

NAT 网关

# 最佳实践

文档版本 02  
发布日期 2024-05-06



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI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 基于云连接和 SNAT 实现跨区域内网访问公网服务器加速.....	1
2 基于公网 NAT 网关和云专线的混合云 Internet 加速.....	5
3 基于私网 NAT 网关和云专线的混合云 SNAT.....	9
4 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.....	12
5 使用私网 NAT 网关服务实现 IDC 网段免修改上云.....	18
5.1 方案概述.....	18
5.2 云上重叠子网间主机互访.....	21
5.3 云上指定 IP 地址访问 VPC 外主机.....	37

# 1 基于云连接和 SNAT 实现跨区域内网访问公网服务器加速

## 应用场景

当客户要加速访问境外时，可以使用虚拟专用网络（VPN）、云连接、NAT网关（添加SNAT规则）、EIP在客户本地侧和境外侧之间建立网络连通且提高访问速度。

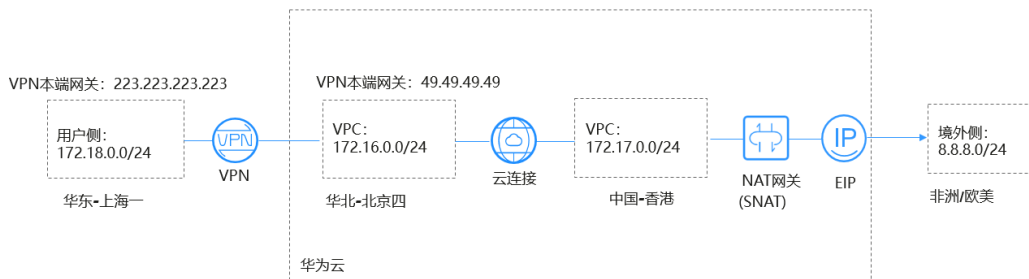
例如：客户希望通过云下数据中心（IDC）的ECS可以访问非洲/欧美的业务且网络速度快不卡顿，那么可以使用本方案。

## 方案架构

1. 通过虚拟专用网络（VPN）将客户本地侧和华北-北京四区域的VPC连通。
2. 通过云连接将华北-北京四区域的VPC和中国-香港区域的VPC连通，并实现网络加速。
3. 通过在中国-香港区域购买NAT网关，添加SNAT规则并绑定EIP，来实现访问境外公网。

应用场景如图1-1所示。

图 1-1 场景示意



### 说明

- 在本方案中，用户云下数据中心（IDC）使用华为云的“华东-上海一”替代。
- 境外网络网段：8.8.8.0/24；境外唯一测试网络：8.8.8.8。

## 方案优势

实现客户跨境访问的同时，加速网络访问，给客户更好地体验。

## 约束与限制

用户账号需具备跨境权限，如果用户账号没有跨境权限，需要将当前的VPC资源授权给具有跨境权限的账号来创建云连接实例。

## 资源和成本规划

表 1-1 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	该VPC所在的区域为华东-上海一，VPC网段为：172.18.0.0/24。 本方案使用华为云的“华东-上海一”来替代用户线下数据中心（IDC）。	1
	VPC-Test02	该VPC所在的区域为华北-北京四，VPC网段为：172.16.0.0/24。	1
	VPC-Test03	该VPC所在的区域为中国-香港，VPC网段为：172.17.0.0/24。	1
弹性公网IP (EIP)	EIP-Test	在中国-香港区域购买EIP。	1
NAT网关	NAT-Test	在VPC-Test03中购买公网NAT网关，并绑定EIP-Test。	1
VPN网关	VPN-GW-Test01	在华北-北京四区域创建VPN网关。 VPN本端网关为：49.49.49.49。	1
	VPN-GW-Test02	在华东-上海一区域创建VPN网关。 VPN本端网关为：223.223.223.223。	1
VPN连接	VPN-Test01	为VPN网关VPN-GW-Test01创建VPN连接。	1
	VPN-Test02	为VPN网关VPN-GW-Test02创建VPN连接。	1
云连接	CC-Test	使用云连接实现华北-北京四和中国-香港跨区域之间访问，并加速网络访问。	1
弹性云服务器 (ECS)	ECS-Test01	在华东-上海一区域的VPC中创建ECS，该ECS的私网地址为：172.18.0.3。	1
	ECS-Test02	在华北-北京四区域的VPC中创建ECS，该ECS的私网地址为：172.16.0.3。	1
	ECS-Test03	在中国-香港区域的VPC中创建ECS，该ECS的私网地址为：172.17.0.3。	1

## 操作流程

1. [创建VPC并设置VPC网段](#)
2. [配置VPN](#)
3. [配置云连接](#)
4. [购买弹性云服务器](#)
5. [购买EIP并配置NAT网关](#)

## 实施步骤

### 步骤1 创建VPC并设置VPC网段

创建流程请详细参考[创建虚拟私有云和子网](#)。

VPC网段请勿冲突。

- 华东-上海一区域的VPC网段（VPC-Test01）：172.18.0.0/24
- 华北-北京四区域的VPC网段（VPC-Test02）：172.16.0.0/24
- 中国-香港区域的VPC网段（VPC-Test03）：172.17.0.0/24

### 步骤2 配置VPN

在华北-北京四区域创建VPN网关VPN-GW-Test01和VPN连接VPN-Test01。

在华东-上海一区域创建VPN网关VPN-GW-Test02和VPN连接VPN-Test02。

经典版VPN创建流程请详细参考[创建VPN网关](#)和[创建VPN连接](#)。

企业版VPN创建流程请详细参考[创建VPN网关](#)和[创建VPN连接](#)。

- 华北-北京四网关和子网配置：
  - 本端网段：172.16.0.0/24，172.17.0.0/24，8.8.8.0/24
  - 远端网关：223.223.223.223
  - 远端子网：172.18.0.0/24
- 华东-上海一网关和子网配置：
  - 本端网段：172.18.0.0/24
  - 远端网关：49.49.49.49
  - 远端子网：172.16.0.0/24，172.17.0.0/24，8.8.8.0/24

