NAT 网关

最佳实践

文档版本 01

发布日期 2025-10-15

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 NAT 网关安全最佳实践

1. **加强权限管理，提高访问控制能力。**

   如果您需要对您所拥有的NAT网关（NAT Gateway）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），详情请参见**权限管理**

2. **建议您妥善管理身份认证信息，减小因凭证泄漏导致的数据泄露风险。**

   NAT网关服务基于统一身份认证服务（Identity and Access Management，IAM），支持三种身份认证方式：用户名密码、访问密钥、临时访问密钥。同时还提供**登录保护**及**登录验证策略**。

   a. **建议使用临时AK/SK进行业务处理，减小凭证泄漏导致您数据泄露的风险。**

      使用NAT API/SDK管理相关资源时，都需要进行身份凭证认证，用于确保请求的机密性、完整性和请求者身份的正确性。建议您为应用程序或服务配置IAM委托或临时AK/SK，通过IAM委托可以获取一组临时AK/SK，临时AK/SK到期自动过期失效，可以有效降低凭证泄露造成的数据泄露风险。详情请参见**临时访问密钥**和**获取委托的临时访问密钥和securitytoken**。

   b. **定期轮转永久AK/SK，减小凭证泄漏导致您数据泄露的风险。**

      如您必须使用永久AK/SK，建议对永久AK/SK进行定期凭证轮转，同时加密存储，避免凭证长期使用过程中预置的明文凭证泄露导致数据泄露。详情请参见**访问密钥**。

   c. **定期修改用户名密码，避免使用弱密码。**

      定期重置密码是提高系统和应用程序安全性的重要措施之一，不仅可以降低密码泄露的风险，还可以帮助用户满足合规要求，减少内部威胁，提高用户的安全意识。同时建议您配置提高密码的复杂度，避免使用弱密码。详情请参见**密码策略**。

3. **使用最新版本的SDK获得更好的操作体验和更强的安全能力。**

   建议您升级SDK并使用最新版本，可以在您使用NAT网关服务的过程中对您的数据提供更好的保护。最新版本SDK在各语言对应界面下载，请参见**NAT SDK**。

4. **建议DNAT规则避免使用高危端口。**

   对于公网NAT网关，可以添加DNAT规则，通过端口映射的方式为您VPC内的云主机对互联网提供服务。但是对于部分运营商判断的高危端口，默认会被屏蔽。建议您将端口修改为其他端口，请参见**哪些端口无法访问**。

2 基于公网 NAT 网关和云专线的混合云 Internet 加速

操作场景

用户本地数据中心（IDC）通过云专线接入虚拟私有云（VPC），若有大量的服务器需要安全、可靠，高速地访问互联网，或者为互联网提供服务，可通过公网NAT网关服务的SNAT功能或DNAT功能来实现。例如各类互联网、游戏、电商、金融等企业的跨云场景。

方案优势

通过云专线接入华为云上VPC，用户可享受高性能、低延迟、安全专用的数据网络。同时华为云专线单线路最大支持10Gbps带宽连接，可满足各类用户带宽需求。

搭配公网NAT网关的SNAT功能与DNAT功能，实现多个服务器共享使用弹性公网IP（EIP），可有效降低成本。公网NAT网关的规格与绑定的EIP均可随时调整，配置简单，即开即用。

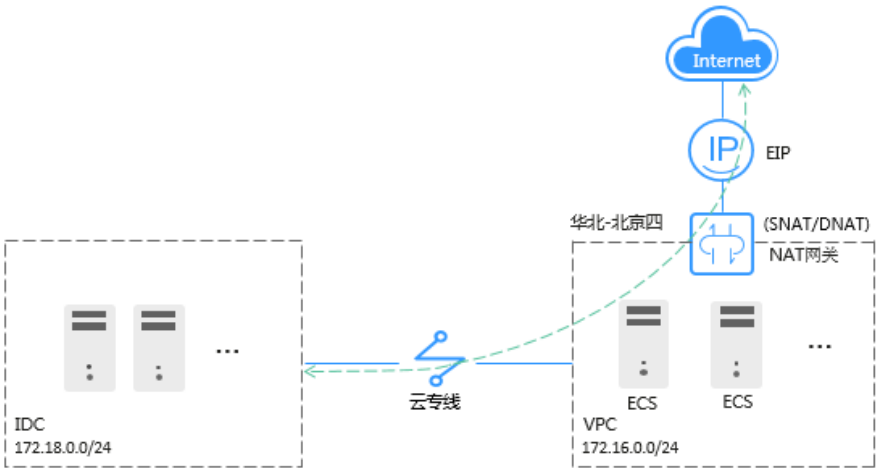
典型拓扑

假设用户IDC网段为172.18.0.0/24，接入VPC区域为“华北-北京四”，VPC子网网段为172.16.0.0/24。

实现方式如下：

1. 通过云专线将用户IDC与VPC连通。
2. 在VPC中搭建公网NAT网关，连通Internet。

图 2-1 组网图



前提条件

- 配置云专线时，需要占用IDC的默认路由，请确保未被使用。
- IDC的网段与云上VPC中的子网网段不能重叠，否则无法通信。

配置步骤

步骤1 创建VPC及子网

具体操作请参见**创建虚拟私有云和子网**。

步骤2 配置云专线

在IDC和“华北-北京四”区域创建云专线。具体操作请参见**通过云专线实现云下IDC访问云上VPC**。

说明

专线开通后，配置本地路由时，需要在云上的本端子网添加0.0.0.0/0网段，可以参照以下两种方式：

- 静态路由模式：需要在IDC侧添加0.0.0.0/0的默认路由指向专线。
- BGP模式：用户本地可通过BGP自动学习到默认路由。

步骤3 购买EIP并配置公网NAT网关

1. 在“华北-北京四”区域购买EIP，具体申请操作请参见**申请弹性公网IP**。
2. 购买公网NAT网关。具体操作请参见**购买公网NAT网关**。
3. 添加SNAT规则，将云专线网段添加到规则中。更多配置SNAT规则信息，请参见**添加SNAT规则**。

   添加云专线网段：172.18.0.0/24，绑定**1**中购买的EIP。

图 2-2 添加 SNAT 规则

4. 添加DNAT规则。更多配置DNAT规则信息，请参见**添加DNAT规则**。
   配置协议及端口信息，此处以“所有端口”为例。添加私网IP：172.18.0.100，绑定EIP。

图 2-3 添加 DNAT 规则

说明

SNAT规则和DNAT规则一般面向不同的业务，如果使用相同的EIP，会面临业务相互抢占问题，请尽量避免。SNAT规则不能和全端口的DNAT规则共用EIP。

----结束

配置验证

配置完成，测试连通性。

从IDC的服务器ping外网地址如：114.114.114.114。

3 基于私网 NAT 网关和云专线的混合云 SNAT

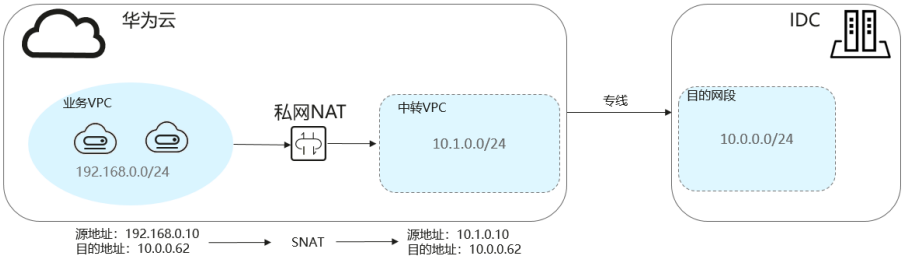
应用场景

VPC中的云主机实例在与用户本地数据中心（IDC）通过云专线进行通信时，需要将VPC中的云主机私网地址转换成IDC信任的私网地址进行通信。

方案架构

1. 通过云专线将用户IDC与中转VPC连通。
2. 配置私网NAT网关，将业务VPC中的ECS私网地址转换成中转VPC中的中转IP（用户IDC信任的私网地址）。

图 3-1 组网图



方案优势

混合云场景中，云上VPC与线下IDC互通时，需要将VPC内云主机实例的私网地址映射为受IDC信任的私网地址，以此来满足安全合规等要求。

约束与限制

- IDC网段与中转VPC、业务VPC中的子网网段都不能重叠，否则无法通信。
- 需要在中转VPC中自定义私网网段，用来为业务VPC中的资源做私网地址映射，一般为用户IDC信任的私网网段或私网地址。

资源和成本规划

表 3-1 资源和成本规划

资源	资源名称	资源说明	数量
虚拟私有云（VPC）	VPC-Test01	业务VPC，VPC子网网段为：192.168.0.0/24。	1
	VPC-Test02	中转VPC，VPC子网网段为：10.1.0.0/24。	1
NAT网关	NAT-Private-Test	购买私网NAT网关，私网NAT网关所在的VPC选择业务VPC（VPC-Test01）。	1
	NAT-Ext-Sub-IP-Test	创建中转IP，中转IP所在的VPC为中转VPC（VPC-Test02），该中转IP地址为：10.1.0.10。	1
云专线	DC-Test	使用云专线将用户IDC和中转VPC连通。	1
弹性云服务器（ECS）	ECS-Test	购买ECS，该ECS所在的VPC选择业务VPC（VPC-Test01），该ECS的私网地址为：192.168.0.10。	1
用户线下数据中心（IDC）	IDC-Test	用户IDC网段为：10.0.0.0/24，其中包含的服务器私网IP为：10.0.0.62。	1

说明

- 在本方案中，将ECS的私网地址192.168.0.10通过私网NAT网关映射为用户IDC信任的私网地址10.1.0.10。
- 本方案所需的VPC、NAT网关、云专线、ECS需在同一区域。

操作流程

1. **创建业务VPC和中转VPC**
2. **配置云专线**
3. **购买并配置私网NAT网关**

实施步骤

步骤1 创建业务VPC和中转VPC

具体操作请参见**创建虚拟私有云和子网**。

步骤2 配置云专线

在IDC和中转VPC所在的区域之间创建云专线。具体操作请参见**通过云专线实现云下IDC访问云上VPC**。

步骤3 购买并配置私网NAT网关

1. 在指定区域购买私网NAT网关，选定业务VPC。
2. 创建中转IP，中转VPC选择VPC-Test02，中转IP选择手动分配，**IP地址为：10.1.0.10**。
3. 进入到上述购买的私网NAT网关的“SNAT规则”页签，单击“添加SNAT规则”，子网选择业务VPC中需要做地址映射的**子网（网段为：192.168.0.0/24）**，中转IP选择上述创建好的。
4. 在业务VPC中添加指向私网NAT网关的路由，**目的地址配置为IDC的网段（目的网段：10.0.0.0/24）**。

图 3-2 添加路由

5. 在目的网段包含的**服务器（私网地址为：10.0.0.62）**中添加入方向安全组规则，用于将发到目的端的流量全部放通。

----结束

配置验证

配置完成，测试连通性。

登录业务VPC中的ECS（ECS-Test），ping对端IDC（目的网段）中的私网IP（10.0.0.62）。

```
[root@ecs-zwq ~]# ping 10.0.0.62
PING 10.0.0.62 (10.0.0.62) 56(84) bytes of data.
64 bytes from 10.0.0.62: icmp_seq=1 ttl=64 time=1.08 ms
64 bytes from 10.0.0.62: icmp_seq=2 ttl=64 time=0.507 ms
64 bytes from 10.0.0.62: icmp_seq=3 ttl=64 time=0.455 ms
```

