NAT 网关

产品介绍

文档版本 01

发布日期 2025-10-30

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。

目 录

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。

视频介绍

本视频介绍什么是NAT网关服务。

公网 NAT 网关

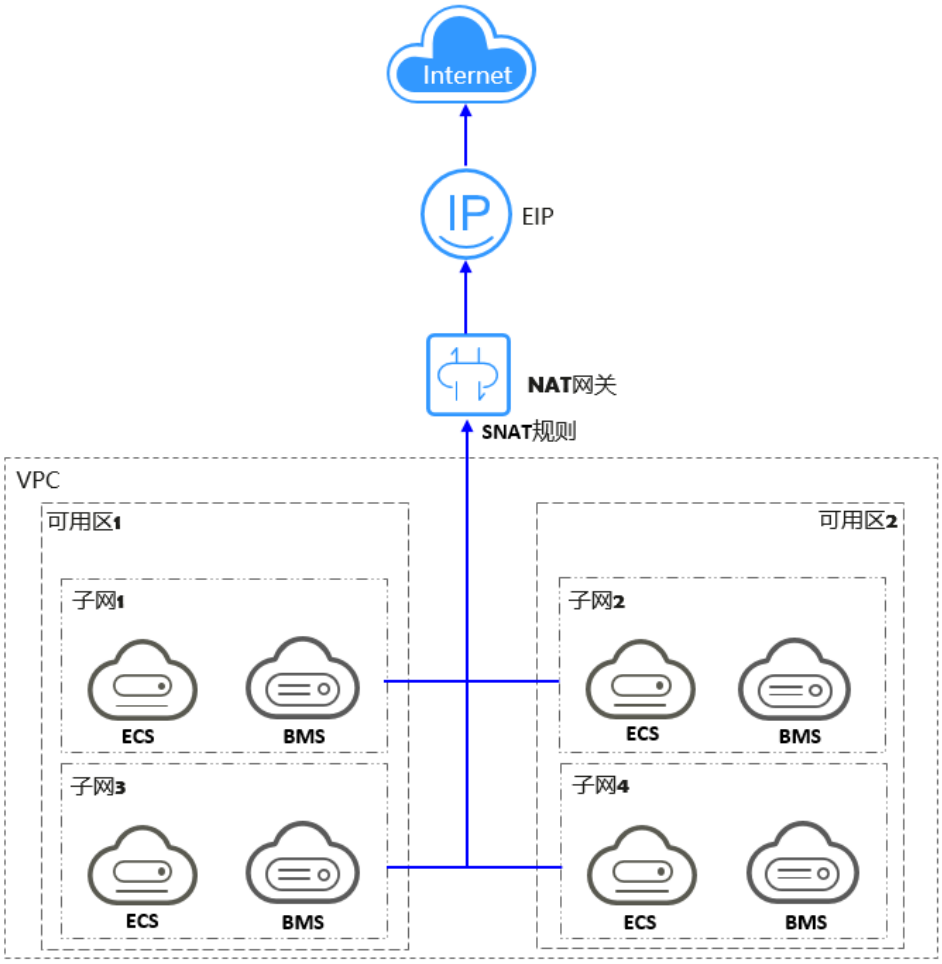
公网NAT网关（Public NAT Gateway）能够为虚拟私有云内的云主机（弹性云服务器、裸金属服务器）或者通过云专线/VPN接入虚拟私有云的本地数据中心的服务器，提供最高20Gbit/s能力的网络地址转换服务，使多个云主机可以共享弹性公网IP访问Internet或使云主机提供互联网服务。

