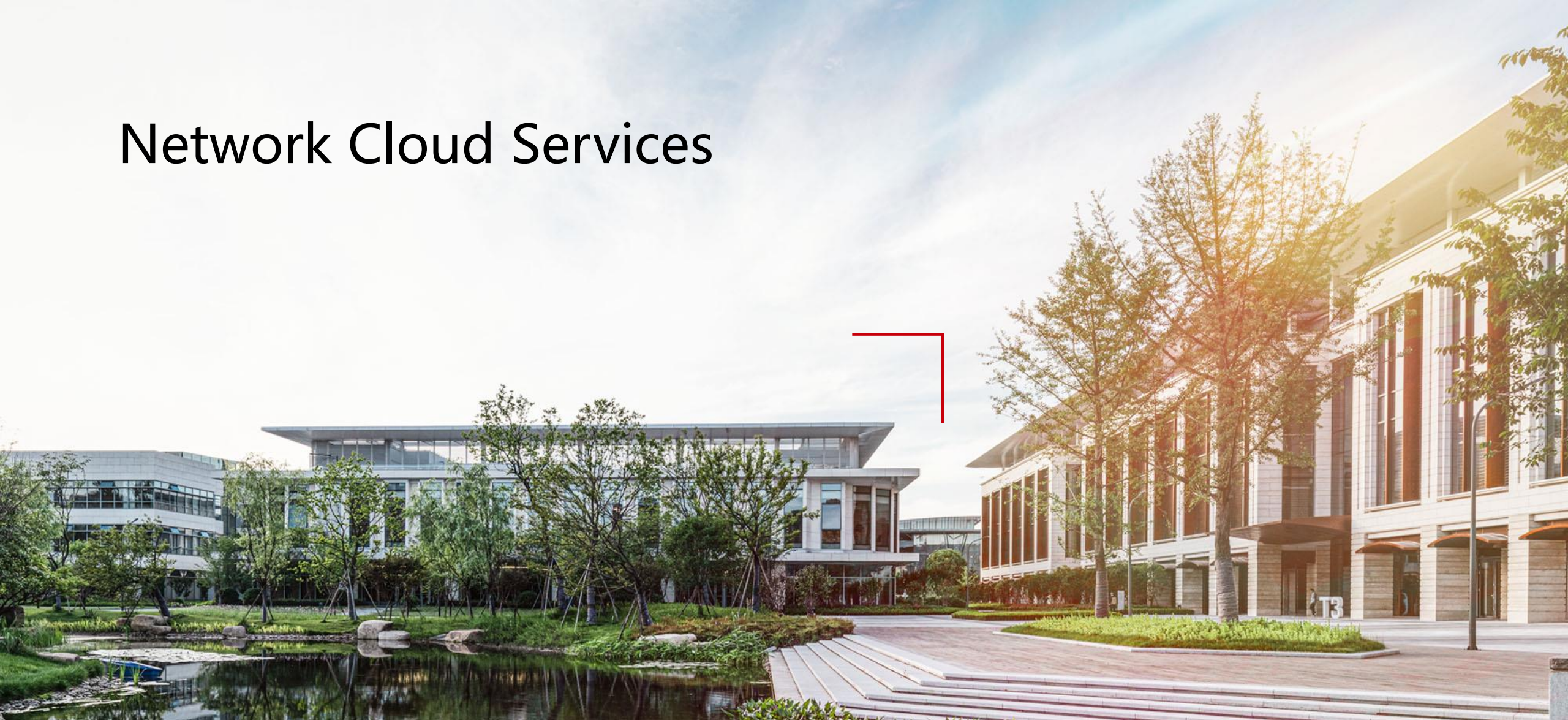


# Network Cloud Services



# Foreword

- Network resources are essential to the development of the ICT infrastructure. With network resources, devices and systems can communicate with each other so that enterprises can provide better services to their end users.
- This chapter describes the network services provided by HUAWEI CLOUD.

# Objectives

- On completion of this course, you will be able to:
  - Understand what network services are and what scenarios different services are designed for.
  - Understand how network services work and how you can use them.

# Network Service Overview



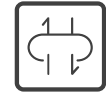
Virtual Private Cloud  
(VPC)



VPC  
Endpoint  
(VPCEP)



Elastic Load  
Balance  
(ELB)



NAT  
Gateway



Elastic IP  
(EIP)



Direct  
Connect



Virtual Private Network  
(VPN)



Cloud  
Connect



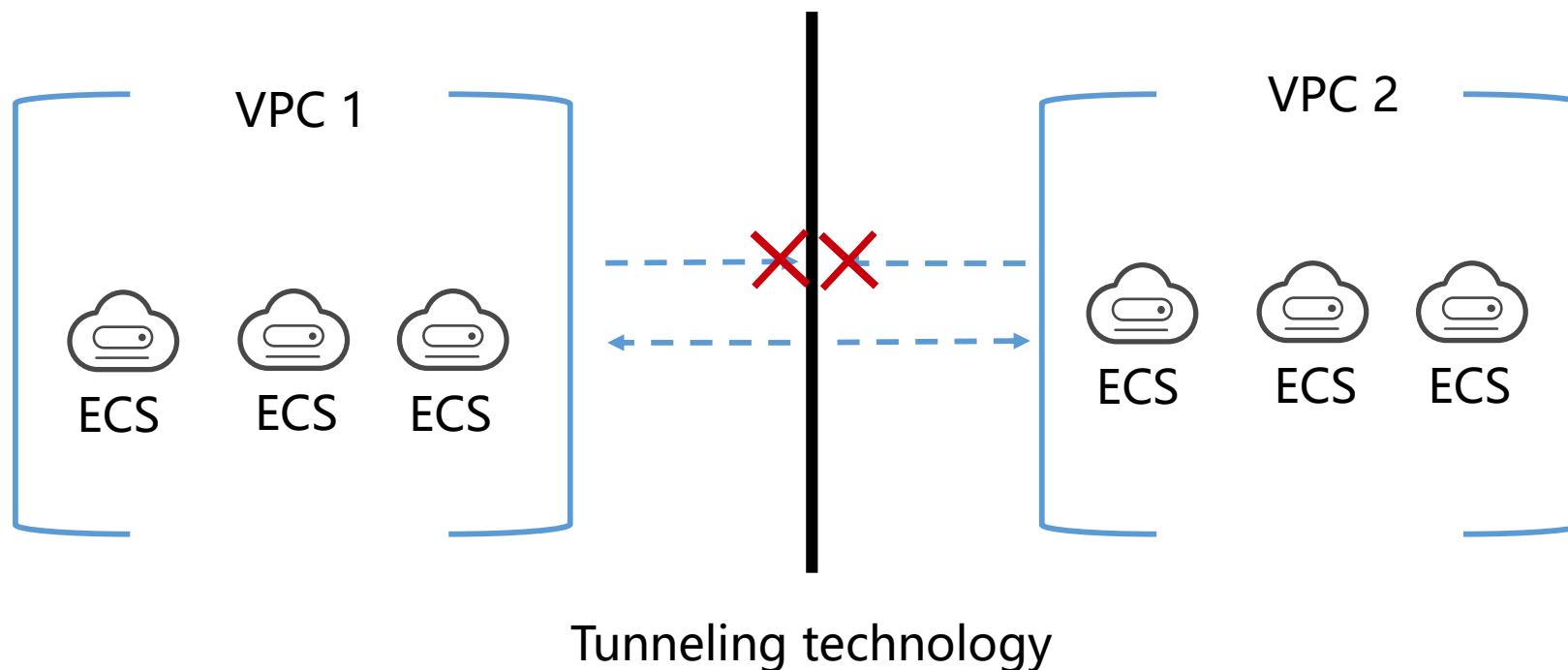
Domain Name Service  
(DNS)

# Contents

- 1. Virtual Private Cloud (VPC)**
2. Elastic Load Balance (ELB)
3. Virtual Private Network (VPN)
4. NAT Gateway
5. Other Services

# What Is a VPC?

- A Virtual Private Cloud (VPC) is a logically isolated virtual network. Within your own VPC, you can create subnets, configure route tables, assign EIPs and bandwidths, and configure security groups to manage access control.





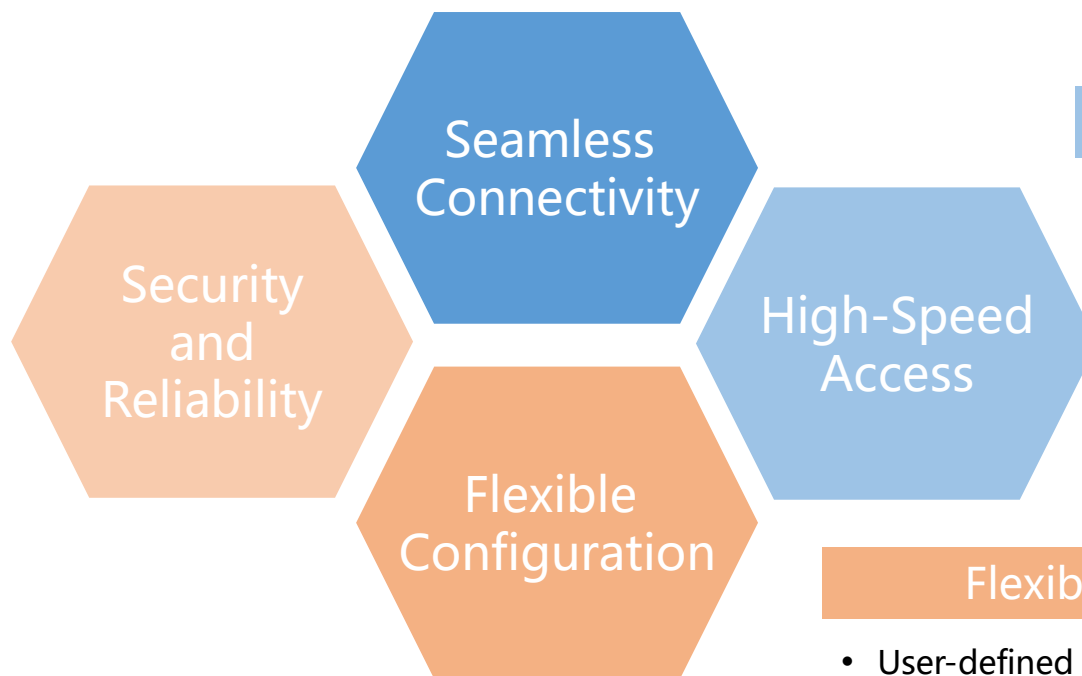
# VPC Advantages

## Seamless Connectivity

- Multiple methods for connecting to the Internet
- A VPC peering connection enables two VPCs to communicate with each other using private IP addresses.

## Security and Reliability

- 100% logical isolation
- Comprehensive security



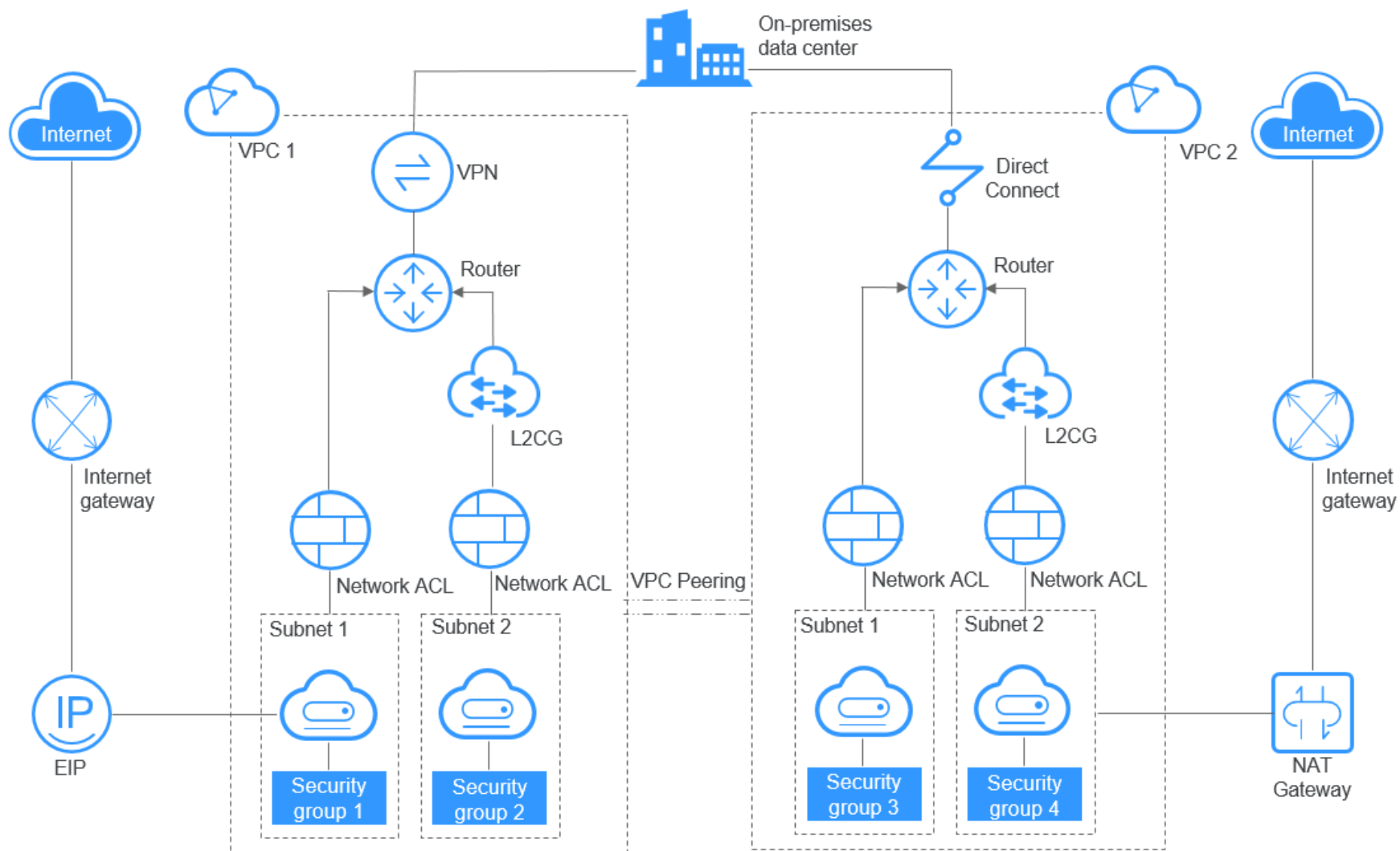
## High-Speed Access

- Dynamic BGP access to multiple carriers
- Automatic failover in real time

## Flexible Configuration

- User-defined network
- ECSs can be deployed across AZs.

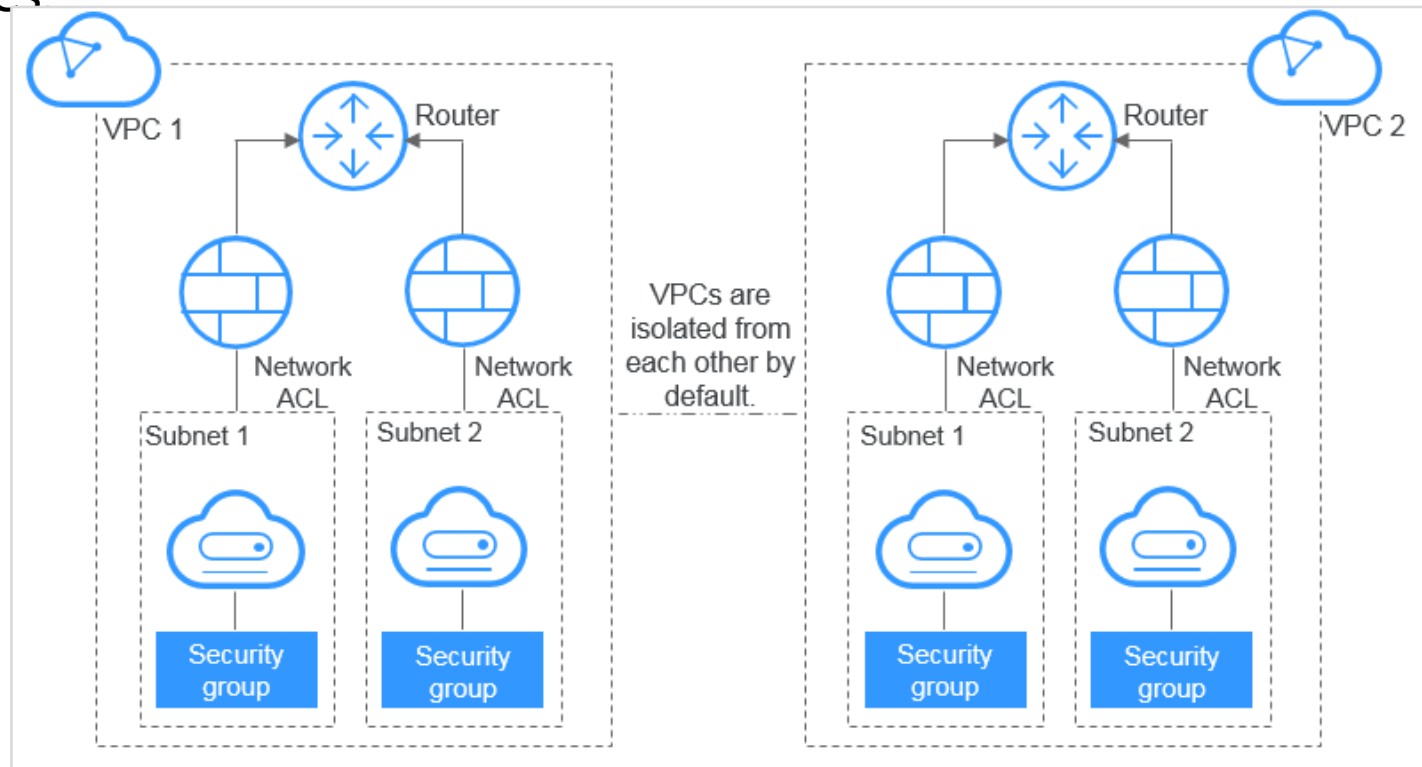
# VPC Architecture





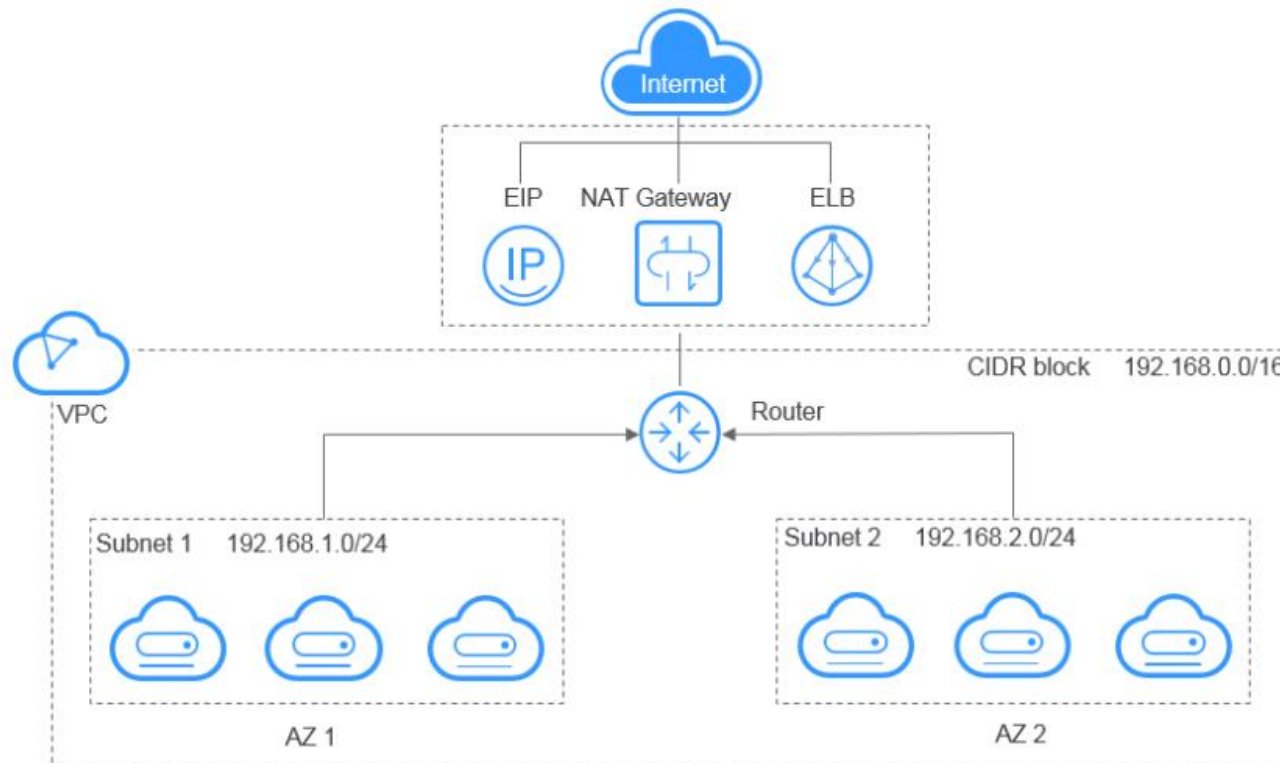
# Application Scenario - Dedicated Networks on Cloud

- Each VPC represents a private network and is logically isolated from other VPCs. You can deploy your service systems in a private network on the cloud. If you have multiple service systems, for example, a production system and a test system, you can keep them isolated by deploying them in two different VPCs



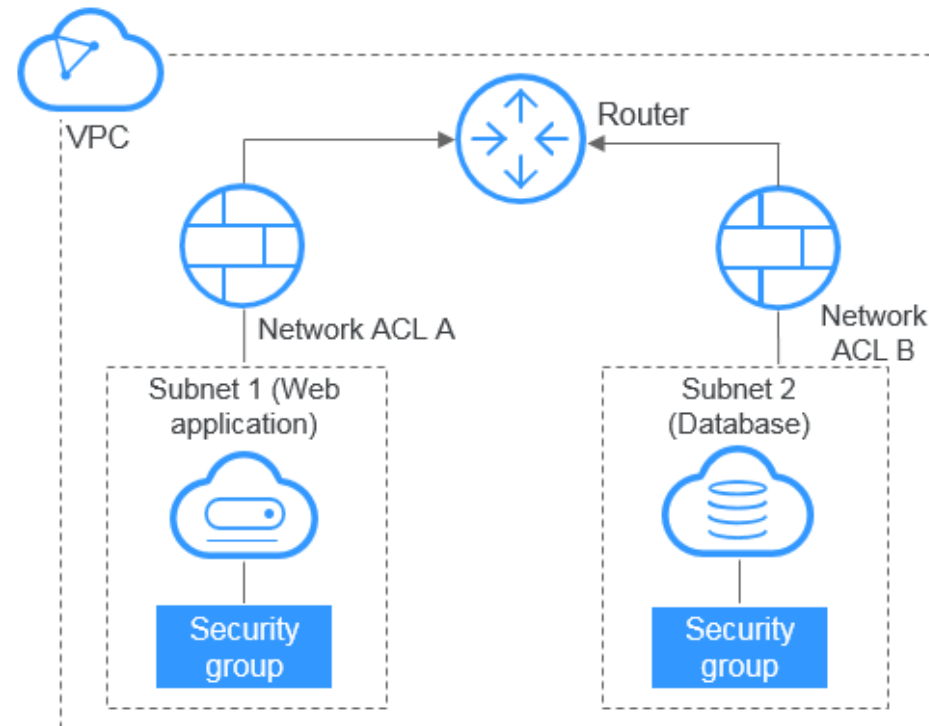
# Application Scenario - Web Application/Website Hosting

- You can host web applications and websites in a VPC and use the VPC as a regular network. With EIPs or NAT gateways, you can connect ECSs running your web applications to the Internet. You can then use load balancers provided by the ELB service to evenly distribute traffic across multiple ECSs.



