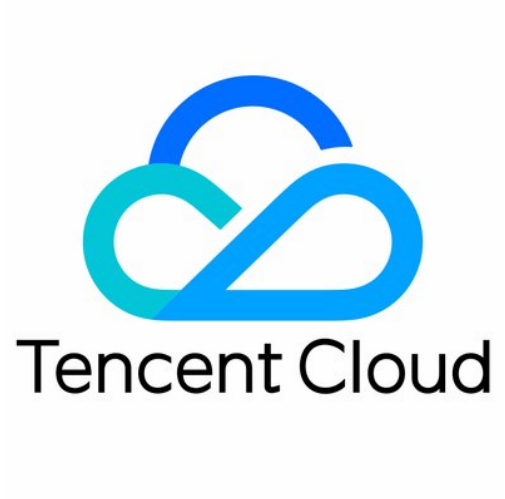
NAT Gateway

Product Introduction

Product Documentation



Contents

Product Introduction

Overview

Last updated：2021-10-13 09:48:04

Overview

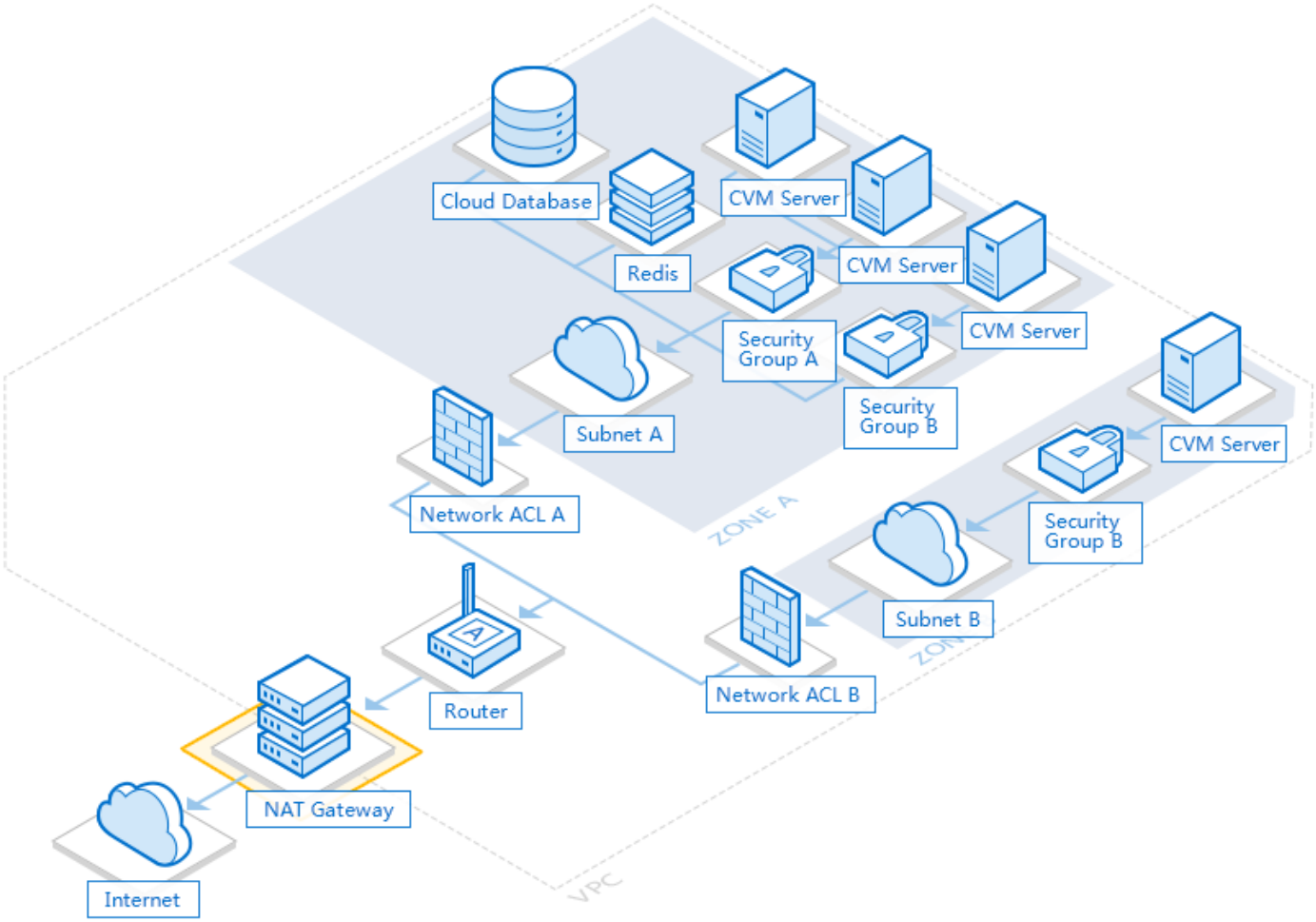
NAT Gateway is a service that supports IP address translation and provides the SNAT (Source Network Address Translation)and DNAT (Destination Network Address Translation)capabilities. It provides secure and high-performance Internet access for resources in VPCs. NAT Gateway supports a high availability of up to 99.99%, 5 Gbps bandwidth, and more than 10 million concurrent connections. Its typical application scenarios are as follows:

