目录

快速入门

本次练习中，您将创建一个VPC和子网，并将一个可以连接到Internet的云服务器部署到您的子网中，最后通过安全组对进出该云服务器的流量进行筛选，保证云服务器通信的安全。您在该部署中的云服务器能够与 Internet 通信，并且您能够从本地计算机访问您的云服务器。在真实应用环境下，您可以使用此方案创建面向公众的 Web服务器；例如，托管一个网站。

您需要完成以下步骤：

- 第1步：创建虚拟私有网络
- 第2步：添加云服务器和弹性IP
- 第3步：编辑安全组规则

进入安全组

1. 点击VPC左侧导航“安全组”按钮，进入安全组管理页面。

创建安全组

1. 点击“新建”，弹出创建安全组浮层。
2. 填写完信息，点击“创建”按钮，完成安全组创建。

删除安全组

1. 勾选需要删除的安全组，点击“删除”按钮，弹出确认删除安全组浮层。
2. 确认信息无误，点击“删除”按钮，删除成功后，会提示删除成功，删除失败，会提示删除失败并告知失败原因。

管理安全组规则

- 安全组规则只作用于绑定的主机。
- 安全组规则默认黑名单。
- 安全组规则默认出站规则全部放行，用户可以删除。

创建安全组规则

1. 点击“创建安全组规则”，弹出创建安全组规则浮层。
2. 填写完信息，点击“创建”按钮，完成安全组规则创建。

删除安全组规则

1. 勾选需要删除的安全组规则，点击“删除”按钮，弹出确认删除安全组规则浮层。
2. 确认信息无误，点击“删除”按钮，删除成功后，会提示删除成功，删除失败，会提示删除失败并告知失败原因。

安全组绑定主机

进入绑定主机页面

1. 点击安全组列表中的“云服务器信息”，进入相应安全组绑定的主机列表页。

更换安全组

1. 勾选需要更换安全组的主机，点击“更换安全组”按钮，弹出确认更换安全组浮层。
2. 填写完信息，点击“绑定”按钮，完成安全组规则更换。

ACL

- 无状态访问控制规则。
- ACL规则只作用于ACL绑定的子网。

进入ACL

1. 点击VPC左侧导航“ACL”按钮，进入ACL管理页面。

创建ACL

1. 点击“新建”按钮，弹出创建ACL浮层
2. 填写完信息，点击“创建”按钮，完成ACL创建。

删除ACL

1. 勾选需要删除的ACL，点击“删除”按钮，弹出确认删除ACL浮层。
2. 确认信息无误，点击“删除”按钮，删除成功后，会提示删除成功，删除失败，会提示删除失败并告知失败原因。

管理ACL规则

- ACL规则只作用于ACL绑定的子网。

创建ACL规则

1. 点击“创建ACL规则”，弹出创建ACL规则浮层。
2. 填写完信息，点击“创建”按钮，完成ACL规则创建。

删除ACL规则

1. 勾选需要删除的ACL，点击“删除ACL”按钮，弹出确认删除ACL浮层。
2. 确认信息无误，点击“删除”按钮，删除成功后，会提示删除成功，删除失败，会提示删除失败并告知失败原因。

ACL绑定解绑子网

进入ACL绑定解绑子网

1. 点击“子网信息”，进入绑定子网页面。

ACL绑定子网

1. 点击“绑定子网”按钮，弹出绑定子网浮层。
2. 填写完信息，点击“绑定”按钮，完成子网绑定。

ACL解绑子网

1. 勾选需要解绑的子网，点击“解绑”按钮，弹出确认解绑子网浮层。
2. 确认信息无误，点击“确认”按钮，解绑成功后，会提示解绑成功，解绑失败，会提示解绑失败并告知失败原因。

创建虚拟私有网络

1.登录私有网络控制台。 2.选择所属地域后，单击**新建**。 3.在新建 VPC 弹窗中，配置私有网络信息和初始子网，然后单击**确定**。

IPv4 CIDR ：建议使用 10.0.0.0/8， 172.16.0.0/12，192.168.0.0/16 等私网地址段。同时请注意，198.18.0.0/15， 100.64.0.0/10， 240.0.0.0/4，11.255.255.0/24，33.0.0.0/8等地址段不可使用。

