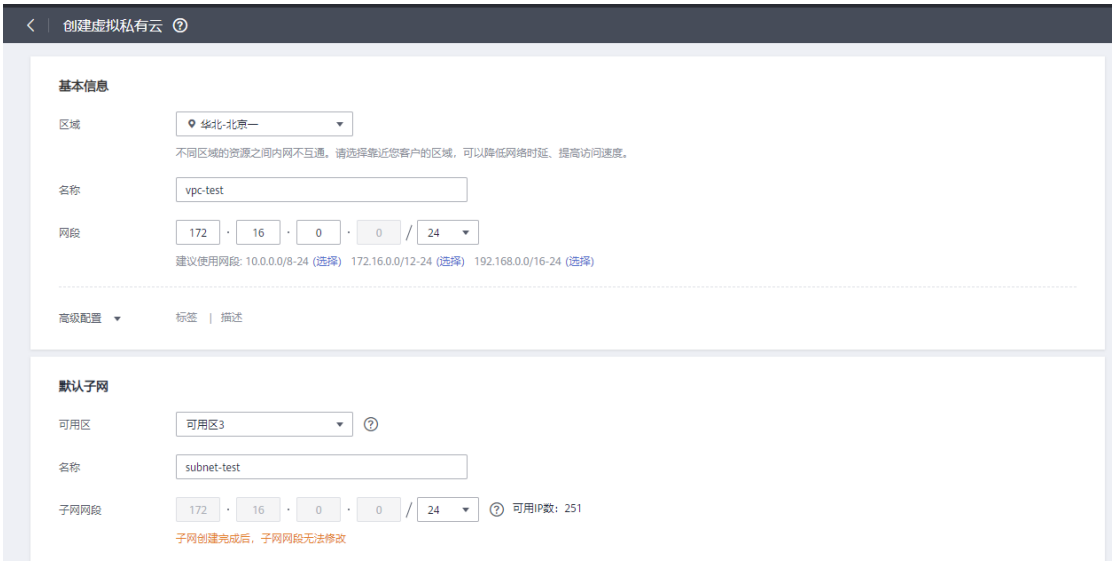
山石vWAF在华为云环境下的部署指南

山石网科通信技术股份有限公司

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



二、 创建云服务器

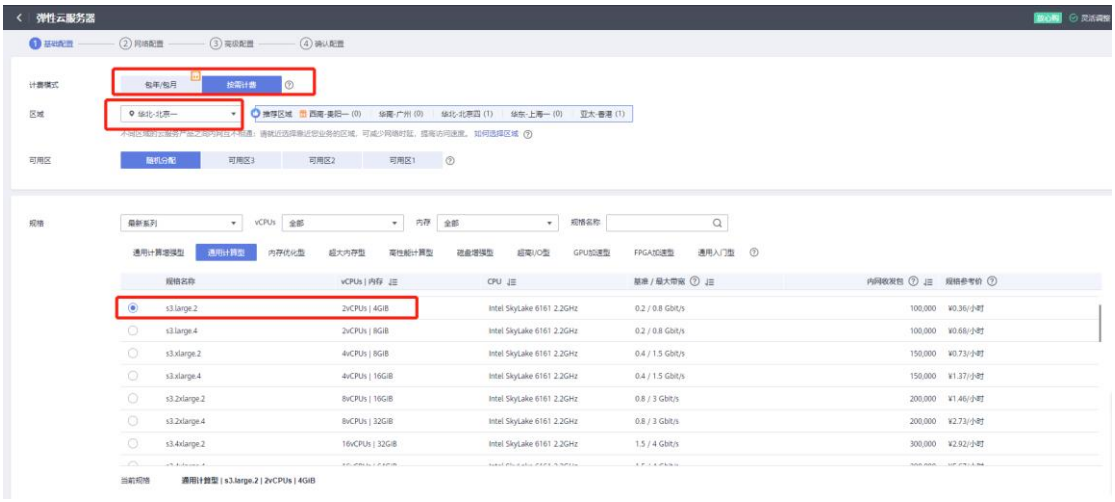
1. 在云控制台选择弹性云服务器，并选择购买弹性云服务器。

2. 计算模式根据需要选择包年或包月，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”

