



NAT网关

产品文档





文档目录

产品简介

产品概述

网关简介

网络拓扑关系

主要功能

SNAT

共享带宽包

流量告警

自动容灾

应用场景

服务能力

配置类型

使用指引

推荐解决方案

大带宽、高可用的公网访问

安全的公网访问

操作指南

创建NAT网关

配置路由表

新建端口转发规则

查询端口转发规则

修改NAT网关配置

管理NAT网关绑定的弹性公网IP

查看NAT网关监控

NAT网关告警设置

删除NAT网关

最佳实践

第一步：创建NAT网关

常见问题

使用相关

NAT网关无法新建

NAT网关无法删除

NAT网关无法解绑弹性IP

使用NAT网关访问公网异常



产品简介

产品概述

网关简介

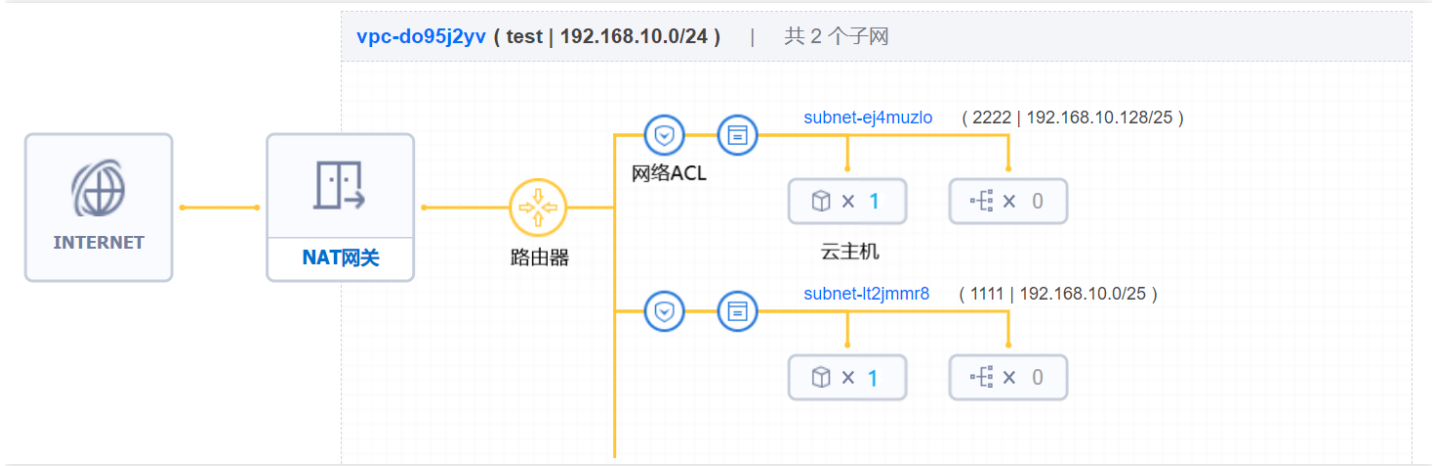
最近更新时间: 2023-03-20 16:05:16

NAT 网关是一种IP地址转换服务，提供SNAT能力，可为私有网络（VPC）内的资源提供安全、高性能的Internet访问服务。例如，为多个无公网访问能力的云服务器提供外网访问的安全出口。

网络拓扑关系

最近更新时间: 2023-03-20 16:05:15

如下图所示，NAT网关串联在租户VPC网络边界路由器与互联网之间，VPC内云主机等通过NAT网关向互联网发送数据包，数据包先经过虚拟路由器，然后NAT网关通过绑定的弹性IP地址作为源IP地址，将数据包发送到互联网。





主要功能

SNAT

最近更新时间: 2023-03-20 16:05:15

SNAT源地址转换：VPC内多个云主机通过同一个互联网IP主动向外访问互联网。



共享带宽包

最近更新时间: 2023-03-20 16:05:15

NAT网关可以配合共享带宽包中的IP带宽包使用，当您为NAT网关绑定了多个EIP时，可将EIP加入共享带宽包，实现多个IP共享公网带宽，可用于不同应用间流量错峰场景，有效降低带宽成本。



