



NAT Gateway

Product Documentation





Contents

NAT Gateway 3

- Product Introduction 3
 - NAT Gateway Overview 3
 - Features 6
 - Use Cases 8
 - Product Specifications 11
 - Relevant Products 14
 - Use Limits 16
- Purchase Guide 17
 - Public NAT Gateway Overview 17
 - Private NAT Gateway Operation Guide 23
 - Purchasing NAT Gateway in Console 26
 - NAT Gateway Overdue Payments 27
 - Billing Overview 28
- Operation Guide 30
 - Configuring a Route Pointing to the NAT Gateway 30
 - Adjusting the Priority of NAT Gateway and EIP 31
 - Managing Port Forwarding Rules 33
 - Creating Port Forwarding Rules 33
 - Querying Port Forwarding Rules 34
 - Modifying NAT Gateway Configuration 35
 - Managing NAT Gateway EIPs 36
 - Managing SNAT Rules 39
 - Viewing Monitoring Information 43
 - Setting Alarms 44
 - Deleting a NAT Gateway 45
- Quick Start 46
- Glossary 49

Product Introduction

NAT Gateway Overview

NAT Gateway is a service that supports IP address translation and provides SNAT (Source Network Address Translation) and DNAT (Destination Network Address Translation) capabilities, which can provide secure and high-performance internet access services for resources within a VPC. NAT Gateway supports up to 99.99% high availability, 5Gbps bandwidth, and more than 10 million concurrent connections. Its typical use cases are as follows:

NAT Gateway supports:

- High availability: up to 99.99%
- Bandwidth: 5 Gbps
- Concurrent connections: more than 10 million

Typical Application Scenarios

- Large bandwidth public network egress: For services such as web crawlers and accessing Internet public services.
- Secure public network egress: When a CVM needs to communicate with the Internet but should not be assigned a public IP for security reasons.

Network Topology

When resources in a VPC (e.g., CVMs) send outbound data packets through the NAT Gateway:

1. Packets first travel through the router.
2. They are then routed according to the routing policy.
3. The NAT Gateway sends the traffic to the Internet using the bound EIP as the source IP.

NAT Gateway vs. Public Gateway

CVMs in a VPC can access the Internet through either a NAT Gateway or a Public Gateway. The differences are summarized below:



Attribute	NAT Gateway	Public Gateway
Availability	Master/Slave hot backup with automatic failover	Manual switching required for failure
Public network bandwidth	Up to 5 Gbps	Depends on CVM network bandwidth
Public IP address	Up to 10 EIPs can be bound	Supports one EIP or ordinary public IP
Rate limit	5 Gbps (up to 50 Gbps with support request)	Depends on CVM
Max concurrent connections	10,000,000	500,000
Private IP usage	VPC private IPs are not consumed	Subnet private IPs are consumed
Security group support	Cannot bind directly; bind to backend CVM instead	Binding supported
Network ACL support	Cannot bind directly; bind to subnet of backend CVM	Cannot bind directly; bind to subnet of public gateway
Fees	Philippines: • Small (up to 1M connections): \$0.09/hr • Medium (up to 3M connections): \$0.27/hr • Large (up to 10M connections): \$0.89/hr	Only CVM fees apply; no extra gateway fee

Advantages of NAT Gateway

1. Large Capacity

Supports up to 10 million concurrent connections, 5 Gbps bandwidth, and 10 EIPs — ideal for large-scale operations.

2. High Availability

Automatic failover ensures disaster recovery and 99.99% service availability, superior to manual public gateway switching.



3. Cost Effectiveness

Three configurations (small, medium, large) allow flexible billing and high cost-efficiency.

Features

Converge Cloud NAT Gateway maps EIPs and ports to the private IPs and ports of CVM instances, allowing VPC CVMs without public IPs to access and be accessed over the public network.

It provides a rich set of features, including:

- Source Network Address Translation (SNAT)
- Destination Network Address Translation (DNAT)
- Gateway traffic control
- Traffic alarms
- Bandwidth packages
- Anti-DDoS protection
- Automatic disaster recovery

SNAT (Source Network Address Translation)

- SNAT enables multiple CVMs in a VPC to access the public network through the same public IP address.
- A single NAT Gateway supports a maximum forwarding capacity of 5 Gbps.
- You can bind multiple EIPs to the NAT Gateway, allowing CVMs to access the public network through random EIPs.
- To specify a particular EIP for public network access, add it to the SNAT address pool to ensure CVMs only use the designated EIP.

DNAT (Destination Network Address Translation)

- DNAT maps public IP addresses, protocols, and ports to the private IPs, protocols, and ports of CVMs in the VPC.
- This allows services hosted on CVMs to be accessible from the Internet.

Bandwidth Packages

- NAT Gateway can be paired with IP bandwidth packages to share public network bandwidth among



multiple IPs.

- After binding EIPs to the NAT Gateway and adding them to bandwidth packages, applications with staggered traffic can effectively reduce bandwidth costs.

Gateway Traffic Control

- Traffic control can be enabled to manage bandwidth from a private IP to the NAT Gateway.
- Provides visual monitoring at the IP-gateway level, helping network operations personnel track traffic patterns.
- Supports IP-level speed limiting to block unhealthy traffic and protect key services.

Traffic Alarm

- Custom traffic alarms can be configured for NAT Gateway metrics.
- Notifications are sent automatically via email or SMS when thresholds are exceeded.
- Monitoring and alarms are free, helping you quickly identify and resolve issues.

Anti-DDoS Protection

- Anti-DDoS Pro defends against DDoS and CC attacks with up to 310 Gbps protection bandwidth.
- You can bind an Anti-DDoS Pro instance to the NAT Gateway to enhance security.

Automatic Disaster Recovery

- NAT Gateway features dual-server hot backup and automatic disaster recovery.
- Services on a failed server are seamlessly switched to the backup server.
- Ensures up to 99.99% availability, maintaining service stability for critical applications.

Use Cases

Converge Cloud NAT Gateway addresses diverse networking requirements across various business scenarios. Below are common use cases that demonstrate how organizations leverage NAT Gateway to optimize their cloud infrastructure.

Secure Internet Access for Private Instances

Organizations often deploy application servers, database instances, and backend services within private subnets for enhanced security. NAT Gateway enables these private instances to initiate outbound connections to the internet for software updates, patch management, API calls to external services, and data synchronization—all without exposing them to inbound internet traffic.

Example: An e-commerce platform runs its inventory management system on private CVMs that need to fetch product data from supplier APIs while remaining isolated from direct internet access for security compliance.

High-Volume Web Scraping and Data Collection

Businesses requiring large-scale data aggregation from public sources benefit from NAT Gateway's high throughput and concurrent connection capacity. The service supports up to 10 million simultaneous connections and 5 Gbps bandwidth, making it ideal for data-intensive operations.

Example: A market research firm operates multiple web crawlers that collect pricing information from thousands of e-commerce websites daily, requiring stable, high-bandwidth outbound connectivity.

Multi-Tier Application Architecture

Modern cloud applications often implement multi-tier architectures with presentation, application, and data layers. NAT Gateway facilitates secure internet connectivity for middle-tier services that need external access without direct public IP exposure.

