Virtual Private Cloud

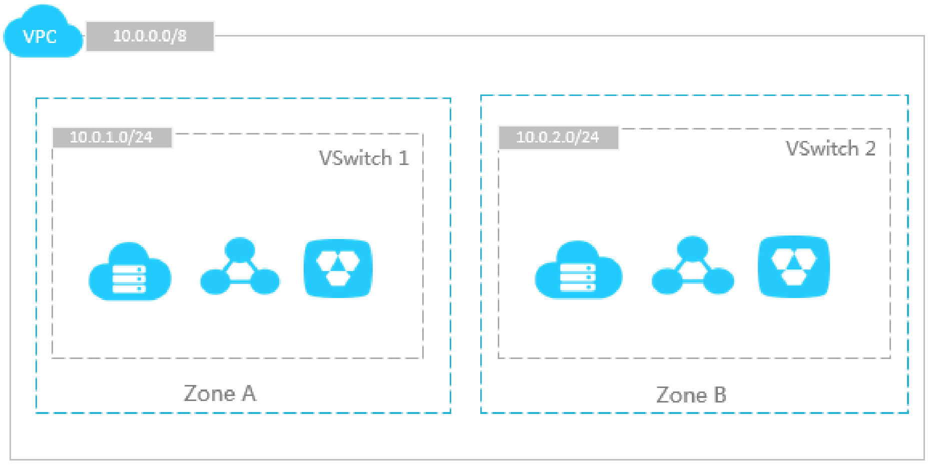
Product Introduction

MORE THAN JUST CLOUD | Alibaba Cloud

Product Introduction

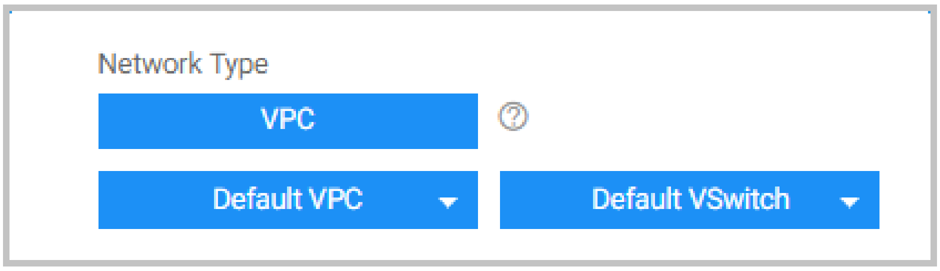
Virtual Private Cloud (VPC) is a private network established in Alibaba Cloud. VPCs are logically isolated from other virtual networks in Alibaba Cloud. VPCs allow you to launch and use Alibaba Cloud resources in your VPC.

You have full control over your Alibaba Cloud VPC. For example, you can select its IP address range, further segment your VPC into subnets, as well as configure route tables and network gateways. Additionally, you can connect VPCs with an on-premises network using a physical connection or VPN to form an on-demand customizable network environment. This allows you to smoothly migrate applications to Alibaba Cloud with little effort.



Default VPC and VSwitch

Alibaba Cloud provides a default VPC and VSwitch in the situation that you do not have any existing VPC and VSwitch to use when creating a cloud product instance. A default VPC and VSwitch will be created with the creation of an instance.



Default VPC and VSwitch feature list

Default VPC	Default VSwitch

The default VPC in each region is unique.	The default VSwitch in each Availability Zone is unique.
The netmask for a default VPC is /16, such as 172.31.0.0/16, providing up to 65536 private IP addresses.	The netmask for a default VSwitch is /20, such as 172.31.0.0/20, providing up to 4096 private IP addresses.
Default VPCs do not count in the allocated VPC quota.	Default VSwitches do not count in the allocated VSwitch quota.
Default VPCs are created by the system, all self-created VPCs are non-default VPCs.	Default VSwitches are created by the system, all self-created VSwitches are non-default VSwitches.
Operations and restrictions for default and non-default VPCs are the same.	Operations and restrictions for default and non-default VSwitches are the same.

Background information

With the continuous development of cloud computing, virtual network requirements are getting higher and higher, such as scalability, security, reliability, privacy, and higher requirements of connection performance. This gives a rise to a variety of network virtualization technologies.

