Elastic IP

Best Practices

Issue	01
Date	2020-09-01

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.

Contents

1 Public Network Access

Products

The public cloud provides EIP, NAT Gateway, and ELB services 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, or 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 check the running state of backend servers to ensure that requests are sent only to healthy servers.

- NAT Gateway

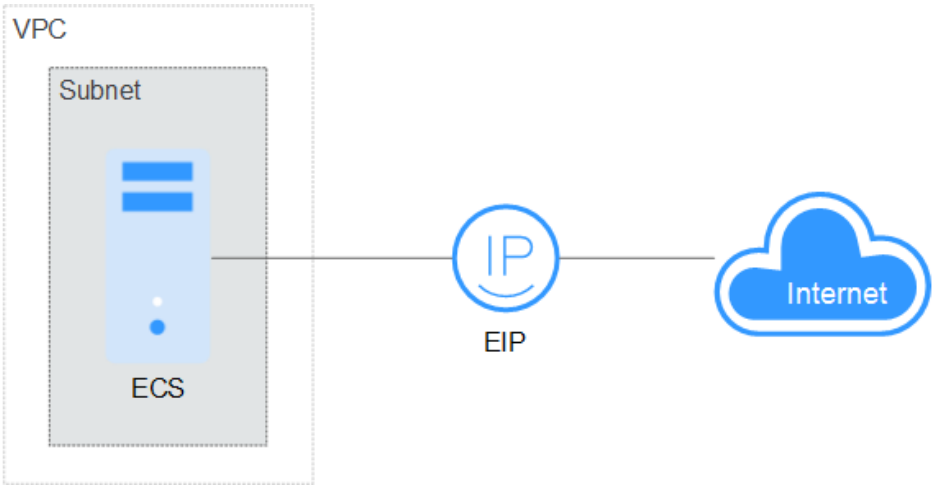
  NAT Gateway provides both SNAT and DNAT for your resources in a VPC and allows servers in your VPC to access or provide services accessible from the Internet.

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.

