



公网 NAT 网关

用户使用指南

天翼云科技有限公司

目录

1	产品简介	3
1.1	产品定义	3
1.2	产品优势	3
1.3	功能特性	4
1.4	产品应用场景	5
1.5	产品规格和使用限制	5
2	快速入门	6
2.1	创建公网 NAT 网关	6
2.2	创建 SNAT 规则	7
2.3	创建 DNAT 规则	8
3	用户指南	10
3.1	修改公网 NAT 网关	10
3.2	修改 SNAT 规则	10
3.3	修改 DNAT 规则	11
3.4	删除公网 NAT 网关	12
3.5	删除 SNAT 规则	13
3.6	删除 DNAT 规则	13
4	常见问题	14

1 产品简介

1.1 产品定义

NAT 网关（NAT Gateway）是一种支持 IP 地址转换的网络云服务，能够为虚拟私有云（Virtual Private Cloud，VPC）内的计算实例提供网络地址转换（Network Address Translation），分为 SNAT 和 DNAT 两个功能。通过 SNAT 可使多个弹性云主机共享使用弹性 IP 访问 Internet。通过 DNAT 可使多个弹性云主机提供互联网服务。NAT 网关是 VPC 内的一个公网流量的出入口，保护私有网络信息不直接对公网暴露。

相关概念：

公网 IP 地址

即互联网协议地址，是互联网上可以被路由的地址。云上资源如果要对外提供服务，需要对外发布云上资源对应的公网 IP 信息。

NAT（网络地址转换）

VPC 内的云上资源分配的是私网 IP，在互联网上私网 IP 不可被路由。如果 VPC 内的云上资源要与互联网互通或对互联网提供服务，则需要将云上资源的私网 IP 转换成可被路由的公网 IP，并对外进行发布。

DNAT（目的地址转换）

定义：通过 IP 映射或端口映射，将 IP 报文中的目的地址进行转换。

将 NAT 网关绑定弹性 IP、使能 DNAT，则可以实现 VPC 内多个云主机资源共享弹性 IP 对外提供服务。

SNAT（源地址转换）

定义：将 IP 报文的源地址、源端口进行转换。

将 NAT 网关绑定弹性 IP、使能 SNAT，将云主机的私网 IP 转换成公网 IP，可以使 VPC 内没有公网 IP 的资源可以直接访问公网，实现 VPC 内多个云主机资源共享弹性 IP 主动访问 Internet。

1.2 产品优势

灵活部署

支持跨子网部署和跨 AZ 部署。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 NAT 网关的业务连续性。NAT 网关的规格、带宽和公网 IP，均可以按需配置。

简单易用

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

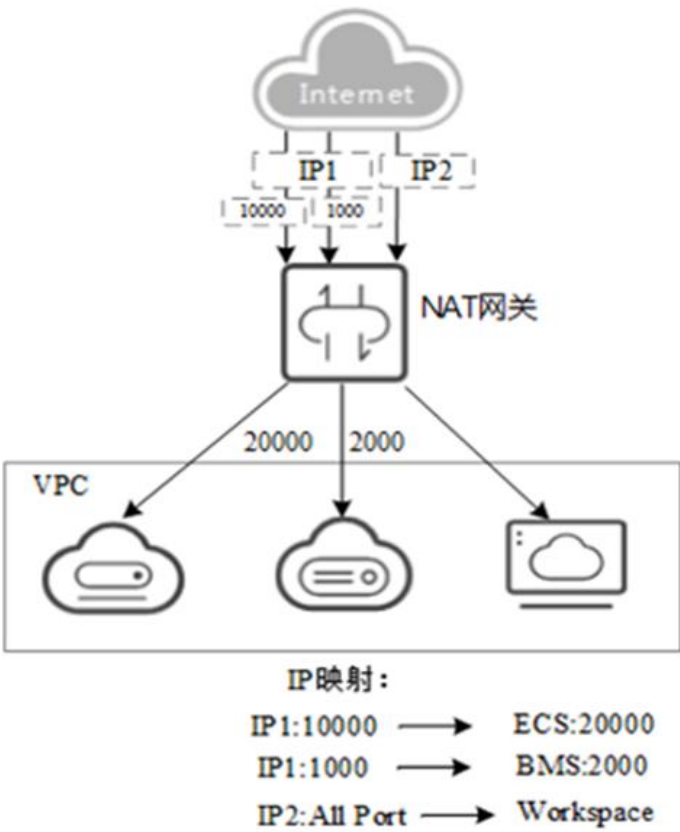
降低成本

多个计算实例共享使用弹性 IP。当您的私有 IP 地址通过 NAT 网关发送流量时，该软件将私有地址转换为公共地址。用户无需为计算实例访问 Internet 购买多余的弹性 IP 和带宽资源，多个计算实例共享使用弹性 IP，有效降低成本。

