



阿里云 vWAF 部署方案

Hillstone Networks Inc.

2019 年 06 月 01 日

内容提交人	审核人	更新内容	日期
李根			
夏咸艳		Vwaf 引流	20191212

目录

1	需求分析	3
2	解决方案一	3
2.1	软硬件信息	3
2.2	开通 OSS（对象存储）	3
2.2.1	新建 Bucket	3
2.3	上传 vWAF 镜像	4
2.4	自定义镜像	5
2.5	创建云主机	8
3	引流原理	11
3.1	专有网络	11
3.2	交换机	11
3.3	路由表	12
4	部署模式	12
4.1	单臂模式	13
4.1.1	服务器配置	13
4.1.2	VWAF 配置	14
4.1.3	创建站点	14
4.1.4	访问日志	16
5	注意事项	16
5.1	OSS(对象存储)需要收取存储费用	16
5.2	自定义镜像需要收取快照费用	17
5.3	虚拟 WAF 规格型号	17

1 需求分析

在阿里云平台部署 vWAF 实现针对客户网站进行安全防护。

2 解决方案一

2.1 软硬件信息

软件版本	SG6000-VW-5.5R6-2.3.qcow2
硬件平台	vWAF

2.2 开通 OSS (对象存储)

2.2.1 新建 Bucket

Bucket 名称可以随意填写，存储类型选择标准存储，读写权限设置为私有。

新建 Bucket

[? 创建存储空间](#)
✕

! 注意: Bucket 创建成功后, 您所选择的**存储类型**、**区域**不支持变更。

Bucket 名称 9/63 ✔

区域 ▼

相同区域内的产品内网可以互通; 订购后不支持更换区域, 请谨慎选择

您在该区域下没有可用的 **存储包**、**流量包**。建议您购买资源包享受更多优惠, 点击 [购买](#)。

Endpoint

存储类型 标准存储 低频访问 归档存储

标准: 高可靠、高可用、高性能, 数据会经常被访问到。
[如何选择适合您的存储类型?](#)

读写权限 私有 公共读 公共读写

私有: 对文件的所有访问操作需要进行身份验证。

同城区域冗余存储 启用 关闭

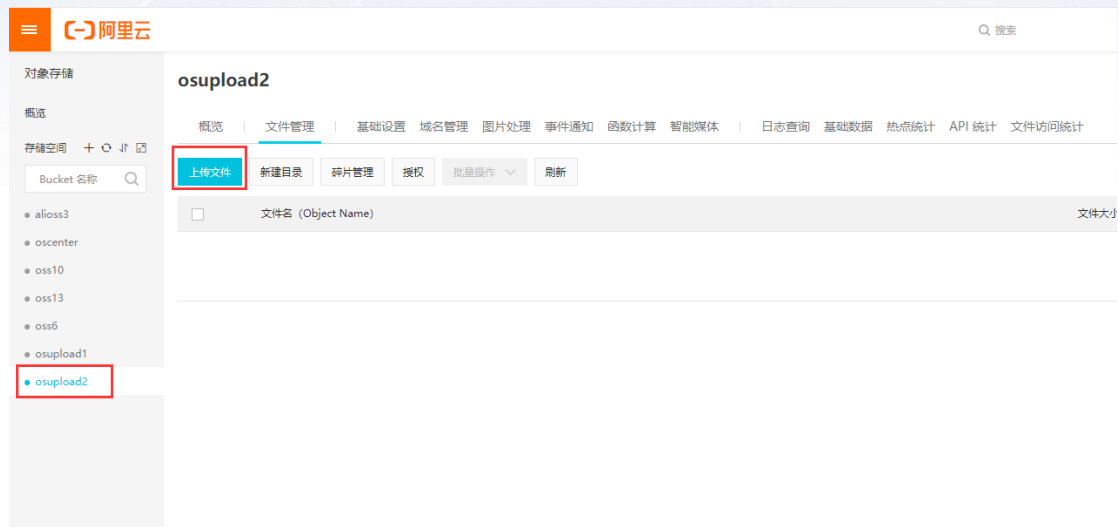
OSS 将用户的数据以冗余的方式存储在单一区域 (Region) 的 3 个可用区 (Zone) 中。提供机房级容灾能力。更多请查看 [详情](#)。