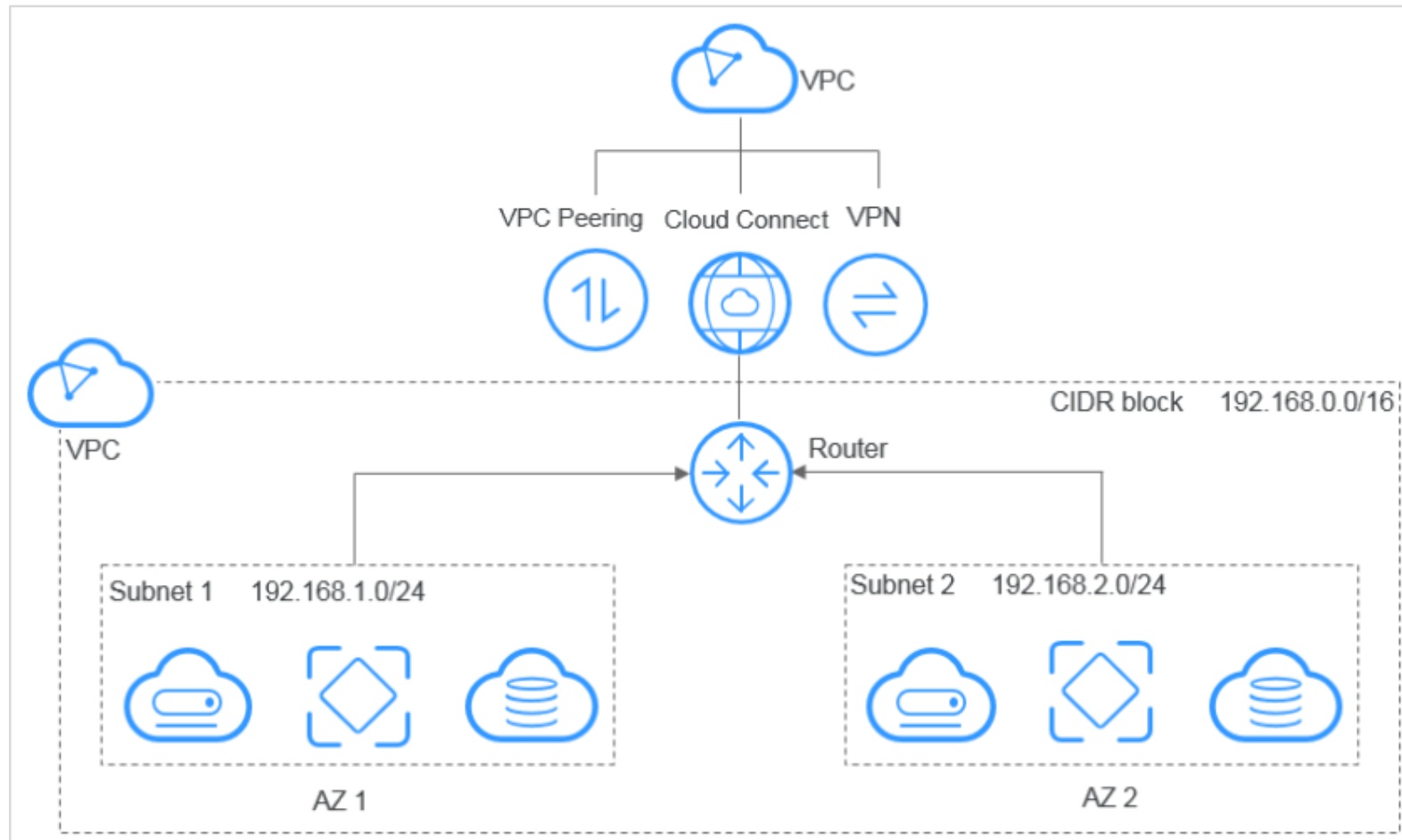
# Application Scenario - Web Application Access Control

- You can create a VPC and multiple security groups to associate web servers and database servers with different security groups and configure different access control rules for security groups. You can launch web servers in a publicly accessible subnet, and also run database servers in subnets that are not publicly accessible. In this way, you can ensure high security.



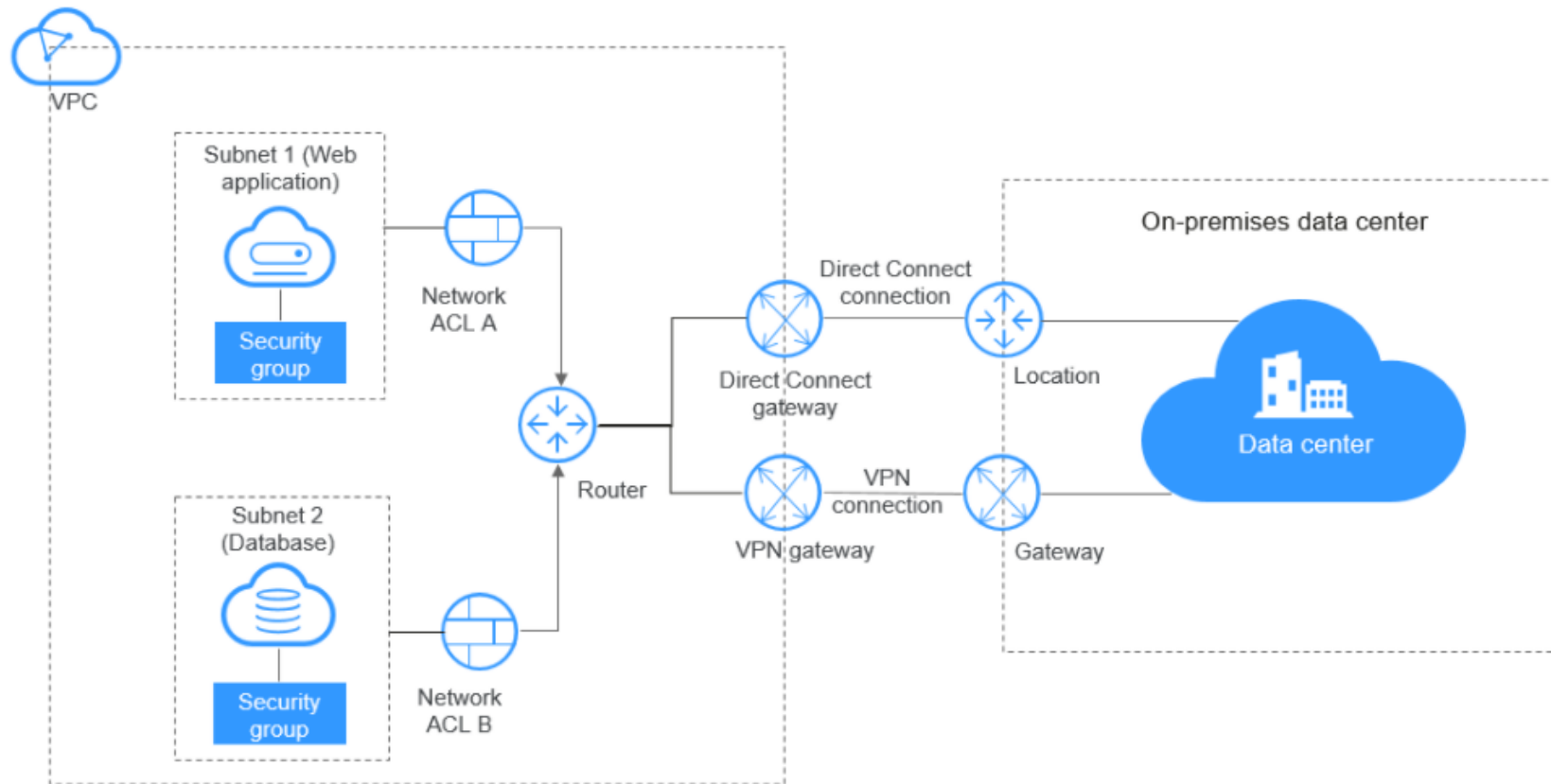
# Application Scenario - VPC Connectivity Options

- You can use the following cloud services to allow two VPCs to communicate with each other.

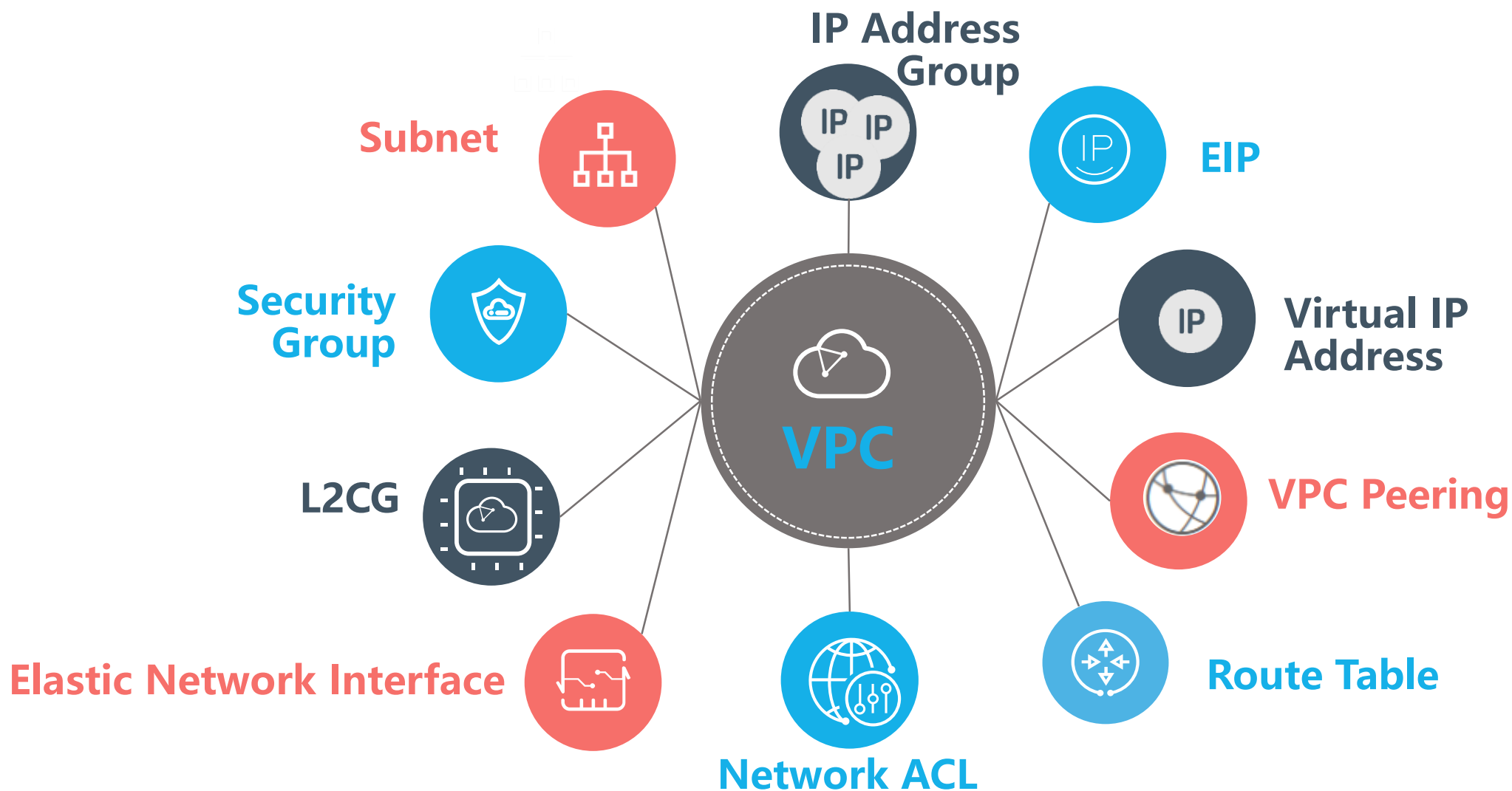


# Application Scenario - Hybrid Cloud Deployment

- If you have an on-premises data center and you do not want to migrate all of your business to the cloud, you can build a hybrid cloud. That way you can keep core data in your own data center.

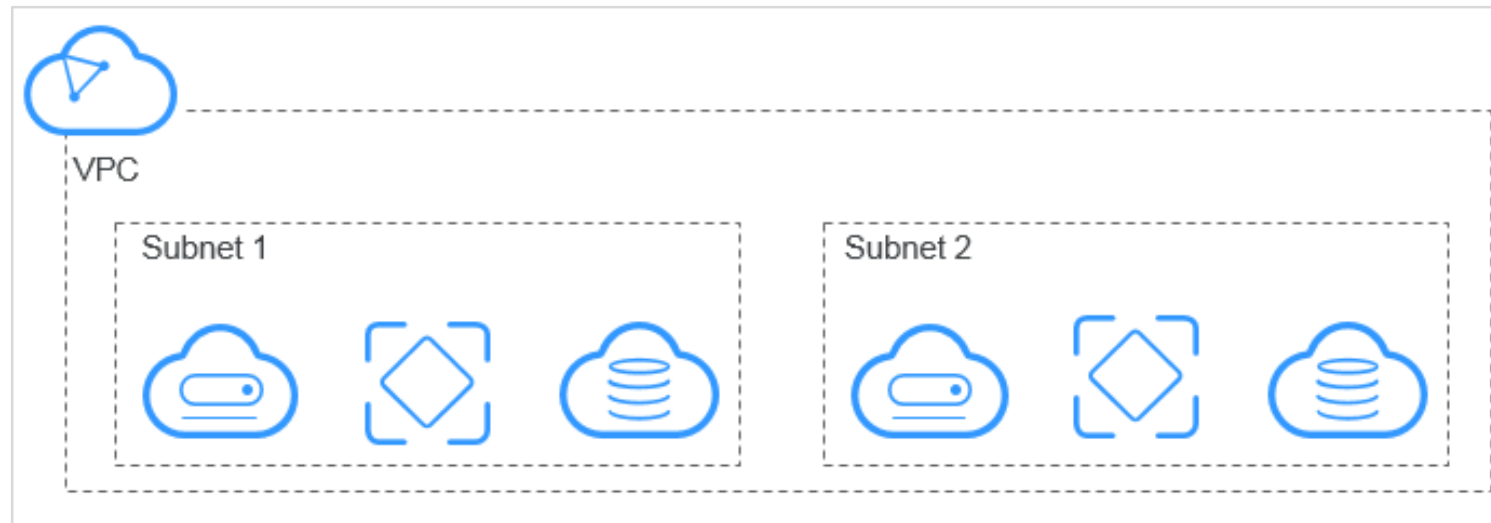


# VPC Concepts



# VPC - Subnet

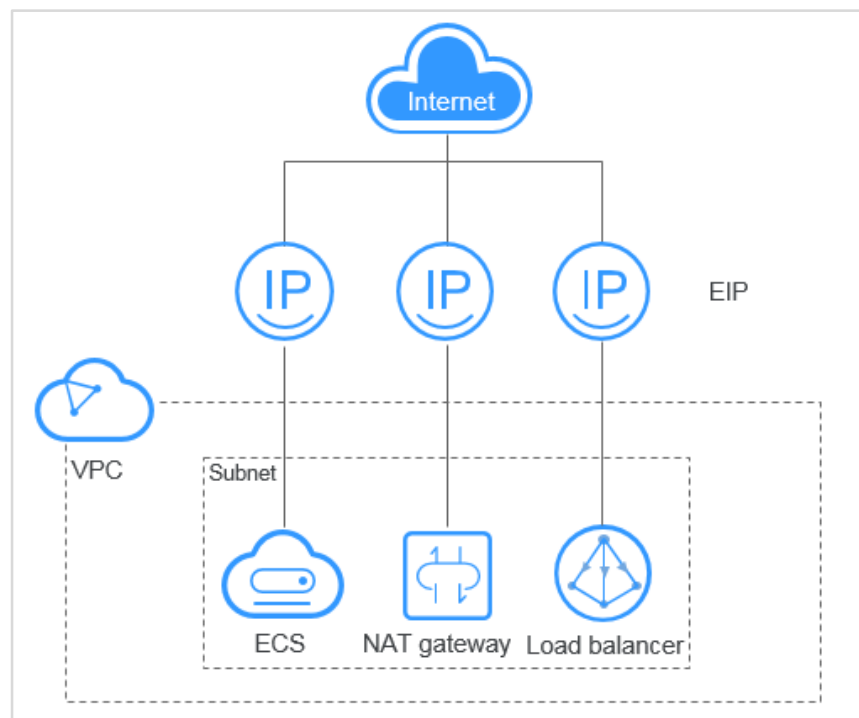
- A subnet is a unique CIDR block, a range of IP addresses, in your VPC. All resources in a VPC must be deployed on subnets. Once a subnet has been created, its CIDR block cannot be modified.





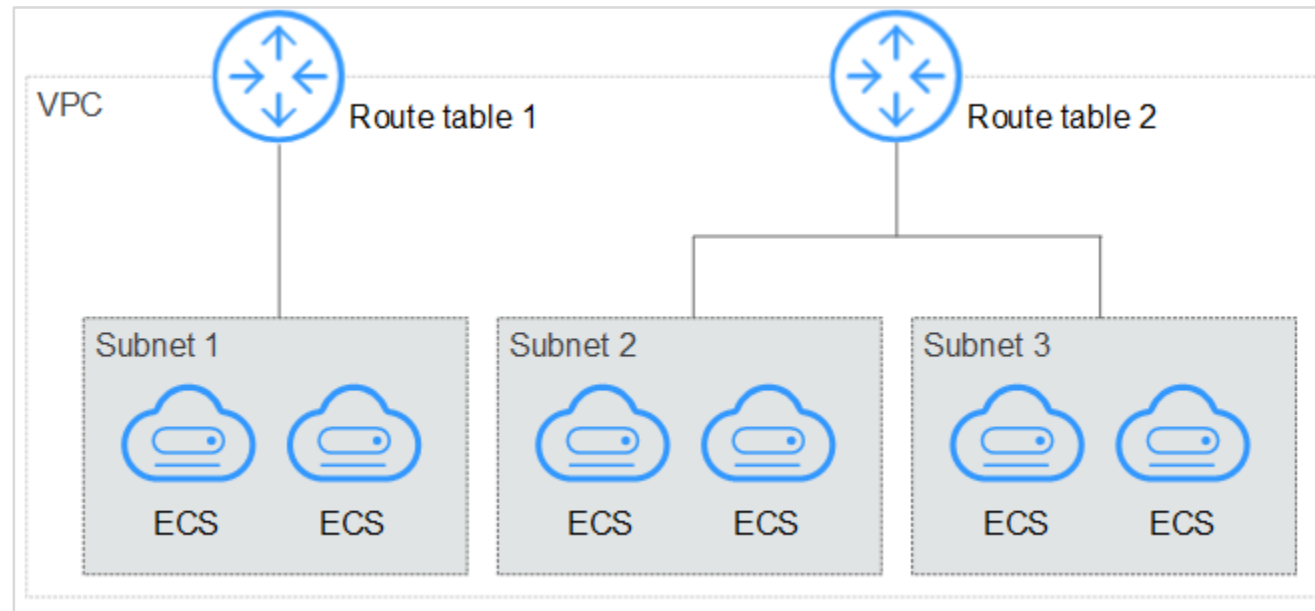
# VPC - EIP

- The Elastic IP (EIP) service enables your cloud resources to communicate with the Internet using static public IP addresses and scalable bandwidths. EIPs can be bound to or unbound from ECSs, BMSs, virtual IP addresses, load balancers, and NAT gateways. Various billing modes are provided to meet diverse service requirements. Each EIP can be used by only one cloud resource at a time.



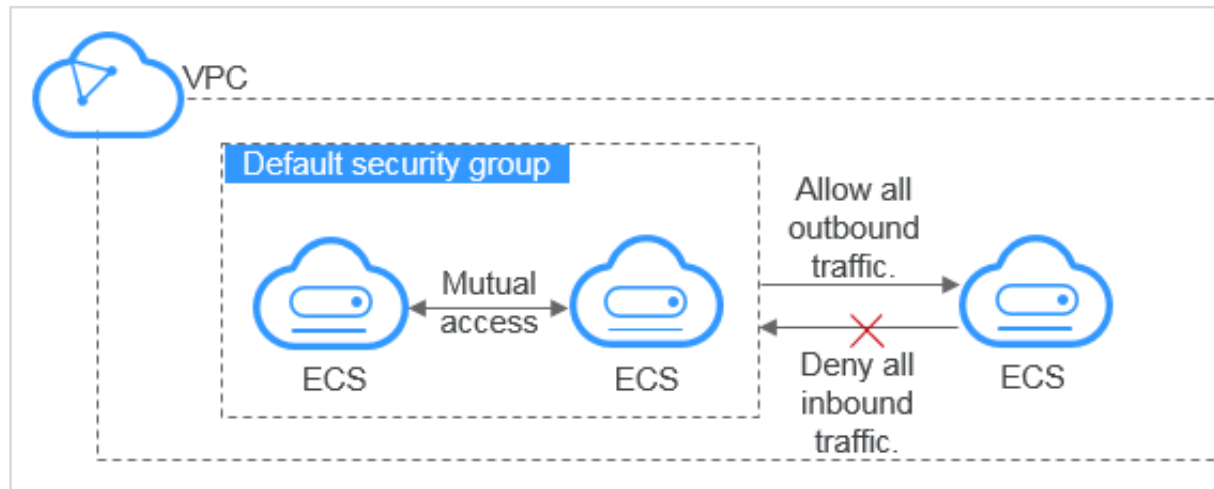
# VPC - Route Table

- A route table contains a set of routes that are used to determine where network traffic from your subnets in a VPC is directed. Each subnet in a VPC must be associated with a route table. A route table can be associated with multiple subnets. However, each subnet can only be associated with one route table.