1.3 功能特性

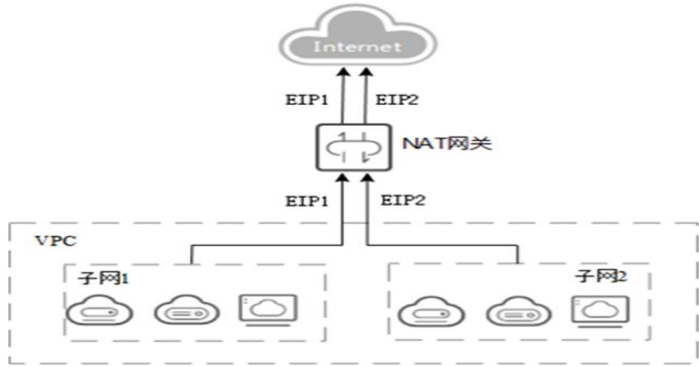
面向 Internet 提供服务

当 VPC 内的云主机需要面向公网提供服务时，可以使用 NAT 网关的 DNAT 功能。DNAT 功能绑定弹性 IP，可通过端口映射方式，NAT 网关会将以指定的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。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 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下图所示。图中示例的云主机类型均可以替换为弹性云主机、物理机的任何一个。



使用 SNAT 主动访问 Internet

当 VPC 内的云主机需要主动访问 Internet，可以使用弹性 IP 绑定云主机实现。但是如果 VPC 内需要主动访问 Internet 的云主机过多时，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，可以使用 NAT 网关的 SNAT 功能。VPC 中一个子网对应一条 SNAT 规则，一条 SNAT 规则配置一个弹性 IP。NAT 网关为您提供不同规格的连接数，根据业务规划，NAT 网关为您提供不同规格的连接数。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下图所示。



高性能

NAT 网关基于 DPDK 优化转发面性能，绕过协议栈直接从网卡驱动获取数据报文，直接将数据报文发送给用户态应用程序，不触发后续中断流程，减少了中断和内存拷贝的消耗，从而提升数据报文处理速度。

高可用

NAT 网关主备集群模式，单网元故障集群内状态同步，秒级故障收敛, 具备高可用性。单个可用区的任何故障都不会影响 NAT 网关的业务连续性。

1.4 产品应用场景

云上网络入口，面向 Internet 提供服务

使用 NAT 网关的 DNAT 端口级转换功能，使云上资源可轻松面向 Internet 提供服务，同时节省大量弹性公网 IP，保护云上私网网络结构。

构建 VPC 云上网络出口

使用 NAT 网关的 SNAT 功能，构建 VPC 主动访问公网出口，使 VPC 内没有弹性 IP 的资源可以直接访问公网，实现云内主机共享使用弹性 IP 访问 Internet。

