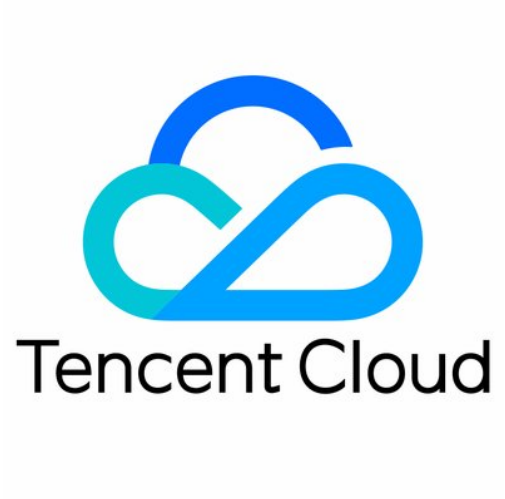
NAT Gateway

Practical Tutorial

Product Documentation



Contents

Practical Tutorial
Enabling Cross-VPC Access to Public Network via Standard NAT Gateway

Last updated：2024-08-01 14:14:49

Use Cases

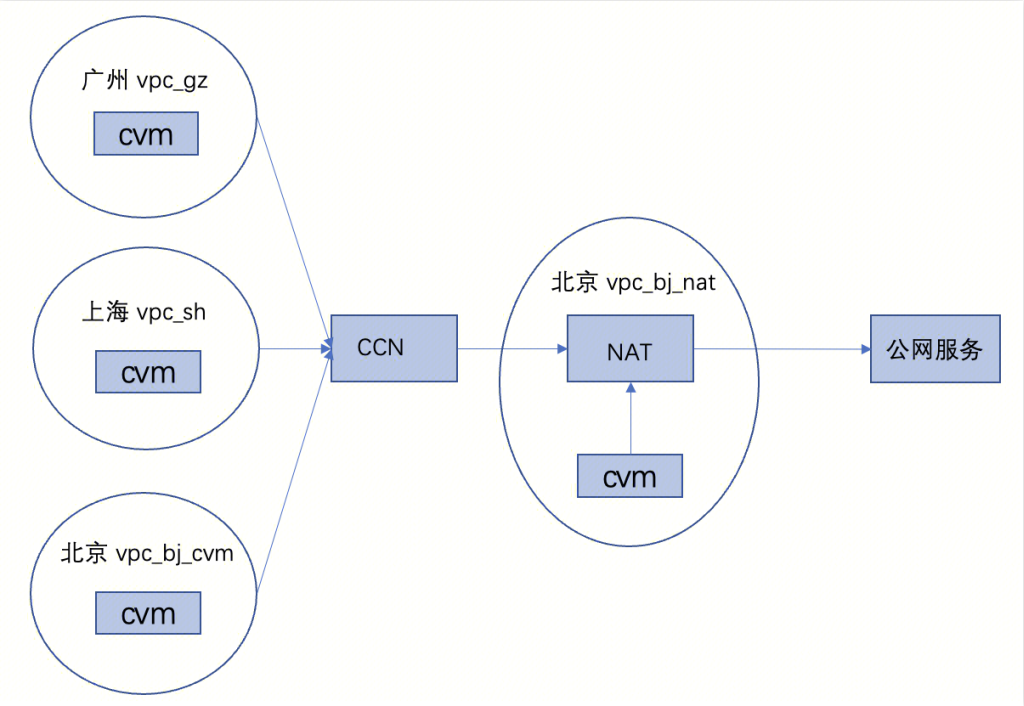
The user has established a NAT gateway in a VPC, and the CVM instances in the same VPC or other VPCs (including VPCs in the same region, cross-region VPCs, and cross-account VPCs) wish to access the public network through the NAT gateway.

Limits

The feature of cross-VPC access to the public network is currently supported only by Standard NAT Gateway but not by Traditional NAT Gateway.
The NAT routes of different VPCs cannot be simultaneously published to the Cloud Connect Network (CCN).
The Standard NAT Gateway is in beta testing. If you need to use it, please submit a ticket for request.

