NAT 网关

用户指南

文档版本 02

发布日期 2020-01-02

华为云计算技术有限公司

商标声明


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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 产品简介 1
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 8
1.5 约束与限制 9
1.6 与其它服务的关系 10
1.7 计费说明 12
1.8 权限管理 12
1.9 区域和可用区 15
1.10 基本概念 16
2 快速入门 17
2.1 使用 SNAT 访问公网 17
2.1.1 入门指引 17
2.1.2 步骤 1：申请弹性 IP 18
2.1.3 步骤 2：创建公网 NAT 网关 18
2.1.4 步骤 3：添加 SNAT 规则 20
2.1.5 步骤 4：结果验证 21
2.2 使用 DNAT 为云主机面向公网提供服务 22
2.2.1 入门指引 22
2.2.2 步骤 1：申请弹性 IP 22
2.2.3 步骤 2：创建公网 NAT 网关 23
2.2.4 步骤 3：添加 DNAT 规则 25
2.2.5 步骤 4：结果验证 26
2.3 云间 NAT 网关高速访问互联网 27
2.3.1 入门指引 27
2.3.2 步骤 1：开通云专线 28
2.3.3 步骤 2：申请弹性 IP 28
2.3.4 步骤 3：创建公网 NAT 网关 29
2.3.5 步骤 4：添加 SNAT 规则 31
2.3.6 步骤 5：添加 DNAT 规则 32
2.4 使用私网 NAT 网关为 VPC 内计算实例实现线上线下互通 33
2.4.1 入门指引 33

2.4.2 步骤 1：创建业务 VPC 及中转 VPC 34
2.4.3 步骤 2：配置云专线（本示例使用 VPC Peering 代替云专线） 35
2.4.4 步骤 3：创建私网 NAT 网关 35
2.4.5 步骤 4：添加 SNAT 规则 37
2.4.6 步骤 5：添加路由 38
2.4.7 步骤 6：添加安全组规则 39
2.5 公网 NAT 网关通过多网关扩展容量 40
2.5.1 入门指引 40
2.5.2 步骤 1：创建 VPC 及子网 41
2.5.3 步骤 2：创建公网 NAT 网关 41
2.5.4 步骤 3：检查默认路由 42
2.5.5 步骤 4：创建路由表 42
2.5.6 步骤 5：创建公网 NAT 网关 43
2.5.7 步骤 6：添加默认路由 44
3 公网 NAT 网关 46
3.1 公网 NAT 网关简介 46
3.2 管理公网 NAT 网关 47
3.2.1 创建公网 NAT 网关 47
3.2.2 查看公网 NAT 网关 49
3.2.3 修改公网 NAT 网关 49
3.2.4 删除公网 NAT 网关 50
3.3 管理 SNAT 规则 50
3.3.1 添加 SNAT 规则 50
3.3.2 查看 SNAT 规则 51
3.3.3 修改 SNAT 规则 52
3.3.4 删除 SNAT 规则 52
3.4 管理 DNAT 规则 53
3.4.1 添加 DNAT 规则 53
3.4.2 查看 DNAT 规则 54
3.4.3 修改 DNAT 规则 55
3.4.4 删除 DNAT 规则 55
3.4.5 批量删除 DNAT 规则 56
3.4.6 DNAT 规则模板导入导出 56
4 私网 NAT 网关 58
4.1 私网 NAT 网关简介 58
4.2 创建私网 NAT 网关 59
4.2.1 概述 59
4.2.2 创建私网 NAT 网关 60
4.2.3 创建中转 IP 61
4.2.4 添加 SNAT 规则 62
4.2.5 添加 DNAT 规则 64
4.3 管理私网 NAT 网关 66

4.3.1 查看私网 NAT 网关 66
4.3.2 修改私网 NAT 网关 66
4.3.3 删除私网 NAT 网关 67
4.4 管理 SNAT 规则 67
4.4.1 查看 SNAT 规则 67
4.4.2 修改 SNAT 规则 68
4.4.3 删除 SNAT 规则 68
4.5 管理 DNAT 规则 69
4.5.1 查看 DNAT 规则 69
4.5.2 修改 DNAT 规则 69
4.5.3 删除 DNAT 规则 70
4.6 管理中转 IP 70
4.6.1 创建中转 IP 70
4.6.2 查看中转 IP 71
4.6.3 删除中转 IP 71
4.7 连接 IDC 或其他虚拟私有云 72
5 权限管理 73
5.1 创建用户并授权使用 NAT 网关 73
5.2 NAT 网关自定义策略 74
6 监控管理 76
6.1 支持的监控指标 76
6.2 创建告警规则 79
6.3 查看监控指标 81
6.4 查看 NAT 网关后端实例对应的监控指标 81
7 常见问题 82
7.1 公网 NAT 网关 82
7.1.1 公网 NAT 网关、弹性 IP 带宽、VPC 内弹性云服务器与 VPC 是什么样的关系? 82
7.1.2 公网 NAT 网关如何实现高可用性? 82
7.1.3 哪些端口无法访问? 82
7.1.4 弹性云服务器使用 NAT 网关和直接绑定弹性 IP 有区别吗? 82
7.1.5 通过 NAT 网关访问 Internet 失败该如何处理? 83
7.1.6 NAT 网关是否支持更换 VPC? 83
7.1.7 NAT 网关的配额是什么? 83
7.1.8 NAT 网关和 SNAT 规则是否支持更新操作? 83
7.1.9 NAT 网关是否支持 IPV6? 84
7.1.10 基于 NAT 网关的用户网络，可以配置哪些安全策略实现访问限制? 84
7.1.11 公网 NAT 网关配置完成后，网络不通如何处理? 84
7.2 私网 NAT 网关 90
7.2.1 私网 NAT 配置后组网不通怎么排查? 90
7.2.2 一个 VPC 最多支持创建多少个私网 NAT? 91
7.2.3 私网 NAT 支持创建的 SNAT 和 DNAT 规则数能否增加? 91

7.2.4 私网 NAT 支持 SNAT 规则和 DNAT 规则共用一个中转 IP 吗? 91
7.2.5 私网 NAT 支持云专线的 IP 转换吗? 91
7.2.6 私网 NAT 和公网 NAT 有什么区别? 91
7.2.7 私网 NAT 是否支持跨使用? 92
7.3 SNAT 规则 92
7.3.1 为什么使用 SNAT? 92
7.3.2 什么是 SNAT 连接数? 92
7.3.3 主机通过 NAT 网关访问外网，请问 NAT 网关的带宽是多少? 在哪里设置? 92
7.3.4 NAT 网关丢包或连接不通该如何处理? 92
7.3.5 通过 NAT 网关访问远端服务器概率性失败该如何处理? 92
7.3.6 NAT 网关里的网段设置与 SNAT 规则里的网段有什么关联与区别? 93
7.4 DNAT 规则 94
7.4.1 为什么使用 DNAT? 94
7.4.2 DNAT 规则是否支持更新操作? 94
A 修订记录 95

1 产品简介

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

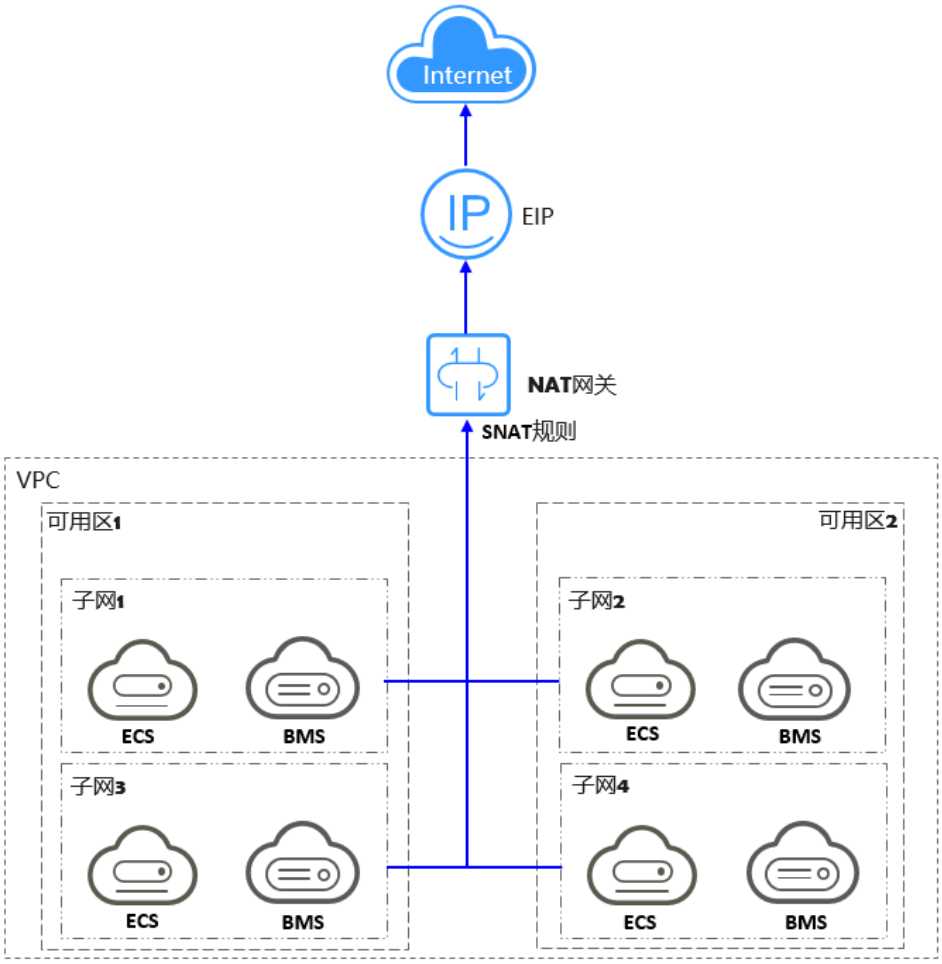
公网NAT网关（Public NAT Gateway）能够为虚拟私有云内的云主机（弹性云服务器、裸金属服务器）或者通过云专线/VPN接入虚拟私有云的本地数据中心的服务器，提供最高20Gbit/s能力的网络地址转换服务，使多个云主机可以共享弹性IP访问Internet或使云主机提供互联网服务。