1.5 产品规格和使用限制

产品规格		
产品规格		
小型	SNAT 最大连接数	6 万
	单个 NAT 网关实例 SNAT 规则数量	1000

	单个 NAT 网关实例 DNAT 规则数量	1000
--	-----------------------	------

使用限制

单个 NAT 网关实例支持绑定的 EIP 上限为 32。

2 快速入门

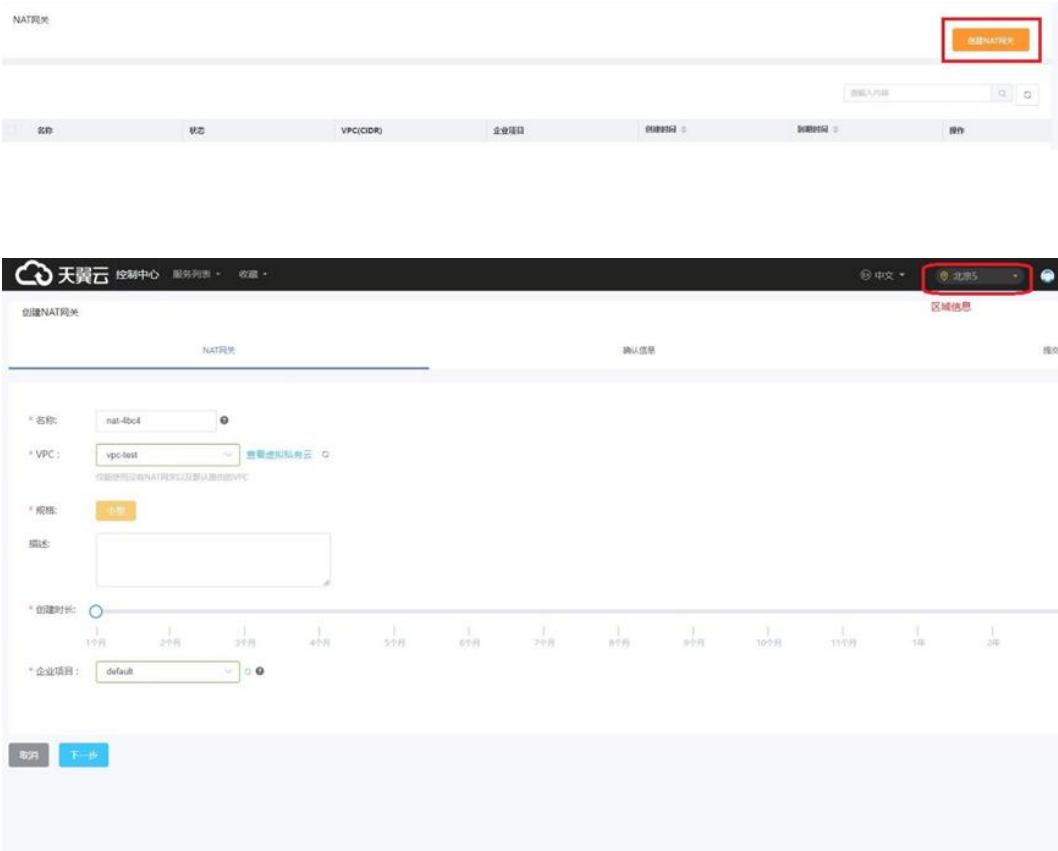
2.1 创建公网 NAT 网关

操作场景

如果您 VPC 中的云主机需要为互联网提供服务，则需要创建 NAT 网关。

操作步骤

- 1、登录天翼云管控制中心。
- 2、在系统首页，单击“网络>NAT 网关”。
- 3、在 NAT 网关页面，单击“创建 NAT 网关”，进入 NAT 网关创建页面。



