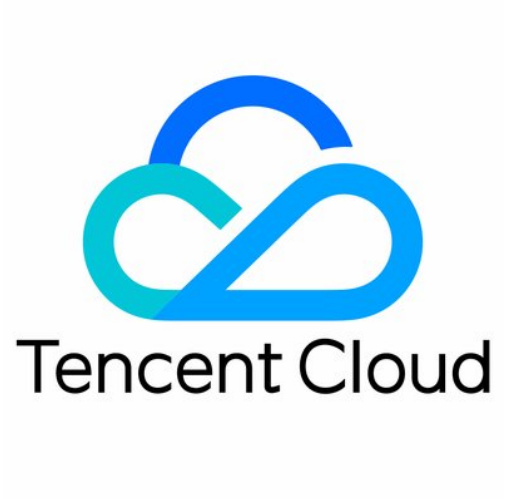
Virtual Private Cloud

FAQ

Product Documentation



Contents

FAQ
General
Concept-Related

Last updated：2020-09-08 14:44:43

How can I establish communication between different subnets of a VPC?

- Each VPC supports private network interconnection by default, and you can find the default route in the corresponding route table. This route indicates that all resources in this VPC can connect with each other over the private network.
- Subnets in different VPC instances are not interconnected over the private network. To interconnect these subnets, establish peering connection or use Cloud Connect Network.

Can CVMs be deployed in different availability zones in the same VPC?

Yes. A VPC is a regional (such as Guangzhou, Beijing, or Seoul) resource, and the subnets in the VPC are resources in availability zones (such as Guangzhou Zone 1 or Guangzhou Zone 2). Therefore, subnets in one VPC can be deployed in different availability zones in the same region. A CVM is also availability zone specific as the subnet it belongs to. So, if you purchase CVMs under subnets in availability zones, you can deploy them in different availability zones.

How can I establish communication between CVMs and databases in different availability zones?

- In the same VPC: CVMs and databases in the same VPC are interconnected by default. If the interconnection fails, you can first troubleshoot the firewall policies of the security group and the network ACL.
- In different VPCs: CVMs and databases are isolated by default. If the interconnection is required, you can establish private network interconnection between VPC instances using peering connection or CCN.

How many private IP addresses can each VPC provide for Tencent Cloud service instances?

A VPC supports a maximum of 65,533 private IP addresses for Tencent Cloud service instances.

What is a CIDR block?

Classless Inter-Domain Routing (CIDR) is a specified independent network address block that uses with IP and mask to implement the overall division of network. It eliminates the concepts of

traditional class A, B and C addresses as well as subnet partitioning, and assigns the IP address spaces more efficiently. You need to create subnets in CIDR format when creating a VPC and its subnets. For example, to create an IP range of `10.0.16.0 - 10.0.17.255`:
This IP range changes to `00001010.00000000.00010000.00000000 - 00001010.00000000.00010001.11111111` in binary format that has the same first 23 digits, and to `10.0.16.0/23` in CIDR format.

Connections
FAQ for Internet Connection

Last updated : 2019-09-24 15:34:49

1. How do instances without public IP addresses (CVMs, databases) access the Internet?

They can access the Internet through NAT gateways/public network gateways.

- NAT gateways. By creating NAT gateways and configuring the routing table associated with relevant subnet, the instances within the subnet can access the Internet. Click to view the operation instructions.
- Public network gateways. CVMs without public IPs can access the Internet via public network gateways located in different subnets.

2. What is the difference between public network gateways and CVMs with public IPs?

A public IP coming with a CVM is equivalent to an additional public network NIC, enabling the CVM to freely access the Internet.

3. Why cannot a routing policy be forwarded after the policy is configured for a subnet and directed to a public network gateway?

When the CVM that accesses the Internet through a public network gateway and the public network gateway are in the same subnet, the forwarding function will fail. Please arrange the CVM and the public network gateway in different subnets.

4. In the routing table, the access to the public network within a subnet is set to be made through NAT gateways,

but the CVMs in the subnet are configured with elastic IPs. So whether these CVMs access the public network through NAT gateways or elastic IPs?

Through the **NAT gateways**. Click to view routing rule priority.

Classiclink-Related

Last updated：2020-09-08 14:48:39

What is Classiclink?

The Classiclink is used to associate CVMs in the classic network to the specific VPC, enabling CVMs to communicate with Tencent Cloud services including CVMs and databases in the VPC. For more information, see Managing Classic Networks.

How can I establish communication between a CVM in a classic network and a CVM in a VPC?

You can use Classiclink to establish communication between classic networks and VPCs.
When using the Classiclink, take note of the following limits:

1. The classic network and the VPC that need to communicate with each other must be in the same region (but can be in different availability zones, such as Guangzhou Zone 1 and Guangzhou Zone 2).
2. The CIDR (IP range) of the VPC must be `10.0.0.0/16 - 10.47.0.0/16` (including subsets), otherwise a conflict occurs.

If your classic network and VPC meet these conditions, you can configure the **Classiclink** tab on the details page of the VPC in the Console to associate the VPC with the CVMs in the classic network for interconnection.

Can resources including cloud load balancers and databases in the classic network communicate with the VPC?

- A terminal connection helps establish communication between instances in a VPC and other instances in a classic network over a private network. Here, the principle is to map the IP addresses of instances in the classic network to VPC IP addresses so that you can access a classic network instance by accessing the corresponding VPC IP address. The services that support the classic network include LB, TencentDB, CMEM, REDIS, MongoDB. Cross-region/cross-account is not supported.
- Direction: one-way (VPC accesses the classic network).
- If you need more directions, submit a ticket to apply.

Can classic network and VPC instances under different accounts communicate with each other?

