阿里云
NAT网关

最佳实践

文档版本：20190719

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier 字体`	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 多应用共享公网带宽

本文介绍如何通过NAT网关的DNAT功能和共享带宽功能实现多个应用共享一份公网带宽，节省公网成本。

背景信息

假设部署了四个面向互联网的应用，需要使用三个公网IP。另外需要一个ECS和一个IP作为服务器管理的跳板机来使用，并准备一个公网IP暂时备用。整体资源规划如下：

- 带宽需求总量：150Mbps
- 公网IP需求总量：5个，其中一个公网IP留作备用
- ECS需求总量：5个
- 公网IP与ECS的映射关系：
  - IP1->ECS1
  - IP2->ECS2
  - IP3->ECS3/ECS4（其中80端口映射给ECS3的80端口；443端口映射给ECS4的443端口）
  - IP4->ECS5（运维跳板机，仅开放22端口）
  - IP5：暂不添加DNAT规则

创建VPC与ECS。注意

VPC（ID: vpc-11af8lxxx）-与ECS资源相关情况如下：

> 说明:
> ECS实例不需要单独配置公网IP。

实例名称	私网IP
ECS1	192.168.1.1
ECS2	192.168.1.2
ECS3	192.168.1.3
ECS4	192.168.1.4

前提条件

1. 为了方便调用API，本教程使用了一个用Python语言编写的Command Line工具。单击此处下载CLI工具。

   Linux环境下可以直接使用wget命令进行下载。

   ```
   wget http://docs-aliyun.cn-hangzhou.oss.aliyun-inc.com/assets/attach
   /42691/cn_zh/1468947102311/api.py
   ```

2. 创建AccessKey。

   您需要为调用API的账号创建一个AccessKey，用于身份验证。详情查看创建AccessKey。

3. 为CLI工具配置AccessKey。

步骤一 创建NAT网关

1. 调用CreateNatGateway接口创建NAT网关。

   ```
   [admin@tester:xxx]$ python api.py CreateNatGateway RegionId=cn-
   shanghai VpcId=vpc-11af8lxxx BandwidthPackage.1.IpCount=4 BandwidthP
   ackage.1.Bandwidth=150 BandwidthPackage.1.Zone=cn-shanghai-a Name=
   MyNatGW Description="My first NAT Gateway"
    =====Request URL======
    https://ecs.aliyuncs.com/?SignatureVersion=1.0&VpcId=vpc-11af8lxxx
   &Name=MyNatGW&Format=json&TimeStamp=2016-05-23T03%3A26%3A21Z&
   BandwidthPackage.1.IpCount=5&RegionId=cn-shanghai&AccessKeyId=
   jZgi0oyrQXXXXXXX&SignatureMethod=HMAC-SHA1&Version=2014-05-26&
   Signature=I4KKhWgjJdImTqk4rCifAB3LbLw%3D&action=CreateNatGateway&
   SignatureNonce=1ebae49c-2096-11e6-b781-2cf0ee28adf2&BandwidthPackage
   .1.Bandwidth=150&BandwidthPackage.1.Zone=cn-shanghai-a&Description=
   My+first+NAT+Gateway
    =====Request URL end======
    ====== Got Response ======
    {
      "BandwidthPackageIds": {
        "BandwidthPackageId": [
          "bwp-11odxu2k7"
        ]
      },
      "ForwardTableIds": {
        "ForwardTableId": [
          "ftb-11tc6xgmv"
        ]
      },
      "NatGatewayId": "ngw-112za33e4",
      "RequestId": "2315DEB7-5E92-423A-91F7-4C1EC9AD97C3"
   ```

2. 调用DescribeNatGateways接口查看NAT网关的详细信息。

   ```
   [admin@tester:xxx]$ python api.py DescribeNatGateways RegionId=cn-
   shanghai VpcId=vpc-11af8lxxx
    =====Request URL======
    https://ecs.aliyuncs.com/?SignatureVersion=1.0&VpcId=vpc-11af8lxxx
   &Format=json&TimeStamp=2016-05-23T03%3A27%3A14Z&RegionId=cn-shanghai
   &AccessKeyId=jZgi0oyrQ6ihgKp9&SignatureMethod=HMAC-SHA1&Version=2014
   -05-26&Signature=JvXErso9g0fZdRTgBtNLepe%2F1e4%3D&action=DescribeNa
   tGateways&SignatureNonce=3e1424eb-2096-11e6-bc31-2cf0ee28adf2
   ```

```
 =====Request URL end======
 ====== Got Response ======
 {
   "NatGateways": {
     "NatGateway": [
       {
         "BandwidthPackageIds": {
           "BandwidthPackageId": [
             "bwp-11odxu2k7"
           ]
         },
         "BusinessStatus": "Normal",
         "CreationTime": "2016-05-23T03:26:23Z",
         "Description": "My first NAT Gateway",
         "ForwardTableIds": {
           "ForwardTableId": [
             "ftb-11tc6xgmv"
           ]
         },
         "InstanceChargeType": "PostPaid",
         "Name": "MyNatGW",
         "NatGatewayId": "ngw-112za33e4",
         "RegionId": "cn-shanghai",
         "Spec": "Small",
         "Status": "Available",
         "VpcId": "vpc-11af8lxxx"
       }
     ]
   },
   "PageNumber": 1,
   "PageSize": 10,
   "RequestId": "FE4C442C-9778-449A-BF7F-7F36C3AF5611",
   "TotalCount": 1
 }
```

3. **调用**DescribeBandwidthPackages**接口查看已创建的共享带宽包的详细信息。**

```
[admin@tester:xxx]$ python api.py DescribeBandwidthPackages RegionId
=cn-shanghai NatGatewayId=ngw-112za33e4
 =====Request URL======
 https://ecs.aliyuncs.com/?SignatureVersion=1.0&Format=json&
TimeStamp=2016-05-23T03%3A33%3A30Z&RegionId=cn-shanghai&NatGateway
Id=ngw-112za33e4&AccessKeyId=jZgi0oyrQ6ihgKp9&SignatureMethod=HMAC
-SHA1&Version=2014-05-26&Signature=KN0C2Q4TUZtfECBn1c2lOdBzrb8%3D&
action=DescribeBandwidthPackages&SignatureNonce=1e8941ae-2097-11e6-
acbb-2cf0ee28adf2
 =====Request URL end======
 ====== Got Response ======
 {
   "BandwidthPackages": {
     "BandwidthPackage": [
       {
         "Bandwidth": "150",
         "BandwidthPackageId": "bwp-11odxu2k7",
         "BusinessStatus": "Normal",
         "CreationTime": "2016-05-23T03:26:24Z",
         "Description": "",
         "InstanceChargeType": "PostPaid",
         "InternetChargeType": "PayByBandwidth",
         "IpCount": "5",
         "Name": "",
         "NatGatewayId": "ngw-112za33e4",
         "PublicIpAddresses": {
```

```
            "PublicIpAddresse": [
              {
                "AllocationId": "nateip-11iopy3sl",
                "IpAddress": "139.xxx.xx.107"
              },
              {
                "AllocationId": "nateip-11pt1f9ph",
                "IpAddress": "139.xxx.xx.55"
              },
              {
                "AllocationId": "nateip-111ul670c",
                "IpAddress": "139.xxx.xx.79"
              },
              {
                "AllocationId": "nateip-11ogfjj85",
                "IpAddress": "139.xxx.xx.59"
              },
              {
                "AllocationId": "nateip-11s2jempe",
                "IpAddress": "139.xxx.xx.58"
              }
            ]
          },
          "RegionId": "cn-shanghai",
          "Status": "Available",
          "ZoneId": "cn-shanghai-a"
        }
      ]
    },
    "PageNumber": 1,
    "PageSize": 10,
    "RequestId": "14406B86-7CA1-4907-9755-86096F476A4F",
    "TotalCount": 1
}
```