#### 说明

华北-北京四、华东-上海一配置VPN连接时，华北-北京四的本端网段和华东-上海一的远端子网设置必须包含外网网段8.8.8.0/24，以便可以ping通外网。

### 步骤3 配置云连接

1. 创建云连接（CC-Test）。  
创建流程请详细参考[创建云连接](#)。
2. 加载网络实例。  
加载网络实例详细参考[加载网络实例](#)。
3. 添加自定义网段。  
添加自定义网段详细参考[添加自定义网段](#)。

- 华北-北京四自定义网段：172.18.0.0/24，172.16.0.0/24。
- 中国-香港自定义网段：172.17.0.0/24，8.8.8.0/24。

#### 📖 说明

为实现所有节点都可以端到端传输，需要添加全部的本端云连接网段。

#### 4. 购买带宽包

云连接默认跨区域互通带宽为10kbps，仅用于测试连通性，需购买带宽包并配置域间带宽以保证业务正常使用。

购买带宽包详细参考[购买带宽包](#)。

#### 5. 配置域间带宽

配置域间带宽详细参考[配置域间带宽](#)。

### 步骤4 购买弹性云服务器

分别购买华东-上海一、华北-北京四、中国-香港区域的ECS。

购买流程请详细参考[购买弹性云服务器](#)。

- 华东-上海一ECS私网地址（ECS-Test01）：172.18.0.3。
- 华北-北京四ECS私网地址（ECS-Test02）：172.16.0.3。
- 中国-香港ECS私有地址（ECS-Test03）：172.17.0.3。

### 步骤5 购买EIP并配置NAT网关

在中国-香港区域购买EIP（EIP-Test），并配置NAT网关（NAT-Test），添加SNAT规则，将以下网段添加到规则中。

购买配置流程请详细参考[申请和绑定弹性公网IP](#)和[添加SNAT规则](#)。

- 添加虚拟私有云网段：172.17.0.0/24
- 添加云专线/云连接网段：172.18.0.0/24；172.16.0.0/24

#### 📖 说明

添加SNAT配置用于连通外网，ping通远端外网网段8.8.8.0/24。

----结束

## 配置验证

配置完成，测试连通性。

从华东-上海一的ECSping外网唯一验证网关：8.8.8.8。

```
[root@ecs-d7e8 ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=51 time=71.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=69.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=69.6 ms
_
```

# 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，高速的访问互联网，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

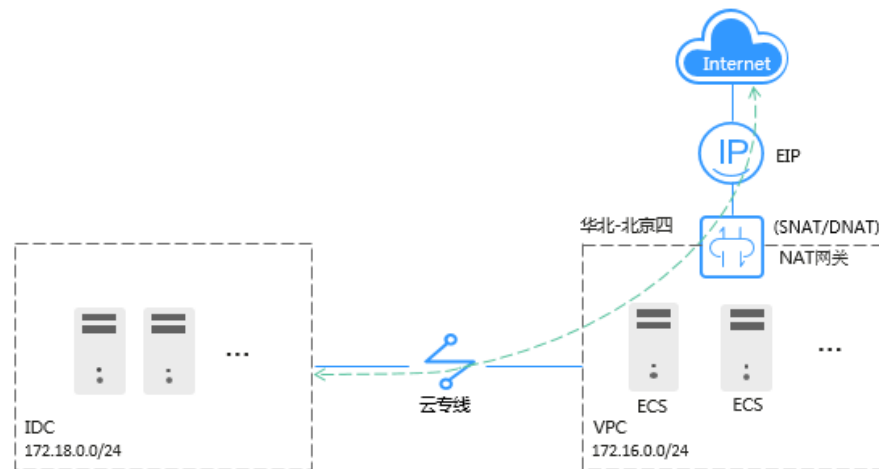
假设用户IDC网段为172.18.0.0/24，接入VPC区域为“华北-北京四”，VPC子网网段为172.16.0.0/24。

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VPC网段

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[配置云专线](#)。

#### 📖 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

添加SNAT规则

NAT网关名称 nat-84b8

\* 使用场景 虚拟私有云 云专线/云连接

172 . 18 . 0 . 0 / 24

\* 弹性公网IP 还可以添加19个 [查看弹性公网IP](#) 所有项目

<input checked="" type="checkbox"/> 弹性公网IP	类型	带宽名称	带宽 (Mbit/s)	计费模式	企业项目
<input checked="" type="checkbox"/>	全动态BGP	bandwidthl	5	按需	default

已选择弹性公网IP (1个): SNAT规则使用多个弹性公网IP时, 业务运行时可能会随机选取其中的一个。

监控 SNAT连接数设置告警, 实时监控运行状态

描述

0/255

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

添加DNAT规则

**i** 针对同一弹性云服务器, 请避免同时配置弹性公网IP服务和NAT服务, 以免对DNAT数据报文可能造成的中断。 [参考链接](#)

- 配置DNAT规则后, 需要放通对应的安全组规则。 [点此跳转](#)
- 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。

NAT网关名称 nat-z408

\* 使用场景 虚拟私有云 云专线/云连接

\* 端口类型 具体端口 所有端口

\* 支持协议 全部

\* 弹性公网IP   [查看弹性公网IP](#)

带宽大小: 1 Mbit/s 计费模式: 按需计费  
企业项目: default

\* 私网IP  [查看云专线虚拟接口](#)

描述

### 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

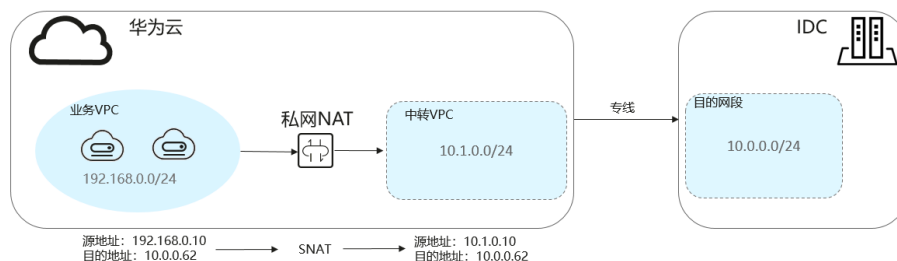
## 应用场景

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

- [创建业务VPC和中转VPC](#)
- [配置云专线](#)
- [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[配置云专线](#)。

