Elastic IP

Best Practices

Issue	01
Date	2025-09-04

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

 Copyright © Huawei Technologies Co., Ltd.

1 Public Network Access

Products

Cloud services, such as EIP, NAT Gateway, and ELB can be used to connect to the Internet.

- EIP

  The EIP service provides independent public IP addresses and bandwidth for Internet access. EIPs can be bound to or unbound from ECSs, BMSs, virtual IP addresses, NAT gateways, and load balancers. Various billing modes are provided to meet diverse service requirements.

- ELB

  ELB distributes access traffic among multiple ECSs to balance the application load, improving fault tolerance and expanding service capabilities of applications. You can create a load balancer, configure a listening protocol and port, and add backend servers to a load balancer. You can also use a listener to check the running state of backend servers to ensure that requests are sent only to healthy servers.

- NAT Gateway

  NAT Gateway provides both SNAT and DNAT for your servers in a VPC and allows servers in your VPC to access or provide services accessible from the Internet through flexible and simple configuration.

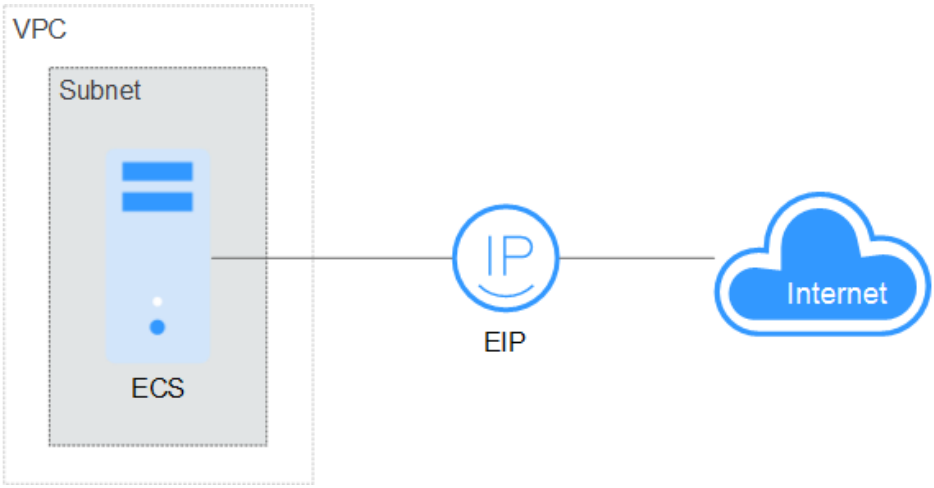
Providing Services Accessible from the Internet

- Single ECS provides services accessible from the Internet.

  If you have only one application and the service traffic is small, you can assign an EIP and bind it to the ECS so that the ECS can provide services accessible from the Internet.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-1 EIP