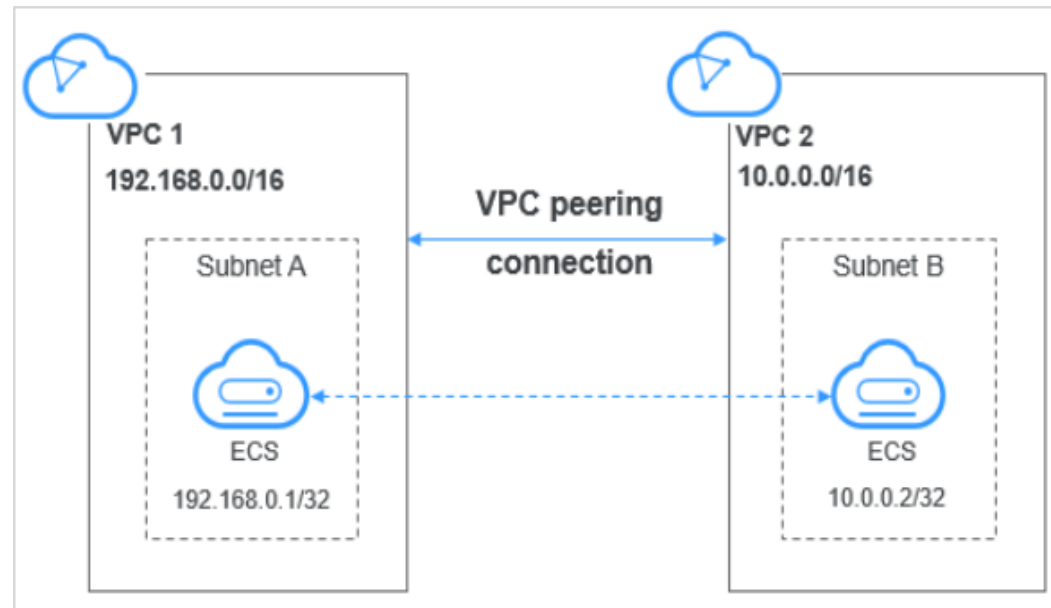
# VPC - Security Group

- A security group is a collection of access control rules for ECSs that have the same security requirements and are mutually trusted within a VPC. After you create a security group, you can create different access rules for the security group, and the rules will apply to any ECS that the security group contains.



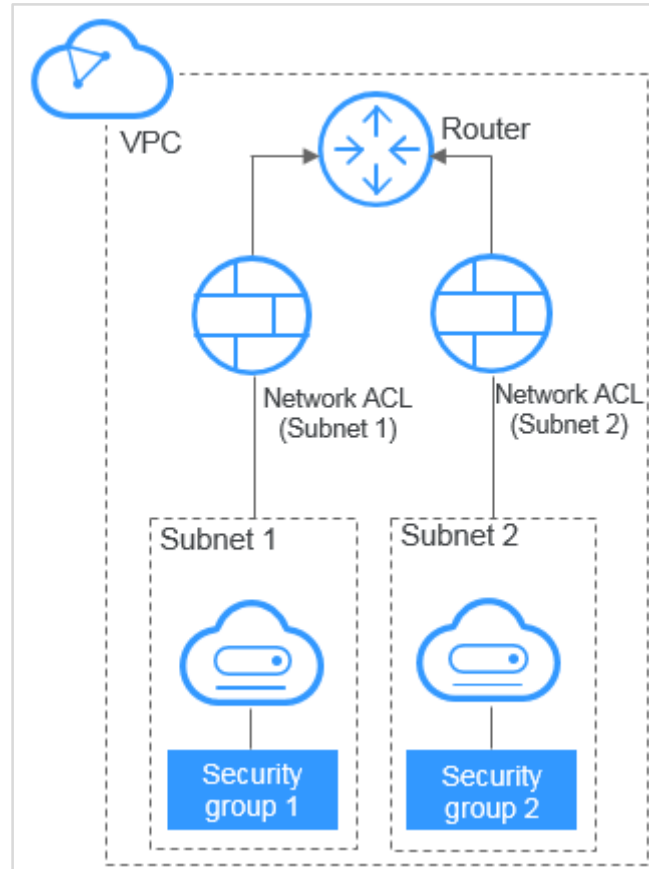
# VPC - VPC Peering

- A VPC peering connection is a network connection between two VPCs in the same region. It enables you to route traffic between them using private IP addresses. You can create a VPC peering connection between your own VPCs, or between your VPC and a VPC of another account within the same region. However, you cannot create a VPC peering connection between VPCs in different regions.



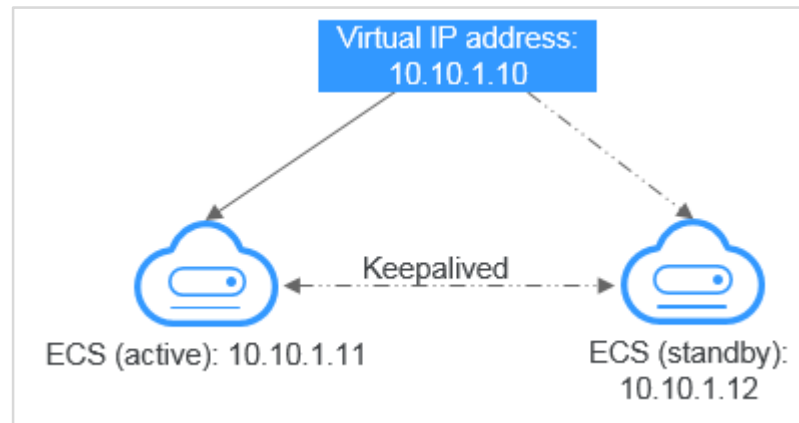
# VPC - Network ACL

- A network ACL allows you to create rules to control traffic in and out of one or more subnets.



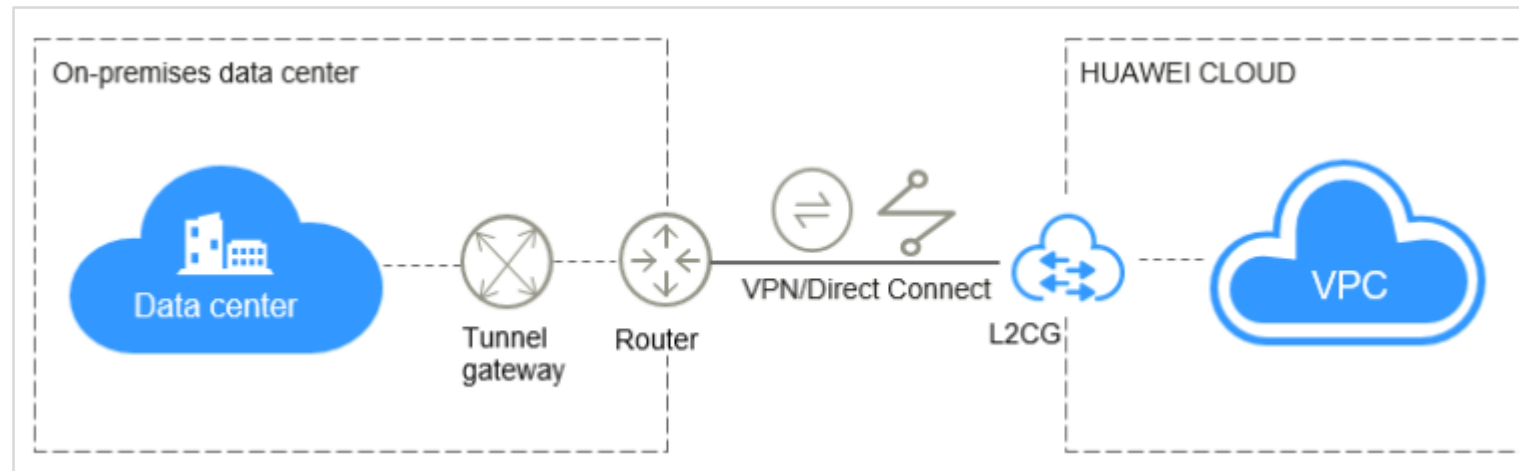
# VPC - Virtual IP Address

- A virtual IP address can be shared among multiple ECSs. An ECS can have both private and virtual IP addresses, and you can access the ECS through either IP address. A virtual IP address has the same network access capability as a private IP address. Virtual IP addresses are used for high availability as they make active/standby ECS switchover possible.



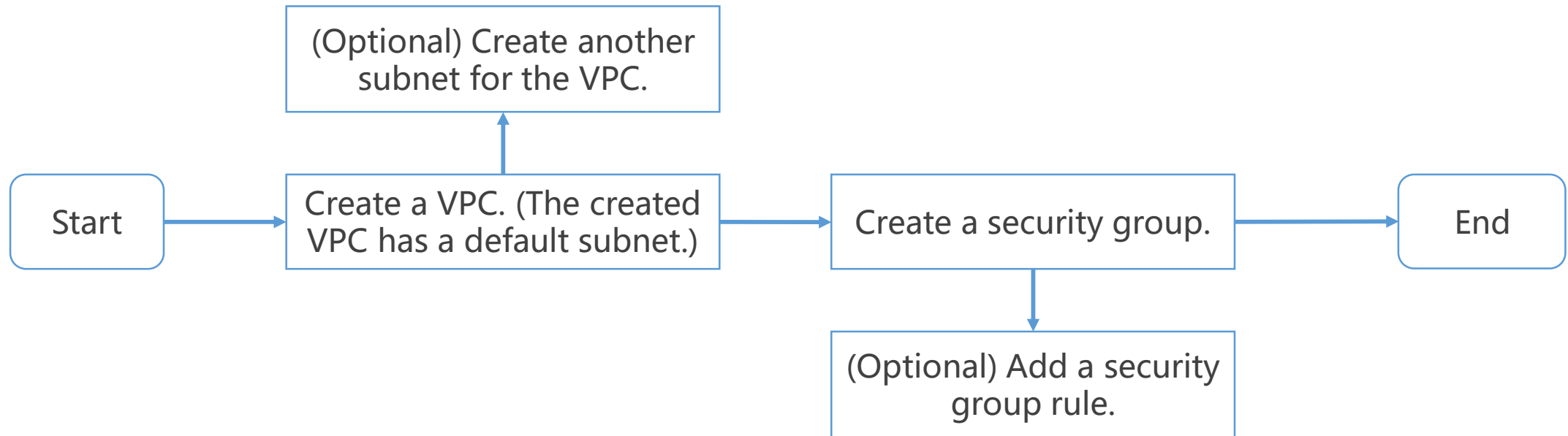
# VPC - L2CG

- An L2CG is a virtual tunnel gateway that works with Direct Connect or VPN to establish network communication between cloud and on-premises networks. The gateway allows you to migrate data center or private cloud services to the cloud without changing subnets and IP addresses.





# VPC Configuration Process



# VPC Configuration - Subnet

- Each VPC comes with a default subnet. If the default subnet cannot meet your requirements, create one.
- The subnet is configured with DHCP by default. When an ECS in this subnet starts, the ECS automatically obtains an IP address using DHCP.
- An AZ is a physical location where resources use independent power supplies and networks within a given region.

Default Subnet

AZ

AZ3 ?

Name

subnet-406f

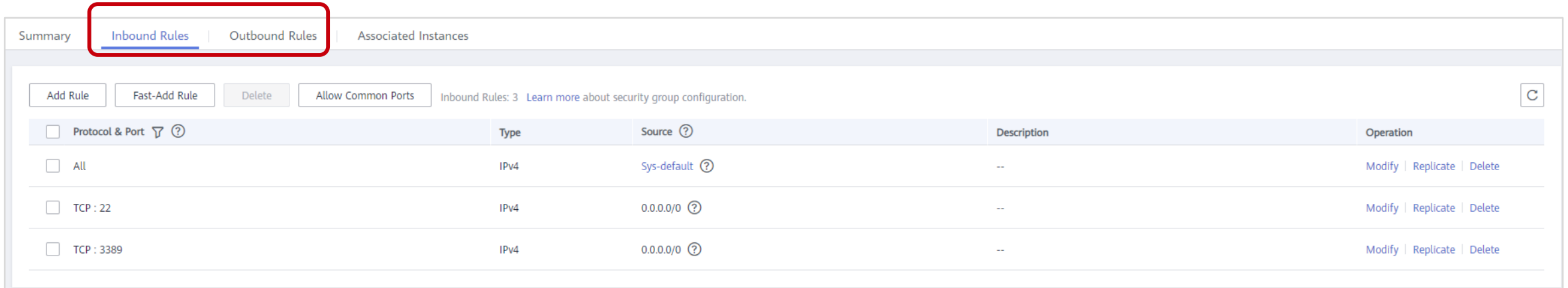
CIDR Block

192 · 168 · 0 · 0 / 24 ? Available IP Addresses: 251

The CIDR block cannot be modified after the subnet has been created.

# VPC Configuration - Security Group

- Your account automatically comes with a default security group. You can add inbound and outbound rules to the default security group or create a new security group.
- Inbound rules control incoming traffic to ECSs in the security group.
- Outbound rules control outgoing traffic from ECSs in the security group.
- Default security group rules



The screenshot displays the 'Inbound Rules' tab of a security group configuration page. The tab is highlighted with a red box. The page shows a table of inbound rules for a security group. The table has columns for 'Protocol & Port', 'Type', 'Source', 'Description', and 'Operation'. There are three rules listed: a default rule for 'All' traffic, and two custom rules for 'TCP : 22' and 'TCP : 3389' traffic. The 'Source' column for the custom rules shows '0.0.0.0/0' with a help icon. The 'Operation' column for each rule has links for 'Modify', 'Replicate', and 'Delete'.

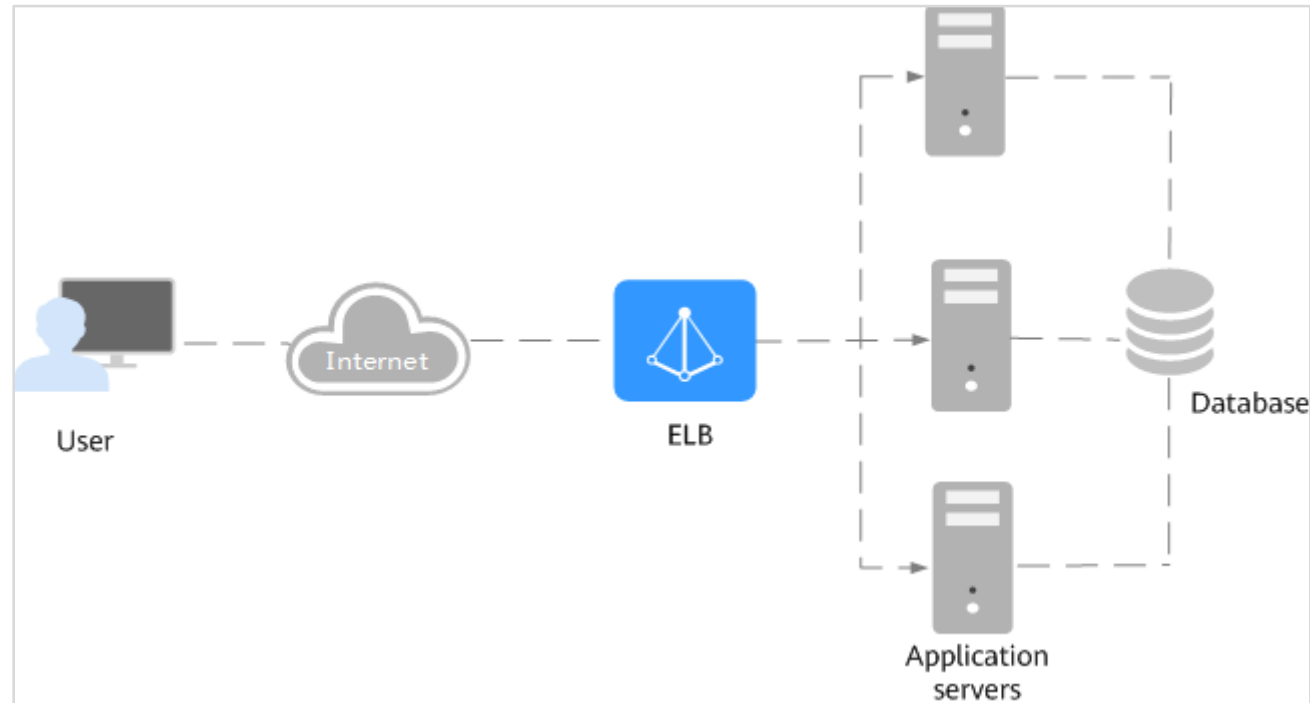
Protocol & Port	Type	Source	Description	Operation
<input type="checkbox"/> All	IPv4	Sys-default	--	<a href="#">Modify</a>   <a href="#">Replicate</a>   <a href="#">Delete</a>
<input type="checkbox"/> TCP : 22	IPv4	0.0.0.0/0	--	<a href="#">Modify</a>   <a href="#">Replicate</a>   <a href="#">Delete</a>
<input type="checkbox"/> TCP : 3389	IPv4	0.0.0.0/0	--	<a href="#">Modify</a>   <a href="#">Replicate</a>   <a href="#">Delete</a>

# Contents

1. Virtual Private Cloud (VPC)
- 2. Elastic Load Balance (ELB)**
3. Virtual Private Network (VPN)
4. NAT Gateway
5. Other Services

# What Is ELB?

- Elastic Load Balance (ELB) automatically distributes incoming traffic across multiple backend servers based on the listening rules you configure. ELB expands the service capabilities of your applications and improves their availability by eliminating single points of failure (SPOFs).



# ELB Advantages

## Robust Performance

- ELB can establish up to 100 million concurrent connections so that your applications can handle a massive volume of concurrent requests.

## Ease-of-Use

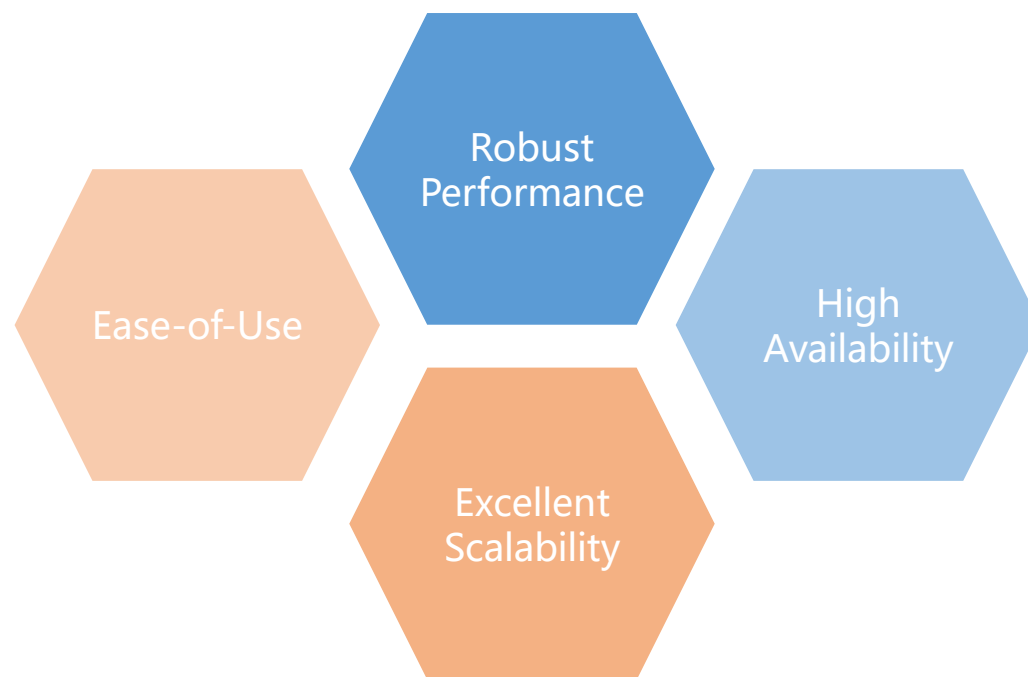
- The deployment is simple and takes effect immediately.
- A diverse set of protocols and algorithms enable you to customize traffic routing policies to your needs.

## High Availability

- ELB is deployed in clusters and ensures that your services run uninterrupted. If servers in one AZ are unhealthy, ELB automatically routes traffic to healthy servers in other AZs.

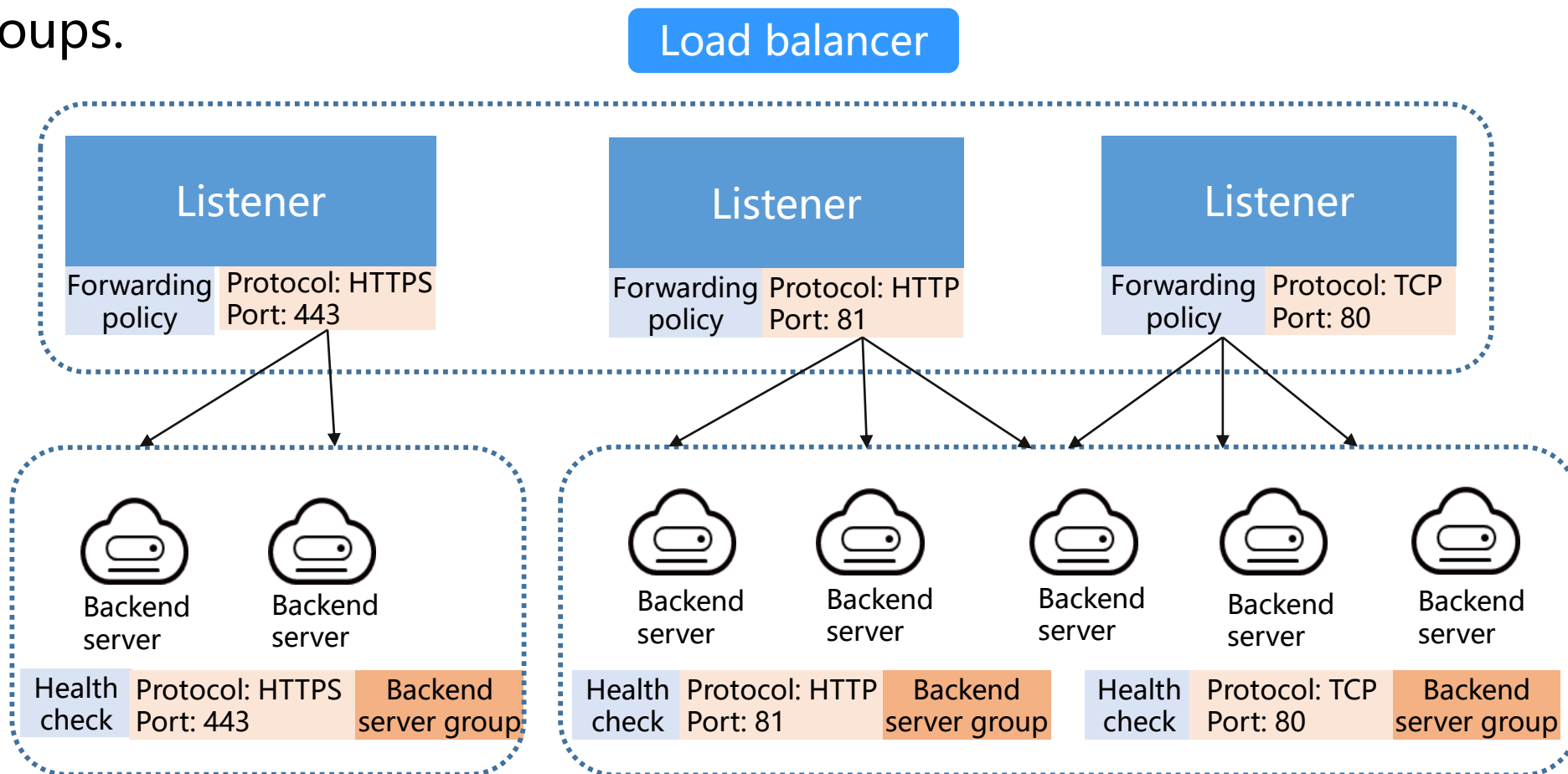
## Excellent Scalability

- ELB automatically scales in line with spikes in incoming traffic to ensure that your applications always stay online. It works with Auto Scaling to flexibly adjust the number of servers and intelligently distribute incoming traffic across them.



