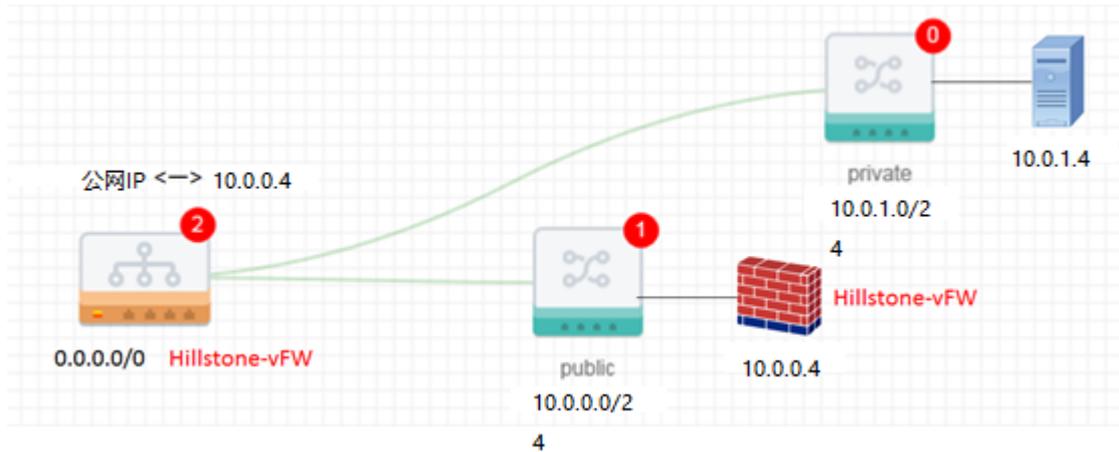


安装部署手册山石云·界在华为云 VPC 环境下的使用指南

一、组网原理

创建一个虚拟网络划分子网做内部公网子网，创建山石云·界时连接到这个内部子网，山石云·界的这个接口同时做为管理口和公网出口。给山石云·界绑一个弹性公网 IP，SNAT 和 DNAT 都用这个 IP。在路由表上配置内网向外网的默认路由都走山石云·界。



二、创建虚拟私有云

1.在华为云控制台网络部分创建虚拟私有云



2.在创建好的虚拟私有云中创建子网

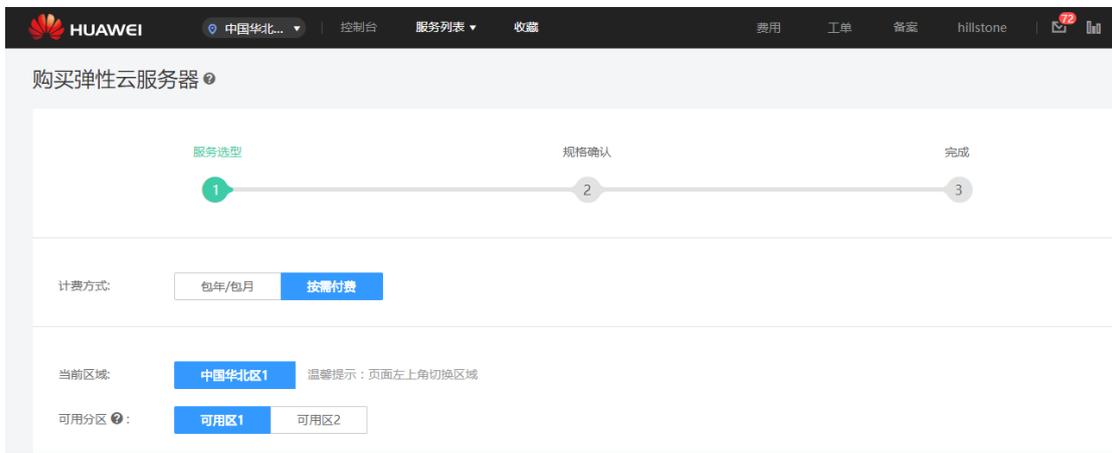


三、创建云服务器（山石云·界部署）

1、在华为云控制台选择弹性云服务器，并选择购买弹性云服务器



2、计费方式根据需求去选择，区域选择应与上面所创建虚拟私有云对应



3、山石网科-虚拟化下一代防火墙 旗舰版(BYOL)是基于私有 Linux 系统的虚拟机镜像产品，当前版本软件限制要求虚拟机资源规格为：2 核、不小于 2G 内存、不小于 4G 系统盘，因此这边云服务器类型选择只需符合最低标准就行



