

# 阿里云 NAT网关

## 产品简介

文档版本：20190701

## 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。	 <b>禁止：</b> 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。	 <b>警告：</b> 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。	 <b>说明：</b> 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
<b>粗体</b>	表示按键、菜单、页面名称等UI元素。	单击 <b>确定</b> 。
<code>courier</code> 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
<code>##</code>	表示参数、变量。	<code>bae log list --instanceid Instance_ID</code>
<code>[]或者[a b]</code>	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
<code>{ }或者{a b}</code>	表示必选项，至多选择一个。	<code>swich {stand   slave}</code>

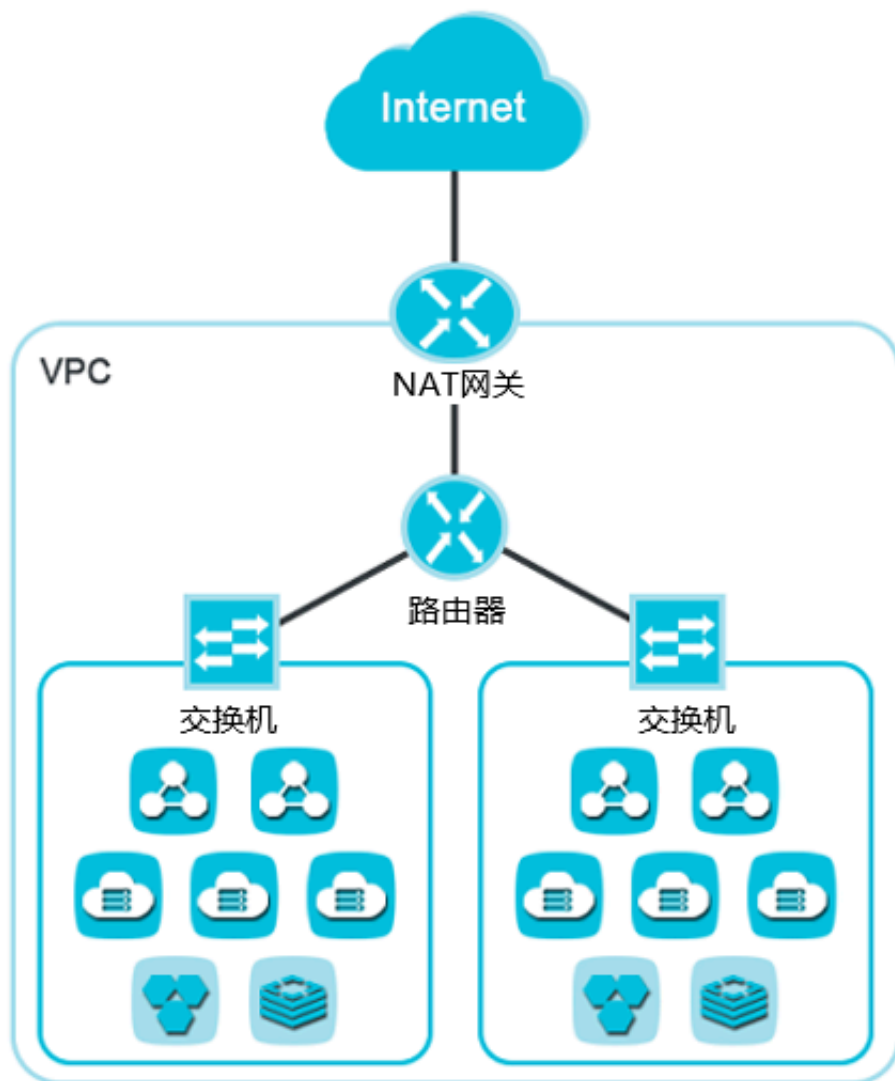
# 目录

---

法律声明.....	I
通用约定.....	I
1 什么是NAT网关.....	1
2 功能概述.....	2
3 产品优势.....	3
4 使用场景.....	4
5 基本概念.....	5
6 使用限制.....	6

# 1 什么是NAT网关

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



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（EIP）。



说明：

对于2018年1月26日之前账号下存在NAT带宽包的账号，您仍需使用NAT带宽包为该NAT网关提供公网IP。如需使用EIP绑定NAT网关功能，请提交工单。

如果您需要使用共享带宽功能，可以在EIP控制台将EIP加入已有的共享带宽，或者在购买共享带宽后，再将EIP加入到共享带宽中。详细说明，请参见[加入共享带宽](#)。

## 2 功能概述

---

NAT网关提供SNAT（源网络地址转换）、DNAT（目的网络地址转换）和共享带宽功能。

### SNAT

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。

此外，NAT网关的SNAT功能还可以作为一个简易防火墙使用。通过SNAT功能保护后端的服务器，只有后端服务主动和外部终端建立连接后，外部终端才可以访问内部服务器，而未建立连接的外部不可信终端无法访问后端服务器。

### DNAT

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。

### 共享带宽

您可以为NAT网关绑定EIP，再将EIP加入到[共享带宽](#)中。EIP加入到共享带宽后，EIP原本的计费模式失效，不额外收取流量或带宽费，只收取绑定NAT网关的EIP实例费。

