NAT Gateway

Getting Started

Issue	01
Date	2020-10-23



HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. 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 Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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 Using SNAT to Access the Internet..... 1
1.1 Overview..... 1
1.2 Preparations..... 1
1.3 Step 1: Buy an EIP..... 2
1.4 Step 2: Buy a Public NAT Gateway..... 2
1.5 Step 3: Add an SNAT Rule..... 5
1.6 Step 4: Verify the Result..... 6
2 Using DNAT to Provide Services Accessible from the Internet..... 8
2.1 Overview..... 8
2.2 Preparations..... 9
2.3 Step 1: Buy an EIP..... 9
2.4 Step 2: Buy a Public NAT Gateway..... 9
2.5 Step 3: Add a DNAT Rule..... 12
2.6 Step 4: Verify the Result..... 14
3 Using SNAT and DNAT Rules to Allow On-premises Servers to Communicate Over the Internet..... 15
3.1 Overview..... 15
3.2 Preparations..... 16
3.3 Step 1: Create a Direct Connect Connection..... 17
3.4 Step 2: Buy an EIP..... 18
3.5 Step 3: Buy a Public NAT Gateway..... 19
3.6 Step 4: Add an SNAT Rule..... 21
3.7 Step 5: Add a DNAT Rule..... 23
4 Using Private NAT Gateways to Enable Communication Between Cloud and On-premises Networks..... 26
4.1 Overview..... 26
4.2 Preparations..... 27
4.3 Step 1: Create a Service VPC and a Transit VPC..... 28
4.4 Step 2: Create a Direct Connect Connection..... 28
4.5 Step 3: Create a Private NAT Gateway..... 28
4.6 Step 4: Add an SNAT Rule..... 31
4.7 Step 5: Add a Route..... 32

 Copyright © Huawei Technologies Co., Ltd.

4.8 Step 6: Add a Security Group Rule....33

5 Using Multiple Public NAT Gateways Together in Performance-Demanding Scenarios....36

5.1 Overview....36
5.2 Preparations....37
5.3 Step 1: Create a VPC and Two Subnets....38
5.4 Step 2: Buy a Public NAT Gateway....38
5.5 Step 3: Check Whether the Default Route Exists....40
5.6 Step 4: Create a Route Table....41
5.7 Step 5: Buy a Public NAT Gateway....42
5.8 Step 6: Add the Default Route....44

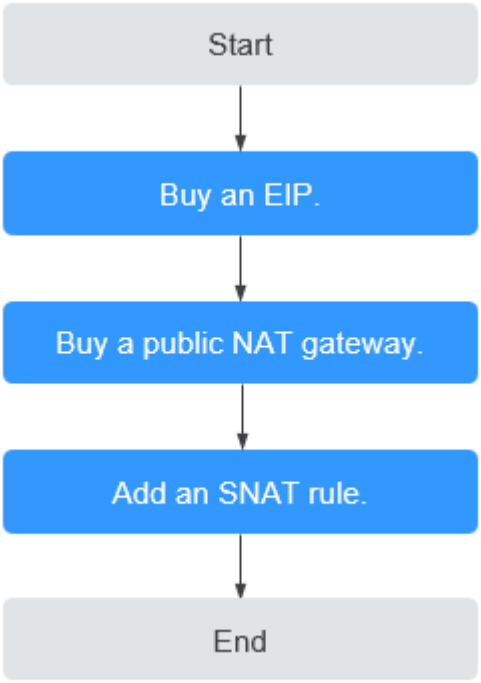
 Copyright © Huawei Technologies Co., Ltd.

1 Using SNAT to Access the Internet

1.1 Overview

If servers (ECSs, BMSs, or desktops) without EIPs bound need to access the Internet, the servers can share one or more EIPs to access the Internet through a public NAT gateway. This method provides access without exposing their IP addresses. **Figure 1-1** illustrates the process.

Figure 1-1 Flowchart



1.2 Preparations

Before using a NAT gateway, you need to complete the items described in this section.

 Copyright © Huawei Technologies Co., Ltd.

Registering with HUAWEI CLOUD and Completing Real-name Authentication

If you already have an authenticated HUAWEI CLOUD account, skip this part. If you do not have a HUAWEI CLOUD account, perform the following steps to create one:

1. Visit **https://www.huaweicloud.com/** and click **Register**.
2. On the displayed page, register an account as prompted. For details, see **Registering with HUAWEI CLOUD.**

   After your registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in **Individual Real-Name Authentication**.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For details about the price of NAT gateways, see **Product Pricing Details**.
- For details about how to top up an account, see **Topping Up an Account**.

1.3 Step 1: Buy an EIP

Scenarios

Buy an EIP and enable your servers in a VPC to access the Internet through a NAT gateway by sharing the EIP.

NOTE

For details about the EIP pricing, see **Billing**.

Procedure

For details, see **Assigning an EIP**. After you assign an EIP, you do not need to bind it to a server here.

1.4 Step 2: Buy a Public NAT Gateway

Scenarios

This section describes how to buy a public NAT gateway to enable your servers to access the Internet or to provide services for external networks.

Prerequisites

- When buying a public NAT gateway, you must specify its VPC, subnet, and type.
- Check whether the default route (0.0.0.0/0) of the VPC has been used by other gateways. If the default route of the VPC has been used by other

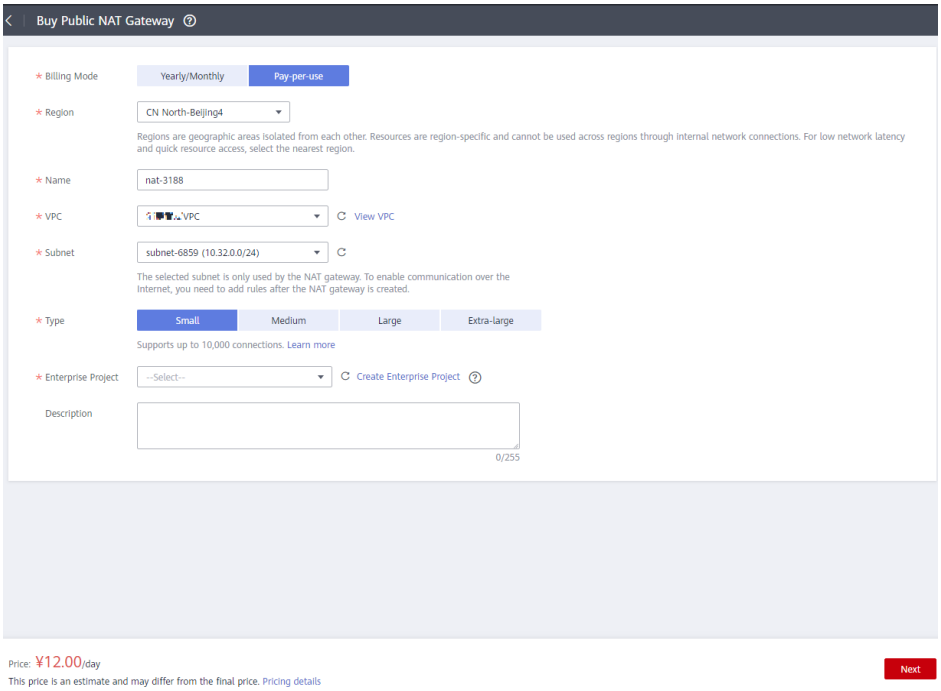
 Copyright © Huawei Technologies Co., Ltd.

gateways, add another route for this gateway or add the default route to a new route table to be associated with the gateway after the gateway is created.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.
4. On the displayed page, click **Buy Public NAT Gateway**.

Figure 1-2 Buy Public NAT Gateway



5. Set the parameters as prompted. For details, see **Table 1-1**.

Table 1-1 Parameter description

Parameter	Description
Region	The region where the public NAT gateway is located.
Billing Mode	Public NAT gateways are billed on a pay-per-use or yearly/monthly basis.
Name	The name of the public NAT gateway. The name can include up to 64 characters and can include digits, letters, underscores (_), and hyphens (-).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
VPC	The VPC that the public NAT gateway belongs to. Check whether the default route (0.0.0.0/0) of the VPC has been used by other gateways. If the default route of the VPC has been used by other gateways, add another route for this gateway or add the default route to a new route table to be associated with the gateway after the gateway is created. The selected VPC cannot be changed after the public NAT gateway is purchased.
Subnet	The subnet of the VPC that the public NAT gateway belongs to. The subnet must have at least one available IP address. The selected subnet cannot be changed after the public NAT gateway is purchased.
Type	The type of the public NAT gateway. The type can be **Small**, **Medium**, **Large**, and **Extra-large**. You can click **Learn more** on the page to view details about each type.
Enterprise Project	The enterprise project that the public NAT gateway belongs to. If an enterprise project is configured for a public NAT gateway, the public NAT gateway belongs to this enterprise project. If you do not specify an enterprise project, the **default** enterprise project will be used.
Description	Supplementary information about the public NAT gateway. The description can contain up to 255 characters.
Required Duration	The required duration of the public NAT gateway.

After these parameters are set, the public NAT gateway price will be displayed. You can click **Pricing details** on the page to view pricing details.

6. Click **Next**. The page for you to confirm the public NAT gateway specifications is displayed.
7. If you do not need to modify the information, click **Submit**.

   It takes 1 to 5 minutes to create a public NAT gateway.
8. In the public NAT gateway list, you can see the public NAT gateway status.

 Copyright © Huawei Technologies Co., Ltd.

1.5 Step 3: Add an SNAT Rule

Scenarios

After the public NAT gateway is created, you need to add SNAT rules. With an SNAT rule, your servers in a specified subnet can access the Internet by sharing the same EIP.

Each SNAT rule is configured for one subnet or CIDR block. If there are multiple subnets or CIDR blocks in a VPC, you can create several SNAT rules to allow multiple servers to share EIPs.