### 步骤3 购买并配置私网NAT网关

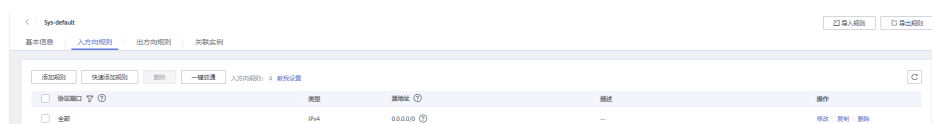
1. 在指定区域购买私网NAT网关，选定业务VPC。
2. 创建中转IP，中转VPC选择VPC-Test02，中转IP选择手动分配，IP地址为：**10.1.0.10**。
3. 进入到上述购买的私网NAT网关的“SNAT规则”页签，单击“添加SNAT规则”，子网选择业务VPC中需要做地址映射的子网（网段为：**192.168.0.0/24**），中转IP选择上述创建好的。
4. 在业务VPC中添加指向私网NAT网关的路由，目的地址配置为IDC的网段（目的网段：**10.0.0.0/24**）。

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**）中添加加入方向安全组规则，用于将发到目的端的流量全部放通。

图 3-3 添加加入方向安全组规则



----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。详情见下方的组网图。

## 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。

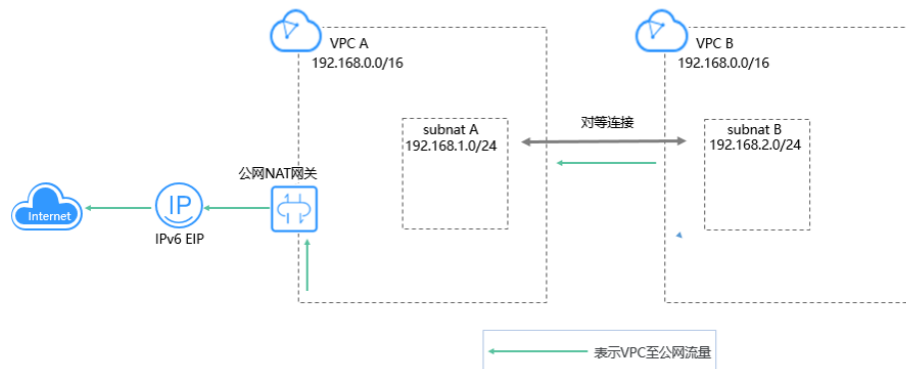
## 典型拓扑

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。

图 4-1 组网图



## 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 4-2 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 4-3 添加 SNAT 规则

**添加SNAT规则**

**说明**

- 当弹性云服务器同时配置弹性公网IP服务和NAT网关服务时，数据均通过弹性公网IP转发。 [参考链接](#)
- 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。

NAT网关名称 nat-84b8

\* 使用场景  虚拟私有云  云专线/云连接

?

\* 弹性公网IP 还可以添加20个 [查看弹性公网IP](#) 所有项目  请输入弹性公网IP地址

<input type="checkbox"/> 弹性公网IP	类型	带宽名称	带宽 (Mbit/s)	计费模式	企业项目
暂无数据 <a href="#">购买弹性公网IP</a>					

已选择弹性公网IP (0个)。SNAT规则使用多个弹性公网IP时，业务运行时会随机选取其中的一个。

监控 SNAT连接数 [设置告警](#)，[实时监控运行状态](#)

### 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 4-4 添加 DNAT 规则

### 添加DNAT规则

**i** 针对同一弹性云服务器，请避免同时配置弹性公网IP服务和NAT服务，以免对DNAT数据报文可能造成的中断。  
[参考链接](#)

- 配置DNAT规则后，需要放通对应的安全组规则。 [点此跳转](#)
- 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。

NAT网关名称 nat-84b8

\* 使用场景  虚拟私有云  云专线/云连接

\* 端口类型  具体端口  所有端口

\* 支持协议

\* 弹性公网IP  [查看弹性公网IP](#)

\* 公网端口

\* 私网IP  [查看可用云主机IP](#)

\* 私网端口

描述

- 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 4-5 添加 DNAT 规则

### 添加DNAT规则

**ⓘ** 针对同一弹性云服务器，请避免同时配置弹性公网IP服务和NAT服务，以免对DNAT数据报文可能造成的中断。  
[参考链接](#)

- 配置DNAT规则后，需要放通对应的安全组规则。 [点此跳转](#)
- 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。

NAT网关名称 nat-84b8

★ 使用场景  虚拟私有云  云专线/云连接

★ 端口类型  具体端口  所有端口

★ 支持协议

★ 弹性公网IP  [查看弹性公网IP](#)

