Enterprise Router

Service Overview

Issue	01
Date	2024-10-14

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.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 What Is an Enterprise Router?

An enterprise router connects VPCs and on-premises networks to build a central hub network. It has high specifications, provides high bandwidth, and delivers high performance. Enterprise routers use the Border Gateway Protocol (BGP) to learn, dynamically select, or switch between routes, thereby ensuring the service continuity and significantly improving network scalability and O&M efficiency.

- You can attach VPCs to enterprise routers to **allow VPCs in different regions to communicate through enterprise routers**.
- You can add two or more enterprise routers to a central network provided by Cloud Connect as attachments to **allow VPCs in different regions to communicate through enterprise routers and the central network**.
- You can also attach a Direct Connect virtual gateway or global DC gateway or a VPN gateway to **allow an on-premises data center to communicate with VPCs through Enterprise Router and Direct Connect**.
- Use Cloud Firewall (CFW) to protect traffic between VPCs. CFW can detect and defend against intrusions in real time, analyze traffic and visualize results, audit logs, and trace traffic sources. For details, see **Configuring CFW for Enterprise Router**.

Figure 1-1 and **Figure 1-2** show the networks with and without enterprise routers, respectively. **Table 1-1** compares the two networks.

Figure 1-1 A network without enterprise routers

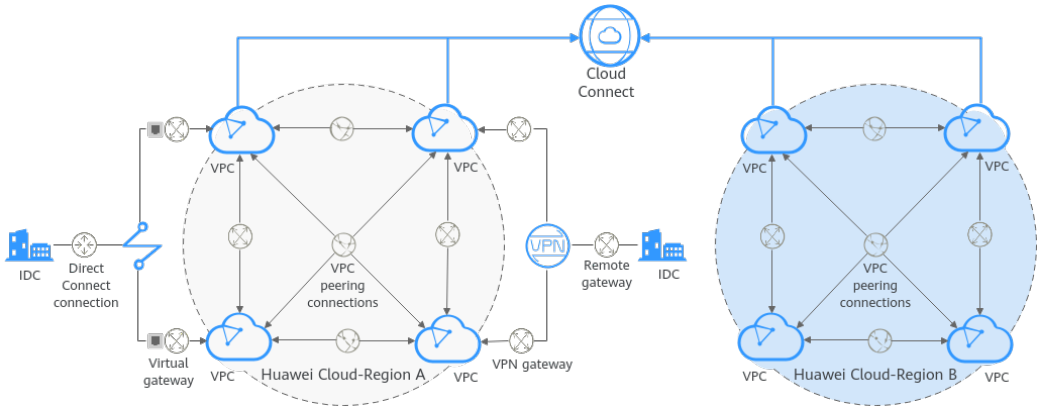


Figure 1-2 A network with enterprise routers

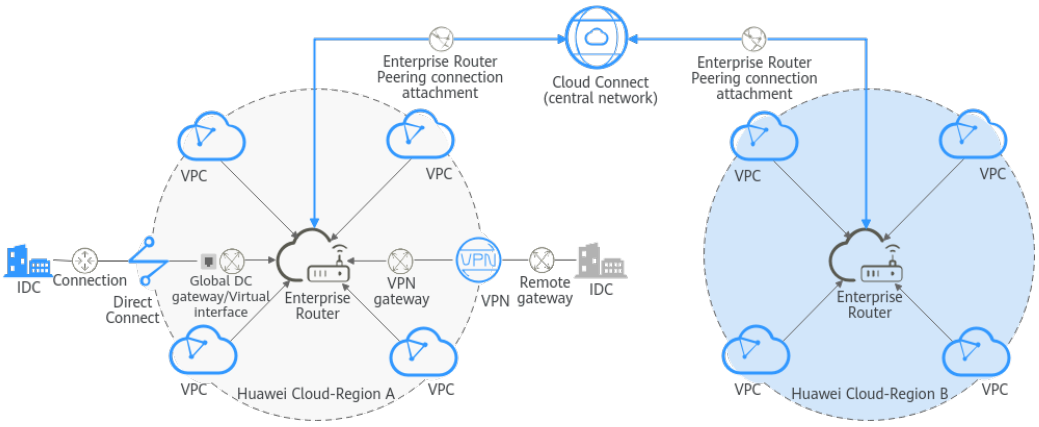


Table 1-1 Comparison between the networks with and without enterprise routers

Item	Without Enterprise Routers	With Enterprise Routers	Benefits of Using Enterprise Routers
Communications among VPCs in the same region	• Create six VPC peering connections between these four VPCs in the same region. • Add 12 routes, with three routes for each VPC to communicate with the other three VPCs.	• Attach the four VPCs to one enterprise router. This router can then handle the traffic from and to all the connected VPCs. • Add routes to the route tables of these four VPCs for routing traffic through the enterprise router. The enterprise router can automatically learn the VPC CIDR blocks and add them to its route table.	• There is no need to configure a large number of VPC peering connections. • Fewer routes need to be added, simplifying the maintenance.

Item	Without Enterprise Routers	With Enterprise Routers	Benefits of Using Enterprise Routers
Communications between VPCs in different regions	Connect all VPCs using Cloud Connect.	You only need to add the enterprise router in each region to a central network as attachments.	• There is no need to connect all VPCs to Cloud Connect, simplifying the network topology. • Route propagation simplifies the route configuration and the networking process.
Communications between an on-premises data center and VPCs	Establish Direct Connect or VPN connections between each VPC and the data center.	Attach the Direct Connect or VPN connection to the enterprise router. These VPCs can then share the connection.	• Route propagation simplifies the route configuration and the O&M. • Multiple lines work in load-sharing or active/standby mode to achieve higher availability.

The comparison shows that the network with enterprise routers is simpler and highly scalable and is also easier to maintain.

2 Why Using Enterprise Routers

Enterprise routers have the following advantages:

High Performance

Enterprise routers use exclusive resources and are deployed in clusters to deliver the highest possible performance for workloads on large-scale networks.

High Availability

Enterprise routers can be deployed in multiple availability zones to work in active-active or multi-active mode, thereby ensuring service continuity and real-time seamless switchovers.

