Alibaba Cloud NAT Gateway

Quick Start

Issue: 20190708

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 due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Tutorial overview

This tutorial provides a step-by-step guide on how to configure SNAT and DNAT so that ECS instances in a VPC can communicate with the Internet through NAT Gateway.

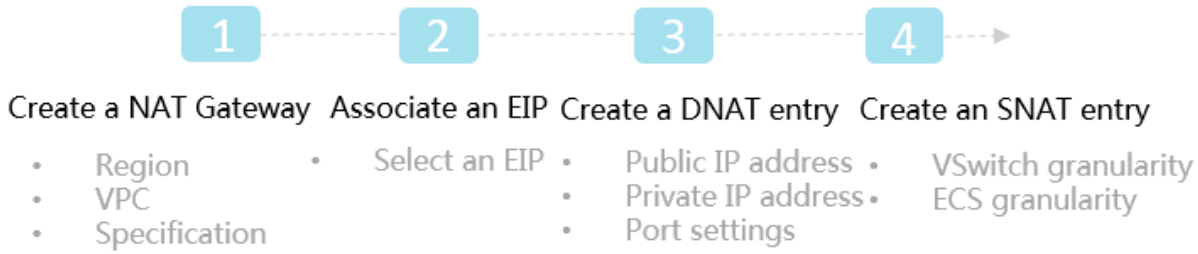
Prerequisites

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

- A VPC and a VSwitch are created. For more information, see Create a VPC and a VSwitch.
- An ECS instance of the VPC network is created. For more information, see Create an instance by using the wizard.

Procedure

An ECS instance without any public IP address is used in this example. The configuration flow chart is as follows:



1. Create a NAT Gateway

   NAT Gateway is an enterprise-class VPC Internet gateway that provides NAT proxy services. You must create a NAT Gateway before configuring SNAT and DNAT entries.

   For more information, see Create a NAT Gateway.

2. Associate an EIP with a NAT Gateway

   A NAT Gateway can work normally only after it is associated with a public IP address. After you create a NAT Gateway, you can associate an Elastic IP Address (EIP) with the NAT Gateway.

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

3. Create a DNAT entry

   NAT Gateway supports DNAT, which maps a public IP address to an ECS instance so that the ECS instance can provide Internet services. DNAT supports both port mapping and IP mapping.

   For more information, see Create a DNAT entry.

4. Create an SNAT entry

   NAT Gateway supports SNAT, which allows ECS instances without a public IP address in a VPC to access the Internet.

   For more information, see Create a SNAT entry.

2 Create a NAT Gateway

This topic describes how to create a NAT Gateway. After you create a NAT Gateway, you can configure SNAT and DNAT entries.

Prerequisites

A VPC and a VSwitch are created. For more information, see Create a VPC and a VSwitch.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click NAT Gateways.
3. On the NAT Gateways page, click Create NAT Gateway.
4. On the displayed purchase page, configure the NAT Gateway and complete the payment. The following table describes the parameters.

Configuration	Description
Region	Select the region where the target VPC (to which the NAT Gateway belongs) is located.
VPC ID	Select the VPC for which you want to create a NAT Gateway. After the NAT Gateway is created, you cannot change the VPC. Note: If you cannot find the target VPC in the VPC list, troubleshoot as follows: · Check whether a NAT Gateway is already configured for the VPC. A VPC can be configured with only one NAT Gateway. · Check whether there is a custom route entry whose destination CIDR block is 0.0.0.0/0 in the VPC. If so, delete this custom route entry.

Configuration	Description
Specification	Select a specification for the NAT Gateway. Different specifications correspond to different Max Connections and Connections Per Second (CPS) of the SNAT function. However, the data throughput is not affected. Note: The specification does not limit the number of connections and throughput of the DNAT function. For more information, see Specifications of NAT Gateway.
Billing cycle	Select a billing cycle for the NAT Gateway.

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 normally only after it is associated with a public IP address. After you associate an EIP with a NAT Gateway, you can use the EIP to configure SNAT entries.

Prerequisites

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

- Your NAT bandwidth package was purchased after January 26, 2018. If you purchased a package before January 26, 2018, you must open a ticket before you can associate an EIP with your NAT Gateway.
- A NAT Gateway and an EIP are created. For more information, see Create a NAT Gateway and Create an EIP.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the NAT Gateway.
4. Find the target NAT Gateway and choose More > Bind Elastic IP Address in the Actions column.
5. On the Bind Elastic IP Address page, complete the following configurations, and then click OK.

Configuration	Description
Select from EIP list	
Usable EIP list	Select an EIP that is used to access the Internet.

Configuration	Description
VSwitch	Select the VSwitch to which you want to add SNAT entries. The system automatically adds SNAT entries so that Alibaba Cloud services connected to this VSwitch can access the Internet. Alternatively, you can skip this step and add SNAT entries after you associate an EIP with a NAT Gateway. For more information, see Create a SNAT entry. Note: This option is displayed only for NAT Gateways that are not associated with an EIP.
Allocate one EIP and bind it to NAT Gateway	
Buy EIP	Displays the number of EIPs to be purchased. The default value is 1 and cannot be modified. The system automatically creates an EIP billed by traffic and associate it with the NAT Gateway.

Note:
One NAT Gateway can be associated with up to 20 EIPs, including up to 10 EIPs billed by traffic. The peak bandwidth of each EIP billed by traffic cannot exceed 200 Mbps. However, you can open a ticket to increase the quota of EIPs that one NAT Gateway can be associated with.