Example: A SaaS platform uses NAT Gateway to enable its application tier to send transactional emails, process payment gateway requests, and integrate with third-party analytics services while maintaining a secure network perimeter.

Centralized Internet Gateway for Multiple Workloads

Organizations with numerous CVM instances can consolidate internet egress through a single NAT Gateway, simplifying network management and reducing IP address consumption. This approach enables centralized traffic monitoring, logging, and security policy enforcement.

Example: A digital agency manages 50+ client websites on separate CVM instances, using NAT Gateway to provide shared internet access while maintaining individual traffic monitoring and cost allocation per client.

Development and Testing Environments

Development teams require internet access for downloading packages, accessing version control repositories, and integrating with CI/CD pipelines, but shouldn't expose development instances directly to the internet. NAT Gateway provides the necessary connectivity while maintaining environment isolation.

Example: A software development company uses NAT Gateway to allow its staging and development CVMs to pull Docker images, access npm registries, and connect to GitHub while keeping these non-production environments secured.

Hybrid Cloud Connectivity

Enterprises operating hybrid cloud architectures use NAT Gateway to facilitate controlled internet access for cloud resources that communicate with on-premises systems, enabling seamless integration without compromising security boundaries.

Example: A financial institution extends its on-premises infrastructure to Converge Cloud, using NAT Gateway to enable cloud-based analytics workloads to access external market data feeds while maintaining strict network segmentation.

Public-Facing Services with IP Preservation

DNAT functionality allows organizations to host publicly accessible services behind NAT Gateway while preserving the ability to map specific ports and protocols. This enables hosting multiple services across



different CVMs using a consolidated set of public IPs.

Example: A media company hosts multiple customer portals, each running on separate CVMs with different private IPs, but presents them all through a unified set of public EIPs via DNAT port mapping configurations.

Cost-Optimized Bandwidth Management

Organizations with variable traffic patterns leverage NAT Gateway's bandwidth package integration to share capacity across multiple applications, reducing costs by avoiding over-provisioning individual instance bandwidth.

Example: An online education platform experiences peak traffic during evening hours while B2B services peak during business hours, using bandwidth packages with NAT Gateway to optimize costs through time-shifted traffic patterns.

Compliance and Audit Requirements

Industries with strict regulatory requirements use NAT Gateway to create auditable, controlled internet access points. Centralized egress simplifies logging, monitoring, and compliance reporting for data protection regulations.

Example: A healthcare provider uses NAT Gateway as the single internet egress point for all systems processing patient data, enabling comprehensive traffic logging and audit trails for HIPAA compliance.

High-Availability Critical Applications

Mission-critical applications requiring guaranteed uptime leverage NAT Gateway's 99.99% availability SLA and automatic failover capabilities to ensure continuous internet connectivity without manual intervention during infrastructure failures.

Example: An IoT platform managing thousands of connected devices uses NAT Gateway to ensure its cloud-based control plane maintains uninterrupted internet connectivity for device communication and telemetry collection.



Product Specifications

Converge Cloud NAT Gateway offers various packages based on product features and specifications. It is classified into:

- Public NAT Gateway
- Private NAT Gateway

Public NAT Gateway

Public NAT Gateway allows multiple CVMs without public IPs in the VPC to:

- Actively access the public network.
- Map EIPs and ports to CVM private IPs and ports so that CVMs can be accessed from the public network.

Public NAT Gateway is further divided into:

- Traditional NAT Gateway
- Standard NAT Gateway

Note:

Standard NAT Gateway is currently in beta testing in the Philippines. To use it, please submit a request ticket. Traditional NAT Gateway includes the original Small, Medium, and Large NAT Gateways. After activating Standard NAT Gateway, the original NAT Gateway types are automatically renamed: - Traditional NAT Gateway – Small - Traditional NAT Gateway – Medium - Traditional NAT Gateway – Large If Standard NAT Gateway is not activated, the console experience remains unchanged.

Comparison: Standard NAT Gateway vs Traditional NAT Gateway

Comparison Item	Standard NAT Gateway	Traditional NAT Gateway
High availability	Natively supports multi-AZ disaster recovery	Achieves cross-availability zone disaster recovery via rapid migration



Comparison Item	Standard NAT Gateway	Traditional NAT Gateway
Gateway specification	Supports 2,000,000 concurrent connections, 100,000 new connections/sec, 5 Gbps BW cap	Supports Small (up to 1,000,000 connections), Medium (up to 3,000,000), Large (up to 10,000,000). Peak outbound BW options: 10, 20, 50, 100, 200, 500, 1,000, 2,000, 5,000 Mbps. Max inbound BW: 5,000 Mbps by default
Gateway fee	Instance fee + CU (Capacity Unit) fee: • Instance fee: charged hourly • CU fee: based on actual performance	Same calculation method as Standard NAT Gateway
ECMP	Supported	Supported
Gateway traffic control	Not yet supported	Supported
Gateway traffic logs	Not yet supported	Supported

Note:

- Public NAT Gateway supports binding up to 10 EIPs. - For SNAT, max connections for the same protocol/destination IP/port = number of bound EIPs × 55,000. Bind new EIPs or adjust destination IP/port to increase connections. - Hybrid ECMP between Standard and Traditional NAT Gateways is not supported. - For other specifications or feature requests, submit a ticket.

Private NAT Gateway

Private NAT Gateway enables CVMs in the VPC to:

- Access other VPCs (public or private).
- Be accessed from public VPCs.

**Note:**

Private NAT Gateway is currently in beta testing in the Philippines. To use it, please submit a request ticket.

Relevant Products

Converge Cloud NAT Gateway interacts with several network products to provide flexible and secure public network access for CVM instances.

EIP (Elastic IP)

The NAT Gateway and EIPs are two ways for a CVM instance to access the public network. You can use either or both in your public network architecture.

Method 1: Using NAT Gateway Only

- CVM instances without a public IP access the public network through the NAT Gateway's public IP.
- Traffic to the public network is forwarded via the private network to the NAT Gateway.

Method 2: Using EIP Only

- CVM instances access the public network directly using EIPs, without a NAT Gateway.
- Traffic to the public network is forwarded from the EIP.

Method 3: Using NAT Gateway and EIP

- CVM instances are bound with an EIP, and the route table directs all subnet traffic to the public network through the NAT Gateway.
- Traffic from the CVM to the public network goes through the NAT Gateway via the private network, and response packets return through the NAT Gateway.
- To use the EIP for public network access, you can adjust the priorities of NAT Gateways and EIPs.
- Traffic from the public network that uses the EIPs to access CVMs will have the CVM response packets returned through the EIPs.

Note:

For more information about EIPs, see the Elastic IP product documentation.

Bandwidth Package

- If a NAT Gateway is bound with multiple EIPs, you can add them to an IP bandwidth package.



- This allows bandwidth sharing across multiple IPs and helps reduce public network costs.

Note:
For more details, see the [Converge Cloud Product Overview](#).