1. Large bandwidth and high-availability public network egress services, such as web crawlers and access to Internet public services.
2. Secure public network egress services, for example, you would like to have a CVM communicates with internet but don’t want to bind the CVM to a public IP address for security reasons.

Network Topology

As shown in the following figure, when resources in the VPC, such as CVMs, send outbound data packets through the NAT gateway, these data packets first travel through the router and then are routed according to the routing policy.

Finally, the NAT gateway sends the traffic to the Internet by using the bound EIP as the source IP address.



Differences Between the NAT Gateway and the Public Gateway

CVMs in a VPC can access the Internet through a NAT gateway or a public gateway. The following table lists the differences between both types of gateways.

Attribute	NAT Gateway	Public Gateway
Availability	Master/Slave hot backup and automatic hot switching	Manually switches the failed gateway.
Public network bandwidth	Maximum of 5 Gbps	Depends on the network bandwidth of the CVM.

Attribute	NAT Gateway	Public Gateway
Public IP address	A maximum of 10 EIPs can be bound	Supports one EIP or ordinary public IP address.
Rate limit of the public network	5 Gbps (The bandwidth cap is 50 Gbps, which is not available until you submit a ticket)	Depends on the rate limit of the CVM.
Max concurrent connections	10,000,000	500,000
Private IP address	Private IP addresses of VPC users are not consumed	Private IP addresses of subnets are consumed.
Security group	Binding a security group to a NAT gateway is not supported. Instead, you can bind a security group to the backend CVM.	Binding a security group is supported.
Network ACL	Binding a network ACL to a NAT gateway is not supported. Instead, you can bind a network ACL to the subnet where the backend CVM resides.	Binding a network ACL is not supported. Instead, you can bind a network ACL to the subnet where the public gateway resides.
Fees	Chinese mainland: Small (up to 1 million connections): 0.09 USD/hr Medium (up to 3 million connections):0.27 USD/hr Large (up tp 10 million connections): 0.89 USD/hr	You only need to pay for the CVM configurations, without paying extra fees

The NAT gateway has the following advantages:

- Large capacity
  It supports a maximum of 10,000,000 concurrent connections, 5 Gbps bandwidth, and 10 EIPs, meeting the demands of customers with a large business scale.
- Highly available master/slave hot backup
  It supports automatic failover in case of a single point of failure to implement automatic disaster recovery and 99.99% service availability, which is superior to the manual switching of a public gateway.
- Cost effectiveness
  Three configuration types (small, medium, and large) are available for users to purchase as needed, offering flexibility in billing and high cost-effectiveness.