Prerequisites

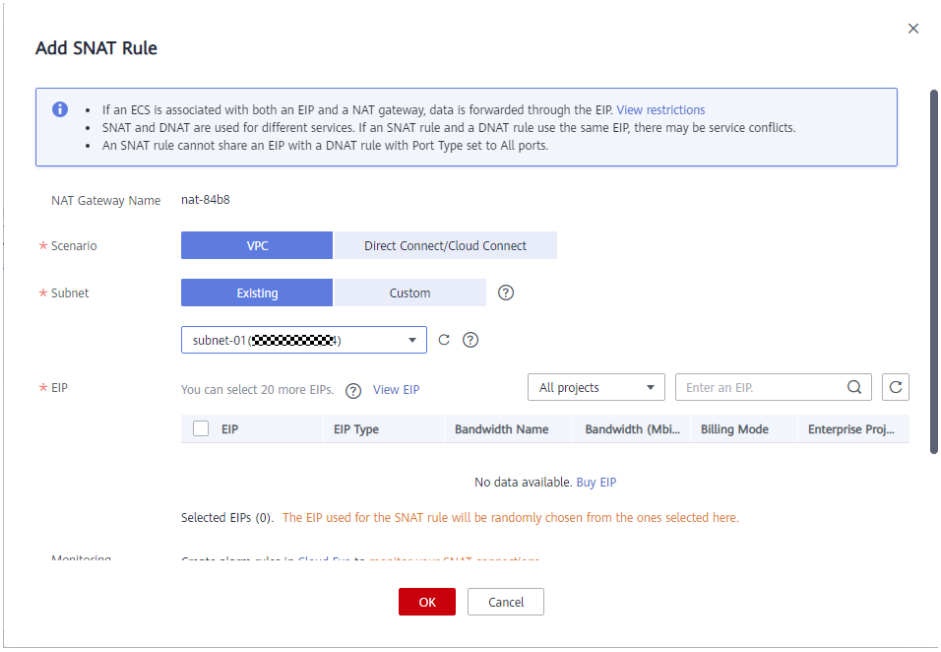
A public NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the public NAT gateway for which you want to add the SNAT rule.
5. On the **SNAT Rules** tab, click **Add SNAT Rule**.

   Figure 1-3 Add SNAT Rule



6. Set the parameters as prompted. **Table 1-2** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 1-2 Parameter description

Parameter	Condition	Description
Scenario	N/A	Select **VPC** if your servers in a VPC will use the SNAT rule to access the Internet. Different servers in a VPC can share the same EIP to access the Internet.
Subnet	This parameter is available only when you select **VPC** for **Scenario**.	Select a subnet or enter a CIDR block in which servers can access the Internet through the SNAT rule.
EIP	This parameter is available when you select **VPC** for **Scenario**.	The EIP used for accessing the Internet. You can select an EIP that either has not been bound, has been bound to a DNAT rule with **Port Type** set to **Specific port** of the current NAT gateway, or has been bound to an SNAT rule of the current NAT gateway. You can select multiple EIPs at once. Up to 20 EIPs can be selected for each SNAT rule. The EIP used for the SNAT rule is randomly chosen from the ones you select when you add the rule.
Monitoring	N/A	Alarm rules are created in Cloud Eye. The alarm rules help you monitor your SNAT connections and keep you informed of any changes in a timely manner.
Description	N/A	Supplementary information about the SNAT rule. The description can contain up to 255 characters.

7. Click **OK**.

   NOTE

   You can add multiple SNAT rules for a public NAT gateway to suite your service requirements.

1.6 Step 4: Verify the Result

Scenario

After you add an SNAT rule to a public NAT gateway, you can verify that the SNAT rule has been added.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.
4. On the displayed page, click the name of the target public NAT gateway.
5. In the SNAT rule list, you can view details about the SNAT rule. If **Status** is **Running**, the rule has been added.

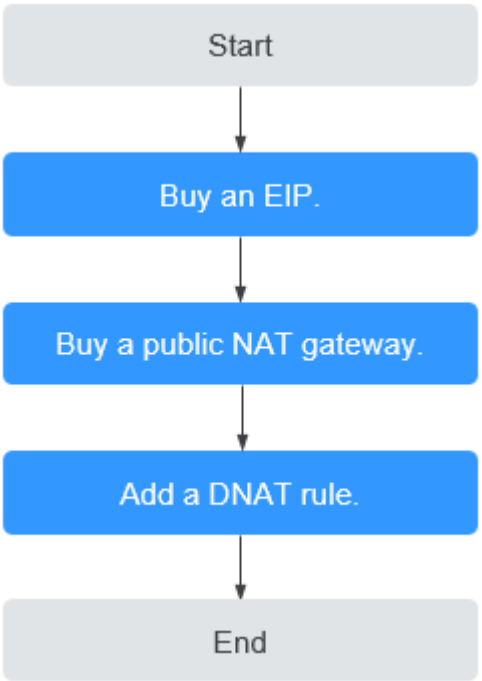
 Copyright © Huawei Technologies Co., Ltd.

2 Using DNAT to Provide Services Accessible from the Internet

2.1 Overview

When one or more servers (ECSs, BMSs, and Workspace desktops) in a VPC need to provide services accessible from the Internet, you can add DNAT rules.

Figure 2-1 Flowchart



 Copyright © Huawei Technologies Co., Ltd.

2.2 Preparations

Before using a NAT gateway, you need to complete the items described in this section.

Registering with HUAWEI CLOUD and Completing Real-name Authentication

If you already have an authenticated HUAWEI CLOUD account, skip this part. If you do not have a HUAWEI CLOUD account, perform the following steps to create one:

1. Visit **https://www.huaweicloud.com/** and click **Register**.
2. On the displayed page, register an account as prompted. For details, see **Registering with HUAWEI CLOUD.**

   After your registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in **Individual Real-Name Authentication**.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For details about the price of NAT gateways, see **Product Pricing Details**.
- For details about how to top up an account, see **Topping Up an Account**.

2.3 Step 1: Buy an EIP

Scenarios

Buy an EIP and enable servers in a VPC to provide services accessible from the Internet using a NAT gateway by sharing the EIP.

NOTE

For details about the EIP pricing, see **Billing**.

Procedure

For details, see **Assigning an EIP**. After you assign an EIP, you do not need to bind it to a server here.

2.4 Step 2: Buy a Public NAT Gateway

Scenarios

This section describes how to buy a public NAT gateway to enable your servers to access the Internet or to provide services for external networks.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

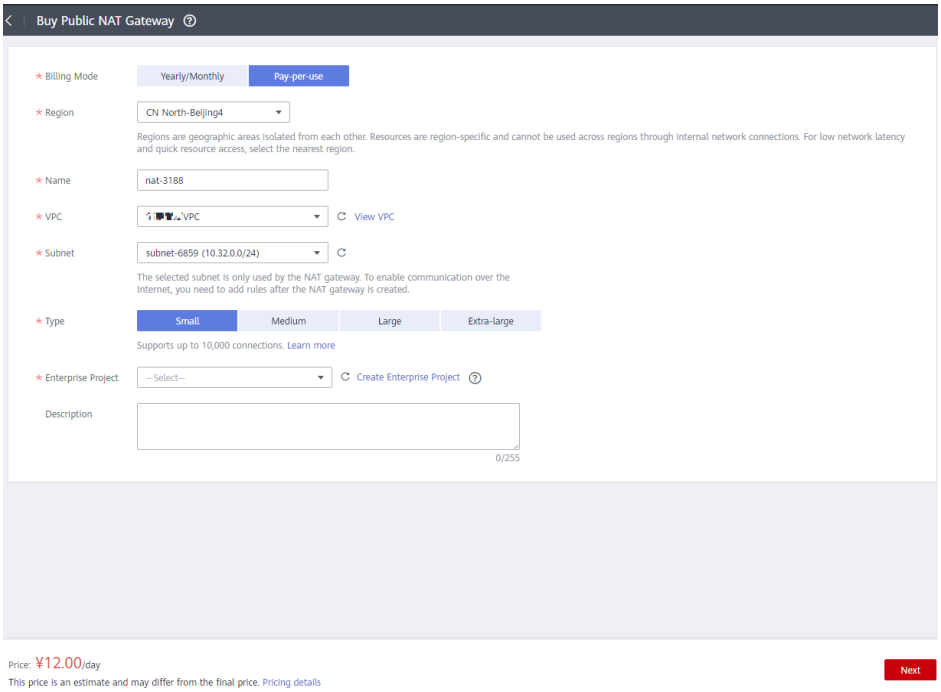
- When buying a public NAT gateway, you must specify its VPC, subnet, and type.
- Check whether the default route (0.0.0.0/0) of the VPC has been used by other gateways. If the default route of the VPC has been used by other gateways, add another route for this gateway or add the default route to a new route table to be associated with the gateway after the gateway is created.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   Switch to the public NAT gateway page.
4. On the displayed page, click **Buy Public NAT Gateway**.

Figure 2-2 Buy Public NAT Gateway



5. Set the parameters as prompted. For details, see **Table 2-1**.

Table 2-1 Parameter description

Parameter	Description
Region	The region where the public NAT gateway is located.
Billing Mode	Public NAT gateways are billed on a pay-per-use or yearly/monthly basis.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Name	The name of the public NAT gateway. The name can include up to 64 characters and can include digits, letters, underscores (_), and hyphens (-).
VPC	The VPC that the public NAT gateway belongs to. Check whether the default route (0.0.0.0/0) of the VPC has been used by other gateways. If the default route of the VPC has been used by other gateways, add another route for this gateway or add the default route to a new route table to be associated with the gateway after the gateway is created. The selected VPC cannot be changed after the public NAT gateway is purchased.
Subnet	The subnet of the VPC that the public NAT gateway belongs to. The subnet must have at least one available IP address. The selected subnet cannot be changed after the public NAT gateway is purchased.
Type	The type of the public NAT gateway. The type can be **Small**, **Medium**, **Large**, and **Extra-large**. You can click **Learn more** on the page to view details about each type.
Enterprise Project	The enterprise project that the public NAT gateway belongs to. If an enterprise project is configured for a public NAT gateway, the public NAT gateway belongs to this enterprise project. If you do not specify an enterprise project, the **default** enterprise project will be used.
Description	Supplementary information about the public NAT gateway. The description can contain up to 255 characters.
Required Duration	The required duration of the public NAT gateway.

