

NAT 网关

# 用户指南

文档版本 01  
发布日期 2025-01-10



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 目录

<b>1 产品介绍</b>	<b>1</b>
1.1 什么是 NAT 网关	1
1.2 产品优势	4
1.3 应用场景	5
1.4 产品规格	9
1.5 约束与限制	10
1.6 权限管理	11
1.7 区域和可用区	14
1.8 基本概念	15
<b>2 快速入门</b>	<b>16</b>
2.1 通过公网 NAT 网关的 SNAT 规则访问公网	16
2.2 通过公网 NAT 网关的 DNAT 规则面向公网提供服务	19
2.3 通过私网 NAT 网关实现云上云下互通	24
<b>3 公网 NAT 网关</b>	<b>29</b>
3.1 公网 NAT 网关简介	29
3.2 创建公网 NAT 网关	30
3.3 管理公网 NAT 网关	32
3.4 管理 SNAT 规则	32
3.4.1 添加 SNAT 规则	33
3.4.2 修改 SNAT 规则	34
3.4.3 删除 SNAT 规则	34
3.5 管理 DNAT 规则	35
3.5.1 添加 DNAT 规则	35
3.5.2 修改 DNAT 规则	37
3.5.3 删除 DNAT 规则	37
3.5.4 批量删除 DNAT 规则	38
3.5.5 DNAT 规则模板导入导出	38
<b>4 私网 NAT 网关</b>	<b>41</b>
4.1 私网 NAT 网关简介	41
4.2 创建私网 NAT 网关	44
4.3 管理私网 NAT 网关	45
4.4 管理 SNAT 规则	46

4.4.1 添加 SNAT 规则.....	46
4.4.2 修改 SNAT 规则.....	47
4.4.3 删除 SNAT 规则.....	47
4.5 管理 DNAT 规则.....	47
4.5.1 添加 DNAT 规则.....	48
4.5.2 修改 DNAT 规则.....	49
4.5.3 删除 DNAT 规则.....	50
4.6 管理中转 IP.....	50
4.6.1 创建中转 IP.....	50
4.6.2 查看中转 IP.....	51
4.6.3 删除中转 IP.....	51
4.7 连接 IDC 或其他虚拟私有云.....	52
<b>5 权限管理.....</b>	<b>53</b>
5.1 创建用户并授权使用 NAT 网关.....	53
5.2 NAT 网关自定义策略.....	54
<b>6 使用 CES 监控 NAT 网关.....</b>	<b>56</b>
6.1 支持的监控指标.....	56
6.2 创建告警规则.....	59
6.3 查看监控指标.....	59
<b>7 常见问题.....</b>	<b>60</b>
7.1 公网 NAT 网关.....	60
7.1.1 公网 NAT 网关、弹性公网 IP 带宽、VPC 内弹性云服务器与 VPC 是什么样的关系? .....	60
7.1.2 公网 NAT 网关如何实现高可用性? .....	60
7.1.3 公网 NAT 网关丢包数超限 (EIP 端口分配超限) 怎么办? .....	60
7.2 私网 NAT 网关.....	60
7.2.1 私网 NAT 配置后组网不通怎么排查? .....	60
7.2.2 一个 VPC 最多支持创建多少个私网 NAT? .....	61
7.2.3 私网 NAT 支持云专线的 IP 转换吗? .....	61
7.2.4 私网 NAT 和公网 NAT 有什么区别? .....	61
7.2.5 私网 NAT 是否支持跨账号使用? .....	62
7.3 SNAT 规则.....	62
7.3.1 为什么使用 SNAT? .....	62
7.3.2 什么是 SNAT 连接数? .....	62
7.4 DNAT 规则.....	62
7.4.1 为什么使用 DNAT? .....	62
7.4.2 DNAT 规则是否支持更新操作? .....	63
<b>A 修订记录.....</b>	<b>64</b>

# 1 产品介绍

## 1.1 什么是 NAT 网关

NAT网关可为您提供网络地址转换服务，分为公网NAT网关和私网NAT网关。

### 公网 NAT 网关

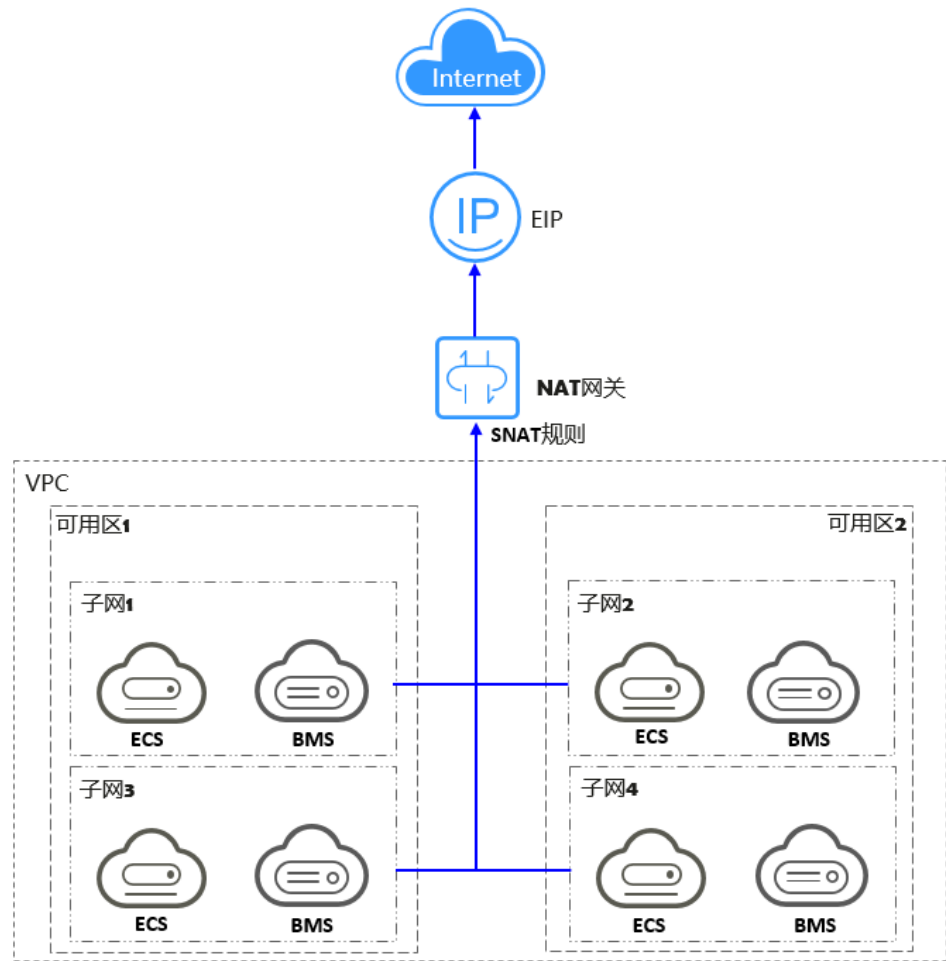
公网NAT网关（Public NAT Gateway）能够为虚拟私有云内的云主机（弹性云服务器、裸金属服务器）或者通过云专线/VPN接入虚拟私有云的本地数据中心的服务器，提供最高20Gbit/s能力的网络地址转换服务，使多个云主机可以共享弹性公网IP访问Internet或使云主机提供互联网服务。

公网NAT网关分为SNAT和DNAT两个功能。

- SNAT功能通过绑定弹性公网IP，实现私有IP向公有IP的转换，可实现VPC内跨可用区的多个云主机共享弹性公网IP，安全，高效的访问互联网。

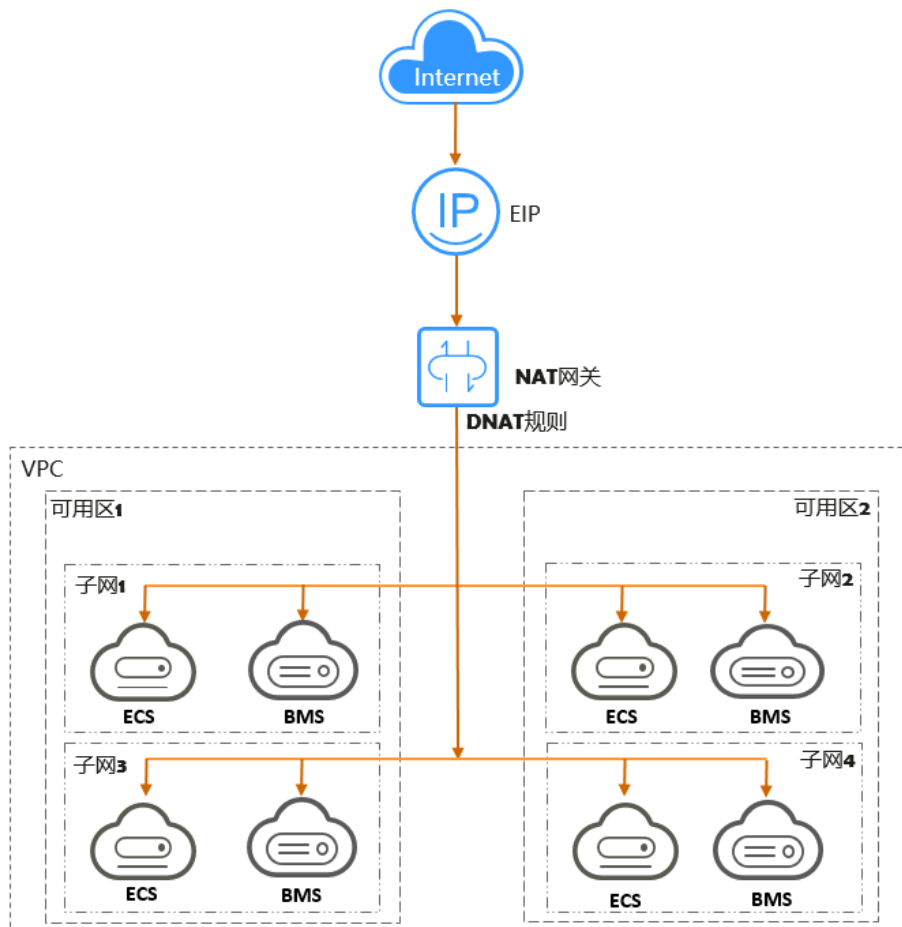
SNAT架构如[图1-1](#)所示。

图 1-1 SNAT 架构图



- DNAT功能绑定弹性公网IP，可通过IP映射或端口映射两种方式，实现VPC内跨可用区的多个云主机共享弹性公网IP，为互联网提供服务。DNAT架构如图1-2所示。

图 1-2 DNAT 架构图



## 私网 NAT 网关

私网NAT网关（Private NAT Gateway），能够为虚拟私有云内的云主机（弹性云服务器、裸金属服务器）提供私网地址转换服务。您可以在私网NAT网关上配置SNAT、DNAT规则，可将源、目的网段地址转换为中转IP，通过使用中转IP实现VPC内的云主机与其他VPC、云下IDC互访。

私网NAT网关分为SNAT和DNAT两个功能：

- SNAT功能通过绑定中转IP，可实现VPC内跨可用区的多个云主机共享中转IP，访问外部数据中心或其他VPC。
- DNAT功能通过绑定中转IP，可实现IP映射或端口映射，使VPC内跨可用区的多个云主机共享中转IP，为外部私网提供服务。

### 中转子网

中转子网相当于一个中转网络，是中转IP所属的子网。

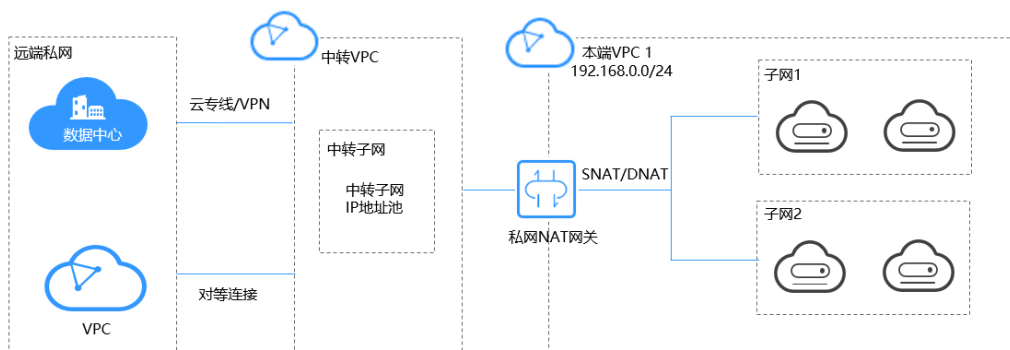
### 中转IP

您可以在中转子网中创建私网IP，即中转IP，使本端VPC中的云主机可以共享该私网IP（中转IP）访问用户IDC或其他远端VPC。

### 中转VPC

中转子网所在VPC。

图 1-3 私网 NAT 网关



## 如何访问 NAT 网关

通过管理控制台、基于HTTPS请求的API（Application Programming Interface）两种方式访问NAT网关。

- **管理控制台方式**  
管理控制台是网页形式的，您可以使用直观的界面进行相应的操作。登录管理控制台，从主页选择“NAT网关”。
- **API方式**  
如果您需要将云平台上的NAT网关集成到您自己的系统，请使用API方式访问NAT网关。

## 1.2 产品优势

### 公网 NAT 网关优势

- **灵活部署**  
支持跨子网部署和跨可用区域部署。公网NAT网关支持跨可用区部署，可用性高，单个可用区的任何故障都不会影响公网NAT网关的业务连续性。公网NAT网关的规格、弹性公网IP，均可以随时调整。
- **多样易用**  
多种网关规格可灵活选择。对公网NAT网关进行简单配置后，即可使用，运维简单，快速发放，即开即用，运行稳定可靠。
- **降低成本**  
多个云主机共享使用弹性公网IP。当您的私有IP地址通过公网NAT网关发送数据，或您的应用面向互联网提供服务时，公网NAT网关服务将私有地址和公网地址进行转换。用户无需为云主机访问Internet创建多余的弹性公网IP和带宽资源，多个云主机共享使用弹性公网IP，有效降低成本。

### 私网 NAT 网关优势

- **简规划**



大企业不同部门间存在大量重叠网段，上云后无法互通，需要在上云前进行企业网络的重新规划。云平台的私网NAT网关服务，支持重叠网段通信，客户可保留原有组网上云、无需重新规划，极大简化了IDC上云的网络规划。

- **易运维管理**

因为组织层级、分权分域、安全隔离等因素，大型企业内不同归属的部门存在分级组网，需要映射至大网才能彼此通信。私网NAT支持私网的IP地址映射，各部门的网段可映射至统一的VPC大网地址进行统一管理，让复杂组网的管理更加简易。

- **高安全**

针对企业各部门间不同的密级，私网NAT支持暴露限定网段的IP和端口，隔离高安全等级的业务。因为安全受限等原因，行业监管部门要求各机构和单位按指定IP地址接入，私网NAT可满足行业监管要求，将私网IP映射为指定IP进行接入。