Simplified Management

Enterprise routers can route traffic among instances, simplify network topology and network management, and improve network O&M efficiency. The network topology is simpler and the network is easier to manage and maintain.

- For cross-VPC communications, you only need to maintain the route tables on the VPCs without requiring so many VPC peering connections.
- For communications between VPCs and an on-premises data center, multiple VPCs can connect to an enterprise router and then communicate with the data center over one Direct Connect or VPN connection. You do not need to establish a Direct Connect or VPN connection between the data center and each of the VPCs.
- Enterprise routers can automatically learn, update, and synchronize routes, eliminating the need to manually configure or update routes whenever the network topology changes.

Seamless Failover Between Lines

Enterprise routers use the Border Gateway Protocol (BGP) to select the best path from multiple lines working in load-sharing or active/standby mode. If a single line fails, services can be failed over to another functioning line within seconds to ensure service continuity.

3 When to Use Enterprise Routers

You can use enterprise routers to build cloud, on-premises, or hybrid networks. Here are some typical application scenarios:

- **Scenario 1: Multiple VPCs communicating or not communicating with each other on the cloud, but communicating with the on-premises data center through a Direct Connect connection**
- **Scenario 2: Dynamic switchover between Direct Connect connections**
- **Scenario 3: Active/Standby Direct Connect and VPN connections**
- **Scenario 4: Cross-cloud, cross-region highly reliable backbone network**
- **Scenario 5: Building a border firewall between VPCs**

Scenario 1: Multiple VPCs communicating or not communicating with each other on the cloud, but communicating with the on-premises data center through a Direct Connect connection

Figure 3-1 Diagram for scenario 1

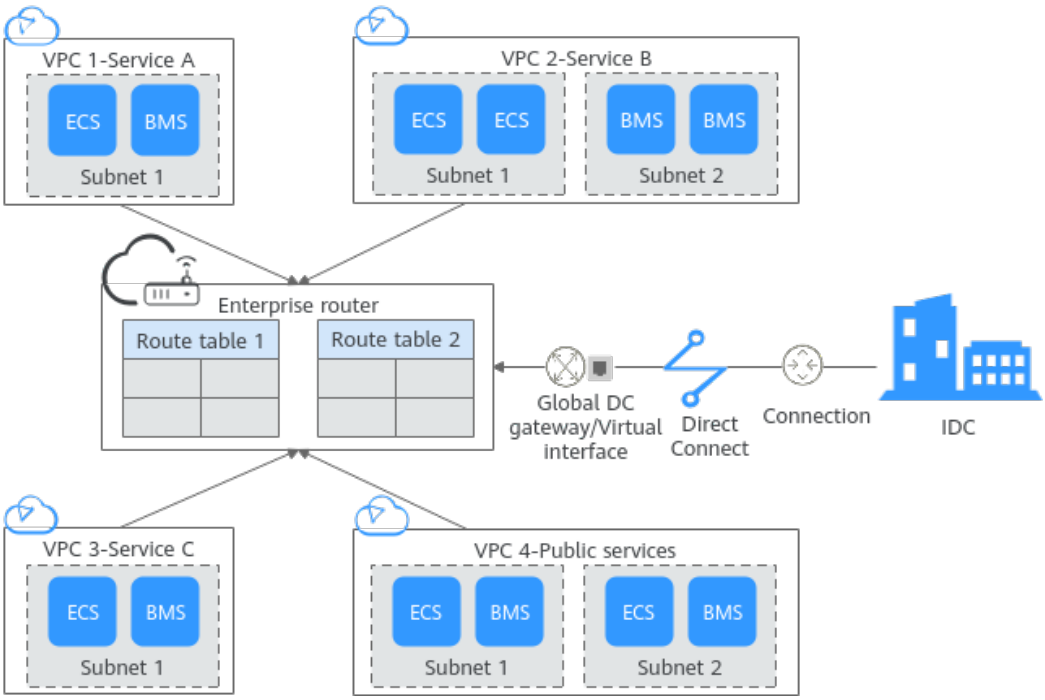


Table 3-1 Using enterprise routers in scenario 1

Customer Requirements	Multiple service networks communicate or do not communicate with each other on the cloud but communicate with the on-premises data center. Suppose you require three VPCs for running the workloads on the public cloud, and the three VPCs (services A, B, and C) need to access public services in VPC 4 and your on-premises data center.
Pain Points	• VPC peering connections are required for communications among these VPCs, but they will complicate the network topology and make the network hard to manage. • VPC peering connections and routes are required for the public service VPC to communicate with each VPC. However, VPC peering connections do not fit in large-scale networks because of the following limitations: – A maximum of 50 VPC peering connections can be created in one region. – A VPC route table can have a maximum of 200 routes. • Direct Connect connections are required for each VPC to communicate with the on-premises data center, but they will incur high costs.

Benefits of Using Enterprise Routers	• VPCs can be associated with different route tables on the enterprise router to enable communication or isolation. The network topology is simple and easy to manage. • Enterprise routers can route traffic among all the connected VPCs without the need to configure a large number of VPC peering connections. – Each enterprise router can have a maximum of 2,000 routes in each route table, making it ideal for large-scale complex networks. • Multiple VPCs can access the on-premises data center over a Direct Connect connection, eliminating the need to configure multiple Direct Connect connections and reducing the costs.
Best Practice	**Using Enterprise Router to Isolate VPCs in the Same Region**