Configuration Principles

After the user creates a NAT gateway and configures the destination IP range as the public IP address and the next hop as the NAT route, the CVM instances in the same VPC can access the public network via the NAT route. Once the NAT route is published to the CCN, other VPCs associated with the CCN can also access the public network through the CCN and NAT.
Note:
The CCN is an independent product. Using it will incur related fees. For details, please refer to Billing Overview.



Use Process

Step 1: Creating a Standard NAT Gateway in the Beijing VPC

Log in to the NAT Gateway console. Refer to Creating NAT Gateway, to create a sample NAT gateway vpc_bj_nat.

Note:

The VPC where the NAT gateway is located cannot have a VPN gateway.

Step 2: Adding a Routing Policy

Log in to the Route Table console and create a routing policy in the route table of the sample gateway vpc_bj_nat for the Beijing VPC, such as the default route `0.0.0.0` with the next hop as the NAT gateway. For detailed operations, refer to Configuring Routes Pointing to NAT Gateway.

At this time, the CVMs in the same VPC can access the public network through this route.

Step 3: Confirming the CVM in the Guangzhou VPC

Log in to the CVM console. Ensure that the Guangzhou VPC has a CVM instance, such as cvm_gz. If there are no CVMs, refer to Creating a CVM Instance.

Step 4: Creating and Joining a CCN

Log in to the VPC - CCN console. Refer to the documents Creating a CCN Instance and Associating Network Instances, to add the Beijing VPC with the NAT gateway and the Guangzhou VPC with the cvm_gz instance to the CCN. Refer to Associating Network Instances.

Note:

1. The CVM instances here can belong to a VPC in the same region, a cross-region VPC, or a cross-account VPC, without regional restrictions.
2. In terms of the process, you can first add the Beijing VPC to the CCN, and then create the NAT gateway route and the CVM under the Guangzhou VPC.

Step 5: Publishing the NAT Route to the CCN

Log in to the VPC - Route Table console and publish the created NAT gateway route to the CCN. For detailed operations, refer to the document Managing Routing Policies.

Note:

1. It does not support publishing the NAT routes of different VPCs to the CCN.
2. It only supports publishing the NAT routes of a single VPC to the CCN, and multiple NAT routes of that VPC can be published to the CCN.

Note:

1. When the NAT routes are published to the CCN, the system will automatically create a route table named system-auto-for-nat-ccn, for which the associated subnet is 0. The route table contains routes used in the return traffic of the public network, namely NAT gateway routes pointing to the CCN. Generally, users do not need to modify it.
2. A VPC will create only 1 route table named system-auto-for-nat-ccn. If already exists, it will not be created again. This route table will be automatically deleted when the last NAT route is withdrawn from the CCN or when the VPC is unbound from the CCN.

Step 6: Enabling a Route

When the NAT route is the default route `0.0.0.0`, you must manually enable the route due to a conflict in the route's destination CIDR. Log in to the VPC - CCN console. For detailed operations, refer to Enabling a Route.

Step 7: Verifying the Traffic

A successful ping on the CVM indicates that the public network can be accessed.

Deletion Process

Step 1: Withdrawing the Route

Log in to the VPC - Route Table console and withdraw the NAT gateway route from the CCN.

Step 2: Verifying the Route

1. Log in to the VPC - Route Table console and check whether the system-auto-for-nat-ccn route table has also been deleted.
2. Log in to the VPC - CCN console and check whether the route `0.0.0.0` in the CCN route table has also been deleted.

Enabling Mutual Access between a Specified VPC Subnet and Public Network Resources via Private NAT Gateway