After these parameters are set, the public NAT gateway price will be displayed. You can click **Pricing details** on the page to view pricing details.

6. Click **Next**. The page for you to confirm the public NAT gateway specifications is displayed.
7. If you do not need to modify the information, click **Submit**.

   It takes 1 to 5 minutes to create a public NAT gateway.
8. In the public NAT gateway list, you can see the public NAT gateway status.

 Copyright © Huawei Technologies Co., Ltd.

2.5 Step 3: Add a DNAT Rule

Scenarios

After a public NAT gateway is created, you can add DNAT rules to allow servers in your VPC to provide services accessible from the Internet.

You can configure a DNAT rule for each port of a server. If multiple servers need to provide services accessible from the Internet, you need to create multiple DNAT rules.

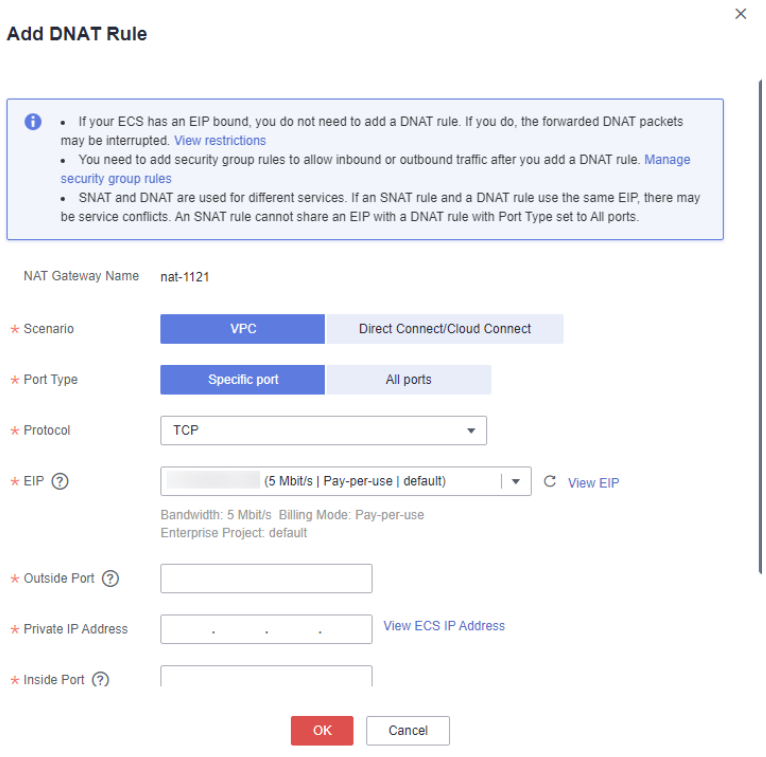
Prerequisites

A public NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the public NAT gateway for which you want to add the DNAT rule.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.
6. Click **Add DNAT Rule**.

Figure 2-3 Add DNAT Rule



 Copyright © Huawei Technologies Co., Ltd.

7. Set the parameters as prompted. For details, see **Table 2-2**.

Table 2-2 Parameter descriptions

Parameter	Description
Scenario	Select **VPC** if your servers in a VPC will use the DNAT rule to provide services accessible from the Internet. Different servers in a VPC can share the same EIP to provide services accessible from the Internet.
Port Type	The port type. You can select **All ports** or **Specific port**. • **All ports**: This is equivalent to assigning an EIP to a server. Any requests on the EIP will be forwarded by the NAT gateway to your server based on IP address mapping. • **Specific port**: The NAT gateway only forwards requests with a specific protocol and port on the EIP to the corresponding port of the target server.
Protocol	The protocol can be TCP or UDP. This parameter is available if you select **Specific port** for **Port Type**. If you select **All ports**, this parameter is **All** by default.
EIP	The EIP that will be used by the server to provide services accessible from the Internet. You can select an EIP that either has not been bound, has been bound to a DNAT rule with **Port Type** set to **Specific port** of the current NAT gateway, or has been bound to an SNAT rule of the current NAT gateway.
Outside Port	The port of the EIP. This parameter is available if you select **Specific port** for **Port Type**. The port number must range from 1 to 65535. You can enter a single port number or a port range, for example, 80 or 80-100.
Private IP Address	The IP address of the server that provides services accessible from the Internet through the DNAT rule. Configure the port of **Private IP Address** if you select **Specific port** for **Port Type**.
Inside Port	The port of the server that provides services accessible from the Internet through the DNAT rule. This parameter is available if you select **Specific port** for **Port Type**. The port number must range from 1 to 65535. You can enter a single port number or a port range, for example, 80 or 80-100.
Description	Supplementary information about the DNAT rule. The description can contain up to 255 characters.

 Copyright © Huawei Technologies Co., Ltd.

8. Click **OK**.

2.6 Step 4: Verify the Result

Scenarios

After you add a DNAT rule to a public NAT gateway, you can verify that the DNAT rule has been added.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.
4. On the displayed page, click the name of the target public NAT gateway.
5. In the DNAT rule list, you can view details about the DNAT rule. If **Status** is **Running**, the DNAT rule has been added.

 Copyright © Huawei Technologies Co., Ltd.

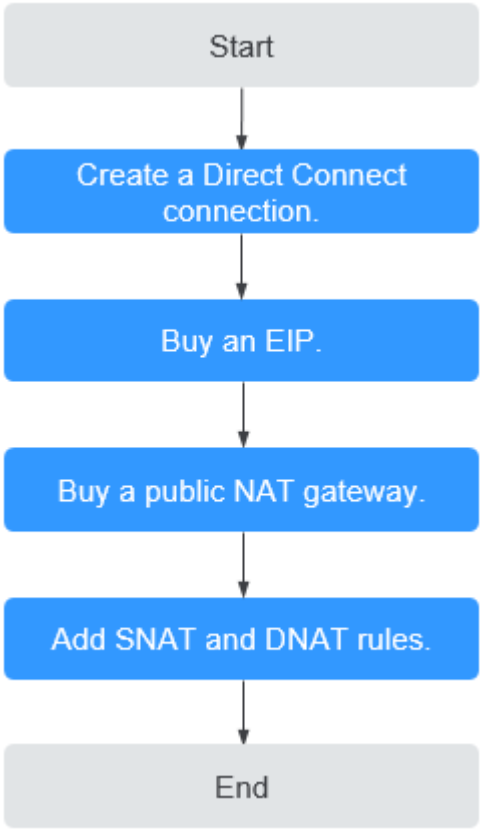
3 Using SNAT and DNAT Rules to Allow On-premises Servers to Communicate Over the Internet

3.1 Overview

Public NAT gateways allow servers in your data center to access the Internet or to provide services accessible from the Internet. You need to first create a Direct Connect or VPN connection to connect your servers in an on-premises data center to the cloud, and then buy public NAT gateways and configure SNAT rules to obtain the required services. **Figure 3-1** shows how servers in an on-premises data center communicate with the Internet.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-1 Servers in a local data center communicating with the Internet



3.2 Preparations

Before using a NAT gateway, you need to complete the items described in this section.

Registering with HUAWEI CLOUD and Completing Real-name Authentication

If you already have an authenticated HUAWEI CLOUD account, skip this part. If you do not have a HUAWEI CLOUD account, perform the following steps to create one:

1. Visit **https://www.huaweicloud.com/** and click **Register**.
2. On the displayed page, register an account as prompted. For details, see **Registering with HUAWEI CLOUD.**

   After your registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in **Individual Real-Name Authentication**.

Topping Up Your Account

Ensure that your account balance is sufficient.

 Copyright © Huawei Technologies Co., Ltd.

- For details about the price of NAT gateways, see **Product Pricing Details**.
- For details about how to top up an account, see **Topping Up an Account**.

3.3 Step 1: Create a Direct Connect Connection

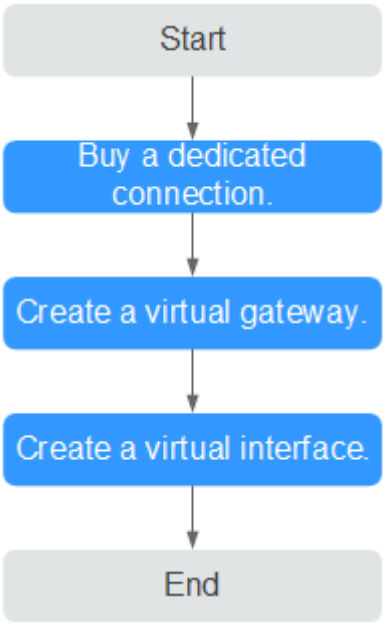
Scenarios

You need to create a Direct Connect connection for connecting a VPC to your data center before enabling your servers in the data center to access the Internet or to provide services accessible from the Internet through public NAT gateways.

Process

You need to apply for a connection, book the port used to connect your data center to the access point, cooperate with the carrier to set up the connection, create a virtual gateway and associate it with a VPC, and finally create a virtual interface to connect to the VPC. **Figure 3-2** shows how to apply for a Direct Connect connection by self-service. For details on how to enable Direct Connect, see **Enabling Direct Connect**.