Scenario 2: Dynamic switchover between Direct Connect connections

Figure 3-2 Diagram for scenario 2

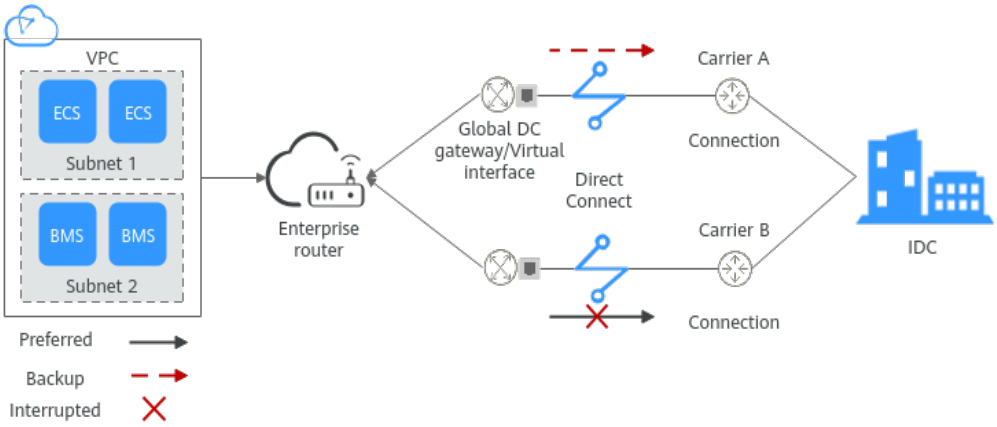


Table 3-2 Using enterprise routers in scenario 2

Customer Requirements	Some services run on the public cloud and some in the on-premises data center. Two independent high-bandwidth Direct Connect connections are deployed between the public cloud and the data center to enable communication between them.
Pain Points	Two Direct Connect connections are independent of each other and cannot work in load-sharing or active/standby mode.

Benefits of Using Enterprise Routers	Direct Connect connections are connected to the enterprise router. • Two Direct Connect connections can work in load-sharing mode to ensure high bandwidth and reliability. • Two Direct Connect connections can also work in active/standby mode. If one of the connections becomes unavailable, services are switched over to the other available connection within seconds, preventing service interruptions.
Best Practice	**Setting Up a Hybrid Cloud Network Using Enterprise Router and a Pair of Direct Connect Connections (Global DC Gateway)**

Scenario 3: Active/Standby Direct Connect and VPN connections

Figure 3-3 Diagram for scenario 3

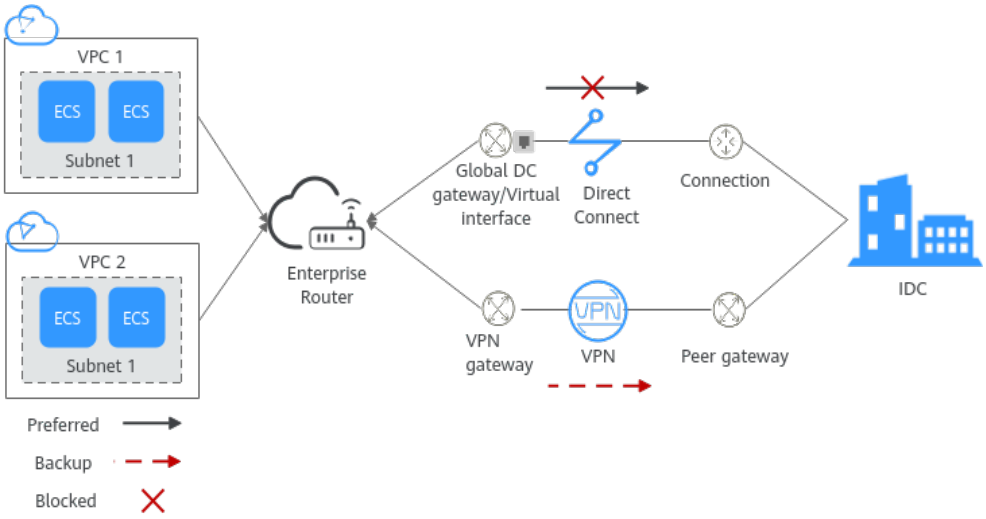


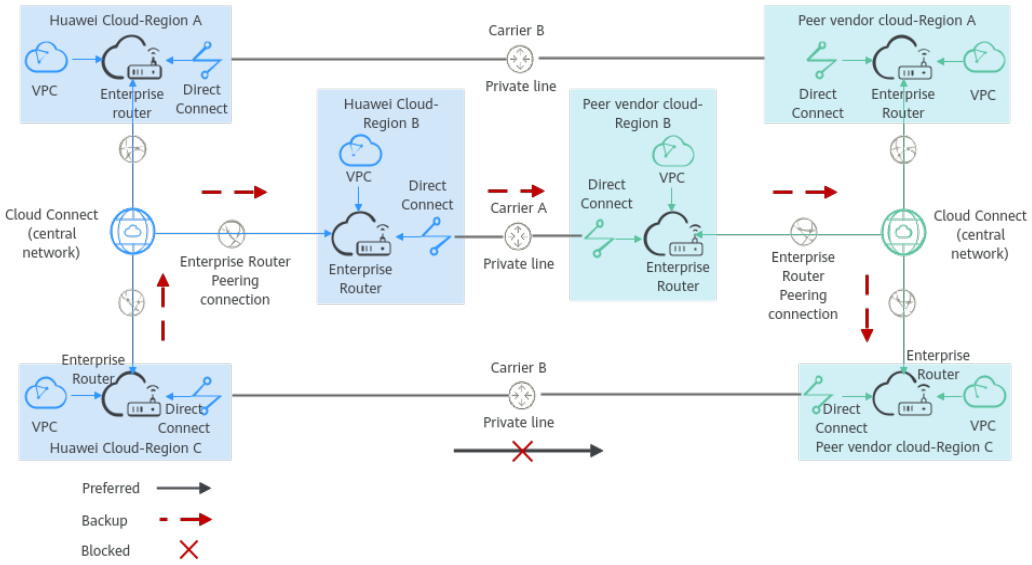
Table 3-3 Using enterprise routers in scenario 3

Customer Requirements	You are running workloads in your on-premises data center and on the public cloud. A single Direct Connect connection connects your on-premises data center to the cloud, which cannot ensure reliability.
Pain Points	You cannot afford another Direct Connect connection.
Benefits of Using Enterprise Routers	In this example, there are two connections, one Direct Connect connection and a VPN connection. Enterprise Router, Direct Connect, and VPC are used to build a hybrid cloud. When the Direct Connect connection becomes faulty, the VPN connection takes over to ensure that connectivity is not interrupted.