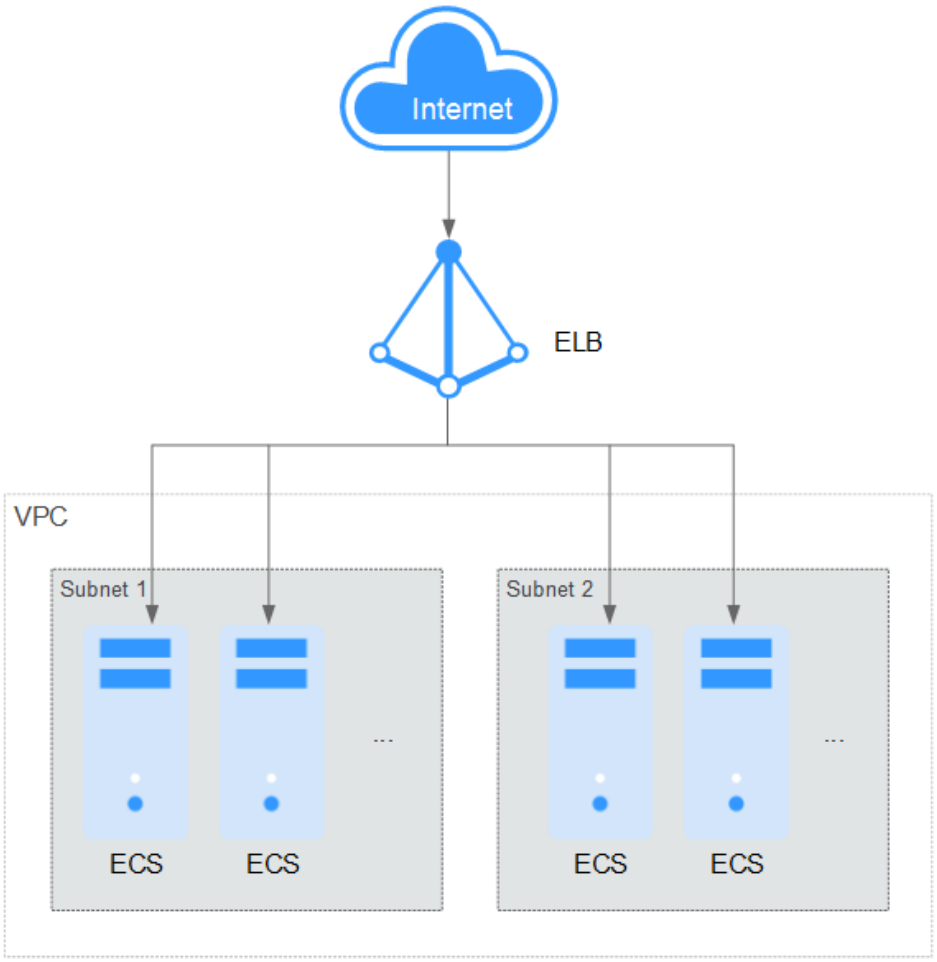
Figure 1-1 EIP



- Multiple ECSs balance workloads.

  In high-concurrency scenarios, such as e-commerce, you can use load balancers provided by the ELB service to evenly 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.

Figure 1-2 ELB

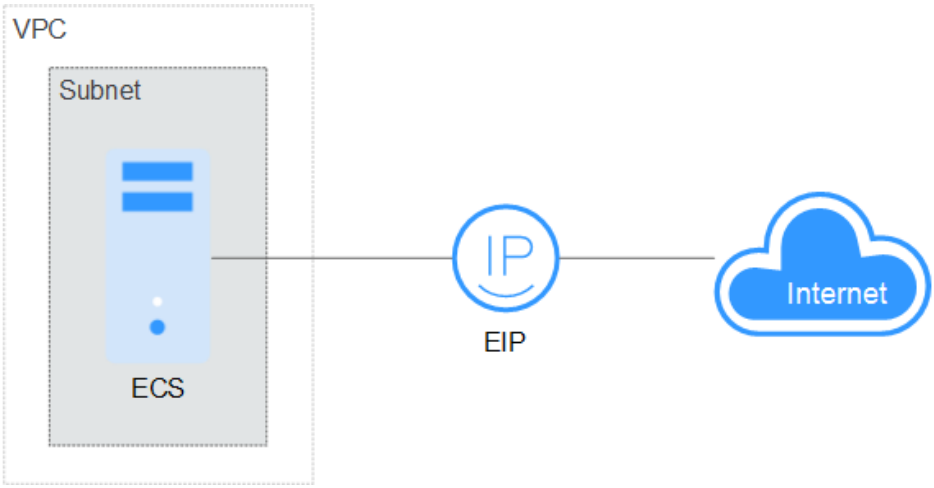


Accessing the Internet

- 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 based on bandwidth usage or amount of traffic. If you do not need to use the EIP, you can flexibly unbind it.