步骤二 配置DNAT

1. **调用CreateForwardEntry接口添加如下转发条目。**

公网IP	公网端口	私网IP	私网端口	协议
IP1	Any	ecs-ip1	Any	Any
IP2	Any	ecs-ip2	Any	Any
IP3	80	ecs-ip3	80	TCP
IP3	443	ecs-ip4	443	TCP
IP4	22	ecs-ip5	22	TCP


```
[admin@tester:xxx]$ python api.py CreateForwardEntry RegionId=cn
-shanghai ForwardTableId=ftb-11tc6xgmv ExternalIp=139.xxx.xx.107
ExternalPort=Any InternalIp=192.168.1.1 InternalPort=Any IpProtocol=
Any
=====Request URL======
https://ecs.aliyuncs.com/?ExternalIp=139.xxx.xx.107&SignatureV
ersion=1.0&Format=json&TimeStamp=2016-05-23T03%3A53%3A18Z&RegionId
=cn-shanghai&ExternalPort=Any&InternalIp=192.168.1.1&Signature
=iR4GSzhJQtowMJOj%2FRth3ABP4FA%3D&AccessKeyId=jZgi0oyrQ6ihgKp9&
ForwardTableId=ftb-11tc6xgmv&SignatureMethod=HMAC-SHA1&Version=
```

```
2014-05-26&IpProtocol=Any&action=CreateForwardEntry&SignatureNonce=
e2ceae11-2099-11e6-b548-2cf0ee28adf2&InternalPort=Any
=====Request URL end======
====== Got Response ======
[admin@tester:xxx]$ python api.py CreateForwardEntry RegionId=cn
-shanghai ForwardTableId=ftb-11tc6xgmv ExternalIp=139.xxx.xx.107
ExternalPort=Any InternalIp=192.168.1.1 InternalPort=Any IpProtocol=
Any
=====Request URL======
https://ecs.aliyuncs.com/?ExternalIp=139.xxx.xx.107&SignatureV
ersion=1.0&Format=json&TimeStamp=2016-05-23T03%3A53%3A18Z&RegionId
=cn-shanghai&ExternalPort=Any&InternalIp=192.168.1.1&Signature
=iR4GSzhJQtowMJOj%2FRth3ABP4FA%3D&AccessKeyId=jZgi0oyrQ6ihgKp9&
ForwardTableId=ftb-11tc6xgmv&SignatureMethod=HMAC-SHA1&Version=
2014-05-26&IpProtocol=Any&action=CreateForwardEntry&SignatureNonce=
e2ceae11-2099-11e6-b548-2cf0ee28adf2&InternalPort=Any
=====Request URL end======
====== Got Response ======
{
"ForwardEntryId": "fwd-119smw5tk",
"RequestId": "A4AEE536-A97A-40EB-9EBE-53A6948A6928"
}
[admin@tester:xxx]$
[admin@tester:xxx]$
[admin@tester:xxx]$
[admin@tester:xxx]$ python api.py CreateForwardEntry RegionId=cn
-shanghai ForwardTableId=ftb-11tc6xgmv ExternalIp=139.xxx.xx.55
ExternalPort=Any InternalIp=192.168.1.2 InternalPort=Any IpProtocol=
Any
=====Request URL======
https://ecs.aliyuncs.com/?ExternalIp=139.xxx.xx.55&SignatureVersion
=1.0&Format=json&TimeStamp=2016-05-23T03%3A53%3A42Z&RegionId=cn-
shanghai&ExternalPort=Any&InternalIp=192.168.1.2&Signature=mFBn%
2BCd4LfHkKj53MwmWyMhzyfs%3D&AccessKeyId=jZgi0oyrQ6ihgKp9&ForwardTab
leId=ftb-11tc6xgmv&SignatureMethod=HMAC-SHA1&Version=2014-05-26&
IpProtocol=Any&action=CreateForwardEntry&SignatureNonce=f09c1b38-
2099-11e6-aa80-2cf0ee28adf2&InternalPort=Any
=====Request URL end======
====== Got Response ======
{
"ForwardEntryId": "fwd-11dz3ly9l",
"RequestId": "5DBC8F86-2D76-4BF4-B839-7FF31B61D516"
}
[admin@tester:xxx]$
[admin@tester:xxx]$
[admin@tester:xxx]$
[admin@tester:xxx]$ python api.py CreateForwardEntry RegionId=cn
-shanghai ForwardTableId=ftb-11tc6xgmv ExternalIp=139.xxx.xx.79
ExternalPort=80 InternalIp=192.168.1.3 InternalPort=80 IpProtocol=
TCP
=====Request URL======
https://ecs.aliyuncs.com/?ExternalIp=139.xxx.xx.79&SignatureVersion
=1.0&Format=json&TimeStamp=2016-05-23T03%3A54%3A10Z&RegionId=cn-
shanghai&ExternalPort=80&InternalIp=192.168.1.3&Signature=OpTui3SKbA
jKXy6gKRoJb%2B9Lazg%3D&AccessKeyId=jZgi0oyrQ6ihgKp9&ForwardTab
leId=ftb-11tc6xgmv&SignatureMethod=HMAC-SHA1&Version=2014-05-26&
IpProtocol=TCP&action=CreateForwardEntry&SignatureNonce=01c41d5c-
209a-11e6-905e-2cf0ee28adf2&InternalPort=80
=====Request URL end======
====== Got Response ======
{
"ForwardEntryId": "fwd-11r23r7p5",
"RequestId": "67B7AAFD-E7AB-4EB8-AA5C-AA38CFFB4A95"
}
```

```
[admin@tester:xxx]$
[admin@tester:xxx]$
[admin@tester:xxx]$
[admin@tester:xxx]$ python api.py CreateForwardEntry RegionId=cn
-shanghai ForwardTableId=ftb-11tc6xgmv ExternalIp=139.xxx.xx.79
ExternalPort=443 InternalIp=192.168.1.4 InternalPort=443 IpProtocol=
TCP
=====Request URL======
https://ecs.aliyuncs.com/?ExternalIp=139.xxx.xx.79&SignatureVersion
=1.0&Format=json&TimeStamp=2016-05-23T03%3A55%3A22Z&RegionId=cn
-shanghai&ExternalPort=443&InternalIp=192.168.1.4&Signature=X%
2BZtHbTeKYf8xU%2FvWhPAmg%2B5scc%3D&AccessKeyId=jZgi0oyrQ6ihgKp9
&ForwardTableId=ftb-11tc6xgmv&SignatureMethod=HMAC-SHA1&Version=
2014-05-26&IpProtocol=TCP&action=CreateForwardEntry&SignatureNonce=
2c3f2573-209a-11e6-be0f-2cf0ee28adf2&InternalPort=443
=====Request URL end======
====== Got Response ======
{
"ForwardEntryId": "fwd-11cdhpjlk",
"RequestId": "260A9673-5522-4F66-844A-1F1AB47CD21C"
}
[admin@tester:xxx]$
[admin@tester:xxx]$
[admin@tester:xxx]$
[admin@tester:xxx]$ python api.py CreateForwardEntry RegionId=cn
-shanghai ForwardTableId=ftb-11tc6xgmv ExternalIp=139.xxx.xx.59
ExternalPort=22 InternalIp=192.168.1.5 InternalPort=22 IpProtocol=
TCP
=====Request URL======
https://ecs.aliyuncs.com/?ExternalIp=139.xxx.xx.59&SignatureVersion
=1.0&Format=json&TimeStamp=2016-05-23T03%3A55%3A44Z&RegionId=cn-
shanghai&ExternalPort=22&InternalIp=192.168.1.5&Signature=%2FZWf5%
2ForHr%2BUR446eEBLC4LNYe8%3D&AccessKeyId=jZgi0oyrQ6ihgKp9&ForwardTab
leId=ftb-11tc6xgmv&SignatureMethod=HMAC-SHA1&Version=2014-05-26&
IpProtocol=TCP&action=CreateForwardEntry&SignatureNonce=39863cf3-
209a-11e6-8f6d-2cf0ee28adf2&InternalPort=22
=====Request URL end======
====== Got Response ======
{
"ForwardEntryId": "fwd-11iv34uj7",
"RequestId": "0884BC12-8EAD-4AAA-826E-30E5435D7C27"
}
```

