

ALIBABA CLOUD

阿里云

专有云企业版

NAT网关
用户指南

产品版本：v3.16.2

文档版本：20220915

 阿里云

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
 危险	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。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会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，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	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。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

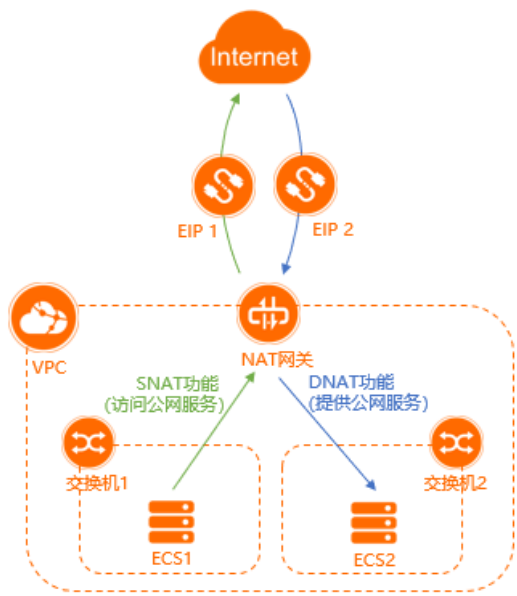
目录

1.什么是NAT网关	06
2.登录NAT网关管理控制台	07
3.快速入门	08
3.1. 入门概述	08
3.2. 创建NAT网关	09
3.3. 绑定弹性公网IP	10
3.4. 创建DNAT条目	10
3.5. 创建SNAT条目	11
4.管理NAT网关	13
4.1. NAT网关实例概述	13
4.2. 创建NAT网关	13
4.3. 修改NAT网关	14
4.4. 删除NAT网关	15
4.5. 管理标签	15
5.管理弹性公网IP	17
5.1. 绑定弹性公网IP	17
5.2. 解绑弹性公网IP	17
6.管理DNAT表	18
6.1. DNAT概述	18
6.2. 创建DNAT条目	18
6.3. 修改DNAT条目	19
6.4. 删除DNAT条目	20
7.管理SNAT表	21
7.1. SNAT表概述	21
7.2. 创建SNAT条目	21
7.3. 修改SNAT条目	22

7.4. 删除SNAT条目	22
8.NAT带宽包	24
8.1. 创建NAT带宽包	24
8.2. 修改NAT带宽包的带宽	24
8.3. 添加IP地址	25
8.4. 释放IP地址	25
8.5. 删除NAT带宽包	25
9.DDoS基础防护	26

1.什么是NAT网关

NAT网关（NAT Gateway）是一款企业级的公网网关，提供NAT代理（SNAT和DNAT）功能，具有10 Gbps级别的转发能力和跨可用区的容灾能力。



功能简介

NAT网关作为一个网关设备，需要绑定公网IP才能正常工作。创建NAT网关后，您可以为NAT网关绑定弹性公网IP（Elastic IP Address，简称EIP）。

NAT网关支持SNAT和DNAT功能，功能说明如下：

功能	说明
SNAT 功能	为专有网络VPC（Virtual Private Cloud）内无公网IP的ECS实例提供访问公网的代理服务。
DNAT 功能	将NAT网关上绑定的EIP映射给ECS实例使用，使ECS实例可以面向公网提供服务。

2. 登录NAT网关管理控制台

本节以Chrome浏览器为例，介绍NAT网关（NAT Gateway）用户如何登录到Apsara Uni-manager运营控制台。


前提条件

- 登录Apsara Uni-manager运营控制台前，确认您已从部署人员处获取Apsara Uni-manager运营控制台的服务域名地址。
- 推荐使用Chrome浏览器。

操作步骤

1. 在浏览器地址栏中，输入Apsara Uni-manager运营控制台的访问地址，按回车键。
2. 输入正确的用户名及密码。


请向运营管理员获取登录控制台的用户名和密码。

 **说明** 首次登录Apsara Uni-manager运营控制台时，需要修改登录用户名的密码，请按照提示完成密码修改。为提高安全性，密码长度必须为 8~20 位，且至少包含以下两种类型：

- 英文大写或小写字母（A~Z、a~z）
- 阿拉伯数字（0~9）
- 特殊符号（感叹号（!）、at（@）、井号（#）、美元符号（\$）、百分号（%）等）

3. 单击**登录**。
4. 如果账号已激活MFA多因素认证，请根据以下两种情况进行操作：
 - 管理员强制开启MFA后的首次登录：
 - a. 在绑定虚拟MFA设备页面中，按页面提示步骤绑定MFA设备。
 - b. 按照步骤2重新输入账号和密码，单击**账号登录**。
 - c. 输入6位MFA码后单击**认证**。
 - 您已开启并绑定MFA：

