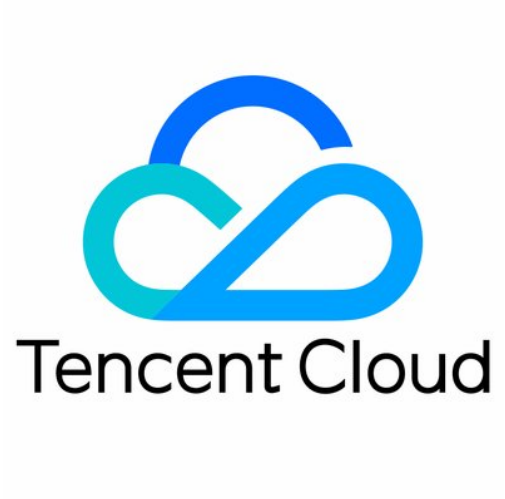
Peering Connection

Best Practices

Product Documentation



Contents

Best Practices
Migrating the Cross-Region Interconnection Service to CCN

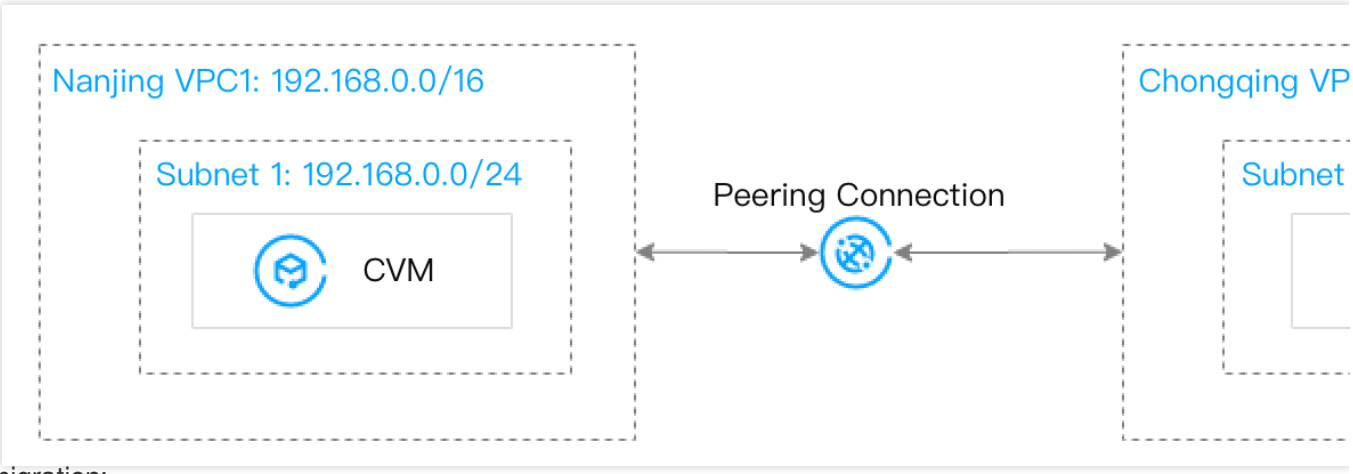
Last updated：2024-01-11 19:57:50

Overview

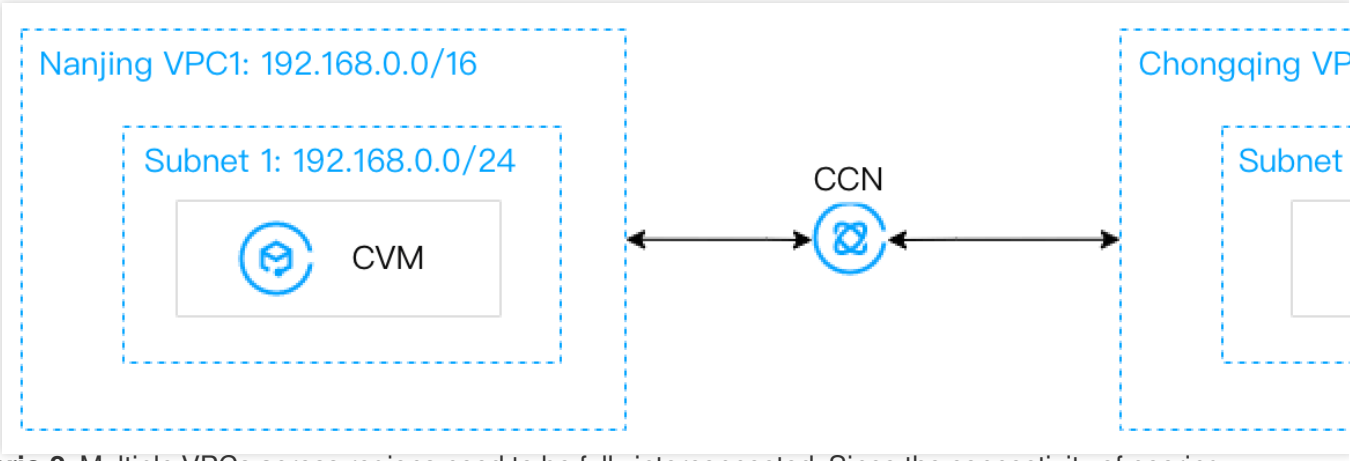
Both CCN and Peering Connection can realize cross-region VPC interconnection. Compared with Peering Connection, CCN features linkage interconnection, self-learning