NAT Gateway

Private NAT Gateway Operation Guide

Product Documentation

Contents

Private NAT Gateway Operation Guide
Creating and Managing a NAT Gateway

Last updated：2024-08-01 14:19:27

Creating Private NAT Gateway

Note

Private NAT Gateway is in beta testing. If you need to use it, please submit a ticket for request.

1. Log in to the NAT Gateway console.

2. Select a region and VPC, and click **Create**.

3. On the **private NAT gateway** purchase page, enter or confirm the relevant parameters as needed, and complete the purchase following the official website guide.

Parameter	Description
Gateway configuration	Billing mode: Pay-as-you-go. Gateway name: Enter the NAT gateway name as needed, which supports up to 60 characters. Region: Select the region for the NAT gateway. Associated instance: supports selecting 3 types of instances associated with the NAT gateway: Direct Connect Gateway, VPC, and CCN. Direct Connect Gateway: mainly solves address translation between the VPC and the Direct Connect IDC within the same region (e.g., within the Beijing region). It is used for mutual access between the VPC and Direct Connect resources. CCN: mainly solves address translation between the cross-region VPCs, and address translation between the VPC and Direct Connect IDC (e.g., from Beijing to Shanghai). It is used for the cross-region VPC to access other public network resources through the CCN. VPC: mainly solves address translation for a specified subnet in a VPC. It is used for mutual access between the specified subnet in the VPC and the public network resources.
Other configuration	Optional configuration. You can choose whether to set tag information for this instance as needed. If not required, you can skip it.

Modifying Private NAT Gateway Information

1. Log in to the Private NAT Gateway console and click the **private NAT gateway ID** that you want to modify in the list, to enter the details page.

2. On the details page, you can perform the following operations:

Click on the


next to the gateway name to modify it. The gateway name cannot exceed 60 characters.

Click on the


in the Tag row to add a tag. You can perform permission management through the tags.

Deleting Private NAT Gateway

Note

During deletion of a private NAT gateway, all associated policies will also be deleted and Internet forwarding requests will be immediately interrupted. Please prepare for network interruptions in advance.

After confirming that the NAT gateway is no longer needed, you can delete it at any time.

1. Log in to the Private NAT Gateway console, locate the NAT gateway that you want to delete in the list, and click **Delete** in the **Operation** column.
2. In the pop-up window, click **Confirm**.

Configuring a Route to Private NAT Gateway

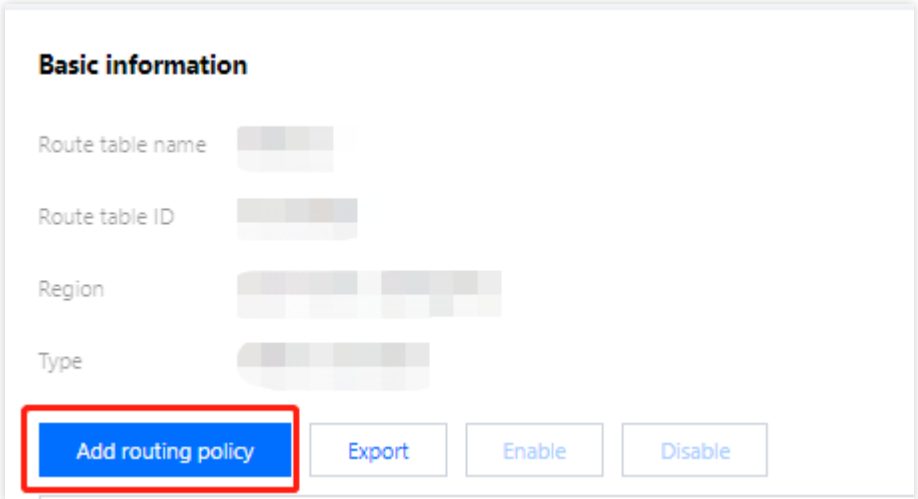
Last updated：2024-08-01 14:18:22

Once a private NAT gateway is created, the cloud resources in the subnet can access public network resources through the private NAT gateway only after you configure the routing rule to the private NAT gateway.
This section describes how to configure a routing policy pointing to the private NAT gateway. The 2 optional methods are as follows:
Method 1: Configuring in the **Private NAT Gateway** Console
Method 2: Configuring in the **Route Table** Console

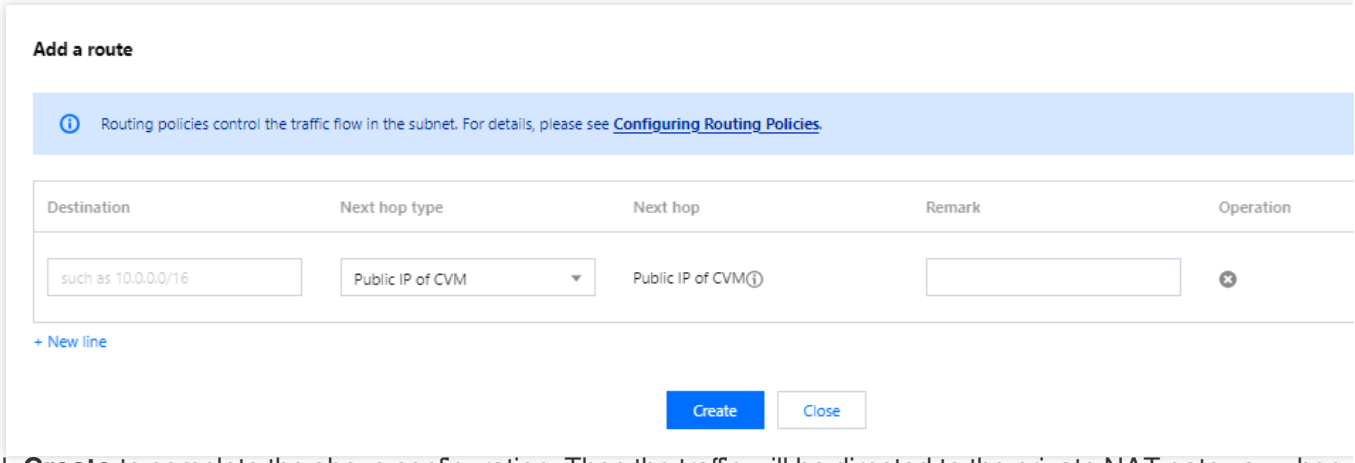
Directions

Method 1: Configuring in the NAT Gateway Console

1. Log in to the NAT Gateway console.
2. Click **Private NAT Gateway** on the left side and click on the **network ID** of the target NAT gateway instance in the private NAT gateway instance list.
3. In the target VPC **Details**>**Basic Information**>**Included Resources**, click **Subnet**.
4. In the subnet list, select the **associated route table ID** in the row of the subnet that requires accessing public VPC/Direct Connect/CCN.
5. On the basic information page of the route table, click **Add Routing Policy**.