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。

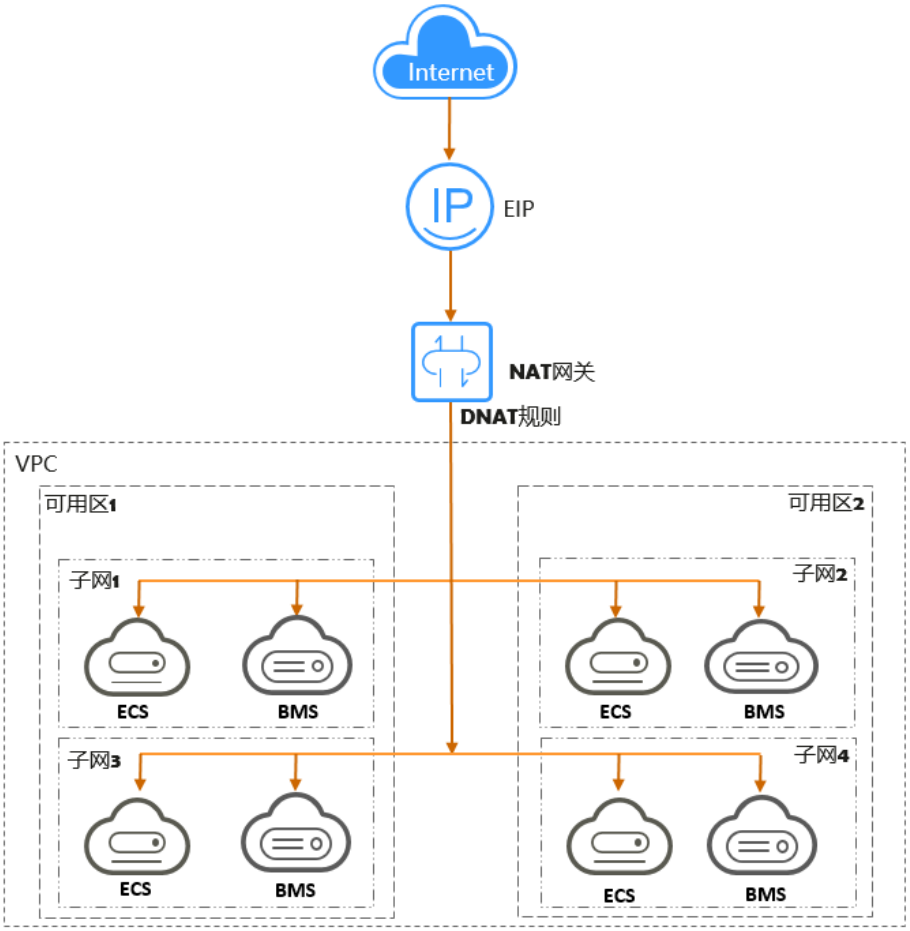
图 1-1 SNAT 架构图



- 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。

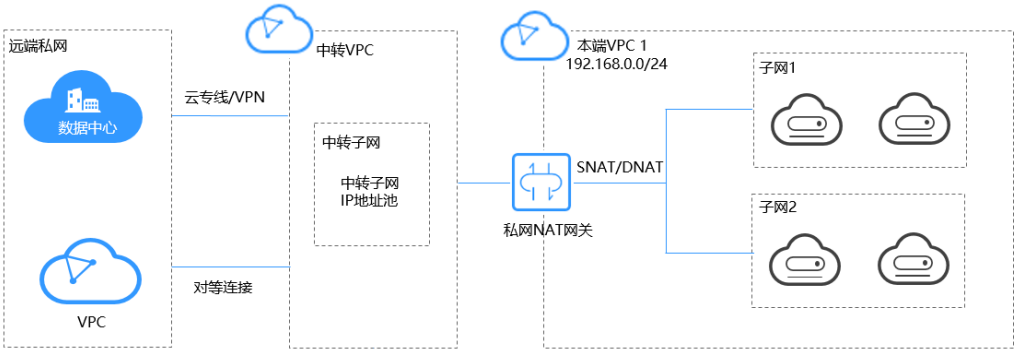
中转IP

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，具体操作请参见《NAT网关API参考》。

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IP和带宽资源，多个云主机共享使用弹性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。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

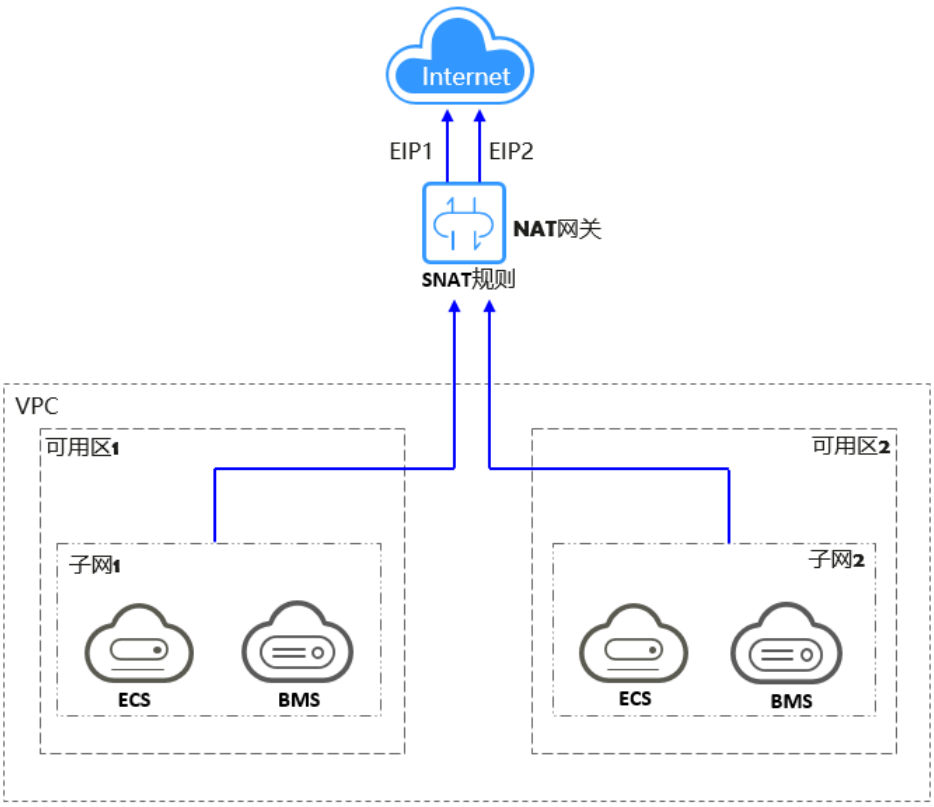
公网 NAT 网关

- **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**

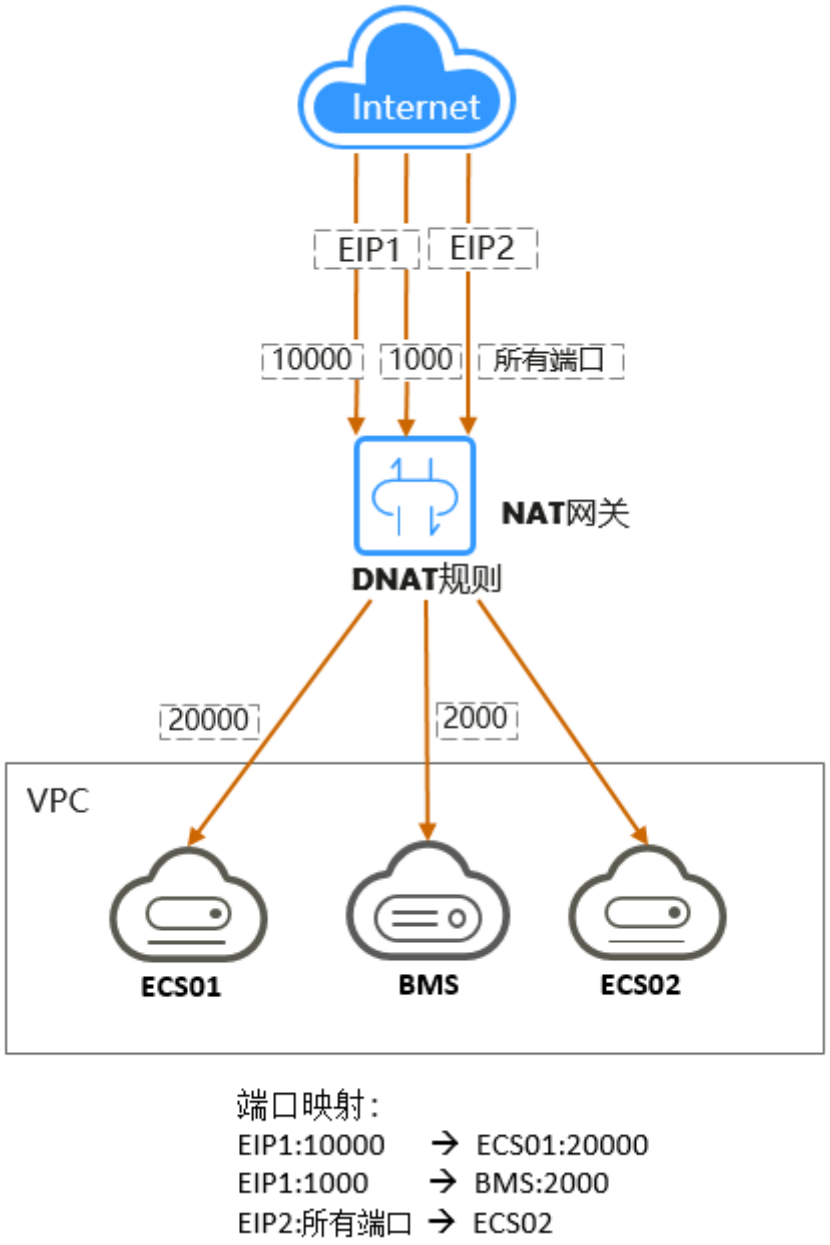
  当VPC内的云主机需要面向公网提供服务时，可以使用公网NAT网关的DNAT功能。

  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IP，任何访问该弹性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

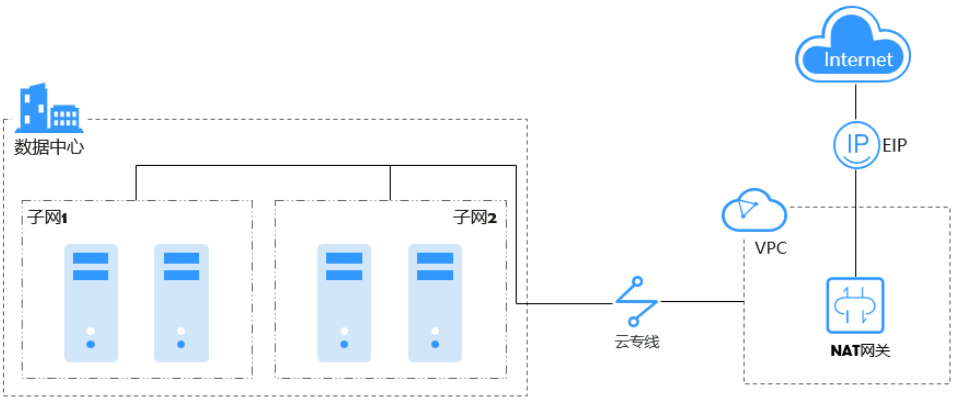


- **使用SNAT或DNAT高速访问互联网**

  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



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
小型	10000	20Gbit/s
中型	50000	20Gbit/s
大型	200000	20Gbit/s
超大型	1000000	20Gbit/s

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
小型	2000	200Mbps
中型	5000	500Mbps
大型	20000	2Gbps
超大型	50000	5Gbps

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IP，不同网关下的规则必须使用不同的弹性IP。
  - 每个VPC支持的NAT网关数为1。
  - 一个VPC支持关联多个公网NAT网关。
  - SNAT和DNAT不能共用同一个弹性IP。
  - 当云主机同时配置弹性IP服务和公网NAT网关服务时，数据均通过弹性IP转发。
  - 出于安全因素考虑，部分运营商会对下列端口进行拦截，导致无法访问。建议避免使用下列端口：

协议	不支持端口
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 4790 5554 5800 5900 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

  - 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
  - DNAT规则不支持将弹性IP绑定到虚拟IP。
  - 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 与其它服务的关系

