

山石vWAF在华为云环境下的 部署指南

山石网科通信科技股份有限公司

一、 创建虚拟私有云

虚拟私有云的网段和子网根据需求自行规划，下图为举例配置

创建虚拟私有云

基本信息

区域: 华北-北京一
不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。

名称: vpc-test

网段: 172.16.0.0 / 24
建议使用网段: 10.0.0.0/8-24 (选择) 172.16.0.0/12-24 (选择) 192.168.0.0/16-24 (选择)

默认子网

可用区: 可用区3

名称: subnet-test

子网网段: 172.16.0.0 / 24 可用IP数: 251
子网创建完成后，子网网段无法修改

二、 创建云服务器

1. 在云控制台选择弹性云服务器，并选择购买弹性云服务器。

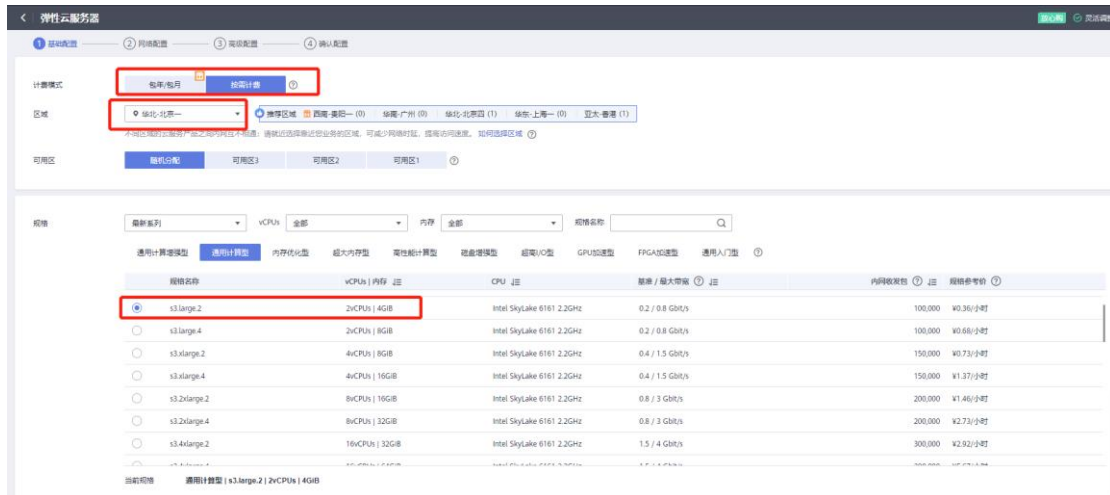


2. 计算模式根据需求选择包年或包月，或者按需计费。

区域选择一定要和镜像在同一个区域。

规格选择最少使用 2 个 vCPU，内存最小为 4GB，

这里使用通用计算型，s3.large.2 | 2vCPUs | 4GB



3. 选择要部署的镜像。



4. 选择网络和安全组，网络就是之前创建的虚拟私有云，选择要部署到的子网，这里选择 DHCP 获取地址，可以根据组网需求配置静态 IP。增加一张扩展网卡。



5. 绑定弹性公网 IP，如果不需通过公网访问，可以选择“暂不购买”

弹性公网IP 现在购买 使用已有 暂不购买 ?

线路 静态BGP 全动态BGP ?

不低于99%可用性保障

公网带宽

按带宽计费 👍
流量较大或较稳定的场景

按流量计费
流量小或流量波动较大场景

加入共享带宽
多业务流量错峰分布场景 ?

指定带宽上限，按实际使用的出公网流量计费，与使用时间无关。

带宽大小

5 10 20 50 100 自定义 带宽范围: 1-300 Mbit/s

免费开启DDoS基础防护

6. 高级配置，设置密码和云服务器名称，其他保持默认。

这里的密码不会同步到 web 控制台。

云服务器名称 允许重名

购买多台云服务器时，名称自动按序增加4位数字后缀。例如：输入ecs，从ecs-0001开始命名；若已有ecs-0010，从ecs-0011开始命名。

登录凭证 密码 密钥对 使用镜像密码

用户名 root

密码 请牢记密码，如忘记密码可登录ECS控制台重置密码。

确认密码

云备份 使用云备份服务，需购买备份存储库，存储库是存放服务器产生的备份副本的容器。

现在购买 使用已有 暂不购买 ?

7. 部署完成，可以通过访问公网 IP 来登录

名称/ID	监控	可用区	状态	规格/镜像	IP地址	计费模式	标签	操作
vWAF-test ee76d89-1055-4ff1-b33d-e59c723e2f5c		可用区2	运行中	2vCPUs 4GB i3.large.2 vWAF5.SR6.2.7.4	114.115.218.63 (弹性公网) 1 Mbit/s 10.0.0.70 (私有)	按量计费 2021/08/19 14:18:10 创建	-	远程登录 更多