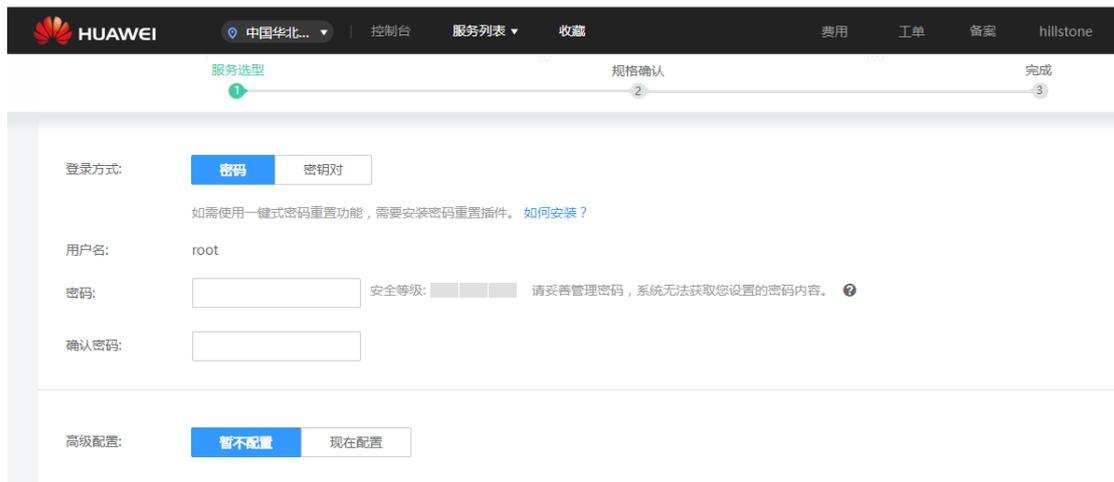
4、选择山石网科云·界镜像，硬盘保持默认



5、选择之前所创建的虚拟私有云及其子网，安全组这边选择默认所有（用户可根据需求去修改安全组规则），并选择给云服务器绑定弹性 IP（可选择以后再绑定）



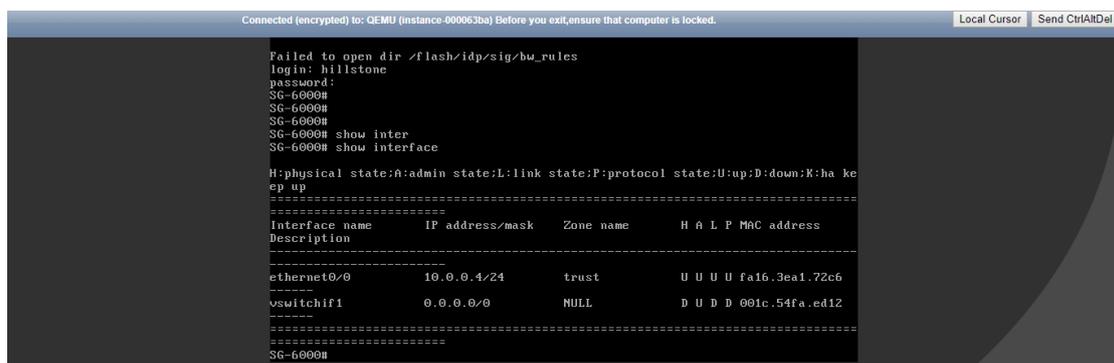
6、给云服务器设置登陆密码，高级配置不需要配置



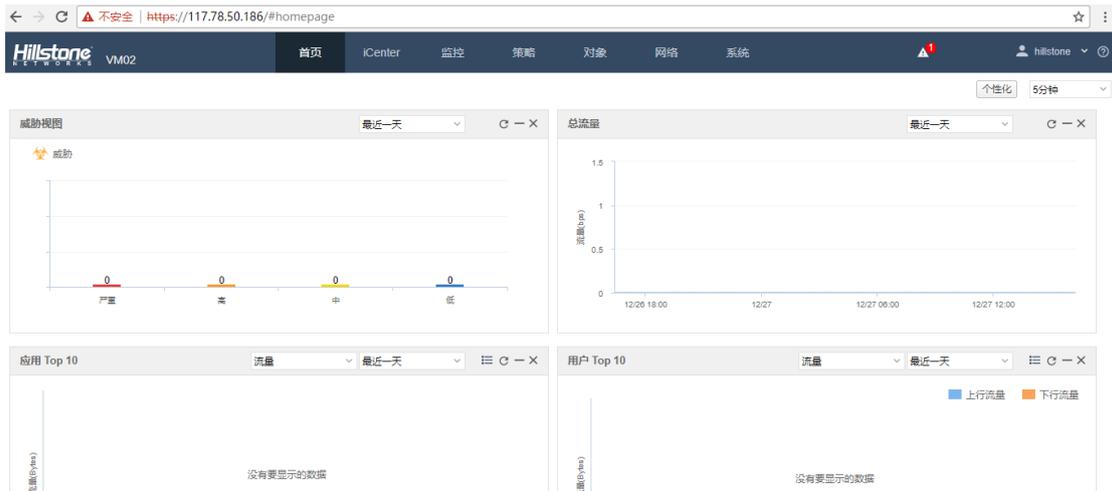
7、云服务器（山石云·界）创建完成



8、点击远程登陆，山石云·界 CLI 界面如下



9、用浏览器（IE11 及以上或 Chrome）https 访问所绑定的弹性公网 IP 即可操作山石云·界的 WEIUI 界面



四、在虚拟私有云路由器上添加默认路由

山石云·界所在子网地址段为 10.0.0.0/24，web 虚拟机所在子网地址段为 10.0.1.0/24,因此在虚拟私有云路由器上添加下一跳指向云·界的默认路由