Figure 3-2 Creating a Direct Connect connection



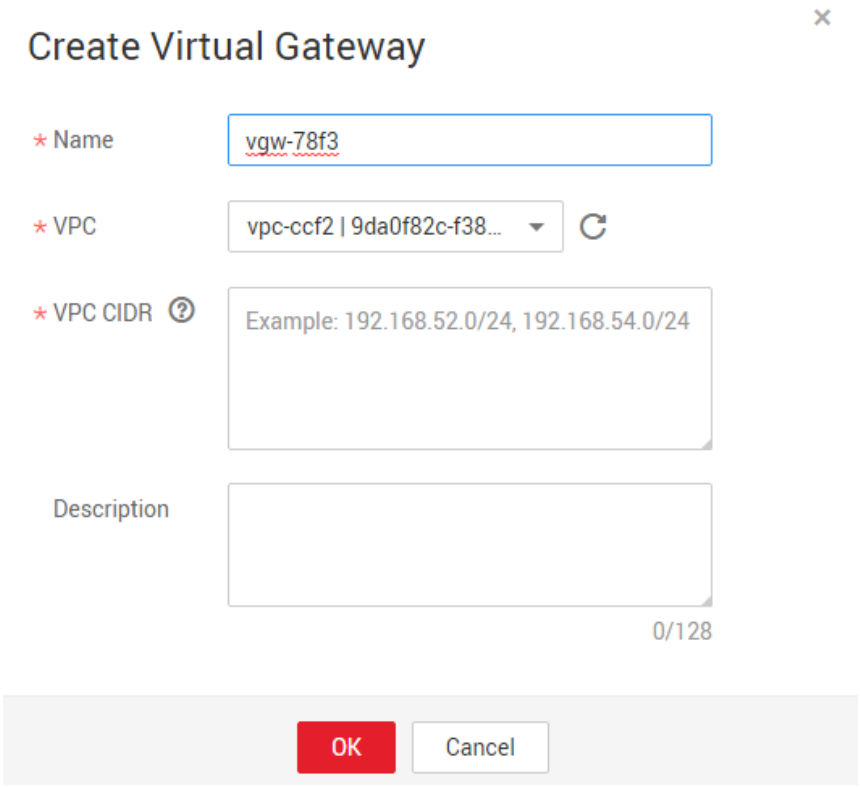
Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **Direct Connect**.
4. In the navigation pane on the left of Network Console, choose **Direct Connect** > **Connections**. You can purchase connections from partners or in self-service mode. For details, see **Enabling Direct Connect**.

 Copyright © Huawei Technologies Co., Ltd.

5. In the navigation pane on the left, choose **Direct Connect** > **Virtual Gateways**. Then, click **Create Virtual Gateway**. In the displayed dialog box, set the parameters as prompted. You are advised to set the VPC CIDR block to **0.0.0.0/0**. For details, see **Creating a Virtual Gateway**.

Figure 3-3 Create Virtual Gateway



6. In the navigation pane on the left, choose **Direct Connect** > **Virtual Interfaces**. Then, click **Create Virtual Interface**. On the displayed page, set the required parameters. For details, see **Creating a Virtual Interface**.

3.4 Step 2: Buy an EIP

Scenarios

You can assign an EIP, which can work together with a NAT gateway to allow servers that are connected to the cloud using Direct Connect or Cloud Connect to access the Internet or to provide services accessible from the Internet.

NOTE

For details about the EIP pricing, see **Billing**.

Procedure

For details, see **Assigning an EIP**. After you assign an EIP, you do not need to bind it to a server here.

 Copyright © Huawei Technologies Co., Ltd.

3.5 Step 3: Buy a Public NAT Gateway

Scenario

This section describes how to buy a public NAT gateway to enable your servers to access the Internet or to provide services for external networks.

Prerequisites

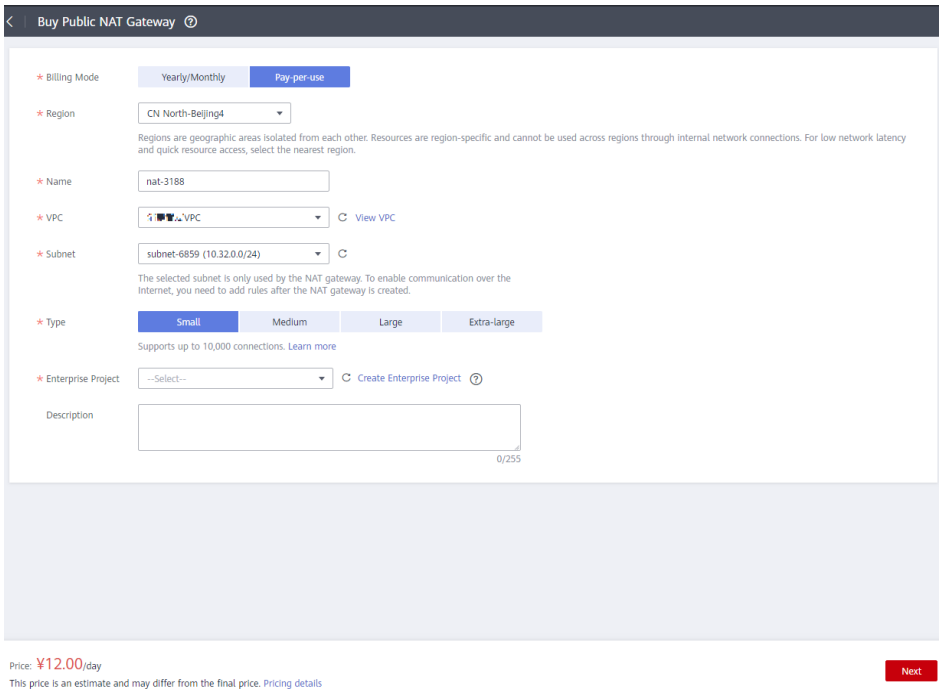
- When buying a public NAT gateway, you must specify its VPC, subnet, and type.
- Check whether the default route (0.0.0.0/0) of the VPC has been used by other gateways. If the default route of the VPC has been used by other gateways, add another route for this gateway or add the default route to a new route table to be associated with the gateway after the gateway is created.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   Switch to the public NAT gateway page.
4. On the displayed page, click **Buy Public NAT Gateway**.

   Figure 3-4 Buy Public NAT Gateway



5. Set the parameters as prompted. For details, see **Table 3-1**.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-1 Parameter descriptions

Parameter	Description
Region	The region where the public NAT gateway is located.
Billing Mode	Public NAT gateways are billed on a pay-per-use or yearly/monthly basis.
Name	The name of the public NAT gateway. The name can include up to 64 characters and can include digits, letters, underscores (_), and hyphens (-).
VPC	The VPC that the public NAT gateway belongs to. Check whether the default route (0.0.0.0/0) of the VPC has been used by other gateways. If the default route of the VPC has been used by other gateways, add another route for this gateway or add the default route to a new route table to be associated with the gateway after the gateway is created. The selected VPC cannot be changed after the public NAT gateway is purchased.
Subnet	The subnet of the VPC that the public NAT gateway belongs to. The subnet must have at least one available IP address. The selected subnet cannot be changed after the public NAT gateway is purchased.
Type	The type of the public NAT gateway. The type can be **Small**, **Medium**, **Large**, and **Extra-large**. You can click **Learn more** on the page to view details about each type.
Enterprise Project	The enterprise project that the public NAT gateway belongs to. If an enterprise project is configured for a public NAT gateway, the public NAT gateway belongs to this enterprise project. If you do not specify an enterprise project, the **default** enterprise project will be used.
Description	Supplementary information about the public NAT gateway. The description can contain up to 255 characters.
Required Duration	The required duration of the public NAT gateway.

After these parameters are set, the public NAT gateway price will be displayed. You can click **Pricing details** on the page to view pricing details.

 Copyright © Huawei Technologies Co., Ltd.

6. Click **Next**. The page for you to confirm the public NAT gateway specifications is displayed.
7. If you do not need to modify the information, click **Submit**.

   It takes 1 to 5 minutes to create a public NAT gateway.
8. In the public NAT gateway list, you can see the gateway status.

3.6 Step 4: Add an SNAT Rule

Scenarios

After a public NAT gateway is created, you can add SNAT rules for it. With SNAT rules, servers that are connected to a VPC using Direct Connect can access the Internet by sharing an EIP.

Each SNAT rule is configured for one CIDR block. If servers that are connected to a VPC using Direct Connect are in multiple CIDR blocks, you can create several SNAT rules to allow the servers to share EIPs.

Prerequisites

A public NAT gateway has been created.

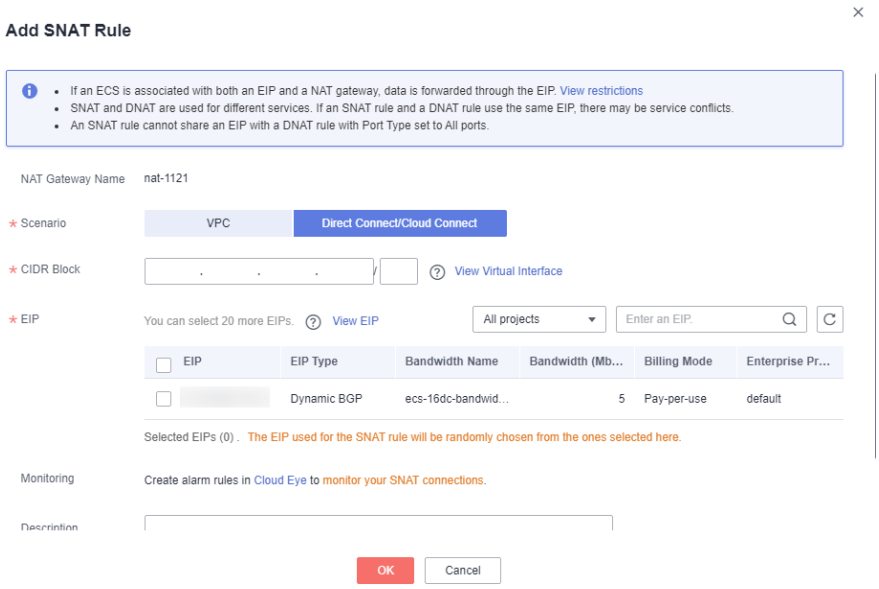
Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the public NAT gateway for which you want to add the SNAT rule.
5. On the **SNAT Rules** tab, click **Add SNAT Rule**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-5 Add SNAT Rule



6. Specify the parameters as prompted. For details, see **Table 3-2**.

Table 3-2 Parameter descriptions

Parameter	Description
Scenario	Select **Direct Connect/Cloud Connect** if servers in your data center need to access the Internet. The servers in your data center that are connected to a VPC through Direct Connect or Cloud Connect can access the Internet through the SNAT rule.
CIDR Block	Local servers whose IP address in this CIDR block can access the Internet through the SNAT rule.
EIP	The EIP used for accessing the Internet. You can select an EIP that either has not been bound, has been bound to a DNAT rule with **Port Type** set to **Specific port** of the current public NAT gateway, or has been bound to an SNAT rule of the current NAT gateway. You can select multiple EIPs at once. Up to 20 EIPs can be selected for each SNAT rule. The EIP used for the SNAT rule is randomly chosen from the ones you select when you add the rule.
Monitoring	Alarm rules are created in Cloud Eye. The alarm rules help you monitor your SNAT connections and keep you informed of any changes in a timely manner.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Description	Supplementary information about the SNAT rule. The description can contain up to 255 characters.