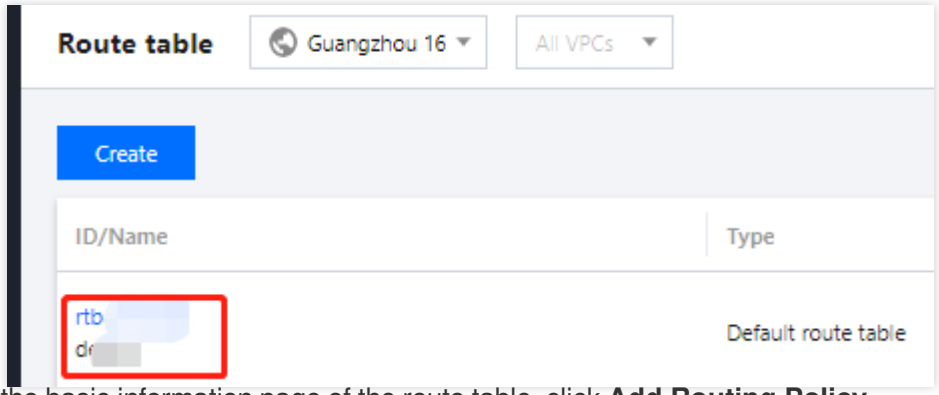
6. In the **Add Routing** pop-up box, enter the destination (IP range corresponding to the destination), select **Private NAT Gateway** as the next hop type, and select the created private NAT gateway ID as the next hop.



7. Click **Create** to complete the above configuration. Then the traffic will be directed to the private NAT gateway when a CVM in the subnet associated with this route table accesses the destination address.

Method 2: Configuring in the Route Table Console

1. Log in to the Route Table console.
2. In the route table list, click the **route table ID** associated with the subnet that requires accessing public VPC/Direct Connect/CCN, to enter the details page.



3. On the basic information page of the route table, click **Add Routing Policy**.
4. In the **Add Routing** pop-up box, enter the destination (IP range corresponding to the destination), select **Private NAT Gateway** as the next hop type, and select the created **private NAT gateway ID** as the next hop.
5. Click **Create** to complete the above configuration. Then the traffic will be directed to the private NAT gateway when a CVM in the subnet associated with this route table accesses the destination address.

Managing SNAT Rules

Last updated：2024-08-01 14:17:28

Different types of private NAT gateway instances correspond to different SNAT rules. This document provides a detailed description of SNAT rules corresponding to different associated instances.

Prerequisites

Before creating an SNAT rule, ensure that the route table for the subnet points to the corresponding NAT gateway. For detailed operations, see Configuring a Route to Private NAT Gateway.

Creating an SNAT Rule

Direct Connect Gateway

The Direct Connect type of private NAT gateways mainly solve address translation between the VPC and Direct Connect IDC in the same region (e.g., within the Beijing region). They are used for mutual access between the VPC and Direct Connect resources. To create an SNAT rule for this type of private NAT gateways, you can take the following steps.

1. Log in to the NAT Gateway console and click on the **private NAT gateway instance** that requires creating an SNAT rule, to enter the details page.
2. On the private NAT gateway instance details page, click the **SNAT Rules** tab > **Create** and enter the information such as mapping direction, mapping type, original IP, mapped IP, and remarks to complete the creation of the SNAT rule. The information of each tag is as follows.

Mapping direction:

Local: translates the private IP addresses of the VPC.

Peer: translates the private IP addresses of the network on the opposite end of the VPC. If the peer is an IDC network, the IP addresses of the IDC are translated.

Mapping type:

Layer-3: only translates the IP addresses.

Layer-4: maps IP addresses and ports to random ports within a specified IP pool.

Original IP: indicates the IP address to be translated. When the mapping direction is set to local, it is the IP address of the VPC; when the mapping direction is set to peer, it is the IP address of the machine within the IDC.

Mapped IP/Mapped IP pool: configures the translated IP/IP pool. The original IP can provide services through this mapped IP/IP pool.

3. After an SNAT rule is created, editing ACL rules is supported for local mapping, but not for peer mapping.

After configuring the SNAT rule, you must bind the NAT gateway on the Direct Connect side. To implement the above process, you can refer to the best practice document Connecting a Local IDC to CVM by Using a VPC NAT Gateway and Direct Connect**.**

Note:

SNAT rules cannot be duplicate.

SNAT rules do not support peer Layer-4.

Layer-3 rules have a higher priority than Layer-4 rules.

For the same ACL, the Layer-4 rule with a higher priority is matched first, and subsequent rules are not matched.

ACL rules can be hidden or shown under each rule, and support display in pages.

Cloud Connect Network (CCN)

The CCN type private NAT gateways mainly solve address translation between cross-region VPCs, and address translation between the VPC and Direct Connect IDC (e.g., from Beijing to Shanghai). They are used for cross-region access from the VPCs to other public network resources through the CCN.

Note:

When a private NAT gateway instance is created, if you select **CCN** for the associated instance, 2 VPCs will be automatically generated after the instance is created, and are used for route configuration during address translation. The 2 VPCs cannot be deleted separately. Their lifecycle is the same as that of the NAT gateway instance. They are respectively named Local VPC and Peer VPC, and both belong to the NAT gateway.

