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

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

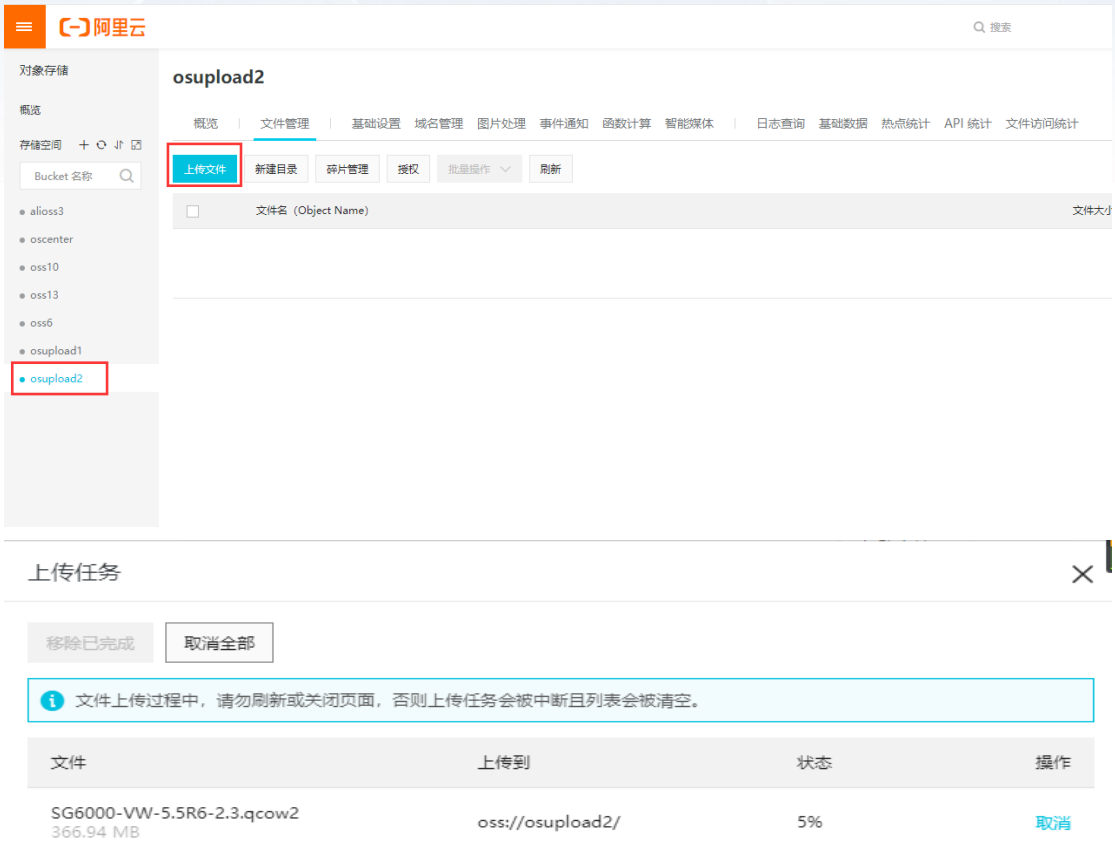
2.2 开通 OSS（对象存储）

2.2.1 新建 Bucket

