ALIBABA CLOUD

Alibaba Cloud

Apsara Stack Enterprise

NAT Gateway

User Guide

Product Version: V3.16.2

Document Version: 20220707

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

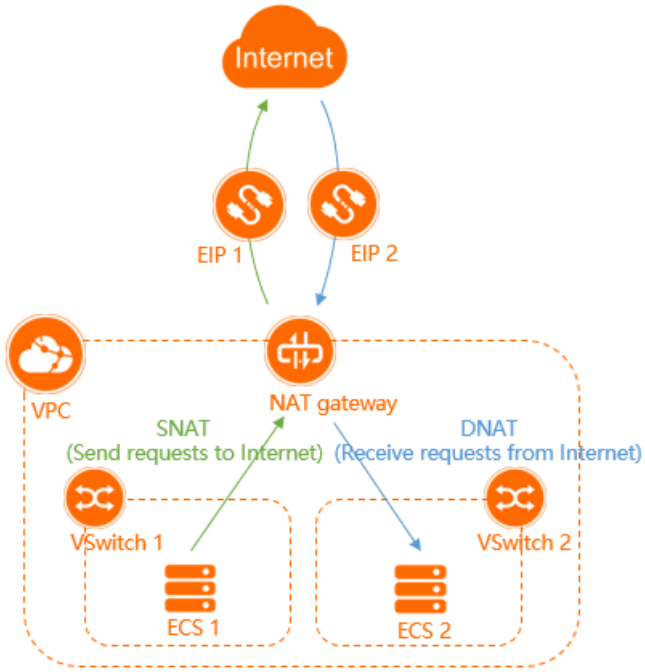
Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.What is NAT Gateway?

NAT gateways are enterprise-class gateways that provide the SNAT and DNAT features. Each NAT gateway provides a throughput capacity of up to 10 Gbit/s. NAT gateways also support cross-zone disaster recovery.



Overview

A NAT gateway works as expected only after an elastic IP address (EIP) is associated with the NAT gateway. After you create a NAT gateway, you can associate an EIP with the NAT gateway.

NAT gateways provide the SNAT and DNAT features. The following table describes the features.

Feature	Description
SNAT	SNAT allows Elastic Compute Service (ECS) instances that are deployed in a virtual private cloud (VPC) to access the Internet when no public IP addresses are assigned to the ECS instances.
DNAT	DNAT maps the EIPs that are associated with a NAT gateway to ECS instances. This way, the ECS instances can provide Internet-facing services.

2.Log on to the NAT Gateway console

This topic describes how to log on to the Apsara Uni-manager Management Console to manage your NAT gateways. The Google Chrome browser is used as an example.

Prerequisites

- The URL of the Apsara Uni-manager Management Console is obtained from the deployment personnel before you log on to the Apsara Uni-manager Management Console.
- A browser is available. We recommend that you use the Google Chrome browser.

Procedure

1. In the address bar, enter the URL of the Apsara Uni-manager Management Console. Press the Enter key.
2. Enter your username and password.

   Obtain the username and password that you can use to log on to the console from the operations administrator.

   > **Note** When you log on to the Apsara Uni-manager Management Console for the first time, you must change the password of your username. Your password must meet complexity requirements. The password must be 8 to 20 characters in length and must contain at least two of the following character types:
   >
   > - Uppercase or lowercase letters
   > - Digits
   > - Special characters, which include ! @ # $ %

3. Click **Login**.
4. If your account has multi-factor authentication (MFA) enabled, perform corresponding operations in the following scenarios:
   - It is the first time that you log on to the console after MFA is forcibly enabled by the administrator.
     a. On the Bind Virtual MFA Device page, bind an MFA device.
     b. Enter the account and password again as in Step 2 and click **Log On**.
     c. Enter a six-digit MFA verification code and click **Authenticate**.
   - You have enabled MFA and bound an MFA device.

     Enter a six-digit MFA authentication code and click **Authenticate**.

     > **Note** For more information, see the *Bind a virtual MFA device to enable MFA* topic in *Apsara Uni-manager Operations Console User Guide*.

5. In the top navigation bar, choose **Products > Networking > Virtual Private Cloud**.
6. In the left-side navigation pane, choose **Internet Access > NAT Gateway**.

3.Quick Start

3.1. Overview

This topic describes how to configure SNAT and DNAT. You can configure SNAT and DNAT to enable Elastic Compute Service (ECS) instances in a virtual private cloud (VPC) to communicate with the Internet through a NAT gateway.

