# Alibaba Cloud NAT Gateway

## Best Practices

Issue: 20190722

# 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:<br>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:<br>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:<br>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:<br>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-94kjwxxxx) 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.

# 2 Create a SNAT IP address pool

This topic describes how to create a SNAT IP address pool by adding multiple EIPs to the SNAT IP address pool. After you create a SNAT IP address pool, ECS instances in a VPC can access the Internet by using the EIPs in the SNAT address pool.

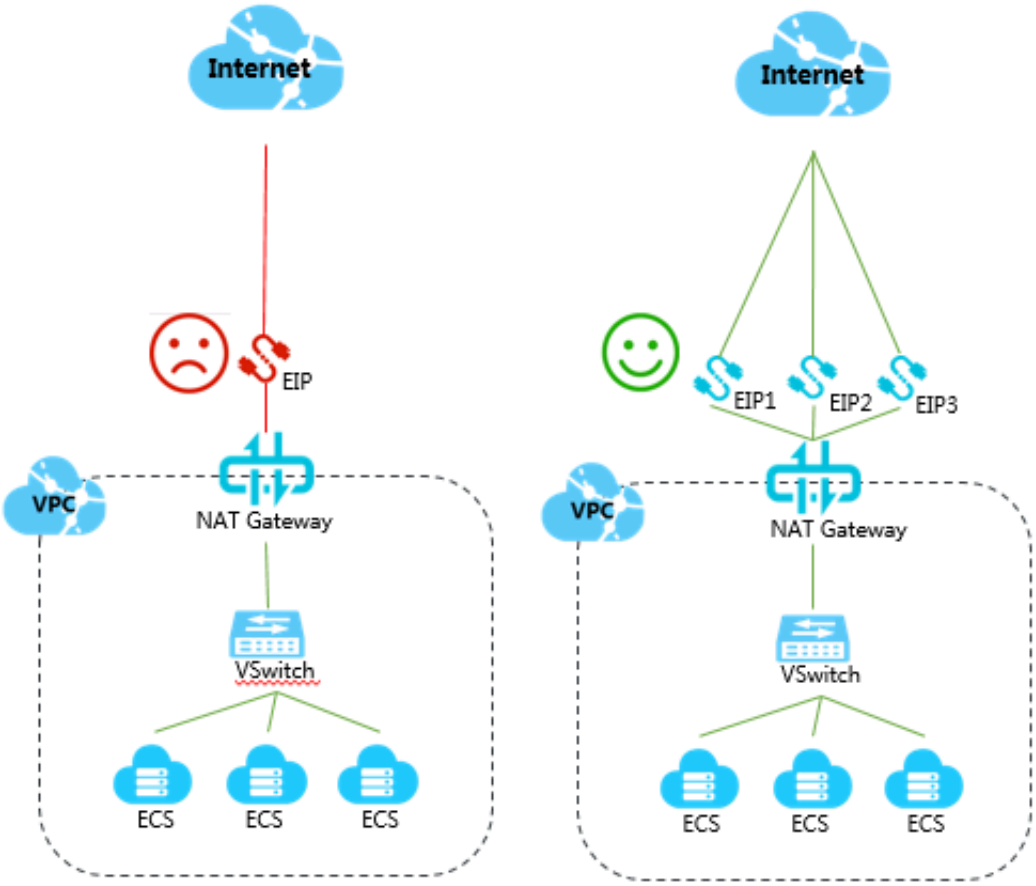
## Prerequisites

- A VPC and a VSwitch are created. For more information, see Create a VPC and a VSwitch.
- An EIP is created. For more information, see Create an EIP.

## Background information

A NAT Gateway is an enterprise-class VPC-based Internet gateway that provides the SNAT function. It enables ECS instances without public IP addresses in a VPC to access the Internet. If you configure only one EIP for the specified VSwitch or ECS instance when you create a SNAT entry, this EIP cannot process huge traffic when the ECS instance initiates a large number of Internet access requests.

You can add multiple EIPs to a SNAT address pool. When an ECS instance in a VPC initiates an access request, the ECS instance randomly accesses the Internet by using an EIP in the SNAT address pool.




### Step 1: Create a NAT Gateway

To create a NAT Gateway, follow these steps:

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.
   - 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.

- Specification: Select the specification of 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 the billing cycle of the NAT Gateway.

### Step 2: Associate an EIP with the NAT Gateway

To associate EIPs with the NAT Gateway, follow these steps:

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.
   - Select from EIP list: Select an EIP from the existing EIP list and associate the EIP with the NAT Gateway.
   - Allocate one EIP and bind it to NAT Gateway: The system automatically creates an EIP billed by traffic and associate the EIP 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.
6. Repeat the preceding steps to associate more EIPs with the NAT Gateway.

### Step 3: Add an EIP to a shared bandwidth

To add an EIP to a shared bandwidth, follow these steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click Elastic IP Addresses.
3. Select the region to which the target EIP belongs.
4. On the Elastic IP Addresses page, find the target EIP, and then choose More > Add to Shared Bandwidth Package in the Actions column.
5. Select the target Internet Shared Bandwidth, and then click OK.

### Step 4: Create a SNAT entry

To create a SNAT entry and add multiple EIPs to a SNAT address pool, follow these steps:

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.