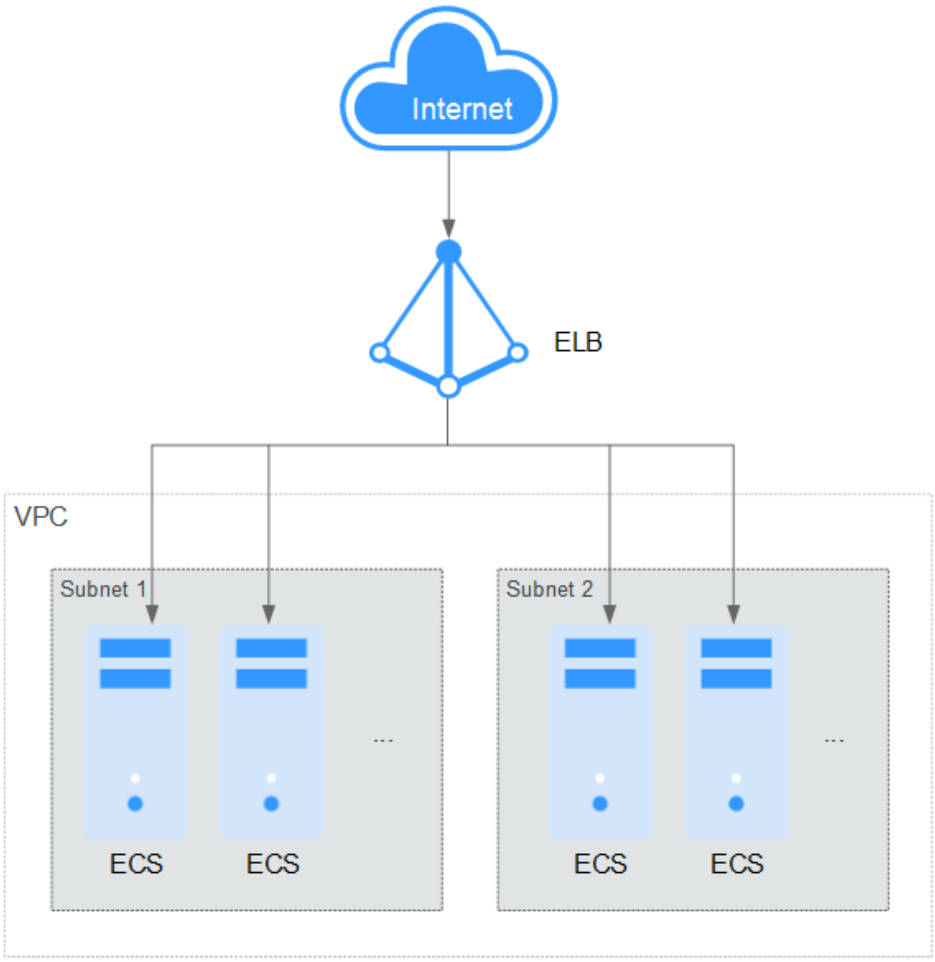


- Multiple ECSs balance workloads.

  In high-concurrency scenarios, such as e-commerce, you can use load balancers to distribute incoming traffic across multiple ECSs, allowing a large number of users to concurrently access your business system or application. ELB deeply integrates with the Auto Scaling (AS) service, which enables automatic scaling based on service traffic and ensures service stability and reliability.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-2 ELB



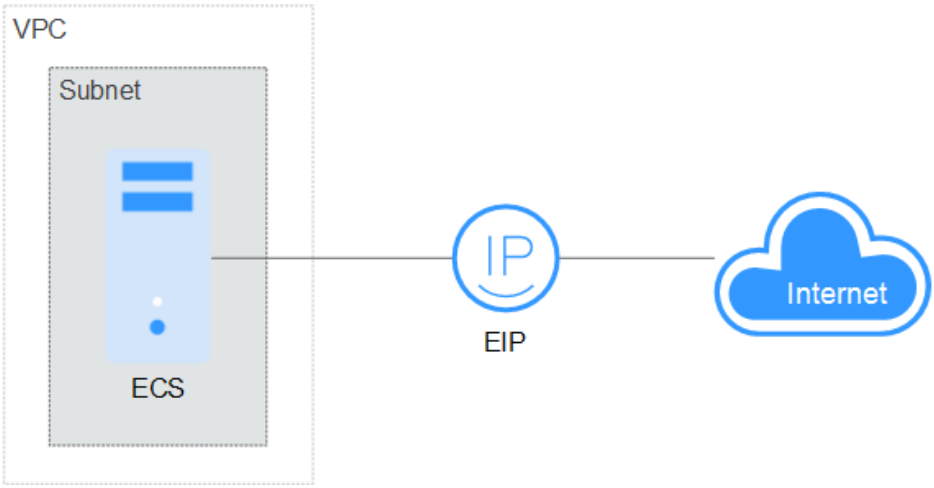
Accessing the Internet

- Single ECS accesses the Internet.

  When an ECS needs to access the Internet, you can bind an EIP to the ECS so that the ECS can access the Internet. Huawei Cloud allows your EIP to be billed on a pay-per-use basis. If you do not need to use the EIP, you can flexibly unbind it.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-3 EIP

