NAT Gateway

Best Practices

Issue	01
Date	2024-11-08

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 Enabling Private Networks to Access the Internet Using a Cloud Connection and SNAT

Scenario

When customers require high-speed Internet access from their on-premises data centers to locations outside the Chinese mainland, they can use VPN, Cloud Connect, NAT Gateway (SNAT rules), and EIP.

For example, these services can enable fast access to services in Africa, Europe, or America.

NOTE

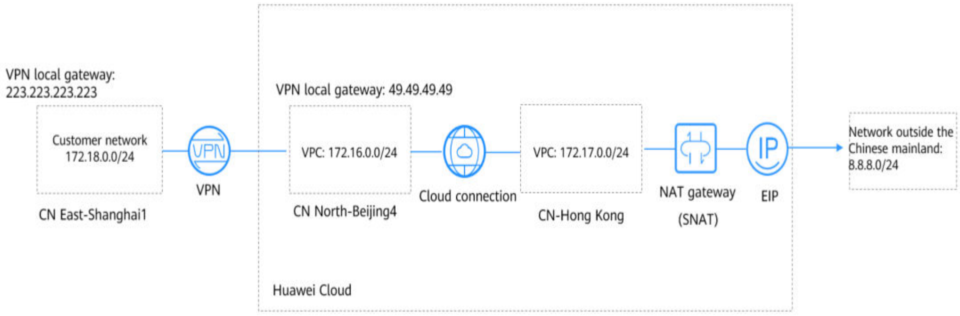
For details about the regions where cloud connections are available, see **Region Availability**.

Use Cases

1. Using VPN to connect a customer's on-premises data center to a VPC in CN North-Beijing4
2. Using a cloud connection to connect the VPC in CN North-Beijing4 to a VPC in CN-Hong Kong for network acceleration
3. Purchasing NAT gateway in CN-Hong Kong, and adding an SNAT rule to enable on-premises servers to share the EIP to access the Internet outside the Chinese mainland

Figure 1-1 shows an example.

Figure 1-1 Enabling access to the Internet


VPN local gateway: 223.223.223.223
Customer network 172.18.0.0/24
CN East-Shanghai1
VPN
VPN
VPN local gateway: 49.49.49.49
VPC: 172.16.0.0/24
CN North-Beijing4
Cloud connection
VPC: 172.17.0.0/24
CN-Hong Kong
NAT gateway (SNAT)
IP
EIP
Network outside the Chinese mainland: 8.8.8.0/24
Huawei Cloud

NOTE

- In this solution, the network in CN East-Shanghai1 represents the on-premises data center.
- The CIDR block of the Internet outside the Chinese mainland is 8.8.8.0/24, and 8.8.8.8 is the only IP address used for testing.

Advantages

Cross-border connectivity and accelerated network access provide better user experience.

Constraints

The user account needs cross-border permissions. Otherwise, the user needs to authorize the current VPCs to an account with the cross-border permissions to create a cloud connection.

Resource Planning

Table 1-1 Resources required

Resource	Resource Name	Description	Quantity
VPC	VPC-Test01	Region: CN East-Shanghai1 CIDR block: 172.18.0.0/24 172.18.0.0/24 represents the on-premises network.	1
	VPC-Test02	Region: CN North-Beijing4 CIDR block: 172.16.0.0/24	1
	VPC-Test03	Region: CN-Hong Kong CIDR block: 172.17.0.0/24	1
EIP	EIP-Test	Region: CN-Hong Kong	1
NAT gateway	NAT-Test	You need to purchase it in **VPC-Test03** and use EIP **EIP-Test**.	1
VPN gateway	VPN-GW-Test01	Region: CN North-Beijing4 Local gateway: 49.49.49.49	1
	VPN-GW-Test02	Region: CN East-Shanghai1 Local gateway: 223.223.223.223	1
VPN connection	VPN-Test01	It is created to connect to **VPN-GW-Test01**.	1
	VPN-Test02	It is created to connect to **VPN-GW-Test02**.	1

Resource	Resource Name	Description	Quantity
Cloud connection	CC-Test	It enables cross-region access between CN North-Beijing4 and CN-Hong Kong and accelerates network access.	1
ECS	ECS-Test01	Region: CN East-Shanghai1 Private IP address: 172.18.0.3	1
	ECS-Test02	Region: CN East-Beijing4 Private IP address: 172.16.0.3	1
	ECS-Test03	Region: CN-Hong Kong region Private IP address: 172.17.0.3	1

Process

1. **Create VPCs**.
2. **Create two VPN connections**.
3. **Create a cloud connection.**
4. **Buy three ECSs**.
5. **Buy an EIP and a NAT gateway**.

Procedure

Step 1 Create VPCs.

For details, see **Creating a VPC**.

Ensure that the VPC CIDR blocks do not conflict with each other.

- VPC in CN East-Shanghai1 (**VPC-Test01**): 172.18.0.0/24
- VPC in CN North-Beijing4 (**VPC-Test02**): 172.16.0.0/24
- VPC in the CN-Hong Kong (**VPC-Test03**): 172.17.0.0/24

Step 2 Create two VPN connections.

Create **VPN-GW-Test01** in CN North-Beijing4 and buy **VPN-Test01**.

Create **VPN-GW-Test02** in CN East-Shanghai1 and buy **VPN-Test02**.

For details, see **Buying a VPN Gateway** and **Buying a VPN Connection**.

For details, see **Creating a VPN Gateway** and **Creating a VPN Connection**.

- In CN North-Beijing4:
  - Local subnets: 172.16.0.0/24, 172.17.0.0/24, and 8.8.8.0/24
  - Remote gateway: 223.223.223.223

  - Remote subnet: 172.18.0.0/24
- In CN East-Shanghai1:
  - Local subnet: 172.18.0.0/24
  - Remote gateway: 49.49.49.49
  - Remote subnets: 172.16.0.0/24, 172.17.0.0/24, and 8.8.8.0/24

NOTE

When configuring the VPN connection between CN North-Beijing4 and CN East-Shanghai1, you need to ensure that local CIDR blocks in CN North-Beijing4 and remote subnets (8.8.8.0/24) in CN East-Shanghai1 are included so that these subnets can access the Internet outside of the Chinese mainland.

Step 3 Create a cloud connection.

1. Create a cloud connection (**CC-Test**).

   For details, see **Creating a Cloud Connection**.

2. Load the three VPCs to the created cloud connection.

   For details, see **Loading a Network Instance**.

3. Add custom CIDR blocks.

   For details, see **Adding Custom CIDR Blocks for a Cloud Connection**.

   - When you load the VPC in CN North-Beijing4, you need to add CIDR blocks 172.18.0.0/24 and 172.16.0.0/24.
   - When you load the VPC in CN-Hong Kong, you need to add CIDR blocks 172.17.0.0/24 and 8.8.8.0/24.

   NOTE

   To enable communication among all nodes, you need to add all local subnets.

4. Buy a bandwidth package.

   By default, a cloud connection provides 10 kbit/s of bandwidth for testing cross-region network connectivity. You need to buy a bandwidth package to ensure normal communication across regions.

   For details, see **Buying a Bandwidth Package**.

5. Assign inter-region bandwidths.

   For details, see **Assigning an Inter-Region Bandwidth**.

Step 4 Buy three ECSs.

Buy one ECS in each of the following regions: CN East-Shanghai1, CN North-Beijing4, and CN-Hong Kong.

For details, see **Purchasing an ECS**.

- Private IP address of the ECS (**ECS-Test01**) in CN East-Shanghai1: 172.18.0.3
- Private IP address of the ECS (**ECS-Test02**) in CN North-Beijing4: 172.16.0.3
- Private IP address of the ECS (**ECS-Test03**) in CN-Hong Kong: 172.17.0.3

Step 5 Buy an EIP and a NAT gateway.

Buy an EIP (**EIP-Test**) in the CN-Hong Kong region, buy a public NAT gateway (**NAT-Test**), and add an SNAT rule for each of the following CIDR blocks:

For details, see **Assigning an EIP and Binding It to an ECS** and **Adding an SNAT Rule**.

- VPC CIDR block: 172.17.0.0/24
- Direct Connect connection/Cloud connection CIDR blocks: 172.18.0.0/24 and 172.16.0.0/24

NOTE

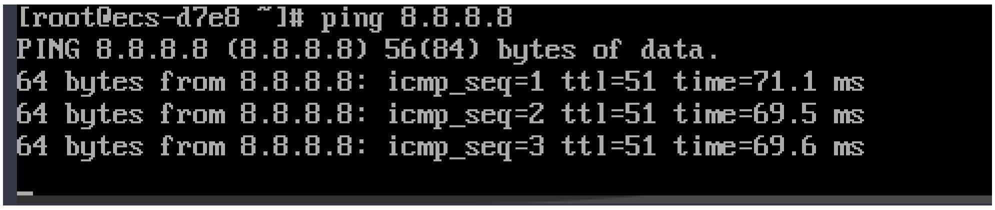
SNAT rules allow servers in private networks to access the Internet (8.8.8.0/24) outside the Chinese mainland.

----End

Verification

Test the network connectivity.

Ping the gateway (8.8.8.8) from the ECS in CN East-Shanghai1.



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

Scenarios

You need to connect your on-premises data center to Huawei Cloud using Direct Connect and then add SNAT rules to enable your on-premises servers to access the Internet through a public NAT gateway in a secure, reliable, and high-speed way, or add DNAT rules to enable your on-premises servers to provide services accessible from the Internet. This practice can be used in similar scenarios 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 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 public NAT gateway types and EIPs bound to it at any time. The configuration is simple and will take effect immediately.

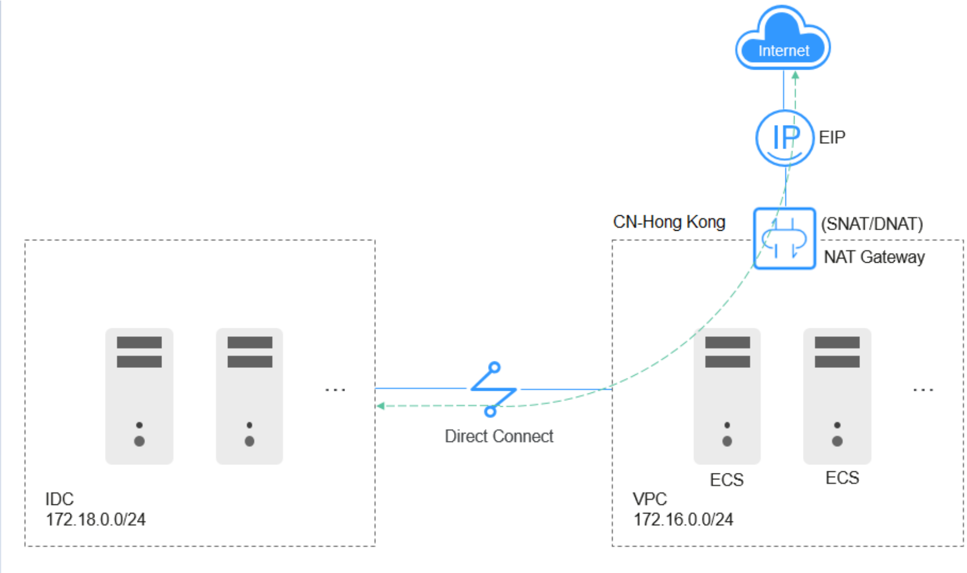
Typical Topology

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 accessed VPC is 172.16.0.0/24.

Implementation methods:

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

Figure 2-1 Network topology



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 does not overlap with the subnet CIDR block of the VPC. Otherwise, the communications between your on-premises data center and the VPC will fail.

Procedure

Step 1 Create a VPC.

For detailed operations, see **Creating a VPC**.

Step 2 Configure a Direct Connect connection.

Create a Direct Connect connection between your on-premises data center and the transit VPC (in the CN-Hong Kong region). For details, see **Overview**.