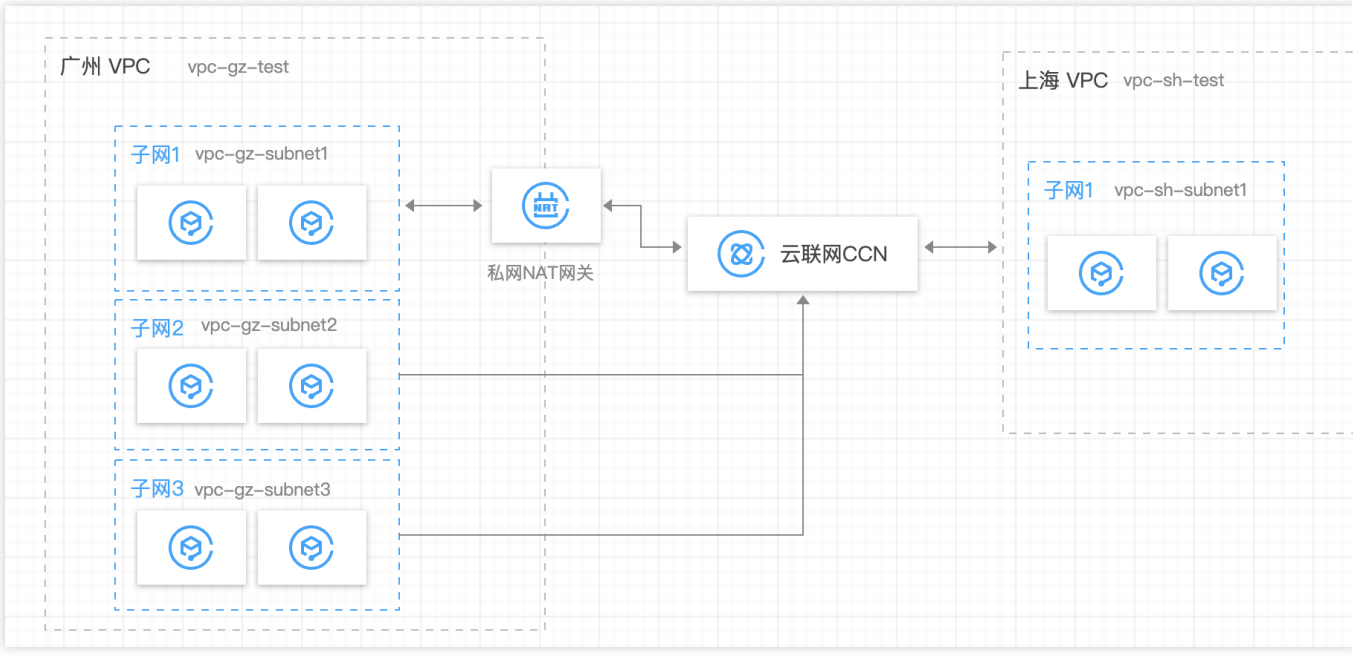
Last updated：2024-08-01 14:14:19

Overview

It applies to address translation of a specified subnet within a VPC, and is used for mutual access between the specified subnet in the VPC and the public network resources.
This document takes the following use case as an example. In the Guangzhou VPC, there are multiple subnets. Subnet 1 is not allowed to perform mutual access with the Shanghai VPC, while Subnet 2 is allowed. Therefore, in this case, Subnet 1 in the Guangzhou VPC implements mutual access with the Shanghai VPC by SNAT to other IPs.

Configuration Scheme

Refer to the diagram for the networking scheme configuration:



Step 1: Creating VPC Resources

Create a VPC in each of the Guangzhou region and the Shanghai region. For VPC creation, refer to Creating VPC.
Create 3 subnets in the Guangzhou VPC and 1 subnet in the Shanghai VPC. Refer to Creating Subnets.
Guangzhou Region:
Create 1 VPC: vpc-gz-test.
Create 3 subnets:
Subnet 1: vpc-gz-subnet1, including 1 CVM: vpc-gz-cvm1;
Subnet 2: vpc-gz-subnet2, including 0 CVMs: none;
Subnet 3: vpc-gz-subnet3, including 1 CVM: vpc-gz-cvm2.
Shanghai Region:
Create 1 VPC: vpc-sh-test.
Create 1 subnet: vpc-sh-subnet1, including 1 CVM: vpc-sh-cvm1.

Step 2: Creating CCN Resources and Binding the 2 VPCs Created in Step 1

Log in to the CCN console and click New to create a CCN instance. For operation details, refer to Creating a CCN Instance.

Step 3: Disabling Self-learning Routes for NAT on the CCN Side

1. Log in to the CCN console and click the **CCN instance** created in Step 2 to enter the instance page.
2. Select the **Route Table** tab and disable the routes of the subnet IP range requiring NAT (corresponding to vpc-gz-subnet1 in the example).
Note:
If the IP range used as the NAT IP also belongs to a subnet IP range or its subset, you must disable the routes of the corresponding subnet. For example, if the IP range of vpc-gz-subnet2 is used as the NAT IP, you must disable the routes of vpc-gz-subnet2.

