

NAT Gateway

Best Practices

Issue 01
Date 2026-03-26



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 NAT Gateway Security Best Practices.....	1
2 Using a Public NAT Gateway and Direct Connect to Accelerate Internet Access	3
3 Using the SNAT Rule of a Private NAT Gateway and Direct Connect to Enable Cloud Servers to Access an On-premises Data Center.....	7
4 Using a Private NAT Gateway and Direct Connect to Enable Communications Between a VPC and an On-premises Data Center.....	10
5 Using a Public NAT Gateway and VPC Peering to Enable Communications Between VPCs and the Internet.....	13
6 Using a Private NAT Gateway to Migrate an On-premises Network to the Cloud While Retaining CIDR Blocks.....	16
6.1 Overview.....	16
6.2 Enabling Mutual Access Between Servers in Overlapping Subnets on the Cloud.....	19
6.3 Using a Transit IP Address to Access Hosts Outside a VPC.....	30
7 Using a Private NAT Gateway to Enable an ECS in a VPC to Access a Load Balancer in Another VPC.....	41
8 Using a Public NAT Gateway to Enable Servers to Share an EIP to Access the Internet.....	49
9 Using CFW to Protect Outbound SNAT Traffic.....	55

1 NAT Gateway Security Best Practices

1. Enhance permission management and improve access control.

If you need to perform fine-grained permissions control on your NAT gateways, you can use [Identity and Access Management \(IAM\)](#). For details, see [Permissions Management](#).

2. Properly manage identity authentication to prevent data leaks.

With IAM, NAT Gateway provides three identity authentication methods: username and password, access key, and temporary access key. In addition, [Login Protection](#) and [Login Authentication Policy](#) are provided.

a. Use a temporary AK/SK.

When you use NAT Gateway APIs or SDKs to manage resources, identity authentication is required to ensure the confidentiality, integrity, and correctness of requests. You are advised to configure an IAM agency to obtain a temporary access key, or directly configure temporary AK/SKs for your applications or cloud services. Temporary AK/SKs will expire after a short period, which reduces data leakage risks. For details, see [Temporary Access Keys](#) and [Obtaining Temporary Access Keys and Security Tokens of an Agency](#).

b. Periodically change permanent access keys.

If you have to use a permanent AK/SK pair for access, periodically change it and store it after encryption. This can prevent data leaks in case you lose the preset plaintext credentials. For details, see [Access Keys](#).

c. Regularly change your username and password and avoid weak passwords.

Regularly resetting passwords is one important measure to enhance system and application security. This practice not only lowers the chances of password exposure but also helps you meet compliance requirements, mitigate internal risks, and boost your security awareness. Also, complex passwords are recommended to reduce risks. For details, see [Password Policy](#).

3. Use the latest SDKs for better experience and security.

You are advised to use the latest version of NAT Gateway SDKs to better protect your data. You can download the latest SDKs in your desired language from [NAT Gateway SDKs](#).

4. **Do not use high-risk ports for DNAT rules.**

DNAT enables servers in a VPC to share an EIP to provide services accessible from the Internet. With an EIP, a public NAT gateway can forward all requests to the servers regardless of which port they originated on. However, high-risk ports are blocked by carriers by default. In this case, change [these ports](#) to common ports.

2 Using a Public NAT Gateway and Direct Connect to Accelerate Internet Access

Scenarios

You can add SNAT or DNAT rules to a public NAT gateway to enable a large number of on-premises servers connected to a VPC using Direct Connect to access the Internet or provide services accessible from the Internet, in a secure, reliable, and high-speed manner. This practice can be used in similar scenarios across sectors like Internet, gaming, e-commerce, and finance.

Solution Advantages

With Direct Connect, you can access a VPC on Huawei Cloud over high-performance, low-latency, and secure networks. A Direct Connect connection supports up to 10 Gbit/s of bandwidth, meeting your service requirements.

With SNAT and DNAT of the public NAT gateway, your servers can share an EIP for Internet access, saving costs on EIPs. You can change the type of the public NAT gateway and EIPs bound to it at any time. The configuration is simple and will take effect immediately.

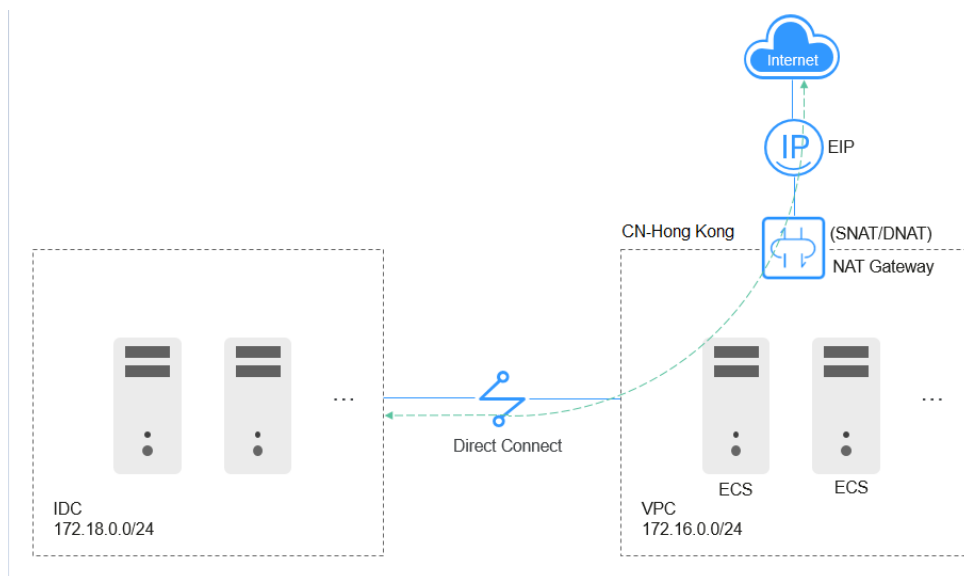
Typical Topology

The CIDR block of your on-premises data center is 172.18.0.0/24, which will access the VPC deployed in the CN-Hong Kong region. The CIDR block of the VPC is 172.16.0.0/24.

Implementation procedure:

1. A Direct Connect connection connects your on-premises data center to the VPC.
2. A public NAT gateway is created in the VPC, enabling Internet connectivity.

Figure 2-1 Networking diagram



Prerequisites

- The default route of your on-premises data center is available for configuring Direct Connect.
- The CIDR block of your on-premises data center cannot overlap with that of the VPC; otherwise, the communications between your on-premises data center and the VPC will fail.

Procedure

Step 1 Create a VPC with a subnet.

For detailed operations, see [Creating a VPC with a Subnet](#).

Step 2 Configure a Direct Connect connection.

Create a Direct Connect connection between your on-premises data center and the VPC (in the CN-Hong Kong region). For details, see [Using Direct Connect to Connect an On-Premises Data Center to the Cloud](#).

NOTE

After the Direct Connect connection is created, configure routes in your on-premises data center as follows:

- **Static:** Add the default route with 0.0.0.0/0 as the destination and set the next hop to the Direct Connect connection.
- **BGP:** The on-premises network can learn the default route using BGP.

Step 3 Buy an EIP and configure a public NAT gateway.

1. Buy an EIP in the CN-Hong Kong region. For details, see [Assigning an EIP](#).
2. Buy a public NAT gateway. For details about how to configure other parameters, see [Buying a Public NAT Gateway](#).
3. Add an SNAT rule and set the CIDR block to that of the Direct Connect connection. For more details, see [Adding an SNAT Rule](#).

Set the CIDR block to **172.18.0.0/24** and select the EIP assigned in step 1.

Figure 2-2 Adding an SNAT rule

Add SNAT Rule
✕

i

- If both an EIP and a NAT gateway are configured for a server, data will be forwarded through the EIP. [View restrictions](#)
- It is not recommended that an SNAT rule and a DNAT rule share the same EIP because there may be service conflicts.
- An SNAT rule cannot share an EIP with a DNAT rule with Port Type set to All ports.

Public NAT Gateway Name
nat-

Scenario

VPC

Direct Connect/Cloud Connect

CIDR Block

Existing

Custom ?

subnet- Q ?

Public IP Address Type

EIP

Select the first 0 records. You can select 20 more EIPs. ? [View EIP](#)

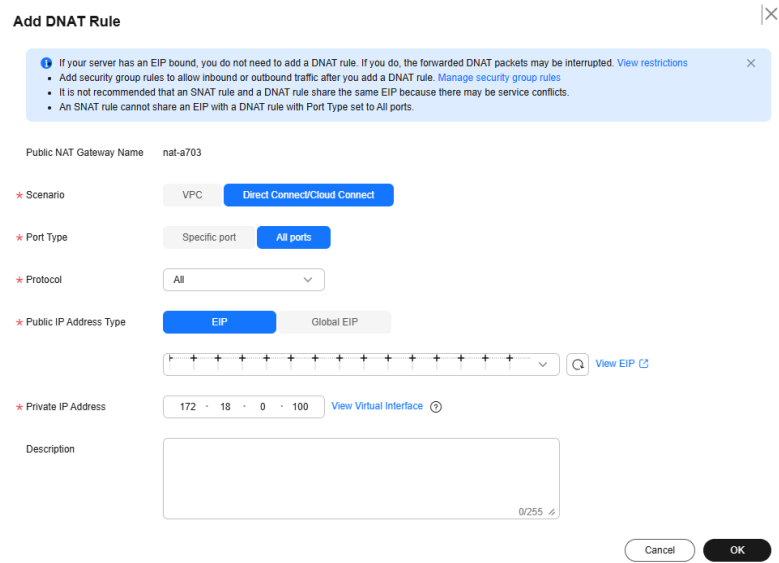
Q Select a property or enter a keyword. Q

EIP	EIP Type	Bandwidth Na...	Bandwidth (M...	Billing Mode	Created ↕	Enterprise Pr...
<div style="display: flex; justify-content: center; align-items: center;"> <div> <p>No data available.</p> <p>Buy EIP</p> </div> </div>						

Cancel
OK

4. Add a DNAT rule. For details, see [Adding a DNAT Rule](#).
Configure the protocol and port type. **All ports** is used as an example. Set **Private IP Address** to **172.18.0.100** and select an EIP.

Figure 2-3 Add DNAT Rule



NOTE

SNAT and DNAT rules are used for different services. If an SNAT rule and a DNAT rule use the same EIP, there may be service conflicts. An SNAT rule cannot share an EIP with a DNAT rule with **Port Type** set to **All ports**.

----End

Verification

Test the network connectivity.

Ping an external IP address, for example, 114.114.114.114, from a server in your on-premises data center.

3 Using the SNAT Rule of a Private NAT Gateway and Direct Connect to Enable Cloud Servers to Access an On-premises Data Center

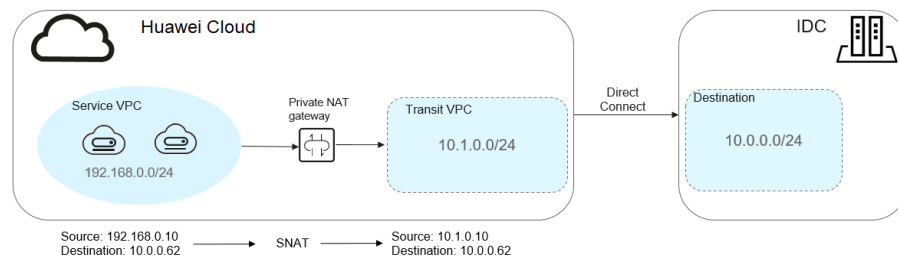
Scenarios

When an ECS in a VPC needs to communicate with an on-premises data center through a Direct Connect connection, the private IP address of the ECS needs to be translated into a private IP address trusted by the on-premises data center.

Solution Architecture

1. A Direct Connect connection connects an on-premises data center to a transit VPC.
2. A private NAT gateway translates the private IP address of the ECS in the service VPC into a transit IP address (private IP address trusted by the on-premises data center) in the transit VPC.

Figure 3-1 Networking diagram



Solution Advantages

In a hybrid cloud network, the private IP addresses of ECSs in the VPC need to be mapped to those trusted by the on-premises data center to meet security compliance requirements.

Constraints

- The CIDR block of your on-premises data center cannot overlap with those of the transit VPC and the service VPC; otherwise, your on-premises data center will be unable to communicate with the service VPC.
- You need to define a CIDR block in the transit VPC to map private IP addresses from the service VPC. Generally, you use a private CIDR block or private IP addresses trusted by your on-premises data center.

