NAT Gateway

Service Overview

Issue 01

Date 2025-11-03

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

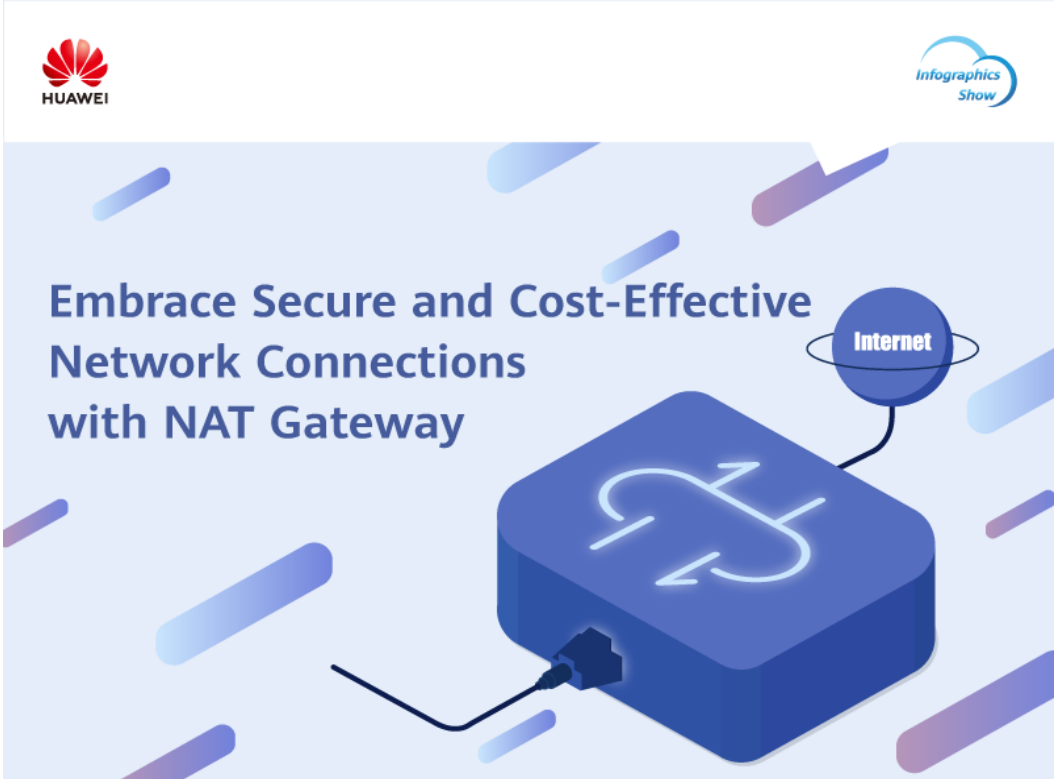
Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud 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 NAT Gateway Infographics



What Is NAT Gateway?

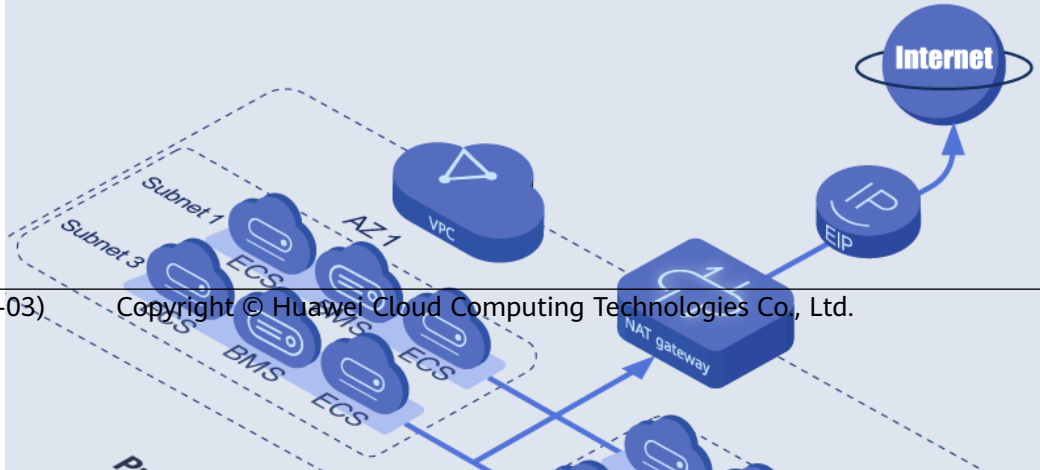
NAT Gateway provides network address translation (NAT).

Public NAT Gateway

Public NAT gateways provide NAT for servers in a VPC or on-premises servers that connect to the cloud through Direct Connect or Virtual Private Network (VPN), allowing multiple servers to share EIPs for Internet connectivity.

Public NAT gateways support **source NAT (SNAT)** and **destination NAT (DNAT)**.

SNAT translates private IP addresses into EIPs, allowing servers within an AZ or across multiple AZs in a VPC to share EIPs to access the Internet.



2 What Is NAT Gateway?

NAT Gateway is a network address translation (NAT) service. It can be a public NAT gateway or a private NAT gateway.

Video Tutorial

This video introduces what NAT Gateway is.

Public NAT Gateways

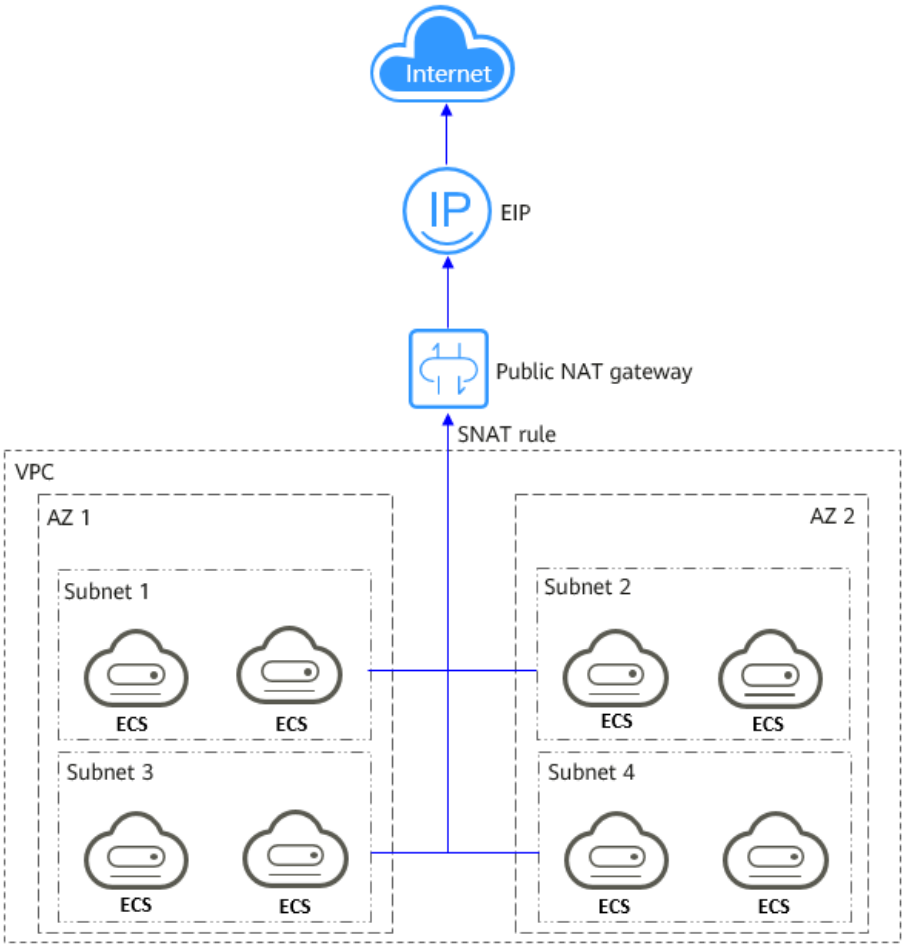
A public NAT gateway enables cloud and on-premises servers in a private subnet to share an EIP to access the Internet or provide services accessible from the Internet. Cloud servers are ECSs and BMSs in a VPC. On-premises servers are servers in on-premises data centers that connect to a VPC through Direct Connect or Virtual Private Network (VPN). A public NAT gateway supports up to 20 Gbit/s of bandwidth.