NAT网关与其他服务关系如图1所示。

图 1-7 NAT 网关与其他服务关系

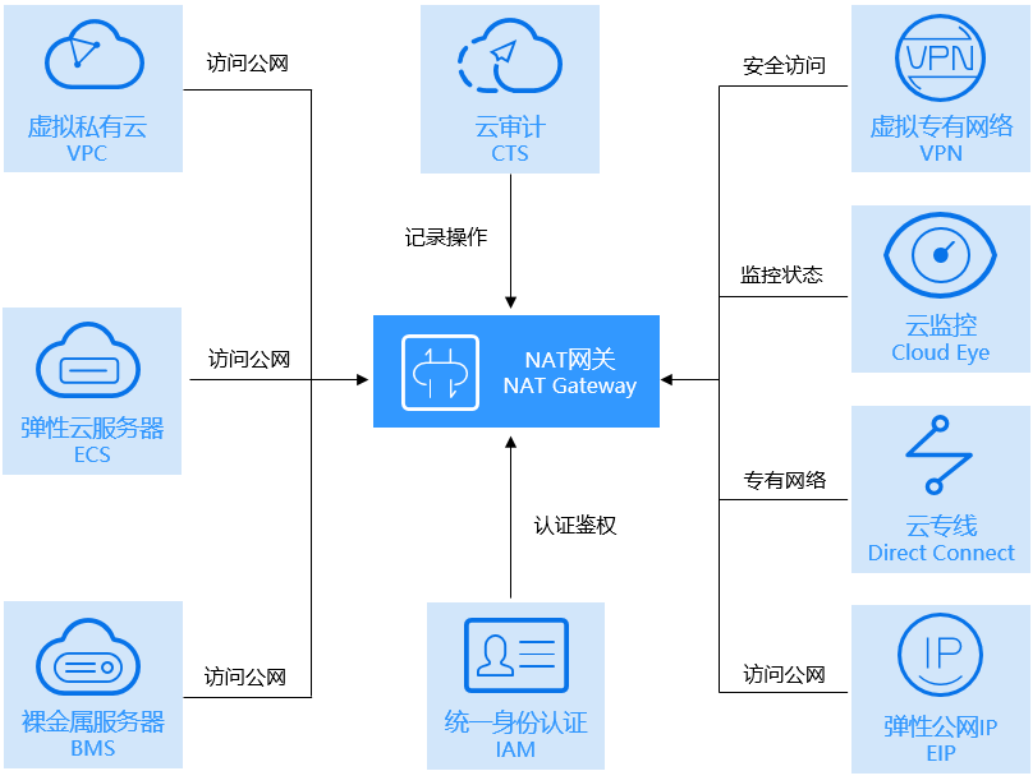


表 1-3 与其他服务的关系

相关服务	交互功能	位置
云专线（Direct Connect，DC）	通过云专线接入VPC的本地服务器，可以通过公网NAT网关访问公网或为公网提供服务。	**云间NAT网关高速访问互联网**
虚拟专用网络（Virtual Private Network，VPN）	通过VPN可以在远端用户和VPC之间建立一条安全加密的公网通信隧道。为通过公网NAT网关访问公网提供了更加安全的访问。	**云间NAT网关高速访问互联网**
弹性云服务器（Elastic Cloud Server，ECS），裸金属服务器（Bare Metal Server，BMS）	公网NAT网关可以为其他云服务提供访问公网或者为公网提供服务的能力。	**使用SNAT访问公网** **使用DNAT为云主机面向公网提供服务**
虚拟私有云（Virtual Private Cloud，VPC）	虚拟私有云内的弹性云服务器与Internet互连	**使用SNAT访问公网**
弹性公网IP（Elastic IP，EIP）	实现VPC中的云主机以公网NAT网关的形式共享弹性公网IP访问公网或为公网提供服务。	**使用SNAT访问公网** **使用DNAT为云主机面向公网提供服务**

相关服务	交互功能	位置
云监控（Cloud Eye Service，CES）	查看NAT网关的监控数据，还可以获取可视化监控图表。	查看监控指标
统一身份认证服务（Identity and Access Management，IAM）	如果您需要对云上创建的NAT网关资源，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。	《统一身份认证服务用户指南》
云审计服务（CTS）	通过云审计服务，可以记录与NAT网关服务相关的操作事件，便于日后的查询、审计和回溯。	《云审计服务用户指南》

1.7 计费说明

计费项

公网NAT网关根据您选择的公网NAT网关规格和使用时长计费。

公网NAT网关共有小型、中型、大型和超大型四种规格。

说明

私网NAT网关目前不计费，可免费使用。

计费模式

说明

按需（天）计费模式的计费周期为：从前一天早上8点至第二天早上8点为一天，不满一天的按一天计算。

例如：您在2022年11月29日6:00:00购买了公网NAT网关，则截止2022年11月30日7:59:59，您使用公网NAT网关的天数为2天。

变更配置

修改规格时，将按照当日使用的最大规格进行计费。

1.8 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1-4所示，包括了NAT网关的所有系统权限。

表 1-4 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1-5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 1-5 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	√	√	√
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	√

说明

- 创建DNAT规则时需注意以下事项：
  - DNAT规则不支持企业项目授权。
  - 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》。
- 查询预定义标签，还需要配置TMS服务的TMS Administrator权限，具体详见《标签管理服务API参考》。

相关链接

- 创建用户并授权使用NAT网关

1.9 区域和可用区

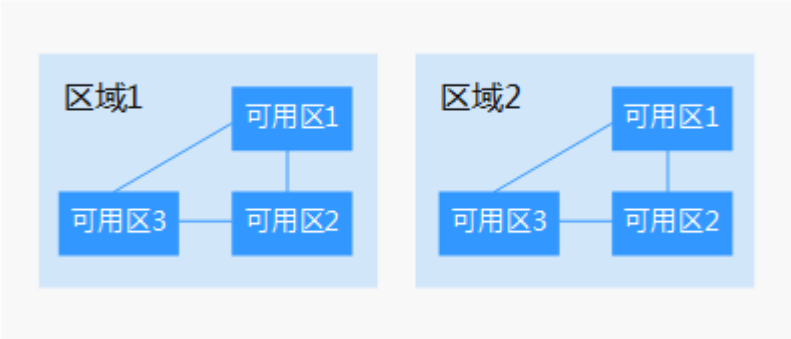
什么是区域、可用区?

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。有关云服务的区域和终端节点的更多信息，请参阅**地区和终端节点**。

1.10 基本概念

弹性 IP

弹性IP是基于互联网上的静态IP地址。

弹性IP地址为可以直接访问Internet的IP地址。私有IP地址为公有云内局域网络所有的IP地址，私有IP地址禁止出现在Internet中。

将弹性IP地址和子网中关联的绑定，可以实现VPC中的通过固定的公网IP地址与互联网互通。

一个弹性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NAT网关，更多内容请参见《 NAT网关用户指南 》。

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转换之后的弹性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。

DNAT 连接

DNAT连接是通过DNAT功能绑定弹性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IP，为互联网提供服务。

2 快速入门

2.1 使用 SNAT 访问公网

2.1.1 入门指引

当多个云主机（弹性云服务器、裸金属服务器）在没有绑定弹性IP的情况下需要访问公网，为了节省弹性IP资源并且避免云主机IP直接暴露在公网上，可以通过NAT网关共享弹性IP的方式访问公网，可以按照图2-1所示，实现无弹性IP的云主机访问公网。

图 2-1 无弹性 IP 的云主机访问公网流程图

2.1.2 步骤 1：申请弹性 IP

操作场景

通过申请弹性IP来实现VPC中的云主机以NAT网关的形式共享弹性IP访问公网。

操作步骤

详细步骤请参考《 虚拟私有云用户指南 》。

这里申请弹性IP后，无需绑定云主机。

2.1.3 步骤 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。

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. 在系统首页，单击“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“创建NAT网关”，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2-1。

表 2-1 参数说明

参数	参数说明
区域	公网NAT网关所在的区域。
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）。

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。 **说明** 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。
规格	公网NAT网关的规格。 公网NAT网关共有小型、中型、大型、超大型四种规格类型，可通过“了解更多”查看各规格详情。
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“>”。

5. 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。
6. 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1-6分钟。
7. 在“公网NAT网关”列表，查看公网NAT网关状态。

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。如下步骤以在自定义路由表中添加路由为例。

添加默认路由指向公网 NAT 网关

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟私有云”。
3. 单击左侧的“路由表”。
4. 在路由表页面，单击右上角的“创建路由表”。
   所属VPC：选择公网NAT网关所在的VPC。
5. 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。

6. 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
7. 单击“确定”。

2.1.4 步骤 3：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，您可以将该子网下的云主机通过共享弹性IP访问互联网。

一个子网或一条网段对应一条SNAT规则，如果VPC中有多个子网或网段需要访问公网，则可以通过创建多个SNAT规则实现共享弹性IP资源。

前提条件

公网NAT网关创建成功。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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。配置参数请参见**表2-2**。

   表 2-2 参数说明

参数	说明
使用场景	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	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。
弹性IP	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IP，或者被绑定到当前公网NAT网关中SNAT规则上的弹性IP。
描述	SNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

6. 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。

2.1.5 步骤 4：结果验证

操作场景

SNAT规则添加完成后，分为以下两步验证：

1. 验证是否成功为目标公网NAT网关添加SNAT规则；
2. 验证未绑定EIP的服务器是否可以通过NAT网关访问公网。

操作前提

SNAT规则已经添加。

验证是否成功添加 SNAT 规则

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在公网NAT网关页面，单击目标公网NAT网关的名称。
4. 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。

验证服务器是否可以通过 NAT 网关访问公网

步骤1 登录管理控制台。

步骤2 登录需要验证的服务器。

步骤3 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

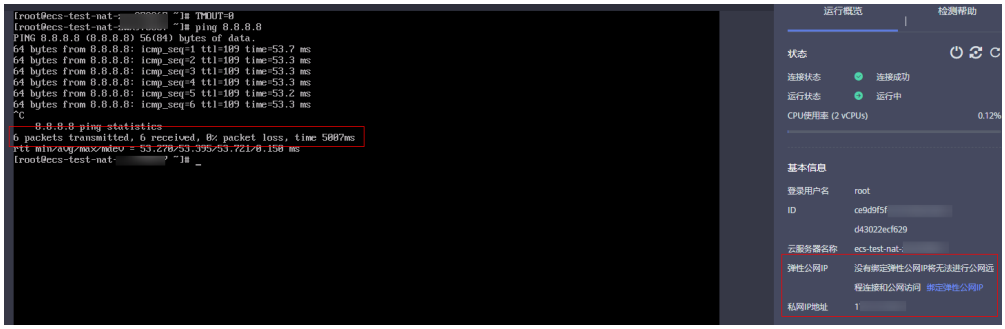
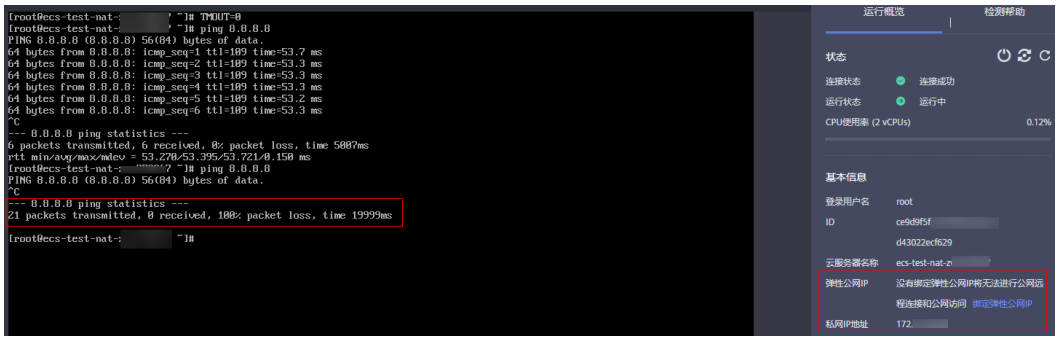


图 2-3 删除 SNAT 规则后无法访问公网



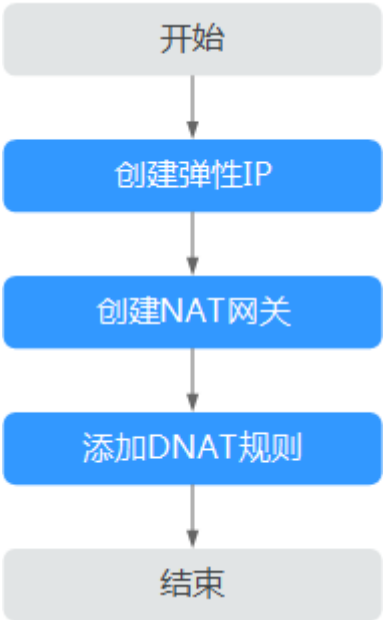
----结束

2.2 使用 DNAT 为云主机面向公网提供服务

2.2.1 入门指引

VPC内的一个或多个云主机（弹性云服务器、裸金属服务器）需要面向公网提供服务时，可以根据图2-4实现对公网提供服务。

图 2-4 面向公网提供服务流程图



2.2.2 步骤 1：申请弹性 IP

操作场景

通过申请弹性IP来实现VPC中的云主机通过NAT的方式为互联网提供服务。

操作步骤

详细步骤请参考《虚拟私有云用户指南》。

这里申请弹性IP后，无需绑定云主机。

2.2.3 步骤 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。

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. 在系统首页，单击“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“创建NAT网关”，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2-3**。

表 2-3 参数说明

参数	参数说明
区域	公网NAT网关所在的区域。
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）。
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。 **说明** 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。

