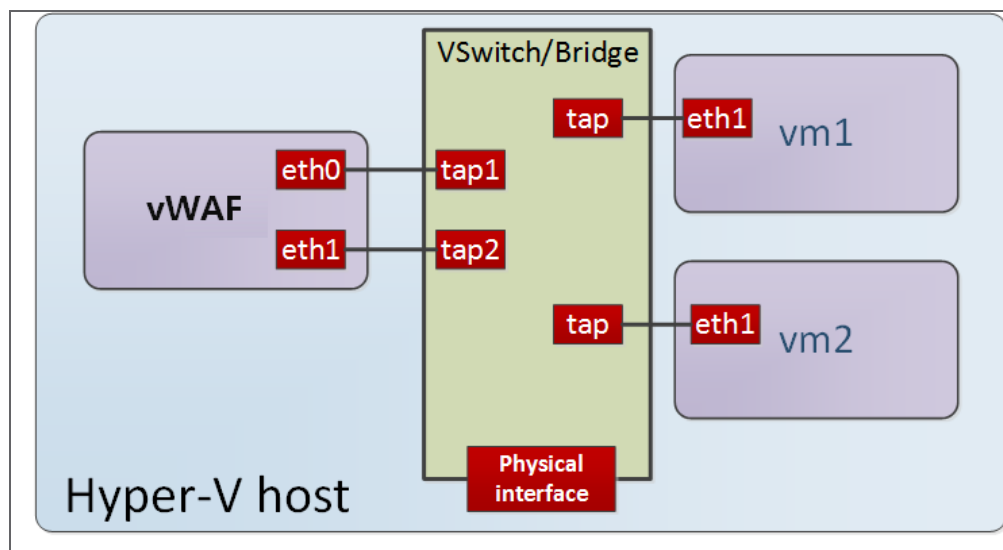
系统要求

在Hyper-V上部署山石网科的虚拟Web应用防火墙，需要宿主机满足以下要求。

- CPU支持Intel VT 或者 AMD-V
- 64位CPU，CPU能虚拟两个内核
- CPU须具备硬件的数据执行保护（DEP）功能，且开启该功能
- 至少能够分配2个虚拟网卡
- 至少4G内存
- 至少100G磁盘
- Windows Server 2012R2操作系统

虚拟Web应用防火墙的工作原理

将虚拟Web应用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（Virtual Switch），虚拟机把虚拟Web应用防火墙设置为默认网关，虚拟Web应用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Web应用防火墙之前，用户已经具有Windows Server 主机，且已经添加Hyper-V功能。

安装步骤

在Hyper-V主机上创建虚拟Web应用防火墙，请按照下面的步骤进行操作：

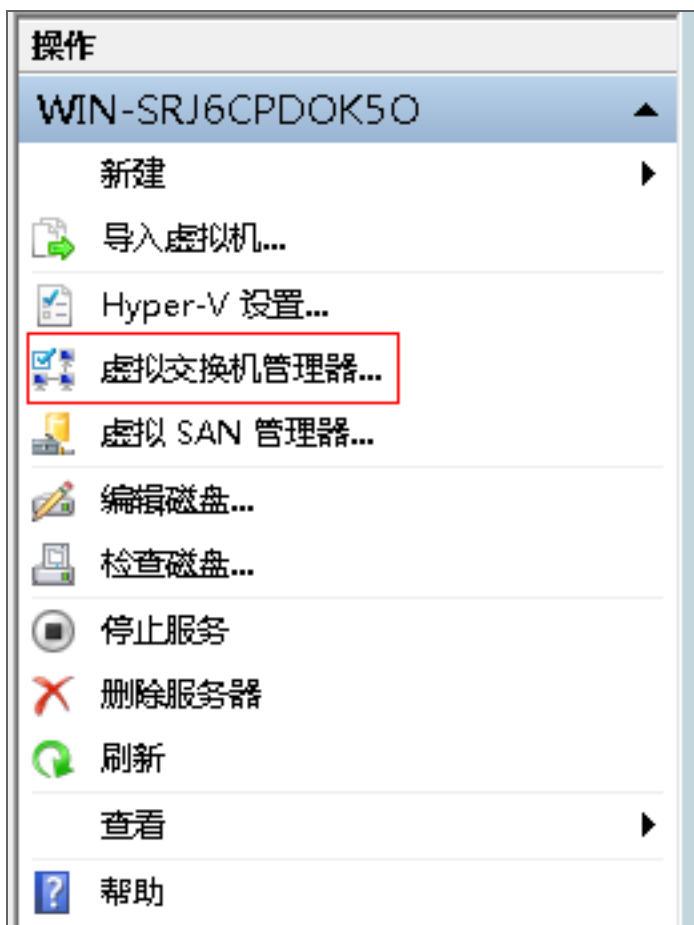
步骤一：获取vWAF软件包

请联系客服人员获取下载vWAF软件包的地址，并将VHD镜像文件保存到Hyper-V主机的文件系统中。

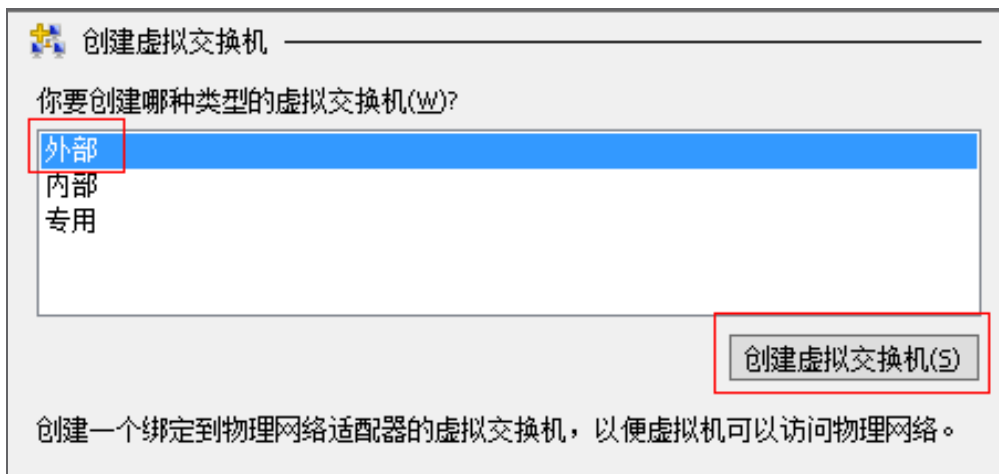
步骤二：创建虚拟机

1. 打开Hyper-V管理器，在菜单栏中点击“操作 > 新建 > 虚拟机”，弹出<新建虚拟机向导>对话框。
2. 在<开始之前>页面点击“下一步”按钮，创建具有自定义配置的虚拟机。
3. 指定虚拟机的名称和存储位置，点击“下一步”。
4. 在<分配内存>页面配置内存大小，点击“下一步”。

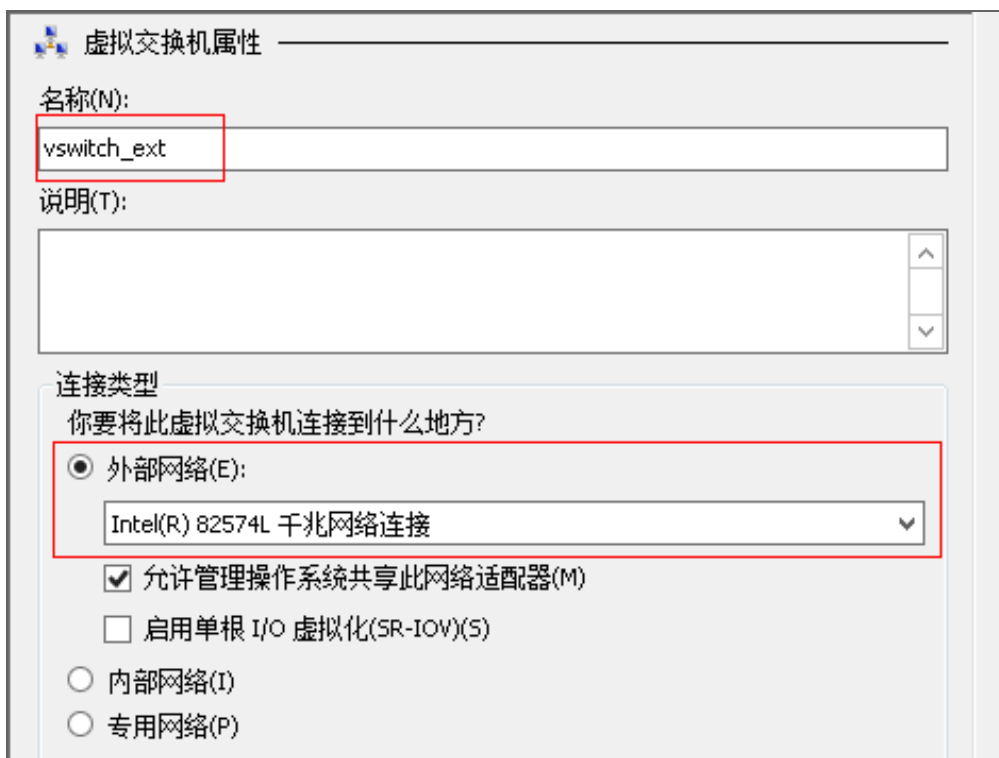
5. 在Hyper-V管理器页面右侧的<操作>面板中，选择<虚拟交换机管理器>页签，创建虚拟网卡。



6. 在管理器中选择<外部>类型，然后点击“创建虚拟交换机”按钮。
创建一个绑定到物理网卡的虚拟交换机，使新创建的虚拟机能够访问外部物理网络。

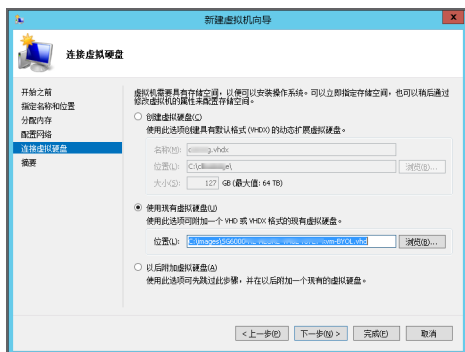


7. 在<虚拟交换机属性>区域配置交换机名称，并在<连接类型>处选择外部网络，点击“确定”。

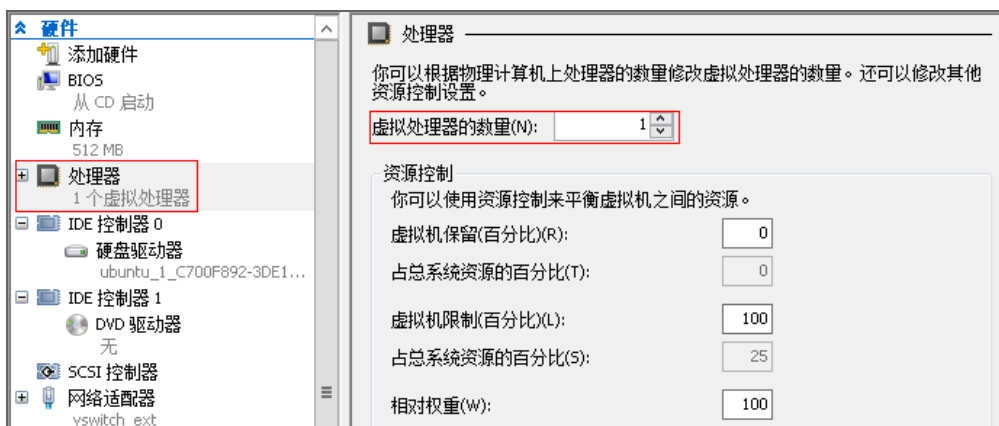


8. 在<新建虚拟机向导>的<配置网络>页面中，在<连接>下拉菜单中选择刚才创建的虚拟交换机，点击“下一步”。

- 在<连接虚拟硬盘>页面，选择<使用现有虚拟硬盘>，浏览本地PC，选择步骤一中的VHD文件，点击“下一步”。



- 在<摘要>页面点击“完成”，虚拟机将出现在虚拟机列表中。
- 如果您安装的虚拟Web应用防火墙版本需要两个虚拟CPU，请在虚拟机列表中选中此虚拟机后单击右键，选择“设置”，点击<处理器>节点，在右侧页面将虚拟处理器的数量设置为2。



步骤三：首次登录vWAF

按照以下的步骤初次登录vWAF。

- 在虚拟机列表中选中此虚拟机后单击右键，选择“连接”，然后在对话框的工具栏中点击启动按钮



稍等片刻，虚拟机即可启动成功。

2. 键入回车后，输入vWAF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vWAF系统进行操作。建议您及时修改用户名和密码。

访问虚拟Web应用防火墙的WebUI界面

虚拟Web应用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. 参考上述步骤三的方法，登录vWAF。
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（建议使用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Web应用防火墙的WebUI管理界面。
6. 关于如何使用vWAF系统，参考vWAF的使用手册（[点击此处](#)）。

升级虚拟Web应用防火墙

vWAF防火墙支持在线升级。用户可以直接通过 WebUI界面的“系统 > 升级管理”页面进行系统升级。具体操作方法请参考《vWAF WebUI用户手册》。

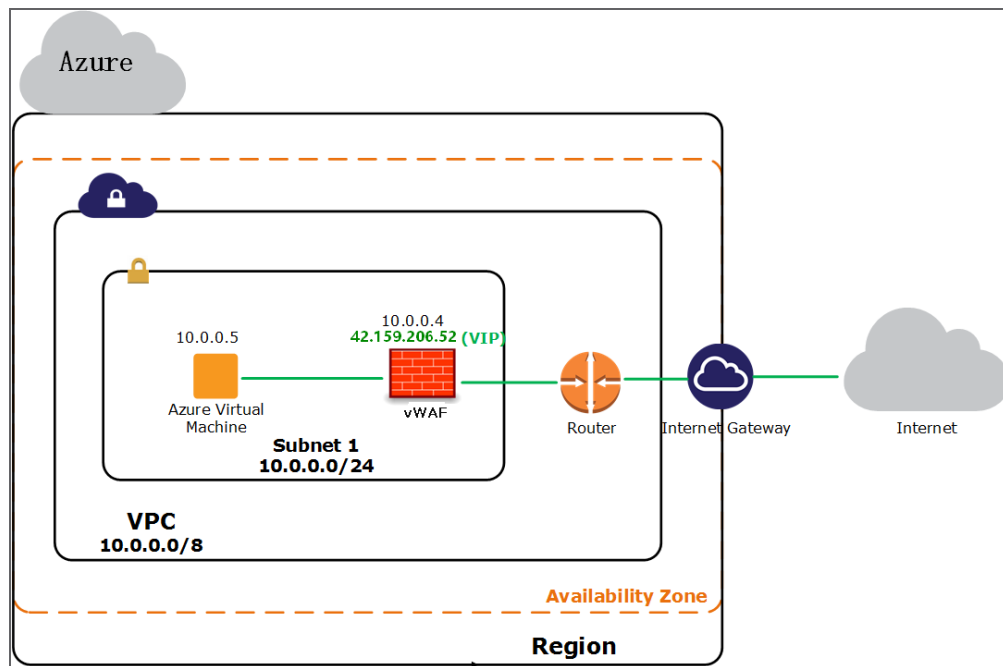
在微软云Azure上部署vWAF

组网设计

本手册以虚拟Web应用防火墙（vWAF）作为互联网网关的部署场景为例，介绍在Azure上安装和使用vWAF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。

在此组网设计中，Azure用户的虚拟网络将包括一个子网，用户可通过vWAF访问公网，同时，其访问私网的流量也会经过vWAF。需要您提前做如下工作：

- 创建如下虚拟网络及子网：
 - 虚拟网络test: 10.0.0.0/8
 - 子网default: 10.0.0.0/24
- 创建存储账户：azurevwafest，bootlogtest
- 创建资源组：vwaf



部署虚拟Web应用防火墙

虚拟Web应用防火墙（vWAF）将运行在位于虚拟网络的虚拟机中。安装完成后，您将：

- 拥有一个运行中的vWAF系统
- 能够访问vWAF的CLI和WebUI界面

第一步：创建容器

1. 登录Azure云。在主页面的导航栏中，选择“存储账户”，点击在准备工作中已创建好的存储账户名称 azurevwaftest，进入到存储账户页面。
2. 在存储账户详情页面左侧的导航栏中，选中“Blob服务 > 容器”，点击“+容器”按钮。
3. 输入容器名称，如“test”，点击“创建”按钮。



4. 点击上一步创建的容器名称，进入到容器的详情界面。

5. 点击左侧导航栏中的“属性”，查看容器的URL路径，并复制粘贴下来，用来后续的上传安装包。



第二步：上传安装包

1. 下载并安装powershell 工具，登录微软云，然后输入用户名及密码登录，具体命令如下：
 - 国际版本: **Login-AzureRmAccount -EnvironmentName AzureCloud**
 - 国内版本: **Login-AzureRmAccount -EnvironmentName AzureChinaCloud**
2. 查看当前的订阅，使用命令: **Get-AzureSubscription**
3. 选择要上传版本的订阅，并查看是否成功，使用命令: **select-azuresubscription**
4. 上传版本，使用命令: **Add-AzureVhd -Destination https://azure-wwafptest.blob.core.chinacloudapi.cn/test/vwaf.vhd -LocalFilePath D:\test\vwaf.vhd**
 - **Destination:** 指定在微软云azure存储中的容器的URL路径。即第一步中创建的容器的URL路径。
 - **LocalFilePath:** 指定安装包所在的本地存储路径。**注意：**由于微软Azure对镜像格式的特殊要求，请在安装之前联系山石网科的产品经理或相关技术支持人员来获取正确的vWAF镜像软件。
5. 等待上传完毕后，关闭powershell即可。

第三步：创建映像

- 1. 在左侧导航栏中选择“映像”，点击“+创建”。
- 2. 页面将进入<创建映像>对话框中。

仪表板 > 映像 >

创建映像 ...