The CCN type private NAT gateways support FullNAT private network addresses. In multi-network scenarios connected through the CCN, please plan the local and peer networks before configuring the SNAT rules.

Local network: supports Layer-3 SNAT, Layer-4 SNAPT, and Layer-4 DNAT rules for the private IPs of this network.

Peer network: only supports Layer-3 SNAT for the private IPs of this network.

Note:

If the private IP addresses of both VPC and IDC networks are translated, the IDC is considered as the peer network and the VPC is the local network since IDC can only perform Layer-3 SNAT translation.

After planning the local and peer networks, you can take the following steps to create an SNAT rule:

1. Log in to the NAT Gateway console and click **Private NAT Gateway** in the left sidebar.
2. On the **private NAT gateway instance** list page, click on the **private NAT gateway instance** that requires creating an SNAT rule, to enter the details page.
3. On the **private NAT gateway instance** details page, click the **SNAT Rules** tab > **Create** and enter the information such as mapping direction, mapping type, original IP, mapped IP, and remarks. Then click **OK** to complete the creation of the SNAT rule. The information of each tag is as follows:

Mapping direction:

Local: translates the private IP addresses of the VPC.

Peer: translates the private IP addresses of the network on the opposite end of the VPC. If the peer is an IDC network, the IP addresses of the IDC are translated.

Mapping type:
Layer-3: only translates the IP addresses.
Layer-4: maps IP addresses and ports to random ports within a specified IP pool.
Original IP: indicates the IP address of the local subnet within the VPC, which needs to be translated.
Mapped IP/Mapped IP pool: configures the translated IP/IP Pool. The original IP can provide services through this mapped IP/IP pool.
4. After an SNAT rule is created, editing ACL rules is supported for local mapping, but not for peer mapping.
After configuring the SNAT rule, you must further configure the routing policies for 2 transit VPCs for the NAT gateway, to ensure the normal operation of the CCN type NAT gateway instance. The specific process is as follows:
1. Configure the routing policies for the 2 transit VPCs for the NAT gateway.
2. Create 2 custom route tables in the CCN, and respectively bind them to the 2 transit VPCs of the NAT gateway. After association, the routes of the transit VPCs will be published to the custom route tables in the CCN.
3. Add the border network 1 to the CCN and bind it to the CCN route table 1. Then add the border network 2 to the CCN and bind it to the CCN route table 2.
After configuration, the data flow is border network 1 > CCN > NAT local transit VPC > NAT peer transit VPC endpoint > CCN > border network 2.

Virtual Private Cloud (VPC)

The VPC type private NAT gateways mainly solve address translation of a specified subnet within a VPC. They are used to translate the private IP of the specified subnet within the VPC to a new IP for communication with other networks. To create an SNAT rule for this type of private NAT gateways, you can take the following steps.
1. Log in to the NAT Gateway console and click on the NAT gateway instance that requires creating an SNAT rule.
2. On the SNAT Rules tab, click **Create** and enter the information such as mapping type, original IP, mapped IP, and remarks to complete the creation of the SNAT rule. The information of each tag is as follows.
Mapping type:
Layer-3: only translates the IP addresses.
Layer-4: maps IP addresses and ports to random ports within a specified IP pool.
Original IP: indicates the original IP to be translated, such as the IP of a customer's local subnet. The specific original IP must be entered only for Layer-3, but is not required for Layer-4 (defaults to all IPs of the NAT's local subnet).
Mapped IP/Mapped IP pool: indicates the translated IP or IP range. For Layer-3 IP translation, enter the IP address; for Layer-4 IP and port translation, enter the IP range or IP address.
3. After an SNAT rule is created, editing ACL rules is supported.
There is an ACL rule under each SNAT rule, which is fully enabled by default. If you need to specify certain data flows for matching the NAT rule, you can set the ACL rule. If all packets should match the NAT rule, no action is needed. The ACL rules can be hidden or shown under each rule, and support display in pages.

Modifying an SNAT Rule

1. Log in to the NAT Gateway console and click on the **private NAT gateway instance** that requires editing the SNAT rules.
2. On the **private NAT gateway instance** details page**,** click the **SNAT Rules** tab. On the right side of the SNAT rule entry, click **Modify** to enter the edit dialog box.
3. Modify the original IP address, mapped IP/IP pool, or description in the SNAT rule, and then click **OK** to complete the modification.

Querying SNAT Rules

1. Log in to the NAT Gateway console and click on the **private NAT gateway instance** that requires querying the SNAT rules.
2. On the **private NAT gateway instance** details page**,** click the **SNAT Rules** tab > **SNAT List**. In the search box at the top right, click to select the filter criteria. It supports query by original IP and mapped IP.
3. Click on

for quick search.

Deleting SNAT Rules

Single Deletion

1. Log in to the NAT Gateway console and click on the **private NAT gateway instance** that requires editing the SNAT rules.
2. On the **private NAT gateway instance** details page, click the **SNAT Rules** tab, and then click **Delete** on the right side of the SNAT rule entry.
3. Click **Confirm** to delete the selected SNAT rule.

Batch Deletion

1. Log in to the NAT Gateway console and click on the **private NAT gateway instance** that requires editing the SNAT rules.
2. On the **private NAT gateway instance** details page, click the **SNAT Rules** tab, select multiple SNAT rules, and click **Delete** at the top.
3. In the pop-up window, click **Delete** to complete batch deletion.

Managing DNAT Rules

Last updated：2024-08-01 14:17:17

The DNAT (Destination Network Address Translation) feature supports mapping the **private IPs**, **protocols**, and **ports** of CVMs within a VPC to **other IPs**, **protocols**, and **ports**, thereby enabling the resources on the CVMs to be accessed by other networks, with their original addresses hidden.

Creating DNAT Rules

1. Log in to the NAT Gateway console and click **Private NAT Gateway** in the left sidebar.
2. On the **private NAT gateway** list page, click the **private NAT gateway instance** for which you need to query the DNAT rules, to enter the details page.
3. On the **private NAT gateway** instance details page, click the **DNAT** tab > **Create**, select the protocol, original IP, original port, mapped IP, and mapped port, and then click **Confirm**.