NOTE

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

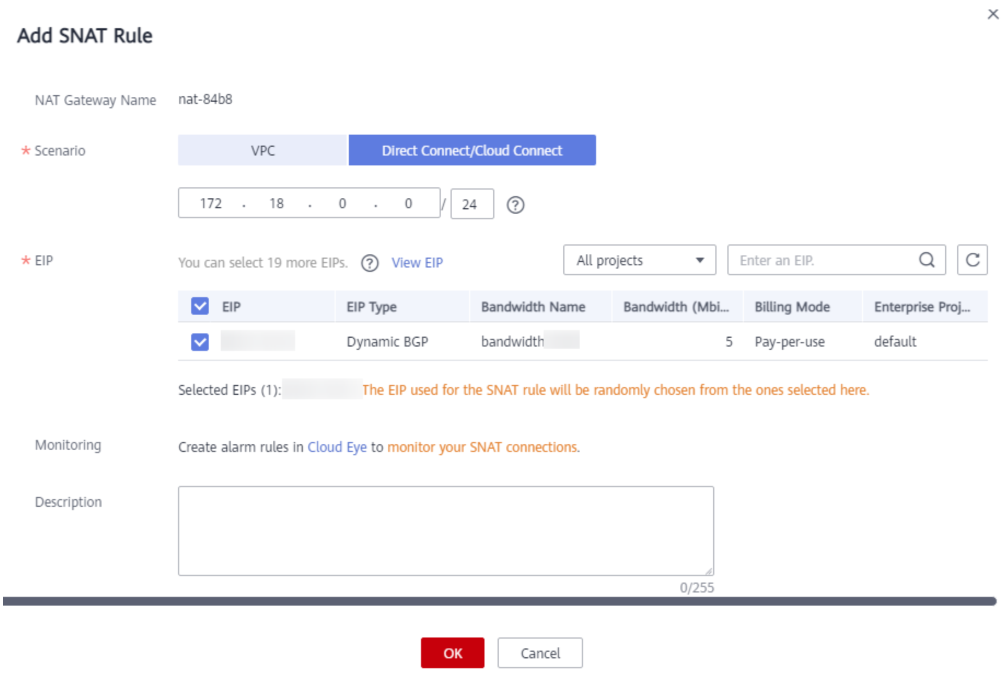
- **Static**: Add the default route with 0.0.0.0/0 as the destination and set the next hop to the Direct Connect connection.
- **BGP**: The on-premises network can learn the default route using BGP.

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 by setting the CIDR block to that of the Direct Connect connection. For more details, see **Adding an SNAT Rule**.

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

Figure 2-2 Add SNAT Rule



Add SNAT Rule

NAT Gateway Name nat-84b8

* Scenario: VPC | **Direct Connect/Cloud Connect**

172 . 18 . 0 . 0 / 24

* EIP: You can select 19 more EIPs. View EIP

☑ EIP	EIP Type	Bandwidth Name	Bandwidth (Mbi...	Billing Mode	Enterprise Proj...
☑ [redacted]	Dynamic BGP	bandwidth[redacted]	5	Pay-per-use	default

Selected EIPs (1): [redacted] The EIP used for the SNAT rule will be randomly chosen from the ones selected here.

Monitoring: Create alarm rules in Cloud Eye to monitor your SNAT connections.

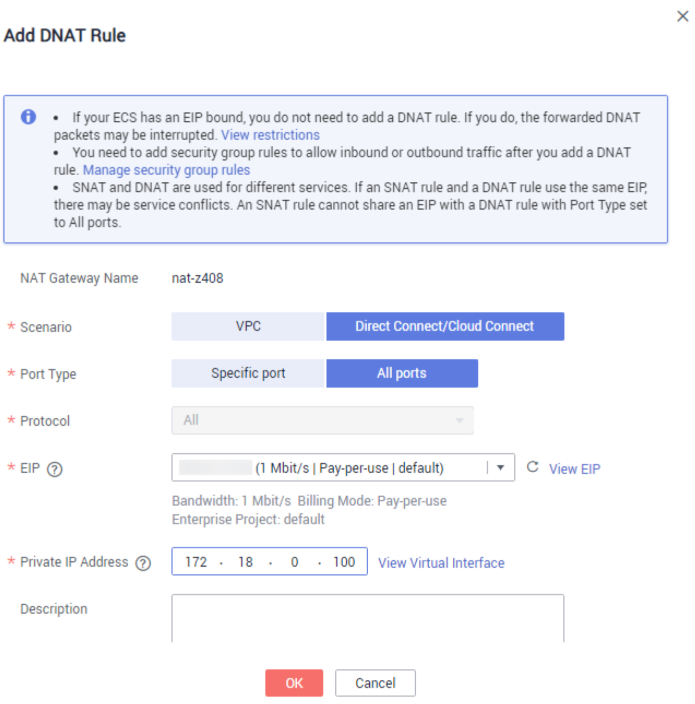
Description

0/255

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



Add DNAT Rule

- If your ECS has an EIP bound, you do not need to add a DNAT rule. If you do, the forwarded DNAT packets may be interrupted. View restrictions
- You need to add security group rules to allow inbound or outbound traffic after you add a DNAT rule. Manage security group rules
- SNAT and DNAT 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.

NAT Gateway Name nat-z408

* Scenario: VPC | **Direct Connect/Cloud Connect**

* Port Type: Specific port | **All ports**

* Protocol: All

* EIP: [redacted] (1 Mbit/s | Pay-per-use | default) View EIP

Bandwidth: 1 Mbit/s Billing Mode: Pay-per-use
Enterprise Project: default

* Private IP Address: 172 . 18 . 0 . 100 View Virtual Interface

Description

NOTE

SNAT and DNAT 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

After the configuration is complete, 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 a Private NAT Gateway and Direct Connect to Enable Communications Between a VPC and an On-premises Data Center

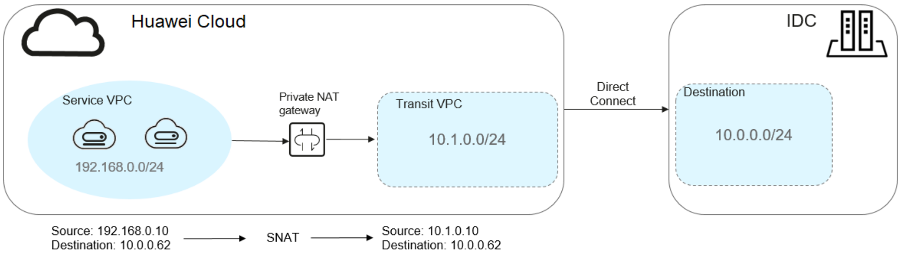
Scenarios

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 is used to connect the on-premises data center to the transit VPC.
2. A private NAT gateway is configured to translate 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 scenario, 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 and Limitations

- The CIDR block of your on-premises data center cannot overlap with the subnet CIDR block of the transit VPC and the CIDR block of the service VPC, or 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 that you can map private IP addresses in the service VPC to. Generally, you either use a private CIDR block or use private IP address trusted by your on-premises data center.

Resource and Cost Planning

Table 3-1 Resource and cost planning

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

NOTE

- 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.

Tasks

1. **Create a service VPC and a transit VPC.**
2. **Configure a Direct Connect connection.**
3. **Buy a private NAT gateway.**

Procedure

Step 1 Create a service VPC and a transit VPC.

For detailed operations, see **Creating a VPC**.

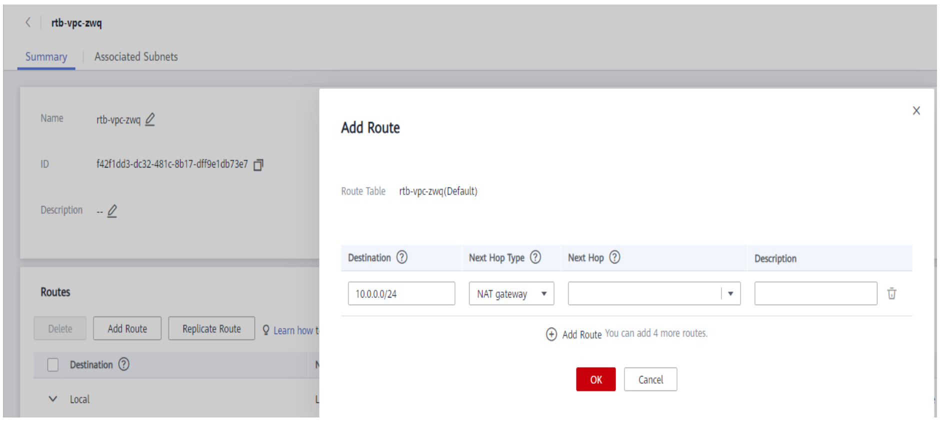
Step 2 Configure a Direct Connect connection.

Create a Direct Connect connection between the on-premises data center and the transit VPC. For details, see **Overview**.

Step 3 Buy a private NAT gateway.

1. Buy a private NAT gateway in the specified region and select a service VPC.
2. Assign a transit IP address by setting **Transit VPC** to **VPC-Test02**, selecting **Manual** for **Transit IP Address**, and setting **IP address** to **10.1.0.10**.
3. On the **SNAT Rules** tab of the purchased 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 to those of the on-premises data center. Set **Transit IP Address** to the address configured in the previous step.
4. Add a route pointing to the private NAT gateway in the service VPC. Set **Destination** to **10.0.0.0/24**.

Figure 3-2 Adding a route



rtb-vpc-zwq

Name rtb-vpc-zwq

ID f42f1dd3-dc32-481c-8b17-dff9e1db73e7

Description --

Add Route

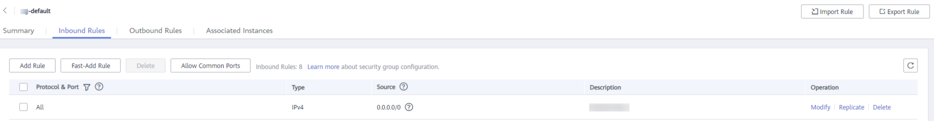
Route Table rtb-vpc-zwq(Default)

Destination	Next Hop Type	Next Hop	Description
10.0.0.0/24	NAT gateway		

Add Route You can add 4 more routes.

5. Add an inbound security group rule for the **on-premises server (private IP address: 10.0.0.62)**.

Figure 3-3 Adding an inbound security group rule



[redacted]-default

Inbound Rules: 8 Learn more about security group configuration.

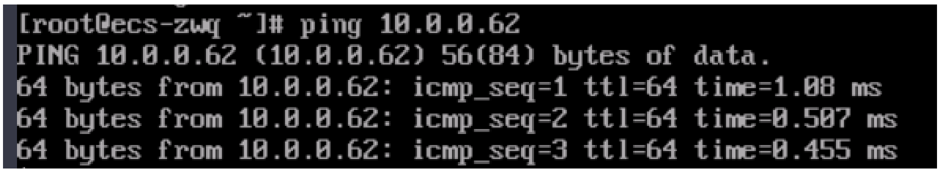
	Protocol & Port	Type	Source	Description	Operation
□	All	IPv4	0.0.0.0/0	[redacted]	Modify | Replicate | Delete

----End

Verification

After the configuration is complete, test the network connectivity.