# ELB Architecture

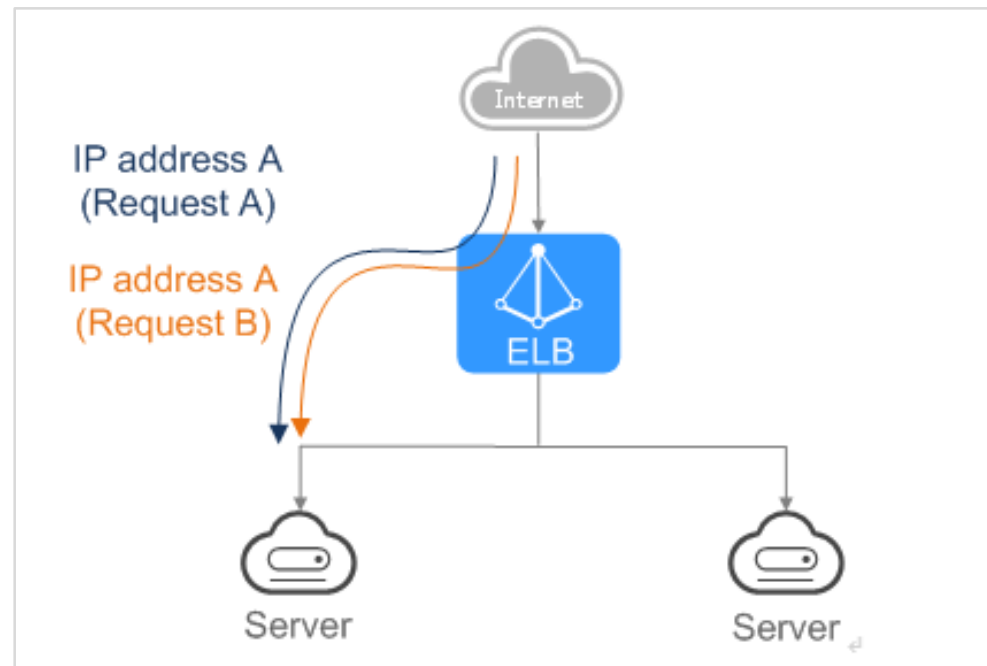
- ELB consists of three components: load balancers, listeners, and backend server groups.





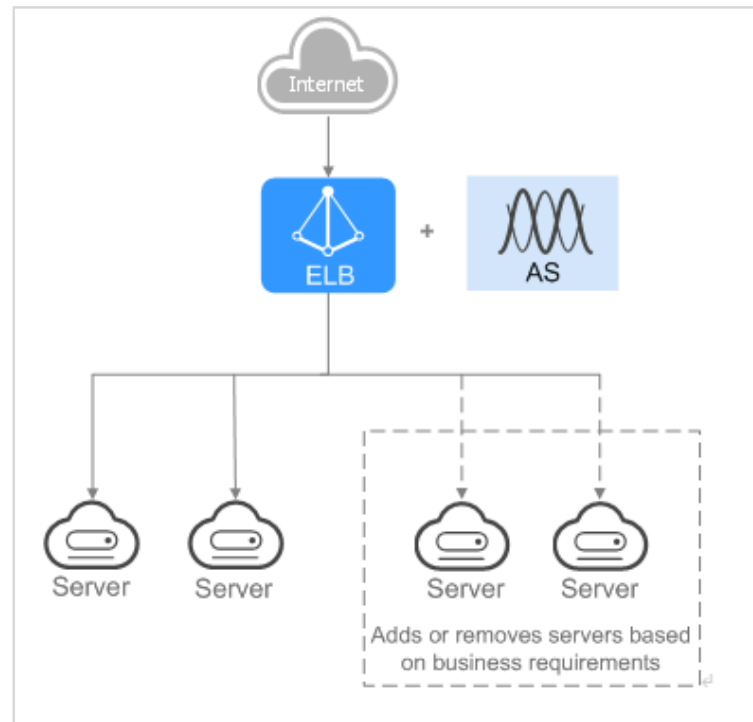
# Application Scenario: Heavy-Traffic Applications

- For an application with heavy traffic, such as a large web portal or mobile app store, ELB evenly distributes incoming traffic to multiple backend servers, balancing the load while ensuring stable performance. Sticky sessions ensure that requests from one client are always forwarded to the same backend server.



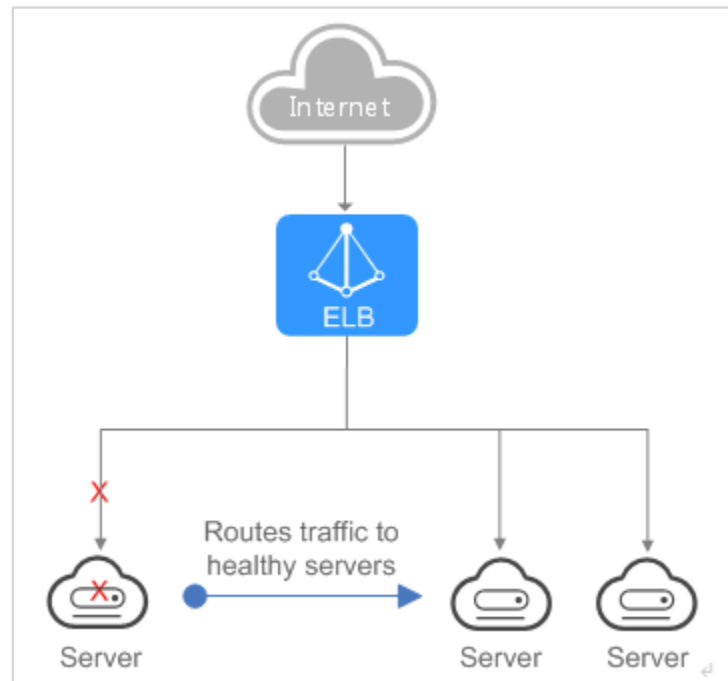
# Application Scenario: Applications with different Traffic

- For an application that has predictable peaks and troughs in traffic volumes, ELB works with AS to add or remove backend servers to keep up with changing demands. One example is flash sales, during which there are predictable traffic spikes that only last a short while. ELB can work with AS to run only the required number of backend servers needed to handle the load of your application.



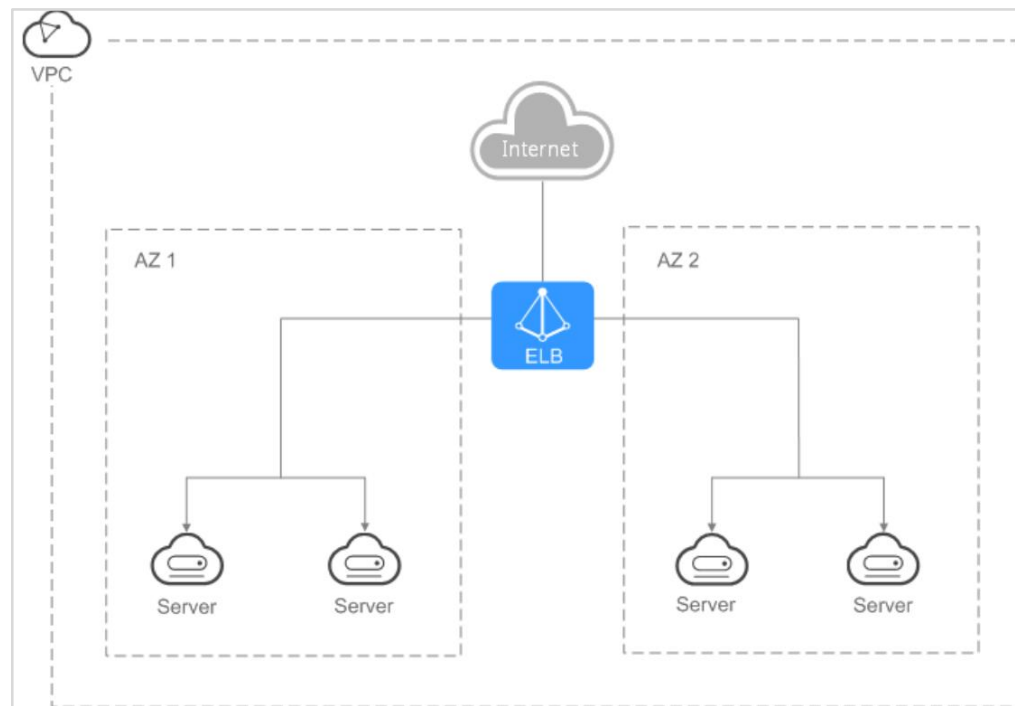
# Application Scenario: Eliminating SPOFs

- ELB routinely performs health checks on backend servers. If any backend server is unhealthy, ELB will not route requests to this server until it recovers. This makes ELB a good choice for running applications that require high reliability.



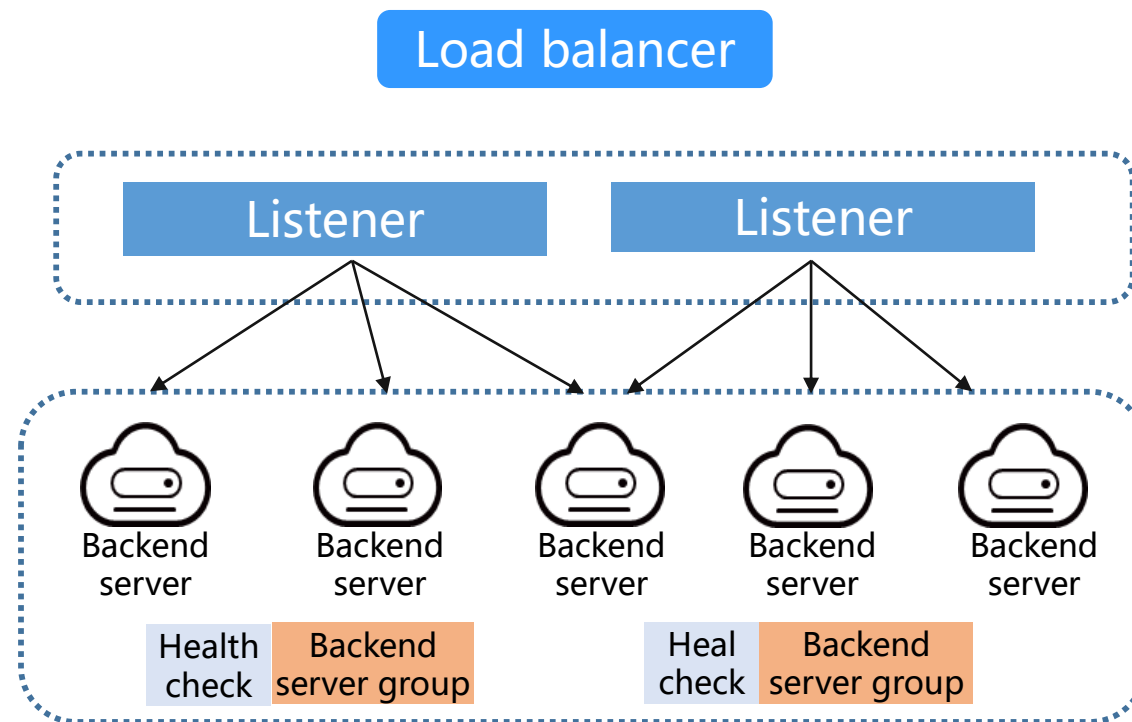
# Application Scenario: Cross-AZ Load Balancing

- ELB can distribute traffic across AZs. If an AZ becomes faulty, ELB distributes incoming traffic across backend servers in other AZs. It is useful for applications that require high availability.



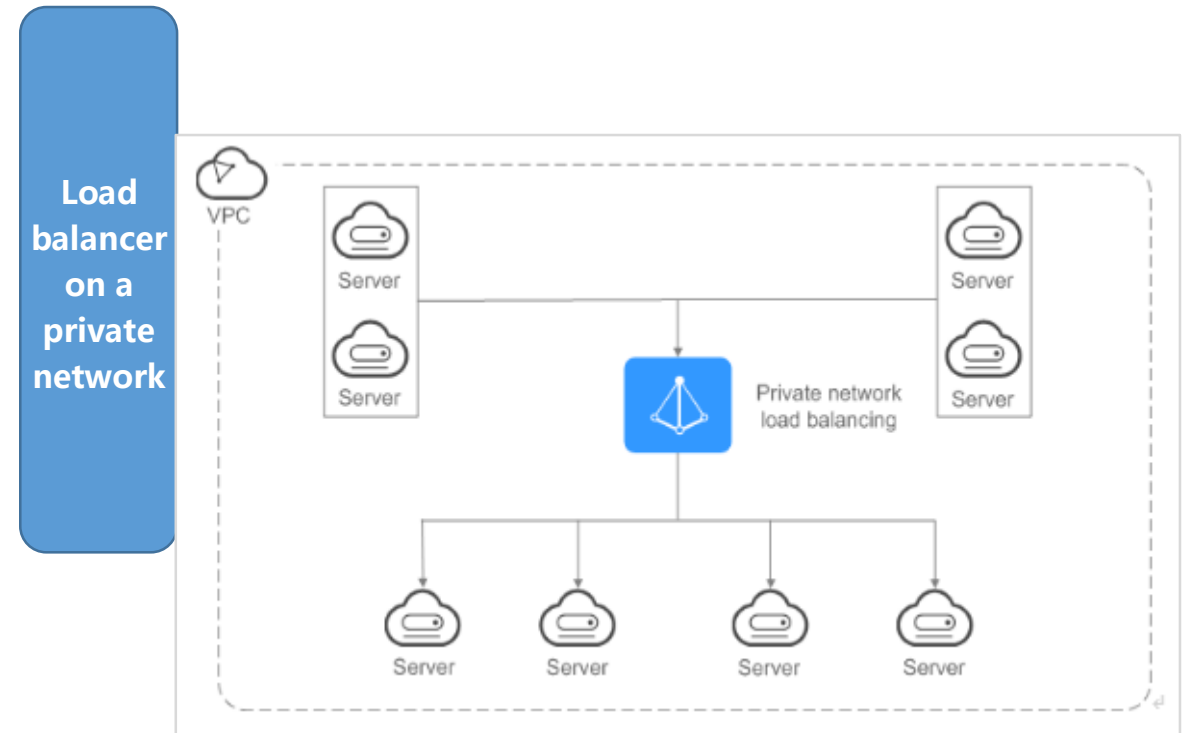
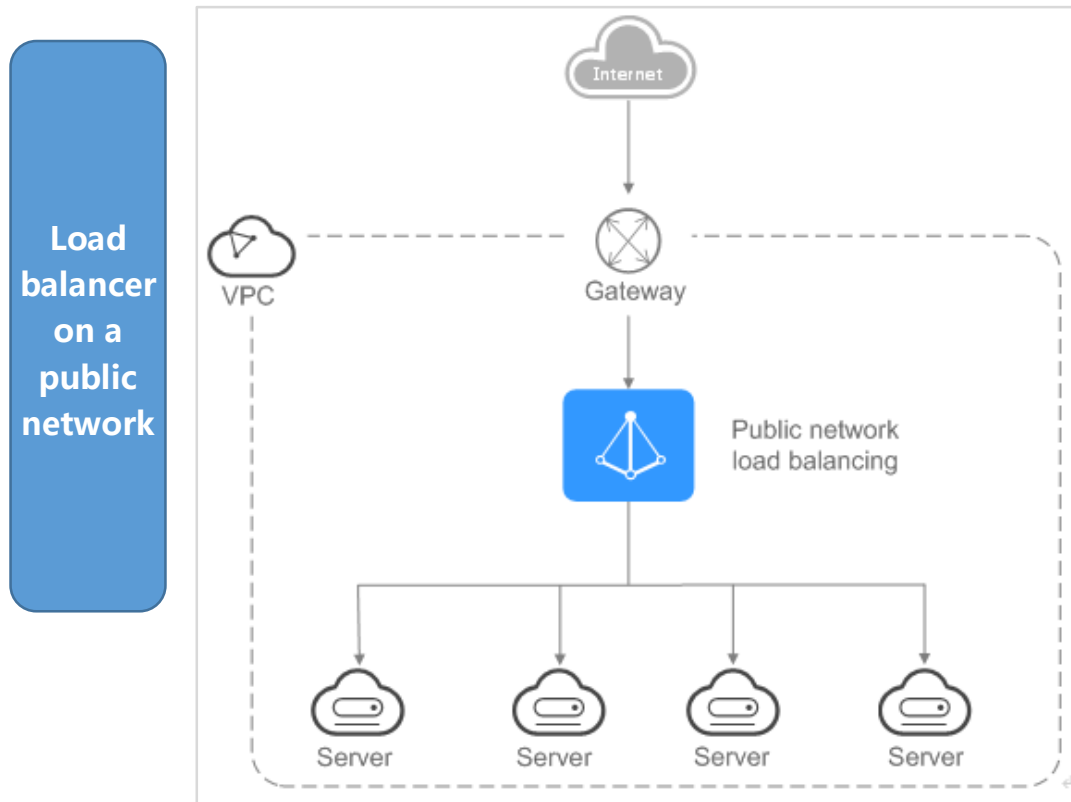
# ELB Concepts

- A load balancer distributes incoming traffic across backend servers.
- A listener listens on requests from clients and routes the requests to backend servers based on the settings that you configure when you add the listener.
- A backend server group is a group of cloud servers that have same features. When you add a listener, you select a load balancing algorithm and create or select a backend server group. Incoming traffic is routed to the corresponding backend server group based on the listener's configuration.
- ELB periodically sends heartbeat messages to associated backend servers to check their health and ensure that traffic is distributed only to healthy backend servers. This can improve the availability of your applications.



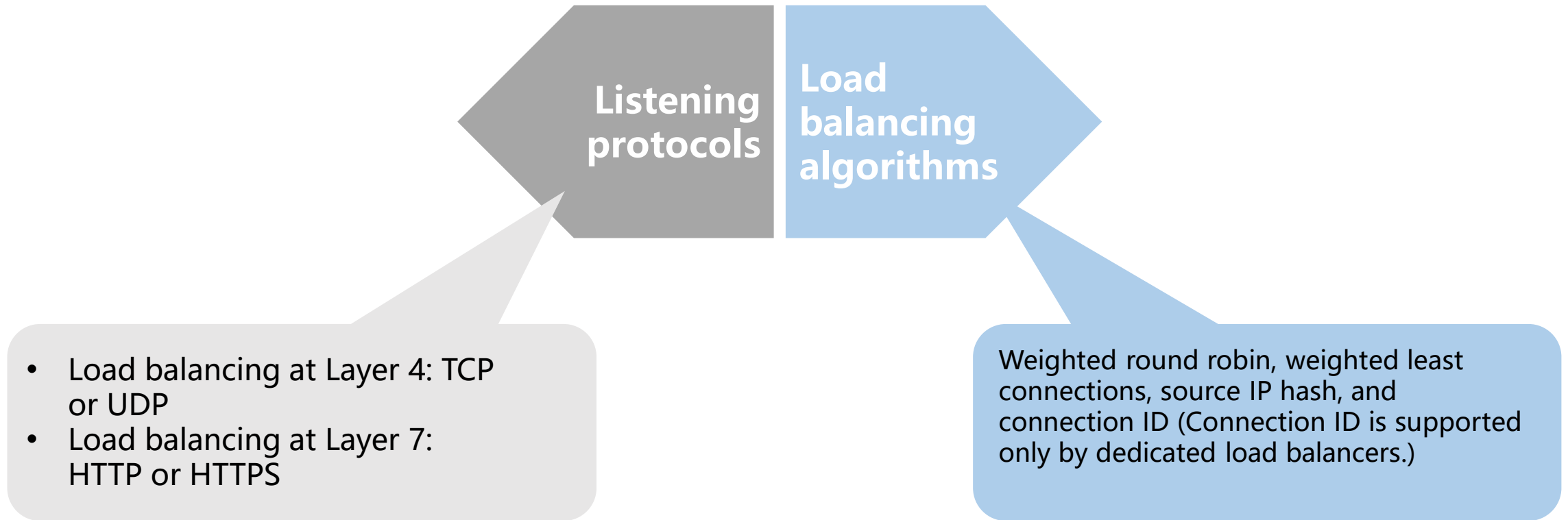
# ELB - Load Balancer

- A load balancer distributes incoming traffic across multiple backend servers. Load balancers can work on both public and private networks.