Public NAT gateways offer source NAT (SNAT) and destination NAT (DNAT).

- SNAT translates private IP addresses into EIPs so that traffic from a private network can go out to the Internet.

  Figure 2-1 shows how an SNAT rule works.

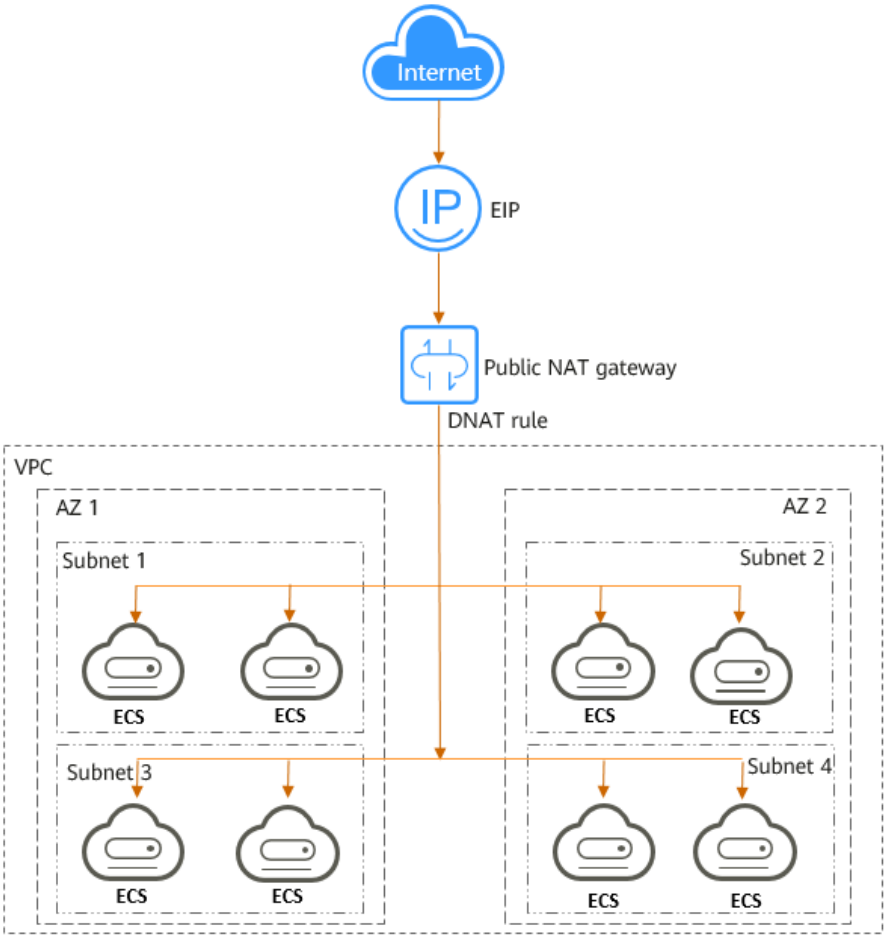
Figure 2-1 NAT gateway with an SNAT rule



- DNAT enables servers in a VPC, regardless of if they are in the same AZ, to share an EIP to provide services accessible from the Internet. With an EIP, a public NAT gateway forwards the Internet requests from only a specific port and over a specific protocol to a specific port of a server, or it can forward all requests to the server regardless of which port they originated on.

  Figure 2-2 shows how a DNAT rule works.

Figure 2-2 NAT gateway with a DNAT rule



Private NAT Gateways

Private NAT gateways provide network address translation, allowing ECSs and BMSs in a VPC to communicate with servers in other VPCs or on-premises data centers. You can configure SNAT and DNAT rules for a NAT gateway to translate the source and destination IP addresses of originating packets into a transit IP address.

Specifically,

- SNAT enables servers in a VPC, regardless of if they are in the same AZ, to share a transit IP address to access on-premises data centers or other VPCs.
- DNAT enables servers in a VPC, regardless of if they are in the same AZ, to share the same transit IP address to provide services accessible from on-premises data centers or other VPCs.

Transit Subnet

A transit subnet is a transit network and is the subnet to which the transit IP address belongs.

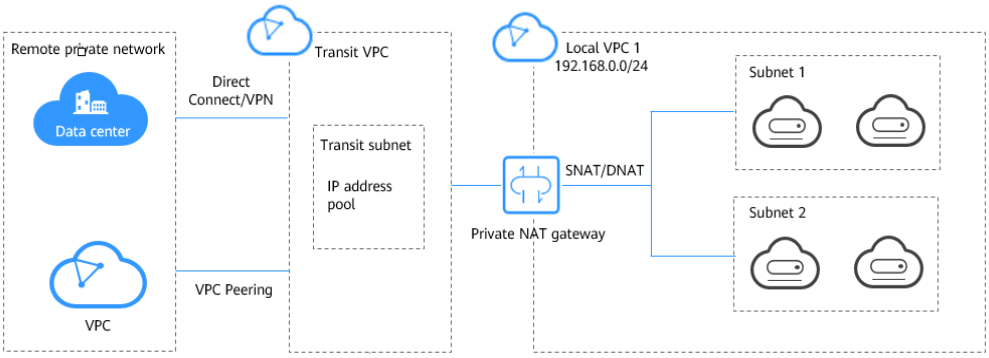
Transit IP Address

A transit IP address is a private IP address that can be assigned from a transit subnet. Cloud servers in your VPC can share a transit IP address to access on-premises networks or other VPCs.

Transit VPC

A transit VPC is where a transit subnet belongs to.

Figure 2-3 Private NAT gateway



How Do I Access the NAT Gateway Service?

You can access the NAT Gateway service through the management console or using HTTPS-based APIs.

- Management console

  Log in to the management console and choose **NAT Gateway** from the service list.

- APIs

  If you need to integrate NAT Gateway on the cloud platform into your own system, use APIs to access NAT Gateway. For details, see **NAT Gateway API Reference**.

Getting Started with NAT Gateways

- **Using a Public NAT Gateway to Enable Servers to Share One or More EIPs to Access the Internet**
- **Using DNAT to Enable Servers to Be Accessed by the Internet**
- **Using a Private NAT Gateway to Connect Cloud and On-premises Networks**

3 NAT Gateway Advantages

Advantages of Public NAT Gateways

- **Flexible deployment**

  A NAT gateway can be shared across subnets and AZs, so that even if an AZ fails, the public NAT gateway can still run normally in another AZ. The specifications and EIP of a public NAT gateway can be changed at any time.

- **Ease of use**

  Multiple NAT gateway specifications are available. Public NAT gateway configuration is simple, the operation & maintenance is easy, and they can be provisioned quickly. Once provisioned, they can run stably.