★ 公网端口

★ 私网IP

★ 私网端口

描述

----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 [redacted]
<!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 [redacted]
<!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 ~]#
```

# 5 使用私网 NAT 网关服务实现 IDC 网段免修改上云

## 5.1 方案概述

### 应用场景

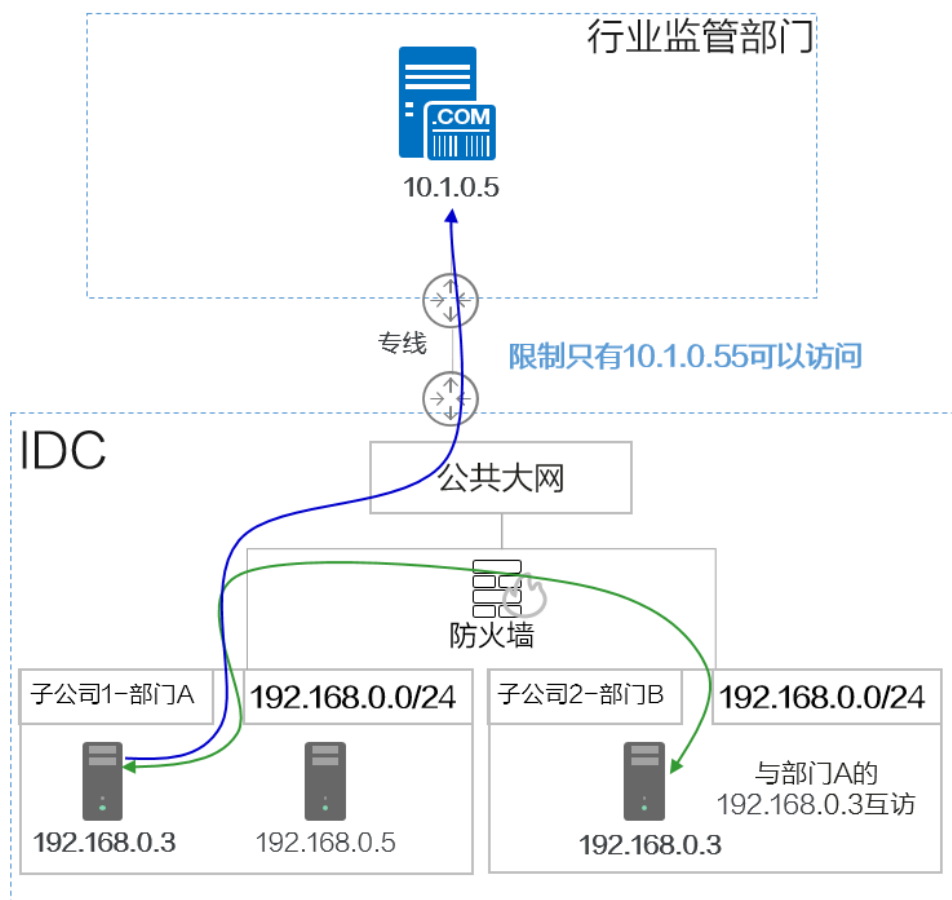
- 在不改变现有IDC网络组织架构的前提下，需要将网络组织架构迁移上云，并实现IDC中的两个重叠网段内的主机相互访问。
- 在不改变现有IDC网络组织架构的前提下，需要将网络组织架构迁移上云，并实现以IDC中指定IP地址访问外部资源。

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5-1，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 5-1 子公司间的网络存在子网重叠



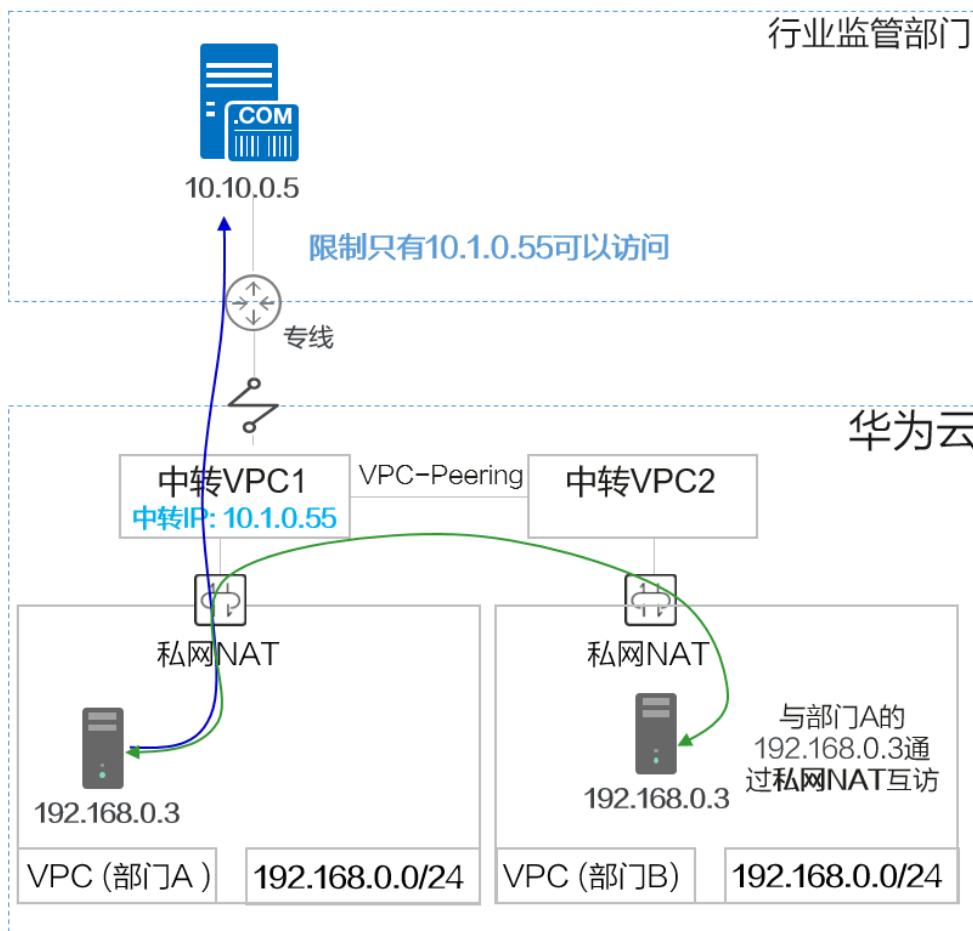
## 方案架构

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5-2：

- 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 5-2 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。

## 5.2 云上重叠子网间主机互访

### 应用场景

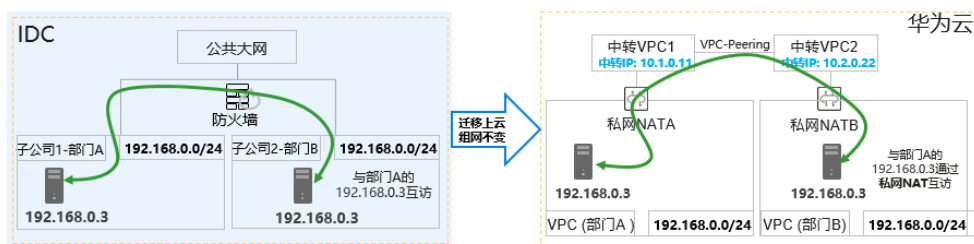
在不改变现有IDC网络组织架构的前提下，需要将网络组织架构迁移上云，并实现IDC中的两个重叠网段内的主机相互访问。

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 5-3 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 5-1 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并配置资源](#)
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** 登录管理控制台。

**步骤2** 在管理控制台左上角单击 ，选择区域和项目。

**步骤3** 在页面左上角单击  图标，打开服务列表，选择“网络 > 虚拟私有云”。  
进入虚拟私有云列表页面。

**步骤4** 单击“创建虚拟私有云”。  
进入“创建虚拟私有云”页面。

**步骤5** 在“创建虚拟私有云”页面，根据[表5-1](#)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
- 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

创建虚拟私有云 ?

---

**基本信息**

区域 华北-北京四

不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。

名称 vpc-部门A

IPv4网段 192 · 168 · 0 · 0 / 24

建议使用网段: 10.0.0.0/8-24 (选择) 172.16.0.0/12-24 (选择) 192.168.0.0/16-24 (选择)

⚠ 该VPC网段 (192.168.0.0/24) 与当前区域下其他VPC网段重叠, 如需使用VPC互通服务, 建议

企业项目 default 新建企业项目 ?

---

高级配置 ▼    标签 | 描述

---

**默认子网**

可用区 可用区1 ?

名称 subnet-A

子网IPv4网段 192 · 168 · 0 · 0 / 24 ? 可用IP数: 251

子网创建完成后, 子网网段无法修改

**步骤6** 重复**步骤4~步骤5**，参考**表5-1**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
- 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 5-4 创建所需 VPC

名称	IPv4网段	状态	子网个数	路由表	服务器个数	企业项目	操作
vpc-中转2	10.2.0.0/24 (主网段)	可用	1	1	0	default	编辑网段 删除
vpc-中转1	10.1.0.0/24 (主网段)	可用	1	1	0	default	编辑网段 删除
vpc-部门B	192.168.0.0/24 (主网段)	可用	1	1	0	default	编辑网段 删除
vpc-部门A	192.168.0.0/24 (主网段)	可用	1	1	0	default	编辑网段 删除

----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5-1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