Resource Planning

Table 3-1 Resource planning

Resource	Resource Name	Description	Quantity
VPC	VPC-Test01	The service VPC with the CIDR block of 192.168.0.0/24 .	1
	VPC-Test02	The transit VPC with the CIDR block of 10.1.0.0/24 .	1
NAT gateway	NAT-Private-Test	The private NAT gateway deployed in VPC-Test01 .	1
	NAT-Ext-Sub-IP-Test	The transit IP address (10.1.0.10) in the transit VPC (VPC-Test02).	1
Direct Connect connection	DC-Test	The Direct Connect connection that connects the on-premises data center to the transit VPC.	1
ECS	ECS-Test	The ECS (private IP address: 192.168.0.10) purchased and deployed in the service VPC (VPC-Test01).	1
On-premises data center	IDC-Test	CIDR block: 10.0.0.0/24 ; private IP address of an on-premises server: 10.0.0.62	1

NOTE

- In this practice, the private IP address (**192.168.0.10**) of the ECS is mapped to the private IP address (**10.1.0.10**) trusted by the on-premises data center through the private NAT gateway.
- The VPC, NAT gateway, Direct Connect connection, and ECS must be in the same region.

Procedure

1. [Create a service VPC and a transit VPC.](#)
2. [Configure a Direct Connect connection.](#)

3. Buy a private NAT gateway.

Implementation Procedure

Step 1 Create a service VPC and a transit VPC.

For details, see [Creating a VPC with a Subnet](#).

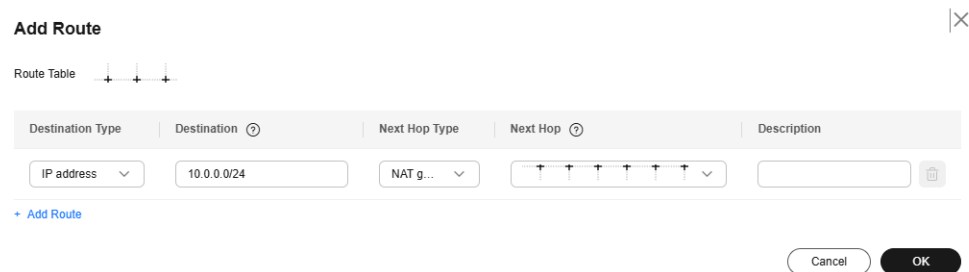
Step 2 Configure a Direct Connect connection.

Create a Direct Connect connection between the on-premises data center and the transit VPC. For details, see [Using Direct Connect to Connect an On-Premises Data Center to the Cloud](#).

Step 3 Buy a private NAT gateway.

- Buy a private NAT gateway in the specified region and select a service VPC.
- Assign a transit IP address. Set **Transit VPC** to **VPC-Test02**. Select **Manual** for **Transit IP Address**, and set **IP Address** to **10.1.0.10**.
- On the **SNAT Rules** tab of the private NAT gateway, click **Add SNAT Rule** and set **Subnet** to **192.168.0.0/24**, the service subnet with the IP addresses that need to access the on-premises data center. Set **Transit IP Address** to the address configured in the previous step.
- Add a route pointing to the private NAT gateway to the route table of the service VPC. Set **Destination** to **10.0.0.0/24**.

Figure 3-2 Adding a route



- Add an inbound security group rule to allow traffic to the destination CIDR block that contains the IP address (**10.0.0.62**) of the on-premises server.

----End

Verification

Test the network connectivity.

Log in to **ECS-Test** in the service VPC and ping the private IP address (**10.0.0.62**) of an on-premises server to verify the network connectivity.

```
[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 Using a Private NAT Gateway and Direct Connect to Enable Communications Between a VPC and an On-premises Data Center

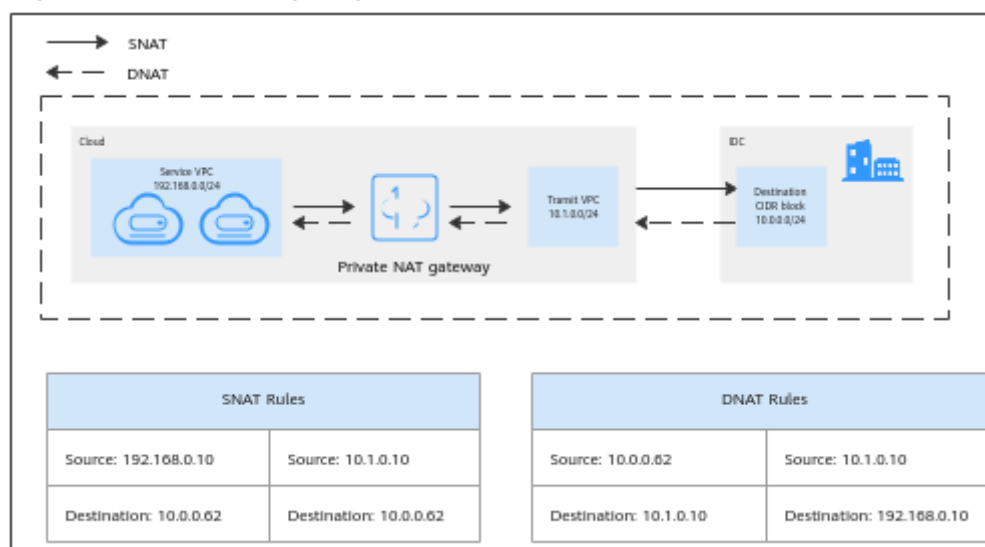
Scenarios

In a hybrid cloud architecture, if the private IP address of a cloud server in a VPC is not trusted by an on-premises data center, the cloud server cannot communicate with the on-premises data center. To address this issue, you can configure a NAT gateway and use Direct Connect or VPN to enable communications between a VPC and an on-premises data center.

Solution Architecture

1. A Direct Connect or VPN connection connects an on-premises data center to a transit VPC.
2. A private NAT gateway translates the source or destination IP address into a transit IP address (private IP address trusted by the on-premises data center) in the transit VPC using an SNAT or DNAT rule.

Figure 4-1 Networking diagram



Solution Advantages

In a hybrid cloud network, the private IP addresses of ECSs in the VPC need to be mapped to those trusted by the on-premises data center to meet security compliance requirements.

Constraints

- The CIDR block of your on-premises data center cannot overlap with those of the transit VPC and the service VPC; otherwise, your on-premises data center will be unable to communicate with the service VPC.
- You need to define a CIDR block in the transit VPC to map private IP addresses from the service VPC. Generally, you use a private CIDR block or private IP addresses trusted by your on-premises data center.

Resource Planning

Table 4-1 Resource planning

Resource	Resource Name	Description	Quantity
VPC	VPC-Test01	The service VPC with the CIDR block of 192.168.0.0/24 .	1
	VPC-Test02	The transit VPC with the CIDR block of 10.1.0.0/24 .	1
NAT gateway	NAT-Private-Test	The private NAT gateway deployed in VPC-Test01 .	1
	NAT-Ext-Sub-IP-Test	The transit IP address (10.1.0.10) in the transit VPC (VPC-Test02).	1
Direct Connect connection	DC-Test	The Direct Connect connection that connects the on-premises data center to the transit VPC.	1
ECS	ECS-Test	The ECS (private IP address: 192.168.0.10) purchased and deployed in the service VPC (VPC-Test01).	1
On-premises data center	IDC-Test	CIDR block: 10.0.0.0/24 ; private IP address of an on-premises server: 10.0.0.62	1

NOTE

- In this practice, the private IP address (**192.168.0.10**) of the ECS is mapped to the private IP address (**10.1.0.10**) trusted by the on-premises data center through the private NAT gateway.
- The VPC, NAT gateway, Direct Connect connection, and ECS must be in the same region.

Procedure

Step 1 Create a service VPC and a transit VPC.

For details, see [Creating a VPC with a Subnet](#).

Step 2 Configure a Direct Connect or VPN connection between the on-premises data center and the transit VPC.

For details, see [Create a Connection](#).

Step 3 Buy a private NAT gateway in the specified region and select the service VPC.

For details, see [Buying a Private NAT Gateway](#).

Step 4 Assign a transit IP address.

Select **VPC-Test02** as the transit VPC and manually assign the transit IP address of **10.1.0.10**.

Step 5 Add an SNAT rule.

On the **SNAT Rules** tab of the private NAT gateway, click **Add SNAT Rule** and set **Subnet** to **192.168.0.0/24**, the service subnet with the IP addresses that need to be mapped. Set **Transit IP Address** to the one assigned in [Step 4](#).

Step 6 Add a DNAT rule.

On the **DNAT Rules** tab of the private NAT gateway, click **Add DNAT Rule**. Set the instance type of the local network to **Server** with the private IP address of 192.168.0.10 and select the transit IP address assigned in [Step 4](#) as the transit IP address of the transit network. For details, see [Adding a DNAT Rule](#).

Step 7 Configure routes.

1. Add a route pointing to the private NAT gateway to the route table of the service VPC. Set **Destination** to **10.0.0.0/24**.
2. Add an inbound security group rule to allow traffic to the destination CIDR block that contains the IP address (**10.0.0.62**) of the on-premises server.

----End

Verifying Network Connectivity

Test the network connectivity.

Log in to **ECS-Test** in the service VPC and ping the private IP address (**10.0.0.62**) of an on-premises server to verify the network connectivity.

```
[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 Using a Public NAT Gateway and VPC Peering to Enable Communications Between VPCs and the Internet

Scenarios

There are two VPCs in the same region: VPC A and VPC B. VPC A has a subnet (**subnet A**), and VPC B has a subnet (**subnet B**). You can create a public NAT gateway in subnet A, and add SNAT and DNAT rules to enable servers in subnet A to access and be accessed from the Internet. Then you can create a VPC peering connection to connect subnet B in VPC B to subnet A in VPC A. In this way, servers in subnet B can use the public NAT gateway in subnet A to access and be accessed from the Internet. You do not need to configure another public NAT gateway for subnet B.

Solution Advantages

Only one public NAT gateway needs to be configured. Servers in the two VPCs can use the same public NAT gateway to communicate with the Internet, saving gateway resources.

Typical Topology

The CIDR block of VPC A is 192.168.0.0/16 and that of subnet A is 192.168.1.0/24.

The CIDR block of VPC B is 192.168.0.0/16 and that of subnet B is 192.168.2.0/24.

Implementation procedure:

1. Create a NAT gateway in VPC A, and add SNAT and DNAT rules.
2. Create a VPC peering connection between subnet A and subnet B, enabling servers in subnet B to use the public NAT gateway in subnet A to access and be accessed from the Internet.

Prerequisites

- If VPCs connected by a VPC peering connection have overlapping CIDR blocks, the connection can only enable communications between specific (non-overlapping) subnets in the VPCs.

- At least one pair of subnets in the two VPCs does not have overlapping CIDR blocks.

Configuring a Public NAT Gateway

Step 1 Buy a public NAT gateway.

Select VPC A for **VPC**. For details about how to configure other parameters, see [Buying a Public NAT Gateway](#).

Step 2 Add SNAT rules.

1. Select **VPC** for **Scenario** and subnet A for **Subnet**. For more details, see [Adding an SNAT Rule](#).
2. Add an SNAT rule for subnet B. Set **Scenario** to **Direct Connect/Cloud Connect** and enter the CIDR block of subnet B.

Step 3 Add DNAT rules.

1. Add a DNAT rule for subnet A. Select **VPC** for **Scenario** and enter an IP address of a server in subnet A for **Private IP Address**. For more details, see [Adding a DNAT Rule](#).
2. Add a DNAT rule for subnet B. Set **Scenario** to **Direct Connect/Cloud Connect** and enter an IP address of a server in subnet B for **Private IP Address**.

----End

Creating a VPC Peering Connection

Step 1 Create VPC A, VPC B, subnet A, and subnet B.

For details, see [Creating a VPC with a Subnet](#).

Step 2 Create a VPC peering connection between subnet A and subnet B.

For detailed operations, see [Creating a VPC Peering Connection to Connect Two VPCs in the Same Account](#).

NOTE

The local VPC is VPC A, and the peer VPC is VPC B.

In addition to the existing local and peer routes, you also need to add a route to the route table of VPC B. Set **Destination** to **0.0.0.0/0** and **Next Hop** to the VPC peering connection between VPC A and VPC B.

----End

Testing Network Connectivity

Test the network connectivity.

Log in to a server in subnet B and ping its EIP. If the following information is displayed, the network is connected.

```
[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
```

Log in to a server that can access the Internet and is not deployed in VPC A or VPC B. Use **curl** to check whether the server can communicate with subnet B via the EIP associated with the DNAT rule configured for subnet B. If the following information is displayed, the network is connected.

```
[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 ~]#
```

6 Using a Private NAT Gateway to Migrate an On-premises Network to the Cloud While Retaining CIDR Blocks

6.1 Overview

Scenarios

The existing network architecture of the on-premises data center needs to be migrated to the cloud without any changes.