of routes, simple configuration, stability and reliability, and lower cost and latency.
This document guides you through plans to migrate the cross-region connection from Peering Connection to CCN.

Scenarios

Scenario 1: Nanjing VPC1 and VPC2 are connected through a peering connection.
Migration plan: Associate the two VPCs with CCN to realize the cross-region VPC interconnection.
Before migration:



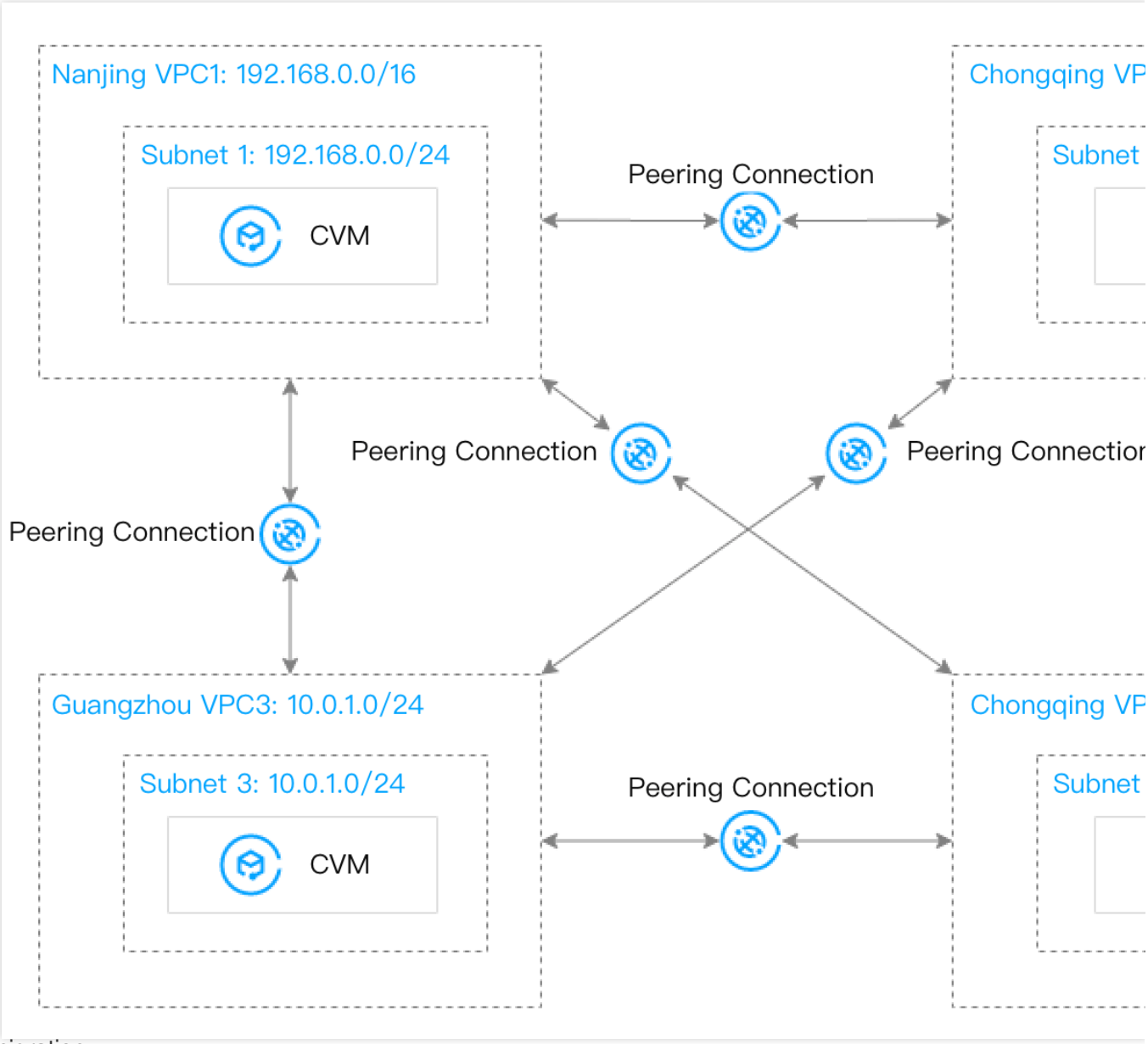
After migration:



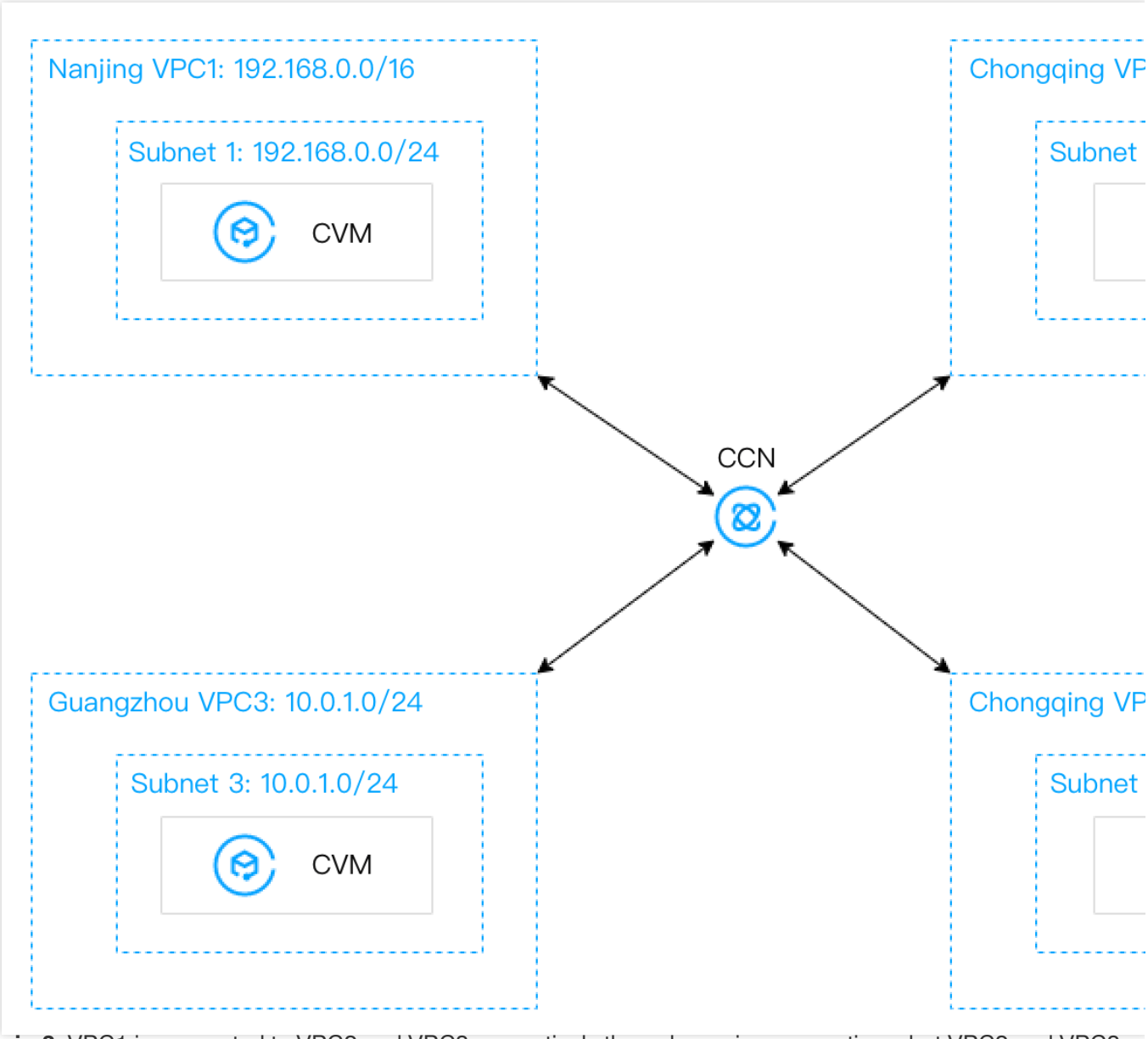
Scenario 2: Multiple VPCs across regions need to be fully interconnected. Since the connectivity of peering connections cannot be transferred, you need to create one peering connection between every two VPCs.