基本 标记 查看 + 创建

创建可用于部署虚拟机和虚拟机规模集的托管映像。此映像包含创建虚拟机所需的托管 blob 和元数据的列表。[了解更多](#)

项目详细信息

选择订阅以管理已部署资源和成本。使用资源组(如文件夹)组织和管理所有资源。

订阅 *

资源组 *

实例详细信息

名称 *

区域 *

OS 磁盘

OS 类型 *

VM 生成 *

存储 blob *

帐户类型 *

主机缓存 *

加密

可使用平台管理的密钥或客户管理的密钥对 OS 和数据磁盘进行加密。[了解详细信息](#)

查看 + 创建

< 上一步

下一步: 标记 >

在<创建映像>对话框的“基本”页面设置基本信息。

选项	说明
项目详细信息	
订阅	选择当前使用的订阅。
资源组	指定映像所属的资源组，选择准备工作中已创建好的资源组“vwaf”。

选项	说明
实例详细信息	
名称	指定映像的名称，如 “test”。
区域	根据实际环境，选择资源组、存储账户所在的区域。
OS 磁盘	
OS类型	选择 “Linux”。
VM 生成	选择 “第一代”。
存储blob	选择第1、2步中对应的容器中的已上传的.vhd安装包。
账户类型	选择 “标准SSD”。
主机缓存	选择 “读/写”。
加密	
加密类型	选择 “（默认）使用平台管理的密钥进行静态加密”。

3. 点击 “查看+创建”，通过验证后继续点击 “创建”，完成配置。

第四步：创建虚拟机

1. 在左侧导航栏中选择 “映像”，选择第三步中创建的映像，点击该映像的名称。
2. 在右侧的VM映像详情界面，点击 “+创建VM” 按钮。

3. 页面将进入<创建虚拟机>对话框。

创建虚拟机

基本

磁盘

网络

管理

高级

标记

查看 + 创建

创建运行 Linux 或 Windows 的虚拟机。从 Azure 市场中选择映像，或使用自定义的映像。完成“基本信息”选项卡，然后通过“查看+创建”，使用默认参数来设置虚拟机，或查看每个选项卡，全部实施自定义。[了解更多信息](#)

项目详细信息

选择订阅以管理已部署资源和成本。使用资源组(如文件夹)组织和管理所有资源。

订阅

资源组

实例详细信息

虚拟机名称

区域

可用性选项

映像

大小

管理员帐户

身份验证类型

用户名

密码

确认密码

入站端口规则

选择可从公共 Internet 访问哪些虚拟机网络端口。可以在“网络”选项卡上指定更多限制或具体网络访问。

公共入站端口

选择入站端口

在<创建虚拟机>对话框的“基本”页面设置基本信息。

选项	说明
订阅	选择当前使用的订阅。
资源组	使用现有项，从下拉单选择开始时所准备的资源组“vwaf”。

在Xen平台上部署vWAF

47

选项	说明
实例详细信息	
虚拟机名称	指定虚拟机的名称。
映像	选择上一步创建的映像。
大小	选择虚拟机的大小，vWAF要求最少使用2个vCPU、内存最小为4GB，硬盘不小于100GB且物理主机须为Intel CPU，推荐使用"Standard_A2_v2-2 vcpu、4GiB内存"。
管理员账户	
身份验证类型	指定管理员身份验证的类型。
入站端口选择	
公共入站端口	选择“允许选定的端口”。
选择入站端口	选择“HTTPS（443）、SSH（22）”。

4. 点击“查看+创建”，验证通过后点击“创建”。
5. 页面自动跳转到“仪表板”，显示系统正在部署vWAF。几分钟后部署完成，点击  按钮进入虚拟机详情页面。

第五步：查看IP

在虚拟机详情页面，点击“概述”，右侧将显示虚拟机的具体信息，可查看到该虚拟机的公共IP地址，该IP地址将用于后续登录设备。若关闭该页面，可按照如下步骤查看IP：

1. 在Azure主页的左侧导航栏中选择<虚拟机>，然后在右侧的实例页面中，点击“第一步”中创建的虚拟机名称。



2. 在虚拟机详情页面点击上方的“概述”，右侧将显示虚拟机的具体信息，查看虚拟机的公共IP地址，该IP地址将用于后续登录设备。



第六步：从外网访问vWAF

创建Azure虚拟机后，vWAF自启动，默认情况下管理口的SSH和HTTPS协议处于开启状态,用户可以通过这两种方式登录到vWAF。

使用SSH2远程登录vWAF：

1. 打开远程终端登录软件。以SecureCRT为例
2. 点击“File > Quick Connect”。在“Protocol”下拉菜单中选择“SSH2”。
3. 在<Hostname>中输入公共IP地址。
4. 在<Username>中输入vWAF默认的用户名/密码（hillstone/hillstone）。
5. 点击“Connect”。
6. 输入创建虚拟机时设置的密码，点击“OK”即可登录。

使用HTTPS远程登录vWAF:

1. 打开浏览器，在地址栏中输入公共IP地址。
2. 在登录页面输入vWAF的默认用户名/密码（hillstone/hillstone）。
3. 按回车键，即可登录。
4. 关于如何使用vWAF系统，参考vWAF的使用手册（[点击此处](#)）。

第七步：购买并申请许可证

此步骤仅适用于BYOL类型的产品，按需付费类型产品请忽略此步骤。

购买BYOL类型的产品后，还需要购买山石网科虚拟化下一代防火墙许可证并安装，才能保证虚拟Web应用防火墙在Azure中正常使用。购买许可证，请与销售人员联系。关于如何申请和安装许可证，请参见"安装许可证" 在第5页。

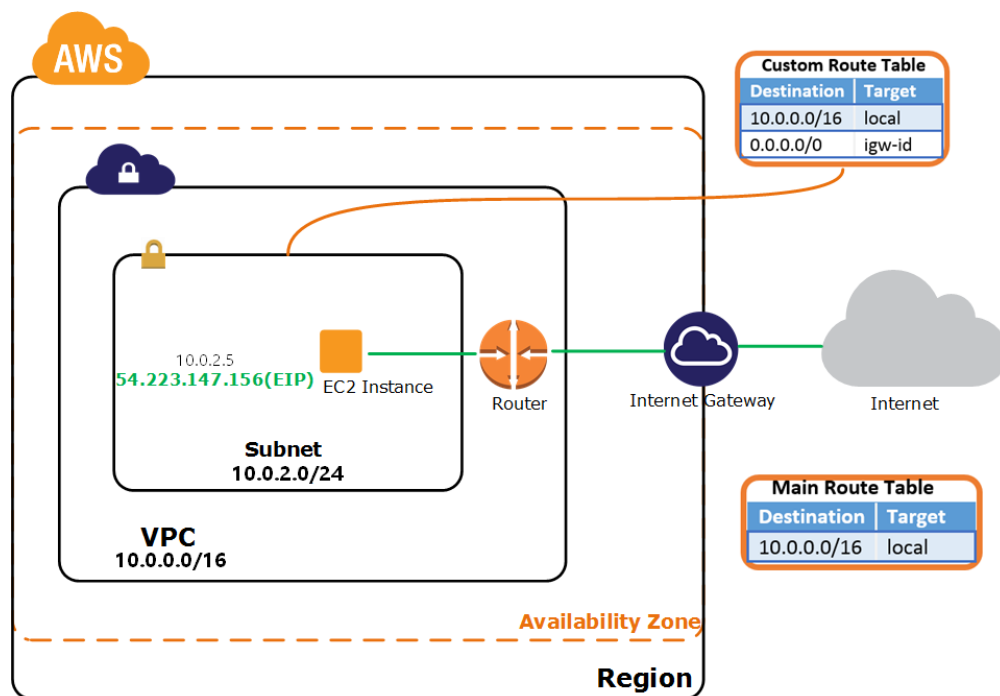
在AWS上部署vWAF

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。

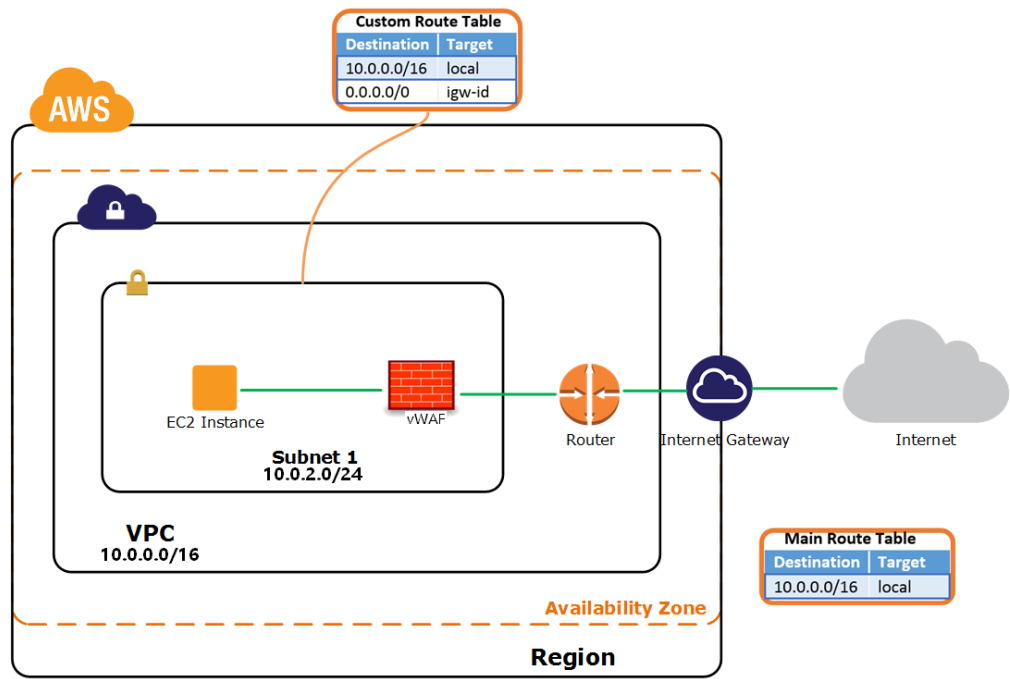
AWS提供的多种组件中，与虚拟Web应用防火墙直接相关的是VPC和EC2。

- 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vWAF

vWAF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Web应用防火墙业务。



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（[点击此处](#)）。更多关于如何配置VPC，请查看AWS的入门文档（[点击此处](#)）。

在本手册的组网设计中，我们假定用户已创建过VPC网络，公有子网的名称命名为Manage，且VPC的路由表中含有目的地址为互联网网关接口的默认路由条目。本部分主要介绍如何创建一个新的子网，在后面的操作中，我们将会把vWAF的eth0接口绑定到该子网中（即把虚拟vWAF部署在该子网中）。

完成这部分后，我们将会得到以下网络：

- VPC: 10.0.0.0/16
- Subnet 1 (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。

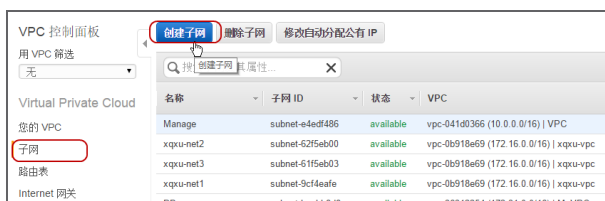


第二步：为VPC添加子网

在本示例的设计中，vWAF的接口eth0同时作为管理接口，用于管理vWAF或者访问VPC。

新建子网，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”。



2. 输入子网名称“Public”，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”。



3. 点击“是，创建”。

第三步：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。为了使刚刚创建的子网（“Subnet 1（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，从而使子网与互联网路由可达。

为子网添加路由，按照以下步骤进行操作：

1. 在VPC控制面板中的“子网”页面，选择刚才创建的子网。
2. 点击下方的“路由表”标签页，然后点击“编辑”按钮。
3. 在<更改为>后面的下拉菜单中，选择含有目的地址为互联网网关接口的默认路由条目的路由表。
4. 点击“保存”。

在亚马逊云AWS上部署vWAF

创建vWAF实例

vWAF将作为一个EC2实例安装在AWS中。vWAF的管理接口（eth0）可以用于访问vWAF系统。

下面介绍如何在AWS中安装vWAF。在完成“安装vWAF”这部分的操作后，您将：

- 拥有一个运行中的vWAF系统
- 看到管理接口eth0获取到私网IP地址和公网IP地址
- 能够访问vWAF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Amazon系统镜像（AMI）

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）。为实例选择Amazon系统镜像，请按照以下步骤进行操作：

1. 接上步，在实例配置向导中，点击“AWS Marketplace”；
2. 在上方的搜索框中，输入“hillstone vwaf”关键字进行搜索。在搜索结果列表中找到“Hillstone Virtual-Web Application Firewall”镜像，点击“选择”按钮。



3. 在弹出的规格确认信息表中，点击“Continue”继续。

其他方法（备选）： vWAF同时支持通过共享AMI模板的方式提供给用户。若您申请使用或购买了vWAF之后，山石网科就会将vWAF镜像文件共享给您的AWS账户。得到共享的vWAF的AMI模板后，可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”。



2. 找到您需要的产品型号，点击“选择”。

第三步：选择实例类型

请根据产品的型号，选择实例类型。具体参考[产品信息](#)。

1. 选择 AMI2. 选择实例类型3. 配置实例4. 添加存储5. 添加标签6. 配置安全组7. 审核

步骤 2: 选择一个实例类型

Amazon EC2 提供多种经过优化，适用于不同使用案例的实例类型以供选择。实例就是可以运行应用程序的虚拟服务器。它们由 CPU、内存、存储和网络容量组成不同的组合，可让您灵活地为您的应用程序选择适当的资源组合。有关实例类型以及这些类型如何满足您的计算需求的信息，请参阅[了解更多](#)。

筛选条件: 所有实例类型 最新一代 显示/隐藏列

当前选择的实例类型: t2.medium (变量 ECU, 2 vCPU, 2.3 GHz, Intel Broadwell E5-2686v4, 4 GiB 内存, 仅限于 EBS)

	系列	类型	vCPU	内存 (GiB)	实例存储 (GiB)	可用的优化 EBS	网络性能	IPv6 支持
☐	通用型	t2.micro	1	1	仅限于 EBS	-	低到中等	是
☐	通用型	t2.small	1	2	仅限于 EBS	-	低到中等	是
☒	通用型	t2.medium	2	4	仅限于 EBS	-	低到中等	是
☐	通用型	t2.large	2	8	仅限于 EBS	-	低到中等	是
☐	通用型	t2.xlarge	4	16	仅限于 EBS	-	中等	是
☐	通用型	t2.2xlarge	8	32	仅限于 EBS	-	中等	是

取消 上一步 选择和启动 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vWAF的VPC，在“子网”下拉菜单选择管理接口eth0所属的子网（Subnet 1（Public）：10.0.2.0/24），其他选项保持默认值。
2. 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 AMI2. 选择实例类型3. 配置实例4. 添加存储5. 添加标签6. 配置安全组7. 审核

步骤 4: 添加存储

您的实例将使用以下存储设备设置启动。您可以将其其他 EBS 卷和实例存储卷附加到您的实例，或编辑根卷的设置。您还可以在启动实例后附加其他 EBS 卷而非实例存储卷。详细了解有关 Amazon EC2 中存储选项的信息。

卷类型	设备	快照	大小 (GiB)	卷类型	IOPS	吞吐量 (MB/s)	终止时删除	加密
根	/dev/sda1	snap-0e55dea556378e23a	101	通用型 SSD (gp2)	303/3000	不适用	☒	未加密

添加新卷

2. 点击“下一步：标签实例”。

第六步：标签实例

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。

分配安全组:

☒ 创建一个新安全组

☐ 选择一个现有的安全组

安全组名称:

VPC

描述:

VPC

2. 添加规则，允许所有类型的流量访问vWAF。

类型 (1)	协议 (1)	端口范围 (1)	来源 (1)
ICMP	TCP	32	任何位置 • 0.0.0.0/0
所有流量	全部	0 - 65535	任何位置 • 0.0.0.0/0

添加规则

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“下载密钥对”，浏览器将自动下载该密钥对（后缀为“.PEM”）。请将该PEM文件保存到本地一个安全的位置。
- 4. 点击“启动实例”。AWS将启动vWAF，您可以点击“查看启动日志”查看启动过程。



- 5. 点击“查看实例”，返回EC2实例列表，vWAF正在启动。

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

配置子网和接口

分配弹性IP地址

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。

由于eth0接口默认开启了DHCP功能，vWAF启动后，eth0接口将被自动赋予一个私网IP地址。我们将再申请一个弹性IP地址，分配给管理接口eth0。这样，vWAF的eth0接口会有一个私网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。

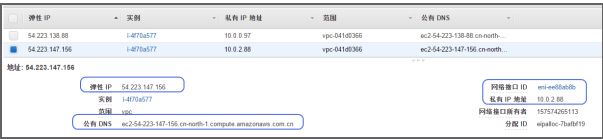
- 1. 在EC2控制面板，点击左侧导航栏的“弹性IP”，进入弹性IP界面。
- 2. 点击“分配新地址”，并在弹出的确认对话框中点击“是，请分配”，就可以获取到一个公网IP地址。



- 3. 选中新的弹性IP，点击上方的“操作 > 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vWAF的管理接口eth0的公网地址。接口的ID号，可以在EC2实例的“描述”标签页查到。



- 4. 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。



在主控制台查看实例

返回EC2控制面板，点击左侧导航栏的“实例”，选中vWAF实例，可以查看vWAF的详细信息。

购买并申请许可证

购买vWAF产品并支付完成后，还需要购买vWAF许可证并安装，才能保证vWAF在AWS中正常使用。购买许可证，请与销售人员联系。关于如何申请和安装许可证，请参见"安装许可证" 在第5页。

访问vWAF

vWAF的缺省设置中，仅开启了管理接口eth0的SSH访问权限，我们将首先使用SSH访问接口eth0。按照亚马逊的指导，以及考虑到支持密钥对，需要选择PuTTY和PuTTYGen作为连接软件。

使用PuTTY访问CLI管理界面

我们以Windows系统为例，介绍如何使用PuTTY和PuTTYgen访问vWAF的CLI管理界面。

首先，检查您是否已经完成以下准备工作：

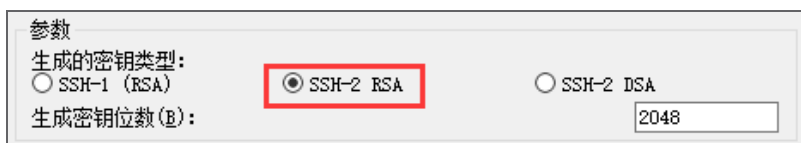
- 已经安装 **PuTTYgen** 和 **PuTTY** 软件。若无，可以通过该下载页面[PuTTY Download Page](#)下载。
- 在AWS的EC2实例页面，获取vWAF的弹性IP地址。
- 确认本地有密钥对文件（后缀名为PEM）。
- vWAF默认已经开启SSH，请不要修改该设置。

步骤一： 使用PuTTYgen转换密钥对

由于PuTTY本身并不支持亚马逊生成的PEM格式的密钥对，所以需要使用PuTTYgen工具将该密钥对进行一次格式转换，转换为PuTTY支持的.ppk格式。

转换密钥对格式，按照以下步骤进行操作：

1. 启动PuTTYgen。
2. 在<生成的密钥类型>字段下面，选择“SSH-2 RSA”。



参数

生成的密钥类型：

☐ SSH-1 (RSA) ☒ SSH-2 RSA ☐ SSH-2 DSA

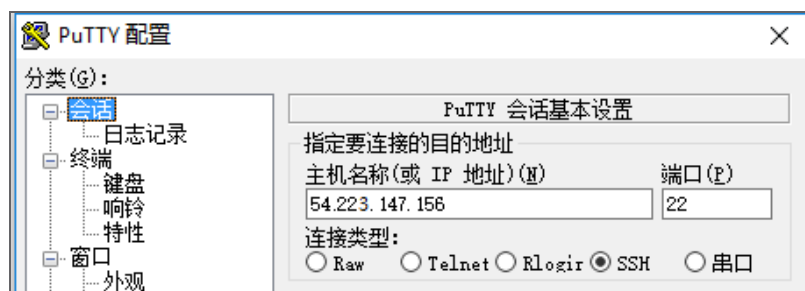
生成密钥位数 (b):

3. 点击“载入”。默认PuTTYgen只查找ppk格式的私钥，请在弹出的<载入密钥>对话框中，将文件类型改为“所有文件”。
4. 浏览计算机，选中之前生成的PEM文件。
5. 点击“保存私钥”，将生成的ppk的文件保存到本地磁盘，留作后续使用。
6. 关闭PuTTYgen。

步骤二：使用PuTTY访问CLI界面

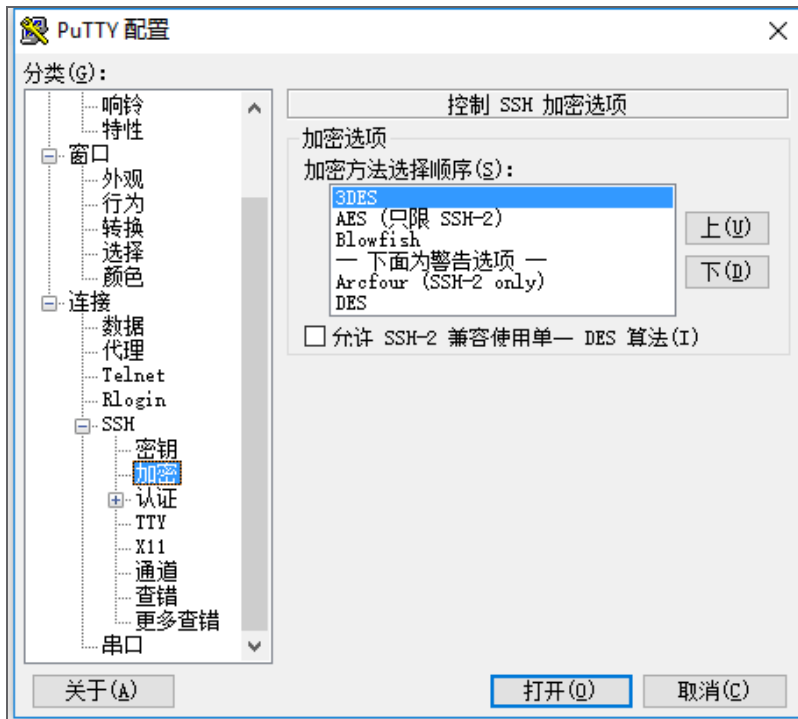
按照以下步骤，连接vWAF实例。您将使用到前面保存的ppk私钥文件。

1. 启动PuTTY。
2. 在左侧<类别>栏目下，选择“会话”，填入以下信息。

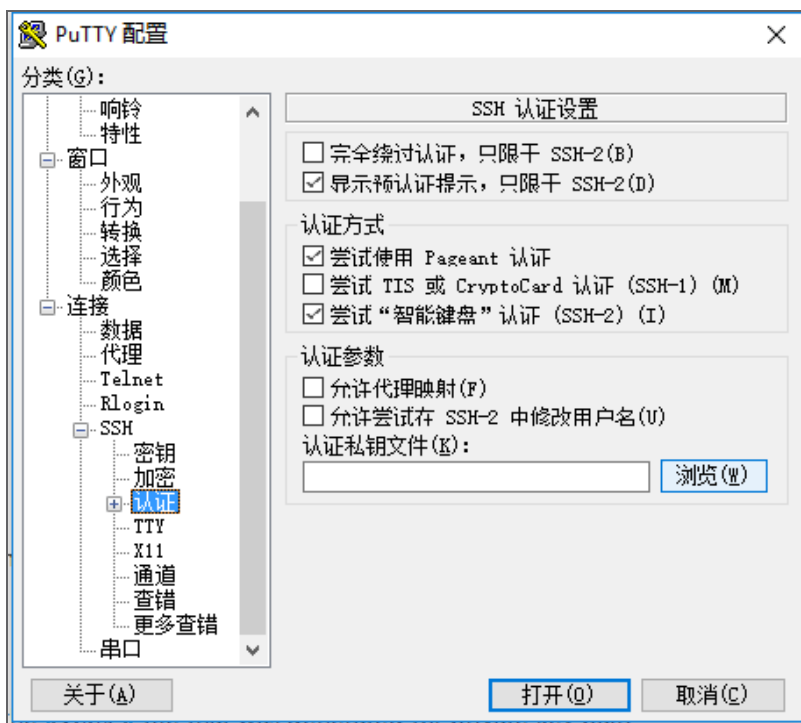


- 在<主机名称>字段：输入实例的弹性IP（接口eth0的公网IP地址）
- 在<连接类型>字段，选择“SSH”。
- 在<端口>字段，确认端口号为22.