7. Click **OK**.
8. View details in the SNAT rule list. If **Status** is **Running**, the rule has been added.

   NOTE

   You can add multiple SNAT rules for a public NAT gateway to suite your service requirements.

3.7 Step 5: Add a DNAT Rule

Scenarios

After a public NAT gateway is created, you can add DNAT rules to allow servers in your data center to provide services accessible from the Internet.

You can configure a DNAT rule for each port of a server. If there are multiple servers, you can create several DNAT rules to allow servers to share EIPs.

Prerequisites

A NAT gateway has been created.

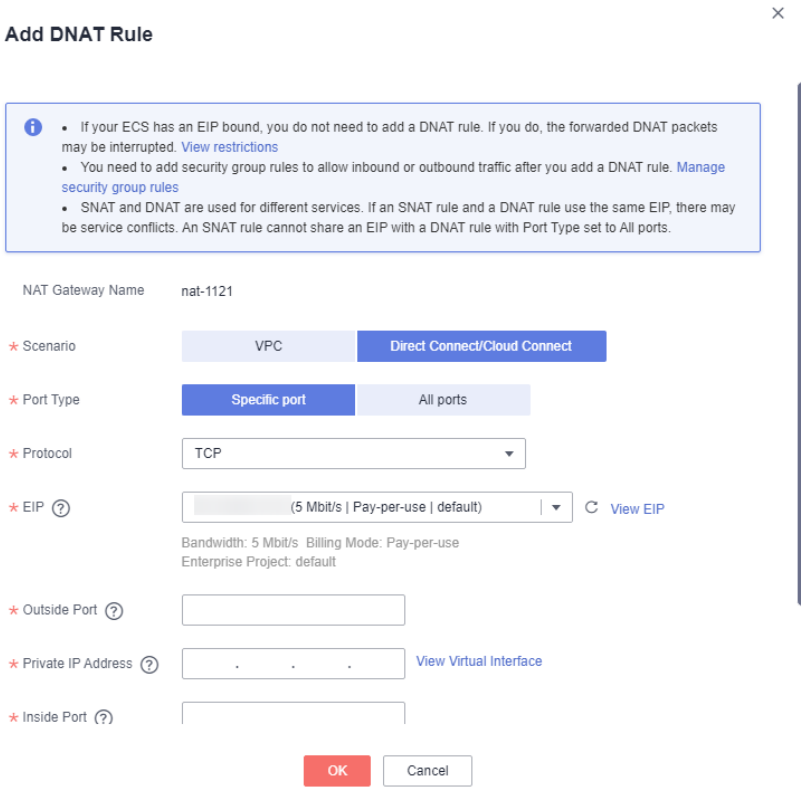
Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the public NAT gateway for which you want to add the DNAT rule.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.
6. Click **Add DNAT Rule**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-6 Add DNAT Rule



7. Set the parameters as prompted. For details, see **Table 3-3**.

Table 3-3 Parameter descriptions

Parameter	Description
Scenario	Select **Direct Connect/Cloud Connect** if servers in your data center need to access the Internet. Servers in your data center that connected to a VPC using Direct Connect or Cloud Connect can provide services accessible from the Internet through the DNAT rule.
Port Type	The port type. You can select **All ports** or **Specific port**. • **All ports**: This is equivalent to assigning an EIP to a server. Any requests on the EIP will be forwarded by the NAT gateway to your server based on IP address mapping. • **Specific port**: The public NAT gateway only forwards requests with a specific protocol and port on the EIP to the corresponding port of the target server.
Protocol	The protocol can be TCP or UDP. This parameter is available if you select **Specific port** for **Port Type**. If you select **All ports**, this parameter is **All** by default.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
EIP	The EIP that will be used by the server to provide services accessible from the Internet. You can select an EIP that either has not been bound, has been bound to a DNAT rule with **Port Type** set to **Specific port** of the current public NAT gateway, or has been bound to an SNAT rule of the current NAT gateway.
Outside Port	The port of the EIP. This parameter is available if you select **Specific port** for **Port Type**. The port number must range from 1 to 65535. You can enter a single port number or a port range, for example, 80 or 80-100.
Private IP Address	The IP address of the servers in the local data center or the user's private IP address. This IP address is used by local servers that are connected to a VPC through Direct Connect or Cloud Connect to provide services accessible from the Internet through DNAT. Configure the port of **Private IP Address** if you select **Specific port** for **Port Type**. This IP address is used by the server to provide services accessible from the Internet through DNAT.
Inside Port	The port of the server that provides services accessible from the Internet through the DNAT rule. This parameter is available if you select **Specific port** for **Port Type**. The port number must range from 1 to 65535. You can enter a single port number or a port range, for example, 80 or 80-100.
Description	Supplementary information about the DNAT rule. The description can contain up to 255 characters.

8. Click **OK**.
9. View details in the DNAT rule list. If **Status** is **Running**, the rule has been added.

 Copyright © Huawei Technologies Co., Ltd.

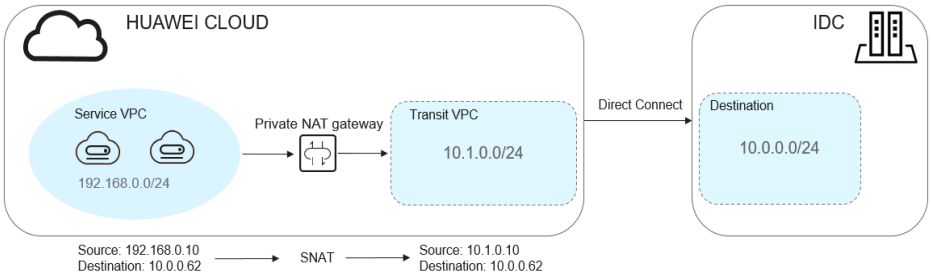
4 Using Private NAT Gateways to Enable Communication Between Cloud and On-premises Networks

4.1 Overview

This section describes how to use a private NAT gateway to enable communication between cloud and on-premises networks.

The following diagram shows how ECSs in a VPC communicate with an on-premises IDC using Direct Connect and a private NAT gateway.

Figure 4-1 Networking diagram



NOTE

The following configuration is used as an example.

In the example shown here, the CIDR block of the IDC is 10.0.0.0/24 and the subnet of the transit VPC in the region **CN North-Beijing4** is 10.1.0.0/24.

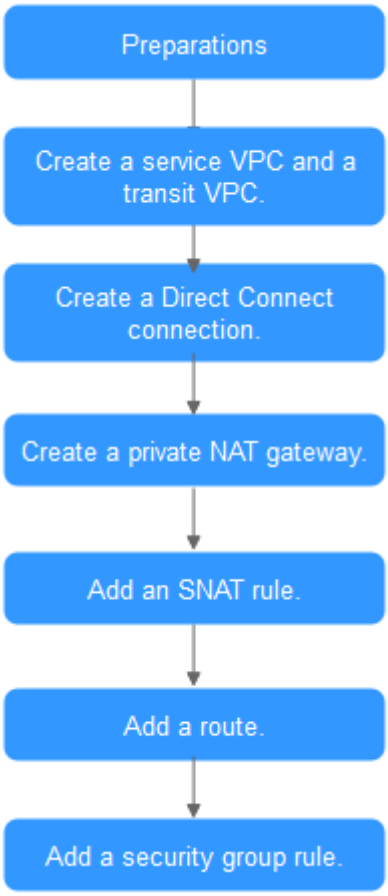
Implementation methods:

1. Connect the transit VPC to the IDC using Direct Connect (VPC Peering is used in a test environment where Direct Connect is unavailable).
2. Create a private NAT gateway to connect the service VPC to the transit VPC.

This following figure shows the procedure.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-2 Procedure



4.2 Preparations

Before using a NAT gateway, you need to complete the items described in this section.

Registering with HUAWEI CLOUD and Completing Real-name Authentication

If you already have an authenticated HUAWEI CLOUD account, skip this part. If you do not have a HUAWEI CLOUD account, perform the following steps to create one:

1. Visit **https://www.huaweicloud.com/** and click **Register**.
2. On the displayed page, register an account as prompted. For details, see **Registering with HUAWEI CLOUD.**

   After your registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in **Individual Real-Name Authentication**.

 Copyright © Huawei Technologies Co., Ltd.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For details about the price of NAT gateways, see **Product Pricing Details**.
- For details about how to top up an account, see **Topping Up an Account**.

4.3 Step 1: Create a Service VPC and a Transit VPC

Scenarios

A VPC provides an isolated virtual network for ECSs. You can configure and manage your network as required.

Procedure

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

4.4 Step 2: Create a Direct Connect Connection

Scenarios

Create a Direct Connect connection between the IDC and the cloud (**CN North-Beijing4** region).

Procedure

For details, see **Process Description**.

4.5 Step 3: Create a Private NAT Gateway

Scenarios

If you want to connect the service VPC to the transit VPC, you need to create a private NAT gateway.

Prerequisites

You have determined the private CIDR block in the transit VPC for performing NAT for resources in the service VPC.