4 基于私网 NAT 网关和云专线实现混合云互通

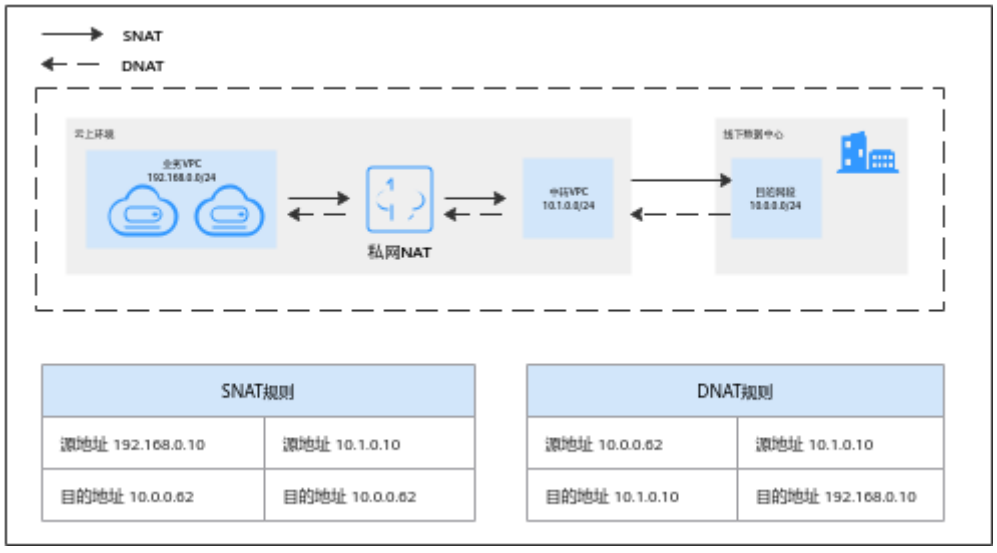
应用场景

在企业混合云架构中，当云上VPC中的云服务器需要与用户本地数据中心（IDC）进行通信时，如果云上VPC的私网地址不是IDC信任分的私网地址，将会导致通信失败。您可以通过配置NAT网关，结合云专线（或VPN）服务实现云上VPC与云下IDC的混合云互通。

方案架构

1. 通过云专线（或VPN）将用户IDC与中转VPC连通。
2. 配置私网NAT网关，使用SNAT（DNAT）规则将源地址（目的地址）转换成中转VPC中的中转IP（用户IDC信任的私网地址）。

图 4-1 组网图



方案优势

混合云场景中，云上VPC与线下IDC互通时，需要将VPC内云主机实例的私网地址映射为受IDC信任的私网地址，以此来满足安全合规等要求。

约束与限制

- IDC网段与中转VPC、业务VPC中的子网网段都不能重叠，否则无法通信。
- 需要在中转VPC中自定义私网网段，用来为业务VPC中的资源做私网地址映射，一般为用户IDC信任的私网网段或私网地址。

资源和成本规划

表 4-1 资源和成本规划

资源	资源名称	资源说明	数量
虚拟私有云（VPC）	VPC-Test01	业务VPC，VPC子网网段为：192.168.0.0/24。	1
	VPC-Test02	中转VPC，VPC子网网段为：10.1.0.0/24。	1
NAT网关	NAT-Private-Test	购买私网NAT网关，私网NAT网关所在的VPC选择业务VPC（VPC-Test01）。	1
	NAT-Ext-Sub-IP-Test	创建中转IP，中转IP所在的VPC为中转VPC（VPC-Test02），该中转IP地址为：10.1.0.10。	1
云专线	DC-Test	使用云专线将用户IDC和中转VPC连通。	1
弹性云服务器（ECS）	ECS-Test	购买ECS，该ECS所在的VPC选择业务VPC（VPC-Test01），该ECS的私网地址为：192.168.0.10。	1
用户线下数据中心（IDC）	IDC-Test	用户IDC网段为：10.0.0.0/24，其中包含的服务器私网IP为：10.0.0.62。	1

说明

- 在本方案中，将ECS的私网地址192.168.0.10通过私网NAT网关映射为用户IDC信任的私网地址10.1.0.10。
- 本方案所需的VPC、NAT网关、云专线、ECS需在同一区域。

操作步骤

步骤1 创建业务VPC和中转VPC

具体操作请参见**创建虚拟私有云和子网**。

步骤2 配置云专线（或VPN）

在IDC和中转VPC所在的区域之间创建云专线。具体操作请参见**配置云专线**。

步骤3 购买并配置私网NAT网关

在指定区域购买私网NAT网关，选定业务VPC。具体操作请参见**购买私网NAT网关**。

步骤4 创建中转IP

中转VPC选择VPC-Test02，中转IP选择手动分配，**IP地址为：10.1.0.10**。

步骤5 添加SNAT规则

进入到上述购买的私网NAT网关的“SNAT规则”页签，单击“添加SNAT规则”，子网选择业务VPC中需要做地址映射的**子网（网段为：192.168.0.0/24）**，中转IP选择上述步骤**步骤4**创建好的中转IP。

步骤6 添加DNAT规则

进入到上述购买的私网NAT网关的“DNAT规则”页签，单击“添加DNAT规则”，本端网络的实例类型选择**服务器（私网地址为：192.168.0.10）**，中转网络的中转IP选择上述步骤**步骤4**创建好的中转IP。更多配置详情请参见**添加DNAT规则**。

步骤7 配置路由

1. 在业务VPC中添加指向私网NAT网关的路由，**目的地址配置为IDC的网段（目的网段：10.0.0.0/24）**。
2. 在目的网段包含的**服务器（私网地址为：10.0.0.62）**中添加入方向安全组规则，用于将发到目的端的流量全部放通。

----结束

配置验证

配置完成，测试连通性。

登录业务VPC中的ECS（ECS-Test），ping对端IDC（目的网段）中的私网IP（10.0.0.62）。

```
[root@ecs-zwq ~]# ping 10.0.0.62
PING 10.0.0.62 (10.0.0.62) 56(84) bytes of data.
64 bytes from 10.0.0.62: icmp_seq=1 ttl=64 time=1.08 ms
64 bytes from 10.0.0.62: icmp_seq=2 ttl=64 time=0.507 ms
64 bytes from 10.0.0.62: icmp_seq=3 ttl=64 time=0.455 ms
```


5 基于公网 NAT 网关和 VPC 对等连接实现跨 VPC 访问公网和对公网提供服务

操作场景

在同一区域下有两个虚拟私有云分别为VPC A和VPC B，VPC A和VPC B对应的子网是subnet A和subnet B。在VPC A中为子网subnet A创建公网NAT网关，通过添加SNAT和DNAT规则可以实现访问公网和对公网提供服务；在VPC B中子网subnet B通过对等连接连通VPC A中的子网subnet A，使用subnet A的公网NAT网关访问公网和对公网提供服务，VPC B中的subnet B不用另配置公网NAT网关。

方案优势

两个VPC只需要配置一个公网NAT网关可以实现两个VPC下的云服务器都能访问公网和对公网提供服务，达到节省资源的目的。

典型拓扑

假设VPC A的网段为192.168.0.0/16，子网subnet A的网段为192.168.1.0/24；VPC B的网段为192.168.0.0/16，子网subnet B的网段为192.168.2.0/24。

实现方式如下：

1. 配置NAT网关。在VPC A创建公网NAT网关，并添加SNAT和DNAT规则。
2. 创建对等连接。通过对等连接将VPC A中的子网subnet A与VPC B中的子网subnet B连通，使subnet B使用公网NAT网关访问公网和对公网提供服务。

前提条件

- 如果两个VPC的网段有重叠，建立对等连接时，只能针对子网建立对等关系。
- 两个VPC中的全部子网网段不能重叠，否则无法通信。

配置公网 NAT 网关

步骤1 购买公网NAT网关

购买公网NAT网关，虚拟私有云选择VPC A。具体操作请参见**购买公网NAT网关**。

步骤2 添加SNAT规则

1. 为subnet A添加SNAT规则，使用场景选择“虚拟私有云”，子网选择subnet A。具体操作请参见**添加SNAT规则**。

图 5-1 添加 SNAT 规则

2. 为subnet B添加SNAT规则，使用场景选择“云专线/云连接”，网段填写subnet B网段。

图 5-2 添加 SNAT 规则

步骤3 添加DNAT规则

1. 为subnet A添加DNAT规则，使用场景选择“虚拟私有云”，私网IP填写subnet A中的云服务器IP地址。具体操作请参见**添加DNAT规则**。

图 5-3 添加 DNAT 规则

2. 为subnet B添加DNAT规则，使用场景选择“云专线/云连接”，私网IP填写subnet B中的云服务器IP地址。

图 5-4 添加 DNAT 规则

----结束

创建对等连接

步骤1 创建VPC A和VPC B及其对应的子网subnet A和subnet B

具体操作请参见**创建虚拟私有云和子网**。

步骤2 创建对等连接

在subnet A和subnet B间创建对等连接。具体操作请参见**创建对等连接**。

说明

在本实践中，本端VPC是VPC A，对端VPC是VPC B。

在原有添加本端和对端路由的基础上，还需在VPC B的路由表中添加0.0.0.0/0的对端路由（下一跳选择已创建的对等连接）。

----结束

测试对等连接的连通性

配置完成，测试连通性。

登录subnet B中的云服务器，ping公网地址。

```
[root@ecs-2670 ~]# ping www.baidu.com
PING www.a.shifen.com (14.215.177.39) 56(84) bytes of data.
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=1 ttl=54 time=5.74 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=2 ttl=54 time=5.44 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=3 ttl=54 time=5.33 ms
^C
--- www.a.shifen.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 5.332/5.507/5.742/0.182 ms
```

登录任一不属于VPC A和VPC B且能访问公网的云服务器，curl子网subnet B对应DNAT规则绑定的弹性公网IP。

```
[root@ecs-cf5f ~]# curl
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a>
<li><a href=".bash_logout">.bash_logout</a>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".bashrc">.bashrc</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
<li><a href=".tcshrc">.tcshrc</a>
</ul>
<hr>
</body>
</html>
[root@ecs-cf5f ~]# curl
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a>
<li><a href=".bash_logout">.bash_logout</a>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".bashrc">.bashrc</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
<li><a href=".tcshrc">.tcshrc</a>
</ul>
<hr>
</body>
</html>
[root@ecs-cf5f ~]#
```