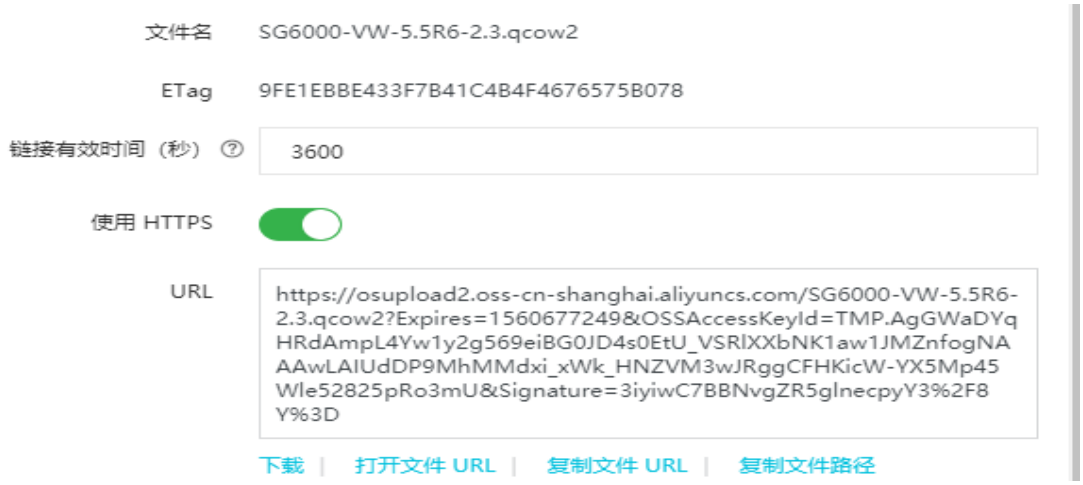
Bucket 名称可以随意填写，存储类型选择标准存储，读写权限设置为私有。

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。

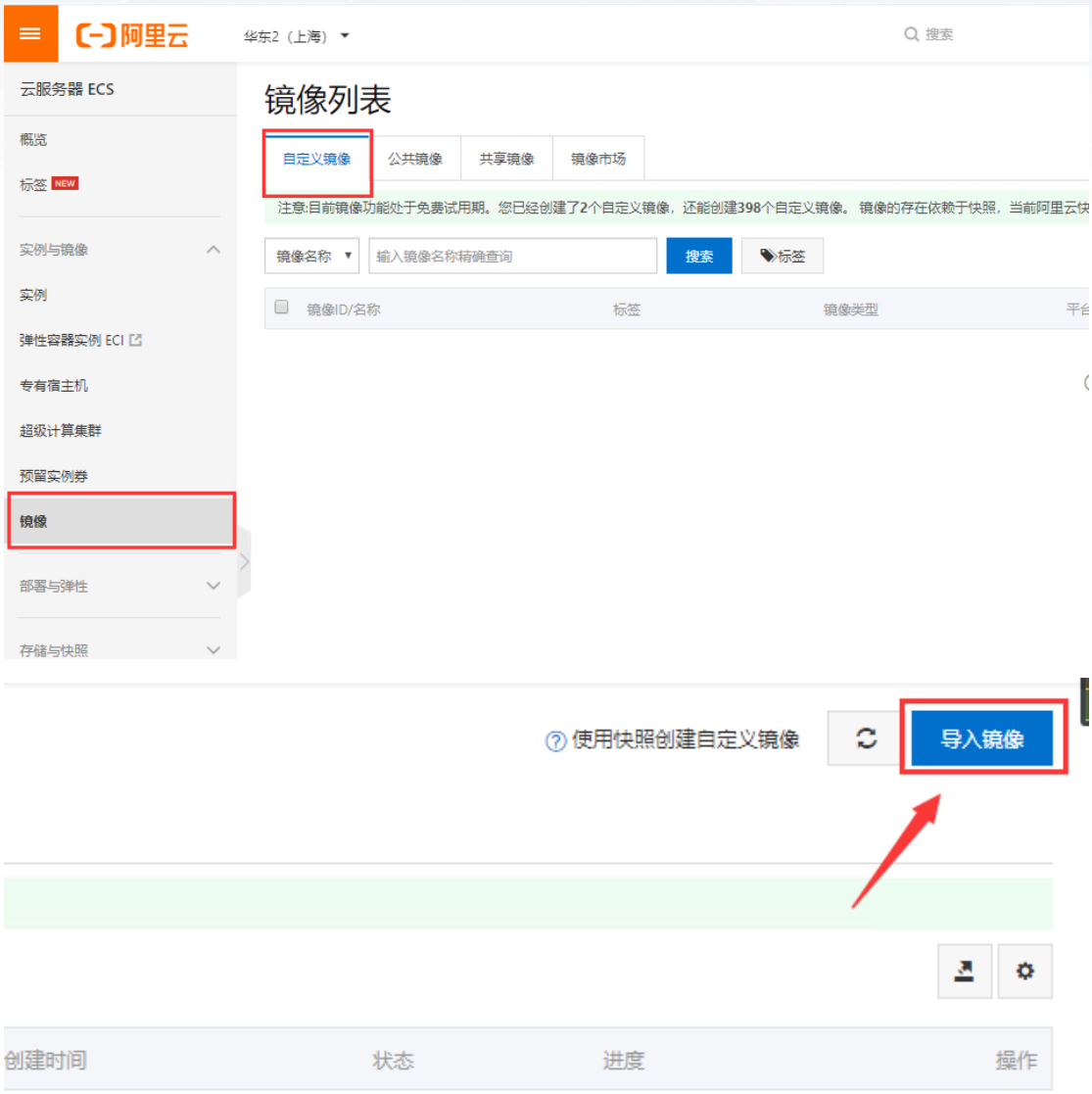