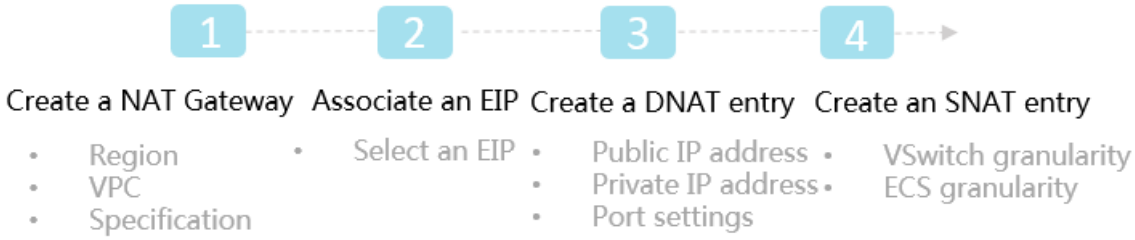
Prerequisites

Before you start, make sure that the following conditions are met:

- A VPC is created. For more information, see the **Create a VPC** topic in the **Quick Start** chapter of *VPC User Guide*.
- An ECS instance is created in the VPC. For more information, see the **Create an ECS instance** topic in the **Quick Start** chapter of *ECS User Guide*.
- An elastic IP address (EIP) is created. For more information, see the **Create an EIP** topic in the **Quick Start** chapter of *EIP User Guide*.

Procedure

The ECS instance used as an example in this topic is deployed in a VPC but is not assigned a public IP address. The following flowchart shows the configuration process.



1. Create a NAT gateway

   NAT gateways are enterprise-class gateways that provide network address translation services for accessing the Internet and VPCs. Before you configure SNAT and DNAT rules, you must create a NAT gateway.

   For more information, see Create a NAT gateway.

2. Associate an EIP with the NAT gateway

   A NAT gateway works as expected only after it is associated with an EIP. After a NAT gateway is created, you must associate an EIP with the NAT gateway.

   For more information, see Associate an EIP with a NAT gateway.

3. Create a DNAT entry

   NAT gateways support the DNAT feature. This feature allows you to map the public IP addresses of NAT gateways to ECS instances. This way, the ECS instances can provide Internet-facing services. DNAT supports port mapping and IP mapping.

   For more information, see Create a DNAT entry.

4. Create an SNAT entry

NAT gateways support the SNAT feature. This feature allows ECS instances that are not assigned public IP addresses in a VPC to access the Internet through a NAT gateway.

For more information, see Create an SNAT entry.

3.2. Create a NAT gateway

NAT gateways are enterprise-class gateways that provide network address translation services. Before you configure SNAT and DNAT rules, you must create a NAT gateway.

Prerequisites

A virtual private cloud (VPC) is created. For more information, see the **Create a VPC** topic in the **Quick Start** chapter of *VPC User Guide*.

Procedure

1. Log on to the NAT Gateway console.
2. On the **NAT Gateways** page, click **Create NAT Gateway**.
3. On the page that appears, set the following parameters and click **Submit**.

Parameter	Description
Region	
Organization	Select the organization to which the NAT gateway belongs.
Resource set	Select the resource set to which the NAT gateway belongs.
Region	Select the region where you want to create the NAT gateway.
Basic configuration	
VPC	Select the VPC to which the NAT gateway belongs. If you cannot find the VPC in the list, perform the following operations: ○ Check whether a NAT gateway is already deployed in the VPC. Only one NAT gateway can be deployed in each VPC. ○ Check whether the VPC contains a custom route entry whose destination CIDR block is 0.0.0.0/0. If the custom route exists, delete it.
Sharing scope	Select the sharing scope of the VPC. ○ **The resource set**: Only the administrator of the current resource set can use the VPC to create resources. ○ **Organization and lower-level organizations**: Only the administrators of the current organization and its subordinate organizations can use the VPC to create resources. ○ **Organization**: Only the administrator of the current organization can use the VPC to create resources.

Parameter	Description
Specifications	Select the size of the NAT gateway. Valid values: ○ **Small**: supports at most 10,000 SNAT connections. ○ **Medium**: supports at most 50,000 SNAT connections. ○ **Large**: supports at most 200,000 SNAT connections. ○ **Super Large**: supports at most 1,000,000 SNAT connections. **Note** The maximum number of SNAT connections is limited by the size of a NAT gateway. However, the gateway size does not affect the maximum number of DNAT connections.
Name	Enter a name for the NAT gateway. The name must be 2 to 128 characters in length, and can contain letters, digits, underscores (_), hyphens (-), and periods (.). The name must start with a letter and cannot start with `http://` or `https://`.