   On the VSwitch Granularity tab page, complete the following settings:

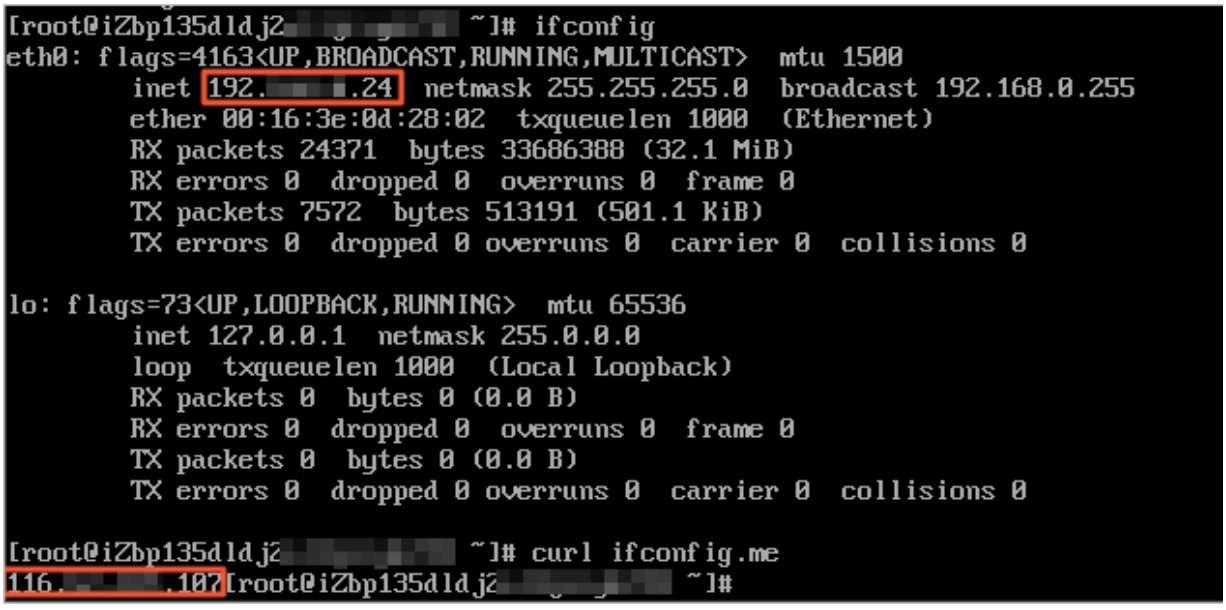
   - VSwitch: Select a VSwitch in the VPC. All ECS instances that belong to the specified VSwitch can access the Internet through the SNAT function.
   - VSwitch CIDR Block: the CIDR block of the VSwitch.
   - Public IP: Select the public IP address that is used to access the Internet. You can select multiple public IP addresses to build a SNAT IP address pool.
   - Entry Name: Enter the name of the SNAT entry.

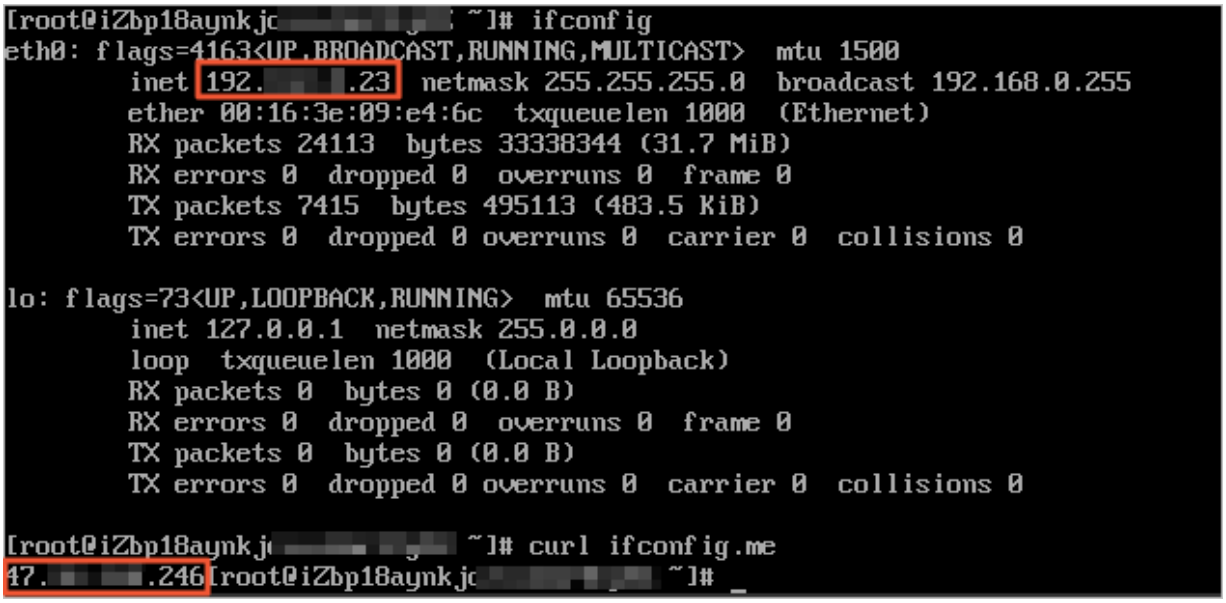
   On the ECS Granularity tab page, complete the following settings:

   - Available ECS Instances: Select an ECS instance in the VPC.
   - 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.
   - Entry Name: Enter the name of the SNAT entry.

### Step 5: Test access to the Internet

Log on to two ECS instances configured with SNAT rules to view the source IP addresses used to access the Internet.




[root@iZbp18aynkjc ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192. .23 netmask 255.255.255.0 broadcast 192.168.0.255
ether 00:16:3e:09:e4:6c txqueuelen 1000 (Ethernet)
RX packets 24113 bytes 33338344 (31.7 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 7415 bytes 495113 (483.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
loop txqueuelen 1000 (Local Loopback)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[root@iZbp18aynkj ~]# curl ifconfig.me
47. .246[root@iZbp18aynkjc ~]#