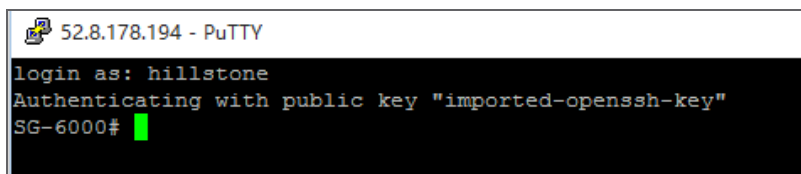
3. 在左侧<类别>目录下，点击“连接 > SSH > 加密”，在右侧将“3DES”加密方法移动到顶端。



4. 点击“连接 > SSH > 认证”，点击“浏览”按钮，选择上面创建的ppk密钥文件。



5. 点击“打开”。若出现提示框，点击“确认”。
6. 系统弹出一个命令行界面，提示输入用户名。输入 **hillstone**，回车后，连接成功。



7. 现在，您可以在该界面上管理vWAF。关于vWAF的配置方法，请参考vWAF的软件用户手册。

访问WebUI界面

由于HTTP连接的默认端口80、HTTPS连接的默认端口443在亚马逊中国禁用，所以，若要访问vWAF的WebUI，需要接口开启HTTPS服务并更换端口号。

访问vWAF的WebUI界面，以HTTPS方式为例，按照以下步骤：

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

```
SG-6000# https port 8888
```

2. 开启eth0接口的http访问权限：

```
SG-6000# interface ethernet0/0
```

```
SG-6000(config-if-eth0/0)# manage https
```

3. 出于安全性的考虑，vWAF的默认密码hillstone会失效，需重新为hillstone用户配置一个新密码，示例如下：

```
SG-6000# admin user hillstone
```

```
SG-6000(config-admin)# password hillstone1234
```

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vWAF WebUI界面。

The image shows the login page of the Hillstone Network WebUI. At the top left is the Hillstone logo. Below it are two input fields for username and password. At the bottom is a blue button with the Chinese characters "登录" (Login).

5. 输入默认的用户名“hillstone”和新密码，点击“登录”进入系统。

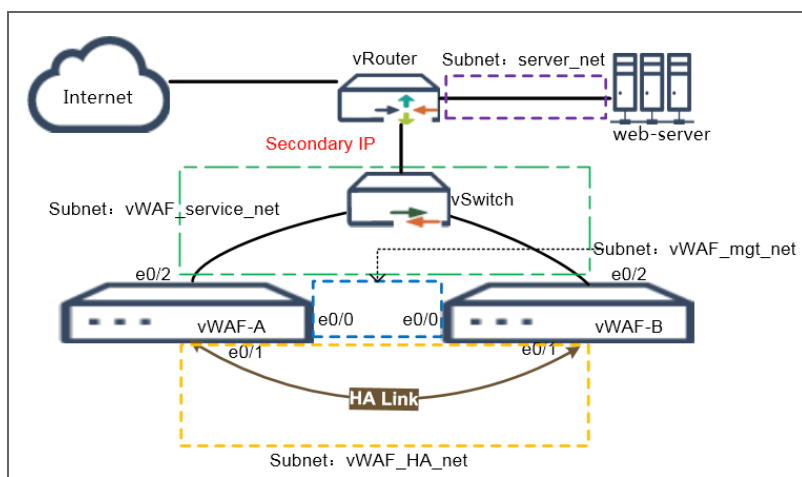
关于如何操作vWAF，参考WAF的用户手册（[点击此处](#)）。

在亚马逊云AWS上进行vWAF的HA部署

组网设计

按照如下拓扑，在亚马逊云AWS环境中有一台云服务器web-server（10.0.2.209），现通过部署vWAF的HA方案对云服务器进行安全防护。

部署完成后，vWAF-A将被选举为主设备，对云服务器进行安全防护；vWAF-B为备份设备。vWAF-A会将其配置信息以及状态数据同步到备份设备vWAF-B。当主设备vWAF-A出现故障不能正常工作时，备份设备vWAF-B会在不影响用户通信的状态下自动切换为主设备，继续对云服务器进行安全防护，从而提高了网络可靠性，保证云服务器的业务不中断。



部署步骤

[第一步：创建VPC及子网](#)

[第二步：创建及启用Internet网关](#)

[第三步：创建策略](#)

[第四步：创建IAM角色](#)

[第五步：创建EC2实例](#)

[第六步：创建网络接口](#)

[第七步：连接并配置vWAF](#)

[第八步：验证HA结果](#)

[第九步：在AWS上配置云服务器的路由](#)

[第十步：在vWAF上配置路由、NAT及安全策略](#)

第一步：创建VPC及子网

登录AWS管理控制台（Console），创建VPC及子网，具体操作方法，请参阅[为VPC添加子网](#)。

原云服务器web-server所在VPC及子网：

- VPC(VPC1): 10.0.0.0/16
- Subnet 0 (server_net) : 10.0.2.0/24
- web-server IP: 10.0.2.209

现需要新建以下子网，且子网所属VPC需与原web-server所在的VPC相同:

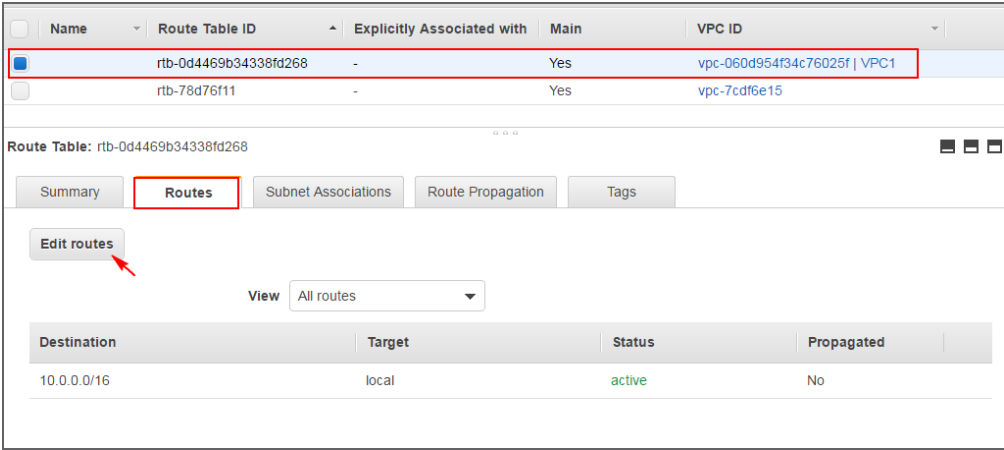
- VPC(VPC1): 10.0.0.0/16
- Subnet 1 (vWAF_service_net) : 10.0.1.0/24
- Subnet 2 (vWAF_mgt_net) : 10.0.10.0/24
- Subnet 3 (vWAF_HA_net) : 10.0.100.0/24

第二步：创建及启用Internet网关

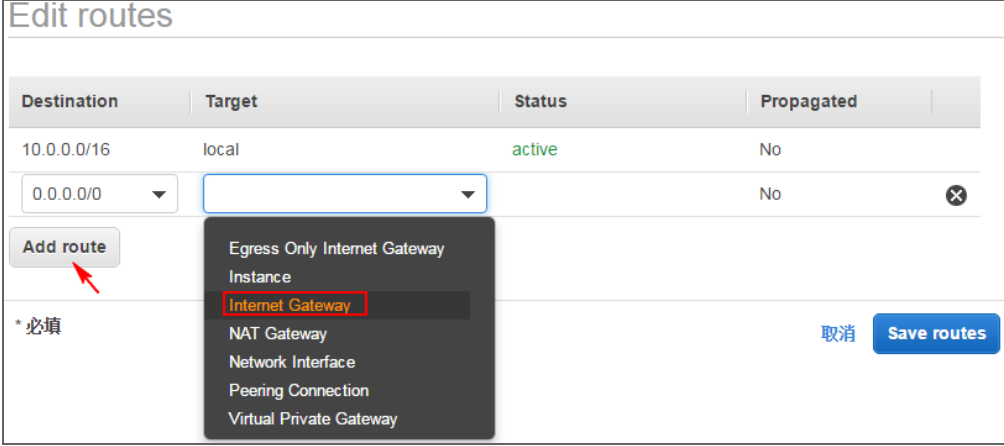
创建Internet网关，实现VPC中的实例与Internet之间的通信。具体操作方法，请按照以下步骤进行：

1. 在VPC控制面板，选择“Internet Gateway”，然后点击“创建Internet网关”按钮。
2. 在<创建Internet网关>页面，输入名称标签“Internet_ha”。
3. 点击“创建”，完成配置。
4. 在Internet网关列表中，选中“Internet_ha”条目，然后点击“操作”下拉菜单，选择“附加到VPC”，选择步骤1创建的“VPC1”进行附加。
5. 在VPC控制面板，选择“路由表”。

6. 选择步骤1中创建的“VPC1”对应的路由，点击页面下方的“路由表”标签页，然后点击“Edit routes”按钮。



7. 在<Edit routes>页面，点击“Add route”按钮，添加一条路由，下一跳为Internet网关“Internet_ha”，即启用Internet网关。



第三步：创建策略

AWS策略定义可向用户、组或角色分配的 AWS 权限。用户可以通过创建策略，可以精细化地限定vWAF调用的云平台的功能权限。若用户不需限定vWAF具体调用的功能权限，可直接跳过该步骤。创建策略，按照如下步骤进行：

1. 点击页面上方导航栏的“服务”下拉菜单，选择“安全&身份 > IAM > 策略”；
2. 点击“创建策略”按钮，进入<创建策略>页面，配置如下信息：
 - 服务选择：EC2
 - 操作：
 - 列表：DescribeNetworkInterfaces和DescribeRouteTables
 - 写入：AssignPrivateIpAddresses和ReplaceRoute
 - 资源：所有资源

创建策略

策略定义可向用户、组或角色分配的 AWS 权限。您可以在可视化编辑器中使用 JSON 创建和编辑策略。 [了解更多](#)

可视化编辑器 JSON 导入托管策略

全部展开 | 全部折叠

EC2 (4 个操作) 克隆 删除

服务 EC2

操作 列表

- DescribeNetworkInterfaces
- DescribeRouteTables

写入

- AssignPrivateIpAddresses
- ReplaceRoute

资源 ☐ 特定 ☒ 所有资源

请求条件 指定请求条件 (可选)

添加其他权限

取消 保存策略

3. 点击“查看策略”，进入第2步的配置界面，输入策略名称“ha-policy”。

4. 点击“创建策略”，完成配置。

第四步：创建IAM角色

创建IAM角色，并配置拥有调用API的权限。当实例引用该IAM角色时，将获得相应的权限。创建IAM角色，按照以下步骤进行操作：

1. 点击页面上方导航栏的“服务”下拉菜单，选择“安全&身份 > IAM > 角色”；
2. 点击“创建角色”按钮，进入<创建角色>页面，配置如下信息：
 - 选择受信任实体的类型：AWS产品；
 - 选择将使用此角色的服务：EC2；
 - 选择您的使用案例：EC2；
3. 点击“下一步：权限”按钮，在<Attach权限策略>页面的策略列表中，勾选在“第三步”中创建的策略“ha-policy”。若用户不需限定vWAF具体调用的功能权限（即跳过了“第三步：创建策略”），可直接使用系统默认的管理员权限所对应的策略“AdministratorAccess”。

创建角色

1 2 3 4

Attach 权限策略

选择一个或多个要附加到新角色的策略。

创建策略

刷新

筛选策略

Q ha-policy

显示 1 个结果

	策略名称	用作	描述
☒	ha-policy	无	

* 必填

取消

上一步

下一步: 标签

或

筛选策略

Q 搜索

显示 215 个结果

	策略名称	用作	描述
☒	AdministratorAccess	Permissions policy (6)	Provides full access to AWS services ...
☐	AmazonAPIGatewayPushToCloudWatchLogs	无	Allows API Gateway to push logs to u...
☐	AmazonChimeFullAccess	无	Provides full access to Amazon Chim...
☐	AmazonChimeReadOnly	无	Provides read only access to Amazon...
☐	AmazonChimeUserManagement	无	Provides user management access t...
☐	AmazonCognitoPowerUser	无	Provides administrative access to ext...
☐	AmazonCognitoReadOnly	无	Provides read only access to Amazon...
☐	AmazonDMSCloudWatchLogsRole	无	Provides access to upload DMS repli...

- 点击“下一步: 标签”按钮, 跳过该步骤, 继续点击“下一步: 审核”。
- 在<审核>页面, 输入角色名称“ha-role”。

创建角色

1 2 3 4

审核

在创建此角色之前在下面提供必需的信息并审核此角色。

角色名称

ha-role

请使用字母数字和“+”、“-”、“.”、“_”字符。最长 64 个字符。

角色描述

Allows EC2 instances to call AWS services on your behalf.

最长 1000 个字符。请使用字母数字和“+”、“-”、“.”、“_”字符。

可信的实体

AWS 服务: ec2.amazonaws.com.cn

策略

ha-policy

权限边界

未设置权限边界

没有添加任何标签。

* 必填

取消

上一步

创建角色

6. 点击“创建角色”，完成配置。

第五步：创建EC2实例

在AWS上创建两台vWAF实例vWAF-A和vWAF-B，用于HA部署方案。具体创建步骤，请参阅在亚马逊云AWS上部署虚拟防火墙。

- 1. 实例规格要求：vWAF-A和vWAF-B实例至少需要2vCPU和4G内存；两实例需使用相同的密钥文件；且默认网卡选择同一个子网，本示例中选择步骤一配置的子网“vWAF_mgt_net”。
- 2. 两台vWAF实例的配置信息如下，其他参数与在亚马逊云AWS上部署虚拟防火墙中保持一致。

选项	配置信息
AMI	在“1.选择AMI”页面中，在AWS Marketplace中，选择v2.5及以上版的AMI，若选择旧版本，可在实例启动后升级为v2.5及以上版本。
实例类型	在“2.选择实例类型”页面中，选择实例类型“通用性t2.medium” (2vCPU,4GiB内存)。
网络	在“3.配置实例”页面中，选择步骤一配置的VPC：VPC1。
子网	在“3.配置实例”页面中，选择步骤一配置子网：vWAF_mgt_net，作为默认网络。
IAM角色	在“3.配置实例”页面中，选择步骤三配置的IAM角色：ha-role。

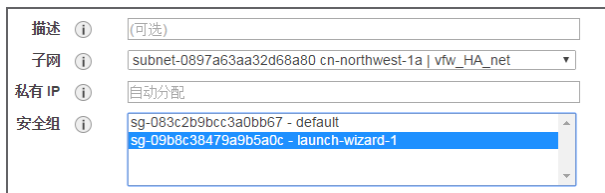
- 3. 配置完成后，可在实例列表中，添加实例的名称“vWAF-A”和“vWAF-B”。

☐	Name	实例 ID	实例类型	可用区	实例状态	状态检查	警报状态	公有 DNS
☐	vWAF-A	i-0aef7fbfb5753eedc	t2.medium	cn-northwest-1a	running	2/2 的检查...	无	
☐	vWAF-B	i-0190252a17aadaf5c	t2.medium	cn-northwest-1a	running	2/2 的检查...	无	

第六步：创建网络接口

vWAF-A和vWAF-B实例还需各添加两个网络接口，用来做HA网络接口和业务接口。在vWAF_HA_net与vWAF_Service_net子网上分别创建两个网络接口，然后附加到vWAF实例上，请按照以下步骤进行：

1. 在EC2控制面板，点击左侧导航栏的“网络接口”，进入网络接口界面。
2. 点击“创建网络接口”按钮，在<创建网络接口>对话框中，子网选择“vWAF_HA_net”，安全组选择所有流量都可通过。



3. 重复步骤1、2，再创建一个vWAF_HA_net子网接口。
4. 重复步骤1、2，为vWAF_service_net子网创建两个网络接口。
5. 点击左侧导航栏的“实例”，进入实例界面，选择实例“vWAF-A”和“vWAF-B”，然后点击“操作”按钮，选择关闭vWAF实例。
6. 点击左侧导航栏的“网络接口”，进入网络接口界面，点击“附加”按钮，将步骤1-4创建的子网接口分别附加到vWAF实例vWAF-A和vWAF-B上。

注意：每台vWAF实例先附加vWAF_HA_net子网的接口，再附加vWAF_service_net子网的接口。



7. 选择vWAF-A（本示例中作为HA主设备的实例）的vWAF_service_net接口，点击“操作”下拉菜单中的“管理IP地址”，为该网络接口分配一个新的IP（即Secondary IP）。



- 分别为vWAF-A和vWAF-B实例的vWAF_mgt_net接口以及vWAF-A的Secondary IP分配弹性IP地址，具体步骤可参考[分配弹性IP地址](#)。
- 分别选择vWAF-A和vWAF-B的vWAF_service_net接口，点击“操作”下拉菜单中的“更改源/目标检查”，然后禁用该检查。
- 启动实例vWAF-A和vWAF-B。
- 查看vWAF-A的各接口的私有IP、公网IP和弹性IP如下：

实例 ID	i-07ede20d93fe14613	公有 DNS	-
实例状态	running	公有 IP	52.83.161.11
实例类型	t2.medium	弹性 IP	52.83.161.11* 52.83.248.84
私有 DNS	ip-10-0-10-32.cn-northwest-1.compute.internal	可用区	cn-northwest-1a
私有 IP	10.0.10.32, 10.0.100.164, 10.0.1.106	安全组	launch-wizard-1. 查看规则. view outbound rules
辅助私有 IP	10.0.1.242	计划的事件	无计划事件