输入6位MFA码后单击**认证**。

 **说明** 绑定并开启MFA的操作请参见Apsara Uni-manager运营控制台用户指南中的**绑定并开启虚拟MFA设备**章节。

5. 在页面顶部的菜单栏中，选择**产品 > 网络 > 专有网络 VPC**。
6. 在左侧导航栏，单击**NAT网关**。

3.快速入门

3.1. 入门概述

本文提供SNAT和DNAT完整的配置过程，使VPC中的ECS实例可以通过NAT网关与互联网通信。

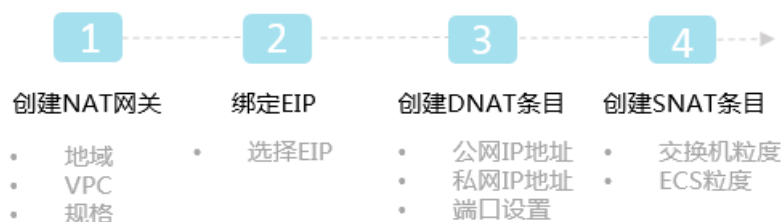
前提条件

在开始之前，请确保满足以下条件：

- 您已经创建了专有网络。更多信息，请参见[专有网络VPC用户指南手册中快速入门下的创建专有网络章节](#)。
- 您已经创建了专有网络类型的ECS实例。更多信息，请参见[云服务器ECS用户指南手册中快速入门下的创建实例章节](#)。
- 您已经创建了弹性公网IP（Elastic IP Address，简称EIP）。更多信息，请参见[弹性公网IP用户指南手册中快速入门下的申请EIP章节](#)。

配置流程说明

本文以一台没有绑定任何公网IP的专有网络ECS实例为例。配置流程图如下：



1. 创建NAT网关

NAT网关是一款企业级的VPC公网网关，提供NAT代理功能。在配置SNAT和DNAT规则前，您需要先创建NAT网关。

具体操作，请参见[创建NAT网关](#)。

2. 绑定EIP

NAT网关作为一个网关设备，需要绑定公网IP才能正常工作。创建NAT网关后，您可以为NAT网关绑定EIP。

具体操作，请参见[绑定弹性公网IP](#)。

3. 创建DNAT条目

NAT网关支持DNAT功能，将NAT网关上的公网IP映射给ECS实例使用，使ECS实例能够提供互联网服务。DNAT支持端口映射和IP映射。

具体操作，请参见[创建DNAT条目](#)。

4. 创建SNAT条目

NAT网关支持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。

具体操作，请参见[创建SNAT条目](#)。

3.2. 创建NAT网关

NAT网关是一款企业级的公网网关，提供NAT代理功能。在配置SNAT和DNAT规则前，您需要先创建一个NAT网关实例。

前提条件

您已经创建了专有网络VPC（Virtual Private Cloud）。具体操作，请参见[专有网络VPC用户指南手册中快速入门下的创建专有网络章节](#)。

操作步骤

1. [登录NAT网关管理控制台](#)。
2. 在NAT网关页面，单击**创建NAT网关**。
3. 在创建NAT网关页面，配置以下参数信息，然后单击**提交**。

配置	说明
区域	
组织	选择NAT网关所属的组织。
资源集	选择NAT网关所属的资源集。
地域	选择NAT网关所属的地域。
基本配置	
VPC	<p>选择NAT网关所属的VPC。</p> <p>如果在VPC列表中，找不到目标VPC，请从以下方面进行排查：</p> <ul style="list-style-type: none">◦ 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。如果存在，请删除该路由条目。
共享范围	<p>选择VPC的共享范围。</p> <ul style="list-style-type: none">◦ 本资源集：本资源集的管理员可以使用共享VPC创建资源。◦ 本组织及下级组织：本组织及下级组织的管理员可以使用共享VPC创建资源。◦ 本组织：本组织的管理员可以使用共享VPC创建资源。
规格	<p>选择NAT网关规格，支持以下规格：</p> <ul style="list-style-type: none">◦ 小型：SNAT最大连接数为1万。◦ 中型：SNAT最大连接数为5万。◦ 大型：SNAT最大连接数为20万。◦ 超大型-1：SNAT最大连接数为100万。 <div><p> 说明 不同规格的NAT网关会影响SNAT最大连接数，但不会影响DNAT连接数。</p></div>