添加云服务器和弹性IP

添加服务器和弹性IP

1.登录金山云控制台，点击导航条【计算资源】下的【云服务器】进入云服务器控制台

2.选择右上角的地域，点击【新建实例】创建云服务器

3.进入云服务器购买页面，选择需要的云服务器配置，点击【下一步】

4.进入弹性IP配置页面，选择需要的弹性IP或购买新的弹性IP，点击【下一步】

5.进入设置VPC页面，选择VPC，点击【下一步】

6.进入设置基本信息页面，填写云服务器的名称及密码等系统信息，点击【下一步】

7.进入订单确认页面，确认订单，点击【提交订单】

8.点击【返回控制台】，回到云服务器控制台

编辑安全组规则

编辑安全组规则

1.登录金山云控制台，点击导航栏【虚拟私有网络】页面下的【安全组】进入安全组控制台

2.选择VPC，选中需要配置的安全组，点击【编辑入/出站规则】

3.进入编辑安全组规则页面，添加您需要放行的安全组规则，点击【确定】，一分钟后您配置的安全规则即可生效

如需了解更多，请参考安全组（防火墙）介绍

快速搭建IPv4私有网络

虚拟私有网络

创建虚拟私有网络

1. 登录虚拟私有网络控制台。
2. 点击虚拟数据中心列表中**新建VPC**。
3. 填写完信息，点击**确定**，完成VPC创建。

删除VPC

1. 勾选需要删除的VPC，点击**删除**按钮，弹出确认删除VPC浮层。
2. 确认信息无误，点击**确认**按钮，删除成功后，会提示删除成功，删除失败，会提示删除失败并告知失败原因。

创建默认VPC

1. 点击VPC列表中**创建默认VPC**按钮，弹出创建弹窗，点击**确认**后创建。

子网

创建子网

1. 点击**新建**按钮。
2. 选择子网类型，填写信息

   云服务器子网：用于关联云服务器 终端子网：用于创建云数据库、对象存储、负载均衡等服务 裸金属服务器子网：用于关联裸金属服务器
3. 点击**确认**按钮，完成子网创建。

删除子网

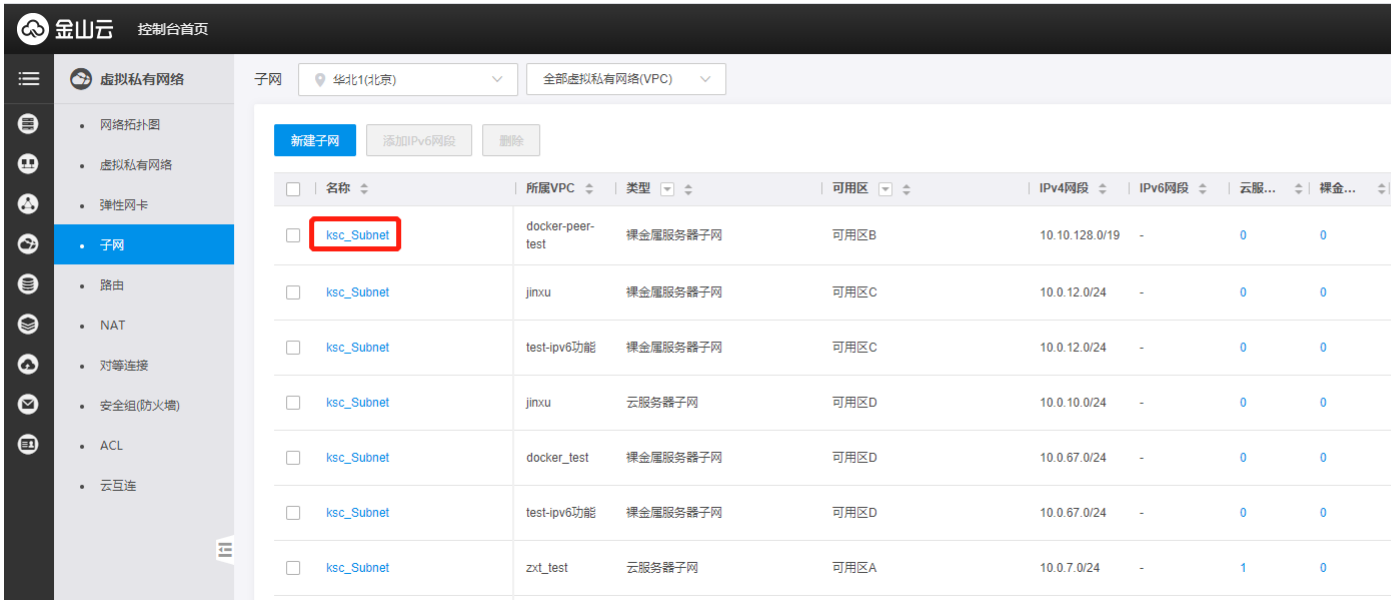
1. 选择需要删除的子网，点击**删除**按钮。
2. 缺认信息无误，点击**删除**。