4 Create a DNAT entry

NAT Gateway supports the DNAT function, which maps a public IP address to an ECS instance so that the ECS instance can provide Internet services. DNAT supports both port mapping and IP mapping.

Prerequisites

A NAT Gateway is created and the NAT Gateway is associated with an EIP. For more information, see Create a NAT Gateway and Associate an EIP with a NAT Gateway.

> Note:
> If your account has purchased a bandwidth package before January 26, 2018, make sure there is an available public IP address in the bandwidth package.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the NAT Gateway.
4. On the NAT Gateways page, find the target NAT Gateway instance and click Configure DNAT in the Actions column.
5. On the DNAT Table page, click Create DNAT Entry.
6. On the Create DNAT Entry page, configure the DNAT entry according to the following information and click OK.

Configuration	Description
Public IP	Select a public IP address. Note: An IP address that is already being used in an SNAT entry cannot be selected.

Configuration	Description
Private IP	Select the private IP address of the ECS instance to access the Internet. You can specify the private IP address in the following ways: · Auto Fill: Select an ECS instance from the ECS instance or ENI list. · Manually Input: Enter the private IP address that you want to map.  Note: It must be within the private CIDR block of the VPC. You can also enter an existing private IP address of the ECS instance.
Port Settings	DNAT supports IP mapping and port mapping. Select a mapping method: · All Ports: Select this option to configure IP mapping. This is the same as associating an EIP with the ECS instance. If this method is used, all requests destined for the public IP address are directed to the ECS instance. · Specific Port: Select this option to configure port mapping. After this method is used, NAT Gateway forwards the requests from the specified protocol and port to the specified port of the ECS instance. After you select Specific Port, enter Public Port (the external port used for traffic forwarding), Private Port (the internal port used for traffic forwarding) and the IP Protocol (the protocol type of the port).

5 Create a SNAT entry

This topic describes how to create a SNAT entry. The SNAT function allows ECS instances that are not associated with a public IP address in a VPC to access the Internet.

Prerequisites

- A NAT Gateway is created and is associated with an Elastic IP Address (EIP). For more information, see Create a NAT Gateway and Associate an EIP with a NAT Gateway.

  Note:
  If you purchased a bandwidth package before January 26, 2018, make sure that a public IP address is available in the bandwidth package.
- If you want to create a SNAT entry with VSwitch granularity, make sure that a VSwitch has been created in the VPC associated with the NAT Gateway. For more information, see Create a VSwitch.
- If you want to create a SNAT entry with ECS granularity, make sure that an ECS instance has been created in the VPC associated with the NAT Gateway. For more information, see Create an instance by using the wizard.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the NAT Gateway.
4. On the NAT Gateways page, find the target NAT Gateway instance and click Configure SNAT in the Actions column.
5. On the SNAT Table page, click Create SNAT Entry.
6. On the Create SNAT Entry page, configure the SNAT entry and click OK. The following table describes the parameters.

Configuration	Description
VSwitch Granularity	

Configuration	Description
VSwitch	Select the VSwitch for which you want to create the SNAT entry in the associated VPC. All ECS instances that belong to the specified VSwitch can access the Internet through the SNAT function. Note: If an ECS instance is already associated with a public IP address (for example, it is assigned a public IP address, associated with an EIP, or configured with DNAT IP mapping), the ECS instance accesses the Internet by using the associated public IP address instead of the SNAT function of the NAT Gateway. To configure ECS instances in a VPC with the same public IP address, see Attach an ENI to an ECS that is allocated with an public IP address, Attach an ENI to an ECS instance associated with an EIP, and Attach an ENI to an ECS instance configured with DNAT IP mapping.
VSwitch CIDR Block	The CIDR block of the selected VSwitch.
Public IP	Select the public IP address that is used to access the Internet. You can select multiple public IP addresses to build a SNAT IP address pool. If you select multiple public IP addresses to build a SNAT IP address pool, make sure that each public IP address is added to the same shared bandwidth. For more information, see Add EIPs to an Internet Shared Bandwidth instance. Note: You cannot select a public IP address that is already used to create a DNAT entry.
Entry Name	Enter a name for the SNAT entry. The name must be 2 to 128 characters in length and can contain letters, numbers, Chinese characters, underscores (_), and hyphens (-). The name must start with a letter or a Chinese character.
ECS Granularity	

Configuration	Description
Available ECS Instances	Select the ECS instance for which you want to create the SNAT entry in the associated VPC. The selected ECS instance will access the Internet by using the specified public IP address. Make sure that the following conditions are met: · The ECS instance is running. · The ECS instance is not associated with any public IP addresses or EIPs.
ECS CIDR Block	The CIDR block of the ECS instance.
Public IP	Select the public IP address that is used to access the Internet. You can select multiple public IP addresses to build a SNAT IP address pool. If you select multiple public IP addresses to build a SNAT IP address pool, make sure that each public IP address is added to the same shared bandwidth. For more information, see Add EIPs to an Internet Shared Bandwidth instance. Note: You cannot select a public IP address that is already used to create a DNAT entry.
Entry Name	Enter a name for the SNAT entry. The name must be 2 to 128 characters in length and can contain letters, numbers, Chinese characters, underscores (_), and hyphens (-). The name must start with a letter or a Chinese character.