8. 通过 https 成功访问 web 页面



9. 通过 ssh 访问，看到接口地址已经自动分配成功，同时下发一条指向网关的默认路由。

如果静态分配 IP 地址，需要手动配置一条指向网关的静态路由。

```
3 114.115.218.63
> For more info, ctrl+click on help or visit our website.

SG-6000#
SG-6000#
SG-6000# show inter
SG-6000# show interface

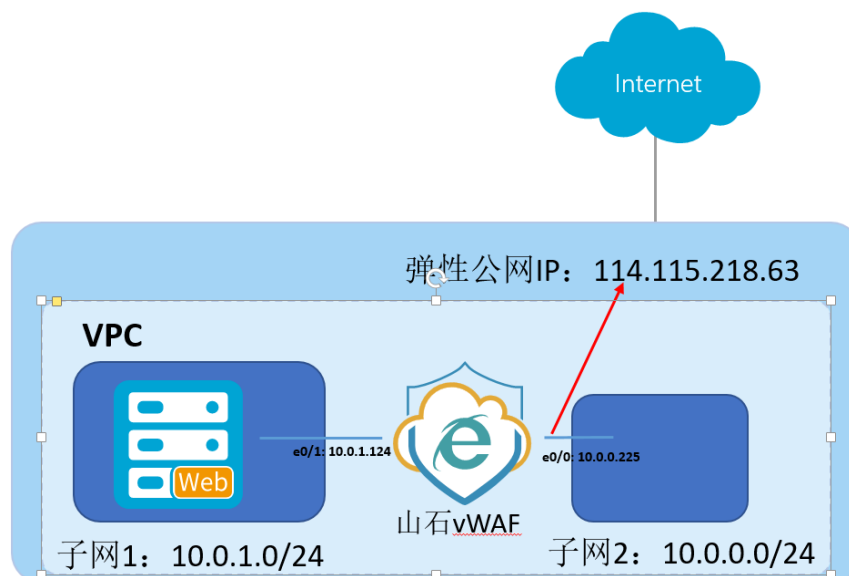
H:physical state;A:admin state;L:link state;P:protocol state;U:up;D:down;K:ha keep up;C:lacp down
=====
Interface name      IP address/mask    Zone name          H A L P MAC address  Description
-----
ethernet0/0         10.0.0.225/24      trust              U U U U fa16.3e28.ea60  -----
ethernet0/1         0.0.0.0/0          NULL               U U U D fa16.3e1c.2f1d  -----
vswitchif1          0.0.0.0/0          NULL               U U U D 001c.54ef.7e1b  -----
=====

SG-6000# show ip ro
SG-6000# show ip route
Codes: K - kernel route, C - connected, S - static, Z - ISP, R - RIP, O - OSPF,
       B - BGP, D - DHCP, P - PPPoE, W - wireless, H - HOST, G - SCVPN, V - VPN, M - IMPORT,
       I - ISIS, Y - SYNC, L - llb outbound, > - selected first nexthop, * - FIB route, b - BFD enable

Routing Table for Virtual Router <trust-vr>
=====
D>* 0.0.0.0/0 [1/0/1] via 10.0.0.1, ethernet0/0
C>* 10.0.0.0/24 is directly connected, ethernet0/0
H>* 10.0.0.225/32 [0/0/1] is local address, ethernet0/0
D>* 169.254.169.254/32 [1/0/1] via 10.0.0.254, ethernet0/0
=====
```

10. vWAF 使用举例

如图所示，我们在 VPC 里创建两个子网，将 vWAF 的 e0/1 接口绑定在子网 1，绑定公网 IP 的 e0/0 接口绑定在子网 2，子网 1 里有一台 web 服务器，vWAF 通过反向代理模式防护 web 服务器。



vWAF 部署成功后，登录 web 页面进行 WAF 初始化安装，设置部署模式为反向代理模式，再配置 WAN 口和 LAN 口地址 IP 和安全域。

WAF安装向导

1 部署方式/接口配置 2 DNS 3 系统时间

选择部署: 反向代理模式 图例

LAN接口配置

LAN接口: ethernet0/1 安全域: trust

IPv4类型: 静态IP 自动获取

IPv4IP地址: 10.0.1.124 子网掩码: 24

IPv6 地址: 前缀长度:

WAN接口配置

WAN接口: ethernet0/0 安全域: trust

IPv4类型: 静态IP 自动获取

IPv4IP地址: 10.0.0.225 子网掩码: 24

IPv6 地址: 前缀长度:

① 设备默认管理接口为ethernet0/0，如果需要配置该接口，建议使用“自动获取”类型，此时会使用DHCP配置接口的IP和路由。如果有需求配置为静态IP，建议先在后台配置好接口ethernet0/0的IP和路由之后，再通过安装向导进行配置。

下一步 取消

配置 DNS 服务器：

WAF安装向导

1 部署方式/接口配置 2 DNS 3 系统时间

首要DNS服务器IP: 114.114.114.114 虚拟路由器: trust-vr

次要DNS服务器IP 1: 虚拟路由器: trust-vr

次要DNS服务器IP 2: 虚拟路由器: trust-vr

设置系统时间：

WAF安装向导

1 部署方式/接口配置 2 DNS 3 系统时间

设置系统时间

与本地时间同步:

启用NTP:

手动配置:

新建站点防护，我们将 web 服务器的 IP 地址和对应服务端口填入

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: test

站点状态: 防护 网站维护

站点类型: HTTP HTTPS

IP IP范围 IPv4/掩码 IPv6/前缀长度	端口 端口范围
10.0.0.104	80

域名: Any 禁止域名为IP的访问

域 (1-255)字节

启用负载均衡，使用 IP Hash 算法

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

IP/域名	端口	权重
10.0.1.229	80	1

确定 取消

取消仅检测勾选，若勾选则只记录，不会进行攻击阻挡。

策略配置

基本配置 防护规则

名称: sql注入 (1-127)字符

模板: policy_normal_template

描述: (0-1023)字符

策略优化: 通过以下选项, WAF系统可以自动优化防护规则

Database: Framework: OS: Web Server:

仅检测:

保存 取消

在策略配置中将注入攻击里的 SQL 注入打开，开启注入攻击防护

策略配置

基本配置 防护规则

以下是WAF系统自动生成的该站点的防护策略

类型	状态	注入攻击 子类型	状态
HTTP协议异常	<input checked="" type="checkbox"/>	SQL注入	<input checked="" type="checkbox"/>
DDoS攻击	<input checked="" type="checkbox"/>	LDAP注入	<input checked="" type="checkbox"/>
注入攻击	<input checked="" type="checkbox"/>	SSI指令注入	<input checked="" type="checkbox"/>
跨站攻击	<input checked="" type="checkbox"/>	XPath注入	<input checked="" type="checkbox"/>
信息泄露	<input checked="" type="checkbox"/>	命令注入	<input checked="" type="checkbox"/>
Cookie安全	<input checked="" type="checkbox"/>	远程文件包含	<input checked="" type="checkbox"/>
探测访问	<input checked="" type="checkbox"/>	本地文件包含	<input checked="" type="checkbox"/>
特殊漏洞攻击	<input checked="" type="checkbox"/>	代码注入	<input checked="" type="checkbox"/>
资源非法访问	<input checked="" type="checkbox"/>	邮件注入	<input checked="" type="checkbox"/>
恶意软件	<input checked="" type="checkbox"/>	XML注入	<input checked="" type="checkbox"/>
用户定义规则	<input checked="" type="checkbox"/>	其他注入	<input checked="" type="checkbox"/>

ID	名称	状态	告警级别	防护动作			抓包	参数
				动作	动作详情	状态码		
1020010020	SELECT语句绕过SQL认证绕过	<input checked="" type="checkbox"/>	严重	告警			<input checked="" type="checkbox"/>	
1020010021	EXISTS句式	<input checked="" type="checkbox"/>	严重	告警			<input checked="" type="checkbox"/>	
1020010023	root@句式	<input checked="" type="checkbox"/>	低	阻断	阻断当次	403	<input checked="" type="checkbox"/>	
1020010024	使用SLEEP函数的SQL盲注攻击	<input checked="" type="checkbox"/>	严重	阻断	阻断当次	403	<input checked="" type="checkbox"/>	
1020010025	使用BENCHMARK函数的SQL盲注攻击	<input checked="" type="checkbox"/>	严重	阻断	阻断当次	403	<input checked="" type="checkbox"/>	
1020010026	使用引号句式进行SQL认证绕过	<input checked="" type="checkbox"/>	严重	告警			<input checked="" type="checkbox"/>	
1020010027	使用ADMIN引号句式进行SQL认证绕过	<input checked="" type="checkbox"/>	严重	告警			<input checked="" type="checkbox"/>	

保存 取消

将该安全策略应用到需要防护的站点上：

test

- 概览
- 威胁详情
- 网页变更历史
- 白名单
- 黑名单
- 例外规则
- 站点配置
- 自学习
- 机器流量分析
- 外链改写

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

域名: Any 禁止域名为IP的访问

域 (1-255)字节

IP防护策略: -----

访问控制策略:

名称	操作

API防护策略: -----

虚拟补丁策略: -----

安全策略: **sql注入**

自学习策略: -----

用户会话跟踪策略: -----

内容改写策略:

名称	操作

PING:

对 web 服务器进行注入攻击，失败！阻挡成功！

→ 不安全 | 114.115.218.63/?name=admin%27%20and%20if(1=1,sleep(5),0)%20and%20%27a%27=%27a

403 Forbidden

HTTP Proxy

在 vWAF 上可以看到攻击记录信息。

test

时间: 今天

时间	规则ID	告警级别	防护类型	客户端IP	域名	用户名	会话标识值	URL
2021/08/20 16:56:43	1020010064	严重	注入攻击	221.224.30.130	114.115.218.63	N/A	N/A	/dirtrav/example3.php?file=hacker
2021/08/20 16:56:43	1020010024	严重	注入攻击	221.224.30.130	114.115.218.63	N/A	N/A	/dirtrav/example3.php?file=hacker
2021/08/20 16:56:43	1020020000	严重	注入攻击	221.224.30.130	114.115.218.63	N/A	N/A	/dirtrav/example3.php?file=hacker
2021/08/20 16:56:43	1020010129	严重	注入攻击	221.224.30.130	114.115.218.63	N/A	N/A	/dirtrav/example3.php?file=hacker