Original IP and original port: indicate the IP address and port of the local subnet in the VPC, namely the IP address and port to be translated.

Mapped IP and mapped port: indicate the translated IP and port. The original IP and port provide services through this mapped IP and port.

Only active access from the peer network to the VPC is supported. The peer network must access the mapped IP and port to communicate with the original IP and port in the VPC. Response packets are not affected.

The range for original ports and mapped ports is 1-65,535.

Batch adding supports up to 50 rules in each batch. If there are many rules, you can add them in multiple batches.

Querying DNAT Rules

1. Log in to the NAT Gateway console and click **Private NAT Gateway** in the left sidebar.
2. On the **private NAT gateway** list page, click the **private NAT gateway instance** for which you want to query the DNAT rules, to enter the details page.
3. On the **private NAT gateway** instance details page, click the **DNAT** tab. In the search box on the right, you can query by protocol, original IP, original port, mapped IP, and mapped port.

Modifying DNAT Rules

1. Log in to the NAT Gateway console and click **Private NAT Gateway** in the left sidebar.

2. On the **private NAT gateway** list page, click the **private NAT gateway instance** for which you want to modify the DNAT rules, to enter the details page.
3. On the **private NAT gateway** instance details page, click the **DNAT** tab, select a specific DNAT rule, and click **Modify** in the **Operation** column. Then you can modify the corresponding rule based on the protocol, original IP, original port, mapped IP, and mapped port.

Deleting DNAT Rules

Deleting DNAT rules supports **Single Deletion** and **Batch Deletion**.
Single Deletion:
1. Log in to the NAT Gateway console and click **Private NAT Gateway** in the left sidebar.
2. On the **private NAT gateway** list page, click the **private NAT gateway instance** for which you want to delete the DNAT rules, and enter the details page.
3. On the **private NAT gateway** instance details page, click the **DNAT** tab, select a specific DNAT rule, and click **Delete** in the **Operation** column to delete the corresponding single rule.
Batch Deletion:
On the **private NAT gateway** instance details page, click the **DNAT** tab, select multiple DNAT rules on the left side, and click **Delete** above the list to batch delete the DNAT rules.

Cloud Access Management

Last updated：2024-08-01 14:15:20

Overview

Through the Cloud Access Management (CAM) policies, users can be granted with the permissions to view and use specific resources in the console. This document provides examples of the permissions to view and use specific resources of a private NAT gateway, for guiding the users on how to use the policies for specific parts of the console.

Authorization Definition

Resources Supporting Private NAT Gateway Authorization in CAM

Resource Type	Resource Description Method in Authorization Policies
NAT gateway instances	`qcs::vpc:{region_short_name}:uin/{Uin}:nat/{NatGatewayId}`
NAT gateway APIs	qcs::vpc:{region_short_name}:uin/{Uin}:nat/*

Where:

All `{region_short_name}` should be the ID of a certain region or empty.

All `{Uin}` should be the AccountId of the resource owner or empty.

All `{NatGatewayId}` should be the ID of a NAT instance or empty.

Others can be deduced similarly.

APIs Supporting Private NAT Gateway Authorization in CAM

In CAM, you can authorize the following actions for a NAT resource.

API Action	Resource Description	API Description
CreatePrivateNatGateway	Creates private NAT gateways.	qcs::vpc:$region:$account:in qcs::vpc:$region:$account:vp
DeletePrivateNatGateway	Deletes private	qcs::vpc:$region:$account:in

	NAT gateways.	
ModifyPrivateNatGatewayAttribute	Modifies private NAT gateway attributes.	qcs::vpc:$region:$account:in
DescribePrivateNatGateways	Queries private NAT gateways.	qcs::vpc:$region:$account:in
DescribePrivateNatGatewayLimits	Queries the number limit for creating private NAT gateways.	qcs::vpc:$region:$account:in qcs::vpc:$region:$account:vp
CreatePrivateNatGatewayTranslationNatRule	Creates the private NAT gateway's source port translation rules.	qcs::vpc:$region:$account:in
DeletePrivateNatGatewayTranslationNatRule	Deletes the private NAT gateway's source port translation rules.	qcs::vpc:$region:$account:in
ModifyPrivateNatGatewayTranslationNatRule	Modifies the private NAT gateway's source port translation rules.	qcs::vpc:$region:$account:in
DescribePrivateNatGatewayTranslationNatRules	Queries	qcs::vpc:$region:$account:in