Best Practice	**Setting Up a Hybrid Cloud Network Using Enterprise Router, VPN, and Direct Connect (Global DC Gateway)**

Scenario 4: Cross-cloud, cross-region highly reliable backbone network

Figure 3-4 Diagram for scenario 4



NOTE

Change the enterprise router on the other cloud shown in **Figure 3-4** to its actual service name of the other cloud.

Table 3-4 Using enterprise routers in scenario 4

Customer Requirements	To improve service DR capabilities, enterprises often run workloads on multiple public clouds. Each public cloud spans across multiple regions for nearest access. They do not have their own backbone networks and use the backbone networks of the public clouds for multi-cloud, multi-region interconnection. Suppose you are running workloads in regions of both Huawei Cloud and another cloud service provider. The two public clouds communicate with each other through private lines of different carriers. Different regions of the same public cloud communicate with each other through the backbone networks (central networks provided by Cloud Connect).
Pain Points	• A large number of routes are required for communication between the VPCs of multiple clouds and regions, resulting in high maintenance costs. • Direct Connect and Cloud Connect connections cannot work in load balancing or active/standby mode.

Benefits of Using Enterprise Routers	The public clouds are connected through private lines, and different regions in the same public cloud are connected through the central network. • Enterprise routers can forward traffic between instances, simplifying the network topology. In addition, route learning is supported. When the network changes, automatic convergence simplifies maintenance and management. • Direct Connect and Cloud Connect connections can work in load-sharing or active/standby mode. Traffic between VPCs of different clouds is preferentially routed through the carriers' private lines. If the private lines become unavailable, requests will be transmitted over the Cloud Connect and dedicated connections. If the private lines between region C of Huawei Cloud and region C of the other cloud service provider become unavailable, the traffic can be first forwarded from region C of Huawei Cloud to region B of Huawei Cloud through Cloud Connect connections, then to the region B of the other cloud service provider through private lines, and finally to Region C of the other cloud service provider through Cloud Connect connections.
Best Practices	**Connecting VPCs Across Regions Using Enterprise Router and Central Network** **Setting Up a Hybrid Cloud Network Using Enterprise Router and Direct Connect (Virtual Gateway)**

Scenario 5: Building a border firewall between VPCs

Figure 3-5 Diagram for scenario 4

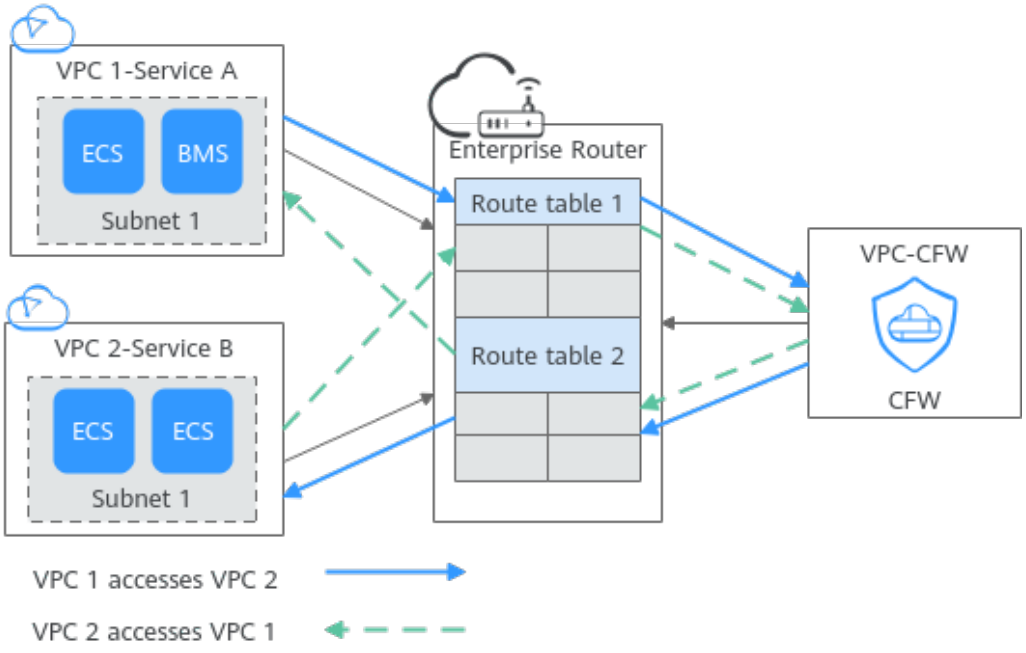


Table 3-5 Using enterprise routers in scenario 5

Customer Requirements	You have two VPCs with each VPC used to run a separate service (service A in VPC 1 and service B in VPC 2). For security purposes, the traffic between service A and service B needs to be filtered by the firewall.
Pain Points	You want to quickly set up a cloud network that meets security requirements.
Benefits of Using Enterprise Routers	A cloud firewall is deployed on the network, and the VPC and cloud firewall are associated with different route tables of the enterprise router to control the mutual access traffic between VPC 1 and VPC 2 to pass through the firewall.
Best Practice	**Using Enterprise Router and CFW to Protect Traffic Between VPCs**

4 Functions

An enterprise router provides the functions listed in **Table 4-1**, allowing you to:

- Manage attachments, custom route tables, associations, propagations, and routes.
- Manage permissions, tags, and quota to improve service security.