公网NAT网关分为SNAT和DNAT两个功能。

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

  SNAT架构如图1-1所示。

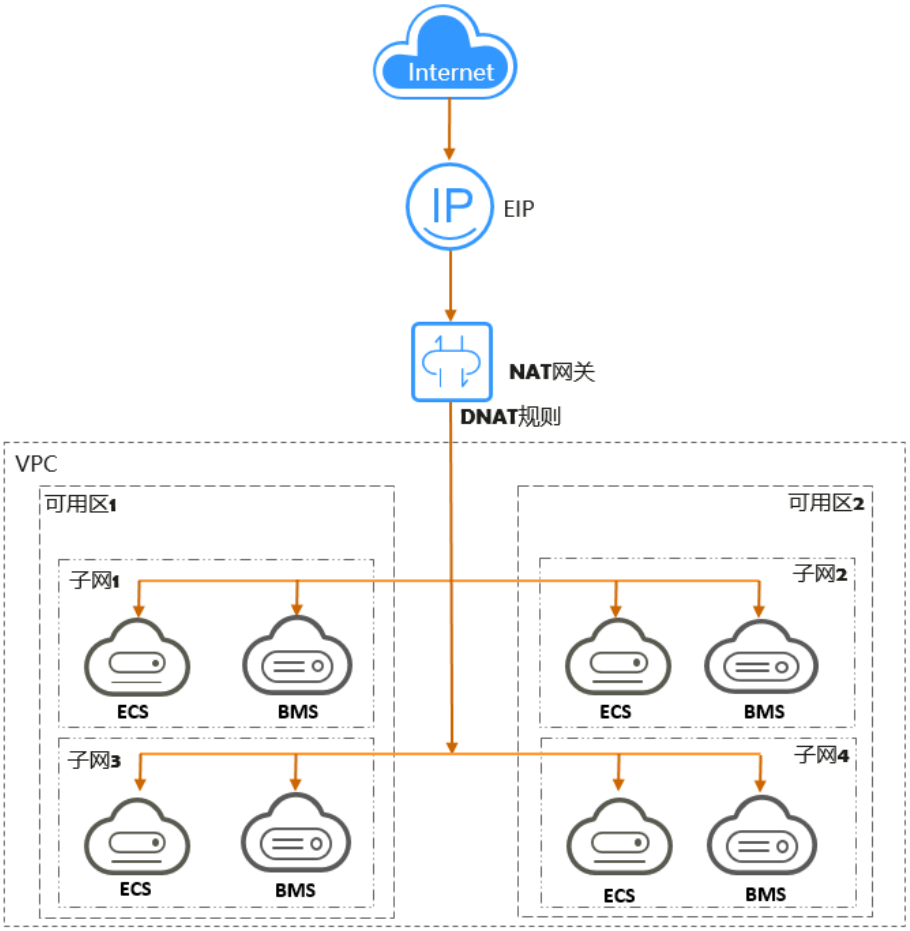
图 1-1 SNAT 架构图



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

  DNAT架构如图1-2所示。

图 1-2 DNAT 架构图



私网 NAT 网关

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

私网NAT网关分为SNAT和DNAT两个功能：

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

中转子网

中转子网相当于一个中转网络，是中转IP所属的子网。

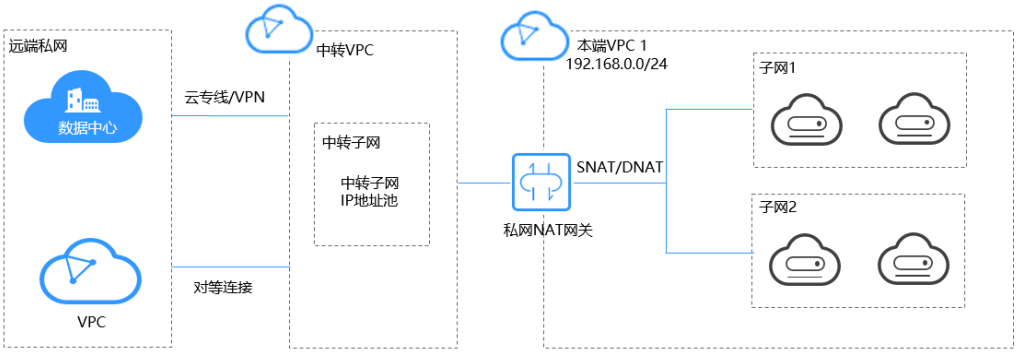
中转IP

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

中转VPC

中转子网所在VPC。

图 1-3 私网 NAT 网关



如何访问 NAT 网关

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

- 管理控制台方式

  管理控制台是网页形式的，您可以使用直观的界面进行相应的操作。登录管理控制台，从主页选择“NAT网关”。

- API方式

  如果您需要将云平台上的NAT网关集成到您自己的系统，请使用API方式访问NAT网关。具体操作请参见**《NAT网关API参考》**。

NAT 网关快速入门

- **通过公网NAT网关的SNAT规则访问公网**
- **通过公网NAT网关的DNAT规则访问公网**
- **通过私网NAT网关实现云上云下互通**

2 产品优势

公网 NAT 网关优势

- **灵活部署**

  支持跨子网部署和跨可用区域部署。公网NAT网关支持跨可用区部署，可用性高，单个可用区的任何故障都不会影响公网NAT网关的业务连续性。公网NAT网关的规格、弹性公网IP，均可以随时调整。

- **多样易用**

  多种网关规格可灵活选择。对公网NAT网关进行简单配置后，即可使用，运维简单，快速发放，即开即用，运行稳定可靠。

- **降低成本**

  多个云主机共享使用弹性公网IP。当您的私有IP地址通过公网NAT网关发送数据，或您的应用面向互联网提供服务时，公网NAT网关服务将私有地址和公网地址进行转换。用户无需为云主机访问Internet购买多余的弹性公网IP和带宽资源，多个云主机共享使用弹性公网IP，有效降低成本。

私网 NAT 网关优势

- **简规划**

  大企业不同部门间存在大量重叠网段，上云后无法互通，需要在上云前进行企业网络的重新规划。华为云首创的私网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。