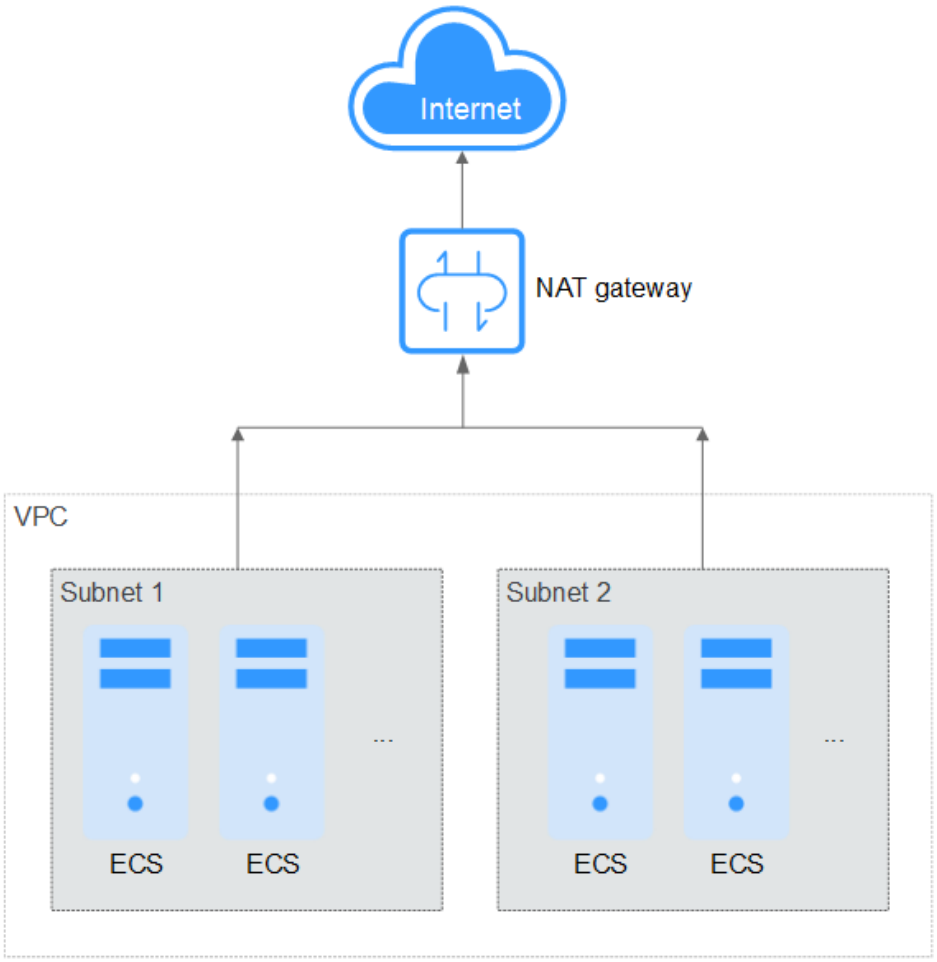
Figure 1-3 EIP



- 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.

Figure 1-4 NAT gateway



2 Lower Network Costs

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

Dedicated Bandwidth

If you want to ensure the bandwidth available for a particular EIP, you are advised to purchase dedicated bandwidth. Dedicated bandwidth can only be used for a single, specific EIP. Dedicated bandwidth is not affected by other services.

An EIP can be billed by bandwidth or by traffic:

- Bandwidth: If your services use a large amount of traffic but are stable, an EIP billed by bandwidth is recommended.
- Traffic: If your services only use a relatively small amount of traffic, an EIP billed by traffic combined with a shared data package is recommended for a more favorable price.

If your traffic is stable, the yearly/monthly billing based on the bandwidth is more cost effective.

Shared Bandwidth

When you host a large number of applications on the cloud, if each EIP uses dedicated bandwidth, a lot of bandwidths are required, which incurs high costs. If all EIPs share the same bandwidth, your network operation costs will be lowered and your system O&M as well as resource statistics will be simplified. Multiple EIPs whose billing mode is pay-per-use can be added to a shared bandwidth. You can bind EIPs to products such as ECSs, NAT gateways, and load balancers so that these products can use the shared bandwidth.

A shared bandwidth can be billed by bandwidth or by 95th percentile bandwidth:

- Bandwidth: If you use a large number of EIPs and their peak hours are different, use shared bandwidth to greatly reduce costs.
- 95th percentile bandwidth (enhanced): If your services frequently reach peaks, you can select this option. This ensures that the service system is not affected by the bandwidth limit at service peaks and avoids the cost waste associated with excessive peak bandwidth peaks.