- **Cost-effectiveness**

  Servers can share one EIP to connect to the Internet. You no longer need to configure one EIP for each server, which saves money on EIPs and bandwidth.

Advantages of Private NAT Gateways

- **Easier network planning**

  Different departments in a large enterprise may have overlapping CIDR blocks, so the enterprise has to replan its network before migrating their workloads to the cloud. The replanning is time-consuming and stressful. The private NAT gateway eliminates the need to replan the network so that customers can retain their original network while migrating to the cloud.

- **Easy operation & maintenance**

  Departments of a large enterprise usually have hierarchical networks for hierarchical organizations, rights- and domain-based management, and security isolation. Such hierarchical networks need to be mapped to a large-scale network for enabling communication between them. A private NAT gateway can map the CIDR block of each department to the same VPC CIDR block, which simplifies the management of complex networks.

- **Strong security**

  Departments of an enterprise may need different levels of security. Private NAT gateways can expose the IP addresses and ports of only specified CIDR blocks to meet high security requirements. An industry regulation agency may require other organizations to use a specified IP address to access their regulation system. Private NAT gateways can help meet this requirement by mapping private IP addresses to that specified IP address.

- **Zero IP conflicts**

  Isolated services of multiple departments usually use IP addresses from the same private CIDR block. After the enterprise migrates workloads to the cloud, IP address conflicts occur. Thanks to IP address mapping, the private NAT gateways allow for communication between overlapping CIDR blocks.

4 Application Scenarios

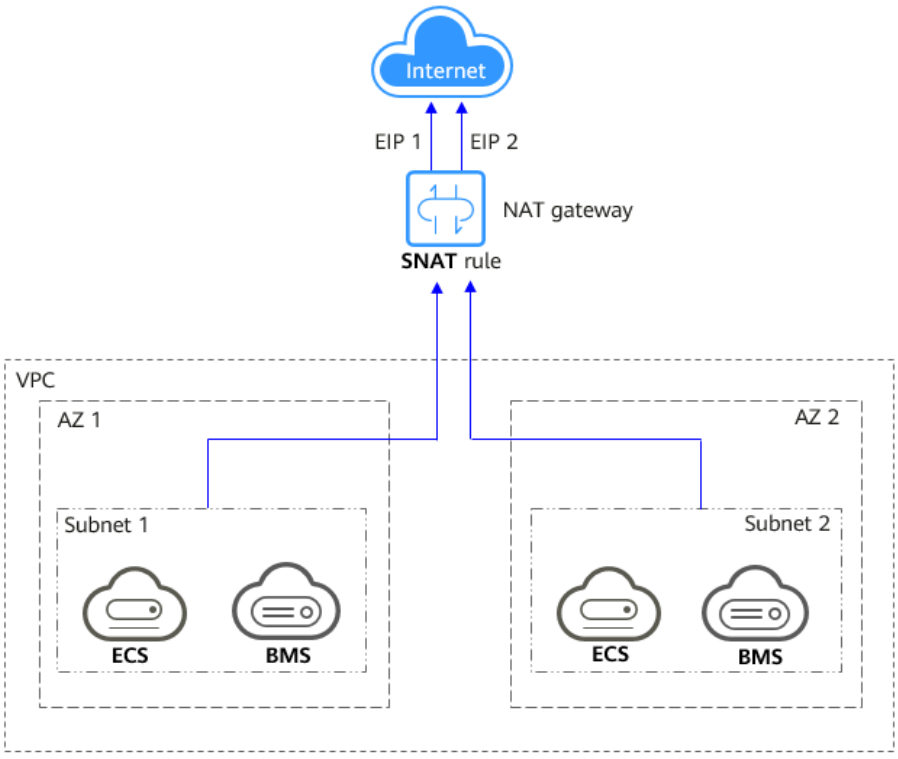
Public NAT Gateway

- **Allowing a private network to access the Internet using SNAT**

  If your servers in a VPC need to access the Internet, you can configure SNAT rules to let these servers use EIPs to access the Internet without exposing their private IP addresses. You can configure only one SNAT rule for each subnet in a VPC and select one or more EIPs for each SNAT rule. Public NAT Gateway provides different numbers of connections, and you can create multiple SNAT rules to meet your service requirements.

  Figure 4-1 shows how servers in a VPC access the Internet using SNAT.

  Figure 4-1 Allowing a private network to access the Internet using SNAT



- **Allowing Internet users to access a service in a private network using DNAT**

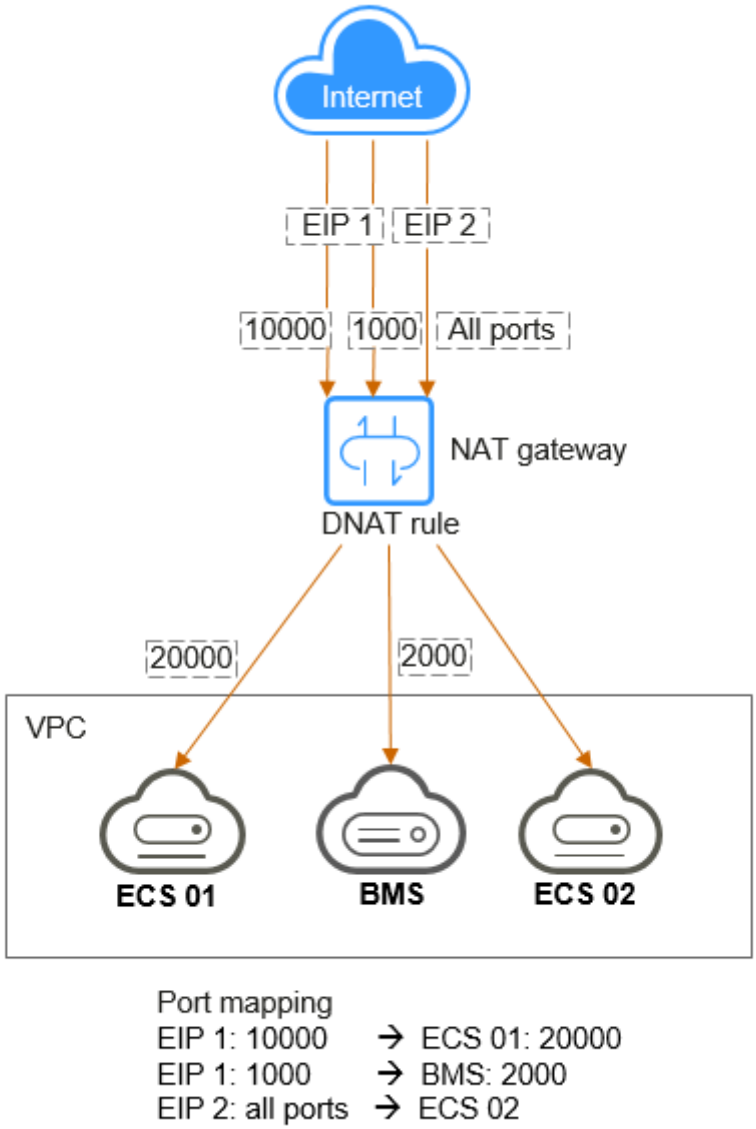
  DNAT rules enable servers in a VPC to provide services accessible from the Internet.

  After receiving requests from a specific port over a specific protocol, the public NAT gateway can forward the requests to a specific port of a server through port mapping. The public NAT gateway can also forward all requests destined for an EIP to a specific server through IP address mapping.