3 应用场景

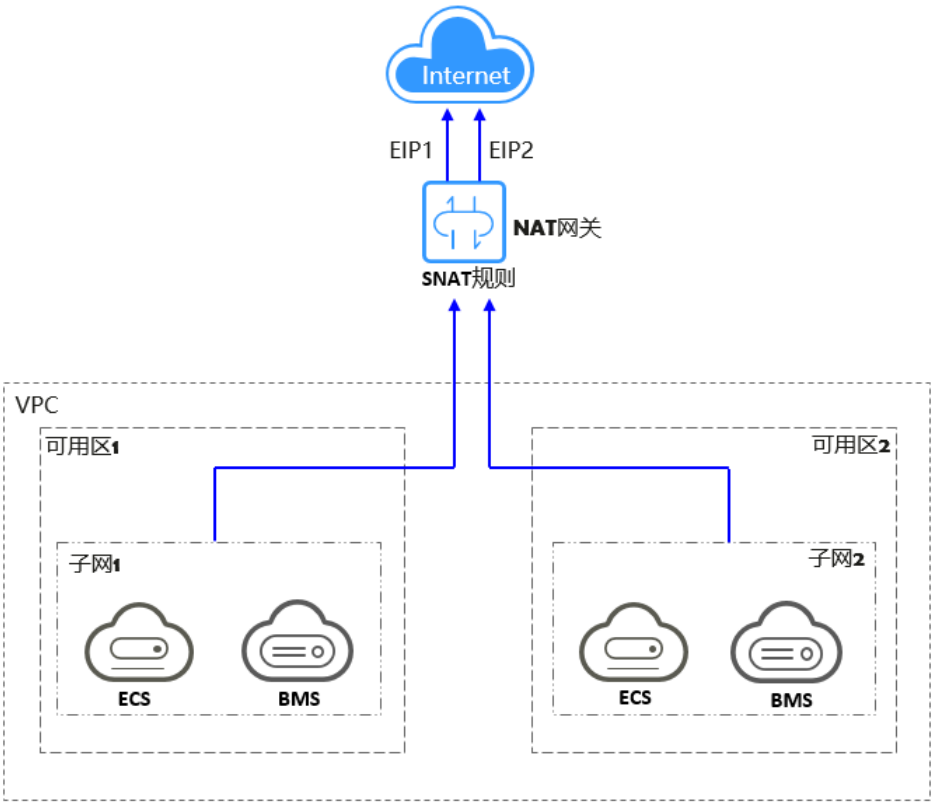
公网 NAT 网关

- **使用SNAT访问公网**

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

  使用SNAT访问公网场景组网图如图3-1所示。

  图 3-1 使用 SNAT 访问公网



- **使用DNAT为云主机面向公网提供服务**

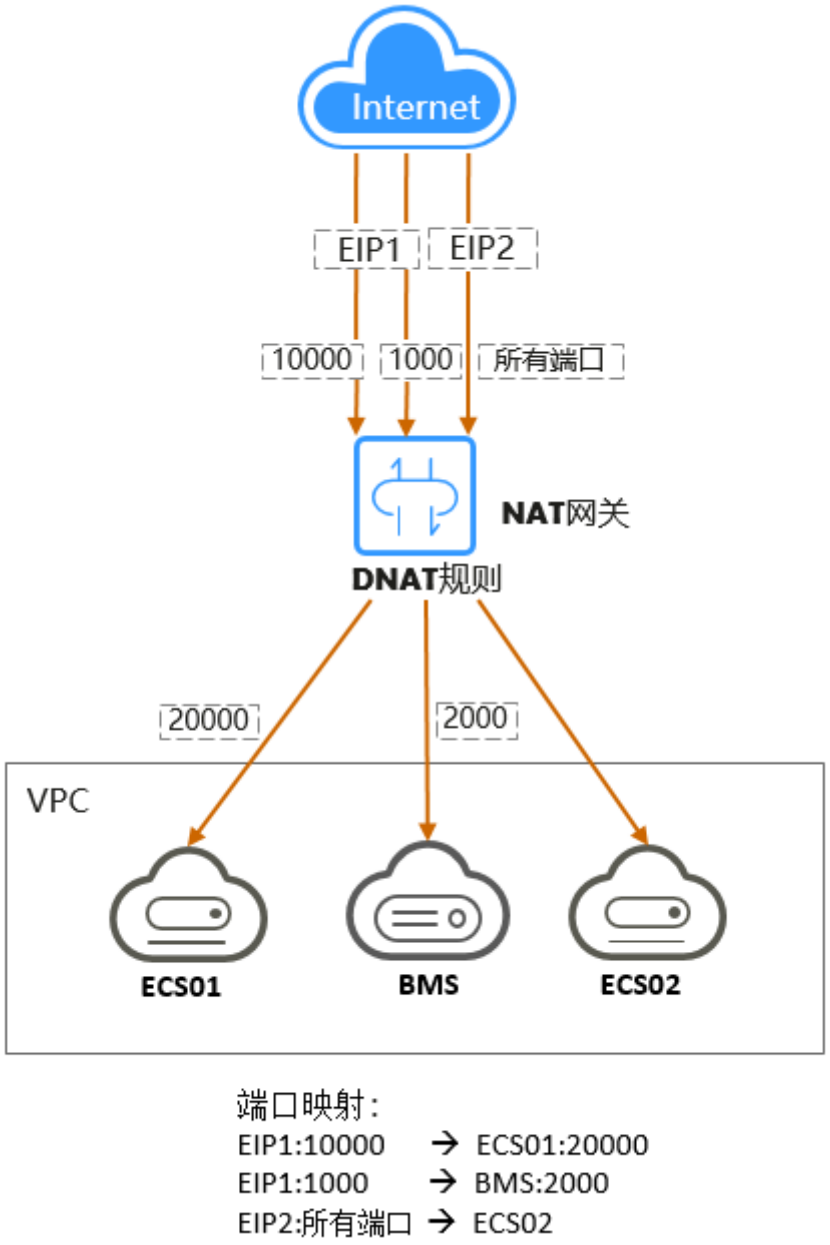
  当VPC内的云主机需要面向公网提供服务时，可以使用公网NAT网关的DNAT功能。

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

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

  使用DNAT为公网提供服务场景组网图如**图3-2**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 3-2 使用 DNAT 为云主机面向公网提供服务

