

Alibaba Cloud NAT Gateway

Product Introduction

Issue: 20190701

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 .
<code>Courier font</code>	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

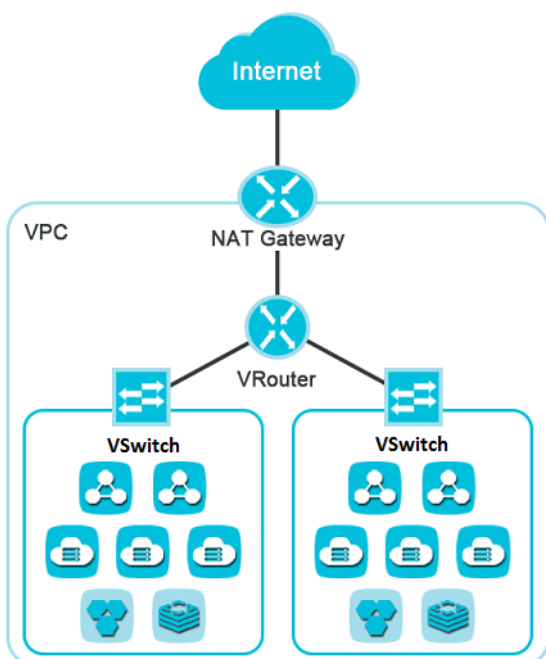
Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 What is NAT Gateway.....	1
2 Features.....	2
3 Benefits.....	3
4 Scenarios.....	4
5 Terms.....	5
6 Limits.....	6

1 What is NAT Gateway

NAT Gateway is an enterprise-class VPC Internet gateway that provides NAT proxy services (SNAT and DNAT), up to 10 Gbps forwarding capacity and cross-zone disaster tolerance.



As an Internet gateway, public IP addresses are required to make NAT Gateway function normally. After creating a NAT Gateway, you can associate an Elastic IP Address (EIP) with the NAT Gateway.



Note:

If your account purchased a NAT bandwidth package before January 26, 2018, you still need to use the bandwidth package to provide public IP addresses. To associate an EIP with the NAT Gateway, please open a ticket.

If you want to use the Internet Shared Bandwidth function, you can add EIPs to an existing Internet Shared Bandwidth in the EIP console or buy an Internet Shared Bandwidth first and then add the EIPs to it. For more information, see [Add EIPs to an Internet Shared Bandwidth instance](#).

2 Features

NAT Gateway provides SNAT, DNAT, and bandwidth sharing functions.

SNAT

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

In addition, SNAT can operate as a simple firewall that protects backend ECS instances. An external terminal can access an ECS instance after the ECS instance actively establishes a connection with the external terminal. An untrustworthy external terminal cannot access a backend ECS instance if no connection is established.

DNAT

NAT Gateway supports DNAT and maps a public IP address to a private IP address. Then, the ECS instance with the public IP address can provide public service.

DNAT supports both port mapping and IP mapping.

Bandwidth sharing

You can associate an NAT Gateway with an EIP and add the EIP to [Internet Shared Bandwidth](#). After an EIP is added to an Internet Shared Bandwidth, the original billing method of the EIP loses effect, and only the instance fee of the EIP is charged.

3 Benefits

NAT Gateway is flexible and easy to use, has high performance and high availability, and supports Pay-As-You-Go billing.

Flexible and easy-to-use

As an enterprise-class public network gateway for VPC, NAT Gateway provides SNAT and DNAT functions, which means you do not have to build your own SNAT gateway for your servers. NAT Gateway features high flexibility, stability, and reliability, and is easy to use.

High performance

NAT Gateway, a virtual network hardware, is based on Alibaba Cloud's self-developed distributed gateway and is supported by SDN virtualization technology. With the forwarding capacity of up to 10 Gbps, NAT Gateway supports large-scale Internet applications.

High availability

NAT Gateway supports the cross-zone disaster recovery. Failure in a single zone does not affect the service of NAT Gateway.