No. Currently, resources (CVMs and databases) in classic networks and VPC instances under different accounts cannot communicate with each other. A VPC supports more features with greater flexibility, so we recommend migrating from the classic network to VPC.

Safety Class
Security

Last updated : 2019-09-24 15:28:41

1. How to ensure the security of CVMs running in a VPC?

A VPC is a network environment that is logically isolated, and security groups and network ACLs can be used for traffic control:

- **Security groups** can be used to specify the inbound and outbound network traffic that is allowed to enter or exit each CVM. Traffic which is not explicitly allowed to or from an instance is automatically denied.
- **Access Control List (ACL)** can also allow or deny the network traffic entering or exiting each subnet.

2. What are the differences between security groups and network ACLs in VPCs?

Click to view the differences between security groups and network ACLs.

Port and Security Group

Last updated : 2020-10-16 14:44:17

Port

Which ports should be opened to the Internet before I log in to an instance?

Generally, you need to open port 22 for a Linux instance, or port 3389 for a Windows instance. For more information about ports applicable to other instance types, see Application Cases of Security Groups.

Why should a port be opened to the Internet? How can I open a specific port?

You can use the service only after you open the port to the Internet in the security group. For example:
If you want to access web pages using port 8080, the port must be enabled and opened to the Internet in the security group.
To open a port to the Internet, follow the steps below:

1. Go to the security group page, and click the ID/name of the security group bound with this instance to go to its details page.
2. Select **Inbound/Outbound rule** and click **Add a Rule**.
3. Enter your IP address (range) and port to be opened, and then select **Allow** to open the port. For more information, see Adding a Security Group Rule.

Why cannot the service be used after I change the port?

After modifying the service port, you also need to open the corresponding port to the Internet in the security group.

Which ports are not supported by Tencent Cloud?

The following ports have security risks. They will be blocked by ISPs and cannot be accessed. To avoid this, we recommend that you change ports and do not use the following ports for listening:

Protocol	Blocked Port
TCP	42, 135, 137, 138, 139, 445, 593, 1025, 1434, 1068, 3127, 3128, 3129, 3130, 4444, 5554, 5800, 5900 and 9996
UDP	1026, 1027, 1434, 1068, 5554, 9996, 1028, 1433 and 135 - 139

Why cannot TCP port 25 be used to connect to an external address, and how can I unblock the port?

- To enhance the quality of sending emails through Tencent Cloud's IP addresses, CVMs are blocked by default from using TCP port 25 to connect to external addresses. To unblock this port, you can log in to the console, hover over the account navigation area at the top, and click **Security Control** to view the link for unblocking port 25.
- You can only unblock the port on a maximum of five monthly subscription CVM instances. However, pay-as-you-go CVM are not supported yet.

For more information about ports, see Common Server Ports.

Security Group

Why does a security group have a reject rule by default?

Security group rules take effect sequentially from top to bottom. If an allow rule that was previously set takes effect, other rules will be rejected by default. If this allow rule opens all ports to Internet, the last reject rule will not take effect. We provide this default setting due to security concerns.

If I bind an incorrect security group to an instance, what impact will this have on the instance? How can I fix this problem?

- **Potential problems**
  - You may fail to remotely connect to a Linux instance over SSH or a Windows instance via remote desktop.
  - You may fail to remotely ping the public IP and private IP addresses of the CVM instance in this security group.
  - You may fail to access over HTTP the web services exposed by the CVM instance in this security group.
  - The CVM instance in this security group may fail to access Internet services.
- **Solutions**
  - If any of the aforementioned problems occur, you can go to **Security Groups** on the console and modify the security group rule. For example, you can change the rule to "bind only all-ports-open security groups by default".
  - For more information on how to set a security group rule, see "Security Group Rules" section of Security Groups.

What do the security group direction and policy mean?

- There are outbound and inbound security group directions. The outbound direction filters the outbound traffic of the CVM instance, whereas the inbound direction filters the inbound traffic of the CVM instance.
- Security group policies are divided into those that **allow** or **reject** traffic.

In which order do the security group policies take effect?

Security group policies take effect sequentially from top to bottom when traffic flows through the security group. Once the traffic matches a policy, the policy will take effect immediately.

Why can’t a port that is opened to the Internet by a security group access the CVM instance?

- The CVM is bound to multiple security groups, and this port is rejected by another security group with a higher priority.
- The network ACL or firewall has been configured.

Why can an IP address that is rejected by a security group still access the CVM instance?

Possible reasons are as follows:

- The CVM is bound to multiple security groups, and this IP address is allowed by another security group among them.
- This IP address belongs to an approved Tencent Cloud public service.

Can iptables be used along with security groups?

Yes. Security groups and iptables can be used at the same time. Your traffic will be filtered twice in the following directions:

- Outbound: processes in your instance > iptables > security groups.
- Inbound: security groups > iptables > processes in your instance.

Why can’t security groups be deleted even though all CVM instances have been returned?

Check whether any CVM instances still exist in the recycle bin. If security groups are still bound to a CVM instance in the recycle bin, they cannot be deleted.

Can the name of a cloned security group be the same as that of a security group in the target region?

No. The name must be different from that of any existing security group in the target region.

Is there any Tencent Cloud API that supports the cloning of a security group across projects and regions?

While console support is provided to help customers who use the console, no Tencent Cloud API can be directly used for this purpose at the moment. You can use the original Tencent Cloud APIs for batch importing and exporting of security group rules to indirectly clone a security group across projects and regions.

When I clone a security group across projects and regions, will CVM instances managed by the security group also be copied?

No. When a security group is cloned across regions, only the inbound and outbound rules of the original security group will be copied. Therefore, you need to bind CVM instances to the security group separately.