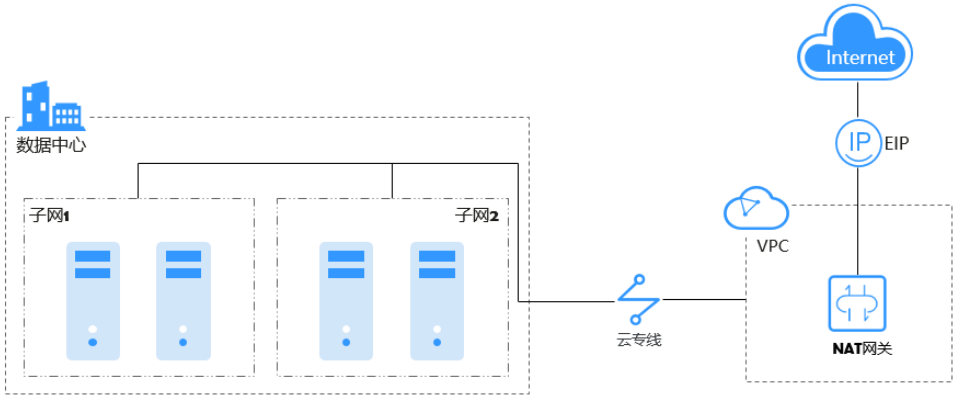


- **使用SNAT或DNAT高速访问互联网**

  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3-3所示。

图 3-3 使用 SNAT 或 DNAT 高速访问互联网



- **搭建高可用的SNAT**

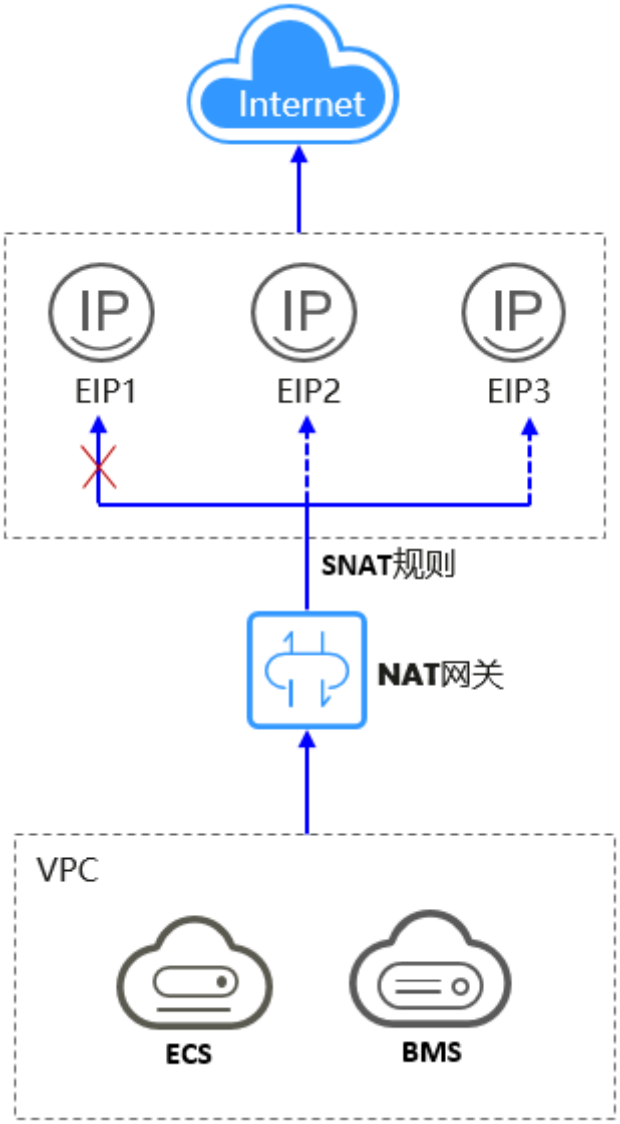
  在IT系统中，往往存在绑定的弹性公网IP被攻击封堵的可能性。如果您想提高系统的高可靠性，可以在配置SNAT规则时，添加多个弹性公网IP，当其中一个弹性公网IP被攻击封堵时，可以最大程度保障使用其他弹性公网IP的业务正常运行。