6 使用私网 NAT 网关服务实现 IDC 网段免修改上云

6.1 方案概述

应用场景

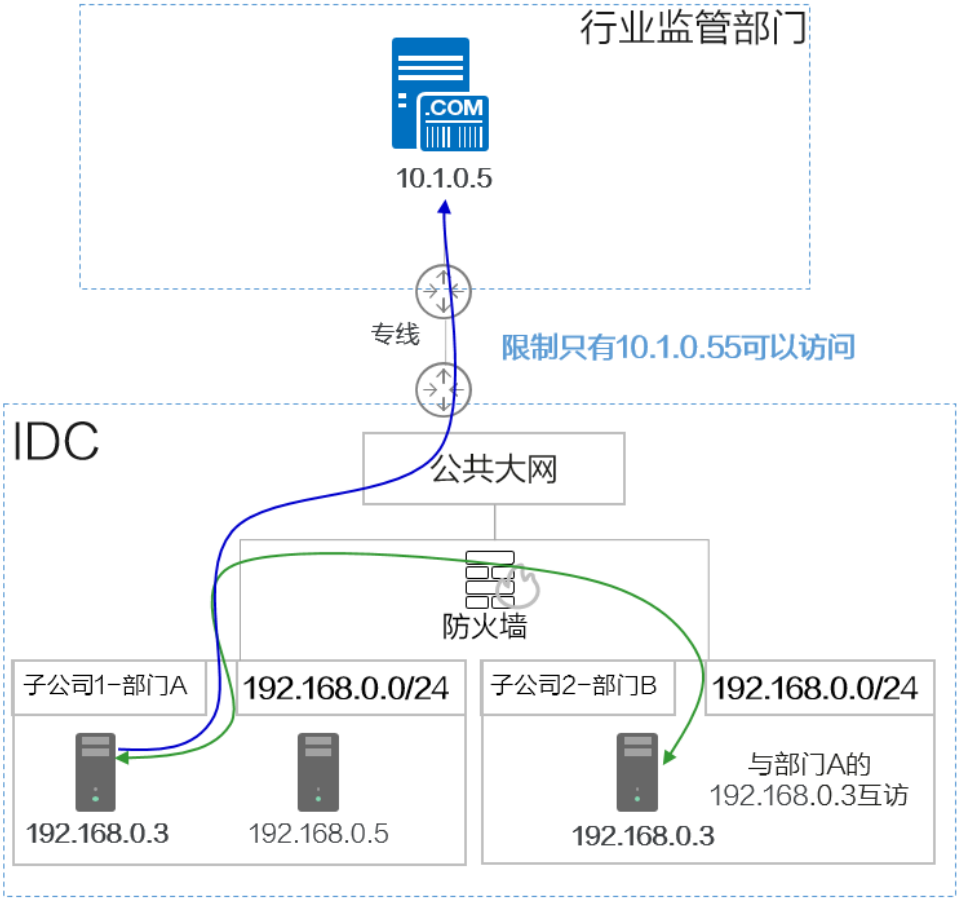
- 在不改变现有IDC网络组织架构的前提下，需要将网络组织架构迁移上云，并实现IDC中的两个重叠网段内的主机相互访问。
- 在不改变现有IDC网络组织架构的前提下，需要将网络组织架构迁移上云，并实现以IDC中指定IP地址访问外部资源。

例如：

某大型公司拥有多个分公司，分公司之间网段独立规划、存在重叠子网。如图6-1，部门A和部门B分配了相同的192.168.0.0/24网段，并且两个网段内的主机可以相互访问；另外，根据行业规范要求，部门A需要定期以指定的IP地址访问行业监管部门的主机归档数据。

IDC内业务复杂且庞大，重新规划并整改网段会影响已有业务的正常运行。客户希望能够保持现有网络规划不变，网段免修改上云，上云后重叠子网的主机仍能相互访问，且部门A的主机仍然可以以指定IP地址访问行业监管部门的主机。

图 6-1 子公司间的网络存在子网重叠



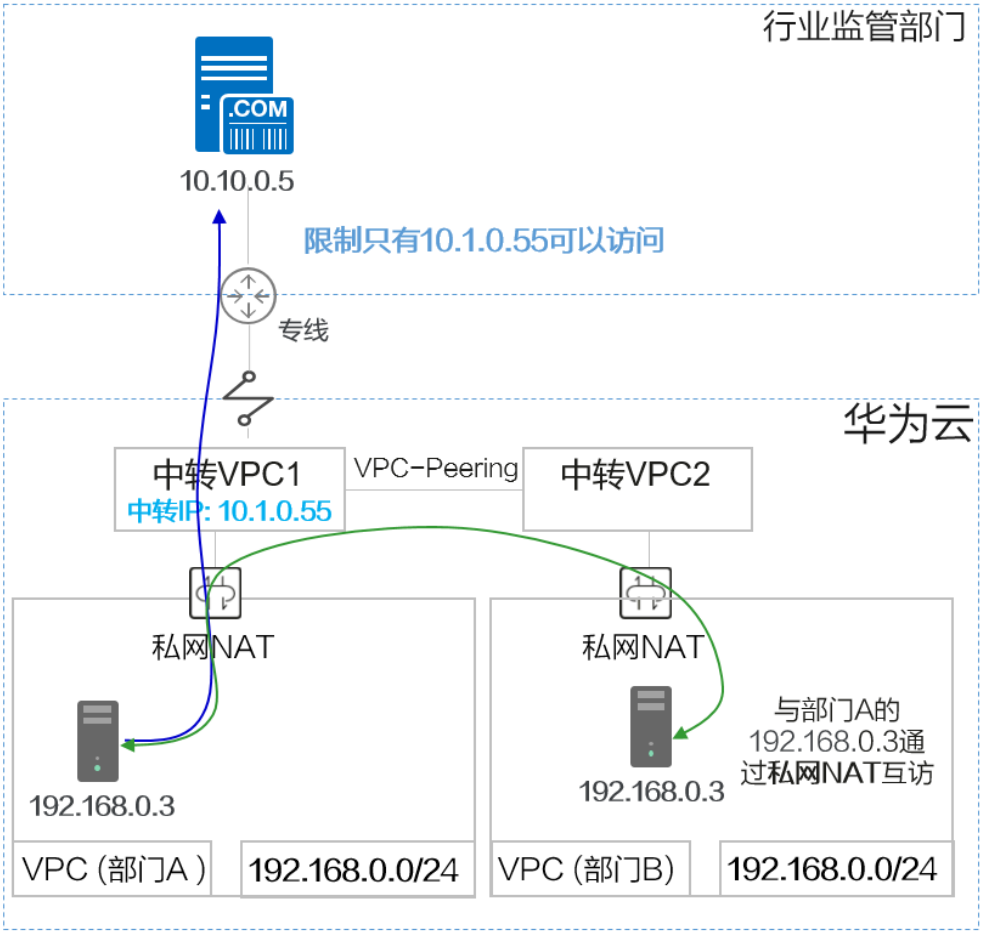
方案架构

华为云私网NAT网关（Private NAT Gateway）能够为虚拟私有云（Virtual Private Cloud）内的云主机提供网络地址转换服务，实现重叠子网VPC内的主机互访以及主机私网地址映射。弥补了VPC对等连接服务中**有重叠子网网段的VPC，不能使用VPC对等连接**的约束限制。

如**图6-2**：

- 将部门A和部门B的192.168.0.0/24网段直接迁移到云上的VPC内，然后使用私网NAT网关实现两个部门的主机相互访问。
- 同时可以通过配置SNAT规则，将部门A的主机私网地址映射为指定的IP地址10.1.0.55访问外部主机。

图 6-2 华为云私网 NAT 服务



方案优势

- 客户不用改造现有网络组织架构，直接将云下IDC业务迁移上云，节省了网络改造的成本。
- 解决了重叠私网IP地址的主机无法相互访问的问题。
- 满足了客户对安全性的要求，可以为私网内的主机指定IP地址访问外部资源。

约束与限制

使用私网NAT网关时，您需要注意以下几点：

- 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。
- VPC内的每个子网只能添加一条SNAT规则。
- SNAT规则和DNAT规则不能共用同一个中转IP。
- DNAT的全端口模式不能和具体端口模式共用同一个中转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。

6.2 云上重叠子网间主机互访

应用场景

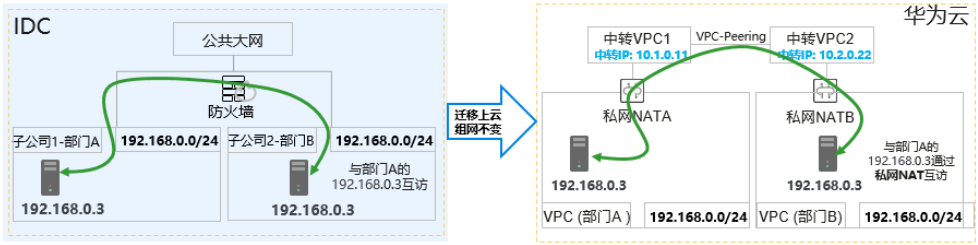
在不改变现有IDC网络组织架构的前提下，需要将网络组织架构迁移上云，并实现IDC中的两个重叠网段内的主机相互访问。

本最佳实践模拟IDC中两个子网重叠的部门，不修改网段直接迁移上云，并且迁移上云后两个部门（重叠子网）能够继续互相访问。

方案架构

- IDC的两个子公司的部门A和部门B均使用192.168.0.0/24网段。网段免修改，直接在云上创建相同网段的VPC。
- 分别为两个子公司的VPC创建私网NAT网关，为部门A的主机（192.168.0.3）和部门B的主机（192.168.0.3）分别映射10.1.0.11和10.2.0.22两个中转IP地址，通过中转IP实现两个主机相互访问。

图 6-3 最佳实践逻辑拓扑



说明

请注意手动配置如下几条路由信息，避免漏配置导致流量不通。

1. VPC（部门A）到私网NATA
2. 中转VPC1到VPC-Peering
3. 中转VPC2到VPC-Peering
4. VPC（部门B）到私网NATB

方案优势

IDC网段免修改直接上云，极大降低用户上云难度。

资源和成本规划

表 6-1 资源和成本规划

资源	名称	规划网段/IP	子网名称	说明
VPC（华北-北京四）	vpc-部门A	192.168.0.0/24	subnet-A	部门A迁移到云上的VPC。
	vpc-部门B	192.168.0.0/24	subnet-B	部门B迁移到云上的VPC。
	vpc-中转1	10.1.0.0/24	ext_sub_T1	部门A的私网NAT网关所需的中转VPC。
	vpc-中转2	10.2.0.0/24	ext_sub_T2	部门B的私网NAT网关所需的中转VPC。
中转IP（vpc-中转）	中转IP-部门A	10.1.0.11	-	部门A对外提供服务的IP地址，部门B通过此IP地址可以访问部门A的主机。
	中转IP-部门B	10.2.0.22	-	部门B对外提供服务的IP地址，部门A通过此IP地址可以访问部门B的主机。
弹性云服务器（华北-北京四）	ecs-部门A	192.168.0.3	-	部门A的主机，可以和部门B互相访问。
	ecs-部门B	192.168.0.3	-	部门B的主机，可以和部门A互相访问。
私网NAT网关	private-nat-A	-	-	为部门A配置的私网NAT网关，所属VPC为vpc-部门A。
	private-nat-B	-	-	为部门B配置的私网NAT网关，所属VPC为vpc-部门B。

前提条件

- 已拥有华为云账号，并且华为云账号已实名认证。
- 华为云账号未欠费，并且有足够的金额可以购买本最佳实践所涉及的资源。
- 已完成私网NAT网关创建。

操作流程

1. **创建VPC**
2. **创建弹性云服务器**
3. **创建中转IP**
4. **创建私网NAT网关并配置转换规则**
5. **配置主机到私网NAT网关的路由信息**

