Alibaba Cloud NAT Gateway

Best Practices

Issue: 20190416

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 Migrate a a self-built SNAT gateway to NAT Gateway

This tutorial illustrates how to migrate a self-built SNAT gateway to NAT Gateway.

Context

If you want to switch over from a self-built SNAT gateway on an ECS instance to the SNAT function based on NAT Gateway, you can remove the self-built SNAT gateway and then create and configure a NAT gateway. However, this will interrupt the SNAT function for a period of time.

The recommended best practice is to follow these steps to seamlessly switch over to a NAT gateway of Alibaba Cloud by using the longest match principle of the route table. During the switching process, the SNAT function will always be available. Interruption of the existing TCP connection only occurs at the instant of switching and you only need to reconnect the application.

The VPC and ECS configurations used in this tutorial are as follows:

- Two ECS instances are created in the VPC:
  - ECS (i-9410jxxxx) that is configured with a self-built SNAT gateway and is bound with an EIP. It also enables forwarding service and configures Iptables rules to achieve SNAT forwarding.
  - ECS (i-94kjwxxxxx) that requires the SNAT function to access the Internet.
- A custom route entry of which the destination CIDR block is 0.0.0.0/0 and the next hop is ECS (i-9410jxxxx) is added to the VRouter of the VPC.

Procedure

1. Add the following eight route entries in the VPC to overwrite existing route entries.

   The destination CIDR blocks are 1.0.0.0/8, 2.0.0.0/7, 4.0.0.0/6, 8.0.0.0/5, 16.0.0.0/4, 32.0.0.0/3, 64.0.0.0/2, 128.0.0.0/1, respectively, and the next hop is always ECS i-9410jxxxx.

   According to the longest match principle, a route entry with the longest subnet mask will always be matched first. However, all data packets, regardless of their IP addresses, will be matched to one of the eight entries. Therefore, the route entry, of which the destination CIDR block is 0.0.0.0/0, is not applied any more.

2. Delete the route entry of which the destination CIDR block is 0.0.0.0/0.
3. Create a NAT gateway.

   A route entry, of which the destination CIDR block is 0.0.0.0/0, pointing to the NAT gateway, is automatically added when creating the NAT gateway.
4. Bind EIPs to the NAT gateway.

   > **Notice:**
   >
   > Ensure the bandwidth of the EIPs bound to the NAT gateway is the same as the bandwidth of the self-built NAT gateway. If you have added an SNAT entry in the NAT gateway, the outbound traffic from the ECS instance specified in the SNAT entry will be limited by the bandwidth of the NAT gateway.
5. Add SNAT entries.
6. Delete the eight route entries added in Step 1, so that the VRouter will forward requests from the Internet to the NAT gateway instead of the self-built SNAT.

   Till now, the migration from the self-built SNAT gateway to the SNAT function of the NAT gateway on Alibaba Cloud is completed.