参数	参数说明
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。
规格	公网NAT网关的规格。 公网NAT网关共有小型、中型、大型、超大型四种规格类型，可通过“了解更多”查看各规格详情。
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“>”。

5. 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。
6. 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1-6分钟。
7. 在“公网NAT网关”列表，查看公网NAT网关状态。

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。如下步骤以在自定义路由表中添加路由为例。

添加默认路由指向公网 NAT 网关

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟私有云”。
3. 单击左侧的“路由表”。
4. 在路由表页面，单击右上角的“创建路由表”。
   所属VPC：选择公网NAT网关所在的VPC。
5. 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。
6. 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
7. 单击“确定”。

2.2.4 步骤 3：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，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。

操作前提

已成功创建公网NAT网关。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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2-4**。

表 2-4 DNAT 规则参数说明

参数	说明
使用场景	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IP，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。 • 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IP，任何访问该弹性IP的请求都将转发到目标云主机实例上。 • 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IP的请求转发到目标云主机实例的指定端口上。
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。
弹性IP	弹性IP地址。 这里只能选择没有被绑定的弹性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IP，或者被绑定到当前公网NAT网关中SNAT规则上的弹性IP。

参数	说明
实例类型	选择对外部公网提供服务的实例类型。 • 服务器 • 虚拟IP地址 • 自定义
网卡	服务器网卡。实例类型为服务器时，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“>”。

7. 配置完成后，单击“确定”，完成“DNAT规则”创建。

须知

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

2.2.5 步骤 4：结果验证

操作场景

DNAT规则添加完成后，分为以下两步验证：

1. 验证是否成功为目标公网NAT网关添加DNAT规则；
2. 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（DNAT规则绑定的EIP为：120.46.131.153）访问到。

操作前提

DNAT规则已经添加。

验证是否成功添加 DNAT 规则

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
3. 在公网NAT网关页面，单击目标公网NAT网关的名称。
4. 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。

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

步骤1 登录管理控制台。

步骤2 登录绑定了EIP的服务器ECS02。

步骤3 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 2-5 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-                ~]#
```

图 2-6 删除 DNAT 规则后无法被访问到

```
[root@ecs-                ~]# ping 120.46.131.153
PING 120.46.131.153 (120.46.131.153) 56(84) bytes of data.
^C
--- 120.46.131.153 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5104ms