- **零冲突**

企业多部门间业务隔离，常常使用同一个私网网段，迁移上云后极易冲突。基于私网NAT网关的大小网映射能力，可支持云上的重叠网段互通，助力客户上云后网络零冲突。

## 1.3 应用场景

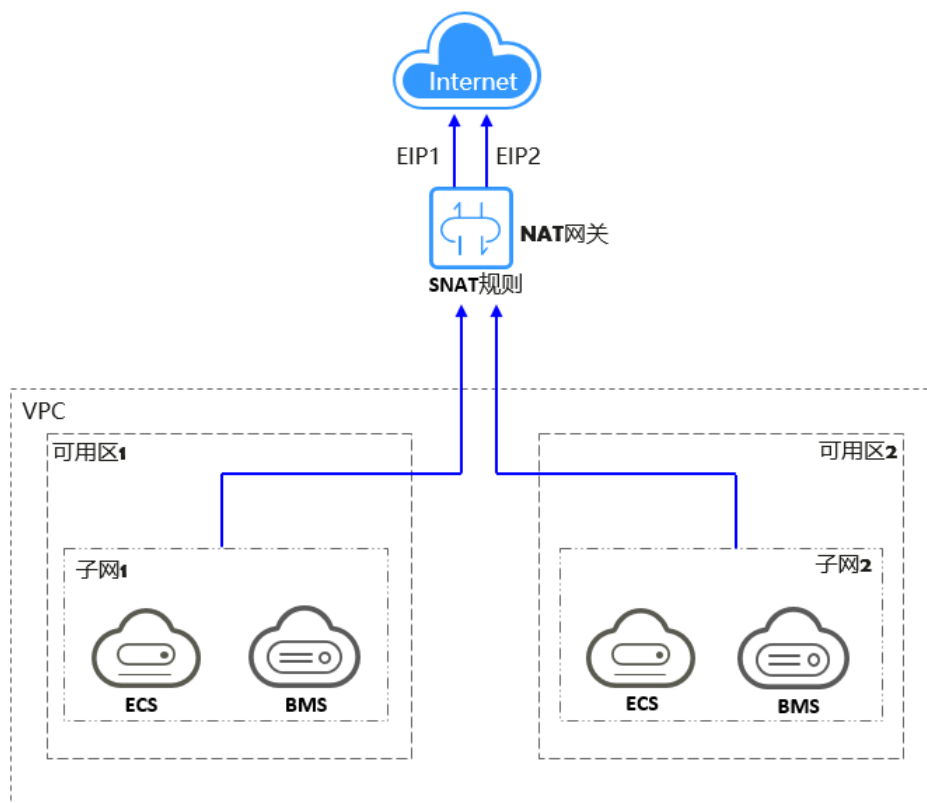
### 公网 NAT 网关

- **使用SNAT访问公网**

当VPC内的云主机需要访问公网，请求量大时，为了节省弹性公网IP资源并且避免云主机IP直接暴露在公网上，您可以使用公网NAT网关的SNAT功能。VPC中一个子网对应一条SNAT规则，一条SNAT规则可以配置多个弹性公网IP。公网NAT网关为您提供不同规格的连接数，根据业务规划，您可以通过创建多条SNAT规则，来实现共享弹性公网IP资源。

使用SNAT访问公网场景组网图如图1-4所示。

图 1-4 使用 SNAT 访问公网



- **使用DNAT为云主机面向公网提供服务**

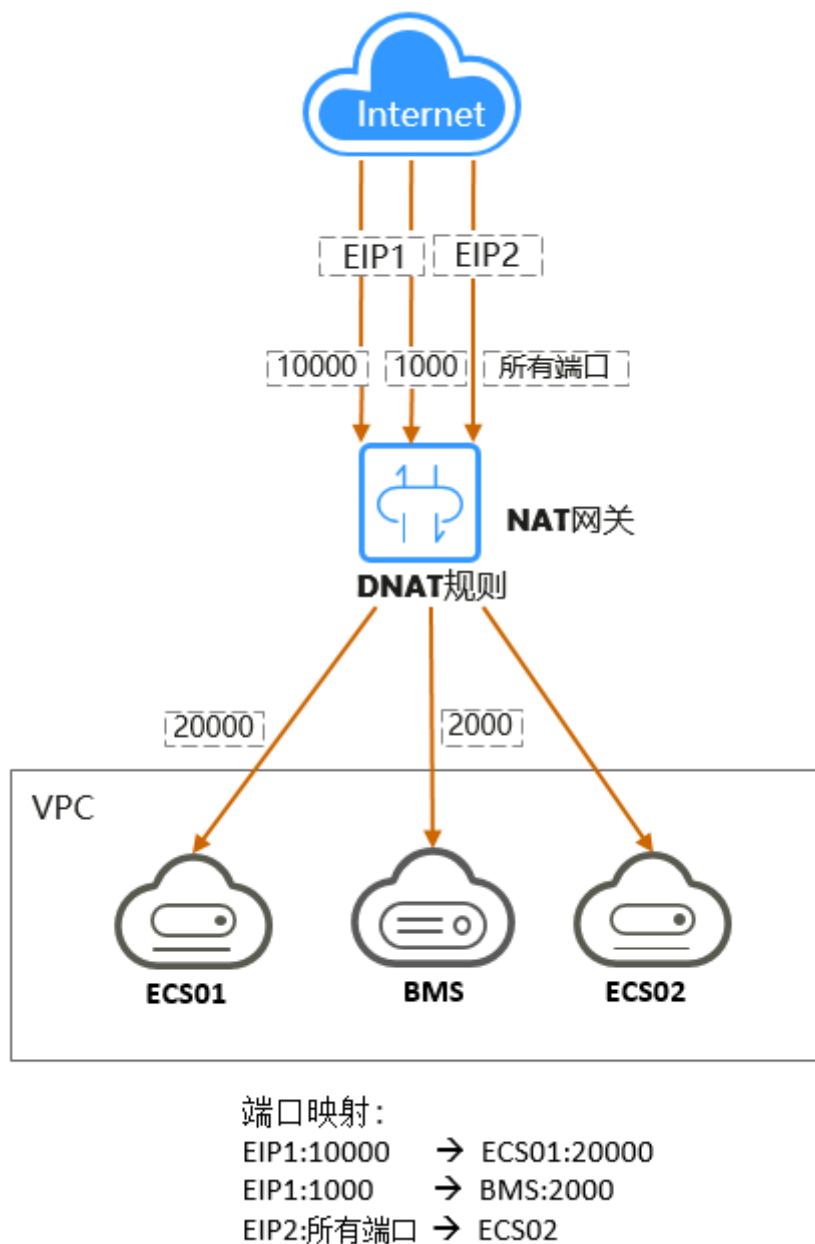
当VPC内的云主机需要面向公网提供服务时，可以使用公网NAT网关的DNAT功能。

DNAT功能绑定弹性公网IP，有两种映射方式（IP映射、端口映射）。可通过端口映射方式，当用户以指定的协议和端口访问该弹性公网IP时，公网NAT网关会将该请求转发到目标云主机实例的指定端口上。也可通过IP映射方式，为云主机配置了一个弹性公网IP，任何访问该弹性公网IP的请求都将转发到目标云主机实例上。使多个云主机共享弹性公网IP和带宽，精确的控制带宽资源。

一个云主机配置一条DNAT规则，如果有多个云主机需要为公网提供服务，可以通过配置多条DNAT规则来共享一个或多个弹性公网IP资源。

使用DNAT为公网提供服务场景组网图如图1-5所示。图中示例的云主机类型均可以替换为弹性云服务器，裸金属服务器中的任何一个。

图 1-5 使用 DNAT 为云主机面向公网提供服务

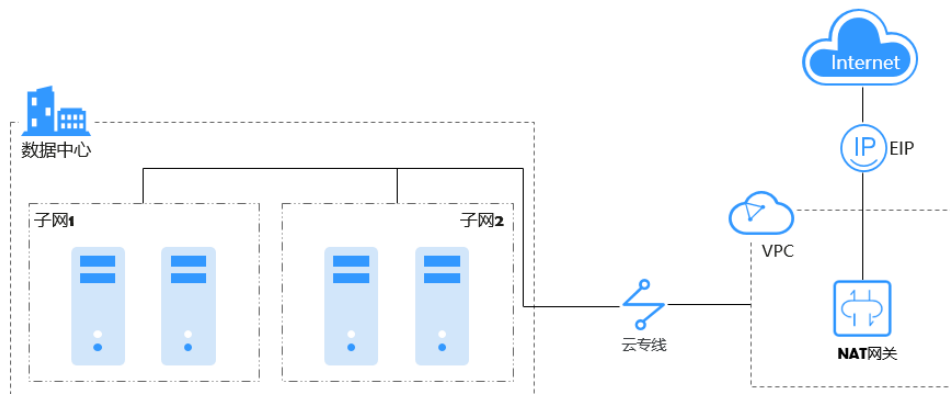


- **使用SNAT或DNAT高速访问互联网**

用户云下数据中心使用云专线/VPN接入虚拟私有云的用户，若有大量的服务器需要实现安全，可靠，高速的访问互联网，或者为互联网提供服务，可通过公网 NAT网关的SNAT功能或DNAT功能来实现。

使用SNAT或DNAT高速访问互联网场景图如[图1-6](#)所示。

图 1-6 使用 SNAT 或 DNAT 高速访问互联网



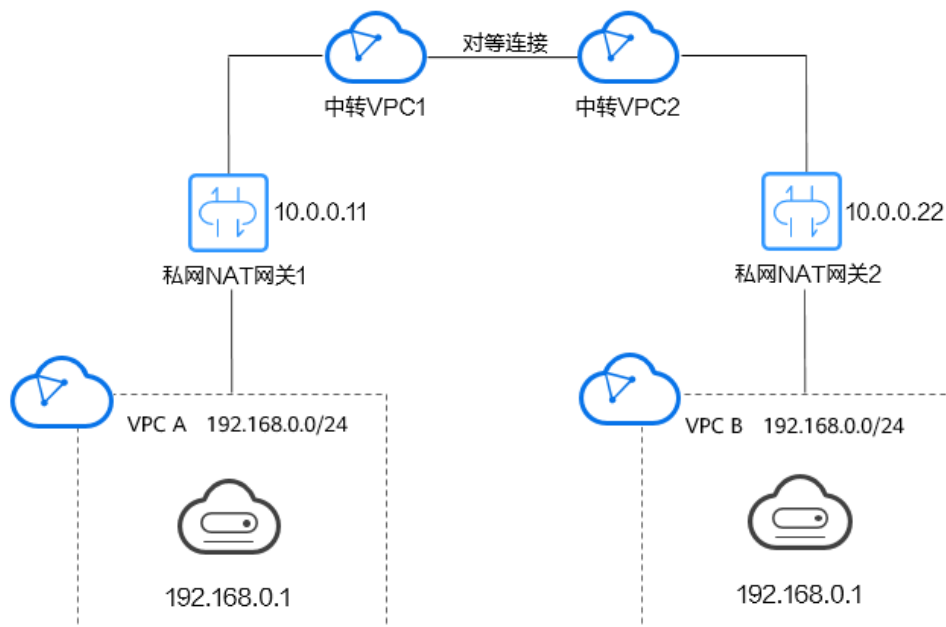
## 私网 NAT 网关

- **重叠网段VPC间互通**

私网NAT网关提供私网地址转换服务，利用两个私网NAT网关，配置SNAT、DNAT规则，可同时将源、目的网段地址转换为中转IP，通过使用中转IP实现两VPC间互通。私网NAT网关解决了两个重叠网段虚拟私有云中的云主机互相访问的问题。

如下图所示，创建2个中转VPC，然后使用两个私网NAT网关将VPC A中IP地址为192.168.0.1的弹性云服务器地址转化为10.0.0.11、将VPC B中IP地址为192.168.0.1的弹性云服务器地址转化为10.0.0.22，通过转化后的IP地址相互访问。

图 1-7 重叠网段 VPC 间互通



- **企业网络上云及指定IP接入**

大企业等机构上云，希望迁移上云保持组网不变，使用私网NAT网关无需对网络做任何更改即可保持原有方式互通。同时，行业监管部门要求指定地址接入，使

用私网NAT网关将各部门的IP地址映射为指定地址接入行业监管部门，满足企业安全规范。

企业部门间存在网段重叠，使用私网NAT网关，实现企业各部门迁移上云后组网不变，部门间保持原有方式互通，简化了IDC上云的网络规划；使用私网NAT网关，配置SNAT规则，将各部门的IP地址映射为符合要求的10.0.0.33地址接入行业监管部门，提升企业的安全性。

## 1.4 产品规格

NAT网关的规格指公网NAT网关与私网NAT网关支持的SNAT最大连接数。

### 公网 NAT 网关

SNAT连接数：由源IP地址、源端口、目的IP地址、目的端口、传输层协议这五个元素组成的集合视为一条连接。其中源IP地址和源端口指SNAT转换之后的弹性公网IP和它的端口。连接能够区分不同会话，并且对应的会话是唯一的。

吞吐量：DNAT规则的弹性公网IP的带宽之和。例如，一个公网NAT网关有两条DNAT规则，其中绑定到第一条规则的EIP带宽为10Mbit/s，绑定到第二条规则的EIP带宽为5Mbit/s，则公网NAT网关的吞吐量为15Mbit/s。

在创建公网NAT网关时，请根据您的网络规划，合理选择公网NAT网关的规格。公网NAT网关支持的规格如表1-1所示。

表 1-1 公网 NAT 网关规格

规格	SNAT最大连接数	带宽	每秒新建报文数 (QPS)
小型	10000	20Gbit/s	10000
中型	50000	20Gbit/s	10000
大型	200000	20Gbit/s	10000
超大型	1000000	20Gbit/s	10000

#### 说明

- 表格中所列的“每秒报文数 (PPS)”是指入方向和出方向的PPS总和。
- 为避免因连接数超过公网NAT网关规格最大值，从而影响业务的情况，建议在云监控中设置公网NAT网关监控指标，并为SNAT连接数合理设置告警。

### 私网 NAT 网关

SNAT连接数：由源IP地址、源端口、目的IP地址、目的端口、传输层协议这五个元素组成的集合视为一条连接。其中源IP地址和源端口指SNAT转换之后的中转IP和它的端口。

在创建私网NAT网关时，请根据您的网络规划，合理选择私网NAT网关的规格。私网NAT网关支持的规格如表1-2所示。

表 1-2 私网 NAT 网关规格

规格	SNAT最大连接数	带宽	每秒新建报文数 (QPS)
小型	2000	200Mbps	6000
中型	5000	500Mbps	9000
大型	20000	2Gbps	10000
超大型	50000	5Gbps	10000