2. **调用**DescribeForwardTableEntries**接口查看已添加的DNAT条目。**

```
[admin@tester:xxx]$ python api.py DescribeForwardTableEntries
RegionId=cn-shanghai ForwardTableId=ftb-11tc6xgmv
 =====Request URL======
 https://ecs.aliyuncs.com/?SignatureVersion=1.0&Format=json&
TimeStamp=2016-05-23T03%3A56%3A18Z&RegionId=cn-shanghai&AccessKeyId
=jZgi0oyrQ6ihgKp9&ForwardTableId=ftb-11tc6xgmv&SignatureMethod=HMAC
-SHA1&Version=2014-05-26&Signature=x4%2B6oNYxIRBmND8rcIbJM9EJ8ts%3D&
action=DescribeForwardTableEntries&SignatureNonce=4db93223-209a-11e6
-81eb-2cf0ee28adf2
 =====Request URL end======
 ====== Got Response ======
 {
   "ForwardTableEntries": {
     "ForwardTableEntry": [
       {
         "ExternalIp": "139.xxx.xx.107",
         "ExternalPort": "any",
         "ForwardEntryId": "fwd-119smw5tk",
```

```
          "ForwardTableId": "ftb-11tc6xgmv",
          "InternalIp": "192.168.1.1",
          "InternalPort": "any",
          "IpProtocol": "any",
          "Status": "Available"
        },
        {
          "ExternalIp": "139.xxx.xx.79",
          "ExternalPort": "443",
          "ForwardEntryId": "fwd-11cdhpjlk",
          "ForwardTableId": "ftb-11tc6xgmv",
          "InternalIp": "192.168.1.4",
          "InternalPort": "443",
          "IpProtocol": "tcp",
          "Status": "Available"
        },
        {
          "ExternalIp": "139.xxx.xx.55",
          "ExternalPort": "any",
          "ForwardEntryId": "fwd-11dz3ly9l",
          "ForwardTableId": "ftb-11tc6xgmv",
          "InternalIp": "192.168.1.2",
          "InternalPort": "any",
          "IpProtocol": "any",
          "Status": "Available"
        },
        {
          "ExternalIp": "139.xxx.xx.59",
          "ExternalPort": "22",
          "ForwardEntryId": "fwd-11iv34uj7",
          "ForwardTableId": "ftb-11tc6xgmv",
          "InternalIp": "192.168.1.5",
          "InternalPort": "22",
          "IpProtocol": "tcp",
          "Status": "Available"
        },
        {
          "ExternalIp": "139.xxx.xx.79",
          "ExternalPort": "80",
          "ForwardEntryId": "fwd-11r23r7p5",
          "ForwardTableId": "ftb-11tc6xgmv",
          "InternalIp": "192.168.1.3",
          "InternalPort": "80",
          "IpProtocol": "tcp",
          "Status": "Available"
        }
      ]
    },
    "PageNumber": 1,
    "PageSize": 10,
    "RequestId": "C84FDDCF-8550-4024-B89C-01E7459D7CF9",
    "TotalCount": 5
}
```

2 自建SNAT网关平滑迁移到NAT网关

通过使用路由表的最长匹配原则，您可以将搭建在ECS实例的SNAT网关平滑迁移至阿里云NAT网关。

背景信息

如果您已经在VPC中基于ECS搭建了SNAT网关，又想将架构切换为基于NAT网关实现的SNAT，您可以将原有自建SNAT网关拆除，再进行NAT网关的创建和配置。但该操作会导致SNAT功能中断一段时间。

本教程的迁移方法利用路由表的一些特性（主要是“最长匹配原则”），实现从自建SNAT网关到阿里云NAT网关的无缝切换。切换过程中，不会出现SNAT功能不可用，仅在切换的一瞬间发生已有TCP连接的断开，应用进行重连即可。

本操作中作为示例的VPC和ECS配置如下：

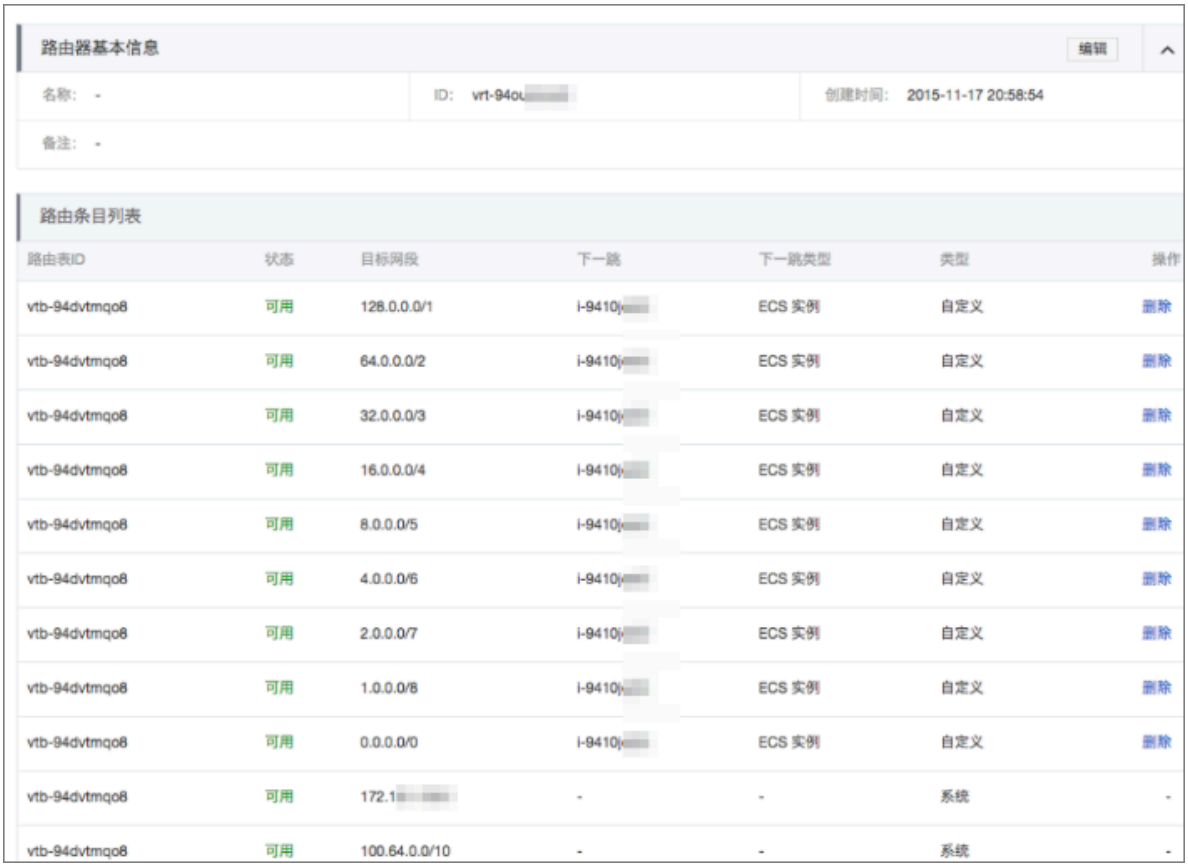
- VPC中有两个ECS实例：
  - i-9410jxxxx配置了自建的SNAT网关。这台ECS上绑定了一个EIP，并且开启了转发服务、配置了iptables规则以实现SNAT转发。
  - i-94kjwxxxx为需要SNAT功能来访问互联网的服务器。
- VPC的路由器上，添加了一条自定义路由（目标网段为0.0.0.0/0），将公网访问请求转发给i-9410jxxxx。