Step 4: Creating a VPC Private NAT Gateway in the Guangzhou VPC (vpc-gz-test)

For details, refer to Creating Private NAT Gateways.

Step 5: Editing the NAT Gateway Rules (Layer-4 SNAT Rules)

1. Log in to the Private NAT Gateway console and click the VPC private NAT gateway ID created in Step 4 to enter the gateway details page.
2. Click the SNAT tab, and edit the NAT gateway rules (Layer-4 SNAT rules).

Note:

The original IP is the IP of vpc-gz-cvm1, and the mapped IP pool (namely NAT IP) can be other third-party IPs, or a subset of other subnet IP ranges (e.g., obtained from the subnet IP range of vpc-gz-subnet2).

Step 6: Configuring the vpc-gz-test Side Routing

1. Log in to the VPC console. In the vpc-gz-test instance, create 2 route tables, vpc-gz-rtb1 and vpc-gz-rtb2, in which vpc-gz-rtb1 is bound to Subnet 1 (vpc-gz-subnet1).
2. In the route table vpc-gz-rtb1, disable all routes learned from CCN.

Note:

Whenever a new VPC joins the CCN, you must disable the corresponding learned routing entries in this route table.

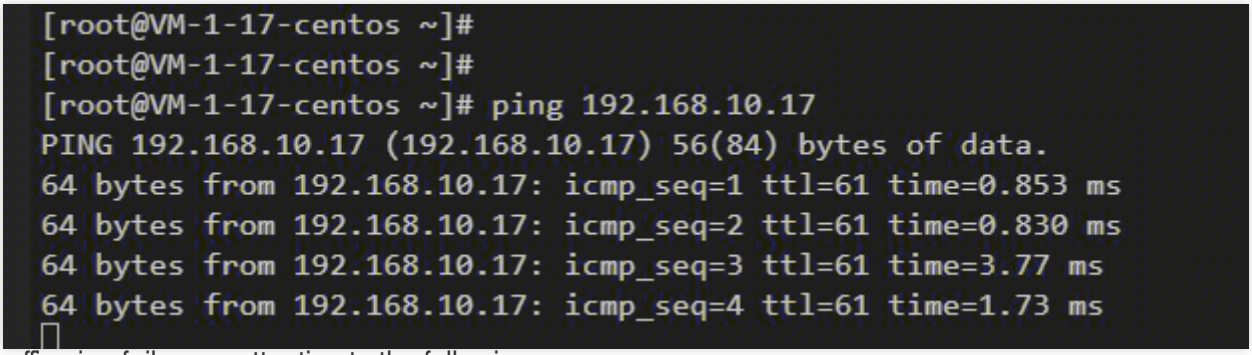
3. Create a routing entry in vpc-gz-rtb1 with the destination being the IP range to be accessed and the next hop being the NAT instance created in Step 4.
4. Create a routing entry in vpc-gz-rtb2 with the destination being the NAT IP range (if allocated from other subnet IP ranges, it must be a subset of the subnet IP range and cannot be exactly the same as the subnet IP range), and publish it to the CCN.

Note:

The destination IP range must cover the NAT IP range of the mapped address pool in Step 4. (It's recommended to take the same values for both.) You can check the CCN route table to confirm whether the routing entry is published.

Step 7: Traffic Verification

Ping Shanghai vpc-sh-cvm1 from Guangzhou vpc-gz-cvm1, to check whether the network is normal and the source IP of the packets captured from vpc-sh-cvm1 is the NAT IP.



If the traffic ping fails, pay attention to the following cases:

1. In vpc-gz-rtb1, the routes published by CCN must be disabled.
2. vpc-gz-rtb2 should not be bound to any subnet.
3. If the NAT IP is allocated from a subnet, the NAT IP range must be a subset of the subnet IP range.
4. CCN must disable the routes of the subnet requiring NAT. (If the NAT IP is allocated from another subnet IP range, the routes of the corresponding IP range must also be disabled.)