## 3 产品优势

---

NAT网关具有以下优势：灵活易用的转发能力、高性能、高可用和按需购买。

### 灵活易用的转发能力

NAT网关作为一款企业级VPC公网网关，提供SNAT和DNAT功能。用户无需基于云服务器自己搭建公网网关，功能灵活、简单易用、稳定可靠。

### 高性能

NAT网关是基于阿里云自研分布式网关，使用SDN技术推出的一款虚拟网络硬件。NAT网关支持10Gbps级别的转发能力，为大规模公网应用提供支撑。

### 高可用

NAT网关跨可用区部署，可用性高。单个可用区的任何故障都不会影响NAT网关的业务连续性。

### 按需购买

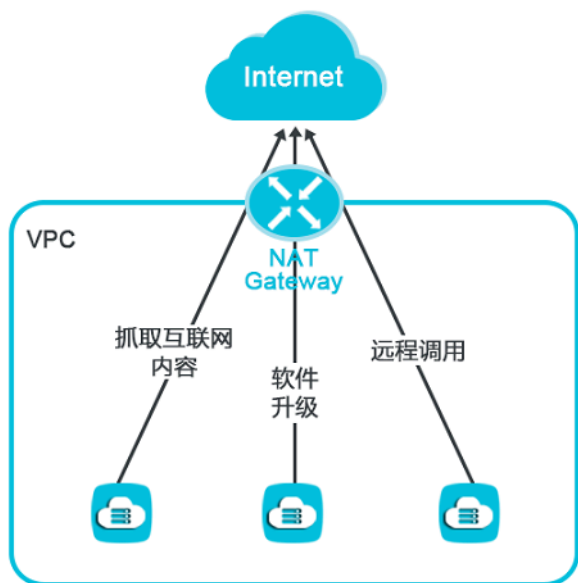
NAT网关的规格、EIP的规格和个数，均可以随时升降，轻松应对业务变化。

## 4 使用场景

NAT网关适用于专有网络类型的ECS实例需要主动访问公网和被公网访问的场景。

### 场景一 搭建高可用的SNAT网关

在IT系统中，往往存在一些服务器需要主动访问互联网，但出于安全性考虑需要避免将这些服务器所持有的公网IP暴露在公网上。此时，您可以使用NAT网关的SNAT功能实现这一需求。详细信息，请参见[创建SNAT条目](#)。



### 场景二 提供公网服务

专有网络类型的ECS实例可以通过端口映射和IP映射的方式对外提供服务。



## 5 基本概念

使用NAT网关功能前，您需要了解以下基本概念。

术语	说明
NAT网关	一款企业级的VPC公网网关，提供NAT代理（SNAT和DNAT）、10Gbps级别的转发能力、地域级别的高可用性和跨可用区的容灾能力。
DNAT表	DNAT表是NAT网关上的一张配置表，用于NAT网关上的DNAT功能配置。可以实现端口映射（Port mapping）和IP映射（IP mapping），将NAT网关上的公网IP映射给ECS实例。
SNAT表	SNAT表是NAT网关上的一张配置表，用于NAT网关上的SNAT功能配置。可以以交换机和ECS为粒度进行SNAT规则配置。 <ul style="list-style-type: none"><li>· 以交换机为粒度：指定交换机下的所有ECS实例均使用指定的公网IP访问互联网。</li><li>· 以ECS为粒度：指定的ECS实例使用指定的公网IP访问互联网。</li></ul>
EIP	EIP是可以独立购买和持有的公网IP地址资源。EIP可绑定到专有网络类型的ECS实例、专有网络类型的私网SLB实例、专有网络类型的辅助弹性网卡、NAT网关和高可用虚拟IP上。

## 6 使用限制

---

在使用NAT网关前，请了解NAT网关及EIP绑定NAT网关的相关限制。

### NAT网关相关限制

- 一个VPC最多只能配置一个NAT网关，无法调整。
- 一个公网IP不能同时用于SNAT表和DNAT表。
- 一个DNAT表最多可添加100个DNAT条目，可提交工单申请调整配额。
- 一个SNAT表最多可添加40个SNAT条目，可提交工单申请调整配额。
- 如果VPC中存在目标网段为0.0.0.0/0的自定义路由，需删除后才可以创建NAT网关。
- 交换机添加SNAT条目后，会受到EIP带宽峰值的限制。

如果EIP已加入到共享带宽中，则交换机会受到共享带宽的带宽峰值的限制。

### EIP绑定NAT网关相关限制

- 一个NAT网关最多绑定20个EIP，可提交工单申请调整配额。
- 一个NAT网关最多绑定10个按流量计费的EIP（可提交工单申请调整配额），且按流量计费的EIP的最大峰值不能大于200Mbps。
- 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 $N \times 55000$ 。
- 当VPC内无公网IP的ECS实例通过NAT网关访问公网上同一个目的IP和端口的带宽大于2Gbps时，建议您为NAT网关绑定4-8个EIP并构建SNAT IP池，避免单个公网IP的端口数量限制可能产生的丢包。详细信息，请参见[构建SNAT IP池](#)。
- 对于2018年1月26日之前账号下存在NAT带宽包的账号，您仍需使用NAT带宽包为该NAT网关提供公网IP。如需使用EIP绑定NAT网关功能，请提交工单。