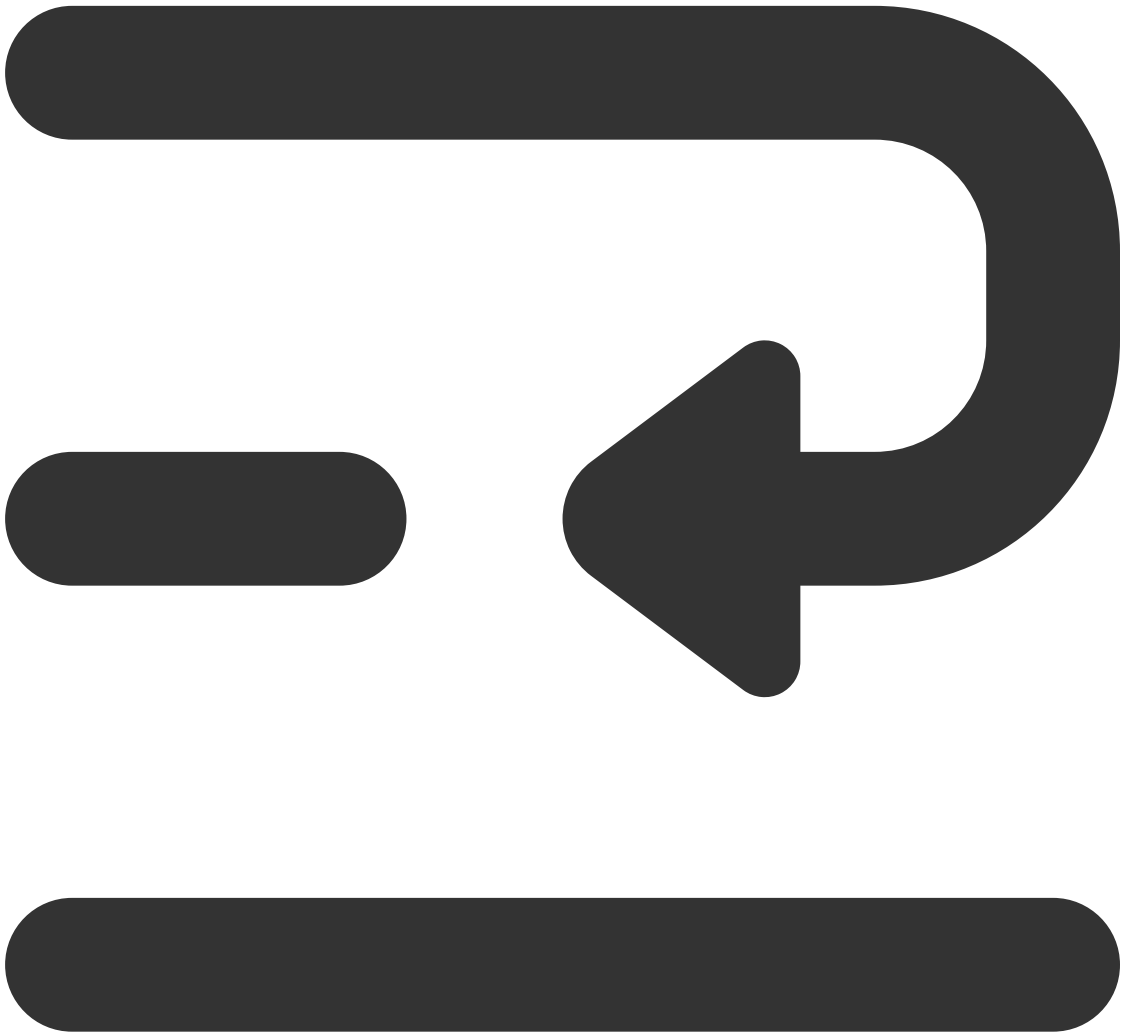
	the private NAT gateway's source port translation rules.	
CreatePrivateNatGatewayTranslationAclRule	Creates the private NAT gateway's source port access control rules.	qcs::vpc:$region:$account:in
DeletePrivateNatGatewayTranslationAclRule	Deletes the private NAT gateway's source port access control rules.	qcs::vpc:$region:$account:in
ModifyPrivateNatGatewayTranslationAclRule	Modifies the private NAT gateway's source port access control rules.	qcs::vpc:$region:$account:in
DescribePrivateNatGatewayTranslationAclRules	Queries the private NAT gateway's source port access control rules.	qcs::vpc:$region:$account:in
CreatePrivateNatGatewayDestinationIpPortTranslationNatRule	Creates the private NAT	qcs::vpc:$region:$account:in