  One DNAT rule can be configured for each server. If there are multiple servers, you can create multiple DNAT rules to map one or more EIPs to the private IP addresses of these servers.

  Figure 4-2 shows how servers (ECSs or BMSs) in a VPC provide services accessible from the Internet using DNAT.

Figure 4-2 Allowing Internet users to access a service in a private network using DNAT

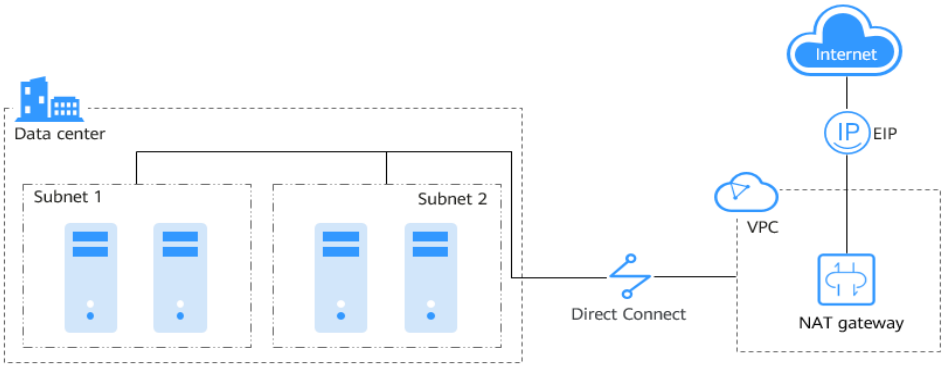


- **Allowing on-premises servers to communicate with the Internet**

  In certain Internet, gaming, e-commerce, and financial scenarios, a large number of servers in a private cloud are connected to a VPC through Direct Connect or VPN. If such servers need secure, high-speed Internet access or need to provide services accessible from the Internet, you can deploy a NAT gateway and configure SNAT and DNAT rules to meet their requirements.

  Figure 4-3 shows how to use SNAT and DNAT to provide high-speed Internet access or provide services accessible from the Internet.

Figure 4-3 Allowing on-premises servers to communicate with the Internet



- **Setting up a highly available system by adding multiple EIPs to an SNAT rule**

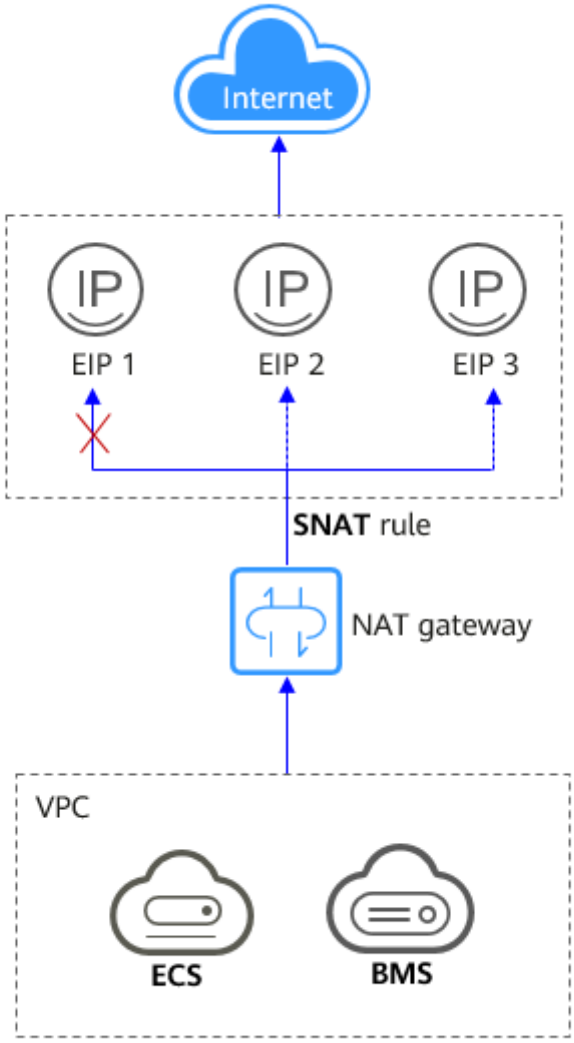
  EIPs may be attacked. To improve system reliability, you can bind multiple EIPs to an SNAT rule so that if one EIP is attacked, another EIP can be used to ensure service continuity.

  Each SNAT rule can have up to 20 EIPs. If an SNAT rule has multiple EIPs, the system randomly selects one EIP for servers to use to access the Internet.

  If any EIP is blocked or attacked, manually remove it from the EIP pool.

  Figure 4-4 shows a highly available system using an SNAT rule of a public NAT gateway.

Figure 4-4 Setting up a highly available system by adding multiple EIPs to an SNAT rule



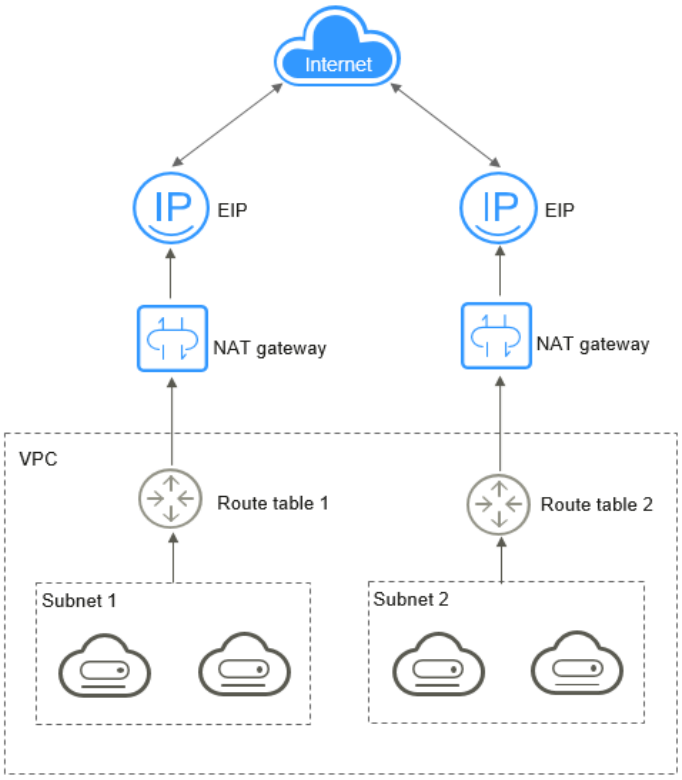
- **Using multiple NAT gateways together**

  If a single NAT gateway performance bottleneck occurs, for example, if there are over one million SNAT connections, or if the maximum bandwidth of 20 Gbit/s cannot meet service requirements, you can use multiple ones.

  To use multiple NAT gateways together, associate route tables of the VPC subnets with these public NAT gateways.

  Figure 4-5 shows how multiple public NAT gateways are used to overcome the performance bottleneck.