Features

Last updated：2021-08-23 16:40:56

Tencent Cloud NAT Gateway maps EIPs and ports to private IPs and ports of CVM instances, allowing VPC CVM instances without any public IP to access and be accessed over the public network.
NAT Gateway features Source Network Address Translation (SNAT), Destination Network Address Translation (DNAT), gateway traffic control, traffic alarm, bandwidth packages, Anti-DDoS, automatic disaster recovery, and a lot more.

SNAT

SNAT makes it possible for multiple CVMs in the VPC to actively access the public network through the same public IP address. A single NAT Gateway instance supports a maximum forwarding capability of 5 Gbps.
You can bind multiple EIPs to NAT Gateway and allow CVM instances to access the public network through a random EIP. If you want to specify an EIP for the public network access, add it to the SANT address pool, so that CVMs can only access the public network through the EIP in the address pool.

DNAT

DNAT is used to map the public IP addresses, protocols, and ports to private IP addresses, protocols, and ports of the CVM in the VPC, so that services on the CVM can be accessed from the internet.

Bandwidth Packages

NAT Gateway can be used with IP bandwidth packages to share the public network bandwidth among multiple IP addresses after you binding EIPs to NAT Gateway and adding them to IP bandwidth packages. This is suitable for applications where traffic can be staggered, effectively reducing bandwidth costs.

Gateway Traffic Control

You can enable the traffic control feature for NAT Gateway to control the bandwidth from a private IP address to the NAT Gateway. This feature provides **monitoring** and **control** capabilities at **IP-gateway** granularity. The visualization helps network OPS personnel get a clear picture of the gateway traffic. The speed limiting capability at IP-gateway granularity helps block unhealthy traffic and protect key businesses.

Traffic Alarm

You can customize traffic alarms for NAT Gateway. When a metric value exceeds its threshold, alarm notifications are sent to you automatically via emails and SMS message. Monitoring and alarm services are free of charge, helping you quickly locate problems.

Anti-DDoS

Anti-DDoS Pro defends against DDoS and CC attacks with a protection bandwidth capability of up to 310 Gbps. 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 the failed server will be imperceptibly switched to the other server to maintain availability up to 99.99% and ensure your service stability.

Use Cases

Last updated：2020-08-19 10:36:20

Public Network Access with Large Bandwidth and High Availability

NAT Gateway applies to the following scenarios:

- Requires ultra-large bandwidth
- Massive use of public IP addresses
- deployment services

Secure Public Network Access

NAT Gateway provides secure IP translation, which can be used in the following scenarios:

- Needs to allow the communication with the public network while the IP address is hidden.
- Needs to hide the public IP address of the CVM in the VPC to avoid exposing its network deployment.

Product Specifications

Last updated：2022-05-30 10:45:26

NAT Gateway provides different types of packages. Select the package that meets your needs.

Configuration Specifications

NAT Gateway supports binding up to 10 EIPs, and a maximum of 5 Gbps traffic surge and 10,000,000 concurrent connections, while providing three configuration specifications:

- Small-scale (a maximum of 1000,000 connections)
- Medium-scale (a maximum of 3000,000 connections)
- Large-scale (a maximum of 10,000,000 connections)

> Note：
> Restricted by standard protocols, for the NAT gateways with the same protocol/destination IP/destination port, the number of maximum connections = the number of bound EIPs × 55000. To increase the number of connections, bind new EIPs or adjust the destination IP/port.

Maximum Public Network Outbound Bandwidth

Available maximum public network outbound bandwidths of the NAT gateway (in Mbps): 10, 20, 50, 100, 200, 500, 1,000, 2,000, and 5,000.

Maximum Public Network Inbound Bandwidth

- The maximum public network inbound bandwidth of a NAT gateway is 5 Gbps by default, which is unchangeable for now.
- The traffic cost of NAT Gateway is calculated based on the maximum public network outbound bandwidth regardless of the public network inbound bandwidth.

For billing details, see Billing Overview.

Usage Limits

Last updated：2022-05-30 10:19:34

This document describes the usage rules and limits of NAT gateways.