Migration plan: Add multiple VPCs to a CCN instance to realize the public and private network interconnection.

Before migration:



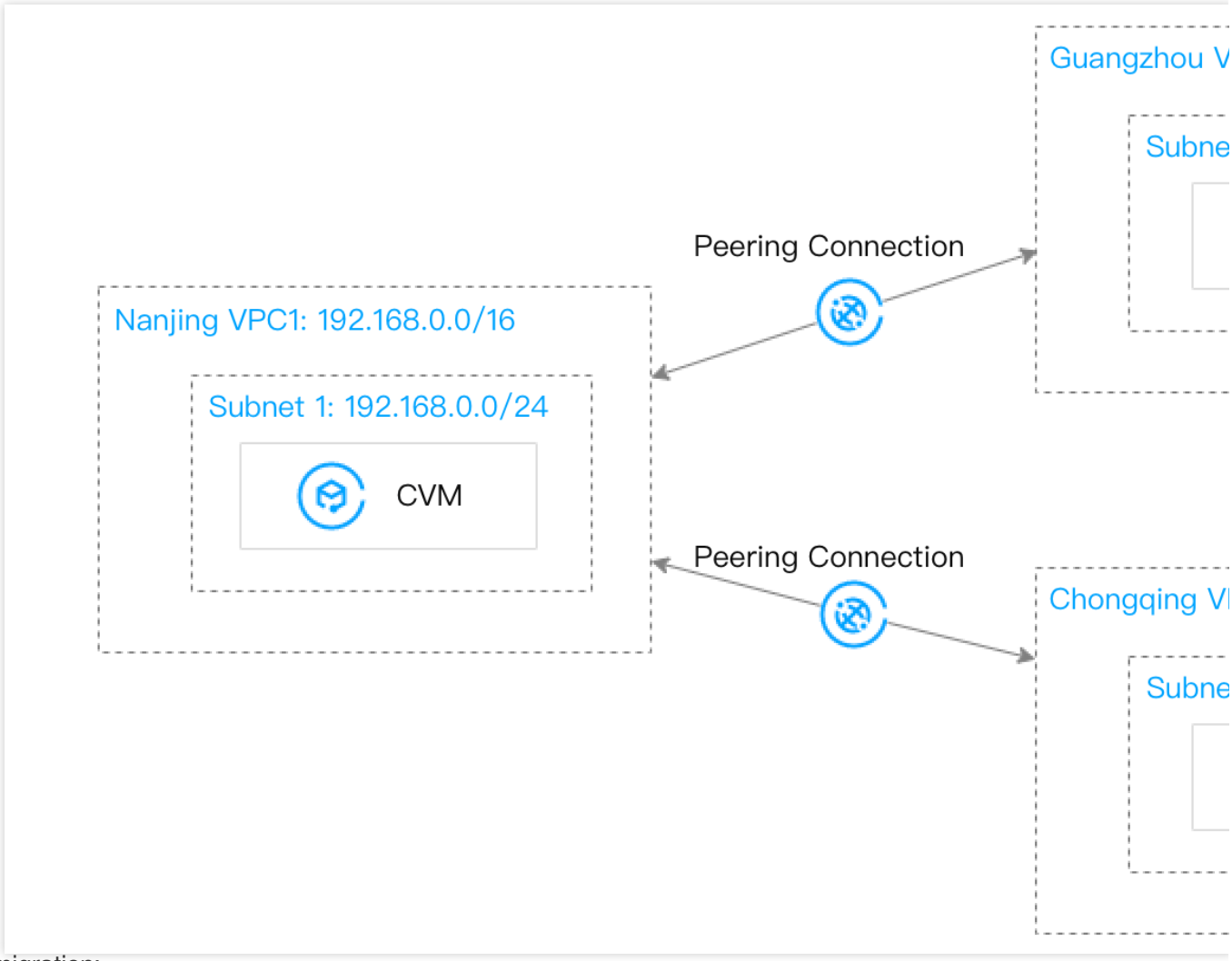
After migration:



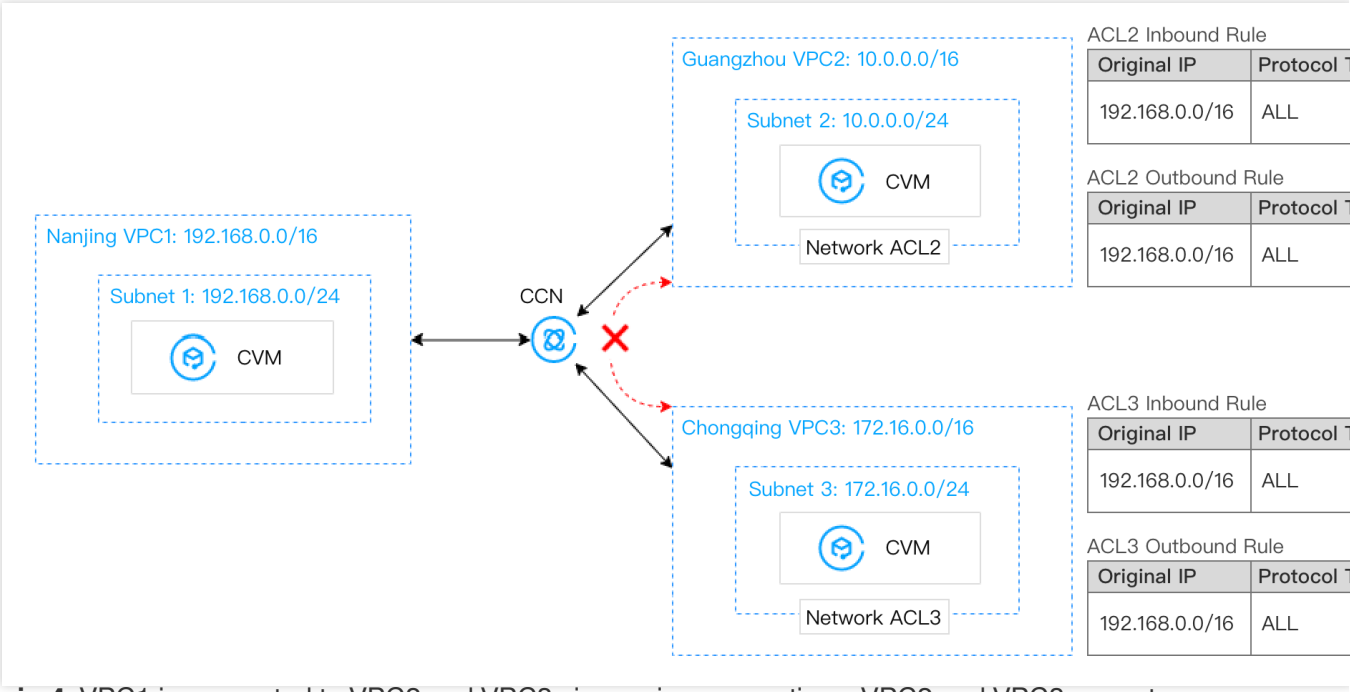
Scenario 3: VPC1 is connected to VPC2 and VPC3 respectively through peering connections, but VPC2 and VPC3 are not interconnected.