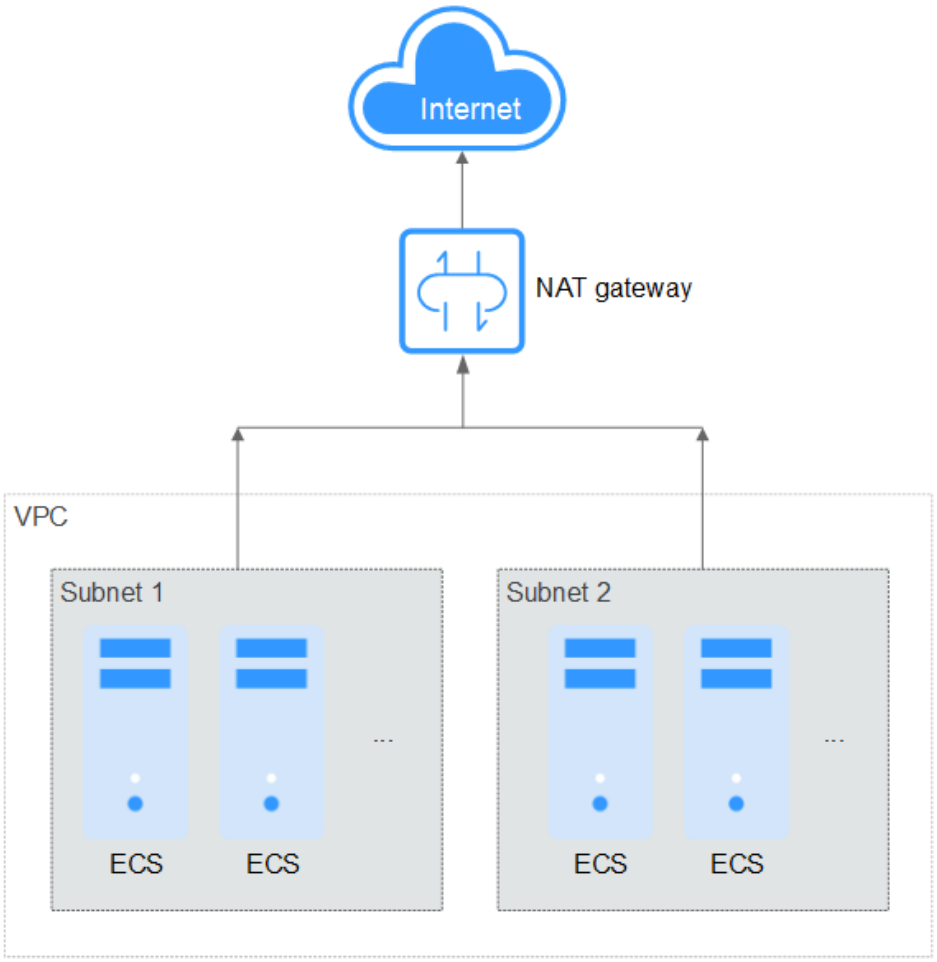


- Multiple ECSs access the Internet.

  If multiple ECSs in your VPC need to access the Internet, you can use a NAT gateway and configure SNAT rules by subnet to allow ECSs in the VPC to access the Internet. If you access to the Internet using an EIP but with no DNAT rules configured, external users cannot directly access the public network address of the NAT gateway through the Internet, ensuring ECS security.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-4 NAT gateway



Copyright © Huawei Technologies Co., Ltd.

2 Lower Public Network Costs

You can select a proper bandwidth and billing mode based on your service requirements.

Shared Bandwidth

A shared bandwidth is an independent bandwidth product. You can **add pay-per-use EIPs to a shared bandwidth** to allow the EIPs to share the bandwidth. You can bind EIPs to resources such as ECSs, NAT gateways, and load balancers so that these resources can use the shared bandwidth. For more information, see **Shared Bandwidth Overview**.

Table 2-1 describes the scenarios and cost savings of different billing modes of shared bandwidth.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-1 Examples of cost savings when you use a shared bandwidth