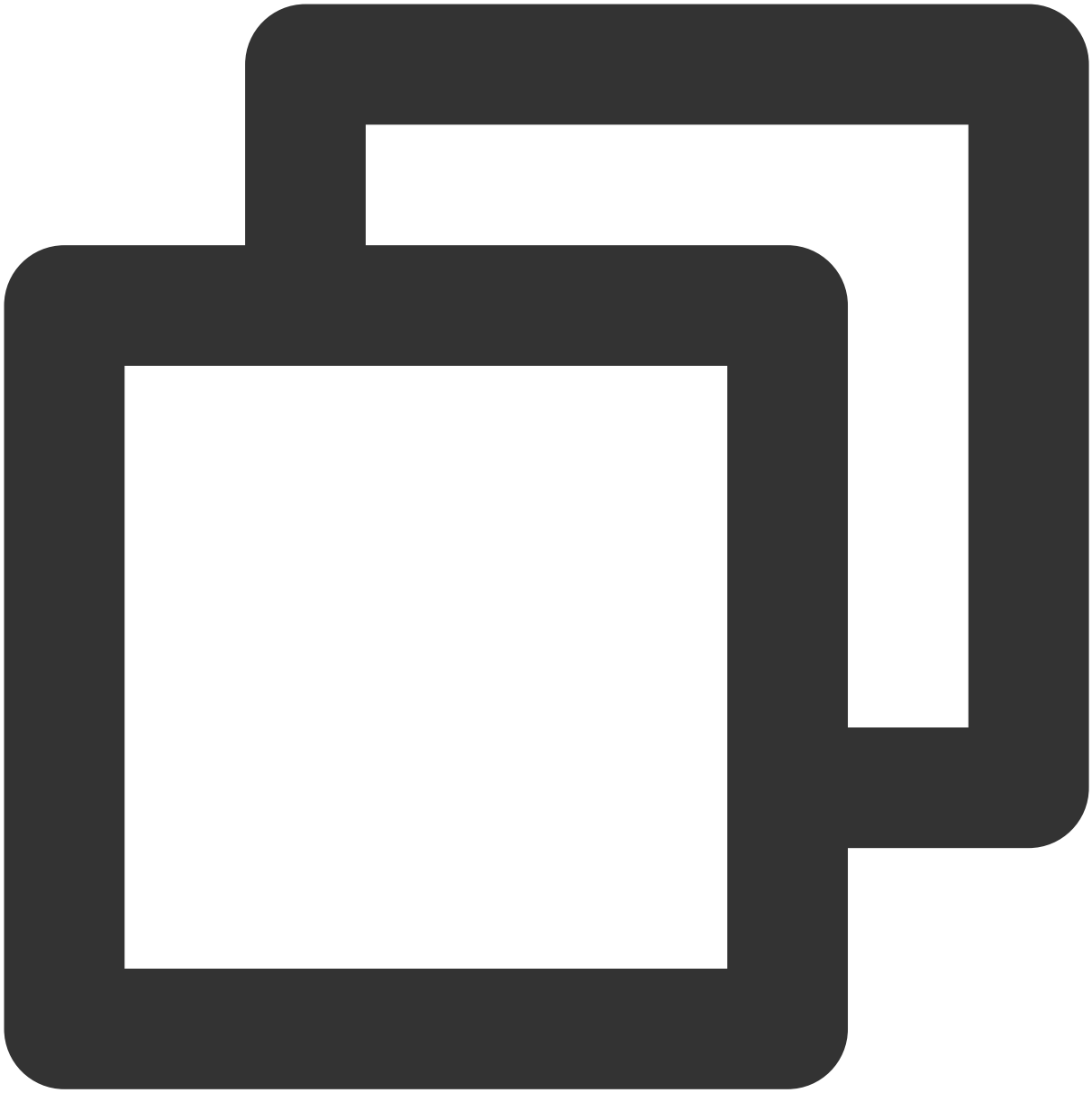
	gateway's destination port translation rules.	
DeletePrivateNatGatewayDestinationIpPortTranslationNatRule	Deletes the private NAT gateway's destination port translation rules.	qcs::vpc:$region:$account:in
ModifyPrivateNatGatewayDestinationIpPortTranslationNatRule	Modifies the private NAT gateway's destination port translation rules.	qcs::vpc:$region:$account:in
DescribePrivateNatGatewayDestinationIpPortTranslationNatRules	Queries the private NAT gateway's destination port translation rules.	qcs::vpc:$region:$account:in
DescribePrivateNatGatewayRegions	Queries the supported regions for the private NAT gateway.	qcs::vpc:$region:$account:in