配置	说明
名称	输入NAT网关的名称。 名称长度在2~128个字符之间，必须以英文字母和中文字符开头，可包含数字、下划线（_）、短划线（-）、半角句号（.），但不能以 <code>http://</code> 或 <code>https://</code> 开头。

3.3. 绑定弹性公网IP

NAT网关作为一个网关设备，需要绑定弹性公网IP（Elastic IP Address，简称EIP）才能正常工作。创建NAT网关后，您可以为NAT网关绑定EIP。

前提条件

EIP绑定NAT网关前，请确保满足以下条件：

- 您已经创建了NAT网关。更多信息，请参见[创建NAT网关](#)。
- 您已经申请了EIP。更多信息，请参见[弹性公网IP用户指南手册中快速入门下的申请EIP章节](#)。

操作步骤

1. [登录NAT网关管理控制台](#)。
2. 在顶部菜单栏，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关实例，然后在操作列选择... > 绑定弹性公网IP。
4. 在绑定弹性公网IP对话框，配置以下信息，然后单击确定。

配置	说明
可用EIP列表	选择提供互联网访问的EIP。

3.4. 创建DNAT条目

NAT网关支持DNAT功能，将NAT网关上的公网IP映射给ECS实例使用，使ECS实例能够提供互联网服务。DNAT支持端口映射和IP映射。

操作步骤

1. [登录NAT网关管理控制台](#)。
2. 在顶部菜单栏，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关实例，然后在操作列单击设置DNAT。
4. 在DNAT管理页签，单击创建DNAT条目。
5. 在创建DNAT条目对话框，根据以下信息配置DNAT条目，然后单击确定。

配置	说明
----	----

配置	说明
公网IP地址	<p>选择一个可用的公网IP。</p> <div><p> 说明 用于创建SNAT条目的公网IP不能再用来创建DNAT条目。</p></div>
私网IP地址	<p>选择要通过DNAT规则进行公网通信的ECS实例。您可以通过以下两种方式指定目标ECS实例的私网IP：</p> <ul style="list-style-type: none">从ECS或弹性网卡对应IP进行选择：从ECS实例或弹性网卡列表中选择ECS实例。自填：输入目标ECS实例的私网IP。 <div><p> 说明 自填的私网IP必需属于本VPC的CIDR范围，也可直接输入一个已有的ECS的私网IP。</p></div>
端口设置	<p>选择DNAT映射的方式：</p> <ul style="list-style-type: none">所有端口：该方式属于IP映射，任何访问该公网IP的请求都将转发到目标ECS实例上。具体端口：该方式属于端口映射，NAT网关会以指定协议和端口访问该公网IP的请求转发到目标ECS实例的指定端口上。 <p>选择具体端口后，请根据业务需求输入公网端口（进行端口转发的外部端口）、私网端口（进行端口转发的内部端口）和协议类型（转发端口的协议类型）。</p>

3.5. 创建SNAT条目

NAT网关的SNAT功能可以为VPC中无公网IP的ECS实例提供访问互联网的代理服务。

操作步骤

1. 登录NAT网关管理控制台。
2. 在顶部菜单栏，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关实例，然后在操作列单击**设置SNAT**。
4. 在SNAT管理页签，单击**创建SNAT条目**。
5. 在创建SNAT条目对话框，根据以下信息配置SNAT条目，然后单击**确定**。