# 3 Uniformly manage public IP addresses of ECS instances in a VPC

## 3.1 Attach an ENI to an ECS that is allocated with an public IP address

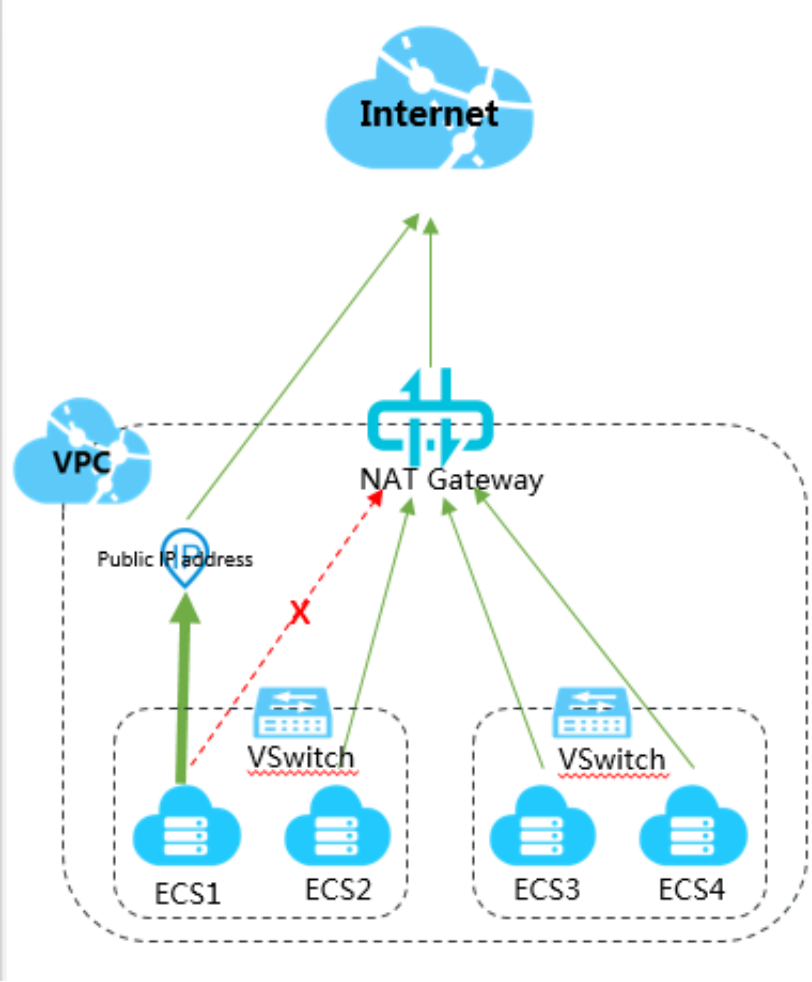
This topic describes how to attach an ENI to an ECS instance that is allocated with a public IP address. When you attach an ENI to an ECS instance, you can uniformly manage the public IP addresses of all ECS instances in a VPC.

### Prerequisites

The VPC to which the ECS instance with an allocated public IP address belongs is configured with the SNAT function. For more information, see Create a SNAT entry.

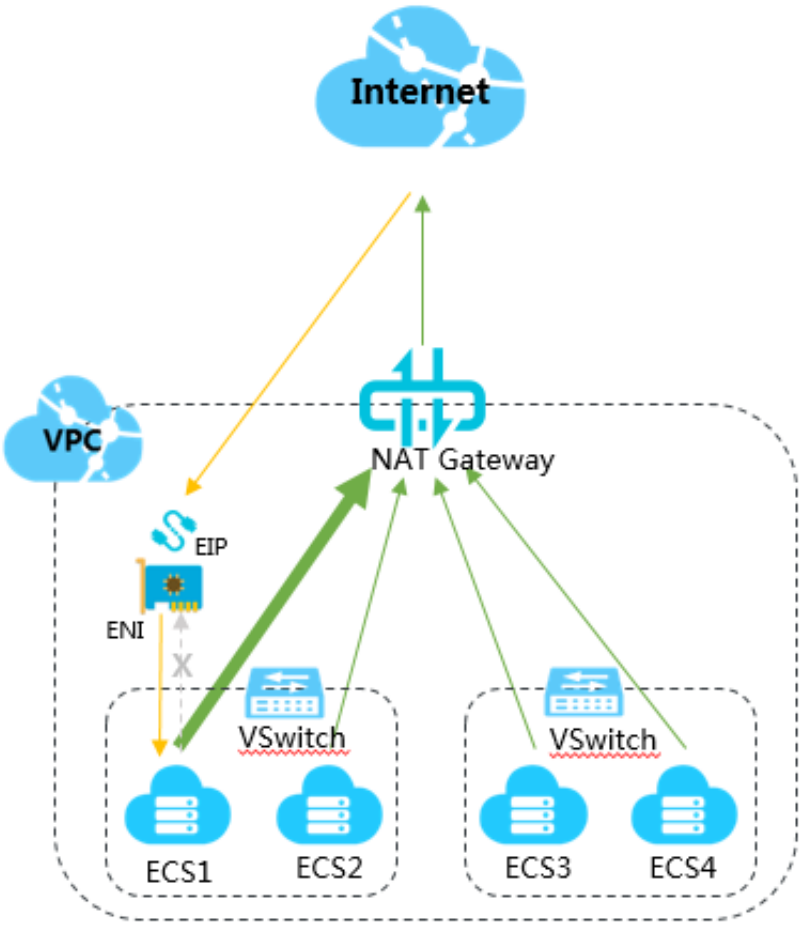
### Background Information

The Alibaba Cloud NAT Gateway supports SNAT. SNAT is a function that allows an ECS instance without a public IP address to access the Internet. If an ECS instance in a VPC is configured with a public IP address, the ECS instance can access the Internet through the public IP address, while other ECS instances in the VPC access the Internet through the SNAT function of NAT Gateway. Therefore, ECS instances in the VPC use different IP addresses to access the Internet.




You can attach an ENI to the ECS instance to uniformly manage the public IP addresses of ECS instances in the VPC.

As shown in the following figure, you can attach an ENI to the ECS instance, convert the public IP address of the ECS instance to an EIP, and associate the EIP to the ENI, so that traffic from the Internet accesses the ECS instance through the ENI, and the ECS instance accesses the Internet through NAT Gateway.