3.3. Associate an EIP with a NAT gateway

This topic describes how to associate an elastic IP address (EIP) with a NAT gateway. A NAT gateway can work as expected only after you associate an EIP with it. After you create a NAT gateway, you can associate an EIP with the NAT gateway.

Prerequisites

Before you associate an EIP with a NAT gateway, make sure that the following requirements are met:

- A NAT gateway is created. For more information, see Create a NAT gateway.
- An EIP is created. For more information, see the **Apply for EIPs** topic in the **Quick Start** chapter of *EIP User Guide*.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.
3. On the **NAT Gateways** page, find the NAT gateway with which you want to associate an EIP and choose **...** > **Bind elastic public network IP** in the **Operation** column.
4. In the **Bind elastic public network IP** dialog box, set the following parameters and click **OK**.

Parameter	Description
List of available EIPs	Select the EIP that you want to associate with the NAT gateway.

3.4. Create a DNAT entry

This topic describes how to create a DNAT entry. DNAT can map public IP addresses of NAT gateways to Elastic Compute Service (ECS) instances. This way, the ECS instances can provide Internet-facing services. DNAT supports port mapping and IP mapping.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.
3. On the **NAT Gateways** page, find the NAT gateway that you want to manage and click **Set DNAT** in the **Operation** column.
4. On the **DNAT management** tab, click **Create DNAT entry**.
5. In the **Create DNAT entry** dialog box, set the following parameters, and then click **OK**.

Parameter	Description
Public IP address	Select an elastic IP address (EIP). **Note** An EIP specified in an SNAT entry cannot be specified in a DNAT entry.
Private IP address	Select the ECS instance that uses the DNAT entry to provide Internet-facing services. You can specify the private IP address of the ECS instance in the following ways: ○ **Select from the corresponding IP of ECS or ENI**: Select the ECS instance from the drop-down list. ○ **Self-filling**: Enter the private IP address of the ECS instance. **Note** This private IP address must fall within the CIDR block of the virtual private cloud (VPC). You can also enter the private IP address of an existing ECS instance.
Port settings	Choose a DNAT mapping method: ○ **All ports**: specifies IP mapping. All requests destined for the EIP are forwarded to the ECS instance. ○ **Specific Port**: specifies port mapping. The NAT gateway forwards requests to the specified ECS instance based on the specified protocol and ports. After you select Specific Port, set the following parameters: **Public network port**, **Private network port**, and **Protocol type**.

3.5. Create an SNAT entry

This topic describes how to create an SNAT entry. SNAT can provide proxy services for Elastic Compute Service (ECS) instances. ECS instances that do not have public IP address assigned in virtual private clouds (VPCs) can access the Internet by using SNAT.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.
3. On the **NAT Gateways** page, find the NAT gateway that you want to manage and click **Set SNAT** in the **Operation** column.
4. On the **SNAT management** tab, click **Create SNAT Entry**.
5. In the **Create SNAT entry** dialog box, set the following parameters, and click **OK**.

Parameter	Description
Granularity setting	Specify whether to create an SNAT entry for a VPC, a vSwitch, an ECS instance, or a custom CIDR block. ○ **Switch granularity**: The ECS instances that belong to the vSwitch use the specified EIP to access the Internet. ■ **Switch**: Select a vSwitch in the VPC. All ECS instances in the vSwitch can access the Internet by using SNAT. ■ **Switch CIDR Block**: The CIDR block of the vSwitch is displayed. ○ **ECS granularity**: The specified ECS instances use the specified EIP to access the Internet. ■ **List of available ECS**: Select an ECS instance in the VPC. The selected ECS instance uses the EIP in the SNAT entry to access the Internet. Make sure that the following requirements are met: ■ The ECS instance is in the Running state. ■ No EIP is associated with the ECS instance and the ECS instance is not assigned a static public IP address. ■ **ECS network segment**: The CIDR block of the ECS instance is displayed.
Public IP address	Select one or more EIPs that are used to access the Internet. You can select one or more EIPs to create an SNAT IP address pool. **Note** An EIP that is already used in a DNAT entry cannot be used in an SNAT entry.
Entry name	Enter a name for the SNAT entry. The name must be 2 to 128 characters in length, and can contain digits, underscores (_), and hyphens (-). The name must start with a letter.

4.Manage a NAT gateway

4.1. Overview

NAT gateways are enterprise-class gateways that support SNAT and DNAT features. Each NAT gateway provides a forwarding capacity of 10 Gbit/s. NAT gateways support cross-zone disaster recovery.