配置	说明
----	----

配置	说明
粒度设置	<p>选择SNAT条目的粒度。</p> <ul style="list-style-type: none">◦ 交换机粒度：指定交换机下的ECS实例通过配置的公网IP访问互联网。<ul style="list-style-type: none">■ 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。◦ ECS粒度：指定的ECS实例通过配置的公网IP访问互联网。<ul style="list-style-type: none">■ 可用ECS列表：选择VPC中的ECS实例。<p>该ECS实例将通过配置的公网IP访问互联网。请确保ECS实例满足以下条件：</p><ul style="list-style-type: none">■ ECS实例的状态处于运行中。■ ECS实例不具备固定公网IP且未绑定其他弹性公网IP。■ ECS网段：显示该ECS实例的网段。
公网IP地址	<p>选择用来提供互联网访问的公网IP。</p> <p>支持选择1个或多个公网IP，多个公网IP可以构建SNAT IP地址池。</p> <div> 说明 用于创建DNAT条目的公网IP不能再用来创建SNAT条目。</div>
条目名称	<p>SNAT条目的名称。</p> <p>名称长度为2~128个字符，以大小写字母或中文开头，可包含数字、下划线（_）和短划线（-）。</p>

4. 管理NAT网关

4.1. NAT网关实例概述

NAT网关（NAT Gateway）是一款企业级的公网网关，提供NAT代理（SNAT和DNAT）、高达10 Gbps级别转发能力以及跨可用区的容灾能力。

实例规格

NAT网关提供小型、中型、大型和超大型-1规格。不同规格的NAT网关会影响SNAT最大连接数和SNAT每秒新建连接数，但不会影响DNAT性能。不同规格的NAT网关的对比如下表所示。

规格	SNAT最大连接数	SNAT每秒新建连接数
小型	1万	1千
中型	5万	5千
大型	20万	1万
超大型-1	100万	5万

在选择NAT网关规格时，请注意：

- NAT网关在云监控控制台只提供最大连接数监控，不提供每秒新建连接数监控。
- NAT网关SNAT的连接超时时间为900秒。
- 为避免网络拥塞、公网抖动可能造成的SNAT连接超时，请确保您的业务应用有自动重连机制，这样可以提供更高的可用性。
- NAT网关暂不支持报文分片。
- 对于公网上同一个目的IP和端口，NAT网关配置的EIP数限制NAT网关的最大并发数，绑定单个EIP最大连接数为55000，绑定多个EIP可以提升为 $N \times 55000$ 。

4.2. 创建NAT网关

NAT网关是一款企业级的公网网关，提供NAT代理功能。在配置SNAT和DNAT规则前，您需要先创建一个NAT网关实例。

前提条件

您已经创建了专有网络VPC（Virtual Private Cloud）。具体操作，请参见[专有网络VPC用户指南手册中快速入门下的创建专有网络章节](#)。

操作步骤

1. [登录NAT网关管理控制台](#)。
2. 在NAT网关页面，单击创建NAT网关。
3. 在创建NAT网关页面，配置以下参数信息，然后单击提交。



配置	说明
区域	
组织	选择NAT网关所属的组织。
资源集	选择NAT网关所属的资源集。
地域	选择NAT网关所属的地域。
基本配置	
VPC	<p>选择NAT网关所属的VPC。</p> <p>如果在VPC列表中，找不到目标VPC，请从以下方面进行排查：</p> <ul style="list-style-type: none"> 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。如果存在，请删除该路由条目。
共享范围	<p>选择VPC的共享范围。</p> <ul style="list-style-type: none"> 本资源集：本资源集的管理员可以使用共享VPC创建资源。 本组织及下级组织：本组织及下级组织的管理员可以使用共享VPC创建资源。 本组织：本组织的管理员可以使用共享VPC创建资源。
规格	<p>选择NAT网关规格，支持以下规格：</p> <ul style="list-style-type: none"> 小型：SNAT最大连接数为1万。 中型：SNAT最大连接数为5万。 大型：SNAT最大连接数为20万。 超大型-1：SNAT最大连接数为100万。 <div> <p> 说明 不同规格的NAT网关会影响SNAT最大连接数，但不会影响DNAT连接数。</p> </div>
名称	<p>输入NAT网关的名称。</p> <p>名称长度在2~128个字符之间，必须以英文字母和中文字符开头，可包含数字、下划线（_）、短划线（-）、半角句号（.），但不能以 <code>http://</code> 或 <code>https://</code> 开头。</p>

4.3. 修改NAT网关

您可以修改NAT网关的名称和描述。

操作步骤

1. 登录NAT网关管理控制台。
2. 在顶部菜单栏，选择NAT网关的地域。

3. 在NAT网关页面，找到目标NAT网关，然后在操作列单击**管理**。
4. 在**基本信息**页签，在NAT网关名称右侧单击图标，在弹出的对话框输入NAT网关的名称，然后单击**确定**。
5. 在**描述**右侧单击图标，在弹出的对话框输入描述信息，然后单击**确定**。