操作步骤

1. 在VPC中添加8条路由条目，对原有路由进行覆盖。

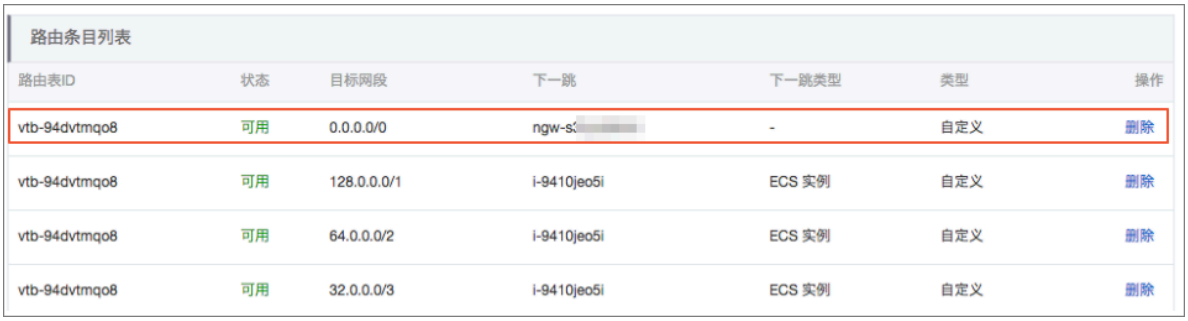
   路由条目的目标网段分别为1.0.0.0/8、2.0.0.0/7、4.0.0.0/6、8.0.0.0/5、16.0.0.0/4、32.0.0.0/3、64.0.0.0/2、128.0.0.0/1，下一跳均为i-9410jxxxx。

   由于路由表按照最长匹配原则，会优先匹配子网掩码最长的路由条目；而去往任意IP地址的数据包，都会匹配到这8条中的一条；因此，0.0.0.0/0这条路由实际上已经不再有用了。



2. 删除目标网段为0.0.0.0/0的路由条目。
3. 创建NAT网关。

   创建NAT网关后，系统会自动添加一条0.0.0.0/0的路由，指向NAT网关。



4. 绑定弹性公网IP。

   注意:

   确保EIP的带宽和自建NAT的带宽一致。因为只要在NAT网关添加了SNAT规则，SNAT规则中的ECS的出公网方向的流量就会受EIP带宽的限速。

5. 配置SNAT规则。
6. 删除VPC中添加的8条路由路由条目，使路由器把公网访问请求不再转发给自建SNAT，而是转发给NAT网关。

   至此，已经完成了从自建SNAT网关到使用官方NAT网关的SNAT功能的全部切换流程。

3 创建SNAT IP地址池

您可以在创建SNAT条目时，将多个EIP加入到一个SNAT地址池。VPC ECS实例可以随机通过SNAT地址池中的EIP访问互联网。

前提条件

- 您已经创建了专有网络和交换机。详细信息，请参见创建专有网络和交换机。
- 您已经申请了待加入到SNAT地址池的EIP。详细信息，请参见申请EIP。

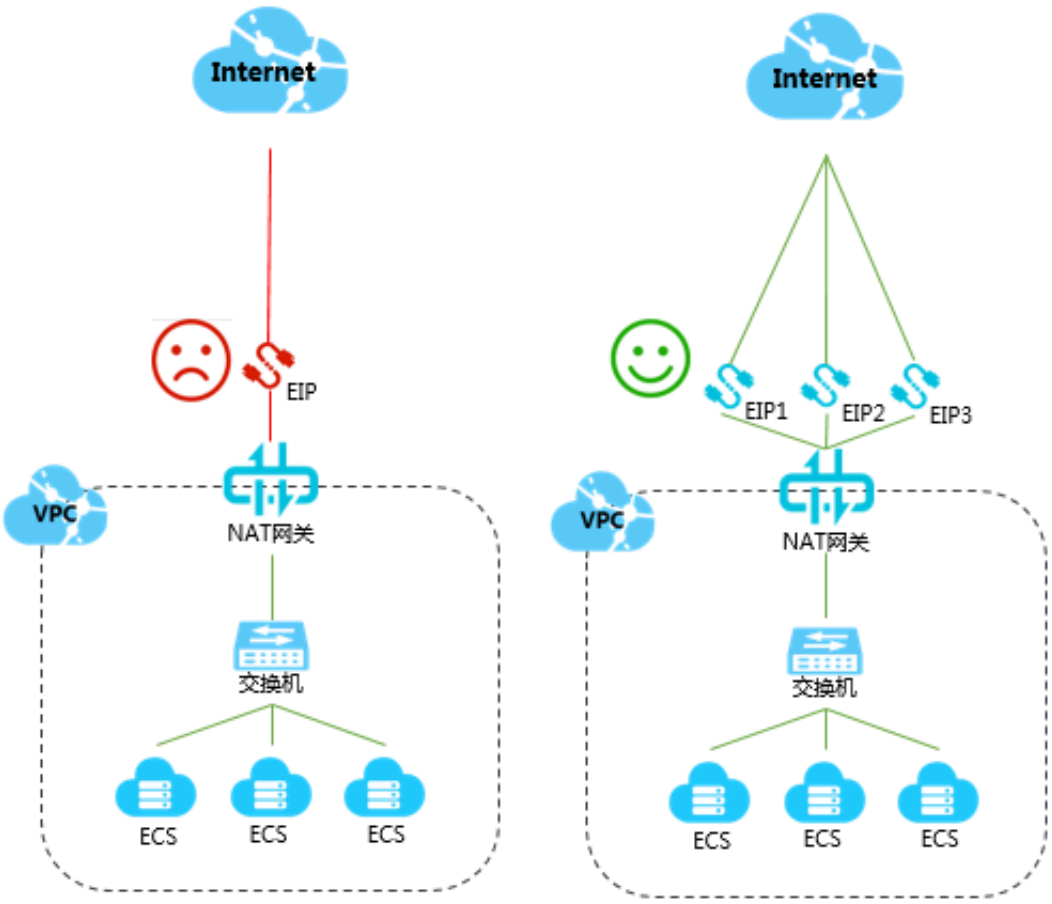
背景信息

NAT网关是一款企业级的VPC公网网关，提供SNAT功能，为VPC内无公网IP的ECS实例提供访问互联网的代理服务。如果您在创建SNAT条目时，只为指定的交换机或ECS实例配置1个EIP。当ECS实例负载激增时，1个EIP无法支撑巨大的访问量。

您可以选择添加多个EIP到一个SNAT地址池中，当VPC ECS实例主动发起对外的访问连接时，VPC ECS实例会随机通过SNAT地址池中的EIP访问互联网。

说明:

对于2017年11月3日 23：59分之前账号下存在NAT带宽包的全部用户，如想创建SNAT IP地址池，请参见创建SNAT IP地址池。



步骤一 创建NAT网关

完成以下操作，创建NAT网关。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击NAT网关。
3. 在NAT网关页面，单击创建NAT网关。
4. 在购买页面，根据以下信息，配置NAT网关并完成支付。
   - 地域：选择需要创建NAT网关的VPC所在的地域。
   - VPC ID：选择需要创建NAT网关的VPC。创建NAT网关后，不能修改VPC。

> 说明:
> 若在VPC列表中，找不到目标VPC，请从以下方面进行排查：
> - 查看该VPC是否已经配置NAT网关。一个VPC只能配置一个NAT网关。

- 查看该VPC中是否存在目标网段为0.0.0.0/0的自定义路由。若存在，需要删除该路由条目。

- 规格：选择NAT网关的规格。NAT网关的规格会影响SNAT功能的最大连接数和每秒新建连接数，但不会影响数据吞吐量。

   说明:
  NAT网关的规格对DNAT功能的连接数和吞吐量没有限制。详细信息，请参见NAT网关规格。

- 计费周期：选择NAT网关的计费周期。

步骤二 将EIP绑定到NAT网关

完成以下操作，将EIP绑定到NAT网关。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击NAT网关。
3. 选择NAT网关的地域。
4. 找到目标NAT网关实例，单击操作列下的更多操作 > 绑定弹性公网IP。
5. 在绑定弹性公网IP页面，完成以下操作，然后单击确定。
   - 从已有EIP列表选取：您可以从已有EIP列表选择EIP并绑定NAT网关。
   - 新购EIP并绑定NAT网关：系统为您创建1个后付费-按使用流量计费的EIP，并绑定到NAT网关。

    说明:
   一个NAT网关最多可绑定20个EIP（最多可绑定10个按流量计费的EIP，每个按流量计费的EIP的最大峰值不能超过200Mbps），您可以提交工单申请更多配额。
6. 重复以上步骤绑定更多EIP。