流量告警

最近更新时间: 2023-03-20 16:05:15

NAT网关支持设置自定义流量告警，当指标超过一定阈值时自动告警，告警消息会通过电子邮件和短信发出，帮助您提前预警风险。



自动容灾

最近更新时间: 2023-03-20 16:05:15

NAT网关支持双机热备、自动容灾，单机出故障自动切换，业务无感知，有较高的服务可用性。



应用场景

服务能力

最近更新时间: 2023-03-20 15:59:59

NAT网关支持双机热备，自动热切换，互联网带宽最大可支持5Gbps，最多可绑定10个弹性公网IP，最大支持连接数上限可达1000万，不占用租户私网IP地址。

NAT网关不支持绑定安全组，可以VPC内部云主机绑定安全组；不支持绑定网络ACL，可以对VPC内部子网绑定网络ACL。



配置类型

最近更新时间: 2023-03-20 15:59:59

连接数：大型（连接数1000万以内），中型（连接数300万以内），小型（连接数100万以内）。

带宽：出方向互联网带宽支持10、20、50、100、200、500、1000、2000、5000Mbps。



使用指引

最近更新时间: 2023-03-20 15:59:59

- (1) 删除NAT网关会自动取消NAT网关与弹性公网IP的绑定关系，但不会释放弹性公网IP，需要手动释放。
- (2) NAT网关不能绑定安全组和网络ACL，需要对VPC内部的云主机进行控制。
- (3) 只有租户VPC内的云主机可以使用NAT网关，租户不能通过对等连接、VPN网关、专线接入将VPC外部流量路由到NAT网关。（例如，VPC1发往Internet的流量都可通过NAT网关实现，VPC1和VPC2建立了对等连接，VPC2中所有的资源可访问VPC1中的所有资源，但VPC2中的所有资源不可以通过NAT网关访问Internet。）
- (4) NAT网关支持TCP/UDP/ICMP协议。
- (5) NAT网关不支持ALG功能，例如FTP主动模式、SIP等协议无法使用NAT网关。
- (6) 每个NAT网关目前支持带宽上限的规格有10、20、50、100、200、500、1000、2000、5000Mbps，支持的最大连接数规格有小型（最大100万连接数）、中型（最大300万连接数）、大型（最大1000万连接数）。
- (7) NAT网关互联网带宽受限于整体互联网运行情况，极端情况下可能会出现拥塞。
- (8) 每个NAT网关最多支持绑定10个弹性公网IP，每个NAT网关最大端口转发条目为200条。



推荐解决方案

大带宽、高可用的公网访问

最近更新时间: 2023-03-20 15:59:59

NAT 网关可满足用户超大带宽、大量公网IP、较多部署服务的公网访问需求场景。



安全的公网访问

最近更新时间: 2023-03-20 15:59:59

具备SNAT功能，可为CVM主动访问公网提供安全的地址转换，避免CVM的公网IP因直接暴露在Internet而产生的网络安全隐患，同时可以避免CVM被外界主动连接，保障云上资源安全。



操作指南

创建NAT网关

最近更新时间: 2023-03-20 16:00:03

登录建行云控制台，在【私有网络】选项中，选择【NAT网关】。点击【新建】并输入“网关名称”、“网关类型”、“VPC名称”、“已有弹性公网IP”（可选）参数，点击确认完成创建。



配置路由表

最近更新时间: 2023-03-20 16:00:03

登陆建行云控制台，点击【私有网络】，进入私有网络页面。选择【路由表】，在路由表中点击需要访问互联网的子网所关联的路由表ID，进入详情页，在路由策略中单击【新增路由策略】，在弹出页面上，填写目的端，下一跳类型选“NAT网关”和“NAT网关ID”，点击创建完成路由表配置。



新建端口转发规则

最近更新时间: 2023-03-20 16:00:03

登陆建行云控制台，点击【私有网络】，进入私有网络页面。选择【NAT网关】，选择NAT网关ID进入详情页，选择“端口转发”；点击新建，选择协议、互联网IP端口、VPC内部云主机的IP端口，点击确定完成新建。



查询端口转发规则

最近更新时间: 2023-03-20 16:00:03

登陆建行云控制台，点击【私有网络】，进入私有网络页面。选择【NAT网关】，选择NAT网关ID进入详情页，选择“端口转发”；在右上角搜索框中，选择IP、端口、描述，填写属性值后，搜索出转发规则。



修改NAT网关配置

最近更新时间: 2023-03-20 16:00:03

登陆建行云控制台，点击【私有网络】，进入私有网络页面。选择【NAT网关】，选择NAT网关ID进入详情页，可以修改NAT网关自定义名称和带宽上限，提交后实时生效，且在线网络会话不会中断。



管理NAT网关绑定的弹性公网IP

最近更新时间: 2023-03-20 16:00:03

登陆建行云控制台，点击【私有网络】，进入私有网络页面。选择【NAT网关】，选择NAT网关ID进入详情页，在关联弹性公网IP列表中，选择新增绑定弹性IP或解绑。



查看NAT网关监控

最近更新时间: 2023-03-20 15:59:59

登陆建行云控制台，点击【私有网络】，进入虚拟私有网络页面。选择【NAT网关】，选择NAT网关ID进入详情页，点击监控选项卡查看该NAT网关的监控信息。



NAT网关告警设置

最近更新时间: 2023-03-20 15:59:59

登陆建行云控制台，点击顶部导航条【云产品】、【管理与审计】、【云监控】，选择【告警配置】、【告警策略】，可以新建告警策略。输入告警策略名称，在策略类型中选型“私有网络-NAT网关”，添加告警触发条件。选择告警接受组后保存，告警设置完成。触发告警后，建行云将通过短信、邮件、站内信等方式通知您，您可以在“告警历史”中查看。