Other Related Products

Product Name	Relationship with NAT Gateway
CVM	NAT Gateway and EIP are two ways for CVM instances to access the Internet
EIP	EIP and NAT Gateway are two ways for CVM instances to access the Internet
VPC	NAT Gateway is part of the VPC
Route Table	After creating a NAT Gateway, configure routing policies to direct subnet traffic to the NAT Gateway
Public Gateway	A CVM with forwarding enabled; can be accessed by NAT Gateway
Anti-DDoS Pro	Can be bound to a NAT Gateway to defend against DDoS and CC attacks
Network ACL	Allows fine-grained control over inbound and outbound traffic of subnets



Use Limits

Note the following when you use a NAT Gateway:

- When a user deletes a NAT Gateway, its EIP is disassociated, but the EIP is not released from the user account.
- Users cannot associate a security group with a NAT Gateway but can bind a security group to instances in a private subnet to control traffic in and out of these instances.
- Users cannot use network ACLs directly to control traffic in and out of a NAT Gateway but can use network ACLs to control traffic in and out of the subnet associated with the NAT Gateway.
- Users cannot route traffic to a NAT Gateway through a VPC peering connection, VPN connection, or Direct Connect because the resources on the other end of such connections cannot use a NAT Gateway.

For example, all traffic from VPC 1 to the internet can be sent through the NAT Gateway. VPC 1 and VPC 2 have established a peering connection. All resources in VPC 2 can access all resources in VPC 1, but all resources in VPC 2 cannot access the internet through the NAT Gateway.

- NAT Gateway supports TCP, UDP, and ICMP protocols, but ESP and AH used by GRE tunnel and IPSec cannot use NAT Gateway and ALG-related technologies are not supported yet. This is determined by the features of the NAT Gateway itself and has nothing to do with the service provider. However, most internet applications are TCP applications, and TCP and UDP applications together account for 99% of internet application types.
- The resource limits supported by the NAT Gateway are shown in the following table.

Note:

Users can request higher quotas for certain resources as indicated in the table below.

Resources	Limit	Can request for high quota
Number of NAT Gateways Supported by Each VPC	3	No
Number of Elastic IPs Supported by Each NAT Gateway	10	Yes
Maximum Forwarding Capacity Supported by Each NAT Gateway	5Gbps	No
Maximum Port Forwarding Entries Per NAT Gateway	200	Yes



Purchase Guide

Public NAT Gateway Overview

Converge Cloud NAT Gateway maps EIPs and ports to the private IPs and ports of CVM instances, allowing VPC CVMs without public IPs to access and be accessed over the public network.

It provides a rich set of features, including:

- Source Network Address Translation (SNAT)
- Destination Network Address Translation (DNAT)
- Gateway traffic control
- Traffic alarms
- Bandwidth packages
- Anti-DDoS protection
- Automatic disaster recovery

SNAT (Source Network Address Translation)

- Enables multiple CVMs in a VPC to access the public network through the same public IP address.
- Maximum forwarding capacity: 5 Gbps per NAT Gateway.
- Multiple EIPs can be bound to the NAT Gateway, allowing CVMs to access the public network through any of them.
- To specify a particular EIP for public network access, add it to the SNAT address pool.

DNAT (Destination Network Address Translation)

- Maps public IP addresses, protocols, and ports to the private IPs, protocols, and ports of CVMs in the VPC.
- Allows services hosted on CVMs to be accessible from the internet.

Bandwidth Packages

- NAT Gateway can be paired with IP bandwidth packages to share public network bandwidth among



multiple IPs.

- After binding EIPs to the NAT Gateway and adding them to bandwidth packages, applications with staggered traffic can reduce bandwidth costs.

Gateway Traffic Control

- Traffic control can manage bandwidth from a private IP to the NAT Gateway.
- Supports IP-level speed limiting and visual monitoring to protect key services.

Traffic Alarm

- Custom traffic alarms can be configured for NAT Gateway metrics.
- Notifications are sent automatically via email or SMS when thresholds are exceeded.
- Monitoring and alarms are free to help identify and resolve issues quickly.

Anti-DDoS Protection

- Anti-DDoS Pro defends against DDoS and CC attacks with up to 310 Gbps protection bandwidth.
- An Anti-DDoS Pro instance can be bound to the NAT Gateway to enhance security.

Automatic Disaster Recovery

- NAT Gateway features dual-server hot backup and automatic disaster recovery.
- Services on a failed server are seamlessly switched to the backup server.
- Ensures up to 99.99% availability for critical applications.

Use Cases

1. Secure Internet Access for Private Instances



- Private CVMs can initiate outbound internet connections without exposing them to inbound traffic.
- Example: E-commerce platform fetching supplier API data securely.

2. High-Volume Web Scraping and Data Collection

- Supports up to 10 million simultaneous connections and 5 Gbps bandwidth.
- Example: Market research firm operating web crawlers for pricing data.

3. Multi-Tier Application Architecture

- Middle-tier services can access external APIs without direct public IPs.
- Example: SaaS platform processing payment gateways and analytics.

4. Centralized Internet Gateway for Multiple Workloads

- Simplifies network management and reduces IP address consumption.
- Example: Digital agency managing 50+ client websites.

5. Development and Testing Environments

- Provides internet access for CI/CD pipelines without exposing non-production CVMs.
- Example: Software development company accessing Docker, npm, GitHub.

6. Hybrid Cloud Connectivity

- Enables cloud resources to communicate with on-premises systems securely.
- Example: Financial institution accessing market data feeds from cloud analytics workloads.

7. Public-Facing Services with IP Preservation

- DNAT allows multiple services behind NAT Gateway using a single set of public IPs.
- Example: Media company hosting multiple customer portals on separate CVMs.

8. Cost-Optimized Bandwidth Management

- Bandwidth package integration reduces over-provisioning costs.
- Example: Online education platform optimizing traffic based on peak hours.

9. Compliance and Audit Requirements

- Centralized internet egress allows traffic logging and auditing for regulations like HIPAA.
- Example: Healthcare provider ensuring secure patient data processing.

10. High-Availability Critical Applications

- Automatic failover ensures continuous internet connectivity.



- Example: IoT platform managing thousands of devices.

NAT Gateway Packages

Public NAT Gateway

- Allows CVMs without public IPs to access the internet and be accessed via mapped EIPs.
- Types:
 - Traditional NAT Gateway: Small, Medium, Large
 - Standard NAT Gateway: Beta in the Philippines (requires request)

Notes:

- Public NAT Gateway supports up to 10 EIPs.
- SNAT max connections = # of EIPs × 55,000.
- Hybrid ECMP between Standard and Traditional not supported.

Comparison: Standard vs Traditional NAT Gateway

Item	Standard NAT Gateway	Traditional NAT Gateway
High availability	Multi-AZ disaster recovery	Cross-AZ via rapid migration
Gateway specification	2,000,000 concurrent connections, 5 Gbps	Small: 1M, Medium: 3M, Large: 10M connections; peak outbound: 10–5,000 Mbps
Gateway fee	Instance fee + CU fee (hourly, postpaid)	Instance fee + network fee
ECMP	Supported	Supported
Gateway traffic control	Not yet supported	Supported
Gateway traffic logs	Not yet supported	Supported

Private NAT Gateway

- Enables CVMs to access other VPCs and be accessed from public VPCs.
- Beta in the Philippines (requires request).