# ELB - Listener

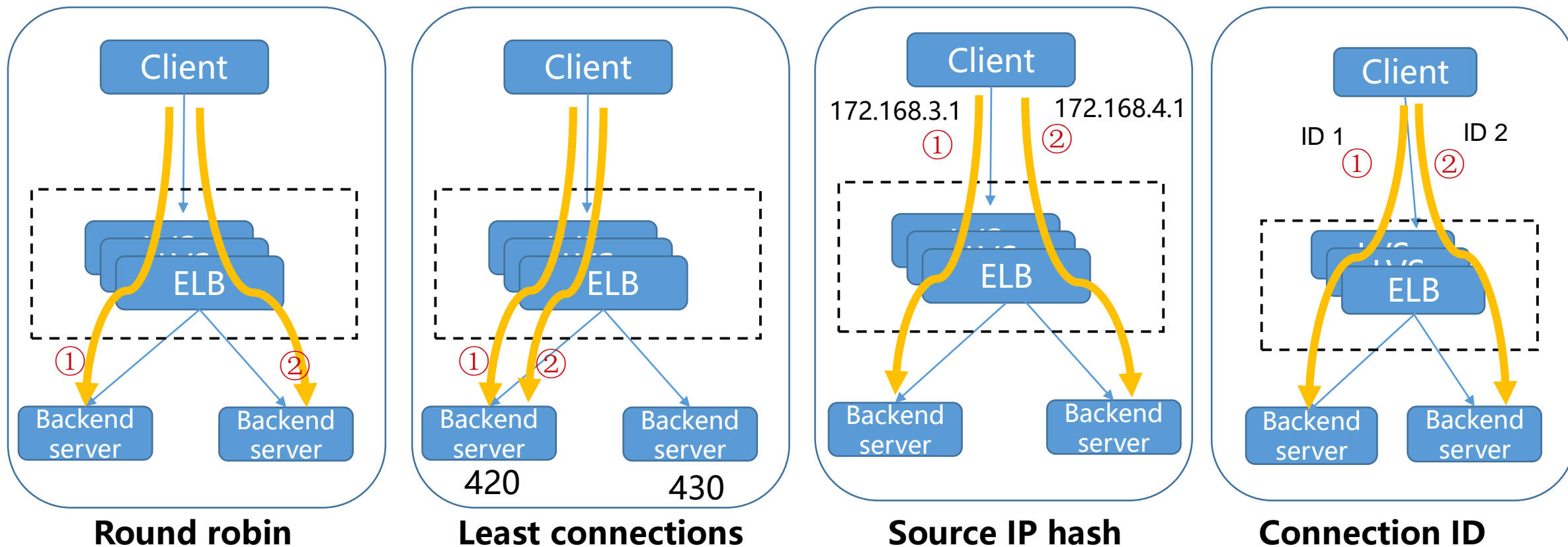
- A listener listens on requests from clients and routes the requests to backend servers based on the settings that you configure when you add the listener.





# ELB - Backend Server Group

- A backend server group contains at least one backend server to process client requests forwarded by a load balancer. When you add a listener to a load balancer, you specify a backend server group to receive requests from the load balancer using the port and protocol you specify for the backend server group and the load balancing algorithm you select. ELB supports the following load balancing algorithms.



# ELB - Health Check

- ELB periodically sends heartbeat messages to associated backend servers to check their health and ensure that traffic is distributed only to healthy servers. This can improve the availability of your applications. If a backend server is unhealthy, the load balancer stops routing traffic to it. The load balancer will resume routing requests to the backend server after it recovers.



# ELB Configuration Process

## 1. Creating a Load Balancer

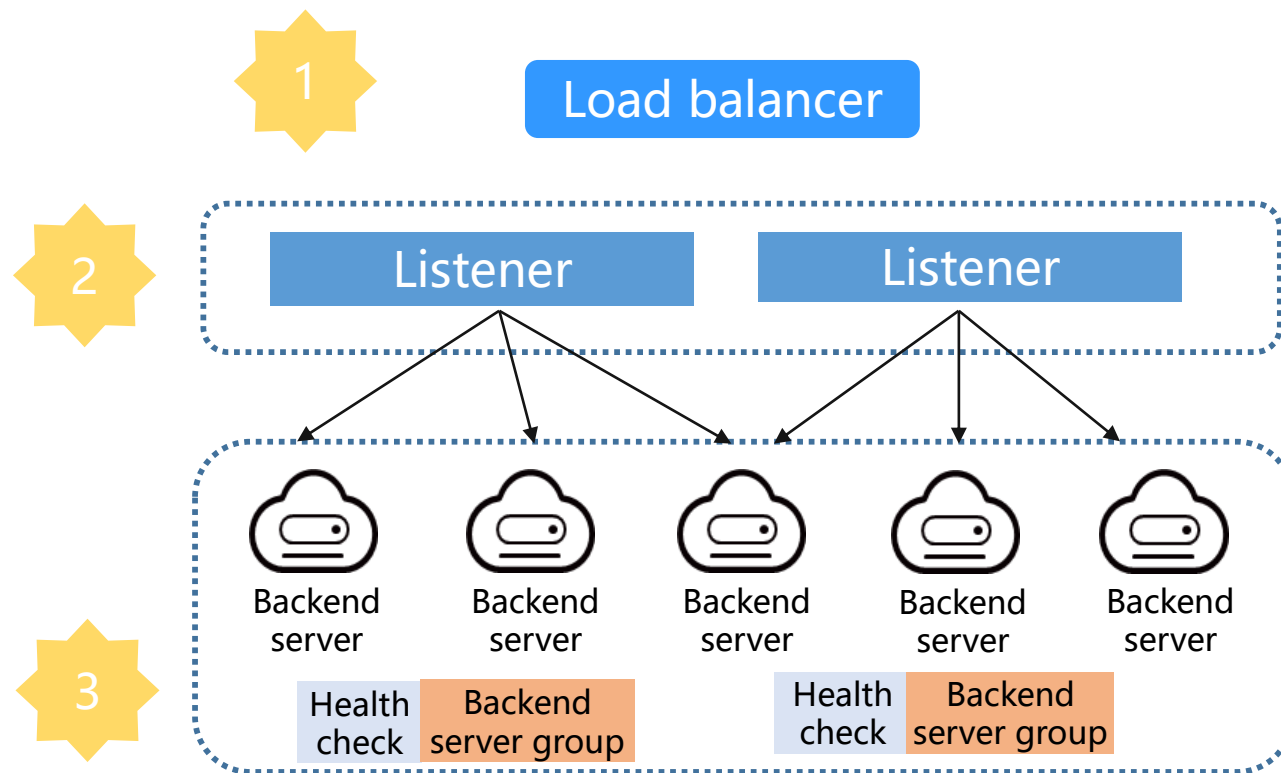
- ❑ Click **Buy Elastic Load Balancer**.
- ❑ Select the load balancer type.
- ❑ Configure the network.

## 2. Adding a Listener

- ❑ Locate the created load balancer.
- ❑ Configure the protocol and port.

## 3. Adding a Backend Server Group

- ❑ Select a load balancing algorithm.
- ❑ Configure a health check.



# ELB Configuration - Creating a Load Balancer

- Before creating a load balancer, you need to plan its region, network, protocol, and backend servers.

★ Region AP-Singapore

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

★ Network Type Public network Private network ?

★ VPC vpc-S01 [View VPC](#)

★ Subnet subnet-01 (192.168.0.0/24) [View Subnet](#) Available private IP addresses: 250

★ Private IP Address Automatically-assigned IP ...

★ EIP ☒ New EIP ☐ Use existing ?

★ EIP Type Dynamic BGP

# ELB Configuration - Adding a Listener

- After you have created a load balancer, you need to add at least one listener. A listener listens on requests from clients and routes the requests to backend servers based on the settings that you configure when you add the listener.

### Add Listener

1 Configure Listener

2 Configure Backend Server Group

3 Finish

\* Name

listener-vivi

\* Frontend Protocol/Port

HTTP

8881

Value range: 1 to 65535

Select TCP or UDP for load balancing at Layer 4. Select HTTP or HTTPS for load balancing at Layer 7.

When HTTPS is selected, the backend protocol can only be HTTP.

# ELB Configuration - Adding a Backend Server Group

- A backend server group is a collection of cloud servers that have the same features and receive the requests routed by the load balancer.

The screenshot displays the AWS Management Console interface for configuring a Backend Server Group. The 'Backend Server Groups' tab is selected. A red box highlights the 'Add Backend Server Group' button. The configuration for the group 'server\_group-vivi' is shown, including its name, listener, algorithm, and a table of two healthy backend servers.

Basic Information

Name: server\_group-vivi

Listener: listener-vivi

Load Balancing Algorithm: Weighted round robin

Sticky Session: Disabled

ID: 9f0eeff9-8c22-417a-8762-655876f67d81

Backend Protocol: HTTP

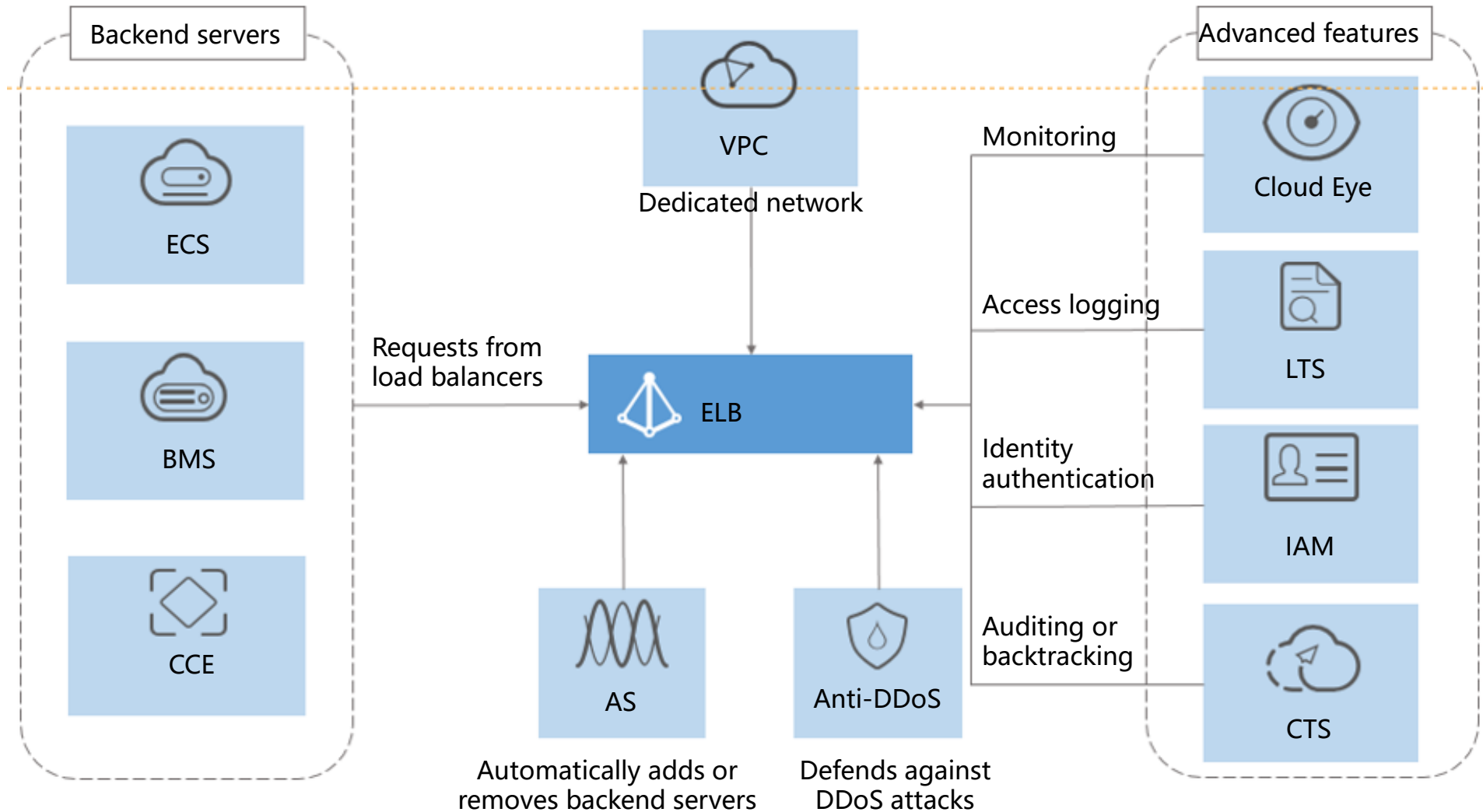
Health Check: Enabled | Configure

Description: --

Available servers: 2

Name	Status	Private IP Address	Health Check Result	Weight	Backend Port
ecs-S01	Running	192.168.0.87	Healthy	1	8889
ecs-S02	Running	192.168.1.109	Healthy	1	8889

# ELB and Related Services



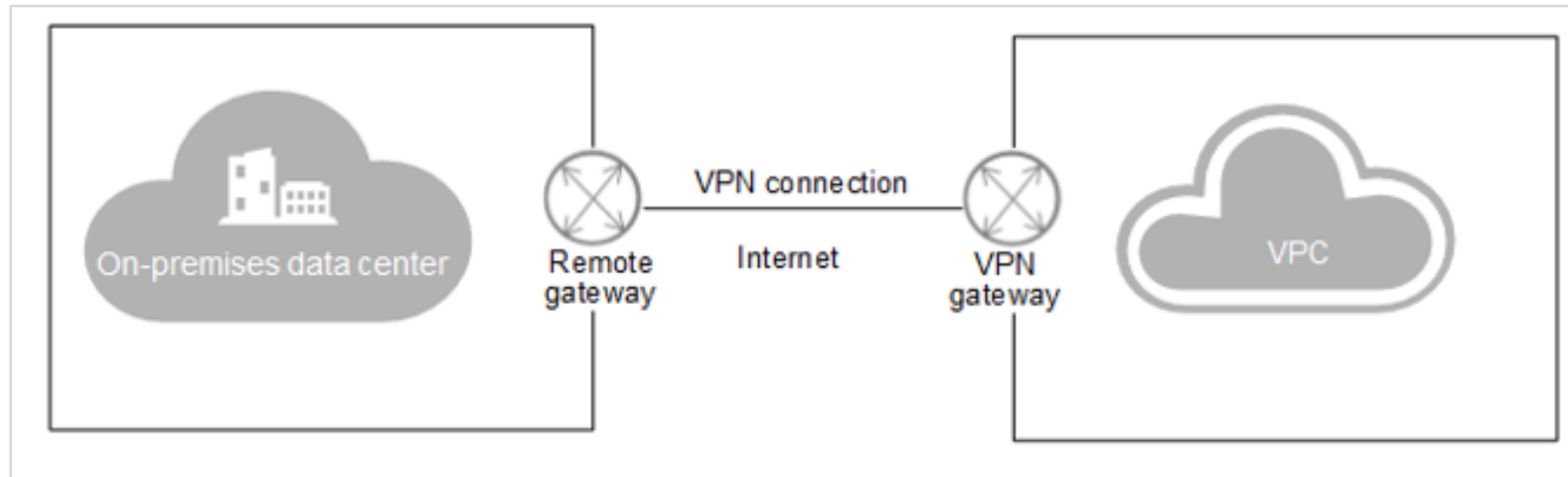
# Contents

1. Virtual Private Cloud (VPC)
2. Elastic Load Balance (ELB)
- 3. Virtual Private Network (VPN)**
4. NAT Gateway
5. Other Services



# Virtual Private Network

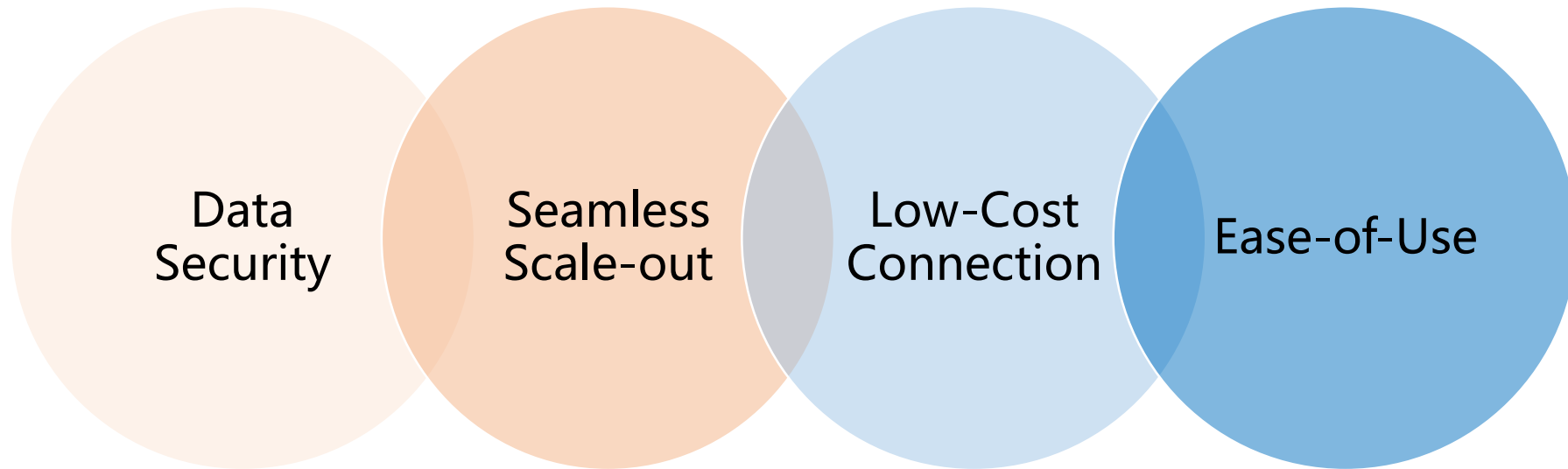
- Virtual Private Network (VPN) allows you to establish an encrypted, Internet-based communications tunnel between your on-premises data center and a VPC, so you can access resources in the VPC remotely.



# VPN Advantages

- Network communications enabled between your on-premises data center and a VPC realized
- Workloads from your on-premises data center quickly migrated to the cloud, forming a hybrid cloud

- Simple configuration on the VPN device in your on-premises data center

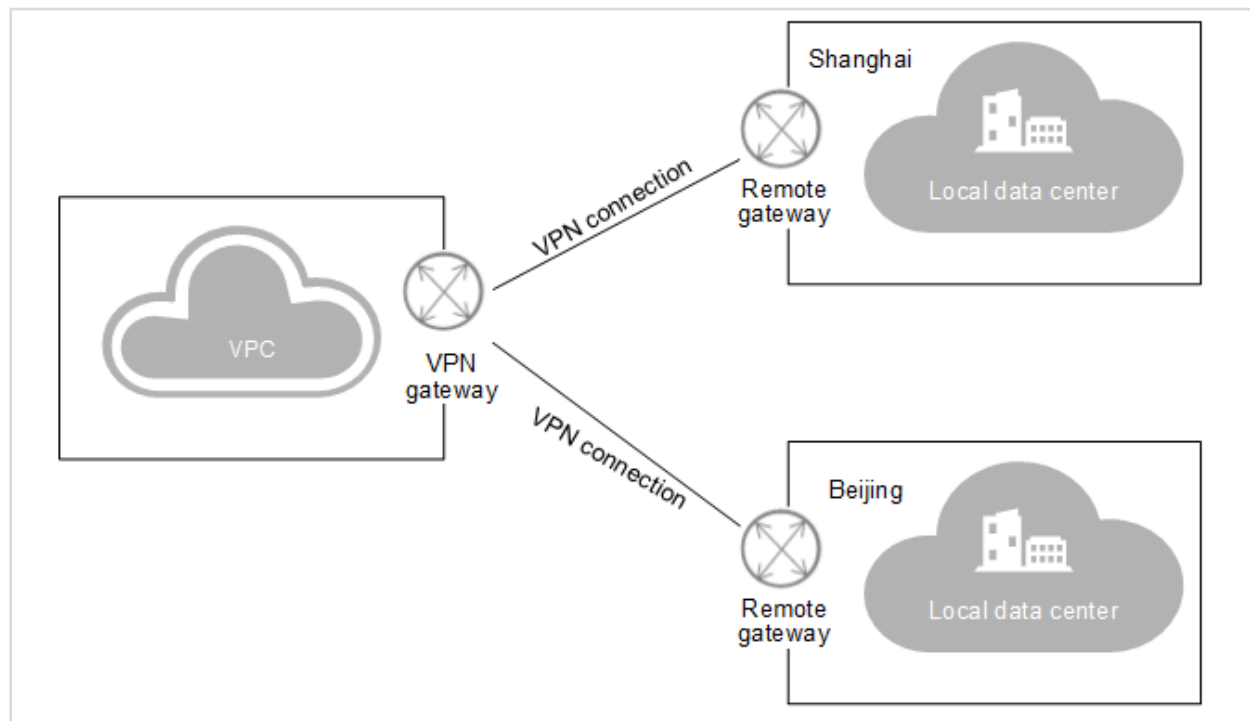


- IKE and IPsec encryption
- A stable VPN connection

- Encrypted IPsec connections over the Internet

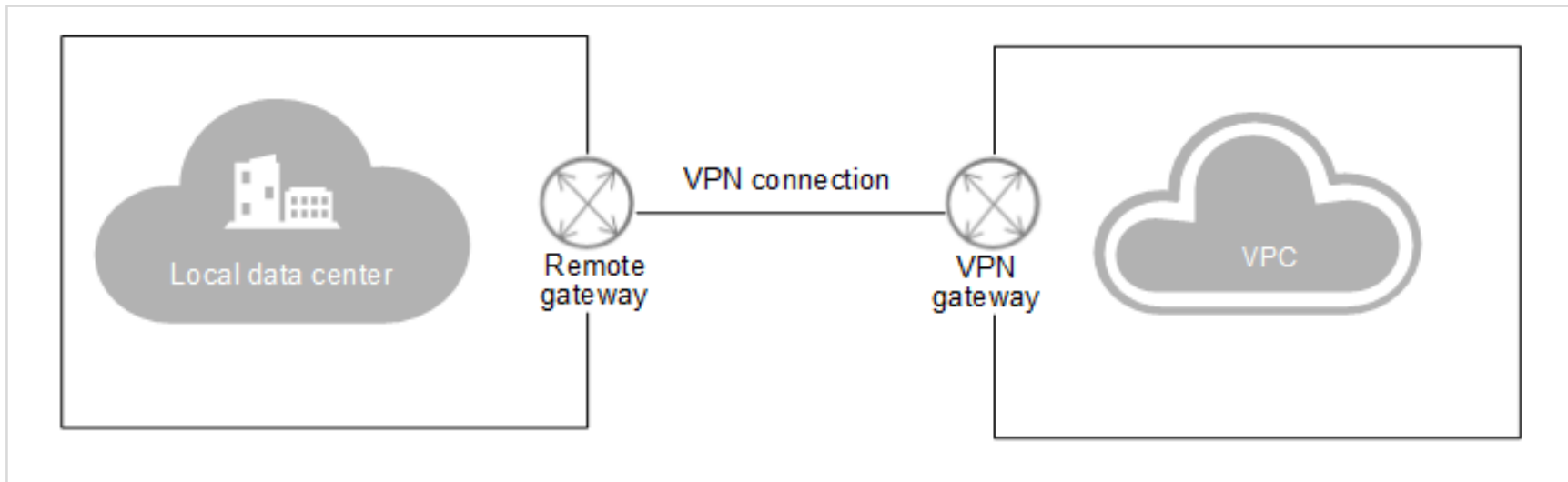
# VPN Networking

- 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 your on-premises data center.
- A VPN connection is an encrypted connection that links the VPN gateway to the remote gateway to enable communications between a VPC and your on-premises data center, quickly establishing a secure hybrid cloud.