- 查看vWAF-B的各接口的私有IP和公网IP如下：

实例 ID	i-06eb93473a0169b43	公有 DNS	-
实例状态	running	公有 IP	52.83.191.210
实例类型	t2.medium	弹性 IP	52.83.191.210*
私有 DNS	ip-10-0-10-89.cn-northwest-1.compute.internal	可用区	cn-northwest-1a
私有 IP	10.0.10.89, 10.0.1.6, 10.0.100.100	安全组	launch-wizard-1. 查看规则. view outbound rules
辅助私有 IP		计划的事件	无计划事件
VPC ID	vpc-060d954f34c76025f	AMI ID	SG6000-Virtualization (ami-03f039da7ecda926e)
子网 ID	subnet-0644706ecc6cd5c6a	平台	-

第七步：连接并配置vWAF

通过WebUI方式登录vWAF-A，具体步骤可查看[访问vWAF虚拟防火墙](#)。

- 初次访问WAF设备时可按照“WAF安装向导”进行配置：
 - 选择部署模式：单臂模式
 - LAN接口：ethernet0/2；安全域：Untrust（该接口为与Web服务器连接的接口）

- IP地址：配置为Secondary IP： 10.0.1.242。
 - 掩码： 24
- 查看vWAF-A，vWAF-B获取的DNS Server地址，本示例中查看到为10.0.0.2。然后继续配置系统时间，完成配置向导。
 - 分别在vWAF-A和vWAF-B的接口eth0/0下配置路由优先级，同时关闭逆向路由检查。



- 在vWAF-A上，将Secondary IP配置到vWAF的vWAF-Service-net对应的接口，本示例对应eth0/2。(此配置可只在主设备进行配置，开启HA后会同步到备设备上。)
- 绑定安全域：三层安全域
 - 安全域： untrust
 - HA同步： 启用
 - 类型： 静态IP
 - IP地址： 10.0.1.242（已配置为Secondary IP地址及其掩码。）
 - 网络掩码： 24

- 管理方式：开启PING

Ethernet 接口

基本配置 IPv6 配置 属性 高级

基本配置

接口名称: ethernet0/2

描述: (0 - 63)字符

绑定安全域: ☐ 二层安全域 ☒ 三层安全域 ☐ TAP ☐ 无绑定

安全域: untrust

HA同步: ☒ 启用

IP配置

类型: ☒ 静态IP ☐ 自动获取

IP地址: 10.0.1.242

子网掩码: 24

☐ 配置为Local IP

高级选项

管理方式

☐ Telnet ☐ SSH ☒ Ping ☐ HTTP ☐ HTTPS ☐ SNMP

路由

逆向路由: ☐ 启用 ☒ 关闭 ☐ 自动

确定 取消

5. 选择“网络 > 路由 > 目的路由”，配置主机路由及DNS，保证vWAF-A和vWAF-B与AWS平台通信。(此配置可只在主设备进行配置，开启HA后会同步到备设备上。)

- 目的地：169.254.169.254（AWS平台内部的地址，云界可通过其获取 Region、vpc id，接口id等）
- 子网掩码：32
- 下一条：网关

- 网关：10.0.10.1（vWAF_mgt_net网关IP）

目的路由配置

目的地: 169.254.169.254

子网掩码: 32

下一跳: ☒ 网关 ☐ 接口

网关: 10.0.10.1

时间表: -----

优先权: 1 (1 - 255), 缺省值: 1

路由权值: 1 (1 - 255), 缺省值: 1

描述: (1 - 63)字符

确定 取消

- 目的地：10.0.0.2（DNS Server地址）
- 子网掩码：32
- 下一条：网关
- 网关：10.0.10.1（vWAF_mgt_net网关IP）

目的路由配置

所属虚拟路由器: trust-vr

目的地: 0.0.0.0

子网掩码: 0

下一跳: ☒ 网关 ☐ 接口

网关: 10.0.1.253

时间表: -----

优先权: 1 (1 - 255), 缺省值: 1

路由权值: 1 (1 - 255), 缺省值: 1

描述: (1 - 63)字符

确定 取消

- 目的地：52.82.209.55（EC2 URL的IP地址之一，共3个：52.82.209.55、52.82.209.81和52.82.209.31。获取方法见下方的“注意”。），故共需加3条路由，其他2条参照本条，继续添加。）
- 子网掩码：32

- 下一条：网关
- 网关：10.0.10.1（vWAF_mgt_net网关IP）

目的路由配置

目的地: 52.82.209.55

子网掩码: 32

下一跳: ☒ 网关 ☐ 接口

网关: 10.0.10.1

时间表: -----

优先权: 1 (1 - 255), 缺省值: 1

路由权值: 1 (1 - 255), 缺省值: 1

描述: (1 - 63)字符

确定 取消



注意:

- “EC2 URL的IP地址” 可通过cmd窗口不断执行**nslookup**命令来获取，最终可获取到三个不同的公网IP地址。
- “EC2 URL地址” 国内版格式为：*ec2.当前所在区域.amazonaws.com.cn*；国际版本：*ec2.当前所有在区域.amazonaws.com。*
- 例如本示例中，执行命令：**nslookup ec2.cn-northwest-1.amazonaws.com.cn。**

6. 主设备vWAF-A上，继续配置HA的相关信息。选择“系统 > HA”，配置如下：

- HA控制连接接口：选择eth0/1
- HA链路本地MAC地址：选择“控制连接接口MAC”
- HA链路本地IP地址：10.0.100.164/255.255.255.0
- HA链路本地MTU：1600
- HA链路对端IP与MAC地址：ip 10.0.100. mac 0224.f8f3.e5e2（备设备上HA连接接口的IP地址，mac地址）

- HA簇ID：1
- 业务接口使用物理MAC：启用
- 在<组0>处配置：
- 优先级：50（设置HA优先级，值越小优先级越高，优先级高的为主设备。）

The screenshot displays the HA configuration interface with the following settings:

- HA控制连接接口:** ethernet0/1
- HA链路本地MAC地址:** ☐ 默认 ☒ 控制连接接口MAC ☐ 自定义
- HA链路本地IP地址:** 10.0.100.164 / 255.255.255.0
- HA链路本地MTU:** 1600 (1280 - 1600)字节
- HA链路对端IP与MAC地址:** 10.0.100.100 0224.f8f3.e5e2
- HA虚前缀:**
- HA簇ID:** 1 **节点ID:** 0 ①
- Peer-mode:** ☐ 启用
- HA Transmit UDP:** ☐ 启用 ①
- 业务接口使用物理MAC:** ☒ 启用
- Buttons:** HA同步配置, HA同步会话
- 组0:**
 - 新建:**
 - 优先级:** 50 (1 - 254)
 - 抢占时间:** 1 (0 - 600)秒, 0: 非抢占
 - Hello报文间隔:** 200 (50 - 10000)毫秒
 - Hello报文警戒值:** 15 (3 - 255)
 - 免费ARP包个数:** 15 (10 - 180)
 - 监测对象:**
 - 描述:** (1 - 31)字符

7. 在备设备vWAF-B上，配置HA相关的信息。

- HA控制连接接口：选择eth0/1
- HA链路本地MAC地址：选择“控制连接接口MAC”
- HA链路本地IP地址：10.0.100.100/255.255.255.0
- HA链路本地MTU：1600
- HA链路对端IP与MAC地址：ip 10.0.100.164 mac 0224.f8f3.e521（备设备上HA连接接口的IP地址，mac地址）

- HA簇ID：1
- 业务接口使用物理MAC：启用
- 在<组0>处配置：
 - 优先级：100（设置HA优先级，值越小优先级越高，优先级高的为主设备。）

HA控制连接接口：ethernet0/1

HA链路本地MAC地址：☐ 默认 ☒ 控制连接接口MAC ☐ 自定义

HA链路本地IP地址：10.0.100.100 / 255.255.255.0

HA链路本地MTU：1600 (1280 - 1600)字节

HA链路对端IP与MAC地址：10.0.100.164 0224.f8f3.e521

HA虚前缀：

HA簇ID：1 节点ID：1 ①

Peer-mode：☐ 启用

HA Transmit UDP：☐ 启用 ①

业务接口使用物理MAC：☒ 启用

HA 同步配置 HA同步会话

组0

新建

优先级：100 (1 - 254)

抢占时间：1 (0 - 600)秒,0：非抢占

Hello报文间隔：200 (50 - 10000)毫秒

Hello报文警戒值：15 (3 - 255)

免费ARP包个数：15 (10 - 180)

监测对象：

描述：

第九步：在AWS上配置云服务器的路由

1. 在VPC控制面板，点击左侧导航栏的“路由表”，进入路由表界面。
2. 点击"Create route table"按钮，在VPC下新建一条路由表“VM_sevice”。
3. 选择步骤上一步中创建的“VM_sevice”路由，点击页面下方的“Routes”标签页，然后点击“Edit routes”按钮。

- 在<Edit routes>页面，点击“Add route”按钮，添加一条路由，下一跳为vWAF-A的Secondary IP地址所在的网络接口。

Edit routes			
Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	eni-075bf835d3a771b4a	active	No

- 在VPC控制面板中的“子网”页面，选择web-server的子网server_net。
- 点击下方的“路由表”标签页，然后点击“编辑”按钮。
- 在<更改为>后面的下拉菜单中，选择步骤1-4创建的路由表。
- 点击“保存”。

第十步：在vWAF配置站点及策略

登录vWAF-A的WebUI管理界面，点击“站点”，进入站点页面。点击“新建站点”按钮。在弹出的<站点配置>对话框中，填入如下信息：

- 站点名称：Web-server
- 站点类型：HTTPS
- 服务：10.0.1.242（配置为SecondaryIP）端口：443
- 域名：Any
- 类型：SSL/TLS
- 密钥文件：指定SSL/TLS类型加密网站的密钥文件。
- 证书文件：指定SSL/TLS类型加密网站的证书文件。
- 安全策略：默认选择“policy_loose”安全策略模板。即仅开启最必要的防护类型，仅防御严重影响服务器功能的漏洞。

用户可按需配置IP防护策略、访问控制策略、虚拟补丁策略、自学习策略等，其他选项均采用默认值，具体可参考<vWAF-WebUI用户手册>。

配置结果

配置完成后，备设备上vWAF-B将同步主设备vWAF的配置信息，最终主备设备上的配置信息将保持一致。当主设备vWAF-A出现故障时，备份设备vWAF-B将自动切换为主设备，原先主设备上的Secondary IP、路由、安全策略等都将自动切换，无需人工重新配置，且不影响原先的业务通信，实现了对云服务器的高可靠的安全保障。

关于如何操作vWAF，请参考vWAF的用户手册 ([点击此处](#))。

在阿里云AliCloud上部署vWAF

系统要求

在阿里云上部署山石网科的虚拟Web应用防火墙（vWAF），需要宿主机满足以下要求。

- vWAF需要至少2个vCPU、4 GB虚拟内存。
- 已经注册阿里云。

准备工作

- 已创建如下VPC：
 - VPC：192.168.0.0/16
 - Subnet 0：192.168.1.0/24
- 创建安全组，并配置安全组规则。

部署虚拟Web应用防火墙

虚拟Web应用防火墙（vWAF）将作为一个ECS实例安装在VPC中。具体部署步骤如下：

"步骤一：创建对象存储" 在第84页

"步骤二：导入镜像" 在第85页

"步骤三：创建ECS实例" 在第85页

"步骤四：为VPC设置默认路由" 在第86页

"步骤五：访问vWAF" 在第86页

步骤一：创建对象存储

1. 登录阿里云，在阿里云的管理控制台中，选择左侧导航栏中“对象存储OSS”。
2. 点击页面右侧的“新建Bucket”按钮。
3. 在<新建Bucket>页面，输入Bucket的名称，如“test-vWAF”，完成配置。
4. 创建完成后，点击左侧导航栏中，刚创建完成的Bucket名称。
5. 在右侧的页面中，选择<文件管理>标签，点击“上传文件”按钮。
6. 在<上传文件>页面，文件ACL选择“私有”，然后将vWAF的".qcow"格式的文件上传。
7. 在文件列表中，点击刚上传的文件的“文件名”，在<预览>界面，复制“URL”的地址，用于后续创建镜像文件。



步骤二：导入镜像

1. 选择左侧导航栏中“云服务器ECS > 快照和镜像 > 镜像” 点击**导入镜像**按钮。
2. 在<导入镜像>的对话框中，配置如下信息。

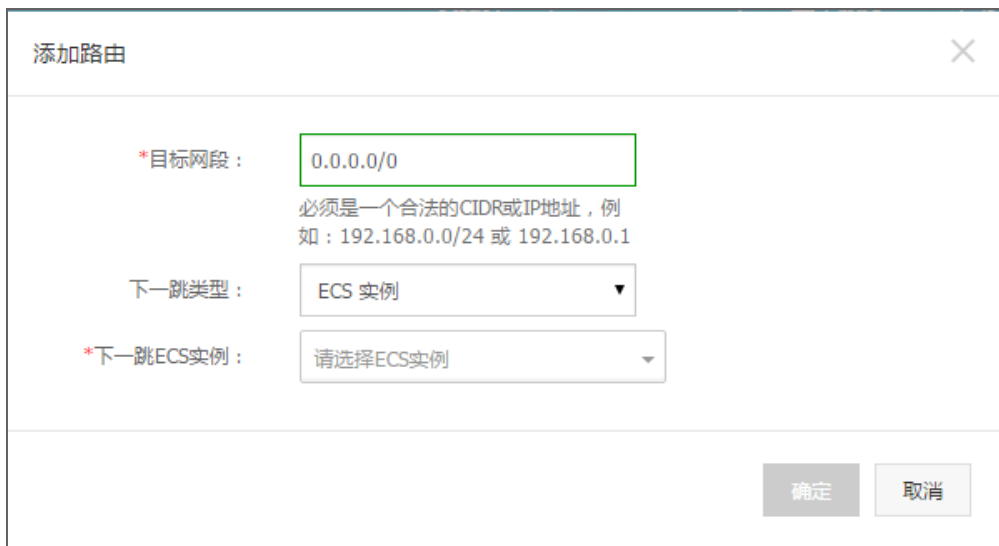
选项	说明
镜像所在地域	选择当前所在区域。
OSS Object地址	输入第一步中复制的“URL”地址。
镜像名称	指定镜像导入后显示的名称，如“vWAF-test”。
操作系统	选择“Linux”。
系统盘大小 (GB)	输入为100GB或根据实际情况填写。系统盘要求不能小于100GB。
系统架构	选择“X86_64”。
系统平台	选择“Other Linux”。
镜像格式	选择“QCOW2”。

步骤三：创建ECS实例

1. 选择左侧导航栏中“云服务器ECS > 实例”，点击**创建实例**按钮。
2. 在<1 基础配置>页面依次配置计费方式、地域、实例规格和镜像及存储。实例规格选择"ecs.c5.large 2vCPU 4GiB"，镜像选择第二步中创建的镜像“vWAF-test”，存储配置100GiB高效云盘。（此例中的配置为vWAF的最小资源配置。）
3. 在<2 网络及安全组>页面，<网络>部分选择“专有网络”，并配置预配置的VPC及私有网络；公网带宽部分勾选“分配公网IPv4地址”，实例将获得公网IP地址；选择ECS实例所属的安全组，如需从外网访问vWAF，此安全组需包含从公网到内网入方向的允许规则。
4. 在<3 系统配置>页面配置登录凭证为“使用镜像预设密码”；然后配置主机名等其他信息。
5. 点击右下角的“确认订单”按钮，页面上方显示当前配置信息，点击“创建实例”即可创建成功。

步骤四：为VPC设置默认路由

1. 在阿里云的管理控制台中，点击“产品与服务 > 专有网络VPC”。
2. 在左侧导航栏中选择<专有网络>页签，然后在vWAF所属的专有网络的操作栏中点击“管理”。
3. 在左侧导航栏中选择<路由器>页签，然后在虚拟路由列表页面的右上角点击“添加路由”按钮，弹出<添加路由>对话框。



4. 添加VPC的默认路由后，点击“确定”。
- 目标网段：任意目的地址0.0.0.0/0。
 - 下一跳类型：选择<ECS实例>类型。
 - 下一跳ECS实例：选择vWAF所在的ECS实例。

步骤五：访问vWAF

创建完成云主机后，云主机将启动，用户可访问Web应用防火墙。默认情况下管理口HTTPS协议处于开启状态,用户可以通过这种方式，使用云主机的公网IP，登录到vWAF。



注意: 如需从外网访问vWAF，ECS安全组需包含从公网到内网入方向的允许规则。

使用HTTPS远程登录vWAF:

1. 打开浏览器，在地址栏中vWAF的弹性公网IP: https://公网IP地址。
2. 在登录页面输入用户名hillstone。
3. 输入密码，默认为hillstone，建议登录WebUI后，修改密码。
4. 按回车键，即可登录。

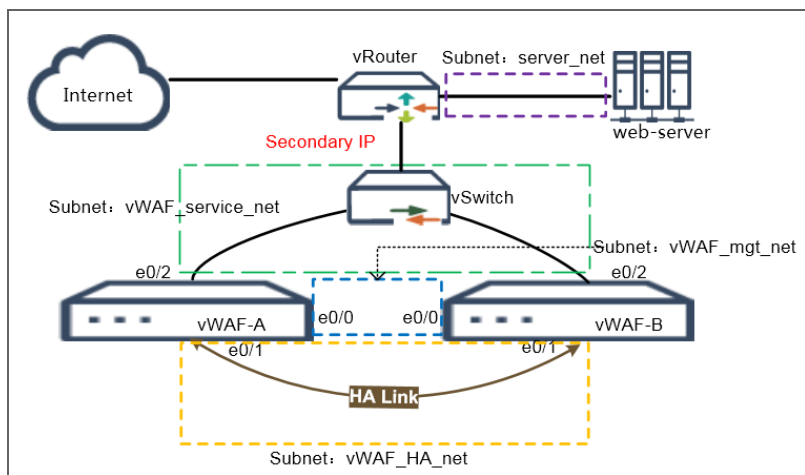
关于如何操作vWAF，参考WAF的用户手册（[点击此处](#)）。

在阿里云上进行vWAF的HA部署

组网设计

按照如下拓扑，在阿里云环境中2台云服务器web-server1和web-server2部署在server_net子网中，现通过部署vWAF的HA方案对2台服务器的流量进行负载均衡及其他应用层服务。

部署完成后，vWAF-A将被选举为主设备，vWAF-B为备份设备。vWAF-A会将其配置信息以及状态数据同步到备份设备vWAF-B。当主设备vWAF-A出现故障不能正常工作时，备份设备vWAF-B会在不影响用户通信的状态下自动切换为主设备，继续对云服务器的流量进行负载均衡及其他应用层服务，从而保证了服务的可靠性。



原云服务器web-server1、2所在VPC及子网：

- VPC(VPC1): 10.0.0.0/16
- vSwitch (server_net) : 10.0.2.0/24
- web-server1 : 10.0.2.209
- web-server2 : 10.0.2.210

现需要新建以下交换机，且子网所属VPC需与原web-server1、2所在的VPC相同：

- VPC(VPC1): 10.0.0.0/16
- vSwitch1 (vWAF_service_net) : 10.0.1.0/24
- vSwitch 2 (vWAF_mgt_net) : 10.0.10.0/24
- vSwitch 3 (vWAF_HA_net) : 10.0.100.0/24

部署步骤

[第一步：创建RAM角色](#)

[第二步：创建交换机](#)

[第三步：创建vWAF实例](#)

[第四步：新增弹性网卡并配置辅助私网IP](#)

[第五步：购买弹性公网IP并绑定到弹性网卡](#)

[第六步：申请AccesKey](#)

[第七步：在vWAF上进行HA相关配置](#)

第一步：创建RAM角色

1. 将鼠标悬浮在右上角的用户头像上，在弹出的对话框中,点击“访问控制”。
2. 选择左侧导航栏中，选择“RAM角色管理”。

3. 点击“创建RAM角色”，配置如下：

- 选择类型：选择“阿里云账号”；
- 配置角色：<角色名称：HA-role>;<选择云账号：选择当前云账号>
- 创建完成。
- 点击“为角色授权”，然后选择权限“AdministratorAccess—管理所有阿里云资源权限”；

4. 点击“确定”。

第二步：创建交换机

1. 选择左侧导航栏中“专有网络VPC > 专有网络 > 交换机” 点击**创建交换机**按钮，弹出<创建交换机>对话框。创建交换机名“vWAF_service_net”，网段为：10.0.1.0/24。

● 专有网络

VPC1/vpc-uf6p1256ymg3uq1sd6j6s

网段

10.0.0.0/8

IPv6网段 ?

