

# 阿里云 **NAT**网关

用户指南

文档版本：20190115

# 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>注意：</b> 您也可以通过按 <b>Ctrl + A</b> 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 <b>确定</b> 。
courier 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid 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>swich {stand   slave}</code>

# 目录

---

法律声明.....	I
通用约定.....	I
<b>1 NAT网关规格.....</b>	<b>1</b>
<b>2 管理NAT网关实例.....</b>	<b>2</b>
<b>3 管理DNAT表.....</b>	<b>4</b>
<b>4 管理SNAT表.....</b>	<b>7</b>
<b>5 绑定和解绑EIP.....</b>	<b>9</b>
<b>6 DDoS防护.....</b>	<b>10</b>

# 1 NAT网关规格

NAT网关提供不同的规格。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。

NAT网关提供如下规格。

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	3万

在选择NAT规格时，请注意：

- NAT网关的规格仅对SNAT的性能有影响，对DNAT没有限制。
- NAT网关的规格与共享带宽包的带宽大小、IP个数之间没有相互制约关系。
- 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。
- 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。


## 2 管理NAT网关实例

NAT网关实例是一个运行的NAT网关服务。在使用SNAT和DNAT功能前，您必须先创建一个NAT网关实例。

### 创建NAT网关

完成以下操作，创建NAT网关：

1. 登录 [VPC管理控制台](#)。
2. 在左侧导航栏，单击**NAT网关**。
3. 单击**创建NAT网关**。
4. 根据以下信息，配置NAT网关并完成支付。

配置	说明
地域	选择需要配置NAT网关的VPC所在的地域。
VPC ID	<p>选择需要配置NAT网关的VPC。创建NAT网关后，将不能修改VPC。若在VPC列表中，找不到目标VPC，可从以下方面进行排查：</p> <ul style="list-style-type: none"><li>• 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。</li><li>• 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。</li></ul>
规格	<p>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。</p> <div> <b>注意：</b> NAT网关的规格对DNAT功能的连接数和吞吐量没有限制。详情参考<a href="#">NAT网关规格</a>。</div>
计费周期	显示NAT网关的计费周期。

### 更改NAT网关规格

您可以根据业务需要，修改NAT网关的规格。NAT网关的规格仅对SNAT的性能有影响，对DNAT性能没有影响。

完成以下操作，修改NAT网关规格：

1. 登录 [VPC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. 单击目标NAT网关的实例ID。
5. 在NAT网关的详细页面，单击**修改规格**。
6. 在配置变更区域，选择新的NAT网关规格，然后单击**去开通**完成变更。

### 编辑NAT网关

完成以下操作，修改NAT网关的名称和描述：

1. 登录 [VPC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. 单击目标NAT网关的实例ID。
5. 在NAT网关的详细页面，分别单击名称和描述右侧的**编辑**，在弹出的对话框中分别输入NAT网关的名称和描述信息，然后单击**确定**完成修改。

### 删除NAT网关

完成以下操作，删除NAT网关：

1. 登录 [VPC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，确保NAT网关中已经没有SNAT、DNAT条目和绑定的EIP后，单击**删除**。在弹出的对话框中，单击**确定**。



#### 注意：

您也可以在弹出的对话框中选择**强制删除**，在删除NAT网关后自动删除NAT网关中的DNAT、SNAT条目，并解绑已绑定的EIP。

## 3 管理DNAT表

NAT网关提供DNAT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可以面向互联网提供服务。

### DNAT条目

NAT网关将DNAT功能的配置，抽象为一张DNAT列表。您可以通过配置DNAT列表中的DNAT条目，实现DNAT功能的配置。

每个DNAT条目由五部分组成：公网IP、公网端口、私网IP、私网端口和协议。其中公网IP为NAT网关绑定的弹性公网IP（EIP），私网IP为专有网络中ECS实例的IP。配置DNAT条目后，公网IP收到的数据将按照自定义的映射规则，转发给专有网络VPC内的ECS。



#### 注意：

对于2018年1月26日之前账户下存在NAT带宽包的用户，DNAT条目中的公网IP为NAT带宽包提供的公网IP。

### 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

配置端口后，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。例如下表中的条目1和条目2。

- IP映射

配置IP映射后，相当于为目标ECS实例配置了一个弹性公网IP。任何访问该公网IP的请求都将转发到目标ECS实例上。例如下表中的条目3。


转发条目	公网IP	公网端口	私网IP	私网端口	协议
条目1	139.224.xx.xx	80	192.168.x.x	80	TCP
条目2	139.224.xx.xx	8080	192.168.x.x	8000	UDP
条目3	139.224.xx.xx	Any	192.168.x.x	Any	Any

### 添加DNAT条目

完成以下操作，添加DNAT条目：



1. 登录 [VPC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. 单击目标NAT网关的实例ID。
5. 在左侧导航栏，单击**DNAT**列表，然后单击创建**DNAT**条目。
6. 根据以下信息，配置DNAT条目。