[root@ecs-                ~]#
```

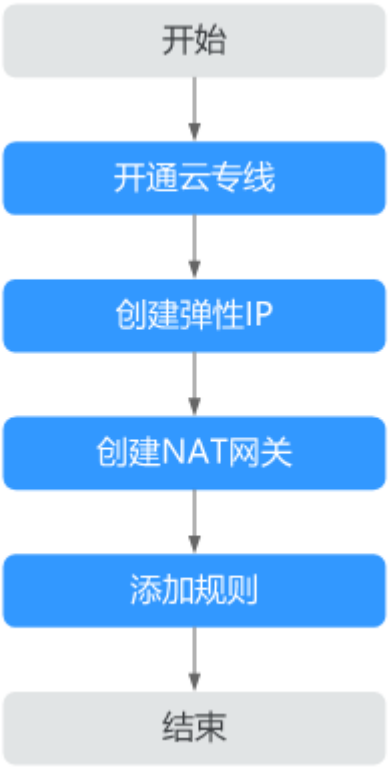
----结束

2.3 云间 NAT 网关高速访问互联网

2.3.1 入门指引

用户本地数据中心的服务器需要访问公网或为公网提供服务时，公网NAT网关可为您提供高效、优质的网络服务。可以通过开通云专线或VPN实现本地数据中心上云，然后创建公网NAT网关，通过配置SNAT规则实现访问公网或配置DNAT规则为互联网提供服务。此快速入门流程以云专线用户为例，本地数据中心用户访问公网快速入门流程如图2-7所示。

图 2-7 本地数据中心用户访问公网流程图



2.3.2 步骤 1：开通云专线

操作场景

用户本地数据中心的服务器需要通过公网NAT网关实现访问公网或为公网提供服务，需要先通过云专线接入虚拟私有云。

操作步骤

详细步骤请参考《 云专线用户指南 》，申请开通云专线。

2.3.3 步骤 2：申请弹性 IP

操作场景

通过申请弹性IP来实现云专线接入公有云的用户，以NAT网关的形式共享弹性IP访问公网或为公网提供服务。

操作步骤

详细步骤请参考《 虚拟私有云用户指南 》。

这里申请弹性IP后，无需绑定云主机。

2.3.4 步骤 3：创建公网 NAT 网关

操作场景

如果您要通过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。

前提条件

- 已创建了公网NAT网关所需的VPC和子网。
- 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. 在系统首页，单击“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“创建NAT网关”，进入公网NAT网关创建页面。
4. 根据界面提示，配置NAT网关的基本信息，配置参数请参见**表2-5**。

表 2-5 参数说明

参数	参数说明
区域	公网NAT网关所在的区域。
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）。
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。 **说明** 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。

参数	参数说明
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。
规格	公网NAT网关的规格。 公网NAT网关共有小型、中型、大型和超大型四种规格类型，可通过“了解更多”查看各规格详情。
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“>”。

5. 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。
6. 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。
7. 在“公网NAT网关”列表，查看公网NAT网关状态。

   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。如下步骤以在自定义路由表中添加路由为例。

添加默认路由指向公网 NAT 网关

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟私有云”。
3. 单击左侧的“路由表”。
4. 在路由表页面，单击右上角的“创建路由表”。

   所属VPC：选择公网NAT网关所在的VPC。
5. 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。
6. 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
7. 单击“确定”。

2.3.5 步骤 4：添加 SNAT 规则

操作场景

公网NAT网关创建成功后，您可以为公网NAT网关添加SNAT规则。通过添加SNAT规则，云专线用户侧端的服务器可以通过共享弹性IP访问互联网。

一个网段对应一条SNAT规则，如果云专线用户侧有多个网段中的服务器需要访问公网，则可以通过创建多个SNAT规则实现共享一个或多个弹性IP资源。

操作前提

公网NAT网关创建成功。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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2-6**。

   表 2-6 SNAT 规则参数说明

参数	说明
使用场景	在云间NAT网关高速访问互联网的场景下，此处选择云专线。 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SNAT的方式访问公网。
网段	通过配置云专线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。
弹性IP	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IP，或者被绑定到当前公网NAT网关中SNAT规则上的弹性IP。
描述	SNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

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

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。

2.3.6 步骤 5：添加 DNAT 规则

操作场景

公网NAT网关创建后，添加DNAT规则，则可以通过映射方式将您本地数据中心的服务器对互联网提供服务。

一个云主机的一个端口对应一条DNAT规则，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规则来实现共享一个或多个弹性IP访问公网。

操作前提

已成功创建公网NAT网关。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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2-7。

表 2-7 DNAT 规则参数说明

参数	说明
使用场景	在云间NAT网关高速访问互联网的场景下，此处选择云专线。 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。 • 所有端口：属于IP映射方式。此方式相当于为服务器配置了一个弹性IP，任何访问该弹性IP的请求都将转发到目标服务器实例上。 • 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IP的请求转发到目标服务器的指定端口上。
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。

参数	说明
弹性IP	弹性IP地址。 这里只能选择没有被绑定的弹性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IP，或者被绑定到当前公网NAT网关中SNAT规则上的弹性IP。
实例类型	选择对外部公网提供服务的实例类型。 • 服务器 • 虚拟IP地址 • 自定义
网卡	服务器网卡。实例类型为服务器时，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“>”。

7. 配置完成后，单击“确定”，完成“DNAT规则”创建。

须知

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

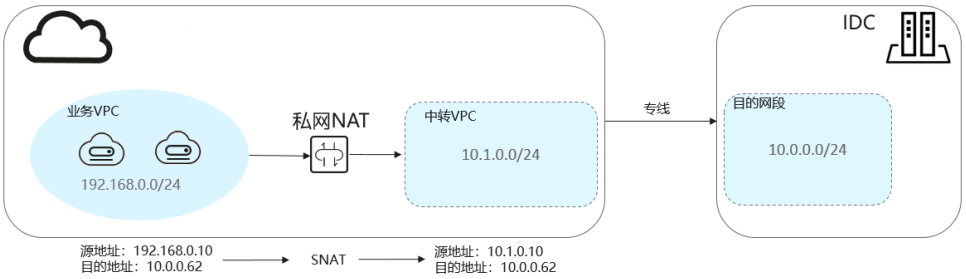
2.4 使用私网 NAT 网关为 VPC 内计算实例实现线上线下互通

2.4.1 入门指引

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 2-8 组网图



下列配置指导仅以VPC Peering做示例，实际专线配置以云专线指导为准。

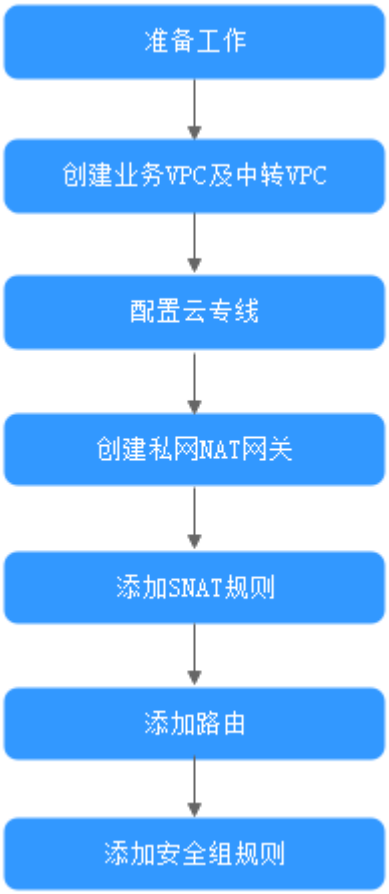
假设用户IDC（Peering目的VPC）网段为10.0.0.0/24，中转VPC子网网段为10.1.0.0/24。

实现方式如下：

1. 通过云专线（Peering）将用户IDC（Peering目的VPC）与中转VPC连通。
2. 搭建私网NAT网关，将业务VPC与目的网段（Peering目的VPC）连通。

您将按以下流程学习如何创建和使用私网NAT网关。

图 2-9 入门流程



2.4.2 步骤 1：创建业务 VPC 及中转 VPC

操作场景

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）。

操作步骤

具体操作请参见《虚拟私有云用户指南》中的“创建虚拟私有云和子网”。

2.4.3 步骤 2：配置云专线（本示例使用 VPC Peering 代替云专线）

操作场景

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。

操作步骤

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《虚拟私有云用户指南》中的“VPC对等连接”。

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《云专线用户指南》配置云专线。

2.4.4 步骤 3：创建私网 NAT 网关

操作场景

如果您要将本端业务VPC与远端私网/远端VPC连通，则需要创建私网NAT网关。

前提条件

中转VPC中需要提前自定义好用来为本端业务VPC中的资源做私网IP地址转换的私网网段（用来定义中转子网中的中转IP）。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，单击“网络 > NAT网关 > 私网NAT网关”。
   进入私网NAT网关页面。
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2-8。

表 2-8 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。

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、大型和超大型四种规格类型。
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“>”。

6. 单击“立即创建”，开始创建私网NAT网关。
7. 在“私网NAT网关”列表，查看私网NAT网关状态。
8. 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。

图 2-10 创建中转 IP

9. 根据界面提示，配置中转IP的基本信息，配置参数请参见**表2-9**。

表 2-9 中转 IP 参数说明

参数	参数说明
中转VPC	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。

参数	参数说明
中转IP	中转IP的分配方式有以下两种。 **自动分配**：由系统自动分配中转IP地址。 **手动分配**：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。

10. 中转IP的分配方式选择“自动分配”，单击“确定”，开始创建中转IP。

2.4.5 步骤 4：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。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，单击“网络 > NAT网关 > 私网NAT网关”。
   进入私网NAT网关页面。
4. 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。
5. 在SNAT规则页签中，单击“添加SNAT规则”。

图 2-11 添加 SNAT 规则

6. 根据界面提示，配置添加SNAT规则参数，详情请参见。

表 2-10 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	中转IP选择**步骤3**创建的中转IP。
描述	SNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

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

2.4.6 步骤 5：添加路由

操作场景

私网NAT网关配置完成后，您还需要在业务VPC中添加指向私网NAT网关的路由。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航栏选择“路由表”。
5. 在路由表列表中，单击业务VPC的路由表名称。
6. 单击“添加路由”，按照提示配置参数。

表 2-11 参数说明

参数	参数说明
目的地址	目的地址网段。 配置为IDC（目的VPC）的私网网段。
下一跳类型	下一跳资源类型选择“NAT网关”。
下一跳	下一跳资源选择创建的私网NAT网关。
描述	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“>”。

7. 单击“确定”，完成添加。

2.4.7 步骤 6：添加安全组规则

操作场景

在目的VPC包含的云主机中添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。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 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。
6. 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 2-12 入方向参数说明

参数	说明	取值样例
协议端口	网络协议。目前支持“All”、“TCP”、“UDP”、“ICMP”和“GRE”等协议。	TCP
	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。	22或22-30
类型	IP地址类型。开通IPv6功能后可见。 ● IPv4 ● IPv6	IPv4
源地址	源地址：可以是IP地址、安全组。用于放通来自IP地址或另一安全组内的实例的访问。例如： ● xxx.xxx.xxx.xxx/32（IPv4地址） ● xxx.xxx.xxx.0/24（子网） ● 0.0.0.0/0（任意地址） ● sg-abc（安全组）	0.0.0.0/0
描述	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“>”。	-

7. 单击“确定”，完成添加。

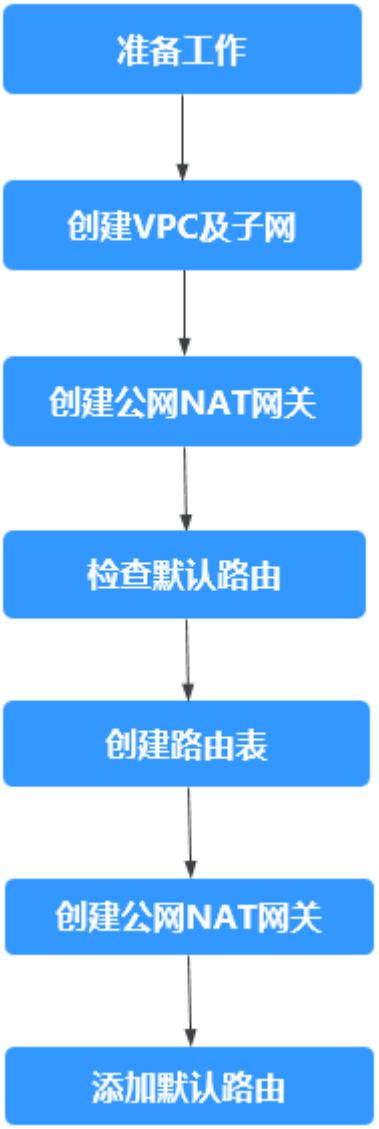
2.5 公网 NAT 网关通过多网关扩展容量

2.5.1 入门指引

当单网关性能达到瓶颈，如SNAT支持最大100万连接不够使用或最高20Gbit/s带宽转换能力无法满足业务需求时，推荐使用多网关来横向扩展容量，同时可达到更好的隔离性。

通过本文档，您可以学习到如何部署公网NAT网关多实例。

图 2-12 入门流程



2.5.2 步骤 1：创建 VPC 及子网

操作场景

本示例需要使用1个VPC和2个子网。首先创建1个VPC，再创建2个子网。

操作步骤

具体操作请参见《虚拟私有云用户指南》中的“创建虚拟私有云和子网”。

2.5.3 步骤 2：创建公网 NAT 网关

操作场景

指定VPC，创建第一个公网NAT网关。

前提条件

业务VPC已经创建完成。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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“创建NAT网关”，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2-13**。
   虚拟私有云请选择**步骤1**创建的业务VPC，子网选择**步骤1**创建的其中一个子网。

表 2-13 参数说明

参数	参数说明
区域	公网NAT网关所在的区域。
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）。
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。
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。

参数	参数说明
规格	公网NAT网关的规格。 公网NAT网关共有小型、中型、大型和超大型四种规格类型，可通过“了解更多”查看各规格详情。
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“>”。

5. 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。
6. 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1-6分钟。
7. 在“公网NAT网关”列表，查看公网NAT网关状态。

2.5.4 步骤 3：检查默认路由

操作场景

公网NAT网关创建好后，进入VPC路由表界面，检查默认路由表下是否存在指向公网NAT网关的默认路由。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航栏选择“路由表”。
5. 在路由表列表中，单击需要查看路由规则的路由表名称。
6. 进入路由表详情页面，检查是否存在指向公网NAT网关的默认路由。

说明

VPC下第一个公网NAT网关创建时会在默认路由表自动下发0.0.0.0/0的默认路由，若VPC下已经存在此路由，则需要在路由表界面手动修改路由，指向所创建的公网NAT网关。

2.5.5 步骤 4：创建路由表

操作场景

公网NAT网关多实例依赖VPC多路由表功能，所以需要在VPC中创建第二张路由表。

说明

如果自定义路由表配额不足，请通过申请扩大路由表的配额。

前提条件

VPC下路由表配额充足。

操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏，选择“路由表”。
4. 在页面右上角，单击“创建路由表”，按照提示配置参数。

表 2-14 参数说明

参数	说明	取值样例
路由表名称	路由表的名称，必填项。 路由表的名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。	rtb-001
所属VPC	选择路由表归属的VPC，必填项。	vpc-001
描述	路由表的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-
添加路由	路由规则信息，非必填项。 路由规则可以在此处添加，也可以在路由表创建完成后。 单击“+”可以依次增加多条路由。	-

5. 单击“确定”，完成创建。
   系统出现信息提示页面，请您根据提示关联子网。请参考以下步骤进行关联：
   a. 单击“关联子网”，进入路由表详情页面的“关联子网”页签。
   b. 单击“关联子网”，选择**步骤1**创建的第二个子网。
   c. 单击“确定”，完成关联。

2.5.6 步骤 5：创建公网 NAT 网关

操作场景

在业务VPC下，创建第二个公网NAT网关。

前提条件

VPC中完成第二张路由表的创建，且已关联第二个子网。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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“创建NAT网关”，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2-15**。
   虚拟私有云请选择**步骤1**创建的业务VPC，子网选择**步骤1**创建的第二个子网。

   表 2-15 参数说明

参数	参数说明
区域	公网NAT网关所在的区域。
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）。
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。
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。
规格	公网NAT网关的规格。 公网NAT网关共有小型、中型、大型和超大型四种规格类型，可通过“了解更多”查看各规格详情。
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“>”。

5. 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。
6. 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1-6分钟。
7. 在“公网NAT网关”列表，查看公网NAT网关状态。

2.5.7 步骤 6：添加默认路由

操作场景

从第二个网关开始，需要在新路由表中创建0.0.0.0/0指向公网NAT网关的默认路由。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航栏选择“路由表”。

5. 在路由表列表中，单击需要添加路由规则的路由表名称。
6. 单击“添加路由”，按照提示配置参数。

   单击 ⊕，可以依次增加多条路由。

   表 2-16 参数说明

参数	说明	取值样例
目的地址	目的地址网段。 目的地址不能与已有路由冲突，目的地址也不能与VPC下子网网段冲突。	0.0.0.0/0
下一跳类型	选择下一跳资源类型。	NAT网关
下一跳	选择下一跳资源。下拉列表包含资源将基于您所选的资源类型进行展示。	-
描述	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“>”。	-

7. 单击“确定”，完成添加。

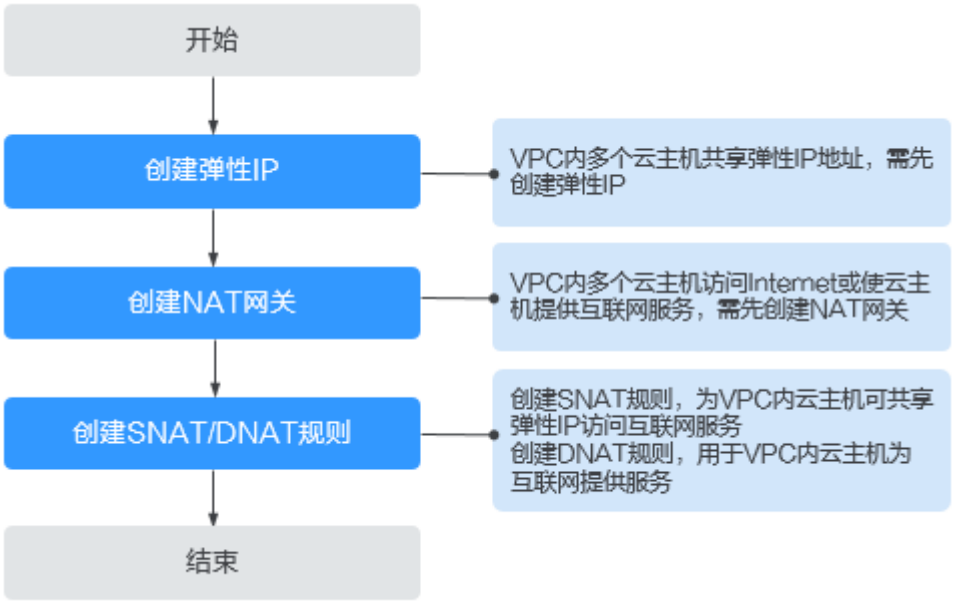
3 公网 NAT 网关

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，使多个云主机可以共享弹性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



说明

由于SNAT和DNAT不能共用同一个弹性IP，所以如果您需要分别创建SNAT规则和DNAT规则时，需要申请2个弹性IP。

3.2 管理公网 NAT 网关

3.2.1 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IP，不同网关下的规则必须使用不同的弹性IP。
- 每个VPC支持的NAT网关数为1。
- 一个VPC支持关联多个公网NAT网关。
- SNAT和DNAT不能共用同一个弹性IP。