开通IPv6

● 名称 ?

vWAF_service_net16/128

● 可用区 ?

可用区资源 ?

ECSRDSALB

● IPv4网段

10.0.1.0/24

一旦创建成功，网段不能修改

2. 重复上述步骤，继续配置交换机vWAF_mgt_net和vWAF_HA_net，注意：三台交换机需在同一个可用区。

交换机的配置信息如下：

选项	配置信息
vWAF_mgt_net	
VPC名称	选择上一步创建的VPC“VPC1”。
交换机名称	指定交换机名称为“vWAF_mgt_net”。
可用区	选择与VPC1相同的区，如华东1可用区A。

选项	配置信息
目标网段	10.0.10.0/24
vWAF_HA_net	
VPC名称	选择上一步创建的VPC “VPC1”。
交换机名称	指定交换机名称为 “vWAF_HA_net”。
可用区	选择与VPC1相同的区，如华东1可用区A。
目标网段	10.0.100.0/24

第三步：创建vWAF实例

1. 选择“云服务器ECS > 实例与镜像 > 实例”在阿里云上创建vWAF实例vWAF-A和vWAF-B，用于部署HA，具体创建步骤请参考“在阿里云AliCloud上部署vWAF” 在第83页。

实例规格要求：最少使用2个vCPU、内存最小为4GB，两个实例的默认网卡均选择同一VPC下同一个交换机vWAF_mgt_net。

HA实例的配置信息如下：

选项	配置信息
vWAF-A	
实例名称	配置为vWAF-A
实例规格	推荐选择 “ecs.ic5.xlarge（4核4GB，密集计算型ic5）”。
网卡	主网卡：VPC：VPC1，交换机vWAF_mgt_net。 辅助网卡：VPC：VPC1，交换机vWAF_HA_net。
公网带宽	勾选“分配公网IPv4地址”，实例将获得公网IP地址
高级选项	实例RAM角色：选择第一步中创建的RAM角色 “HA-role”。
vWAF-B	
实例名称	配置为vWAF-B
实例规格	推荐选择 “ecs.ic5x.large（4核4GB，密集计算型ic5）”。

选项	配置信息
网卡	主网卡：VPC：VPC1，交换机vWAF_mgt_net。 辅助网卡：VPC：VPC1，交换机vWAF_HA_net。
高级选项	实例RAM角色：选择第一步中创建的RAM角色“HA-role”。

第四步：新增弹性网卡并配置辅助私网IP

1. 选择“云服务器ECS > 网络与安全 > 弹性网卡”，点击“创建弹性网卡”创建弹性网卡“vWAF-HA”。

- 网卡名称：vWAF_serviceA
- 专有网络：VPC1
- 交换机：vWAF_service_net
- 安全组：选择与实例相同的安全组。

网卡名称：

vWAF_serviceA

长度为2-128个字符，不能以http://或https://开头，必须以大小字母或中文开头，可包含数字，“_”或“-”。

*专有网络：

vpc-uf6p1256ymg3uq1sd6j6s / VPC1

*交换机：

vsw-uf6sgxbzwn6iu230393i / vWAF_ser...

选择的交换机的可用区，需要和将绑定的实例相同
交换机地址段：10.0.1.0/24 (cn-shanghai-a)

主私网IP：

必须是在所属VSwitch的地址段内的空闲地址。默认随机分配该交换机中的空闲地址。

辅助私网IP：

最大可分配9个私网IP

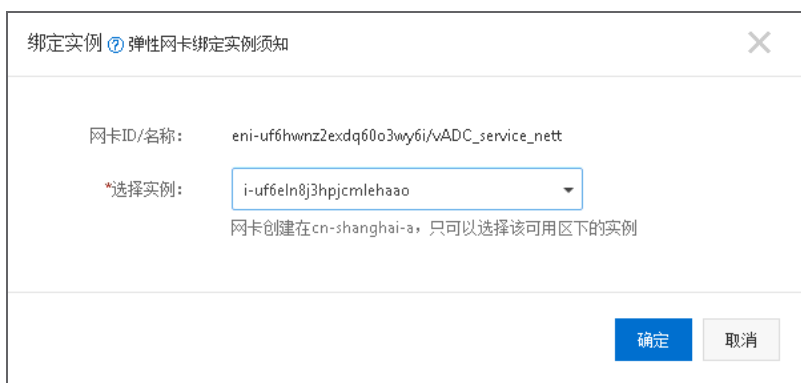
☒ 不设置
☐ 自动分配
☐ 指定地址

*安全组：

选择专有网络安全组

安全组名称	安全组ID
sg-uf62ltuhpyd5577...	sg-uf62ltuhpyd55772u6g2

2. 点击“确定”，创建完成。
3. 在弹性网卡列表中，选择刚才创建的网卡后的“绑定实例”，然后选择上面创建的实例“vWAF-A”。



4. 同理，重复步骤1-2，继续创建一个弹性网卡vWAF_serviceB： vWAF_service_net，然后绑定到实例vWAF-B。
5. 绑定完成所有网卡后，重启实例vWAF-A和vWAF-B。
6. 在网卡列表中，选择HA主设备vWAF-A的业务网卡“vWAF_service1”，点击“管理辅助私网IP”，点击“分配新IP”，配置私网辅助IP，如：10.0.1.242。

第五步：购买弹性公网IP并绑定到弹性网卡

1. 选择“云服务器ECS > 网络与安全 > 弹性公网IP”，点击“购买弹性公网IP”。
2. 购买后，选中该弹性公网IP，点击列表下方的“绑定”按钮，在<绑定弹性公网IP至资源>对话框中，选择vWAF-A的辅助弹性网卡： vWAF_serviceA；
3. 点击“确定”，完成绑定。

第六步：申请AccessKey

1. 将鼠标悬浮在右上角的用户头像上，在弹出的对话框中，点击“AccessKey管理”。
2. AccessKey是阿里云API的密钥，具有当前账号的完全权限，需经过管理员手机验证，申请后续妥善保管

好。

3. 点击“创建AccessKey”进行创建，然后复制粘贴AccessKey ID和Secret，用于后续步骤的使用。

第七步：在vWAF上进行HA相关配置

1. 在云平台上，查看vWAF-A和vWAF-B的vWAF_mgt_net的弹性公网IP地址等信息并记录，然后使用弹性公网IP地址登录vWAF-A的WebUI界面，具体方法，请参考[使用HTTPS登录vWAF](#)。
2. 初次访问WAF设备时可按照“WAF安装向导”进行配置：
 - 选择部署模式：单臂模式
 - LAN接口：ethernet0/2；安全域：Untrust（该接口为vWAF_service_net对应的接口）
 - IP地址：配置为辅助私网IP：10.0.1.242。
 - 掩码：24
3. 查看vWAF-A，vWAF-B获取的DNS Server地址，本示例中查看到为10.0.0.2。然后继续配置系统时间，完成配置向导。
4. 分别在vWAF-A和vWAF-B的接口eth0/0下配置路由优先级，同时关闭逆向路由检查。



5. 在vWAF-A上，将辅助私网IP配置到vWAF的vWAF-Service-net对应的接口，本示例对应eth0/2。(此配置可只在主设备进行配置，开启HA后会同步到备设备上。)

- 绑定安全域：三层安全域
- 安全域：untrust
- HA同步：启用
- 类型：静态IP
- IP地址：10.0.1.242（已配置为辅助私网IP地址及其掩码。）
- 网络掩码：24
- 管理方式：开启PING

6. 选择“网络 > 路由 > 目的路由”，配置静态默认路由，下一跳地址是vWAF_service_net子网的网关地址。(此配置可只在主设备进行配置，开启HA后会同步到备设备上。)

- 目的地：0.0.0.0
- 子网掩码：0

- 下一条：网关
- 网关：10.0.1.253（vWAF_service_net网关IP）

目的路由配置

所属虚拟路由器：trust-vr

目的地：0.0.0.0

子网掩码：0

下一跳：
☒ 网关
☐ 接口

网关：10.0.1.253

时间表：-----

优先权：1 (1 - 255), 缺省值：1

路由权值：1 (1 - 255), 缺省值：1

描述：(1 - 63)字符

确定 取消

7. 主设备vWAF-A上，继续配置HA的相关信息。选择“系统 > HA”，配置如下：

- HA控制连接接口：选择eth0/1
- HA链路本地MAC地址：选择“控制连接接口MAC”
- HA链路本地IP地址：10.0.100.164/255.255.255.0
- HA链路本地MTU：1600
- HA链路对端IP与MAC地址：ip 10.0.100. mac 0224.f8f3.e5e2（备设备上HA连接接口的IP地址，mac地址）
- HA簇ID：1
- HA Transmit UDP：启用
- 业务接口使用物理MAC：启用
- 阿里云部署HAVIP：不启用
- 访问密钥ID：配置为前面第六步复制保存的AccessKey ID。
- 访问密钥密码：配置为前面第六步复制保存的AccessKey Secret。

- 在<组0>处配置：
- 优先级：50（设置HA优先级，值越小优先级越高，优先级高的为主设备。）

HA控制连接接口：
ethernet0/1

HA链路本地MAC地址：
☐ 默认
☒ 控制连接接口MAC
☐ 自定义

HA链路本地IP地址：
10.0.100.164 / 255.255.255.0

HA链路本地MTU：
1600 (1280 - 1600)字节

HA链路对端IP与MAC地址：
10.0.100.100 0224.f8f3.e5e2

HA虚前缀：

HA簇ID：
1 节点ID：
0 ①

Peer-mode:
☐ 启用

HA Transmit UDP:
☒ 启用 ①

业务接口使用物理MAC：
☒ 启用

阿里云部署HAVIP:
☐ 启用 ①

访问密钥ID：
LTAI4FgjDcL99Jw/jiuQjdPr (0 - 64)字符

访问密钥密码：
(0 - 32)字符

HA同步配置
HA同步会话

组0

新建

优先级：
150 (1 - 254)

抢占时间：
1 (0 - 600)秒,0: 非抢占

Hello报文间隔：
200 (50 - 10000)毫秒

Hello报文警戒值：
15 (3 - 255)

免费ARP包个数：
15 (10 - 180)

监测对象：

描述：
(1 - 31)字符

确定

8. 在备设备vWAF-B上，配置HA相关的信息。

- HA控制连接接口：选择eth0/1
- HA链路本地MAC地址：选择“控制连接接口MAC”
- HA链路本地IP地址：10.0.100.100/255.255.255.0
- HA链路本地MTU：1600

- HA链路对端IP与MAC地址：ip 10.0.100.164 mac 0224.f8f3.e521（主设备上HA连接接口的IP地址，mac地址）
- HA簇ID：1
- HA Transmit UDP：启用
- 业务接口使用物理MAC：启用
- 阿里云部署HAVIP：不启用
- 访问密钥ID：配置为前面步骤一复制保存的AccessKey ID。
- 访问密钥密码：配置为前面步骤一复制保存的AccessKey Secret。
- 在<组0>处配置：

- 优先级：100（设置HA优先级，值越小优先级越高，优先级高的为主设备。）

HA控制连接接口：
HA链路本地MAC地址：
HA链路本地IP地址：
HA链路本地MTU：
HA链路对端IP与MAC地址：
HA虚前缀：
HA簇ID：
Peer-mode：
HA Transmit UDP：
业务接口使用物理MAC：
阿里云部署HAVIP：
访问密钥ID：
访问密钥密码：

ethernet0/1

☐ 默认
☒ 控制连接接口MAC
☐ 自定义

10.0.100.100 / 255.255.255.0

1600 (1280 - 1600)字节

10.0.100.164 0224.f8f3.e521

1 节点ID： 1

☐ 启用

☒ 启用

☒ 启用

☐ 启用

LTAl4FgjDcL99JwJiuQjdPr (0 - 64)字符

..... (0 - 32)字符

HA同步配置
HA同步会话

组0

新建

优先级：
抢占时间：
Hello报文间隔：
Hello报文警戒值：
免费ARP包个数：
监测对象：
描述：

100 (1 - 254)
1 (0 - 600)秒,0：非抢占
200 (50 - 10000)毫秒
15 (3 - 255)
15 (10 - 180)

(1 - 31)字符

确定

第八步：在vWAF配置站点及策略

登录vWAF-A的WebUI管理界面，点击“站点”，进入站点页面。点击“新建站点”按钮。在弹出的<站点配置>对话框中，填入如下信息：

- 站点名称：Web-server
- 站点类型：HTTPS
- 服务：10.0.1.242（配置为辅助私网IP）端口：443
- 域名：Any

- 类型：SSL/TLS
- 密钥文件：指定SSL/TLS类型加密网站的密钥文件。
- 证书文件：指定SSL/TLS类型加密网站的证书文件。
- 安全策略：默认选择“policy_loose”安全策略模板。即仅开启最必要的防护类型，仅防御严重影响服务器功能的漏洞。
- 在<负载均衡>页签下，配置Web-server的IP地址10.0.2.11。

用户可按需配置IP防护策略、访问控制策略、虚拟补丁策略、自学习策略等，其他选项均采用默认值，具体可参考<vWAF-WebUI用户手册>。

配置结果

配置完成后，备设备上vWAF-B将同步主设备vWAF的配置信息，最终主备设备上的配置信息将保持一致。当主设备vWAF-A出现故障时，备份设备vWAF-B将自动切换为主设备，原先主设备上的Secondary IP、路由、安全策略等都将自动切换，无需人工重新配置，且不影响原先的业务通信，实现了对云服务器的高可靠的安全保障。

关于如何操作vWAF，请参考vWAF的用户手册（[点击此处](#)）。

在腾讯云上部署vWAF

系统要求

在腾讯云上部署山石网科的虚拟Web应用防火墙（vWAF），需要宿主机满足以下要求。

- vWAF至少需要2个vCPU、4GB虚拟内存。
- 已经注册腾讯云。

安装步骤

"步骤一：创建VPC" 在第101页

"步骤二：创建子网" 在第102页

"步骤三：创建对象存储" 在第103页

"步骤四：导入镜像" 在第103页

"步骤五：创建云服务器" 在第104页

"步骤六：访问vWAF" 在第107页

步骤一：创建VPC

1. 登录腾讯云，点击“控制台”进入控制台界面，点击**云产品>网络>私有网络**，页面跳转到“私有网络”界面。

2. 点击“新建”按钮，弹出<新建VPC>对话框，配置私有网络和初始子网的信息。示例如下：

新建VPC

私有网络信息

所属地域华东地区（上海）

名称test

CIDR172.16.0.0 / 16

创建后不可修改，查看约束

初始子网信息

子网名称private

CIDR172.16.0.0 / 24

可用区上海一区

关联路由表默认

创建

取消

3. 点击“创建”，完成配置。

步骤二：创建子网

1. 点击左侧导航栏>子网，页面跳转到“子网”界面，点击“新建”按钮，弹出<创建子网>对话框。

创建子网

所属网络vpc-l1ksujz4 (test | 172.16.0.0/16)

已有1个子网

子网名称	CIDR	可用区	关联路由表	操作
请输入子网名称	0/60 172.16.0.0 / 24	上海一区	default	-

+ 新增一行

创建

取消

2. 在“所属网络”下拉列表中，选择上一步创建的VPC。

3. 在子网列表中，输入“子网名称”及CIDR等信息，若需添加多个网段可点击“新增一行”。
4. 点击“创建”，完成配置。

步骤三：创建对象存储

1. 选择“存储>对象存储>存储桶列表”，点击“创建存储桶”，创建存储桶，例如“test”。
2. 创建完成后，在存储桶列表中，点击刚创建完成的存储桶名称。
3. 进入<文件列表>标签页，点击“上传文件”按钮。
4. 在<上传文件>页面，将vWAF的".qcow"格式的软件包文件上传。
5. 上传完成后，在文件列表中，点击刚上传的文件的“详情”链接，在<文件列表>标签页，点击“复制链接”复制存储对象的URL地址，用于后续创建镜像文件。



步骤四：导入镜像

1. 选择“云服务器>镜像”，点击**导入镜像**按钮。
2. 在<导入镜像前准备>页面中，勾选“我已做好以上准备”，点击“下一步”按钮。
3. 在<导入镜像>的对话框中，配置如下信息。

选项	说明
镜像文件URL	输入上一步中复制的“URL”链接地址。
镜像名称	指定镜像导入后显示的名称，如“vWAF-test”。
地域	选择所在区域。
操作系统	选择“Linux”。
系统架构	选择“64位”。
系统平台	选择“Other Linux”。
镜像格式	选择“QCOW2”。
导入方式	选择“强制”导入方式。

步骤五：创建云服务器

1. 在子网列表中，点击步骤二创建的子网后面的添加云主机图标，页面跳转到<云服务器CVM>界面。



子网 华东地区（上海） 全部私有网络 私有网络与子网帮助文档									
火热内测：网关精细化流量分析和带宽控制，提供基于IP-网关粒度的“监”与“控”功能，前往申请，查看操作指南									
+新建 筛选									
搜索子网的名称/ID									
ID/名称	所属网络	CIDR	可用区	关联路由表	云主机	可用IP	默认子网	操作	
subnet-h72iedwf private	vpc-41ksujz4 test	172.16.1.0/24	上海一区	rtb-af08leg9 default	0 	253	否	删除 更换路由表	

2. 选择<自定义配置>,然后开始配置：<1.选择地域和机型>。如下示例配置：配置完成后，点击“下一步：选择镜像”按钮。

- **计费模式**：按量计费；
- **地域**：根据实际环境选择；
- **机型**：选择“标准S1，S1.MEDIUM4”（vWAF虚拟Web应用防火墙要求最少使用2个vCPU、内存最小为4GB，硬盘不小于100GB。

注意：为达到vWAF最佳使用性能，推荐使用机型：标准型s1、标准型s2（2vCPU+4G内存、

8vCPU+16G内存)和标准型sa1 (2vCPU+4G内存))。

1.选择地域与机型 2.选择镜像 3.选择存储与网络 4.设置信息

计费模式 ⑦ 包年包月 按量计费 详细对比

地域 华南地区 华东地区 华北地区 西南地区 东南亚地区 亚太地区 北美地区

广州 上海 北京 成都 香港 新加坡 首尔 悉尼 多伦多

美国西部 欧洲地区 美国东部 美国中部 亚太地区 南美地区

硅谷 法兰克福 华盛顿 达拉斯 印度金奈 悉尼 巴西圣保罗 更多地域

不同地域云产品之间内网不互通；选择最靠近您客户的地域，可降低访问时延，创建成功后不支持切换地域。 查看我的云服务器地域 详细对比

可用区 ⑦ 上海一区

系列 ⑦ 系列1 系列2 详细对比

机型 标准型S1 内存型M1 高IO型I1

机型	规格	vCPU ⑦	内存 ⑦	费用 ⑦
☐ 标准型S1	S1.SMALL4	1核	4G	0.46元/小时起
☐ 标准型S1	S1.MEDIUM2	2核	2G	0.46元/小时起
☒ 标准型S1	S1.MEDIUM4	2核	4G	0.61元/小时起
☐ 标准型S1	S1.MEDIUM8	2核	8G	0.91元/小时起
☐ 标准型S1	S1.MEDIUM12	2核	12G	1.22元/小时起
☐ 标准型S1	S1.LARGE4	4核	4G	0.92元/小时起

下一步：选择镜像 初始价格仅包含CPU及内存价格，不包含系统盘、数据盘、镜像和带宽等其他价格。

3. 在<2.选择镜像>标签页，**镜像提供方**选择“自定义镜像”，并选择上一步中创建的镜像文件。

1.选择地域与机型 2.选择镜像 3.选择存储和带宽 4.设置安全组和主机 5.确认配置信息

镜像 公共镜像 自定义镜像 共享镜像 镜像市场 ⑦

镜像版本 已选择：wv02 ⑦ 搜索镜像关键字

wv02 镜像ID：img-d451jnf，描述：WAF Wv02

wv02-1207 镜像ID：img-3kasru03，描述：无

cma-vwaf-1210 镜像ID：img-a59owlbr，描述：test-cma

cma-vfw 镜像ID：img-clm5p6pd，描述：无

上一步 下一步：选择存储和带宽

4. 在<3.选择存储与带宽>标签页中，如下示例：配置**系统盘**：选择100GB高性能云硬盘；**网络类型**：选择私有网络，并选择步骤一、二所配置的VPC和子网；**带宽计费模式**：选择“按使用流量”，然后点

击“下一步：设置信息”。

1.选择地域与机型

2.选择镜像

3.选择存储和带宽

4.设置安全组和主机

5.确认配置信息

系统盘

高性能云硬盘

SSD云硬盘

⑦ 选购指引

购买成功后，系统盘不支持更换介质

0GB

500GB

1024GB

-

100

+

GB

数据盘

+ 新建云硬盘数据盘

还可添加 10 云硬盘 ⑦

网络计费模式

按带宽计费

按使用流量

⑦ 详细对比

带宽上限

0Mbps

5Mbps

20Mbps

100Mbps

-

46

+

Mbps ⑦

☒ 分配免费公网IP ⑦

注意：流量费用每小时结算一次，当账户余额不足时，两小时内将被停止流量服务。

公共网关

☐ 用作公网网关 ⑦

5. 在<4.设置信息>标签页中，如下示例：配置**主机名**：选择“立即命名”，并配置主机名为vWAF；**登录方式**：选择“保留镜像设置”；**安全组**：已有安全组，并从下拉列表中选择安全组。

1.选择地域与机型

2.选择镜像

3.选择存储和带宽

4.设置安全组和主机

5.确认配置信息

所属项目

默认项目

?

