NAT 网关

最佳实践

腾讯云

文档目录

最佳实践
通过标准型 NAT 实现跨 VPC 访问公网

最近更新时间：2024-01-16 15:42:11

使用场景

用户在某个 VPC 建立了 NAT 网关，同 VPC 或者其他 VPC（包括同地域，跨地域，跨账号）的 CVM 实例希望通过 NAT 网关出公网。

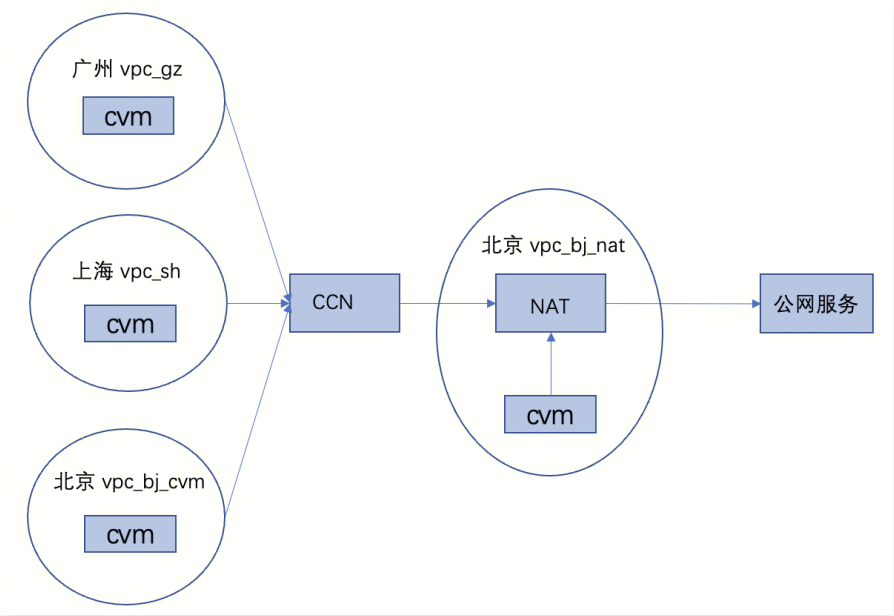
限制条件

- 跨 VPC 访问公网功能，当前仅标准型 NAT 网关支持，传统型 NAT 网关不支持。
- 不同 VPC 的 NAT 路由不支持同时发布到 云联网（Cloud Connect Network，CCN）。
- 标准型 NAT 网关正在灰度测试中。如需使用，请 提交工单 申请。

配置原理

用户创建 NAT 网关，并配置目的网段为公网地址且下一跳为 NAT 的路由之后，同 VPC 的 CVM 实例即可通过 NAT 的路由出公网；将 NAT 的路由发布到 CCN 之后，关联 CCN 的其他 VPC 即可通过 CCN 和 NAT 出公网。

> **说明：**
> 云联网为独立产品，使用 CCN 会产生相关费用，详情请参考 计费总览 。



使用流程

步骤一：在北京 VPC 创建标准型 NAT 网关

登录 NAT 网关控制台，可参见 创建 NAT 网关，创建示例 NAT 网关：vpc_bj_nat。

> **说明：**

NAT 网关所在的 VPC 不能存在VPN 网关。

步骤二：新增路由策略

登录 路由表控制台，在示例北京 VPC：vpc_bj_nat 的路由表中创建一条路由策略，例如 0.0.0.0 的默认路由，下一跳为 NAT 网关。详细操作，可参见 配置指向 NAT 网关的路由 。
此时同 VPC 的 CVM 即可通过该路由出公网。

步骤三：确认广州 VPC 的 CVM

登录 CVM 控制台，确保在广州 VPC 已有 CVM 实例，例如广州 VPC 的 CVM 实例：cvm_gz，若没有 CVM，可参见 创建 CVM 实例 。

步骤四：创建 CCN 并加入 CCN

登录 私有网络–云联网 控制台，参考文档 新建云联网实例 和 关联网络实例，将 NAT 网关所在的北京 VPC 加入 CCN，将 cvm_gz 实例所在的广州 VPC 加入 CCN，可参见 关联网络实例 。

说明：

1. 此处的 CVM 实例可以是同地域，跨地域，跨账号的 VPC；地域不受限制。
2. 流程上也可以先把北京 VPC 加入 CCN，再创建 NAT 路由和创建广州 VPC 下的 CVM。

步骤五：NAT 路由发布到 CCN

登录 私有网络-路由表 控制台，将所创建 NAT 网关的路由发布到 CCN，详细操作，可参见文档 管理路由策略 。

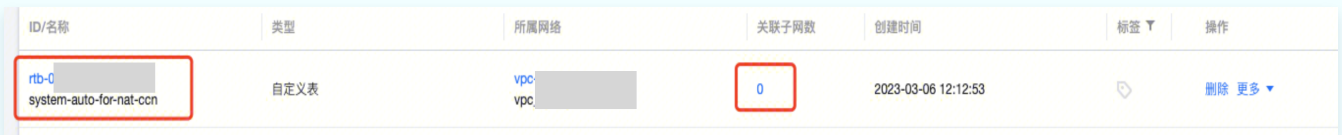
说明：

1. 不支持不同 VPC 的 NAT 的路由发布到 CCN。
2. 仅支持单个 VPC 的 NAT 的路由发布到 CCN，并且支持该 VPC 的多条 NAT 的路由发布到 CCN。

注意：

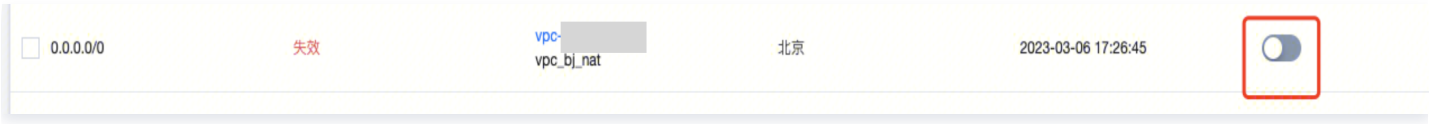
1. NAT 的路由发布到 CCN 时，系统会自动创建一个名称为"system-auto-for-nat-ccn"路由表：关联子网为0，用于公网回向流量的路由，即 NAT 网关指向 CCN 的路由，用户一般无需修改它。
2. 一个 VPC 仅会创建一个"system-auto-for-nat-ccn"路由表，已经存在则不再重复创建。最后一个 NAT 路由从 CCN 撤销时或者 VPC 和 CCN 解绑时会自动删除该路由表。