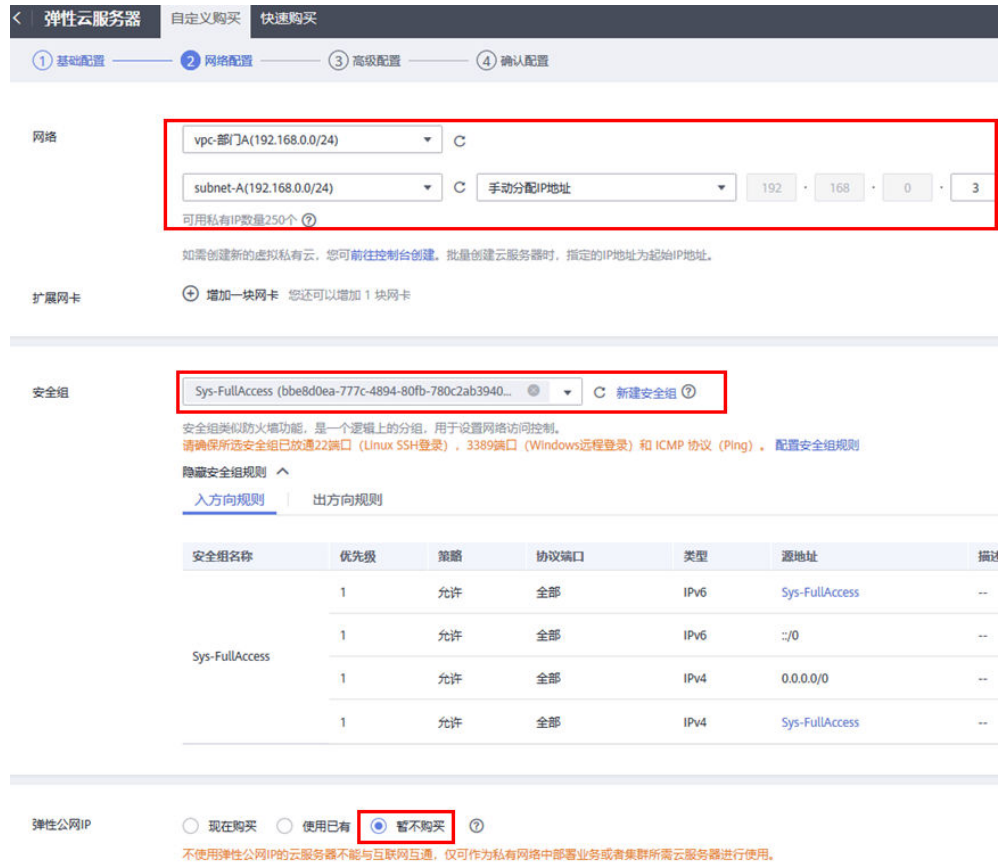
The screenshot displays the 'Elastic Cloud Server' (弹性云服务器) configuration page. It is divided into four steps: 1. Basic Configuration (基础配置), 2. Network Configuration (网络配置), 3. Advanced Configuration (高级配置), and 4. Confirmation Configuration (确认配置). The 'Basic Configuration' step is active.

Key configuration options shown include:

- 计费模式 (Billing Mode):** 按需计费 (Pay-as-you-go) is selected and highlighted with a red box.
- 区域 (Region):** 华北-北京四 (North China-4) is selected and highlighted with a red box. A tooltip shows recommended regions: 华北-乌兰察布二... (19) and 西南-贵阳, 华东-上海一 (4).
- 可用区 (Availability Zone):** 随机分配 (Randomly allocate) is selected.
- CPU架构 (CPU Architecture):** x86计算 (x86 Compute) is selected.
- 规格 (Instance Type):** 最新系列 (Latest Series) is selected. The '通用计算增强型' (General Purpose Compute Enhanced) category is active. A table lists instance types: c6.large.2 (2vCPUs | 4GiB) and c6.3xlarge.4 (12vCPUs | 48GiB). The c6.large.2 instance type is selected and highlighted with a red box.
- 镜像 (Image):** 公共镜像 (Public Image) is selected. The image 'CentOS 8.0 64bit(40GB)' is selected and highlighted with a red box.

### 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5-1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。

弹性云服务器 自定义购买 快速购买

① 基础配置 ② 网络配置 ③ 高级配置 ④ 确认配置

云服务器名称   允许重名  
购买多台云服务器时，支持自动增加数字后缀命名或者自定义规则命名。

登录凭证

用户名 root

密码   
请牢记密码，如忘记密码可登录ECS控制台重置密码。

确认密码

---

云备份 使用云备份服务，需购买备份存储库，存储库是存放服务器产生的备份副本的容器。

云备份存储库

备份策略  [管理备份策略](#)

**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。

弹性云服务器

名称/ID	监控	可用区	状态	规格/镜像	IP地址	计费	企业项目	标签	操作
ecs-部门B a29c4fe7-8407-...		可用区7	运行中	2vCPUs   4GiB... CentOS 8.0 64...	192.168.0.3...	按量计费 2021/05...	default	--	远程登录 更多
ecs-部门A 59b88eb0-2199-...		可用区7	运行中	2vCPUs   4GiB... CentOS 8.0 64...	192.16...	按量计费 2021/05...	default	--	远程登录 更多

**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 ~]# TMOU=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 并配置资源

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”页面，根据表5-1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** 选择“网络 > NAT网关”，选择“私网NAT网关”。
- 步骤2** 在私网NAT网关页面，单击“购买私网NAT网关”。
- 步骤3** 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4** 配置完成后，单击“立即购买”。
- 步骤5** 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6** 切换至“DNAT规则”页签，单击“添加DNAT规则”。
- 步骤7** 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。