  当SNAT规则上绑定了多个EIP时，系统会随机选择一个弹性公网IP访问公网。

  每条SNAT规则支持添加20个弹性公网IP，当SNAT规则中添加的弹性公网IP被攻击封堵或不可用时，需要手动从EIP池中删除。

  使用公网NAT网关的SNAT规则搭建高可用场景组网图如**图3-4**所示。

图 3-4 使用公网 NAT 网关的 SNAT 规则搭建高可用场景



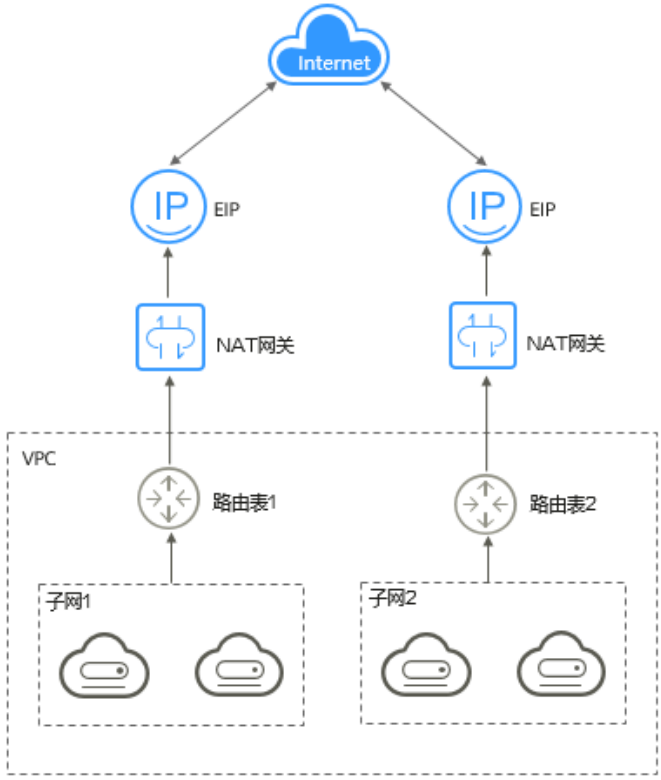
- **NAT网关多实例**

  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。

  如果您想实现多网关扩容，只需将关联了VPC子网的路由表与公网NAT网关实例进行关联。

  公网NAT网关多实例场景图如图3-5所示。

图 3-5 公网 NAT 网关多实例



说明

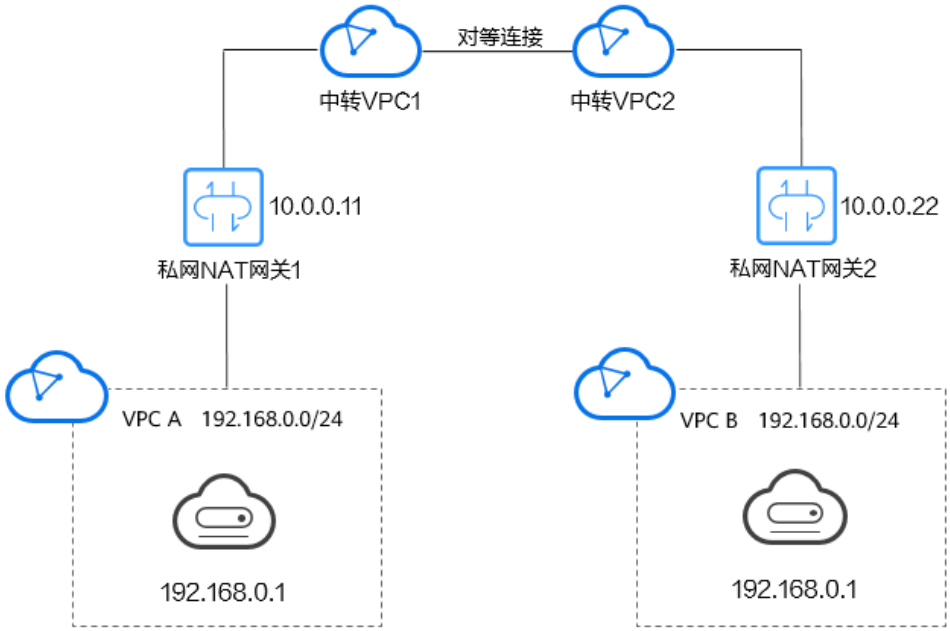
- 对于新建公网NAT网关实例，系统不会在后台下发默认路由，需要您在对应路由表中添加公网NAT网关的路由。
- 每个公网NAT网关对应一张路由表，公网NAT网关数量取决于VPC下路由表的数量限制。

私网 NAT 网关

- **重叠网段VPC间互通**

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

图 3-6 重叠网段 VPC 间互通

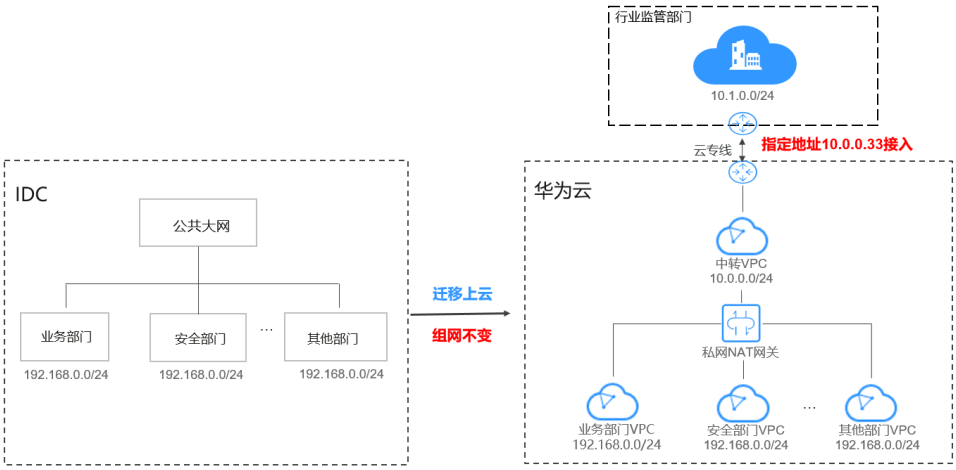


- **企业网络上云及指定IP接入**

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

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

图 3-7 企业网络上云及指定 IP 接入



4 产品规格

NAT网关的规格指公网NAT网关与私网NAT网关支持的SNAT最大连接数。

公网 NAT 网关

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

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

每个公网NAT网关支持的最大转发带宽为20Gbit/s。

说明

上海二、北京一区域每个公网NAT网关支持的最大转发带宽为5Gbit/s。

公网NAT网关TCP SNAT的默认连接超时时间为900秒。

公网NAT网关UDP SNAT的默认连接超时时间为300秒。

在购买公网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4-1所示。

表 4-1 公网 NAT 网关规格

规格	SNAT最大连接数	带宽	每秒报文数（PPS）	每秒新建报文数（QPS）
小型	10000	20Gbit/s	2000000	10000
中型	50000	20Gbit/s	2000000	10000
大型	200000	20Gbit/s	2000000	10000
超大型	1000000	20Gbit/s	2000000	10000

说明

- 表格中所列的“每秒报文数（PPS）”是指入方向和出方向的PPS总和。
- 为避免因连接数超过公网NAT网关规格最大值，从而影响业务的情况，建议在云监控中设置公网NAT网关监控指标，并为SNAT连接数合理设置告警。
- 公网NAT网关支持的DNAT规则数与规格无关，每种规格的公网NAT网关最多支持添加200条DNAT规则。仅超大型规格支持提升DNAT规则数，您可以**提交工单**申请。

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。

在购买私网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4-2**所示。

表 4-2 私网 NAT 网关规格

规格	SNAT最大连接数	带宽	每秒报文数（PPS）	每秒新建报文数（QPS）	NAT规则数（SNAT+DNAT）
小型	2000	200Mbps	20000	6000	20
中型	5000	500Mbps	50000	9000	50
大型	20000	2Gbps	200000	10000	200
超大型	50000	5Gbps	500000	10000	500