Network Products Related to NAT Gateway

- EIP (Elastic IP): Alternative or combined public network access with NAT Gateway.
- Bandwidth Package: Share bandwidth across multiple EIPs to reduce costs.
- Other Related Products:
 - CVM: NAT Gateway enables internet access.
 - VPC: NAT Gateway is part of VPC.
 - Route Table: Configure subnet routing through NAT Gateway.
 - Public Gateway: CVM accessible by NAT Gateway.
 - Anti-DDoS Pro: Defend NAT Gateway from attacks.
 - Network ACL: Control subnet inbound/outbound traffic.

Accessing the Internet via NAT Gateway

Step 1: Create a NAT Gateway

- Log in to NAT Gateway console → +New → configure:
 - Gateway Name: Up to 60 characters
 - Region: Select
 - VPC: Select
 - Gateway Type: Small, Medium, Large
 - Outbound Bandwidth Cap: 10–5,000 Mbps
 - EIP Configuration: Existing or new
- Note: Outbound bandwidth cap $\leq$ total EIP bandwidth.

Step 2: Configure Route Table for Subnet

- In NAT Gateway list → click VPC ID → Subnets → select subnet → click route table → +New routing policy:
 - Destination: Public IP range
 - Next Hop Type: NAT Gateway
 - Next Hop: Choose existing NAT Gateway → Create

Step 3: Enable Gateway Traffic Monitoring (Optional)

- NAT Gateway console → select NAT Gateway → Monitoring tab → Enable Gateway Traffic Monitoring Details.



NAT Gateway Fee Description

Standard NAT Gateway

- Instance Fees: Billed hourly



Private NAT Gateway Operation Guide

Billing Structure

Private NAT Gateway fees include:

- Instance fee
- Capacity Unit (CU) fee

Both are postpaid and billed hourly.

Formulas

Instance Fee

Instance fee = Instance price × Usage duration (hours)

CU Fee

CU fee = CU price × Number of CUs × Usage duration (hours)

- Number of CUs is based on the maximum CU consumption among all metrics:

Number of CUs = MAX[
Number of CUs for hourly active connections,
Number of CUs for hourly new connections,
Number of CUs for hourly traffic processed
]

Capacity Unit (CU) Metrics

CU measures performance and traffic processing. Metrics include active connections, new connections, and processed traffic.

Metric	CU Coefficient	Description	Calculation Formula
Active connections	Example: 10,000	Number of simultaneous connections	Max active connections per minute ÷ CU coefficient



Metric	CU Coefficient	Description	Calculation Formula
New connections	Example: 1,000	Number of new connections per second	Max new connections per second ÷ CU coefficient
Traffic processed	Example: 1 GB	Total inbound and outbound traffic	Total processed traffic ÷ CU coefficient

Note:

The billing system records performance metrics per hour and selects the metric with the highest CU consumption to calculate CU fees.

Billing Example

Private NAT Gateway instance used for 1 hour in a region.

Average per hour:

- Active connections: 15,000
- New connections: 3,000
- Traffic processed: 10 GB

CU Calculation:

Metric	Calculation
Active connections	$15,000 \div 10,000 = 1.5$
New connections	$3,000 \div 1,000 = 3$
Traffic processed	$10 \div 1 = 10$

- Max CU for billing: 10

Total Fee Formula

Total fee = Instance fee + CU fee

Note:



Pricing policies may change, and any discounts or adjustments are applied according to official guidelines.



Purchasing NAT Gateway in Console

Directions

1. Log in to the NAT Gateway console.
2. Select a region and VPC, then click Create.
3. On the NAT Gateway purchase page, complete the parameters and confirm the purchase.

Parameters

Parameter	Description
Gateway name	Enter a NAT Gateway name, up to 60 characters.
Region	Select the region where the NAT Gateway will be deployed.
VPC	Select the VPC where the NAT Gateway will belong.
Gateway type	Choose from: • Small (up to 1,000,000 connections) • Medium (up to 3,000,000 connections) • Large (up to 10,000,000 connections)
Outbound bandwidth cap	Maximum outbound bandwidth for the NAT Gateway. Valid values: 10, 20, 50, 100, 200, 500, 1000, 2000, 5000 Mbps.
EIP configuration	Associate the NAT Gateway with existing EIPs or create new EIPs: • Using existing EIPs: Ensure idle EIPs are available in the same region. • Creating new EIPs: General BGP IPs are automatically created. Configure quantity and bandwidth cap as needed.

Note:

- Internet traffic is limited by both the NAT Gateway and EIP bandwidth caps. The smaller cap applies.
- For more details on operations, see Getting Started in the NAT Gateway documentation.

NAT Gateway Overdue Payments

Note:

- If you are a customer of a Converge Cloud partner, the rules regarding resource usage and overdue payments are subject to the agreement between you and the partner.

Grace Period and Service Shutdown

Initial Grace Period (up to 2 hours)

- From the moment your account balance reaches zero, you can continue using your NAT Gateway.
- Usage during this period will be billed once your account is topped up.

Automatic Shutdown (after 2 hours)

- If the account remains negative for more than 2 hours, the NAT Gateway service automatically shuts down.
- Billing stops immediately once the service is shut down.

Recovery Window (up to 24 hours)

- Within 24 hours after automatic shutdown, the NAT Gateway remains unavailable.
- If you top up your account to a positive balance during this period, the NAT Gateway service resumes and billing continues.

Repossessed NAT Gateway (after 24 hours)

- If the account balance remains negative beyond 24 hours after shutdown, the NAT Gateway is repossessed immediately.
- Converge Cloud will notify the account owner and all collaborators via email and SMS when repossession occurs.



Billing Overview

This document introduces the fee structure of the NAT Gateway.

Billing Description

The NAT Gateway service fee consists of two parts: gateway fee (billed by hour) and network fee (billed by traffic). The gateway fee is billed on the NAT Gateway, and the network fee is billed on the EIP bound to the NAT Gateway.

Gateway Inquiry

You can select different bandwidth specifications on the NAT Gateway purchase page to learn about the corresponding gateway fees.



Create NAT Gateway



Gateway Name *

You can enter 60 more characters

Gateway Type *

Small (up to 1,000,000 connections) ▼

Region luzon

AZ *

ncr-1 ▼

Network *

vpc-im07w0ld (Dedicated firewall Group VPC ... ▼

Bandwidth Limitation *

100Mbps ▼

EIP

Create EIP ▼

[Bind EIP](#)

Up to 10 IPs can be bound?

Carrier *

BGP ▼

The maximum number of EIPs that can be created under this carrier is 20, and 16 can still be created.

Tag	Tag Key	Tag Value	Delete
	Please select	▼	

[+ Add](#)

If the existing tag or tag value does not meet your requirements, you can [create a tag](#) on the console.

Gateway Fee(Before discount)

0.1 USD/hr

Gateway Fee(After discount)

0.1 USD/hr

Note: The network fee is charged on the elastic IP bound to the NAT gateway.

Create

Cancel

Operation Guide

Configuring a Route Pointing to the NAT Gateway

After you create a NAT Gateway, you need to configure routing rules to direct subnet traffic to the NAT Gateway.