安全组

新建安全组

已有安全组

?

sg-gwwq4dap | 放通全部端口

?

使用指引

如您有业务需要放通其他端口，您可以 新建安全组

安全组规则

入站规则

出站规则

目标	协议端口	策略	备注
0.0.0.0/0	ALL	允许	-
0.0.0.0/0	ALL	拒绝	-

注意：目标为0.0.0.0/0 表示所有IP地址都可以用于访问，建议填写您常用的IP地址

实例名称

vWAF

你还可以输入56个字符

?

登录方式

设置密码

立即关联密钥

自动生成密码

保留镜像设置

?

注：创建后，您可使用自定义镜像内登录信息(密钥/密码)登录。

**注意:** 如需从外网访问vWAF，安全组需包含从公网到内网入方向的允许规则。

6. 点击“开通”按钮，完成云主机的配置。

步骤六：访问vWAF

创建完成云主机后，云主机将启动，用户可访问Web应用防火墙。默认情况下管理口HTTPS协议处于开启状态,用户可以通过这种方式，使用云主机的公网IP，登录到vWAF。

ID/主机名	监控/状态	可用区	主机类型	配置	主IP地址	主机计费模式	所属项目	操作
ins-art7ujph vWAF	运行中	上海一区	标准型S1	2核 4GB 1Mbps 系统盘：本地硬盘 网络：test	115.159.95.51 (公网) 172.16.1.7 (内网)	按量计费 2018-03-15 09:57 创建	默认项目	登录 更多

使用HTTPS远程登录vWAF

1. 打开浏览器，在地址栏中输入https://公网IP地址。
2. 在登录页面输入创建虚拟机时设置的用户名和密码。
3. 按回车键，即可登录。

关于如何操作虚vWAF，参考Web应用防火墙的用户手册（[点击此处](#)）。



注意:

使用腾讯云API创建vWAF实例时，通过LoginSettings.Password参数设置的密码不生效或在腾讯云WebUI上创建vWAF实例时，通过“自定义配置>设置安全组和主机”界面设置的密码也不生效。

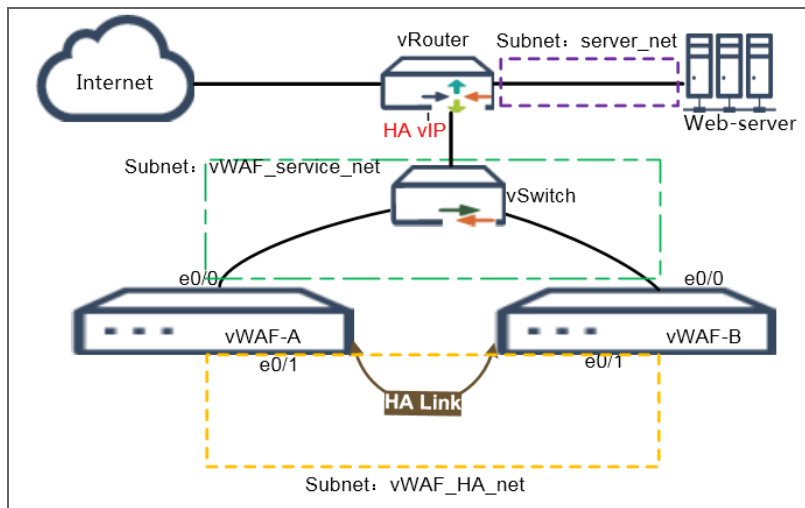
建议：请使用自动导入配置文件脚本的方式设置密码。

在腾讯云上进行vWAF的HA部署

组网设计

按照如下拓扑，在腾讯云环境中有一台云服务器Web-server（10.0.2.11），现通过部署vWAF的HA方案对云服务器进行安全防护。

部署完成后，vWAF-A将被选举为主设备，对云服务器进行安全防护；vWAF-B为备份设备。vWAF-A会将其配置信息以及状态数据同步到备份设备vWAF-B。当主设备vWAF-A出现故障不能正常工作时，备份设备vWAF-B会在不影响用户通信的状态下自动切换为主设备，继续对云服务器进行安全防护，从而提高了网络可靠性，保证云服务器的业务不中断。



部署步骤

"步骤一：创建VPC及子网" 在第110页

"步骤二：创建vWAF云主机" 在第110页

"步骤三：创建弹性网卡" 在第111页

"步骤四：申请高可用虚拟IP" 在第112页

"步骤五：在vWAF上进行HA相关配置" 在第113页

"步骤六：验证HA结果" 在第118页

步骤一：创建VPC及子网

登录腾讯云，点击“控制台”进入控制台界面，创建VPC及子网，具体操作方法，请参阅"在腾讯云上部署vWAF"在第101页中的“创建VPC”和“创建子网”章节。

原云服务器Web-server所在VPC及子网：

- VPC(VPC1): 10.0.0.0/16
- Subnet 0 (server_net) : 10.0.2.0/24
- Web-server IP: 10.0.2.11

现需要新建以下子网，且子网所属VPC需与原Web-server所在的VPC相同：

- VPC(VPC1): 10.0.0.0/16
- Subnet 1 (vWAF_service_net) : 10.0.1.0/24
- Subnet 2 (vWAF_HA_net) : 10.0.100.0/24

步骤二：创建vWAF云主机

1. 选择“私有网络 > 子网”，在子网“vWAF_service_net”上，创建2台vWAF云主机vWAF-A和vWAF-B，具体创建步骤请参考"在腾讯云上部署vWAF"在第101页。

注意：在<3.选择存储和带宽>页面中，不要勾选“分配免费公网IP界面”。

2. **云主机规格要求：**最少使用2个vCPU、内存最小为4GB，两个云主机的默认网卡均选择网络vWAF_service_net。（由于两台云主机的配置一样，可直接购买2台，然后重命名为vWAF-A和vWAF-B。vWAF-A将作为HA场景中的主设备，vWAF-B将作为备设备。）

步骤三：创建弹性网卡

- 1. 选择“私有网络 > IP与网卡 > 弹性网卡”，点击“新建”按钮。
- 2. 在<新建弹性网卡>对话框中，配置如下信息:

新建弹性网卡

名称

vWAF-A-HA

所在地域

广州

所属网络

vpc-a1p3dhij (VPC1 | 10.0.0.0/16)

所属子网

subnet-m9t3i72vWAF-HA-net | 0.0.100.0/24

可用区

广州四区

可分配IP数

1/30个 (当前子网可用IP剩余251个)

分配IP

主 IP

自动分配

系统将自动分配IP地址

增加一个辅助IP

确定

取消

- 3. 弹性网卡的配置信息如下：

选项	配置信息
名称	指定弹性网卡的名称为"vWAF-A-HA"。
所属网络	选择步骤一中配置私有网络的“VPC1”
所属子网	选择步骤一中配置的子网“vWAF_HA_net”。

- 4. 重复步骤1-3，创建弹性网卡“vWAF-B-HA”。
- 5. 在弹性网卡列表界面，选中“vWAF-A-HA”条目的操作列的“绑定云主机”按钮。

6. 在<绑定云主机>对话框中，选择步骤三中创建的云主机“vWAF-A”。
7. 重复步骤5、6,将弹性网卡“vWAF-B-HA”绑定到云主机“vWAF-B”。

步骤四：申请高可用虚拟IP

1. 选择“私用网络>IP与网卡>高可用虚拟IP”，点击“申请”按钮。**注意：**只有腾讯云主账号才能申请高可用虚拟IP，子账号不支持申请。
2. 在<新建高可用虚拟IP>对话框中，配置如下信息：

申请高可用虚拟IP

名称

HA-vip

所在地域

广州

私有网络

vpc-a1p3dhij(VPC1 | 10.0.0.0/16)

子网

subnet-iuizb7j2(vWAF-service|10.0.1.0/24)

可用区

广州四区

子网CIDR

10.0.1.0/24

子网可用IP

251

可分配

0/10

IP地址

自动分配

确定

取消

高可用虚拟IP的配置信息如下：

选项	配置信息
名称	指定高可用虚拟IP的名称为"HA-vIP"。
所在网络	选择步骤一中配置私有网络的“VPC1”
所属子网	选择步骤一中配置的子网“vWAF-service-net”。

- 选择“私有网络 > IP与网卡 > 弹性公网IP”，申请一个弹性公网IP。
- 点击操作列的“绑定”，将其与高可用虚拟IP绑定。

ID/名称	监控	状态 ▾	弹性IP地址	计费模式 ▾	绑定资源	绑定资源类型
elip-rtsc4y8c 未命名		已绑定	111.230.56.224	停止计费	havip-3uh9jmhq	HA VIP

步骤五：在vWAF上进行HA相关配置

- 创建完成云主机后，云主机将启动，用户可访问Web应用防火墙。默认情况下管理口HTTPS协议处于开启状态,用户可以通过这种方式，使用云主机的公网IP，登录到vWAF。具体方法可查看[使用HTTPS远程登录vWAF](#)。
- 输入用户名、密码（默认分别为hillstone、hillstone）登录到实例vWAF-A，选择“网络 > 接口”，选择ethernet0/0口，配置如下：
 - 绑定安全域：三层安全域
 - 安全域：untrust
 - 类型：静态IP
 - IP地址：配置为云平台上的高可用虚拟IP地址。
 - 网络掩码：24
 - 高级选项 > 管理IP :配置为vWAF-A中Subnet 1（vWAF_service_net）子网的IP地址。

- 管理方式：开启SSH/PING/HTTPS



3. 选择"网络 > 路由 > 目的路由", 配置静态默认路由, 下一跳地址是vWAF_service_net子网的网关地址。



4. 登录vWAF-B, 选择“网络 > 接口”, 选择ethernet0/0口, 配置如下信息。

- 绑定安全域：三层安全域
- 安全域：untrust

- 类型：静态IP，即关闭DHCP自动获取

The screenshot shows the 'Ethernet 接口' configuration window with the following details:

- 基本配置**
 - 接口名称: ethernet0/0
 - 描述: (0 - 63)字符
 - 绑定安全域: ☐ 二层安全域 ☒ 三层安全域 ☐ TAP ☐ 无绑定
 - 安全域: untrust
 - HA同步: ☐ 启用
- IP配置**
 - 类型: ☒ 静态IP ☐ 自动获取
 - IP地址:
 - 子网掩码:
 - ☐ 配置为Local IP
 - 高级选项
- 管理方式**
 - ☐ Telnet ☒ SSH ☒ Ping ☐ HTTP ☒ HTTPS ☐ SNMP
- 路由**
 - 逆向路由: ☐ 启用 ☒ 关闭 ☐ 自动

Buttons at the bottom: 确定, 取消

5. 主设备vWAF-A上，配置HA的监测对象。选择“对象 > 监测对象”，并点击“新建”。

- 名称: track1
- 警戒值: 255
- 监测类型: 选择<接口>单选按钮，并点击“添加”按钮。在弹出的<添加监测对象>对话框，指

定接口为“ethernet0/0”，权值为“255”

监测对象配置

监测对象

名称：

track

(1 - 31)字符

警戒值：

255

(1 - 255)，缺省值：255

监测类型：

接口

HTTP/Ping/ARP/DNS/TCP

链路质量探测

HA同步：

启用

添加监测成员

+ 添加 - 删除

☐	类型	接口	权值
☐	接口	ethernet0/0	255

确定

取消

6. 主设备vWAF-A上，继续配置HA的相关信息。选择“系统 > HA”，配置如下：
- HA控制连接接口：选择eth0/1
 - HA链路本地MAC地址：选择“控制连接接口MAC”
 - HA链路本地IP地址：10.0.100.4/255.255.255.0
 - HA链路本地MTU：1600
 - HA链路对端IP与MAC地址：ip 10.0.100.5 mac 0224.f8f3.c5e2（备设备上HA连接接口的IP地址，mac地址）
 - HA簇ID：1
 - 业务接口使用物理MAC：启用
 - 在<组0>处配置。
 - 优先级：50（设置HA优先级，值越小优先级越高，优先级高的为主设备。）

- 监测对象：track1

The screenshot shows a configuration window for HA (High Availability) settings. The top section contains fields for:

- HA控制连接接口: ethernet0/1
- HA链路本地MAC地址: Radio buttons for 默认, 控制连接接口MAC (selected), and 自定义.
- HA链路本地IP地址: 10.0.100.4 / 255.255.255.0
- HA链路本地MTU: 1600 (1280 - 1600)字节
- HA链路对端IP与MAC地址: 10.0.100.5 / 0224.f8f3.e5e2
- HA虚前缀: (empty)
- HA簇ID: 1 (dropdown), 节点ID: 0 (dropdown) with an info icon.
- Peer-mode: ☐ 启用
- HA Transmit UDP: ☐ 启用 (with an info icon)
- 业务接口使用物理MAC: ☒ 启用

 Below these are two buttons: HA同步配置 and HA同步会话.

 The bottom section is titled '组0' and contains a '新建' button followed by several configuration fields:

- 优先级: 50 (1 - 254)
- 抢占时间: 1 (0 - 600)秒, 0: 非抢占
- Hello报文间隔: 200 (50 - 10000)毫秒
- Hello报文警戒值: 15 (3 - 255)
- 免费ARP包个数: 15 (10 - 180)
- 监测对象: track1 (dropdown)
- 描述: (empty) (1 - 31)字符

7. 在备设备vWAF-B上，配置HA相关的信息。

- HA控制连接接口：选择eth0/1
- HA链路本地MAC地址：选择“控制连接接口MAC”
- HA链路本地IP地址：10.0.100.5/255.255.255.0
- HA链路本地MTU：1600
- HA链路对端IP与MAC地址：ip 10.0.100.4 mac 0224.f8f3.e521（备设备上HA连接接口的IP地址，mac地址）
- 业务接口使用物理MAC：启用
- HA簇ID：1

- 在<组0>处配置。
- 优先级：100（设置HA优先级，值越小优先级越高，优先级高的为主设备。）

HA控制连接接口：
HA链路本地MAC地址：
HA链路本地IP地址：
HA链路本地MTU：
HA链路对端IP与MAC地址：
HA虚前缀：
HA簇ID：
Peer-mode：
HA Transmit UDP：
业务接口使用物理MAC：

ethernet0/1

☐ 默认
☒ 控制连接接口MAC
☐ 自定义

10.0.100.5 / 255.255.255.0

1600 (1280 - 1600)字节

10.0.100.4 0224.f8f3.ee21

1 节点ID：1

☐ 启用

☐ 启用

☒ 启用

HA同步配置

HA同步会话

组0

新建

优先级：100 (1 - 254)

抢占时间：1 (0 - 600)秒,0：非抢占

Hello报文间隔：200 (50 - 10000)毫秒

Hello报文警戒值：15 (3 - 255)

免费ARP包个数：15 (10 - 180)

监测对象：

描述：

步骤六：验证HA结果

配置完成后，优先级高的vWAF-A会自动协商为主设备，优先级低的vWAF-B为备设备，，点击“系统 > 系统信息”，两台设备的HA状态分别如下显示：

- Device A
HA状态：Master
- Device B
HA状态：Backup

由于两台设备已经协商成功，因此之后的配置只需在主设备上配置即可，配置完后会自动同步到备设备上。

当vWAF-A出现故障不能正常转发流量或vWAF-A的ethernet0/0接口断开时，vWAF-B会在不影响用户通信的状态下切换为主设备，继续转发流量。

步骤七：在vWAF配置站点及策略

登录vWAF-A的WebUI管理界面，点击“站点”，进入站点页面。点击“新建站点”按钮。在弹出的<站点配置>对话框中，填入如下信息：

- 站点名称：Web-server
- 站点类型：HTTPS
- 服务：10.0.1.251（指定为虚拟高可用IP地址）端口：443
- 域名：Any
- 类型：SSL/TLS
- 密钥文件：指定SSL/TLS类型加密网站的密钥文件。
- 证书文件：指定SSL/TLS类型加密网站的证书文件。
- 安全策略：默认选择“policy_loose”安全策略模板。即仅开启最必要的防护类型，仅防御严重影响服务器功能的漏洞。

用户可按需配置IP防护策略、访问控制策略、虚拟补丁策略、自学习策略等，其他选项均采用默认值，具体可参考<vWAF-WebUI用户手册>。



注意：若HA未正常启动或启动失败，高可用虚拟IP将无法使用，可能会导致防护的站点无法正常访问。

配置结果

配置完成后，备设备上vWAF-B将同步主设备vWAF的配置信息，最终主备设备上的配置信息将保持一致。当主设备vWAF-A出现故障时，备份设备vWAF-B将自动切换为主设备，原先主设备上的虚拟高可用IP、路由、安全策略等都将自动切换，无需人工重新配置，且不影响原先的业务通信，实现了对云服务器的高可靠的安全保障。

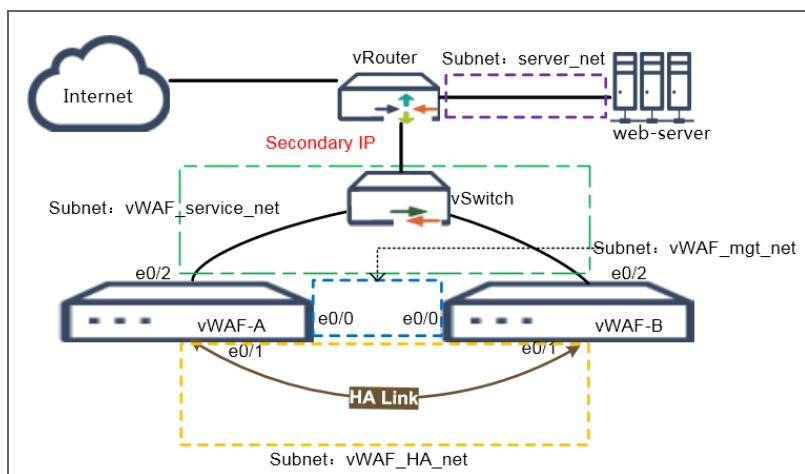
关于如何操作vWAF，请参考vWAF的用户手册 ([点击此处](#))。

在腾讯云上通过辅助IP进行vWAF的HA部署

组网设计

按照如下拓扑，在腾讯云环境中有一台云服务器Web-server（10.0.2.11），现通过部署vWAF的HA方案对云服务器进行安全防护。本案例主要介绍通过配置辅助IP的方式进行HA部署的方法。