6. 高级配置，设置密码和云服务器名称，其他保持默认。

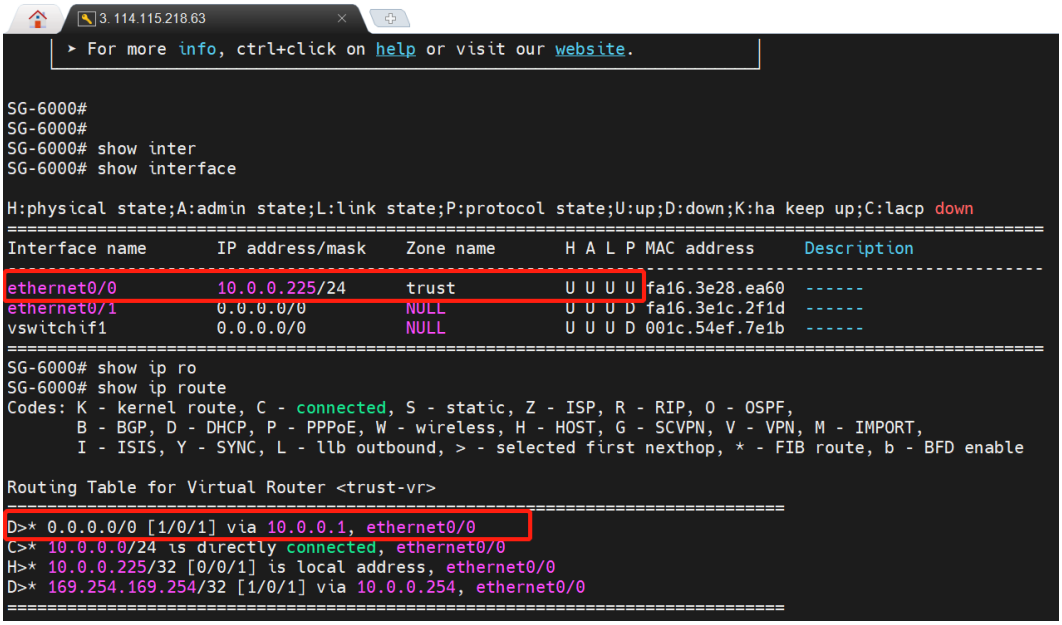
   这里的密码不会同步到 web 控制台。

7. 部署完成，可以通过访问公网 IP 来登录

8. 通过 https 成功访问 web 页面

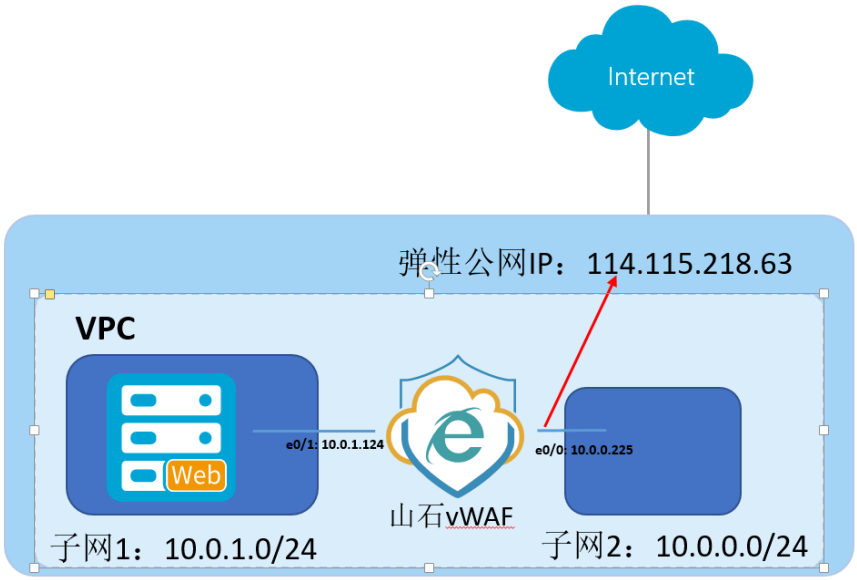
9. 通过 ssh 访问，看到接口地址已经自动分配成功，同时下发一条指向网关的默认路由。