Sizes of NAT gateways

NAT gateways are available in multiple sizes, including small, middle, large, and super large-1. The size of a NAT gateway determines the SNAT performance, which includes the maximum number of connections and the number of new connections per second. However, the size of a NAT gateway does not affect the DNAT performance. The following table describes available sizes of NAT gateways.

Size	Maximum number of SNAT connections	Number of new SNAT connections per second
Small	10,000	1,000
Medium	50,000	5,000
Large	200,000	10,000
Super Large-1	1,000,000	50,000

When you specify the size of a NAT gateway, take note of the following limits:

- CloudMonitor monitors only the maximum number of SNAT connections for NAT gateways. CloudMonitor does not monitor the number of new SNAT connections per second.
- The timeout period of SNAT connections on NAT gateways is 900 seconds.
- To avoid timeouts of SNAT connections caused by network congestion or Internet jitter, make sure that your applications support automatic reconnection.
- NAT gateways do not support packet fragmentation.
- If you use the same destination public IP address and port, the maximum number of concurrent connections is based on the number of elastic IP addresses (EIPs) that are associated with the NAT gateway. Each EIP that is associated with the NAT gateway supports up to 55,000 concurrent connections. If N EIPs are associated with the NAT gateway, the maximum number of concurrent connections that the NAT gateway supports is N × 55,000.

4.2. Create a NAT gateway

NAT gateways are enterprise-class gateways that provide network address translation services. Before you configure SNAT and DNAT rules, you must create a NAT gateway.

Prerequisites

A virtual private cloud (VPC) is created. For more information, see the **Create a VPC** topic in the **Quick Start** chapter of *VPC User Guide*.

Procedure

1. Log on to the NAT Gateway console.
2. On the **NAT Gateways** page, click **Create NAT Gateway**.
3. On the page that appears, set the following parameters and click **Submit**.

Parameter	Description
Region	
Organization	Select the organization to which the NAT gateway belongs.
Resource set	Select the resource set to which the NAT gateway belongs.
Region	Select the region where you want to create the NAT gateway.
Basic configuration	
VPC	Select the VPC to which the NAT gateway belongs. If you cannot find the VPC in the list, perform the following operations: ○ Check whether a NAT gateway is already deployed in the VPC. Only one NAT gateway can be deployed in each VPC. ○ Check whether the VPC contains a custom route entry whose destination CIDR block is 0.0.0.0/0. If the custom route exists, delete it.
Sharing scope	Select the sharing scope of the VPC. ○ **The resource set**: Only the administrator of the current resource set can use the VPC to create resources. ○ **Organization and lower-level organizations**: Only the administrators of the current organization and its subordinate organizations can use the VPC to create resources. ○ **Organization**: Only the administrator of the current organization can use the VPC to create resources.
Specifications	Select the size of the NAT gateway. Valid values: ○ **Small**: supports at most 10,000 SNAT connections. ○ **Medium**: supports at most 50,000 SNAT connections. ○ **Large**: supports at most 200,000 SNAT connections. ○ **Super Large**: supports at most 1,000,000 SNAT connections. **Note** The maximum number of SNAT connections is limited by the size of a NAT gateway. However, the gateway size does not affect the maximum number of DNAT connections.

Parameter	Description
Name	Enter a name for the NAT gateway. The name must be 2 to 128 characters in length, and can contain letters, digits, underscores (_), hyphens (-), and periods (.). The name must start with a letter and cannot start with `http://` or `https://`.

4.3. Modify a NAT gateway

You can modify the name and description of a NAT gateway.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.
3. On the **NAT Gateways** page, find the NAT gateway that you want to modify and click **Management** in the **Operation** column.
4. On the **Basic information** page, click next to **NAT Gateway name**. In the dialog box that appears, enter a name for the NAT gateway and click **OK**.

   The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (-). The name must start with a letter.
5. Click next to **Description**. In the dialog box that appears, enter a description for the NAT gateway and click **OK**.

   The description must be 2 to 256 characters in length. The description cannot start with `http://` or `https://`.

4.4. Delete a NAT gateway

You can delete a NAT gateway that you no longer need.

Prerequisites

Before you delete a NAT gateway, make sure that the following requirements are met:

- No elastic IP address (EIP) is associated with the NAT gateway. If an EIP is associated with the NAT gateway, disassociate the EIP from the NAT gateway. For more information, see Disassociate an EIP from a NAT gateway.
- The DNAT table does not contain DNAT entries. If the DNAT table contains DNAT entries, delete the DNAT entries. For more information, see Delete a DNAT entry.
- The SNAT table does not contain SNAT entries. If the SNAT table contains SNAT entries, delete the SNAT entries. For more information, see Delete an SNAT entry.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.