部署完成后，vWAF-A将被选举为主设备，对云服务器进行安全防护；vWAF-B为备份设备。vWAF-A会将其配置信息以及状态数据同步到备份设备vWAF-B。当主设备vWAF-A出现故障不能正常工作时，备份设备vWAF-B会在不影响用户通信的状态下自动切换为主设备，继续对云服务器进行安全防护，从而提高了网络可靠性，保证云服务器的业务不中断。



部署步骤

步骤一：创建VPC及子网

步骤二：创建vWAF云主机

步骤三：创建弹性网卡并配置辅助IP

步骤四：创建访问密钥

步骤五：在vWAF上进行HA相关配置

步骤六：验证HA结果

[步骤七：在vWAF配置站点及策略](#)

步骤一：创建VPC及子网

登录腾讯云，点击“控制台”进入控制台界面，选择云产品 > 网络 > 私有网络创建VPC及子网，具体操作方法，请参阅"在腾讯云上部署vWAF" 在第101页中的“创建VPC”和“创建子网”章节。

原云服务器Web-server所在VPC及子网：

- VPC(VPC1): 10.0.0.0/16
- Subnet 0 (server_net) : 10.0.2.0/24
- Web-server IP: 10.0.2.11

现需要新建以下子网，且子网所属VPC需与原Web-server所在的VPC相同：

- VPC(VPC1): 10.0.0.0/16
- Subnet 1 (vWAF_mgt_net) : 10.0.10.0/24
- Subnet 3 (vWAF_HA_net) : 10.0.100.0/24
- Subnet 2 (vWAF_service_net) : 10.0.1.0/24

步骤二：创建vWAF云主机

1. 在腾讯云控制台上选择“私有网络 > 子网”，在子网“vWAF_mgt_net”上，创建2台vWAF云主机vWAF-A和vWAF-B，具体创建步骤请参考"在腾讯云上部署vWAF" 在第101页。

注意：在<3.选择存储和带宽>页面中，不要勾选“分配免费公网IP界面”。

2. **云主机规格要求：**最少使用2个vCPU、内存最小为4GB，两个云主机的默认网卡均选择网络vWAF_mgt_net。（说明：由于两台云主机的配置一样，可直接购买2台，然后重命名为vWAF-A和vWAF-B。vWAF-A将作为HA场景中的主设备，vWAF-B将作为备设备。）

步骤三：创建弹性网卡并配置辅助IP

- 在腾讯云控制台上，选择“私有网络 > IP与网卡 > 弹性网卡”，点击“新建”按钮。
- 在<新建弹性网卡>对话框中，配置如下信息：

新建弹性网卡

名称

vWAF-A-HA

所在地域

广州

所属网络

vpc-a1p3dhij (VPC1 | 10.0.0.0/16)

所属子网

subnet-m9t3i72vWAF-HA-net | 0.0.100.0/24

可用区

广州四区

可分配IP数

1/30个 (当前子网可用IP剩余251个)

分配IP

主 IP

自动分配

系统将自动分配IP地址

增加一个辅助IP

确定

取消

- vWAF-A-HA弹性网卡的配置信息如下：

选项	配置信息
名称	指定弹性网卡的名称为"vWAF-A-HA"。
所属网络	选择步骤一中配置私有网络的“VPC1”
所属子网	选择步骤一中配置的子网“vWAF_HA_nct”。

- 配置完成后，在弹性网卡列表界面，选中“vWAF-A-HA”条目的操作列的“绑定云主机”按钮。
- 在<绑定云主机>对话框中，选择云主机“vWAF-A”。
- 按照同样的方法，新建弹性网卡vWAF_A_service并配置辅助IP，配置信息如下：

选项	配置信息
名称	指定弹性网卡的名称为“vWAF_A_service”。
所属网络	选择步骤一中配置私有网络的“VPC1”
所属子网	选择步骤一中配置的子网“vWAF_service_net”。
分配IP	主IP：手动填写：10.0.1.211 添加一个辅助IP：手动填写：10.0.1.242

7. 在弹性网卡列表界面，选中“vWAF_A_service”条目的操作列的“绑定云主机”按钮。
8. 在<绑定云主机>对话框中，选择步骤三中创建的云主机“vWAF-A”。
9. 重复上述步骤，新建弹性网卡vWAF-B-HA和vWAF-B-service，不需配置辅助IP，然后分别绑定到云主机“vWAF-B”。

步骤四：创建访问密钥

1. 在腾讯云控制台上，选择“管理与审计>访问管理>访问密钥>API密码管理”。
2. 点击“创建密钥”进行创建，然后复制粘贴APP ID 和密钥，用于后续步骤的使用。

步骤五：在vWAF上进行HA相关配置

1. 创建完成云主机后，云主机将启动，用户可访问Web应用防火墙。默认情况下管理口HTTPS协议处于开启状态,用户可以通过这种方式，使用云主机的公网IP，登录到vWAF。具体方法可查看[使用HTTPS远程登录vWAF](#)。
2. 初次访问WAF设备时可按照“WAF安装向导”进行配置：
 - 选择部署模式：单臂模式
 - LAN接口：ethernet0/2；安全域：Untrust
 - IP地址：配置为辅助IP：10.0.1.242。
 - 掩码：24

3. 查看vWAF-A, vWAF-B获取的DNS Server地址, 本示例中查看到为183.60.83.19。然后继续配置系统时间, 完成配置向导。
4. 分别在vWAF-A和vWAF-B的接口eth0/0下配置路由优先级, 同时关闭逆向路由检查。



5. 选择“网络 > 路由 > 目的路由”, 配置静态默认路由, 下一跳地址是vWAF_service_net子网的网关地址 10.0.1.1。(此配置可只在主设备进行配置, 开启HA后会同步到备设备上。)
- 目的地: 0.0.0.0
 - 子网掩码: 0
 - 下一条: 网关

- 网关：10.0.1.1（vWAF_service_net网关IP）

6. 主设备vWAF-A上，继续配置HA的相关信息。选择“系统 > HA”，配置如下：

- HA控制连接接口：选择eth0/1
- HA链路本地MAC地址：选择“控制连接接口MAC”
- HA链路本地IP地址：10.0.100.164/255.255.255.0
- HA链路本地MTU：1600
- HA链路对端IP与MAC地址：ip 10.0.100.165 mac 000c.2928.3b60（备设备上HA连接接口的IP地址，mac地址）
- HA簇ID：1
- 业务接口使用物理MAC：启用
- 云平台：选择“腾讯云”
- 部署方式：选择“访问密钥”
- 访问密钥ID：输入上一步骤已申请的APP ID
- 访问密钥密码：输入上一步骤已申请的APP ID的密钥密码
- 在<组0>处配置。

- 优先级：50（设置HA优先级，值越小优先级越高，优先级高的为主设备。）
- 监测对象：track1

HA控制连接接口：	ethernet0/1	
HA链路本地MAC地址：	☐ 默认 ☒ 控制连接接口MAC	
HA链路本地IP地址：	10.0.100.164 / 255.255.255.0	
HA链路本地MTU：	1600 (1280 - 1600)字节	
HA链路对端IP与MAC地址：	10.0.100.165	000c.2928.3b60
HA虚前缀：		
HA簇ID：	-----	
HA Transmit UDP：	☒ 启用	
业务接口使用物理MAC：	☒ 启用	
云平台：	☒ 腾讯云 ☐ 无	
部署模式：	☐ HA VIP ☒ 访问密钥	
访问密钥ID：	DADAG23425545456664 (0 - 64)字符	
访问密钥密码：	 (0 - 32)字符	

HA 同步配置
HA同步会话

组0

新建

优先级：	50	(1 - 254)
抢占时间：	0	(0 - 600)秒,0：非抢占
Hello报文间隔：	200	(50 - 10000)毫秒
Hello报文警戒值：	15	(3 - 255)
免费ARP包个数：	15	(10 - 180)
监测对象：	track1	
描述：		(1 - 31)字符

7. 在备设备vWAF-B上，配置HA相关的信息。

- HA控制连接接口：选择eth0/1
- HA链路本地MAC地址：选择“控制连接接口MAC”
- HA链路本地IP地址：10.0.100.165/255.255.255.0
- HA链路本地MTU：1600

- HA链路对端IP与MAC地址：ip 10.0.100.164 mac 0224.f8f3.e521（备设备上HA连接接口的IP地址，mac地址）
- 业务接口使用物理MAC：启用
- 云平台：选择“腾讯云”
- 部署方式：选择“访问密钥”
- 访问密钥ID：输入上一步骤已申请的APP ID
- 访问密钥密码：输入上一步骤已申请的APP ID的密钥密码
- HA簇ID：1

- 在<组0>处配置。
- 优先级：100（设置HA优先级，值越小优先级越高，优先级高的为主设备。）

HA控制连接接口：
HA链路本地MAC地址：
HA链路本地IP地址：
HA链路本地MTU：
HA链路对端IP与MAC地址：
HA虚前缀：
HA簇ID：
HA Transmit UDP：
业务接口使用物理MAC：
云平台：
部署模式：
访问密钥ID：
访问密钥密码：

ethernet0/1

☐ 默认
☒ 控制连接接口MAC

10.0.100.165 / 255.255.255.0

1600 (1280 - 1600)字节

10.0.100.164 0224.f8f3.e521

☒ 启用

☒ 启用

☒ 腾讯云
☐ 无

☐ HA VIP
☒ 访问密钥

DADAG23425545456664 (0 - 64)字符

..... (0 - 32)字符

HA 同步配置
HA同步会话

组0

新建

优先级：

抢占时间：

Hello报文间隔：

Hello报文警戒值：

免费ARP包个数：

监测对象：

100

0

200

15

15

track1

(1 - 254)

(0 - 600)秒,0：非抢占

(50 - 10000)毫秒

(3 - 255)

(10 - 180)

步骤六：验证HA结果

配置完成后，优先级高的vWAF-A会自动协商为主设备，优先级低的vWAF-B为备设备，点击“系统 > 系统信息”，两台设备的HA状态分别如下显示：

- Device A
HA状态：Master

- Device B

HA状态: Backup

由于两台设备已经协商成功，因此之后的配置只需在主设备上配置即可，配置完后会自动同步到备设备上。

当vWAF-A出现故障不能正常转发流量或vWAF-A的ethernet0/0接口断开时，vWAF-B会在不影响用户通信的状态下切换为主设备，继续转发流量。

步骤七：在vWAF配置站点及策略

登录vWAF-A的WebUI管理界面，点击“站点”，进入站点页面。点击“新建站点”按钮。在弹出的<站点配置>对话框中，填入如下信息：

- 站点名称: Web-server
- 站点类型: HTTPS
- 服务: 10.0.1.242（指定为辅助IP地址）端口: 443
- 域名: Any
- 类型: SSL/TLS
- 密钥文件: 指定SSL/TLS类型加密网站的密钥文件。
- 证书文件: 指定SSL/TLS类型加密网站的证书文件。
- 安全策略: 默认选择“policy_loose”安全策略模板。即仅开启最必要的防护类型，仅防御严重影响服务器功能的漏洞。
- 在<负载均衡>页签下，配置Web-server的IP地址10.0.2.11。

用户可按需配置IP防护策略、访问控制策略、虚拟补丁策略、自学习策略等，其他选项均采用默认值，具体可参考<vWAF-WebUI用户手册>。



注意: 若HA未正常启动或启动失败，高可用虚拟IP将无法使用，可能会导致防护的站点无法正常访问。

配置结果

配置完成后，备设备上vWAF-B将同步主设备vWAF的配置信息，最终主备设备上的配置信息将保持一致。当主设备vWAF-A出现故障时，备份设备vWAF-B将自动切换为主设备，原先主设备上的辅助私网IP、路由、安全策略等都将自动切换，无需人工重新配置，且不影响原先的业务通信，实现了对云服务器的高可靠的安全保障。

关于如何操作vWAF，请参考vWAF的用户手册（[点击此处](#)）。

在华为云上部署vWAF

系统要求

在华为云上部署山石网科的虚拟Web应用防火墙(vWAF)，需要宿主机满足以下要求。

- 要求至少能够提供2个CPU、4 GB内存。
- 已经购买华为云。

安装步骤

步骤一：创建虚拟私有云

1. 登录华为云，点击“控制台”进入控制台界面，在<服务列表>页签下，选择“网络>虚拟私有云”，点击“虚拟私有云 VPC”。



2. 在<虚拟私有云>页面，点击页面右上角的“创建虚拟私有云”按钮。
3. 在<创建虚拟私有云>页面，配置私有云名称和网段等信息：

|

在<创建虚拟私有云>页面，配置如下参数

选项	说明
基本信息	
区域	指定VPC所在的区域。
名称	指定VPC的名称。
IPv4网段	指定VPC所在的网段。
默认子网	
可用区	指定默认子网所在的可用区。
名称	指定默认子网的名称。
子网IPv4网段	指定默认子网所在的IPv4网段。

4. 点击“立即创建”，等待几秒钟，页面跳转到虚拟私有云列表，虚拟私有云创建完成。
5. 若需额外创建子网，选择“网络控制台 > 子网”，点击“创建子网”，弹出<创建子网>对话框。

在<创建子网>对话框中进行设置。

选项	说明
虚拟私有云	指定子网所属的虚拟私有云。
可用区	指定子网的可用区。
名称	指定子网的名称。
子网IPv4网段	指定子网网段。

6. 点击确定，完成子网的创建。

步骤二：创建云服务器/部署vWAF

1. 点击页面左上角“华为云”图标返回华为云首页，在顶部导航栏点击“云市场”进入云市场页面，在页面顶部搜索框中搜索并选择“山石网科虚拟化Web应用防火墙”，点击“立即购买”进入配置云服务器页面。
2. 在<基础配置>页面，配置计费模式、区域、可用区、CPU架构、规格、镜像、系统盘等参数：

|

在<基础配置>页面，配置如下参数：

选项	说明
计费模式	可按需选择计费模式。
区域	指定弹性云服务器所在的地理区域，需与虚拟私有云所在区域一致。
可用区	指定弹性云服务器所在的可用区，需与子网所在可用区一致。
规格	vWAF虚拟Web应用防火墙要求最少使用2个vCPU、内存最小为4GB，这里推荐使用“通用计算型 s6.large.2 2vCPUs 4GiB”。
镜像	保持默认即可。
磁盘	可按需选择。这里选择100GiB用作示例。

3. 在<网络配置>页面，配置VPC、子网、安全组、弹性IP等参数：

|

在<网络配置>页面，配置如下参数：

选项	说明
网络	选择步骤一创建的虚拟私有云及子网(自动分配IP)。若需增加网卡，可在扩展网卡出添加网卡，并选择相应的子网。
安全组	可按需选择，这里选择放通SSH(TCP:22)、HTTPS(TCP:443)、Windows远程连接（TCP:3389）服务端口的自定义安全组“hill-stone-test”用作示例。
弹性公网IP	推荐选择“暂不购买”，若此处选择“立即购买”，EIP绑定到云服务器后，会出现无法解绑的情况。建议使用“步骤三：绑定弹性IP”所示的方法进行绑定。

4. 在<高级配置>页面，配置云服务器名称、登陆凭证等参数：

|

在<高级配置>页面，配置如下参数：

选项	说明
云服务器名称	指定云服务器的名称。
登录凭证	选择“密码”，并配置密码及确认密码。

5. 点击“下一步：确认配置”，进入配置详情页面，勾选“我已阅读并同意”。
6. 点击“立即购买”，页面将提示任务提交成功，华为云服务器创建完成，即vWAF部署完成。

步骤三：绑定弹性公网IP

1. 在页面左侧导航栏中点击“服务列表”，选择“网络>弹性公网IP EIP”。
2. 在<弹性公网IP>页面，点击左上角的“购买弹性公网IP”。
3. 在<购买弹性公网IP>页面配置计费模式、区域、线路、带宽大小等参数。

|

在<购买弹性公网IP>页面，配置如下参数：

选项	说明
计费模式	可按需选择计费模式。
区域	指定弹性公网IP所在的区域，需与云服务器所在区域一致。
线路	选择“全动态BGP”。
带宽大小	可按需选择带宽大小。

4. 点击“立即购买”，确定产品信息后，点击“提交”，完成购买后，页面跳转到<弹性公网IP>页面。
5. 在<弹性公网IP>页面，找到上一步购买的弹性公网IP条目，点击“操作”列的“绑定”，弹出<绑定弹性公网IP>对话框。

||

6. 在<绑定弹性公网IP>对话框，选择步骤二创建的云服务器，并指定网卡，点击“确定”完成绑定。

步骤四：访问vWAF

完成创建弹性云服务器并绑定弹性公网IP后，按照以下步骤访问vWAF：

1. 在页面左侧导航栏中点击“服务列表”，选择“计算>弹性云服务器ECS”。
2. 在弹性云服务器列表，找到步骤二创建的云服务器条目，点击“操作”列的“远程登录”。

|

3. 在<登录Linux弹性云服务器>页面任选一种方式登录CLI控制界面。

|

步骤五：通过外网访问vWAF

默认情况下管理口的SSH和HTTPS协议处于开启状态,用户可以通过这两种方式使用云服务器所绑定的弹性IP，登录到vWAF。

使用SSH2远程登录

1. 打开远程终端登录软件。以SecureCRT为例
2. 点击“File > Quick Connect”。在“Protocol”下拉菜单中选择“SSH2”。
3. 在<Hostname>中输入弹性IP地址。
4. 在<Username>中输入用户名: hillstone。
5. 点击“Connect”。
6. 输入密码: hillstone，点击“OK”即可登录。

使用HTTPS登录vWAF

1. 打开浏览器，在地址栏中输入https://弹性IP地址。
2. 在登录页面输入默认用户名/密码：hillstone/hillstone。
3. 按回车键，即可登录。

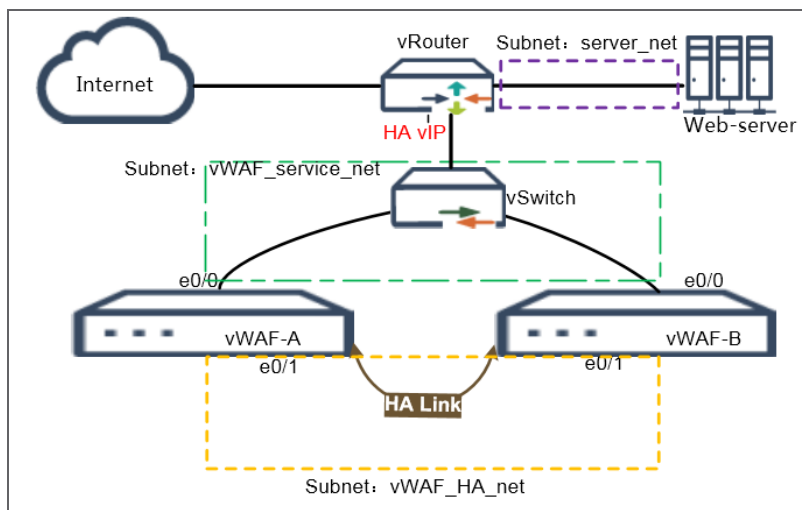
关于如何操作vWAF，参考vWAF的用户手册（[点击此处](#)）。

在华为云上进行vWAF的HA部署

组网设计

按照如下拓扑，在华为云环境中有一台云服务器Web-server（10.0.2.11），现通过部署vWAF的HA方案对云服务器进行安全防护。

部署完成后，vWAF-A将被选举为主设备，对云服务器进行安全防护；vWAF-B为备份设备。vWAF-A会将其配置信息以及状态数据同步到备份设备vWAF-B。当主设备vWAF-A出现故障不能正常工作时，备份设备vWAF-B会在不影响用户通信的状态下自动切换为主设备，继续对云服务器进行安全防护，从而提高了网络可靠性，保证云服务器的业务不中断。