1. In the sidebar on the left side of the VPC console, click Route Table.
2. In the route table list, click the route table ID associated with the subnet that needs to access the internet to enter the route table details page, then click Add Routing Policy in the routing policy.

Create			
ID/Name	Network	Type	Associated Subnets
rtb-labmli1w	vpc-	Default Route Table	1

3. Enter the destination in the pop-up box, select NAT Gateway for the next hop type, and select the created NAT Gateway ID for the next hop.

Add Routing Policy ×

Destination	Next Hop Type	Next Hop	Remarks	Action
Example: 10.10.10.0/24	NAT Gateway	gateway.		-

[Add One Line](#)

Create

Cancel

4. Click Create, and after the above configuration is completed, the traffic from the CVM in the subnet associated with this route table will be directed to the NAT Gateway when the CVM accesses the internet.

Adjusting the Priority of NAT Gateway and EIP

When a subnet is associated with a NAT gateway, and the CVM in the subnet has a public network IP address (or an EIP), the CVM accesses the Internet through the NAT gateway by default because the priority of the exact match route is higher than that of the public network IP. However, you can set a routing policy to allow the CVM to access the Internet through its public network IP.

Directions

1. View the routing table associated with the subnet where the CVM is located. Ensure that a routing policy that points to the NAT gateway exists so that CVMs in the subnet that have no public network IP can still access the Internet through the NAT gateway.

Destination	Next Hop Type	Next Hop	Remarks	Action
Local	Local	Local	The system delivers the configuration by default, indicating that the connectivity between CVMs in the VPC is normal.	
0.0.0.0/0	NAT Gateway	nat-623H4vw TEST		Modify Delete

2. Add a new routing policy with the Next Hop Type as Public Network IP of Cloud Virtual Machine and enter the Destination.
 - Destination: Enter the specific public network IP range or default route (0.0.0.0/0, default route indication: if the destination is not in the routing table, default route for all data packets) to be accessed by the service.
 - Next Hop Type: CVM.

Note:

- This routing policy, when configured with routing rules that have the same destination as the original ones pointing to the NAT Gateway, CVM, and public network gateway, always matches this route preferentially.
- This routing policy will affect all subnets associated with this route table (please confirm the impact of this operation). Specifically, cloud servers within these subnets that have public IP addresses (or elastic IPs) will access the Internet via their public IPs instead of through the NAT Gateway.
- Cloud servers within the subnets associated with this route table that do not have public IP addresses can still access the Internet via the NAT Gateway and will not be affected.



Add Routing Policy



Destination	Next Hop Type	Next Hop	Remarks	Act...
Example: 10.10.10.0/24	CVM	Enter a private IP address		-

Managing Port Forwarding Rules

Creating Port Forwarding Rules

The port forwarding table is a configuration table on the NAT Gateway. It is used to configure the DNAT feature on the NAT Gateway, which maps the private IP address, protocol, and port of CVMs within the VPC to the public IP address, protocol, and port, enabling resources on CVMs to be accessed from the public network.

The following will introduce you in detail how to create port forwarding rules.

1. Log in to the cloud console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console, and click NAT Gateway in the sidebar on the left.
2. In the list, click the NAT Gateway ID that needs to be modified to enter the details page, and click Port Forwarding in the tab.
3. Click Create, select the protocol, external IP port, and internal IP port, and click OK.

Create Port Forwarding ✕

Protocol * ☒ TCP ☐ UDP

External IP and Port *

10.1.1.2.9 ▼

0-65535

Internal IP and Port *

Private IP of a CVM within VPC

0-65535

Description

A maximum of 100 characters are supported.

If the private IP is unassociated from the CVM, the rule is also deleted.

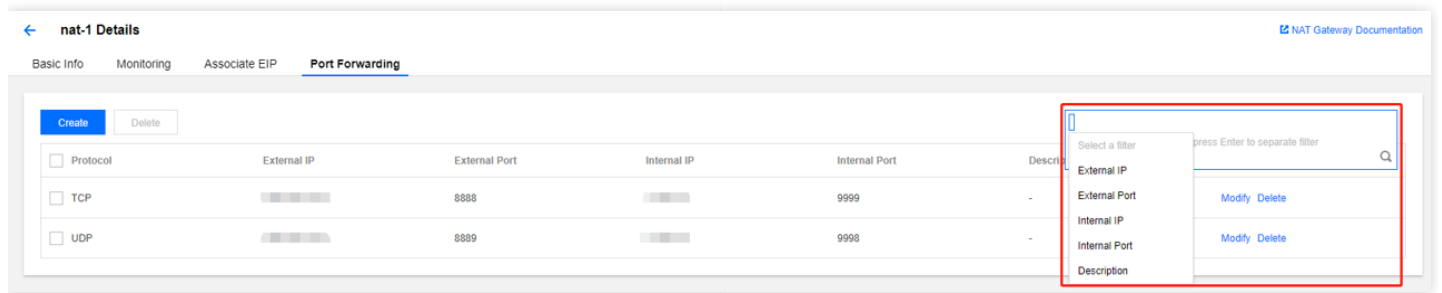
OK

Cancel

Querying Port Forwarding Rules

The following will introduce you in detail how to query port forwarding rules.

1. Log in to the cloud console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console, and click NAT Gateway in the left sidebar.
2. In the list, click the NAT Gateway ID you want to query to enter the details page and select Port Forwarding.
3. In the search box, select a resource attribute value or enter a keyword to query related port forwarding rules.



nat-1 Details [NAT Gateway Documentation](#)

Basic Info Monitoring Associate EIP **Port Forwarding**

Create Delete

Protocol	External IP	External Port	Internal IP	Internal Port	Description
☐ TCP	[IP Address]	8888	[IP Address]	9999	-
☐ UDP	[IP Address]	8889	[IP Address]	9998	-

Search box: Select a filter, Press Enter to separate filter. Filter options: External IP, External Port, Internal IP, Internal Port, Description. Action buttons: Modify, Delete.

Modifying NAT Gateway Configuration

After you create a NAT Gateway, you can modify its attributes.

1. Log in to the cloud console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console, and click NAT Gateway in the sidebar on the left.
 2. In the list, click the NAT Gateway ID that needs to be modified to enter the details page. On the Basic Information page of the details page, you can complete the following operations.
- Modify the custom name of the gateway.
 - Change the NAT Gateway type.
 - Modify maximum bandwidth.

← nat-1 Details

Basic Info

Monitoring

Associate EIP

Port Forwarding

Basic Info

Gateway Name	nat-1
Gateway ID	nat- 6y
Gateway Type	Small-scale (Max. number of concurrent connections: 100 x 10K)
Max. Bandwidth	10Mbps Modify Bandwidth
Network	vpc-khd4nkpz (test 1 0/16)
Region	s
AZ	yfm17
Created At	2020-08-10 20:25:35

Managing NAT Gateway EIPs

After creating a NATGW, you can manage the EIPs of the NATGW. The following section describes the management method in detail.

1. Log in to the VPC console.
2. In the left directory, click NATGW to go to the NATGW List page.
3. Click a gateway ID in the list to go to the details page.
4. Select the EIP Association tab, on which you can choose to bind or unbind an EIP.