3. On the **NAT Gateways** page, find the NAT gateway that you want to delete and choose ... > **Delete** in the **Operation** column.
4. In the message that appears, click **OK**.

> **Note** If you select **Force deletion**, the DNAT and SNAT entries of the NAT gateway are automatically deleted. The EIPs associated with the NAT gateway are also disassociated. If you select Force deletion, you do not need to delete the DNAT entries and SNAT entries, or disassociate the EIPs before you delete the NAT gateway.

5.Manage EIPs

5.1. Associate an EIP with a NAT gateway

This topic describes how to associate an elastic IP address (EIP) with a NAT gateway. A NAT gateway can work as expected only after you associate an EIP with it. After you create a NAT gateway, you can associate an EIP with the NAT gateway.

Prerequisites

Before you associate an EIP with a NAT gateway, make sure that the following requirements are met:

- A NAT gateway is created. For more information, see Create a NAT gateway.
- An EIP is created. For more information, see the **Apply for EIPs** topic in the **Quick Start** chapter of *EIP User Guide*.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.
3. On the **NAT Gateways** page, find the NAT gateway with which you want to associate an EIP and choose **...** > **Bind elastic public network IP** in the **Operation** column.
4. In the **Bind elastic public network IP** dialog box, set the following parameters and click **OK**.

Parameter	Description
List of available EIPs	Select the EIP that you want to associate with the NAT gateway.

5.2. Disassociate an EIP from a NAT gateway

This topic describes how to disassociate an elastic IP address (EIP) from a NAT gateway. After an EIP is disassociated from a NAT gateway, the NAT gateway can no longer communicate with the Internet by using the EIP.

Prerequisites

Make sure that the EIP to be disassociated is not used in an SNAT entry or a DNAT entry. If the EIP is used in an SNAT or a DNAT entry, delete the SNAT or DNAT entry first. For more information, see Delete an SNAT entry and Delete a DNAT entry.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.

3. On the **NAT Gateways** page, find the NAT gateway that you want to manage and choose ... > **Unbind flexible public network IP** in the **Operation** column.
4. In the **Unbind flexible public network IP** dialog box, select the EIP that you want to disassociate, and click **OK**.

6.Manage a DNAT table

6.1. DNAT overview

NAT Gateway supports the DNAT feature. You can create DNAT entries to map public IP addresses to Elastic Compute Service (ECS) instances in a virtual private cloud (VPC). This way, the ECS instances can provide Internet-facing services.

DNAT entries

You can configure port mapping when you create a DNAT entry. After the DNAT entry is created, requests destined for the specified public IP address are forwarded to the ECS instances within a VPC based on the port mapping rule.

Each DNAT entry consists of the following items:

- **Public IP address**: the elastic IP address (EIP) associated with the NAT gateway.
- **Private IP address**: the private IP address assigned to the ECS instance in the VPC.
- **Public Port**: the external port on which requests from the Internet are received.
- **Private Port**: the internal port to which the requests received on the external port are forwarded.
- **IP Protocol**: the protocol used by the ports.

Port mapping and IP mapping

The DNAT feature supports port mapping and IP mapping:

- Port mapping

  After you configure port mapping for a NAT gateway, the NAT gateway forwards the requests that are destined for the specified public IP address to the specified ECS instance. The requests are forwarded based on the specified source and destination port and the specified protocol. The DNAT entries in the following table are used as an example:

  - Entry 1: The NAT gateway forwards requests that are destined for 1.1.XX.XX and TCP port 80 to 192.168.1.1 and TCP port 80.
  - Entry 2:The NAT gateway forwards requests that are destined for 2.2.XX.XX and UDP port 8080 to 192.168.1.2 and TCP port 8000.

DNAT entry	Public IP address	Public port	Private IP address	Private port	Protocol
Entry 1	1.1.XX.XX	80	192.168.1.1	80	TCP
Entry 2	2.2.XX.XX	8080	192.168.1.2	8000	UDP

- IP mapping

  After you configure IP mapping for a NAT gateway, the NAT gateway forwards all the requests that are destined for the specified public IP address to the specified ECS instance. The DNAT entry in the following table is used as an example.The NAT gateway forwards all the requests that are destined for 3.3.XX.XX to the ECS instance whose IP address is 192.168.1.3.