### Step 1: Convert the public IP address to an EIP

Support for converting a public IP address to an EIP varies according to the billing methods:

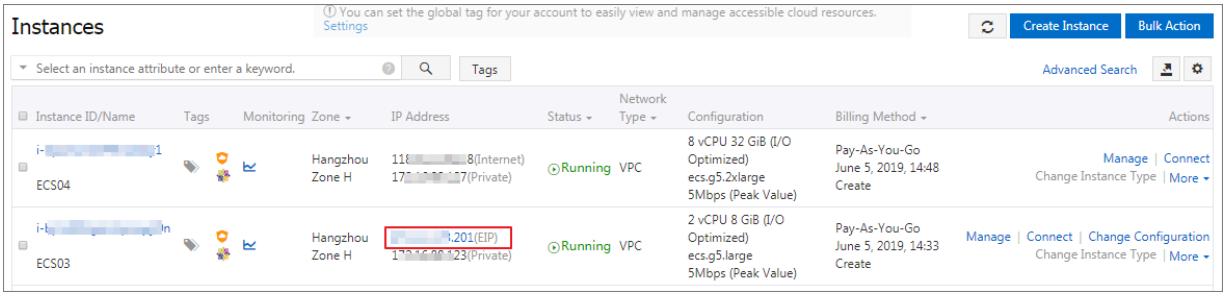
- Pay-As-You-Go ECS instances support directly converting a public IP address to an EIP.
- Subscription ECS instances do not support directly converting a public IP address to an EIP. To convert a public IP address of a Subscription ECS instance to an EIP, you must first change the Subscription instance to a Pay-As-You-Go instance. For more information, see Change a Subscription instance to a Pay-As-You-Go instance.

To convert an public IP address of an ECS instance to an EIP, follow these steps:

1. Log on to the ECS console.
2. In the left-side navigation pane, click Instances.
3. Select the region of the target ECS instance.
4. On the Instances page, find the target ECS instance, and choose More > Network and Security Group > Convert to EIP in the Actions column.

5. In the displayed dialog box, click OK.
6. Refresh the list of ECS instances.

   After the the ECS public IP address is converted to an EIP, the original public IP address is labelled as EIP.




### Step 2: Create an ENI

To create an ENI for an ECS instance, follow these steps:

1. Log on to the ECS console.
2. In the left-side navigation pane, click Network and Security > ENI.
3. Select the target region.

   **Note:**
   The ENI and the ECS instance must be in the same region.
4. On the Network Interfaces page, click Create ENI.
5. On the Create ENI page, configure the ENI according to the following information and click OK.

   - Network Interface Name: Enter the name of the ENI.
   - VPC: Select the VPC to which the ECS instance belongs.
   - VSwitch: Select the VSwitch of the zone to which the ECS instance belongs.
   - Primary Private IP (optional): Enter the primary private IPv4 address of the ENI. The IPv4 address must be an idle address in the CIDR block of the specified VSwitch. If you do not specify one, an idle private IPv4 address is automatically assigned to your ENI after the ENI is created.
   - Security Group: Select a security group of the VPC.
   - Description (optional): Enter a description for the ENI.

### Step 3: Attach the ENI to the ECS instance

To attach the ENI to the ECS instance, follow these steps:

1. Log on to the ECS console.
2. In the left-side navigation pane, click Network and Security > ENI.
3. Select the target region.
4. On the Network Interfaces page, find the target ENI, and click Bind to Instance in the Actions column.
5. In the displayed dialog box, select the ECS instance to attach and click OK.

### Step 4: Disassociate the EIP from the ECS instance

To disassociate the EIP from the ECS instance, follow these steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click Elastic IP Addresses.
3. Select the region of the target EIP.
4. On the Elastic IP Addresses page, find the target EIP and click Unbind in the Actions column.
5. In the displayed dialog box, click OK.

### Step 5: Associate the EIP with the ENI

To associate the EIP with the ENI, follow these steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click Elastic IP Addresses.
3. Select the region of the target EIP.
4. On the Elastic IP Addresses page, find the target EIP and click Bind in the Actions column.
5. On the Bind Elastic IP Address page, associate the EIP with the ENI according to the following information and click OK.
   - IP Address: Displays the EIP.
   - Instance Type: Select Secondary ENI.
   - Resource Group (optional): Select the resource group to which the EIP belongs.
   - Mode (optional): Select the NAT mode.
   - Secondary ENI: Select the ENI to be associated.

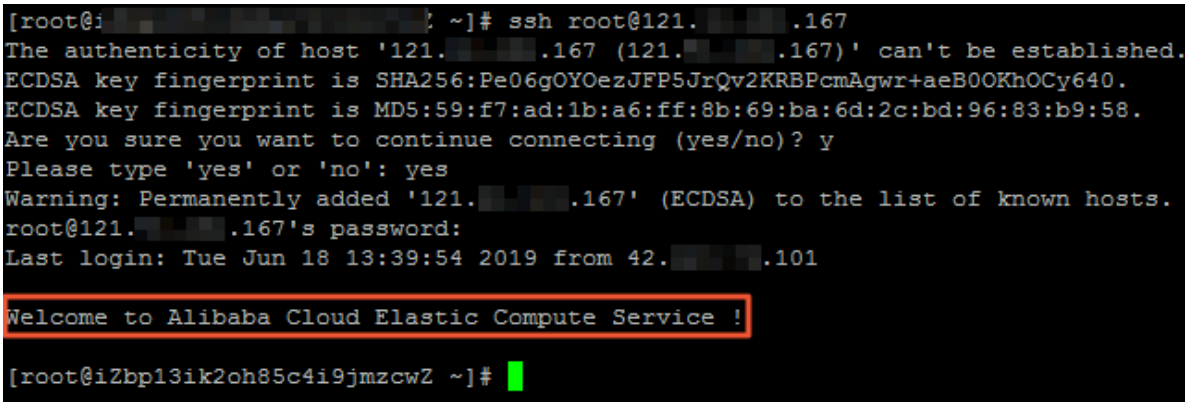
### Step 6: Test the network connectivity

Follow these steps to test whether the ECS instance can be accessed from the Internet through the EIP associated with the ENI. In this tutorial, a Linux instance is accessed from a remote Linux client.