Billing Mode	Scenario	Example
Pay-per-use (billed by bandwidth)	You host a large number of applications on the cloud. If each ECS uses a dedicated bandwidth, a lot of bandwidths are required, which incurs high costs. You can add your instances to a pay-per-use shared bandwidth (billed by bandwidth). This can reduce network operations costs especially for workloads with different traffic peaks and troughs.	**Using pay-per-use EIPs (billed by bandwidth), each with a dedicated bandwidth:** Assume that you have 10 ECSs in CN-Hong Kong and each ECS has an EIP bound. Each EIP is billed by bandwidth with a maximum value of 100 Mbit/s. In this case, you need to pay the price of 10 EIPs each with a maximum bandwidth of 100 Mbit/s, that is, $788 USD per day. **Using a pay-per-use shared bandwidth (billed by bandwidth):** Traffic analysis of 10 EIPs shows services reach peaks and troughs at different times. The peak outbound bandwidth of the 10 ECSs to the Internet is about 500 Mbit/s. You only need to purchase one shared bandwidth of 500 Mbit/s for the 10 ECSs to share. Each ECS can enjoy a peak bandwidth 5 times higher than the original one, and you only need to pay $408 USD per day for the 500 Mbit/s of shared bandwidth, saving $380 USD per day, or about 48% of the bandwidth cost.

Copyright © Huawei Technologies Co., Ltd.

Billing Mode	Scenario	Example
Pay-per-use (billed by enhanced 95th percentile bandwidth)	The peak bandwidth is not limited. The billing is based on bandwidth usage excluding peak values. Your services have frequent traffic bursts, which makes bandwidth upper limit hard to estimate. If the upper limit is set too high, bandwidths will be wasted. If the upper limit is set too low, there will be packet loss, affecting service expansion and user experience. In this case, you can use a pay-per-use shared bandwidth (billed by enhanced 95th percentile bandwidth).	**Using a pay-per-use shared bandwidth (billed by bandwidth):** Assume that you buy a pay-per-use shared bandwidth of 500 Mbit/s and use it for one month (30 days). You need to pay $12,240 USD. **Using a pay-per-use shared bandwidth (billed by enhanced 95th percentile bandwidth):** Traffic analysis shows that traffic fluctuates greatly, but the bandwidth is within 400 Mbit/s in most stable states. You can purchase a shared bandwidth of 400 Mbit/s billed by enhanced 95th percentile bandwidth on a pay-per-use basis. The price is $9,720 USD per month. This is about 20% lower than that of a pay-per-use shared bandwidth billed by bandwidth.
Yearly/ Monthly (billed by bandwidth)	For long-term workloads with stable traffic, you can select a yearly/monthly shared bandwidth (billed by bandwidth).	**Using a pay-per-use shared bandwidth (billed by bandwidth):** Assume that you buy a pay-per-use shared bandwidth of 500 Mbit/s and use it for one month (30 days). You need to pay $12,240 USD. **Using a yearly/monthly shared bandwidth (billed by bandwidth):** You can buy a yearly/monthly shared bandwidth of 500 Mbit/s for one month at $8,100 USD. This is about 34% lower than that of a pay-per-use shared bandwidth billed by bandwidth.

NOTICE

The prices are just for your reference. See the actual prices by visiting **EIP Pricing Details**.

Copyright © Huawei Technologies Co., Ltd.

Shared Data Package

A shared data package provides a quota for data usage. Such packages are cost-effective and easy to use.

Shared data packages can only be used by **pay-per-use dedicated bandwidths billed by traffic**. After a shared data package takes effect, bandwidths will use the shared data package first. For more information about shared data packages, see **Shared Data Package**.

- **How Much Can I Save by Using a Shared Data Package?**

  The price of a shared data package is affordable and cost-effective.

  If you purchase a pay-per-use EIP bandwidth (billed by traffic) of $0.153 USD per GB, you need to pay $15.3 USD for 100 GB. You only need to pay $13.8 USD for a 100 GB shared data package. This is about 10% cheaper than the pay-per-use EIP bandwidth billed by traffic.

  NOTICE

  The prices are just for your reference. See the actual prices by visiting **EIP Pricing Details**.

- **What Are the Application Scenarios of a Shared Data Package?**

  You can use shared data packages for **pay-per-use EIP bandwidths (billed by traffic)**. You can save more money by using more traffic in scenarios, such as promotions and live streaming.

- **Notes on Using Shared Data Packages**
  - **Package validity**: A shared data package is valid for one month or one year from purchase. Expired shared data packages will longer be available for use.

    To avoid waste, you can evaluate usage history, start with a smaller package, and increase the package size if needed.
  - **Usage sequence**: If there are multiple shared data packages, the one that expires earliest is used first.
  - **Billing**: If shared data packages are used up, resources using packages will be billed on a pay-per-use basis (billed by traffic). Your service will not be interrupted.