根据界面提示，配置 NAT 网关相关参数：

区域：选择对应的区域资源池。

名称：NAT 网关实例名称。

虚拟私有云：NAT 网关所属的 VPC。

创建时长：包周期时长。

配置好相关参数后，点击“下一步”、“确认下单”即完成 NAT 网关创建。

2.2 创建 SNAT 规则

操作步骤

1、登录天翼云管控制中心。

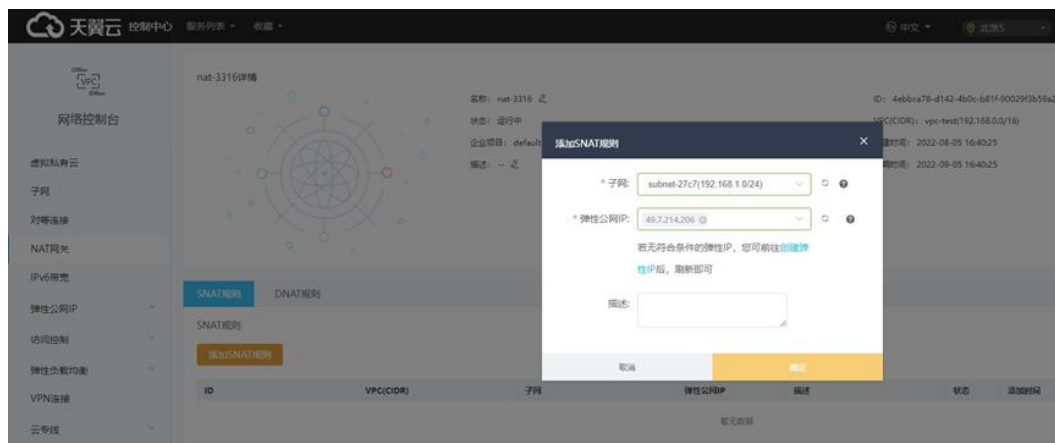
2、选择目标区域节点。

3、选择“网络>NAT 网关”，进入 NAT 网关信息展示页面。点击 NAT 网关名称，进入 NAT 网关详情规则页面。



4、点击“添加 SNAT 规则”，弹出添加 SNAT 规则对话框，进行参数配置。





子网：选择要使用 SNAT 的对应子网。

弹性 IP：选择用来提供互联网访问的公网 IP。

5、点击“确定”，即完成 SNAT 规则的设置。

6、SNAT 规则创建完成后，可在 SNAT 规则信息展示列表查询相应信息。

2.3 创建 DNAT 规则

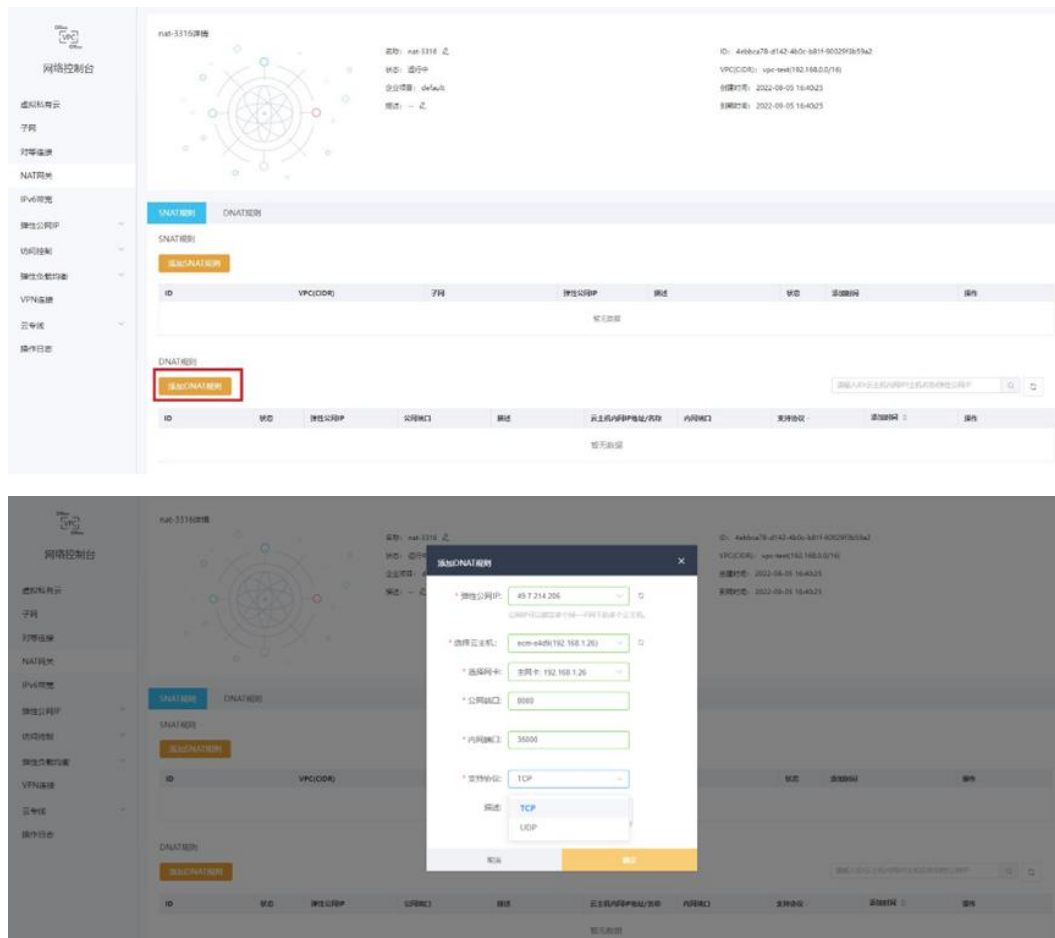
操作步骤

1、登录天翼云管控制中心。