## 添加DNAT规则

私网NAT网关名称 private-nat-A

端口类型  具体端口  所有端口

支持协议 全部

\* 中转子网  [查看中转子网](#)

\* 中转IP  [查看中转IP](#)

\* 实例类型  服务器  虚拟IP地址  负载均衡器  自定义

所有项目  所有运行状态  名称

名称	状态	私有IP地址	企业项目	虚拟私有云
<input checked="" type="radio"/> ecs-部门A	<span style="color: green;">➔</span> 运行中	192.168.0.3	default	vpc-部门A

**步骤8** 返回私网NAT网关页面，并单击“购买私网NAT网关”。

**步骤9** 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10** 配置完成后单击“立即购买”。

**步骤11** 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12** 切换至“DNAT规则”页签，单击“添加DNAT规则”。

**步骤13** 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。

### 添加DNAT规则

私网NAT网关名称 private-nat-B

端口类型  具体端口  所有端口

支持协议

\* 中转子网  [查看中转子网](#)

\* 中转IP  [查看中转IP](#)

\* 实例类型  服务器  虚拟IP地址  负载均衡器  自定义

名称	状态	私有IP地址	企业项目	虚拟私有云
<input checked="" type="radio"/> ecs-部门B	<span style="color: green;">+</span> 运行中	192.168.0.3	default	vpc-部门B

----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

### 添加路由

路由表 rtb-vpc-部门A(默认路由表)

目的地址 <input type="text" value="0.0.0.0/0"/>	下一跳类型 <input type="text" value="NAT网关"/>	下一跳 <input type="text" value="private-nat-A(c441afea-0bfa-4116-8 ...)"/>	描述
<input type="button" value="继续添加"/>			
<input type="button" value="确定"/>		<input type="button" value="取消"/>	

**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

### 添加路由

路由表 rtb-vpc-部门B(默认路由表)

目的地址 ?	下一跳类型 ?	下一跳 ?
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="NAT网关"/>	<input type="text" value="private-nat-B(c9a0fd01-bc8c-437a-9 ..."/>
<a href="#">+ 继续添加</a>		
<input type="button" value="确定"/> <input type="button" value="取消"/>		

----结束

### 配置中转 VPC1 到 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

## 创建对等连接

选择本端VPC

\* 名称

\* 本端VPC

本端VPC网段 10.1.0.0/24

选择对端VPC

\* 帐户  当前帐户  ?

\* 对端项目  ?

\* 对端VPC

对端VPC网段 10.2.0.0/24

描述

0/255

**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

## 添加路由

路由表 rtb-vpc-中转(默认路由表)

目的地址 ?	下一跳类型 ?	下一跳 ?
<input type="text" value="0.0.0.0/0"/>	<span>对等连接</span> ▼	<span>peering-TtoT(d27b997e-c297-417b-9...  </span> ▼
<span>⊕ 继续添加</span>		
<span>确定</span> <span>取消</span>		

**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，单击“确认”。

## 添加路由

路由表 rtb-vpc-中转2(默认路由表)

目的地址 ?	下一跳类型 ?	下一跳 ?
<input type="text" value="0.0.0.0/0"/>	<span>对等连接</span> ▼	<span>peering-TtoT(9c68446f-ee77-4581-8...  </span> ▼

----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