Procedure

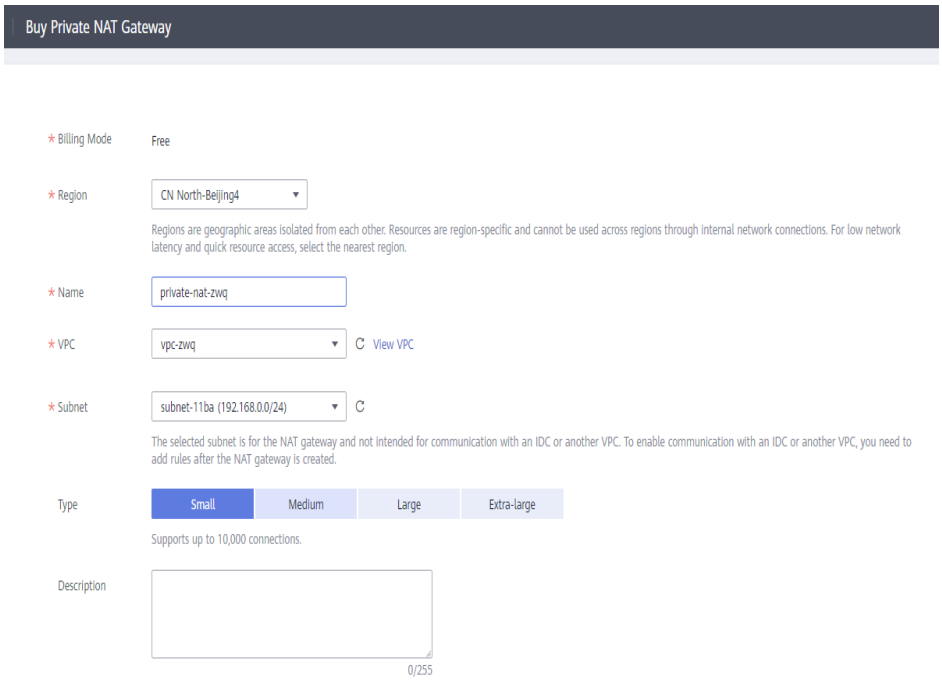
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **NAT Gateway**. In the navigation pane on the left, choose **Private NAT Gateway**.

   The private NAT gateway console is displayed.

 Copyright © Huawei Technologies Co., Ltd.

4. Click **Buy Private NAT Gateway**.

Figure 4-3 Buy Private NAT Gateway



5. Set the parameters as prompted. For details, see **Table 4-1**.

Table 4-1 Parameter descriptions

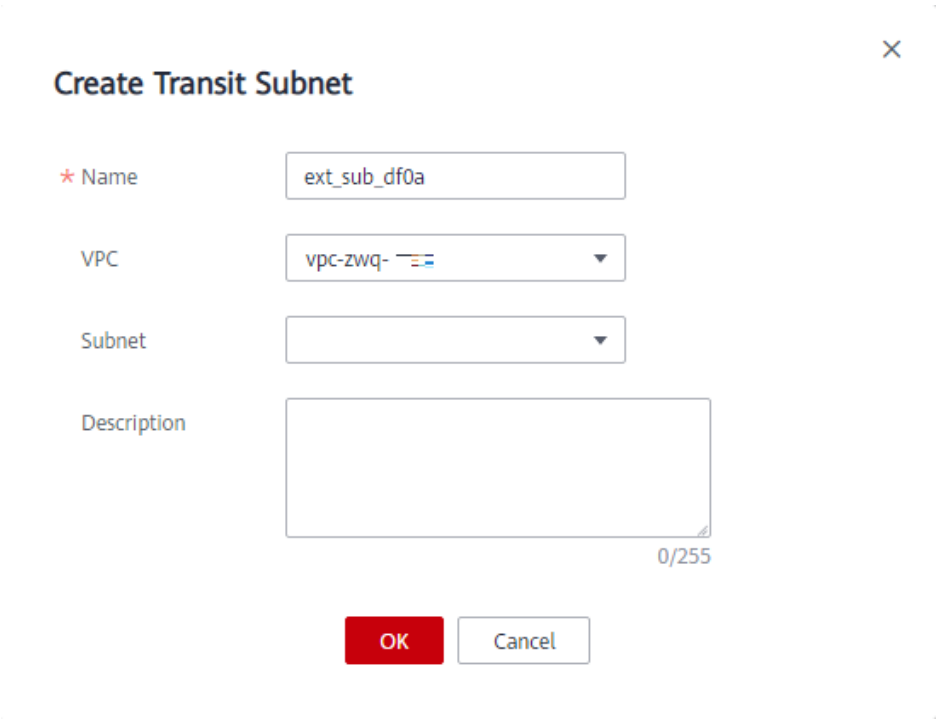
Parameter	Description
Region	The region where the private NAT gateway is located.
Billing Mode	Private NAT gateways are free during the OBT.
Name	The name of the private NAT gateway. The name can include up to 64 characters and can include digits, letters, underscores (_), and hyphens (-).
VPC	The VPC that the private NAT gateway belongs to. Select a VPC that is not used by any other NAT gateways and has no default route. The selected VPC cannot be changed after the private NAT gateway is created.
Subnet	The subnet of the VPC that the private NAT gateway belongs to. The subnet must have at least one available IP address. The selected subnet cannot be changed after the private NAT gateway is created.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Type	The type of the private NAT gateway. The type can be **Small**, **Medium**, **Large**, and **Extra-large**. You can click **Learn more** on the page to view details about each type.
Description	Supplementary information about the private NAT gateway. The description can contain up to 255 characters.

6. Click **Buy Now**.
7. In the private NAT gateway list, you can see the gateway status.
8. On the **Private NAT Gateway** page, click **Transit Subnets** and then **Create Transit Subnet**.

Figure 4-4 Create Transit Subnet



9. Set the parameters as prompted. For details, see **Table 4-2**.

Table 4-2 Parameter descriptions

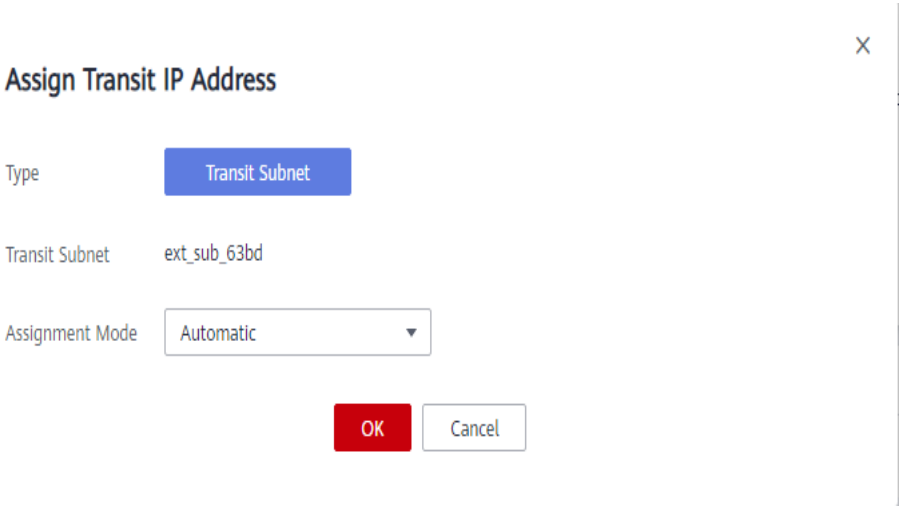
Parameter	Description
Name	The transit subnet name. The name can include up to 64 characters and can include digits, letters, underscores (_), and hyphens (-).
VPC	The transit VPC.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Subnet	A subnet in the transit VPC. The subnet must have at least one available IP address.
Description	Supplementary information about the transit subnet. The description can contain up to 255 characters.

10. In the transit subnet list, click the name of the created transit subnet.
    On the displayed page, click **Assign Transit IP Address**.

    Figure 4-5 Assign Transit IP Address



11. Set **Assignment Mode** to **Automatic** and click **OK**.

4.6 Step 4: Add an SNAT Rule

Scenarios

After the private NAT gateway is created, you need to add SNAT rules. An SNAT rule allows all or some servers in a VPC subnet to access your on-premises data center or remote VPC by sharing a transit IP address.

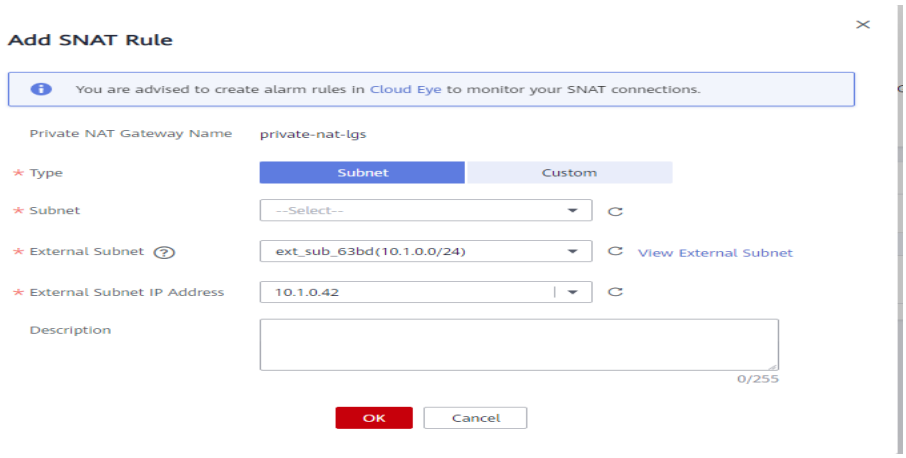
Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **NAT Gateway**. In the navigation pane on the left, choose **Private NAT Gateway**.
   The private NAT gateway console is displayed.
4. In the NAT gateway list, click the name of the private NAT gateway for which you want to add the SNAT rule.

 Copyright © Huawei Technologies Co., Ltd.

5. On the **SNAT Rules** tab, click **Add SNAT Rule**.

Figure 4-6 Add SNAT Rule



6. Specify the parameters as prompted. For details, see **Table 4-3**.

Table 4-3 Parameter descriptions

Parameter	Description
Type	Specifies whether servers in a VPC subnet or a subset of a current VPC subnet need to use the SNAT rule.
Subnet	A service VPC subnet where IP addresses need translation.
Transit Subnet	The transit subnet created in **Step 3: Create a Private NAT Gateway**.
Transit IP Address	The transit IP address assigned in **Step 3: Create a Private NAT Gateway**.
Description	Supplementary information about the SNAT rule. The description can contain up to 255 characters.