2、选择目标区域节点。

3、选择“网络>NAT 网关”，进入 NAT 网关信息展示页面。点击 NAT 网关名称，进入 NAT 网关详情规则页面。

4、点击“添加 DNAT 规则”，弹出添加 DNAT 规则对话框，进行参数配置。



弹性公网 IP：用于外部公网用户进行服务访问的目的 IP。

公网端口：外部公网用户访问服务的端口。

云主机：选择 DNAT 规则对应的内部云主机。

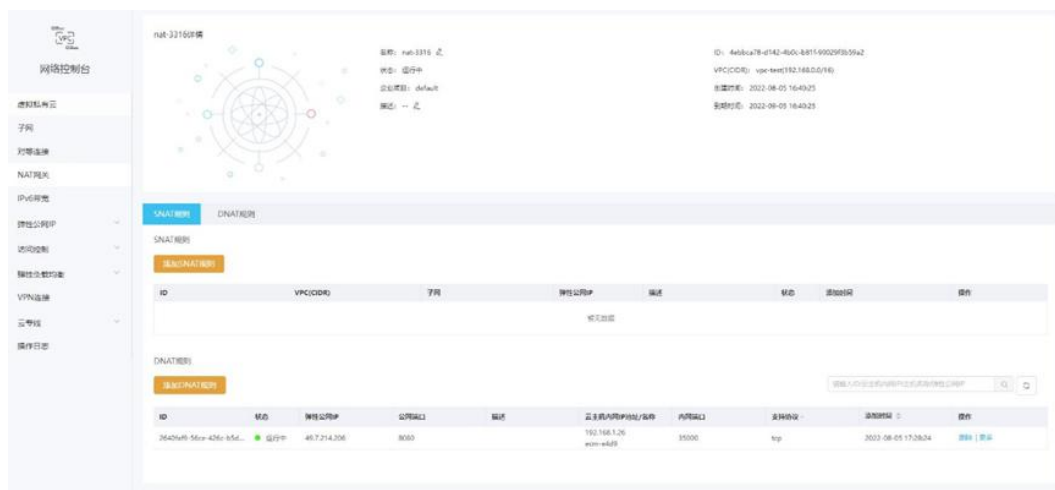
网卡：选择 DNAT 规则对应的内网 IP。

内网端口：应用在内部提供服务使用的端口。

支持协议：TCP、UDP 协议。

5、设置好对应参数后，点击“确定”，即完成 DNAT 规则的创建。

6、DNAT 规则创建完成后，可在 DNAT 规则信息展示列表查询相应信息。



3 用户指南

3.1 修改公网 NAT 网关

操作步骤

- 1、登录天翼云管控制中心。
- 2、选择目标区域节点。
- 3、选择“网络>NAT 网关”，进入 NAT 网关信息展示页面。
- 4、选中对应 NAT 网关实例，点击“修改”。进入 NAT 网关实例信息修改页面。