Bind an EIP

Note:

When a NATGW is bound to multiple EIPs, the system automatically performs load balancing.

Click Bind EIP, select the EIP to be bound in the dropdown list, and click Save.

← nat-1 Details

Basic InfoMonitoringAssociate EIPPort Forwarding

Associate EIP

The NAT gateway can be bound with up to 10 intra-region EIPs.

IP	Action
	Unbind

Please select

SaveCancel

Bind EIP

Unbinding an EIP

Note:

A NATGW should be bound to at least one EIP.

In the Operation column of the EIP that needs to be unbound, click Unbind.

nat-1 Details

Basic Info Monitoring **Associate EIP** Port Forwarding

Associate EIP

The NAT gateway can be bound with up to 10 intra-region EIPs.

IP	Action
109.2.9	Unbind

[Bind EIP](#)

Are you sure you want to unbind the public IP?

After unbinding, the port forwarding entry using this IP address as the external IP address will be deleted, and the bandwidth upper limit will be restored to 1 Mbit/s. Go to the EIP console for management.

OK **Cancel**

At least 1 EIP must be retained.

Setting Active/Standby EIPs

Note:

- When a NATGW is bound to only one EIP, it does not support setting a standby IP. When a NATGW is bound to two or more EIPs, it supports setting a standby IP.
- Multiple active EIPs and only one standby EIP can be set.

1. In the Operation column of the line where the corresponding EIP is located, click Set to Standby IP.
2. Click OK in the pop-up box to complete the standby IP settings.
3. When you no longer need a standby IP, you can restore the EIP to the active IP. In the Operation column of the EIP, click Restore to Active IP.
4. Click OK in the pop-up box to complete the active IP restoration.

Actual Forwarding Logic of Active/Standby EIPs

EIPs have corresponding health detections. When the health of the active EIP is detected to be abnormal:

- If there are EIPs in standby status and the number of available EIPs is greater than or equal to 1, data plane forwarding will be stopped for the abnormal EIP. An "(Abnormal)" suffix will be added to the abnormal EIP, while the processing logic and suffix of the original EIP in the "Standby" status remain unchanged.
- If there are EIPs in standby status and the number of available EIPs is zero, data plane forwarding will be stopped for the abnormal EIP. An "(Abnormal)" suffix will be added to the abnormal EIP, while the data plane of the original EIP in the "Standby" status will start forwarding, and its suffix will change to "(Standby, in use)".

When the active EIP is recovered:

- The data plane of the active EIP resumes forwarding first, then the standby EIP stops data plane forwarding, and the suffix is restored to its original status.

Managing SNAT Rules

When a NAT Gateway is bound to multiple EIPs, you can create SNAT rules to specify the EIPs for public network access for CVMs in different business groups.

For example, when a NAT Gateway is bound to multiple EIPs such as EIP1, EIP2, EIP3, and EIP4, the system automatically performs load balancing to access the public network among all bound EIPs. If EIP1, EIP2, and EIP3 are added to the SNAT address pool, the system uses the EIPs in the SNAT address pool to access the public network and automatically performs load balancing on the EIPs in the SNAT address pool. CVMs without SNAT rules configured can access the public network through all EIPs bound to NAT.

Note:

- When the load on the CVM instance surges, one EIP may not be able to support the huge amount of traffic. In this case, multiple EIPs can be configured to share the traffic.
- NAT Gateway supports using the same EIP to configure both SNAT rules and port forwarding rules.

This document describes how to create and manage SNAT rules.

SNAT Rule Limits

- When a NAT Gateway disassociates an EIP, if the EIP is the only EIP in the SNAT rule, the SNAT rule is deleted at the same time; if the EIP is not the only EIP in the SNAT rule, the EIP is deleted from the SNAT rule.
- If the subnet used in the SNAT rule does not exist, the SNAT rule is deleted at the same time.
- If the CVM used in the SNAT rule does not exist, the CVM is deleted from the SNAT rule at the same time. If the CVM is the last CVM in the SNAT rule, the SNAT rule is deleted at the same time.
- Due to standard protocol limits, for the same protocol/destination IP address/destination port, the upper limit of the number of connections = number of bound EIPs x 55,000. To increase the number of connections, add a new bound EIP or adjust the destination IP address/port.
- The description of the rule limit switch for cloud resources accessing the public network through the NAT Gateway is as follows:
 - Disabled by default: When no SNAT rules are configured, all cloud resources pointing to the NAT Gateway can access the public network through all EIPs on the NAT Gateway. When SNAT rules are configured, specified cloud resources can access the public network through specified EIPs, while other cloud resources without SNAT rules configured can access the public network through all EIPs on the NAT Gateway.
 - After enabling: Only cloud resources configured with SNAT rules are allowed to access the public network through the NAT Gateway; other cloud resources are not allowed to access the public network through the NAT Gateway.

- When an EIP is in the standby status, it does not support binding to SNAT rules. Only the active EIP supports binding.
- EIPs that are bound to SNAT rules cannot be set to standby EIPs.

Prerequisites

Before creating an SNAT rule, ensure that the route table of the subnet points to the corresponding NAT Gateway.

Creating an SNAT Rule

1. Log in to the VPC console.
2. In the left directory, click NAT Gateway to go to the NAT Gateway List page.
3. Click a gateway ID in the list to go to the details page.
4. Select the SNAT Rule tab to go to the SNAT Rule Management page.
5. Click Create, and the SNAT Rule Creation dialog box pops up.
6. Set the SNAT rule.
 - Source IP Range Granularity: Supports subnet and CVM granularity.
 - Subnet: When a subnet is selected, the route table associated with the subnet should point to the NAT Gateway, and all CVMs in the subnet access the public network according to the SNAT rules.
 - CVM: When a CVM is selected, the route table associated with the subnet where the CVM is located should point to the NAT Gateway. Only the selected CVM can access the public network according to the SNAT rules. CVMs without SNAT rules configured can access the public network through all EIPs bound to NAT.
 - Subnet: Select a subnet or the subnet to which the CVM belongs.
 - CVM: A CVM should be specified only when the source IP range granularity is CVM. Multiple CVMs can be added.
 - Public IP Address: Specify the EIP for public network access.
 - Description: Custom description information, supporting up to 60 characters.

Create SNAT Rule

Source IP Range Granularity

☐ Subnet

☒ CVM

Subnet

Please select

CVM

Please select

Public IPs

Please select

Delete

+ Add public IPs

Description

Optional

60 more characters allowed

Submit

Cancel

7. After the SNAT rule parameter settings are completed, click Submit.

Editing an SNAT Rule

Note:

Modifying public IP addresses in the existing SNAT rules may cause the original business connection to be interrupted, which can be restored after reconnection. Proceed with caution.

1. On the SNAT Rule tab, click Edit on the right of the SNAT rule entry, and an editing dialog box pops up.
2. Modify the public IP address or description in the SNAT rule, and click Submit to complete the modification.
3. Click the edit icon next to the description in the SNAT rule to modify it directly.