> **Note:**
> The security group rules of the Linux instance must allow access from the SSH (22) port. For more information, see Add security group rules.

1. Log on to the Linux client.
2. Run the `ssh root@public IP address` command and enter the logon password of the Linux instance to check if the remote access is successful.

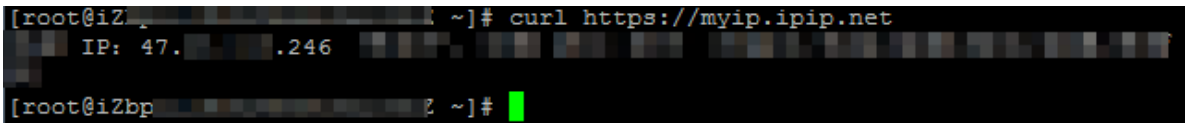
   If `Welcome to Alibaba Cloud Elastic Compute Service!` is displayed, it means that the connection has been established.




Follow these steps to test if the ECS instance can access the Internet through the SNAT function of NAT Gateway. In this tutorial, the public IP address used is checked.

1. Log on to the ECS instance.
2. Run the `curl https://myip.ipip.net` to view the public IP address.

   If the public IP address is the same as the IP address in the SNAT entry of the NAT Gateway, it means that the ECS instance accesses the Internet through the SNAT function of NAT Gateway.



# 3.2 Attach an ENI to an ECS instance associated with an EIP

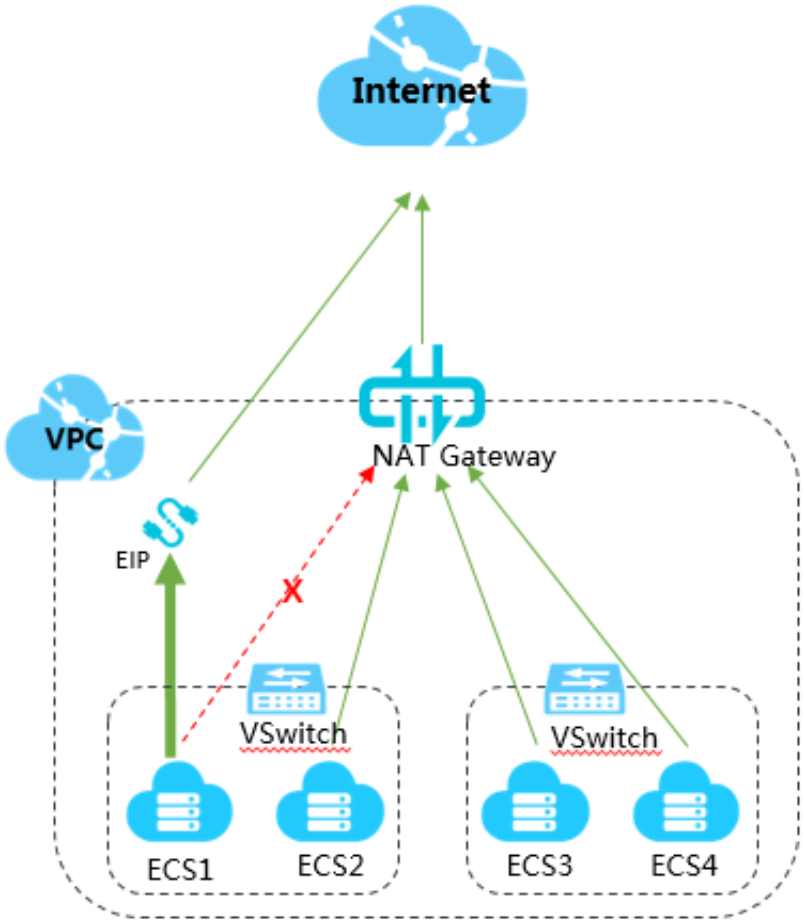
The topic describes how to attach an ENI to an ECS instance associated with an EIP. When you attach an ENI to an ECS instance, you can uniformly manage public IP addresses of the ECS instances in a VPC.

## Prerequisites

The VPC to which the ECS instance associated with an EIP belongs is configured with the SNAT function. For more information, see Create a SNAT entry.