The earlier solutions combined the virtual machine's network with the physical network to form a flat network architecture, such as the large layer-2 network. With the increase of virtual network scalability, problems are getting more serious for the earlier solutions. These problems include ARP spoofing, broadcast storms, host scanning, and more. Various network isolation technologies emerged to resolve these problems by completely isolating the physical networks from the virtual networks. One technology isolates users with VLAN, but VLAN only supports up to 4096 nodes. It cannot support the huge amount of users in the cloud.

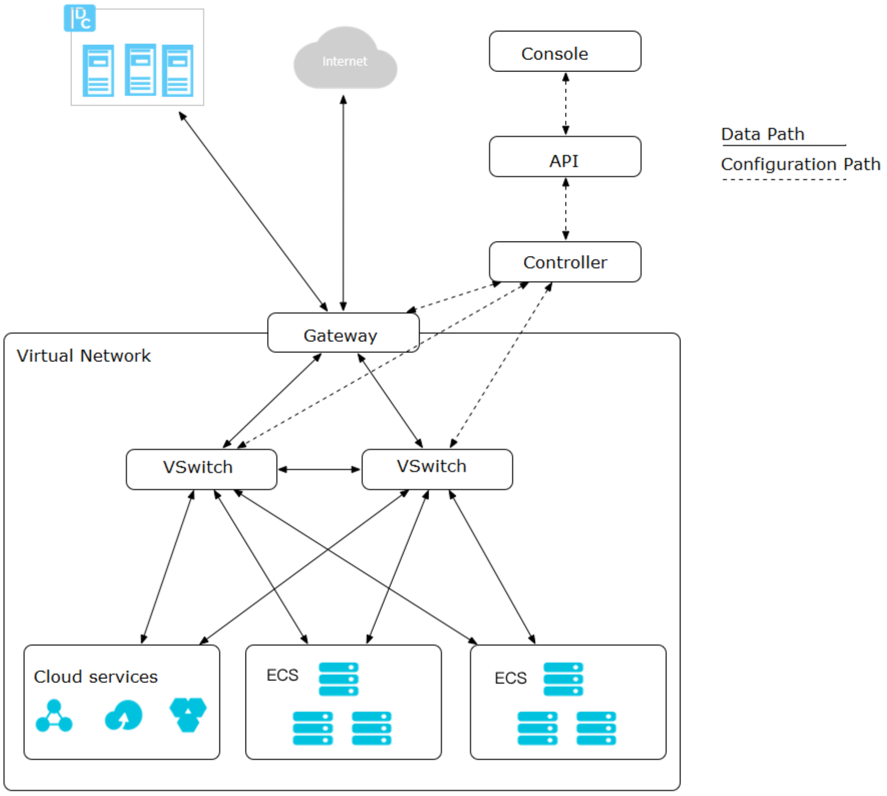
VPC theory

VPCs isolate virtual networks based on mainstream tunneling technologies. Each VPC has a unique tunnel ID, and a tunnel ID corresponds to only one VPC. A tunnel encapsulation carrying a unique tunnel ID is added to each data packet transmitted between the ECS instances within a VPC. Then, the data packet is transmitted over the physical network. Because the tunnel IDs are different for ECS instances in different VPCs and the IDs are located on two different routing planes, the ECS instances from different VPCs cannot communicate with each other and are isolated by nature.

Based on the tunneling and SDN technologies, the Alibaba Cloud research and development team has developed the VPC in the basis of hardware gateways and self-developed switch equipment.

Logical architecture

As shown in the following figure, the VPC architecture contains three main components: VSwitches, gateway, and controller.



VSwitches and gateways form the key data path. Controllers use the self-developed protocol to forward the forwarding table to the gateway and VSwitches, completing the key configuration path. In the overall architecture, the configuration path and data path are separated from each other.

VSwitches are distributed nodes, the gateway and controller are deployed in clusters, and all links have redundant disaster recovery. This improves the overall availability of the VPC. Alibaba Cloud's VSwitch and gateway performances are leaders in the field. The self-developed SDN protocol and controllers can easily control thousands of VPCs in the cloud.

VPCs allow you to establish an isolated network environment in Alibaba Cloud. Alibaba Cloud also provides each VPC with an independent VRouter and VSwitch. You have full control over your private virtual network, such as the private IP address range, VSwitch CIDR, the route table, and so on.

VPC

You can create and manage cloud product instances in your VPC, such as ECS, SLB, and RDS.

When creating a VPC, you must specify the private IP address range for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block. For more details, refer to Classless Inter-Domain Routing.

You can use the following standard CIDR block and the subset as the IP address range of your VPC. The available IP address exclude system reserved addresses.