DNAT entry	Public IP address	Public port	Private IP address	Private port	Protocol
Entry 3	3.3.XX.XX	All	192.168.1.3	All	All

6.2. Create a DNAT entry

This topic describes how to create a DNAT entry. DNAT can map public IP addresses of NAT gateways to Elastic Compute Service (ECS) instances. This way, the ECS instances can provide Internet-facing services. DNAT supports port mapping and IP mapping.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.
3. On the **NAT Gateways** page, find the NAT gateway that you want to manage and click **Set DNAT** in the **Operation** column.
4. On the **DNAT management** tab, click **Create DNAT entry**.
5. In the **Create DNAT entry** dialog box, set the following parameters, and then click **OK**.

Parameter	Description
Public IP address	Select an elastic IP address (EIP). **Note** An EIP specified in an SNAT entry cannot be specified in a DNAT entry.
Private IP address	Select the ECS instance that uses the DNAT entry to provide Internet-facing services. You can specify the private IP address of the ECS instance in the following ways: ○ **Select from the corresponding IP of ECS or ENI**: Select the ECS instance from the drop-down list. ○ **Self-filling**: Enter the private IP address of the ECS instance. **Note** This private IP address must fall within the CIDR block of the virtual private cloud (VPC). You can also enter the private IP address of an existing ECS instance.
Port settings	Choose a DNAT mapping method: ○ **All ports**: specifies IP mapping. All requests destined for the EIP are forwarded to the ECS instance. ○ **Specific Port**: specifies port mapping. The NAT gateway forwards requests to the specified ECS instance based on the specified protocol and ports. After you select Specific Port, set the following parameters: **Public network port**, **Private network port**, and **Protocol type**.

6.3. Modify a DNAT entry

This topic describes how to modify a DNAT entry. You can modify the public IP address, private IP address, and port in a DNAT entry.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.
3. On the **NAT Gateways** page, find the NAT gateway that you want to manage and click **Set DNAT** in the **Operation** column.
4. On the **DNAT management** tab, find the DNAT entry that you want to modify and click **Edit** in the **Operation** column.
5. In the **Edit DNAT entry** dialog box, modify the public IP address, private IP address, or port in the DNAT entry, and then click **OK**.

6.4. Delete a DNAT entry

If you no longer need an ECS instance to provide Internet-facing services, you can delete the DNAT entry created for the ECS instance.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.
3. On the **NAT Gateways** page, find the NAT gateway that you want to manage and click **Set DNAT** in the **Operation** column.
4. On the **DNAT management** tab, find the DNAT entry that you want to delete and click **Delete** in the **Operation** column.
5. In the message that appears, click **OK**.

7.Manage an SNAT table

7.1. SNAT table overview

This topic describes how to configure SNAT. SNAT allows Elastic Compute Service (ECS) instances that are not assigned public IP addresses in a virtual private cloud (VPC) to access the Internet through a NAT gateway.

SNAT entries

You can add SNAT entries to an SNAT table to allow ECS instances to access the Internet.

Each SNAT entry consists of the following items:

- **vSwitches or ECS instances**: the vSwitch or ECS instances that require Internet access by using SNAT.
- **Public IP address**: the public IP address used to access the Internet.

vSwitch granularity and ECS granularity

SNAT entries can be created based on the following granularity to enable ECS instances in a VPC to access the Internet.

- vSwitch granularity

  If you create an SNAT entry for a vSwitch, the ECS instances attached to the vSwitch access the Internet by using the public IP address specified in the SNAT entry and through the NAT gateway on which the SNAT entry is created. By default, all ECS instances attached to the vSwitch can use the specified public IP address to access the Internet.

  > **Note** If an ECS instance has a public IP address, for example, the ECS instance is assigned a static public IP address, associated with an elastic IP address (EIP), or has DNAT IP mapping configured, the ECS instance uses the public IP address to access the Internet instead of the SNAT feature.

- ECS granularity

  If you create an SNAT entry for an ECS instance, the ECS instance can access the Internet by using the specified public IP address. The ECS instance accesses the Internet by using the public IP address specified in the SNAT entry and through the NAT gateway on which the SNAT entry is created.

7.2. Create an SNAT entry

This topic describes how to create an SNAT entry. SNAT can provide proxy services for Elastic Compute Service (ECS) instances. ECS instances that do not have public IP address assigned in virtual private clouds (VPCs) can access the Internet by using SNAT.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.
3. On the **NAT Gateways** page, find the NAT gateway that you want to manage and click **Set SNAT** in the **Operation** column.