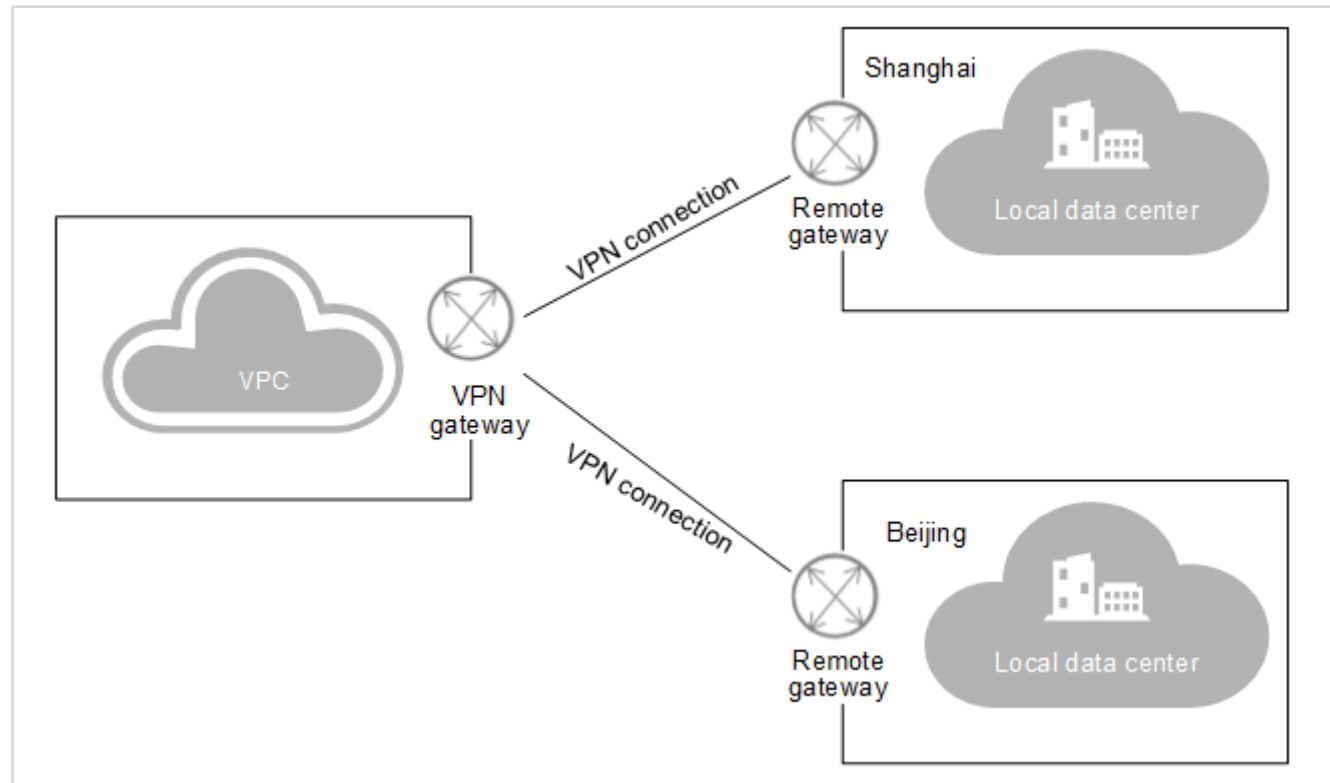
# Site-to-Site VPN Connection

- You can set up a VPN to connect your on-premises data center to a VPC, effectively creating a hybrid cloud.



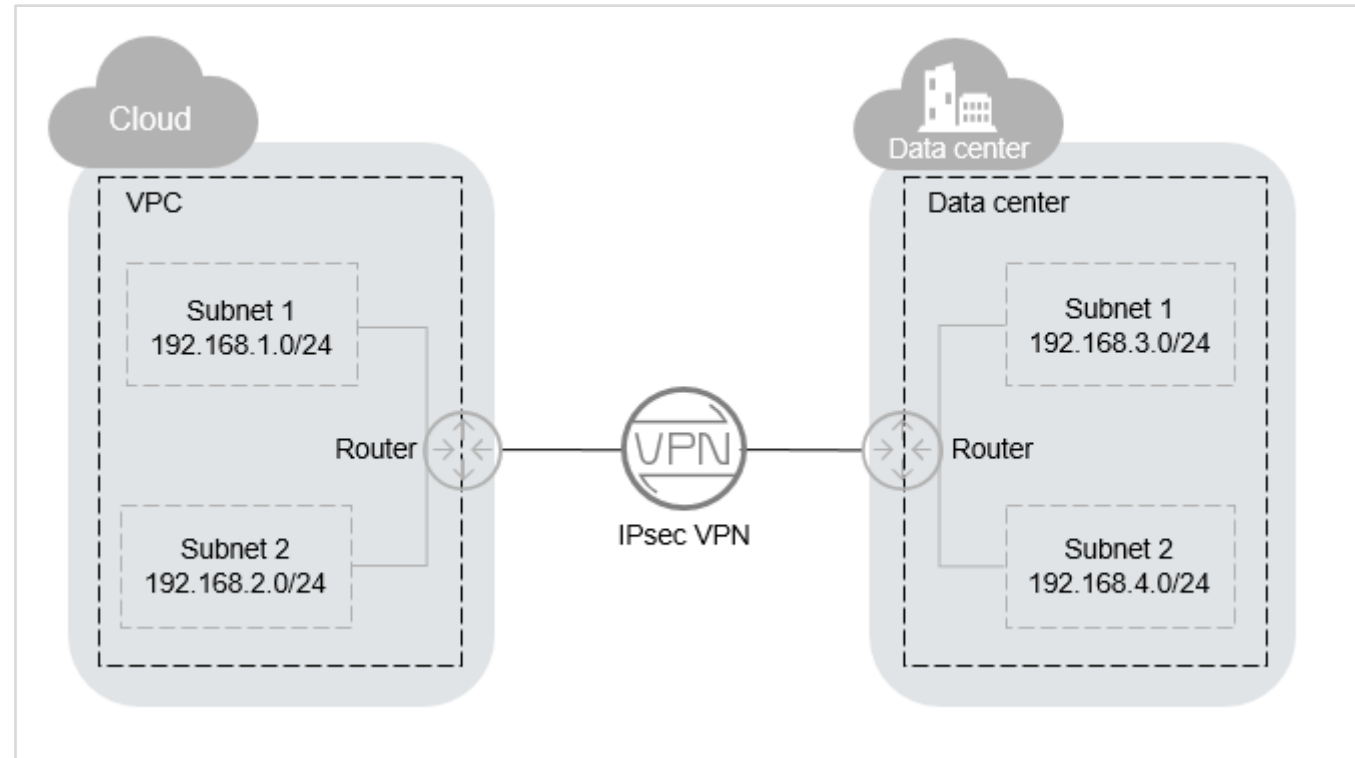
# Hub-and-Spoke VPN Connection

- You can also set up a VPN to connect multiple on-premises data centers to a VPC, also creating a hybrid cloud.



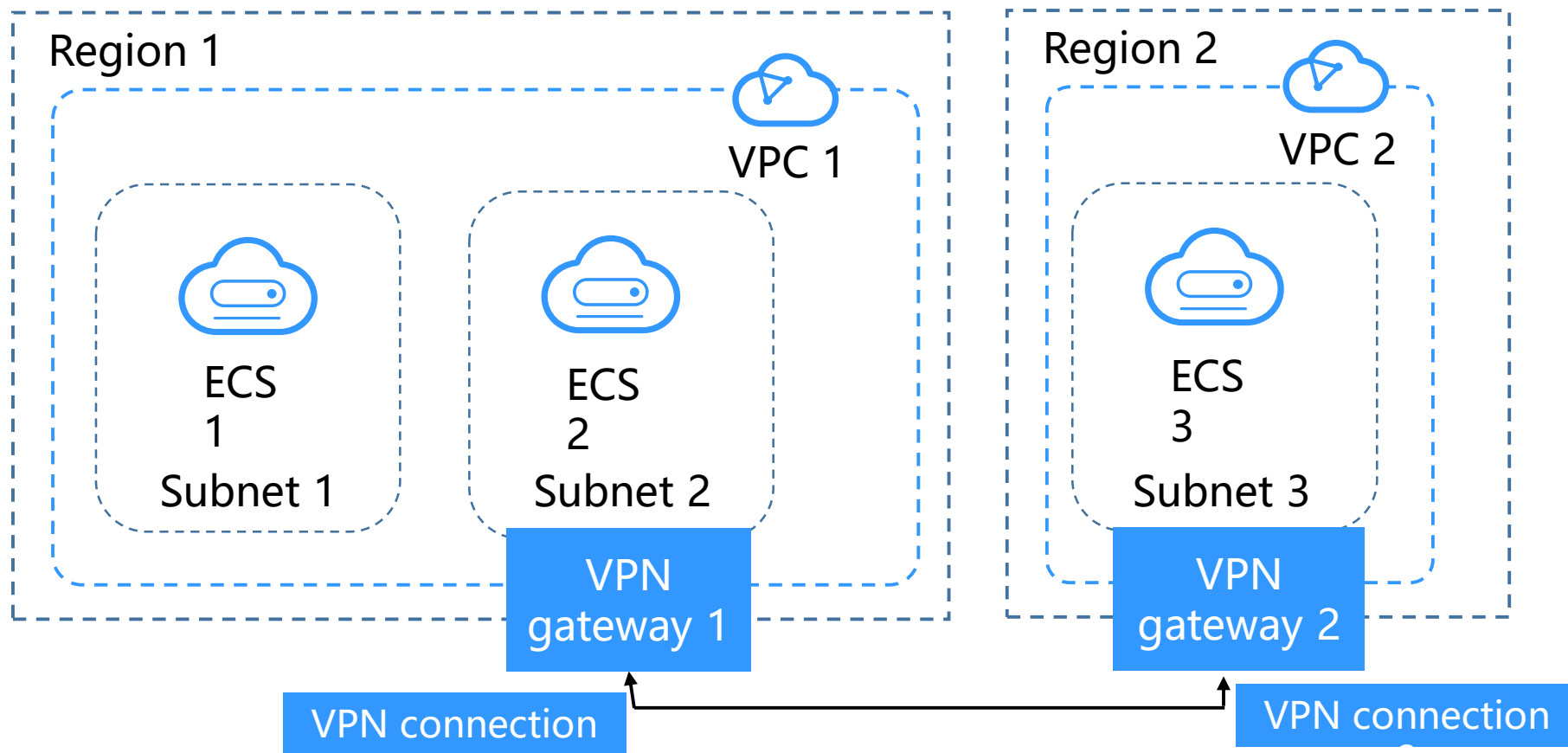
# VPN Concepts - IPsec VPN

- Internet Protocol Security (IPsec) VPN uses a secure network protocol suite that authenticates and encrypts data packets to provide secure encrypted communications between different networks. The VPN service uses an IPsec VPN.



# VPN Configuration Process

- You can create a VPN gateway and a VPN connection on the management console.



# VPN Configuration: VPN Gateway

- To allow your ECSs in a VPC to access your on-premises network, you must first create a VPN gateway.

The screenshot shows the configuration page for a VPN Gateway in the Huawei Cloud console. The interface includes several labeled fields and options:

- Name:** A text input field containing "Huawei-Vivi".
- VPC:** A dropdown menu showing "vpc-default". To its right is a circular refresh icon and a "Create VPC" link.
- Type:** A button labeled "IPsec".
- Billed By:** Two buttons, "Bandwidth" (which is highlighted in dark blue) and "Traffic" (which is light blue).
- Bandwidth (Mbit/s):** A row of buttons representing different bandwidth options: 5, 10, 20, 50, 100, 200, and 300. The "5" button is highlighted in dark blue.



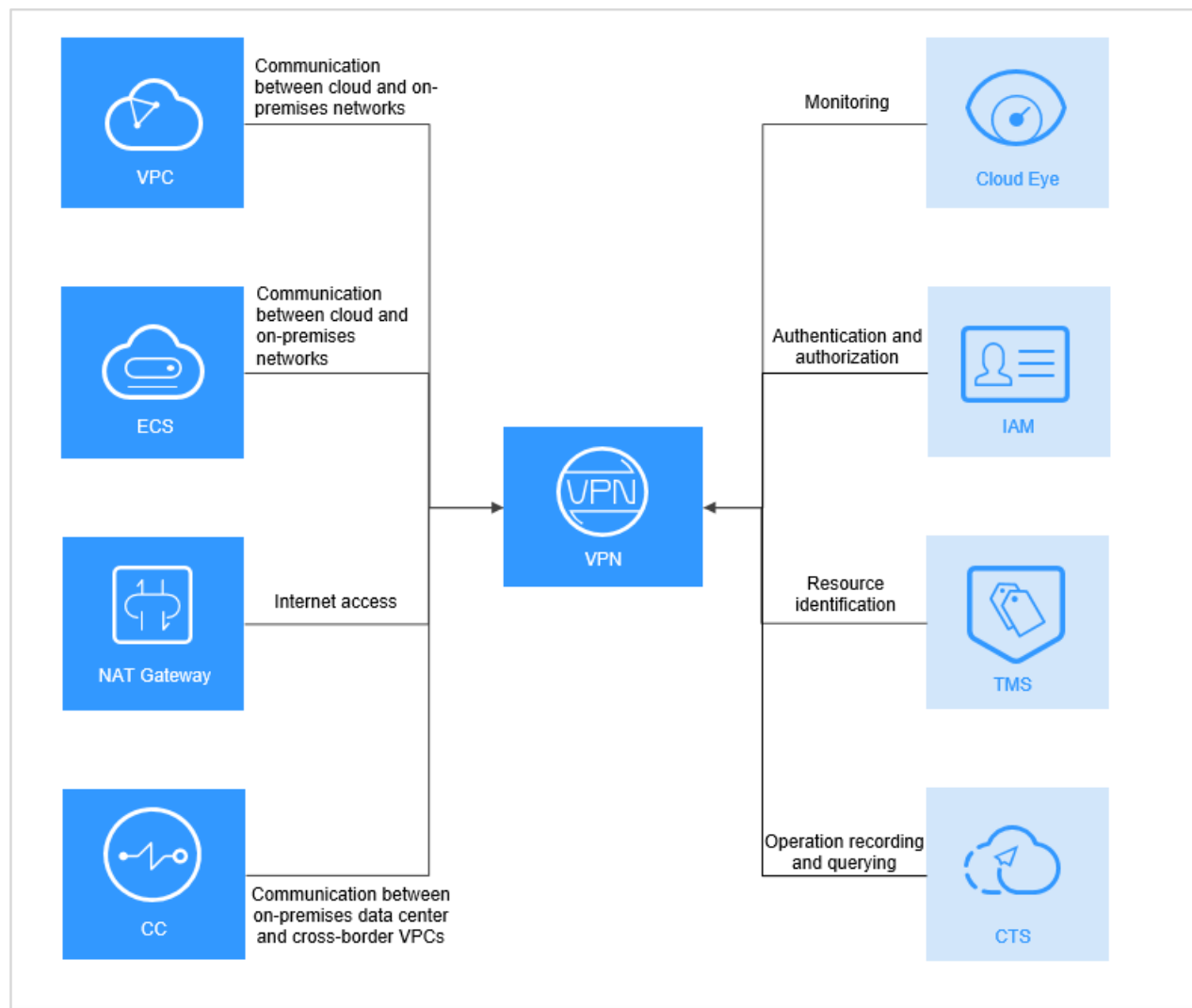
# VPN Configuration: VPN Connection

- To connect your ECSs in a VPC to your private network, after the VPN gateway is obtained, you also have to create a VPN connection.

The screenshot shows the 'VPN Connection' configuration page in the Huawei Cloud console. The form is as follows:

- Name:** vpn-43fd
- VPN Gateway:** A dropdown menu with the text 'Select a VPN gateway to proceed.' and a 'C' icon. Below it, a message states: 'No VPN gateways available. Create a VPN gateway. Buy VPN Gateway'.
- Local Subnet:** A dropdown menu with the text 'Select a VPN gateway to proceed.' and a 'C' icon. Below it, a message states: 'No VPN gateways available. Create a VPN gateway. Buy VPN Gateway'.
- Remote Gateway:** A text input field with a placeholder '.\*.\*.\*.\*'.
- Remote Subnet:** A text input field with a placeholder 'Use commas (,) to separate multiple CIDR blocks, for example, 192.168.52.0/24,192.168.54.0/24'. Below it, a message states: 'Using 100.64.0.0/10 as the customer subnet may cause services such as OBS, DNS, API Gateway to become unavailable.'
- PSK:** A text input field with a placeholder 'Enter a pre-shared key.'
- Confirm PSK:** A text input field with a placeholder 'Enter the pre-shared key again.'

# VPN and Related Services

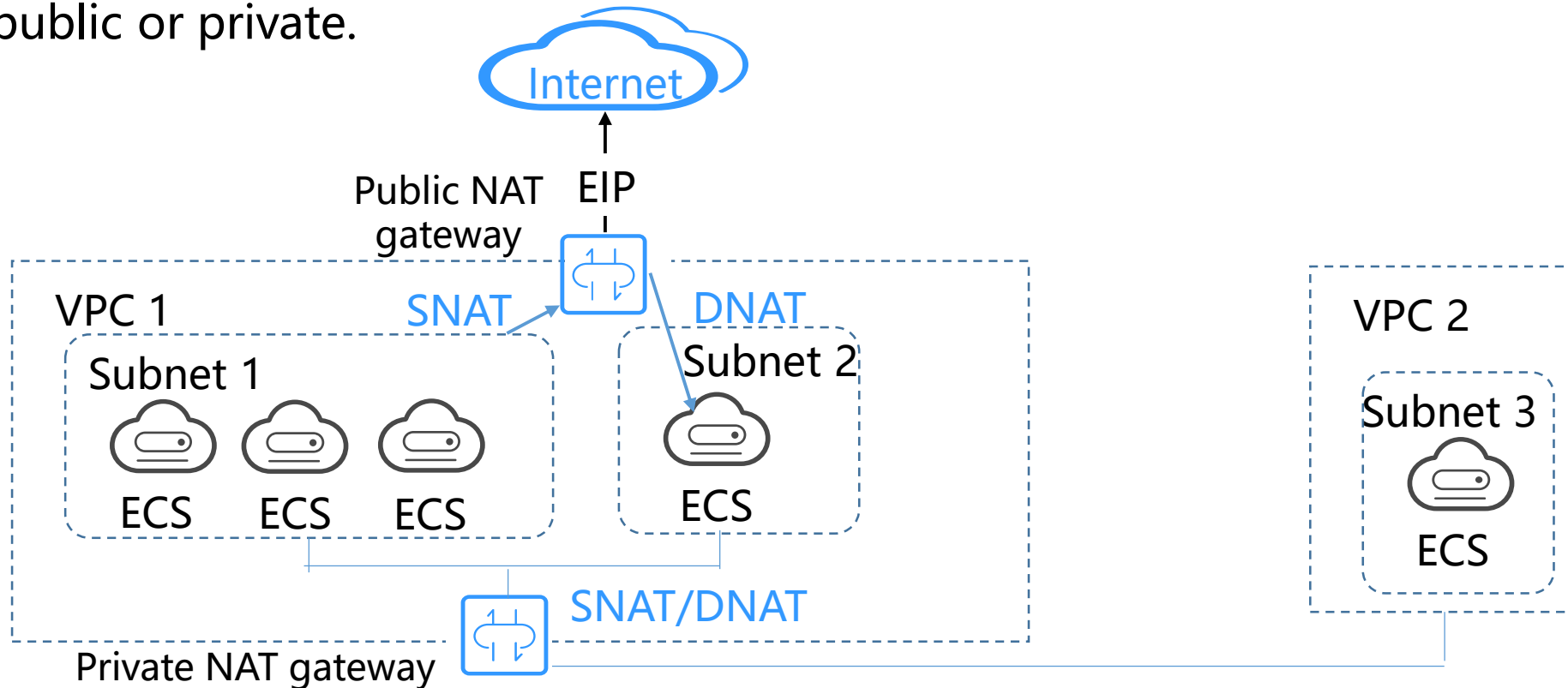


# Contents

1. Virtual Private Cloud (VPC)
2. Elastic Load Balance (ELB)
3. Virtual Private Network (VPN)
- 4. NAT Gateway**
5. Other Services

# NAT Gateway

- The NAT Gateway service provides network address translation (NAT) service for servers in a VPC and enables servers to share an EIP to access the Internet. NAT gateways can be either public or private.



# NAT Gateway Advantages

- Cross-AZ deployment
- The type and EIP of a NAT gateway can be changed at any time.



The diagram consists of three triangles arranged horizontally. The left triangle is light blue and labeled 'Low Cost'. The middle triangle is inverted and bright blue, labeled 'Flexible Deployment'. The right triangle is bright blue and labeled 'Multiple Types'. Below each triangle is a bulleted list of specific advantages.