CIDR block	Number of available IP addresses
192.168.0.0/16	65,532
172.16.0.0/12	1,048,572
10.0.0.0/8	16,777,212

The CIDR block cannot be changed once a VPC is created. Therefore, we recommend to use a larger sized CIDR block to avoid IP expansion. The system does not create the system route based on the VPC CIDR block. That is, using a relatively large CIDR block will not impact your business application.

VSwitch

A VSwitch is a basic network device for a VPC and is designed to connect the cloud product instances in the VPC. You can further segment your VPC into subnets by adding VSwitches. A VPC must contain at least 1 VSwitch and can contain up to 24 VSwitches.

Note: VSwitch does not support multicast or broadcast.

When creating a VSwitch in a VPC, you need to specify the private IP address range in the form of a Classless Inter-Domain Routing (CIDR) block. The allowed block size for a VSwitch is between a /16 netmask and /29 netmask.

IP addresses

IP addresses allow the VPC resources to communicate with each other and resources on the Internet. In a VPC, you may need to use the following IP addresses:

Private IP

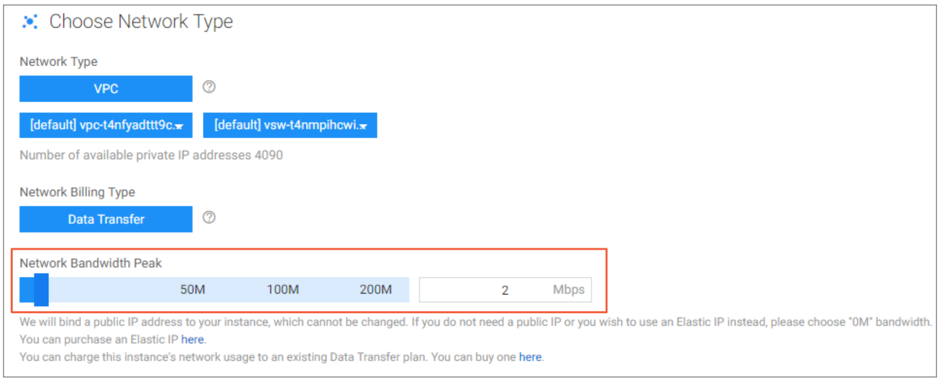
The system allocates a private IP address to each VPC cloud product instance, such as ECS instance, SLB instance, and RDS instance. The private IP address can be used for the intranet access among the VPC cloud product instances, but cannot be used for the external Internet access.

The private IP address is unique in the VPC, which is allocated based on the VSwitch CIDR block.

Public IP

A public IP address is allocated to the VPC-type ECS instance. You can use this IP address to access the Internet or provide public services.

Note: If you set a value larger than 0 for the network bandwidth peak, a public IP address is not allocated to a VPC ECS instance by default.



Choose Network Type

Network Type: VPC

[default] vpc-t4nfyadttt9c. [default] vsw-t4nmpihcwi.

Number of available private IP addresses 4090

Network Billing Type: Data Transfer

Network Bandwidth Peak: 2 Mbps

We will bind a public IP address to your instance, which cannot be changed. If you do not need a public IP or you wish to use an Elastic IP instead, please choose "0M" bandwidth.
You can purchase an Elastic IP here.
You can charge this instance's network usage to an existing Data Transfer plan. You can buy one here.

Elastic IP

Elastic IP addresses (EIPs) are public IP address resources that you can purchase and possess separately. EIPs can be dynamically bound to a VPC ECS instance. With an EIP, ECS instances can communicate with the Internet.

An EIP address is a NAT IP. It is located in the public network gateway of the Alibaba Cloud and mapped to the private network interface card (NIC) of the bound ECS instance by NAT. Therefore, the ECS instance that has bound an EIP can communicate with the Internet without disclosing its EIP in the NIC.

VRouter

A VRouter is a hub in the VPC connecting all VSwitches in the VPC and serves as a gateway device connecting the VPC with other networks.

The VRouter supports static routing, load sharing, EMCP, standby routing, and other configuration methods in the scenario that a leased line is connected to a VPC.

A VRouter and route table are automatically created after you create a VPC. You cannot create or delete them directly. They will be deleted automatically with the deletion of the VPC. You can add route entries to the route table to route network traffic.

Each entry in the route table is a route entry determining where network traffic is directed. There are two types of route entries: system route entries and custom route entries.