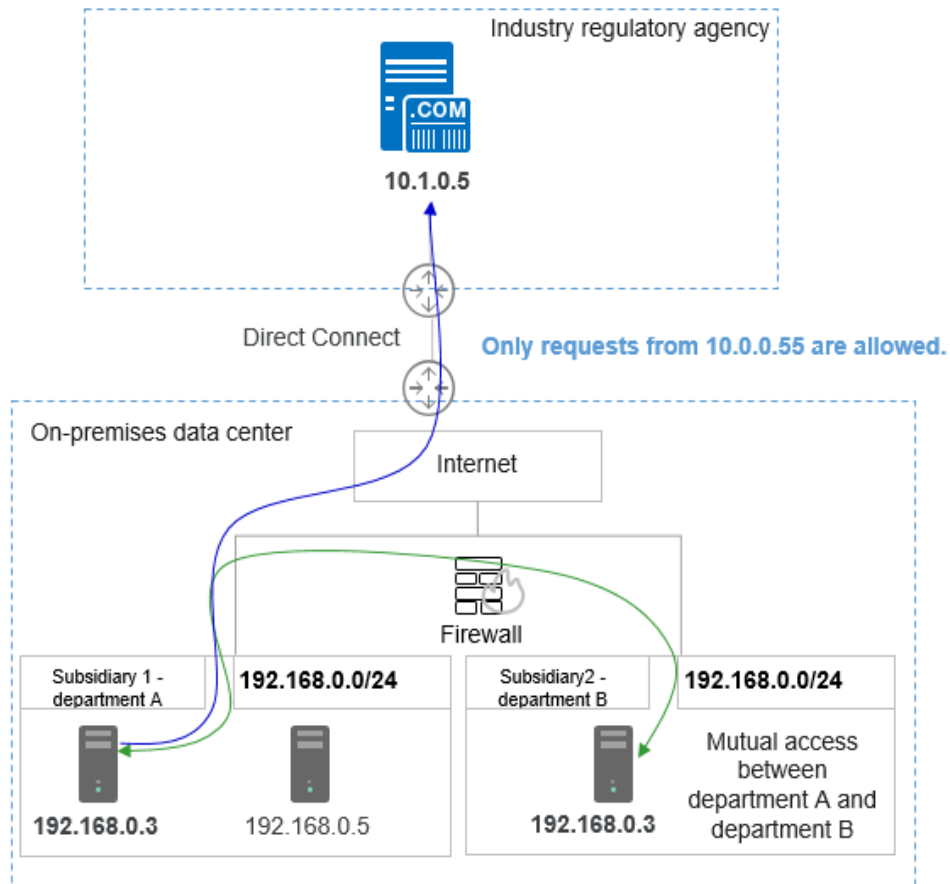
- Servers in two overlapping CIDR blocks in the on-premises data center need to access each other.
- Servers need to access external resources with a specified IP address.

For example:

A company with multiple branches had overlapping subnets for different branch offices. In [Figure 6-1](#), department A and department B are assigned the same CIDR blocks 192.168.0.0/24, and servers on the two CIDR blocks can communicate with each other. In addition, department A needs to periodically use a specified IP address to access archived data of hosts in the industry supervision agency.

Workloads in the on-premises data center were huge and complex. Re-planning and reconstructing CIDR blocks would impact existing workloads. The customer wanted to migrate the existing network to the cloud without any modifications. They needed servers in the overlapping subnets to remain accessible after the migration. Additionally, department A's server had to retain access the industry supervision agency's server via a specific IP address.

Figure 6-1 Overlapping subnets of departments from different subsidiaries



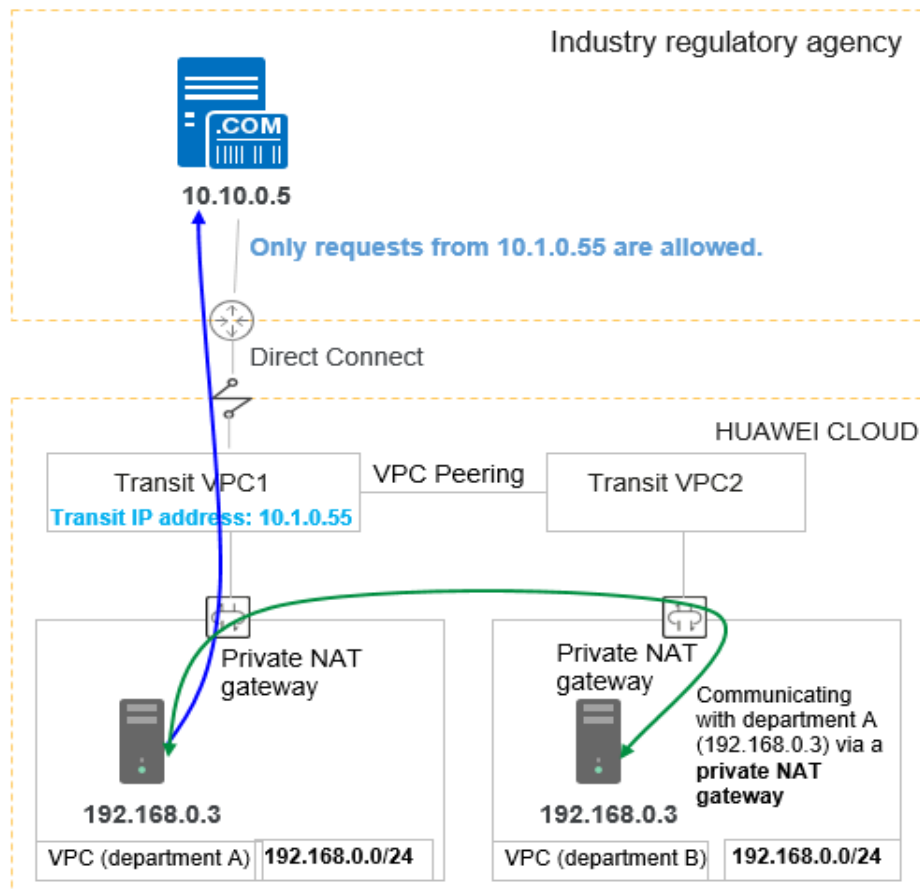
Solution Architecture

Private NAT gateways of Huawei Cloud provide network address translation (NAT) for servers in a VPC to enable mutual access between servers in overlapping subnets of VPCs. This resolves the issue where **VPC peering connections fail when VPCs have overlapping subnet CIDR blocks**.

In **Figure 6-2**:

- The CIDR block (192.168.0.0/24) of department A and department B was migrated to the VPC, and two private NAT gateways were used to enable mutual access between servers from the two departments.
- SNAT rules were configured to map the private IP addresses of servers of department A to 10.1.0.55 to access external servers.

Figure 6-2 Huawei Cloud private NAT gateways



Solution Advantages

- Customers can directly migrate on-premises services to the cloud without reconstructing the existing network architecture, reducing network reconstruction costs.
- Servers in overlapping CIDR blocks can communicate with each other.
- Servers in a private network can access external resources using a specified IP address to meet security requirements.

Constraints

Note the following when using a private NAT gateway:

- Manually add routes in a VPC to connect it to a remote private network through a VPC peering connection, Direct Connect, or VPN connection.
- Only one SNAT rule can be added for each VPC subnet.
- SNAT and DNAT rules cannot share a transit IP address.
- A DNAT rule with **Port Type** set to **All ports** cannot share a transit IP address with a DNAT rule with **Port Type** set to **Specific port**.
- The total number of DNAT and SNAT rules that can be added on a private NAT gateway varies with the private NAT gateway specifications.

- Small: 20 or less
- Medium: 50 or less
- Large: 200 or less
- Extra-large: 500 or less

6.2 Enabling Mutual Access Between Servers in Overlapping Subnets on the Cloud

Scenarios

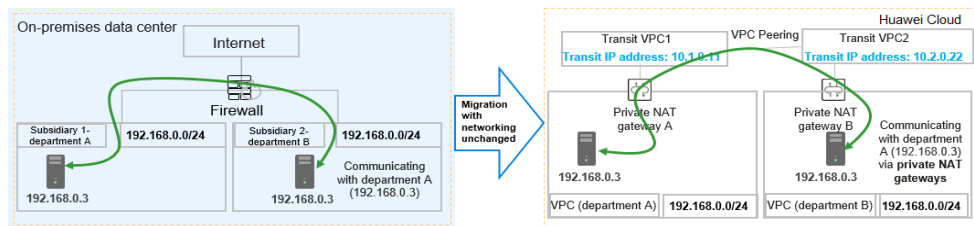
You can migrate an on-premise network to the cloud while keeping the network architecture unchanged, allowing servers in two overlapping CIDR blocks in the on-premises data center to access each other.

In this practice, departments A and B deploy workloads in overlapping on-premises subnets. They migrate these workloads to the cloud while keeping their subnet CIDR blocks unchanged. After the migration, the overlapping subnets can still communicate with each other.

Solution Architecture

- Departments A and B use the same CIDR block (192.168.0.0/24). To keep the network unchanged, you need to create two VPCs with the same CIDR block on the cloud.
- Each department's VPC has its own private NAT gateway. Servers in departments A and B share the same IP address (192.168.0.3), but they are mapped to different transit IP addresses (10.1.0.11 for department A and 10.2.0.22 for department B). These transit IP addresses enable the two servers to communicate with each other.

Figure 6-3 Logical topology



NOTE

Manually configure the following routes to ensure traffic forwarding from:

- VPC (department A) to private NAT gateway A
- Transit VPC1 to the VPC peering connection
- Transit VPC2 to the VPC peering connection
- VPC (department B) to private NAT gateway B

Solution Advantages

CIDR blocks of departments A and B are kept unchanged after on-premises workloads are migrated to the cloud.

Resource Planning

Table 6-1 Resource planning

Resource	Name	CIDR Block/IP Address	Subnet Name	Description
VPC (CN-Hong Kong)	vpc-departmentA	192.168.0.0/24	subnet-A	VPC that workloads of department A are migrated to.
	vpc-departmentB	192.168.0.0/24	subnet-B	VPC that workloads of department B are migrated to.
	vpc-transit1	10.1.0.0/24	ext_sub_T1	Transit VPC required by the private NAT gateway of department A.
	vpc-transit2	10.2.0.0/24	ext_sub_T2	Transit VPC required by the private NAT gateway of department B.
Transit IP address (vpc-transit)	transit IP-departmentA	10.1.0.11	N/A	IP address used by department A to provide services accessible from other departments. Department B can use this IP address to access servers of department A.
	transit IP-departmentB	10.2.0.22	N/A	IP address used by department B to provide services accessible from other departments. Department A can use this IP address to access servers of department B.
ECS (CN-Hong Kong)	ecs-departmentA	192.168.0.3	N/A	Server for deploying workloads of department A. It can communicate with the server of department B.
	ecs-departmentB	192.168.0.3	N/A	Server for deploying workloads of department B. It can communicate with the server of department A.

Resource	Name	CIDR Block/IP Address	Subnet Name	Description
Private NAT gateways	private-nat-A	N/A	N/A	Private NAT gateway configured in vpc-departmentA .
	private-nat-B	N/A	N/A	Private NAT gateway configured in vpc-departmentB .

Prerequisites

- There is a HUAWEI ID.
- Your account is not in arrears and the account balance is sufficient to pay for the resources involved in this best practice.

Procedure

1. [Creating VPCs](#)
2. [Creating ECSs](#)
3. [Assigning Transit IP Addresses](#)
4. [Buying a Private NAT Gateway and Adding Rules](#)
5. [Configuring a Route for Directing Traffic from a Server to a Private NAT Gateway](#)
6. [Configuring a VPC Peering Connection Between vpc-transit1 and vpc-transit2](#)
7. [Verifying Connectivity Between the Server in Department A and That in Department B](#)

Creating VPCs

Step 1 Go to the [Create VPC](#) page.

Step 2 On the **Create VPC** page, configure the VPC for department A based on [Table 6-1](#) and click **Create Now**.

- **Region:** Select CN-Hong Kong.
- **Name:** Set it to **vpc-departmentA**.
- **IPv4 CIDR Block:** Set it to **192.168.0.0/24**.
- **Subnet Name:** Set it to **subnet-A**.
- **IPv4 CIDR Block:** Retain the default value.
- Retain the default values for other parameters or configure them as prompted.

Figure 6-4 Create VPC

< Create VPC ⓘ

Basic Configuration

Region
CN North-Beijing1

Regions are geographic areas isolated from each other. For low network latency and quick resource access, select the region nearest to where your services will be accessed.