上传完成后查看文件详情，复制里面的 URL，后面自定义镜像的时候会用到。



2.4 自定义镜像

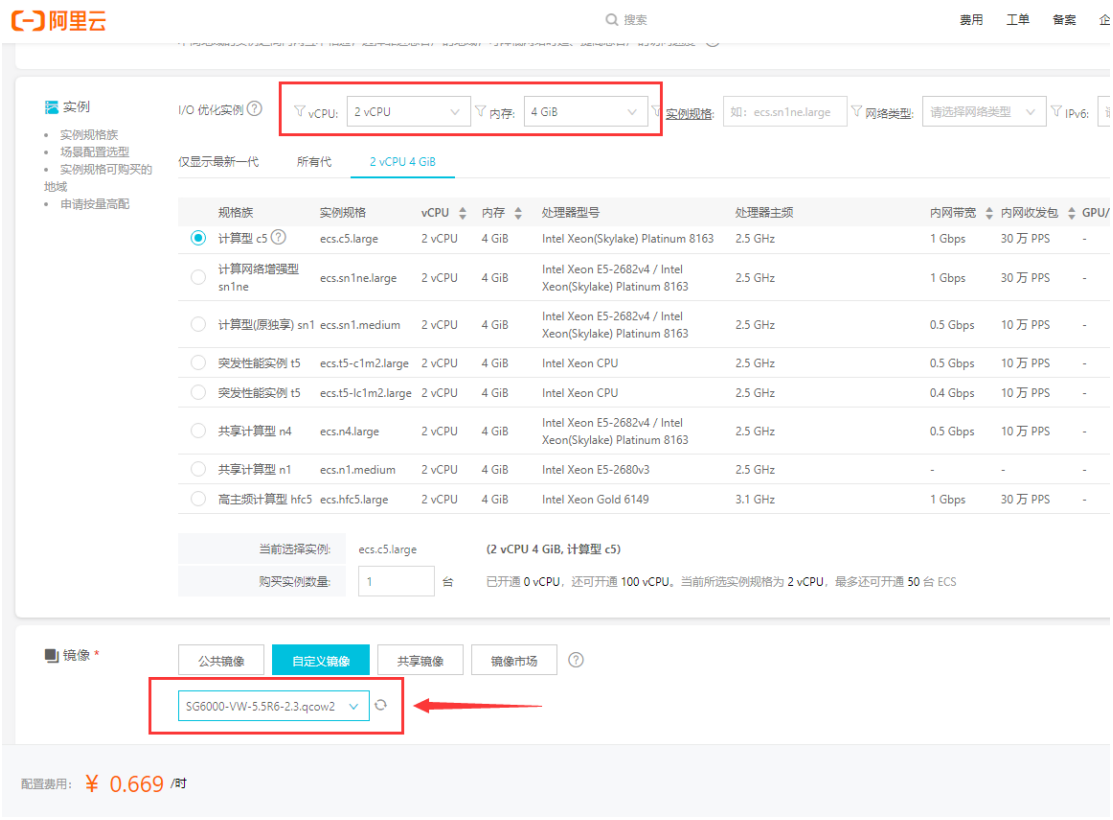
云服务器 ECS》镜像》自定义镜像》导入镜像


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
使用快照创建自定义镜像
导入镜像
创建时间
状态
进度
操作