## 5.3 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。**

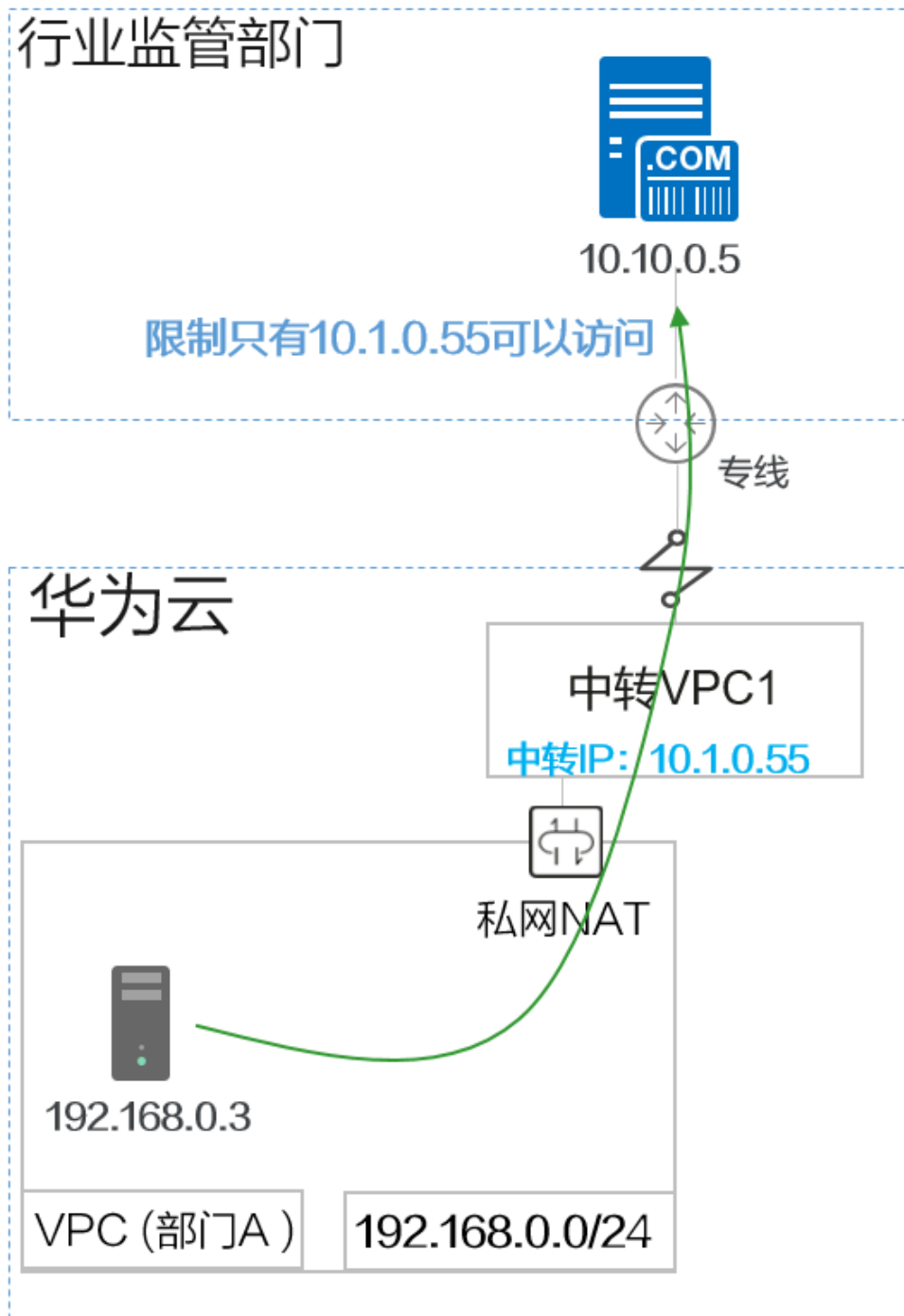
在本最佳实践中，根据行业监管部门的要求，业务上云之后仍需要部门A定期以指定的IP地址（10.1.0.55）访问行业监管部门的主机，上传必要的监管数据。

### 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 5-5 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 5-2 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5-2](#)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

**基本信息**

区域: 华北-北京四  
不同区域的资源之间内网不互通。请选择靠近您客户的区域,可以降低网络时延、提高访问速度。

名称: vpc-监管

IPv4网段: 10 · 10 · 0 · 0 / 24  
建议使用网段: 10.0.0.0/8-24 (选择) 172.16.0.0/12-24 (选择) 192.168.0.0/16-24 (选择)

⚠ 该VPC网段 (10.10.0.0/24) 与当前区域下其他VPC网段重叠,如需使用VPC互通服务,建议...

企业项目: default 新建企业项目 ?

---

高级配置 ▾ 标签 | 描述

---

**默认子网**

可用区: 可用区1 ?

名称: subnet-W

子网IPv4网段: 10 · 10 · 0 · 0 / 24 ? 可用IP数: 251  
子网创建完成后,子网网段无法修改

----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

## 创建安全组

\* 名称

\* 企业项目  [新建企业项目](#) ?

\* 模板

描述

0/255

**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。

< | **sg-监管**

基本信息 | **入方向规则** | 出方向规则 | 关联实例

入方向规则: 7 [教我设置](#)

<input checked="" type="checkbox"/>	优先级 <span>?</span>	策略 <span>?</span>	协议端口 <span>?</span>
<input checked="" type="checkbox"/>	1	允许	ICMP : 全部
<input checked="" type="checkbox"/>	1	允许	TCP : 3389
<input checked="" type="checkbox"/>	1	允许	全部
<input checked="" type="checkbox"/>	1	允许	TCP : 80
<input checked="" type="checkbox"/>	1	允许	TCP : 443
<input checked="" type="checkbox"/>	1	允许	全部
<input checked="" type="checkbox"/>	1	允许	TCP : 22

**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

添加入方向规则 [教我设置](#)

**i** 安全组入方向规则为白名单（允许），放通入方向网络流量。

安全组 sg-监管

如您要添加多条规则，建议单击导入规则以进行批量导入。

优先级 ?	策略	协议端口 ?	类型	源地址 ?
1	允许	全部放通	IPv4	IP地址
		1-65535		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5-2配置监管部门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

弹性云服务器 自定义购买 快速购买

1 基础配置 2 网络配置 3 高级配置 4 确认配置

计费模式 包年/包月 按需计费 竞价计费

区域 华北-北京四 推荐区域 华北-乌兰察布二... (19) 西南-贵阳 华东-上海一 (4)

不同区域的云服务产品之间内网互不相通；请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。

可用区 随机分配 可用区1 可用区2 可用区3

CPU架构 x86计算 鲲鹏计算

规格 最新系列 vCPUs 全部 内存

通用计算增强型 通用计算型 内存优化型 超大内存型 磁盘增强型

规格名称	vCPUs   内存
c6.large.2	2vCPUs   4GiB
c6.3xlarge.4	12vCPUs   48GiB

当前规格 通用计算增强型 | c6.large.2 | 2vCPUs | 4GiB

镜像 公共镜像 私有镜像 共享镜像 市场镜像

CentOS CentOS 8.0 64bit(40GB)

**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5-2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

弹性云服务器 自定义购买 快速购买