Shared Data Package

A shared data package is a prepaid package for public network traffic. The price of the package is lower than that for the postpaid billing by traffic. Shared data packages greatly reduce the cost of traffic on a public network. A shared data package takes effect immediately after being purchased and no additional operations are required. If you have subscribed to pay-per-use EIPs using bandwidth billed by traffic in a region and buy a shared data package in the same region, the EIPs will use the shared data package.

- When to use a shared data package

  After a shared data package takes effect for a bandwidth billed by traffic, the traffic used by the bandwidth is deducted from the shared data package first. After the shared data package is used up, the bandwidth is billed by the amount of traffic used. A shared data package saves more if your amount of traffic used is huge.

- Additional notes on shared data packages
  - Only the traffic generated in the region selected when the shared data package is purchased can be deducted.
  - Dynamic and static shared data packages are used to deduct the traffic generated by dynamic BGP and static BGP EIPs, respectively.
  - A shared data package has a validity period of one calendar month or one calendar year from the date of purchase. After this period expires, the unused traffic expires as well and cannot be used. You are advised to evaluate the size of a shared data package required based on the historical usage.
  - A shared data package will not be renewed automatically. If you are uncertain which package to purchase, buy a small one the first time.
  - After a shared data package is used up, your service will not automatically stop. The system automatically bills you based on traffic, ensuring service system availability.

3 On-premises IDCs Providing Internet-Accessible Services Using IPv6 EIPs

Scenario

The IPv6 function of the EIP service can map IPv4 addresses into IPv6 addresses. Enabling the IPv6 EIP function allows you to obtain both IPv4 and IPv6 EIPs.

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, IPv6 EIPs can be used to connect to the on-premises IDC. Then, the on-premises IDC can provide Internet-accessible services using IPv6 EIPs without the need to reconstruct the existing IPv4 network.

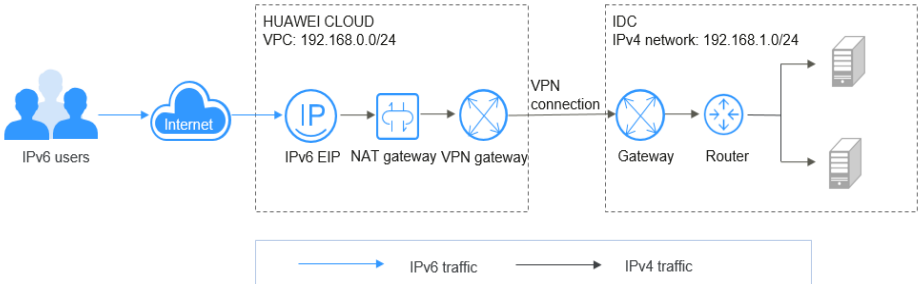
Network Topology

In the following example, the IDC CIDR block is 192.168.1.0/24, and the VPC CIDR block is 192.168.0.0/24.

The deployment diagram is as follows:

1. A virtual private network (VPN) connects an IDC to a VPC.
2. A NAT gateway in the VPC uses an IPv6 EIP to provide Internet-accessible services.

Figure 3-1 Networking



NOTE

- The IPv6 EIP can only be used to provide Internet-accessible services and cannot access IPv6 addresses.
- The network CIDR block of the IDC does not overlap with the subnet CIDR block of the VPC on the cloud. Otherwise, the communication between the IDC and the VPC will fail.

Prerequisites

You need to add security group rules to allow inbound traffic from and outbound traffic to the network 198.19.0.0/16. The IPv6 EIP uses NAT64, which converts the source IP address in the inbound rule into an IPv4 address in the IP address range **198.19.0.0/16**, converts the source port to a random port, and converts the destination IP address to a private IPv4 address of your local machine. The destination port remains the same.