Sample Policies

Full Read-Write Policy for All NAT Gateways

Grant a sub-account with full administrative permissions for the NAT service, including creation, management, and all other operations.



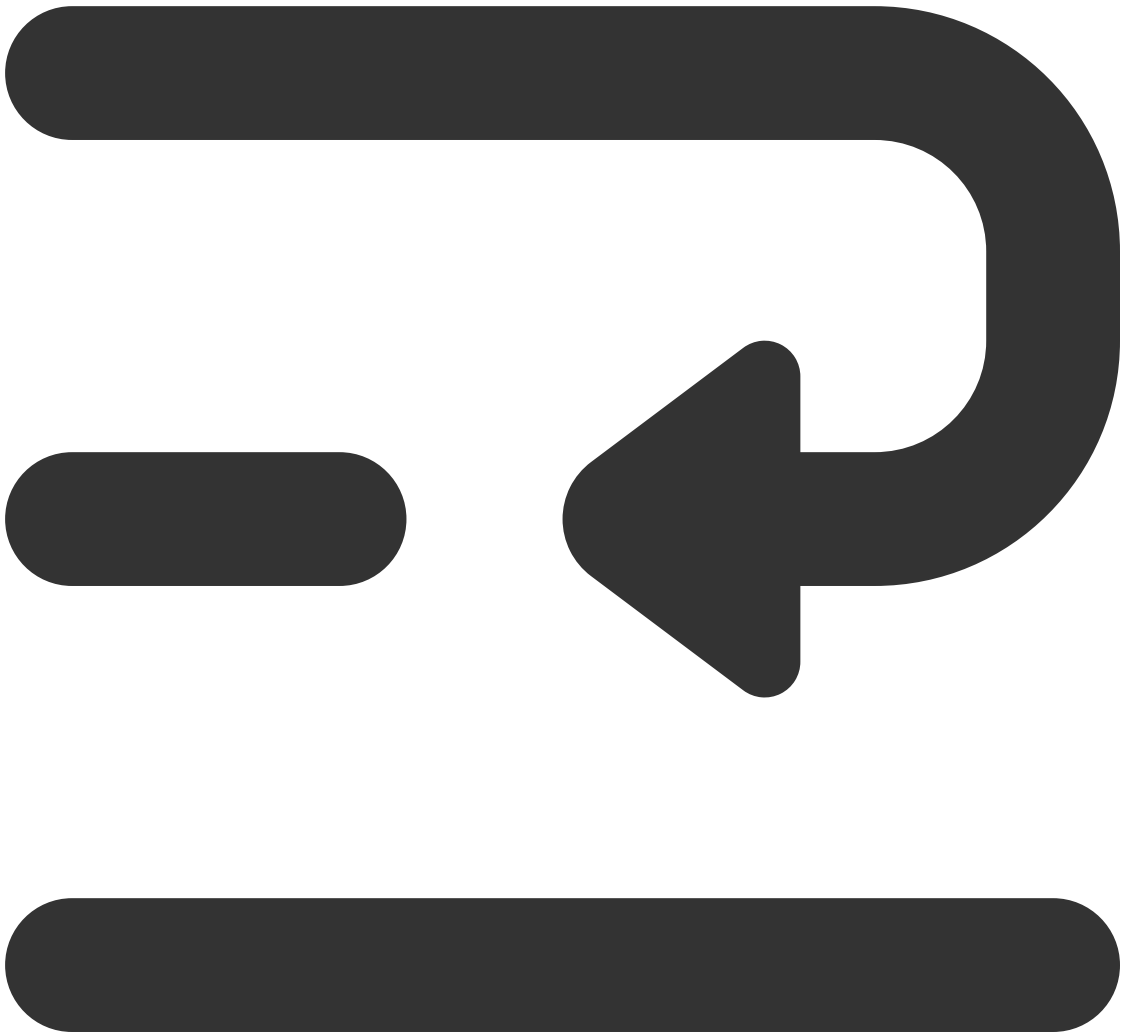


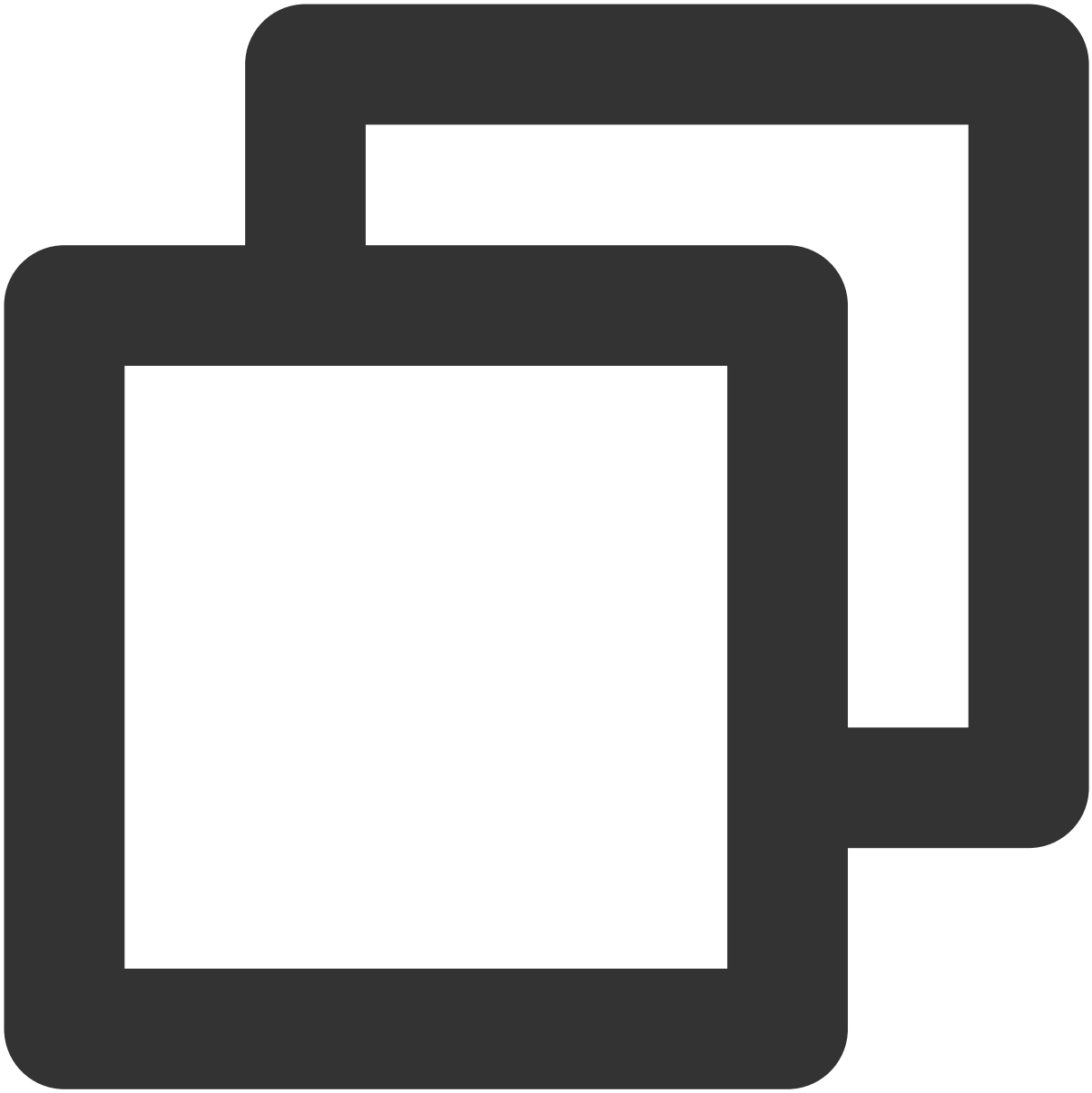
```
{
"version": "2.0",
"statement": [{
"action": [
"vpc:*"
],
"resource": "qcs::vpc::$uin:nat/*",
"effect": "allow"
}]}
{
"version": "2.0",
```

```
"statement": [{
"action": [
"vpc:*"
],
"resource": "qcs::vpc::$uin:intranat/*",
"effect": "allow"
}]}
```

Read-Only Policy

Grant a sub-account with the read-only access permission for NAT gateways.