修改DNS

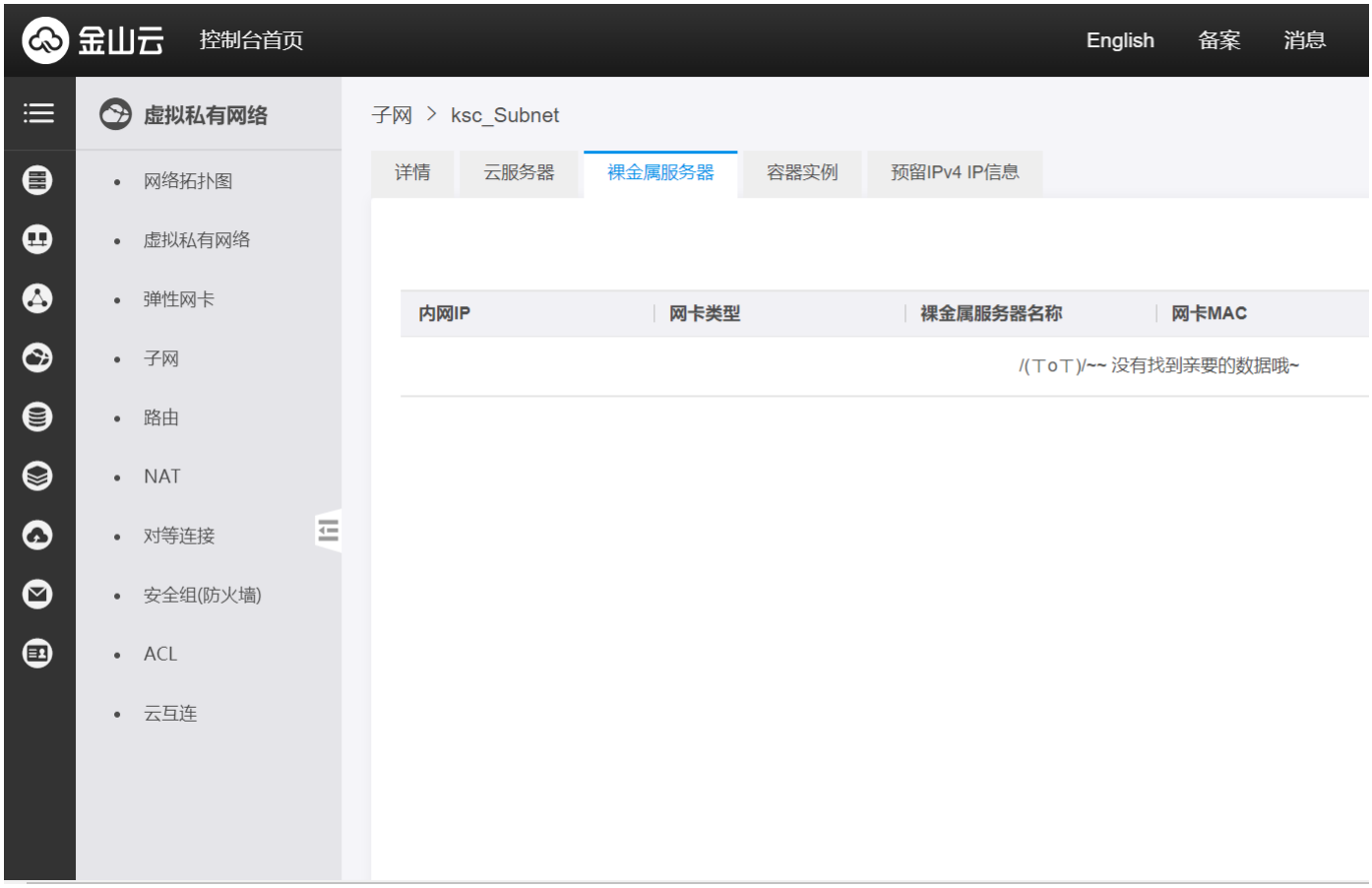
1. 点击子网列表中需要修改的DNS的编辑图标 。

查询子网下资源

1. 点击子网名称或**查看**进入子网详细信息页面



2. 选择资源类型



路由

创建虚拟私有网络后，可以在路由控制台来管理专有网络的流量。 路由表中的每一项是一条路由条目。路由条目指定了网络流量的导向目的地，由目标网段、下一跳类型、下一跳三部分组成。