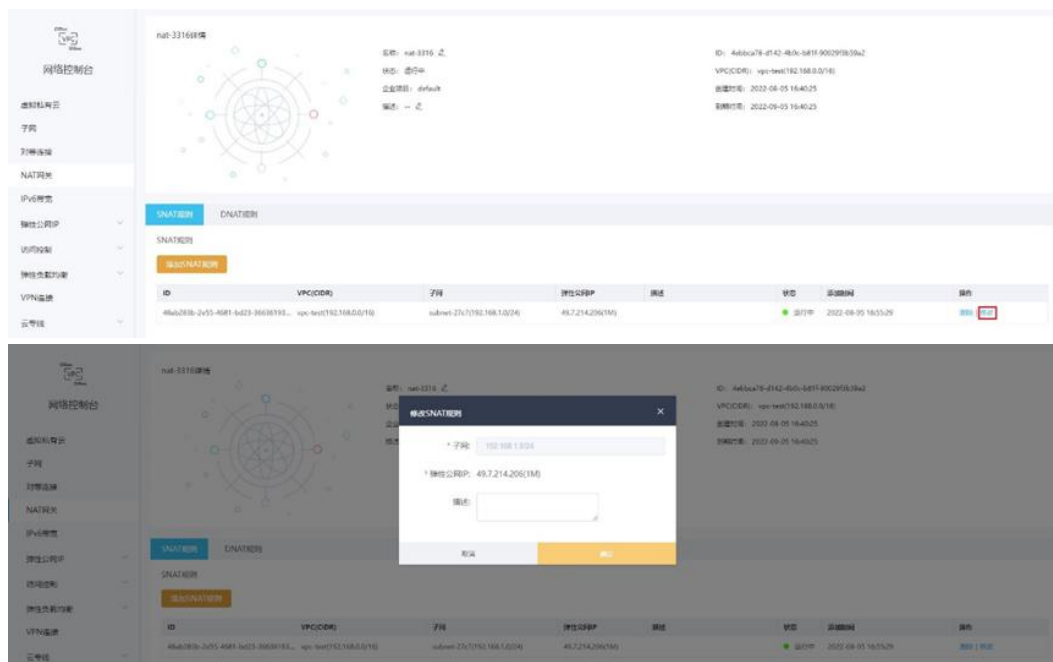


可按需进行 NAT 网关实例名称、自定义描述修改。

3.2 修改 SNAT 规则

操作步骤

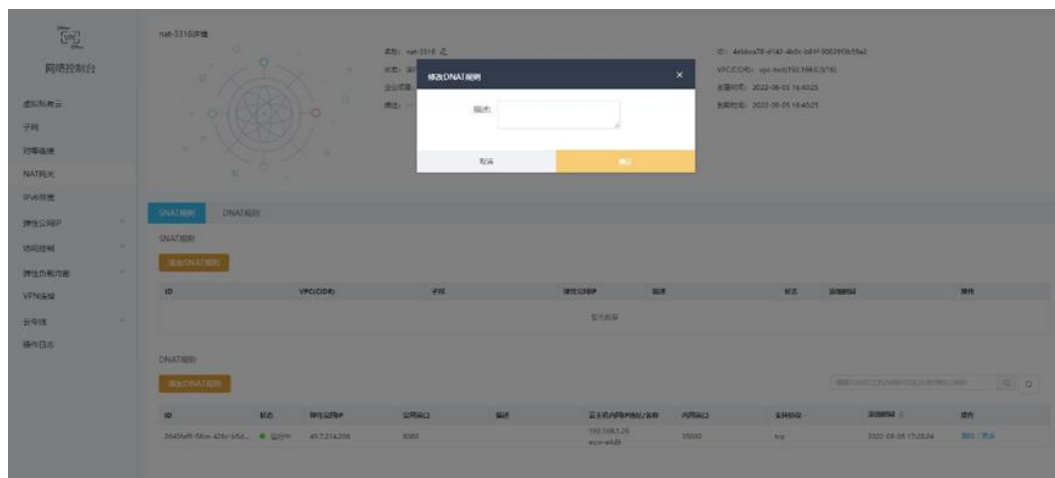
- 1、登录天翼云管控制中心。
- 2、选择目标区域节点。
- 3、选择“网络>NAT 网关”，进入 NAT 网关信息展示页面。点击 NAT 网关名称，进入 NAT 网关详情规则页面。
- 4、选择对应 SNAT 规则点击“修改”，进行 SNAT 规则自定义描述修改。



3.3 修改 DNAT 规则

操作步骤

- 1、登录天翼云管控制中心。
- 2、选择目标区域节点。
- 3、选择“网络>NAT 网关”，进入 NAT 网关信息展示页面。点击 NAT 网关名称，进入 NAT 网关详情规则页面。
- 4、选择对应 DNAT 规则点击“更多”>“修改”，进行 DNAT 规则自定义描述修改。



3.4 删除公网 NAT 网关

操作步骤

- 1、登录天翼云管控制中心。
- 2、选择目标区域节点。
- 3、选择“网络>NAT 网关”，进入 NAT 网关信息展示页面。
- 4、选择对应 NAT 网关实例点击“退订”，弹出二次确认删除提醒对话框。点击“确定”，即完成 NAT 网关实例的删除。