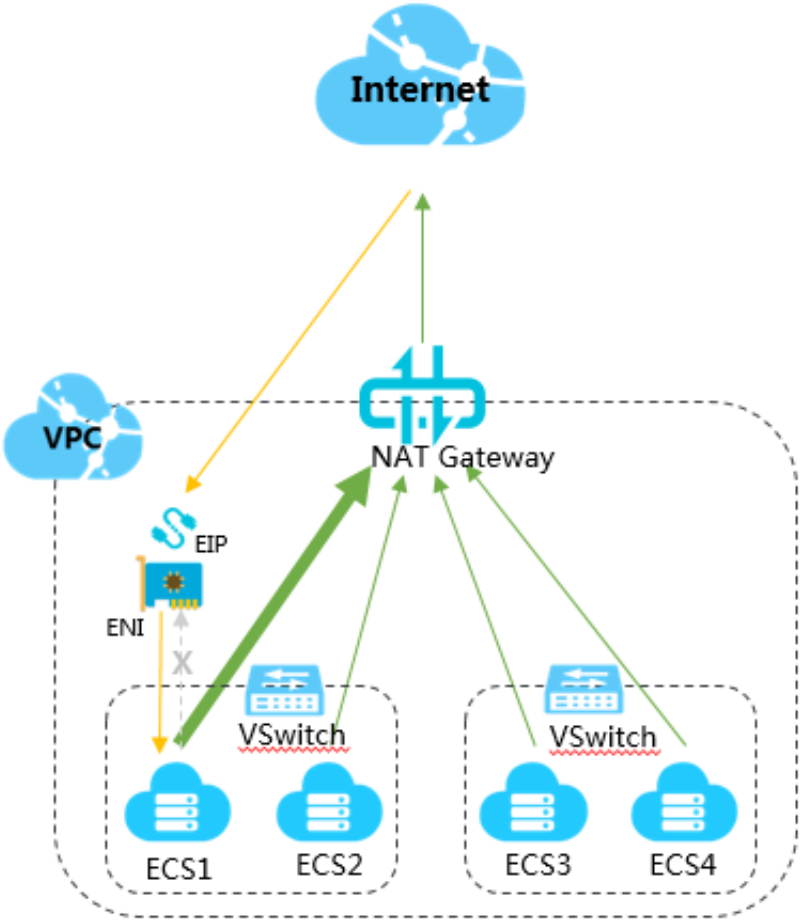
## Background Information

NAT Gateway supports SNAT, which allows an ECS instance without a public IP address in a VPC to access the Internet. If an ECS instance in a VPC is configured with an EIP, the ECS instance accesses the Internet through the EIP, while other ECS instances in the VPC access the Internet through the SNAT function of NAT Gateway. Therefore, ECS instances in the VPC use different IP addresses to access the Internet.




You can attach an ENI to the ECS instance to uniformly manage the public IP addresses of the ECS instances in a VPC.

As shown in the following figure, you can attach an ENI to the ECS instance and associate the EIP with the ENI, so that traffic from the Internet accesses the ECS instance through the ENI, and the ECS instance accesses the Internet through NAT Gateway.




### Step 1: Create an ENI

To create an ENI for an ECS instance, follow these steps:

1. Log on to the ECS console.
2. In the left-side navigation pane, click Network and Security > ENI.
3. Select the target region.

> **Note:**
> The ENI and the ECS instance must be in the same region.

4. On the Network Interfaces page, click Create ENI.

5. On the Create ENI page, configure the ENI according to the following information and click OK.
   - Network Interface Name: Enter the name of the ENI.
   - VPC: Select the VPC to which the ECS instance belongs.
   - VSwitch: Select the VSwitch of the zone to which the ECS instance belongs.
   - Primary Private IP (optional): Enter the primary private IPv4 address of the ENI. The IPv4 address must be an idle address in the CIDR block of the specified VSwitch. If you do not specify one, an idle private IPv4 address is automatically assigned to your ENI after the ENI is created.
   - Security Group: Select a security group of the VPC.
   - Description (optional): Enter a description for the ENI.

### Step 2: Attach the ENI to the ECS instance

To attach the ENI to the ECS instance, follow these steps:

1. Log on to the ECS console.
2. In the left-side navigation pane, click Network and Security > ENI.
3. Select the target region.
4. On the Network Interfaces page, find the target ENI, and click Bind to Instance in the Actions column.
5. In the displayed dialog box, select the ECS instance to attach and click OK.

### Step 3: Disassociate the EIP from the ECS instance

To disassociate the EIP from the ECS instance, follow these steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click Elastic IP Addresses.
3. Select the region of the target EIP.
4. On the Elastic IP Addresses page, find the target EIP and click Unbind in the Actions column.
5. In the displayed dialog box, click OK.

### Step 4: Associate the EIP with the ENI

To associate the EIP with the ENI, follow these steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click Elastic IP Addresses.

3. Select the region of the target EIP.
4. On the Elastic IP Addresses page, find the target EIP and click Bind in the Actions column.
5. On the Bind Elastic IP Address page, associate the EIP with the ENI according to the following information and click OK.
   - IP Address: Displays the EIP.
   - Instance Type: Select Secondary ENI.
   - Resource Group (optional): Select the resource group to which the EIP belongs.
   - Mode (optional): Select the NAT mode.
   - Secondary ENI: Select the ENI to be associated.

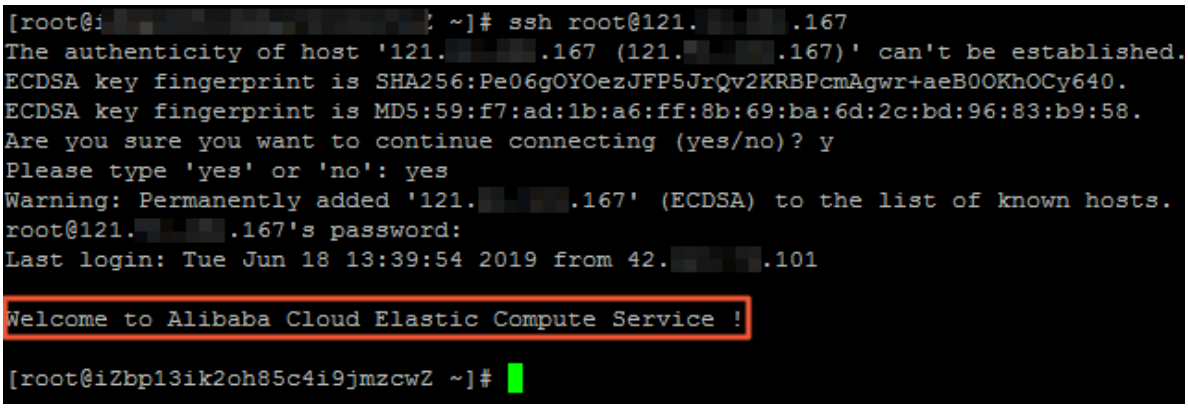
### Step 5: Test the network connectivity

Follow these steps to test whether the ECS instance can be accessed from the Internet through the EIP associated with the ENI. In this tutorial, a Linux instance is accessed from a remote Linux client.

> **Note:**
> The security group rules of the Linux instance must allow access from the SSH (22) port. For more information, see Add security group rules.

1. Log on to the Linux client.
2. Run the `ssh root@public IP address` command and enter the logon password of the Linux instance to check if the remote access is successful.

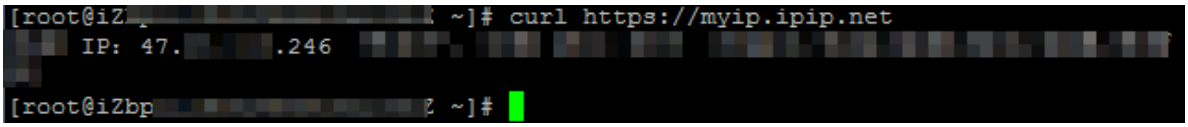
   If `Welcome to Alibaba Cloud Elastic Compute Service!` is displayed, it means that the connection has been established.