7. Click **OK**.
8. View details in the SNAT rule list. If **Status** is **Running**, the rule has been added.

4.7 Step 5: Add a Route

Scenarios

After the private NAT gateway is configured, you need to add a route pointing to the private NAT gateway in the service VPC.

Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. In the route table list, click the name of the route table associated with the service VPC.
6. Click **Add Route** and set parameters as prompted.

Figure 4-7 Add Route

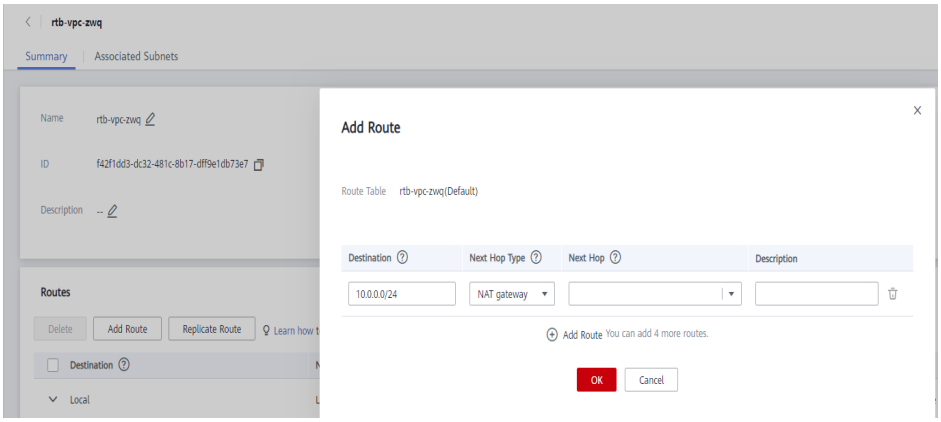


Table 4-4 Parameter descriptions

Parameter	Description
Destination	The destination CIDR block. Set the value to the private CIDR block of the IDC.
Next Hop Type	Set **Next Hop Type** to **NAT gateway**.
Next Hop	Set **Next Hop** to the created private NAT gateway.
Description	Supplementary information about the route. This parameter is optional. The description can contain up to 255 characters but cannot contain angle brackets (< or >).

7. Click **OK**.

4.8 Step 6: Add a Security Group Rule

Scenario

Add an inbound security group rule to allow traffic to be forwarded to the destination.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules.
6. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

   You can click **+** to add more inbound rules.

Figure 4-8 Add Inbound Rule

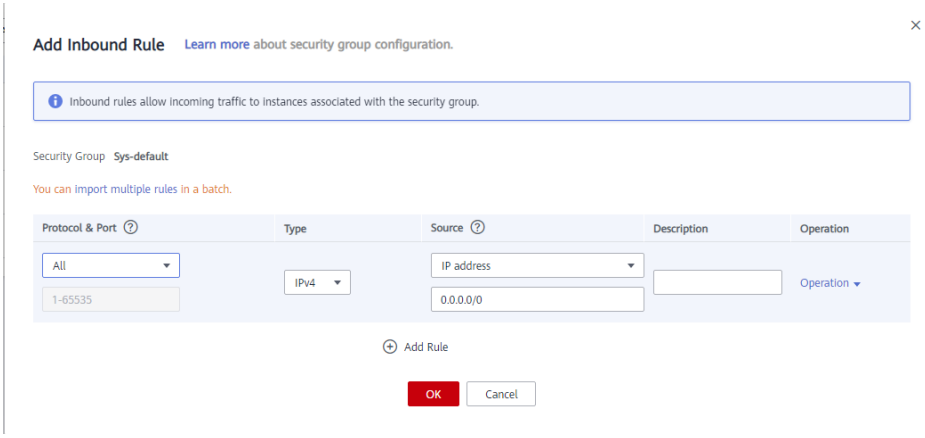


Table 4-5 Inbound rule parameter descriptions

Parameter	Description	Example Value
Protocol & Port	**Protocol**: Network protocol. The value can be **All**, **TCP**, **UDP**, **ICMP**, or **GRE**.	TCP
	Port: The port or port range over which the traffic can reach your ECS. The value ranges from 1 to 65535. For common ports, see **Common Ports Used by ECSs**.	22 or 22-30
Type	The IP address type. This parameter is available after the IPv6 function is enabled. • IPv4 • IPv6	IPv4

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Source	The source of the security group rule. The value can be a single IP address or a security group to allow access from the IP address or instances in the security group. For example: • xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (IP address range) • 0.0.0.0/0 (all IP addresses) • sg-abc (security group) For more information about IP address groups, see **IP Address Group Overview**.	0.0.0.0/0
Description	(Optional) Supplementary information about the security group rule. The description can contain up to 255 characters but cannot contain angle brackets (< or >).	-

7. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

5 Using Multiple Public NAT Gateways Together in Performance-Demanding Scenarios

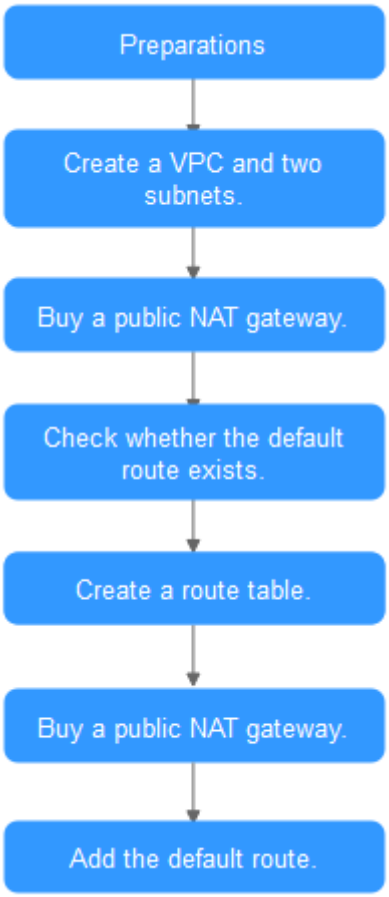
5.1 Overview

If a single NAT gateway becomes a performance bottleneck, for example, if there are over 1 million SNAT connections, or if the maximum bandwidth of 10 Gbit/s cannot meet service requirements, it is recommended that you use multiple NAT gateways together.

This section describes how to deploy multiple public NAT gateways together.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-1 Procedure



5.2 Preparations

Before using a NAT gateway, you need to complete the items described in this section.

Registering with HUAWEI CLOUD and Completing Real-name Authentication

If you already have an authenticated HUAWEI CLOUD account, skip this part. If you do not have a HUAWEI CLOUD account, perform the following steps to create one:

1. Visit **https://www.huaweicloud.com/** and click **Register**.
2. On the displayed page, register an account as prompted. For details, see **Registering with HUAWEI CLOUD.**

   After your registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in **Individual Real-Name Authentication**.

 Copyright © Huawei Technologies Co., Ltd.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For details about the price of NAT gateways, see **Product Pricing Details**.
- For details about how to top up an account, see **Topping Up an Account**.

5.3 Step 1: Create a VPC and Two Subnets

Scenarios

This example requires one VPC and two subnets.

Procedure

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

5.4 Step 2: Buy a Public NAT Gateway

Scenarios

Buy a public NAT gateway with VPC set to the one created in **Step 1: Create a VPC and Two Subnets**.

Prerequisites

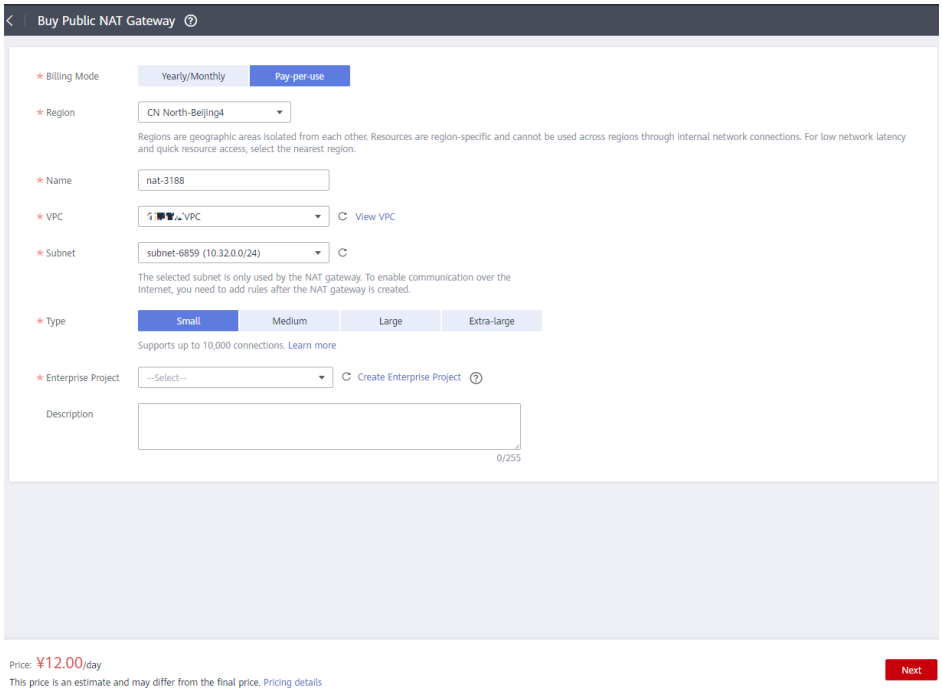
A VPC has been created.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.
4. On the displayed page, click **Buy Public NAT Gateway**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-2 Buy Public NAT Gateway



5. Set the parameters as prompted. For details, see **Table 5-1**.

   Select the VPC created in **Step 1: Create a VPC and Two Subnets** for **VPC** and a subnet created in **Step 1: Create a VPC and Two Subnets** for **Subnet**.