6. **配置中转VPC1到中转VPC2的对等连接**
7. **验证部门A和部门B内的主机相互访问**

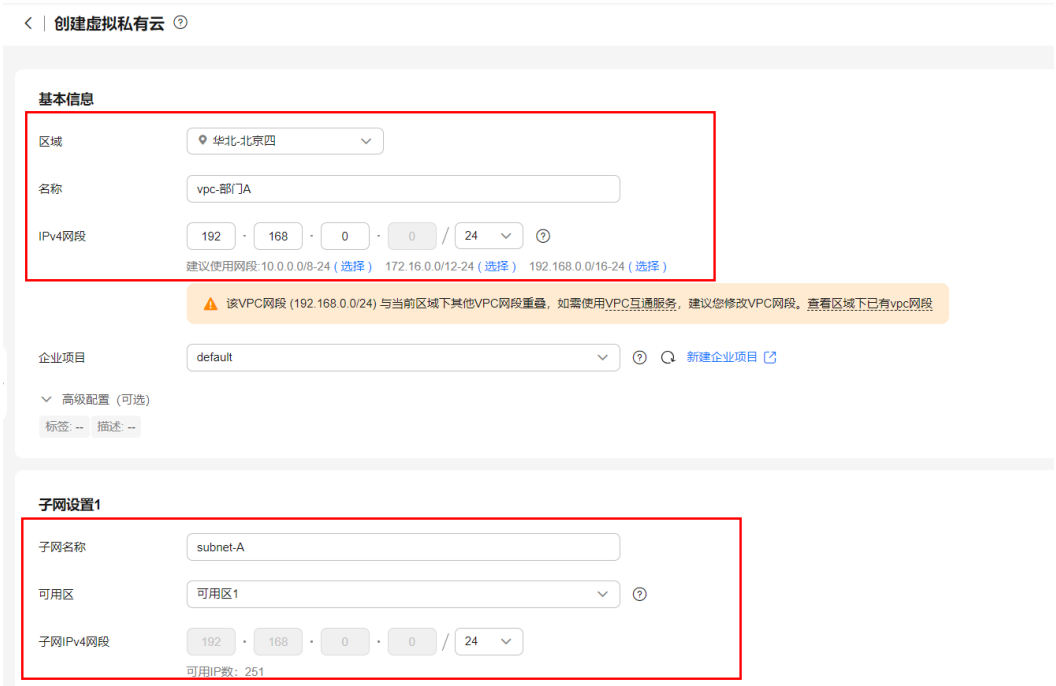
创建 VPC

步骤1 进入**创建虚拟私有云页面**。

步骤2 在“创建虚拟私有云”页面，根据**表6-1**配置部门A的VPC，完成后单击“立即创建”。

- 区域：选择华北-北京四
- 名称：vpc-部门A
- IPv4网段：192.168.0.0/24
- 可用区：可用区1
- 子网名称：subnet-A
- 子网IPv4网段：保持默认
- 未提及参数，保持默认或根据界面引导配置

图 6-4 创建虚拟私有云



步骤3 重复以上步骤，参考**表6-1**规划，创建所有需要的VPC。

- 区域：选择华北-北京四
- 名称：vpc-部门B
- IPv4网段：192.168.0.0/24
- 可用区：可用区1
- 子网名称：subnet-B
- 子网IPv4网段：保持默认
- 未提及参数，保持默认或根据界面引导配置

图 6-5 创建所需 VPC

----结束

创建弹性云服务器

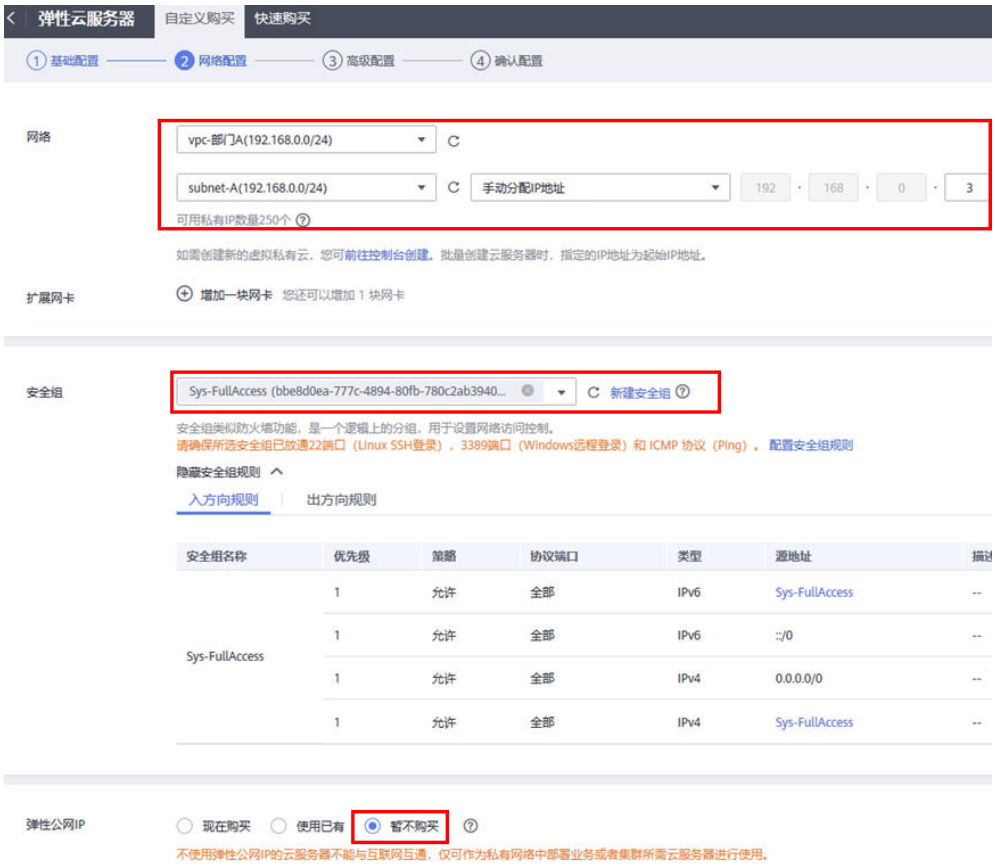
步骤1 选择“计算 > 弹性云服务器”，单击“购买弹性云服务器”。

步骤2 在“购买弹性云服务器”页面，根据表6-1配置部门A的弹性云服务器的基础信息，完成后单击“下一步：网络配置”。

- 计费模式：按需计费
- 区域：选择华北-北京四
- 规格：用户自定义。本实践以c6.large.2举例。
- 镜像：公共镜像。具体镜像用户自定义，本实践以CentOS 8.0举例。
- 未提及参数，保持默认或根据界面引导配置

步骤3 配置部门A的ECS的网络信息。

- 网络：选择部门A的VPC“vpc-部门A”，并选择“手动分配IP地址”，指定IP地址为**表6-1**规划的ecs-部门A的IP地址“192.168.0.3”。
- 安全组：Sys-FullAccess。本实践选择一个全部放通的安全组作为测试安全组，后期可以根据业务情况重新绑定业务所需的安全组，提升业务安全性。
- 弹性公网IP：暂不购买
- 未提及参数，保持默认或根据界面引导配置



步骤4 配置完成后单击“下一步：高级配置”。

步骤5 设置云服务器名称和密码等信息。

- 云服务器名称：ecs-部门A
- 登录凭证：密码；并输入密码。
- 未提及参数，保持默认或根据界面引导配置。

步骤6 设置完成后单击“下一步：确认配置”。

步骤7 确认ECS信息无误后，勾选“协议”并单击“立即购买”，完成部门A的ECS创建。

步骤8 单击弹性云服务器总览页面所在行的“远程登录”，选择VNC方式登录。

步骤9 使用root账号登录ECS，并执行如下命令查询ECS的私网IP地址是否为规划的IP地址。

```
ifconfig
```



```
ecs-a login: root
Password:

        Welcome to Huawei Cloud Service

[root@ecs-a ~]# TMOUT=0
[root@ecs-a ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.3  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::f816:3eff:fe9e:9c0b  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:9e:9c:0b  txqueuelen 1000  (Ethernet)
        RX packets 296  bytes 72067 (70.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 394  bytes 55175 (53.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-a ~]# _
```

步骤10 重复**步骤1**~**9**，完成其他已规划的ECS的创建。

----结束

创建中转 IP

步骤1 选择“网络 > NAT网关”，选择“私网NAT网关”，切换至“中转IP”页签。

步骤2 单击“创建中转IP”，进入“中转IP”页面。

步骤3 在“中转IP”弹窗，根据**表6-1**为部门A创建中转IP。

- 中转VPC：vpc-中转1·
- 中转子网：ext_sub_T1
- 中转IP：手动分配
- IP地址：10.1.0.11

步骤4 设置完成后，单击“确定”。

步骤5 重复**1**~**4**，参数按照如下设置，为部门B创建中转IP（10.2.0.22）。

- 中转VPC：vpc-中转2
- 中转子网：ext_sub_T2
- 中转IP：手动分配
- IP地址：10.2.0.22

----结束

创建私网 NAT 网关并配置转换规则

步骤1 在私网NAT网关页面，单击“购买私网NAT网关”。

步骤2 为部门A创建私网NAT网关配置参数。

- 区域：华北-北京四
- 名称：private-nat-A
- 虚拟私有云：vpc-部门A
- 未提及参数，保持默认或根据界面引导配置

步骤3 配置完成后，单击“立即购买”。

步骤4 在私网NAT网关列表页签，单击需要添加DNAT规则的私网NAT网关名称。

步骤5 切换至“DNAT规则”页签，单击“添加DNAT规则”。

步骤6 配置部门A的DNAT规则参数，完成后单击“确定”。

- 端口类型：所有端口
- 中转子网：ext_sub_T1
- 中转IP：10.1.0.11
- 实例类型：选择服务器，并选择部门A的ECS。

步骤7 返回私网NAT网关页面，并单击“购买私网NAT网关”。

步骤8 为部门B创建私网NAT网关配置参数。

- 区域：华北-北京四
- 名称：private-nat-B
- 虚拟私有云：vpc-部门B
- 未提及参数，保持默认或根据界面引导配置

步骤9 配置完成后单击“立即购买”。

步骤10 在私网NAT网关列表页签，单击需要添加DNAT规则的私网NAT网关名称。

步骤11 切换至“DNAT规则”页签，单击“添加DNAT规则”。

步骤12 配置部门B的DNAT规则参数，完成后单击“确定”。

- 端口类型：所有端口
- 中转子网：ext_sub_T2
- 中转IP：10.2.0.22
- 实例类型：选择服务器，并选择部门B的ECS。

----结束

配置主机到私网 NAT 网关的路由信息

步骤1 选择“网络 > 虚拟私有云”，在左侧导航栏选择“路由表”。

步骤2 进入路由表列表页面，单击“rtb-vpc-部门A”的名称，在基本信息页面单击“添加路由”。

步骤3 配置部门A的主机访问部门A的私网NAT网关的路由，单击“确认”。

- 目的地址：设置为0.0.0.0/0（实际操作时也可根据业务需要设置指定目的地址。）
- 下一跳类型：NAT网关
- 下一跳：系统自动关联出部门A的私网NAT网关