Follow these steps to test if the ECS instance can access the Internet through the SNAT function of NAT Gateway. In this tutorial, the public IP address used is checked.

1. Log on to the ECS instance.
2. Run the `curl https://myip.ipip.net` to view the public IP address.

   If the public IP address is the same as the IP address in the SNAT entry of the NAT Gateway, it means that the ECS instance accesses the Internet through the SNAT function of NAT Gateway.




## 3.3 Attach an ENI to an ECS instance configured with DNAT IP mapping

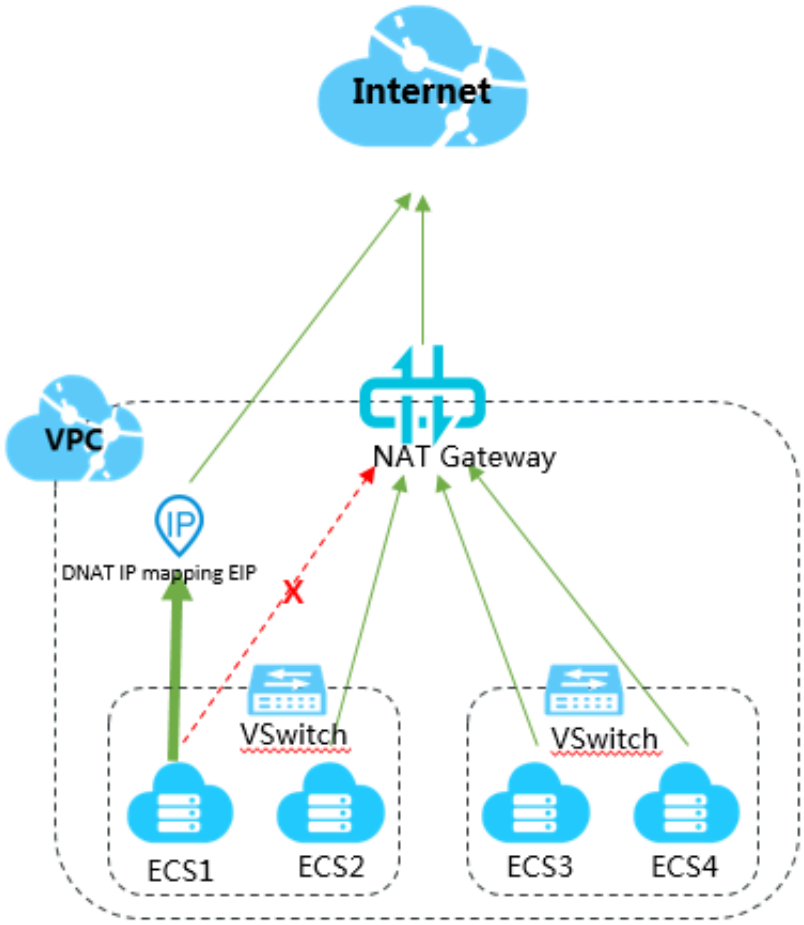
This topic describes how to attach an ENI to an ECS instance configured with DNAT IP mapping. After you attach an ENI to an ECS instance configured with DNAT IP mapping, you can uniformly manage public IP addresses of ECS instances in a VPC.

### Prerequisites

The VPC to which the ECS instance configured with DNAT IP mapping is configure with the SNAT function. For more information, see Create a SNAT entry.

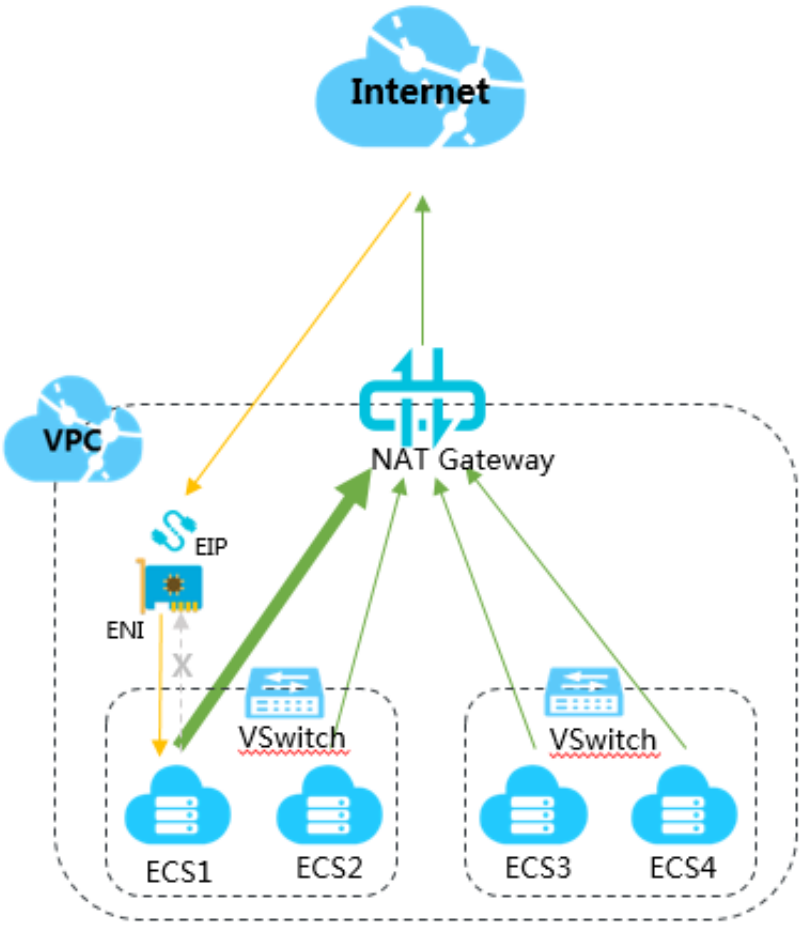
### Background information

NAT Gateway supports SNAT, which is a function that allows ECS instances without a public IP address in a VPC to access the Internet. If an ECS instance in a VPC is configured with DNAT IP mapping (full port mapping), the ECS instance accesses the Internet through the public IP address in the corresponding DNAT entry, while other ECS instances in the VPC access the Internet through the SNAT function of NAT Gateway. Therefore, ECS instances in the VPC use different IP addresses to access the Internet.