① 基础配置 ———— ② 网络配置 ———— ③ 高级配置 ———— ④ 确认配置

网络

vpc-监管(10.10.0.0/24) C

subnet-W(10.10.0.0/24) C 手动分配IP地址 10 · 10 · 0 · 5

可用私有IP数量250个

如需创建新的虚拟私有云，您可前往控制台创建。批量创建云服务器时，指定的IP地址为起始IP地址。

扩展网卡  增加一块网卡 您还可以增加 1 块网卡

---

安全组

sg-监管 (1fa72d41-1452-431d-9750-fc9aeb80f87c) C 新建安全组

安全组类似防火墙功能，是一个逻辑上的分组，用于设置网络访问控制。  
请确保所选安全组已放通22端口（Linux SSH登录），3389端口（Windows远程登录）和 ICMP 协议（Ping）。配置安全组规则  
展开安全组规则

---

弹性公网IP  现在购买  使用已有  暂不购买

不使用弹性公网IP的云服务器不能与互联网互通，仅可作为私有网络中部署业务或者集群所需云服务器进行使用。

**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

弹性云服务器 自定义购买 快速购买

① 基础配置 ———— ② 网络配置 ———— ③ 高级配置 ———— ④ 确认配置

云服务器名称

ecs-监管  允许重名

购买多台云服务器时，支持自动增加数字后缀命名或者自定义规则命名。

登录凭证

密码 密钥对 创建后设置

用户名

root

密码

请牢记密码，如忘记密码可登录ECS控制台重置密码。

确认密码

**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:fed: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

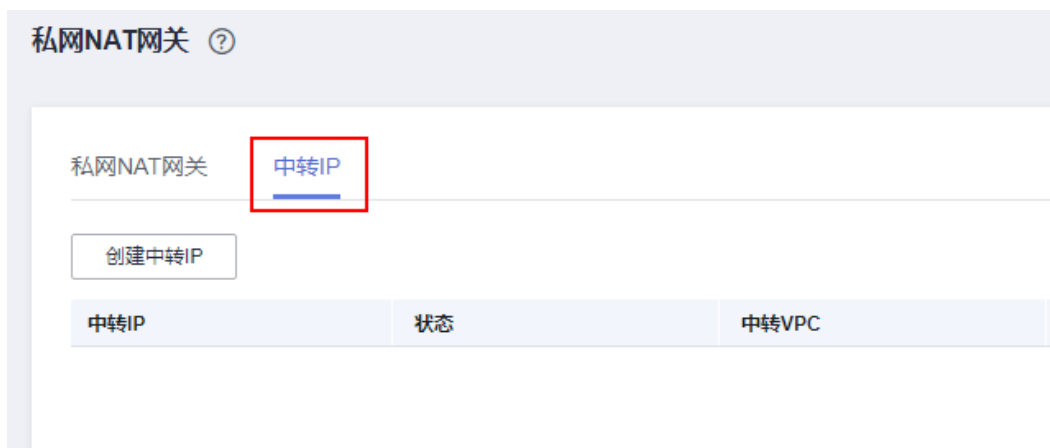
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped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

### 添加SNAT规则

 建议您为SNAT连接数设置告警，实时监控运行状态。

私网NAT网关名称 private-nat-A

\* 子网 使用已有  自定义

subnet-A(192.168.0.0/24) C

\* 中转子网 ? ext\_sub\_T1(10.1.0.0/24) C 查看中转子网

\* 中转IP 10.1.0.55 C 查看中转IP

**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

## 创建对等连接

选择本端VPC

\* 名称

peering-TtoW

\* 本端VPC

vpc-中转1

本端VPC网段 10.1.0.0/24

选择对端VPC

\* 帐户

当前帐户

其他帐户

\* 对端项目

cn-north-4

\* 对端VPC

vpc-监管

对端VPC网段 10.10.0.0/24

----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

## 添加路由

路由表 rtb-vpc-中转(默认路由表)

目的地址 ?	下一跳类型 ?	下一跳 ?
<input type="text" value="0.0.0.0/0"/>	对等连接 ▼	peering-TtoW(d27b997e-c297-417b- ... ▼

+ 继续添加

**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

## 添加路由

路由表 rtb-vpc-监管(默认路由表)

目的地址 ?	下一跳类型 ?	下一跳 ?
<input type="text" value="0.0.0.0/0"/>	对等连接 ▼	peering-TtoW(d27b997e-c297-417b- ... ▼

+ 继续添加

----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
```

```
[root@ecs-a ~]# ping 10.10.0.5
PING 10.10.0.5 (10.10.0.5) 56(84) bytes of data.
64 bytes from 10.10.0.5: icmp_seq=1 ttl=64 time=0.862 ms
64 bytes from 10.10.0.5: icmp_seq=2 ttl=64 time=0.513 ms
^C
--- 10.10.0.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 26ms
rtt min/avg/max/mdev = 0.513/0.687/0.862/0.176 ms
[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 3684 bytes 1256203 (1.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4717 bytes 1032822 (1008.6 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