### 说明

为避免因连接数超过私网NAT网关规格最大值，从而影响业务的情况，建议在云监控中设置私网NAT网关监控指标，并为SNAT连接数合理设置告警。

## 1.5 约束与限制

### 公网 NAT 网关

关于公网NAT网关的使用，您需要注意以下几点：

- 公共限制
  - 同一个公网NAT网关下的多条规则可以复用同一个弹性公网IP，不同网关下的规则必须使用不同的弹性公网IP。
  - 一个VPC支持关联多个公网NAT网关。
  - SNAT、DNAT可以共用同一个弹性公网IP，节省弹性公网IP资源。但是在选用全端口模式下，DNAT优先占用全部端口，这些端口不能被SNAT使用。因此SNAT规则不能和全端口的DNAT规则共用EIP，以免出现业务相互抢占问题。
  - 当云主机同时配置弹性公网IP服务和公网NAT网关服务时，数据均通过弹性公网IP转发。
  - NAT网关支持TCP、UDP和ICMP协议，暂不支持ALG相关技术，且GRE隧道和IPSec使用的ESP、AH无法使用NAT网关，这是由NAT网关本身的特性决定的。
- SNAT限制
  - VPC内的每个子网只能添加一条SNAT规则。
  - SNAT规则中添加的自定义网段，对于虚拟私有云的配置，必须是虚拟私有云子网网段的子集，不能相等。
  - SNAT规则中添加的自定义网段，对于云专线的配置，必须是云专线侧网段，且不能与虚拟私有云侧的网段冲突。
  - 公网NAT网关支持添加的SNAT规则的数量没有限制。
- DNAT限制
  - 一个云主机的一个端口对应一条DNAT规则，一个端口只能映射到一个EIP，不能映射到多个EIP。

- 公网NAT网关支持添加的DNAT规则的数量为200个。

## 私网 NAT 网关

关于私网NAT网关的使用，您需要注意以下几点：

- 公共限制
  - 用户需要在VPC下手动添加私网路由，即通过创建对等连接或开通云专线/VPN连接远端私网。
  - 中转IP和目的IP不能在同一个VPC中。
  - SNAT规则和DNAT规则不能共用同一个中转IP。
  - 私网NAT网关支持添加的DNAT规则和SNAT规则的数量如下：
    - 小型：DNAT规则和SNAT规则的总数不超过20个。
    - 中型：DNAT规则和SNAT规则的总数不超过50个。
    - 大型：DNAT规则和SNAT规则的总数不超过200个。
    - 超大型：DNAT规则和SNAT规则的总数不超过500个。
- SNAT限制
  - VPC内的每个子网只能添加一条SNAT规则。
- DNAT限制
  - DNAT的全端口模式不能和具体端口模式共用同一个中转IP。

## 1.6 权限管理

如果您需要对云服务平台上创建的NAT网关（NAT Gateway）资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权来控制他们对云服务平台资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有NAT网关的创建、查看的权限，但是不希望他们拥有删除NAT网关等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用NAT网关，但是不允许删除NAT网关的权限，控制他们对NAT网关资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用NAT网关服务的其它功能。

IAM是云服务平台提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见《IAM用户指南》。

### NAT 网关权限

默认情况下，账号管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

NAT网关部署时通过物理区域划分，为项目级服务，授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项

目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问 NAT 网关时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- **角色：** IAM 最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云服务平台各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- **策略：** IAM 最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对 NAT 网关服务，账号管理员能够控制 IAM 用户仅能对 NAT 网关或 SNAT 规则等进行指定的管理操作。多数细粒度策略以 API 接口为粒度进行权限拆分，NAT 网关（NAT Gateway）支持的 API 授权项请参见《NAT 网关接口参考》策略及授权项说明章节。

如表 1-3 所示，包括了 NAT 网关的所有系统权限。

表 1-3 NAT 网关系统权限

策略名称	描述	类型
NAT FullAccess	对 NAT 网关全部资源的所有执行权限。	系统策略
NAT ReadOnlyAccess	NAT 网关只读权限，对 NAT 网关全部资源的只读权限。	系统策略
NAT Administrator	对 NAT 网关全部资源的所有执行权限。拥有该权限的用户必须同时拥有 Tenant Guest 权限。	系统角色

表 1-4 列出了 NAT 网关常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 1-4 常用操作与系统权限的关系

操作	NAT FullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
创建 NAT 网关	√	x	√
查询 NAT 网关列表	√	√	√
查询 NAT 网关详情	√	√	√
更新 NAT 网关	√	x	√
删除 NAT 网关	√	x	√
添加 SNAT 规则	√	x	√
查看 SNAT 规则	√	√	√



操作	NAT FullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
修改SNAT规则	√	x	√
删除SNAT规则	√	x	√
添加DNAT规则	√	x	√
查看DNAT规则	√	√	√
修改DNAT规则	√	x	√
删除DNAT规则	√	x	√
创建中转子网	√	x	√
查询中转子网列表	√	√	√
查询中转子网详情	√	√	√
修改中转子网	√	x	√
删除中转子网	√	x	√
创建中转IP	√	x	√
查询中转IP	√	√	√
删除中转IP	√	x	√

## 📖 说明

- 创建DNAT规则时需注意以下事项：
  - 若实例类型选择服务器，并且为弹性云服务器ECS，还需要配置ECS服务的ECS ReadOnlyAccess权限，或添加细粒度权限ecs:cloudServers:get和ecs:cloudServers:list，具体详见《弹性云服务器API参考》。
  - 若实例类型选择服务器，并且为裸金属服务器BMS，还需要配置BMS服务的BMS ReadOnlyAccess权限，或添加细粒度权限bms:servers:get和bms:servers:list，具体详见《裸金属服务器API参考》。
  - 若创建私网NAT的DNAT规则，并且实例类型选择负载均衡器，还需要配置ELB ReadOnlyAccess，或添加细粒度权限elb:loadbalancers:get和elb:loadbalancers:list，具体详见《弹性负载均衡API参考》。
  - 创建DNAT规则后，需在VPC中放通对应的安全组规则，否则DNAT规则不能生效，所以还需要配置VPC服务的VPC FullAccess权限，或添加细粒度权限vpc:securityGroups:create，具体详见《虚拟私有云API参考》。
- 查看监控指标，还需要配置CES服务的CES ReadOnlyAccess权限，具体详见《云监控服务API参考》。
- 查看访问日志，还需要配置LTS服务的LTS ReadOnlyAccess权限，具体详见《云日志服务API参考》。

## 1.7 区域和可用区

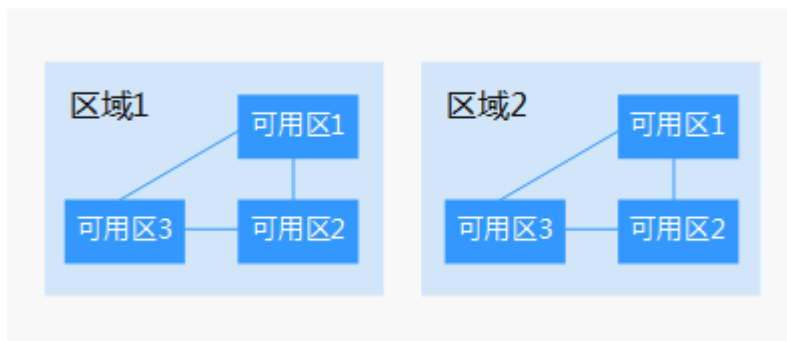
### 什么是区域、可用区？

区域和可用区用来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）指物理的数据中心。每个区域完全独立，这样可以实现最大程度的容错能力和稳定性。资源创建成功后不能更换区域。
- 可用区（AZ，Availability Zone）是同一区域内，电力和网络互相隔离的物理区域，一个可用区不受其他可用区故障的影响。一个区域内可以有多个可用区，不同可用区之间物理隔离，但内网互通，既保障了可用区的独立性，又提供了低价、低时延的网络连接。

图1-8阐明了区域和可用区之间的关系。

图 1-8 区域和可用区



### 如何选择区域？

建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

### 如何选择可用区？

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

### 区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关的区域和终端节点的更多信息，请参阅[地区和终端节点](#)。

## 1.8 基本概念

### 弹性公网 IP

弹性公网IP是基于互联网上的静态IP地址。

弹性公网IP地址为可以直接访问Internet的IP地址。私有IP地址为云平台内局域网络所有的IP地址，私有IP地址禁止出现在Internet中。

将弹性公网IP地址和子网中关联的弹性云服务器绑定，可以实现VPC中的弹性云服务器通过固定的公网IP地址与互联网互通。

一个弹性公网IP只能直接给一个弹性云服务器使用。如要实现VPC内跨可用区的多个云主机共享弹性公网IP，可选择公网NAT网关。

### SNAT 连接

由源IP地址、源端口、目的IP地址、目的端口、传输层协议这五个元素组成的集合视为一条连接。其中源IP地址和源端口指SNAT转换之后的IP地址和它的端口。连接能够区分不同会话，并且对应的会话是唯一的。

### DNAT 连接

DNAT连接是通过DNAT功能绑定弹性公网IP，再通过IP映射或端口映射两种方式，实现VPC内跨可用区的多个云主机共享弹性公网IP，为互联网提供服务。

# 2 快速入门

## 2.1 通过公网 NAT 网关的 SNAT 规则访问公网

### 操作场景

当多个云服务器在没有绑定弹性公网IP的情况下需要访问公网，为了节省弹性公网IP资源并且避免云服务器IP直接暴露在公网上，可以通过公网NAT网关共享弹性公网IP的方式实现无弹性公网IP的云服务器访问公网。

### 操作流程

操作步骤	说明
<a href="#">步骤一：购买EIP</a>	购买一个弹性公网IP。
<a href="#">步骤二：购买公网NAT网关</a>	购买一个公网NAT网关。
<a href="#">步骤三：添加SNAT规则</a>	为公网NAT网关添加SNAT规则，使得对应子网网段内的云服务器共享EIP访问公网。
<a href="#">步骤四：验证是否成功添加SNAT规则</a>	验证SNAT规则已在运行中。
<a href="#">步骤五：验证服务器是否可以通过NAT网关访问公网</a>	验证SNAT规则生效网段内的云服务器可以访问公网。

### 步骤一：购买 EIP

1. 在“创建弹性公网IP”页面，根据界面提示配置弹性公网IP参数。请您按需选择EIP的配置参数，具体可请参见。

## 步骤二：购买公网 NAT 网关

1. 在“创建公网NAT网关”页面，根据界面提示配置公网NAT网关参数。

表 2-1 公网 NAT 网关参数说明

参数	示例	参数说明
区域	华北-北京四	公网NAT网关所在的区域。
规格	小型	公网NAT网关的规格。 公网NAT网关共有小型、中型、大型、超大型四种规格类型，可通过“了解更多”查看各规格详情。
名称	public-nat-01	公网NAT网关名称。最大支持64个字符，仅支持中文、数字、字母、_（下划线）、-（中划线）、.（点号）。
虚拟私有云	VPC-A	公网NAT网关所属的VPC。 VPC仅在创建公网NAT网关时可以选择，后续不支持修改。 <b>说明</b> 由于需要放通到公网NAT网关的流量，即在VPC中需要有指向公网NAT网关的路由，因此在创建公网NAT网关时，会自动在VPC的默认路由表中添加一条0.0.0.0/0的默认路由指向所创建的公网NAT网关。如果在创建公网NAT网关前，VPC默认路由表中已经存在0.0.0.0/0的默认路由，则会导致自动添加该默认路由指向公网NAT网关失败，此时需要在公网NAT网关创建成功后，手动为此网关添加一条不同的路由或在新路由表中创建0.0.0.0/0的默认路由指向该网关。
子网	Subnet-A01	公网NAT网关所属VPC中的子网。 子网至少有一个可用的IP地址。 子网仅在创建公网NAT网关时可以选择，后续不支持修改。 本子网仅为系统配置NAT网关使用，NAT网关对整个VPC生效，需要在购买后继续添加规则，才能够连通Internet。
高级配置（可选）	-	单击下拉箭头，可配置公网NAT网关的高级参数。
高级配置 > SNAT连接TCP老化时间（秒）	900	通过SNAT规则建立的TCP连接的超时时间，如果TCP连接在该时间内没有数据交换将被关闭。 取值范围：40~7200。
高级配置 > SNAT连接UDP老化时间（秒）	300	通过SNAT规则建立的UDP连接的超时时间，如果UDP连接在该时间内没有数据交换将被关闭。 取值范围：40~7200。

参数	示例	参数说明
高级配置 > SNAT连接 ICMP老化时间 (秒)	10	通过SNAT规则建立的ICMP连接的超时时间, 如果ICMP连接在该时间内没有数据交换将被关闭。 取值范围: 10~7200。
高级配置 > TCP连接延迟关闭时间 (秒)	5	TCP连接关闭时TIME_WAIT状态持续时间。 取值范围: 0~1800。
高级配置 > 描述	无需配置	公网NAT网关信息描述。最大支持255个字符, 且不能包含“<”和“>”。
高级配置 > 标签	无需配置	公网NAT网关的标识, 包括键和值。可以创建20个标签。

2. 单击“立即创建”，在“规格确认”页面，您可以再次核对公网NAT网关信息。
3. 确认无误后，单击“提交”，开始创建公网NAT网关。  
返回公网NAT网关列表页面，可以查看已购买的公网NAT网关。

### 步骤三：添加 SNAT 规则

1. 在公网NAT网关页面，单击需要添加SNAT规则的NAT网关名称。
2. 在SNAT规则页签中，单击“添加SNAT规则”。
3. 根据界面提示，配置添加SNAT规则参数。配置参数请参见[表2-2](#)。

表 2-2 SNAT 参数说明

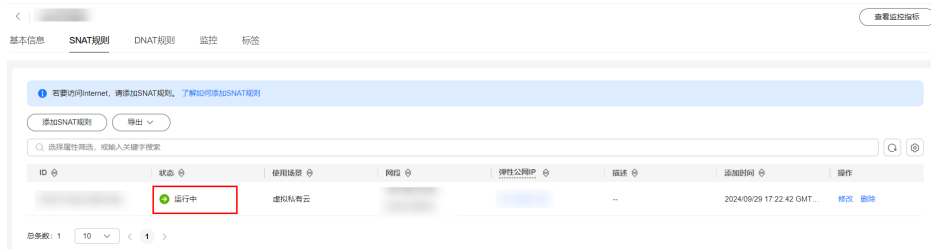
参数	示例	说明
使用场景	虚拟私有云	在使用SNAT访问公网的场景下，此处选择虚拟私有云。 表示虚拟私有云中的云主机使用SNAT规则访问公网。
网段	使用已有	通过配置虚拟私有云子网中的某个网段，使该网段中的云主机通过SNAT方式访问公网。 下拉选择子网网段。
公网IP类型	弹性公网IP	用来访问公网的IP。
监控	-	为SNAT连接数设置告警。 可通过设置告警及时了解SNAT连接数运行状况，从而起到预警作用。
描述	无需配置	SNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