Migration plan: Use CCN to connect VPC1 with VPC2 and VPC3. For the non-interconnection between VPC2 and VPC3, associate their subnets with the network ACLs to realize access control, that is, allow the IP range used for communication only in the ACL.

Before migration:



After migration:



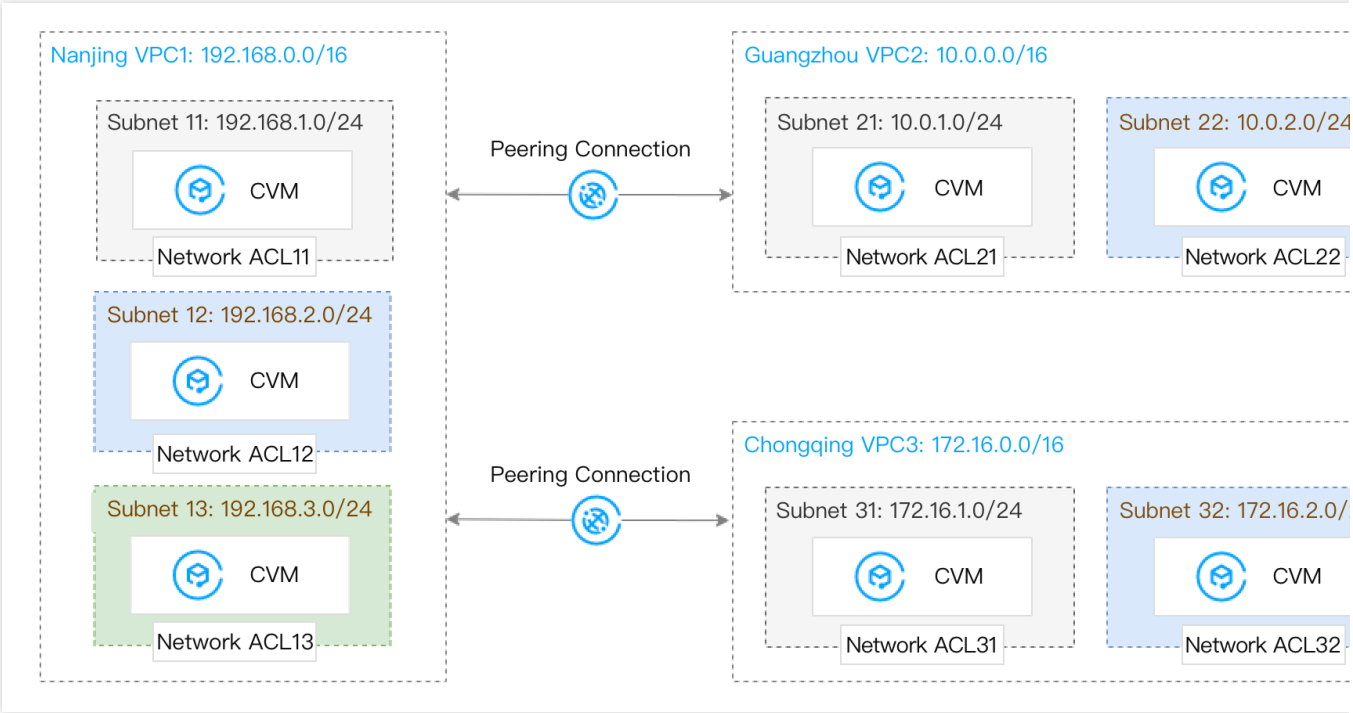
Scenario 4: VPC1 is connected to VPC2 and VPC3 via peering connections. VPC2 and VPC3 are not interconnected. The VPC1 subnet 11 is connected to the VPC2 subnet 21 and the VPC3 subnet 31. The VPC1 subnet 13 is connected to the VPC2 subnet 23 and the VPC3 subnet 33.