如下所示：NAT 所在 VPC：vpc_bj_nat 的路由表列表页：



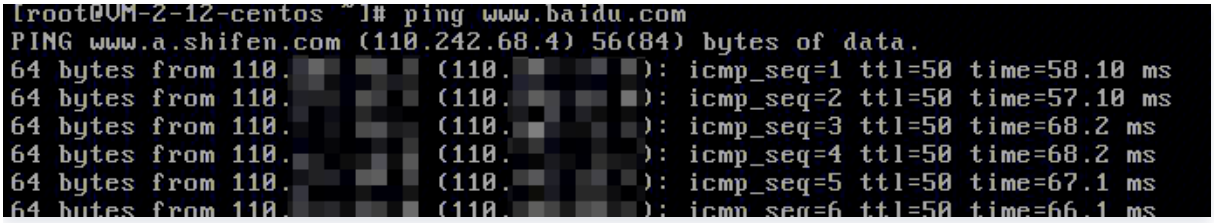
步骤六：启用路由

当 NAT 路由为 0.0.0.0 的默认路由时，由于路由的目的 CIDR 存在冲突，需要手动启用路由。登录 私有网络-云联网 控制台，详细操作，可参见 启用路由 。



步骤七：流量验证

在 CVM 上可以 ping 通，即可访问外网。



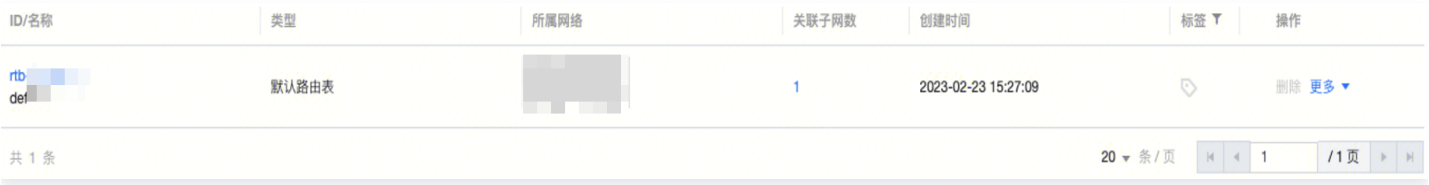
删除流程

步骤一：路由撤销

登录 私有网络-路由表 控制台，将 NAT 网关的路由从 CCN 撤销。

步骤二：路由校验

登录 私有网络-路由表 控制台，查看"system-auto-for-nat-ccn"路由表也被联动删除了。如下所示：NAT 所在 VPC：vpc_bj_nat 的路由表列表页。



登录 私有网络-云联网 控制台，查看 CCN 路由表里的 0.0.0.0 的路由也联动删除了。


ccn 详情
关联实例
监控
带宽管理
路由表
2020年9月15日之后创建的专线网关默认发布路由方式为VPC网段，点击查看详情
启用路由
禁用路由
多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔
目的端
状态
下一跳
下一跳所属地域
更新时间
启用路由
有效
广州
2023-02-23 14:44:10
有效
广州
2023-03-06 11:32:48
有效
北京
2023-03-06 11:44:11
共 3 条
10 条 / 页
1
/ 1 页