Flexible  
Deployment

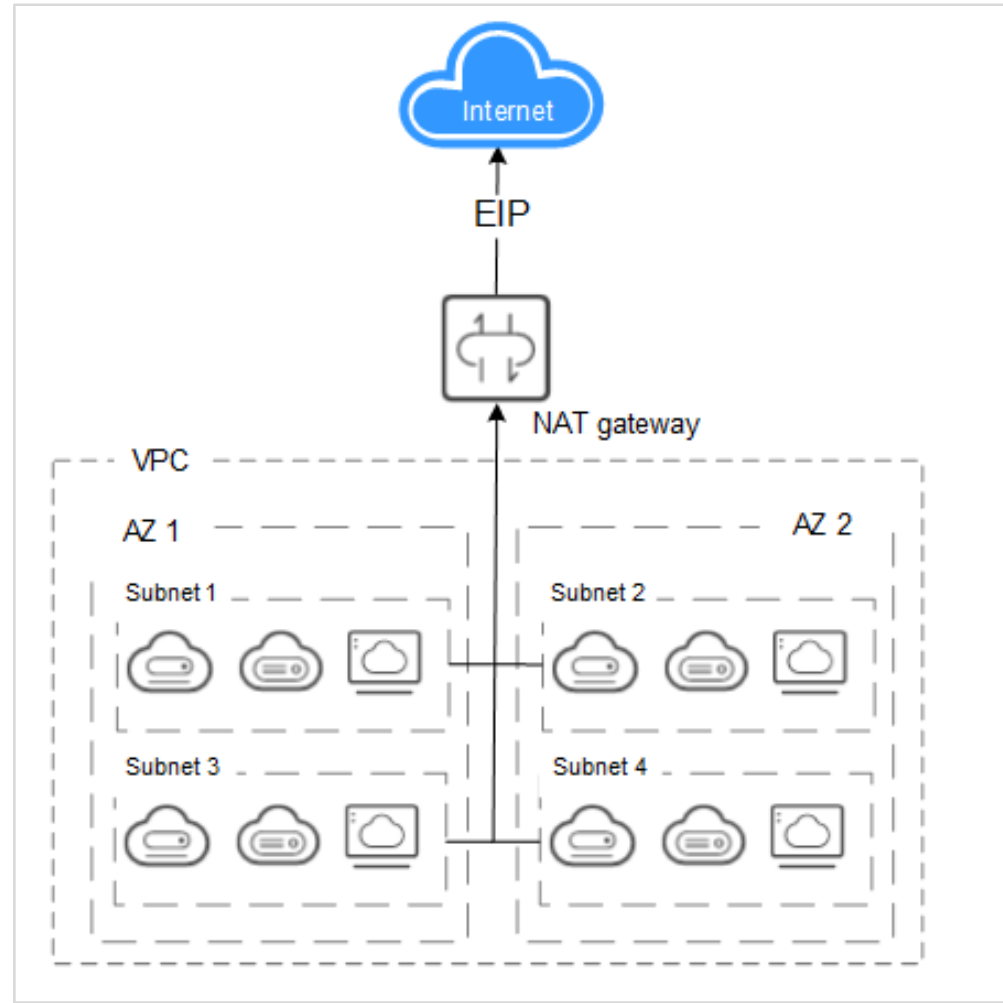
Low Cost

- Shared EIP

Multiple  
Types

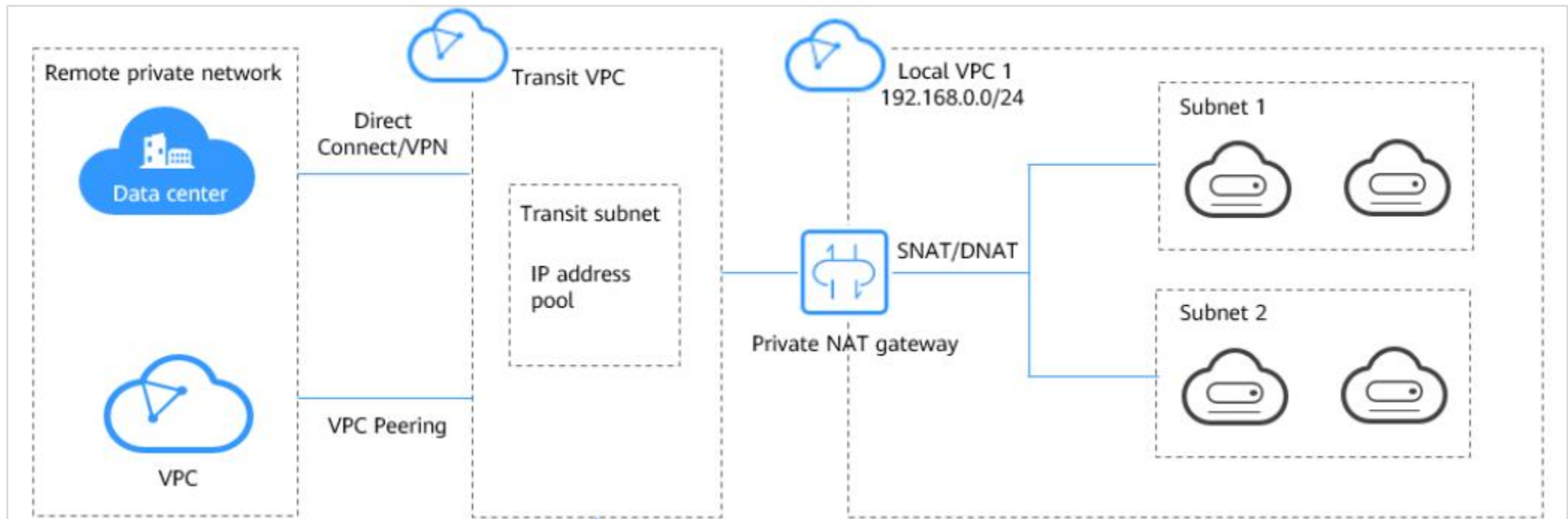
- Simple configuration
- Easy O&M and quick provisioning
- Stability and reliability

# NAT Gateway Architecture (Public NAT Gateway)



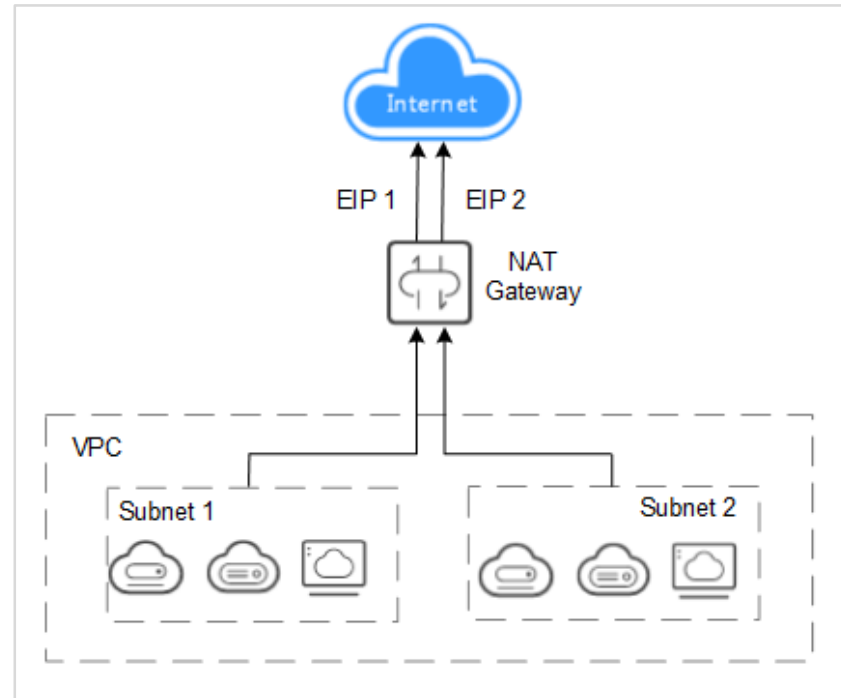
# NAT Gateway Architecture (Private NAT Gateway)

- A private NAT gateway provides NAT service for servers in a VPC, so that multiple servers can share a private IP address to access or provide services accessible from an on-premises data center or other VPCs.



# Public NAT Gateway: Using SNAT

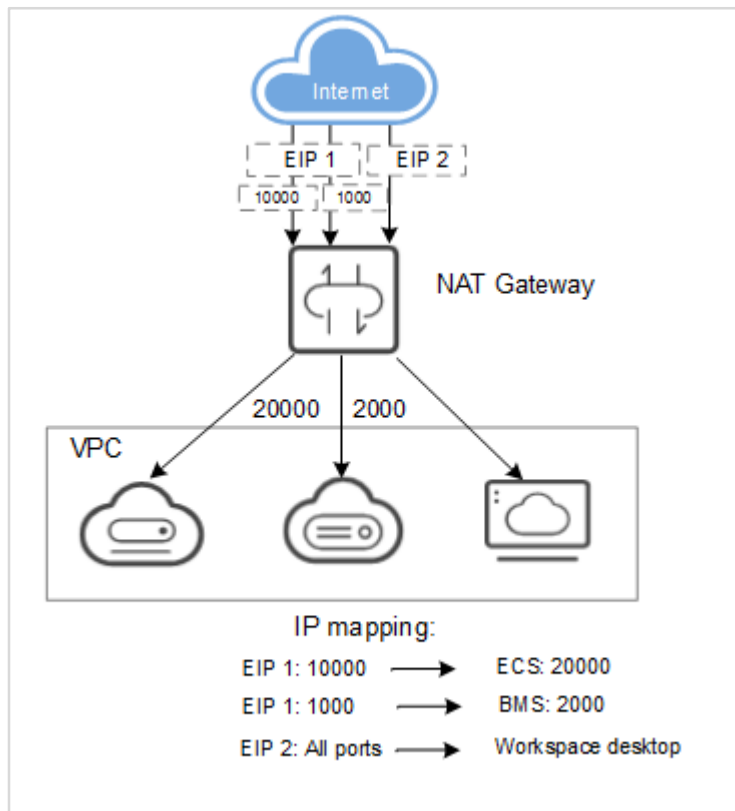
- If your servers in a VPC require Internet access, you can use SNAT to let the servers share one or more EIPs to access the Internet without exposing their IP addresses. NAT Gateway provides different types of NAT gateways for different numbers of connections. You can create multiple SNAT rules to meet different service requirements.





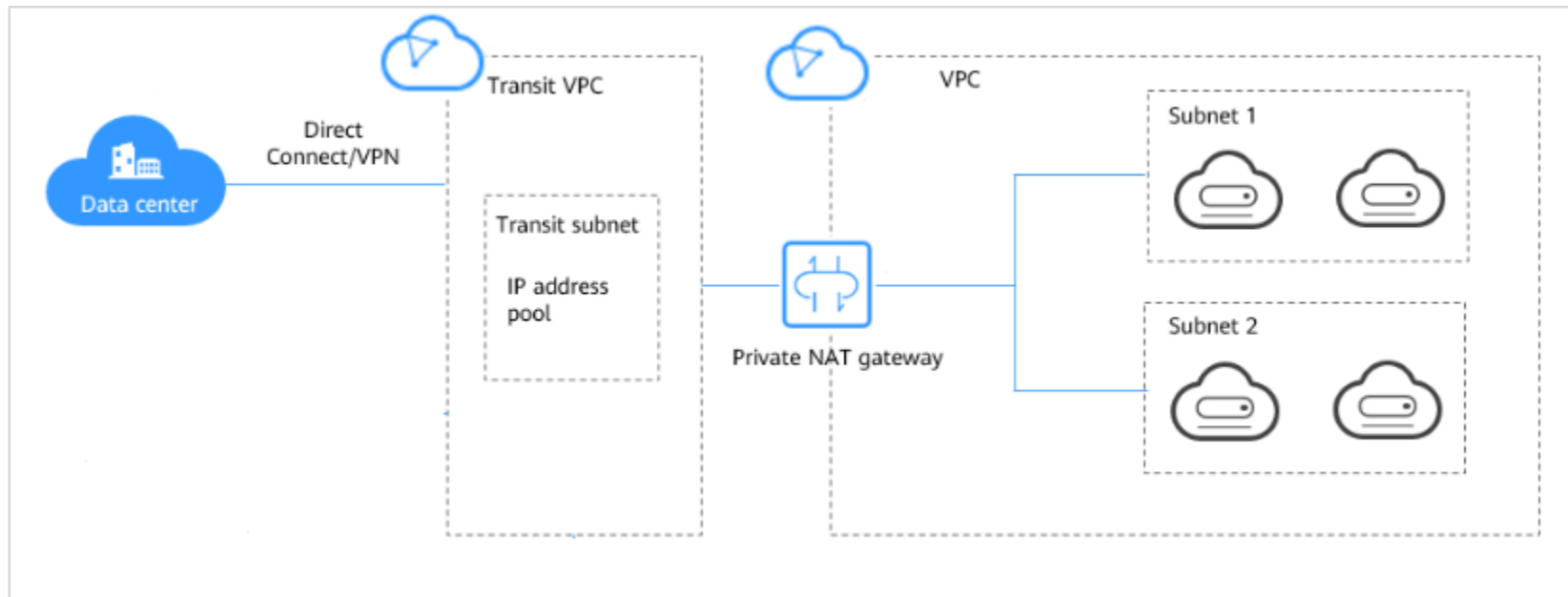
# Public NAT Gateway: Using DNAT

- DNAT lets servers in a VPC to provide services accessible from the Internet.



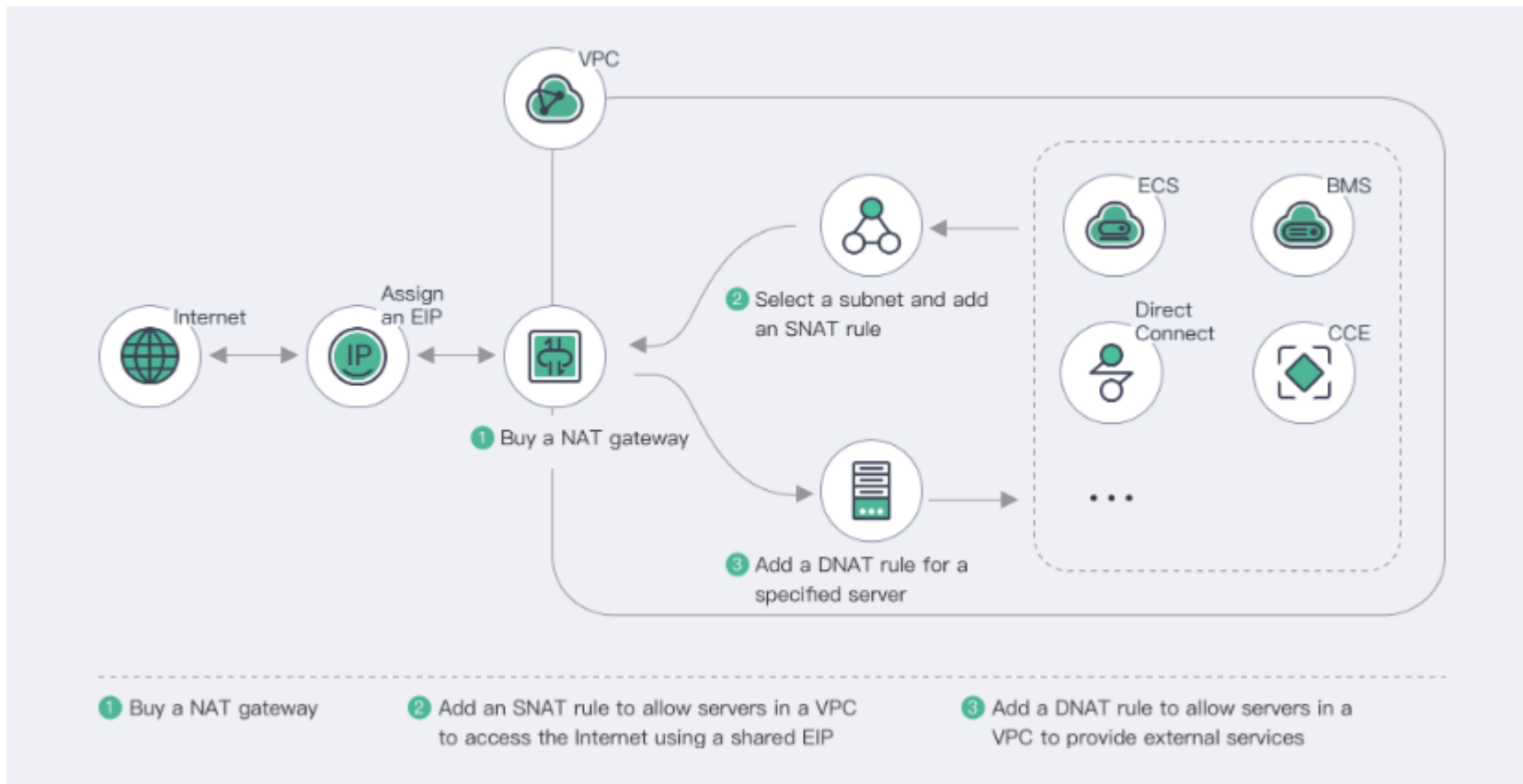
# Private NAT Gateway: Enterprise Network Management

- To ensure security compliance, an enterprise may require that all its branches and departments map their IP addresses to the same IP address for internal communications. To accomplish this, the enterprise can use a private NAT gateway to enable these communications without changing the original network after migrating workloads to the cloud.



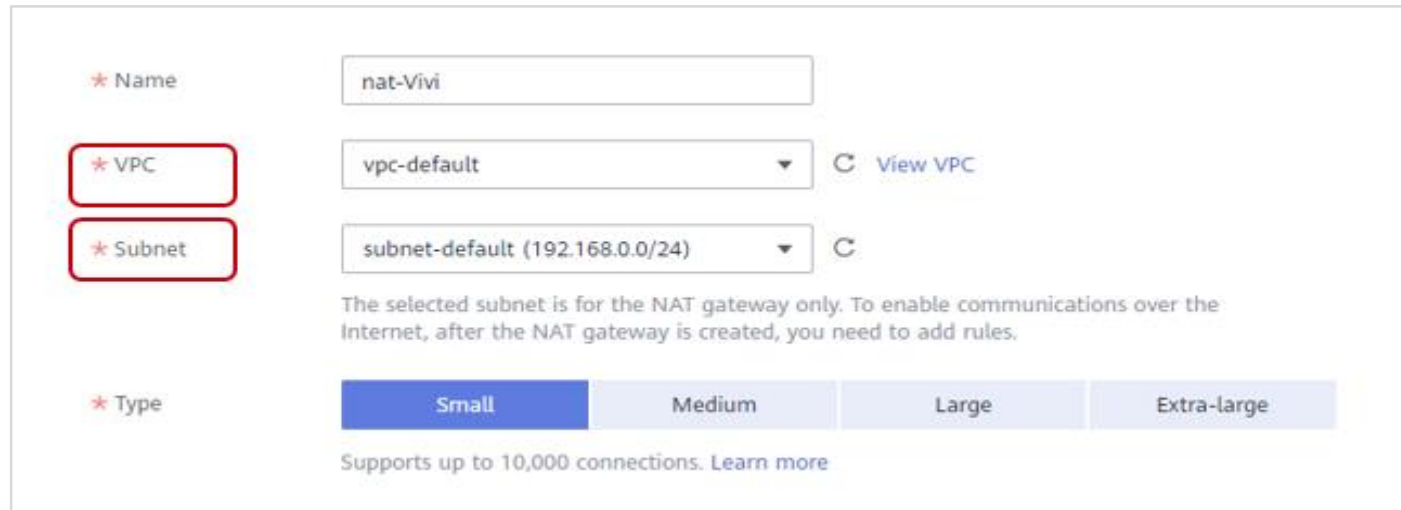
# Process for Buying a NAT Gateway

Public NAT gateway:



# Buying a NAT Gateway

- When you buy a public NAT gateway, you must specify its VPC, subnet, and type.
- Check whether the default route (0.0.0.0/0) of the VPC is in use by any other gateways. If yes, add another route for the gateway you purchased or add the default route to a new route table that you will associate with the gateway.



The screenshot shows a configuration form for purchasing a NAT Gateway. The form includes the following fields and options:

- Name:** A text input field containing "nat-Vivi".
- VPC:** A dropdown menu showing "vpc-default". To the right of the dropdown is a link labeled "View VPC".
- Subnet:** A dropdown menu showing "subnet-default (192.168.0.0/24)". To the right of the dropdown is a link labeled "View Subnet".
- Type:** A set of four buttons: "Small" (selected), "Medium", "Large", and "Extra-large".

Below the "Subnet" dropdown, there is a note: "The selected subnet is for the NAT gateway only. To enable communications over the Internet, after the NAT gateway is created, you need to add rules." At the bottom of the form, it says "Supports up to 10,000 connections. [Learn more](#)".

# SNAT Rule Configuration

- If your servers are in a VPC and need to access the Internet, select VPC.
- If your on-premises servers access a VPC over a Direct Connect or VPN connection need to access the Internet, select Direct Connect/Cloud Connect.

NAT Gateway Name nat-Vivi

\* Scenario ☒ VPC ☐ Direct Connect/Cloud Connect

\* EIP

You can select 19 more EIPs. [View EIP](#)

<input checked="" type="checkbox"/> EIP	EIP Type	Bandwidth Name	Bandwidth (Mbi...	Billing Mode
<input checked="" type="checkbox"/> 159.138.121.173	Dynamic BGP	bandwidth-Vivi	5	Pay-per-use

Selected EIPs (1): 159.138.121.173. The EIP used for the SNAT rule will be randomly chosen from the ones selected here.

# DNAT Rule Configuration

- VPC: A DNAT rule allows servers in a VPC to share an EIP and provide services accessible from the Internet.
- Direct Connect/Cloud Connect: A DNAT rule allows servers in an on-premises data center connected to a VPC through Direct Connect or Cloud Connect to provide services accessible from the Internet.