Log in to ECS (**ECS-Test**) in the service VPC and ping the private IP address (**10.0.0.62**) of the on-premises data center to confirm the configuration was successful.



```
[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 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**. VPC B has a subnet **subnet B**. Create a public NAT gateway for **subnet A**. Then add SNAT and DNAT rules to enable servers in **subnet A** to access the Internet and provide services accessible from the Internet. **subnet B** connects to **subnet A** through a VPC peering connection. Then servers in **subnet B** can use the public NAT gateway for **subnet A** to access the Internet and provide services accessible from the Internet. You do not need to configure another public NAT gateway specifically 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 methods:

1. Configure NAT Gateway in VPC A. Add SNAT and DNAT rules.
2. Create a VPC peering connection between subnet A and subnet B, enabling servers in subnet B to use a public NAT gateway to access the Internet and provide services accessible 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.

- All subnets of the two VPCs do not overlap with each other.

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 an SNAT rule.

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 a DNAT rule.

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 detailed operations, see **Creating a VPC**.

Step 2 Create a VPC peering connection.

Create a VPC peering connection between subnet A and subnet B. For detailed operations, see **Creating a VPC Peering Connection with Another VPC in Your Account**.

NOTE

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

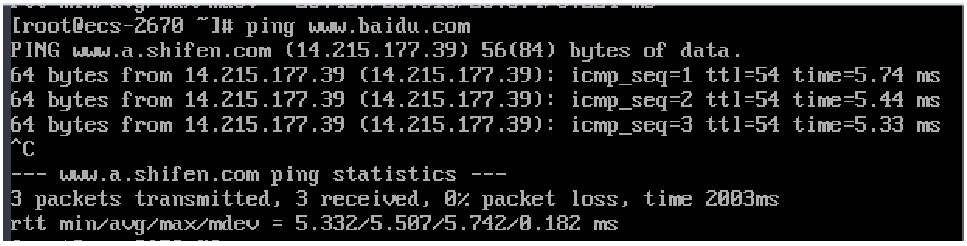
Add a route in the route table of VPC B. Set **Destination** to **0.0.0.0/0** and **Next Hop** to the created VPC peering connection between VPC A and VPC B.

----End

Testing Connectivity of a VPC Peering Connection

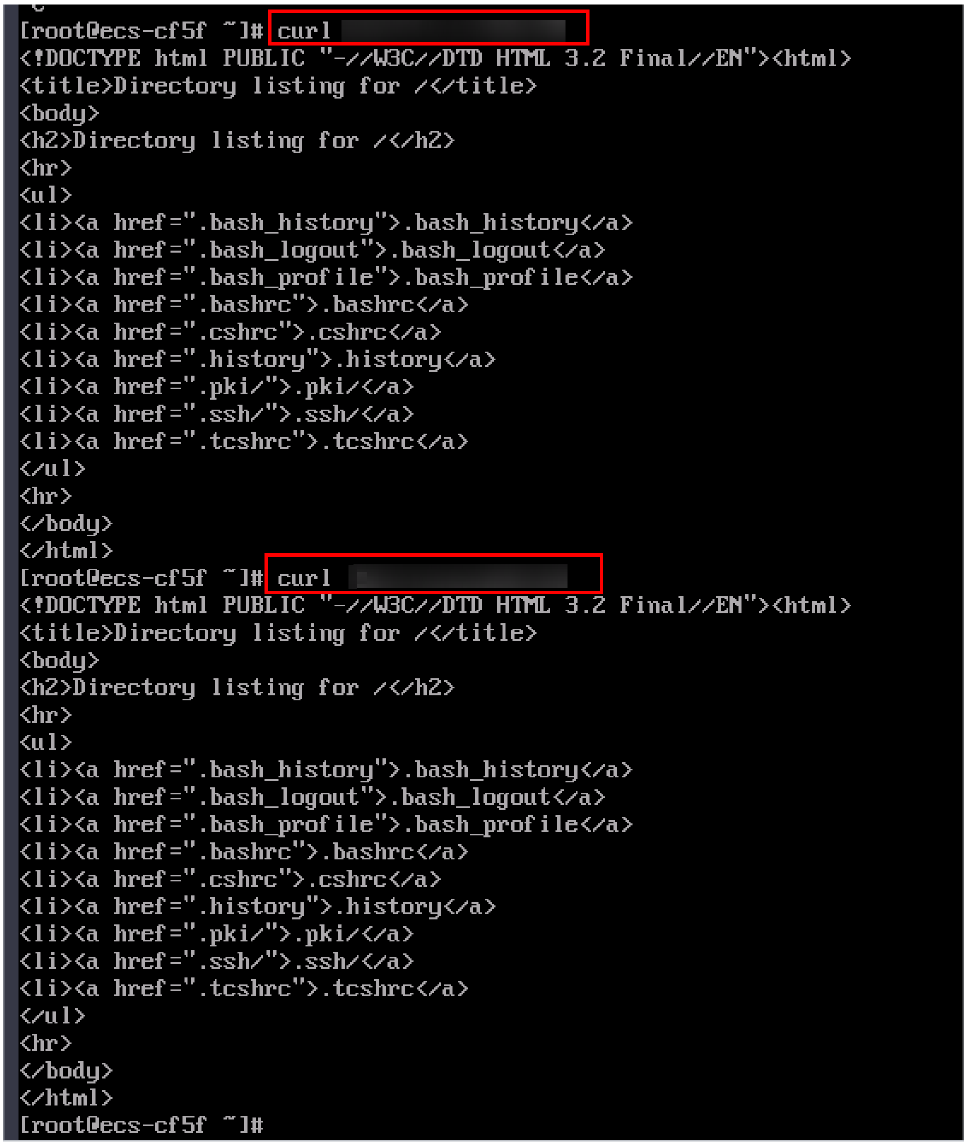
After the configuration is complete, test the network connectivity.

Log in to a server in subnet B and ping a public IP address.