Table 4-1 Enterprise router functions

Function	Description	Reference
Enterprise routers	An enterprise router is a high-performance centralized router that supports route learning. When creating an enterprise router, you can set parameters such as its region, AZ, and name. After an enterprise router is created, you can still change its parameters based on service requirements.	**Creating an Enterprise Router**
Attachments	You can attach network instances to the enterprise router. Network instances are attached to the enterprise router in different ways. • VPCs are attached to the enterprise router on the Enterprise Router console. • Virtual gateways are attached through the Direct Connect console. • VPN gateways are attached through the VPN console. • Enterprise routers in other regions are added to a central network on the Cloud Connect console. • Global DC gateways are attached through the Direct Connect console. • CFW instances are created on the CFW console.	**Attachment Overview**

Function	Description	Reference
Route tables	Route tables are used by enterprise routers to forward packets. Route tables contain associations, propagations, and routes. An enterprise router can have multiple route tables. You can associate attachments with different route tables to enable communication or isolation between network instances.	**Route Table Overview**
Associations	Associations are created manually or automatically to associate attachments with enterprise router route tables. • Manually: Select a route table and create an association for an attachment in the route table. • Automatically: You just need to enable **Default Route Table Association** and specify the default route table. The system automatically creates an association for an attachment in the default route table.	**Association Overview**
Propagations	A propagation is created manually or automatically to enable an enterprise router to learn the routes to an associated attachment. • Manually: Select a route table and create a propagation for an attachment in the route table. • Automatically: You just need to enable **Default Route Table Propagation** and specify the default route table. A propagation is automatically created for an attachment in the default propagation route table.	**Propagation Overview**
Routes	A route consists of information such as the destination address, next hop, and route type. There are two types of routes: • Propagated routes • Static routes	**Route Overview**
Sharing	Integration with Resource Access Manager (RAM) allows you to share enterprise routers in your accounts with other accounts so that these other users can attach their network instances to your enterprise router for network connectivity. After you share your enterprise router with other accounts, these principals can attach their network instances to your enterprise router, so that their network instances can access your enterprise router.	**Sharing Overview**

Function	Description	Reference
Flow logs	A flow log records traffic of attachments on enterprise routers in real time. The logs allow you to monitor the network traffic of attachments and analyze network attacks, improving the O&M efficiency. Flow logs can capture traffic of the following types of attachments: • VPC • Virtual gateway • VPN gateway • Peering connection • Global DC gateway	**Flow Log Overview**
Monitoring	You can use Cloud Eye to monitor the network status of enterprise routers and their attachments.	**Supported Metrics**
Auditing	You can use Cloud Trace Service (CTS) to record operations associated with your enterprise routers for future query, audit, and backtracking.	**Key Operations Recorded by CTS**
Permissions	You can use Identity and Access Management (IAM) to set different permissions for employees in your enterprise to control their access to enterprise routers.	**Creating a User and Granting Permissions**
Tags	Tags are used to identify cloud resources. You can add tags to enterprise routers and route tables.	**Tag Overview**
Quotas	Quotas can limit the number or amount of resources available to users, for example, how many enterprise routers can be created, how many attachments can be created for each enterprise router, and how many routes can be added to each route table.	**Quotas**

5 How Enterprise Routers Work

You can attach your network connections to an enterprise router to quickly construct diversified networks and meet various service requirements. **Figure 5-1** shows the process of using an enterprise router, including creating an enterprise router, adding attachments to the enterprise router, and configure routes.

Enterprise routers support the following attachments:

- **VPC attachment**: Attach a VPC from the same region as that of an enterprise router.
- **Virtual gateway attachment**: Attach a Direct Connect virtual gateway from the same region as that of an enterprise router.
- **VPN gateway attachment**: Attach a VPN gateway from the same region as that of an enterprise router.
- **Peering connection attachment**: Connect enterprise routers from different regions through a central network.
- **Global DC gateway attachment**: Attach a Direct Connect global DC gateway in the same region.
- **CFW instance attachment**: Connect an enterprise router to the VPC border firewall in the same region.

Figure 5-1 Processing of using an enterprise router

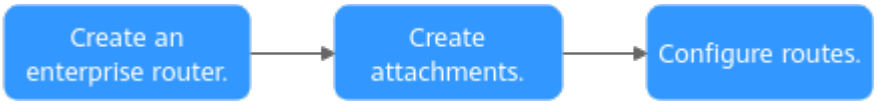


Figure 5-2 shows how an enterprise router works. **Table 5-2** describes the traffic flows in detail if an enterprise router is used for networking.

Figure 5-2 How an enterprise router works

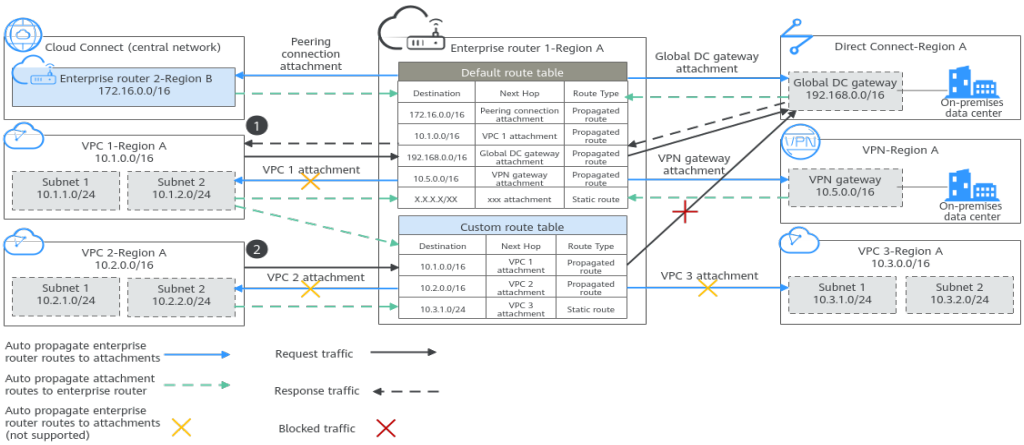


Table 5-1 Network traffic flows

No.	Route	Description
1	Request path: from VPC1 to the global DC gateway	After receiving requests from VPC 1 to the global DC gateway, enterprise router 1 searches the default route table for the route to the global DC gateway and forwards the requests through this route.
	Response path: from global DC gateway to VPC1	After receiving responses from the global DC gateway to VPC 1, enterprise router 1 searches the default route table for the route to VPC 1 and forwards the responses through this route.
2	Request path: from VPC2 to the global DC gateway	Enterprise router 1 cannot forward requests from VPC 2 to the global DC gateway because the custom route table of enterprise router 1 that is associated with VPC 2 does not contain the route to this global DC gateway.