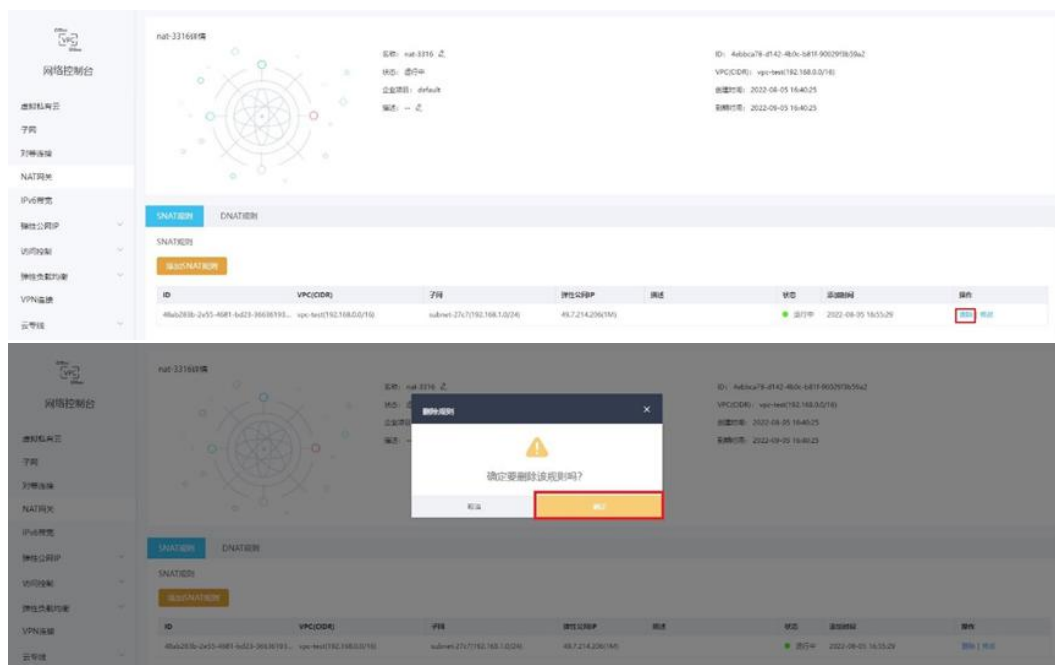




3.5 删除 SNAT 规则

操作步骤

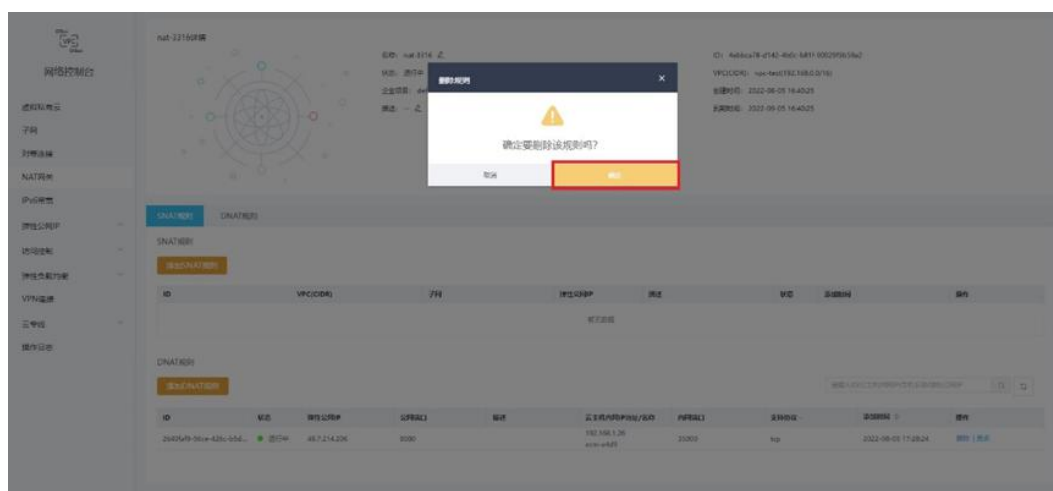
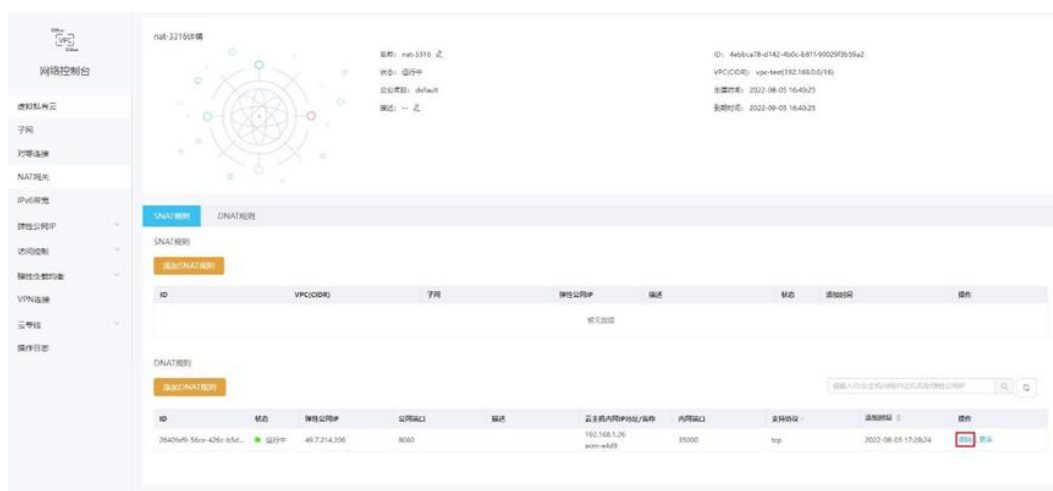
- 1、登录天翼云管控制中心。
- 2、选择目标区域节点。
- 3、选择“网络>NAT 网关”，进入 NAT 网关信息展示页面。点击 NAT 网关名称，进入 NAT 网关详情规则页面。
- 4、选择对应 SNAT 规则点击“删除”，弹出二次确认删除提醒对话框。点击“确定”，即完成 SNAT 规则的删除。