步骤三 将EIP加入共享带宽

完成以下操作，将EIP加入共享带宽。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击弹性公网IP。
3. 选择EIP的地域。
4. 在弹性公网IP页面，找到目标EIP，单击操作列下的更多操作 > 加入共享带宽。
5. 选择要加入的共享带宽，然后单击确定。

步骤四 创建SNAT条目

完成以下操作，创建SNAT条目，将多个EIP加入到一个SNAT地址池。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击NAT网关。
3. 选择NAT网关的地域。
4. 在NAT网关页面，找到目标NAT网关实例，单击操作列下的设置SNAT。
5. 在SNAT表页面，单击创建SNAT条目。
6. 在创建SNAT条目页面，根据以下信息配置SNAT条目，然后单击确定。

   以交换机为粒度：

   - 交换机：选择VPC中的交换机。该交换机下所有ECS实例都将通过SNAT功能进行公网访问。
   - 交换机网段：显示该交换机的网段。
   - 公网IP地址：选择用来提供互联网访问的公网IP。支持选择多个公网IP，多个公网IP构建SNAT IP地址池。
   - 条目名称：输入SNAT条目的名称。

   以ECS为粒度：

   - 可用ECS列表：选择VPC中的ECS实例。
   - ECS网段：显示该ECS实例的网段。
   - 公网IP地址：选择用来提供互联网访问的公网IP。支持选择多个公网IP，多个公网IP构建SNAT IP地址池。
   - 条目名称：输入SNAT条目的名称。

步骤五 测试访问

分别登录两台设置了SNAT规则的ECS实例，查看出网的源IP地址。

```
[root@iZbp135dldj2 ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.  .24  netmask 255.255.255.0  broadcast 192.168.0.255
        ether 00:16:3e:0d:28:02  txqueuelen 1000  (Ethernet)
        RX packets 24371  bytes 33686388 (32.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7572  bytes 513191 (501.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@iZbp135dldj2 ~]# curl ifconfig.me
116.  .107[root@iZbp135dldj2 ~]#
```

```
[root@iZbp18aynkjc ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.  .23  netmask 255.255.255.0  broadcast 192.168.0.255
        ether 00:16:3e:09:e4:6c  txqueuelen 1000  (Ethernet)
        RX packets 24113  bytes 33338344 (31.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7415  bytes 495113 (483.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@iZbp18aynkj ~]# curl ifconfig.me
47.  .246[root@iZbp18aynkjc ~]# _
```

4 统一公网出口IP

4.1 为已分配固定公网IP的ECS实例统一公网出口IP

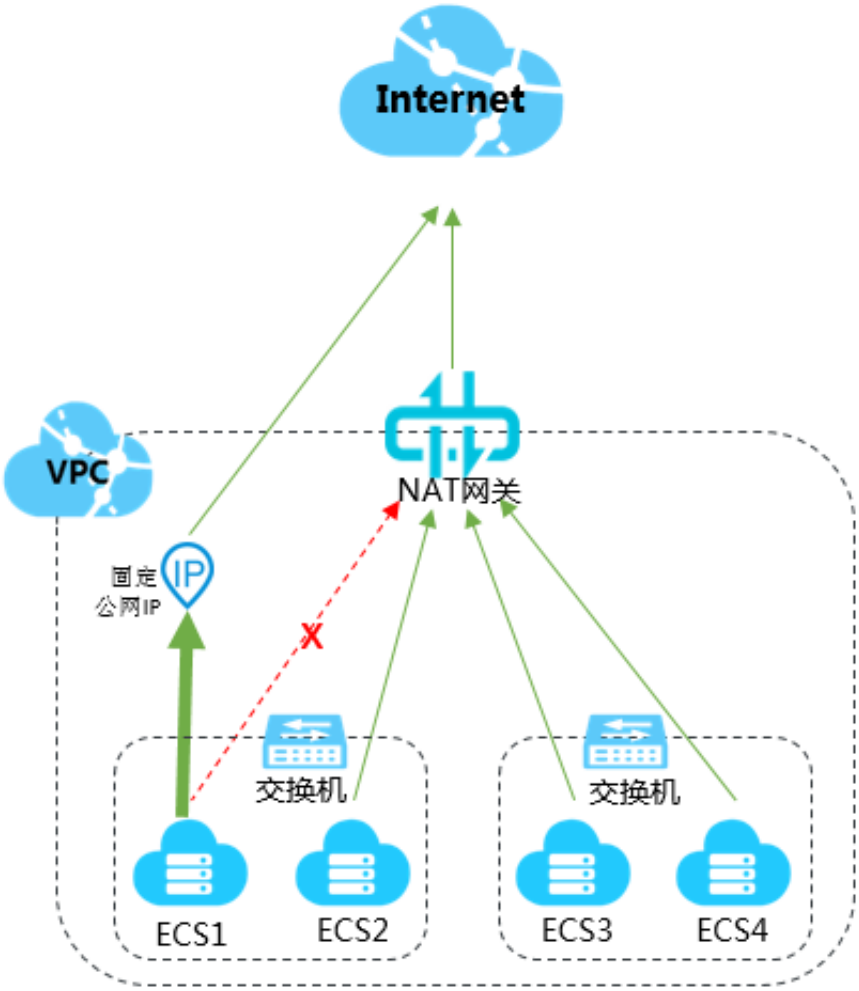
统一ECS实例的公网出口IP，有利于您更高效的管理互联网业务。本文为您介绍如何为已分配固定公网IP的ECS实例统一公网出口IP。

前提条件

分配了固定公网IP的ECS实例所在的VPC已经配置了SNAT功能。详细信息，请参见创建SNAT条目。

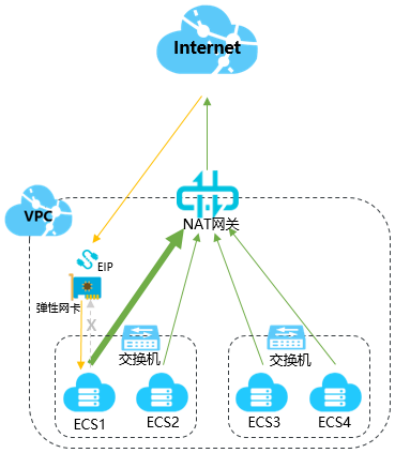
背景信息

NAT网关提供SNAT功能，为VPC内无公网IP的ECS实例提供访问互联网的代理服务。如果VPC内某些ECS实例已经分配了固定公网IP，这些ECS实例会优先通过固定公网IP访问互联网，而VPC内的其他ECS实例通过NAT网关的SNAT功能代理访问互联网，造成VPC内ECS实例的公网出口IP不一致，不利于统一管理业务。



您可以通过为ECS实例绑定弹性网卡来解决ECS实例公网出口IP不统一的问题。

如下图，您可以为ECS实例单独分配一块弹性网卡，并将固定公网IP转为EIP，然后将EIP绑定到弹性网卡，这样来自互联网的访问流量会经过弹性网卡到达ECS实例，当ECS实例需要访问互联网时会通过NAT网关进行转发。