Table 5-2 Working principles of an enterprise router

No.	Action	Description
1	Add **attachments** to the enterprise router.	Attach network instances to enterprise router 1 in region A. • Network instances from the same region – **VPC attachments**: VPC 1, VPC 2, and VPC 3 – **Global DC gateway attachment**: global DC gateway – **VPN gateway attachment**: VPN gateway • Network instances from a different region **Peering connection attachment**: Enterprise router 2 in region B

No.	Action	Description
2	Associate the **attachments** with the **route tables** of the enterprise router. Each attachment can only be associated with one route table.	• Associate VPC 1 with the default route table of enterprise router 1 and create a propagation to propagate the routes learned from VPC 1 attachment to the default route table and custom route table of enterprise router 1. • Associate VPC 2 with the custom route table of enterprise router 1 and create a propagation to propagate the routes learned from VPC 2 to the custom route table. • Associate VPC 3 with the custom route table of enterprise router 1, and add static routes for VPC 3 to this custom route table. • Associate the Direct Connect global DC gateway with the default route table of enterprise router 1 and create a propagation to propagate the routes learned from the global DC gateway attachment to the default route table. • Associate the VPN gateway with the default route table of enterprise router 1 and create a propagation to propagate the routes learned from the VPN gateway attachment to the default route table. • Establish a peering connection between enterprise router 2 in region B and enterprise router 1 in region A, associate the peering connection with the default route table of enterprise router 1, and create a propagation to propagate the routes for the peering connection attachment to the default route table.
3	Create **propagation** for the attachments to propagate the **routes** to the enterprise router's **route tables**. You can create multiple propagation records for the same attachment.	

Attachments

If you want to attach a network instance to an enterprise router, you need to add an attachment of a specific type to the enterprise router. The attachment type varies by type of the network instance, as listed in **Table 5-3**.

Table 5-3 Attachments

Attachment Type	Network Instance
VPC attachment	VPC
Virtual gateway attachment	Virtual gateway of Direct Connect
VPN gateway attachment	VPN gateway

Attachment Type	Network Instance
Peering connection attachment	Enterprise routers from different regions. You can add enterprise routers from different regions to a central network as attachments. Each connection between enterprise routers is a peering connection attachment.
Global DC gateway attachment	Global DC gateway in Direct Connect
CFW instance attachment	VPC border firewall

Route Tables

Route tables are used by enterprise routers to forward packets. Route tables contain associations, propagations, and routes. Route tables are classified into custom and default route tables, as detailed in **Table 5-4**.

Table 5-4 Route tables

Route Table Type	Description
Custom route table	You can create multiple custom route tables on an enterprise router and use different routes for flexible communication and isolation between network instances.
Default route table	If you enable **Default Route Table Association** and **Default Route Table Propagation**, the system then automatically associates and propagates new attachments with the default route table. You can specify a custom route table as the default route table. If you do not specify any route table as the default route table, the system automatically creates a default route table.

Associations

Each attachment can be associated with one route table for:

- Packet forwarding: Packets from the attachment are forwarded through the routes specified in the associated route table.
- Route propagation: The routes in the associated route tables are automatically propagated to the route table of the attachment.

Not all attachments can propagate routes. For details, see **Table 5-5**.

Table 5-5 Associations

Attachment Type	Route Learning
VPC	Not supported
Virtual gateway	Supported
VPN gateway	Supported
Peering connection	Supported
Global DC gateway	Supported
CFW instance	Not supported

Route Propagation

You can create a propagation for each attachment to propagate routes to one or more route tables on an enterprise router.

For VPC attachments, their CIDR blocks are propagated to the enterprise router. For other attachments, all routes are propagated to the enterprise router. For details, see **Table 5-6**.

Table 5-6 Propagation

Attachment Type	Propagated Routes to Enterprise Router
VPC	VPC CIDR blocks
Virtual gateway	All routes
VPN gateway	All routes
Peering connection	All routes
Global DC gateway	All routes
CFW instance	CIDR blocks of the VPCs protected by CFW

Routes

Routes are used to forward packets. A route contains information such as the destination, next hop, and route type. **Table 5-7** describes the routes of different types.

Table 5-7 Routes

Route Type	Description	Attachment
Propagated routes	Propagated routes are automatically learned through propagation and cannot be modified or deleted.	• VPC • Virtual gateway • VPN gateway • Peering connection • Global DC gateway • CFW instance
Static routes	Static routes are manually created and can be modified or deleted.	• VPC • Peering connection • CFW instance

6 Billing

An enterprise router can have multiple types of attachments, such as VPC attachments, virtual gateway attachments, VPN gateway attachments, and peering connection attachments. Each type of attachment has different pricing rules. For details, see **Billing**.

7 Security

7.1 Shared Responsibilities

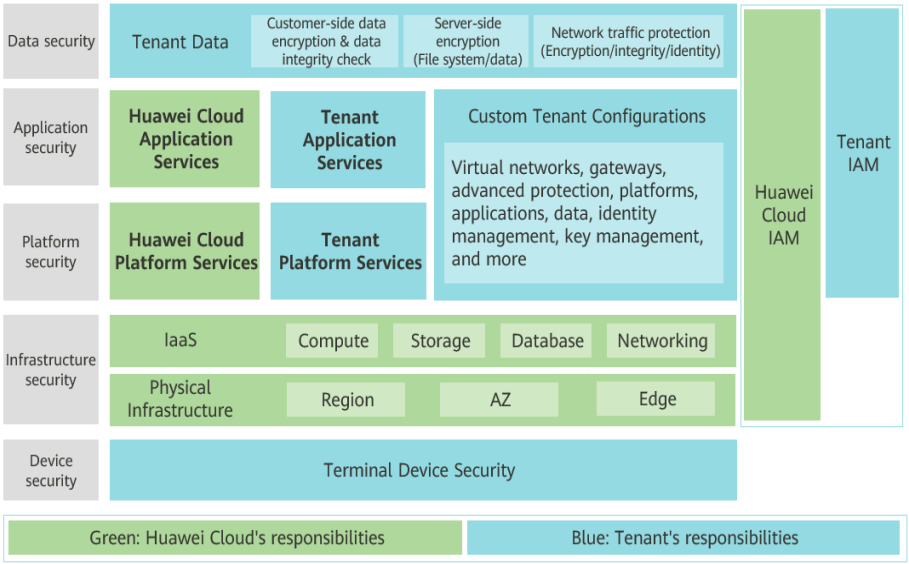
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 7-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 7-1 Huawei Cloud shared security responsibility model



7.2 Identity Authentication and Access Control

Identity and Access Management (IAM) enables you to easily manage users and control their access to Huawei Cloud services and resources.