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。

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。



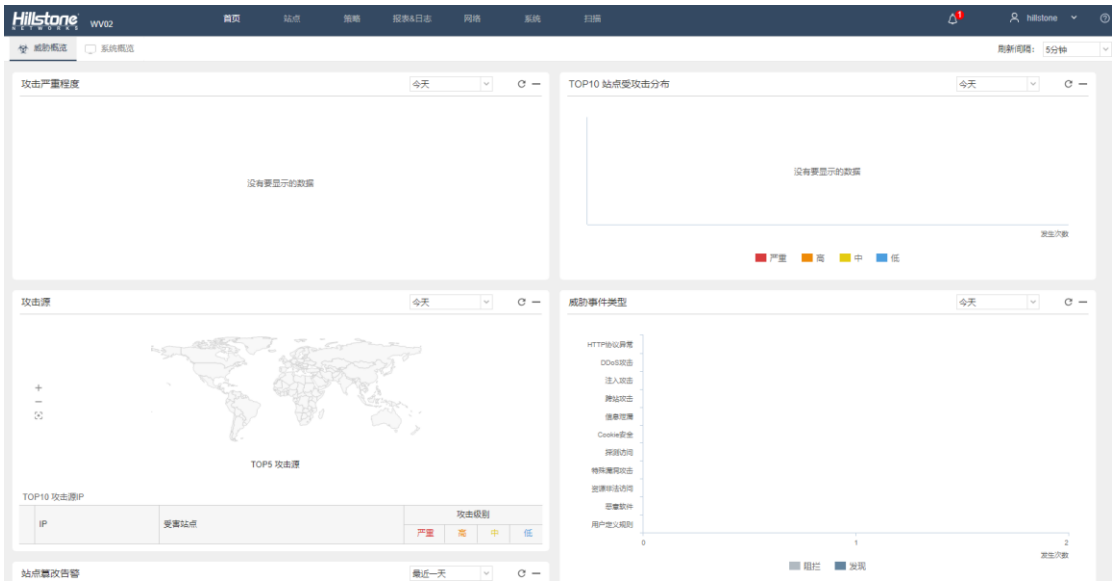
网络需要选择和客户业务相同的 VPC，同时设置 vWAF 的带宽，这里也可以不勾选分配公网 IPv4 地址，后期申请弹性公网 IP 直接绑定在 vWAF 上。

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
网络和安全组
系统配置
使用时限
服务协议
保存为启动模板
生成Open API最佳实践脚本
上一步：分组设置
创建实例


实例列表
ECS控制台操作指南
创建实例
批量操作
选择实例属性项搜索，或者输入关键字识别搜索
标签
高级搜索
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)
192.168.1.110(私有)
运行中
专有网络