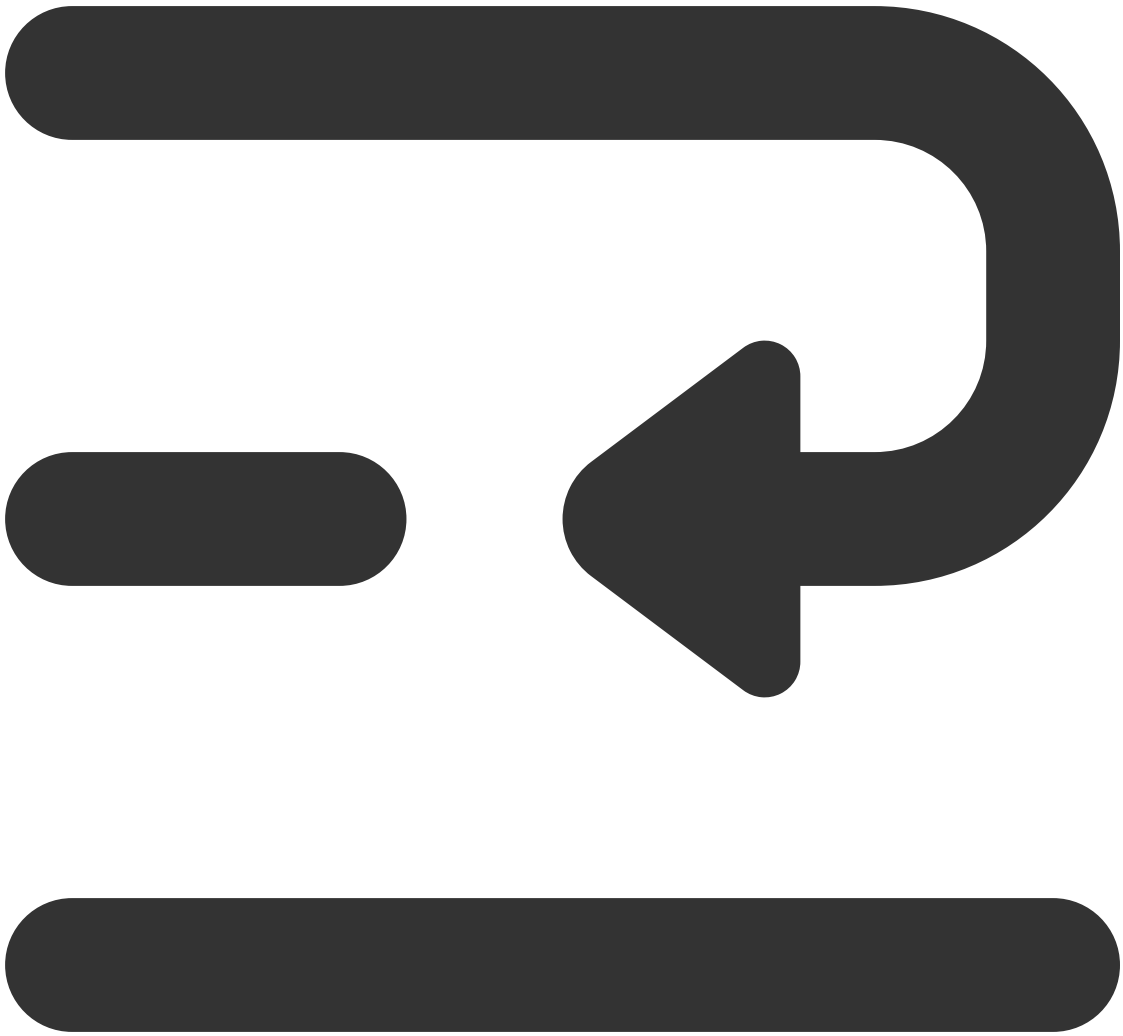


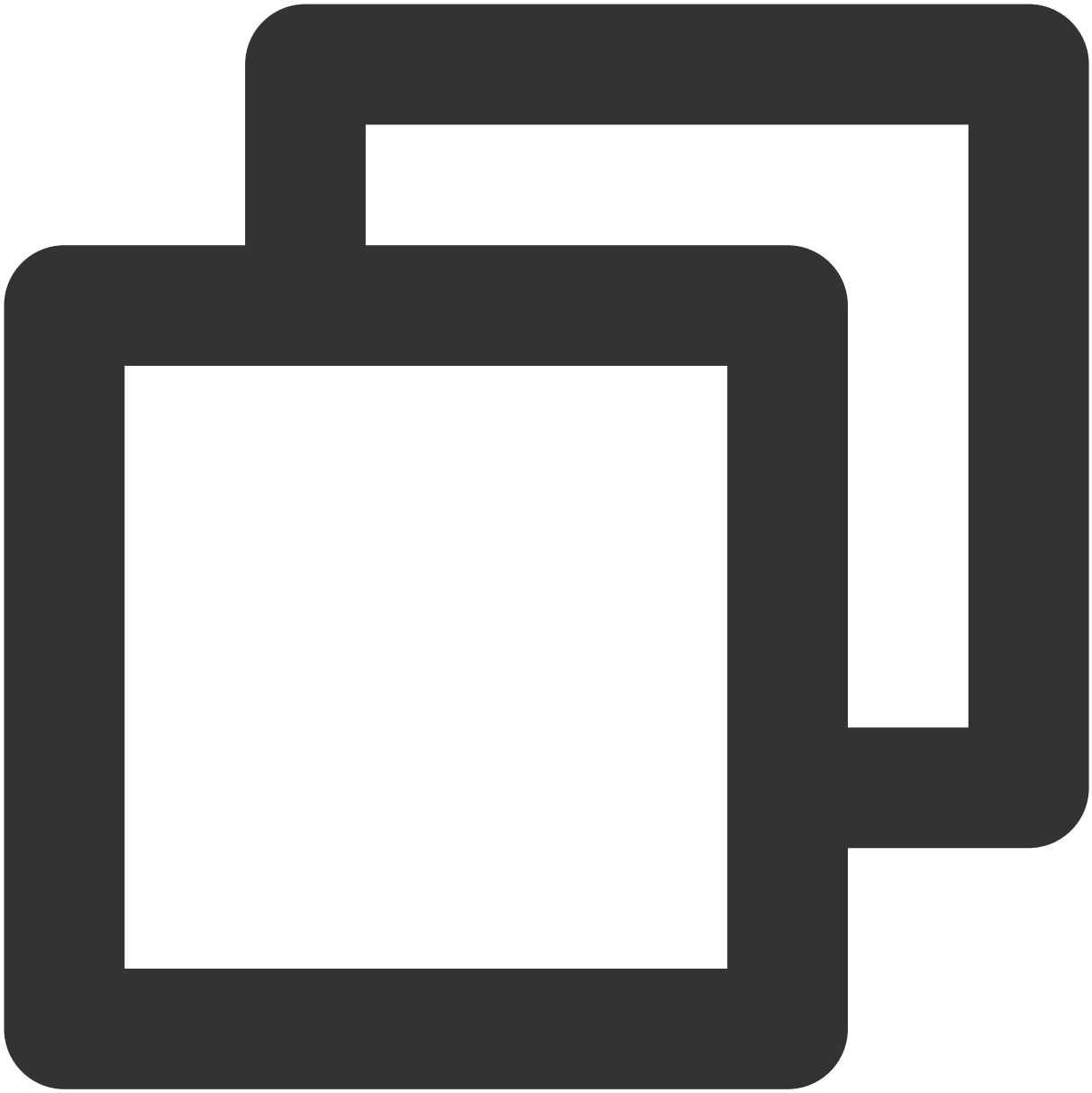


```
{
"version": "2.0",
"statement": [{
 "action": [
 "vpc:Describe*"
 ],
  "resource": "qcs::vpc::$uin:nat/*",
  "effect": "allow" }]}
{
"version": "2.0",
 "statement": [{
```

```
"action": [
"vpc:Describe*"
],
"resource": "qcs::vpc::$uin:intranat/*",
"effect": "allow"
}]}
```

Full Read-Write Policy for a NAT Gateway Under a Specific Tag





```
{
"version":"2.0",
"statement":[{
"effect":"allow",
"action":"*",
"resource":"*",
"condition":{
"for_any_value:string_equal":{
"qcs:tag":[
"tagkey&tagvalue"
]}}}]}
```