实时日志查询 开通 不开通

OSS 与日志服务深度结合, 免费提供最近7天内的 OSS 实时日志查询。开通该功能后, 用户可对 Bucket 的访问记录进行实时查询分析, [了解详情](#)

2.3 上传 vWAF 镜像

选中刚刚新建的 upload2 对象存储, 点击上传文件, 选中我们的虚拟 WAF 镜像, 格式为 qcow2。



上传完成后查看文件详情，复制里面的 URL，后面自定义镜像的时候会用到。



2.4 自定义镜像

云服务器 ECS》镜像》自定义镜像》导入镜像

阿里云 华东2 (上海) 搜索

云服务器 ECS

概览

标签 **NEW**

实例与镜像

实例

弹性容器实例 ECI

专有宿主机

超级计算集群

预留实例券

镜像

部署与弹性

存储与快照

镜像列表

自定义镜像 公共镜像 共享镜像 镜像市场

注意:目前镜像功能处于免费试用期。您已经创建了2个自定义镜像,还能创建398个自定义镜像。镜像的存在依赖于快照,当前阿里云快

镜像名称 输入镜像名称精确查询 搜索 标签

镜像ID/名称	标签	镜像类型	平台
---------	----	------	----

使用快照创建自定义镜像

刷新 导入镜像

创建时间 状态 进度 操作

导入镜像 ? 如何导入镜像
✕

创建镜像的同时系统默认会创建相关快照，当前阿里云快照已经商业化，保有镜像会产生一定的快照费用。

导入/导出镜像步骤(通过Packer自动化构建镜像):

1. 首先需要您**开通OSS**
2. 将制作好的镜像文件上传到与导入镜像相同地域的bucket下。
3. 请确认已经授权ECS官方服务账号可以访问您的OSS的权限**确认地址**
4. 在导入/导出镜像之前，请务必满足**自定义镜像要求**

* 镜像所在地域: 华东2 (上海)

* OSS Object地址: [如何获取OSS文件的访问地址](#)

* 镜像名称:

* 操作系统:

* 系统盘大小(GiB):
系统盘大小取值为5-500GB

* 系统架构:

* 系统平台:

镜像格式:

镜像描述:

添加数据盘镜像

在 OSS Object 地址中粘贴从 OSS 中获取的镜像 URL，系统盘大小最小 100GB，系统平台选择 Other Linux，镜像格式为 QCOW2。

镜像列表
使用快照创建自定义镜像
✕
导入镜像

自定义镜像 公共镜像 共享镜像 镜像市场

注: 目前镜像功能处于免费试用期，您已经创建了2个自定义镜像，近期创建398个自定义镜像。镜像的存在依赖于快照，当前阿里云快照已经商业化，保有自定义镜像会产生一定的快照费用。

镜像名称

镜像ID/名称	标签	镜像类型	平台	系统位数	创建时间	状态	进度	操作
m-ef530hoad5uyanoa7u3 SG6000-VW-5.5R6-2.3.qc...		自定义镜像	Others Linux	64位	2019年6月16日 16:33	等待	0%	删除镜像 镜像描述 相关实例 共享镜像

共有1条, 每页显示: 20 条

2.5 创建云主机

vWAF02 最低需要 2 核 4G 内存, vWAF04 最低需要 4 核 8G 内存, 硬盘最小 100G。

The screenshot shows the Alibaba Cloud ECS console. The instance configuration is as follows:

规格族	实例规格	vCPU	内存	处理器型号	处理器主频	内网带宽	内网收发包	GPU
计算型 c5	ecs.c5.large	2 vCPU	4 GiB	Intel Xeon(Skylake) Platinum 8163	2.5 GHz	1 Gbps	30 万 PPS	-
计算网络增强型 sn1ne	ecs.sn1ne.large	2 vCPU	4 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	1 Gbps	30 万 PPS	-
计算型(原焕享) sn1	ecs.sn1.medium	2 vCPU	4 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	0.5 Gbps	10 万 PPS	-
突发性能实例 t5	ecs.t5-c1m2.large	2 vCPU	4 GiB	Intel Xeon CPU	2.5 GHz	0.5 Gbps	10 万 PPS	-
突发性能实例 t5	ecs.t5-1c1m2.large	2 vCPU	4 GiB	Intel Xeon CPU	2.5 GHz	0.4 Gbps	10 万 PPS	-
共享计算型 n4	ecs.n4.large	2 vCPU	4 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	0.5 Gbps	10 万 PPS	-
共享计算型 n1	ecs.n1.medium	2 vCPU	4 GiB	Intel Xeon E5-2680v3	2.5 GHz	-	-	-
高主频计算型 hfc5	ecs.hfc5.large	2 vCPU	4 GiB	Intel Xeon Gold 6149	3.1 GHz	1 Gbps	30 万 PPS	-