Enabling Secure Mutual Access with Public Network via Public CLB and NAT Gateway

Last updated：2024-08-01 14:14:06

Overview

With the business growth of customers, for security reasons, the customers require not exposing the CVM's private IPs to the public network, and want to achieve two-way hiding of the CVM's private IPs.

Configuration Scheme

Based on the above requirements, secure mutual access with the public network while hiding the CVM's private IPs can be achieved by using a CLB and a NAT gateway, in combination with the capabilities of Tencent Cloud products.
Active access from the CVM to the public network: It can be implemented by using a public NAT gateway. The NAT gateway can translate the private IP address of the CVM to a public IP address through the SNAT feature, thereby hiding the CVM's private IP address.
Access from the public network to the CVM: If needed, the CVM can be accessed from the public network in a unified manner through the public network CLB's VIP, thereby hiding the CVM's private IP address and achieving secure access from the public network to the CVM.

Configuration Process

Assuming that the customer has created a business VPC and deployed related services on the CVM within the VPC, the following steps can be taken for configuration:
1. Creating a NAT Gateway and Configuring Subnet Routing to the NAT Gateway
2. Creating a Public Network CLB Instance and Configuring Listener Rules
3. Configuring Security Policies
4. Operation Verification

Directions

Creating a NAT Gateway and Configuring Subnet Routing to the NAT Gateway

Create a public NAT gateway and configure subnet routing to the NAT gateway. In this way, the subnet traffic is directed to the NAT gateway and the public network can be accessed using the public IP on the NAT gateway, thereby hiding the private IP and enabling secure access to the public network. For details, see Getting Started with NAT.

Step 1: Creating a NAT Gateway

1. Log in to the NAT Gateway console.
2. Click **Create** in the upper left corner and configure the parameters in the pop-up box.
3. After the parameters are configured, complete the purchase as prompted. For details, see Purchase Methods.

Step 2: Configuring the Subnet Route Table to the NAT Gateway

1. In the NAT gateway list, click the VPC ID of the target NAT gateway.
2. In the VPC details, click **Subnets**.
3. In the subnet list, select the route table ID of the subnet that requires accessing the public network.
4. On the basic information page of the route table, click **Add Routing Policy**.
5. In the **Add Routing** pop-up box, enter the destination (IP range corresponding to the destination public network), select **Public NAT Gateway** as the next hop type, and select the created NAT gateway ID as the next hop.
6. Click **Create** to complete the above configuration. In this way, when the CVM in the subnet associated with this route table accesses the public network, the traffic will be directed to the NAT gateway and the public network will be accessed through the public IP on the NAT gateway.

Step 3: (Optional) Configuring SNAT Rules

The NAT gateway supports binding multiple public IPs. When the subnet route points to the NAT gateway, all CVMs in the subnet can access the public network through all public IPs on the NAT gateway by default. To specify a CVM accessing the public network through a specified public IP on the NAT gateway, you can configure a SNAT rule. For details, see Creating a SNAT Rule.

Step 4: (Optional) Configuring Port Forwarding Rules

The NAT gateway supports active access from the private network to the public network by default. If access from the public network is required, it can also be achieved by configuring the port forwarding rules.
In other words, the **private IP**, **protocol**, and **port** of a CVM in the VPC can be mapped to the **public IP**, **protocol**, and **port**, so that the resources on the CVM can be accessed one-to-one from the public network. For details, see Configuring Port Forwarding Rules.

Note：

The port forwarding service of the NAT gateway only supports one-on-one access from the public network. If access from the public network through a unified IP address is required, refer to the following steps to achieve this by using a public network CLB.

Creating a Public Network CLB Instance and Configuring Listener Rules

By creating a public network CLB and configuring listener rules, public network clients can access backend CVM services via the public VIP of the CLB. The traffic passing through the public network CLB is forwarded to the backend CVMs. For details, see Getting Started with CLB.