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。

5 约束与限制

公网 NAT 网关

关于公网NAT网关的使用，您需要注意以下几点：

- 公共限制
  - 同一个公网NAT网关下的多条规则可以复用同一个弹性公网IP，不同网关下的规则必须使用不同的弹性公网IP。
  - 一个VPC支持关联多个公网NAT网关。
  - SNAT、DNAT可以共用同一个弹性公网IP，节省弹性公网IP资源。但是在选用全端口模式下，DNAT优先占用全部端口，这些端口不能被 SNAT 使用。因此SNAT规则不能和全端口的DNAT规则共用EIP，以免出现业务相互抢占问题。
  - 公网NAT网关支持转换的资源类型不包括企业型VPN。
  - 当云主机同时配置弹性公网IP服务和公网NAT网关服务时，数据均通过弹性公网IP转发。
  - 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，对于云专线的配置，必须是云专线侧网段，且不能与虚拟私有云侧的网段冲突。
  - 公网NAT网关支持添加的SNAT规则的数量没有限制。

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

私网 NAT 网关

关于私网NAT网关的使用，您需要注意以下几点：

- 公共限制
  - 用户需要在VPC下手动添加私网路由，即通过创建对等连接或开通云专线/VPN连接远端私网。
  - 中转IP和目的IP不能在同一个VPC中。
  - 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。

6 与其他服务的关系

NAT网关与其他服务关系如图1所示。

图 6-1 NAT 网关与其他服务关系

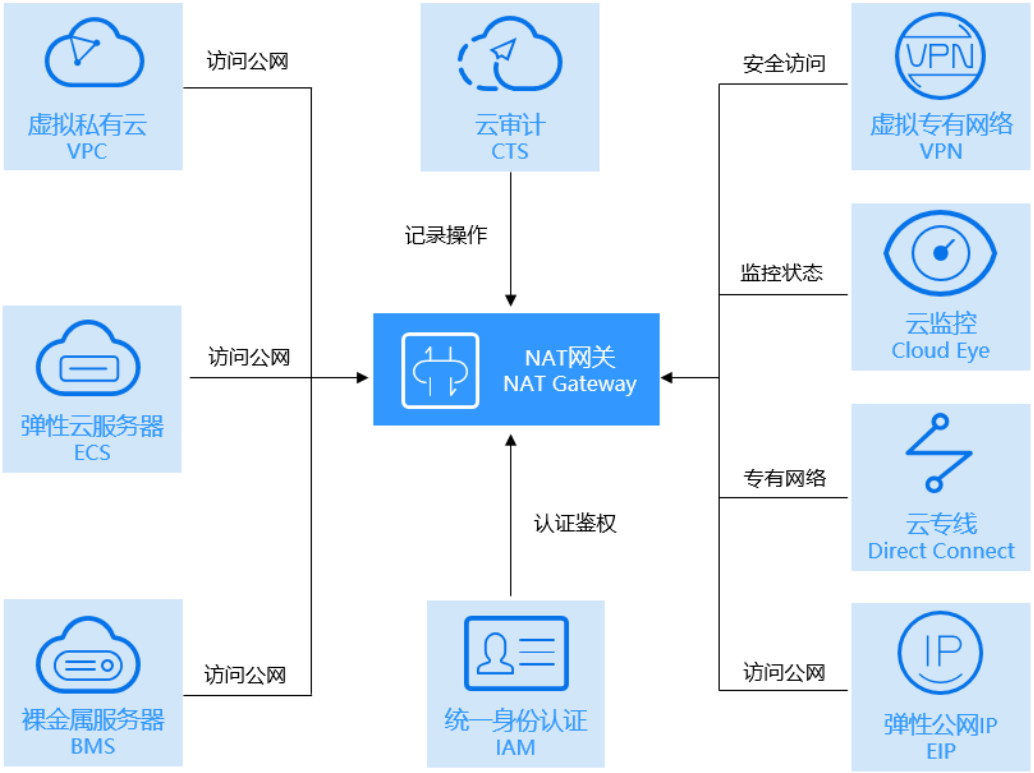


表 6-1 与其他服务的关系

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。	基于公网NAT网关和云专线的混合云Internet加速

相关服务	交互功能	位置
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。	基于云连接和SNAT实现跨区域内网访问公网服务器加速
弹性云服务器（Elastic Cloud Server，ECS）	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。	通过公网NAT网关的SNAT规则访问公网 通过公网NAT网关的DNAT规则面向公网提供服务
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	通过公网NAT网关的SNAT规则访问公网
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。	通过公网NAT网关的SNAT规则访问公网 通过公网NAT网关的DNAT规则面向公网提供服务
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
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