Note:

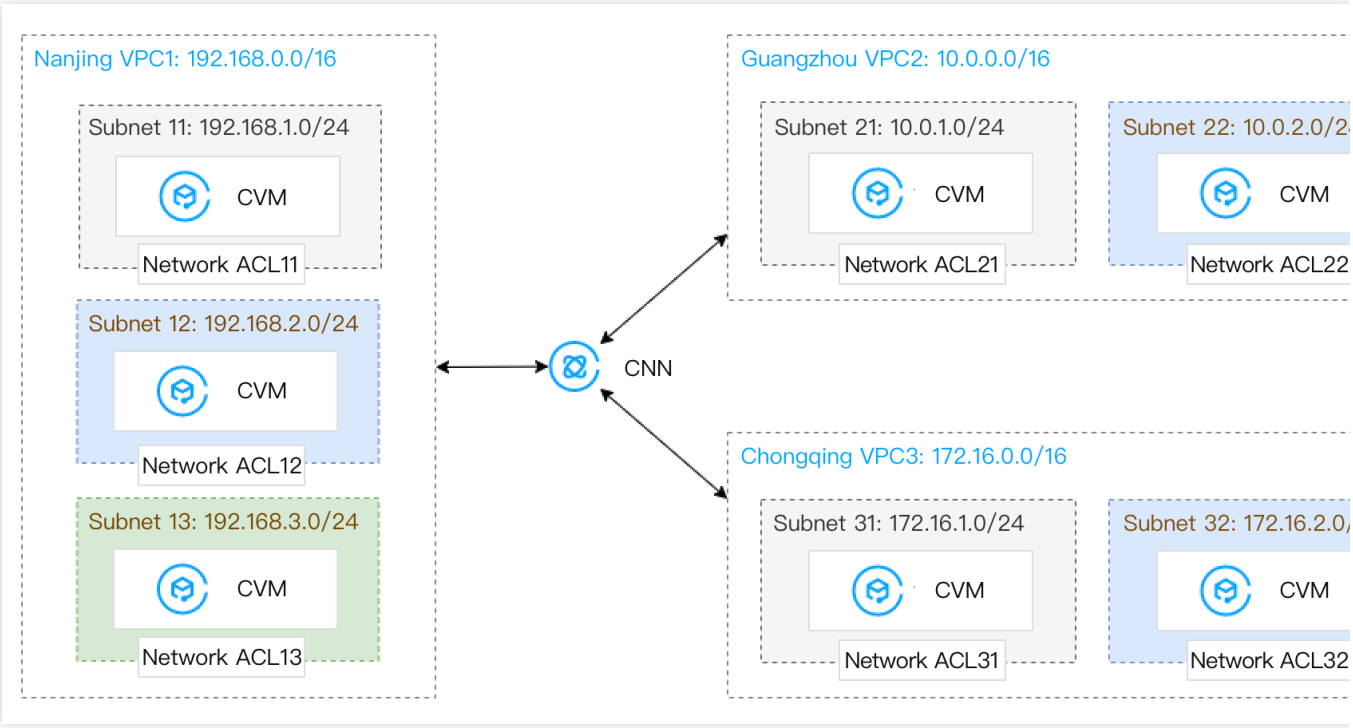
Access control between subnets is implemented through their own network ACLs. For example, for the network ACL21 of the VPC2 subnet 21, only the IP range of subnet 11 within VPC1 is allowed for communication, so as to realize the traffic access control between subnets.

Migration plan: Use CCN to fully connect VPC1, VPC2, and VPC3. Confirm the ACL rules of each subnet in advance to ensure that only the required subnet IP ranges are allowed.

Before migration:



After migration:



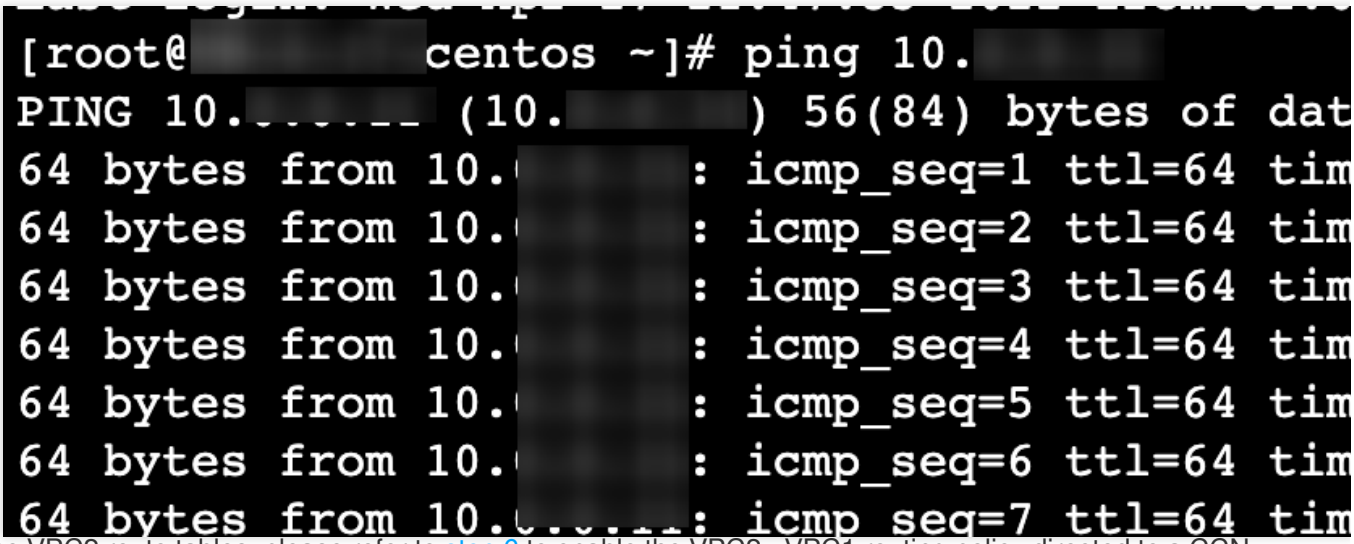
Directions

Note:

The directions are given based on scenario 1.

In scenario 2, multiple VPCs are fully interconnected. Please add these VPCs to CCN one by one, and check the routing conditions in CCN and VPCs in time. When a route conflict occurs due to overlapping IP ranges, the route

becomes invalid. For solutions, see Use Limits and Migrating VPCs with Peering Connection to CCN.
In scenario 3 and scenario 4, please configure an appropriate ACL policy as instructed in Managing Network ACLs for the subnet in advance according to the communication between the subnets. Then associate the VPCs with CCN one by one, and migrate the routes to CCN. During the period, you can monitor the business situation in real time.
1. Create a CCN Instance and associate the VPC1 to it.
2. Click the CCN instance ID and enter the route table tab. You can see the routing policy whose destination is the VPC1 subnet. To add a CCN route, see Route Overview.
3. Associate VPC2 with the CCN instance as instructed in Associating Network Instances.
4. Click the CCN instance ID again and re-enter the route table tab. You can see a new routing policy whose destination is the VPC2 subnet. For solutions of CCN routing exceptions, see Use Limits.
5. Check the route tables associated with the subnets of VPC1 and VPC2 respectively. You can see both VPC1 and VPC2 subnets have added a routing policy with the next hop to CCN. But due to the routing conflict, when the destination IP range overlaps, the routing policy added later is invalid, so the communication between VPC1 and VPC2 is still implemented through the peering connection.
6. In the VPC1 ro
ute tabl
es, enable VPC1 - VPC2 routing policy directed to a CCN instance, and disable the VPC1 - VPC2 routing policy directed to a peering connection instance, as instructed in Managing Routing Policies. At this time, VPC1 communicates with VPC2 via a CCN connection, while VPC2 communicates with VPC1 via a peering connection.
7. Check the monitoring information as instructed in View Monitoring Information or Viewing Monitoring Data of Network Traffic Over a Cross-region Peering Connection or log in to a CVM instance as instructed in Logging In to Linux Instance (Web Shell). `Ping` the network to check whether the traffic is normal. If it is not normal, please submit a ticket.



8. In the VPC2 route tables, please refer to step 6 to enable the VPC2 - VPC1 routing policy directed to a CCN instance, and disable the VPC2 - VPC1 routing policy directed to a peering connection instance.
9. Check the monitoring information or check whether the traffic is normal by a `ping` test.

If the traffic is abnormal, please submit a ticket.
If the business traffic is normal within a week, and monitoring reveals that the peering connections have no traffic, you can refer to Managing Routing Policies and Deleting a Peering Connection to delete the routing policies directed to peering connection in the VPC1 and VPC2 route tables and the peering connection instances that you no longer use.