当前选择实例: ecs.c5.large (2 vCPU 4 GiB, 计算型 c5)

购买实例数量: 1 台 已开通 0 vCPU, 还可开通 100 vCPU。当前所选实例规格为 2 vCPU, 最多还可开通 50 台 ECS

镜像: 公共镜像 自定义镜像 共享镜像 镜像市场

SG6000-VW-5.5R6-2.3.qcow2

配置费用: ¥ 0.669 /时

网络需要选择和客户业务相同的 VPC, 同时设置 vWAF 的带宽, 这里也可以不勾选分配公网 IPv4 地址, 后期申请弹性公网 IP 直接绑定在 vWAF 上。

The screenshot shows the '网络' (Network) configuration step in the Alibaba Cloud ECS console. The configuration is as follows:

- 网络: 教我选择网络
- 专有网络: 业务网络
- 服务器网段: 服务器网段2
- 可用私有IP数量: 252 个

如需创建新的专有网络, 您可前往控制台创建>

所选专有网络: 业务网络 / vpc-uf6iddebrlmods0fgv3dc

交换机所在可用区: 华东 2 可用区 F



安全组需要开放 22、443、80 端口。



登录凭证选择创建后设置，默认 hillstone/hillstone。



云服务器 ECS 一键购买 自定义购买

基础配置 (必填) 网络和和安全组 (必填) 系统配置 分组设置 5 确认订单 (必填)

所选配置

基础配置

计费方式: 按量付费
购买数量: 1 台
地域: 华东 2 可用区 F
镜像: SG6000-VW-3.5R6-2.3.qcow2
实例: 计算型 c5 / ecs.c5.large(2vCPU 4GB)
系统盘: 高效云盘 100GB

网络和安全组

网络: 专有网络
公网带宽: 按使用流量计费 5Mbps
VPC: 业务网络/vpc-uf6d6brimods0lgy3dc
安全组: 默认安全组 (自定义端口)
交换机: 服务器网络2/vsw-uf63ky5bm0bx4mwo5f7m/192.168.1.0/24

系统配置

登录凭证: 创建后设置, 若需[远程登录ECS](#)可返回第二步系统配置里配置登录凭证
实例名称: launch-advisor-20190616

[保存为自定义模板](#) [生成Open API最佳实践脚本](#)

使用期限

设置自动释放服务时间
ECS实例将在您指定的时间进行释放, 实例释放后数据及IP地址不会被保留且无法找回, 请谨慎操作。

服务协议

[《云服务器 ECS 服务协议》](#)
购买须知
订单创建的发展信息, 请在 管理中心->设置管理 中设置。
云产品默认使用 TCP 25 端口和基于此端口的邮箱服务, 特殊需求需提前报备审批后使用, [查看详情](#)

公网带宽: 5Mbps 按使用流量计费 配置费用: **¥ 0.669 /时** + 公网流量费用: **¥ 0.800 /GB**

[上一步: 分组设置](#) [创建实例](#)

实例列表

ECS控制台操作指南 [刷新](#) [创建实例](#) [批量操作](#)

选择实例属性进行搜索, 或者输入关键字识别搜索

搜索项: 实例ID: i-uf6463d7ovhshwm51lu5 X 清除

实例ID/名称	标签	监控	可用区	IP地址	状态	网络类型	配置	付费方式	操作
i-uf6463d7ovhshwm51lu5 launch-advisor-2...			华东 2 可用区 F	47.103.103.219(公网) 192.168.1.110(私有)	运行中	专有网络	2vCPU 4 GB (I/O优化) ecs.c5.large 5Mbps (峰值)	按量	2019年6月16日 19:09 创建 管理 远程连接 更改实例规格 更多