You can use IAM to control access to your enterprise router 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 the permissions required by Enterprise Router to the user group. Then, all users in this group automatically inherit the granted permissions.

- **IAM Functions**
- **Permissions**

7.3 Auditing and Logging

Cloud Trace Service (CTS) is a log audit service for Huawei Cloud security. It allows you to collect, store, and query cloud resource operation records. You can use these records to perform security analysis, audit compliance, track resource changes, and locate faults.

After CTS is enabled, it can record enterprise router operations.

- If you want to enable and configure CTS, refer to **CTS Getting Started**.
- If you want to know supported operations on enterprise routers, refer to **Key Operations Recorded by CTS**.

If you want to view traces, refer to **Viewing Traces**.

7.4 Risk Monitoring

You can use Cloud Eye to monitor the status and usage of enterprise routers. You can also configure alarm rules and notifications to help you learn about enterprise router metrics in a timely manner.

If you want to know supported enterprise router metrics, see **Supported Metrics**.

8 Permissions

If you need to assign different permissions to employees in your enterprise to control their access to your cloud resources, you can use the Identity and Access Management (IAM) for fine-grained permissions management. IAM provides functions such as identity authentication, permissions management, and access control.

On the IAM console, you can create IAM users and assign permissions to control their access to specific resources. For example, you can create IAM users for software developers and assign permissions to allow them to use enterprise router resources but disallow them from performing any high-risk operations such as deleting such resources.

IAM is free of charge.

For more information, see **IAM Service Overview**.

Enterprise Router Permissions

By default, new IAM users do not have any permissions assigned. You need to add them to one or more groups and attach policies or roles to these groups so that these users can inherit permissions from the groups and perform specified operations on cloud services.

An enterprise router is a project-level service deployed in a specific region. You need to select a project such as **ap-southeast-2** for which the permissions will be granted. If you select **All projects**, the permissions will be granted for all the projects. You need to switch to the authorized region before accessing an enterprise router.

To manage access to cloud resources, you need to create roles or policies and attach them to IAM users.

- Role-based authorization: It is a coarse-grained authorization that defines permissions based on user responsibilities. There are only a limited number of roles, and some of them may depend on others. If so, you need to assign both roles to grant permissions. Role-based authorization is not an ideal choice for fine-grained authorization and minimum access control.
- Policy-based authorization: a type of fine-grained authorization that defines permissions required to perform operations on specific cloud resources under certain conditions. It is more flexible than role-based authorization and can

achieve minimum access control. For example, you can grant IAM users only the permissions to perform specified operations on enterprise routers.

Table 8-1 lists all the system-defined policies on enterprise routers.

Table 8-1 System-defined policies on enterprise routers

System Policy	Description	Type	Dependency
ER FullAccess	Administrator permissions for enterprise routers. Users with such permissions can operate and use all resources on enterprise routers.	System-defined policy	None
ER ReadOnlyAccess	Read-only permissions for enterprise routers. Users with such permissions can only view data on enterprise routers.	System-defined policy	None

Table 8-2 lists the common operations supported by each system-defined policy. You can select a proper one as required.

Table 8-2 Common operations supported by each system policy

Operation	Tenant Administrator	Tenant Guest	ER FullAccess	ER ReadOnlyAccess
Creating an enterprise router	√	x	√	x
Modifying an enterprise router	√	x	√	x
Viewing an enterprise router	√	√	√	√
Deleting an enterprise router	√	x	√	x
Adding a Virtual Private Cloud (VPC) to an enterprise router	√	x	√	x
Deleting a VPC attachment	√	x	√	x
Viewing attachments of all types	√	√	√	√

Operation	Tenant Administrator	Tenant Guest	ER FullAccess	ER ReadOnlyAccess
Creating a route table	√	x	√	x
Renaming a route table	√	x	√	x
Viewing a route table	√	√	√	√
Deleting a route table	√	x	√	x
Creating an association for an attachment in a route table	√	x	√	x
Viewing associations in a route table	√	√	√	√
Deleting an association from a route table	√	x	√	x
Creating a propagation for an attachment in the route table	√	x	√	x
Viewing a propagation in a route table	√	√	√	√
Deleting a propagation from a route table	√	x	√	x
Creating a static route	√	x	√	x
Modifying a static route	√	x	√	x
Viewing a route	√	√	√	√
Deleting a static route	√	x	√	x
Creating a flow log	√	x	√	x
Viewing a VPC flow log	√	√	√	√

Operation	Tenant Administrator	Tenant Guest	ER FullAccess	ER ReadOnlyAccess
Disabling a flow log	√	x	√	x
Enabling a flow log	√	x	√	x
Deleting a flow log	√	x	√	x
Adding a resource tag	√	x	√	x
Modifying a resource tag	√	x	√	x
Viewing a resource tag	√	√	√	√
Deleting a resource tag	√	x	√	x

Related Links

- What Is IAM?
- Creating a User and Granting Permissions to Access the Enterprise Router

9 Notes and Constraints

Quotas

Table 9-1 lists the quotas about enterprise router resources. Some default quotas can be increased.

You can log in to the console to view default quotas. For details, see **Viewing Quotas**.