```
[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.



```
[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 Preserving Your Network with NAT Gateways During Cloud Migration

5.1 Overview

Scenarios

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

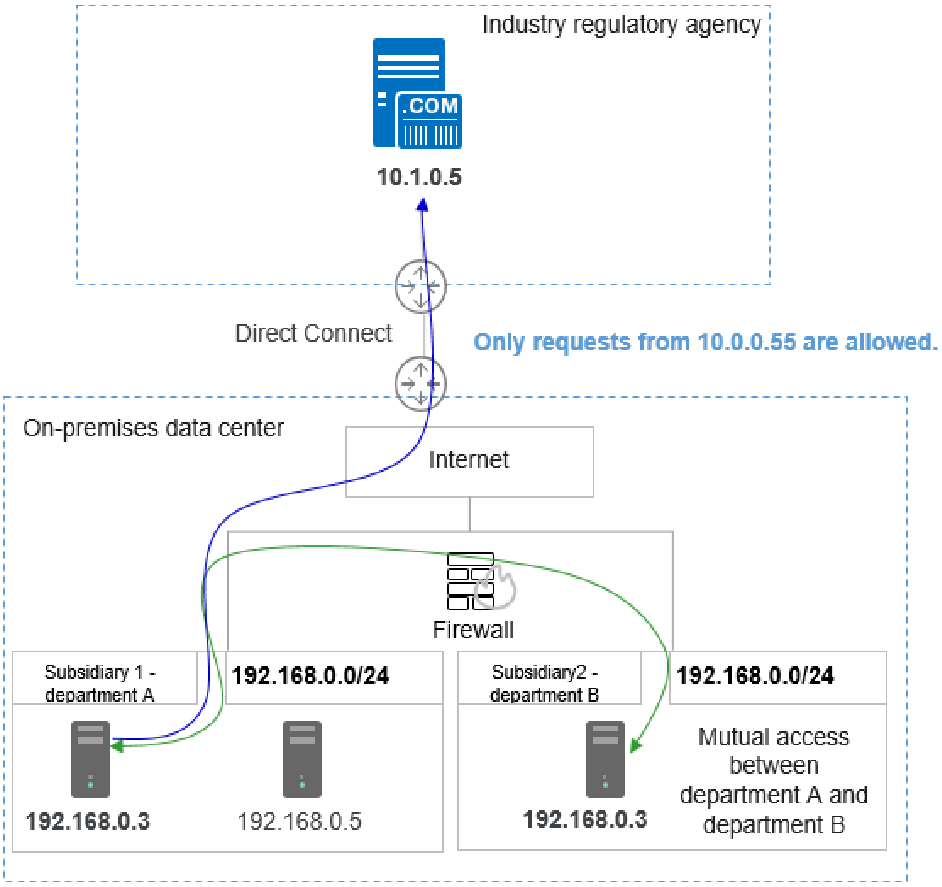
- Servers in two overlapping CIDR blocks in the on-premises data center need to access each other.
- Servers need to access external resources with a specified IP address.

For example:

A company with multiple branches had overlapping subnets for different branch offices. In **Figure 5-1**, 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 and required that servers in the overlapping subnets could still access each other after the migration. In addition, servers in department A can still access serves in the industry supervision agency using the specified IP address.

Figure 5-1 Overlapping subnets of departments from different subsidiaries


Industry regulatory agency
.COM
10.1.0.5
Direct Connect
Only requests from 10.0.0.55 are allowed.
On-premises data center
Internet
Firewall
Subsidiary 1 - department A
192.168.0.0/24
Subsidiary2 - department B
192.168.0.0/24
192.168.0.3
192.168.0.5
192.168.0.3
Mutual access between department A and department B

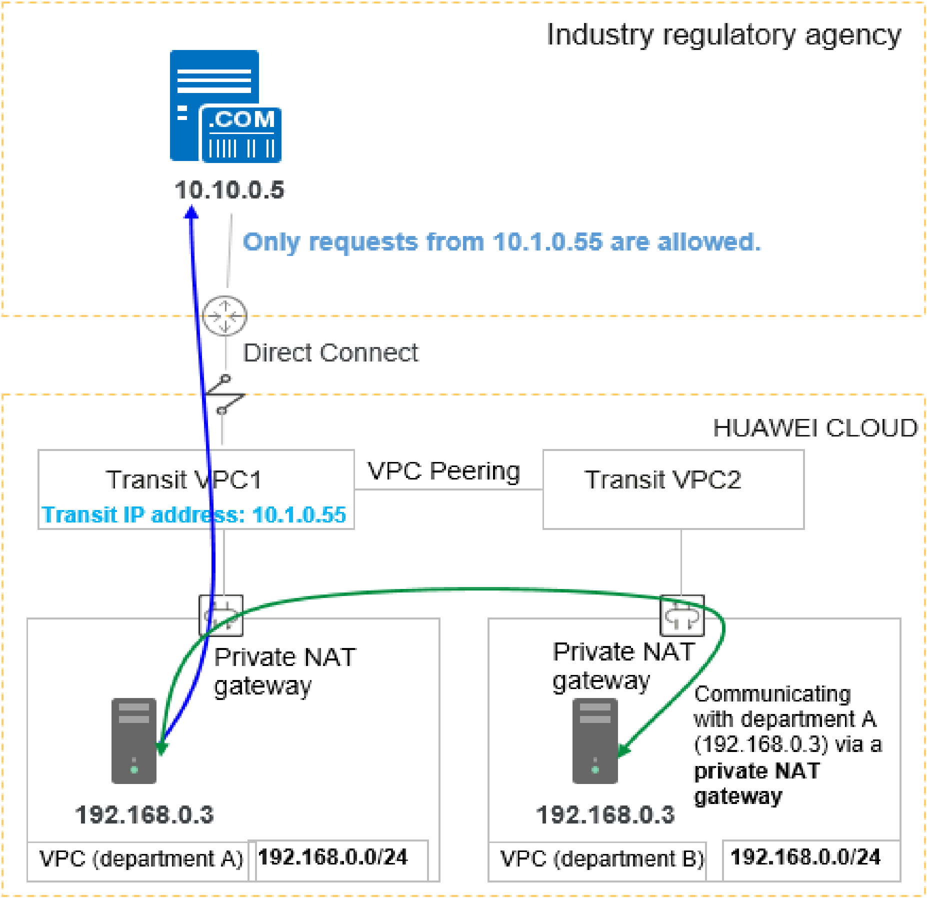
Solution Architecture

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 and private address mapping of servers. This resolves the issue **that VPC peering connections created between VPCs that have overlapping subnet CIDR blocks may not take effect**.

See **Figure 5-2**.

- The CIDR block 192.168.0.0/24 of department A and that of department B were 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 in department A to 10.1.0.55 to access external servers.

Figure 5-2 Huawei Cloud private NAT gateways



Solution Advantages

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

Constraints and Limitations

Pay attention to the following points 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

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

Scenarios

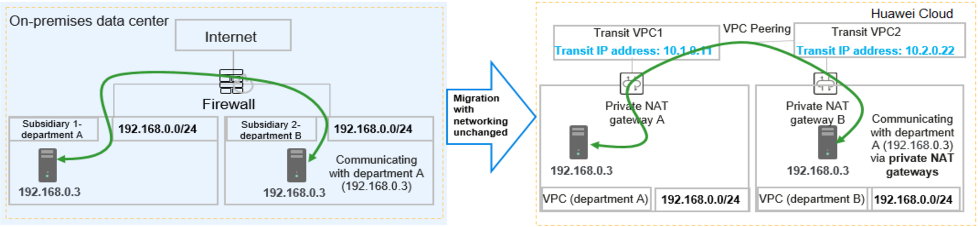
The existing network architecture of the on-premises data center needs to be migrated to the cloud without any changes. In addition, servers in two overlapping CIDR blocks in the on-premises data center can access each other.

Department A and department B in the same on-premises data center have an overlapping subnet. Workloads of the two departments need to be migrated to a cloud without changing CIDR blocks of their subnets. In addition, the overlapping subnets of the two departments should be able to communicate with each other after the migration.

Solution Architecture

- Department A and department B of two subsidiaries use the same CIDR block (192.168.0.0/24), so two VPCs with the same CIDR block are created on the cloud.
- The department A and B servers both used 192.168.0.3, so they were respectively assigned 10.1.0.11 and 10.2.0.22, as transit addresses. These transit addresses enabled the two servers to communicate with each other.

Figure 5-3 Logical topology



NOTE

Manually configure the following routes to ensure traffic forwarding:

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

Solution Advantages

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

Resource and Cost Planning

Table 5-1 Resource and cost planning

Resource	Parameter	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)	transitIP-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 in department A.
	Transit IP address-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 in department B.
ECS (CN-Hong Kong)	ecs-departmentA	192.168.0.3	N/A	Server of department A, which can communicate with the server of department B
	ecs-departmentB	192.168.0.3	N/A	Server of department B, which can communicate with the server of department A
Private NAT gateways	private-nat-A	N/A	N/A	Private NAT gateway configured in **vpc-departmentA**

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

Prerequisites

- A Huawei Cloud account is available.
- Your account is not in arrears and the account balance is sufficient to pay for the resources involved in this best practice.
- A private NAT gateway is available.

Procedures

1. **Creating VPCs**
2. **Creating ECSs**
3. **Assigning Transit IP Addresses**
4. **Buying a Private NAT Gateway and Adding Rules**
5. **Configuring a Route from a Server to a Private NAT Gateway**
6. **Configuring a VPC Peering Connection Between vpc-transit1 and vpc-transit2**
7. **Verifying Communication Between the Server in Departments A and that in Department B**

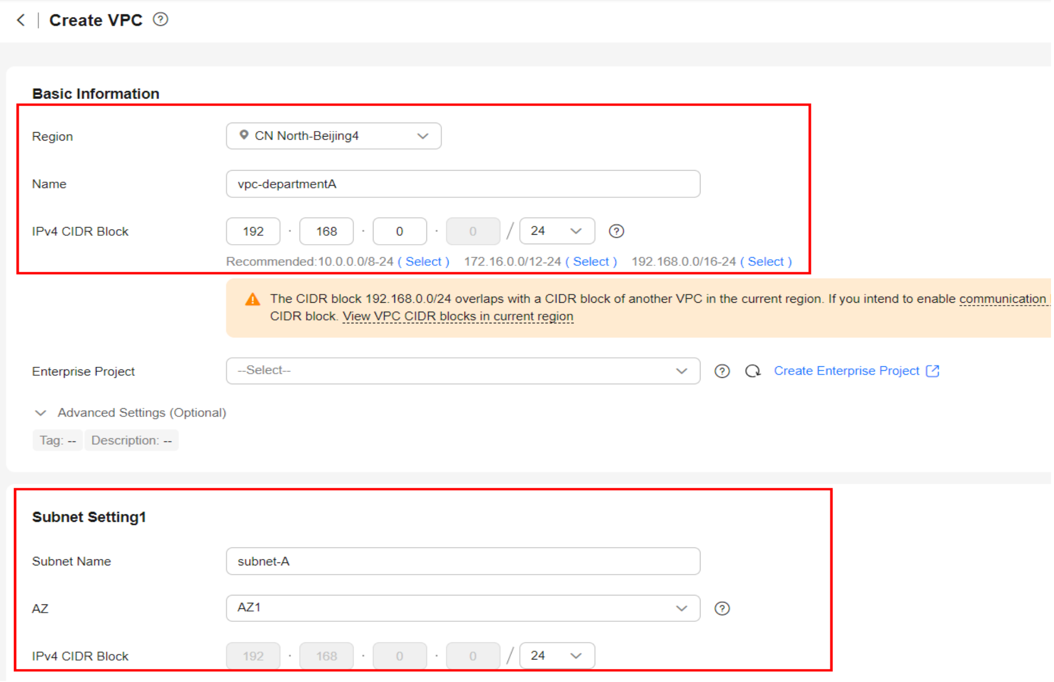
Creating VPCs

Step 1 Go to the **Create VPC** page.

Step 2 On the **Create VPC** page, configure the VPC for department A based on **Table 5-1** 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.
- For parameters not mentioned, retain their default values or configure them as prompted.

Figure 5-4 Create VPC



Basic Information

Region: CN North-Beijing4

Name: vpc-departmentA

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

Recommended:10.0.0.0/8-24 (Select) 172.16.0.0/12-24 (Select) 192.168.0.0/16-24 (Select)

The CIDR block 192.168.0.0/24 overlaps with a CIDR block of another VPC in the current region. If you intend to enable communication
CIDR block. View VPC CIDR blocks in current region

Enterprise Project: --Select--

Tag: -- Description: --

Subnet Setting1

Subnet Name: subnet-A

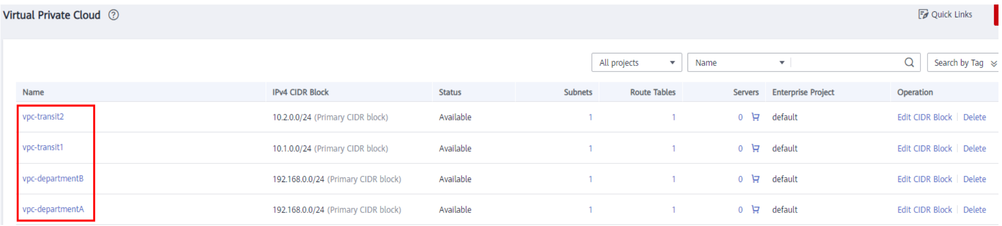
AZ: AZ1

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

Step 3 Repeat the above steps to create all required VPCs in **Table 5-1**.

- **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.
- For parameters not mentioned, retain their default values or configure them as prompted.

Figure 5-5 Creating a VPC



Name	IPv4 CIDR Block	Status	Subnets	Route Tables	Servers	Enterprise Project	Operation
vpc-transit2	10.2.0.0/24 (Primary CIDR block)	Available	1	1	0	default	Edit CIDR Block | Delete
vpc-transit1	10.1.0.0/24 (Primary CIDR block)	Available	1	1	0	default	Edit CIDR Block | Delete
vpc-departmentB	192.168.0.0/24 (Primary CIDR block)	Available	1	1	0	default	Edit CIDR Block | Delete
vpc-departmentA	192.168.0.0/24 (Primary CIDR block)	Available	1	1	0	default	Edit CIDR Block | Delete

----End

Creating ECSs

Step 1 Under **Compute**, select **Elastic Cloud Server**. On the **Elastic Cloud Server** page displayed, click Create **ECS**.

Step 2 Based on **Table 5-1**, configure basic information about the ECS of department A and click **Next: Configure Network**.

- **Billing Mode**: Select **Pay-per-use**.

- **Region**: Select **CN-Hong Kong**.
- **Specifications**: You can select ECS specifications based on your project requirements. This example uses **c6.large.2** as an example.
- **Image**: Select **Public image**. This example uses a CentOS 8.0 image.
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 3 Configure network information for the ECS of department A.

- **Network**: Select VPC **vpc-departmentA**, select **Manually specify IP address**, and set the IP address to **192.168.0.3** planned in **Table 5-1**.
- **Security Group**: Select **Sys-FullAccess**. In this example, we will select a security group that allows all inbound and outbound traffic as the test security group, but you can select a different security group based on service requirements if needed.
- **EIP**: Select **Not required**.
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 4 Click **Next: Configure Advanced Settings**.

Step 5 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.

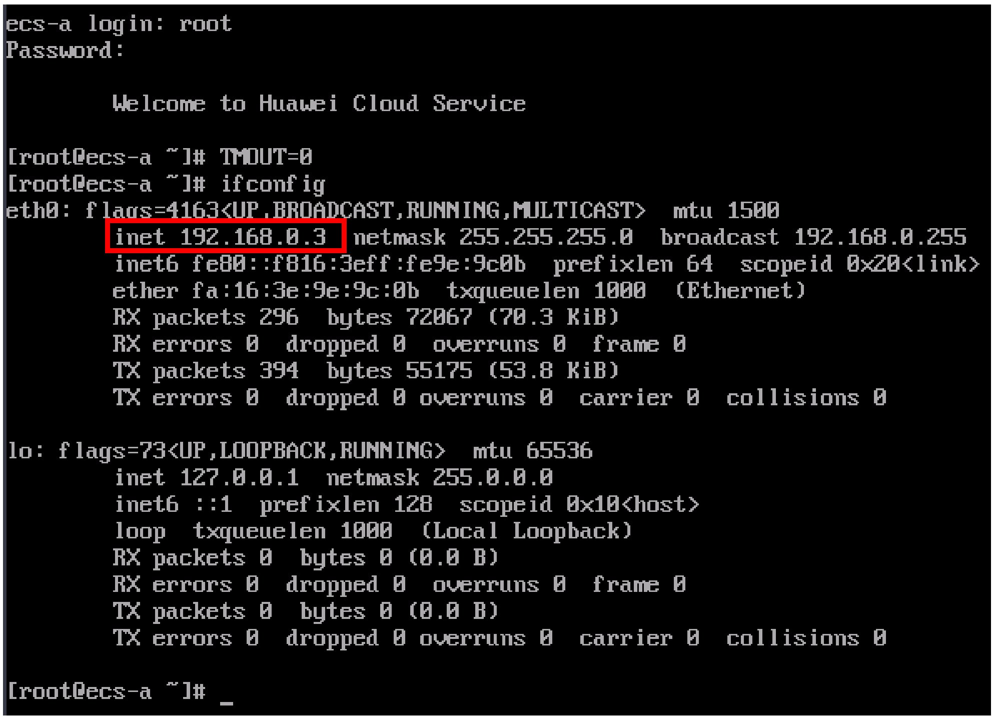
Step 6 Click **Next: Confirm**.

Step 7 Confirm the ECS information, read the agreement and select the **Agreement** option, and click **Submit** to finish the ECS creation for department A.

Step 8 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 9 Log in to the ECS as user **root** and check whether the private IP address of the ECS is the one you planned.

```
ifconfig
```



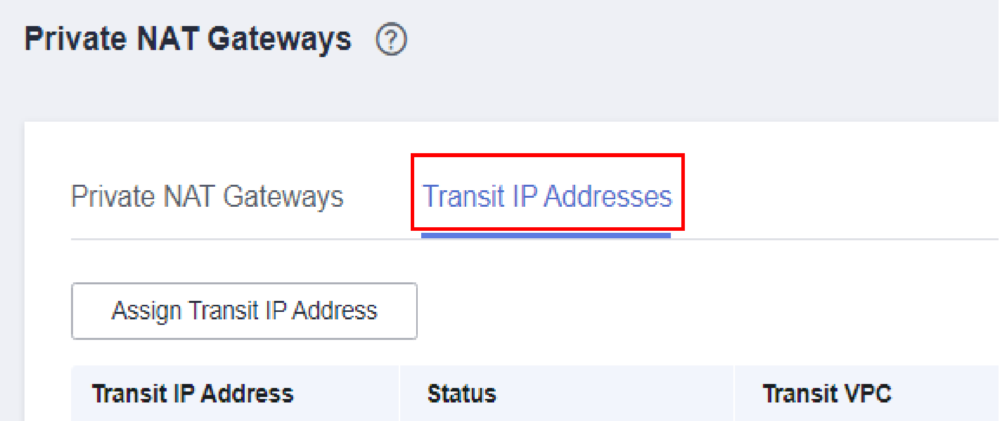
```
ecs-a login: root
Password:

        Welcome to Huawei Cloud Service

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

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

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

Step 10 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.