4.4. 删除NAT网关

如果您不需要NAT网关服务了，您可以删除NAT网关。


前提条件

删除NAT网关前，请确保满足以下条件。

- NAT网关没有绑定EIP，如有绑定请解绑。具体操作，请参见[解绑弹性公网IP](#)。
- DNAT列表中没有DNAT条目，如有请删除。具体操作，请参见[删除DNAT条目](#)。
- SNAT列表中没有SNAT条目，如有请删除。具体操作，请参见[删除SNAT条目](#)。

操作步骤


1. [登录NAT网关管理控制台](#)。
2. 在顶部菜单栏，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关，然后在操作列选择... > **删除**。
4. 在弹出的对话框，单击**确定**。

 **说明** 您也可以在弹出的对话框选中**强制删除**，在删除NAT网关后自动删除NAT网关中的DNAT条目、SNAT条目，并解绑EIP。强制删除NAT网关时，无需提前删除NAT网关中的DNAT条目、SNAT条目及绑定的EIP。

4.5. 管理标签

NAT网关支持标签功能，您可以通过标签功能来标记和分类NAT网关实例，以便于您对实例进行搜索和筛选。

操作步骤

1. [登录NAT网关管理控制台](#)。
2. 在顶部菜单栏，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关实例，鼠标悬停在**标签**列下-或已有标签右侧，然后单击图标。
4. 在**编辑标签**对话框，单击**添加**，根据以下信息配置标签，然后单击**确定**。

配置	说明
标签键	标签的标签键，支持选择已有标签键或输入新的标签键。 标签键最多支持64个字符，不能以 <code>aliyun</code> 或 <code>acs:</code> 开头，不能包含 <code>http://</code> 和 <code>https://</code> 。

配置	说明
标签值	标签的标签值，支持选择已有标签值或输入新的标签值。 标签值最多支持128个字符，不能以 aliyun 或 acs: 开头，不能包含 http:// 和 https:// 。

5. 返回NAT网关页面，单击**标签筛选**，可在**标签筛选**对话框根据标签键和标签值来筛选NAT网关实例。

5.管理弹性公网IP

5.1. 绑定弹性公网IP

NAT网关作为一个网关设备，需要绑定弹性公网IP（Elastic IP Address，简称EIP）才能正常工作。创建NAT网关后，您可以为NAT网关绑定EIP。

前提条件

EIP绑定NAT网关前，请确保满足以下条件：

- 您已经创建了NAT网关。更多信息，请参见[创建NAT网关](#)。
- 您已经申请了EIP。更多信息，请参见[弹性公网IP用户指南手册中快速入门下的申请EIP](#)章节。

操作步骤

1. [登录NAT网关管理控制台](#)。
2. 在顶部菜单栏，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关实例，然后在操作列选择... > 绑定弹性公网IP。
4. 在绑定弹性公网IP对话框，配置以下信息，然后单击确定。

配置	说明
可用EIP列表	选择提供互联网访问的EIP。

5.2. 解绑弹性公网IP

如果您的NAT网关不需要与公网通信，您可以将NAT网关与弹性公网IP（Elastic IP Address，简称EIP）解绑。

前提条件

请确保要解绑的EIP没有被任何SNAT或DNAT条目占用。如有占用，请先删除SNAT条目和DNAT条目。具体操作，请参见[删除SNAT条目](#)和[删除DNAT条目](#)。

操作步骤

1. [登录NAT网关管理控制台](#)。
2. 在顶部菜单栏，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关，然后在操作列单击... > 解绑弹性公网IP。
4. 在解绑弹性公网IP对话框，选择要解绑的EIP，然后单击确定。

6. 管理DNAT表

6.1. DNAT概述

NAT网关支持目的网络地址转换DNAT（Destination Network Address Translation）功能，将NAT网关上的公网IP映射给专有网络的ECS实例使用，使ECS实例可以面向互联网提供服务。

DNAT条目

您可以通过在DNAT表中创建DNAT条目，实现端口转发的功能。创建DNAT条目后，公网IP收到的请求将按照自定义的映射规则，转发给专有网络VPC内的ECS实例。

每个DNAT条目由以下五部分组成：

- **公网IP**：NAT网关绑定的弹性公网IP（EIP）。
- **私网IP**：专有网络中ECS实例的私网IP。
- **公网端口**：进行端口转发的外部端口。
- **私网端口**：进行端口转发的内部端口。
- **协议类型**：转发端口的协议类型。