部署步骤

[步骤一：创建VPC及子网](#)

[步骤二：创建vWAF云服务器](#)

[步骤三：申请虚拟IP](#)

[步骤四：在vWAF上进行HA相关配置](#)

[步骤五：验证HA结果](#)

步骤一：创建虚拟私有云VPC及子网

登录华为云，点击“控制台”进入控制台界面，选择“服务列表>网络>虚拟私有云VPC”，创建虚拟私有云VPC及子网，具体操作方法，请参阅[在华为云上部署vWAF](#)中的“步骤一：创建虚拟私有云”章节。

原云服务器Web-server所在VPC及子网：

- 虚拟私有云VPC(VPC1)：10.0.0.0/16
- Subnet 0 (server_net)：10.0.2.0/24
- Web-server IP：10.0.2.11

现在需要在原Web-server所在的虚拟私有云VPC1下继续创建如下子网。点击虚拟私有云名称VPC1，进入VPC1的详情界面，在<子网>标签下，点击“创建子网”按钮，添加如下子网网段：

- Subnet 1 (vWAF_service_net)：10.0.1.0/24
- Subnet 2 (vWAF_HA_net)：10.0.100.0/24

步骤二：创建vWAF云服务器

1. 在华为云控制台，选择“服务列表>计算>弹性云服务器”，点击进入弹性云服务器界面。创建2台vWAF云服务器vWAF-A和vWAF-B，具体创建步骤请参考[在华为云上部署vWAF](#)。
2. 配置弹性云服务器的基本信息。

选项	说明
基础配置	
计费模式	可按需选择计费方式，如“按需计费”。
区域	选择所在区域。
规格	vWAF虚拟Web应用防火墙要求最少使用2个vCPU、内存最小为4GB，这里推荐使用“通用计算型 s3.large.2 2vCPUs 4GB”。
镜像	选择“私有镜像”，然后选择已创建的镜像。

选项	说明
磁盘	至少100GB，用户可根据需要来选择磁盘大小。点击“下一步：网络配置”按钮。
网络配置	
网络	选择步骤1创建的虚拟私有云VPC-子网vWAF_service_net”；同时添加一个扩展网卡，选择“虚拟私有云VPC-子网vWAF_HA_net”。
安全组	可选择默认，即所有用户可修改安全组规则。
弹性IP	选择“暂不购买”，然后点击“下一步：高级配置”。
高级配置	
云服务器名称	指定云服务器的名称为vWAF-A或vWAF-B。
登录凭证	选择“密码”，并配置密码及确认密码，然后点击“下一步：确认配置”。
确认配置	
企业项目	可选择“Default”。
购买数量	选择需购买的数量。
协议	选择“我同意....”。

说明：由于两台云服务器的配置一样，可直接购买2台，然后重命名为vWAF-A和vWAF-B。vWAF-A将作为HA场景中的主设备，vWAF-B将作为备设备。)

步骤三：申请虚拟IP

1. 选择“服务列表 > 网络 > 虚拟私有云VPC”，点击步骤一中虚拟私有云名称VPC1，进入VPC1详情页面。
2. 然后在子网列表中，选择步骤一中配置的子网“vWAF-service-net”并点击其名称，进入子网详情界面。

3. 点击<虚拟IP>页签，点击“申请虚拟IP地址”按钮。
4. 在<申请虚拟IP地址>对话框中，可选择“手动分配”，如10.0.1.88。
5. 点击“确定”，完成申请。
6. 在虚拟IP列表中，点击刚申请的虚拟IP地址后的“绑定服务器”，选择步骤二已创建的云服务器vWAF-A，网卡将自动选择云服务器所对应当前子网的网卡。重复该步骤，再次绑定云服务器WAF-B。
7. 在虚拟IP列表中，点击刚申请的虚拟IP地址后的“绑定弹性公网IP”，选择一个弹性公网IP地址进行绑定。

步骤四：在vWAF上进行HA相关配置

1. 在华为云平台上，查看vWAF上的公网IP地址IP地址等信息并记录，然后登录vWAF-A的WebUI界面，具体方法，请参考[使用HTTPS登录vWAF](#)。
2. 输入用户名、密码（默认分别为hillstone、hillstone）登录到实例vWAF-A，选择“网络>接口”，选择ethernet0/0口，配置示例：
 - 绑定安全域：三层安全域
 - 安全域：untrust
 - 类型：静态IP
 - IP地址：配置为云平台上的高可用虚拟IP地址。
 - 网络掩码：24
 - 高级选项>管理IP:配置为vWAF-A中Subnet 1（vWAF_service_net）子网的IP地址。

- 管理方式：开启SSH/PING/HTTPS

Ethernet 接口

基本配置

接口名称: ethernet0/0

描述: (0 - 63)字符

绑定安全域: ☐ 二层安全域 ☒ 三层安全域 ☐ TAP ☐ 无绑定

安全域: untrust

HA同步: ☐ 启用

IP配置

类型: ☒ 静态IP ☐ 自动获取

IP地址: 10.0.1.88

子网掩码: 255.255.255.0

☐ 配置为Local IP

高级选项

管理方式

☐ Telnet ☒ SSH ☒ Ping ☐ HTTP ☒ HTTPS ☐ SNMP

路由

逆向路由: ☐ 启用 ☒ 关闭 ☐ 自动

确定 取消

3. 选择"网络 > 路由 > 目的路由", 配置静态默认路由, 下一跳地址是vWAF_service_net子网的网关地址。

目的路由配置

目的地: 0.0.0.0

子网掩码: 0

下一跳: ☒ 网关 ☐ 接口

网关: 10.0.1.1

时间表: -----

优先权: 1 (1 - 255), 缺省值: 1

路由权值: 1 (1 - 255), 缺省值: 1

描述: (1 - 63)字符

确定 取消

4. 登录vWAF-B, 选择“网络 > 接口”, 选择ethernet0/0口, 配置示例如:

- 绑定安全域: 三层安全域
- 安全域: untrust

- 类型：静态IP，即关闭DHCP自动获取

The screenshot shows the 'Ethernet 接口' configuration window with the following settings:

- 基本配置**
 - 接口名称: ethernet0/0
 - 描述: (0 - 63)字符
 - 绑定安全域: ☐ 二层安全域 ☒ 三层安全域 ☐ TAP ☐ 无绑定
 - 安全域: untrust
 - HA同步: ☐ 启用
- IP配置**
 - 类型: ☒ 静态IP ☐ 自动获取
 - IP地址:
 - 子网掩码:
 - ☐ 配置为Local IP
 - 高级选项
- 管理方式**
 - ☐ Telnet ☒ SSH ☒ Ping ☐ HTTP ☒ HTTPS ☐ SNMP
- 路由**
 - 逆向路由: ☐ 启用 ☒ 关闭 ☐ 自动

5. 主设备vWAF-A上，配置HA的监测对象。选择“对象 > 监测对象”，并点击“新建”，配置示例：

- 名称：track1
- 警戒值：255
- 监测类型：选择<接口>单选按钮，并点击“添加”按钮。在弹出的<添加监测对象>对话框，指

定接口为“ethernet0/0”，权值为“255”

监测对象配置

监测对象

名称：

track

(1 - 31)字符

警戒值：

255

(1 - 255)，缺省值：255

监测类型：

接口

HTTP/Ping/ARP/DNS/TCP

链路质量探测

HA同步：

启用

添加监测成员

+ 添加

- 删除

☐ 类型	接口	权值
☐ 接口	ethernet0/0	255

确定

取消

6. 主设备vWAF-A上，继续配置HA的相关信息。选择“系统 > HA”，配置如下：
- HA控制连接接口：选择eth0/1
 - HA链路本地MAC地址：选择“控制连接接口MAC”
 - HA链路本地IP地址：10.0.100.4/255.255.255.0
 - HA链路本地MTU：1600
 - HA链路对端IP与MAC地址：ip 10.0.100.5 mac 0224.f8f3.c5e2（备设备上HA连接接口的IP地址，mac地址）
 - HA簇ID：1
 - 业务接口使用物理MAC：启用
 - 在<组0>处配置。
 - 优先级：50（设置HA优先级，值越小优先级越高，优先级高的为主设备。）

- 监测对象：track1

The screenshot shows a configuration window for HA (High Availability) settings. The top section contains fields for:

- HA控制连接接口: ethernet0/1
- HA链路本地MAC地址: Radio buttons for 默认, 控制连接接口MAC (selected), and 自定义.
- HA链路本地IP地址: 10.0.100.4 / 255.255.255.0
- HA链路本地MTU: 1600 (1280 - 1600)字节
- HA链路对端IP与MAC地址: 10.0.100.5 / 0224.f8f3.e5e2
- HA虚前缀: (empty)
- HA簇ID: 1 (dropdown), 节点ID: 0 (dropdown) with an info icon.
- Peer-mode: ☐ 启用
- HA Transmit UDP: ☐ 启用 ①
- 业务接口使用物理MAC: ☒ 启用

 Below these are two buttons: HA 同步配置 and HA 同步会话.

 The bottom section is titled '组0' and contains a '新建' button followed by several configuration fields:

- 优先级: 50 (1 - 254)
- 抢占时间: 1 (0 - 600)秒, 0: 非抢占
- Hello报文间隔: 200 (50 - 10000)毫秒
- Hello报文警戒值: 15 (3 - 255)
- 免费ARP包个数: 15 (10 - 180)
- 监测对象: track1 (dropdown)
- 描述: (empty) (1 - 31)字符

7. 在备设备vWAF-B上，配置HA相关的信息，配置示例如：

- HA控制连接接口：选择eth0/1
- HA链路本地MAC地址：选择“控制连接接口MAC”
- HA链路本地IP地址：10.0.100.5/255.255.255.0
- HA链路本地MTU：1600
- HA链路对端IP与MAC地址：ip 10.0.100.4 mac 0224.f8f3.e521（备设备上HA连接接口的IP地址，mac地址）
- HA簇ID：1
-

- 业务接口使用物理MAC：启用
- 在<组0>处配置。
- 优先级：100（设置HA优先级，值越小优先级越高，优先级高的为主设备。）

HA控制连接接口：

ethernet0/1

HA链路本地MAC地址：

默认

控制连接接口MAC

自定义

HA链路本地IP地址：

10.0.100.5

/

255.255.255.0

HA链路本地MTU：

1600

(1280 - 1600)字节

HA链路对端IP与MAC地址：

10.0.100.4

0224.f8f3.eef21

HA虚前缀：

HA组ID：

1

节点ID：

1

Peer-mode：

☐

启用

HA Transmit UDP：

☐

启用

业务接口使用物理MAC：

☒

启用

HA同步配置

HA同步会话

组0

新建

优先级：

100

(1 - 254)

抢占时间：

1

(0 - 600)秒,0：非抢占

Hello报文间隔：

200

(50 - 10000)毫秒

Hello报文警戒值：

15

(3 - 255)

免费ARP包个数：

15

(10 - 180)

监测对象：

描述：

(1 - 31)字符

步骤五：验证HA结果

配置完成后，优先级高的vWAF-A会自动协商为主设备，优先级低的vWAF-B为备设备，，点击“系统 > 系统信息”，两台设备的HA状态分别如下显示：

- Device A
HA状态：Master
- Device B
HA状态：Backup

由于两台设备已经协商成功，因此之后的配置只需在主设备上配置即可，配置完后会自动同步到备设备上。

当vWAF-A出现故障不能正常转发流量或vWAF-A的ethernet0/0接口断开时，vWAF-B会在不影响用户通信的状态下切换为主设备，继续转发流量。

步骤六：在vWAF配置站点及策略

登录vWAF-A的WebUI管理界面，点击“站点”，进入站点页面。点击“新建站点”按钮。在弹出的<站点配置>对话框中，填入如下信息：

- 站点名称：Web-server
- 站点类型：HTTPS
- 服务：10.0.1.88（指定为虚拟高可用IP地址）端口：443
- 域名：Any
- 类型：SSL/TLS
- 密钥文件：指定SSL/TLS类型加密网站的密钥文件。
- 证书文件：指定SSL/TLS类型加密网站的证书文件。
- 安全策略：默认选择“policy_loose”安全策略模板。即仅开启最必要的防护类型，仅防御严重影响服务器功能的漏洞。

用户可按需配置IP防护策略、访问控制策略、虚拟补丁策略、自学习策略等，其他选项均采用默认值，具体可参考<vWAF-WebUI用户手册>。

配置结果

当主设备vWAF-A出现故障时，备份设备vWAF-B将自动切换为主设备，原先主设备上的IP、路由、策略等信息都将自动切换，无需人工重新配置，且不影响原先的业务通信，实现了对云服务器的高可靠的安全保障。

关于如何使用vWAF系统，参考Web应用防火墙的使用手册（[点击此处](#)）。

2. 配置虚拟交换机名称后，点击下一步，继续添加主机网卡。

增加虚拟交换机

1 基本信息

2 添加主机网卡

3 确认主机网卡

▼

☒

cvknode

☒

eth1

上一步

下一步

配置详情

虚拟交换机名称vSW-1

虚拟交换机描述

转发模式VEB

VLAN ID

3. 选定主机网卡后，点击下一步，确认主机网卡，不需配置其他信息，确认网卡即可。

增加虚拟交换机

1 基本信息

2 添加主机网卡

3 确认主机网卡

主机和网卡

主机名称	网卡名称	IP地址	子网掩码	网关
cvknode	eth1			

注：一个主机只能配置一个网关。如果配置多个，将有可能导致不可预知的问题。

上一步

确定

配置详情

虚拟交换机名称vSW-1

虚拟交换机描述

转发模式VEB

VLAN ID

4. 点击“确定”按钮，完成配置。

步骤二：创建vWAF虚拟机

1. 点击左侧导航栏云资源>node>cluster>cvknode，页面跳转到“主机：cvknode”页面，点击左上角“增加虚拟机”按钮，弹出<增加虚拟机>对话框。在<基本信息>页签下，配置虚拟机名称及显示名称，

操作系统选择“Linux”,版本选择“Other 2.6.x Linux（64-bit）”,然后点击“下一步”按钮，示例如下：

增加虚拟机

1 基本信息

2 硬件信息

虚拟机名称*

test1

显示名称*

test1

描述

操作系统

Windows

Linux

版本

Other 2.6.x Linux(64-bit)

自动迁移

否

CAStools自动升级

是

下一步

配置详情

操作系统

Other 2.6.x Linux(64-bi...

虚拟机名称

test1

显示名称

test1

描述

自动迁移

否

CAStools自动升级

是

2. 在<硬件信息>页签下，配置CPU为2个，内存为4GB，网络选择步骤一配置的虚拟交换机网络，点击磁盘的查询按钮，上传vWAF镜像文件。

增加虚拟机

1 基本信息

2 硬件信息

CPU*

2

内存*

4

GB

网络*

VSW-

磁盘*

软驱

自动加载高速驱动

光驱

增加硬件

上一步

确定

配置详情

操作系统

Other 2.6.x Linux(64-bi...

虚拟机名称

test1

显示名称

test1

描述

自动迁移

否

CAStools自动升级

是

CPU个数

2

CPU工作模式

兼容模式

体系结构

x86_64

CPU调度优先级

中

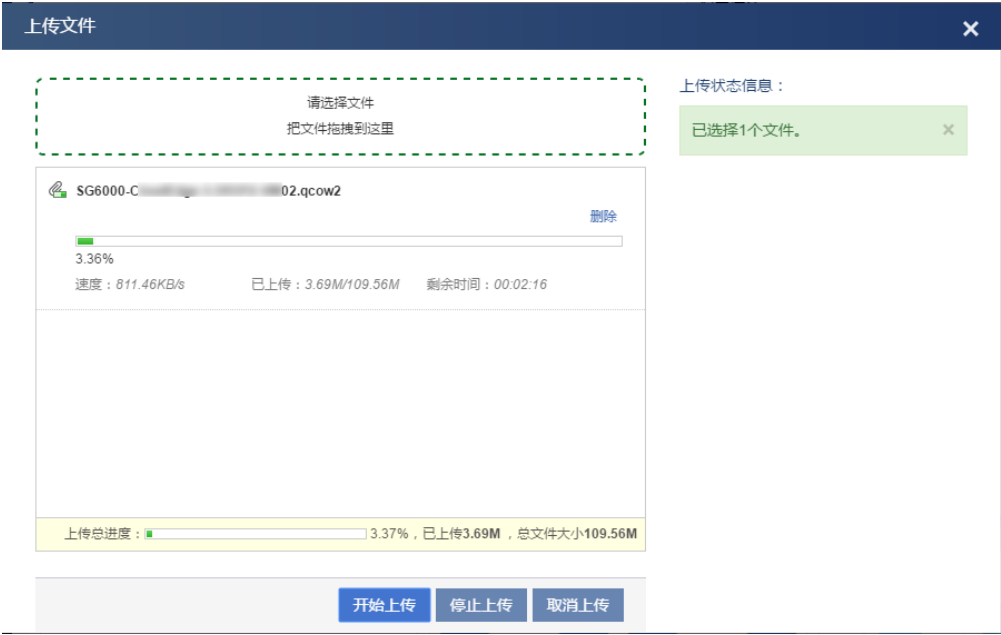
I/O优先级

中

内存

4GB

3. 在<选择存储>界面，选择默认的“defaultpool”，点击“上传文件”按钮，上传vWAF的镜像文件，示例如下：



4. 选择上一步上传的镜像文件后，在增加虚拟机的<硬件信息>页签下，点击“确定”按钮，完成配置。

步骤三：登录vWAF进行相关配置

创建完成vWAF虚拟机后，虚拟机默认处于关机状态，点击“启动”按钮，待虚拟机变为绿色运行状态后，点击“控制台”按钮，将弹出vWAF的CLI控制台界面。由于H3C CAS不提供DHCP服务器功能，故用户需要在vWAF上进行如下相关配置，配置完成后，用户将可以通过SSH和HTTPS的方式访问设备。具体配置如下：

1. 进入控制台后，输入用户名/密码（默认为：hillstone/hillstone），登录vWAF。
2. 进入ethernet0/0接口，关闭接口的DHCP自动获取IP功能，配置接口IP地址，并开启SSH和HTTPS管理功能。

```
SG-6000# interface ethernet0/0
SG-6000(ext-if)# no ip address dhcp
SG-6000(ext-if)# ip address 10.90.3.220/24
```

```
SG-6000(ext-if)# manage ssh  
  
SG-6000(ext-if)# manage https  
  
SG-6000(ext-if)# exit
```

3. 配置静态路由。

```
SG-6000# ip vrouter trust-vr  
  
SG-6000(ext-vrouter)# ip route 0.0.0.0/0 10.90.3.254  
  
SG-6000(ext-vrouter)# exit
```

4. 完成上述配置后，用户即可通过SSH和HTTPS方式访问vWAF。

访问vWAF

管理口的SSH和HTTPS协议已配置为开启状态,用户可以通过这两种方式，使用**步骤三**配置的IP地址，访问vWAF。

使用SSH2远程登录

1. 打开远程终端登录软件。以SecureCRT为例
2. 点击“File > Quick Connect”。在“Protocol”下拉菜单中选择“SSH2”。
3. 在<Hostname>中输入IP地址：10.90.3.220。
4. 在<Username>中输入用户名（默认为：hillstone）。
5. 点击“Connect”。
6. 输入密码（默认为：hillstone），点击“OK”即可登录。

使用HTTPS远程登录

1. 打开浏览器，在地址栏中输入https://10.90.3.220。
2. 在登录页面输入用户名和密码（默认为：hillstone/hillstone）。
3. 按回车键，即可登录。

关于如何操作vWAF，参考vWAF的用户手册（[点击此处](#)）。