Virtual Private Cloud

Name
vpc-departmentA

IPv4 CIDR Block ⓘ
192 . 168 . 0 . 0 / 24

• Recommended: 10.0.0/8-24 Select | 172.16.0.0/12-24 Select | 192.168.0.0/16-24 Select
• To enable communications between VPCs or between a VPC and an on-premises data center, ensure their CIDR blocks do not overlap. [Learn more about network planning](#)

Enterprise Project ⓘ
default

More (Optional)
Tag: -- Description: --

Subnet 1

Subnet Name
subnet-A

CIDR Block
192 . 168 . 0 . 0 / 24 Available IP Addresses: 251

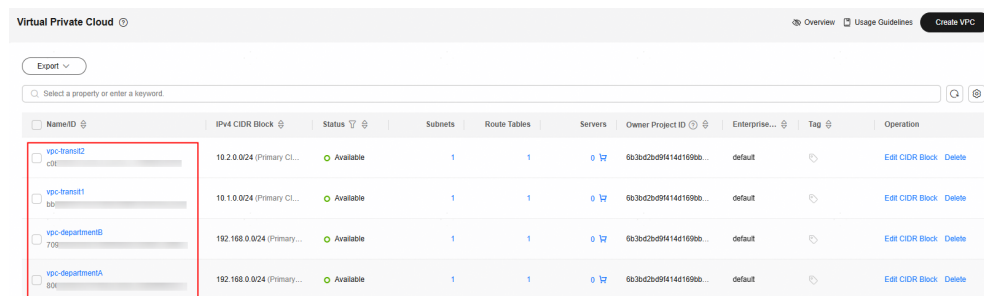
⚠ The CIDR block cannot be modified after the subnet is created. Before creating a subnet, [plan subnet CIDR blocks](#) as required.

Associated Route Table ⓘ
Default

Advanced Settings (Optional)

Step 3 Repeat the above steps to create all required VPCs in [Table 6-1](#).

- **Region:** Select **CN-Hong Kong**.
- **Name:** Set it to **vpc-departmentB**.
- **IPv4 CIDR Block:** Set it to **192.168.0.0/24**.
- **Subnet Name:** Set it to **subnet-B**.
- **IPv4 CIDR Block:** Retain the default value.
- Retain the default values for other parameters or configure them as prompted.

Figure 6-5 Creating all required VPCs

NameID	IPv4 CIDR Block	Status	Subnets	Route Tables	Servers	Owner Project ID	Enterprise...	Tag	Operation
vpc-transit2 c8f	19.2.0.0/24 (Primary CL...	Available	1	1	0	663bc2bd9f414d1690b...	default		Edit CIDR Block Delete
vpc-transit1 bb	19.1.0.0/24 (Primary CL...	Available	1	1	0	663bc2bd9f414d1690b...	default		Edit CIDR Block Delete
vpc-departmentB 79b	192.168.0.0/24 (Primary...	Available	1	1	0	663bc2bd9f414d1690b...	default		Edit CIDR Block Delete
vpc-departmentA 80c	192.168.0.0/24 (Primary...	Available	1	1	0	663bc2bd9f414d1690b...	default		Edit CIDR Block Delete

----End

Creating ECSs

- Step 1** Under **Compute**, select **Elastic Cloud Server**. On the **Elastic Cloud Server** page, click **Buy ECS**.
- Step 2** On the **Buy ECS** page, configure the basic information about the ECS of department A based on [Table 6-1](#).
 - **Billing Mode:** Select **Pay-per-use**.
 - **Region:** Select **CN-Hong Kong**.
 - **Specifications:** You can select ECS specifications based on your project requirements. This practice uses **c6.large.2** as an example.
 - **Image:** Select a public image as needed. This practice uses a CentOS 8.0 image.
 - Retain the default values for other parameters or configure them as prompted.
- Step 3** Configure the network information for the ECS of department A.
 - **Network:** Select **vpc-departmentA**, choose **Manually specify IP address**, and set the IP address to **192.168.0.3** planned in [Table 6-1](#).
 - **Security Group:** Select **Sys-FullAccess**. For testing purposes, choose a security group that allows all inbound and outbound traffic. You may pick another security group depending on your specific needs.
 - **EIP:** Select **Not required**.
 - Retain the default values for other parameters or configure them as prompted.
- Step 4** Configure the ECS name, password, and other information.
 - **ECS Name:** Set it to **ecs-departmentA**.
 - **Login Mode:** Select **Password** and enter a password.
 - For parameters not mentioned, retain their default values or configure them as prompted.
- Step 5** Confirm the ECS information, set the number of ECSs you want to create, and click **Submit**.
- Step 6** In the ECS list, locate the ECS for department A and click **Remote Login** in the **Operation** column. In the displayed dialog box, click **Log In** under **Other Login Modes**.

Step 7 Log in to the ECS as user **root** and check whether the private IP address of the ECS is the one you planned.

```
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

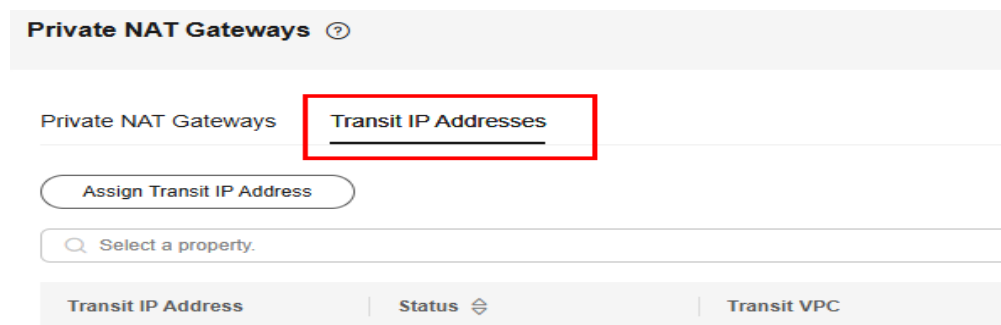
[root@ecs-a ~]# _
```

Step 8 Repeat **Step 1** through **9** to create other ECSs as planned.
----End

Assigning Transit IP Addresses

Step 1 On the management console, under **Networking**, select **NAT Gateway**. In the left navigation pane, choose **Private NAT Gateways**. Click the **Transit IP Addresses** tab.

Figure 6-6 Assigning a transit IP address



Step 2 Click **Assign Transit IP Address**.

Step 3 In the **Assign Transit IP Address** dialog box, assign a transit IP address for department A based on **Table 6-1**.

- **Transit VPC:** Select **vpc-transit1**.
- **Transit Subnets:** Select **ext_sub_T1**.
- **Transit IP Address:** Select **Manual**.
- **IP Address:** Enter **10.1.0.11**.

Step 4 Click **OK**.

Step 5 Repeat **1** through **4** to assign a transit IP address (10.2.0.22) for department B.

- **Transit VPC:** Select **vpc-transit2**.
- **Transit Subnet:** Select **ext_sub_T2**.
- **Transit IP Address:** Select **Manual**.
- **IP Address:** Enter **10.2.0.22**.

----End

Buying a Private NAT Gateway and Adding Rules

Step 1 Go back to the **Private NAT Gateways** page and click **Buy Private NAT Gateway** in the upper right corner.

Step 2 Configure parameters for creating a private NAT gateway for department A.

- **Region:** Select **CN-Hong Kong**.
- **Name:** Set it to **private-nat-A**.
- **VPC:** Select **vpc-departmentA**.
- Retain the default values for other parameters or configure them as prompted.

Step 3 Click **Next**.

Step 4 On the **Private NAT Gateways** tab, click the name of the private NAT gateway on which you need to add a DNAT rule.

Step 5 Switch to the **DNAT Rules** tab and click **Add DNAT Rule**.

Step 6 Configure DNAT rule parameters and click **OK**.

- **Port Type:** Select **All ports**.
- **Instance Type:** Select **Server** and the ECS of department A.
- **Transit IP Address:** Enter **10.1.0.11**.
- **Transit Subnet:** Select **ext_sub_T1**.

Step 7 Go back to the **Private NAT Gateways** page and click **Buy Private NAT Gateway** in the upper right corner.

Step 8 Configure parameters for creating a private NAT gateway for department B.

- **Region:** Select **CN-Hong Kong**.
- **Name:** Set it to **private-nat-B**.
- **VPC:** Select **vpc-departmentB**.
- Retain the default values for other parameters or configure them as prompted.

Step 9 Click **Next**.

- Step 10** On the **Private NAT Gateways** tab, click the name of the private NAT gateway on which you need to add a DNAT rule.
- Step 11** Switch to the **DNAT Rules** tab and click **Add DNAT Rule**.
- Step 12** Configure DNAT rule parameters and click **OK**.
- **Port Type:** Select **All ports**.
 - **Instance Type:** Select **Server** and the ECS of department B.
 - **Transit IP Address:** Enter **10.2.0.22**.
 - **Transit Subnet:** Select **ext_sub_T2**.

Figure 6-7 Adding a DNAT rule

Add DNAT Rule

Private NAT Gateway Name
private-nat-A

Port Type
Specific port **All ports**

The private NAT gateway directs all requests received by the transit IP address to the private IP address of the destination cloud server.

Protocol
All

Instance Type
Server Virtual IP address Load balancer Custom

Select a property.

Name	Status	Private IP Address	VPC	Enterprise Project
ecs-departmentB	Running	192.168.0.3	vpc-departmentB	default

Total Records: 1

NIC
IP: 192.168.0.3, MAC: fa:16:3e:14:6c:6f Primary NIC

Transit IP Address
Select a property or enter a keyword.

Transit IP Address	Status	Transit VPC	Transit Subnet	Assigned	Enterprise Project
10.2.0.22 587a46b5-3885-4632-9...	Running	VPC-B 3fe141f2-c895-4f16-...	est_sbu_T2 10.2.0.0/24	Jun 29, 2025 22:34:...	default

Cancel **OK**

----End

Configuring a Route for Directing Traffic from a Server to a Private NAT Gateway

- Step 1** Choose **Networking > Virtual Private Cloud**. In the navigation pane on the left, choose **Route Tables**.
- Step 2** Click **rtb-vpc-departmentA**. On the **Summary** page, click **Add Route**.
- Step 3** Configure a route for the server in department A to access the private NAT gateway of department A and click **OK**.
- **Destination:** Enter **0.0.0.0/0**. (In actual operations, configure this parameter based on service requirements.)

- **Next Hop Type:** Select **NAT gateway**.
- **Next Hop:** The system automatically displays the private NAT gateway of department A.

Figure 6-8 Adding a route

The screenshot shows a dialog box titled "Add Route" for the route table "rtb-vpc-departmentA". It contains a table with the following columns: Destination Type, Destination, Next Hop Type, Next Hop, and Description. The values are: IP address, 0.0.0.0/1, NAT gateway, private-nat-A(7331ab41-a692-...), and an empty field. There is an "Add Route" button and "Cancel" and "OK" buttons at the bottom right.

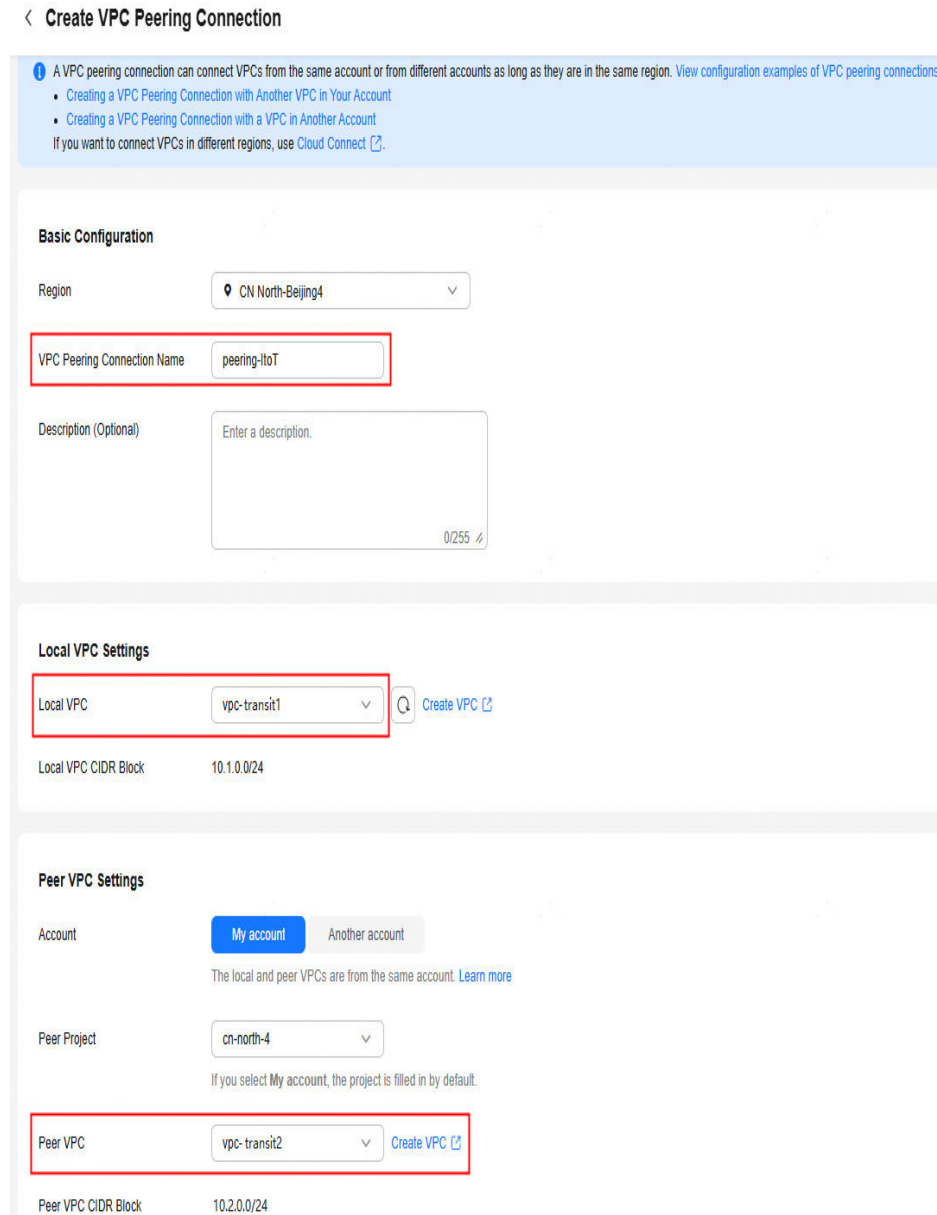
- Step 4** Go back to the **Route Tables** page, click **rtb-vpc-departmentB**, and click **Add Route**.
- Step 5** Configure a route for the server in department B to access the private NAT gateway of department B and click **OK**.
- **Destination:** Set it to **0.0.0.0/0**.
 - **Next Hop Type:** Select **NAT gateway**.
 - **Next Hop:** The system automatically displays the private NAT gateway of department B.