通过私网 NAT 实现 VPC 内指定子网和外部资源互访

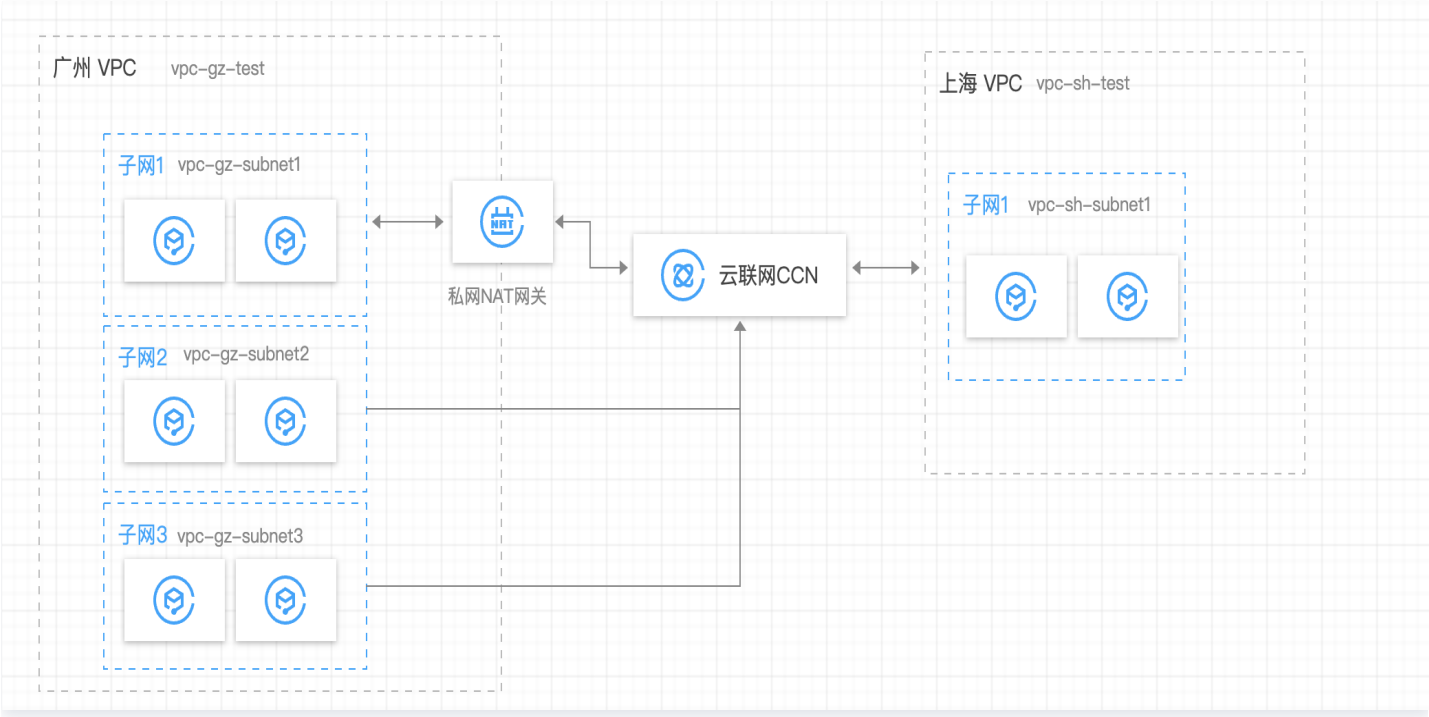
最近更新时间：2023-10-24 17:00:41

应用场景

适用于解决 VPC 内指定子网的地址转换，用于 VPC 内指定子网和外部资源的互访。
本文以下述场景为例：在广州的 VPC 内存在多个子网，不允许子网1直接和上海的 VPC 互访，允许子网2直接和上海的 VPC 互访。因此，在本案例中，广州 VPC 子网1通过 SNAT 到其他 IP，实现和上海的 VPC 互访。

配置方案

组网方案可参考图示配置：



步骤一：创建 VPC 资源

分别在广州地域和上海地域各创建一个 VPC，创建 VPC 可参见 创建私有网络 。广州 VPC 内创建3个子网，上海 VPC 内创建1个子网，可参见 创建子网 。
广州地域：
创建1个 VPC：vpc-gz-test
创建3个子网：

- 子网1 vpc-gz-subnet1；其中1台 CVM：vpc-gz-cvm1
- 子网2 vpc-gz-subnet2；其中0台 CVM：无
- 子网3 vpc-gz-subnet3；其中1台 CVM：vpc-gz-cvm2

上海地域：

创建1个VPC：vpc-sh-test
创建1个子网：vpc-sh-subnet1；其中1台 CVM：vpc-sh-cvm1

步骤二：创建 CCN 资源，同时绑定步骤1中创建的两个 VPC

新建云联网实例 时，在**关联实例**项，绑定步骤一中创建的两个 VPC 实例。

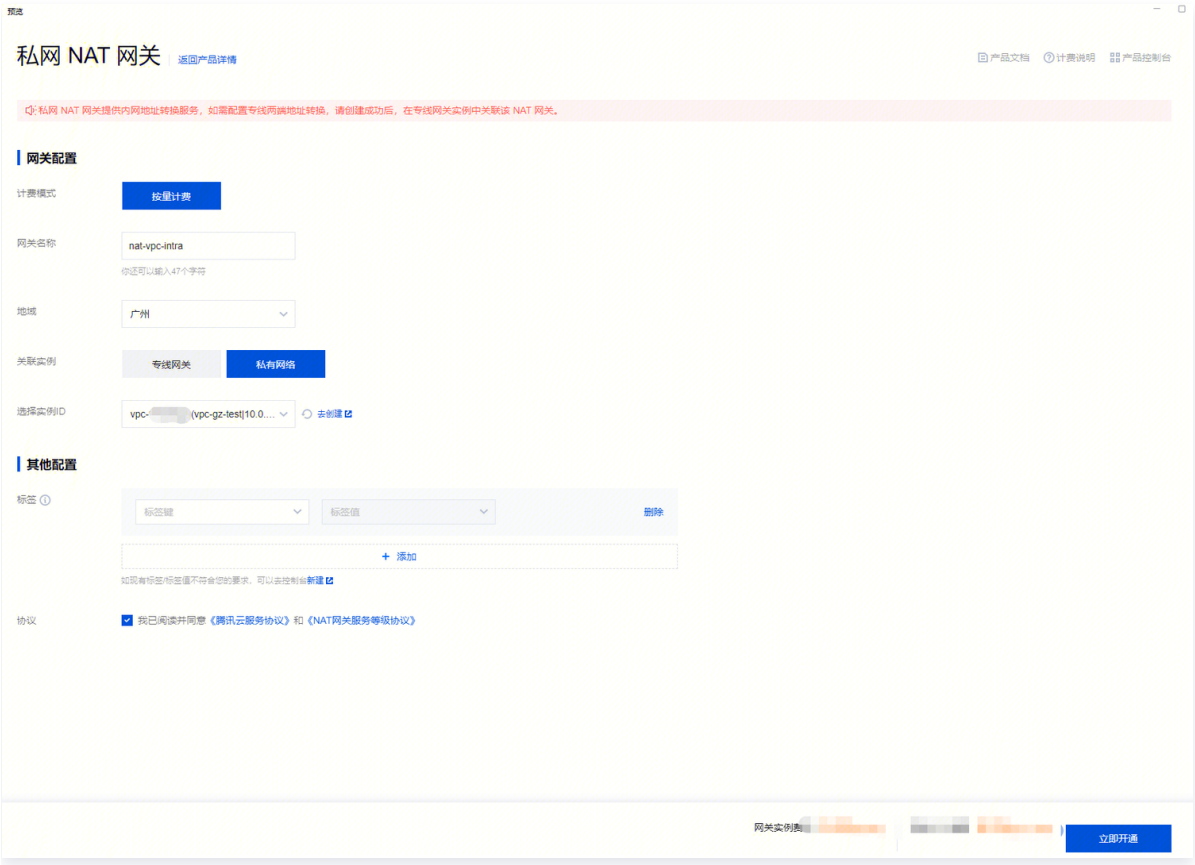
步骤三：关闭 CCN 端涉及 NAT 的自学习路由

1. 登录 云联网控制台，单击步骤二中创建的 **CCN 实例**，进入实例页面。
2. 选择**路由表**页签，关闭需要 NAT 的子网网段路由(示例中对应 vpc-gz-subnet1)。

> **说明：**
> 如果用作 NAT IP 的网段也属于某个子网网段或子集，那么需要关闭对应子网的路由，例如 vpc-gz-subnet2 的网段 IP 作为 NAT IP，则关闭 vpc-gz-subnet2 的路由。