4. 配置完成后，单击确定，完成“SNAT规则”创建。

## 步骤四：验证是否成功添加 SNAT 规则

1. 在SNAT页签的SNAT规则列表中，可以看到SNAT规则详细信息。若“状态”为“运行中”，表示创建成功。

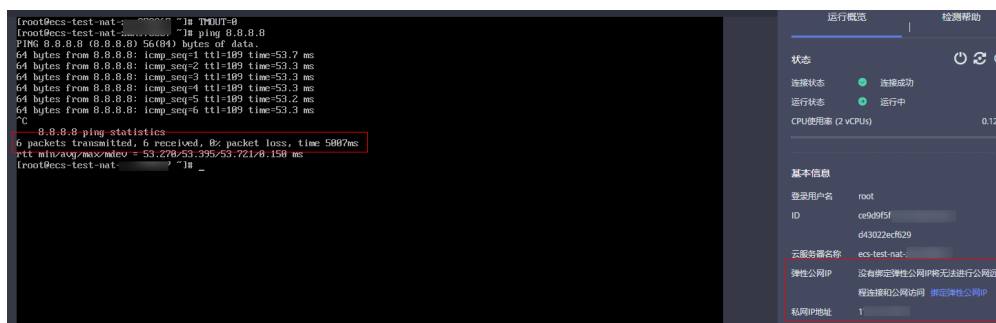
图 2-1 验证是否成功添加 SNAT 规则



## 步骤五：验证服务器是否可以通过 NAT 网关访问公网

1. 登录需要验证的服务器。
2. 验证服务器可以访问外网。

图 2-2 验证服务器可以访问外网



## 2.2 通过公网 NAT 网关的 DNAT 规则面向公网提供服务

### 操作场景

同一个VPC内的一个或多个云服务器需要面向公网提供服务时，可以参考本文为公网 NAT网关配置DNAT规则实现。

### 操作流程

操作步骤	说明
<b>步骤一：购买EIP</b>	购买一个弹性公网IP。
<b>步骤二：购买公网NAT网关</b>	购买一个公网NAT网关。
<b>步骤三：添加默认路由指向公网NAT网关</b>	添加路由表。

操作步骤	说明
步骤四：添加DNAT规则	为公网NAT网关添加DNAT规则，使得对应子网网段内的云服务器共享EIP访问公网。
步骤五：验证是否成功添加DNAT规则	验证DNAT规则已在运行中。
步骤六：验证私网服务器可以被外部公网服务器通过NAT网关访问	验证DNAT规则生效的云服务器可以被公网客户端成功访问。

## 步骤一：购买 EIP

1. 在“创建弹性公网IP”页面，根据界面提示配置弹性公网IP参数。  
请您按需选择EIP的配置参数，具体可请参见。

## 步骤二：购买公网 NAT 网关

1. 在“创建公网NAT网关”页面，根据界面提示配置公网NAT网关参数。

表 2-3 公网 NAT 网关参数说明

参数	示例	参数说明
区域	华北-北京四	公网NAT网关所在的区域。
规格	小型	公网NAT网关的规格。 公网NAT网关共有小型、中型、大型、超大型四种规格类型，可通过“了解更多”查看各规格详情。
名称	public-nat-01	公网NAT网关名称。最大支持64个字符，仅支持中文、数字、字母、_（下划线）、-（中划线）、.（点号）。
虚拟私有云	VPC-A	公网NAT网关所属的VPC。 VPC仅在创建公网NAT网关时可以选择，后续不支持修改。 <b>说明</b> 由于需要放通到公网NAT网关的流量，即在VPC中需要有指向公网NAT网关的路由，因此在创建公网NAT网关时，会自动在VPC的默认路由表中添加一条0.0.0.0/0的默认路由指向所创建的公网NAT网关。如果在创建公网NAT网关前，VPC默认路由表中已经存在0.0.0.0/0的默认路由，则会导致自动添加该默认路由指向公网NAT网关失败，此时需要在公网NAT网关创建成功后，手动为此网关添加一条不同的路由或在新路由表中创建0.0.0.0/0的默认路由指向该网关。



参数	示例	参数说明
子网	<b>Subnet-A01</b>	公网NAT网关所属VPC中的子网。 子网至少有一个可用的IP地址。 子网仅在创建公网NAT网关时可以选择，后续不支持修改。 本子网仅为系统配置NAT网关使用，NAT网关对整个VPC生效，需要在购买后继续添加规则，才能够连通Internet。
高级配置（可选）	-	单击下拉箭头，可配置公网NAT网关的高级参数。
高级配置 > SNAT连接TCP老化时间（秒）	<b>900</b>	通过SNAT规则建立的TCP连接的超时时间，如果TCP连接在该时间内没有数据交换将被关闭。 取值范围：40~7200。
高级配置 > SNAT连接UDP老化时间（秒）	<b>300</b>	通过SNAT规则建立的UDP连接的超时时间，如果UDP连接在该时间内没有数据交换将被关闭。 取值范围：40~7200。
高级配置 > SNAT连接ICMP老化时间（秒）	<b>10</b>	通过SNAT规则建立的ICMP连接的超时时间，如果ICMP连接在该时间内没有数据交换将被关闭。 取值范围：10~7200。
高级配置 > TCP连接延迟关闭时间（秒）	<b>5</b>	TCP连接关闭时TIME_WAIT状态持续时间。 取值范围：0~1800。
高级配置 > 描述	<b>无需配置</b>	公网NAT网关信息描述。最大支持255个字符，且不能包含“<”和“>”。
高级配置 > 标签	<b>无需配置</b>	公网NAT网关的标识，包括键和值。可以创建20个标签。

2. 单击“立即创建”，在“规格确认”页面，您可以再次核对公网NAT网关信息。
3. 确认无误后，单击“提交”，开始创建公网NAT网关。  
返回公网NAT网关列表页面，可以查看已购买的公网NAT网关。

### 步骤三：添加默认路由指向公网 NAT 网关

1. 在路由表页面，单击右上角的“创建路由表”。  
所属VPC：选公网NAT网关所在的VPC。
2. 自定义路由表创建成功后，单击自定义路由表名称。进入自定义路由表基本信息页。
3. 单击“添加路由”，按照如下配置参数。  
目的地址：0.0.0.0/0  
下一跳类型：NAT网关

下一跳：选择已创建的NAT网关

图 2-3 添加路由



4. 单击“确定”。

## 步骤四：添加 DNAT 规则

1. 在公网NAT网关页面，单击需要添加DNAT规则的公网NAT网关名称。
2. 在公网NAT网关详情页面中，单击“DNAT规则”页签。
3. 在DNAT规则页签中，单击“添加DNAT规则”。
4. 根据界面提示，配置添加DNAT规则参数，详情请参见表2-4。

表 2-4 DNAT 规则参数说明

参数	示例	说明
使用场景	虚拟私有云	在使用DNAT为云主机面向公网提供服务场景下，此处选择虚拟私有云。 表示虚拟私有云中的云主机将通过DNAT的方式共享弹性公网IP，为公网提供服务。
端口类型	具体端口	分为所有端口和具体端口两种类型。 <ul style="list-style-type: none"><li>● 所有端口：属于IP映射方式。此方式相当于为云主机配置了一个弹性公网IP，任何访问该弹性公网IP的请求都将转发到目标云服务器实例上。</li><li>● 具体端口：属于端口映射方式。公网NAT网关会将以指定协议和端口访问该弹性公网IP的请求转发到目标云服务器实例的指定端口上。</li></ul>
支持协议	TCP	协议类型分为TCP和UDP两种类型。端口类型为具体端口时，可配置此参数，端口类型为所有端口时，此参数默认设置为All。
公网IP类型	弹性公网IP	公网IP地址。
公网端口	80-100	弹性公网IP的端口，有效数值为1-65535。 公网端口的范围可以为具体的数值，也可以为连续的数值范围，例如端口可以为80，也可以为80-100。
实例类型	服务器	DNAT规则生效的实例类型。

参数	示例	说明
网卡	-	选择服务器对应的网卡。
私网端口	80-100	在使用DNAT为云服务器面向公网提供服务场景下，指云服务器的端口号。当端口类型为具体端口时，需要配置此参数，有效数值为1-65535。 私网端口的范围可以为具体的数值，也可以为连续的数值范围，例如端口可以为80，也可以为80-100。
描述	无需配置	DNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

5. 配置完成后，单击“确定”，完成“DNAT规则”创建。

#### 须知

配置DNAT规则后，需在对应的云服务器中放通对应的安全组规则，否则DNAT规则不能生效。具体操作步骤，请参见。

### 步骤五：验证是否成功添加 DNAT 规则

1. 在DNAT页签的DNAT规则列表中，可以看到DNAT规则详细信息验证是否成功添加DNAT规则。  
若“状态”为“运行中”，表示创建成功。

### 步骤六：验证私网服务器可以被外部公网服务器通过 NAT 网关访问

1. 登录绑定了EIP的服务器ECS02。
2. 在ECS02上pingNAT网关的DNAT规则绑定的EIP（120.46.131.153），验证私网服务器ECS01是否可以被外部公网服务器ECS02通过NAT网关访问到。

图 2-4 验证私网服务器是否可以被外部公网服务器通过 NAT 网关访问

```
[root@ecs-~]# ping 120.46.131.153
PING 120.46.131.153 (120.46.131.153) 56(84) bytes of data:
64 bytes from 120.46.131.153: icmp_seq=1 ttl=58 time=1.19 ms
64 bytes from 120.46.131.153: icmp_seq=2 ttl=58 time=0.939 ms
64 bytes from 120.46.131.153: icmp_seq=3 ttl=58 time=0.905 ms
64 bytes from 120.46.131.153: icmp_seq=4 ttl=58 time=0.896 ms
64 bytes from 120.46.131.153: icmp_seq=5 ttl=58 time=0.906 ms
64 bytes from 120.46.131.153: icmp_seq=6 ttl=58 time=0.889 ms
64 bytes from 120.46.131.153: icmp_seq=7 ttl=58 time=0.860 ms
64 bytes from 120.46.131.153: icmp_seq=8 ttl=58 time=0.905 ms
64 bytes from 120.46.131.153: icmp_seq=9 ttl=58 time=0.886 ms
^C
--- 120.46.131.153 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8137ms
rtt min/avg/max/mdev = 0.860/0.930/1.192/0.102 ms
[root@ecs-~]#
```

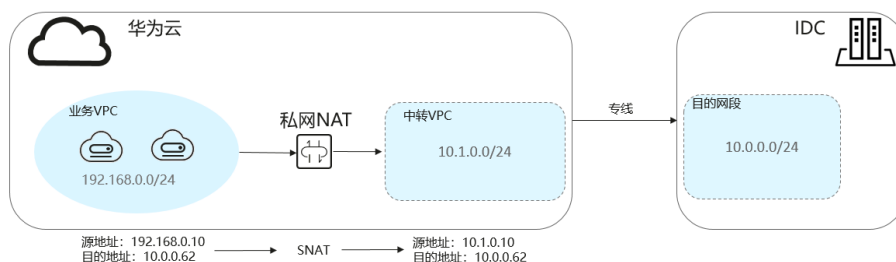
## 2.3 通过私网 NAT 网关实现云上云下互通

### 操作场景

本文档将以部署VPC内计算实例以指定私网地址接入线下本地数据中心为场景，帮助您学习如何创建和使用私网NAT网关。

用户本地数据中心（IDC）通过云专线接入虚拟私有云（VPC），VPC中的ECS需要转换成IDC指定的私网网段进行通信，详情可见下方的组网图。

图 2-5 组网图



### 操作流程

操作步骤	说明
<b>步骤一：创建业务VPC和中转VPC</b>	创建业务VPC（含业务子网）和中转VPC（含中转子网）。
<b>步骤二：配置VPC Peering</b>	创建VPC对等连接将用户IDC（Peering目的VPC）与中转VPC连通。
<b>步骤三：购买私网NAT网关</b>	购买一个私网NAT网关。
<b>步骤四：创建中转IP</b>	创建中转IP，使虚拟私有云内多个云服务器可以共享中转IP。
<b>步骤五：添加SNAT规则</b>	为私网NAT网关添加SNAT规则，通过绑定中转IP可实现VPC内的多个云服务器共享中转IP，访问外部数据中心或其他VPC。
<b>步骤六：添加路由</b>	自定义路由，路由包括目的地址、下一跳类型、下一跳地址等信息，可以决定网络流量的走向。
<b>步骤七：添加安全组规则</b>	在目的VPC包含的云服务器中添加加入方向安全组规则，用于将转发到目的端的流量全部放通。

### 准备工作

在使用NAT网关服务前，您需要注册华为账号并开通华为云、完成实名认证、为账户充值。

- 。
- 参考完成个人或企业账号实名认证。
- 您需要确保账户有足够金额，请参见。

## 步骤一：创建业务 VPC 和中转 VPC

虚拟私有云可以为您的弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境。

创建业务VPC（含业务子网）和中转VPC（含中转子网）。

具体操作请参见。

## 步骤二：配置 VPC Peering

您需要在IDC和云上区域创建云专线。本示例使用VPC对等连接代替云专线。

通过创建VPC对等连接将用户IDC（Peering目的VPC）与中转VPC连通。详细步骤请参见。

### 📖 说明

如要使用云专线将用户IDC（Peering目的VPC）与中转VPC连通，请参见。

## 步骤三：购买私网 NAT 网关

1. 在“创建私网NAT网关”页面，根据界面提示配置私网NAT网关参数。

表 2-5 私网 NAT 网关参数说明

参数	参数说明
区域	私网NAT网关所在的区域。
名称	私网NAT网关名称。最大支持64个字符，仅支持中文、数字、字母、_（下划线）、-（中划线）。
虚拟私有云	私网NAT网关所属的业务VPC。 VPC仅在创建私网NAT网关时可以选择，后续不支持修改。
子网	私网NAT网关所属VPC中的子网。 子网至少有一个可用的IP地址。 子网仅在创建私网NAT网关时可以选择，后续不支持修改。
规格	私网NAT网关的规格。
企业项目	配置私网NAT网关归属的企业项目。当没有指定企业项目时，将默认使用项目名称为default的企业项目。 当您的账号开通企业项目权限后，才支持配置私网NAT网关归属的企业项目。
标签	私网NAT网关的标识，包括键和值。可以创建20个标签。

参数	参数说明
描述	私网NAT网关信息描述。最大支持255个字符，且不能包含“<”和“>”。

2. 单击“立即创建”，开始创建私网NAT网关。
3. 在“私网NAT网关”列表，查看私网NAT网关状态。

## 步骤四：创建中转 IP

1. 在私网NAT网关页面，单击“中转IP > 创建中转IP”，进入创建中转IP页面。
2. 根据界面提示，配置中转IP的基本信息，配置参数请参见表2-6。

表 2-6 中转 IP 参数说明

参数	示例	参数说明
中转VPC	-	选择中转IP所在的VPC。
中转子网	-	中转子网相当于一个中转网络，是中转IP所属的子网。 子网至少有一个可用的IP地址。
中转IP	自动分配	中转IP的分配方式有以下两种。 <b>自动分配</b> ：由系统自动分配中转IP地址。 <b>手动分配</b> ：手动指定中转IP地址。
企业项目	default	中转IP所属的企业项目。
标签	无需配置	中转IP的标识，包括键和值。可以创建20个标签。