五、山石云·界的配置和使用

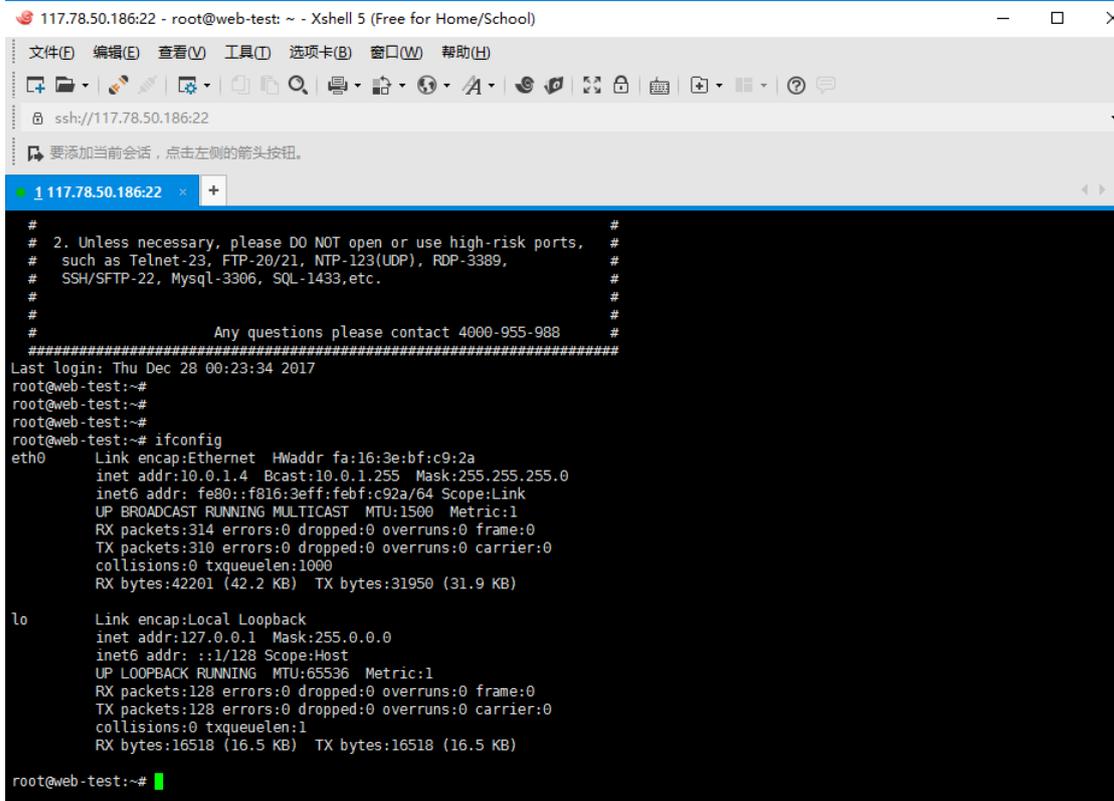
在云·界上配置一条访问控制策略（此处配置的为全通策略）



在云·界上配置一条 DNAT 策略，将访问云·界 e0/0 接口地址 SSH 服务的给映射到环境中的 web 虚拟机上



验证 DNAT 策略（在外网通过 SSH 云·界所绑定的弹性 IP 可以连接到环境中的 web 虚拟机）



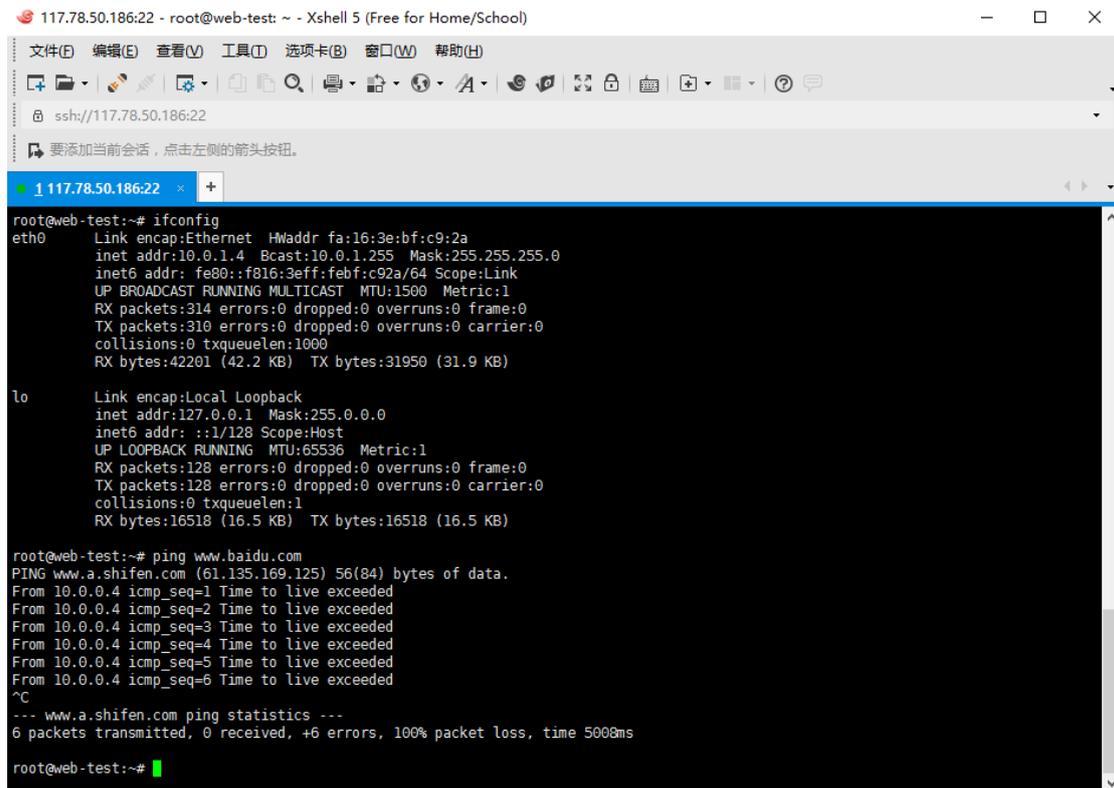
在云·界上配置一条 SNAT 策略，将出流量源地址转换成出接口 IP（云·界 e0/0 接口地址）



关闭所创建的云·界上网卡的源/目的检查（点击弹性云服务器名称进入后台配置）



没有配置 SNAT 前环境中的 web 虚拟机无法 ping 通外网



验证 SNAT 策略，配置完 SNAT 后 web 虚拟机可以 ping 通外网

```
117.78.50.186:22 - root@web-test: ~ - Xshell 5 (Free for Home/School)
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://117.78.50.186:22
要添加当前会话，点击左侧的箭头按钮。
1 117.78.50.186:22 * +
RX packets:128 errors:0 dropped:0 overruns:0 frame:0
TX packets:128 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:16518 (16.5 KB) TX bytes:16518 (16.5 KB)

root@web-test:~# ping www.baidu.com
PING www.a.shifen.com (61.135.169.125) 56(84) bytes of data.
From 10.0.0.4 icmp_seq=1 Time to live exceeded
From 10.0.0.4 icmp_seq=2 Time to live exceeded