步骤四：在广州 VPC(vpc-gz-test) 新建 VPC 类型私网 NAT 网关

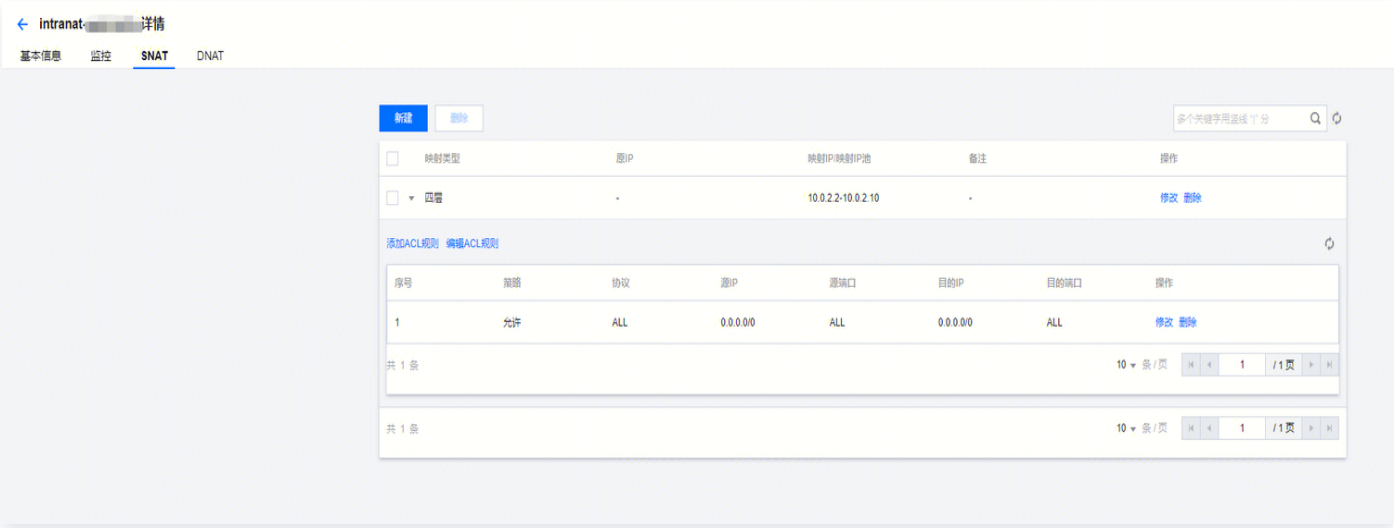
详细信息，可参见 创建私网 NAT 网关 。



步骤五：编辑 NAT 网关规则 (四层 SNAT 规则)

1. 登录 私网 NAT 网关控制台，单击步骤四中创建的 VPC 类型私网 NAT 网关 ID，进入网关详情页。
2. 单击 SNAT 页签，编辑 NAT 网关规则（四层 SNAT 规则）。

> **说明：**
> 原 IP 是 vpc-gz-cvm1 IP， 映射 IP 池(即 NAT IP) 可以是其它第三方 IP，或者是其它子网网段子集。（例如从 vpc-gz-subnet2 子网网段范围内获取）。



步骤六：配置 vpc-gz-test 端路由

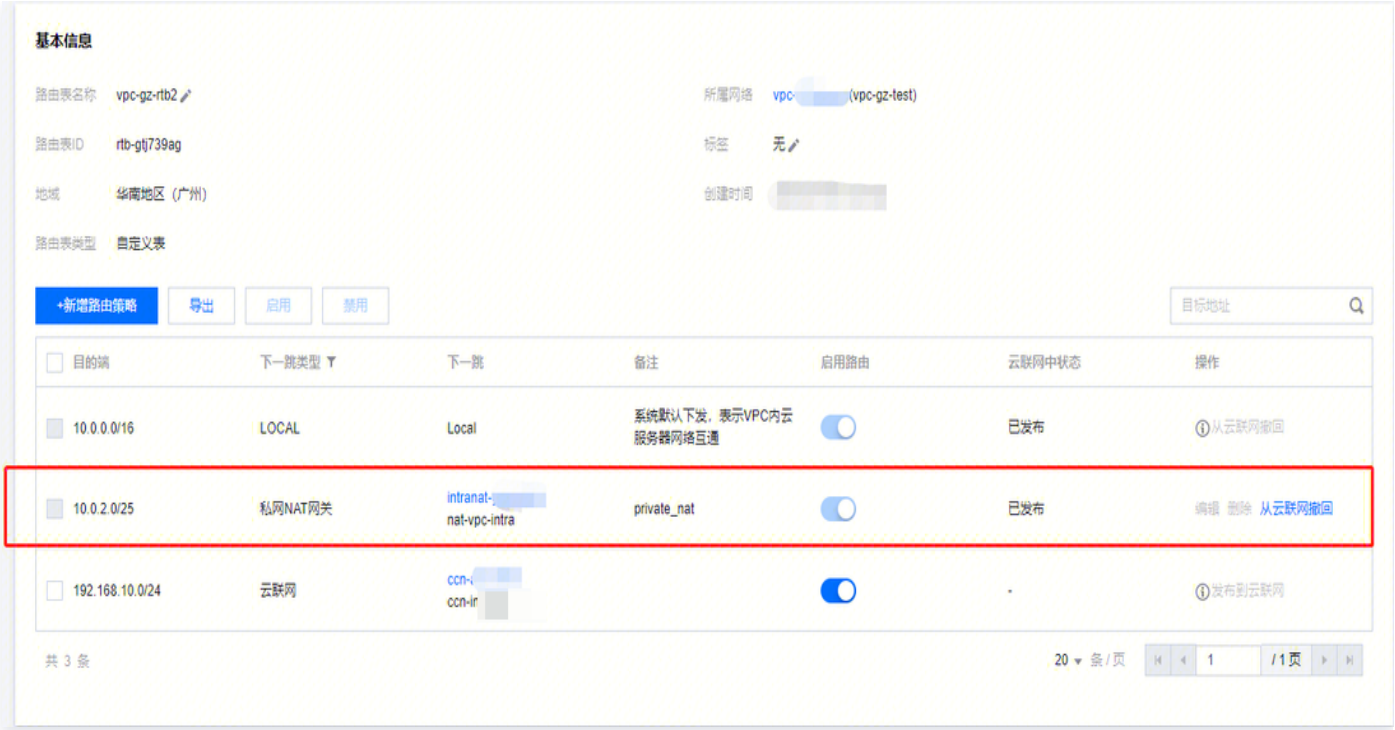
1. 登录 私有网络控制台，在 vpc-gz-test 实例中，新建两个路由表，vpc-gz-rtb1 和 vpc-gz-rtb2，其中 vpc-gz-rtb1 绑定子网1(vpc-gz-subnet1) 。