创建路由

1. 点击**新建路由**。
2. 填写完信息，点击**确定**按钮，完成路由创建。

删除路由

3. 勾选需要删除的路由，点击**删除**按钮。
4. 确认信息无误，点击**确认**按钮。

NAT

- NAT网关，可提供主机的公网访问。
- 创建VPC会创建默认VPC类型的内网NAT，用于访问金山云yum源、DNS等服务。
- 映射范围是VPC类型的NAT只能创建一个，作用于整个VPC。
- 映射范围是VNET类型的NAT可以创建多个，作用于绑定的VNET。

创建NAT

1. 点击**新建NAT**
2. 填写信息，选择计费方式，点击**立即购买**

删除NAT

1. 勾选需要删除的NAT，点击**删除**
2. 确认信息无误，点击**删除**按钮

绑定子网(子网类型NAT)

1. 点击NAT名称或**查看**进入NAT详细信息页面
2. 选择绑定子网信息页面
3. 选择想要绑定的子网，点击**绑定**，即可完成子网绑定。

解绑子网(子网类型NAT)

1. 勾选需要解绑的子网，点击**解绑**按钮
2. 确认信息无误，点击**确认**

对等连接

VPC内部专线，用于两个VPC实例的网络互通。

创建对等连接

1. 点击**新建对等连接**

2. 配置以下购买信息，点击**确定**按钮，完成对等连接创建。

删除对等连接

3. 勾选需要删除的对等连接，点击**删除**
4. 确认信息无误，点击**删除**按钮

安全组

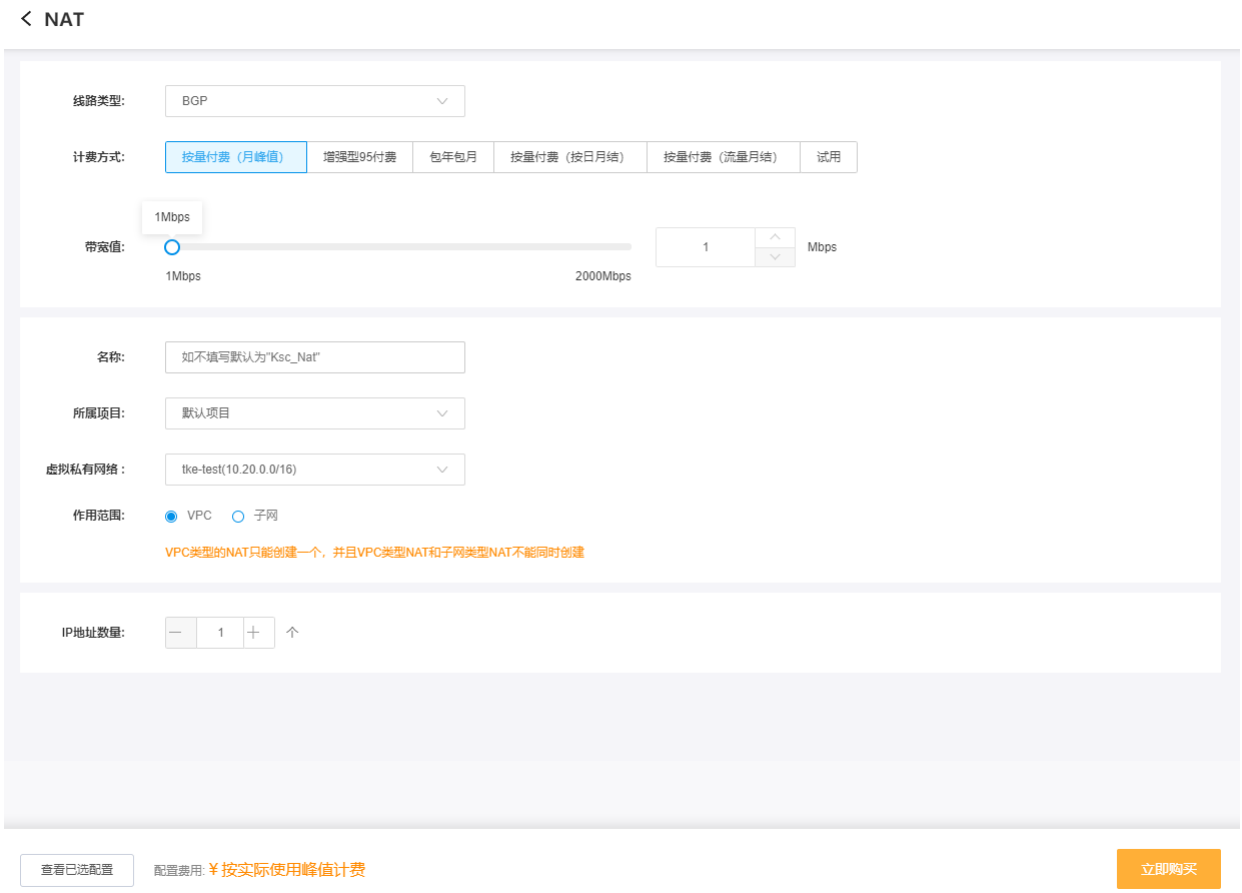
- 有状态防火墙白名单。
- 默认安全组不可删除。
- 安全组规则只作用于绑定的主机。
- 安全组规则默认黑名单。
- 安全组规则默认出站规则全部放行，用户可以删除。