----End

Configuring a VPC Peering Connection Between vpc-transit1 and vpc-transit2

- Step 1** Under **Networking**, select **Virtual Private Cloud**. In the navigation pane on the left, choose **VPC Peering Connections**.
- Step 2** Click **Create VPC Peering Connection**.
- Step 3** Configure **vpc-transit1** as the local VPC and **vpc-transit2** as the peer VPC. Configure the following parameters and click **Create Now**.
- **VPC Peering Connection Name:** **peering-TtoT**
 - **Local VPC:** Select **vpc-transit1**.
 - **Peer VPC:** Select **vpc-transit2**.
 - Retain the default values for other parameters or configure them as prompted.

Figure 6-9 Creating a VPC peering connection



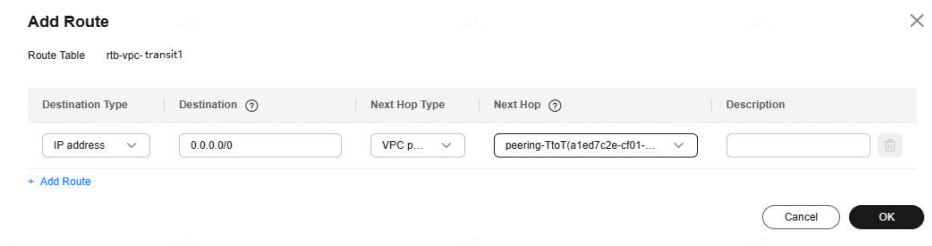
Step 4 Go back to the **VPC Peering Connections** page. In the navigation pane on the left, choose **Route Tables**.

Step 5 Click **rtb-vpc-transit1**. On the **Summary** page, click **Add Route**.

Step 6 Configure the route for directing traffic from **vpc-transit1** to **peering-TtoT** and click **OK**.

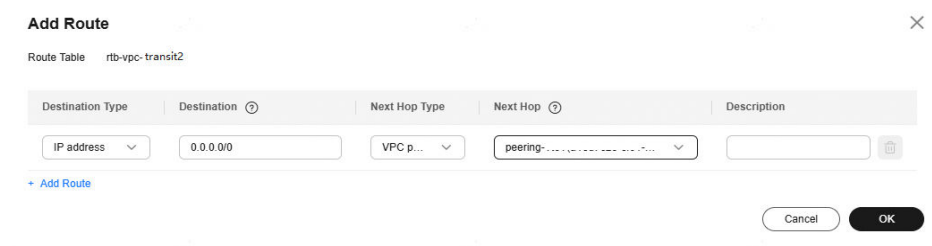
- **Destination:** Set it to **0.0.0.0/0**.
- **Next Hop Type:** Select **VPC peering connection**.
- **Next Hop:** The system automatically displays the VPC peering connection.

Figure 6-10 Adding a route



Step 7 Repeat 5 and 6 (selecting `rtb-vpc-transit2`) to configure the route for directing traffic from `vpc-transit2` to `peering-TtoT`.

Figure 6-11 Adding a route



----End

Verifying Connectivity Between the Server in Department A and That in Department B

Step 1 Under **Compute**, select **Elastic Cloud Server**. Log in to `ecs-departmentA` and `ecs-departmentB` using VNC, respectively.

Step 2 On `ecs-departmentA`, verify that it can access the server in department B:
`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
```

Step 3 On `ecs-departmentB`, verify that it can access the server in department A:

```
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
```

The servers in the overlapping subnets can now communicate with each other through the private NAT gateway.

----End

6.3 Using a Transit IP Address to Access Hosts Outside a VPC

Scenarios

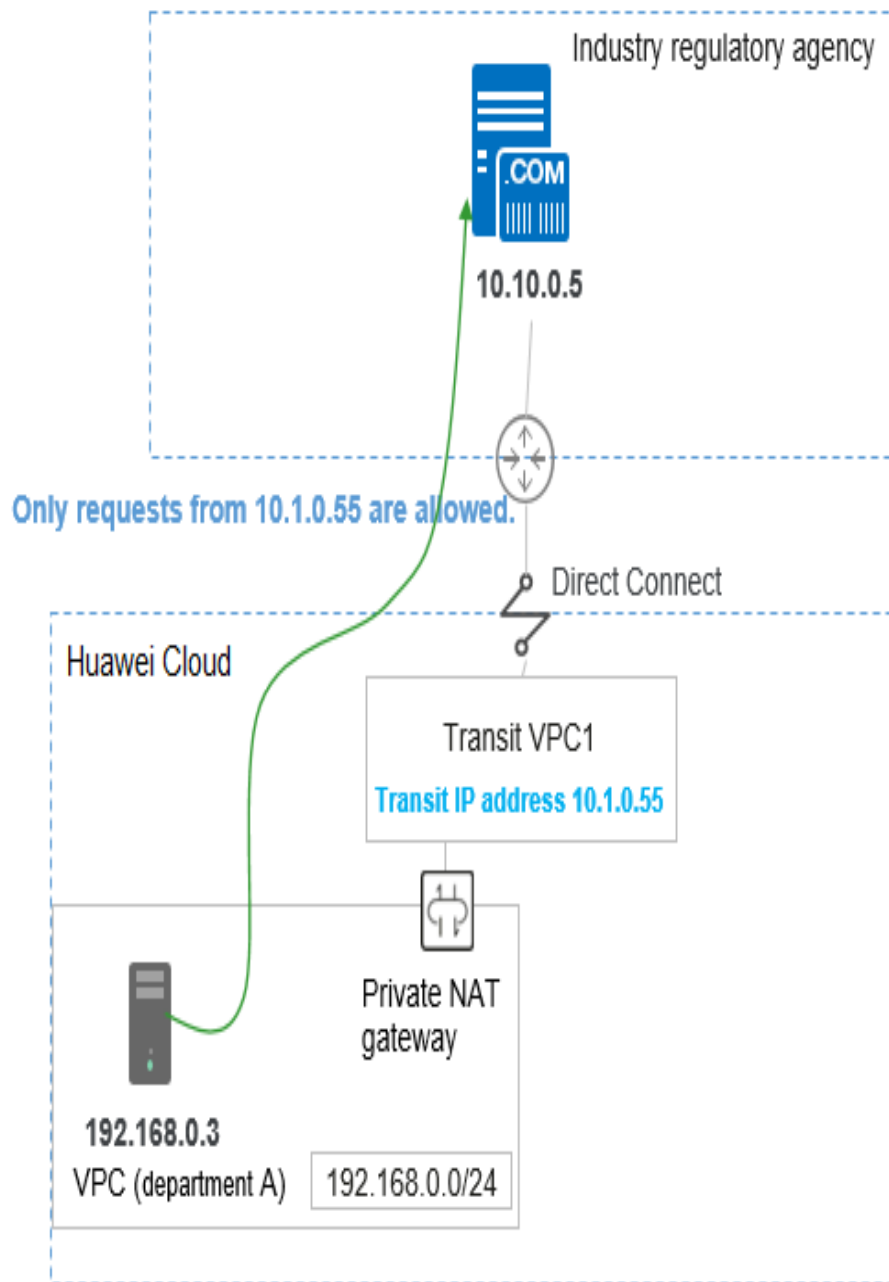
The existing network architecture of the on-premises data center needs to be migrated to the cloud without any changes. **In addition, servers can access external resources with a specified IP address.**

In this best practice, department A needs to use a specified IP address (10.1.0.55) to access servers in a regulatory agency to upload required data after migrating its workloads to the cloud.

Solution Architecture

- The regulatory agency allows requests only from specified IP address (10.1.0.55).
- The server (192.168.0.3) in department A uses a private NAT gateway to translate 192.168.0.3 to the specified IP address (10.1.0.55) to periodically access the industry regulatory agency server (10.10.0.5).

Figure 6-12 Logical topology



Solution Advantages

You can assign a transit IP address to allow all servers in a VPC to use it to access hosts outside a VPC.

Resource Planning

Table 6-2 Resource planning

Resource	Name	CIDR Block/IP Address	Subnet Name	Description
VPC (CN-Hong Kong)	vpc-departmentA	192.168.0.0/24	subnet-A	VPC that workloads of department A are migrated to.
	vpc-transit1	10.1.0.0/24	ext_sub_T1	Transit VPC required by the private NAT gateway.
	vpc-regulation	10.10.0.0/24	subnet-W	Simulated VPC of the regulatory agency.
ECS (CN-Hong Kong)	ecs-departmentA	192.168.0.3	N/A	Server for deploying workloads of department A. It can access servers in the industry regulatory agency.
	ecs-regulation	10.10.0.5	N/A	Simulated host of the regulatory agency.
Transit IP address (vpc-transit1)	transit IP-departmentA	10.1.0.55	N/A	IP address that can be used by servers in department A to access the regulatory agency.

Prerequisites

- There is a HUAWEI ID.
- Your account is not in arrears and the account balance is sufficient to pay for the resources involved in this best practice.
- There is a private NAT gateway.
- You have performed operations in [Enabling Mutual Access Between Servers in Overlapping Subnets on the Cloud](#).

Procedure

1. [Creating a VPC](#)
2. [Creating a Security Group](#)
3. [Creating an ECS](#)
4. [Configuring a Private NAT Gateway](#)
5. [Configuring a VPC Peering Connection](#)
6. [Configuring Routes](#)

7. Verifying that Department A Can Access the Regulatory Agency

Creating a VPC

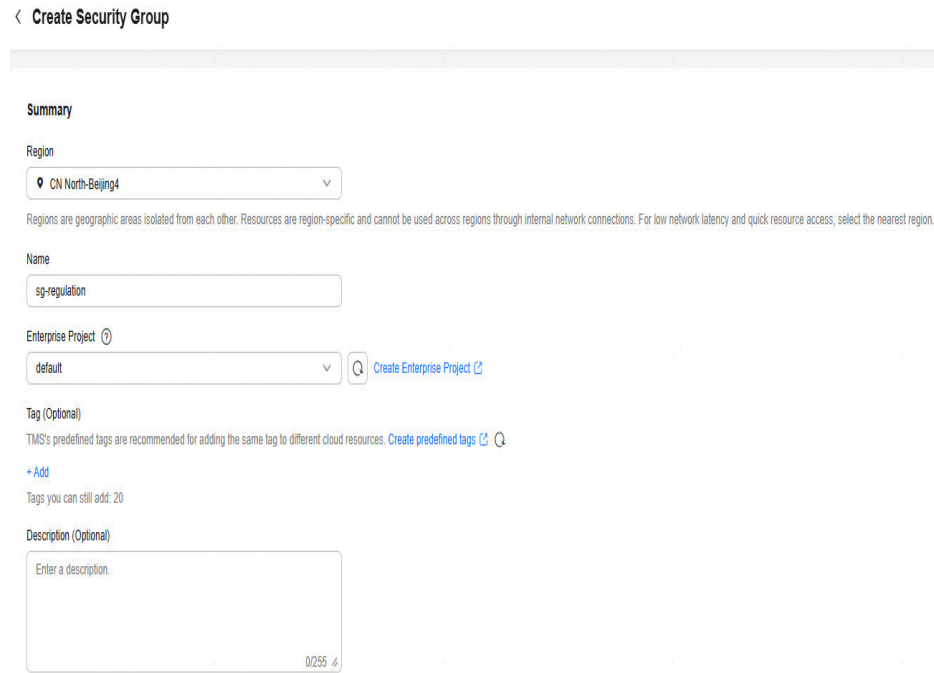
- Step 1** Log in to the Huawei Cloud management console and select the **CN-Hong Kong** region.
- Step 2** Under **Networking**, select **Virtual Private Cloud**. On the **Virtual Private Cloud** page displayed, click **Create VPC**.
- Step 3** Configure a VPC for the regulatory agency based on **Table 6-2** and click **Create Now**.
- **Region:** Select **CN-Hong Kong**.
 - **Name:** Set it to **vpc-regulation**.
 - **IPv4 CIDR Block:** Set it to **10.10.0.0/24**.
 - **Subnet Name:** Set it to **subnet-W**.
 - **IPv4 CIDR Block:** Retain the default value.
 - Retain the default values for other parameters or configure them as prompted.

----End

Creating a Security Group

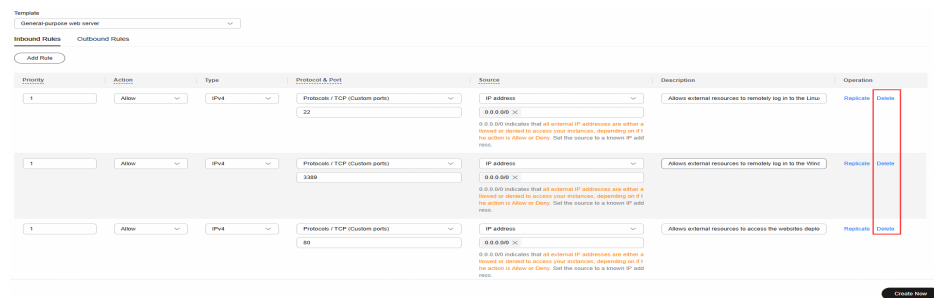
- Step 1** Under **Networking**, select **Virtual Private Cloud**. In the navigation pane on the left, choose **Access Control > Security Groups** and click **Create Security Group** in the upper right corner.
- Step 2** Configure the security group parameters and click **Create Now**.
- **Name:** Set it to **sg-regulation**.
 - **Template:** Select **General-purpose web server**.
 - Retain the default values for other parameters or configure them as prompted.

Figure 6-13 Creating a security group



Step 3 In the **Inbound Rules** tab and delete all existing rules.

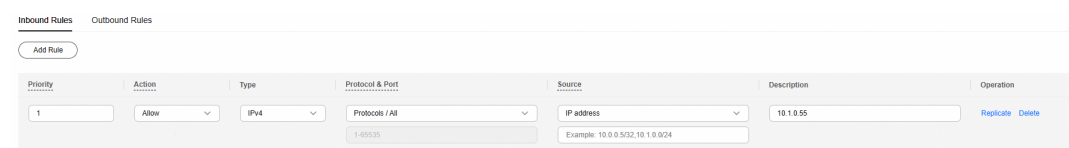
Figure 6-14 Inbound rules



Step 4 Click **Add Rule** to allow only the IP address 10.1.0.55 to access the regulatory agency server. Configure the following parameters and click **OK**.

- **Priority:** Set it to **1**.
- **Action:** Select **Allow**.
- **Type:** Select **IPv4**.
- **Protocol & Port:** Select **Protocols/All**.
- **Source:** Enter **10.1.0.55**.

Figure 6-15 Adding a rule



----End

Creating an ECS

- Step 1** Under **Compute**, select **Elastic Cloud Server**. On the **Elastic Cloud Server** page, click **Buy ECS**.
- Step 2** Configure the basic information about the ECS of the regulatory department based on [Table 6-2](#).
- **Billing Mode:** Select **Pay-per-use**.
 - **Region:** Select **CN-Hong Kong**.
 - **Specifications:** You can select ECS specifications based on your project requirements. This practice uses **c6.large.2** as an example.
 - **Image:** Select a public image as needed. This practice uses a CentOS 8.0 image as an example.
 - Retain the default values for other parameters or configure them as prompted.
- Step 3** Configure the network information for the ECS of the regulatory department.
- **Network:** Select **vpc-regulation**, choose **Manually specify IP address**, and set the IP address to **10.10.0.5** planned in [Table 6-2](#).
 - **Security Group:** Select **sg-regulation**.
 - **EIP:** Select **Not required**.
 - Retain the default values for other parameters or configure them as prompted.
- Step 4** Configure the ECS name, password, and other information.
- **ECS Name:** Set it to **ecs-regulation**.
 - **Login Mode:** Select **Password** and enter a password.
 - Retain the default values for other parameters or configure them as prompted.
- Step 5** Confirm the ECS information, read and select the agreement, and click **Submit**.
- Step 6** In the ECS list, locate the ECS for the regulatory agency and click **Remote Login** in the **Operation** column. In the displayed dialog box, click **Log In** under **Other Login Modes**.
- Step 7** Log in to the ECS as user **root** and check whether the private IP address of the ECS is the one you planned.

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
```