3. 单击“确定”，开始创建中转IP。

## 步骤五：添加 SNAT 规则

1. 在私网NAT网关页面，单击需要添加SNAT规则的私网NAT网关名称。
2. 在SNAT规则页签中，单击“添加SNAT规则”。
3. 根据界面提示，配置添加SNAT规则参数，详情请参见表2-7。

表 2-7 SNAT 规则参数说明

参数	示例	参数说明
子网	使用已有	SNAT规则的子网类型，选择“使用已有”或“自定义”。 选择业务VPC中需要做地址映射的子网。
监控	-	可以为SNAT连接数设置告警，实时监控运行状态。

参数	示例	参数说明
中转IP	-	中转IP选择 <a href="#">步骤四</a> 创建的中转IP。
描述	<b>无需配置</b>	SNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

4. 配置完成后，单击确定，完成“SNAT规则”创建。
5. 在SNAT规则列表中查看详情，若“状态”为“运行中”，表示创建成功。

## 步骤六：添加路由

1. 在路由表列表中，单击业务VPC的路由表名称。
2. 单击“添加路由”，按照提示配置参数。

表 2-8 添加路由参数说明

参数	示例	参数说明
目的地址	<b>10.0.0.0/24</b>	目的地址网段。 配置为IDC（目的VPC）的私网网段。
下一跳类型	<b>NAT网关</b>	下一跳的资源类型。
下一跳	<b>private-nat-01</b>	下一跳资源选择创建的私网NAT网关。
描述	<b>无需配置</b>	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。

3. 单击“确定”，完成添加。

## 步骤七：添加安全组规则

1. 在安全组列表中，单击目标安全组所在行的操作列下的“配置规则”。  
进入安全组规则配置页面。
2. 在入方向规则页签，单击“添加规则”，添加入方向规则。  
单击“+”可以依次增加多条入方向规则。

表 2-9 入方向参数说明

参数	取值样例	说明
优先级	<b>1</b>	规则的优先级，优先级数字越小，规则的优先级别越高

参数	取值样例	说明
策略	允许	安全组规则策略，支持的策略如下： <ul style="list-style-type: none"><li>• 如果“策略”设置为允许，表示允许源地址访问安全组内云服务器的指定端口。</li><li>• 如果“策略”设置为拒绝，表示拒绝源地址访问安全组内云服务器的指定端口。</li></ul>
协议端口	TCP	网络协议。目前支持“All”、“TCP”、“UDP”、“ICMP”和“GRE”等协议。
	22或22-30	端口：允许远端地址访问弹性云服务器指定端口，取值范围为：1~65535。
源地址	0.0.0.0/0	源地址：可以是IP地址、安全组、IP地址组。用于放通来自IP地址或另一安全组内的实例的访问。
描述	无需配置	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。

3. 单击“确定”，完成添加。



# 3 公网 NAT 网关

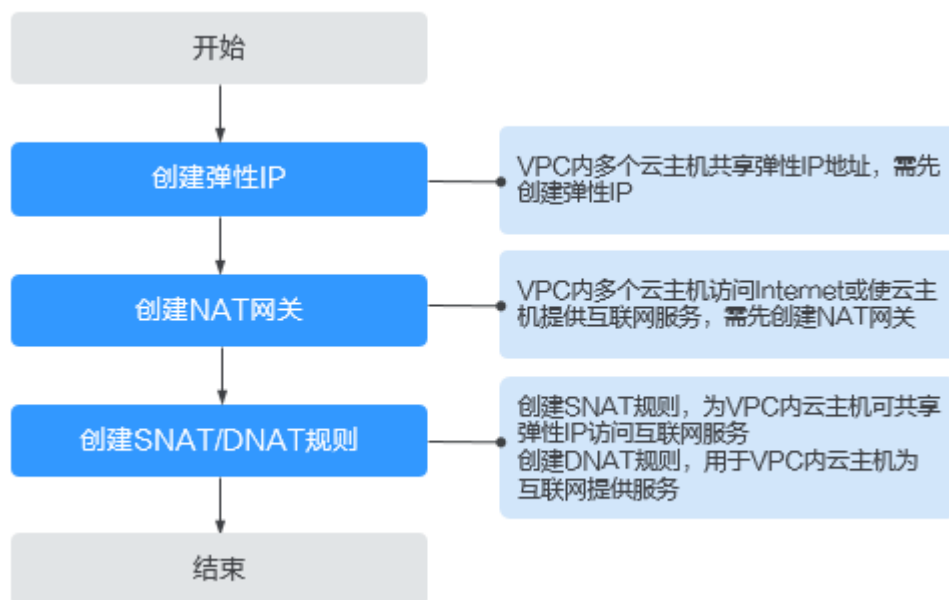
## 3.1 公网 NAT 网关简介

公网NAT网关（Public NAT Gateway）能够为虚拟私有云内的云主机或者通过云专线/VPN接入虚拟私有云的本地数据中心的服务器，提供最高20Gbit/s能力的网络地址转换服务。

公网NAT网关可以使多个云主机可以共享弹性公网IP访问Internet或使云主机提供互联网服务。

公网NAT网关使用流程如下：

图 3-1 公网 NAT 使用流程



## 3.2 创建公网 NAT 网关

### 操作场景

如果您要通过公网NAT网关访问公网或为公网提供服务，则需要创建公网NAT网关。

### 约束与限制

- 同一个公网NAT网关下的多条规则可以复用同一个弹性公网IP，不同网关下的规则必须使用不同的弹性公网IP。
- 一个VPC支持关联多个公网NAT网关。
- SNAT、DNAT可以共用同一个弹性公网IP，节省弹性公网IP资源。但是在选用全端口模式下，DNAT优先占用全部端口，这些端口不能被SNAT使用。因此SNAT规则不能和全端口的DNAT规则共用EIP，以免出现业务相互抢占问题。
- 当云主机同时配置弹性公网IP服务和公网NAT网关服务时，数据均通过弹性公网IP转发。

### 前提条件

- 创建公网NAT网关必须指定公网NAT网关所在VPC、子网。
- 由于需要放通到公网NAT网关的流量，即在VPC中需要有指向公网NAT网关的路由，因此在创建公网NAT网关时，会自动在VPC的默认路由表中添加一条0.0.0.0/0的默认路由指向所创建的公网NAT网关。如果在创建公网NAT网关前，VPC默认路由表下已经存在0.0.0.0/0的默认路由，则会导致自动添加该默认路由指向公网NAT网关失败，此时需要在公网NAT网关创建成功后，手动为此网关添加一条不同的路由或在新路由表中创建0.0.0.0/0的默认路由指向该网关。

### 操作步骤



1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > NAT网关”。进入公网NAT网关页面。
3. 在公网NAT网关页面，单击，进入公网NAT网关创建页面。
4. 根据界面提示，配置公网NAT网关的基本信息，配置参数请参见表3-1。

表 3-1 参数说明

参数	参数说明
区域	公网NAT网关所在的区域。
规格	公网NAT网关的规格。 公网NAT网关共有小型、中型、大型、超大型规格类型，可通过“了解更多”查看各规格详情。
名称	公网NAT网关名称。最大支持64个字符，仅支持中文、数字、字母、_（下划线）、-（中划线）、.（点号）。

参数	参数说明
虚拟私有云	公网NAT网关所属的VPC。 VPC仅在创建公网NAT网关时可以选择，后续不支持修改。 <b>说明</b> 由于需要放通到公网NAT网关的流量，即在VPC中需要有指向公网NAT网关的路由，因此在创建公网NAT网关时，会自动在VPC的默认路由表中添加一条0.0.0.0/0的默认路由指向所创建的公网NAT网关。如果在创建公网NAT网关前，VPC默认路由表下已经存在0.0.0.0/0的默认路由，则会导致自动添加该默认路由指向公网NAT网关失败，此时需要在公网NAT网关创建成功后，手动为此网关添加一条不同的路由或在新路由表中创建0.0.0.0/0的默认路由指向该网关。
子网	公网NAT网关所属VPC中的子网。 子网至少有一个可用的IP地址。 子网仅在创建公网NAT网关时可以选择，后续不支持修改。 本子网仅为系统配置NAT网关使用，NAT网关对整个VPC生效，需要在购买后继续添加规则，才能够连通Internet。
高级配置（可选）	单击下拉箭头，可配置公网NAT网关的高级参数，比如描述。
高级配置 >描述	公网NAT网关信息描述。最大支持255个字符，且不能包含“<”和“>”。

- 单击“立即创建”，在“规格确认”页面，您可以再次核对公网NAT网关信息。
- 确认无误后，单击“提交”，开始创建公网NAT网关。  
公网NAT网关的创建过程一般需要1-5分钟。
- 在“公网NAT网关”列表，查看公网NAT网关状态。

#### 说明

公网NAT网关创建成功后，查看该公网NAT网关所在的VPC的默认路由表下是否存在0.0.0.0/0的默认路由指向该公网NAT网关，如果不存在，请在默认路由表中添加一条指向该公网NAT网关的路由，或创建一个自定义路由表并在自定义路由表中添加0.0.0.0/0的默认路由指向该公网NAT网关。

## 高频问题

### NAT 网关连接数超过规格限制怎么办？

- 为避免因连接数超过公网NAT网关规格最大值，从而影响业务的情况，建议在云监控中设置公网NAT网关监控指标，并为SNAT连接数合理设置告警。
- 如果您的业务连接数超过当前NAT网关规格，建议您及时通过[管理公网NAT网关](#)进行扩容。

## 修改 NAT 网关规格对业务有影响吗？

提升公网NAT网关规格不影响业务；降低公网NAT网关规格取决于当前的业务量是否超过降档后规格的上限。

## 3.3 管理公网 NAT 网关

### 操作场景


公网NAT网关创建后，如果您在使用过程中发现当前的公网NAT网关规格不能满足自己的需求，可以修改公网NAT网关规格、名称和描述。如果您不再需要使用公网NAT网关，可以通过删除公网NAT网关，释放资源。

提升公网NAT网关规格不影响业务；降低公网NAT网关规格取决于当前的业务量是否超过降档后规格的上限。


#### 说明

- 降低公网NAT网关规格需要评估当前业务量是否超过降低后的规格上限，避免造成业务中断。
- 提升公网NAT网关规格，业务不受影响。

### 修改公网 NAT 网关

1. 登录管理控制台。
2. 在页面左上角单击  图标，打开服务列表，选择“网络 > NAT网关”。进入公网NAT网关页面。
3. 在公网NAT网关页面，单击需要修改的公网NAT网关操作列中的“修改”。
4. 根据界面提示，修改公网NAT网关的名称、规格或者描述信息。

### 删除公网 NAT 网关

1. 登录管理控制台。
2. 在页面左上角单击  图标，打开服务列表，选择“网络 > NAT网关”。进入公网NAT网关页面。
3. 在公网NAT网关页面，单击需要删除的公网NAT网关操作列中的“删除”。
4. 在删除确认对话框，输入“DELETE”。
5. 单击“确定”。

## 3.4 管理 SNAT 规则

## 3.4.1 添加 SNAT 规则

### 操作场景

公网NAT网关创建成功后，您需要创建SNAT规则。通过创建SNAT规则，虚拟私有云子网中全部或部分云主机可以通过共享弹性公网IP访问公网，或云专线用户侧端该网段下的服务器可以通过共享弹性公网IP访问公网。

一个子网对应一条SNAT规则，如果VPC中有多个子网需要访问公网，则可以通过创建多个SNAT规则实现共享一个或多个弹性公网IP资源。

### 约束与限制

- VPC内的每个子网只能添加一条SNAT规则。
- SNAT规则中添加的自定义网段，对于虚拟私有云的配置，必须是虚拟私有云子网网段的子集，不能相等。
- SNAT规则中添加的自定义网段，对于云专线的配置，必须是云专线侧网段，且不能与虚拟私有云侧的网段冲突。
- 公网NAT网关支持添加的SNAT规则的数量没有限制。

### 添加 SNAT 规则


1. 登录管理控制台。
2. 在页面左上角单击  图标，打开服务列表，选择“网络 > NAT网关”。进入公网NAT网关页面。
3. 在公网NAT网关页面，单击需要添加SNAT规则的公网NAT网关名称。
4. 在SNAT规则页签中，单击“添加SNAT规则”。
5. 根据界面提示，配置添加SNAT规则参数，详情请参见表3-2。

表 3-2 SNAT 规则参数说明

参数	说明
使用场景	SNAT规则使用的场景。 当虚拟私有云中的云主机需要访问公网时，选择虚拟私有云。 当云专线/VPN本地数据中心端的服务器需要访问公网时，选择云专线。
网段	使用场景为虚拟私有云时，通过配置虚拟私有云子网中的某个网段，使该网段中的云主机通过SNAT方式访问公网。 使用场景为云专线时，通过配置专线侧本地数据中心的某个网段，使该网段中的服务器通过SNAT方式访问公网。

参数	说明
公网IP类型	用来提供互联网访问的公网IP。 这里只能选择没有被绑定的弹性公网IP，或者被绑定在当前公网NAT网关中非“所有端口”类型DNAT规则上的弹性公网IP，或者被绑定到当前公网NAT网关中SNAT规则上的弹性公网IP。
监控	为SNAT连接数设置告警。 可通过设置告警及时了解SNAT连接数运行状况，从而起到预警作用。
描述	SNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

- 配置完成后，单击确定，完成“SNAT规则”创建。

#### 说明

- 根据您的业务需求，可以为一个公网NAT网关添加多条SNAT规则。
- VPC内的每个子网只能添加一条SNAT规则。

## 3.4.2 修改 SNAT 规则

### 操作场景

添加SNAT规则后，如果SNAT规则设置有误，或者SNAT规则中的一些参数需要更新时，可以修改SNAT规则。

当您修改SNAT规则前，请您务必了解该操作可能带来的影响，避免误操作造成网络中断。

### 操作前提

公网NAT网关下存在成功添加的SNAT规则。

### 操作步骤

- 登录管理控制台。
- 在公网NAT网关页面，单击目标公网NAT网关的名称。
- 系统跳转至目标公网NAT网关详情页面，单击“SNAT规则”页签。
- 在SNAT规则列表中，单击目标SNAT规则操作列中的“修改”。
- 在弹出的对话框中，修改参数中的内容。
- 单击“确定”，完成SNAT规则的修改。

## 3.4.3 删除 SNAT 规则

### 操作场景

添加SNAT规则后，如果不再需要此SNAT规则，您可以删除SNAT规则。

## 操作前提

公网NAT网关下存在成功添加的SNAT规则。

## 操作步骤

1. 登录管理控制台。
2. 在公网NAT网关页面，单击目标公网NAT网关的名称。
3. 在SNAT页签的SNAT规则列表中，单击目标SNAT规则操作列中的“删除”。
4. 如果您确定要删除，在弹出的对话框中输入“DELETE”，然后单击“确定”，完成SNAT规则的删除。