删除NAT网关

最近更新时间: 2023-03-20 15:59:59

登陆建行云控制台，点击【私有网络】，进入私有网络页面。选择【NAT网关】，选择要删除的NAT网关，点击删除并确认。删除后会将此NAT网关的路由表路由策略一并删除，互联网转发请求立即中断。



最佳实践

第一步：创建NAT网关

最近更新时间: 2023-03-20 15:51:31

- (1) 登陆建行云控制台，在【私有网络】选项中，选择【NAT网关】。
- (2) 单击左上角的“新建”，在弹出框中依次输入或确定如下参数：

参数	说明
网关名称	按需输入NAT网关名称，支持60个字符。
网关类型	NAT 网关的类型有： - o 小型（最大100万连接数） - o 中型（最大300万连接数） - o 大型（最大1000万连接数）
所属AZ	选择NAT网关所属AZ。
私有网络	选择NAT网关所属的私有网络。
出带宽上限	NAT 网关的最大出带宽上限，可选值有（单位：Mbps）：10，20，50，100，200,500，1000，2000，5000。
弹性公网 IP 配置	可选择通过已有弹性公网IP或新建弹性公网IP来配置NAT网关上绑定的弹性公网IP资源。（目前部分区域只支持绑定已有的弹性公网IP，绑定弹性公网IP个数上限为10个） 已有弹性公网IP，选择此方式时，需要该账户下有与NAT网关同地域的闲置EIP资源，通过下拉选择已有EIP，并根据需要配置EIP的带宽上限。

参数配置完成后，点击创建按钮完成NAT网关的创建。



新建NAT网关



网关名称 *

您还可以输入60个字符

网关类型 *

小型（最大并发连接数100万） ▼

所在地域

武汉

所属AZ *

武汉二区 ▼

所属网络 *

vpc-b9mk5e5n (lqc3 | 10.0.0.0/16) ▼

带宽上限 *

100Mbps ▼

弹性IP

新建弹性IP ▼

[+ 添加绑定IP](#)

最多可绑定10个IP

创建

取消



常见问题

使用相关

NAT网关无法新建

最近更新时间: 2023-03-20 15:51:31

- (1) 检查是否是主账号限制了子账号配额，若是则登录主账号调整相应配额数量。
- (2) 检查是否是主账号的配额达到上限，若是则需要联系建行云调整主账号的相应配额数量。
- (3) 若创建NAT网关后显示创建失败，则在创建NAT网关时须选择已有弹性IP。没有已有的弹性IP时则需要先新建弹性IP，再创建NAT网关（部分区域存在此限制）。
- (4) 若不属于以上3种情况，创建NAT网关时使用F12查看CreateNatGateway接口返回结果,联系建行云处理。



NAT网关无法删除

最近更新时间: 2023-03-20 15:51:31

- (1) 检查要删除的NAT网关是否处于运行中，若该NAT网关的状态不处于运行中,需要联系建行云处理。
- (2) 联系建行云查看要删除的NAT网关实例是否处于被探测机探测的状态。
- (3) 若不属于以上2种情况，删除NAT网关时使用F12查看DeleteNatGateway接口返回结果,联系建行云处理。



NAT网关无法解绑弹性IP

最近更新时间: 2023-03-20 15:51:31

- (1) 检查该NAT网关是否至少绑定了两个弹性IP。若只绑定了一个弹性IP，请先申请一个弹性IP，将NAT实例绑定该弹性IP，再解绑弹性IP。
- (2) 解绑弹性IP时使用F12查看EipUnBindNatGateway接口返回结果,联系建行云处理。



使用NAT网关访问公网异常

最近更新时间: 2023-03-20 15:51:31

- (1) 检查CVM所在子网绑定的路由表中的路由表项是否正确。
- (2) 检查CVM绑定的安全组（包括出站规则和入站规则）是否放通需要用到的源、目的IP和源、目的端口以及协议。
- (3) 检查子网绑定的ACL是否放通需要用到的源、目的IP和源、目的端口以及协议。
- (4) 检查业务路径中是否有其他环节（如防火墙）限制业务转发。
- (5) 检查CVM本机的用于IP地址和域名快速解析的文件/etc/hosts中的配置是否正确。
- (6) 检查NAT网关的带宽上限以及绑定弹性IP的带宽上限。
- (7) 检查NAT网关实例实时、近24小时的外网出带宽、外网入带宽、出包量、入包量、连接数的监控是否正常。
- (8) 若以上检查均正常，需要联系建行云处理。