2. 在路由表 vpc-gz-rtb1 中，关闭所有从 CCN 学习到的路由。

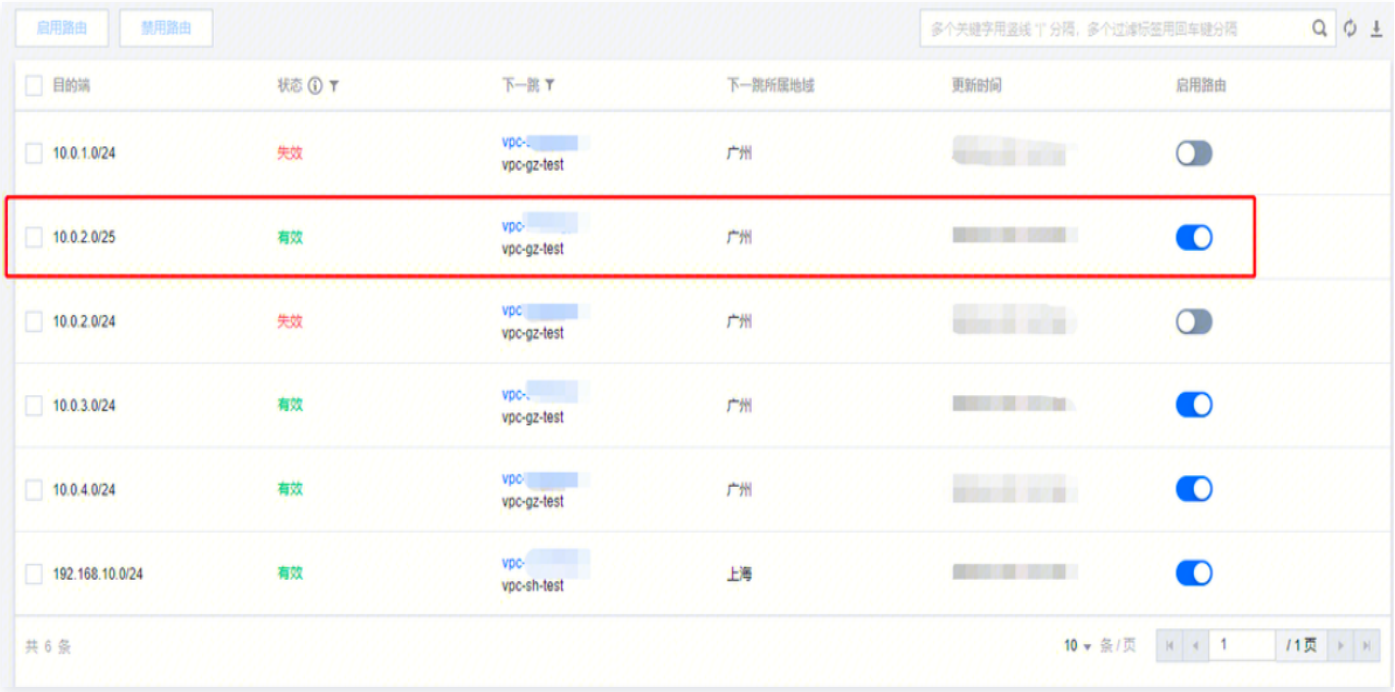
> **说明：**
> 一旦有新加入云联网的 VPC，都需要在这个路由表中关闭对应学习到的路由条目。

3. vpc-gz-rtb1 中新建路由条目，目的是要访问的网段，下一跳是第3步中新建的 NAT 实例。

4. vpc-gz-rtb2 中新建路由条目，目的是NAT IP网段(如果是其它子网网段分配，则需要是子网网段子集，不能和子网网段完全相同)，并且要发布到云联网。



> **注意：**
> 该目的网段IP必须覆盖 第4步中的映射地址池NAT IP范围。(推荐二者取相同值)可以从CCN路由表进行确认是否发布成功。



步骤七：流量验证

从广州 vpc-gz-cvm1 ping 上海 vpc-sh-cvm1， 网络正常，并且在 vpc-sh-cvm1 抓包源 IP 是NAT IP。

```
[root@VM-1-17-centos ~]#
[root@VM-1-17-centos ~]#
[root@VM-1-17-centos ~]# ping 192.168.10.17
PING 192.168.10.17 (192.168.10.17) 56(84) bytes of data.
64 bytes from 192.168.10.17: icmp_seq=1 ttl=61 time=0.853 ms
64 bytes from 192.168.10.17: icmp_seq=2 ttl=61 time=0.830 ms
64 bytes from 192.168.10.17: icmp_seq=3 ttl=61 time=3.77 ms
64 bytes from 192.168.10.17: icmp_seq=4 ttl=61 time=1.73 ms
```

如流量 ping 不通，可注意以下情况：

1. vpc-gz-rtb1 要禁用CCN发布的路由；
2. vpc-gz-rtb2 不能绑定任何子网；
3. 如果NAT IP是从子网内分配，NATIP网段必须属于子网网段的子集；
4. CCN上要禁用需要NAT的子网路由。（ NAT IP如果从其它子网网段分配，则也需要禁用相应网段的路由 ）