You can attach an ENI to the ECS instance to uniformly manage the public IP addresses of ECS instances in the VPC.

As shown in the following figure, you can attach an ENI to the ECS instance, remove the corresponding DNAT entry in the NAT Gateway, create a new DNAT entry, and map a public IP address on the NAT Gateway to the ENI, so that traffic from the Internet accesses the ECS instance through the ENI, and the ECS instance accesses the Internet through NAT Gateway.




### Step 1: Create an ENI

To create an ENI for an ECS instance, follow these steps:

1. Log on to the ECS console.
2. In the left-side navigation pane, click Network and Security > ENI.
3. Select the target region.

   Note:
   The ENI and the ECS instance must be in the same region.
4. On the Network Interfaces page, click Create ENI.

5. On the Create ENI page, configure the ENI according to the following information and click OK.
   - Network Interface Name: Enter the name of the ENI.
   - VPC: Select the VPC to which the ECS instance belongs.
   - VSwitch: Select the VSwitch of the zone to which the ECS instance belongs.
   - Primary Private IP (optional): Enter the primary private IPv4 address of the ENI. The IPv4 address must be an idle address in the CIDR block of the specified VSwitch. If you do not specify one, an idle private IPv4 address is automatically assigned to your ENI after the ENI is created.
   - Security Group: Select a security group of the VPC.
   - Description (optional): Enter a description for the ENI.

### Step 2: Attach the ENI to the ECS instance

To attach the ENI to the ECS instance, follow these steps:

1. Log on to the ECS console.
2. In the left-side navigation pane, click Network and Security > ENI.
3. Select the target region.
4. On the Network Interfaces page, find the target ENI, and click Bind to Instance in the Actions column.
5. In the displayed dialog box, select the ECS instance to attach and click OK.

### Step 3: Remove the DNAT entry

To remove the corresponding DNAT entry in the NAT Gateway, follow these steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the target region.
4. On the NAT Gateways page, find the target NAT Gateway and click Configure DNAT in the Actions column.
5. On the DNAT Entry List page, find the target DNAT entry and click Remove in the Actions column.
6. In the displayed dialog box, click OK.

### Step 4: Create a DNAT entry

To create a DNAT entry and map a public IP address in the NAT Gateway to the ENI, follow these steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click NAT Gateways.
3. On the NAT Gateways page, find the target NAT Gateway instance and click Configure DNAT in the Actions column.
4. On the DNAT Entry List page, click Create DNAT Entry.
5. On the Create DNAT Entry page, configure the DNAT entry according to the following information and click OK.
   - Public IP: Select an available public IP address. An IP address that is already being used in an SNAT entry cannot be selected.
   - Private IP address: Select the ENI instance.
   - Port Settings: Select All Ports.
   - Entry Name: Enter the name of the DNAT entry.

### Step 5: Test the network connectivity

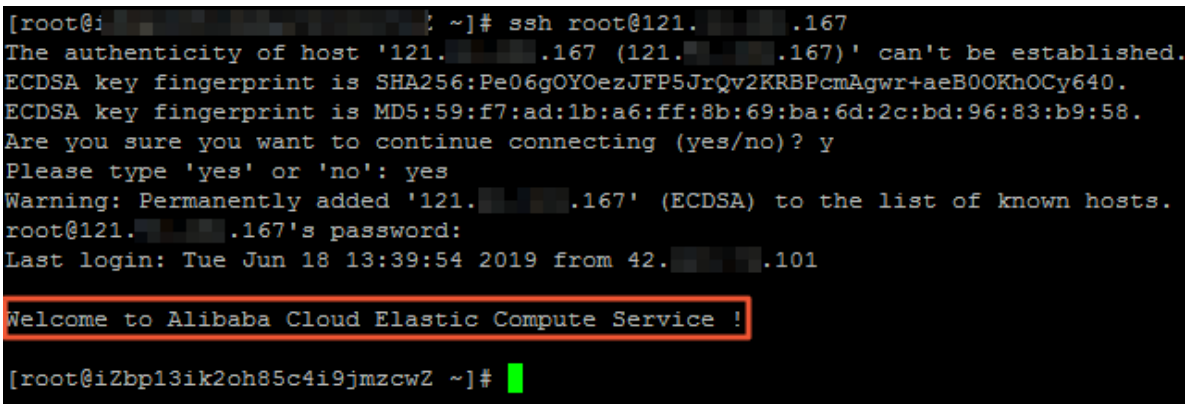
Follow these steps to test whether the ECS instance can be accessed from the Internet through the EIP associated with the ENI. In this tutorial, a Linux instance is accessed from a remote Linux client.

> Note:
> The security group rules of the Linux instance must allow access from the SSH (22) port. For more information, see Add security group rules.

1. Log on to the Linux client.

2. Run the `ssh root@public IP address` command and enter the logon password of the Linux instance to check if the remote access is successful.

   If `Welcome to Alibaba Cloud Elastic Compute Service!` is displayed, it means that the connection has been established.




Follow these steps to test if the ECS instance can access the Internet through the SNAT function of NAT Gateway. In this tutorial, the public IP address used is checked.

1. Log on to the ECS instance.
2. Run the `curl https://myip.ipip.net` to view the public IP address.

   If the public IP address is the same as the IP address in the SNAT entry of the NAT Gateway, it means that the ECS instance accesses the Internet through the SNAT function of NAT Gateway.