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。



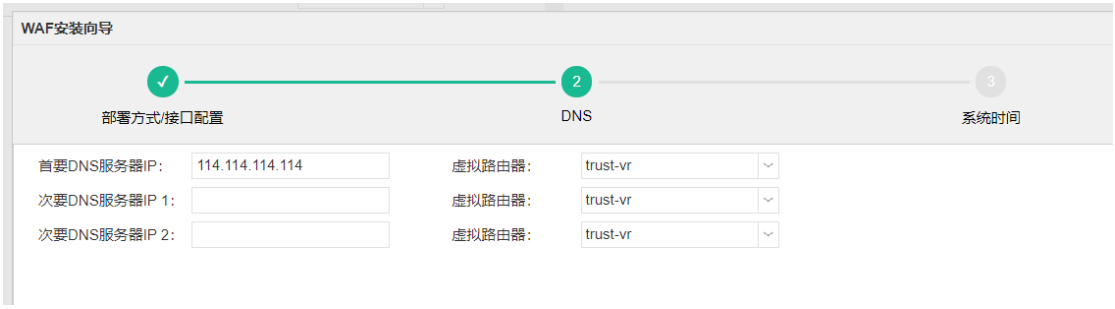
10. vWAF 使用举例

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。

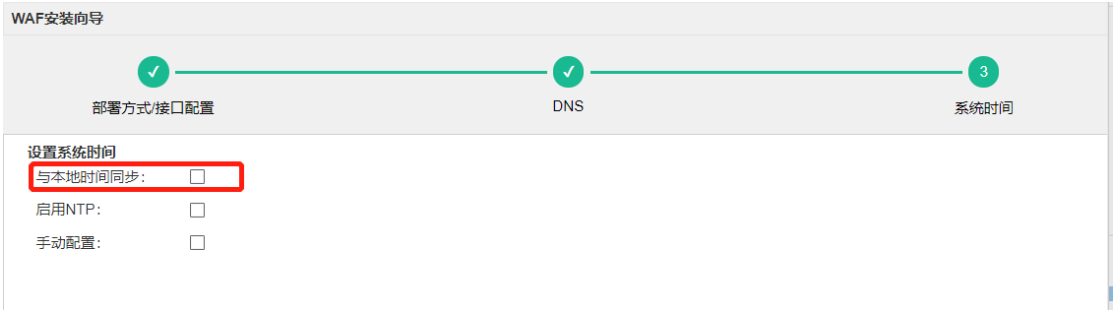


vWAF 部署成功后，登录 web 页面进行 WAF 初始化安装，设置部署模式为反向代理模式，再配置 WAN 口和 LAN 口地址 IP 和安全域。

配置 DNS 服务器：