步骤一 固定公网IP转EIP

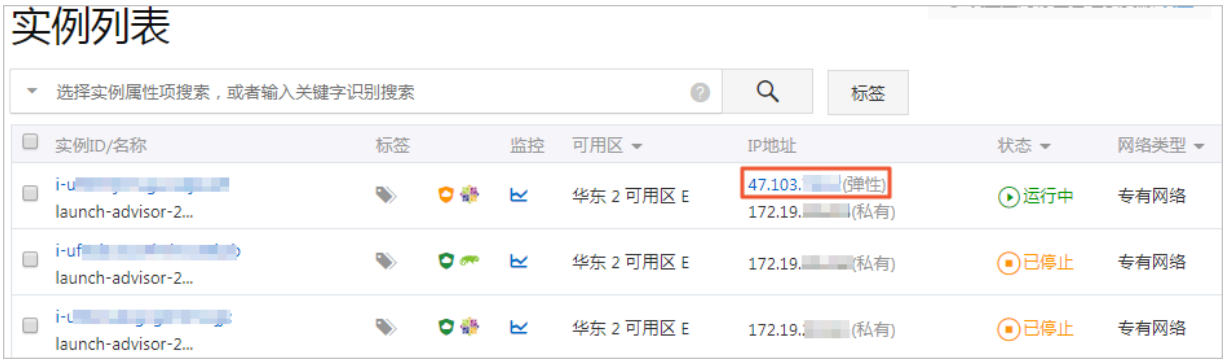
不同计费模式的ECS实例，对固定公网IP转EIP的支持不同：

- 后付费类型的ECS实例，支持直接将固定公网IP转为EIP。
- 预付费类型的ECS实例，不支持直接将固定公网IP转为EIP。您需要先将预付费ECS实例转为后付费ECS实例，再将后付费ECS实例的固定公网IP转为EIP。预付费ECS实例转为后付费ECS实例的详细操作说明，请参见预付费转后付费。

完成以下操作，将后付费ECS实例的固定公网IP转为EIP。

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏，单击实例。
3. 选择ECS实例的地域。
4. 在实例列表页面，找到目标ECS实例，单击操作列下的更多 > 网络和安全组 > 公网IP转换为弹性公网IP。
5. 在弹出的对话框中，单击确定。
6. 刷新实例列表。

   转换成功后，原来的公网IP地址会标注为弹性。



步骤二 创建弹性网卡

完成以下操作，为ECS实例创建弹性网卡。

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏，单击网络与安全 > 弹性网卡。
3. 选择弹性网卡的地域。

   说明:
   弹性网卡的地域必须与ECS实例的地域相同。

4. 在网卡列表页面，单击创建弹性网卡。

5. 在创建弹性网卡页面，根据以下信息配置弹性网卡，然后单击确定。
   - 网卡名称：输入弹性网卡的名称。
   - 专有网络：选择ECS实例所在的专有网络。
   - 交换机：选择ECS实例所在可用区的交换机。
   - 主私网IP（可选）：输入弹性网卡的主私网IPv4地址。此IPv4地址必须属于交换机的CIDR网段中的空闲地址。如果您没有指定，创建弹性网卡时将自动为您分配一个空闲的私网IPv4地址。
   - 安全组：选择当前专有网络的一个安全组。
   - 描述（可选）：输入对弹性网卡的描述。

步骤三 将弹性网卡绑定到ECS实例

完成以下操作，将弹性网卡绑定到ECS实例。

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏中，选择网络与安全 > 弹性网卡。
3. 选择弹性网卡的地域。
4. 在网卡列表页面，找到目标弹性网卡，单击操作列下的绑定实例。
5. 在弹出的对话框中，选择要绑定的ECS实例，然后单击确定。

步骤四 将EIP与ECS实例解绑

完成以下操作，将EIP与ECS实例解绑。

1. 登录专有网络管理控制台
2. 在左侧导航栏，单击弹性公网IP。
3. 选择弹性公网IP的地域。
4. 在弹性公网IP页面，找到目标弹性公网IP，单击操作列下的解绑。
5. 在弹出的对话框中，单击确定。

步骤五 将EIP绑定到弹性网卡

完成以下操作，将EIP绑定到弹性网卡。

1. 登录专有网络管理控制台
2. 在左侧导航栏，单击弹性公网IP。
3. 选择弹性公网IP的地域。
4. 在弹性公网IP页面，找到目标弹性公网IP，单击操作列下的绑定。

5. 在绑定弹性公网IP页面，根据以下信息绑定EIP至弹性网卡，然后单击确定。
   - IP地址：显示弹性公网IP地址。
   - 实例类型：选择辅助弹性网卡。
   - 资源组（可选）：选择该弹性公网IP所属的资源组。
   - 绑定模式（可选）：选择弹性公网IP绑定模式。
   - 辅助弹性网卡：选择要绑定的辅助弹性网卡。

步骤六 测试网络连通性

完成以下操作，测试互联网是否可以通过弹性网卡绑定的EIP访问ECS实例。本操作以本地Linux设备远程连接Linux实例为例。

> 说明:
> 远程连接Linux实例，Linux实例的安全组必须放行SSH（22）端口。详细信息，请参见添加安全组规则。

1. 登录本地Linux设备。
2. 执行`ssh root@公网IP`命令，然后输入Linux实例的登录密码，查看是否可以远程连接到实例。

   若界面上出现`Welcome to Alibaba Cloud Elastic Compute Service!`时，表示您已经成功连接到实例。

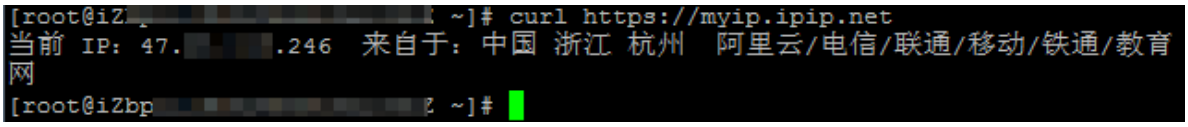
```
[root@i                    ~]# ssh root@121.      .167
The authenticity of host '121.      .167 (121.      .167)' can't be established.
ECDSA key fingerprint is SHA256:Pe06gOYOezJFP5JrQv2KRBPcmAgwr+aeB0OKhOCy640.
ECDSA key fingerprint is MD5:59:f7:ad:1b:a6:ff:8b:69:ba:6d:2c:bd:96:83:b9:58.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '121.      .167' (ECDSA) to the list of known hosts.
root@121.      .167's password:
Last login: Tue Jun 18 13:39:54 2019 from 42.      .101

Welcome to Alibaba Cloud Elastic Compute Service !

[root@iZbp13ik2oh85c4i9jmzcwZ ~]#
```

完成以下操作，测试ECS实例是否可以通过NAT网关的SNAT功能主动访问互联网。本操作以在linux实例上查看公网出口IP为例。

1. 登录ECS实例。

2. 执行`curl https://myip.ipip.net`查看公网出口IP。

   若公网出口IP与NAT网关SNAT条目中的IP一致，即ECS实例优先通过NAT网关的SNAT功能主动访问互联网。



4.2 为已绑定EIP的ECS实例统一公网出口IP

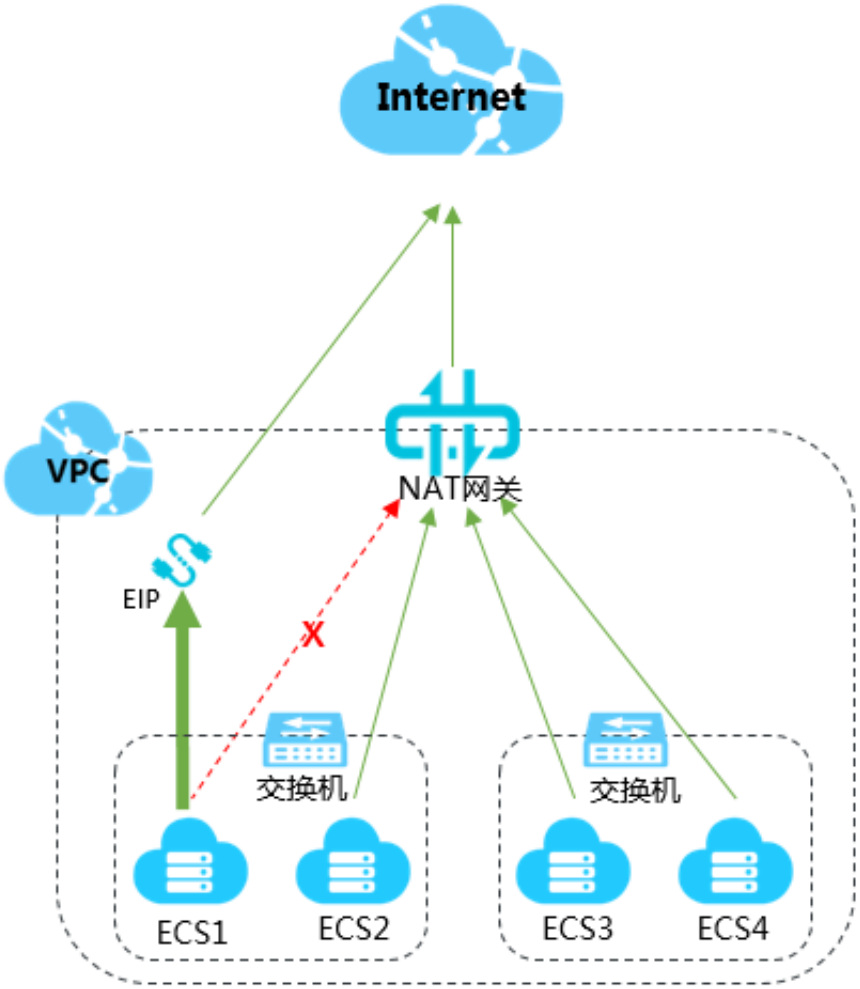
统一ECS实例的公网出口IP，有利于您更高效的管理互联网业务。本文为您介绍如何为已绑定EIP的ECS实例统一公网出口IP。