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 5-1**.

- **Transit VPC**: Select **vpc-transit1**.
- **Transit Subnet**: 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**.
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 3 Click **Buy Now**.

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

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**.
- For parameters not mentioned, retain their default values or configure them as prompted.

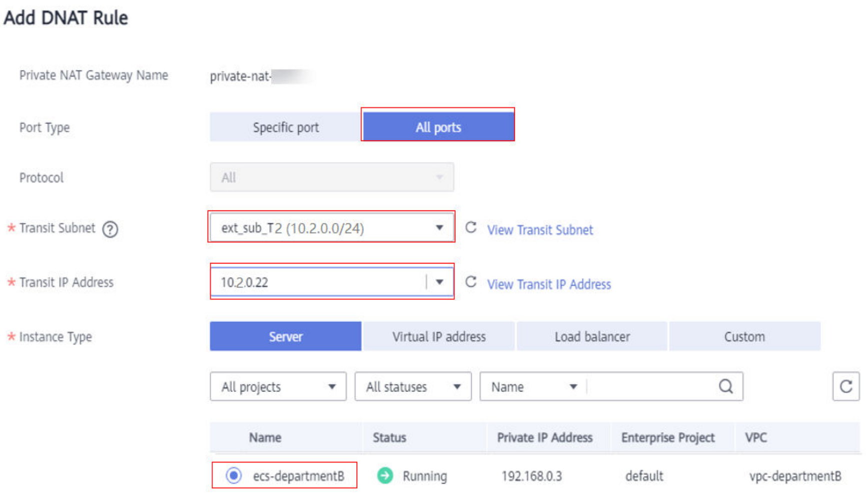
Step 9 Click **Buy Now**.

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**.
- **Transit Subnet**: Select **ext_sub_T2**.
- **Transit IP Address**: Select **10.2.0.22**.
- **Instance Type**: Select **Server** and the ECS of department B.



Add DNAT Rule

Private NAT Gateway Name: private-nat-[redacted]

Port Type: Specific port | All ports

Protocol: All

* Transit Subnet: ext_sub_T2 (10.2.0.0/24) — View Transit Subnet

* Transit IP Address: 10.2.0.22 — View Transit IP Address

* Instance Type: Server | Virtual IP address | Load balancer | Custom

All projects | All statuses | Name

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

----End

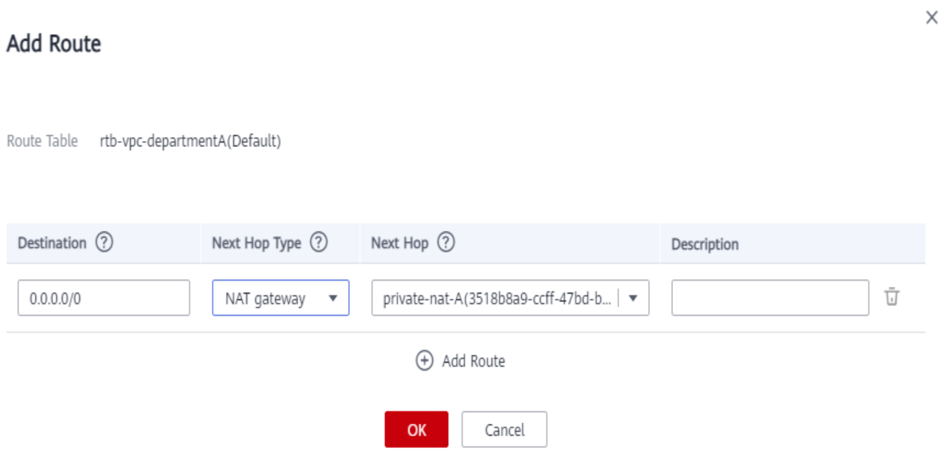
Configuring a Route from a Server to a Private NAT Gateway

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.



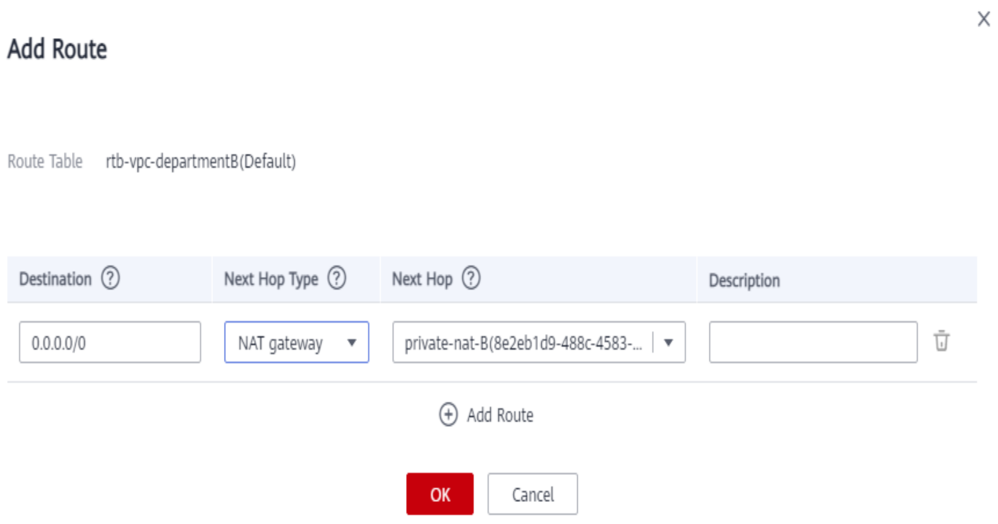
Route Table rtb-vpc-departmentA(Default)

Destination	Next Hop Type	Next Hop	Description
0.0.0.0/0	NAT gateway	private-nat-A(3518b8a9-ccff-47bd-b...	

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.



Route Table rtb-vpc-departmentB(Default)

Destination	Next Hop Type	Next Hop	Description
0.0.0.0/0	NAT gateway	private-nat-B(8e2eb1d9-488c-4583-...	

----End

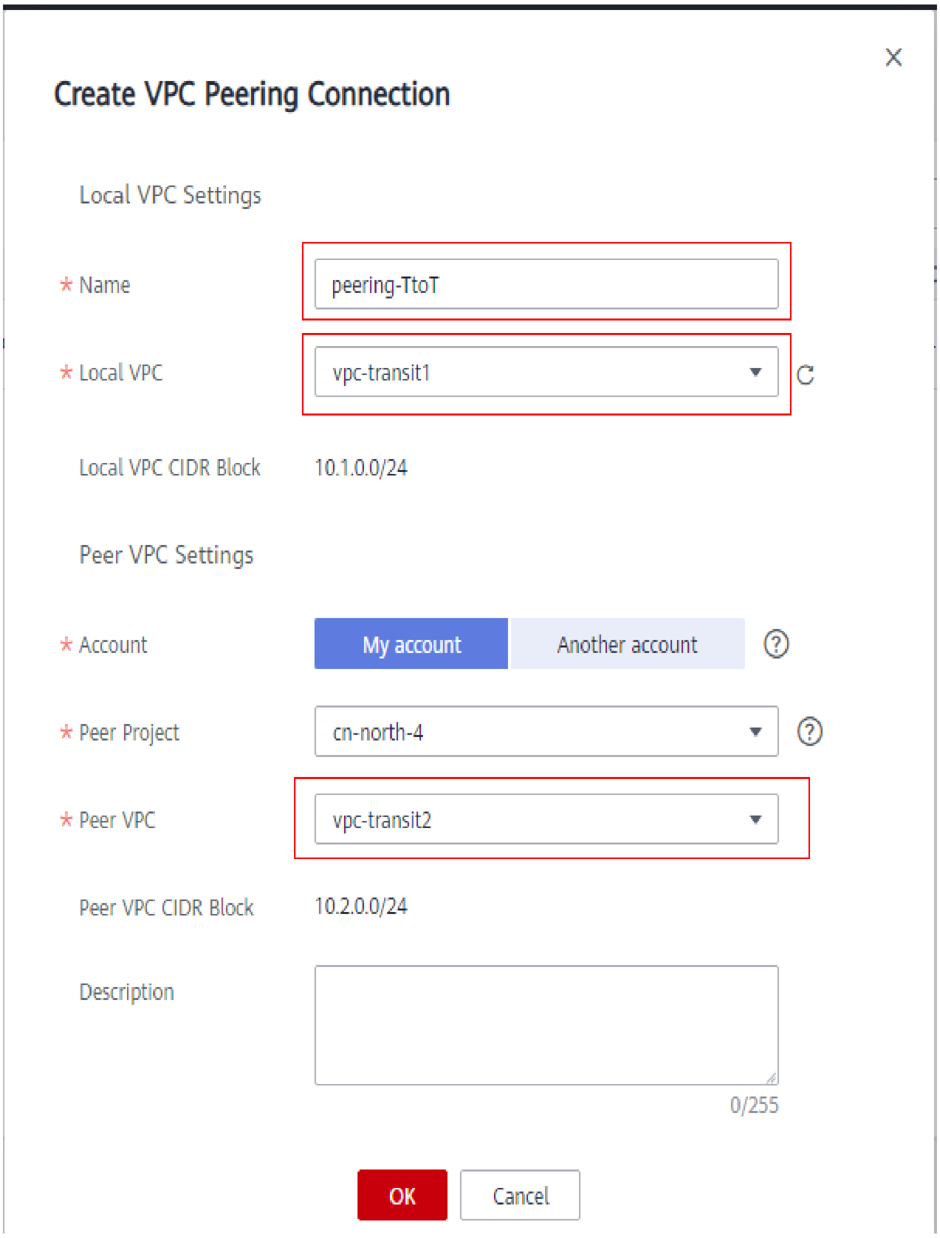
Configuring a VPC Peering Connection Between vpc-transit1 and vpc-transit2

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 transit VPC1 as the local VPC and transit VPC2 as the peer VPC. Configure the following parameters and click **OK**.

- **Name**: Set it to **peering-TtoT**.
- **Local VPC**: Select **vpc-transit1**.
- **Peer VPC**: Select **vpc-transit2**.
- For parameters not mentioned, retain their default values or configure them as prompted.



Create VPC Peering Connection

Local VPC Settings

* Name: peering-TtoT

* Local VPC: vpc-transit1

Local VPC CIDR Block: 10.1.0.0/24

Peer VPC Settings

* Account: My account | Another account

* Peer Project: cn-north-4

* Peer VPC: vpc-transit2

Peer VPC CIDR Block: 10.2.0.0/24

Description: 0/255

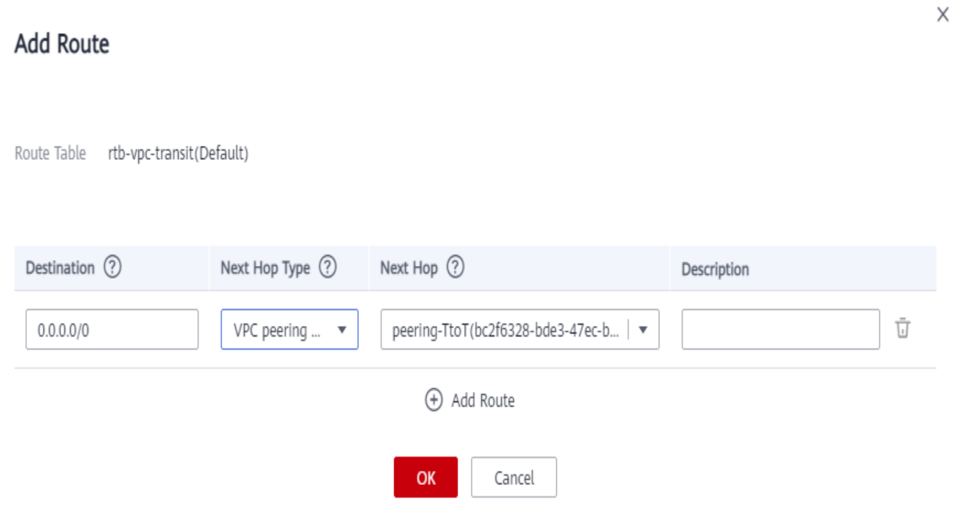
Step 4 Go back to the **VPC Peering Connections** page. In the navigation pane on the left, choose **Route Tables**.