Querying SNAT Rules

1. In the search box in the upper right corner of the SNAT Rule tab, click to select the following filter conditions and enter the corresponding parameter values in the input box.
2. Click the search icon for a quick search.



3. Click a subnet/CVM ID to redirect to the corresponding resource details page.

Deleting an SNAT Rule

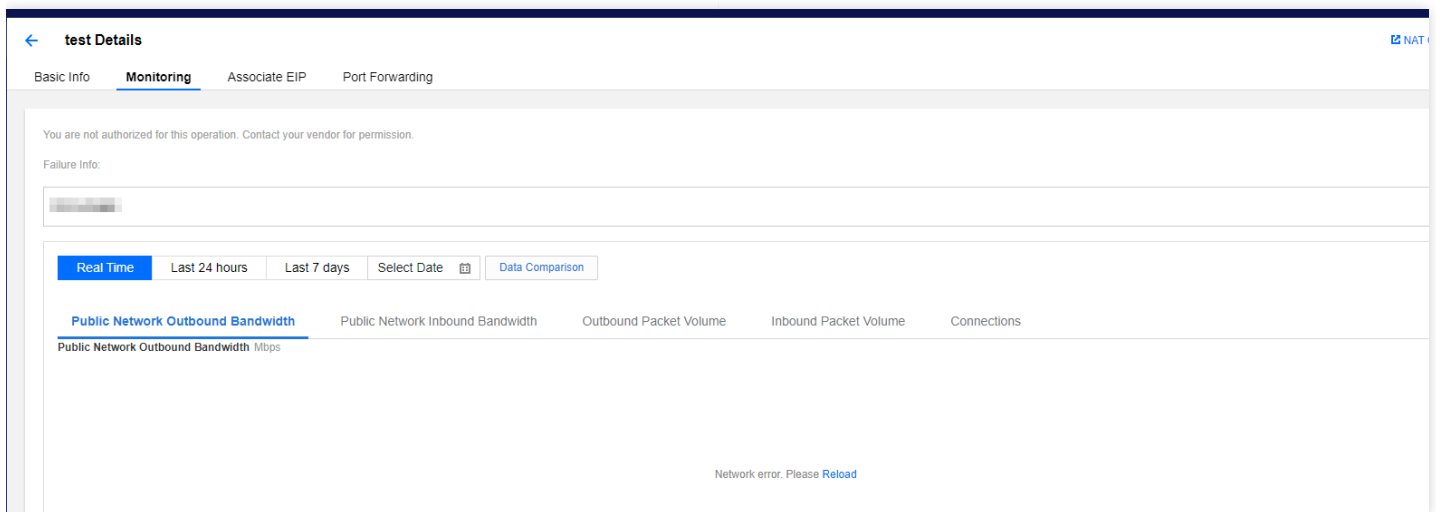
If you do not need to specify an EIP for the CVM to access the public network, you can delete the SNAT rule.

- Single-rule deletion
 - On the SNAT Rule tab, click Delete on the right of the SNAT rule entry.
 - Click OK to delete the SNAT rule.
- Batch deletion
 - On the SNAT Rule tab, select multiple SNAT rules and click Delete above.
 - In the pop-up dialog box, click Delete to complete the batch deletion.

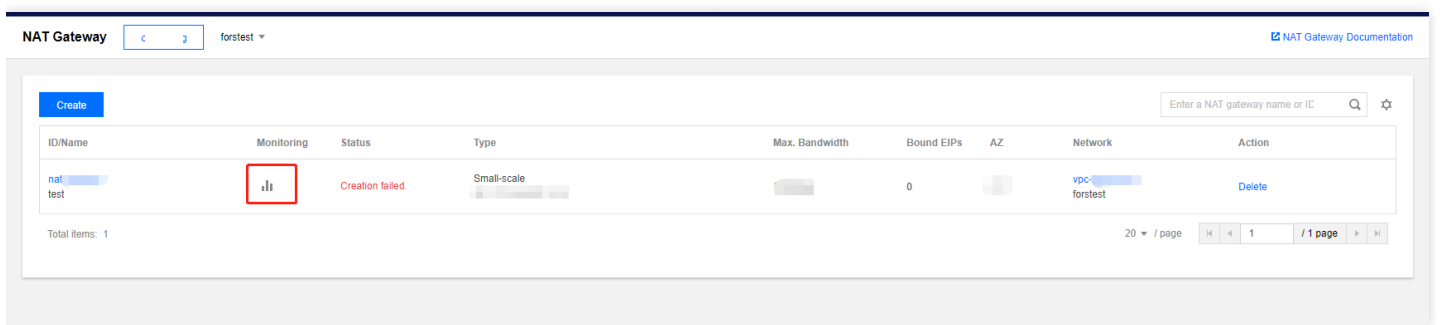
Viewing Monitoring Information

After you create a NAT Gateway, you can view monitoring information and export data through the console.

1. Log in to the cloud console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console, and click NAT Gateway in the sidebar on the left.
2. In the NAT Gateway list, click the gateway ID you want to view to enter the details page and click the Monitoring tab to view the monitoring information.



3. You can also click the monitor icon in the NAT Gateway entry you want to view in the NAT Gateway list to view the monitoring information.



Setting Alarms

You can set alarms for NAT gateways to monitor the status of NAT gateways.

1. Log in to the Cloud Monitor console.
2. In the directory on the left, select Alarm Configuration > Alarm Policy to enter the alarm policy configuration page, and click Create.
3. Enter the name of the alarm policy, select NAT Gateway as the policy type, select the alarm object, set the alarm policy, select the alarm receiving group and alarm channel, and click Complete. You can view the set alarm policy in the alarm policy list.

Note:

After an alarm policy is created, you need to unbind all resources before you can delete it.

4. Viewing an Alarm Message

When an alarm condition is triggered, you will receive an alarm through the selected alarm channel (SMS/email/message center), or you can click Alarm History in the left directory to view it.

Deleting a NAT Gateway

Note:

When you delete it, the route table containing this NAT Gateway and related routing policies will be deleted together, and internet forwarding requests will be interrupted immediately. Please be prepared for network interruption.

You can delete a NAT Gateway at any time if you decide that you do not need it.

1. Log in to the cloud console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console, and click NAT Gateway in the sidebar on the left.
2. Find the NAT Gateway you want to delete in the list, click Delete in the Action column, and click OK in the pop-up.



Quick Start

You only need to complete the following two steps to access the internet through a NAT Gateway.

Step 1: Create a NAT Gateway

- 1. Log in to the cloud console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console, and click NAT Gateway on the left.
- 2. Click Create in the upper left corner.

Create					
ID/Name	Monitor...	Status	Type	Max. Bandwidth	Bound EIPs

3. In the pop-up New dialog box, gateway parameters involved are:

Parameter description:

- Gateway Name: Customize the gateway name.
- Gateway Type: The gateway type supports small, medium, and large. Please set it according to the actual situation.
- AZ: Select the availability zone to which the NAT Gateway belongs.
- Network: Select the VPC to which the NAT gateway belongs.
- Max. Bandwidth: Select according to your needs.
- EIP: Bind an EIP to the NAT Gateway. You can select an existing EIP or purchase and bind a new one.
- Carrier: Select an ISP based on your actual situation.