Table 9-1 Enterprise router resource quotas

Item	Adjustable
Maximum number of enterprise routers that can concurrently connect to a VPC	No
Maximum number of VPCs that can be attached to an enterprise router	**Yes**
Maximum number of peering connections that can be attached to an enterprise router	**Yes**
Maximum number of virtual gateways that can be attached to an enterprise router	**Yes**
Maximum number of VPN gateways that can be attached to an enterprise router	**Yes**
Maximum number of route tables allowed on each enterprise router	No
Maximum number of routes allowed on each enterprise router	No
Maximum number of static routes allowed in each route table	**Yes**
Maximum number of flow logs that can be created by each account	No

Specifications

Table 9-2 lists the specifications of the enterprise router.

Table 9-2 Enterprise router specifications

Item	Default Setting	Adjustable
Maximum number of enterprise routers that can be created by each account	1	Yes
Maximum forwarding capability supported by each enterprise router	100 Gbit/s	Yes

Constraints

There are some constraints on using enterprise routers, as described in Table 9-3. You can follow our suggestions to handle these issues.

Table 9-3 Constraints on enterprise routers

Constraint	Suggestion
If a service VPC is being used by ELB, VPC Endpoint, NAT Gateway (private NAT gateway), Distributed Cache Service (DCS), or hybrid DNS, this VPC cannot be attached to an enterprise router. **NOTICE** If you attach a service VPC to an enterprise router when Elastic Load Balance (ELB), VPC Endpoint, or DCS is being used together with Enterprise Router, persistent connections may be intermittently interrupted during service reliability assurance, such as a DR switchover, an upgrade, or elastic scaling. Ensure that the clients are capable of automatic reconnection in case of intermittent disconnection.	Submit a service ticket to confirm the service compatibility and preferentially use a transit VPC for networking. For details, see scheme 2 in Selecting a Networking Scheme.

Constraint	Suggestion
Traffic cannot be forwarded from a VPC to the enterprise router that the VPC is attached to if you set the destination of a route whose next hop is the enterprise router to 0.0.0.0/0 in the VPC route table and if: • An ECS in the VPC has an EIP bound. • The VPC is being used by ELB (either dedicated or shared load balancers), NAT Gateway, VPC Endpoint, and DCS.	• Suggestion 1: Change the destination address of the route. For details, see **Why Traffic Can't Be Forwarded from a VPC with a Route Destination of 0.0.0.0/0 to Its Enterprise Router?** • Suggestion 2: Use a transit VPC for networking. For details, see scheme 2 in **Selecting a Networking Scheme**.
If a VPC attached to an enterprise router has a NAT gateway associated and **Scenario** of the SNAT or DNAT rules is set to **Direct Connect/Cloud Connect**, the network from the on-premises data center to the VPC is disconnected.	Use a transit VPC for networking. For details, see scheme 2 in **Selecting a Networking Scheme**.

10 Enterprise Router and Other Services

Figure 10-1 illustrates how an enterprise router works with other cloud services on Huawei Cloud.

Figure 10-1 How an enterprise router works with other cloud services

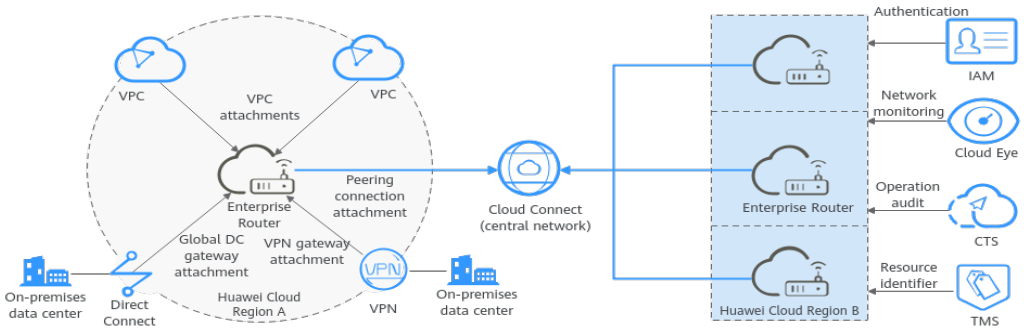


Table 10-1 Interactions between an enterprise router and other cloud services

Service	Interaction
Virtual Private Cloud (VPC)	You can attach VPCs to an enterprise router to enable communication between multiple VPCs without configuring a large number of VPC peering connections.
Direct Connect	You can attach a Direct Connect virtual gateway to an enterprise router to connect VPCs to an on-premises data center through one Direct Connect connection.
Virtual Private Network (VPN)	You can attach a VPN gateway to an enterprise router to connect VPCs to an on-premises data center through a shared VPN connection.

Service	Interaction
Cloud Connect	You can add two or more enterprise routers to a central network as attachments to establish peering connections for cross-region communications on the cloud.
Identity and Access Management (IAM)	You can use IAM to assign different permissions to different users to control their access to enterprise router resources.
Cloud Eye	You can use Cloud Eye to monitor the network status of enterprise routers and their attachments, and report alarms when exceptions occur, ensuring smooth service running.
Cloud Trace Service (CTS)	You can use CTS to record operations associated with your enterprise routers for future query, audit, and backtracking.
Tag Management Service (TMS)	You can use tags to identify enterprise routers and route tables.

11 Region and AZ

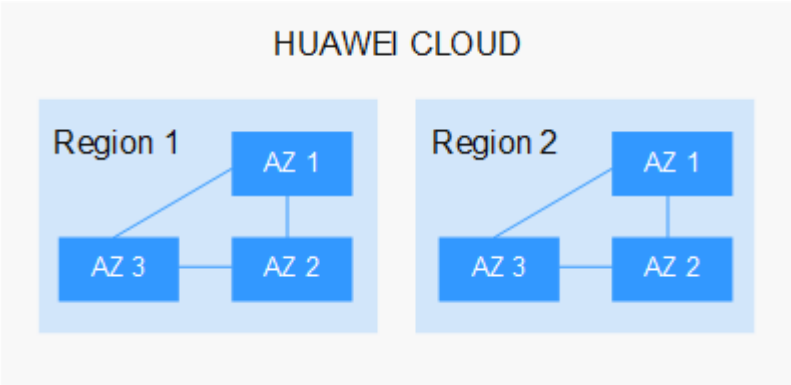
Concept

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 Regions**.

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**.