Table 5-1 Parameter descriptions

Parameter	Description
Region	The region where the public NAT gateway is located.
Billing Mode	Public NAT gateways are billed on a pay-per-use or yearly/monthly basis.
Name	The name of the public NAT gateway. The name can include up to 64 characters and can include digits, letters, underscores (_), and hyphens (-).
VPC	The VPC that the public NAT gateway belongs to. The selected VPC cannot be changed after the public NAT gateway is purchased.
Subnet	The subnet of the VPC that the public NAT gateway belongs to. The subnet must have at least one available IP address. The selected subnet cannot be changed after the public NAT gateway is purchased.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Type	The type of the public NAT gateway. The type can be **Small**, **Medium**, **Large**, and **Extra-large**. You can click **Learn more** on the page to view details about each type.
Enterprise Project	The enterprise project that the public NAT gateway belongs to. If an enterprise project is configured for a public NAT gateway, the public NAT gateway belongs to this enterprise project. If you do not specify an enterprise project, the **default** enterprise project will be used.
Description	Supplementary information about the public NAT gateway. The description can contain up to 255 characters.
Required Duration	The required duration of the public NAT gateway.

After these parameters are set, the public NAT gateway price will be displayed. You can click **Pricing details** on the page to view pricing details.

6. Click **Next**. The page for you to confirm the public NAT gateway specifications is displayed.
7. If you do not need to modify the information, click **Submit**.

   It takes 1 to 5 minutes to create a public NAT gateway.
8. In the public NAT gateway list, you can see the public NAT gateway status.

5.5 Step 3: Check Whether the Default Route Exists

Scenarios

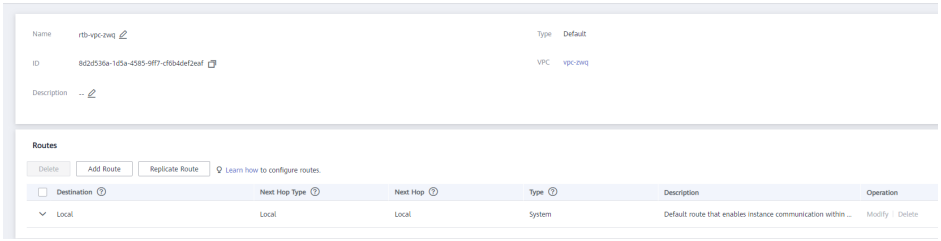
After the gateway is created, go to the route table list and check whether the default route with the next top set to the public NAT gateway exists in the default route table.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. In the route table list, click the name of the default route table.
6. Go to the route table details page and check whether the default route with the next top type of NAT gateway exists.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-3 Route table



NOTE

When the first public NAT gateway in a VPC is created, the default route (0.0.0.0/0) is automatically created in the default route table. If the default route already exists in the VPC, you need to add a route and set the next hop of the route to the created NAT gateway.

5.6 Step 4: Create a Route Table

Scenarios

Each NAT gateway requires its unique route table. You need to create the second route table for the VPC.

Prerequisites

A route table can be created in the VPC.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. In the upper right corner, click **Create Route Table**. On the displayed page, configure parameters as prompted.

Table 5-2 Parameter descriptions

Parameter	Description	Example Value
Name	The name of the route table. This parameter is mandatory. The name can include up to 64 characters and can include letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	rtb-001
VPC	The VPC that the route table belongs to. This parameter is mandatory.	vpc-001

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Description	Supplementary information about the route table. This parameter is optional. The description can contain up to 255 characters but cannot contain angle brackets (< or >).	-
Route Settings	Supplementary information about the route. This parameter is optional. You can add a route when creating the route table or after the route table is created. You can click **+** to add more routes.	-

6. Click **OK**.

   A message indicating that subnets can now be associated with the created route table is displayed. Perform the following steps to associate the second subnet with the route table:

   a. Click **Associate Subnet**. The **Associated Subnets** page is displayed.

   b. Click **Associate Subnet** and select the second subnet created in **Step 1: Create a VPC and Two Subnets**.

   c. Click **OK**.

5.7 Step 5: Buy a Public NAT Gateway

Scenarios

Buy a public NAT gateway with VPC set to the one created in **Step 1: Create a VPC and Two Subnets**.

Prerequisites

Another route table has been created in the VPC and associated with the second subnet.

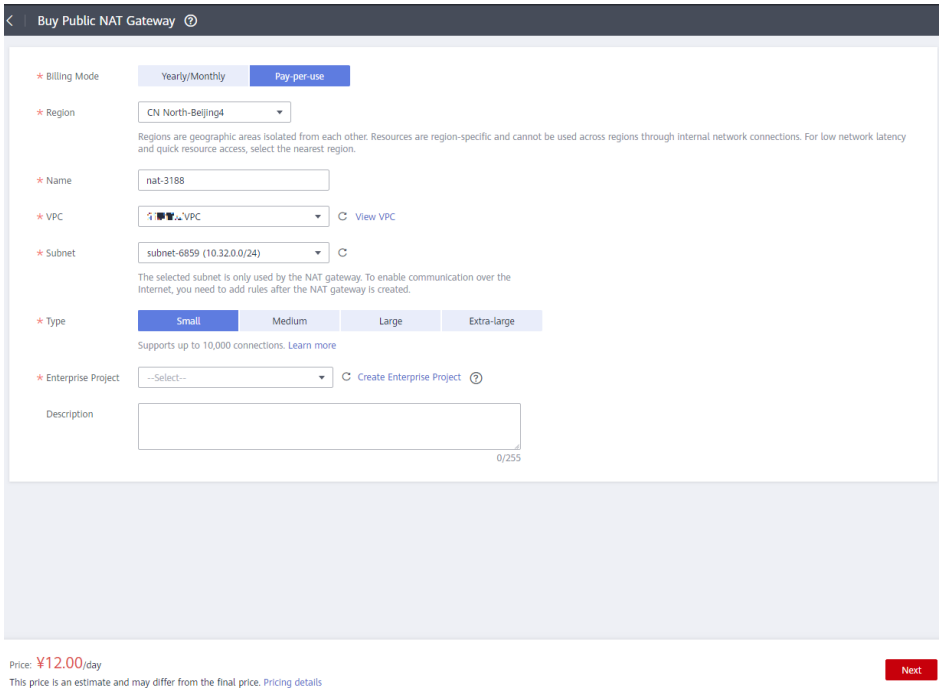
Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   Switch to the public NAT gateway page.
4. On the displayed page, click **Buy Public NAT Gateway**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-4 Buy Public NAT Gateway



5. Set the parameters as prompted. For details, see **Table 5-3**.

   Select the VPC created in **Step 1: Create a VPC and Two Subnets** for **VPC** and the other subnet created in **Step 1: Create a VPC and Two Subnets** for **Subnet**.

Table 5-3 Parameter descriptions

Parameter	Parameter descriptions
Region	The region where the public NAT gateway is located.
Billing Mode	Public NAT gateways are billed on a pay-per-use or yearly/monthly basis.
Name	The name of the public NAT gateway. The name can include up to 64 characters and can include digits, letters, underscores (_), and hyphens (-).
VPC	The VPC that the public NAT gateway belongs to. The selected VPC cannot be changed after the public NAT gateway is purchased.
Subnet	The subnet of the VPC that the public NAT gateway belongs to. The subnet must have at least one available IP address. The selected subnet cannot be changed after the public NAT gateway is purchased.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Parameter descriptions
Type	The type of the public NAT gateway. The type can be **Small**, **Medium**, **Large**, and **Extra-large**. You can click **Learn more** on the page to view details about each type.
Enterprise Project	The enterprise project that the public NAT gateway belongs to. If an enterprise project is configured for a public NAT gateway, the public NAT gateway belongs to this enterprise project. If you do not specify an enterprise project, the **default** enterprise project will be used.
Description	Supplementary information about the public NAT gateway. The description can contain up to 255 characters.
Required Duration	The required duration of the public NAT gateway.

After these parameters are set, the public NAT gateway price will be displayed. You can click **Pricing details** on the page to view pricing details.

6. Click **Next**. The page for you to confirm the public NAT gateway specifications is displayed.
7. If you do not need to modify the information, click **Submit**.

   It takes 1 to 5 minutes to create a public NAT gateway.
8. In the public NAT gateway list, you can see the public NAT gateway status.

5.8 Step 6: Add the Default Route

Scenarios

If the VPC already has one or more NAT gateways configured, a route table must be created for this gateway and you need to add the default route (0.0.0.0/0) with next hop set to the NAT gateway to the route table.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. In the route table list, click the name of the route table to which you want to add a route.
6. Click **Add Route** and set parameters as prompted.

   You can click **+** to add more routes.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-5 Add Route

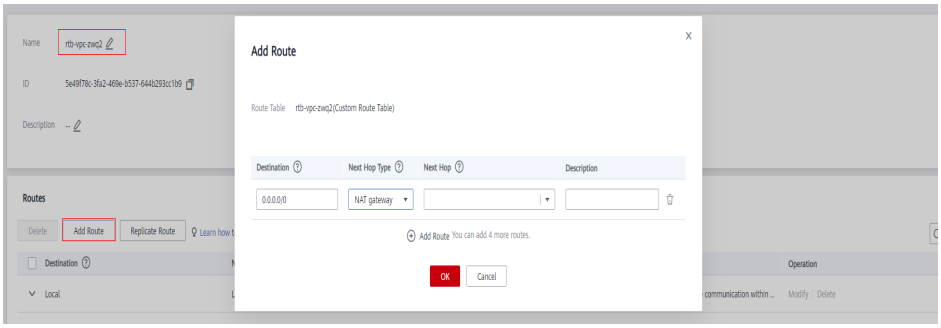


Table 5-4 Parameter descriptions

Parameter	Description	Example Value
Destination	The destination CIDR block. The destination of each route must be unique. The destination cannot overlap with any subnet CIDR block in the VPC.	0.0.0.0/0
Next Hop Type	Set the type of the next hop.	NAT gateway
Next Hop	Set the next hop. The resources in the drop-down list box are displayed based on the selected next hop type.	-
Description	Supplementary information about the route. This parameter is optional. The description can contain up to 255 characters but cannot contain angle brackets (< or >).	-

7. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.