步骤4 配置完成后返回路由表列表页面，单击“rtb-vpc-部门B”，单击“添加路由”。

步骤5 配置部门B的主机访问部门B的私网NAT网关的路由，单击“确认”。

- 目的地址：设置为0.0.0.0/0

- 下一跳类型：NAT网关
- 下一跳：系统自动关联出部门B的私网NAT网关

----结束

配置中转 VPC1 到中转 VPC2 的对等连接

步骤1 选择“网络 > 虚拟私有云”，在左侧导航栏选择“对等连接”。

步骤2 进入对等连接列表页面，单击“创建对等连接”。

步骤3 配置中转VPC1和中转VPC2分别作为本端VPC和对端VPC，完成后单击“确定”。

- 名称：peering-TtoT
- 本端VPC：vpc-中转1
- 对端VPC：vpc-中转2
- 未提及参数，保持默认或根据界面引导配置

步骤4 返回到对等连接列表页面，并单击左侧导航栏的“路由表”。

步骤5 单击“rtb-vpc-中转1”的名称，在基本信息页面单击“添加路由”。

步骤6 配置中转VPC1到VPC-Peering的路由，单击“确认”。

- 目的地址：设置为0.0.0.0/0
- 下一跳类型：对等连接
- 下一跳：系统自动关联对等连接实例

步骤7 重复5~6，选择“rtb-vpc-中转2”并配置中转VPC2到VPC-Peering的路由。

----结束

验证部门 A 和部门 B 内的主机相互访问

步骤1 选择“计算 > 弹性云服务器”，并使用VNC方式登录“ecs-部门A”和“ecs-部门B”2台主机。

步骤2 在“ecs-部门A”主机上，执行如下命令，验证主机可以访问部门B的主机。

```
ping 10.2.0.22
```



```
[root@ecs-a ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.3  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::f816:3eff:feaa:ff9  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:aa:0f:f9  txqueuelen 1000  (Ethernet)
        RX packets 1317  bytes 436261 (426.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1439  bytes 325449 (317.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-a ~]# ping 10.2.0.22
PING 10.2.0.22 (10.2.0.22) 56(84) bytes of data.
64 bytes from 10.2.0.22: icmp_seq=1 ttl=64 time=0.894 ms
64 bytes from 10.2.0.22: icmp_seq=2 ttl=64 time=0.600 ms
^C
--- 10.2.0.22 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 0.600/0.747/0.894/0.147 ms
```

步骤3 在“ecs-部门B”主机上，执行如下命令，验证主机可以访问部门A的主机。

```
ping 10.1.0.11
```

```
[root@ecs-b ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.3  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::f816:3eff:febf:8dcc  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:bf:8d:cc  txqueuelen 1000  (Ethernet)
        RX packets 1320  bytes 435434 (425.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1440  bytes 325139 (317.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-b ~]# ping 10.1.0.11
PING 10.1.0.11 (10.1.0.11) 56(84) bytes of data.
64 bytes from 10.1.0.11: icmp_seq=1 ttl=64 time=0.913 ms
64 bytes from 10.1.0.11: icmp_seq=2 ttl=64 time=0.642 ms
64 bytes from 10.1.0.11: icmp_seq=3 ttl=64 time=0.704 ms
^C
--- 10.1.0.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 52ms
rtt min/avg/max/mdev = 0.642/0.753/0.913/0.115 ms
```

至此重叠子网内的主机通过私网NAT网关服务实现相互访问的最佳实践配置完成。

----结束

6.3 云上指定 IP 地址访问 VPC 外主机

应用场景

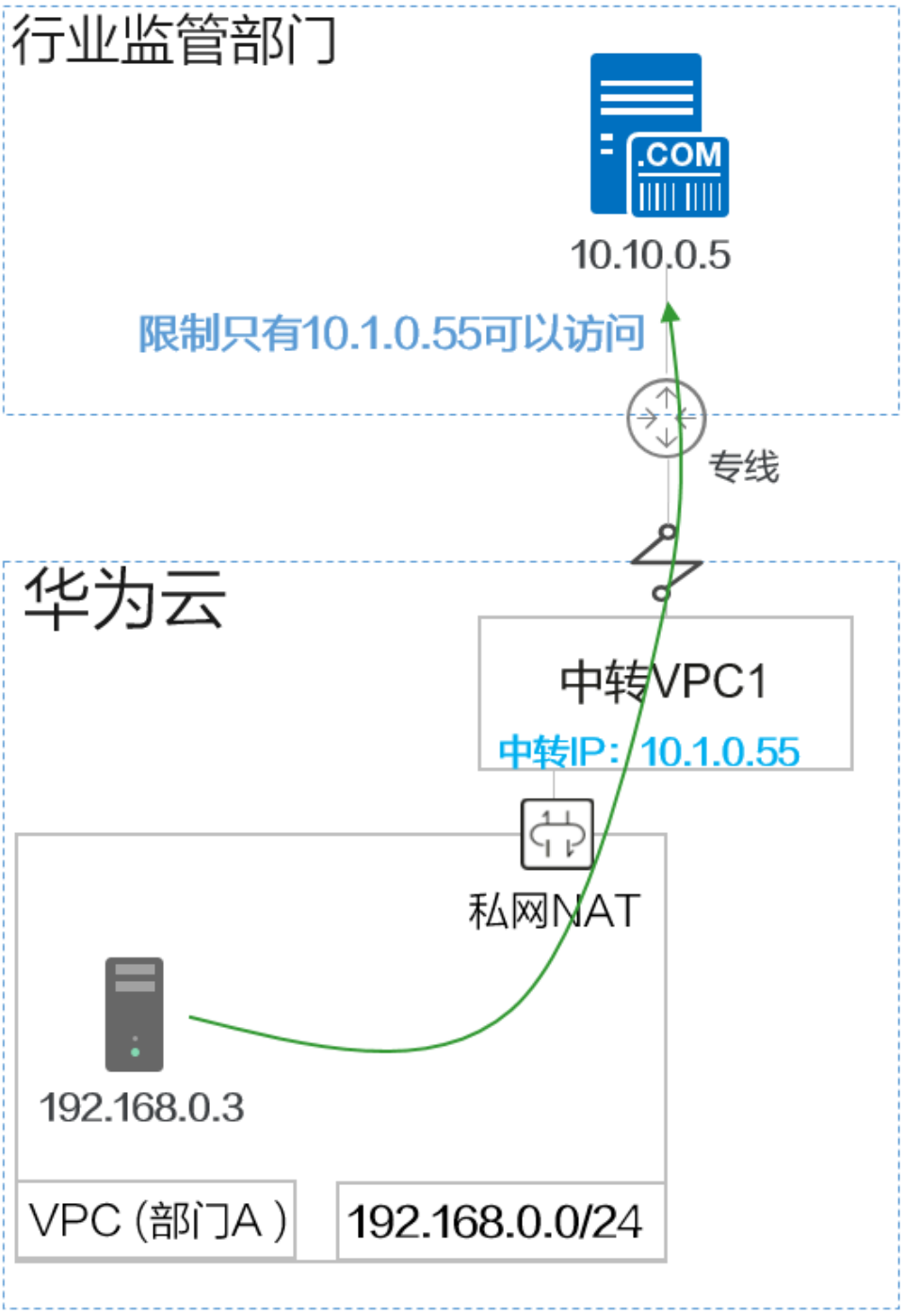
在不改变现有IDC网络组织架构的前提下，需要将网络组织架构迁移上云，**并实现以IDC中指定IP地址访问外部资源**。

在本最佳实践中，根据行业监管部门的要求，业务上云之后仍需要部门A定期以指定的IP地址（10.1.0.55）访问行业监管部门的主机，上传必要的监管数据。

方案架构

- 监管部门限定只有特定的IP地址（10.1.0.55）的主机可以访问。
- 部门A内的主机（192.168.0.3）通过私网NAT网关，将私有IP地址转换为规定的IP地址（10.1.0.55），定期访问行业监管部门的主机（10.10.0.5）。

图 6-6 最佳实践逻辑拓扑



方案优势

灵活指定IP地址，VPC内所有主机可以共用此IP访问VPC外主机。

资源和成本规划

表 6-2 资源和成本规划

资源	名称	规划网段/IP	子网名称	说明
VPC（华北-北京四）	vpc-部门A	192.168.0.0/24	subnet-A	部门A迁移到云上的VPC。
	vpc-中转1	10.1.0.0/24	ext_sub_T1	私网NAT网关所需的中转VPC。
	vpc-监管	10.10.0.0/24	subnet-W	模拟监管部门的VPC。
弹性云服务器（华北-北京四）	ecs-部门A	192.168.0.3	--	部门A的主机，可以访问行业监管部门的主机。
	ecs-监管	10.10.0.5	--	模拟监管部门的主机。
中转IP（vpc-中转1）	部门A中转IP	10.1.0.55	--	部门A主机通过监管部门分配的IP地址访问监管部门的主机。

前提条件

- 已拥有华为云账号，并且华为云账号已实名认证。
- 华为云账号未欠费，并且有足够的金额可以购买本最佳实践所涉及的资源。
- 已完成私网NAT网关创建。
- 已完成**云上重叠子网间主机互访**操作。

操作流程

1. **创建VPC**
2. **创建安全组**
3. **创建弹性云服务器**
4. **配置私网NAT网关**
5. **配置VPC对等连接**
6. **配置路由**
7. **验证部门A访问监管部门**

创建 VPC

步骤1 登录华为云管理控制台，并选择“华北-北京四”区域。

步骤2 选择“网络 > 虚拟私有云”，单击“创建虚拟私有云”。

步骤3 根据**表6-2**配置监管部门的VPC，单击“立即创建”。

- 区域：选择华北-北京四

- 名称：vpc-监管
- IPv4网段：10.10.0.0/24
- 可用区：可用区1
- 名称：subnet-W
- 子网IPv4网段：保持默认
- 未提及参数，保持默认或根据界面引导配置

----结束

创建安全组

步骤1 选择“网络 > 虚拟私有云”，选择“访问控制 > 安全组”，单击“创建安全组”。

步骤2 配置安全组信息，完成后单击“确定”。

- 名称：sg-监管
- 模板：通用Web服务器
- 未提及参数，保持默认或根据界面引导配置

步骤3 在安全组列表页，单击操作列的“配置规则”，切换至“入方向规则”页签，删除当前的所有规则。

步骤4 单击“添加规则”，设定只有10.1.0.55的IP才能访问监管部门的主机，配置完成后单击“确定”。

- 优先级：1
- 策略：允许
- 协议端口：全部放通。
- 类型：IPv4
- 源地址：10.1.0.55

----结束

创建弹性云服务器

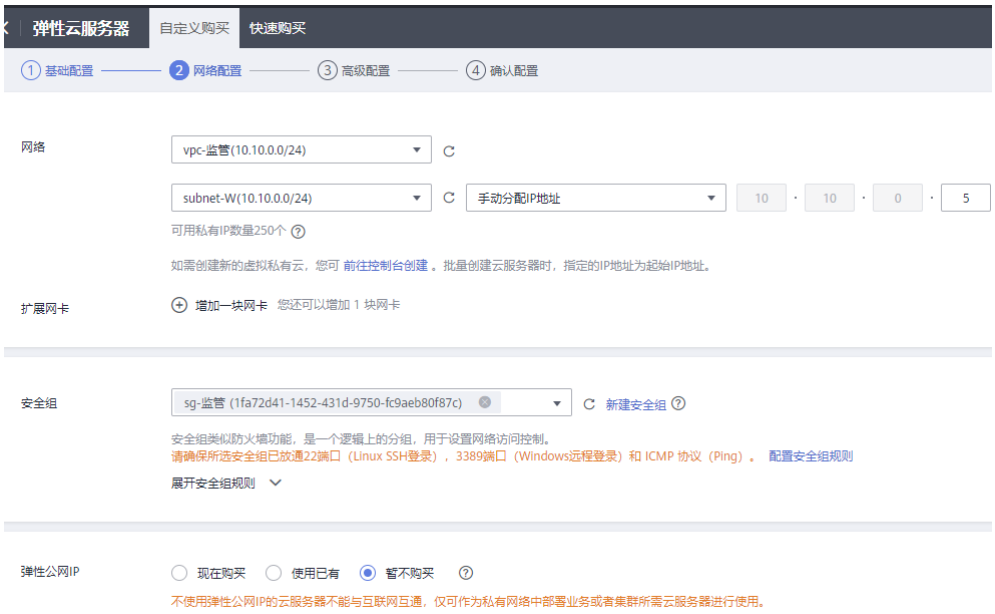
步骤1 选择“计算 > 弹性云服务器”，单击“购买弹性云服务器”。

步骤2 根据表6-2配置监管部门的弹性云服务器的基础信息，完成后单击“下一步：网络配置”。

- 计费模式：按需计费
- 区域：选择华北-北京四
- 规格：用户自定义。本实践以c6.large.2举例。
- 镜像：公共镜像，具体镜像用户自定义。本实践以CentOS 8.0举例。
- 未提及参数，保持默认或根据界面引导配置