System route entry

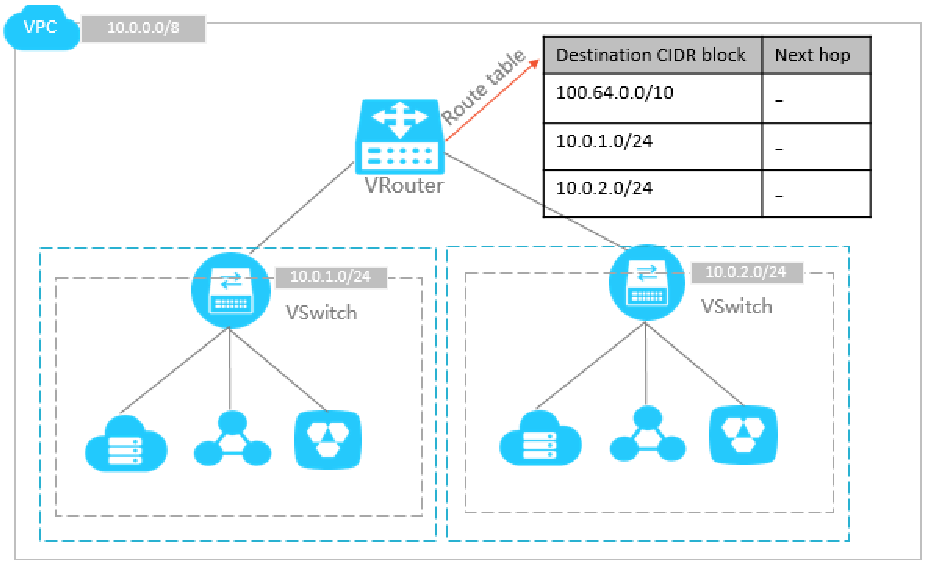
A route entry with the destination CIDR block 100.64.0.0/10 is added by the system when you create a VPC. This allows for communication between cloud product instances in the VPC.

Additionally, a route entry is added for each VSwitch by the system when you create a VSwitch. The destination CIDR block of this system route entry is the CIDR block of the VSwtich.

Custom route entry

You are allowed to add customized route entries for your VPC. For details, refer to Manage a route table.

The following figure indicates how VRouter works.



Destination CIDR block	Next hop
100.64.0.0/10	-
10.0.1.0/24	-
10.0.2.0/24	-

Security isolation

- The cloud servers of different users are located in different VPCs.
- Different VPCs are isolated by tunnel IDs. Using VSwitches and VRouters, you can segment your VPC into subnets as you would in the traditional network environment. Different cloud servers in the same subnet use the VSwitch to communicate with each other, while cloud servers in different subnets within a VPC use VRouters to communicate with each other.
- The intranet between different VPCs is completely isolated and can only be interconnected by external mapping of IP (Elastic IP and NAT IP).
- Because the IP packets of cloud servers are encapsulated with the tunneling ID, the data link layer (two-layer MAC address) of the cloud server will not transfer to the physical network. Therefore, the two-layer network of different cloud servers is isolated. That is, the two-layer networks between different VPCs are isolated.
- ECS instances within a VPC use a security group firewall to control the network access. This is the third layer isolation.

Access control

- Security groups provide flexible access control rules.
- Compliant with security isolation rules of government and financial users.

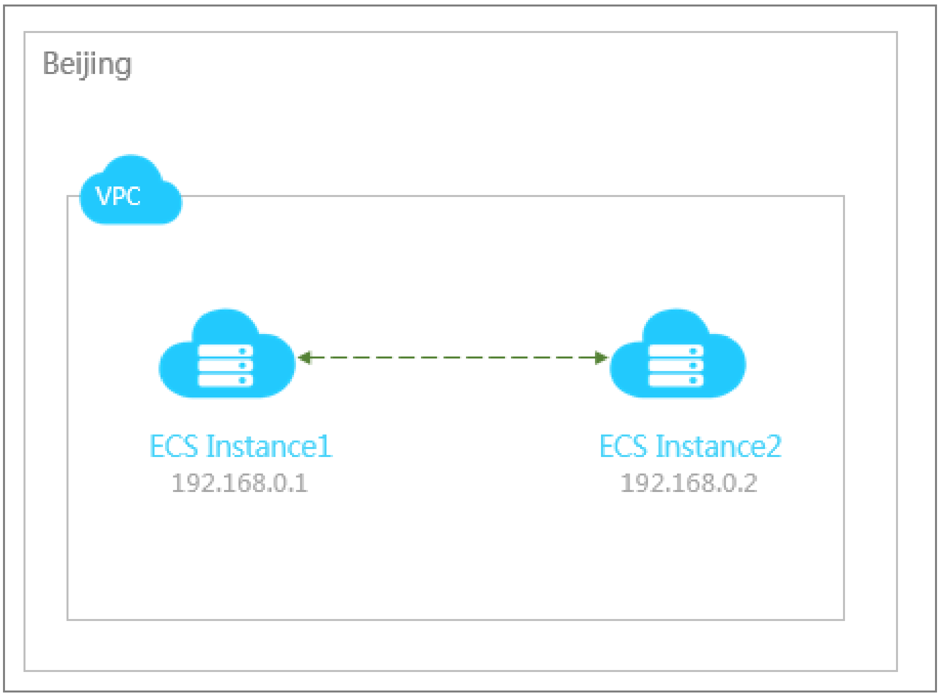
Software Defined Network (SDN)