Example of Public Network Cost Saving

The table below recommends bandwidths for various scenarios. You can choose one based on your service needs and adjust as necessary to optimize resource use and costs.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-2 Recommended bandwidth in different scenarios

Scenarios	Traffic Feature	Recommended Solution
Enterprise or SaaS applications	The traffic peak is stable and the usage period is long.	• Use a **yearly/monthly** dedicated bandwidth or shared bandwidth. • If there are temporary service bursts, increase the bandwidth by **paying the price difference** and **reduce the bandwidth** after the service is complete.
E-commerce platforms and gaming services	Traffic shows strong, periodic fluctuations, while services require long-term deployment.	Use a shared bandwidth billed by **bandwidth** or **95th percentile bandwidth (enhanced)** to reduce costs.
E-commerce and gaming promotions	The traffic fluctuates greatly and the service period is short.	Use a **pay-per-use** dedicated bandwidth **(billed by traffic)**. You can also use a **shared data package** to provide quota for resources in the same region under the same account to reduce costs.

Copyright © Huawei Technologies Co., Ltd.

3 Using IPv6 EIPs to Enable On-premises Data Centers to Provide Internet-Accessible Services

Scenarios

You can use the IPv6 function of the EIP service to map existing IPv4 EIPs into IPv6 EIPs. After the IPv6 EIP function is enabled, you will obtain both an IPv4 EIP and its corresponding IPv6 EIP. External IPv6 addresses can access cloud resources through this IPv6 EIP.

If existing services in an on-premises data center (IDC) cannot be migrated to the cloud because they use IPv4 addresses and also the IPv4/IPv6 dual-stack reconstruction cannot be completed for these services in a short period, you can use IPv6 EIPs to connect to the on-premises data center. Then, the data center can provide internet-accessible services using IPv6 EIPs without the need to reconstruct the existing IPv4 network.

Architecture

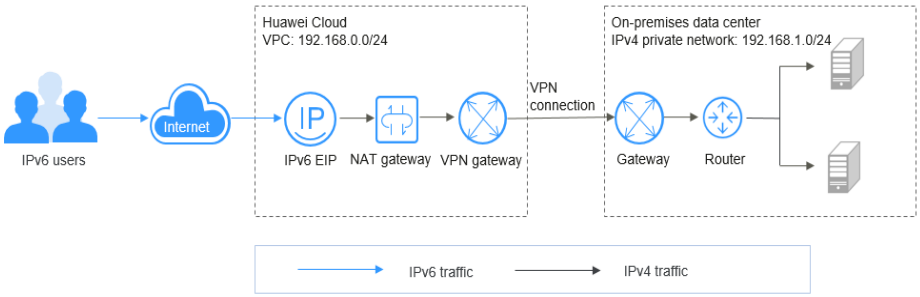
1. A virtual private network (VPN) connects an on-premises data center to a VPC.
2. A NAT gateway in the VPC uses an IPv6 EIP to provide internet-accessible services.

NOTE

- IPv6 EIPs can only be used to provide internet-accessible services and cannot access IPv6 addresses.
- The CIDR block of an on-premises data center cannot overlap with that of the VPC subnet. Otherwise, the communication between them will fail.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-1 Networking diagram



Advantages

The IPv6 EIP function allows on-premises data centers to provide services for both IPv4 and IPv6 users on the Internet, without the need to reconstruct their existing IPv4 networks.

Constraints

After IPv6 EIP is enabled, inbound and outbound security group rules need to be added to allow packets to and from the IP addresses in 198.19.0.0/16. IPv6 EIP uses NAT64 to convert the source IPv6 address in the inbound direction to an IPv4 address in the IP address range 198.19.0.0/16. The source port can be a random one, the destination IP address is the private IPv4 address of your local server, and the destination port remains unchanged.