4. On the **SNAT management** tab, click **Create SNAT Entry**.
5. In the **Create SNAT entry** dialog box, set the following parameters, and click **OK**.

Parameter	Description
Granularity setting	Specify whether to create an SNAT entry for a VPC, a vSwitch, an ECS instance, or a custom CIDR block. ○ **Switch granularity**: The ECS instances that belong to the vSwitch use the specified EIP to access the Internet. ■ **Switch**: Select a vSwitch in the VPC. All ECS instances in the vSwitch can access the Internet by using SNAT. ■ **Switch CIDR Block**: The CIDR block of the vSwitch is displayed. ○ **ECS granularity**: The specified ECS instances use the specified EIP to access the Internet. ■ **List of available ECS**: Select an ECS instance in the VPC. The selected ECS instance uses the EIP in the SNAT entry to access the Internet. Make sure that the following requirements are met: ■ The ECS instance is in the Running state. ■ No EIP is associated with the ECS instance and the ECS instance is not assigned a static public IP address. ■ **ECS network segment**: The CIDR block of the ECS instance is displayed.
Public IP address	Select one or more EIPs that are used to access the Internet. You can select one or more EIPs to create an SNAT IP address pool. **Note** An EIP that is already used in a DNAT entry cannot be used in an SNAT entry.
Entry name	Enter a name for the SNAT entry. The name must be 2 to 128 characters in length, and can contain digits, underscores (_), and hyphens (-). The name must start with a letter.

7.3. Modify an SNAT entry

This topic describes how to modify the name of an SNAT entry and the elastic IP address (EIP) specified in the SNAT entry.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.
3. On the **NAT Gateways** page, find the NAT gateway that you want to manage and click **Set SNAT** in the **Operation** column.

4. On the **SNAT management** page, find the SNAT entry that you want to modify and click **Edit** in the **Operation** column.
5. In the **Edit SNAT entry** dialog box, modify the EIP and name of the SNAT entry, and click **OK**.

7.4. Delete an SNAT entry

You can delete an SNAT entry if the Elastic Compute Service (ECS) instances that do not have public IP addresses in a virtual private cloud (VPC) no longer need SNAT to access the Internet.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.
3. On the **NAT Gateways** page, find the NAT gateway that you want to manage and click **Set SNAT** in the **Operation** column.
4. On the **SNAT management** tab, find the SNAT entry that you want to delete and click **Delete** in the **Operation** column.
5. In the message that appears, click **OK**.

8.NAT service plan

8.1. Create a NAT service plan

You can associate an elastic IP address (EIP) or a NAT service plan to a NAT gateway. However, you can choose only one of them for the NAT gateway. If you want to associate a NAT service plan with the NAT gateway, you must create a NAT service plan first. Then, you can configure SNAT or DNAT for the NAT gateway. A NAT service plan consists of public IP addresses and Internet bandwidth.

Procedure

1. Log on to the NAT Gateway console.
2. On the **NAT Gateways** page, find the target NAT gateway and choose **Purchase NAT Bandwidth Package** in the **Internet Shared Bandwidth** column.
3. On the **Bandwidth Package Details** page, click **Purchase**.
4. On the **NAT Bandwidth Package** page, set the following parameters, and click **Submit**.

Parameter	Description
Region	Indicates the region for which the NAT service plan is purchased.
Billing methods	Select the billing method of the NAT service plan. Only **By Bandwidth** is supported.
Bandwidth (Mbit/s)	Enter a bandwidth value for the NAT service plan that you want to purchase. The maximum value is 5000 Mbit/s.
Name	Enter a name for the NAT service plan. The name must be 2 to 128 characters in length and can contain letters, digits, underscores (_), and hyphens (-). It must start with a letter or Chinese character.
Description	Enter a description for the NAT service plan. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.
Quantity	Enter the number of NAT bandwidth plans that you want to purchase.

8.2. Modify the bandwidth of a NAT service plan

This topic describes how to modify the bandwidth of a NAT bandwidth plan. The modification takes effect immediately.

Procedure

1. Log on to the NAT Gateway console.
2. On the **NAT Gateways** page, find the target NAT gateway and click the ID of the NAT service plan in the **Internet Shared Bandwidth** column.
3. On the **Bandwidth Package Details** page, click the target NAT service plan, and then choose **Modify Bandwidth**.
4. On the **Modify Bandwidth** page, modify the bandwidth, and then click **Submit**.

   Each NAT bandwidth plan supports a maximum of 5,000 Mbit/s in bandwidth.