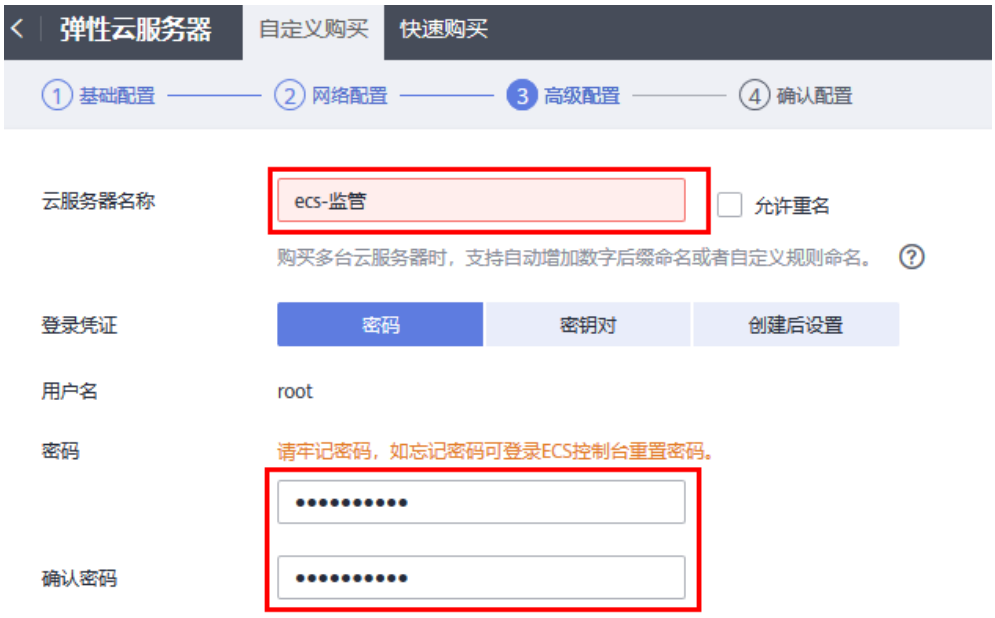
步骤3 配置监管部门ECS的网络信息，完成后单击“下一步：高级配置”。

- 网络：选择“vpc-监管”，并选择“手动分配IP地址”，指定IP地址为表6-2规划的ecs-监管的IP地址“10.10.0.5”。
- 安全组：sg-监管。
- 弹性公网IP：暂不购买
- 未提及参数，保持默认或根据界面引导配置



步骤4 设置云服务器名称和密码等信息，完成后单击“下一步：确认配置”。

- 云服务器名称：ecs-监管
- 登录凭证：密码，并输入密码。
- 未提及参数，保持默认或根据界面引导配置



步骤5 确认ECS信息无误后，勾选“协议”并单击“立即购买”，完成ECS创建。

步骤6 单击弹性云服务器总览页面所在行的“远程登录”，选择VNC方式登录。

步骤7 使用root账号登录ECS，并执行如下命令查询ECS的私网IP地址是否为规划的IP地址。

ifconfig

```
ecs login: root
Password:

        Welcome to Huawei Cloud Service

[root@ecs ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.0.5  netmask 255.255.255.0  broadcast 10.10.0.255
        inet6 fe80::f816:3eff:fefd:d4f5  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:fd:d4:f5  txqueuelen 1000  (Ethernet)
        RX packets 150  bytes 29171 (28.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 238  bytes 25575 (24.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

----结束

配置私网 NAT 网关

创建中转IP

步骤1 选择“网络 > NAT网关”，选择“私网NAT网关”，切换至“中转IP”页签。

步骤2 单击“创建中转IP”，按照如下参数设置。

- 中转VPC：vpc-中转1
- 中转子网：ext_sub_T1
- 中转IP：手动分配
- IP地址：10.1.0.55

步骤3 返回私网NAT网关页面，切换至“私网NAT网关”页签，并单击“private-nat-A”。

步骤4 进入“SNAT规则”页签，单击“添加SNAT规则”。

- 子网：使用已有，系统会自动关联部门A的子网。
- 中转子网：ext_sub_T1
- 中转IP：10.1.0.55

步骤5 SNAT规则参数配置完成后，单击“确定”。

步骤6 返回网络控制台，在左侧导航栏选择“路由表”，单击“rtb-vpc-部门A”。确认已添加部门A到私网NAT网关的路由信息。

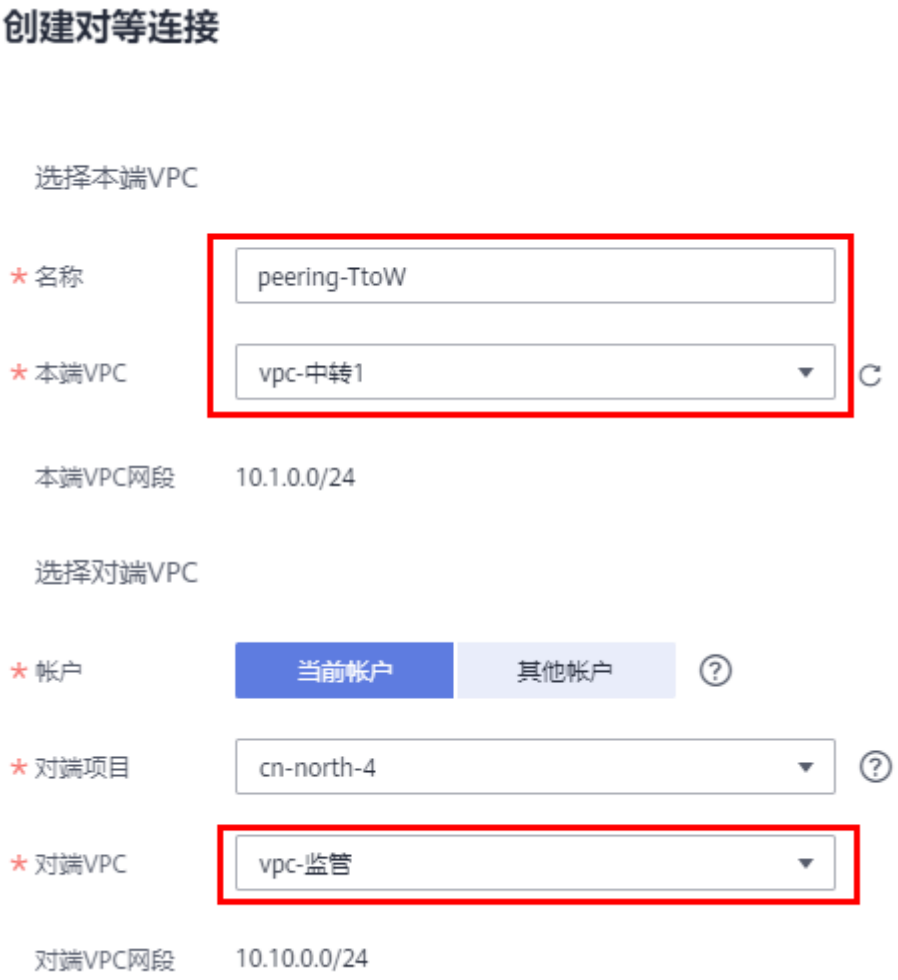
----结束

配置 VPC 对等连接

步骤1 选择“网络 > 虚拟私有云”，在左侧导航栏选择“对等连接”。

步骤2 配置对等连接，完成后单击“确定”。

- 名称：peering-TtoW
- 本端VPC：vpc-中转1
- 对端VPC：vpc-监管
- 未提及参数，保持默认或根据界面引导配置



----结束

配置路由

步骤1 选择“网络 > 虚拟私有云”，在左侧导航栏选择“路由表”。

步骤2 单击“rtb-vpc-中转1”，删除已有的“0.0.0.0/0”路由规则。

步骤3 单击“添加路由”，配置路由相关信息，单击“确认”。

- 目的地址：设置为0.0.0.0/0
- 下一跳类型：对等连接
- 下一跳：系统自动关联对等连接实例

步骤4 返回至“路由表”控制台，单击“rtb-vpc-监管”，单击“添加路由”。

步骤5 配置路由相关信息，单击“确认”。

- 目的地址：设置为0.0.0.0/0
- 下一跳类型：对等连接
- 下一跳：系统自动关联对等连接实例

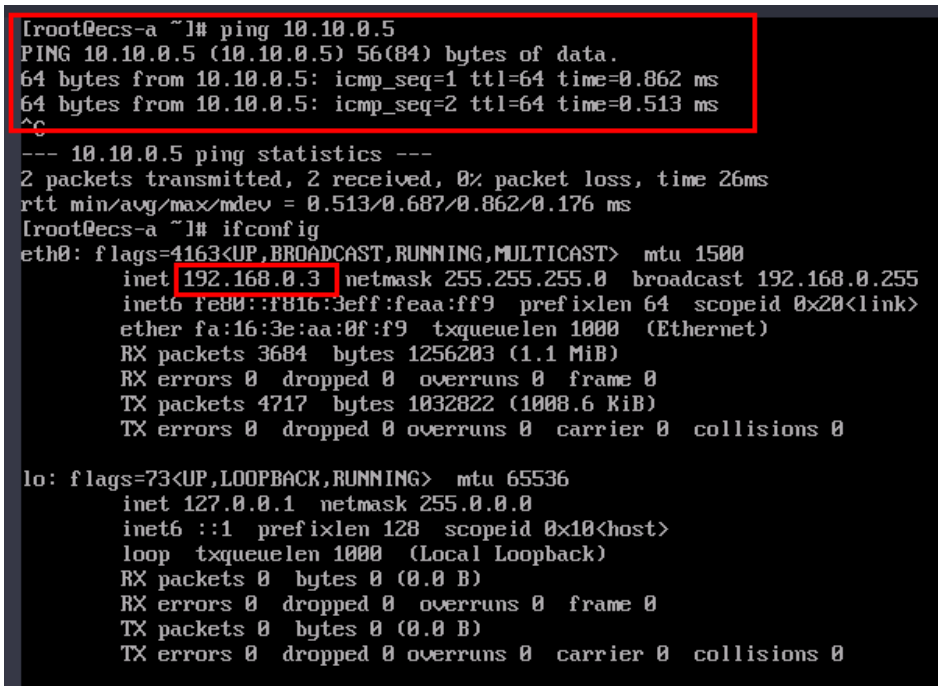
----结束

验证部门 A 访问监管部门

步骤1 选择“计算 > 弹性云服务器”，并使用VNC方式登录“ecs-部门A”的主机。

步骤2 在“ecs-部门A”主机上，执行如下命令，验证主机可以访问监管部门的主机。