Figure 4-5 Using multiple public NAT gateways together



NOTE

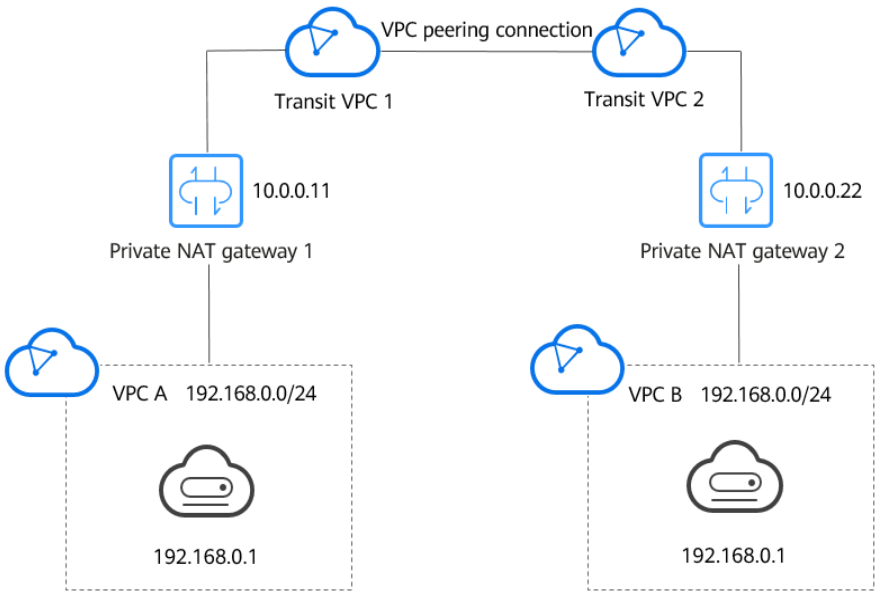
- The system does not add a default route for a public NAT gateway. You need to add a route pointing to the public NAT gateway to the corresponding route table.
- Each public NAT gateway has an associated route table. The number of public NAT gateways that can be created in a VPC is determined by the number of route tables for the VPC.

Private NAT Gateway

- **Connecting VPCs with overlapping CIDR blocks**

  You can configure two private NAT gateways for two VPCs with overlapping CIDR blocks. Then, add SNAT and DNAT rules on the two private NAT gateways to enable servers in the two VPCs to use the transit IP addresses to communicate with each other.

Figure 4-6 Connecting VPCs with overlapping CIDR blocks

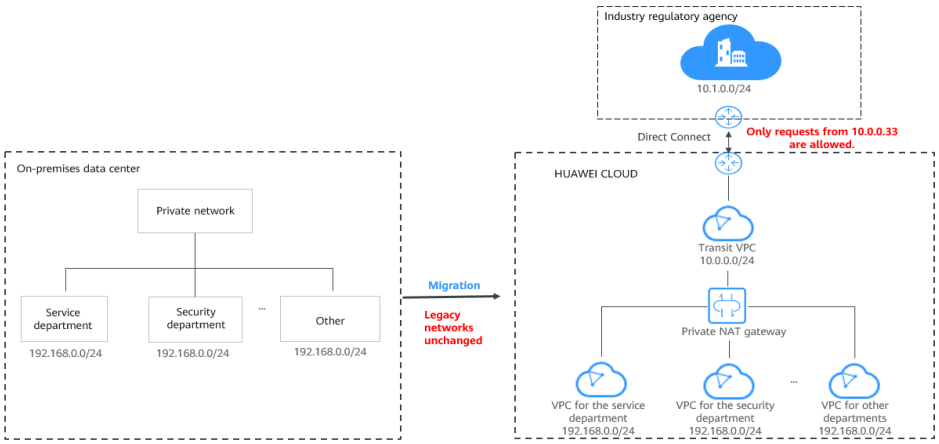


- **Keeping the network topology while migrating workloads to the cloud, or accessing regulatory agencies from specific IP addresses**

  Organizations may want to migrate their workloads to the cloud without making any changes to their existing network topology. They may also have to access regulatory agencies from specific IP addresses as required by these agencies. A private NAT gateway is a good choice.

  Subnets of different departments in an enterprise network may overlap. A private NAT gateway allows the enterprise to keep the existing network topology unchanged while migrating their workloads to the cloud. In this example, the private NAT gateway maps the IP address of each department to 10.0.0.33 so that each department can use 10.0.0.33 to securely access the regulatory agency.

  Figure 4-7 Migrating workloads to the cloud without changing the network topology or accessing regulatory agencies from specific IP addresses



5 Functions

Public NAT Gateway

Public NAT gateways provide network address translation (NAT) with 20 Gbit/s of bandwidth for servers in a VPC or for servers in on-premises data centers that connect to a VPC through Direct Connect or VPN.

Public NAT gateways provide source NAT (SNAT) and destination NAT (DNAT).

- SNAT translates private IP addresses into EIPs, allowing servers within an AZ or across AZs in a VPC to share an EIP to access the Internet.
- DNAT enables servers within an AZ or across AZs in a VPC to share an EIP to provide services accessible from the Internet. With an EIP, a public NAT gateway forwards the Internet requests from only a specific port over a specific protocol to the specified port of a server, or it can forward all requests to the private IP address of a server regardless of which port they originated on.

Private NAT Gateway

Private NAT gateways provide private address translation (NAT) for cloud servers (ECSs and BMSs) in a VPC. You can configure SNAT and DNAT rules to translate the source and destination IP addresses into transit IP addresses, so that servers in the VPC can communicate with other VPCs or on-premises data centers.

Private NAT gateways provide source NAT (SNAT) and destination NAT (DNAT).

- SNAT enables servers within an AZ or across AZs in a VPC to share a transit IP address to access servers in remote private networks, like servers in an on-premises data center or a different VPC.
- DNAT enables servers within an AZ or across AZs in a VPC to share a transit IP address to provide services accessible from servers in remote private networks, like servers in an on-premises data center or a different VPC.

6 NAT Gateway Specifications

The NAT gateway performance is determined by the maximum number of SNAT connections supported.

Public NAT Gateway

An SNAT connection consists of a source IP address, source port, destination IP address, destination port, and a transport layer protocol. The source IP address is the EIP, and the source port is the EIP port. An SNAT connection uniquely identifies a session.

Throughput is the total bandwidth of all EIPs in DNAT rules. For example, a public NAT gateway has two DNAT rules. The EIP bandwidth in the first DNAT rule is 10 Mbit/s, and that in the second DNAT rule is 5 Mbit/s. The throughput of the public NAT gateway will be 15 Mbit/s.

A public NAT gateway supports up to 20 Gbit/s of bandwidth.

The default timeout period of an SNAT connection over TCP is 900 seconds.

The default timeout period of an SNAT connection over UDP is 300 seconds.

Select a public NAT gateway based on your service requirements. **Table 6-1** lists the public NAT gateway specifications.

Table 6-1 Public NAT gateway specifications

Specifications	SNAT Connections	Bandwidth	Packets Per Second (PPS)	Queries Per Second (QPS)
Small	10,000	20 Gbit/s	2,000,000	10,000
Medium	50,000	20 Gbit/s	2,000,000	10,000
Large	200,000	20 Gbit/s	2,000,000	10,000
Extra-large	1,000,000	20 Gbit/s	2,000,000	10,000

NOTE

- The PPS of different NAT gateway specifications is the total PPS in both inbound and outbound directions.
- If the number of requests exceeds the maximum allowed connections of a public NAT gateway, services will be adversely affected. To avoid this situation, create alarm rules on the Cloud Eye console to monitor the number of SNAT connections.
- The DNAT rules of a public NAT gateway are irrelevant to the NAT gateway specifications. Up to 200 DNAT rules can be added to a public NAT gateway. The number of DNAT rules of only extra-large NAT gateways can be increased. To do so, **submit a service ticket**.