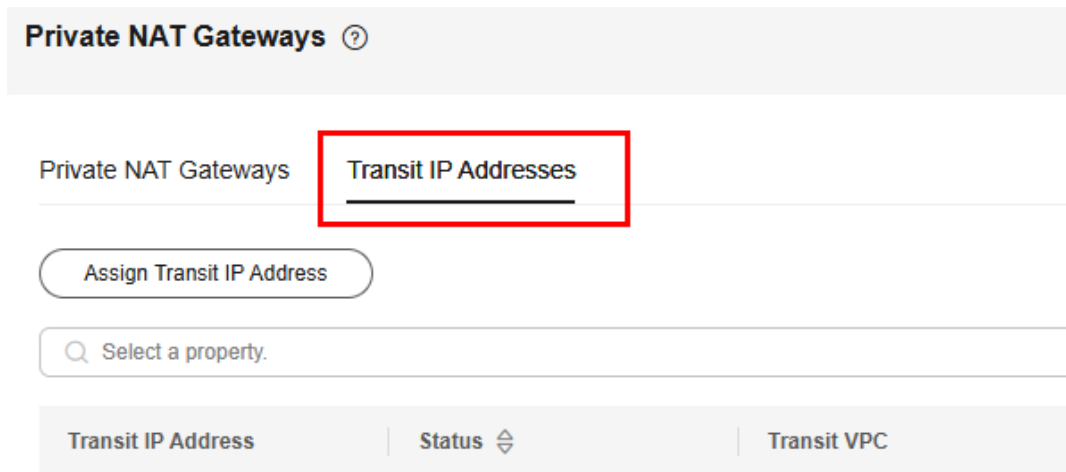
----End

Configuring a Private NAT Gateway

Assigning a Transit IP Address

- Step 1** On the management console, under **Networking**, select **NAT Gateway**. In the left navigation pane, choose **Private NAT Gateways**. Click the **Transit IP Addresses** tab.

Figure 6-16 Assigning a transit IP address



- Step 2** Click **Assign Transit IP Address** and configure the parameters as follows:

- **Transit VPC:** Select **vpc-transit1**.
- **Transit Subnets:** Select **ext_sub_T1**.

- **Transit IP Address:** Select **Manual**.
- **IP Address:** Enter **10.1.0.55**.

Step 3 Click the **Private NAT Gateways** tab and click **private-nat-A**.

Step 4 On the **SNAT Rules** tab, click **Add SNAT Rule**.

- **Subnet:** Select **Existing**. The system automatically displays the subnet of department A.
- **Transit Subnet:** Select **ext_sub_T1**.
- **Transit IP Address:** Enter **10.1.0.55**.

Figure 6-17 Adding an SNAT rule

Add SNAT Rule

Private NAT Gateway Name
private-nat-A

Local VPC
vpc-departmentA

Subnet
Existing Custom
subnet-A (192.168.0.0/24)

Monitoring
You are advised to create alarm rules in [Cloud Eye](#) to monitor your SNAT connections.

Transit IP Address
Up to 20 transit IP addresses from the same transit subnet can be selected.
Select a property or enter a keyword.

<input checked="" type="checkbox"/> Transit IP Address	Status	Transit VPC	Transit Subnet	Assigned	Enterprise Project
<input checked="" type="checkbox"/> 10.1.0.55 72e3a6ad-734c-4a7f-...	Running	vpc-transit1 1bc88dc7-def4-42d...	ext_sub_T1 10.1.0.0/24	Jan 28, 2026 11:19...	default

Total Records: 1
Items selected: 1
10.1.0.55

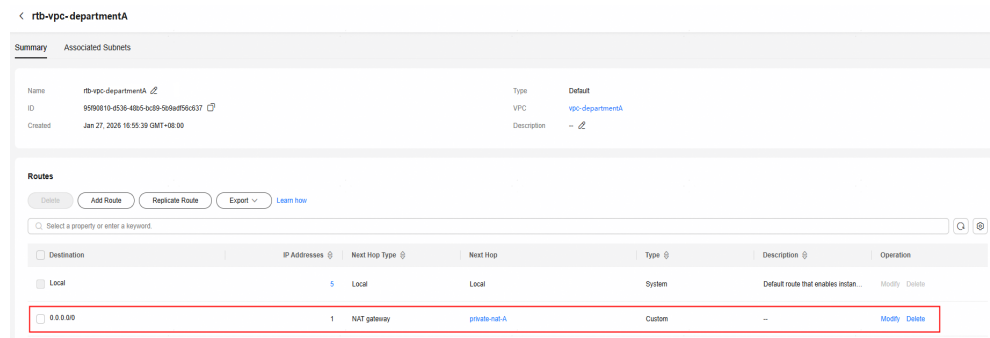
Description (Optional)
Enter a description.

Cancel OK

Step 5 After the SNAT rule parameters are configured, click **OK**.

Step 6 Go back to **Network Console**. In the navigation pane on the left, choose **Route Tables** and click **rtb-vpc-departmentA**. Confirm that the route for directing traffic from the department A's server to private NAT gateway **private-nat A** has been added.

Figure 6-18 Confirming the route information



----End

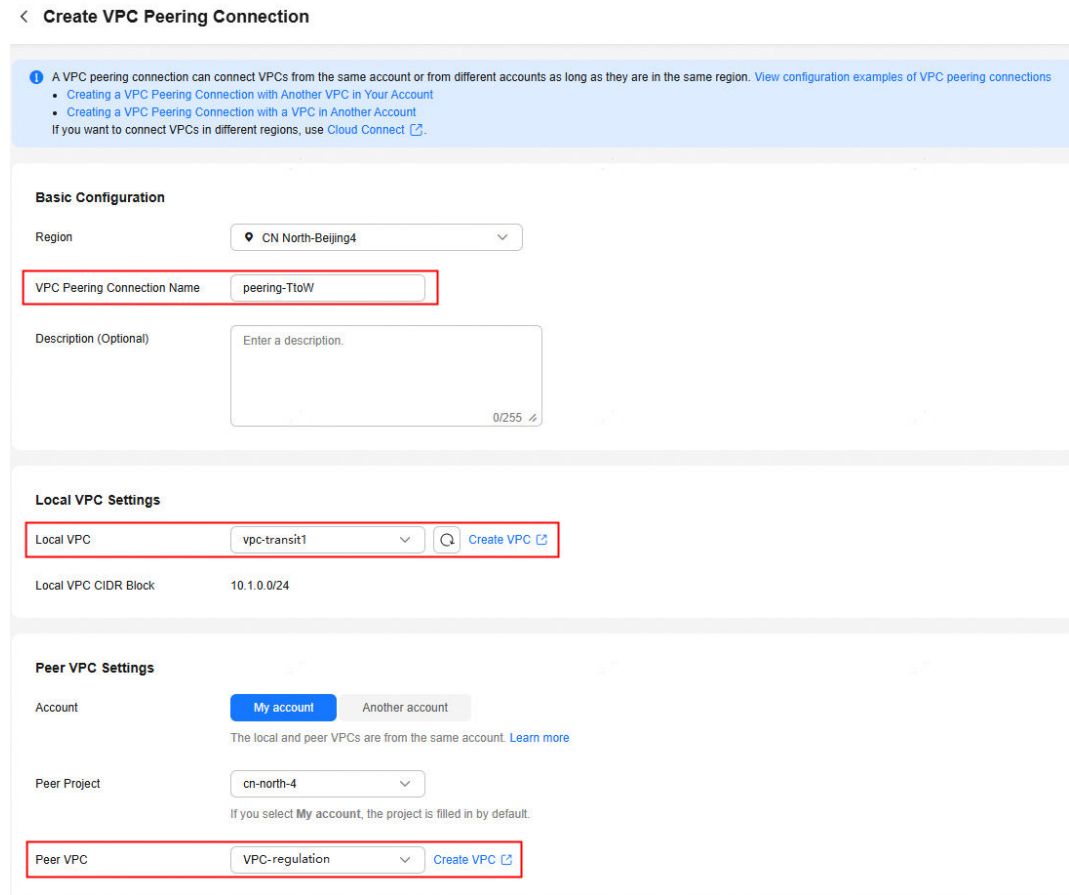
Configuring a VPC Peering Connection

Step 1 Under **Networking**, select **Virtual Private Cloud**. In the navigation pane on the left, choose **VPC Peering Connections**.