3.6 删除 DNAT 规则

操作步骤

- 1、登录天翼云管控制中心。
- 2、选择目标区域节点。
- 3、选择“网络>NAT 网关”，进入 NAT 网关信息展示页面。点击 NAT 网关名称，进入 NAT 网关详情规则页面。
- 4、选择对应 DNAT 规则点击“删除”，弹出二次确认删除提醒对话框。点击“确定”，即完成 DNAT 规则的删除。



4 常见问题

什么是 NAT 网关？

NAT 网关能够为 VPC 内的计算实例提供 NAT（网络地址转换）服务，使多个计算实例可以共享使用弹性 IP 访问 Internet，或使多个计算实例通过同一弹性 IP 对外提供服务。

NAT 网关、弹性 IP、弹性云主机、VPC 之间是什么样的关系？

- 1、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。
- 2、NAT 网关通过网络地址转换，可以为 VPC 内的云主机提供访与 Internet 互通的能力。
- 3、弹性 IP 是可以提供互联网上合法的静态公网 IP 地址的服务，VPC 的的吞吐量由弹性 IP 带宽决定。
- 4、云主机是 VPC 内运行的计算实例，可以使用 NAT 网关或弹性 IP 与 Internet 互通。

NAT 网关故障是否会影响业务运行？

不会。NAT 网关采用集群形式部署，集群内状态实时同步。单网元故障时，故障自动切换，业务无感知。同时为用户提供告警服务，降低风险提高可用性。

一个 NAT 网关实例支持绑定多少个弹性 IP？

NAT 网关可绑定多个 EIP，单个 NAT 网关实例绑定 EIP 上限为 32。

一个弹性 IP 可以同时用于 DNAT 和 SNAT 条目吗？

不可以。实际的业务部署中，SNAT 规则和 DNAT 规格一般面向不同的业务。如果使用相同的弹性 IP，可能存在业务相互抢占的风险。

弹性 IP 和 NAT 网关如何选择使用？

- 1、当云主机需要使用公网 IP 所有端口，直接与 Internet 互通时，建议云主机直接绑定弹性 IP。云主机直接绑定弹性 IP，如果云主机数量过多的话，会消耗较多公网 IP。
- 2、希望保护 VPC 内虚拟网络结构，并且希望多个云主机共用公网 IP、通过端口号区分与 Internet 互通，建议使用 NAT 网关。

云主机同时绑定弹性公网 IP 和使用 NAT 网关是否冲突？

- 1、当云主机同时绑定弹性公网 IP 和使用 NAT 网关的场景下，所有云主机主动访问 Internet 的流量默认是通过内网转发至 NAT 网关，回包也经过 NAT 网关返回至云主机，此部分流量不会受弹性 IP 定义的带宽上限限制。
- 2、如果来自 Internet 的流量主动访问云主机的弹性公网 IP，则云主机回包统一通过弹性公网 IP 返回，这样产生的公网出流量受到云主机绑定的弹性 IP 所定义的带宽上限限制。
- 3、如果客户需要更改默认外访流量是通过弹性 IP 的话，可以在路由表添加一条下一跳类型为“云服务器的公网 IP”的路由策略。此路由策略会影响该路由表关联的所有子网，即这些子网内有公网 IP（或弹性 IP）的云服务器访问 Internet，将不再通过 NAT 网关，而是其公网 IP。