- SDN provides customized network configurations.
- Management operations take effect in real time.

Various network connection methods

- Software VPNs are supported.
- Lease line connection is supported.

VPC provides a completely isolated network environment. By default, intranet communications can be implemented between ECSs and cloud services within the same VPC, but the VPC itself cannot communicate with other VPCs, classic networks, or the Internet. You can use Internet-facing products such as the EIP, Express Connect, NAT, VPN Gateway, and Internet-facing SLB to implement communications between VPCs.

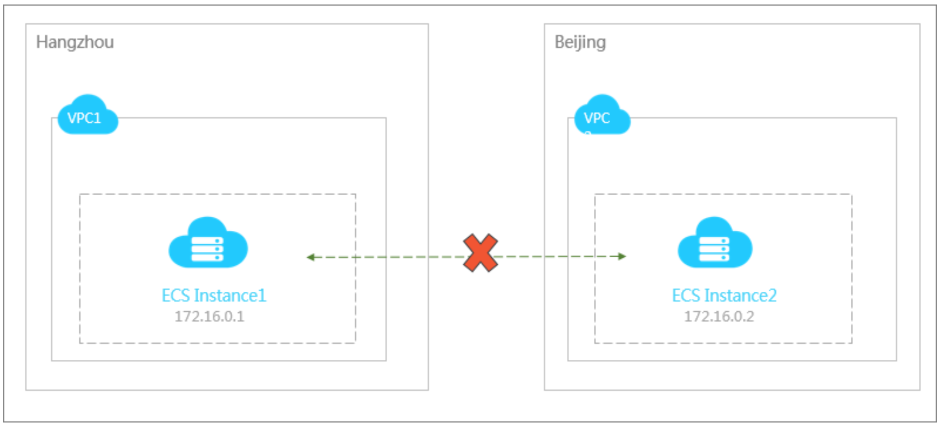


This article describes VPC communications in the following scenarios:

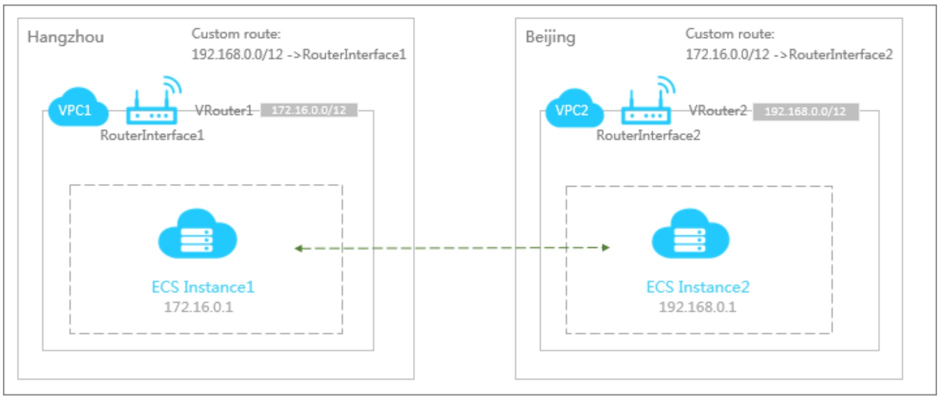
- Communications between VPCs
- Communications between VPC and Classic Network
- Communications between the VPC and the Internet
- Communications between the VPC and the local IDC

Communications between VPCs

By default, ECSs from different VPCs cannot communicate directly over the intranet.