通过公网 CLB + NAT 方式实现安全的公网互访

最近更新时间：2024-04-12 10:20:41

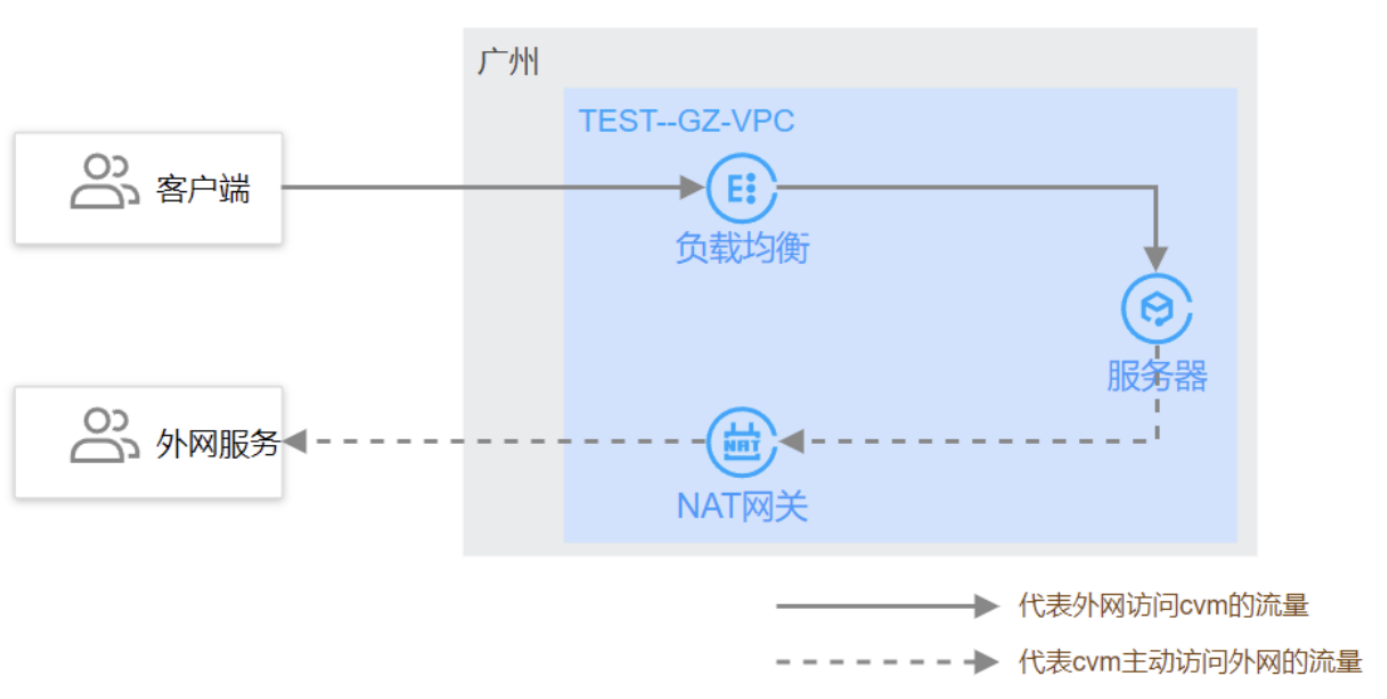
应用场景

随着客户业务增长，出于安全考虑，客户希望云服务器内网 IP 不要暴露在公网，希望能实现云内 IP 地址的**双向隐藏**。

配置方案

基于如上需求，结合腾讯云产品能力，可通过 CLB + NAT 网关方式实现在隐藏云服务器内网 IP 情况下，安全地与公网互访：

- CVM 主动访问外网：即云服务器主动访问外网，可以通过公网 NAT 网关实现。通过 NAT 网关的 SNAT 功能将云服务器的内网 IP 地址转换为 SNAT 后的公网 IP 地址，从而**隐藏**云服务器的内网 IP 地址。
- 外网访问 CVM：当云服务器需要对外提供服务时，可通过公网负载均衡 VIP 统一对外提供服务，从而**隐藏**云服务器的内网 IP 地址，实现公网到云服务器的安全访问。



配置流程

假设客户已创建了业务 VPC，并在 VPC 内云服务器上部署相关业务，可按照如下流程配置：

1. 创建 NAT 网关并配置子网路由指向 NAT 网关
2. 创建公网负载均衡 CLB 实例并配置监听器规则
3. 配置安全策略
4. 操作验证

操作步骤

创建 NAT 网关并配置子网路由指向 NAT 网关

创建公网 NAT 网关并配置子网路由指向 NAT 网关，可以将子网流量引流到 NAT 网关，统一通过 NAT 网关上的公网 IP 来访问公网，从而隐藏内网 IP，实现安全的公网访问。详情请参见 NAT 快速入门。

步骤一：创建 NAT 网关

1. 登录 NAT 网关控制台 。
2. 单击左上角的**新建**，在弹出框中依次配置参数。
3. 参数配置完成后，按照界面提示完成购买即可。详情请参见 创建 NAT 网关 。

步骤二：配置子网路由表指向 NAT 网关

1. 在 NAT 实例列表中，单击目标 NAT 实例所在行的私有网络 ID。
2. 在私有网络详细信息中，单击**子网**。
3. 在子网列表中，选择需要访问公网的子网所在行的路由表 ID。
4. 在路由表基本信息页面，单击**新增路由策略**。
5. 在**新增路由**弹框中，输入目的端（目的公网对应的 IP 地址段）、下一跳类型选择公网 NAT 网关、下一跳选择已创建的 NAT 网关 ID。

6. 单击**创建**完成以上配置后，关联此路由表的子网内的云服务器访问公网的流量将指向该 NAT 网关，并通过 NAT 网关上的公网 IP 访问公网。

步骤三：（可选）配置 SNAT 规则

NAT 支持绑定多个公网 IP，子网路由指向 NAT 网关时，默认子网下的云服务器均可通过 NAT 上的所有公网 IP 访问公网。如需指定云服务器通过 NAT 上指定的公网 IP 访问公网，则可以配置 SNAT 规则，详情请参见 创建 SNAT 规则 。

步骤四：（可选）配置端口转发规则

NAT 网关默认提供主动内访外的能力，如需要对外提供服务，也可以通过配置端口转换规则来实现。
即可将 VPC 内云服务器的**内网 IP**，**协议**，**端口**映射成**外网 IP**，**协议**，**端口**，使得云服务器上的资源可一对一地被外网访问，详情请参见 配置端口转发规则 。

> **说明**
> NAT 网关的端口转换服务仅能提供一对一的对外访问服务，如需通过统一的 IP 地址对外提供服务，则参考如下步骤通过公网 CLB 来实现。

创建公网负载均衡 CLB 实例并配置监听器规则

通过创建公网 CLB，并配置监听器规则，使得外部客户端可通过 CLB 的外网 VIP 访问后端的云服务器业务，通过公网 CLB 的流量将转发至后端云服务器上。详情请参见 负载均衡快速入门 。