端口映射和IP映射

DNAT功能包括端口映射与IP映射：

- **端口映射**

配置端口映射后，NAT网关会将指定协议和端口访问该公网IP的请求转发到目标ECS实例的指定端口上。如下表DNAT条目为例：

- 条目1：NAT网关会将访问1.1.XX.XX的TCP 80端口的请求转发到192.168.1.1的TCP 80端口上。
- 条目2：NAT网关会将访问2.2.XX.XX的UDP 8080端口的请求转发到192.168.1.2的UDP 8000端口上。

转发条目	公网IP	公网端口	私网IP	私网端口	协议
条目1	1.1.XX.XX	80	192.168.1.1	80	TCP
条目2	2.2.XX.XX	8080	192.168.1.2	8000	UDP

- **IP映射**

配置IP映射后，NAT网关会将任何访问该公网IP的请求都将转发到目标ECS实例上。如下表DNAT条目为例，NAT网关会将任何访问3.3.XX.XX的请求转发到192.168.1.3实例上。

转发条目	公网IP	公网端口	私网IP	私网端口	协议
条目3	3.3.XX.XX	任意端口	192.168.1.3	任意端口	任意协议

6.2. 创建DNAT条目

NAT网关支持DNAT功能，将NAT网关上的公网IP映射给ECS实例使用，使ECS实例能够提供互联网服务。DNAT支持端口映射和IP映射。

操作步骤

1. 登录NAT网关管理控制台。
2. 在顶部菜单栏，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关实例，然后在操作列单击设置DNAT。
4. 在DNAT管理页签，单击创建DNAT条目。
5. 在创建DNAT条目对话框，根据以下信息配置DNAT条目，然后单击确定。

配置	说明
公网IP地址	<p>选择一个可用的公网IP。</p> <div>? 说明 用于创建SNAT条目的公网IP不能再用来创建DNAT条目。</div>
私网IP地址	<p>选择要通过DNAT规则进行公网通信的ECS实例。您可以通过以下两种方式指定目标ECS实例的私网IP：</p> <ul style="list-style-type: none">◦ 从ECS或弹性网卡对应IP进行选择：从ECS实例或弹性网卡列表中选择ECS实例。◦ 自填：输入目标ECS实例的私网IP。 <div>? 说明 自填的私网IP必需属于本VPC的CIDR范围，也可直接输入一个已有的ECS的私网IP。</div>
端口设置	<p>选择DNAT映射的方式：</p> <ul style="list-style-type: none">◦ 所有端口：该方式属于IP映射，任何访问该公网IP的请求都将转发到目标ECS实例上。◦ 具体端口：该方式属于端口映射，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ECS实例的指定端口上。 <p>选择具体端口后，请根据业务需求输入公网端口（进行端口转发的外部端口）、私网端口（进行端口转发的内部端口）和协议类型（转发端口的协议类型）。</p>

6.3. 修改DNAT条目

创建DNAT条目后，您可以修改DNAT条目的公网IP、私网IP或端口。

操作步骤

1. 登录NAT网关管理控制台。
2. 在顶部状态栏处，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关实例，然后在操作列单击设置DNAT。
4. 在DNAT管理页签，找到目标DNAT条目，然后在操作列单击编辑。
5. 在编辑DNAT条目对话框，修改DNAT条目的公网IP地址、私网IP地址或端口，然后单击确定。

6.4. 删除DNAT条目

如果您不需要ECS实例面向互联网提供服务，您可以删除DNAT条目。

操作步骤

1. [登录NAT网关管理控制台](#)。
2. 在顶部菜单栏，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关实例，然后在操作列单击**设置DNAT**。
4. 在**DNAT管理**页签，找到目标DNAT条目，然后在操作列单击**删除**。
5. 在弹出的对话框，单击**确定**。