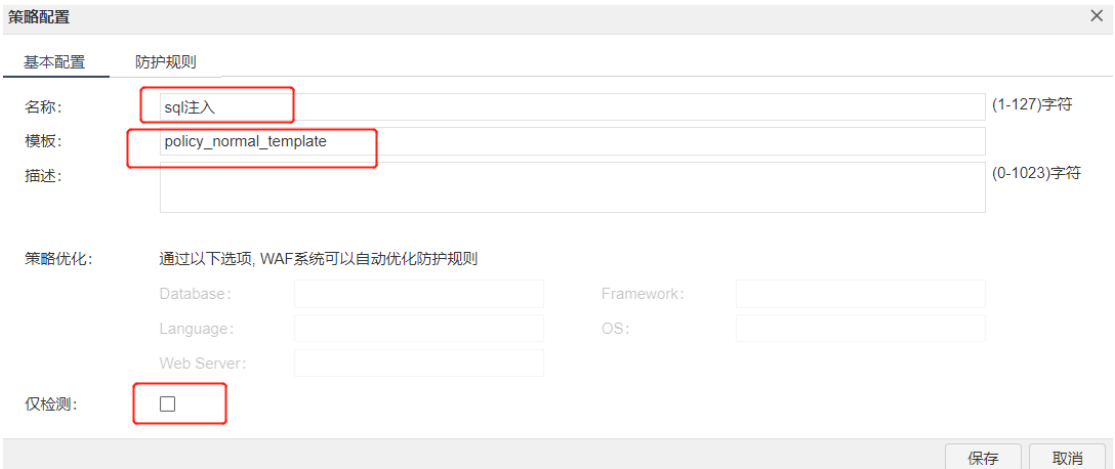
设置系统时间：



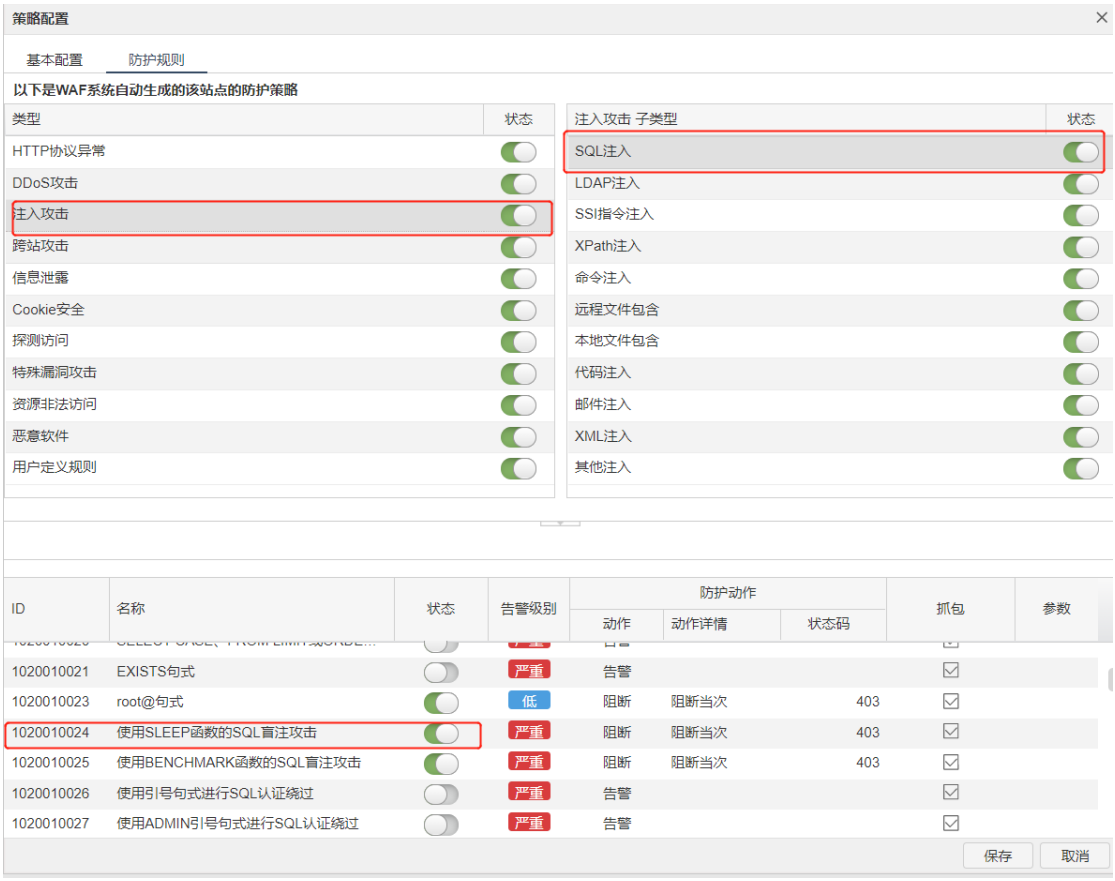
新建站点防护，我们将 web 服务器的 IP 地址和对应服务端口填入

启用负载均衡，使用 IP Hash 算法

取消仅检测勾选，若勾选则只记录，不会进行攻击阻挡。



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



将该安全策略应用到需要防护的站点上：

对 web 服务器进行注入攻击，失败！阻挡成功！

在 vWAF 上可以看到攻击记录信息。