前提条件

绑定了EIP的ECS实例所在的VPC已经配置了SNAT功能。详细信息，请参见创建SNAT条目。

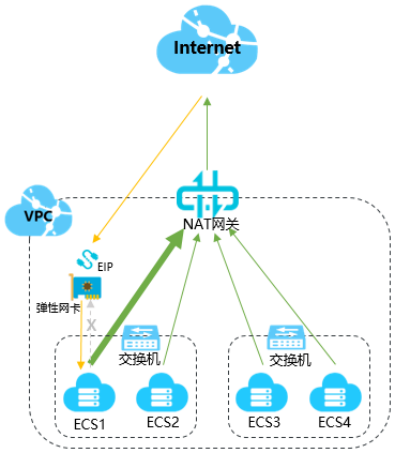
背景信息

NAT网关提供SNAT功能，为VPC内无公网IP的ECS实例提供访问互联网的代理服务。如果VPC内某些ECS实例已经绑定了EIP，这些ECS实例会优先通过绑定的EIP访问互联网，而VPC内的其他ECS实例通过NAT网关的SNAT功能代理访问互联网，造成VPC内ECS实例的公网出口IP不一致，不利于统一管理业务。



您可以通过为ECS实例绑定弹性网卡来解决ECS实例公网出口IP不统一的问题。

如下图，您可以为ECS实例单独分配一块弹性网卡，并将EIP绑定到弹性网卡，这样来自互联网的访问流量会经过弹性网卡到达ECS实例，当ECS实例需要访问互联网时会通过NAT网关进行转发。



步骤一 创建弹性网卡

完成以下操作，为ECS实例创建弹性网卡。

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏，单击网络与安全 > 弹性网卡。
3. 选择弹性网卡的地域。

   
   说明:
   弹性网卡的地域必须与ECS实例的地域相同。
4. 在网卡列表页面，单击创建弹性网卡。
5. 在创建弹性网卡页面，根据以下信息配置弹性网卡，然后单击确定。
   - 网卡名称：输入弹性网卡的名称。
   - 专有网络：选择ECS实例所在的专有网络。
   - 交换机：选择ECS实例所在可用区的交换机。
   - 主私网IP（可选）：输入弹性网卡的主私网IPv4地址。此IPv4地址必须属于交换机的CIDR网段中的空闲地址。如果您没有指定，创建弹性网卡时将自动为您分配一个空闲的私网IPv4地址。
   - 安全组：选择当前专有网络的一个安全组。
   - 描述（可选）：输入对弹性网卡的描述。

步骤二 将弹性网卡绑定到ECS实例

完成以下操作，将弹性网卡绑定到ECS实例。

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏中，选择网络与安全 > 弹性网卡。
3. 选择弹性网卡的地域。
4. 在网卡列表页面，找到目标弹性网卡，单击操作列下的绑定实例。
5. 在弹出的对话框中，选择要绑定的ECS实例，然后单击确定。

步骤三 将EIP与ECS实例解绑

完成以下操作，将EIP与ECS实例解绑。

1. 登录专有网络管理控制台
2. 在左侧导航栏，单击弹性公网IP。
3. 选择弹性公网IP的地域。
4. 在弹性公网IP页面，找到目标弹性公网IP，单击操作列下的解绑。
5. 在弹出的对话框中，单击确定。

步骤四 将EIP绑定到弹性网卡

完成以下操作，将EIP绑定到弹性网卡。

1. 登录专有网络管理控制台
2. 在左侧导航栏，单击弹性公网IP。
3. 选择弹性公网IP的地域。
4. 在弹性公网IP页面，找到目标弹性公网IP，单击操作列下的绑定。
5. 在绑定弹性公网IP页面，根据以下信息绑定EIP至弹性网卡，然后单击确定。
   - IP地址：显示弹性公网IP地址。
   - 实例类型：选择辅助弹性网卡。
   - 资源组（可选）：选择该弹性公网IP所属的资源组。
   - 绑定模式（可选）：选择弹性公网IP绑定模式。
   - 辅助弹性网卡：选择要绑定的辅助弹性网卡。

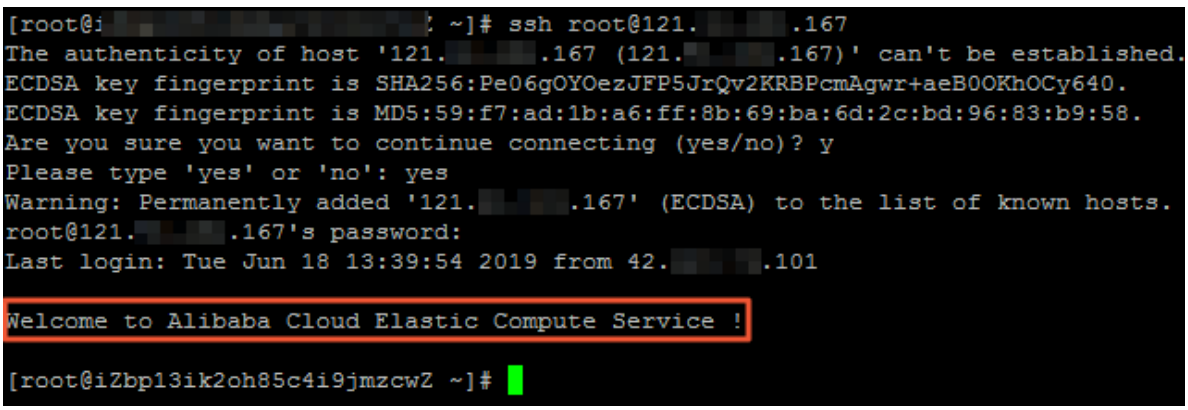
步骤五 测试网络连通性

完成以下操作，测试互联网是否可以通过弹性网卡绑定的EIP访问ECS实例。本操作以本地Linux设备远程连接Linux实例为例。

> 说明:
> 远程连接Linux实例，Linux实例的安全组必须放行SSH（22）端口。详细信息，请参见添加安全组规则。

1. 登录本地Linux设备。
2. 执行`ssh root@公网IP`命令，然后输入Linux实例的登录密码，查看是否可以远程连接到实例。

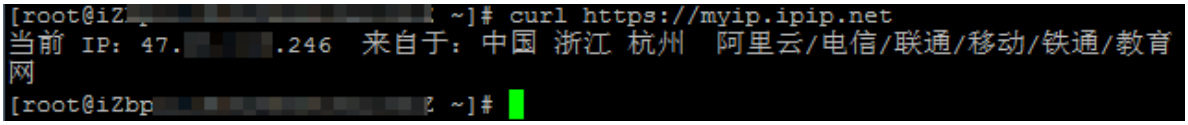
   若界面上出现`Welcome to Alibaba Cloud Elastic Compute Service!`时，表示您已经成功连接到实例。