- 当云主机同时配置弹性IP服务和公网NAT网关服务时，数据均通过弹性IP转发。
- 出于安全因素考虑，部分运营商会对下列端口进行拦截，导致无法访问。建议避免使用下列端口：

协议	不支持端口
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 4790 5554 5800 5900 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

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. 在系统首页，单击“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“创建NAT网关”，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。
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）。
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。 **说明** 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。
规格	公网NAT网关的规格。 公网NAT网关共有小型、中型、大型、超大型四种规格类型，可通过“了解更多”查看各规格详情。
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“>”。

5. 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。
6. 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1-6分钟。
7. 在“公网NAT网关”列表，查看公网NAT网关状态。

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。如下步骤以在自定义路由表中添加路由为例。

添加默认路由指向公网 NAT 网关

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟私有云”。

3. 单击左侧的“路由表”。
4. 在路由表页面，单击右上角的“创建路由表”。
   所属VPC：选择公网NAT网关所在的VPC。
5. 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。
6. 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
7. 单击“确定”。

3.2.2 查看公网 NAT 网关

操作场景

公网NAT网关创建后，可以查看已经创建的公网NAT网关的详情。

操作前提

公网NAT网关创建成功。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
   进入公网NAT网关页面。
3. 在公网NAT网关页面，单击需要查看详情的公网NAT网关名称。
4. 系统跳转至目标公网NAT网关详情页面，即可查看目标公网NAT网关的详情。

3.2.3 修改公网 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。

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。

操作前提

公网NAT网关创建成功。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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。

3.2.4 删除公网 NAT 网关

操作场景

公网NAT网关创建后，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，节省费用。

操作前提

- 必须保证公网NAT网关下的SNAT规则和DNAT规则已全部删除。如果公网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，请先在公网NAT网关页面进行**删除SNAT规则**和**删除DNAT规则**操作。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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. 在弹出的对话框中单击“是”，完成公网NAT网关的删除。

3.3 管理 SNAT 规则

3.3.1 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。

前提条件

公网NAT网关创建成功。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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。
弹性IP	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IP，或者被绑定到当前公网NAT网关中SNAT规则上的弹性IP。
描述	SNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

6. 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。

3.3.2 查看 SNAT 规则

操作场景

SNAT规则添加完成后，可以查看为目标公网NAT网关添加的SNAT规则。

操作前提

SNAT规则已经添加。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
   进入公网NAT网关页面。
3. 在公网NAT网关页面，单击目标公网NAT网关的名称。
4. 在SNAT页签的SNAT规则列表中，查看目标公网NAT网关已经创建的SNAT规则详细信息。

3.3.3 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。

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. 在系统首页，单击“网络 > NAT网关”。
   进入公网NAT网关页面。
3. 在公网NAT网关页面，单击目标公网NAT网关的名称。
4. 系统跳转至目标公网NAT网关详情页面，单击“SNAT规则”页签。
5. 在SNAT规则列表中，单击目标SNAT规则操作列中的“修改”。
6. 在弹出的对话框中，修改参数中的内容。
7. 单击“确定”，完成SNAT规则的修改。

3.3.4 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. 在系统首页，单击“网络 > NAT网关”。
   进入公网NAT网关页面。
3. 在公网NAT网关页面，单击目标公网NAT网关的名称。
4. 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”。

5. 在弹出的对话框中单击“是”，完成SNAT规则的删除。

3.4 管理 DNAT 规则

3.4.1 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

- DNAT规则不支持将弹性IP绑定到虚拟IP。
- 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。

操作前提

已成功创建公网NAT网关。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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。

参数	说明
端口类型	分为所有端口和具体端口两种类型。 • 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IP，任何访问该弹性IP的请求都将转发到目标云服务器实例上。 • 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IP的请求转发到目标云主机实例的指定端口上。
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。
弹性IP	弹性IP地址。 这里只能选择没有被绑定的弹性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IP，或者被绑定到当前公网NAT网关中SNAT规则上的弹性IP。
实例类型	选择对外部公网提供服务的实例类型。 • 服务器 • 虚拟IP地址 • 自定义
网卡	服务器网卡。实例类型为服务器时，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“>”。

7. 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。

3.4.2 查看 DNAT 规则

操作场景

DNAT规则添加完成后，可以查看为目标公网NAT网关添加的DNAT规则。

操作前提

DNAT规则已经添加。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
   进入公网NAT网关页面。
3. 在公网NAT网关页面，单击目标公网NAT网关的名称。
4. 系统跳转至目标公网NAT网关详情页面，单击“DNAT规则”页签。
5. 在DNAT规则列表中，查看目标公网NAT网关已经创建的DNAT规则详细信息。

3.4.3 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。

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. 在系统首页，单击“网络 > NAT网关”。
   进入公网NAT网关页面。
3. 在公网NAT网关页面，单击目标公网NAT网关的名称。
4. 系统跳转至目标公网NAT网关详情页面，单击“DNAT规则”页签。
5. 在DNAT规则列表中，单击目标DNAT规则操作列中的“修改”。
6. 在弹出的对话框中，修改参数中的内容。
7. 单击“确定”，完成DNAT规则的修改。

3.4.4 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. 在系统首页，单击“网络 > NAT网关”。
   进入公网NAT网关页面。
3. 在公网NAT网关页面，单击目标公网NAT网关的名称。

4. 系统跳转至目标公网NAT网关详情页面，单击“DNAT规则”页签。
5. 在DNAT规则列表中，单击目标DNAT规则操作列中的“删除”。
6. 在弹出的对话框中单击“是”，完成DNAT规则的删除。

3.4.5 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. 在系统首页，单击“网络 > NAT网关”。
   进入公网NAT网关页面。
3. 在公网NAT网关页面，单击目标NAT网关的名称。
4. 系统跳转至目标公网NAT网关详情页面，单击“DNAT规则”页签。
5. 在DNAT规则列表中，勾选目标DNAT规则，单击“删除DNAT规则”。
6. 在弹出的对话框中单击“是”，完成DNAT规则的批量删除。

3.4.6 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。

一个云主机绑定一条DNAT规则，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。

操作前提

已成功创建公网NAT网关。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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“导入DNAT规则列表”，下载模板。
6. 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。 ● 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。 ● 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。
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	● 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。 ● 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。 ● 协议类型为TCP、UDP时，需要配置私网IP的端口。
私网端口	● 当使用场景为虚拟私有云时，指云主机的端口号。 ● 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。 ● 端口类型为“全部”时，不需要配置此参数。 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“>”。

7. 模板填写完后，单击“导入DNAT规则列表”图标，选择本地模板，单击“导入”。
8. 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。
9. 在弹出的对话框中单击“是”，完成DNAT规则的批量删除。

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。

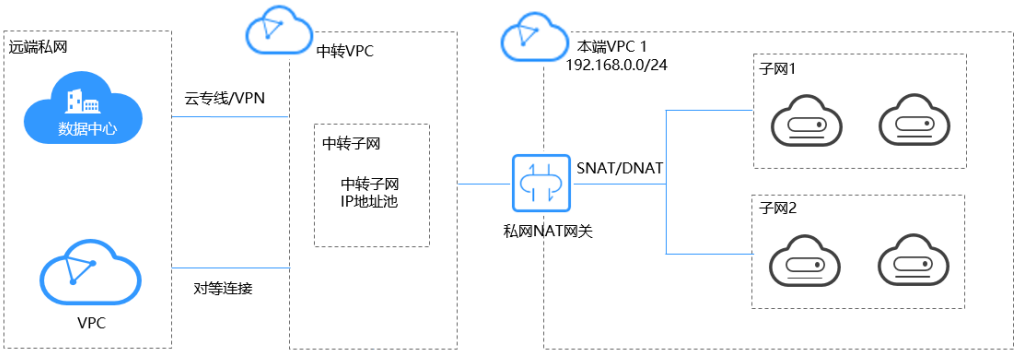
中转子网

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



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IP	中转IP

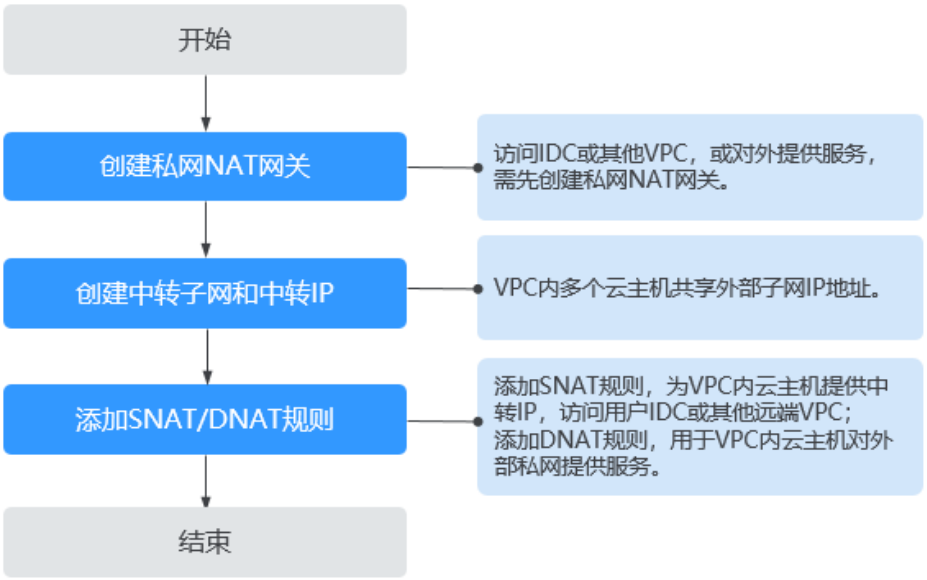
4.2 创建私网 NAT 网关

4.2.1 概述

本章主要介绍创建私网NAT网关以及配置私网NAT网关。

私网NAT网关的使用流程如下：

图 4-2 私网 NAT 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**。

4.2.2 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. 在系统首页，单击“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）。
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《产品简介》中的“产品规格”章节。
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“>”。

表 4-3 标签命名规则

参数	规则
键	• 不能为空。 • 对于同一NAT网关键值唯一。 • 长度不超过36个字符。
值	• 长度不超过43个字符。

6. 单击“立即创建”。

相关链接

管理私网NAT网关

4.2.3 创建中转 IP

操作场景

私网NAT网关创建成功后，您需要创建中转IP。

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。

前提条件

- 中转VPC已创建成功。
- 云专线接入的用户，云专线的虚拟网关中，“VPC网段”参数建议设置为"0.0.0.0/0"。具体配置请参考《云专线用户指南》。

操作步骤

1. 登录管理控制台。

2. 在系统首页，单击“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“中转IP > 创建中转IP”，进入创建中转IP页面。

图 4-3 创建中转 IP

5. 根据界面提示，配置中转IP的基本信息，配置参数请参见表4-4。

表 4-4 中转 IP 参数说明

参数	参数说明
中转VPC	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	中转IP的分配方式有以下两种。 **自动分配**：由系统自动分配中转IP地址。 **手动分配**：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。

6. 单击“确定”，完成中转IP创建。

4.2.4 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. 在系统首页，单击“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，单击需要添加SNAT规则的私网NAT网关名称。
5. 在SNAT规则页签中，单击“添加SNAT规则”。
6. 根据界面提示，配置添加SNAT规则参数，详情请参见。

图 4-4 添加 SNAT 规则

表 4-5 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。

参数	参数说明
描述	SNAT规则信息描述。最大支持255个字符，且不能包含“<”和“>”。

7. 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

4.2.5 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. 登录管理控制台。
2. 在系统首页，单击“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，单击需要添加DNAT规则的私网NAT网关名称。
5. 在私网NAT网关详情页面中，单击“DNAT规则”页签。
6. 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。

7. 根据界面提示，配置添加DNAT规则参数，详情请参见表4-6。

图 4-5 添加 DNAT 规则

表 4-6 DNAT 规则参数说明

参数	说明
本端网络	
端口类型	分为具体端口和所有端口两种类型。 • 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。 • 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。
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。
实例类型	选择对外部私网提供服务的实例类型。 • 服务器 • 虚拟IP地址 • 负载均衡器 • 自定义
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。

参数	说明
中转网络	
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“>”。

8. 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

4.3 管理私网 NAT 网关

4.3.1 查看私网 NAT 网关

操作场景

私网NAT网关创建后，可以查看已经创建的私网NAT网关的详情。

前提条件

私网NAT网关创建成功。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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，单击需要查看详情的私网NAT网关名称。
5. 系统跳转至目标私网NAT网关详情页面，即可查看目标私网NAT网关的详情。

4.3.2 修改私网 NAT 网关

操作场景

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。

前提条件

私网NAT网关创建成功。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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，单击需要修改的私网NAT网关操作列中的“修改”。
5. 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。
6. 修改完成后，单击“确定”，完成私网NAT网关信息的修改。
   在私网NAT网关列表可以看到修改后的信息。

4.3.3 删除私网 NAT 网关

操作场景

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，节省费用。

前提条件

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。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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，单击目标私网NAT网关操作列中的“删除”。
5. 在弹出的对话框中单击“是”，完成私网NAT网关的删除。

4.4 管理 SNAT 规则

4.4.1 查看 SNAT 规则

操作场景

SNAT规则添加完成后，可以查看为目标私网NAT网关添加的SNAT规则。

前提条件

SNAT规则已经添加。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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，单击目标私网NAT网关的名称。
5. 在SNAT规则页签的SNAT规则列表中，查看目标私网NAT网关已经创建的SNAT规则详细信息。

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。

前提条件

私网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. 在系统首页，单击“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，单击目标私网NAT网关的名称。
5. 系统跳转至目标私网NAT网关详情页面，单击“SNAT规则”页签。
6. 在SNAT规则列表中，单击目标私网SNAT规则操作列中的“修改”。
7. 在弹出的对话框中，修改参数中的内容。
8. 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

1. 登录管理控制台。
2. 在系统首页，单击“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，单击目标私网NAT网关的名称。
5. 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”。
6. 在弹出的对话框中单击“是”，完成SNAT规则的删除。

4.5 管理 DNAT 规则

4.5.1 查看 DNAT 规则

操作场景

DNAT规则添加完成后，可以查看为目标私网NAT网关添加的DNAT规则。

前提条件