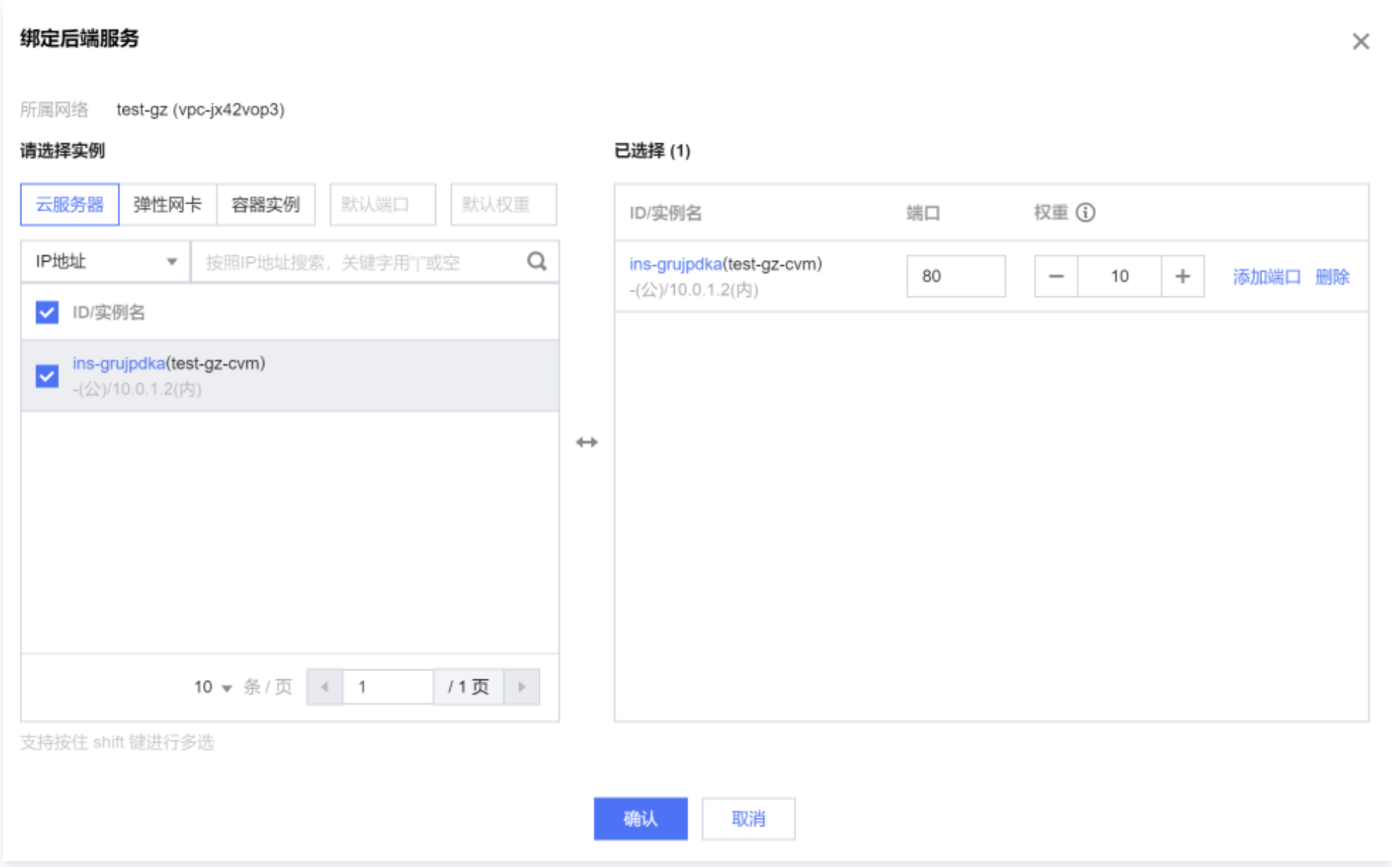
步骤一：购买负载均衡实例

1. 登录腾讯云 负载均衡服务购买页 。
2. 在负载均衡 CLB 购买页面，地域选择与云服务器相同的地域，实例类型选择**负载均衡**，网络类型选择**公网**。详情请参见 创建负载均衡实例 。
3. 单击**立即购买**，完成付款。

步骤二：配置负载均衡监听器

当客户端发起请求时，负载均衡会根据监听的前端协议与端口接收请求并向后端服务器转发请求，详情请参见 配置 TCP 监听器 。

1. 在负载均衡列表页，单击目标负载均衡实例右侧的**配置监听器**。
2. 在**监听器管理**页签对应协议区域下，单击**新建**。
3. 在**创建监听器**对话框中，逐步配置监听器健康检查，会话保持等相关参数，单击**提交**。
4. 在右侧监听器详情中，单击绑定，为 CLB 绑定后端云服务器，并配置云服务器端口和权重，完成后单击确定。

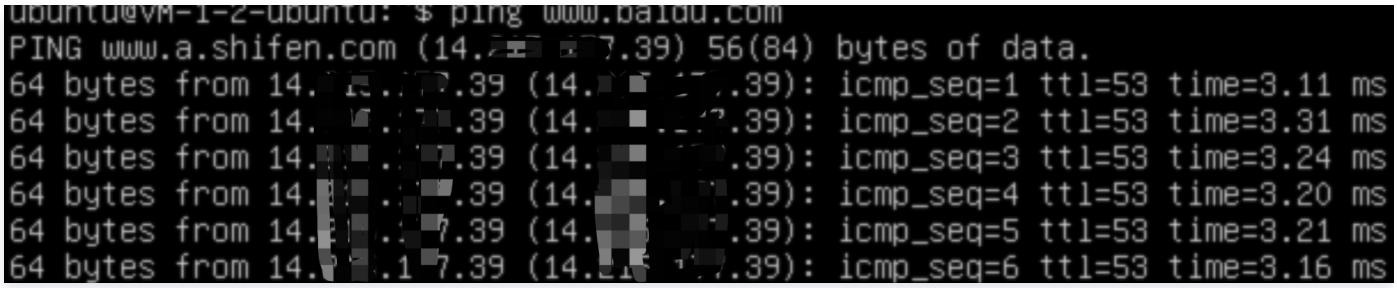


配置安全策略

1. 创建完负载均衡后，您可以配置负载均衡的安全组来隔离公网流量，详情请参考 配置 CLB 安全组 。
2. 可以为云服务器绑定安全组，实现云服务器级别的流量控制，详情请参见 添加安全组规则 和 关联实例至安全组 。
3. 可以 配置 WAF 对负载均衡的监听域名进行 Web 安全防护 。
4. 可以为 NAT 网关绑定 DDoS 高防包以抵御 DDoS 攻击。