7 安全

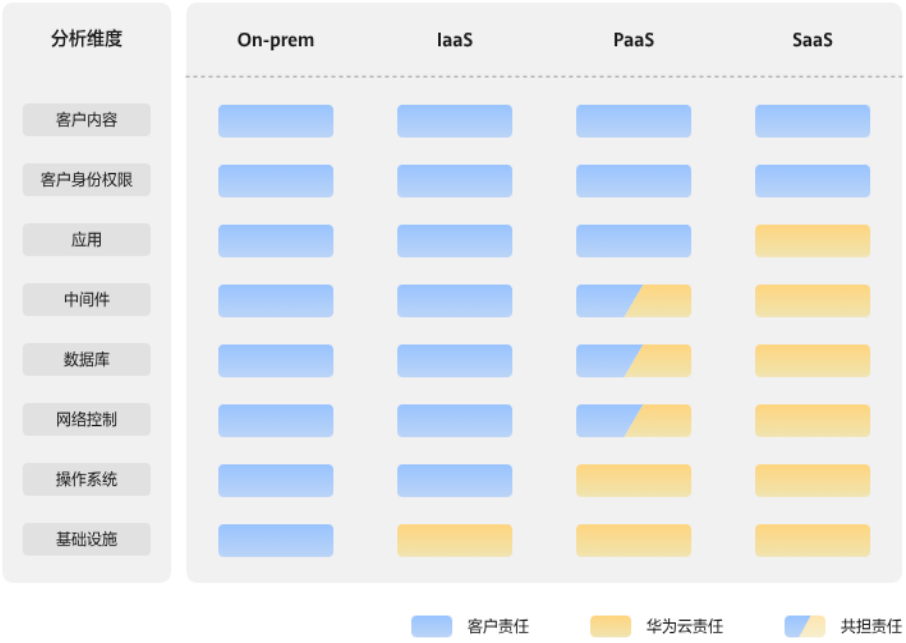
7.1 责任共担

华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如图7-1所示。

- **华为云**：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户**：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

图 7-1 华为云安全责任共担模型



云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图7-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS服务）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

7.2 身份认证与访问控制

NAT网关服务支持通过IAM权限策略进行访问控制。IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。管理员创建IAM用户后，需要将用户加入到一个用户组中，IAM可以对这个组授予NAT网关服务所需的权限，组内用户自动继承用户组的所有权限。

详情请参见**权限管理**。

7.3 审计与日志

云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务后，CTS可记录NAT网关的操作事件用于审计。

- CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。
- NAT网关支持审计的操作事件请参见**支持审计的关键操作**。
- 查看审计日志请参见**查看审计日志**。

7.4 监控安全风险

云监控（Cloud Eye）服务是面向华为云资源的监控平台，提供了实时监控、及时告警、资源分组、站点监控等能力，使您全面了解云上资源的使用情况和业务的运行状况。

监控是保持NAT网关服务可靠性、可用性和性能的重要部分。通过云监控服务，可以按时间轴查看连接数、PPS、流入/流出流量等指标。通过创建告警规则，设置监控阈值并配置通知，让您在第一时间得知NAT网关服务资源发生异常，迅速处理故障，避免因资源问题造成业务损失。

关于NAT网关服务支持的监控指标，以及如何创建监控告警规则等内容，请参见**监控**。

7.5 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 7-2 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 7-3 资源中心

合规资质证书

华为云安全服务提供了网络安全专用产品安全检测证书、软件著作权等证书，供用户下载和参考。具体请查看**合规资质证书**。

图 7-4 网络安全专用产品安全检测证书&软件著作权证书

8 权限管理

如果您需要对华为云上购买的NAT网关（NAT Gateway）资源，为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华为云资源的访问。如果华为云账号已经能满足您的要求，不需要通过IAM对用户进行权限管理，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是华为云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。

通过IAM，您可以通过授权控制他们对华为云资源的访问范围。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（NAT Gateway）的使用权限，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进行权限分配，通过授予用户仅能使用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。

目前IAM支持两类授权，一类是角色与策略授权，另一类为身份策略授权。

两者有如下的区别和关系：

表 8-1 角色授权与策略授权的区别

名称	核心关系	涉及的权限	授权方式	适用场景
角色与策略授权	用户-权限-授权范围	• 系统角色 • 系统策略 • 自定义策略	为主体授予角色或策略	核心关系为“用户-权限-授权范围”，每个用户根据所需权限和所需授权范围进行授权，无法直接给用户授权，需要维护更多的用户组，且支持的条件键较少，难以满足细粒度精确权限控制需求，更适用于对细粒度权限管控要求较低的中小企业用户。

名称	核心关系	涉及的权限	授权方式	适用场景
身份策略授权	用户-策略	• 系统身份策略 • 自定义身份策略	• 为主体授予身份策略 • 身份策略附加至主体	核心关系为“用户-策略”，管理员可根据业务需求定制不同的访问控制策略，能够做到更细粒度更灵活的权限控制，新增资源时，对比角色与策略授权，基于身份策略的授权模型可以更快速地直接给用户授权，灵活性更强，更方便，但相对应的，整体权限管控模型构建更加复杂，对相关人员专业能力要求更高，因此更适用于中大型企业。

例如：如果需要对IAM用户授予可以创建华北-北京四区域的ECS和华南-广州区域的OBS的权限，基于角色与策略授权的场景中，管理员需要创建两个自定义策略，并且为IAM用户同时授予这两个自定义策略才可以实现权限控制。在基于身份策略授权的场景中，管理员仅需要创建一个自定义身份策略，在策略中通过条件键“g:RequestedRegion”的配置即可达到策略对于授权区域的控制。将策略附加主体或为主体授予该策略即可获得相应权限，权限配置方式更细粒度更灵活。

两种授权场景下的策略/身份策略、授权项等并不互通，推荐使用身份策略进行授权。**角色与策略权限管理**和**身份策略权限管理**分别介绍两种模型的系统权限。

关于IAM的详细介绍，请参见**IAM产品介绍**。

角色与策略权限管理

NAT网关服务支持角色与策略授权。默认情况下，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，“授权范围”需要选择“指定区域项目资源”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果“授权范围”选择“所有资源”，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。

如**表2**所示，包括了NAT网关的所有系统权限。角色与策略授权场景的系统策略和身份策略授权场景的并不互通。

表 8-2 NAT 网关系统权限

系统角色/策略名称	描述	类型	依赖关系
NAT FullAccess	对NAT网关全部资源的所有执行权限。	系统策略	无

系统角色/策略名称	描述	类型	依赖关系
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	无
NAT Gateway 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	依赖Tenant Guest和Tenant Administrator角色，在同项目中勾选依赖的角色。