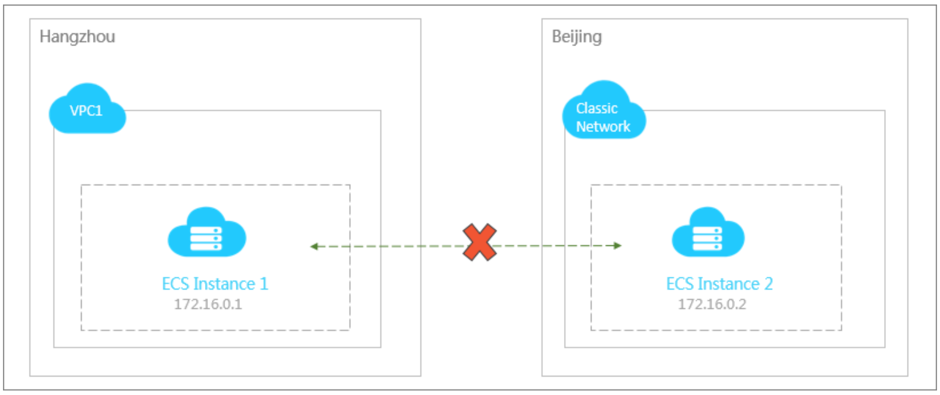


By creating router interfaces on both sides of the VPCs to build a Express Connect on Alibaba’ s backbone transmission network, you can easily implement fast, secure, reliable, and convenient communications between VPCs. For detailed configurations, see Establish an intranet connection between VPCs in different regions.



Communications between VPC and Classic Network

By default, ECSs from different VPCs cannot communicate directly over the intranet.



Access the classic network by the VPC

A VPC can communicate with a classic network using a public IP. A VPC can access cloud services of the classic network when the ECS instance of the VPC and the classic network or the public IP of the cloud instance complies with any one of the requirements listed in the following table.

Network Type	Configuration requirements
VPC	- Assign a public IP to the ECS instance when it is created. - Bind an EIP to the ECS instance. - Configure a NAT gateway (SNAT) on the ECS instance.
Classic network	- The ECS instance has an available public IP. - This ECS instance has been added to an Internet-facing SLB instance.

Access the VPC by the classic network

The classic network can also access the VPC using a public IP if the public IP has been configured on the ECS instance or cloud services of the VPC.

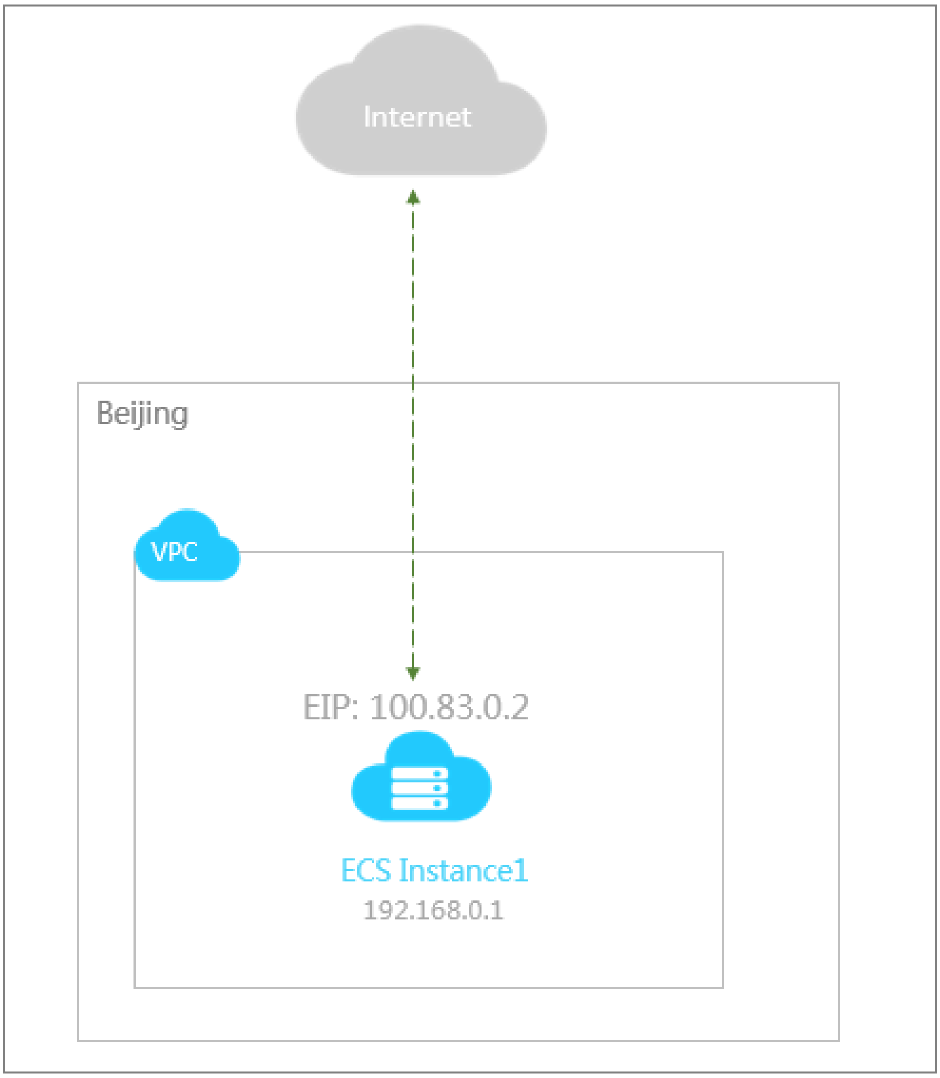
Network	Configuration requirements
Classic network	- The ECS instance has an available public IP.
VPC	- Assign a public IP to the ECS instance when it is created. - Bind an EIP to the ECS instance. - Configure a NAT gateway (DNAT) on the ECS instance. - This ECS instance has been added to an Internet-facing SLB instance.The request from the Internet is forwarded to the backend ECS using the Internet-facing SLB instance.