8.3. Add an IP address

This topic describes how to add IP addresses to a NAT service plan. The added IP addresses can be used to create Source Network Address Translation (SNAT) and Destination Network Address Translation (DNAT) rules.

Procedure

1. Log on to the NAT Gateway console.
2. On the **NAT Gateways** page, find the target NAT gateway and click the ID of the NAT service plan in the **Internet Shared Bandwidth** column.
3. On the **Bandwidth Package Details** page, click the target NAT service plan, and then choose **Add IP Address**.
4. On the **Modify IP Addresses** page, enter the number of IP addresses to be added, and then click **Submit**.

8.4. Release an IP address

This topic describes how to release IP addresses in a NAT service plan. The NAT service plan must contain at least one IP address.

Prerequisites

Before you release an IP address in the NAT service plan, make sure that the IP address is not used in Source Network Address Translation (SNAT) and Destination Network Address Translation (DNAT) entries. If the IP address is used in an SNAT or DNAT entry, delete the SNAT or DNAT entry first. For more information, see Delete a DNAT entry and Delete an SNAT entry.

Procedure

1. Log on to the NAT Gateway console.
2. On the **NAT Gateways** page, find the target NAT gateway and click the ID of the NAT service plan in the **Internet Shared Bandwidth** column.
3. On the **Bandwidth Package Details** page, click the target NAT service plan.
4. In the **Public IP List** section, find the target IP address, and click **Release** in the **Actions** column.
5. In the **Release IP** dialog box, click **OK**.

8.5. Delete a NAT service plan

This topic describes how to delete a service plan.

Prerequisites

Before you start, make sure that the following requirements are met:

- Delete the IP addresses that are used in Destination Network Address Translation (DNAT) entries. For more information, see Delete a DNAT entry.
- Delete the IP addresses that are used for Source Network Address Translation (SNAT) entries. For more information, see Delete an SNAT entry.

Procedure

1. Log on to the NAT Gateway console.
2. On the **NAT Gateways** page, find the target NAT gateway and click the ID of the NAT service plan in the **Internet Shared Bandwidth** column.
3. On the **Bandwidth Package Details** page, find the target NAT service plan and click **Delete**.
4. In the **Delete Shared Internet Shared Bandwidth** dialog box, click **OK**.

9.Anti-DDoS Origin Basic

A distributed denial-of-service (DDoS) attack is a malicious network attack against one or more systems, which can crash the targeted network. Alibaba Cloud provides up to 5 Gbit/s of basic anti-DDoS protection for a NAT gateway free of charge. Anti-DDoS Origin Basic can effectively prevent DDoS attacks.

How Anti-DDoS Origin Basic works

After you enable Anti-DDoS Origin Basic, traffic from the Internet must pass through Alibaba Cloud Security before the traffic arrives at the NAT gateway. Anti-DDoS Origin Basic scrubs and filters common DDoS attacks at Alibaba Cloud Security. Anti-DDoS Origin Basic protects your services against attacks such as SYN floods, UDP floods, ACK floods, ICMP floods, and DNS Query floods.

Anti-DDoS Origin Basic specifies the traffic scrubbing and blackhole triggering thresholds based on the bandwidth limit of the elastic IP address (EIP) that is associated with the NAT gateway. When the inbound traffic reaches the threshold, traffic scrubbing or blackhole is triggered:

- Traffic scrubbing: When the attack traffic from the Internet exceeds the scrubbing threshold or matches the attack traffic pattern, Alibaba Cloud Security starts to scrub the attack traffic. Traffic scrubbing includes packet filtering, bandwidth capping, and traffic throttling.
- Blackhole: When the attack traffic from the Internet exceeds the blackhole triggering threshold, blackhole is triggered and all inbound traffic is dropped.

Traffic scrubbing and blackhole triggering thresholds

The following table describes the methods that are used to calculate the traffic scrubbing and blackhole triggering thresholds on NAT gateways.

Bandwidth limit of the EIP	Traffic scrubbing threshold (bit/s)	Traffic scrubbing threshold (pps)	Default blackhole triggering threshold
Lower than or equal to 800 Mbit/s	800 Mbit/s	120,000	1.5 Gbit/s
Higher than 800 Mbit/s	Predefined bandwidth	Predefined bandwidth × 150	Predefined bandwidth × 2

If the bandwidth limit of the EIP is 1,000 Mbit/s, the traffic scrubbing threshold (bit/s) is 1,000 Mbit/s, the traffic scrubbing threshold (pps) is 150,000, and the default blackhole triggering threshold is 2 Gbit/s.