Table 3-1 Security group rules

Direction	Protocol	Source and Destination
Inbound	All	Source: 198.19.0.0/16
Outbound	All	Destination: 198.19.0.0/16

Resource Planning

Table 3-2 Resources

Resource	Resource Name	Description	Quantity
VPC	VPC-Test01	This VPC (192.168.0.0/24) will have an EIP and a NAT gateway deployed.	1
EIP	EIP-IPv4&IPv6	This is an IPv4 EIP. To obtain a corresponding IPv6 EIP, enable the IPv6 EIP function.	1
NAT gateway	NAT-Test	This public NAT gateway will have an EIP bound.	1

 Copyright © Huawei Technologies Co., Ltd.

Resource	Resource Name	Description	Quantity
VPN gateway	VPN-GW-Test	This VPN gateway is an egress gateway in a VPC and allows reliable and encrypted communications between a VPC and an on-premises data center.	1
VPN connection	VPN-Test	This VPN connection quickly builds a reliable and encrypted communications channel between a VPN gateway and a remote gateway.	1
On-premises data center	IDC-Test	This on-premises data center (192.168.1.0/24) includes remote gateways, routers, and backend servers.	1

Operation Process

1. **Buy an EIP and enable the IPv6 EIP function.**
2. **Configure a VPN.**
3. **Configure a public NAT gateway.**

Procedure

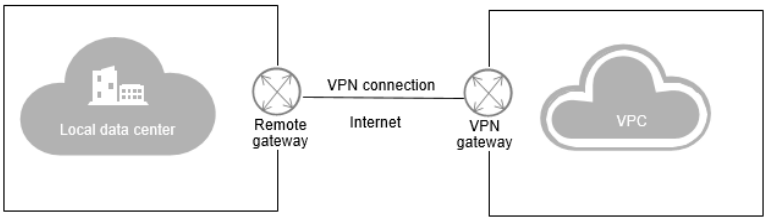
1. **Buy an EIP and enable the IPv6 EIP function.**

   Buy an EIP with the required bandwidth and select the **IPv6 EIP** option.

   For details, see **Assigning an EIP**.

2. **Configure a VPN.**

   A VPN consists of a VPN gateway and one or more VPN connections. A VPN gateway provides an internet egress for a VPC and works together with the gateway in the on-premises data center.

   a. Create a VPC.

      Set the VPC CIDR block to 192.168.0.0/24. The CIDR block of the on-premises data center is 192.168.1.0/24.

      The CIDR block of an on-premises data center cannot overlap with that of the VPC subnet. Otherwise, the communication between them will fail.

 Copyright © Huawei Technologies Co., Ltd.

For details, see **Creating a VPC**.

b. Create a VPN gateway.

VPC: Select the VPC created in **2.a**.

Bandwidth: Select the bandwidth based on your service requirements.

For details, see **Buying a VPN Gateway**.

c. Create a VPN connection.

Local Subnet: Select subnets or manually enter CIDR blocks, for example, **192.168.0.0/24,198.19.0.0/16**.

Remote Gateway: Set it to public IP address of the gateway in the data center.

Remote Subnet: Set it to the CIDR block 192.168.1.0/24 of the data center.

For details, see **Creating a VPN Connection**.

NOTE

After the IPv6 EIP function is enabled, the source IP address will be translated into one in the IP address range 198.19.0.0/16. Therefore, you need to enter the VPC subnet and then the IP address range 198.19.0.0/16 in sequence in the **Local Subnet** area.

d. Configure the VPN device in the data center.

After configuring the VPN on the cloud, you need to configure the VPN device in the IDC. For details, see **Virtual Private Network Administrator Guide**.

3. **Configure a public NAT gateway.**

After purchasing a public NAT gateway, you can add DNAT rules to enable your servers in the VPC or servers in your data center that are connected to the VPC to provide internet-accessible services.

a. Buy a public NAT gateway.

VPC: Select the VPC created in **2.a**.

Subnet: Select a subnet in the VPC created in **2.a**.

For details, see **Buying a Public NAT Gateway**.

b. Add a DNAT rule.

Select the EIP purchased in **1** and add a DNAT rule based on the private IP address and port of the data center. For example, you can set **Port Type** to **Specific port**, **Protocol** to **TCP**, **Private IP Address** to **192.168.1.22**, and select the EIP to be associated.

For details, see **Adding a DNAT Rule**.