配置	说明
公网IP地址	<p>选择一个可用的公网IP。</p> <div>  <b>注意：</b> 用于创建SNAT条目的公网IP地址不能再用来创建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"> <li>• 自填：输入目标ECS实例的私网IP。</li> <li>• 从ECS对应IP进行选择：从ECS实例列表中选择ECS实例，系统自动填充IP地址。</li> </ul>
端口设置	<p>选择DNAT映射的方式：</p> <ul style="list-style-type: none"> <li>• 所有端口：该方式属于IP映射，相当于为目标ECS实例配置了一个弹性公网IP。任何访问该公网IP的请求都将转发到目标ECS实例上。</li> <li>• 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。</li> </ul> <p>选择具体端口后，请根据业务需求输入公网端口（源端口）、私网端口（目的端口）和协议类型。</p>

### 编辑DNAT条目

完成以下操作，编辑DNAT条目：

1. 登录 [VPC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. 单击目标NAT网关的设置**DNAT**选项。

5. 单击目标DNAT条目的编辑，更新DNAT条目配置。

#### 删除DNAT条目

完成以下操作，删除：

1. 登录[VPC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. 单击目标NAT网关的设置**DNAT**选项。
5. 单击目标DNAT条目的移除，然后单击确定。

## 4 管理SNAT表

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。

### SNAT条目

NAT网关将SNAT功能的配置，抽象为一张SNAT列表。您可以通过配置SNAT列表中的SNAT条目，实现SNAT功能的配置。

每个SNAT条目由交换机和公网IP组成。交换机为专有网络ECS实例所属的交换机，公网IP为NAT网关绑定的弹性公网IP（EIP），如下表所示。



#### 注意：

对于2018年1月26日之前账户下存在NAT带宽包的用户，SNAT条目中的公网IP为NAT带宽包提供的公网IP。

交换机	公网IP
vsw-184ipsxxx	139.224.xx.xx
vsw-11qht5xxx	139.224.xx.xx

配置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（代理上网服务），且使用的公网IP地址为指定的公网IP。默认情况下交换机下的所有ECS实例都可以使用配置的公网IP发起互联网访问。



#### 注意：



若某台持有公网IP的ECS实例（比如已经绑定了EIP）发起互联网访问时，会优先使用其持有的公网IP，而不会使用NAT网关的SNAT功能。

### 添加SNAT条目

完成以下操作，添加SNAT条目：

1. 登录 [VPC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. 单击目标NAT网关的实例ID。
5. 在左侧导航栏，单击**SNAT列表**，然后单击创建**SNAT条目**。

## 6. 根据以下信息，配置SNAT条目。

配置	说明
交换机	<p>选择VPC中的交换机。该交换机下所有的ECS实例都将可以通过SNAT功能进行公网访问。</p> <div> <b>注意：</b> 如果某台持有公网IP的ECS实例（比如已经绑定了EIP）发起互联网访问时，会优先使用其持有的公网IP，而不会使用NAT网关的SNAT功能。</div>
交换机网段	显示该交换机的网段。
公网IP	<p>选择用来提供互联网访问的公网IP。</p> <div> <b>注意：</b> 用于创建DNAT条目的公网IP地址不能再用来创建SNAT条目。</div>

### 编辑SNAT条目

完成以下操作，编辑SNAT条目：

1. 登录 [VPC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. 单击目标NAT网关的设置**SNAT**选项。
5. 单击目标SNAT条目的编辑，更新SNAT条目配置。

### 删除SNAT条目

完成以下操作，删除SNAT条目：

1. 登录 [VPC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. 单击目标NAT网关的设置**SNAT**选项。
5. 单击目标SNAT条目的移除，然后单击确定。

## 5 绑定和解绑EIP

创建NAT网关后，您还需要为NAT网关配置公网IP。您可以通过绑定弹性公网IP（EIP）的方式为NAT网关配置公网IP。



**注意：**

对于2018年1月26日之前账号下存在NAT带宽包的用户，默认无法使用EIP绑定NAT网关的功能。如需使用EIP绑定NAT网关功能，请提交工单。

### 绑定EIP

确保在绑定EIP前，您已经创建NAT网关和EIP。

完成以下操作，将EIP绑定到NAT网关：

1. 登录 [VPC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，然后单击更多操作 > 绑定弹性公网IP。
5. 在弹出的对话框，完成以下操作：
  - a. 公网IP地址：选择一个弹性公网IP作为NAT网关的公网IP。
  - b. 交换机（可选）：系统会自动添加SNAT规则，使已选交换机下的云产品可以通过EIP访问公网。
6. 重复以上步骤绑定更多EIP。

### 解绑EIP

在解绑EIP前，确保该EIP没有被任何SNAT或DNAT条目占用。

完成以下操作，解绑EIP：

1. 登录 [VPC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，然后单击更多操作 > 解绑弹性公网IP。
5. 选择要解绑的EIP，然后单击确定。

## 6 DDoS防护

阿里云免费为NAT网关提供最高5G的DDoS基础防护。所有来自Internet的流量都要先经过云盾再到达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的攻击流量较大或符合某些特定攻击流量模型特征时，云盾将会针对攻击流量启动清洗操作，清洗包括攻击报文过滤、流量限速、包限速等。
- 黑洞：当来自Internet的攻击流量非常大时，为保护整个集群的安全，流量将会被黑洞处理，即所有入流量全部被丢弃。

NAT网关的清洗阈值计算方式如下表所示。比如EIP带宽为1000Mbps，则最大bps清洗阈值为1000Mbps，最大pps清洗阈值15万，默认黑洞阈值2Gbps。

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	800Mbps	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