Private NAT Gateway

An SNAT connection consists of a source IP address, source port, destination IP address, destination port, and a transport layer protocol. The source IP address is the transit IP address, and the source port is the port of the transit IP address.

Select a private NAT gateway based on your service requirements. **Table 6-2** lists the private NAT gateway specifications.

Table 6-2 Private NAT gateway specifications

Specifications	SNAT Connections	Bandwidth	PPS	QPS	Number of NAT Rules (SNAT Rules +DNAT Rules)
Small	2,000	200 Mbit/s	20,000	6000	20
Medium	5,000	500 Mbit/s	50,000	9000	50
Large	20,000	2 Gbit/s	200,000	10,000	200
Extra-large	50,000	5 Gbit/s	500,000	10,000	500

NOTE

If the number of requests exceeds the maximum allowed connections of a private NAT gateway, services will be adversely affected. To avoid this situation, create alarm rules on the Cloud Eye console to monitor the number of SNAT connections.

7 Notes and Constraints

Public NAT Gateway

When using a public NAT gateway, note the following:

- Common restrictions
  - Rules on one public NAT gateway can use the same EIP, but rules on different NAT gateways must use different EIPs.
  - Each VPC can be associated with multiple public NAT gateways.
  - SNAT and DNAT rules can use the same EIP to save resources. However, when **Port Type** of a DNAT rule is set to **All ports**, the resource in the DNAT rule will preferentially use all ports of the EIP. So an SNAT rule cannot share an EIP with such a DNAT rule.
  - The public NAT gateway does not translate IP addresses for Enterprise Edition VPN.
  - If both an EIP and a public NAT gateway are configured for a server, data will be forwarded through the EIP.
  - Some carriers will block the following ports for security reasons. It is recommended that you do not use the following ports.

Protocol	Port
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 4790 5554 5800 5900 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

  - NAT Gateway supports TCP, UDP, and ICMP, but does not support application layer gateway (ALG)-related technologies. In addition, NAT Gateway does not support Encapsulating Security Payload (ESP) and Authentication Header (AH) used by Generic Routing Encapsulation (GRE) tunnels and Internet Protocol Security (IPsec). This is determined by the features of NAT Gateway.
- SNAT restrictions

  - Only one SNAT rule can be added for each VPC subnet.
  - If an SNAT rule is used in the Direct Connect scenario, the custom CIDR block must be a CIDR block of a Direct Connect connection and cannot overlap with the NAT gateway's VPC subnets.
  - There is no limit on the number of SNAT rules that can be added on a public NAT gateway.
- DNAT restrictions
  - Only one DNAT rule can be configured for each port on a server. One port can be mapped to only one EIP.
  - A maximum of 200 DNAT rules can be added on a public NAT gateway.

Private NAT Gateway

When using a private NAT gateway, note the following:

- Common restrictions
  - Manually add routes in a VPC to connect it to a remote private network through a VPC peering connection, Direct Connect, or VPN connection.
  - The transit IP address and destination IP address cannot be in the same VPC.
  - The total number of DNAT and SNAT rules that can be added on a private NAT gateway varies with the private NAT gateway specifications.
    - Small: 20 or less
    - Medium: 50 or less
    - Large: 200 or less
    - Extra-large: 500 or less
- SNAT restrictions
  - Only one SNAT rule can be added for each VPC subnet.
- DNAT restrictions
  - A DNAT rule with **Port Type** set to **All ports** cannot share a transit IP address with a DNAT rule with **Port Type** set to **Specific port**.

8 NAT Gateway and Other Services

Figure 8-1 shows the relationship between NAT Gateway and other services.

Figure 8-1 Relationship between NAT Gateway and other services

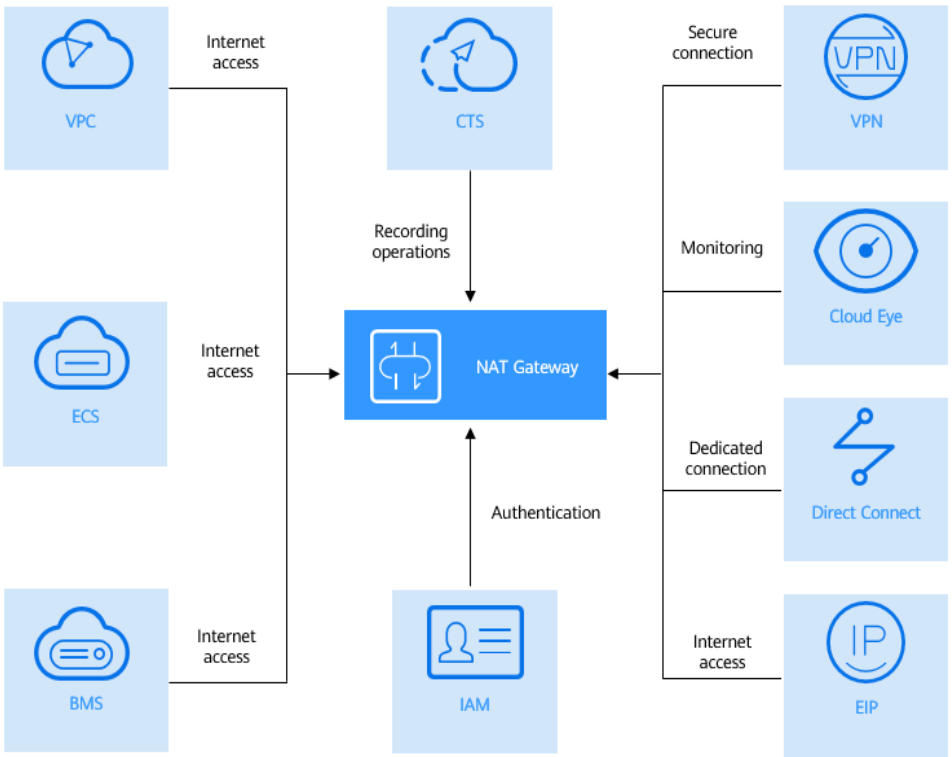


Table 8-1 Related services

Cloud Service	Interaction	Reference
Direct Connect	On-premises servers connected to a VPC through Direct Connect can use a public NAT gateway to communicate with the Internet.	**Using a Public NAT Gateway and Direct Connect to Accelerate Internet Access**
Virtual Private Network (VPN)	A VPN establishes an encrypted, Internet-based communication tunnel between your on-premises network and a VPC. This ensures secure access to the Internet through a public NAT gateway.	**Enabling Private Networks to Access the Internet Using Cloud Connect and SNAT**
Elastic Cloud Server (ECS)	ECSs can use a public NAT gateway to communicate with the Internet.	**Using a Public NAT Gateway to Enable Servers to Share One or More EIPs to Access the Internet** **Using a Public NAT Gateway to Enable Servers to Be Accessed by the Internet**
VPC	ECSs in a VPC can connect to the Internet.	**Using a Public NAT Gateway to Enable Servers to Share One or More EIPs to Access the Internet**
Elastic IP (EIP)	With a public NAT gateway, servers in a VPC can share an EIP to access the Internet or provide Internet-accessible services.	**Using a Public NAT Gateway to Enable Servers to Share One or More EIPs to Access the Internet** **Using a Public NAT Gateway to Enable Servers to Be Accessed by the Internet**
Cloud Eye	You can view NAT gateway monitoring data on the Cloud Eye console.	**Viewing Metrics**

Cloud Service	Interaction	Reference
Identity and Access Management (IAM)	If you need to assign different permissions to employees in your enterprise to control their access to your NAT Gateway resources, IAM is a good choice for fine-grained permissions management.	**Identity and Access Management**
Cloud Trace Service (CTS)	With CTS, you can record operations on NAT Gateway for later query, audit, and backtracking.	**Cloud Trace Service**

9 Security

9.1 Shared Responsibilities

Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in **Figure 9-1**.