启动 停止 重启 重置实例密码 续费 按量付费转包月 释放设置 更多

共有1条, 每页显示: 20 条

Hillstone W02 首页 终端 策略 报表&日志 网络 系统 扫描

威胁概览 系统概览 最新时间: 5分钟

攻击严重程度 今天

没有要显示的数据

TOP10 站点受攻击分布 今天

没有要显示的数据

攻击源

TOP5 攻击源

TOP10 攻击源IP

IP	受攻击站点	攻击级别
		严重 高 中 低

威胁事件类型 今天

HTTP响应异常
DOS攻击
注入攻击
跨站攻击
恶意程序
Cookie异常
探测访问
特殊异常攻击
搜索引擎访问
异常软件
用户自定义规则

攻击次数

攻击源 发现

站点篡改告警 最近一天

3 引流原理

私有网络有三个核心组成成分：专有网络、交换机、路由表。针对数据进行引流首要的是要了解这三者之间的关联。

3.1 专有网络

用户在创建专有网络时，需要用 CIDR（无类别域间路由）作为私有网络指定 IP 地址组。阿里云专有网络 CIDR 支持使用如下私有网段中的任意一个：

10.0.0.0 - 10.255.255.255（掩码范围需在 8 - 24 之间）

172.16.0.0 - 172.31.255.255（掩码范围需在 8- 24 之间）

192.168.0.0 - 192.168.255.255（掩码范围需在 8- 24 之间）

● IPv4网段 ?

推荐网段

高级配置网段

请输入网段

192.168.0.0/16

① 一旦创建成功，网段不能修改。支持使用 192.168.0.0/16、172.16.0.0/12、10.0.0.0/8 及其子网作为专有网络地址段，网段掩码有效范围 8-24。填写示例：192.168.0.0/16。如需使用公网地址段作为专有网络地址段，请申请公网私有白名单。[点击申请](#)

描述 ?

实例ID/名称	IPv4网段	状态	默认专有网络	路由表	交换机
vpc-uf6e92lxv87p5p1gqxa9e Sec_Network	192.168.0.0/16	● 可用 ● 未绑定云企业网	否	1	2

3.2 交换机

一个交换机由至少一个子网组成，子网的 CIDR 必须在专有网络的 CIDR 内。

交换机用于管理弹性云服务器网络平面的一个网络，可以提供 IP 地址管理、DNS 等服务。专有网络中的所有云资源（如云服务器、云数据库等）都必须部署在交换机内。

实例ID/名称	所属专有网络	状态	IPv4网段	可用IP数	默认交换机	可用区	路由表	路由表类型
vsw-uf6jx3vsfmsq8qolh21xe test	vpc-uf6e92lxv87p5p1gqxa9e Sec_Network	● 可用	192.168.10.0/24	251	否	上海 可用区 G	vtb-uf6o7emc714z02l5bt1kk	系统
vsw-uf63cgcb1nd8ovjmjhrz2 Test	vpc-uf6e92lxv87p5p1gqxa9e Sec_Network	● 可用	192.168.20.0/24	250	否	上海 可用区 G	vtb-uf6o7emc714z02l5bt1kk	系统

3.3 路由表

路由表由多条路由策略组成，用于控制专有网络内交换机的出流量走向。每个交换机仅且只能关联一个路由表，一个路由表可以关联多个交换机。

实例ID/名称	所属专有网络	路由器ID	路由表类型	已绑定交换机
vtb-uf6o7emc714z02l5bt1kk	vpc-uf6e92lxv87p5p1gqxa9e Sec_Network	vrt-uf6jyv70o6m8ilirev38z	系统	vsw-uf6jx3vsfmsq8qolh21xe; vsw-uf63cgcb1nd8ovjmjhrz2;

路由表

路由表基本信息

路由表ID: vtb-uf6o7emc714z02l5bt1kk 专有网络ID: vpc-uf6e92lxv87p5p1gqxa9e

名称: [编辑](#) 路由表类型: 系统

创建时间: 2019年10月25日 16:33:15 描述: [编辑](#)