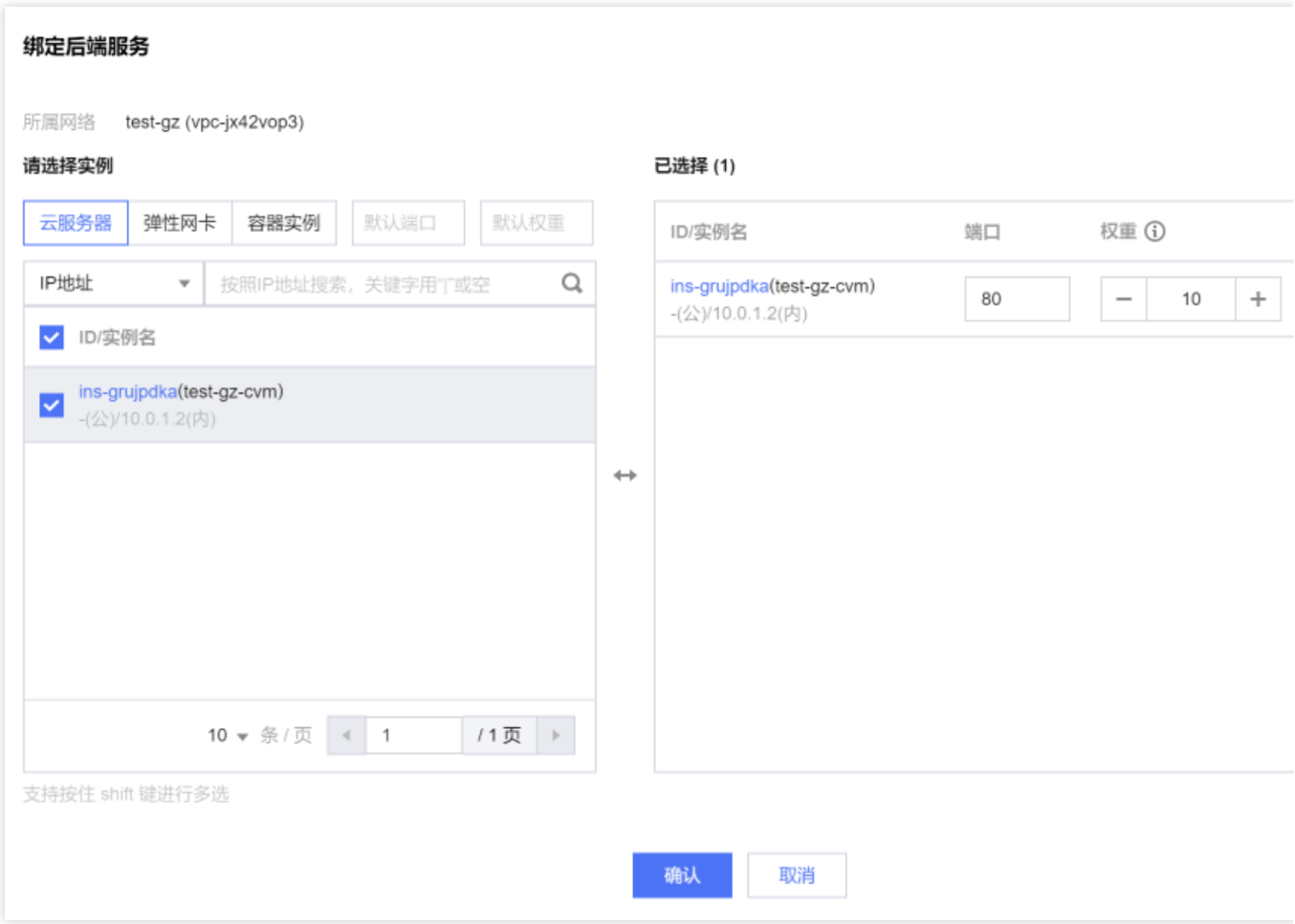
Step 1: Purchasing a CLB Instance

1. Log in to the Tencent Cloud CLB service purchase page.
2. On the CLB purchase page, select the region in which the CVM is located, and select **CLB** as the instance type and **Public Network** as the network type. For details, see Creating CLB Instances.
3. Click **Buy Now** to complete the payment.

Step 2: Configuring a CLB Listener

When a client initiates a request, the CLB will receive the request according to the listening frontend protocol and port, and then forward the request to the backend server. For details, see Configuring TCP Listener.

1. On the CLB list page, click **Configure Listener** on the right side of the target CLB instance.
2. In the **Listener Management** tab, click **Create** in the corresponding protocol section.
3. In the **Create Listener** dialog box, configure the listener parameters such as health check and session persistence step by step, and then click **Submit**.
4. In the listener details on the right, click **Bind** to bind a backend CVM to the CLB, and then configure the CVM port and weight. After completion, click **OK**.