Pay-AS-You-Go billing

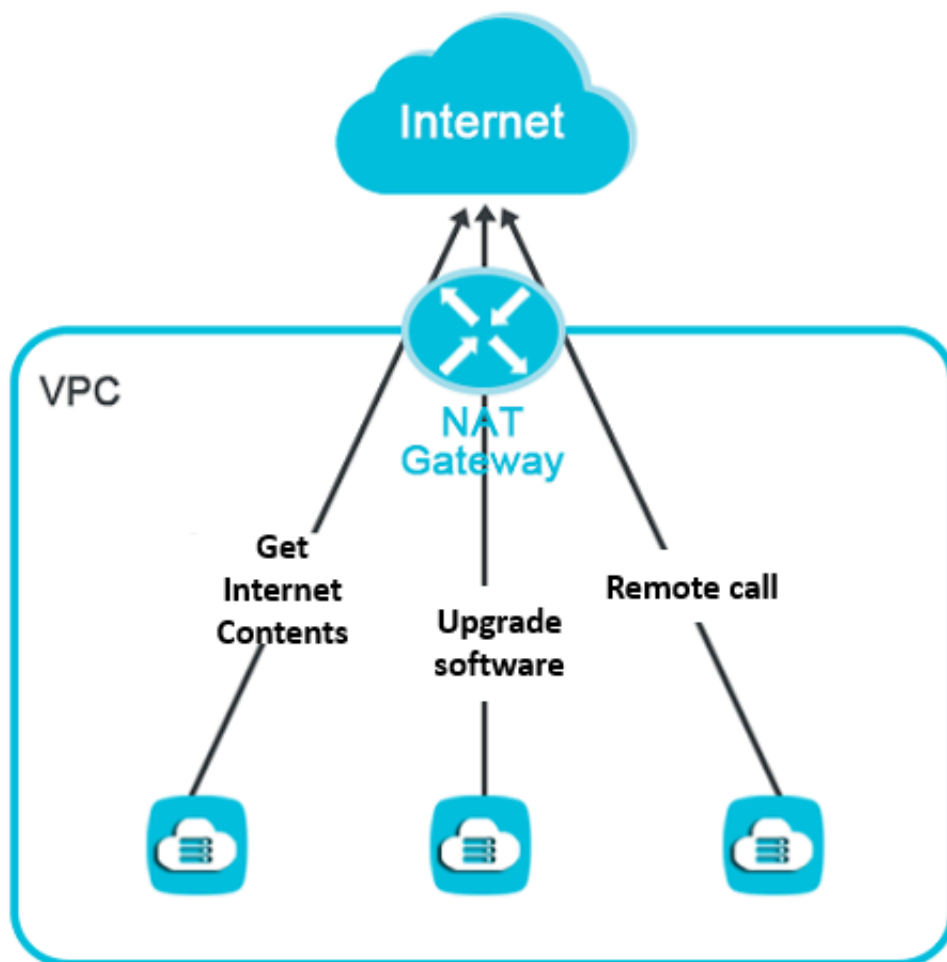
You can change the gateway specification and the number of EIPs at any time to meet changing service requirements.

4 Scenarios

NAT Gateway applies to scenarios where ECS instances of the VPC network need to access the Internet or provide public services.

Scenario 1: Set up a high-availability SNAT Gateway

In an IT system, some ECS instances need to access the Internet. Out of security concerns, public IP addresses of these ECS instances cannot be exposed on the Internet. In such cases, you can use the SNAT function of NAT Gateway. For more information, see [Create an SNAT entry](#).



Scenario 2: Provide public services

The ECS instances of the VPC network can provide public services by configuring IP mapping or port mapping.

5 Terms

This topic describes basic concepts of NAT Gateway.

Term	Description
NAT Gateway	NAT Gateway is an enterprise-class public network gateway that provides Internet proxy services (SNAT and DNAT) with up to 10 Gbps forwarding capability. It also features high availability in a region and disaster recovery across zones.
DNAT table	A DNAT table is a configuration table used for configuring DNAT. You can map a public IP address in a NAT bandwidth package to an ECS instance. DNAT supports IP mapping and port mapping.
SNAT table	An SNAT table is a configuration table used for configuring SNAT entries. You can configure SNAT entries for a VSwitch or for an ECS instance. <ul style="list-style-type: none">· Configure SNAT entries for a VSwitch: All ECS instances in the VSwitch use the specified public IP address to access the Internet.· Configure SNAT entries for an ECS instance: The ECS instance uses the specified public IP address to access the Internet.
EIP	Elastic IP Address (EIP) is a public IP address resource that can be independently purchased and owned. You can associate an EIP with an ECS instance of the VPC network, a private SLB instance of the VPC network, an ENI of the VPC network, and a NAT Gateway, or a HAVIP. <ul style="list-style-type: none">·

6 Limits

This topic describes limits related to the usage of NAT Gateway and EIPs.

Limits on NAT Gateway

- Only one NAT Gateway can be configured for a VPC.
- A public IP address cannot be used as an SNAT entry and a DNAT entry at the same time.
- Up to 100 DNAT entries can be added to a DNAT table. If you want to increase the quota, open a ticket.
- Up to 40 SNAT entries can be added to an SNAT table. If you want to increase the quota, open a ticket.
- If a VPC contains a custom route entry whose the destination CIDR block is 0.0.0.0/0, you must delete the CIDR block before you can create a NAT Gateway.
- If a VSwitch is associated with an SNAT entry, it is limited by the peak bandwidth of the selected EIP.

If the EIP is added to an Internet Shared Bandwidth, the VSwitch is limited by the peak bandwidth of the Internet Shared Bandwidth.

Limits on associating EIPs

- You can associate up to 20 EIPs with a NAT Gateway. If you want to increase the quota, open a ticket.
- You can associate up to 10 EIPs billed based on traffic with a NAT Gateway, and the peak bandwidth of each EIP billed based on traffic cannot be larger than 200 Mbps.
- For the same destination IP address and port, the number of EIPs set for a NAT Gateway limits the Max Connections for the NAT Gateway. The Max Connections for a NAT Gateway associated with only one EIP is 55,000, and the Max Connections for a NAT Gateway associated with multiple EIPs is $N \times 55,000$.
- ECS instances in a VPC that are not associated with any public IP addresses can access the Internet through a NAT Gateway. If the bandwidth at which the ECS instances access the same public IP address and port is greater than 2 Gbit/s, packets may be discarded due to limited ports. To resolve this issue, we recommend that you associate four to eight EIPs with the NAT Gateway and create an SNAT IP address pool.

- **If your account includes a NAT bandwidth package purchased before January 26, 2018, you still need to use the bandwidth package to provide public IP addresses. To associate an EIP with the NAT Gateway, open a ticket.**