路由条目列表 已绑定交换机

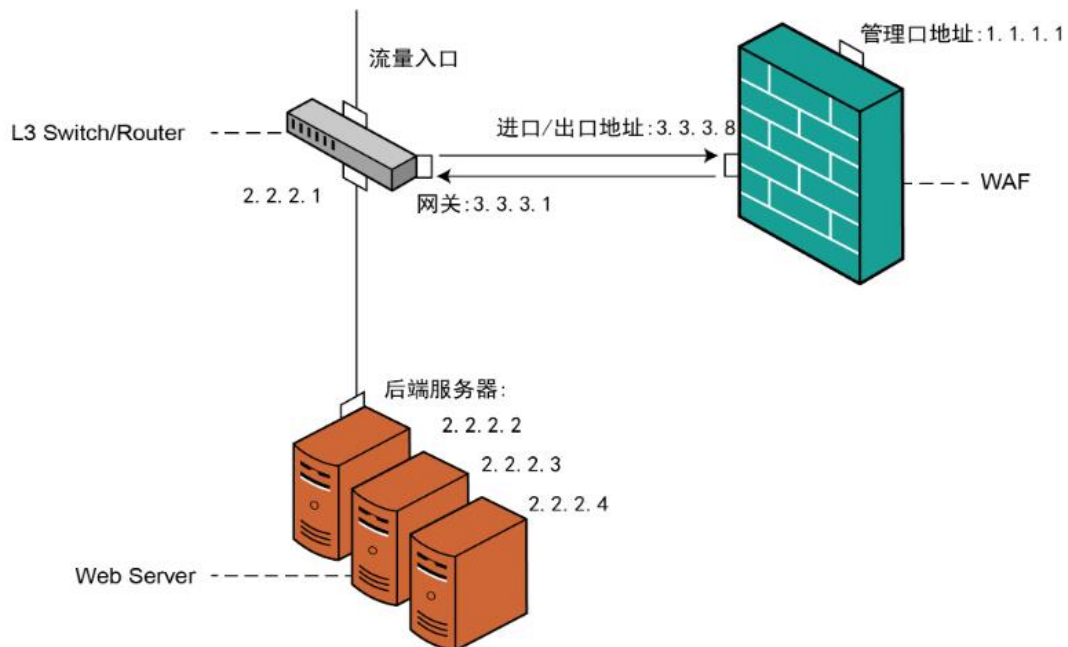
目标网段	状态	下一跳	类型	描述
192.168.10.0/24	● 可用	-	系统	
192.168.20.0/24	● 可用	-	系统	
100.64.0.0/10	● 可用	-	系统	

4 部署模式

VWAF 安装完成后，主要是为了保护云平台上的 WEB 服务器，下面针对不同的部署模式进

行验证，及阿里云上的配置介绍，可结合自身的需求进行选择。

4.1 单臂模式



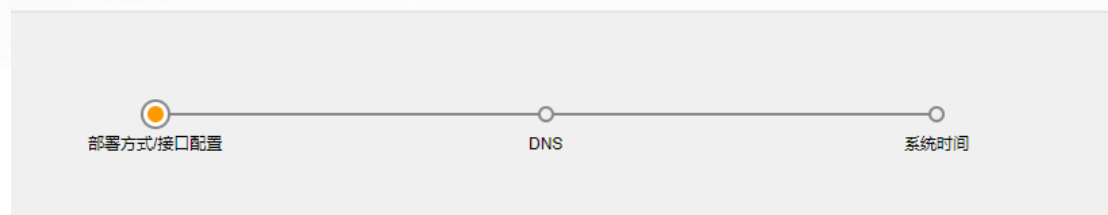
4.1.1 服务器配置

创建一个服务器，内网网段是 192.168.30.0/24，web 服务器的地址是 192.168.30.121，waf 的地址 192.168.30.120。

实例列表

实例ID/名称	标签	监控	可用区	IP地址	状态	网络类型
i-uf6anl9ux8zpk1n7jm5p launch-advisor-2...			华东 2 可用区 D	47.100.54.197(公) 192.168.30.121(私有)	运行中	专有网络
i-uf68t468lakh7or45800 launch-advisor-2...			华东 2 可用区 D	192.168.30.120(私有)	运行中	专有网络