管理NAT网关

创建NAT网关

1. 登录NAT网关管理控制台。
2. 在NAT网关页面，单击**新建NAT**。
3. 在创建NAT网关面板，配置购买信息，然后单击**立即购买**。

带宽值：默认可选择1-200Mbps带宽 IP地址数量：最多可支持20个IP



删除NAT网关

1. 在NAT网关页面，找到目标NAT网关
2. 点击操作列的更多操作 > **删除**，即可完成删除NAT网关。

调整带宽

1. 在NAT网关页面，找到目标NAT网关，单击操作列的**调整带宽**。
2. 选择调整后带宽，点击**立即支付**
3. 点击**提交订单**。当服务状态为已成功后，说明您购买成功。

绑定NAT IP

1. 在NAT网关页面，找到目标NAT网关，进入详情页面。
2. 在NAT IP页签，点击**添加NAT IP**，填写添加量，即可绑定IP。

解绑NAT IP

1. 在NAT网关页面，找到目标NAT网关，进入详情页面。
2. 在NAT IP页签，选中要解绑的EIP，然后单击操作列的**删除**，即可完成解绑。

创建SNAT实现访问公网服务

您可以使用NAT网关的SNAT功能，为VPC中无公网IP的云服务器提供访问互联网的代理服务。

创建SNAT条目

1. 登录NAT网关管理控制台。
2. 在NAT网关页面，找到目标NAT网关实例，单击实例名称进入详情界面。
3. 选择SNAT页签，点击**绑定**。
   - 子网粒度：指定子网的云服务器通过配置的公网IP访问互联网。
   - 主机粒度：指定的云服务器通过配置的公网IP访问互联网。

删除SNAT条目

1. 选择SNAT页签，选中目标条目，点击操作列的**删除**，即可删除目标条目。

创建DNAT提供公网服务

NAT网关支持DNAT功能，将NAT网关上的公网IP映射给云服务器使用，使云服务器能够提供互联网服务。DNAT支持端口映射和IP映射。

背景信息

1. 绑定DNAT规则的IP不允许删除。
2. DNAT端口映射，可与SNAT共享一个IP。

创建DNAT规则

1. 登录NAT网关管理控制台。
2. 在NAT网关页面，找到目标NAT网关实例，单击实例名称进入详情界面。
3. 选择DNAT页签，点击**创建DNAT规则**。
4. 在创建DNAT条目页面，配置以下参数，然后单击**确认**。

   公网IP：提供互联网通信的公网IP 私网IP：要通过DNAT规则进行公网通信的实例的私网IP 公网端口：公网IP的端口，即进行端口转发的外部端口 私网端口：私网IP的端口 协议类型：

转发端口的协议类型

IP映射

定义： NAT网关会将任何访问该公网IP的请求都将转发到目标服务器上，协议不变，端口不变。 限制： NAT网关至少需要有两个IP，且至少有一个IP未绑定端口映射规则 举例：	公网IP	公网端口	私网IP	私网端口	协议类型
11.11.11.11	Any	192.168.0.33	Any	IP	

NAT网关会将任何来自公网访问11.11.11.11的请求转发到192.168.0.33实例上。

端口映射

定义： NAT网关会将以指定协议和端口访问该公网IP的请求转发到目标服务器的指定端口上。 **限制：**

- SNAT规则不能和全端口的DNAT规则共用IP
- 绑定DNAT的端口，不能做SNAT出向源端口，如果端口正在被SNAT使用，则中断SNAT连接
- 允许绑定EIP的实例绑定DNAT。绑定EIP的主机SNAT规则不生效
- 端口映射不能与 IP 映射共享一个IP。并且需要有至少2个 IP 绑定至 NAT 网关。

举例：	公网IP	公网端口	私网IP	私网端口	协议类型
1.1.1.1	80	192.168.1.1	80	TCP	
2.2.2.2	8080	192.168.1.2	8000	UDP	

NAT网关会将访问1.1.1.1的TCP 80端口的请求转发到192.168.1.1的TCP 80端口上。 NAT网关会将访问2.2.2.2的UDP 8080端口的请求转发到192.168.1.2的UDP 8000端口上。