Communications between the VPC and the Internet

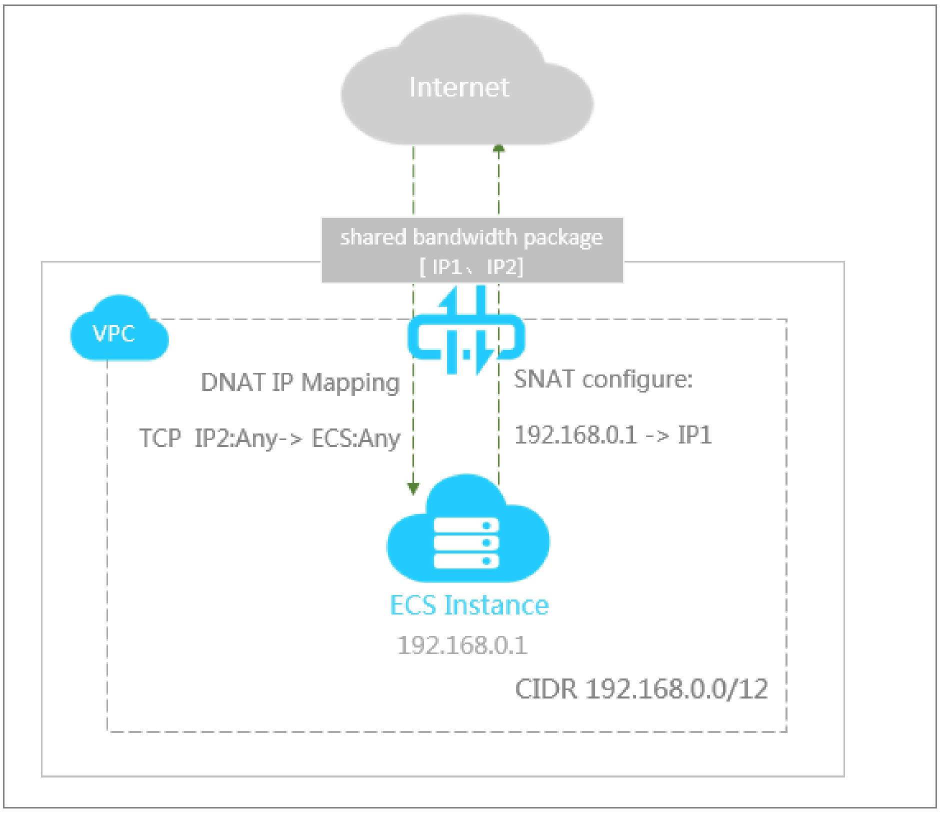
By default, the ECS in the VPC cannot communicate with the Internet. You can enable the communications between the VPC and the Internet in the following ways:

Assign a public IP to the ECS instance in the VPC to implement communications between the VPC and the Internet. For more information, see Allocate a public IP.