Create NAT Gateway



Gateway Name *

You can enter 60 more characters

Gateway Type *

Small (up to 1,000,000 connections) ▼

Region

AZ *

▼

Network *

▼

Bandwidth *

100Mbps ▼

EIP

Create EIP ▼

[Bind EIP](#)

Up to 10 IPs can be bound(?)

Carrier *

▼

The maximum number of EIPs that can be created under this carrier is 100, and 100 can still be created.

Tag

Tag Key	Tag Value	Delete
Please select	▼	

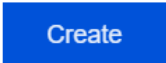
[+ Add](#)

If the existing tag or tag value does not meet your requirements, you can [create a tag](#) on the console.

Gateway Fee(Before discount)

Gateway Fee(After discount)

Note: The network fee is charged on the elastic IP bound to the NAT gateway.

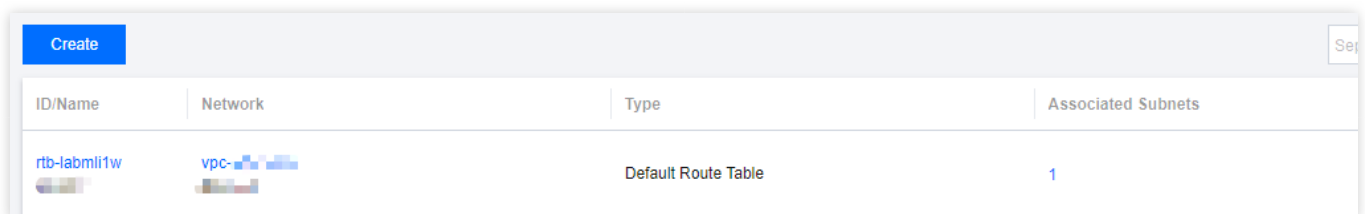


4. After the parameter settings are completed, click Create to create the NAT Gateway.

Step 2: Configure the route table associated with the subnet

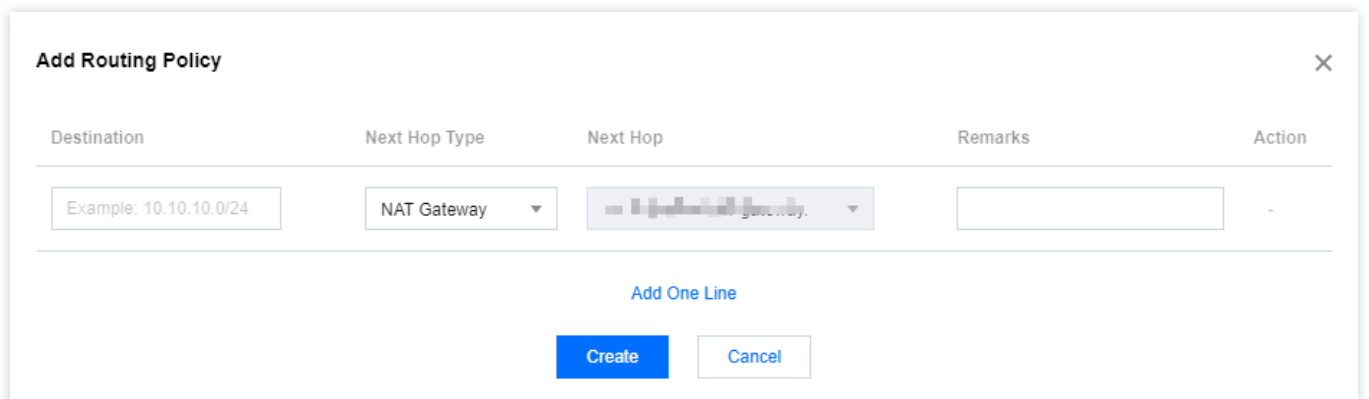
After you create a NAT Gateway, you need to configure routing rules to direct subnet traffic to the NAT Gateway.

1. In the sidebar on the left side of the VPC console, click Route Table.
2. In the route table list, click the route table ID associated with the subnet that needs to access the internet to enter the route table details page, then click Add Routing Policy in the routing policy.



Create				Set
ID/Name	Network	Type	Associated Subnets	
rtb-labmli1w	vpc- 	Default Route Table	1	

3. Enter the destination (the public IP address segment to be accessed) in the pop-up box, select NAT Gateway for the next hop type, and select the created NAT Gateway ID for the next hop.



Add Routing Policy ×

Destination	Next Hop Type	Next Hop	Remarks	Action
Example: 10.10.10.0/24	NAT Gateway ▼	 gateway. ▼		-

Add One Line

Create

Cancel

4. Click Create, and after the above configuration is completed, the traffic from the CVM in the subnet associated with this route table will be directed to the NAT Gateway when the CVM accesses the internet.

Glossary

Security Group

A Security Group is a virtual firewall with state-based packet filtering, used to control network access for one or more CVMs.

You can group CVMs with the same network security requirements into a security group and filter inbound and outbound traffic based on security policies.

Note:

- Security Groups act as virtual firewalls, ensuring CVMs in the same VPC follow consistent network policies.

Peering Connections

A Peering Connection allows communication between different VPCs, including cross-account and cross-region scenarios.

Public Network Gateway

A Public Network Gateway is a CVM that forwards traffic between the internet and VPCs. CVMs without a public IP can access the internet via a public gateway.

Route Table

A Route Table is a collection of routing policies that define the traffic flow for subnets within a VPC.

- A subnet can associate with only one route table, but a table can serve multiple subnets in the same VPC.

Routing Policy

A Routing Policy specifies the path network traffic takes. It includes three parameters:

- Destination: The target IP range (cannot be the VPC's own range)
- Next hop type: e.g., public gateway, VPN gateway
- Next hop: The specific gateway to which traffic is directed

Private IP

A Private IP is assigned to a CVM in a VPC or basic network.

- Not accessible from the internet
- Used for communication between instances in the same VPC

NAT Gateway

A NAT Gateway translates private IPs in a VPC to public IPs, enabling internet access when networks are isolated.

- Supports up to 5 Gbps traffic surge
- Supports 10,000,000 concurrent connections
- High availability with master/slave hot backup for automatic failover

Note:

- NAT Gateways allow private CVMs without public IPs to securely access the internet and provide automatic failover.

Virtual Private Cloud (VPC)

A Virtual Private Cloud (VPC) is a logically isolated network within Converge Cloud.

- Similar to a traditional on-premises network
- Supports services such as CVMs, Load Balancers, and databases
- Flexible IP ranges, routing policies, and subnets
- Can use EIPs, NAT Gateways, and public gateways for internet access or hybrid connectivity

EIP (Elastic IP)

An Elastic IP (EIP) is a static public IP that can be dynamically bound or unbound to CVMs or NAT Gateways.



Main functions:

- Retain an IP for DNS or licensing purposes
- Enable failover by remapping to another instance without downtime

Public IP

A Public IP is an internet-accessible IP used for communication between CVMs and the internet or other Converge Cloud resources.

Subnet

A Subnet segments a VPC into different IP ranges.

- Supports secure deployment of multi-layer applications
- Allows elastic hosting of services within the VPC