DNAT规则已经添加。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“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，单击目标私网NAT网关的名称。
5. 系统跳转至目标私网NAT网关详情页面，单击“DNAT规则”页签。
6. 在DNAT规则列表中，查看目标私网NAT网关已经创建的DNAT规则详细信息。

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。

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. 登录管理控制台。

2. 在系统首页，单击“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，单击目标私网NAT网关的名称。
5. 系统跳转至目标私网NAT网关详情页面，单击“DNAT规则”页签。
6. 在DNAT规则列表中，单击目标DNAT规则操作列中的“修改”。
7. 在弹出的对话框中，修改参数中的内容。
8. 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. 登录管理控制台。
2. 在系统首页，单击“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，单击目标私网NAT网关的名称。
5. 系统跳转至目标私网NAT网关详情页面，单击“DNAT规则”页签。
6. 在DNAT规则列表中，单击目标DNAT规则操作列中的“删除”。
7. 在弹出的对话框中单击“是”，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. 在系统首页，单击“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“中转IP > 创建中转IP”，进入创建中转IP页面。

图 4-6 创建中转 IP

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. 登录管理控制台。
2. 在系统首页，单击“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“中转IP”页签，单击目标中转IP名称。
5. 进入中转IP详情页，即可查看已创建的中转IP的详细信息。

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. 登录管理控制台。
2. 在系统首页，单击“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“中转IP”页签，单击目标中转IP操作列的“释放”。
5. 单击“是”。

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：**权限管理**。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“NAT ReadOnlyAccess”。
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NAT ReadOnlyAccess），表示“NAT ReadOnlyAccess”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NAT ReadOnlyAccess）的任一服务，若提示权限不足，表示“NAT ReadOnlyAccess”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 监控管理

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	≥ 0个	公网NAT网关实例	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	公网NAT网关实例	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	≥0 bit/s	公网NAT网关实例	1分钟
inbound_pps	入方向PPS	该指标用于统计SNAT入方向PPS。 单位：个	≥0个	公网NAT网关实例	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网关实例	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网关实例	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网关实例	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网关实例	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实例最大带宽20Gbit/s，则入方向带宽使用率为：**实际使用带宽/公网NAT实例最大带宽***100%。 单位：百分比 **说明** 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网关实例	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实例最大带宽为20Gbit/s，则出方向带宽使用率为：**实际使用带宽/公网NAT实例最大带宽***100%。 单位：百分比 **说明** 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网关实例	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网关实例	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网关实例	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网关实例	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网关实例	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网关实例	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网关实例	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网关实例	1分钟

维度

Key	Value
nat_gateway_id	公网NAT网关实例标识
vpc_nat_gateway_id	私网NAT实例标识

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”进行添加，或者选择已有的告警规则进行修改，设置NAT网关的告警规则。
5. 在“创建告警规则”界面，根据界面提示配置参数。
   a. 根据界面提示，配置告警规则的基本信息。

表 6-3 配置规则信息

参数	参数说明
名称	系统会随机产生一个名称，用户也可以进行修改。 取值样例：alarm-b6al
描述	告警规则描述（此参数非必填项）。

   b. 选择监控对象，配置告警内容参数。

表 6-4 配置告警内容

参数	参数说明	取值样例
资源类型	配置告警规则监控的服务名称。	NAT网关
维度	用于指定告警规则对应指标的维度名称	公网NAT网关
监控范围	告警规则适用的资源范围，可选择资源分组或指定资源。 **说明** • 当选择资源分组时，该分组下任何资源满足告警策略时，都会触发告警通知。 • 选择指定资源时，勾选具体的监控对象，单击  将监控对象同步到右侧对话框。	指定资源
选择类型	根据需要可选择从模板导入或自定义创建。	自定义创建

参数	参数说明	取值样例
模板	选择需要导入的模板。 您可以选择系统预置的默认告警模板，或者选择自定义模板。	-
告警策略	触发告警规则的告警策略。 当资源类型选择站点监控、日志监控、自定义监控、具体的云服务时，是否触发告警取决于连续周期的数据是否达到阈值。例如SNAT连接数监控周期为1分钟，连续三个周期原始值≥8000个，则触发告警。	-
告警级别	根据告警的严重程度不同等级，可选择紧急、重要、次要、提示。	重要

c. 根据界面提示，配置告警通知参数。

表 6-5 配置告警通知

参数	参数说明
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知对象	需要发送告警通知的对象，可选择云账号联系人或主题名称。 ● 云账号联系人为注册账号时的手机和邮箱。 ● 主题是消息发布或客户端订阅通知的特定事件类型，若此处没有需要的主题则需先创建主题并添加订阅，创建主题并添加订阅请参见《 云监控用户指南 》。
生效时间	该告警规则仅在生效时间内发送通知消息。 如生效时间为08:00-20:00，则该告警规则仅在08:00-20:00发送通知消息。
触发条件	可以选择“出现告警”、“恢复正常”两种状态，作为触发告警通知的条件。

6. 规则参数设置完成后，单击“立即创建”。
   NAT网关告警规则设置完成后，当符合规则的告警产生时，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。

6.4 查看 NAT 网关后端实例对应的监控指标

操作场景

如果您需要查看特定NAT网关的某个监控指标下各个后端实例对应的该监控指标情况，您可以按照如下步骤操作。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > NAT网关”。
   进入NAT网关页面。
3. 在NAT网关页面，单击需要查看监控指标的NAT网关名称。
4. 切换至“监控”页签，单击页面中间的“查看更多指标详情”。
   进入云监控服务的查看NAT网关监控指标页面。
5. 选择所需查看的监控指标时间段。
6. 单击页面右上角的切换视图图标  ，来切换各个监控指标展示的方式。
7. 选择所需查看的监控指标并在显示的监控指标图中选择某一时间点。
   在页面下方就可以查看到NAT网关后端实例对应的该监控指标情况。

7 常见问题

7.1 公网 NAT 网关

7.1.1 公网 NAT 网关、弹性 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 哪些端口无法访问?

出于安全因素考虑，部分运营商会对下列端口进行拦截，导致无法访问。建议避免使用下列端口：

协议	不支持端口
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 4790 5554 5800 5900 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

7.1.4 弹性云服务器使用 NAT 网关和直接绑定弹性 IP 有区别吗?

公网NAT网关提供SNAT和DNAT功能，可允许多台弹性云服务器共享弹性IP。

弹性云服务器直接绑定弹性IP为独占IP的方式。

当同一个弹性云服务器同时设置了SNAT和弹性IP时，会优先使用弹性IP进行转发。

当同一个弹性云服务器同时设置了DNAT和弹性IP时，入云方向的弹性IP取决于客户端用户的自主选择（DNAT规则绑定的弹性IP或ECS直接绑定的弹性IP），而出云方向优先使用弹性云服务器直接绑定的弹性IP，所以如果入云和出云使用的弹性IP不一致，流量会不通。

不建议弹性云服务器同时使用公网NAT网关和直接绑定弹性IP。

7.1.5 通过 NAT 网关访问 Internet 失败该如何处理?

用户通过公网NAT网关访问Internet失败，可能是由于VPC路由表配置错误引起的，可以通过以下方法重新配置VPC路由表。

1. 找到VPC对应的子网关联的路由表。
2. 查看路由表是否有到NAT网关的路由，如果不包含，请添加对应的路由。
3. 如果用户自行修改到公网NAT网关的路由，请确保路由的目的地址包含待访问的目的地址。

7.1.6 NAT 网关是否支持更换 VPC?

不支持。

公网NAT网关在创建时选定VPC，不支持后续进行更换。

7.1.7 NAT 网关的配额是什么?

什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您创建的SNAT最多可关联多少条EIP。如果有需要，您可以申请扩大配额。

本节指导您如何查询指定区域下，NAT网关服务各资源的使用情况，以及总配额。

怎样查看我的配额?

1. 登录管理控制台。
2. 单击页面右上角的“My Quota”图标 。
   系统进入“服务配额”页面。
3. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
   如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额?

目前系统暂不支持在线调整配额大小。

如您需要调整配额，请联系运营管理员。

7.1.8 NAT 网关和 SNAT 规则是否支持更新操作?

公网NAT网关支持更新，SNAT规则不支持。

7.1.9 NAT 网关是否支持 IPV6?

目前公网NAT网关不支持IPV6协议。

7.1.10 基于 NAT 网关的用户网络，可以配置哪些安全策略实现访问限制?

基于NAT网关的用户网络，可以通过配置安全组和网络ACL实现访问限制。

- 安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当云服务器加入该安全组后，即受到这些访问规则的保护。
- 网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。

安全组对弹性云服务器进行防护，网络ACL对子网进行防护，两者结合起来，可以实现更精细、更复杂的安全访问控制。

安全组与网络ACL的详情，请参见章节。

7.1.11 公网 NAT 网关配置完成后，网络不通如何处理?

问题描述

您创建了一个公网NAT网关，并按照步骤配置了SNAT、DNAT规则，但是您的云主机不能访问互联网或不能为互联网提供服务。配置了公网NAT网关的网络是否可以连通互联网与路由表配置、安全组配置、网络ACL配置等多个环节相关联。任意一个环节出现问题，都会导致网络不通。本节操作介绍公网NAT网关配置完成后，网络不通时的排查思路。

排查思路

以下排查思路根据原因的出现概率进行排序，建议您从高频率原因往低频率原因排查，从而帮助您快速找到问题的原因。

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 7-1 网络不通排查思路

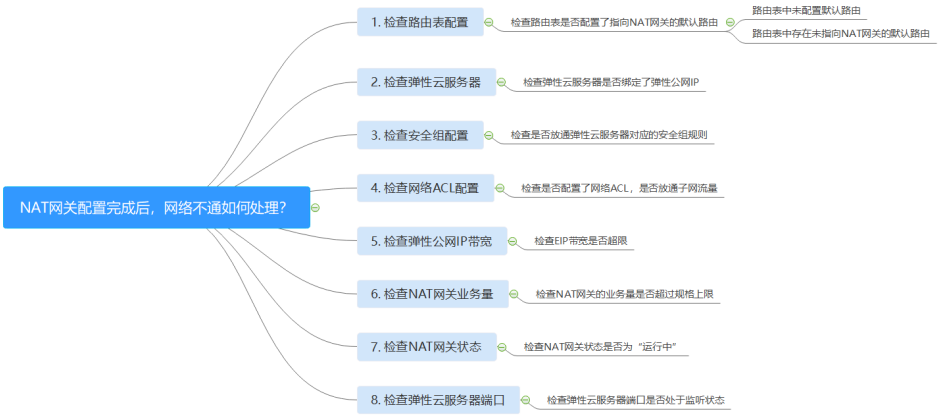


表 7-1 网络不通排查思路

可能原因	处理措施
路由表配置不正确	请在路由表中添加指向公网NAT网关的默认路由或路由，详细操作请参考**检查路由表是否配置指向公网NAT网关网关的默认路由**。
弹性云服务器绑定了弹性公网IP	请为弹性云服务器解绑弹性公网IP，详细操作请参考**检查弹性云服务器是否绑定了弹性公网IP**。
安全组规则未放通	请放通弹性云服务器对应的安全组规则，详细操作请参考**检查安全组规则**。
网络ACL配置不正确	请配置网络ACL规则放通子网流量，详细操作请参考**检查网络ACL是否放通子网流量**。
弹性IP的带宽超限	请扩大EIP带宽，详细操作请参考**检查弹性公网IP的带宽是否超限**。
公网NAT网关业务量超过规格上限	请提升公网NAT网关规格，详细操作请参考**检查公网NAT网关业务量是否超过规格上限**。
公网NAT网关的状态异常	请确保公网NAT网关资源状态为“运行中”，详细操作请参考**检查公网NAT网关状态是否异常**。
弹性云服务器端口未监听	请重新开启弹性云服务器端口，详细操作请参考**检查弹性云服务器端口**。

检查路由表是否配置指向公网 NAT 网关网关的默认路由

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航栏选择“路由表”。
5. 在路由表列表中，单击公网NAT网关所在VPC的路由表名称。
6. 检查路由列表中是否存在指向公网NAT网关的默认路由（0.0.0.0/0）。
   - 如果未存在默认路由，请在路由表中添加指向公网NAT网关的默认路由。
     i. 单击“添加路由”，按照提示配置参数。

表 7-2 参数说明

参数	参数说明
目的地址	目的地址网段。 配置为0.0.0.0/0。
下一跳类型	下一跳资源类型选择“NAT网关”。
下一跳	下一跳资源选择创建的公网NAT网关。

参数	参数说明
描述	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“>”。

ii. 单击“确定”，完成添加。

- 如果存在默认路由，但是未指向公网NAT网关，请在路由表中添加指向公网NAT网关的路由或者新增路由表并添加指向公网NAT网关的默认路由。

  - 路由表中添加指向公网NAT网关的路由详细步骤：

    1) 单击“添加路由”，按照提示配置参数。

    表 7-3 参数说明

参数	参数说明
目的地址	目的地址网段。
下一跳类型	下一跳资源类型选择“NAT网关”。
下一跳	下一跳资源选择创建的公网NAT网关。
描述	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“>”。

    2) 单击“确定”，完成添加。

  - 新增路由表并添加指向公网NAT网关的默认路由：

    1) 在路由表列表页面右上角，单击“创建路由表”，按照提示配置参数。

    表 7-4 参数说明

参数	说明	取值样例
路由表名称	路由表的名称，必填项。 路由表的名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。	rtb-001
所属VPC	选择路由表归属的VPC，必填项。	vpc-001
描述	路由表的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

参数	说明	取值样例
添加路由	路由规则信息。 路由规则可以在此处添加，单击“继续添加”。 添加目的地址为“0.0.0.0/0”，下一跳资源类型选择“NAT网关”，下一跳资源选择创建的公网NAT网关。	-

2) 单击“确定”，完成创建。
   系统出现信息提示页面，您可根据提示选择立即关联子网。
3) 单击“关联子网”，进入路由表详情页面的“关联子网”页签。
4) 单击“关联子网”，选择需要关联的子网。
5) 单击“确定”，完成关联。

检查弹性云服务器是否绑定了弹性 IP

当同一个弹性云服务器同时设置了SNAT和弹性IP时，会优先使用弹性IP进行转发。

当同一个弹性云服务器同时设置了DNAT和弹性IP时，入云方向的弹性IP取决于客户端用户的自主选择（DNAT规则绑定的弹性IP或ECS直接绑定的弹性IP），而出云方向优先使用弹性云服务器直接绑定的弹性IP，所以如果入云和出云使用的弹性IP不一致，流量会不通。

如果弹性云服务器绑定了弹性IP，请为弹性云服务器解绑弹性IP。

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表，查看“IP地址”列，检查弹性云服务器是否绑定了弹性IP。
   - 如果弹性云服务器未绑定弹性IP，请检查下一项。
   - 如果弹性云服务器绑定了弹性IP，请为弹性云服务器解绑弹性IP。
     为弹性云服务器解绑弹性IP详情请参见《虚拟私有云用户指南》中的“解绑定和释放弹性云服务器的弹性IP”章节。

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实例对应的安全组中添加放行该端口的规则。

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
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。
5. 选择“安全组”页签，展开安全组规则。
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，请检查下一项。
- 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。

  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。入方向和出方向规则参数详情请参见《虚拟私有云用户指南》中的“添加安全组规则”章节。

检查网络 ACL 是否放通子网流量

检查VPC的子网是否关联了网络ACL，如果关联了网络ACL，请检查“ 网络ACL”规则。

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航栏选择“子网”。
5. 查看NAT网关对应的子网是否关联了网络ACL。

   显示具体的网络ACL名称说明已关联网络ACL。
6. 单击网络ACL名称查看网络ACL的详细信息。
7. 检查入方向规则和出方向规则是否添加了放通子网流量的规则。

   如果未添加放通子网流量的规则，请添加入方向、出方向规则放通子网流量或者将网络ACL与子网取消关联。

   详情请参见《虚拟私有云用户指南》中的“添加网络ACL”章节和《虚拟私有云用户指南》中的“解除关联子网”章节。

   说明

   需要注意“网络ACL”的默认规则是丢弃所有出入方向的包，若关闭“网络ACL”后，其默认规则仍然生效。

检查弹性公网 IP 的带宽是否超限

公网NAT网关绑定了弹性IP时，通过带宽提供公网和公网NAT网关间的访问流量。

如果出现网络不通，请排查弹性IP带宽是否超过带宽最大上限。

检查公网 NAT 网关业务量是否超过规格上限

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 选择“管理与监管 > 云监控服务”。
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“查看监控指标”，查看公网NAT网关的监控指标详情。
6. 检查公网NAT网关SNAT连接数是否超过NAT网关规格上限。
   - 如果SNAT连接数未超过公网NAT网关规格上限，请检查下一项。
   - 如果SNAT连接数超过公网NAT网关规格上限，请提升公网NAT网关规格。

提升公网NAT网关规格请参见《NAT网关用户指南》中的“修改NAT网关”章节。

检查公网 NAT 网关状态是否异常

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 选择“网络 > NAT网关”。
4. 在公网NAT网关列表，检查公网NAT网关状态是否异常。
   - 如果公网NAT网关状态为“运行中”，请检查下一项。
   - 如果公网NAT网关状态不是“运行中”，主要有以下情况：
     - 因使用云平台资源违反了相关安全要求或法律法规，导致您的账号账号或资源被冻结。如果您在整改期限内完成整改并达到相关安全和法律要求，那么就可以解冻您的账号和资源；如果您在整改期限内未完成整改，那么将删除您的资源。

检查弹性云服务器端口

确保弹性云服务器端口正常工作，处于LISTEN状态。表7-5为常见TCP状态。

- Linux操作系统云服务器端口通信问题排查

  使用**netstat -antp**命令检查服务的状态，确认端口是否正常监听。

  例如：**netstat -ntulp |grep 80**

  图 7-2 查看端口监听状态_linux