7. 管理SNAT表

7.1. SNAT表概述

NAT网关支持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。

SNAT条目

您可以通过在SNAT表中创建SNAT条目，实现代理上网功能。

每个SNAT条目由以下两部分组成：


- **交换机或ECS实例**：需要使用SNAT代理服务的交换机或ECS实例。
- **公网IP**：用来提供互联网访问的公网IP。

交换机粒度和ECS粒度

SNAT功能提供如下两种粒度，以实现VPC内ECS实例访问互联网。

- **交换机粒度**

选择交换机为粒度创建SNAT条目后，当指定交换机下的ECS实例发起互联网访问请求时，NAT网关会为其提供SNAT服务，且使用的公网IP为指定的公网IP。默认情况，交换机下的所有ECS实例都可以使用配置的公网IP访问互联网。

 **说明** 如果ECS实例已经持有了公网IP（如分配了固定公网IP、绑定EIP和设置了DNAT IP映射），当该ECS实例发起互联网访问时，会优先通过持有的公网IP访问互联网，而不会使用NAT网关的SNAT功能访问互联网。

- **ECS粒度**

选择ECS为粒度创建SNAT条目后，指定的ECS实例通过配置的公网IP访问互联网。当指定的ECS实例发起互联网访问请求时，NAT网关会为其提供SNAT服务，且使用的公网IP为指定的公网IP。

7.2. 创建SNAT条目

NAT网关的SNAT功能可以为VPC中无公网IP的ECS实例提供访问互联网的代理服务。

操作步骤

1. [登录NAT网关管理控制台](#)。
2. 在顶部菜单栏，选择NAT网关的地域。
3. 在**NAT网关**页面，找到目标NAT网关实例，然后在操作列单击**设置SNAT**。
4. 在**SNAT管理**页签，单击**创建SNAT条目**。
5. 在**创建SNAT条目**对话框，根据以下信息配置SNAT条目，然后单击**确定**。

配置	说明
----	----

配置	说明
粒度设置	<p>选择SNAT条目的粒度。</p> <ul style="list-style-type: none"> 交换机粒度：指定交换机下的ECS实例通过配置的公网IP访问互联网。 <ul style="list-style-type: none"> 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。 ECS粒度：指定的ECS实例通过配置的公网IP访问互联网。 <ul style="list-style-type: none"> 可用ECS列表：选择VPC中的ECS实例。 <p>该ECS实例将通过配置的公网IP访问互联网。请确保ECS实例满足以下条件：</p> <ul style="list-style-type: none"> ECS实例的状态处于运行中。 ECS实例不具备固定公网IP且未绑定其他弹性公网IP。 ECS网段：显示该ECS实例的网段。
公网IP地址	<p>选择用来提供互联网访问的公网IP。</p> <p>支持选择1个或多个公网IP，多个公网IP可以构建SNAT IP地址池。</p> <div>  说明 用于创建DNAT条目的公网IP不能再用来创建SNAT条目。 </div>
条目名称	<p>SNAT条目的名称。</p> <p>名称长度为2~128个字符，以大小写字母或中文开头，可包含数字、下划线（_）和短划线（-）。</p>

7.3. 修改SNAT条目

创建SNAT条目后，您可以修改SNAT条目的公网IP和条目名称。

操作步骤

1. 登录NAT网关管理控制台。
2. 在顶部状态栏处，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关实例，然后在操作列单击设置SNAT。
4. 在SNAT管理页签，找到目标SNAT条目，然后在操作列单击编辑。
5. 在编辑SNAT条目对话框，修改SNAT条目的公网IP、条目名称，然后单击确定。

7.4. 删除SNAT条目

如果您不需要为VPC内无公网IP的ECS实例提供访问互联网的代理服务，您可以删除SNAT条目。

操作步骤

1. 登录NAT网关管理控制台。

2. 在顶部菜单栏，选择NAT网关的地域。
3. 在NAT网关页面，找到目标NAT网关实例，然后在操作列单击设置SNAT。
4. 在SNAT管理页签，找到要删除的SNAT条目，然后在操作列单击删除。
5. 在弹出的对话框，单击确定。

8.NAT带宽包

8.1. 创建NAT带宽包

您可以使用弹性公网IP（Elastic IP Address，简称EIP）或NAT带宽包绑定NAT网关，但您只能使用其中一种方式绑定NAT网关。如果您使用NAT带宽包，您需要创建一个NAT带宽包，然后才可以配置DNAT或SNAT功能。NAT带宽包由公网IP和公网带宽组成。

操作步骤

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，单击带宽包列下的**购买NAT带宽包**。
3. 在NAT带宽包页签，单击**创建**。
4. 在NAT带宽包页面，根据以下信息配置NAT带宽包，然后单击**提交**。