```
ping 10.10.0.5
```

----结束

7 基于私网 NAT 网关实现跨 VPC 访问 ELB 实例

应用场景

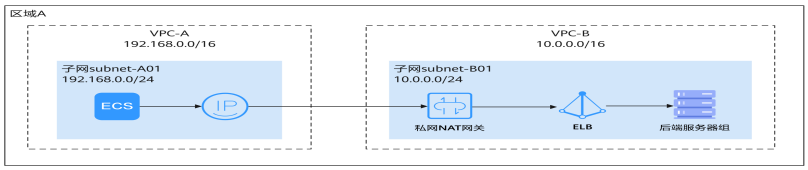
应用服务A和应用服务B分别部署在两个不同的VPC中，如果应用服务A希望访问到部署在应用服务B内的ELB服务，但是由于两个VPC的网络不互通无法完成访问。您可以通过配置私网NAT网关的DNAT规则实现应用服务A跨VPC访问应用服务B，从而实现应用服务A访问到应用服务B中的ELB服务。

方案架构

本文着重介绍使用私网NAT网关实现跨VPC访问ELB的实践案例。

1. 应用服务A与应用服务B分别部署在VPC-A和VPC-B中，应用服务之间互相隔离。
2. 通过私网NAT网关创建DNAT规则，将VPC-A的中转IP映射到VPC-B中的ELB实例，实现VPC-A中的应用服务A跨VPC访问到VPC-B中的ELB实例。
3. 本实践方案无需配置路由。

图 7-1 应用服务 A 实现跨 VPC 访问 ELB



方案优势

1. 业务A和业务B分别部署在不同的VPC中，实现了网络相互隔离，保证了业务的安全性。
2. 通过DNAT规则，实现了通过映射方式将您VPC-B内的实例对其他VPC A提供服务，VPC-B中的其他业务不会对VPC-A暴露，实现了精细化的网络管理。

约束与限制

针对同一个ELB实例，仅支持在一个VPC内创建一个DNAT规则进行访问，不支持在多个VPC内创建多个中转IP后使用DNAT规则进行访问。

资源规划说明

本示例中需要创建虚拟私有云VPC、弹性云服务器ECS、私网NAT网关和弹性负载均衡ELB，资源规划总体说明请参见表7-1。

表 7-1 资源规划

资源	数量	说明
虚拟私有云和子网	2个虚拟私有云和其下子网	• VPC-A，本示例网段为：192.168.0.0/16。 • subnet-A01，本示例网段为：192.168.0.0/24。
		• VPC-B，本示例网段为：10.0.0.0/16。 • subnet-B01，本示例网段为：10.0.0.0/24。
私网NAT网关	1个	本示例名称为private_nat_gateway，用于通过DNAT规则打通VPC-A和VPC-B网络。
弹性负载均衡	1个	被访问的ELB实例，部署在VPC-B内。
弹性云服务器	2台。	• ECS-A，部署在VPC-A中。 • ECS-B，部署在VPC-B中。

准备工作

- 购买两台ECS并配置应用服务，一台ECS-A部署在VPC-A中，一台ECS-B部署在VPC-B中。购买ECS详情请参考**快速购买和使用Linux ECS**。
- 创建一个HTTP协议的的后端服务器组-B，暂不关联弹性负载均衡，所属虚拟私有云为VPC-B，并将ECS-B添加到该后端服务器组中。创建后端服务器组详情请参考**创建后端服务器组**。

步骤一：创建负载均衡器

1. 进入**购买弹性负载均衡页面**。
2. 根据界面提示选择负载均衡器的基础配置，关键配置参数如**表7-2**所示。

   表 7-2 负载均衡器的基础配置

参数	示例	说明
实例类型	**独享型**	负载均衡的实例类型，选定后不支持修改。
区域	**华北-北京四**	不同区域的资源之间内网不互通
可用区	• **可用区1** • **可用区2**	在同一区域下，电力、网络隔离的物理区域，可用区之间内网互通，不同可用区之间物理隔离。
名称	**ELB01**	待创建负载均衡器的名称。

3. 选定独享型负载均衡实例的基础配置后，您需选择弹性负载均衡的实例规格，实例规格配置参数如**表7-3**所示。

表 7-3 负载均衡器的规格说明

参数	示例	说明
规格	• **弹性规格** • **应用型**	选择ELB的实例规格。

4. 请根据界面提示选择负载均衡器的网络配置，配置参数如**表7-4**所示。

表 7-4 负载均衡器的网络配置

参数	示例	说明
网络类型	**IPv4私网**	选择ELB实例的网络类型。
所属VPC	**VPC-B**	负载均衡器所属虚拟私有云，**独享型ELB创建完成后不支持切换**，请做好相关网络规划。
前端子网	**subnet-B01**	前端子网为独享型负载均衡提供私网IP地址，**用于与内网中的资源进行通信**。 ELB实例创建完成后，如果需要更换前端子网，可以通过解绑并绑定新的IPv4和IPv6地址实现。解绑IP地址可能会影响业务的正常运行，请谨慎操作。
IPv4地址	**自动分配IP地址**	如果网络类型选择了“IPv4私网”，则需要选择IPv4地址的分配方式。
后端子网	**与前端子网保持一致**	后端子网为独享型负载均衡提供私网IP地址，**用于与后端服务器进行通信和健康检查**。

5. 其余参数保持默认，单击“立即购买”，完成ELB实例的创建。

步骤二：添加 HTTP 监听器并配置后端服务器组

为**ELB01**添加HTTP监听器，并将准备工作中创建的**后端服务器组-B**添加到该监听器下，监听器的“访问控制”设置为“**允许所有IP访问**”，详情请参考**添加HTTP监听器**。

步骤三：创建中转 IP

1. 进入**私网NAT网关列表页**。
2. 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 7-2 创建中转 IP

3. 根据界面提示，配置中转IP，配置参数请参见**表7-5**。

图 7-3 创建中转 IP

表 7-5 中转 IP 参数说明

参数	示例	参数说明
中转VPC	**VPC-A**	中转IP所在的VPC。
中转子网	**subnet-A01**	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	**自动分配**	选择中转IP的分配方式。

4. 完成中转IP的创建。

步骤四：创建私网 NAT 网关

1. 进入**购买私网NAT网关页面**。
2. 根据界面提示，配置私网NAT网关的基本信息，关键配置参数请参见**表7-6**，其余配置保持默认。

表 7-6 参数说明

参数	示例	参数说明
名称	**private_nat_gateway**	私网NAT网关名称。
虚拟私有云	**VPC-B**	私网NAT网关所属的VPC。
子网	**subnet-B01**	私网NAT网关所属VPC中的子网。
规格	**小型**	私网NAT网关的规格。

3. 单击“立即购买”，完成私网NAT网关的创建。

步骤五：创建 DNAT 规则

1. 进入**私网NAT网关列表页**。
2. 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。
3. 在私网NAT网关详情页面中，单击“DNAT规则”页签。
4. 在DNAT规则页签中，单击“添加DNAT规则”。
5. 根据界面提示，配置添加DNAT规则参数，详情请参见**表7-7**。

表 7-7 DNAT 规则参数说明

参数	示例	说明
本端网络		
端口类型	**具体端口**	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。
支持协议	**TCP**	协议类型分为TCP和UDP两种类型。
实例类型	**负载均衡器**	选择对外部私网提供服务的实例类型，本示例选择**步骤一**中创建完成的负载均衡器ELB01。
业务端口	**80**	实例对外提供服务的协议端口号。
中转网络		
中转IP	**192.168.0.144**	通过该中转IP访问用户IDC或其他VPC，本示例选择**步骤三**中创建的中转IP。
中转IP端口	**80**	中转IP对外提供服务的端口号。

6. 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。

步骤六：验证网络连通性

1. 远程登录ECS-B，启动ELB部署的后端服务。

   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

   执行命令参考：

   ```
   python3 -m http.server 80
   ```

   图 7-4 启动 ELB 部署的后端服务

2. 远程登录ECS-A。
3. 执行以下命令确认网络连通性：

   ```
   curl http://${中转IP地址}
   ```

   收到类似如下信息，表示ECS-A可以访问到跨VPC的ELB01。

   图 7-5 验证跨 VPC 访问到 ELB 实例

8 使用公网 NAT 网关统一管理公网出口 IP

应用场景

在云上环境中，当VPC内需要管理大量的ECS实例时，如果采用逐一配置弹性公网IP的方式，不仅会显著降低管理和运营效率，还会增加ECS实例遭受恶意扫描和攻击的风险。

您可以使用公网NAT网关统一管理ECS实例的出入云需求，从以下两个方面提升运维效率，降低安全风险。

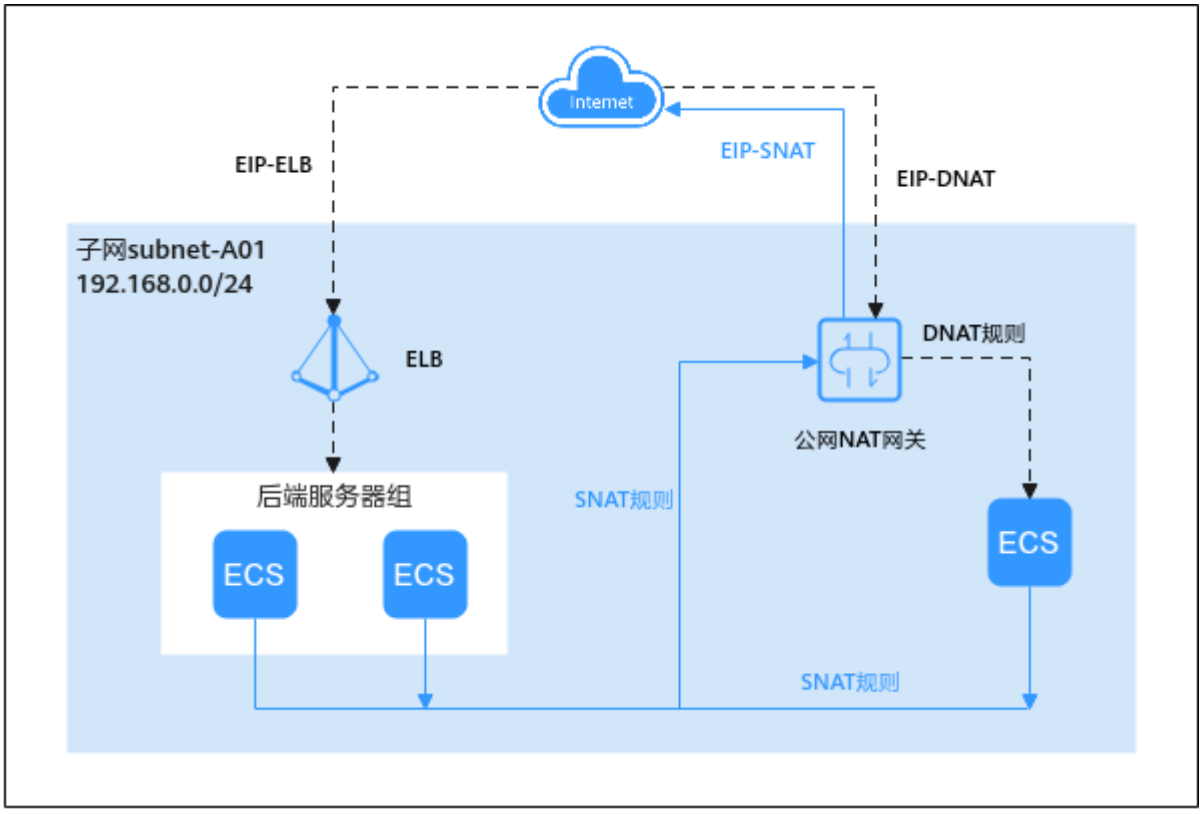
- 在确保原有资源正常运行的前提下，通过**SNAT规则**为VPC内的所有ECS实例统一提供公网访问能力。
- 对于直接绑定弹性公网IP的ECS实例，通过将EIP从ECS实例解绑并创建**DNAT规则**，在确保客户端访问ECS实例方式不变的同时，有效控制端口暴露范围。

方案架构

在企业级应用中，为了提高服务的可用性和管理效率，通常需要对后端服务进行集中管理。然而，直接暴露后端服务到公网会带来安全风险。如果您的服务器有主动访问公网的业务诉求，推荐您使用以下方案对公网出入口进行统一管理：

1. 使用ELB对后端服务进行集中管理，统一对外提供服务的入口。
2. 使用公网NAT网关统一公网出口IP，如**图8-1**的方案，不仅能够集中管理后端服务，还能有效降低安全风险，提升运维效率。

图 8-1 统一管理公网出口 IP



资源规划说明

本示例中需要创建虚拟私有云VPC、弹性云服务器ECS、公网NAT网关和弹性负载均衡ELB，资源规划总体说明请参见表7-1。

表 8-1 资源规划

资源	数量	说明
虚拟私有云和子网	1个虚拟私有云和其下子网	• VPC-A，本示例网段为：192.168.0.0/16。 • subnet-A01，本示例网段为：192.168.0.0/24。
公网NAT网关	1个	本示例名称为nat_public，用于通过SNAT规则统一ECS访问公网的IP。
弹性负载均衡	1个	外部流量通过ELB主动访问云上的ECS。
弹性云服务器	3台	ECS-A，ECS-B，ECS-C都部署在子网subnet-A01中。

资源	数量	说明
弹性公网IP	3个	• EIP-ELB：用于绑定ELB，ECS通过ELB面向公网客户端提供服务。 • EIP-SNAT：ECS使用EIP-SNAT通过SNAT规则主动访问公网客户端。 • EIP-DNAT：外部客户端访问EIP-DNAT通过DNAT规则访问到ECS。

准备工作

- 如**表8-1**所示，购买3个EIP分别用作EIP-ELB、EIP-SNAT和EIP-DNAT。
- 购买一个ELB实例和三台ECS并配置应用服务，其中两台ECS部署为ELB的后端服务器，详情请参考**实现单个Web应用的负载均衡**。

步骤一：创建公网 NAT 网关

1. 进入**购买公网NAT网关页面**。
2. 根据界面提示，配置公网NAT网关的基本信息，配置参数详细说明请参考**购买公网NAT网关**。

图 8-2 购买公网 NAT 网关

步骤二：添加 SNAT 规则

虚拟私有云子网subnet-A01中的ECS可以共享SNAT规则绑定的弹性公网IP访问公网。

1. 进入**公网NAT网关列表页面**。
2. 在公网NAT网关页面，单击需要**步骤一**中购买的公网NAT网关。

进入公网NAT网关详情页。

3. 切换到SNAT规则页签，单击“添加SNAT规则”。
4. 根据界面提示，添加SNAT规则，公网IP类型选择“弹性公网IP”并勾选准备工作中已经创建完成的EIP-SNAT作为公网IP。

图 8-3 添加 SNAT 规则

5. 单击“确定”，完成SNAT规则创建。

步骤三：添加 DNAT 规则

虚拟私有云子网subnet-A01中的ECS可以共享DNAT规则绑定的弹性公网IP面向公网提供访问。

1. 进入**公网NAT网关列表页面**。
2. 在公网NAT网关页面，单击需要**步骤一**中购买的公网NAT网关。

   进入公网NAT网关详情页。
3. 切换到DNAT规则页签，单击“添加DNAT规则”。
4. 根据界面提示，添加DNAT规则。

   端口类型选择“所有端口”，公网IP类型选择“弹性公网IP”并勾选准备工作中已经创建完成的EIP-DNAT作为公网IP。

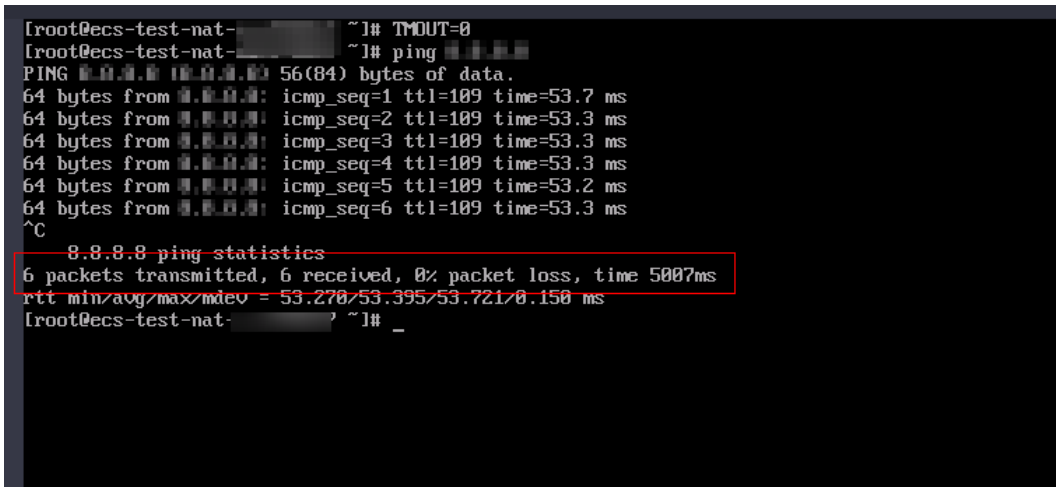
图 8-4 添加 DNAT 规则

5. 单击“确定”，完成DNAT规则创建。

步骤四：验证结果

1. 远程登录部署了后端服务的ECS。
   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。
2. 在ECS上分别ping三个EIP，验证可以正常对外提供公网访问。

图 8-5 服务器正常对外提供公网访问



3. 分别在三台ECS上执行以下命令，获取服务器访问公网的IP地址。