表8-3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 8-3 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	√
批量删除DNAT规则	√	x	√
DNAT规则模板导入	√	x	√

操作	NAT FullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
DNAT规则模板导出	√	√	√
创建中转子网	√	x	√
查询中转子网列表	√	√	√
查询中转子网详情	√	√	√
修改中转子网	√	x	√
删除中转子网	√	x	√
创建中转IP	√	x	√
查询中转IP	√	√	√
删除中转IP	√	x	√

身份策略权限管理

NAT网关服务支持身份策略授权。如表4所示，包括了NAT网关基于策略授权中的所有系统身份策略。身份策略授权场景的系统身份策略和角色与策略授权场景的并不互通。

表 8-4 NAT 网关系统身份策略

系统身份策略名称	描述	策略类别
NATFullAccessPolicy	对NAT网关全部资源的所有执行权限。	系统身份策略
NATReadOnlyPolicy	NAT网关只读权限，对NAT网关全部资源的只读权限。	系统身份策略

表8-5列出了NAT Gateway常用操作与系统身份策略的授权关系，您可以参照该表选择合适的系统策略。

表 8-5 常用操作与系统身份策略的关系

操作	NATFullAccessPolicy	NATReadOnlyPolicy
创建NAT网关	√	x
查询NAT网关列表	√	√
查询NAT网关详情	√	√

操作	NATFullAccessPolicy	NATReadOnlyPolicy
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
批量删除DNAT规则	√	x
DNAT规则模板导入	√	x
DNAT规则模板导出	√	√
创建中转子网	√	x
查询中转子网列表	√	√
查询中转子网详情	√	√
修改中转子网	√	x
删除中转子网	√	x
创建中转IP	√	x
查询中转IP	√	√
删除中转IP	√	x

NAT 控制台功能依赖的角色或策略

表 8-6 NAT 控制台依赖服务的角色或策略

控制台功能	依赖服务	需配置角色/策略
公网NAT网关控制台添加SNAT规则	弹性公网IP EIP	IAM用户设置了NATFullAccessPolicy权限后，需要增加EIP ReadOnlyAccess权限后，在为公网NAT网关添加SNAT规则时，才可以访问全域弹性公网IP资源列表。

控制台功能	依赖服务	需配置角色/策略
公网NAT网关控制台修改SNAT规则	弹性公网IP EIP	IAM用户设置了NATFullAccessPolicy权限后，需要增加EIP ReadOnlyAccess权限后，在修改公网NAT网关的SNAT规则时，才可以访问全域弹性公网IP资源列表。
公网NAT网关控制台添加DNAT规则	弹性公网IP EIP	IAM用户设置了NATFullAccessPolicy权限后，需要增加EIP ReadOnlyAccess权限后，在为公网NAT网关添加DNAT规则时，才可以访问全域弹性公网IP资源列表。
公网NAT网关控制台修改DNAT规则	弹性公网IP EIP	IAM用户设置了NATFullAccessPolicy权限后，需要增加EIP ReadOnlyAccess权限后，在修改公网NAT网关的DNAT规则时，才可以访问全域弹性公网IP资源列表。
公网NAT网关控制台删除公网NAT网关	弹性公网IP EIP	IAM用户设置了NATFullAccessPolicy权限后，需要增加EIP ReadOnlyAccess权限后，在删除公网NAT网关时，才可以查询到公网NAT网关绑定的全域弹性公网IP。
公网NAT网关控制台解绑全域弹性公网IP	弹性公网IP EIP	IAM用户设置了NATFullAccessPolicy权限后，需要增加EIP FullAccess权限后，在删除公网NAT网关的SNAT规则或DNAT规则时，才可以查询并解绑全域弹性公网IP。

相关链接

- **IAM产品介绍**
- **通过IAM进行授权**
- 身份策略授权参考，请参见《 NAT网关API参考 》中的**策略及授权项说明**

9 区域和可用区

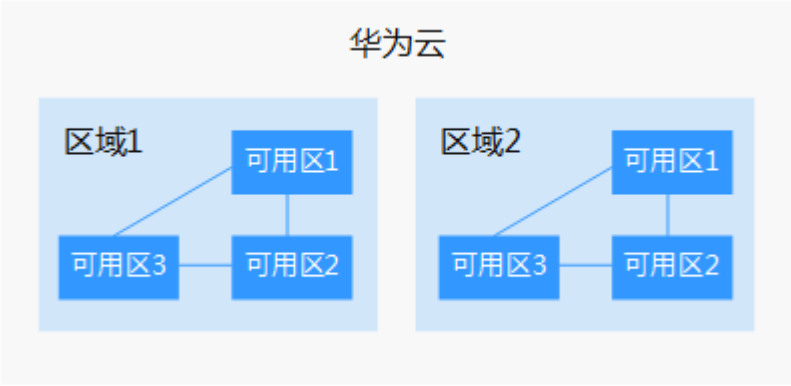
什么是区域、可用区?

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）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图9-1阐明了区域和可用区之间的关系。

图 9-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。更多信息请参见华为云全球站点。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，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。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

    说明

    “拉美-圣地亚哥”区域位于智利。

- 资源的价格

  不同区域的资源价格可能有差异，请参见华为云服务价格详情。

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。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

10 基本概念

弹性公网 IP

弹性公网IP是基于互联网上的静态IP地址。

弹性公网IP地址为可以直接访问Internet的IP地址。私有IP地址为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。

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

一个弹性公网IP只能直接给一个弹性云服务器使用。如要实现VPC内跨可用区的多个云主机共享弹性公网IP，可选择公网NAT网关。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IP地址和它的端口。连接能够区分不同会话，并且对应的会话是唯一的。

DNAT 连接

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