## 3.5 管理 DNAT 规则

### 3.5.1 添加 DNAT 规则

#### 操作场景

公网NAT网关创建后，通过添加DNAT规则，则可以通过映射方式将您VPC内的云主机对互联网提供服务。

一个云主机的一个端口对应一条DNAT规则，一个端口只能映射到一个EIP，不能映射到多个EIP。如果您有多个云主机需要为互联网提供服务，则需要创建多条DNAT规则。

#### 约束限制

- 一个云主机的一个端口对应一条DNAT规则，一个端口只能映射到一个EIP，不能映射到多个EIP。
- 公网NAT网关支持添加的DNAT规则的数量为200个。

#### 操作步骤


1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > NAT网关”。进入公网NAT网关页面。
3. 在公网NAT网关页面，单击需要添加DNAT规则的公网NAT网关名称。
4. 在公网NAT网关详情页面中，单击“DNAT规则”页签。
5. 在DNAT规则页签中，单击“添加DNAT规则”。
6. 根据界面提示，配置添加DNAT规则参数，详情请参见[表3-3](#)。

表 3-3 DNAT 规则参数说明

参数	说明
使用场景	虚拟私有云表示虚拟私有云中的云主机将通过DNAT的方式共享弹性公网IP，为公网提供服务。 云专线表示通过云专线方式接入虚拟私有云的本地数据中心中的服务器，将通过DNAT的方式为公网提供服务。
端口类型	分为所有端口和具体端口两种类型。 <ul style="list-style-type: none"><li>所有端口：属于IP映射方式。此方式相当于为云主机配置了一个弹性公网IP，任何访问该弹性公网IP的请求都将转发到目标云服务器实例上。</li><li>具体端口：属于端口映射方式。公网NAT网关会以指定协议和端口访问该弹性公网IP的请求转发到目标云主机实例的指定端口上。</li></ul>
支持协议	协议类型分为TCP和UDP两种类型。端口类型为具体端口时，可配置此参数，端口类型为所有端口时，此参数默认设置为All。
公网IP类型	弹性公网IP地址。 只能选择没有被绑定的弹性公网IP，或者被绑定在当前公网NAT网关中非“所有端口”类型DNAT规则上的弹性公网IP，或者被绑定到当前公网NAT网关中SNAT规则上的弹性公网IP。
公网端口	弹性公网IP的端口。当端口类型为具体端口时，需要配置此参数，有效数值为1-65535。 公网端口的范围可以为具体的数值，也可以为连续的数值范围，例如端口可以为80，也可以为80-100。
实例类型	选择对外部公网提供服务的实例类型。 <ul style="list-style-type: none"><li>服务器</li><li>虚拟IP地址</li><li>自定义</li></ul>
网卡	服务器网卡。实例类型为服务器时，需要配置此参数。
私网IP	<ul style="list-style-type: none"><li>当使用场景为虚拟私有云时，私网IP地址只能为本虚拟私有云下云主机的IP地址。表示此IP地址的云主机将通过DNAT方式为公网提供服务。</li><li>当使用场景为云专线时，指用户本地数据中心中服务器的IP地址或者用户的私有IP地址。表示通过云专线接入到虚拟私有云的本地数据中心端的此私有IP服务器，可以通过DNAT方式为公网提供服务。</li><li>端口类型为具体端口时，需要配置私网IP的端口。</li></ul>



参数	说明
私网端口	在使用DNAT为云主机面向公网提供服务场景下，指云主机的端口号。当端口类型为具体端口时，需要配置此参数，有效数值为1-65535。 私网端口的范围可以为具体的数值，也可以为连续的数值范围，例如端口可以为80，也可以为80-100。
描述	DNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

- 配置完成后，单击“确定”，可在DNAT规则列表中查看详情，若“状态”为“运行中”，表示创建成功。

#### 须知

配置DNAT规则后，需在对应的云主机中放通对应的安全组规则，否则DNAT规则不能生效。

## 3.5.2 修改 DNAT 规则

### 操作场景

添加DNAT规则后，如果DNAT规则设置有误，或者DNAT规则中的一些参数需要更新时，可以修改DNAT规则。

当您修改DNAT规则前，请您务必了解该操作可能带来的影响，避免误操作造成网络中断。

### 操作前提

公网NAT网关下存在成功添加的DNAT规则。

### 操作步骤

- 登录管理控制台。
- 在公网NAT网关页面，单击目标公网NAT网关的名称。
- 系统跳转至目标公网NAT网关详情页面，单击“DNAT规则”页签。
- 在DNAT规则列表中，单击目标DNAT规则操作列中的“修改”。
- 在弹出的对话框中，修改参数中的内容。
- 单击“确定”，完成DNAT规则的修改。

## 3.5.3 删除 DNAT 规则

### 操作场景

添加DNAT规则后，如果不需要此DNAT规则，您可以删除DNAT规则。

## 操作前提

公网NAT网关下存在成功添加的DNAT规则。

## 操作步骤

1. 登录管理控制台。
2. 在公网NAT网关页面，单击目标公网NAT网关的名称。
3. 系统跳转至目标公网NAT网关详情页面，单击“DNAT规则”页签。
4. 在DNAT规则列表中，单击目标DNAT规则操作列中的“删除”。
5. 如果您确定要删除，在弹出的对话框中输入“DELETE”，然后单击“确定”，完成DNAT规则的删除。

### 3.5.4 批量删除 DNAT 规则

## 操作场景

添加DNAT规则后，如果不需要此DNAT规则，您可以删除DNAT规则。

## 操作前提

公网NAT网关下存在成功添加的DNAT规则。

## 操作步骤

1. 登录管理控制台。
2. 在公网NAT网关页面，单击目标NAT网关的名称。
3. 系统跳转至目标公网NAT网关详情页面，单击“DNAT规则”页签。
4. 在DNAT规则列表中，勾选目标DNAT规则，单击“删除DNAT规则”。
5. 在弹出的对话框中单击“确定”，完成DNAT规则的批量删除。

### 3.5.5 DNAT 规则模板导入导出

## 操作场景

公网NAT网关创建后，通过添加DNAT规则，则可以通过映射方式将您VPC内的云主机对互联网提供服务。

在不同环境或多个NAT网关间迁移配置规则时，您可以通过DNAT规则的导入和导出功能，简化DNAT规则配置的过程，提高DNAT规则配置的灵活性和效率。

## 导入 DNAT 规则

1. 登录管理控制台。
2. 在公网NAT网关页面，单击需要导入DNAT规则的公网NAT网关名称。
3. 在公网NAT网关详情页面中，单击“DNAT规则”页签。
4. 在DNAT规则页签中，单击“导入”后，下载模板。
5. 根据模板中的表头，填写DNAT规则参数，详情请参见[表3-4](#)。

表 3-4 DNAT 规则参数说明

参数	说明
使用场景	分为虚拟私有云和云专线两种方式。 <ul style="list-style-type: none"><li>虚拟私有云：表示虚拟私有云中的云主机将通过DNAT的方式共享弹性IP，为公网提供服务。</li><li>云专线：表示通过云专线方式接入虚拟私有云的本地数据中心中的服务器，将通过DNAT的方式为公网提供服务。</li></ul>
支持协议	协议类型分为TCP、UDP、全部三种类型。
弹性IP	弹性IP地址及公网端口。 只能使用未绑定的弹性IP或者被绑定在当前VPC中DNAT规则上的弹性IP。
公网端口	弹性IP的端口。当端口类型为“全部”时，不需要配置此参数。 公网端口的范围可以为具体的数值，也可以为连续的数值范围，例如端口可以为80，也可以为80-100。
私网IP	<ul style="list-style-type: none"><li>当使用场景为虚拟私有云时，私网IP地址只能为本虚拟私有云下云主机的IP地址。表示此IP地址的云主机将通过DNAT方式为公网提供服务。</li><li>当使用场景为云专线时，指用户本地数据中心中服务器的IP地址或者用户的私有IP地址。表示通过云专线接入到虚拟私有云的本地数据中心端的此私有IP服务器，可以通过DNAT方式为公网提供服务。</li><li>协议类型为TCP、UDP时，需要配置私网IP的端口。</li></ul>
私网端口	<ul style="list-style-type: none"><li>当使用场景为虚拟私有云时，指云主机的端口号。</li><li>当使用场景为云专线时，指用户本地数据中心中服务器的端口号或私有端口号。</li><li>端口类型为“全部”时，不需要配置此参数。</li></ul> 私网端口需要与对应弹性IP的公网端口数量保持一致。
描述	DNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

6. 模板填写完后，单击“添加文件”，选择本地模板，单击“导入”。
7. 可在DNAT规则列表中查看详情，若“状态”为“运行中”，表示导入成功。

## 导出 DNAT 规则

1. 登录管理控制台。
2. 在公网NAT网关页面，单击需要导出DNAT规则的公网NAT网关名称。
3. 在公网NAT网关详情页面中，单击“DNAT规则”页签。
4. 在DNAT规则列表页，选择目标规则后，单击“导出”。
  - a. 选择“导出全部数据到XLSX”：系统会将当前区域内所有数据自动导出为Excel文件，并下载至本地。

- b. 选择“导出已选中数据到XLSX”：系统会将当前区域内您所选中的数据自动导出为Excel文件，并下载至本地。

# 4 私网 NAT 网关

## 4.1 私网 NAT 网关简介

### 什么是私网 NAT 网关？

私网NAT网关（Private NAT Gateway），能够为虚拟私有云内的云主机（弹性云服务器、裸金属服务器）提供私网地址转换服务。您可以在私网NAT网关上配置SNAT、DNAT规则，可将源、目的网段地址转换为中转IP，通过使用中转IP实现VPC内的云主机与其他VPC、云下IDC互访。

私网NAT网关分为SNAT和DNAT两个功能：

- SNAT功能通过绑定中转IP，可实现VPC内跨可用区的多个云主机共享中转IP，访问外部数据中心或其他VPC。
- DNAT功能通过绑定中转IP，可实现IP映射或端口映射，使VPC内跨可用区的多个云主机共享中转IP，为外部私网提供服务。

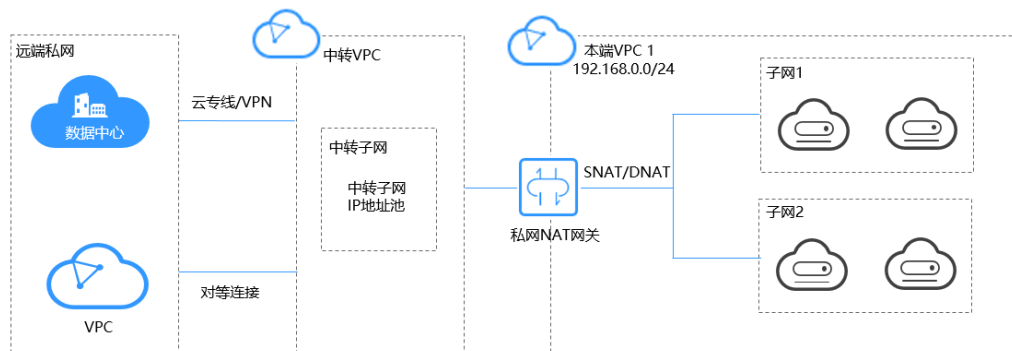
### 中转子网

中转子网相当于一个中转网络，您可以在中转子网中创建私网IP，即中转IP，使本端VPC中的云主机可以共享该中转IP访问用户IDC或其他远端VPC。

### 中转VPC

中转子网所在VPC。

图 4-1 私网 NAT 网关



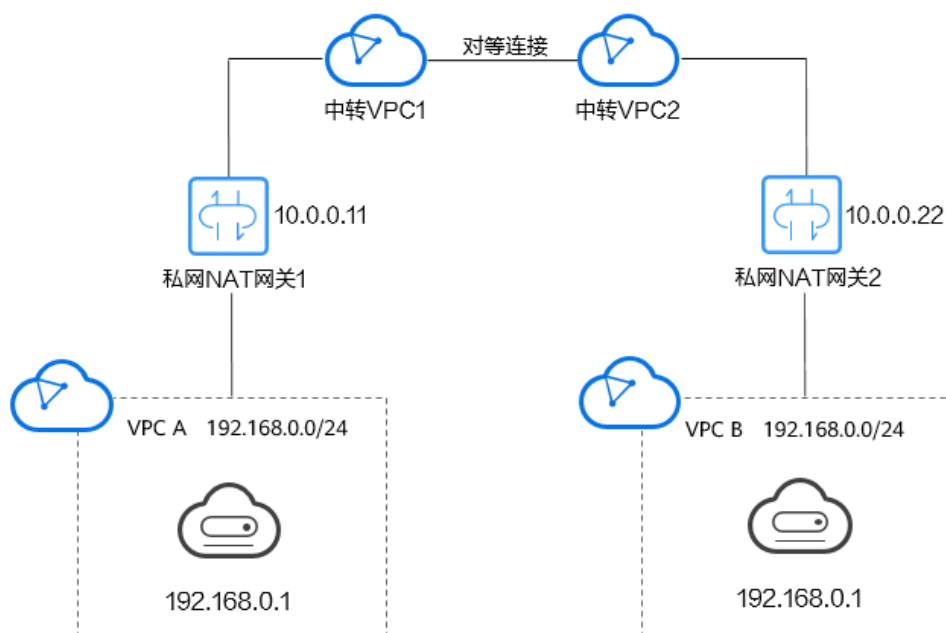
## 应用场景

- 重叠网段VPC间互通

私网NAT网关提供私网地址转换服务，利用两个私网NAT网关，配置SNAT、DNAT规则，可同时将源、目的网段地址转换为中转IP，通过使用中转IP实现两VPC间互通。私网NAT网关解决了两个重叠网段虚拟私有云中的云主机互相访问的问题。

如下图所示，创建一个中转VPC，然后使用两个私网NAT网关将VPC A中IP地址为192.168.0.1的弹性云服务器地址转化为10.0.0.11、将VPC B中IP地址为192.168.0.1的弹性云服务器地址转化为10.0.0.22，通过转化后的IP地址相互访问。

图 4-2 重叠网段 VPC 间互通

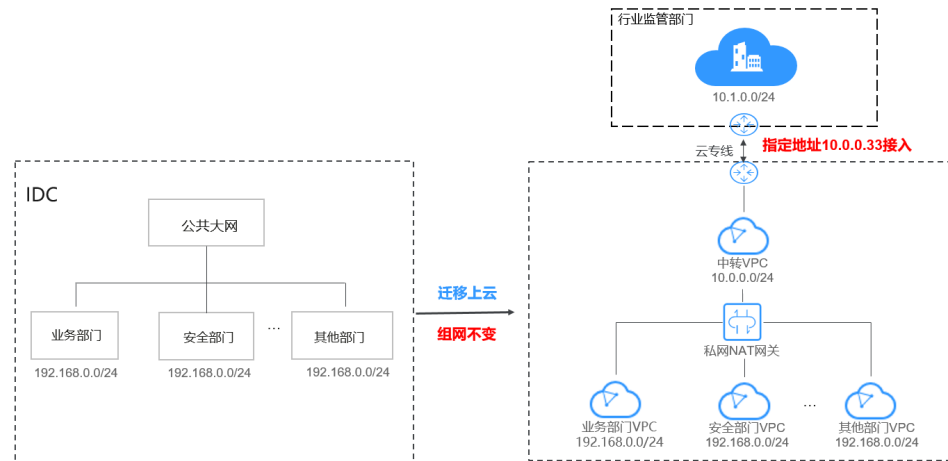


- 企业网络上云及指定IP接入

大企业等机构上云，希望迁移上云保持组网不变，使用私网NAT网关无需对网络做任何更改即可保持原有方式互通。同时，行业监管部门要求指定地址接入，使用私网NAT网关将各部门的IP地址映射为指定地址接入行业监管部门，满足企业安全规范。