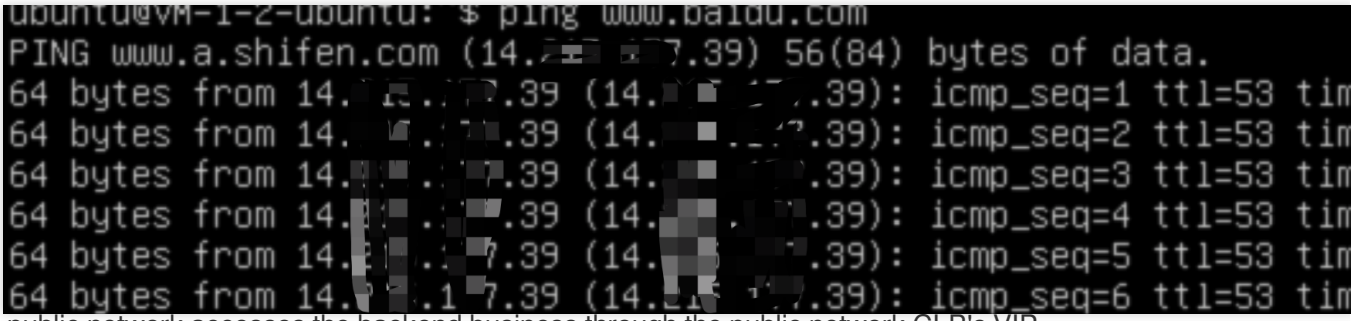


Configuring Security Policies

1. After creating the CLB, you can configure a CLB security group to isolate the public network traffic. For details, see Configuring CLB Security Group.
2. You can bind security groups to CVMs for traffic control at the CVM level. For details, see Adding Security Group Rules and Associating CVM Instances with Security Groups.
3. You can configure WAF protection for CLB listening domain names.
4. You can bind an Anti-DDoS Pro instance to a NAT gateway to defend against DDoS attacks. For details, see Anti-DDoS Pro.

Operation Verification

1. The CVM actively accesses the public network.



2. The public network accesses the backend business through the public network CLB's VIP.

Related Documents

When a subnet is associated with a NAT gateway, the CVMs having public IPs (or EIPs) within the subnet will access the Internet through the NAT gateway by default, because the priority of the exact match route is higher than that of the public IP. However, you can set a routing policy to allow the CVM to access the Internet through the public IP. For details, see Adjusting the Priorities of NAT Gateways and EIPs.

If you use a CLB to forward the business traffic to a CVM, corresponding configurations on the CVM's security group are required to ensure the health check feature. For details, see Configuring CVM Security Groups.

Adjusting the Priorities of NAT Gateways and EIPs

Last updated：2024-08-01 14:13:54

Description of NAT Gateway and EIP Priorities

When a subnet is associated with a NAT gateway, the CVMs having public IPs (or EIPs) in the subnet will access the Internet through the NAT gateway by default, because the priority of the exact match route is higher than that of the public IP. However, you can set a routing policy to allow the CVMs to access the Internet through their public IPs.

Directions

1. View the route table associated with the subnet where the CVM is located. Make sure that there is a routing policy pointing to the NAT gateway, to ensure that the CVMs having no public IPs in the subnet can still access the Internet through the NAT gateway.
2. Add a routing policy with the next hop type set to Public IP of the CVM and enter the destination.
Destination: Enter the specific public network IP range to be accessed by the business or the default route (0.0.0.0/0, indicating that the destination is not in the route table and all data packets are transmitted using the default route).
Next hop type: Public IP of the CVM.

Note

When this routing policy is configured with the same destination as the routing rules pointing to the NAT gateway, the CVM, and the public gateway, this route will be matched first.
This routing policy affects all subnets associated with the route table (please confirm the impact of the operation). In other words, the CVMs having public IPs (or EIPs) in these subnets will access the Internet through their respective public IP instead of the NAT gateway.
In the subnets associated with the route table, the CVMs having no public IPs can still access the Internet through the NAT gateway, without being affected.