From 10.0.0.4 icmp_seq=3 Time to live exceeded
From 10.0.0.4 icmp_seq=4 Time to live exceeded
From 10.0.0.4 icmp_seq=5 Time to live exceeded
From 10.0.0.4 icmp_seq=6 Time to live exceeded
^C
--- www.a.shifen.com ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5000ms

root@web-test:~# ping www.baidu.com
PING www.a.shifen.com (61.135.169.125) 56(84) bytes of data.
64 bytes from 61.135.169.125: icmp_seq=1 ttl=46 time=2.88 ms
64 bytes from 61.135.169.125: icmp_seq=2 ttl=46 time=2.49 ms
64 bytes from 61.135.169.125: icmp_seq=3 ttl=46 time=3.47 ms
64 bytes from 61.135.169.125: icmp_seq=4 ttl=46 time=3.12 ms
64 bytes from 61.135.169.125: icmp_seq=5 ttl=46 time=3.41 ms
64 bytes from 61.135.169.125: icmp_seq=6 ttl=46 time=3.39 ms
64 bytes from 61.135.169.125: icmp_seq=7 ttl=46 time=3.34 ms
64 bytes from 61.135.169.125: icmp_seq=8 ttl=46 time=3.41 ms
^C
--- www.a.shifen.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 2.499/3.192/3.477/0.324 ms
root@web-test:~#
```