You can bind an EIP to the ECS to connect the VPC to the Internet. For more information, see Bind an EIP.



Configure the NAT gateway on the ECS in the VPC to implement communications between the VPC and the Internet. For more information, see Port Mapping and SNAT Configuration.



Note: If multiple ECSs need to communicate with the Internet, you can use the shared bandwidth package of the NAT gateway to share the bandwidth with all the ECS instances in the bandwidth package, thus saving your cost.

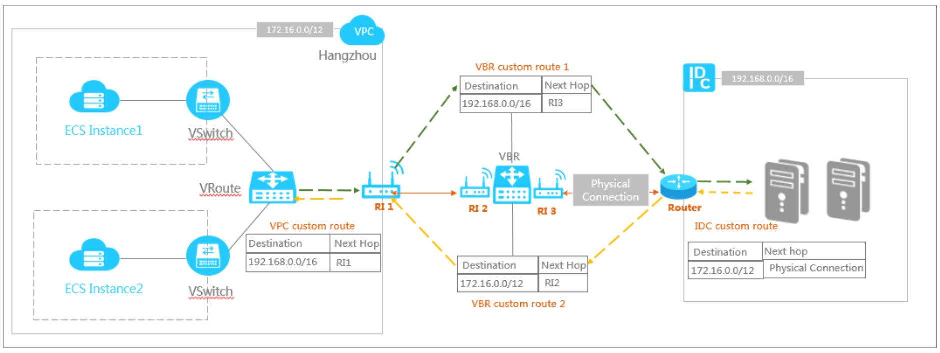
Add an ECS instance of the VPC to an Internet-facing SLB instance. For more information, see Configure an Internet-facing SLB.

Note: In this case, the ECS instance in the VPC cannot access the Internet. It can only receive the Internet request forwarded by the SLB.

Communications between the VPC and the local IDC

By default, the local IDC does not communicate with the VPC. You can implement communications between the local IDC and the VPC in the following ways:

You can use Express Connect (Physical Connection) to connect an on-premises IDC to the dedicated access points of Alibaba Cloud, and establish a virtual border router as a bridge that forwards your data from the VPC to the IDC. For more information, see Physical connection.



You can use the VPN gateway to implement communications between an on-premises IDC and a VPC. For more information, see Create a VPN gateway.

Terms	Descriptions
Virtual Private Cloud (VPC)	VPC is a private network established in Alibaba Cloud. It is logically isolated from other virtual networks in Alibaba Cloud. Alibaba Cloud VPC enables you to launch and use the Alibaba Cloud resources in your own VPC.
VSwitch	A VSwitch is a basic network device of a VPC and used to connect different cloud product instances. When creating a cloud product instance in a VPC, you must specify the VSwitch that the instance is located.
VRouter	A VRouter is a hub in the VPC that connects all VSwitches in the VPC and serves as a gateway device that connects the VPC to other networks. VRouter routes the network traffic according to the configurations of route entries.
Route Entry	Each entry in a route table is a route entry. A route entry specifies the next hop address for the network traffic destined to a CIDR block. It has two types of entries: system route entry and custom route entry.
Route Table	A route table is a list of route entries in a VRouter.

VPC

Items	Limits	Ticket submission permits exemption
Available CIDR blocks	192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, and their subsets	Supported
Maximum number of VPCs for an account	10	Supported
Maximum number of	1	Unsupported

VRouters in a VPC		
Maximum number of VSwitches in a VPC	24	Unsupported
Maximum number of route tables in a VPC	1	Unsupported
Maximum number of route entries in a route table	48	Supported
Maximum number of cloud product instances that can run in a VPC	10,000	Unsupported

VRouter and VSwitch

Items	Limits
VRouter	- Each VPC can have only one VRouter. - VRouter does not support dynamic route protocols, such as BGP or OSPF. - Each VRouter has only one route table. - Route entries in a route table affect all the cloud product instances in the VPC. Currently, the source IP routing rules are not supported by VSwitches and cloud product instances.
VSwitch	- VSwitches are a layer-3 switch, therefore the layer-2 broadcast and multicast are not supported. - The number of instances that a VSwitch can have = 10,000 - the number of existing instances in the VPC. - The CIDR block cannot be modified.