  ```
  [root@elb-mq02 ~]# netstat -antpu | grep sshd
  tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      7178/sshd
  ```

  如果端口没有被正常监听，请重新开启弹性云服务器端口。

- Windows操作系统云服务器端口通信问题排查

  使用远程端口检测命令：

  a. 打开CMD命令行窗口。

  b. 执行**netstat -ano | findstr “*PID*”**命令查看进程使用的端口号。

  例如：**netstat -ano | findstr “80”**

  图 7-3 查看端口监听状态_windows

  ```
  C:\Users\Administrator>netstat -ano |findstr "80"
    TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
    TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       880
    TCP    [::]:80                [::]:0                 LISTENING       4
    TCP    [::]:49155             [::]:0                 LISTENING       880
    UDP    0.0.0.0:123            *:*                                    808
    UDP    [::]:123               *:*                                    808
  ```

  如果端口没有被正常监听，请重新开启弹性云服务器端口。

表 7-5 常见 TCP 状态

TCP状态	说明	对应场景
LISTEN	侦听来自远方的TCP端口的连接请求	正常TCP服务端
ESTABLISHED	代表一个打开的连接	正常TCP连接
TIME-WAIT	等待足够的时间以确保远程TCP接收到连接中断请求的确认	已关闭的TCP连接，一般1分钟后清除。
CLOSE-WAIT	等待从本地用户发来的连接中断请求	应用程序BUG，没有关闭socket。出现在网络中断后。一般是进程死循环或等待其他条件。可以重启对应进程。
FIN-WAIT-2	从远程TCP等待连接中断请求	网络中断过，需要12分钟左右自行恢复。
SYN-SENT	再发送连接请求后等待匹配的连接请求	TCP连接请求失败。一般是服务端CPU占用率过高，处理不及时导致。DDos攻击也会出现此情况。
FIN-WAIT-1	等待远程TCP连接中断请求，或先前的连接中断请求的确认	网络中断过，此状态可能不会自行修复（等15分钟以上确认），如果长期占用端口需要重启OS恢复。

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 > ”。

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 支持创建的 SNAT 和 DNAT 规则数能否增加?

可以，需要通过**提交工单**来解决。

7.2.4 私网 NAT 支持 SNAT 规则和 DNAT 规则共用一个中转 IP 吗?

私网NAT目前暂不支持SNAT规则和DNAT规则共用一个中转IP。

7.2.5 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。

7.2.6 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。

7.2.7 私网 NAT 是否支持跨使用?

私网NAT本身不支持跨使用，但可以通过实现跨账户通信，VPC对等连接打通两个的中转VPC，实现两个私网NAT转换IP后的跨通信。

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使用系统提供的服务，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）。

7.3.2 什么是 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。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状态的连接数和实际SNAT连接数有时会不一致。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。

7.3.3 主机通过 NAT 网关访问外网，请问 NAT 网关的带宽是多少?在哪里设置?

NAT网关的SNAT功能通过绑定弹性公网IP，实现云主机私有IP到公网IP的转换。云主机通过NAT网关访问外网时，其带宽大小和您申请弹性公网IP时选择的带宽大小有关。

带宽大小调整操作请参考。

7.3.4 NAT 网关丢包或连接不通该如何处理?

通过NAT网关上网的服务器出现丢包或连接不通的情况时，可以通过云监控查看NAT网关的SNAT连接数。若SNAT连接数超过NAT网关规格上限，则会导致使用NAT网关的服务器出现丢包或者连接不通的现象。如果超过NAT网关规格上限，可修改NAT网关规格，增大NAT网关规格数。

7.3.5 通过 NAT 网关访问远端服务器概率性失败该如何处理?

弹性云服务器通过SNAT访问公网上服务器，出现TCP建链失败的情况，可通过以下方法进行排查。

1. 执行以下命令，查看远端服务器是否开启了“tcp_tw_recycle”。

sysctl -a|grep tcp_tw_recycle

tcp_tw_recycle取值为1时，表示开启。

2. 执行以下命令，查看远端服务器内核丢包数量。

cat /proc/net/netstat | awk '/TcpExt/ { print $21,$22 }'

如果ListenDrops数值非0，表示存在丢包，即存在网络问题。

处理方法：

方法一：修改远端服务器的内核参数

- 临时修改参数方法（重启远端服务器后该设置失效），设置如下：

  sysctl -w net.ipv4.tcp_tw_recycle=0

- 永久修改参数方法：

  a. 执行以下命令，修改“/etc/sysctl.conf”文件。

  vi /etc/sysctl.conf

  在该文件中添加以下内容：

  net.ipv4.tcp_tw_recycle=0

  b. 按“**Esc**”输入“**:wq!**”，保存后退出文件。

  c. 执行以下命令，生效配置。

  sysctl -p

方法二：修改本地客户端的内核参数

- 临时修改参数方法（重启本地客户端后该设置失效），设置如下：

  sysctl -w net.ipv4.tcp_timestamps=0

- 永久修改参数方法：

  a. 执行以下命令，修改“/etc/sysctl.conf”文件。

  vi /etc/sysctl.conf

  在该文件中添加以下内容：

  net.ipv4.tcp_timestamps=0

  b. 按“**Esc**”输入“**:wq!**”，保存后退出文件。

  c. 执行以下命令，生效配置。

  sysctl -p

7.3.6 NAT 网关里的网段设置与 SNAT 规则里的网段有什么关联与区别?

NAT网关里的网段是在创建NAT网关时必须指定NAT网关所在VPC及子网网段。此网段仅用于系统后台使用，并非SNAT使用的网段。

创建SNAT规则且当场景是虚拟私有云时，需要配置对应VPC的子网网段，使该网段中的云主机通过SNAT方式进行访问。

创建SNAT规则且当场景是云专线时，需要配置云专线对应的本地数据中心的某个网段或另一VPC的网段，使该网段中的云主机通过SNAT方式进行访问。

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IP，为互联网提供服务。详见**添加DNAT规则**。

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网关支持修改DNAT规则。

A 修订记录

发布日期	修订记录
2020-01-02	第二次发布。 • 新增DNAT功能。 • 快速入门新增章节**使用DNAT为云主机面向公网提供服务**和**云间NAT网关高速访问互联网**。
2018-08-15	第一次发布。