2 vCPU 4 GiB (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
按量付费转包年包月
释放设置
更多


Hillstone
WV02
首页
站点
策略
报表&日志
网络
系统
扫描
威胁概览
系统概览
攻击严重程度
TOP10 站点受攻击分布
没有要显示的数据
攻击源
威胁事件类型
TOP5 攻击源
TOP10 攻击源IP
IP
受害站点
攻击级别
严重
高
中
低
站点篡改告警

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

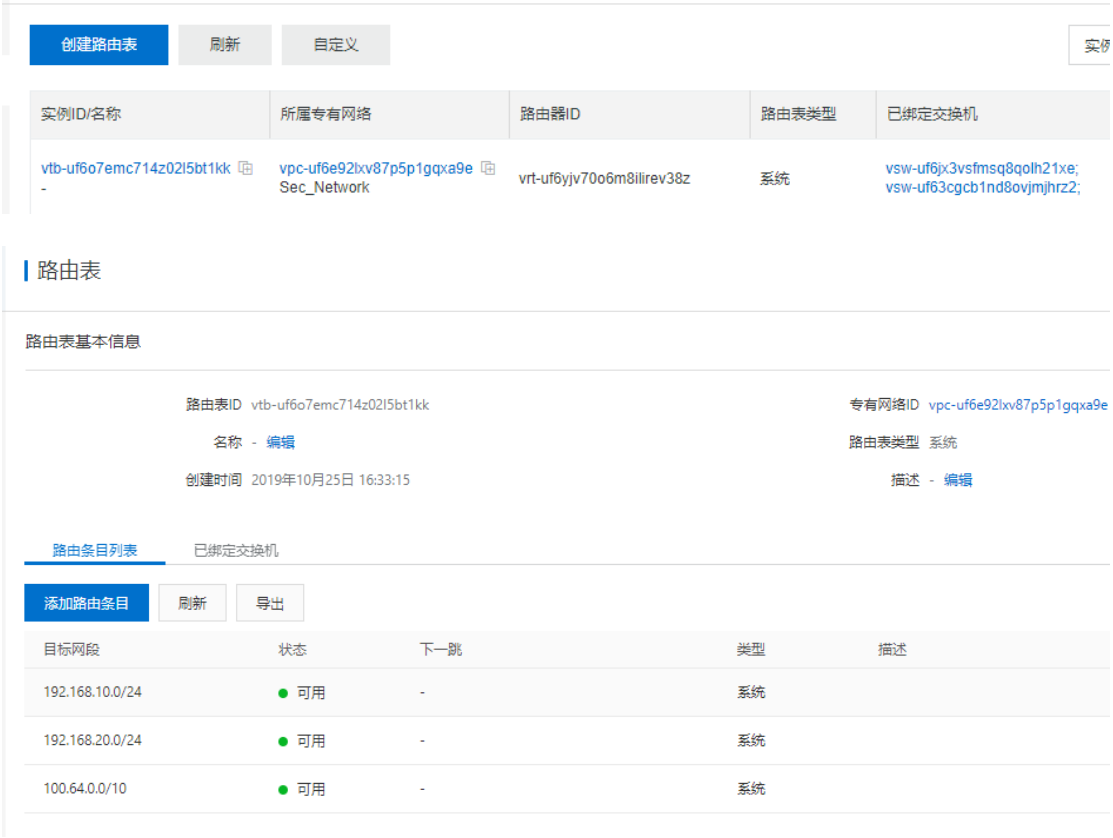
用户在创建专有网络时，需要用 CIDR（无类别域间路由） 作为私有网络指定 IP 地址组。
阿里云专有网络 CIDR 支持使用如下私有网段中的任意一个：
10.0.0.0 - 10.255.255.255（掩码范围需在 8 - 24 之间）
172.16.0.0 - 172.31.255.255（掩码范围需在 8- 24 之间）
192.168.0.0 - 192.168.255.255 （掩码范围需在 8- 24 之间）