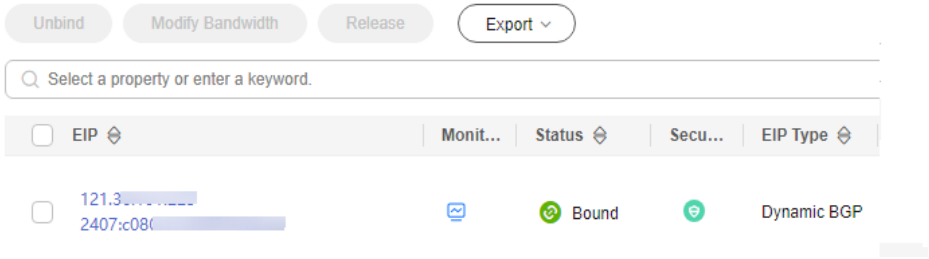
Verification

After the preceding operations are complete, the IPv6 EIPs can be used to provide internet-accessible services.

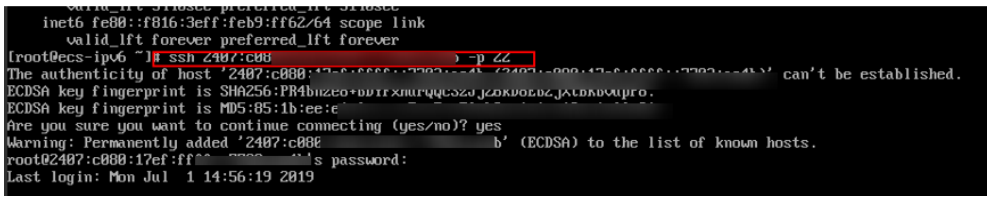
You can query the IPv6 addresses on the **EIPs** page.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-2 IPv6 addresses



Use an IPv6 client that can access the internet to test the connectivity of the IPv6 EIP.



 Copyright © Huawei Technologies Co., Ltd.

4 Using a Shared Bandwidth to Enable ECSs to Access the Internet via the Same Network Egress

Scenarios

A shared bandwidth allows multiple EIPs in the same region to share the same bandwidth. After a shared bandwidth is assigned, you can add multiple EIPs in the same region to the shared bandwidth. In this way, multiple EIPs can share the same bandwidth and their public network egresses can be managed in a unified manner. You can bind EIPs to ECSs, NAT gateways, or load balancers. After the EIPs are bound, these instances share the same bandwidth.

This section describes how to use shared bandwidths to provide unified public network egresses for ECSs.

Scenario 1: ECSs with EIPs Bound Using a Shared Bandwidth

If you have ECSs that have EIPs bound, you can add these EIPs to a shared bandwidth to manage the public network egress in a unified manner.

Configuration Process

Figure 4-1 Configuration process for ECSs with EIPs bound using a shared bandwidth

Procedure

1. Buy a shared bandwidth in the region where the ECSs are located.
   For details, see **Assigning a Shared Bandwidth**.
2. Add the EIPs bound to the ECSs to the shared bandwidth.
   For details, see **Adding EIPs to a Shared Bandwidth**.

 Copyright © Huawei Technologies Co., Ltd.

Scenario 2: ECSs Without EIPs Bound Using a Shared Bandwidth

If you have ECSs that need to have EIPs bound, you can add the EIPs to a shared bandwidth when assigning the EIPs to manage the public network egress in a unified manner.

Configuration Process

Figure 4-2 Configuration process for ECSs without EIPs bound using a shared bandwidth

Procedure

1. Buy a shared bandwidth in the region where the ECSs are located.

   For details, see **Assigning a Shared Bandwidth**.
2. Buy EIPs and add them to the shared bandwidth.
   a. If there are **no available EIPs** in the region where the ECS is located, **buy an EIP** and add it to the shared bandwidth.
   b. If there are **available EIPs** in the region where the ECS instance is located, select an EIP and **add it to the shared bandwidth**.
3. Bind the EIPs to the ECS.

   For details, see **Binding an EIP to an Instance**.

Related Operations

Unbinding an EIP from an Instance: Unbind an EIP when the EIP is no longer required.

Releasing or Unsubscribing From an EIP: Release a pay-per-use EIP or unsubscribe from a yearly/monthly EIP when the EIP is no longer required.

Copyright © Huawei Technologies Co., Ltd.