配置	说明
区域	
组织	显示要创建NAT带宽包的组织。
资源集	显示要创建NAT带宽包的资源集。
地域	显示要创建NAT带宽包的地域。
基本配置	
NAT网关ID	显示要创建NAT带宽包的NAT网关实例的ID。
计费方式	选择NAT带宽包的计费方式。 目前，仅支持 按带宽 计费。
带宽(Mbps)	输入要创建的NAT带宽包的带宽。
名称	输入NAT带宽包的名称。
描述	输入NAT带宽包的描述。
个数	输入要创建NAT带宽包的个数。

8.2. 修改NAT带宽包的带宽

您可以修改NAT带宽包的带宽。修改后，立即生效。

操作步骤

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，单击带宽包列下的NAT带宽包实例ID。
3. 在NAT带宽包页签的**规格信息**区域，单击**修改带宽**。

4. 在NAT带宽包带宽变配页面，修改带宽，然后单击提交。

NAT带宽包最大支持5000 Mbps。

8.3. 添加IP地址

您可以向NAT带宽包中添加IP地址，添加的IP地址可以用于创建DNAT和SNAT规则。

操作步骤

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，单击带宽包列下的NAT带宽包实例ID。
3. 在NAT带宽包页签的公网IP列表区域，单击添加IP地址。
4. 在NAT带宽包IP变配页面，输入要添加的IP地址的个数，然后单击提交。

8.4. 释放IP地址

您可以释放NAT带宽包中的IP地址，但需保证NAT带宽包下至少包含一个IP地址。

前提条件

释放IP地址前，请确保该IP地址未被用于DNAT条目和SNAT条目。如有请先删除。具体操作，请参见[删除DNAT条目](#)和[删除SNAT条目](#)。

操作步骤

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，然后在带宽包列单击NAT带宽包实例ID。
3. 在NAT带宽包页签的公网IP列表区域，找到目标IP地址，然后在操作列单击释放。
4. 在释放IP对话框，单击确定。

8.5. 删除NAT带宽包

您可以删除一个不需要的NAT带宽包。

前提条件

开始前，请确保满足以下条件：

- NAT带宽包中的IP未被DNAT条目使用，如有请删除。具体操作，请参见[删除DNAT条目](#)。
- NAT带宽包中的IP未被SNAT条目使用，如有请删除。具体操作，请参见[删除SNAT条目](#)。

操作步骤

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，在带宽包列单击NAT带宽包实例ID。
3. 在带宽包详情页面，找到目标NAT带宽包，单击删除。
4. 在删除带宽包对话框，单击确认。

9.DDoS基础防护

DDoS攻击是一种针对目标系统的恶意网络攻击行为，会导致被攻击者的业务无法正常访问。阿里云免费为NAT网关提供最高5 Gbps的DDoS基础防护，DDoS基础防护服务可以有效防止DDoS攻击。

DDoS基础防护工作原理

启用DDoS基础防护功能后，所有来自Internet的流量都将先经过云盾再到达NAT网关，云盾会针对常见的攻击进行清洗过滤。云盾DDoS基础防护可以防御SYN Flood、UDP Flood、ACK Flood、ICMP Flood 和DNS Flood等DDoS攻击。

云盾DDoS基础防护根据NAT网关实例的EIP带宽自动设定清洗阈值和黑洞阈值。当入方向流量达到阈值上限时，触发清洗和黑洞：

- 清洗：当来自Internet的攻击流量超过清洗阈值或符合攻击流量模型特征时，云盾将启动清洗操作，清洗操作包括过滤攻击报文、流量限速、包限速等。
- 黑洞：当来自Internet的攻击流量超过黑洞阈值时，为保护集群安全，流量将会被黑洞处理，即所有入流量全部被丢弃。

清洗阈值

NAT网关的清洗阈值计算方式如下表所示：

EIP带宽	最大bps清洗阈值	最大pps清洗阈值	默认黑洞阈值
小于等于800 Mbps	800 Mbps	12万	1.5 Gbps
大于800 Mbps	设定的带宽值	设定的带宽值×150	设定的带宽值×2

例如EIP带宽为1000 Mbps，则最大bps清洗阈值为1000 Mbps，最大pps清洗阈值15万，默认黑洞阈值为2 Gbps。