```
curl myip.ipip.net
```

如图8-6所示，三台ECS都返回EIP-SNAT的地址。

图 8-6 获取服务器访问公网的 IP 地址

9 通过公网 NAT 网关和云防火墙 CFW 防护 SNAT 规则出网流量

应用场景

在云上环境中，当VPC内需要管理大量的ECS实例时，如果采用逐一配置弹性公网IP的方式，不仅会显著降低管理和运营效率，还会增加ECS实例遭受恶意扫描和攻击的风险。

您可以使用公网NAT网关管理统一管理ECS实例的出入云需求，从以下两个方面提升运维效率，降低安全风险。

- 在确保原有资源正常运行的前提下，通过**公网NAT网关SNAT**规则为VPC内的所有ECS实例统一提供公网访问能力。
- 对于直接绑定弹性公网IP的ECS实例，通过将EIP从ECS实例解绑并创建**DNAT规则**，在确保客户端访问ECS实例方式不变的同时，有效控制端口暴露范围。

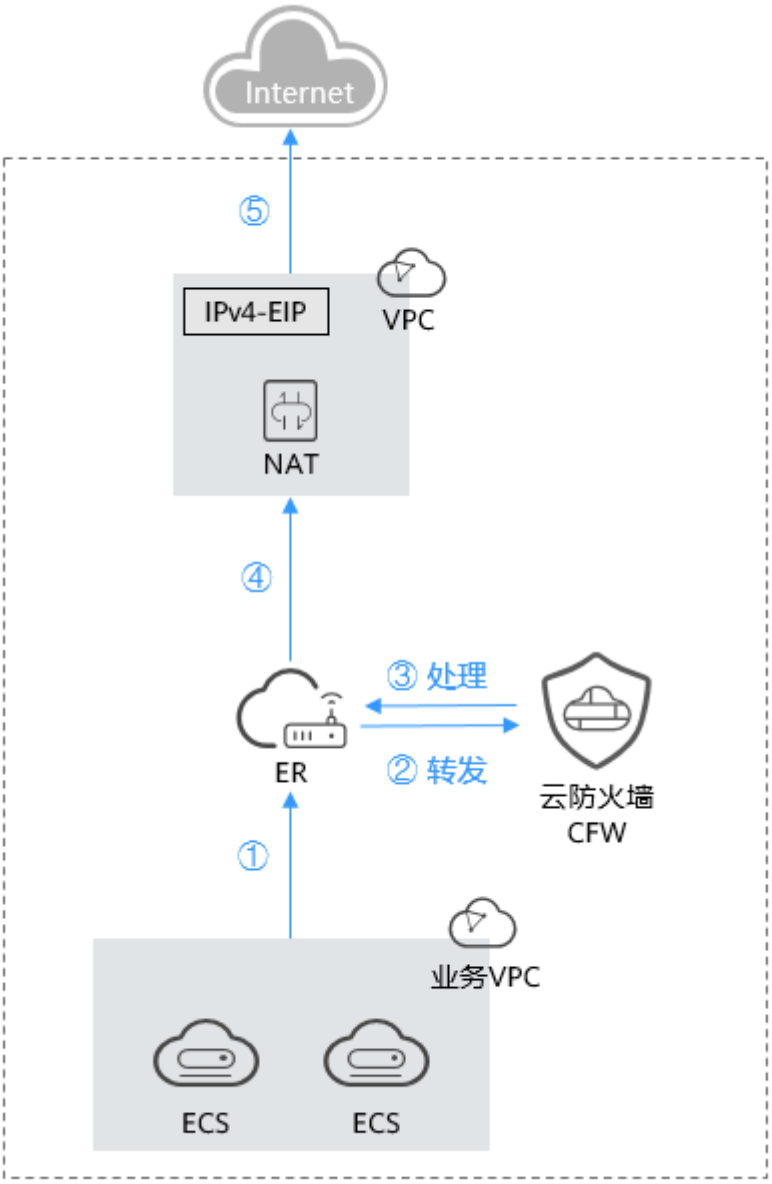
准备工作

- 配置中需要使用企业路由器（Enterprise Router, ER），关于企业路由器请参见**什么是企业路由器?** 。
- 需完成创建防火墙，具体配置请参见**创建防火墙**。

约束与限制

- 仅“专业版”云防火墙支持私网IP的访问控制。
- 云防火墙当前默认支持标准私网网段，如果您需要配置其它的网段，请您修改私网网段或**提交工单**进行私网网段扩容。

SNAT 防护网



说明

请求流量和响应流量为同一个路径。

配置建议

- 建议为NAT网关创建独立VPC不用于云服务器等实例网络配置，避免影响后续的访问控制。
- 在前期网络规划复杂甚至不合理的情况下（例如存在VPC网段重叠、NAT网关已有复杂配置、已通过VPC-Peering配置东西向通信等场景下），请充分评估网络互连、环路、路由冲突等风险。

- 因涉及组件多，不建议直接将现网业务导入，可先创建测试机，并在业务VPC路由表中配置目的地址路由，利用业务VPC中的测试机验证整个业务流是否走通及配置的规则是否有效，再对现网业务进行切流。
- 使用云防火墙后，避免第一时间配置拦截规则。建议首先验证流量接入防火墙后业务是否正常，逐步增加规则，并及时验证功能，一旦发现有问题，需及时关闭防护，避免现网业务受损。
- 对于SNAT EIP，外到内无法主动访问，内到外的访问控制规则使用的是互联网边界防护的能力，建议不在“弹性公网IP管理”页面中对SNAT所绑定的EIP开启防护，避免规则和日志混乱。

配置流程

配置详情请参见**通过配置CFW防护规则实现SNAT流量防护**。

图 9-1 SNAT 防护配置流程