Procedure

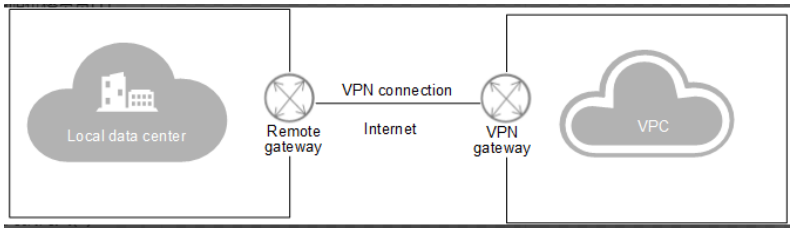
1. **Buy an EIP.**

   Buy an EIP with the required bandwidth and select **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 local data center.

   a. Create a VPC.

      Create a VPC and set its CIDR block to 192.168.0.0/24. The IDC private network is 192.168.1.0/24.

      The network CIDR block of the IDC does not overlap with the subnet CIDR block of the VPC on the cloud. Otherwise, the communication between the IDC and the VPC will fail.

      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 **Creating a VPN Gateway**.

   c. Create a VPN connection.

      Local Subnet: Select a subnet or manually specify a CIDR block, for example, 192.168.0.0/24,192.19.0.0/16.

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

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

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

NOTE

After the IPv6 function is enabled for the EIP, 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 IDC.

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 NAT gateway.**

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

a. Buy a NAT gateway.

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

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

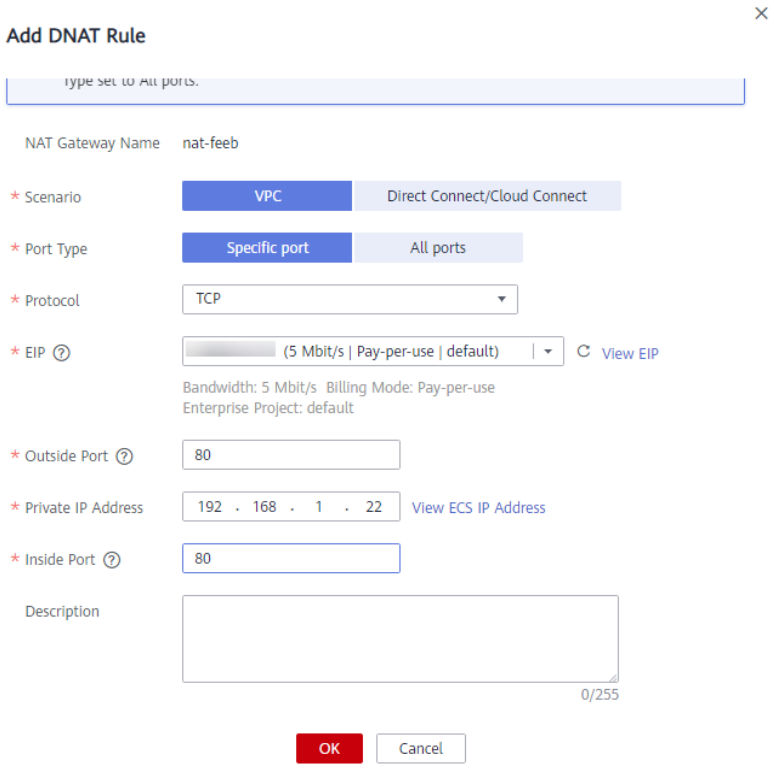
For details, see **Buying a NAT Gateway**.

b. Add a DNAT rule.

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

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

Figure 3-2 Add DNAT Rule

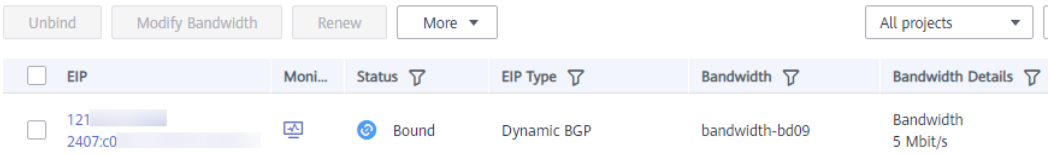


Verification

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

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

Figure 3-3 IPv6 addresses



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