4.1.2 VWAF 配置



部署方式/接口配置 DNS 系统时间

选择部署模式: 图例

接口配置:

接口: 安全域: IP地址: 掩码:

① 设备默认管理接口为ethernet0/0，建议在WAF安装向导的接口配置中避免使用ethernet0/0，不当配置可能造成设备无法管理。

当前部署模式: **单臂模式**

重置部署模式

站点缓存过期时间:	<input type="text" value="5"/>	(1 - 1440)分钟	确定
防篡改爬虫容量限制:	<input type="text" value="100"/>	(10 - 2000) MB	确定
防篡改爬虫扫描周期:	<input type="text" value="15"/>	(2 - 60)分钟	确定
请求体内容扫描长度:	<input type="text" value="2048"/>	(1 - 1073741824)字节	确定
响应体内容扫描长度:	<input type="text" value="10240"/>	(1 - 1073741824)字节	确定
客户端连接超时时间:	<input type="text" value="65"/>	(0 - 3600)秒	确定
服务器响应超时时间:	<input type="text" value="300"/>	(10 - 1800)秒	确定
使用X-Header作为客户端IP:	<input type="radio"/> OFF <input type="radio"/> X-Forwarded-For		确定
	<input type="radio"/> 取左 <input checked="" type="radio"/> 取右		
编码探测:	请求行探测: <input type="checkbox"/> 请求体探测: <input type="checkbox"/>		确定
	响应体探测: <input type="checkbox"/>		

4.1.3 创建站点

服务 ip 应当填写 waf 的接口 ip。

站点防护配置

基本配置 负载均衡 站点加速 站点防篡改 健康状态检测 自定义错误提示页面

站点名称: 192.168.30.121

站点类型: HTTP HTTPS

服务:

IP/IP范围	端口/端口范围	
192.168.30.120	80	-
		+

域名: Any

域 (1-256)字节

访问控制策略:

名称	操作	
		+

虚拟补丁策略: -----

安全策略: low_security_level

自学习策略: -----

X-Forwarded-For:

请求体内容检测:

响应体内容检测:

确定 取消

负载均衡器中填写 web 服务器的真实 ip;

站点防护配置

基本配置 负载均衡 站点加速 站点防篡改 健康状态检测 自定义错误提示页面

负载均衡算法: 加权轮询 最少连接 IP Hash

负载均衡服务器:

<input checked="" type="checkbox"/>	IP/域名	端口	权重
<input checked="" type="checkbox"/>	192.168.30.121	80	1

+ -

确定 取消

4.1.4 访问日志



5 注意事项

5.1 OSS(对象存储)需要收取存储费用

OSS 计费区分按量付费和包年包月两种，临时使用建议按量付费，用完可以删除。想要长期保存镜像建议包年包月。具体定价需要到阿里云官网查看：

[https://help.aliyun.com/document_detail/59636.html?spm=a2c4g.11186623.6.551.](https://help.aliyun.com/document_detail/59636.html?spm=a2c4g.11186623.6.551.2d4c7b55CV5QPf)

[2d4c7b55CV5QPf](https://help.aliyun.com/document_detail/59636.html?spm=a2c4g.11186623.6.551.2d4c7b55CV5QPf)

5.2 自定义镜像需要收取快照费用

镜像功能处于免费试用期，但镜像的存在依赖于快照，保留自定义镜像会产生一定的快照费用。保留自定义镜像会产生一定的快照费用。建议建完 WAF 后可以删除。

快照价格需要到阿里云官网查看：

<https://www.aliyun.com/price/product/?spm=5176.2020520101.0.0.47614df5uFIN>

[Yt#/disk/detail](#)

5.3 虚拟 WAF 规格型号

CPU 和内存不满足最小配置，无法启动，不建议采取添加第二块硬盘的方式。

项目\型号	WV02 默认许可	WV02	WV04
vCPU最小配置	2	2	4
内存最小配置	4G	4G	8G
磁盘最小配置	100G	100G	100G
网卡数量	10	10	10
站点数量	1	8	16
全局不同 IP/port对数	32	32	64
全局IP/port/domain 组合数	128	128	256
Session数 (IPv6减半)	2000	40w	120w