- **Huawei Cloud**: Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer**: As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

Figure 9-1 Huawei Cloud shared security responsibility model

Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in **Figure 9-1**, customers can select different cloud service types (such as IaaS, PaaS, and SaaS services) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

9.2 Identity Authentication and Access Control

You can use Identity and Access Management (IAM) to control access to your NAT Gateway resources. IAM permissions define which actions on your cloud resources are allowed or denied. After creating an IAM user, the administrator needs to add it to a user group and grant NAT Gateway permissions to the user group. Then, all users in this group automatically inherit the granted permissions.

For details, see **Permissions Management**.

9.3 Auditing and Logging

Cloud Trace Service (CTS) records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, track resource changes, audit compliance, and locate faults.

After CTS is enabled, traces can be generated for operations performed on the NAT Gateway console.

- If you want to enable and configure CTS, refer to **Enabling CTS**.
- If you want to know supported NAT Gateway operations, refer to **Key Operations Recorded by CTS**.
- If you want to view traces, refer to **Viewing Traces**.

9.4 Monitoring Security Risks

Cloud Eye is a monitoring service provided by Huawei Cloud. It provides capabilities like real-time monitoring, timely alarm reporting, resource groups, and website monitoring, enabling you to keep track of your resource usages and service statuses on the cloud.

Monitoring is critical to ensuring the reliability, availability, and performance of NAT Gateway. With Cloud Eye, you can view metrics such as SNAT connections, PPS, inbound traffic, and outbound traffic by time axis. When creating alarm rules, you can configure monitoring thresholds and alarm notifications. This will ensure you learn about NAT Gateway resource issues in a timely manner, so you can handle faults quickly and prevent services from being interrupted.

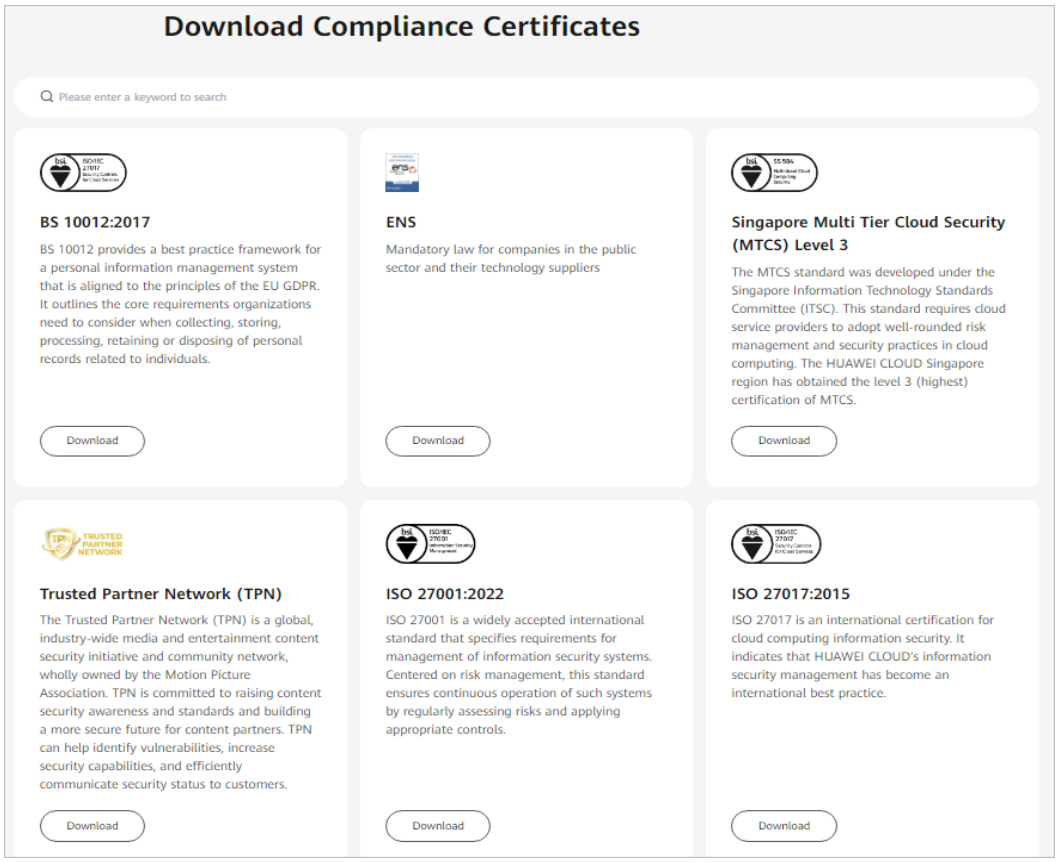
For details about supported metrics and how to create alarm rules, see **Supported Metrics**.

9.5 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can **download** them from the console.

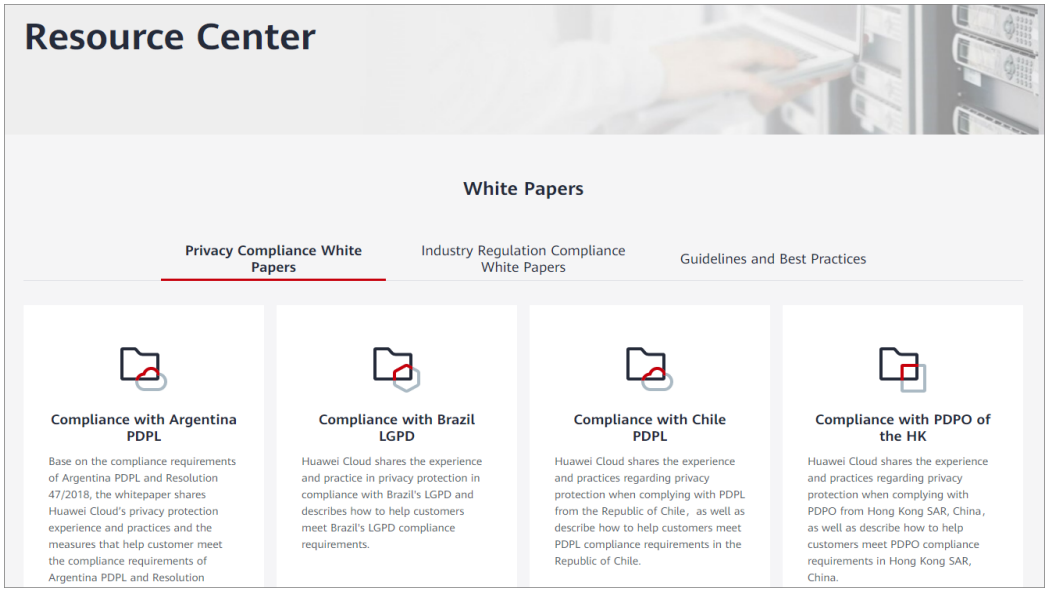
Figure 9-2 Downloading compliance certificates



Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 9-3 Resource center



10 Permissions Management

If you need to grant your enterprise personnel permission to access your NAT Gateway resources, use Identity and Access Management (IAM). IAM provides identity authentication, fine-grained permissions management, and access control. IAM helps you secure access to your Huawei Cloud resources.