Step 2 Click **Create VPC Peering Connection**. On the displayed page, enter information, and click **Create Now**.

- **VPC Peering Connection Name:** peering-TtoW
- **Local VPC:** Select **vpc-transit1**.
- **Peer VPC:** Select **vpc-regulation**.
- Retain the default values for other parameters or configure them as prompted.

Figure 6-19 Creating a VPC peering connection

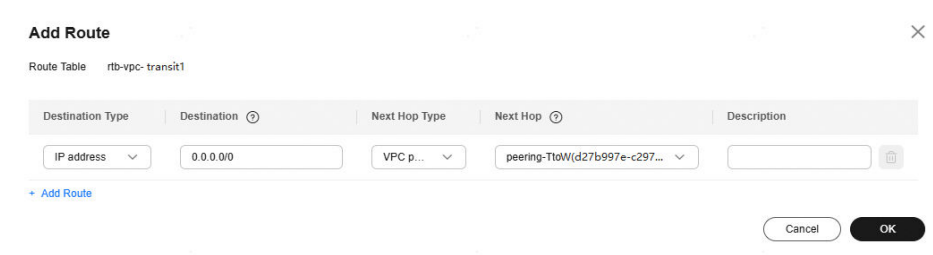


----End

Configuring Routes

- Step 1** Choose **Networking > Virtual Private Cloud**. In the navigation pane on the left, choose **Route Tables**.
- Step 2** Click **rtb-vpc-transit1** to delete the existing 0.0.0.0/0 routing rule.
- Step 3** Click **Add Route**, configure required parameters, and click **OK**.
 - **Destination:** Set it to **0.0.0.0/0**.
 - **Next Hop Type:** Select **VPC peering connection**.
 - **Next Hop:** The system automatically displays the VPC peering connection.

Figure 6-20 Adding a route

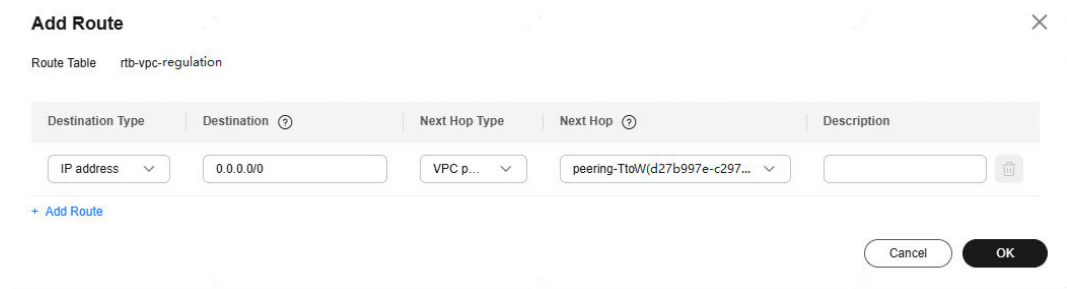


Step 4 Go back to the **Route Tables** page, click **rtb-vpc-regulation**, and click **Add Route**.

Step 5 Configure route information and click **OK**.

- **Destination:** Set it to **0.0.0.0/0**.
- **Next Hop Type:** Select **VPC peering connection**.
- **Next Hop:** The system automatically displays the VPC peering connection.

Figure 6-21 Adding a route



----End

Verifying that Department A Can Access the Regulatory Agency

Step 1 Under **Computing**, select **Elastic Cloud Server** and use VNC to log in to **ecs-departmentA**.

Step 2 On **ecs-departmentA**, verify that it can access the regulatory agency.

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
```

----End

7 Using a Private NAT Gateway to Enable an ECS in a VPC to Access a Load Balancer in Another VPC

Scenarios

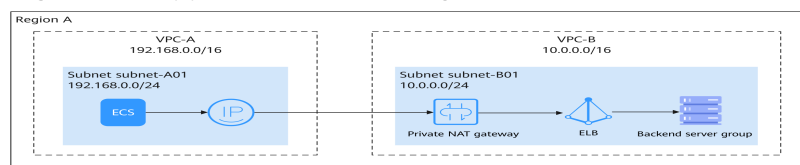
There are two applications (A and B) deployed in different VPCs. VPCs are isolated from each other by default, so the two applications cannot communicate with each other. To enable an application to access another, you can create a private NAT gateway and add a DNAT rule to it.

Solution Architecture

The following describes how to use a private NAT gateway to access a load balancer from a different VPC.

1. Applications A and B are deployed in VPC-A and VPC-B, respectively. The two applications are isolated from each other.
2. You can add a DNAT rule to a private NAT gateway to enable application A on the ECS in VPC-A to use the transit IP address in the same VPC to access the load balancer in VPC-B.
3. No route configuration is required in this practice.

Figure 7-1 Application A accessing a load balancer in a different VPC



Solution Advantages

1. Deploying applications A and B in different VPCs keeps their networks isolated and secure.
2. A DNAT rule allows only specific instances in VPC-B to provide services accessible from VPC-A, hiding other services in VPC-B from VPC-A. This enables refined network control.

Constraints

A load balancer can only be configured for one DNAT rule of a private NAT gateway in the same VPC. You cannot configure multiple transit IP addresses in different VPCs to access this load balancer.

Resource Planning

In this practice, you need to create VPCs, ECSs, a private NAT gateway, and a load balancer. For details about the resource planning, see [Table 7-1](#).

Table 7-1 Resource planning

Resource	Quantity	Description
VPC and subnet	Two VPCs, each with a subnet	<ul style="list-style-type: none">VPC-A, with the CIDR block of 192.168.0.0/16subnet-A01, with the CIDR block of 192.168.0.0/24
		<ul style="list-style-type: none">VPC-B, with the CIDR block of 10.0.0.0/16subnet-B01, with the CIDR block of 10.0.0.0/24
Private NAT gateway	1	In this practice, the name of the private NAT gateway is private_nat_gateway . It is used to connect VPC-A and VPC-B through a DNAT rule.
Load balancer	1	The load balancer in VPC-B to be accessed by the ECS in VPC-A
ECS	2	<ul style="list-style-type: none">ECS-A running in VPC-AECS-B running in VPC-B

Preparations

- Create two ECSs (ECS-A in VPC-A and ECS-B in VPC-B) and configure an application on each ECS. For details about how to purchase an ECS, see [Purchasing and Using a Linux ECS \(New Edition\)](#).
- Create an HTTP backend server group (backend server group-B) and add ECS-B in VPC-B to it. Do not associate a load balancer with the backend server group. For details about how to create a backend server group, see [Creating a Backend Server Group](#).

Step 1: Create a Load Balancer

- Go to the [Buy Elastic Load Balancer](#) page.
- Complete the basic configurations based on [Table 7-2](#).

Table 7-2 Parameters for configuring the basic information

Parameter	Example Value	Description
Type	Dedicated load balancer	Specifies the type of the load balancer. The type cannot be changed after the load balancer is created.
Region	CN North-Beijing4	Specifies the desired region. Resources in different regions cannot communicate with each other over internal networks.
AZ	<ul style="list-style-type: none"> • AZ1 • AZ2 	Specifies the AZs where the load balancer works. An AZ is a part of a region and has its own independent power supplies and networks. AZs are physically isolated but interconnected through internal networks.
Name	ELB01	Specifies the load balancer name.

3. Select specifications for the dedicated load balancer based on [Table 7-3](#).

Table 7-3 Load balancer specifications

Parameter	Example Value	Description
Specifications	<ul style="list-style-type: none"> • Elastic • Application load balancing 	Specifies the required specifications.

4. Complete the network configurations based on [Table 7-4](#).

Table 7-4 Configuring network parameters

Parameter	Example Value	Description
Network Type	Private IPv4 network	Specifies the network type of the load balancer.
VPC	VPC-B	Specifies the VPC where the dedicated load balancer works. You cannot change the VPC after the load balancer is created. Plan the VPC as required.

Parameter	Example Value	Description
Frontend Subnet	subnet-B01	Specifies the frontend subnet from which an IP address will be assigned to the dedicated load balancer to communicate with resources over the private network . After the load balancer is created, you can unbind the existing IP address and bind IPv4 and IPv6 addresses in a different subnet to the load balancer. Unbinding an IP address may affect services.
IPv4 Address	Automatically assign IP address	Specifies how you want the IPv4 address to be assigned if Network Type is set to Private IPv4 network .
Backend Subnet	Subnet of the load balancer	Specifies the backend subnet from which IP addresses will be assigned to the dedicated load balancer to forward requests to and perform health checks on backend servers .

5. Retain the default values for other parameters and click **Buy Now**.

Step 2: Add an HTTP Listener and Associate It with a Backend Server Group

Add an HTTP listener for **ELB01** and associate the listener with **backend server group-B** you have created. Set **Access Control** to **All IP addresses**. For details, see [Adding an HTTP Listener](#).

Step 3: Assign a Transit IP Address

1. Go to the [private NAT gateway list](#) page.
2. On the **Private NAT Gateways** page, click **Transit IP Addresses > Assign Transit IP Address**.

Figure 7-2 Assigning a transit IP address

3. Configure required parameters based on [Table 7-5](#).

Figure 7-3 Assigning a transit IP address

Table 7-5 Parameter for configuring a transit IP address

Parameter	Example Value	Description
Transit VPC	VPC-A	The VPC where the transit IP address is located.
Transit Subnets	subnet-A01	The subnet from which the transit IP address is assigned. A transit subnet is a transit network.
Transit IP Address	Automatic	How you want the transit IP address to be assigned.

4. Click **OK**.

Step 4: Create a Private NAT Gateway

1. Go to the [Buy Private NAT Gateway](#) page.
2. Configure the basic information about the private NAT gateway. For details about the key parameters, see [Table 7-6](#). Use the default values for other parameters.

Table 7-6 Parameter descriptions

Parameter	Example Value	Description
Name	private_nat_gateway	The name of the private NAT gateway.
VPC	VPC-B	The VPC where the private NAT gateway is created.
Subnet	subnet-B01	The subnet where the private NAT gateway is created.
Specifications	Small	The specifications of the private NAT gateway.

3. Click **Next**.

Step 5: Add a DNAT Rule

1. Go to the [private NAT gateway list](#) page.
2. On the **Private NAT Gateways** page, click the name of the private NAT gateway on which you need to add a DNAT rule.
3. On the private NAT gateway details page, click the **DNAT Rules** tab.
4. Click **Add DNAT Rule**.
5. Configure required parameters based on [Table 7-7](#).

Table 7-7 Parameter descriptions

Parameter	Example Value	Description
Local Network		
Port Type	Specific port	Specific port: The private NAT gateway only forwards requests with a specific protocol and port on the transit IP address to the specified port of the target server.
Protocol	TCP	The protocol can be TCP or UDP.

Parameter	Example Value	Description
Instance Type	Load balancer	Select the instance that provides services accessible from the external private network. In this practice, select ELB01 created in Step 1 .
Internal Port	80	The port used by the instance to provide services accessible from the external network.
Transit Network		
Transit IP Address	192.168.0.144	The transit IP address used to provide services accessible from on-premises data centers or other VPCs. In this practice, select the transit IP address assigned in Step 3 .
Transit IP Address Port	80	The transit IP address port that will be used to access the load balancer.

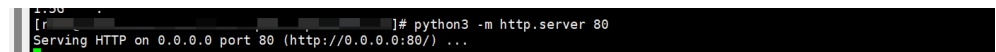
6. Click **OK**. Once the DNAT rule is created, its status changes to **Running**.

Step 6: Verify the Network Connectivity

1. Remotely log in to ECS-B and start the backend application of ELB01. Multiple methods are available for logging in to an ECS. For details, see [Logging In to an ECS](#).

Example command:
python3 -m http.server 80

Figure 7-4 Starting the backend application of ELB01



2. Remotely log in to ECS-A.
3. Run the following command to check the network connectivity:
curl http://\${transit-IP-address}

If information similar to the following is displayed, ECS-A can access ELB01 in another VPC.

Figure 7-5 Verifying cross-VPC access to the load balancer