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

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

- **Destination**: Set it to **0.0.0.0/0**.

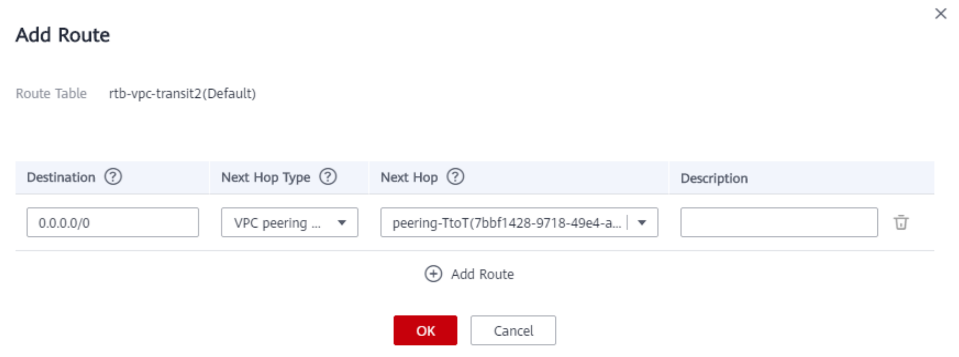
- **Next Hop Type**: Select **VPC peering connection**.
- **Next Hop**: The system automatically displays the VPC peering connection.



Route Table rtb-vpc-transit(Default)

Destination	Next Hop Type	Next Hop	Description
0.0.0.0/0	VPC peering ...	peering-TtoT(bc2f6328-bde3-47ec-b...	

Step 7 Repeat **5** and **6** (selecting **rtb-vpc-transit2**) to configure the route from **vpc-transit2** to the VPC peering connection.



Route Table rtb-vpc-transit2(Default)

Destination	Next Hop Type	Next Hop	Description
0.0.0.0/0	VPC peering ...	peering-TtoT(7bbf1428-9718-49e4-a...	

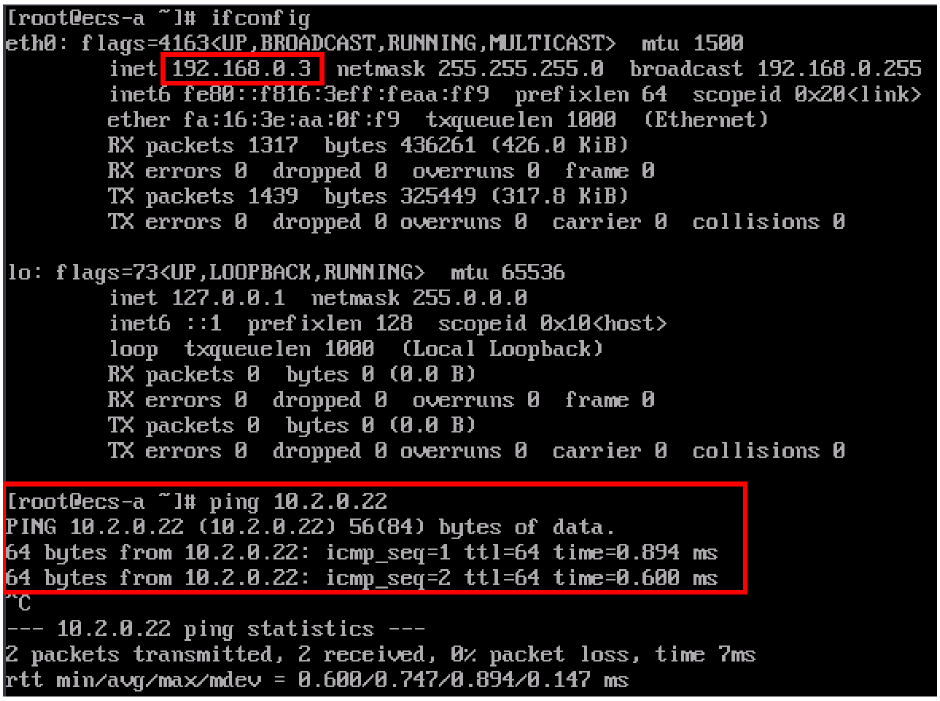
----End

Verifying Communication Between the Server in Departments 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:

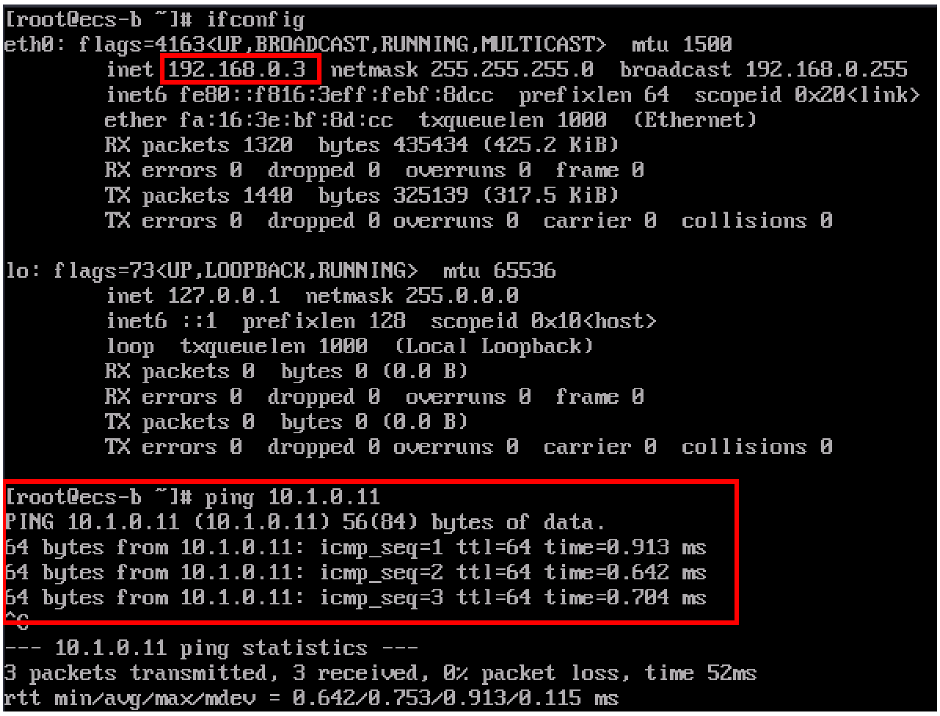
```
ping 10.2.0.22
```



```
[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

5.3 Using a Specified IP Address to Access Hosts Outside a VPC

Scenarios

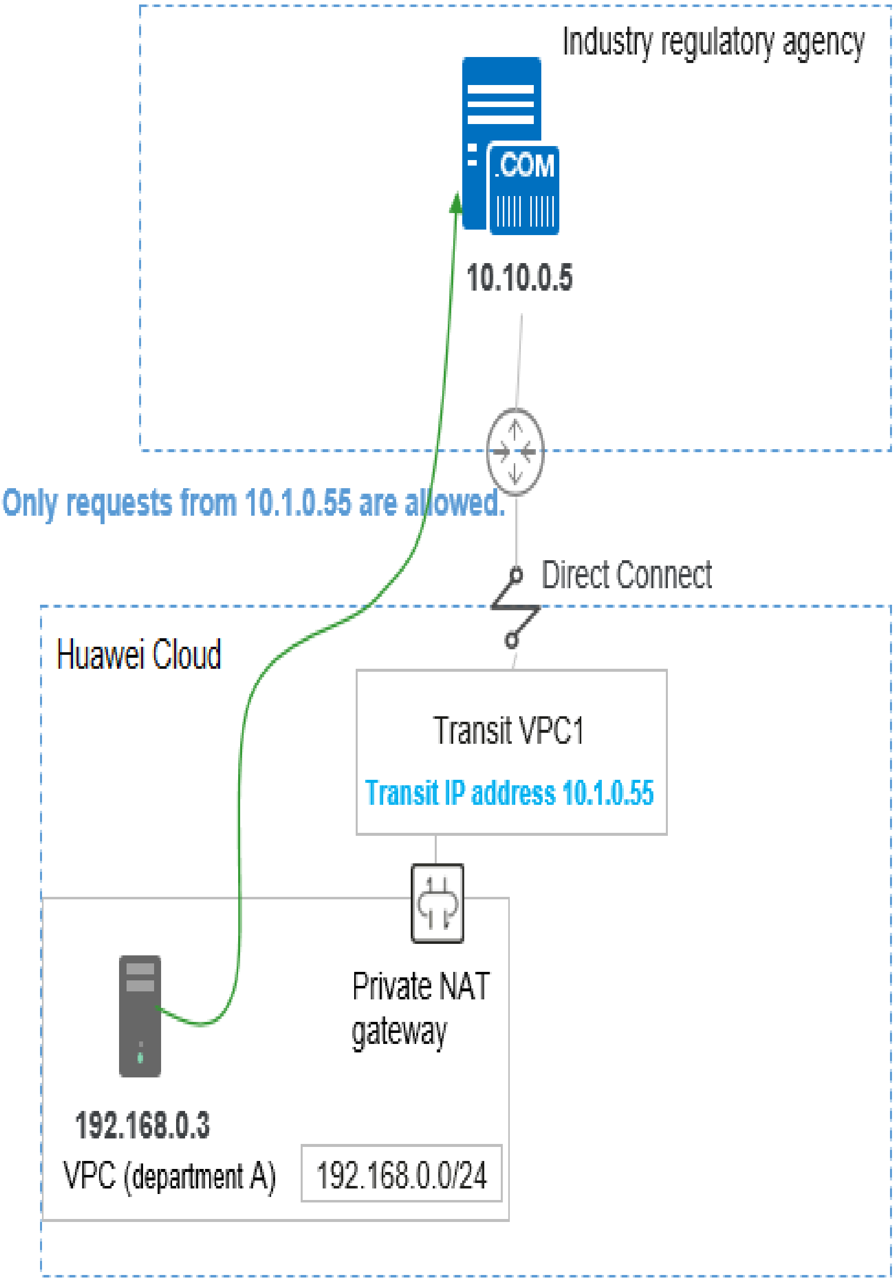
The existing network architecture of the on-premises data center needs to be migrated to the cloud without any changes. **In addition, servers can access external resources with a specified IP address.**

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 (10.10.0.5).

Figure 5-6 Logical topology



Solution Advantages

You can flexibly assign a transit IP address. All servers in the VPC can then use the transit IP address to access hosts outside the VPC.

Resource and Cost Planning

Table 5-2 Resource and cost planning

Resource	Parameter	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 private NAT gateways
	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 in department A, which 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 address of department A	10.1.0.55	N/A	IP address assigned by the regulatory agency. Servers in department A use this IP address to access the regulatory agency.

Prerequisites

- A Huawei Cloud account is available.
- Your account is not in arrears and the account balance is sufficient to pay for the resources involved in this best practice.
- A private NAT gateway is available.
- You have performed operations in **Enabling Mutual Access Between Servers in Overlapping Subnets on the Cloud**.

Procedures

1. **Creating a VPC**
2. **Creating a Security Group**
3. **Creating an ECS**
4. **Configuring Private NAT Gateways**
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 5-2** 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**.
- **AZ**: Select **AZ1**.
- **Name**: Set it to **subnet-W**.
- **IPv4 CIDR Block**: Retain the default value.
- For parameters not mentioned, retain their default values or configure them as prompted.

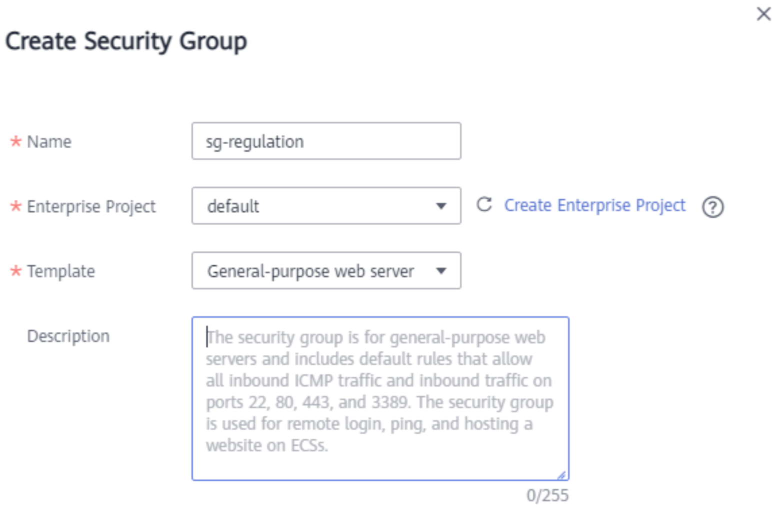
----End

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 **OK**.

- **Name**: Set it to **sg-regulation**.
- **Template**: Select **General-purpose web server**.
- For parameters not mentioned, retain their default values or configure them as prompted.



Create Security Group

* Name: sg-regulation

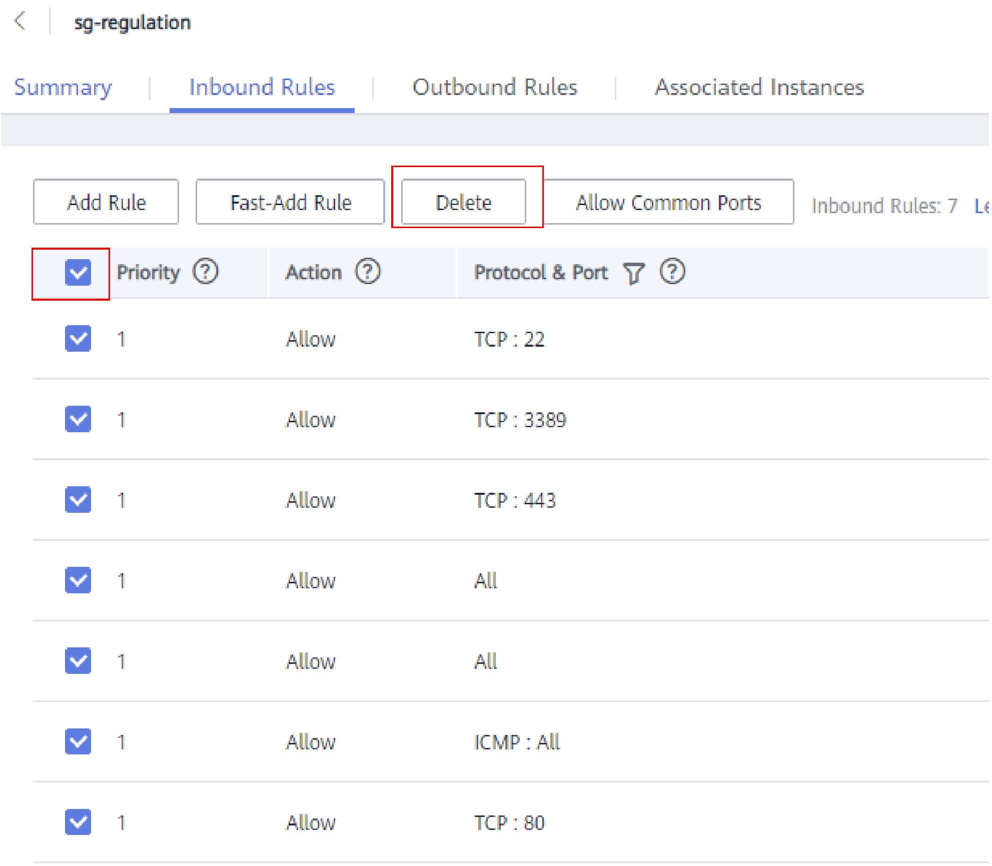
* Enterprise Project: default

* Template: General-purpose web server

Description: The security group is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and inbound traffic on ports 22, 80, 443, and 3389. The security group is used for remote login, ping, and hosting a website on ECSs.

0/255

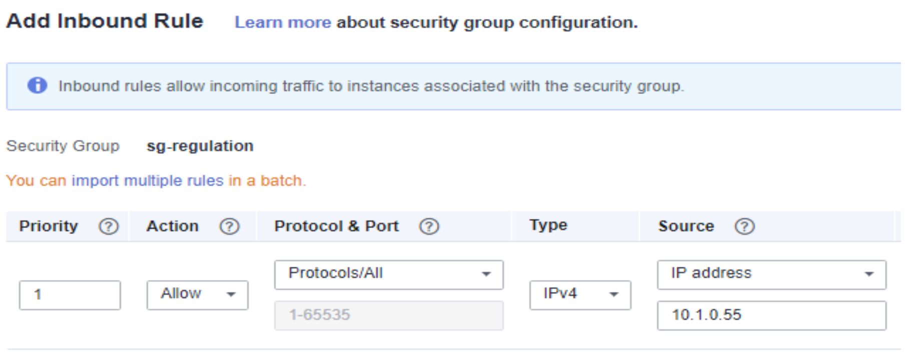
Step 3 Locate **sg-regulation** and click **Manage Rule** in the **Operation** column. On the **sg-regulation** details page, click the **Inbound Rules** tab and delete all rules displayed.



☑	Priority ?	Action ?	Protocol & Port ?
☑	1	Allow	TCP : 22
☑	1	Allow	TCP : 3389
☑	1	Allow	TCP : 443
☑	1	Allow	All
☑	1	Allow	All
☑	1	Allow	ICMP : All
☑	1	Allow	TCP : 80

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

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



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group sg-regulation

You can import multiple rules in a batch.

Priority ?	Action ?	Protocol & Port ?	Type	Source ?
1	Allow	Protocols/All 1-65535	IPv4	IP address 10.1.0.55

----End

Creating an ECS

Step 1 Under **Compute**, select **Elastic Cloud Server**. On the **Elastic Cloud Server** page displayed, click **Buy ECS**.

Step 2 Based on Table 5-2, configure basic information about the ECS of the regulatory agency and click **Next: Configure Network**.

- **Billing Mode**: Select **Pay-per-use**.
- **Region**: Select **CN-Hong Kong**.
- **Specifications**: You can select ECS specifications based on your project requirements. This example uses **c6.large.2** as an example.
- **Image**: Select **Public image**. This example uses a CentOS 8.0 image as an example.
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 3 Configure the ECS network information and click **Next: Configure Advanced Settings**.

- **Network**: Select VPC **vpc-regulation**, select **Manually specify IP address**, and set the IP address to **10.10.0.5** planned in Table 5-2.
- **Security Group**: Select **sg-regulation**.
- **EIP**: Select **Not required**.
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 4 Set the ECS name and password and click **Next: Confirm**.

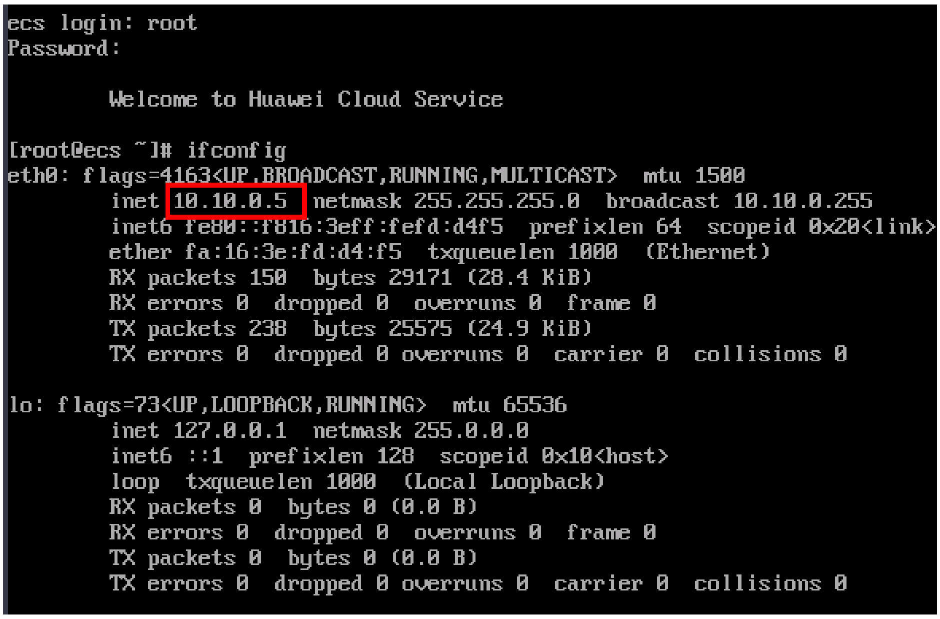
- **ECS Name**: Set it to **ecs-regulation**.
- **Login Mode**: Select **Password** and enter a password.
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 5 Confirm the ECS information, read the agreement and select the **Agreement** option, and click **Submit** to finish the ECS creation for the regulatory agency.

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
```