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。

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。

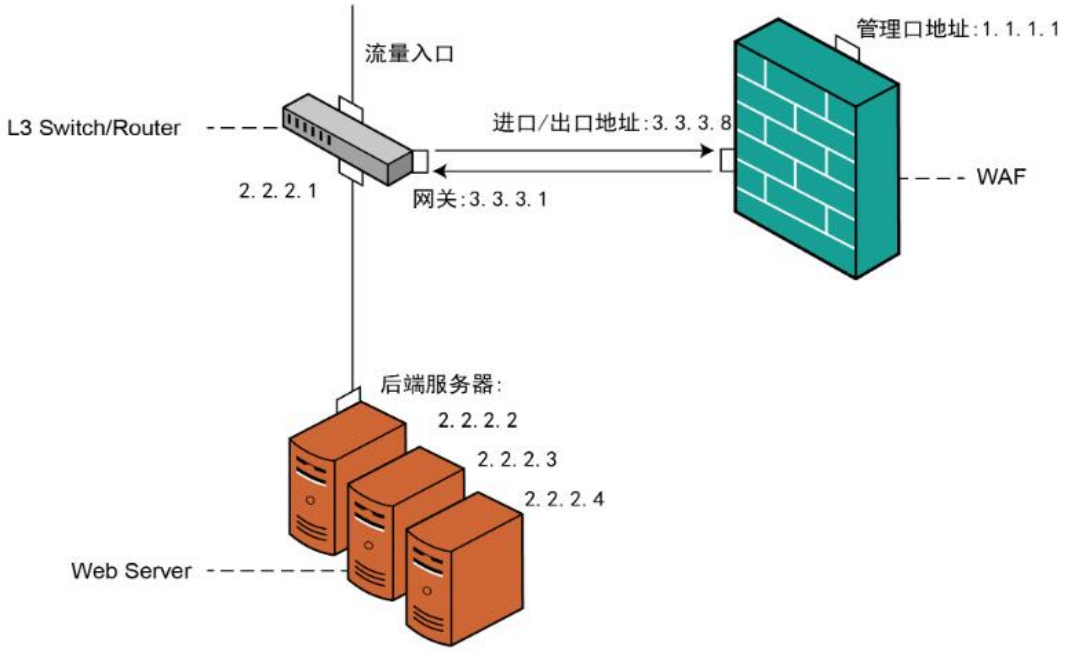


4 部署模式

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

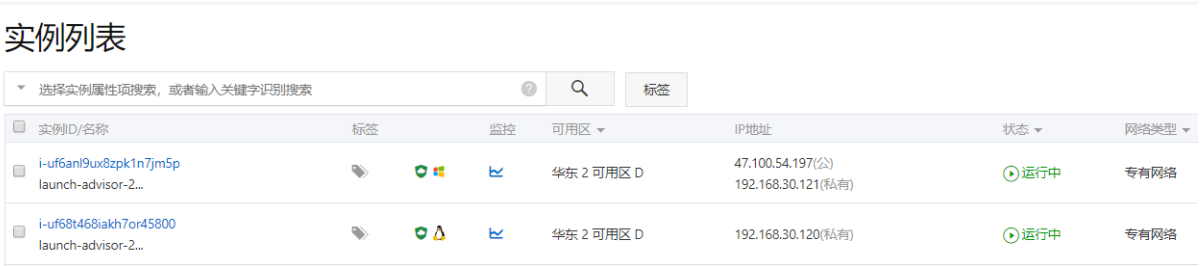
行验证，及阿里云上的配置介绍，可结合自身的需求进行选择。

4.1 单臂模式

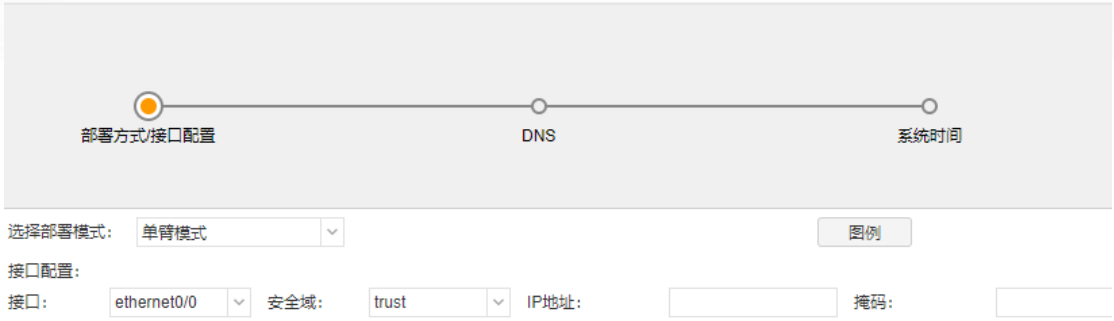


4.1.1 服务器配置

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.