With IAM, you can create IAM users and grant them permissions to access only specific resources. For example, if you want some software developers in your enterprise to be able to use NAT Gateway resources but do not want them to be able to delete NAT gateways or perform any other high-risk operations, you can create IAM users and grant permission to use NAT gateways but not permission to delete them.

If your Huawei Cloudcloud account does not require individual IAM users for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account. For more information about IAM, see **What Is IAM?**

NAT Gateway Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and then attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

NAT Gateway is a project-level service deployed for specific regions. To assign NAT Gateway permissions to a user group, specify the scope as region-specific projects and select projects for which you want the permissions to take effect. If you select **All projects**, the permissions will take effect for the user group in all region-specific projects. When accessing NAT gateways, the users need to switch to the authorized region.

You can grant users permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy that defines permissions by job responsibility. Only a limited number of service-level roles are available for authorization. Huawei Cloud services often depend on each other. When you grant permissions using roles, you also need to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.

- Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only permission to manage a certain type of NAT gateways. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by NAT Gateway, see **Permissions Policies and Supported Actions**.

Table 10-1 lists all the system-defined permissions for NAT Gateway.

Table 10-1 System-defined permissions for NAT Gateway

Policy Name	Description	Type
NAT FullAccess	All operations on NAT Gateway resources.	System-defined policy
NAT ReadOnlyAccess	Read-only permissions for all NAT Gateway resources.	System-defined policy
NAT Administrator	All operations on NAT Gateway resources. To be granted this permission, users must also have the **Tenant Guest** permissions.	System-defined role

Table 10-2 lists the common operations supported by each NAT Gateway system policy or role. Select the policies or roles as required.

Table 10-2 Common operations supported by each system-defined policy or role of NAT Gateway

Operation	NAT FullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
Creating a NAT gateway	√	x	√
Querying NAT gateways	√	√	√
Querying NAT gateway details	√	√	√
Updating a NAT gateway	√	x	√
Deleting a NAT gateway	√	x	√
Adding an SNAT rule	√	x	√

Operation	NAT FullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
Viewing an SNAT rule	√	√	√
Modifying an SNAT rule	√	x	√
Deleting an SNAT rule	√	x	√
Adding a DNAT rule	√	x	√
Viewing a DNAT rule	√	√	√
Modifying a DNAT rule	√	x	√
Deleting a DNAT rule	√	x	√
Deleting DNAT rules in batches	√	x	√
Importing DNAT rules using templates	√	x	√
Exporting DNAT rules using templates	√	√	√
Creating a transit subnet	√	x	√
Querying transit subnets	√	√	√
Querying details about a transit subnet	√	√	√
Modifying a transit subnet	√	x	√
Deleting a transit subnet	√	x	√
Assigning a transit IP address	√	x	√

Operation	NAT FullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
Querying a transit IP address	√	√	√
Releasing a transit IP address	√	x	√

NOTE

- To create a yearly/monthly public NAT gateway, you also need to obtain the **BSS Administrator** permissions of the Billing Center. For details, see the *Billing Center User Guide*.
- Note the following when creating a DNAT rule:
  - DNAT rule permissions cannot be managed by enterprise project.
  - If you set **Instance Type** to **Server** and select an ECS, you also need to obtain the **ECS ReadOnlyAccess** permissions or the fine-grained permissions for actions **ecs:cloudServers:get** and **ecs:cloudServers:list**. For details, see the *Elastic Cloud Server API Reference*.
  - If you set **Instance Type** to **Server** and select a BMS, you also need to obtain the **BMS ReadOnlyAccess** permissions or the fine-grained permissions for actions **bms:servers:get** and **bms:servers:list**. For details, see the *Bare Metal Server API Reference*.
  - If you create a DNAT rule on a private NAT gateway and select **Load balancer** for **Instance Type**, you need to obtain the **ELB ReadOnlyAccess** permissions or the fine-grained permissions for actions **elb:loadbalancers:get** and **elb:loadbalancers:list**. For details, see the *Elastic Load Balance API Reference*.
  - After a DNAT rule is created, add a security group rule to allow the Internet to access servers for which the DNAT rule is configured. Otherwise, the DNAT rule does not take effect. Obtain the **VPC FullAccess** permissions or the fine-grained permissions for action **vpc:securityGroups:create** by referring to the *Virtual Private Cloud API Reference*.
- To view metrics, obtain the **CES ReadOnlyAccess** permissions. For details, see the *Cloud Eye API Reference*.
- To view access logs, obtain the **LTS ReadOnlyAccess** permissions. For details, see the *Log Tank Service API Reference*.
- To query predefined tags, obtain the **TMS Administrator** permissions. For details, see the *Tag Management Service API Reference*.

Helpful Links

- **What Is IAM?**
- **Creating a User and Granting NAT Gateway Permissions**
- **Permissions Policies and Supported Actions**

11 Region and AZ

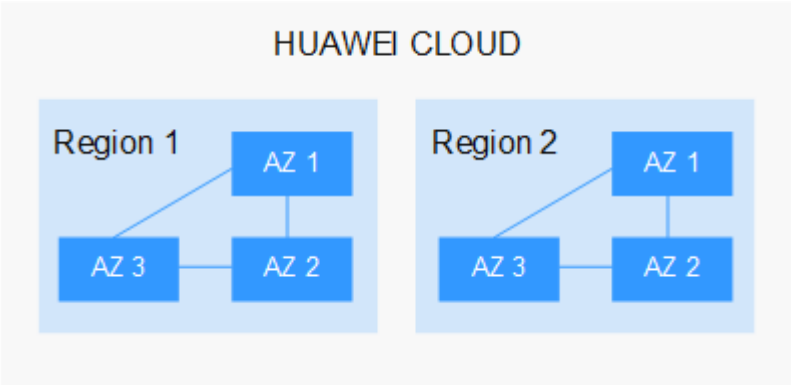
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters.

Figure 11-1 shows the relationship between regions and AZs.

Figure 11-1 Regions and AZs



Huawei Cloud provides services in many regions around the world. You can select a region and an AZ based on requirements. For more information, see **Huawei Cloud Global Products and Services**.

Selecting a Region

When selecting a region, consider the following factors:

- Location

  It is recommended that you select the closest region for lower network latency and quick access.

  - If your target users are in Asia Pacific (excluding the Chinese mainland), select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If your target users are in Africa, select the **AF-Johannesburg** region.
  - If your target users are in Latin America, select the **LA-Santiago** region.

    NOTE

    The **LA-Santiago** region is located in Chile.

- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

12 Basic Concepts

EIP

An EIP is a static, public IP address.

An EIP can be directly accessed over the Internet. A private IP address is an IP address on a local area network (LAN) and cannot be routed through the Internet.

You can bind an EIP to an ECS in your subnet to enable the ECS to communicate with the Internet.

Each EIP can be used by only one ECS at a time. To enable servers in a VPC, regardless of if they are in the same AZ, to share an EIP, use a public NAT gateway. For more information, see **NAT Gateway User Guide**.

SNAT Connections

An SNAT connection consists of a source IP address, source port, destination IP address, destination port, and a transport layer protocol. The source IP address and port are the IP address and port translated by SNAT. An SNAT connection uniquely identifies a session.

DNAT Connections

DNAT connections enable servers in a private network, regardless of if they are in the same AZ, to share an EIP to provide services accessible from the Internet.