如下图所示，企业部门间存在网段重叠，使用私网NAT网关，实现企业各部门迁移上云后组网不变，部门间保持原有方式互通，简化了IDC上云的网络规划；使用私网NAT网关，配置SNAT规则，将各部门的IP地址映射为符合要求的10.0.0.33地址接入行业监管部门，提升企业的安全性。

图 4-3 企业网络上云及指定 IP 接入



## 公网 NAT 网关与私网 NAT 网关对比

公网NAT网关通过配置SNAT规则将私有IP映射为弹性公网IP，实现VPC内的云主机通过共享弹性公网IP访问互联网；配置DNAT规则共享弹性公网IP为公网提供服务。

私网NAT网关通过配置SNAT规则将私有IP映射为中转IP，实现VPC内的云主机访问私网中的用户数据中心或其他VPC；配置DNAT规则共享中转IP为私网提供服务。

表1概括了公网NAT网关和私网NAT网关间的差异：

表 4-1 公网 NAT 网关与私网 NAT 网关对比

功能项	公网NAT网关	私网NAT网关
功能	私网和公网间互通	私网和私网间互通
SNAT功能	访问公网	访问私网中的IDC或其他VPC
DNAT功能	为公网提供服务	为私网中的IDC或其他VPC提供服务
互通媒介	弹性公网IP	中转IP

## 私网 NAT 网关使用流程

私网NAT网关的使用流程如下：

图 4-4 私网 NAT 网关使用流程



私网NAT网关配置完成，如果需要连接IDC或其他虚拟私有云，请参考[连接IDC或其他虚拟私有云](#)。

## 4.2 创建私网 NAT 网关

### 操作场景

如果您的VPC中的资源要通过私网NAT网关访问用户本地数据中心（IDC）或其他虚拟私有云，或面向私网提供服务，则需要私网NAT网关。

### 约束与限制

- 用户需要在VPC下手动添加私网路由，即通过创建对等连接或开通云专线/VPN连接远端私网。
- SNAT规则和DNAT规则不能共用同一个中转IP。
- 私网NAT网关支持添加的DNAT规则和SNAT规则的数量如下：
  - 小型：DNAT规则和SNAT规则的总数不超过20个。
  - 中型：DNAT规则和SNAT规则的总数不超过50个。
  - 大型：DNAT规则和SNAT规则的总数不超过200个。
  - 超大型：DNAT规则和SNAT规则的总数不超过500个。

#### 注意

创建私网NAT网关必须指定私网NAT网关所在VPC、子网、私网NAT网关规格。

### 操作步骤


1. 登录管理控制台。
2. 在页面左上角单击  图标，打开服务列表，选择“网络 > NAT网关”。  
进入NAT 网关页面。
3. 在NAT网关页面，单击“NAT网关 > 私网NAT网关”。
4. 在私网NAT网关页面，单击“创建私网NAT网关”，进入私网NAT网关创建页面。
5. 根据界面提示，配置私网NAT网关的基本信息，配置参数请参见表4-2。

表 4-2 参数说明

参数	参数说明
区域	私网NAT网关所在的区域。
名称	私网NAT网关名称。最大支持64个字符，仅支持中文、数字、字母、_（下划线）、-（中划线）、.（点）。
虚拟私有云	私网NAT网关所属的VPC。 VPC仅在创建私网NAT网关时可以选择，后续不支持修改。



参数	参数说明
子网	私网NAT网关所属VPC中的子网。 子网至少有一个可用的IP地址。 子网仅在创建私网NAT网关时可以选择，后续不支持修改。
规格	私网NAT网关的规格。 私网NAT网关共有小型、中型、大型、超大型四种规格类型。规格详情参见 <a href="#">产品规格</a> 。
描述	私网NAT网关信息描述。最大支持255个字符，且不能包含“<”和“>”。

- 单击“立即创建”。

## 更多操作

- [创建中转IP](#)
- [添加SNAT规则](#)
- [添加DNAT规则](#)
- [管理私网NAT网关](#)

## 4.3 管理私网 NAT 网关

私网NAT网关创建后，您可对您的私网NAT网关进行统一管理，包括修改私网NAT网关信息和删除私网NAT网关。

### 修改私网 NAT 网关

私网NAT网关创建后，如果您在使用过程中发现当前的NAT网关规格不能满足自己的需求，可以修改私网NAT网关规格、名称和描述。

- 登录管理控制台。
- 在NAT网关页面，单击“NAT网关> 私网NAT网关”。
- 在私网NAT网关页面，单击需要修改的私网NAT网关操作列中的“修改”。
- 根据界面提示，修改私网NAT网关的名称、规格或者描述等信息。
- 修改完成后，单击“下一步”。
- 确认私网NAT网关信息的修改，单击“提交”。

### 删除私网 NAT 网关

私网NAT网关创建后，如果您不再需要使用私网NAT网关，可以通过删除私网NAT网关，释放资源。

#### 说明

必须保证私网NAT网关下的SNAT规则和DNAT规则已全部删除。如果私网NAT网关下的SNAT规则和DNAT规则未被全部删除，则无法执行删除，请先在私网NAT网关页面进行[删除SNAT规则](#)和[删除DNAT规则](#)操作。

1. 登录管理控制台。
2. 在NAT网关页面，单击“NAT网关> 私网NAT网关”。
3. 在私网NAT网关页面，单击目标私网NAT网关操作列中的“删除”。
4. 在删除确认对话框，输入“DELETE”。
5. 单击“确定”。

## 4.4 管理 SNAT 规则

### 4.4.1 添加 SNAT 规则

#### 操作场景

私网NAT网关创建成功后，您需要创建SNAT规则。通过创建SNAT规则，VPC子网中全部或部分云主机可以通过共享中转IP访问用户本地数据中心（IDC）或其他VPC。

#### 约束与限制

VPC内的每个子网只能添加一条SNAT规则。

#### 前提条件

- 私网NAT网关创建成功。
- 中转IP创建成功。

#### 操作步骤

1. 登录管理控制台。
2. 在NAT网关页面，单击“NAT网关> 私网NAT网关”。
3. 在私网NAT网关页面，单击需要添加SNAT规则的私网NAT网关名称。
4. 在SNAT规则页签中，单击“添加SNAT规则”。
5. 根据界面提示，配置添加SNAT规则参数，详情请参见[表4-3](#)。

表 4-3 参数说明

参数	参数说明
子网	SNAT规则的子网类型，选择“使用已有”或“自定义”。 选择业务VPC中需要做地址映射的子网。
监控	可以为SNAT连接数设置告警，实时监控运行状态。
中转IP	选择已创建好的中转IP。
描述	SNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

- 配置完成后，单击确定，完成“SNAT规则”创建。

#### 说明

根据您的业务需求，可以为一个私网NAT网关添加多条SNAT规则。

## 相关链接

[管理SNAT规则](#)

## 4.4.2 修改 SNAT 规则

### 操作场景

添加SNAT规则后，如果SNAT规则设置有误，或者SNAT规则中的一些参数需要更新时，可以修改SNAT规则。

当您修改SNAT规则前，请您务必了解该操作可能带来的影响，避免误操作造成网络中断。

### 前提条件

私网NAT网关下存在成功添加的SNAT规则。

### 操作步骤

- 在私网NAT网关页面，单击目标私网NAT网关的名称。
- 系统跳转至目标私网NAT网关详情页面，单击“SNAT规则”页签。
- 在SNAT规则列表中，单击目标私网SNAT规则操作列中的“修改”。
- 在弹出的对话框中，修改参数中的内容。
- 单击“确定”，完成SNAT规则的修改。

## 4.4.3 删除 SNAT 规则

### 操作场景

添加SNAT规则后，如果不再需要此SNAT规则，您可以删除SNAT规则。

### 前提条件

私网NAT网关下存在成功添加的SNAT规则。

### 操作步骤

- 在私网NAT网关页面，单击目标私网NAT网关的名称。
- 在SNAT页签的SNAT规则列表中，单击目标SNAT规则操作列中的“删除”。
- 在弹出的对话框中单击“确定”，完成SNAT规则的删除。

## 4.5 管理 DNAT 规则

## 4.5.1 添加 DNAT 规则

### 操作场景

私网NAT网关创建后，通过添加DNAT规则，则可以通过映射方式将您VPC内的云主机实例对外部私网（IDC或其他VPC）提供服务。

云主机的每个端口分别对应一条DNAT规则，一个云主机的多个端口或者多个云主机需要为外部私网提供服务，则需要创建多条DNAT规则。

### 约束与限制

DNAT的全端口模式不能和具体端口模式共用同一个中转IP。

### 前提条件

- 已成功创建私网NAT网关。
- 中转IP创建成功。

### 操作步骤

1. 在私网NAT网关页面，单击需要添加DNAT规则的私网NAT网关名称。
2. 在私网NAT网关详情页面中，单击“DNAT规则”页签。
3. 在DNAT规则页签中，单击“添加DNAT规则”。

#### 须知

配置DNAT规则后，需在目标云主机实例中放通对应的安全组规则，否则DNAT规则不能生效。

4. 根据界面提示，配置添加DNAT规则参数，详情请参见[表4-4](#)。

表 4-4 DNAT 规则参数说明

参数	说明
<b>本端网络</b>	
端口类型	分为具体端口和所有端口两种类型。 <ul style="list-style-type: none"><li>• 具体端口：属于端口映射方式。私网NAT网关会将以指定协议和端口访问该中转IP的请求转发到目标云主机实例的指定端口上。</li><li>• 所有端口：属于IP映射方式。此方式相当于为云主机配置了一个私网IP（中转IP），任何访问该中转IP的请求都将转发到目标云服务器实例上。</li></ul>
支持协议	协议类型分为TCP和UDP两种类型。端口类型为所有端口时，此参数默认设置为All。 端口类型为具体端口时，可配置此参数。

参数	说明
实例类型	选择对外部私网提供服务的实例类型。 <ul style="list-style-type: none"><li>• 服务器</li><li>• 虚拟IP地址</li><li>• 负载均衡器</li><li>• 自定义</li></ul>
网卡	服务器网卡。实例类型为服务器时，需要配置此参数。
IP地址	对外部私网提供服务的云主机IP地址。实例类型为自定义时，需要配置此参数。
业务端口	实例对外提供服务的协议端口号。端口范围是1 ~ 65535。端口类型为具体端口时，需要配置此参数。
<b>中转网络</b>	
中转IP	通过该中转IP访问用户IDC或其他VPC。 这里只能选择没有被绑定的中转IP，或者被绑定在当前私网NAT网关中非“所有端口”类型DNAT规则上的中转IP，或者被绑定到当前私网NAT网关中SNAT规则上的中转IP。
中转IP端口	中转IP对外提供服务的端口号。端口范围是1 ~ 65535。端口类型为具体端口时，需要配置此参数。
描述	DNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

5. 配置完成后，单击“确定”，可在DNAT规则列表中查看详情，若“状态”为“运行中”，表示创建成功。

## 相关链接

[管理DNAT规则](#)

## 4.5.2 修改 DNAT 规则

### 操作场景

添加DNAT规则后，如果DNAT规则设置有误，或者DNAT规则中的一些参数需要更新时，可以修改DNAT规则。

当您修改SNAT规则前，请您务必了解该操作可能带来的影响，避免误操作造成网络中断。

### 前提条件

私网NAT网关下存在成功添加的DNAT规则。

## 操作步骤

1. 在私网NAT网关页面，单击目标私网NAT网关的名称。
2. 系统跳转至目标私网NAT网关详情页面，单击“DNAT规则”页签。
3. 在DNAT规则列表中，单击目标DNAT规则操作列中的“修改”。
4. 在弹出的对话框中，修改参数中的内容。
5. 单击“确定”，完成DNAT规则的修改。

### 4.5.3 删除 DNAT 规则

#### 操作场景

添加DNAT规则后，如果不需要此DNAT规则，您可以删除DNAT规则。

#### 前提条件

私网NAT网关下存在成功添加的DNAT规则。

#### 操作步骤

1. 在私网NAT网关页面，单击目标私网NAT网关的名称。
2. 系统跳转至目标私网NAT网关详情页面，单击“DNAT规则”页签。
3. 在DNAT规则列表中，单击目标DNAT规则操作列中的“删除”。
4. 在弹出的对话框中单击“确定”，完成DNAT规则的删除。

## 4.6 管理中转 IP

### 4.6.1 创建中转 IP

#### 操作场景

通过创建中转IP，使虚拟私有云内多个云主机可以共享中转IP访问用户本地数据中心（IDC）或其他虚拟私有云，或面向私网提供服务。

#### 操作步骤

1. 登录管理控制台。
2. 在NAT网关页面，单击“NAT网关> 私网NAT网关”。
3. 在私网NAT网关页面，单击“中转IP > 创建中转IP”，进入创建中转IP页面。
4. 根据界面提示，配置中转IP的基本信息，配置参数请参见表4-5。

表 4-5 中转 IP 参数说明

参数	参数说明
中转VPC	中转IP所在的VPC。

参数	参数说明
中转子网	中转子网相当于一个中转网络，是中转IP所属的子网。 子网至少有一个可用的IP地址。
中转IP	中转IP的分配方式有以下两种。 <b>自动分配：</b> 由系统自动分配中转IP地址。 <b>手动分配：</b> 手动指定中转IP地址。
IP地址	当中转IP的分配方式选择“手动分配”时，需要指定中转IP地址。 单击下方“查看已使用IP地址”可以查看所选子网中已使用的IP地址。
标签	私网NAT网关的标识，包括键和值。可以创建20个标签。

5. 单击“确定”，完成中转IP创建。

## 4.6.2 查看中转 IP

### 操作场景

中转IP创建完成后，您可以查看已创建的中转IP。

### 操作步骤

1. 在“中转IP”页签，单击目标中转IP名称。
2. 进入中转IP详情页，即可查看已创建的中转IP的详细信息。  
您可以查看到该中转IP所属的中转VPC、中转子网和关联的私网NAT网关等信息。