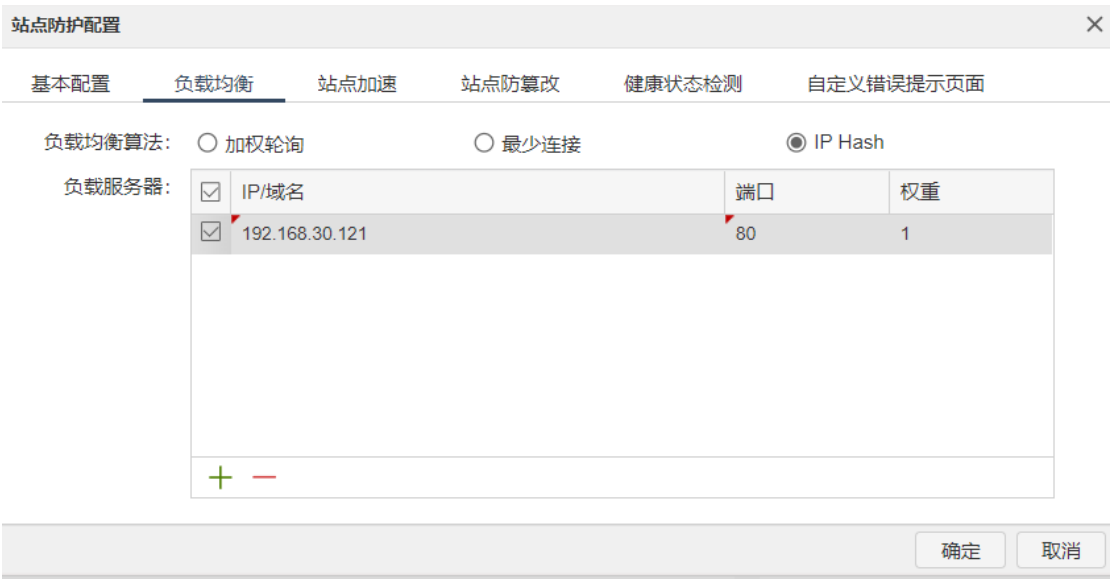
4.1.2 VWAF 配置



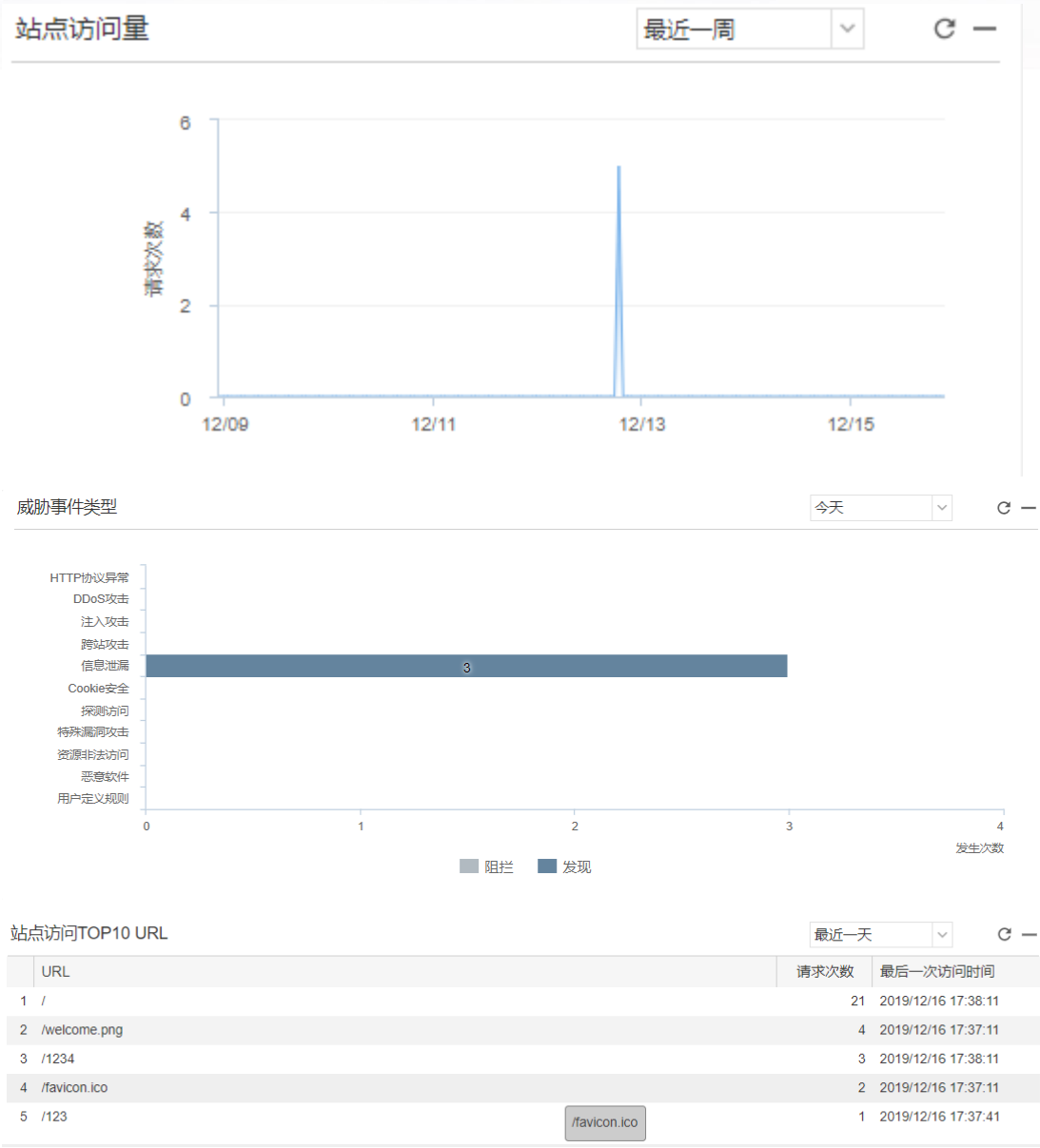
4.1.3 创建站点

服务 ip 应当填写 waf 的接口 ip。

负载服务器中填写 web 服务器的真实 ip；



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.11186623.6.551.2d4c7b55CV5QPf

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=5176.2020520101.0.0.47614df5uFINYt#/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