操作验证

1. 云服务器主动访问外网。



2. 外网通过公网 CLB 的 VIP 访问后端业务。

相关文档

- 当一个子网关联了 NAT 网关，且子网内云服务器有公网 IP（或弹性 IP）时，会默认通过 NAT 网关访问 Internet（因为最精确路由的优先级高于公网 IP），但您可以设置路由策略，实现通过云服务器公网 IP 访问 Internet，详情请参见 调整 NAT 网关和 EIP 的优先级 。
- 若您使用 CLB 转发业务流量到 CVM 上，为保障健康检查功能，在 CVM 的安全组上需做相应配置，详情请参见 后端云服务器的安全组配置 。

调整 NAT 网关和 EIP 的优先级

最近更新时间：2024-04-03 17:36:51

NAT 网关/EIP 优先级说明

当一个子网关联了 NAT 网关，且子网内云服务器有公网 IP（或弹性 IP）时，会默认通过 NAT网关访问 Internet（因为最精确路由的优先级高于公网 IP），但您可以设置路由策略，实现通过云服务器公网 IP 访问 Internet。

操作步骤

1. 查看该云服务器所在子网关联的路由表。确保有指向 NAT 网关的路由策略，以保证该子网下，无公网 IP 的云服务器仍可以通过 NAT 网关访问 Internet 。

2. 新增下一跳类型为“云服务器的公网 IP”的路由策略，并填入目的端。
   - 目的端：填写业务需要访问的具体公网网段或默认路由（0.0.0.0/0，默认路由表示：目的端不在路由表中，所有数据包都会使用该默认路由）。
   - 下一跳类型：云服务器的公网 IP。

> **注意**
> - 此路由策略与原来指向 NAT 网关、云服务器、公网网关的路由规则配置相同目的端时，均会优先匹配该路由。
> - 此路由策略会影响该路由表关联的所有子网（请您确认操作带来的影响），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。
> - 该路由表关联的子网内，无公网 IP 的云服务器仍可以通过 NAT 网关访问 Internet，不会受到影响。

通过 VPC 高级特性实现境外访问优化

最近更新时间：2023-11-24 15:44:51

使用场景

通过公共互联网，优化境内访问境外网站的访问速度。

> **注意：**
> - 该功能在遵守国家相关法规政策的前提下，对境外访问质量进行优化。
> - 该功能正在灰度测试中。如需使用，请 提交工单 申请。

限制条件

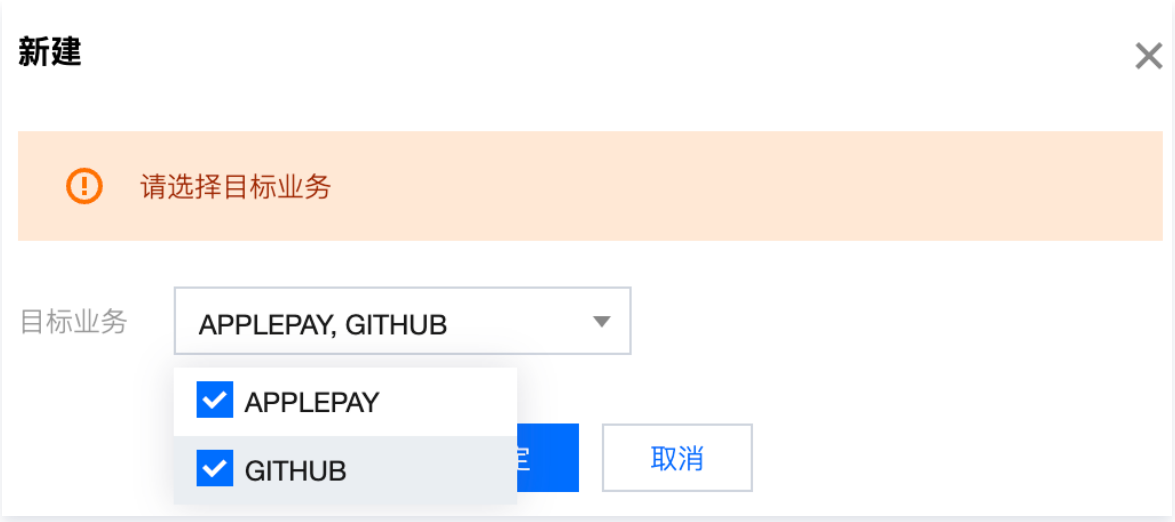
- 每个腾讯云账号 UIN 在某一具体地域，仅允许5个 VPC 加速。
- 当前可支持加速地域：北京、上海、广州，建议优先使用北京和广州地域。
- 每个 VPC 可加速带宽共50Mbps。
- 当前仅支持部分服务的部分域名加速，具体服务内容可参考登录 VPC控制台 查看。

> **注意：**
> 受底层资源限制，海外访问优化服务总量有限，且处于动态变动中，当全量资源被消耗完成后，腾讯云会针对处于以下状态的 VPC 做出限制：
> 1. 未开启海外访问优化的 VPC 将无法开启该服务。
> 2. 已开启海外访问优化功能，但在一段时间内没有流量访问。
>
> 腾讯云会持续进行底层资源改造，在资源补充后，被限制的 VPC 可重新开启海外访问优化功能。

使用流程

1. 登录 私有网络控制台，选择需要开启海外访问优化服务的 VPC，选择**高级特性**页签。
2. **单击**  ，开启海外访问优化。

3. 在**新建**弹窗中，选择要开启的目标业务。


新建
请选择目标业务
目标业务
APPLEPAY, GITHUB
APPLEPAY
GITHUB
取消

4. **单击确定，完成开启。**


海外访问优化
新建
业务名称
域名
操作
GITHUB
关闭
APPLEPAY
关闭