## 4.6.3 删除中转 IP

### 操作场景

当您不需要某个中转IP时，可以进行删除操作。

### 操作步骤

1. 在“中转IP”页签，单击目标中转IP操作列的“释放”。
2. 单击“确定”。

#### 说明

当中转IP已关联SNAT或DNAT规则时，无法删除。此时，如果要删除中转IP，请先释放该中转IP所关联的所有规则。

## 4.7 连接 IDC 或其他虚拟私有云

### 连接 IDC

当您需要VPC内的多个云主机与用户IDC进行连通时，可通过在中转VPC与用户IDC间创建云专线/VPN来实现。

高质量连通选择云专线，具体请参见《云专线用户指南》。

低成本连通选择VPN，具体请参见《虚拟专用网络用户指南》。

### 连接其他 VPC

当您需要VPC内的多个云主机与其他远端VPC进行连通时，可通过在中转VPC与其他远端VPC间创建对等连接来实现。

对等连接内容请参见《虚拟私有云用户指南》。



# 5 权限管理

## 5.1 创建用户并授权使用 NAT 网关

如果您需要对您所拥有的NAT网关（NAT Gateway，简称NAT网关）进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用NAT网关。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将NAT网关委托给更专业、高效的其他账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用NAT网关服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如[图5-1](#)所示。

### 前提条件

给用户组授权之前，请您了解用户组可以添加的NAT网关权限，并结合实际需求进行选择，NAT网关支持的系统权限，请参见：NAT网关系统权限。若您需要对除NAT网关之外的其它服务授权，IAM支持服务的所有策略请参见权限集。

## 示例流程

图 5-1 给用户授权 NAT 网关权限流程



1. 创建用户组并授权  
在IAM控制台创建用户组，并授予NAT网关服务权限“NATReadOnlyAccess”。
2. 创建用户并加入用户组  
在IAM控制台创建用户，并将其加入[1.创建用户组并授权](#)中创建的用户组。
3. 用户登录并验证权限。  
新创建的用户登录控制台，切换至授权区域，验证权限：
  - 在“服务列表”中选择NAT网关，进入NAT网关主界面，单击右上角“创建NAT网关”，如果无法创建NAT网关（假设当前权限仅包含NATReadOnlyAccess），表示“NATReadOnlyAccess”已生效。
  - 在“服务列表”中选择除NAT网关外（假设当前策略仅包含NATReadOnlyAccess）的任一服务，若提示权限不足，表示“NATReadOnlyAccess”已生效。

## 5.2 NAT 网关自定义策略

如果系统预置的NAT网关权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考《NAT网关接口参考》策略及授权项说明。

目前云服务平台支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：《统一身份认证服务》中“用户指南 > 管理细粒度策略 > 创建自定义策略。本章为您介绍常用的NAT网关自定义策略样例。

## 策略样例

- 示例1：授权用户创建和删除NAT网关

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "nat:natGateways:create",
        "nat:natGateways:delete"
      ]
    }
  ]
}
```

- 示例2：拒绝用户删除NAT网关

拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

如果您给用户授予NAT FullAccess的系统策略，但不希望用户拥有NAT FullAccess中定义的删除NAT网关权限，您可以创建一条拒绝删除NAT网关的策略，然后同时将NAT FullAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以对NAT网关执行除了删除NAT网关外的所有操作。拒绝策略示例如下：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "nat:natGateways:delete"
      ],
      "Effect": "Deny"
    }
  ]
}
```

- 示例3：多个授权项策略

一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "nat:natGateways:update",
        "nat:natGateways:create"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "vpc:vpcs:update"
      ],
      "Effect": "Allow"
    }
  ]
}
```

# 6 使用 CES 监控 NAT 网关

## 6.1 支持的监控指标

### 功能说明

本节定义了NAT网关上报云监控的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控提供的管理控制台或API接口来检索NAT网关产生的监控指标。

### 命名空间

SYS.NAT

### 监控指标

表 6-1 公网 NAT 网关支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
snat_connection	SNAT 连接数	该指标用于统计测量对象的SNAT连接数。 单位：个	$\geq 0$ 个	公网NAT网关	1分钟
inbound_bandwidth	入方向带宽	该指标用于统计入方向带宽。 单位：比特/秒	$\geq 0$ bit/s	公网NAT网关	1分钟
outbound_bandwidth	出方向带宽	该指标用于统计SNAT出方向带宽。 单位：比特/秒	$\geq 0$ bit/s	公网NAT网关	1分钟
inbound_pps	入方向PPS	该指标用于统计SNAT入方向PPS。 单位：个	$\geq 0$ 个	公网NAT网关	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
outbound_pps	出方向 PPS	该指标用于统计SNAT出方向PPS。 单位：个	≥0个	公网NAT网关	1分钟
inbound_traffic	入方向流量	该指标用于统计SNAT入方向流量。 单位：字节	≥0 bytes	公网NAT网关	1分钟
outbound_traffic	出方向流量	该指标用于统计SNAT出方向流量。 单位：字节	≥0 bytes	公网NAT网关	1分钟
snat_connection_ratio	SNAT连接数使用率	该指标用于统计测量对象的SNAT连接数使用率。连接数最大为规格限制的连接数。 单位：百分比	≥0	公网NAT网关	1分钟
inbound_bandwidth_ratio	入方向带宽使用率	该指标用于统计SNAT入方向带宽使用率。 公网NAT网关最大带宽20Gbit/s，则入方向带宽使用率为： <b>实际使用带宽/公网NAT实例最大带宽*100%</b> 。 单位：百分比 <b>说明</b> 该监控项为针对公网NAT实例性能的监控而不是针对EIP带宽的监控。	≥0	公网NAT网关	1分钟
outbound_bandwidth_ratio	出方向带宽使用率	该指标用于统计SNAT出方向带宽使用率。 公网NAT网关最大带宽为20Gbit/s，则出方向带宽使用率为： <b>实际使用带宽/公网NAT实例最大带宽*100%</b> 。 单位：百分比 <b>说明</b> 该监控项为针对公网NAT网关性能的监控而不是针对EIP带宽的监控。	≥0	公网NAT网关	1分钟

表 6-2 私网 NAT 网关支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
snat_connection	SNAT连接数	该指标用于统计测量对象的SNAT连接数。 单位: 个	≥ 0 个	私网NAT网关	1分钟
inbound_bandwidth	入方向带宽	该指标用于统计入方向带宽。 单位: 比特/秒	≥0 bit/s	私网NAT网关	1分钟
outbound_bandwidth	出方向带宽	该指标用于统计出方向带宽。 单位: 比特/秒	≥0 bit/s	私网NAT网关	1分钟
inbound_pps	入方向PPS	该指标用于统计入方向PPS。 单位: 个	≥0个	私网NAT网关	1分钟
outbound_pps	出方向PPS	该指标用于统计出方向PPS。 单位: 个	≥0个	私网NAT网关	1分钟
inbound_traffic	入方向流量	该指标用于统计入方向流量。 单位: 字节	≥0 bytes	私网NAT网关	1分钟
outbound_traffic	出方向流量	该指标用于统计出方向流量。 单位: 字节	≥0 bytes	私网NAT网关	1分钟

## 维度

Key	Value
nat_gateway_id	公网NAT网关
vpc_nat_gateway_id	私网NAT网关

## 6.2 创建告警规则

### 操作场景

通过设置NAT网关告警规则，用户可自定义监控目标与通知策略，及时了解NAT网关运行状况，从而起到预警作用。

### 操作步骤

1. 登录管理控制台。
2. 选择“管理与部署 > 云监控服务”。
3. 在左侧导航树栏，选择“告警 > 告警规则”。
4. 在“告警规则”界面，单击“创建告警规则”，根据界面提示，填写对应参数。
5. 规则参数设置完成后，单击“下一步”，根据界面提示，配置规则信息参数。
6. 单击“创建”，完成SNAT连接数告警规则的创建。设置告警规则后，超过设置的阈值，系统会自动进行通知。

#### 说明

更多关于设置告警规则的信息，请参见《云监控用户指南》。

## 6.3 查看监控指标

### 前提条件

- NAT网关正常运行，并且已经创建SNAT规则。
- 由于监控数据的获取与传输会花费一定时间，因此，请等待一段时间后再查看监控数据。

### 操作场景

查看NAT网关的监控指标详情。

### 操作步骤

1. 登录管理控制台。
2. 在左上角中的切换区域下拉列框中，选择目标区域。
3. 选择“管理与部署 > 云监控”。
4. 单击页面左侧的“云服务监控”，选择“NAT网关”。
5. 单击“操作”列的“查看监控图表”，查看NAT网关的监控指标详情。  
支持查看“近1小时”、“近3小时”和“近12小时”的数据。

# 7 常见问题

## 7.1 公网 NAT 网关

### 7.1.1 公网 NAT 网关、弹性公网 IP 带宽、VPC 内弹性云服务器与 VPC 是什么样的关系？

- VPC是虚拟私有云，通过逻辑方式进行网络隔离，提供安全、隔离的网络环境。
- 公网NAT网关能够为VPC内的弹性云服务器提供访问外网的能力。
- 弹性公网IP是可以提供互联网上合法的静态IP地址的服务，VPC的吞吐量由弹性公网IP带宽决定。
- 弹性云服务器是VPC内的运行实例，使用公网NAT网关访问外网。

### 7.1.2 公网 NAT 网关如何实现高可用性？

公网NAT网关后台已通过双机热备实现自动容灾，降低风险提高可用性。

### 7.1.3 公网 NAT 网关丢包数超限（EIP 端口分配超限）怎么办？

如果公网NAT网关使用中，监控显示丢包数超限（EIP端口分配超限），这是SNAT规则上绑定的EIP端口已被占用完导致的。建议您在SNAT规则上增加绑定的EIP数量以解决该问题。

## 7.2 私网 NAT 网关


### 7.2.1 私网 NAT 配置后组网不通怎么排查？

#### 检查安全组规则


如果安全组没有放通弹性云服务器访问和对外提供服务使用的端口，需要在弹性云服务器对应的安全组中添加放行该端口的规则。

**步骤1** 登录管理控制台。



- 步骤2** 在管理控制台左上角单击 ，选择区域和项目。
- 步骤3** 选择“计算 > 弹性云服务器”。
- 步骤4** 在弹性云服务器列表，单击待检查安全组规则的弹性云服务器名称。
- 步骤5** 选择“安全组”页签，展开安全组规则。
- 步骤6** 检查入方向规则和出方向规则是否已经配置放行弹性云服务器使用端口的规则。
- 如果已配置放行弹性云服务器使用端口规则，请[检查路由表是否配置指向私网 NAT 网关的路由](#)。
  - 如果未配置放行弹性云服务器使用端口的规则，请单击“配置规则”，进入安全组详情页，按[步骤7](#)进行配置。
- 步骤7** 在安全组详情页，单击“入方向规则”或“出方向规则”，分别根据弹性云服务器使用的端口添加入方向规则或出方向规则。
- 结束

## 检查路由表是否配置指向私网 NAT 网关的路由

- 步骤1** 登录管理控制台。
- 步骤2** 在管理控制台左上角单击 ，选择区域和项目。
- 步骤3** 在系统首页，选择“网络 > 虚拟私有云”。
- 步骤4** 在左侧导航栏选择“路由表”。
- 步骤5** 在路由表列表中，单击私网 NAT 网关所在 VPC 的路由表名称。
- 步骤6** 检查路由列表中是否存在指向私网 NAT 网关的路由。
- 结束

## 7.2.2 一个 VPC 最多支持创建多少个私网 NAT？

当前单个 VPC 最多支持创建 10 个私网 NAT。

## 7.2.3 私网 NAT 支持云专线的 IP 转换吗？

支持。在创建 DNAT 规则时，选择自定义模式，可添加通过云专线接入的客户云下 IP。

## 7.2.4 私网 NAT 和公网 NAT 有什么区别？

私网 NAT 是实现私网 IP 与私网 IP 之间的地址转换。

私网 NAT 的作用有：

- 通过私网 IP 地址转换，解决私网 IP 地址冲突的问题。
- 通过私网 IP 地址转换，满足指定地址接入的需求。

公网 NAT 是实现私网 IP 与公网 IP 之间的地址转换。

公网 NAT 的作用有：

- 更安全：避免云主机公网IP直接暴露在外。
- 省成本：共享EIP，共享带宽，节约EIP资源。

## 7.2.5 私网 NAT 是否支持跨账号使用？

私网NAT本身不支持跨账号使用，但可以通过VPC对等连接实现跨账户通信，VPC对等连接打通两个账号的中转VPC，实现两个私网NAT转换IP后的跨账号通信。

## 7.3 SNAT 规则

### 7.3.1 为什么使用 SNAT？

对公网NAT网关来说，一些弹性云服务器不仅需要系统提供的服务，还需要访问外网以获取信息或下载软件。但是，给弹性云服务器分配公网IP需要消耗稀缺资源（如IPv4地址），增加额外的成本，并有可能增加虚拟环境遭受攻击的几率。因此，多个弹性云服务器共享同一公网IP是一种可行的方法，具体实施方法为源地址转换（SNAT）。

对私网NAT网关来说，在大企业不同部门间存在大量重叠网段，上云后无法互通，通过私网SNAT可以将一个部门多个弹性云服务器的IP转化为一个中转IP去访问别的部门；因为安全受限等原因，行业监管部门要求各机构和单位按指定IP地址接入，通过私网SNAT可以将多个弹性云服务器的IP转化为一个中转IP，去访问行业监管部门。

### 7.3.2 什么是 SNAT 连接数？

SNAT连接数是NAT网关执行源地址转换时创建的活动连接的数量。由源IP地址、源端口、目的IP地址、目的端口、传输层协议这五个元素组成的集合视为一条连接。连接能够区分不同会话，并且对应的会话是唯一的。其中源IP地址和源端口指SNAT转换之后的IP和它的端口。

由于SNAT支持TCP、UDP和ICMP三种协议，每一个目的IP和目的端口，NAT网关最多可支持55000个并发连接。如果目的IP、端口或者协议（TCP/UDP/ICMP）发生变化，则可以再创建55000个连接。弹性云服务器中通过netstat命令看到ESTABLISHED状态的连接数，仅反映了服务器侧视角的连接数。但实际的SNAT连接数包括了NAT网关上维护的连接表项，由于存在连接超时、连接复用等影响，可能与弹性云服务器侧ESTABLISHED状态的连接数存在差异。假设一个弹性云服务器平均每秒钟创建100个与固定目的的连接，不考虑连接老化的话，大约10分钟会将55000个连接耗尽导致连接无法新建。

NAT网关中SNAT连接如果长时间没有数据报文，会超时断开。

## 7.4 DNAT 规则

### 7.4.1 为什么使用 DNAT？

公网NAT网关的DNAT功能绑定弹性公网IP，可通过IP映射或端口映射两种方式，实现VPC内跨可用区的多个云主机共享弹性公网IP，为互联网提供服务。详见[添加DNAT规则](#)。

私网NAT网关的DNAT功能通过绑定中转IP，可实现IP映射或端口映射，使VPC内跨可用区的多个云主机共享中转IP，为外部私网提供服务。详见《NAT网关用户指南》私网NAT网关中的“添加DNAT规则”章节。

## 7.4.2 DNAT 规则是否支持更新操作？

DNAT规则支持更新操作。公网NAT网关和私网NAT网关均支持修改DNAT规则。

# A 修订记录

---

发布日期	修订记录
2024-04-15	第一次发布。