> Note：
> NAT Gateway supports TCP, UDP and ICMP, while ESP and AH for the GRE tunnel and IPSec cannot be used for the NAT Gateway, and ALG technologies are not supported. This is specific to NAT Gateway and irrelevant to service providers. Nevertheless, these supported protocols can mostly meet your application demands.

Use Rules

Note the following when using NAT Gateway:

- After a NAT Gateway is deleted, the associated EIPs are disassociated but not released.
- A NAT Gateway cannot be associated with security groups. However, you can bind security groups to instances within the VPC subnet to control their inbound and outbound traffic.
- The inbound and outbound traffic of the NAT Gateway cannot be directly controlled by the network ACL. Instead, you can use network ACL to control the traffic of the subnet associated with the NAT Gateway.
- You cannot use VPC peering connection or VPN connection to route traffic to a NAT Gateway.
  For example, a NAT Gateway enables traffic from VPC1 to the Internet, and VPC1 establishes a peering connection with VPC2. In this case, all the resources within VPC2 can access VPC1, but cannot access the Internet through the NAT Gateway.

Rule Limits

- When an EIP is disassociated from a NAT gateway, the SANT rule is also deleted if the EIP is the only EIP.
- If the subnet configured for a SNAT rule does not exist, the SNAT rule is deleted as well.
- If the CVM configured for a SNAT rule does not exist, the SNAT rule is also deleted if this is the last CVM; otherwise, the CVM is deleted from the SNAT rule.
- Restricted by standard protocols, for the NAT gateways with the same protocol/destination IP/destination port, the number of maximum connections = the number of bound EIPs × 55000. To increase the number of connections, bind new EIPs or adjust the destination IP/port.

Service Quota

The following table lists the restrictions on the supported resources for the NAT Gateway. For limits on other VPC resources, see Quota Limit.

Resource	Limit
Number of NAT Gateways per VPC	3
Number of EIPs per NAT Gateway	10
Maximum forwarding capability per NAT Gateway	5 Gbps
Maximum number of forwarding rules per NAT Gateway	200
Number of SNAT rules per NAT Gateway	200

Relevant Products

Last updated：2021-11-16 18:41:06

This document describes the network products related to NAT Gateway.

EIP

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

Method 1: using NAT Gateway only

The CVM instance without any public IP uses the public IP of the NAT Gateway to access the public network. Traffic to the public network is forwarded to the NAT Gateway via the private network.

Method 2: using the EIP only

The CVM instance uses EIPs to access the public network without any NAT Gateway. Traffic to the public network will be forwarded from the EIP.

Method 3: using NAT Gateway and EIP

> Note：
> For more information about EIPs, see Elastic IP.

The CVM instance is bound with an EIP, and the route table directs all traffic from the subnet to the public network to the NAT Gateway.

- All traffic from the CVM instance to the public network **uses the NAT Gateway through the private network**, and the response packets are returned through the NAT Gateway. If you want to use the EIP to access the public network, you can adjust priorities of NAT Gateways and EIPs.
- When the traffic from the public network uses the EIPs to access CVM, the CVM response packets are returned through the EIPs.

Bandwidth Package

If your NAT Gateway is bound with multiple EIPs, you can add them to the IP bandwidth package to share the bandwidth and save public network costs. For more information, see Product Overview.

Other Products

The table below lists other products related to the NAT Gateway:

Product Name	Relationship
CVM	The NAT Gateway and the EIP are two ways for CVM instances to access the Internet.
EIP	The EIP and the NAT Gateway are two ways for CVM instances to access the Internet.
VPC	NAT Gateway is part of VPC.
Route Table	After creating a NAT Gateway, you need to configure routing policies to direct the subnet traffic to the NAT Gateway.
Public Gateway	A public gateway is a CVM with the forwarding feature enabled and can be accessed by NAT Gateway.
Anti-DDoS Pro	Anti-DDoS Pro instance can be bound to a NAT Gateway to defend against DDoS and CC attacks.
Network ACL	Use network ACL to finely control the inbound and outbound traffic of subnets.