NAT Gateway Name nat-Vivi

★ Scenario **VPC** Direct Connect/Cloud Connect

★ Port Type **Specific port** All ports

★ Protocol TCP

★ EIP 159.138.121.173 (5 Mbit/s | Pay-per-use) View EIP

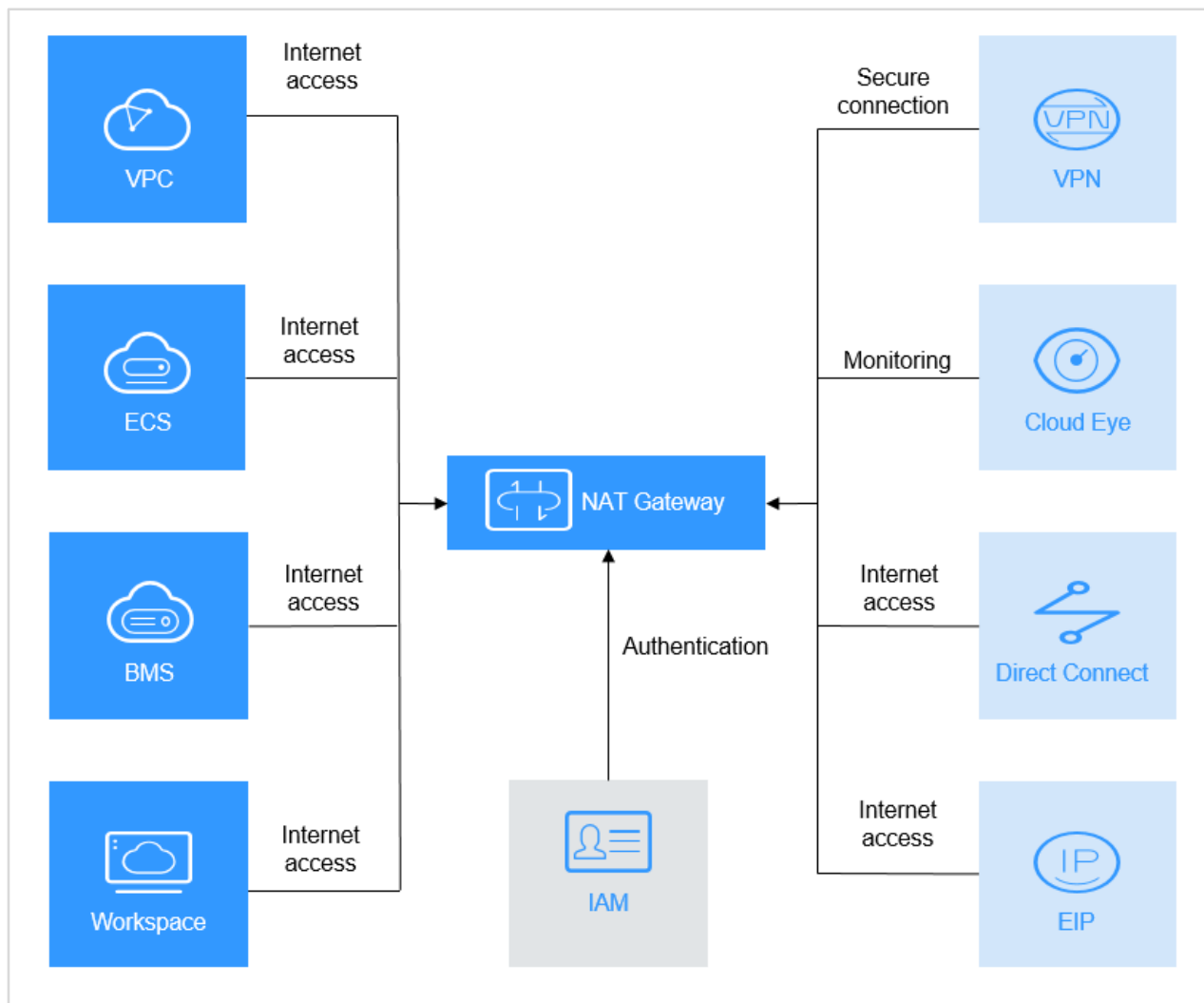
Bandwidth: 5 Mbit/s Billing Mode: Pay-per-use

★ Outside Port 22

★ Private IP Address 192 . 168 . 10 . 1 View ECS IP Address

★ Inside Port 22

# NAT Gateway and Related Services



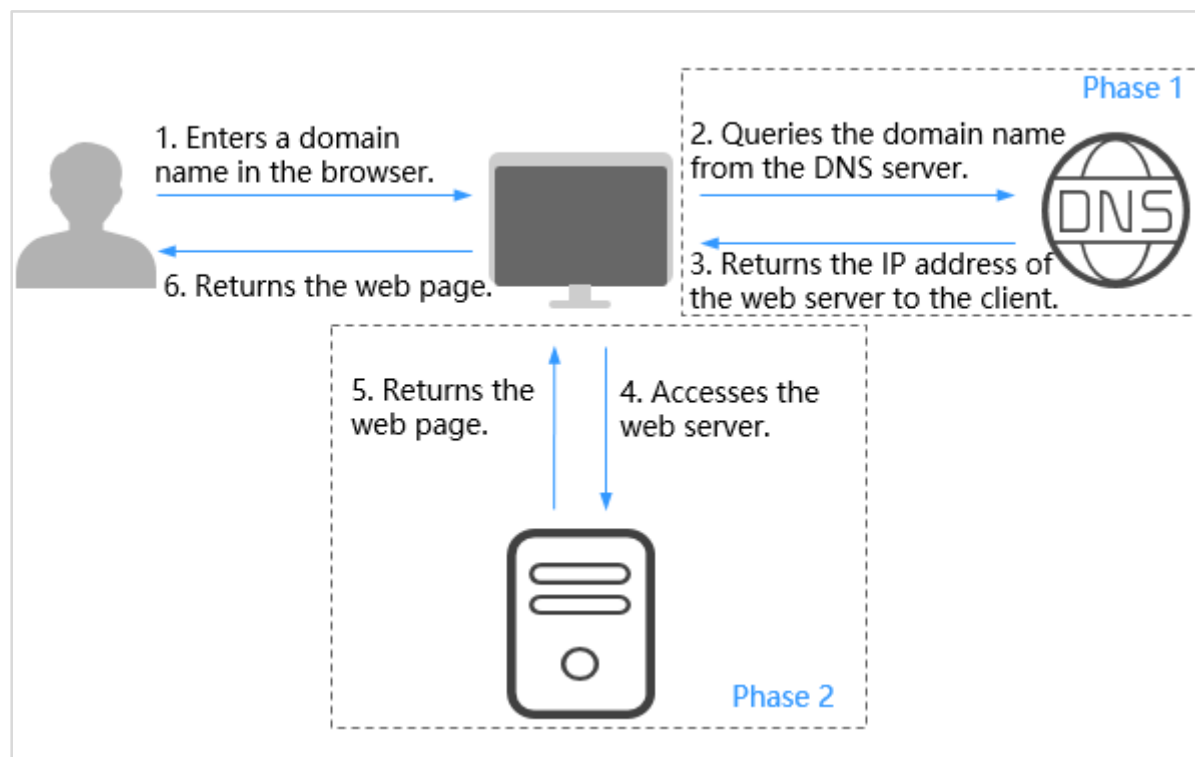
# Contents

1. Virtual Private Cloud (VPC)
2. Elastic Load Balance (ELB)
3. Virtual Private Network (VPN)
4. NAT Gateway
- 5. Other Services**

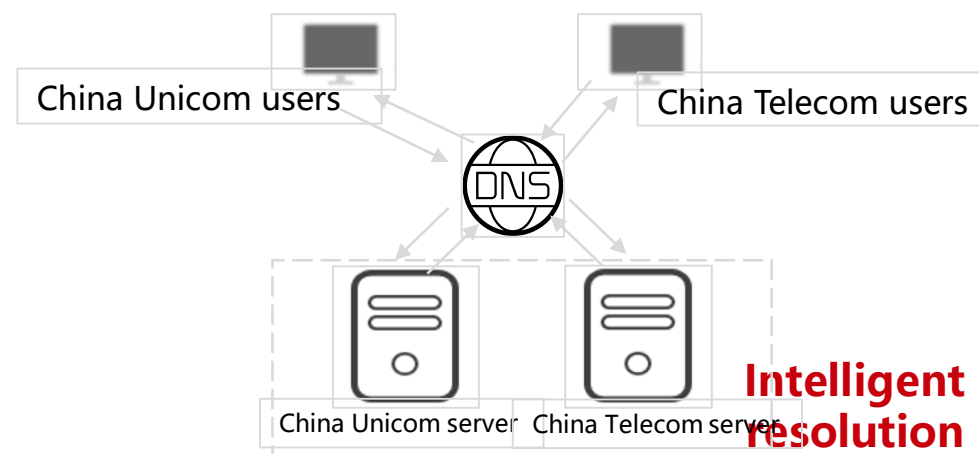
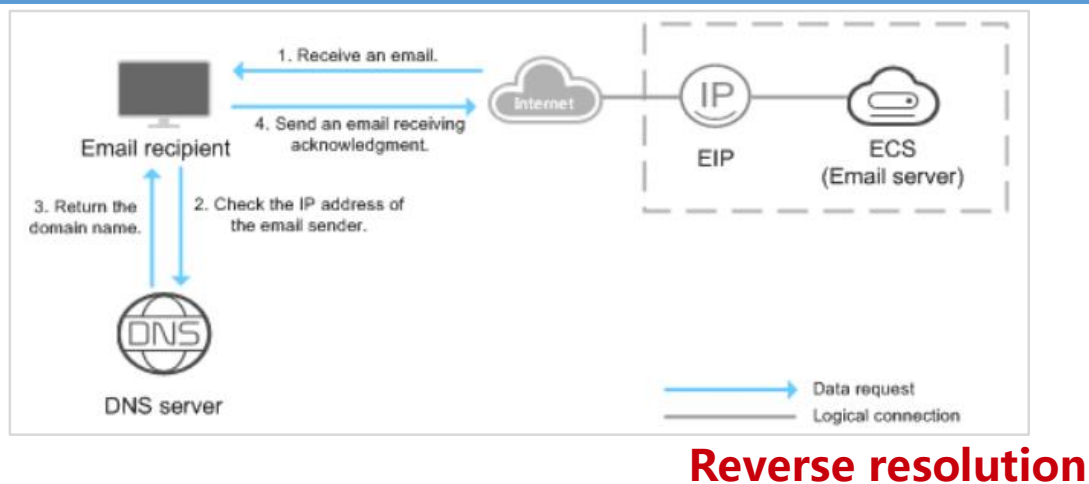
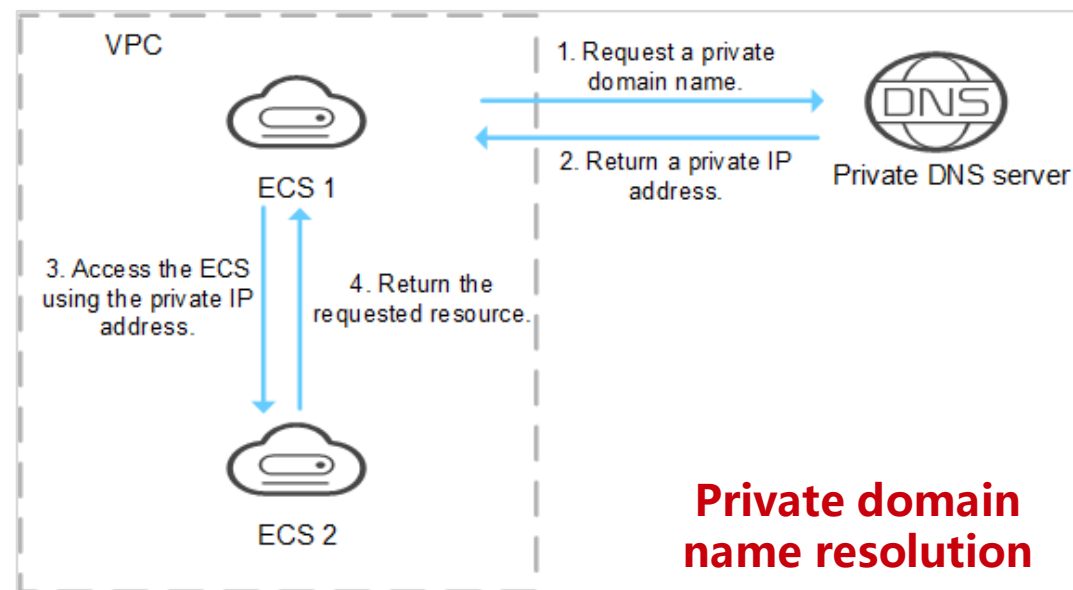
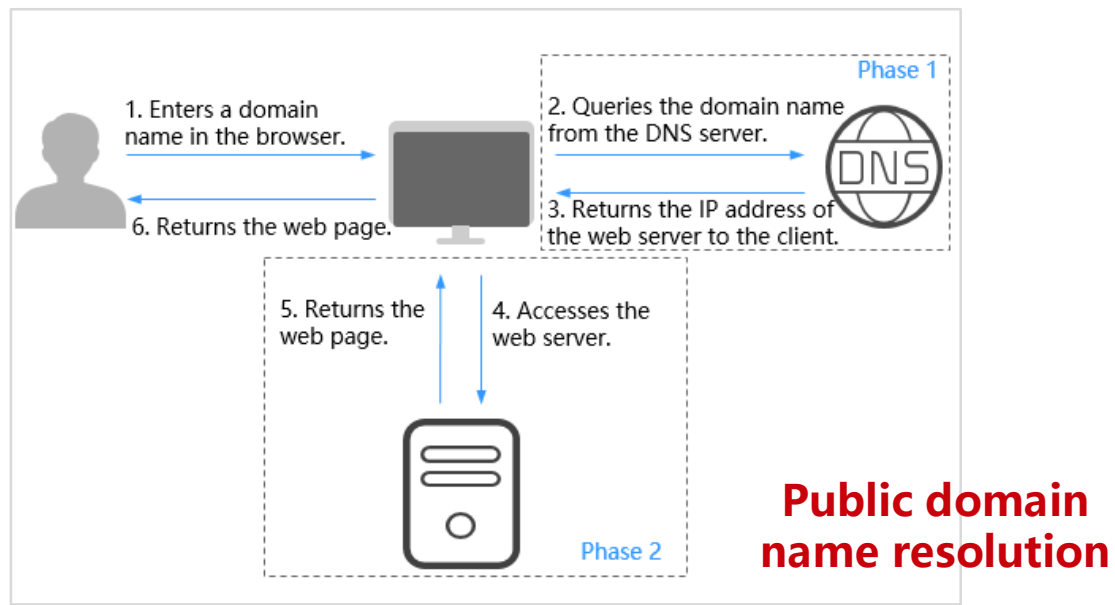


# What Is DNS?

- Domain Name Service (DNS) provides highly available and scalable authoritative DNS services that translate domain names into IP addresses required for network connection, reliably directing end users to your applications.



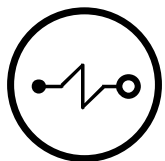
# DNS Resolution Services



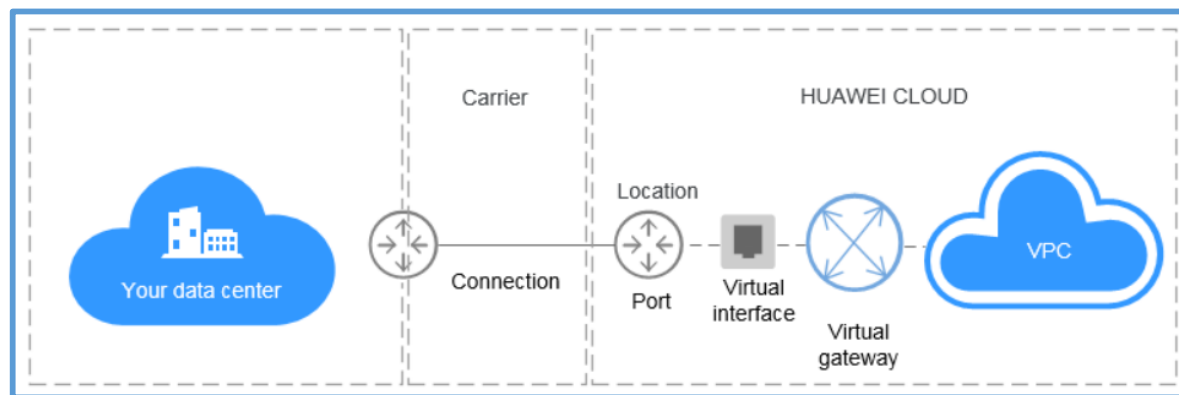
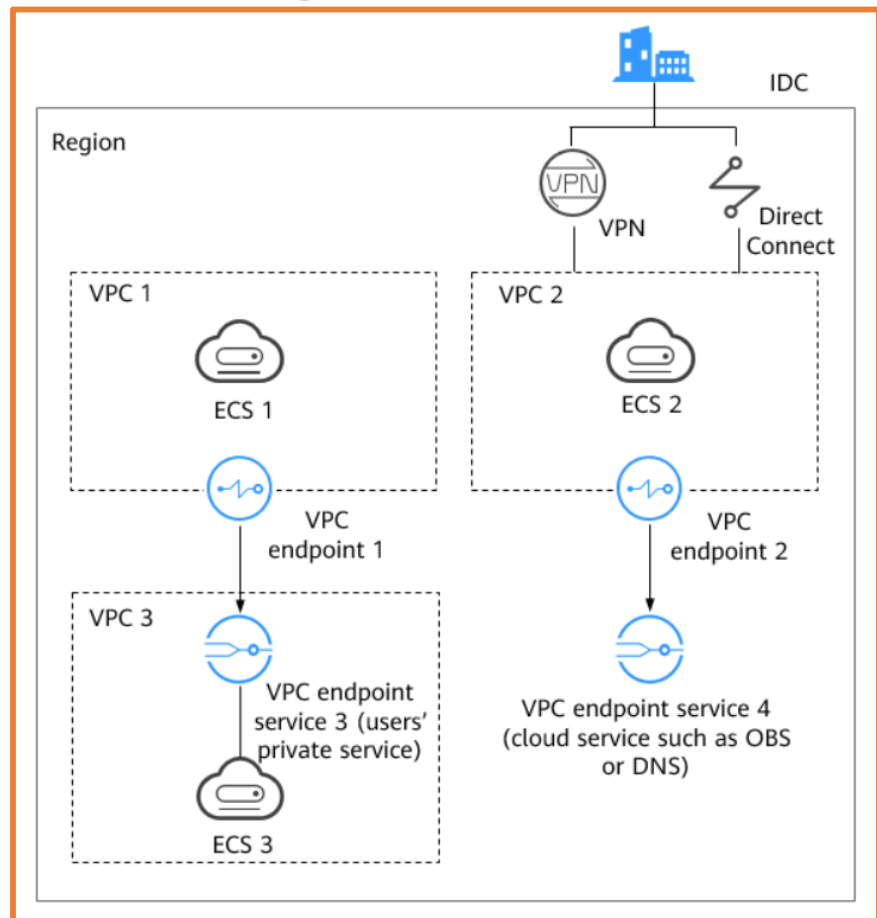
# Domain Name Format and DNS Hierarchy

- **A valid domain name meets the following requirements:**
  - A domain name is segmented using periods (.) into multiple labels.
  - A label can contain supported language-specific characters, letters, digits, and hyphens (-) and cannot start or end with a hyphen.
  - A label cannot exceed 63 characters.
  - The total length of a domain name, including the period at the end, cannot exceed 254 characters.
- **A domain name is divided into the following levels based on its structure:**
  - Root domain: . (a dot)
  - Top-level domain: for example, **.com**, **.net**, **.org**, and **.cn**
  - Second-level domain: subdomain names of the top-level domain names, such as **example.com**, **example.net**, and **example.org**
  - Third-level domain: subdomain names of the second-level domain names, such as **abc.example.com**, **abc.example.net**, and **abc.example.org**

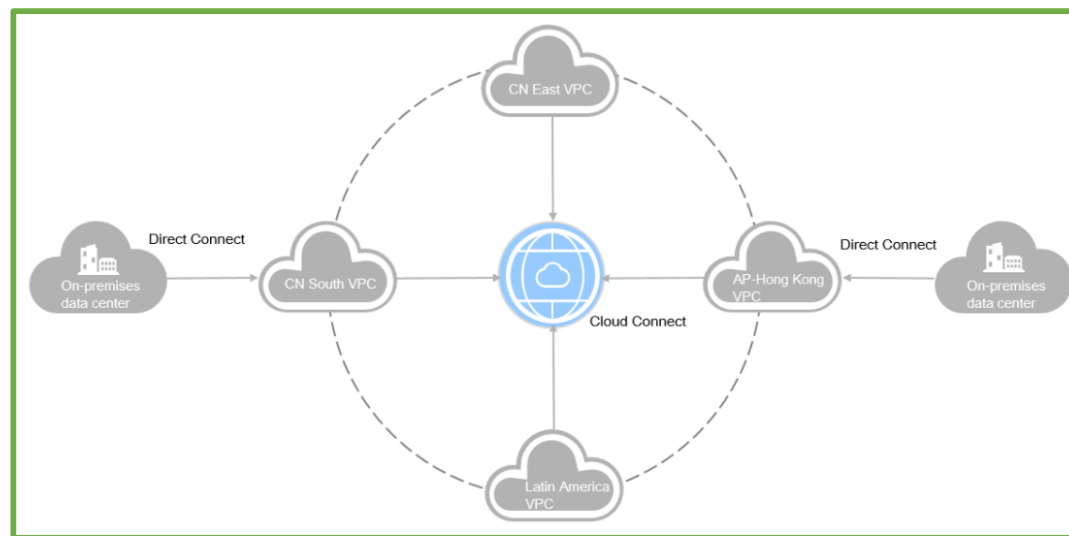
# Other Network Services



VPCEP



Direct Connect



Cloud Connect

# Quiz

---

1. (Single choice) Which of the following is not a component of ELB?
  - A. Backend server group
  - B. Listener
  - C. Load balancer
  - D. NAT Gateway
2. (Single choice) Can resources in a subnet of one VPC communicate with those in a subnet of another VPC in the same region?
  - A. Yes
  - B. No
  - C. Yes, they can communicate with each other by default
  - D. Yes, but VPN is required

# Summary

- This chapter described basic network knowledge and common network cloud services. After completing this course, you will be able to understand the functions of networks as well as how network cloud services work and where you can use these services. For example, a VPC is like the internal network used by an enterprise, and applications can provide Internet-accessible services using EIPs. Mastering these concepts can help you better prepare for cloud migration of legacy systems.

# Recommendations

- Huawei Learning
  - <https://e.huawei.com/en/talent/#/>
- HUAWEI CLOUD technical support
  - <https://support.huaweicloud.com/intl/en-us/help-novice.html>
- HUAWEI CLOUD Academy
  - <https://edu.huaweicloud.com/intl/en-us/>

# Acronyms and Abbreviations

- ACL: access control list
- AS: autonomous system
- BGP: Border Gateway Protocol
- CC: Cloud Connect
- DHCP: Dynamic Host Configuration Protocol
- DNAT: destination network address translation
- DNS: Domain Name System/Domain Name Service
- ECS: Elastic Cloud Server



# Acronyms and Abbreviations

- EIP: Elastic IP
- ELB: Elastic Load Balance
- HTTP: Hypertext Transfer Protocol
- HTTPS: Hypertext Transfer Protocol Secure
- ICT: information and communications technology
- IDC: Internet data center
- IPsec: IP security
- NAT: network address translation

# Acronyms and Abbreviations

- SNAT: source network address translation
- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol
- VPC: Virtual Private Cloud
- VPCEP: VPC Endpoint
- VPN: Virtual Private Network
- Web: World Wide Web (WWW)

# Thank you.

把数字世界带入每个人、每个家庭、  
每个组织,构建万物互联的智能世界.

Bring digital to every person, home, and  
organization for a fully connected,  
intelligent world.

**Copyright©2021 Huawei Technologies Co., Ltd.  
All Rights Reserved.**

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