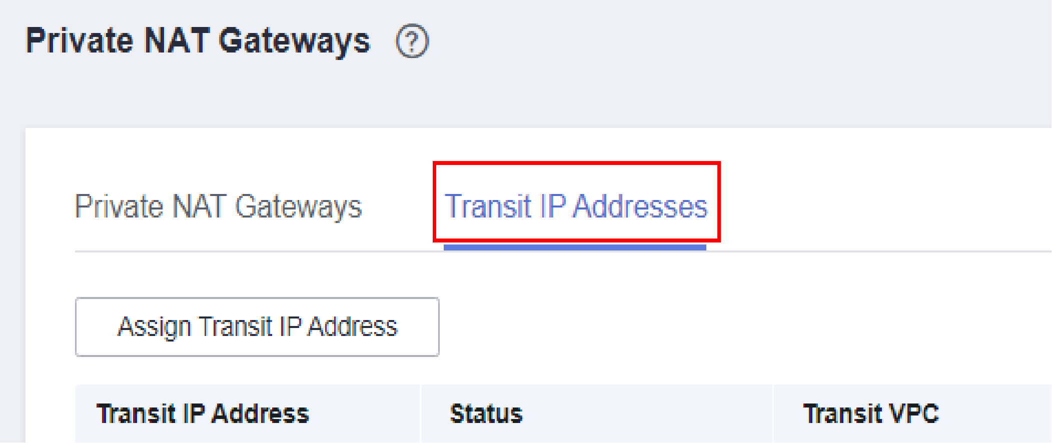
```
ecs login: root
Password:

        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:fefd:d4f5  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:fd:d4:f5  txqueuelen 1000  (Ethernet)
        RX packets 150  bytes 29171 (28.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 238  bytes 25575 (24.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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

----End

Configuring Private NAT Gateways

To assign 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.



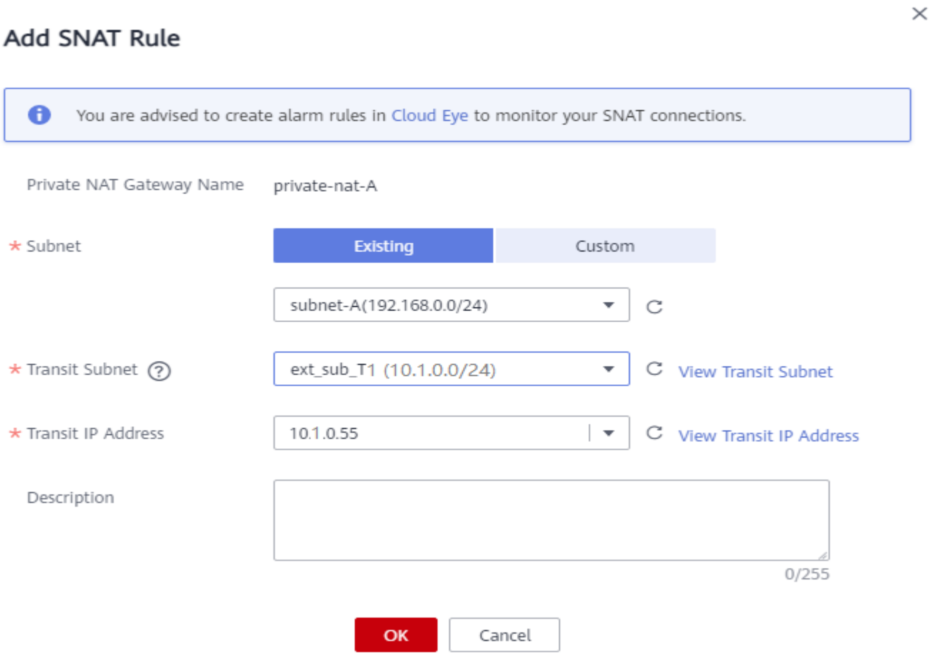
Step 2 Click **Assign Transit IP Address** and configure the parameters as follows:

- **Transit VPC**: Select **vpc-transit1**.
- **Transit Subnet**: 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**.



Add SNAT Rule

You are advised to create alarm rules in Cloud Eye to monitor your SNAT connections.

Private NAT Gateway Name: private-nat-A

* Subnet: Existing | Custom

subnet-A(192.168.0.0/24)

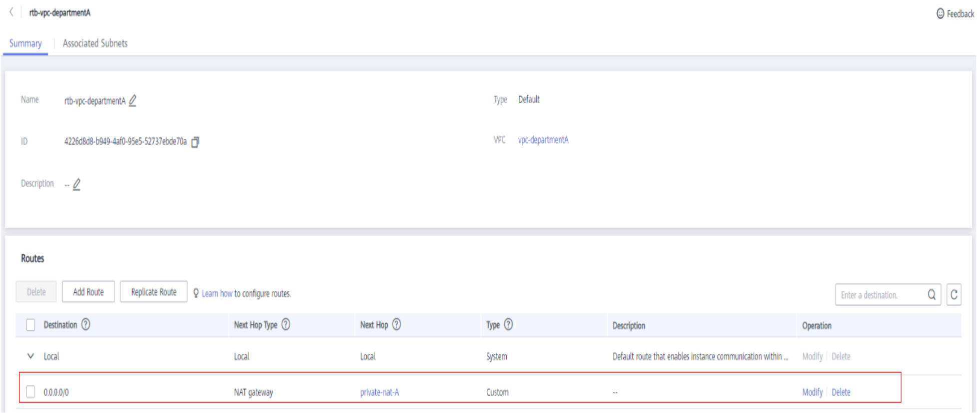
* Transit Subnet: ext_sub_T1 (10.1.0.0/24) View Transit Subnet

* Transit IP Address: 10.1.0.55 View Transit IP Address

Description: 0/255

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 from department A to private NAT gateway **private-nat A** has been added.



rtb-vpc-departmentA

Name: rtb-vpc-departmentA
Type: Default
ID: 4226d8d8-b949-4af0-95e5-52737ebde70a
VPC: vpc-departmentA
Description: --

Routes

Learn how to configure routes.

Destination	Next Hop Type	Next Hop	Type	Description	Operation
Local	Local	Local	System	Default route that enables instance communication within ...	Modify | Delete
0.0.0.0/0	NAT gateway	private-nat-A	Custom	--	Modify | Delete

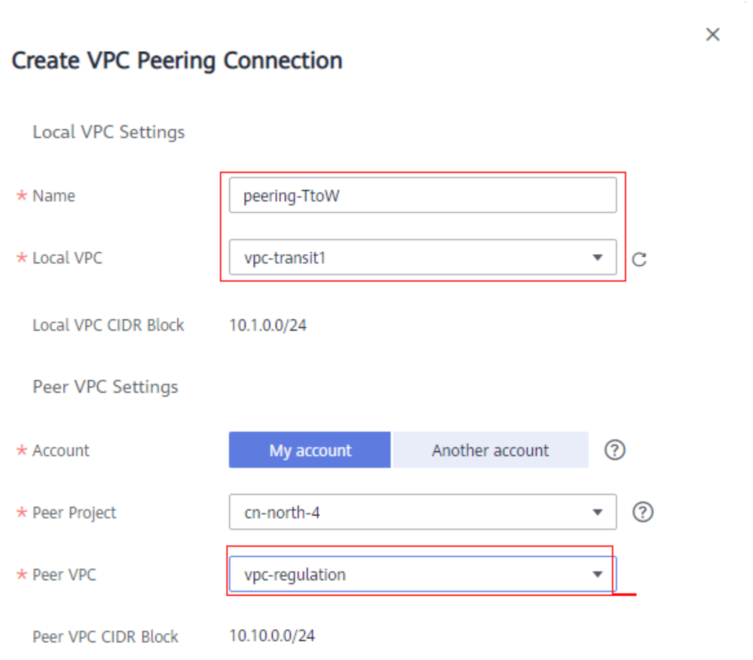
----End

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 Configure the following parameters and click **OK**.

- **Name**: Set it to **peering-TtoW**.
- **Local VPC**: Select **vpc-transit1**.
- **Peer VPC**: Select **vpc-regulation**.
- For parameters not mentioned, retain their default values or configure them as prompted.



Create VPC Peering Connection

Local VPC Settings

* Name: peering-TtoW

* Local VPC: vpc-transit1

Local VPC CIDR Block: 10.1.0.0/24

Peer VPC Settings

* Account: My account | Another account

* Peer Project: cn-north-4

* Peer VPC: vpc-regulation

Peer VPC CIDR Block: 10.10.0.0/24

----End

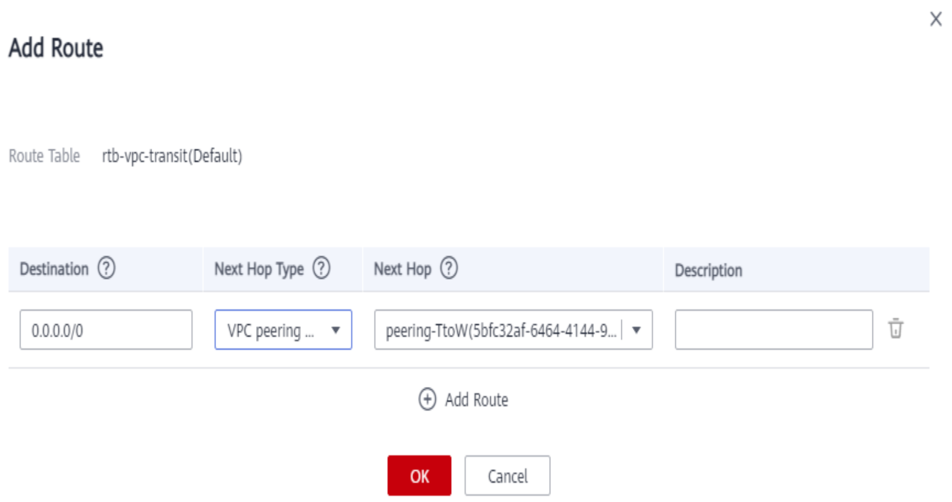
Configuring Routes

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.



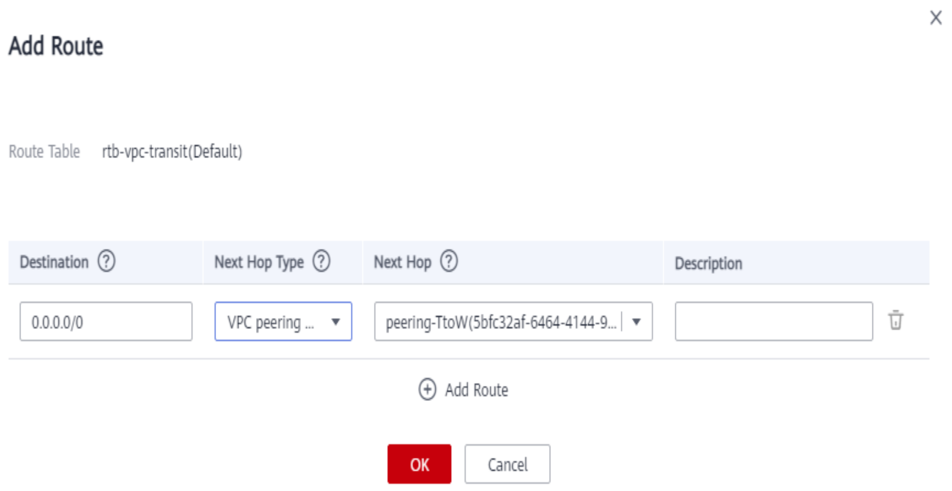
Route Table rtb-vpc-transit(Default)

Destination	Next Hop Type	Next Hop	Description
0.0.0.0/0	VPC peering ...	peering-TtoW(5bfc32af-6464-4144-9...	

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.



Route Table rtb-vpc-transit(Default)

Destination	Next Hop Type	Next Hop	Description
0.0.0.0/0	VPC peering ...	peering-TtoW(5bfc32af-6464-4144-9...	

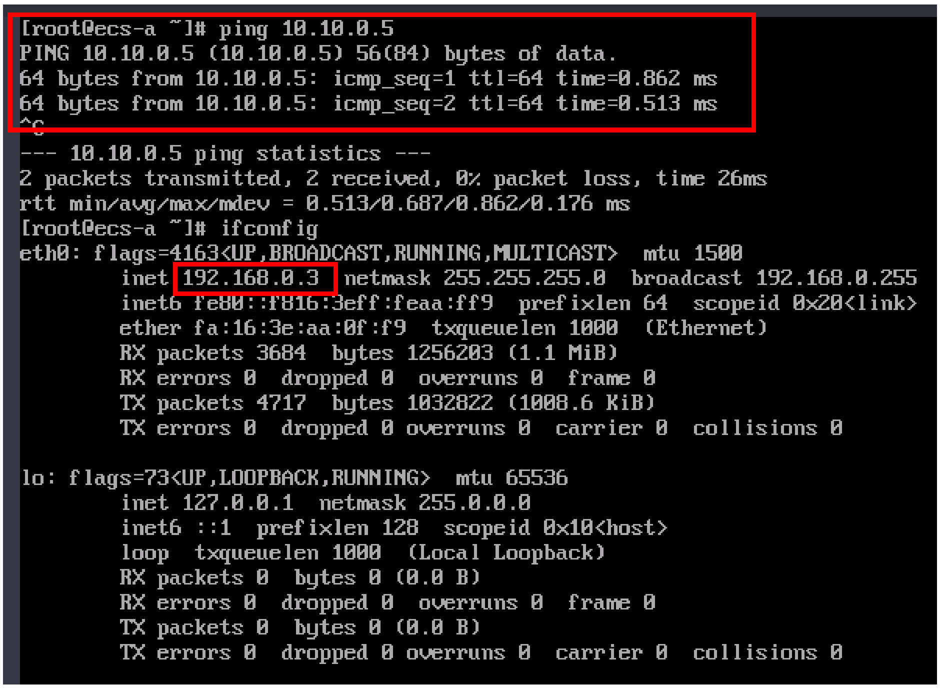
----End

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