完成以下操作，测试ECS实例是否可以通过NAT网关的SNAT功能主动访问互联网。本操作以在linux实例上查看公网出口IP为例。

1. 登录ECS实例。
2. 执行`curl https://myip.ipip.net`查看公网出口IP。

   若公网出口IP与NAT网关SNAT条目中的IP一致，即ECS实例优先通过NAT网关的SNAT功能主动访问互联网。



4.3 为设置了DNAT IP映射的ECS实例统一公网出口IP

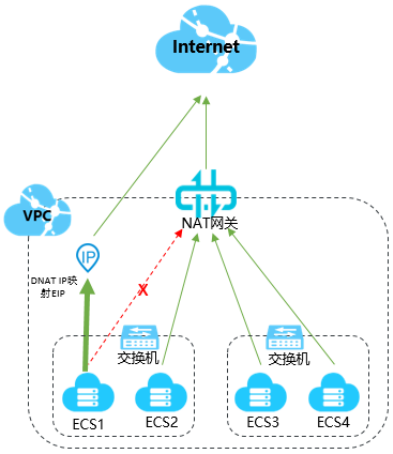
统一ECS实例的公网出口IP，有利于您更高效的管理互联网业务。本文为您介绍如何为设置了DNAT IP映射的ECS实例统一公网出口IP。

前提条件

设置了DNAT IP映射的ECS实例所在的VPC已经配置了SNAT功能。详细信息，请参见创建SNAT条目。

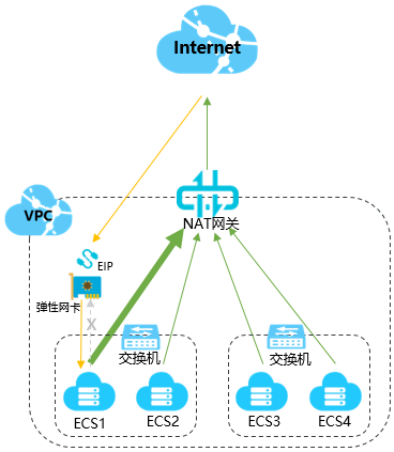
背景信息

NAT网关提供SNAT功能，为VPC内无公网IP的ECS实例提供访问互联网的代理服务。如果VPC内某些ECS实例已经设置了DNAT IP映射（IP映射即所有端口映射），这些ECS实例会优先通过DNAT条目中的公网IP访问互联网，而VPC内的其他ECS实例通过NAT网关的SNAT功能代理访问互联网，造成VPC内ECS实例的公网出口IP不一致，不利于统一管理业务。



您可以通过为ECS实例绑定弹性网卡来解决ECS实例公网出口IP不统一的问题。

如下图，您可以为ECS实例单独分配一块弹性网卡，然后移除NAT网关中的DNAT IP映射条目并创建新的DNAT条目，建立NAT网关上的公网IP与弹性网卡的映射关系，这样来自互联网的访问流量会经过弹性网卡到达ECS实例，当ECS实例需要访问互联网时会通过NAT网关进行转发。



步骤一 创建弹性网卡

完成以下操作，为ECS实例创建弹性网卡。

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏，单击网络与安全 > 弹性网卡。
3. 选择弹性网卡的地域。

> 说明:
> 弹性网卡的地域必须与ECS实例的地域相同。

4. 在网卡列表页面，单击创建弹性网卡。
5. 在创建弹性网卡页面，根据以下信息配置弹性网卡，然后单击确定。
   - 网卡名称：输入弹性网卡的名称。
   - 专有网络：选择ECS实例所在的专有网络。
   - 交换机：选择ECS实例所在可用区的交换机。
   - 主私网IP（可选）：输入弹性网卡的主私网IPv4地址。此IPv4地址必须属于交换机的CIDR网段中的空闲地址。如果您没有指定，创建弹性网卡时将自动为您分配一个空闲的私网IPv4地址。
   - 安全组：选择当前专有网络的一个安全组。
   - 描述（可选）：输入对弹性网卡的描述。

步骤二 将弹性网卡绑定到ECS实例

完成以下操作，将弹性网卡绑定到ECS实例。

1. 登录云服务器ECS管理控制台。
2. 在左侧导航栏中，选择网络与安全 > 弹性网卡。
3. 选择弹性网卡的地域。
4. 在网卡列表页面，找到目标弹性网卡，单击操作列下的绑定实例。
5. 在弹出的对话框中，选择要绑定的ECS实例，然后单击确定。

步骤三 移除DNAT IP映射

完成以下操作，移除NAT网关中的DNAT IP映射条目。

1. 登录专有网络管理控制台
2. 在左侧导航栏，单击NAT网关。
3. 选择NAT网关的地域。
4. 在NAT网关页面，找到目标NAT网关实例，单击操作列下的设置DNAT。
5. 在DNAT表页面，找到目标DNAT条目，单击操作列下的移除。
6. 在弹出的对话框中，单击确定。

步骤四 创建DNAT条目

完成以下操作，创建DNAT条目，建立NAT网关上的公网IP与弹性网卡的映射关系。

1. 登录专有网络管理控制台
2. 在左侧导航栏，单击NAT网关。
3. 在NAT网关页面，找到目标NAT网关实例，单击操作列下的设置DNAT。
4. 在DNAT表页面，单击创建DNAT条目
5. 在创建DNAT条目页面，根据以下信息配置DNAT条目，然后单击确定。
   - 公网IP地址：选择一个可用的公网IP。用于创建SNAT条目的公网IP不能再用来创建DNAT条目。
   - 私网IP地址：选择弹性网卡实例。
   - 端口设置：选择所有端口。
   - 条目名称：输入DNAT条目的名称。

步骤五 测试网络连通性

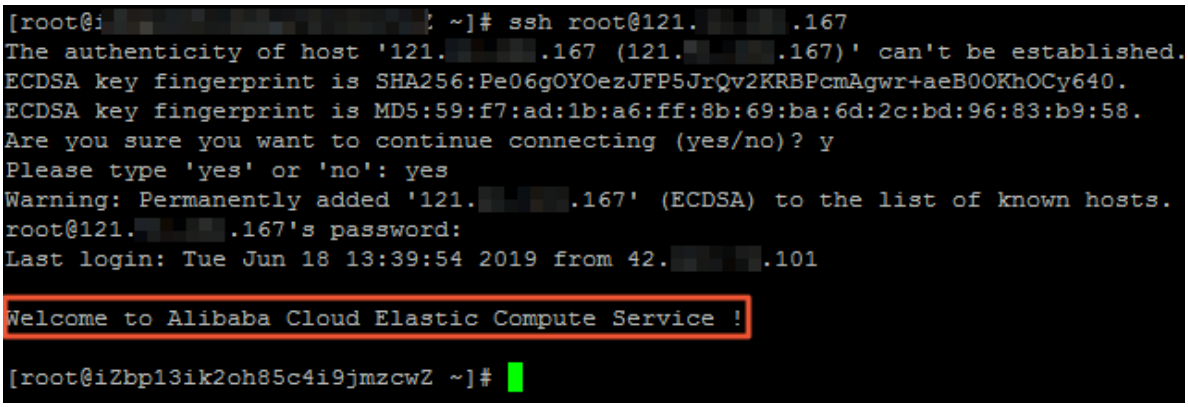
完成以下操作，测试互联网是否可以通过弹性网卡绑定的EIP访问ECS实例。本操作以本地Linux设备远程连接Linux实例为例。

说明:

远程连接Linux实例，Linux实例的安全组必须放行SSH（22）端口。详细信息，请参见添加安全组规则。

1. 登录本地Linux设备。
2. 执行`ssh root@公网IP`命令，然后输入Linux实例的登录密码，查看是否可以远程连接到实例。

   若界面上出现`Welcome to Alibaba Cloud Elastic Compute Service!`时，表示您已经成功连接到实例。



完成以下操作，测试ECS实例是否可以通过NAT网关的SNAT功能主动访问互联网。本操作以在linux实例上查看公网出口IP为例。

1. 登录ECS实例。
2. 执行`curl https://myip.ipip.net`查看公网出口IP。

   若公网出口IP与NAT网关SNAT条目中的IP一致，即ECS实例优先通过NAT网关的SNAT功能主动访问互联网。