```
root@ecs-9fbc: ~# curl http://192.168.0.144:80
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a></li>
<li><a href=".bash_logout">.bash_logout</a></li>
<li><a href=".bash_profile">.bash_profile</a></li>
<li><a href=".bashrc">.bashrc</a></li>
<li><a href=".cache">.cache</a></li>
<li><a href=".cshrc">.cshrc</a></li>
<li><a href=".history">.history</a></li>
<li><a href=".ssh">.ssh</a></li>
<li><a href=".tcshrc">.tcshrc</a></li>
</ul>
<hr>
</body>
</html>
```

8 Using a Public NAT Gateway to Enable Servers to Share an EIP to Access the Internet

Scenarios

When there is a large number of ECSs running in a VPC, assigning an EIP to each of them reduces management efficiency and raises exposure to potential scans and attacks.

To address these issues, you can use a public NAT gateway to centrally manage the Internet ingress and egress:

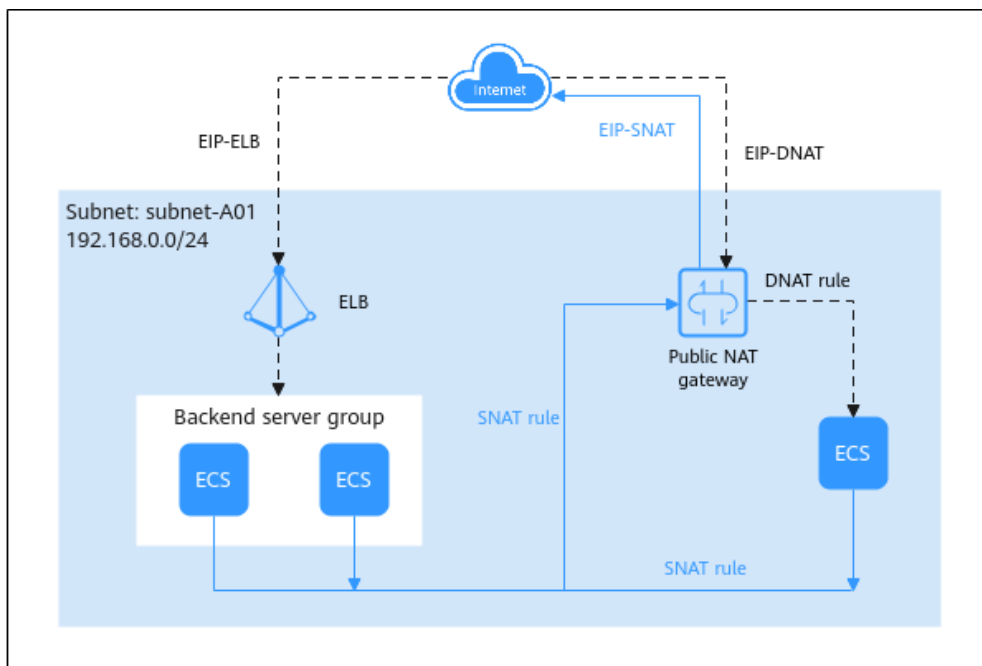
- Add an SNAT rule and configure an EIP to allow all ECSs in a VPC to share this EIP to access the Internet, and keep all resources in the VPC running properly.
- Unbind the EIP from each ECS and add a DNAT rule to minimize port exposure risks and keep access mode unchanged.

Solution Architecture

In enterprise applications, backend services are usually centrally managed to improve service availability and management efficiency. However, directly exposing backend services to the Internet brings security risks. If your servers need to access the Internet, use the following solution to centrally manage the Internet ingress and egress:

1. Use a load balancer as the unified ingress to distribute external requests across backend servers.
2. Use a public NAT gateway as the unified egress, as shown in [Figure 8-1](#). This solution helps you centrally manage backend services, reduce security risks, and improve O&M efficiency.

Figure 8-1 Unified egress



Resource Planning

In this practice, you need to create a VPC, three ECSs, a public NAT gateway, and a load balancer. For details about the resource planning, see [Table 7-1](#).

Table 8-1 Resource planning

Resource	Quantity	Description
VPC and subnet	One VPC with a subnet	<ul style="list-style-type: none"> VPC-A, with the CIDR block of 192.168.0.0/16 subnet-A01, with the CIDR block of 192.168.0.0/24
Public NAT gateway	1	In this practice, the NAT gateway is named nat_public . You can add an SNAT rule to this NAT gateway to allow ECSs to share an EIP to access the Internet.
Load balancer	1	This load balancer distributes external traffic across ECSs.
ECS	3	ECS-A , ECS-B , and ECS-C are deployed in subnet-A01 .

Resource	Quantity	Description
EIP	3	<ul style="list-style-type: none"> ● EIP-ELB: You can bind this EIP to the load balancer to distribute client requests from the Internet across ECSs. ● EIP-SNAT: You can select this EIP for an SNAT rule to allow ECSs to share this EIP to access the Internet clients. ● EIP-DNAT: You can select this EIP for a DNAT rule to allow Internet clients to access the ECSs through this EIP.

Preparations

- Buy three EIPs (**EIP-ELB**, **EIP-SNAT**, and **EIP-DNAT**), as shown in [Table 8-1](#).
- Buy a load balancer and three ECSs, and deploy applications on these ECSs. Add two ECSs as backend servers of the load balancer. For details, see [Using ELB to Distribute Traffic to a Web Application Across ECSs](#).

Step 1: Create a Public NAT Gateway

1. Go to the [Buy Public NAT Gateway](#) page.
2. Configure the required parameters. For details, see [Buying a Public NAT Gateway](#).

Figure 8-2 Buying a public NAT gateway

Basic Configuration

Region

Regions are geographic areas isolated from each other. For low network latency and quick resource access, select the region nearest to where your services will be accessed.

Billing Mode
 Yearly/Monthly Pay-per-use
Billed by the day. Each billing period starts from 08:00:00 and there is a one-day minimum. [Learn more](#)

Specifications
 Small Medium Large Extra-large
Supports up to 10,000 connections. [Learn more](#)

Name

VPC
 [Create VPC](#) [View VPCs](#)

Subnet
 [Create Subnet](#) [View Subnets](#)
Available private IP addresses: 251
 The selected subnet is for the NAT gateway only. To enable communications over the Internet, add rules after the NAT gateway is created.

Enterprise Project
 [Create Enterprise Project](#)

Advanced Settings
SNAT Connection TCP Timeout (s): 900 SNAT Connection UDP Timeout (s): 300 SNAT Connection ICMP Timeout (s): 10 TCP TIME_WAIT (s): 5 Description: -- Tag (Optional): --

Step 2: Add an SNAT Rule

ECSs in **subnet-A01** can share the EIP configured for the SNAT rule to access the Internet.

1. Go to the [public NAT gateway list](#) page.
2. On the **Public NAT Gateways** page, click the public NAT gateway purchased in **Step 1**.
The public NAT gateway details page is displayed.
3. On the **SNAT Rules** tab, click **Add SNAT Rule**.
4. Add an SNAT rule as prompted. Set **Public IP Address Type** to **EIP** and select **EIP-SNAT**.

Figure 8-3 Adding an SNAT rule

Add SNAT Rule

Public NAT Gateway Name
nat-

Scenario
VPC Direct Connect/Cloud Connect

CIDR Block
Existing Custom

subnet-

Public IP Address Type
EIP

Select the first 0 records. You can select 20 more EIPs. [View EIP](#)

Select a property or enter a keyword.

EIP	EIP Type	Bandwidth Na...	Bandwidth (M...	Billing Mode	Created	Enterprise Pr...
-----	----------	-----------------	-----------------	--------------	---------	------------------

No data available.
[Buy EIP](#)

Cancel OK

5. Click **OK**.

Step 3: Add a DNAT Rule

ECSs in **subnet-A01** can share the EIP configured for the DNAT rule to provide services accessible from the Internet.

1. Go to the [public NAT gateway list](#) page.

Figure 8-5 Successful Internet access to the server

```
[root@ecs-test-nat-... ~]# TIMEOUT=0
[root@ecs-test-nat-... ~]# ping 8.8.8.8
PING 8.8.8.8: 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=53.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=109 time=53.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=109 time=53.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=109 time=53.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=109 time=53.2 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=109 time=53.3 ms
^C
 8.8.8.8 ping statistics:
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 53.270/53.395/53.721/0.150 ms
[root@ecs-test-nat-... ~]#
```

3. Run the following command on each of the three ECSs to obtain the IP address used by the ECSs to access the Internet:
curl myip.ipip.net

As shown in **Figure 8-6**, EIP-SNAT is returned for each of the ECS.

Figure 8-6 Obtaining the IP address used by each server to access the Internet

```
[root@ecs-... ~]# curl myip.ipip.net
IP 113...
[root@ecs-... ~]#
```

9 Using CFW to Protect Outbound SNAT Traffic

Scenarios

When there is a large number of ECSs running in a VPC, assigning an EIP to each of them reduces management efficiency and raises exposure to potential scans and attacks.

You can use a public NAT gateway to centrally manage the Internet ingress and egress of ECSs, reducing security risks. Cloud Firewall (CFW) is a next-generation cloud native firewall that protects Internet and VPC borders on the cloud. This section describes how to use CFW to protect private IP addresses against attacks when they access the Internet through an SNAT rule of a NAT gateway.

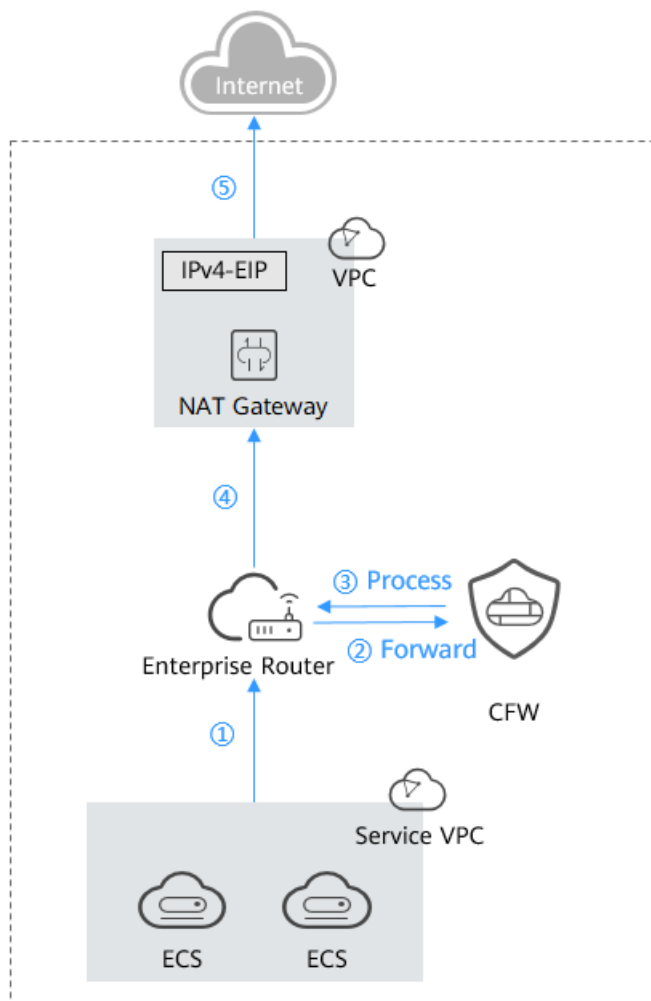
Preparations

- Create an enterprise router. For more information, see [What Is an Enterprise Router?](#)
- Create a firewall. For more information, see [Creating a Firewall](#).

Constraints

- Only the CFW professional edition supports access control by private IP address.
- By default, CFW supports standard private CIDR blocks. To configure other CIDR blocks, modify the CIDR blocks or [submit a service ticket](#) to expand the CIDR blocks.

Networking for SNAT Protection



NOTE

The request traffic and response traffic are transmitted over the same path.

Configuration Suggestions

- Create an independent VPC for the NAT gateway. To avoid affecting access control, do not deploy ECSs or other instances in this VPC.
- If the existing network is complex or improperly configured (for example, VPC CIDR blocks overlap, the NAT gateway has complex configurations, or east-west communication has been configured using VPC Peering), fully evaluate risks in network connectivity, route loops, and route conflicts.
- Test firewall configurations before applying them to a network. You can create a test server, configure the destination address route in the VPC route table, and use the test server in the VPC to check whether the entire service flow runs properly and whether the configured rules are effective. Switch the service flow over to the live network after the configurations pass the test.
- Before configuring blocking rules after CFW is enabled, check whether workloads are normal after traffic passes through the firewall. Gradually add

rules and verify them in a timely manner. Once a problem is detected, disable protection in a timely manner to avoid affecting workloads.

- SNAT EIPs do not allow inbound access from the external network. Their outbound access control rules use the Internet border protection capabilities. Do not enable protection for EIPs bound to SNAT rules on the **EIPs** page because doing so may interrupt rule implementation and logging.

Configuration Process

For details, see [Configuring a Protection Rule to Protect SNAT Traffic](#).

Figure 9-1 SNAT protection configuration process

