03 Introduction to Tencent Cloud Networking

Course Objectives

- At the end of this course, you will have a better understanding of:
  - The features, advantages, and use cases of Tencent Cloud VPC
  - The features, advantages, and impact of Tencent Cloud networking
  - The features, advantages, and use cases of Tencent Cloud CLB
  - The billing plans for Tencent Cloud networking products

CONTENTS

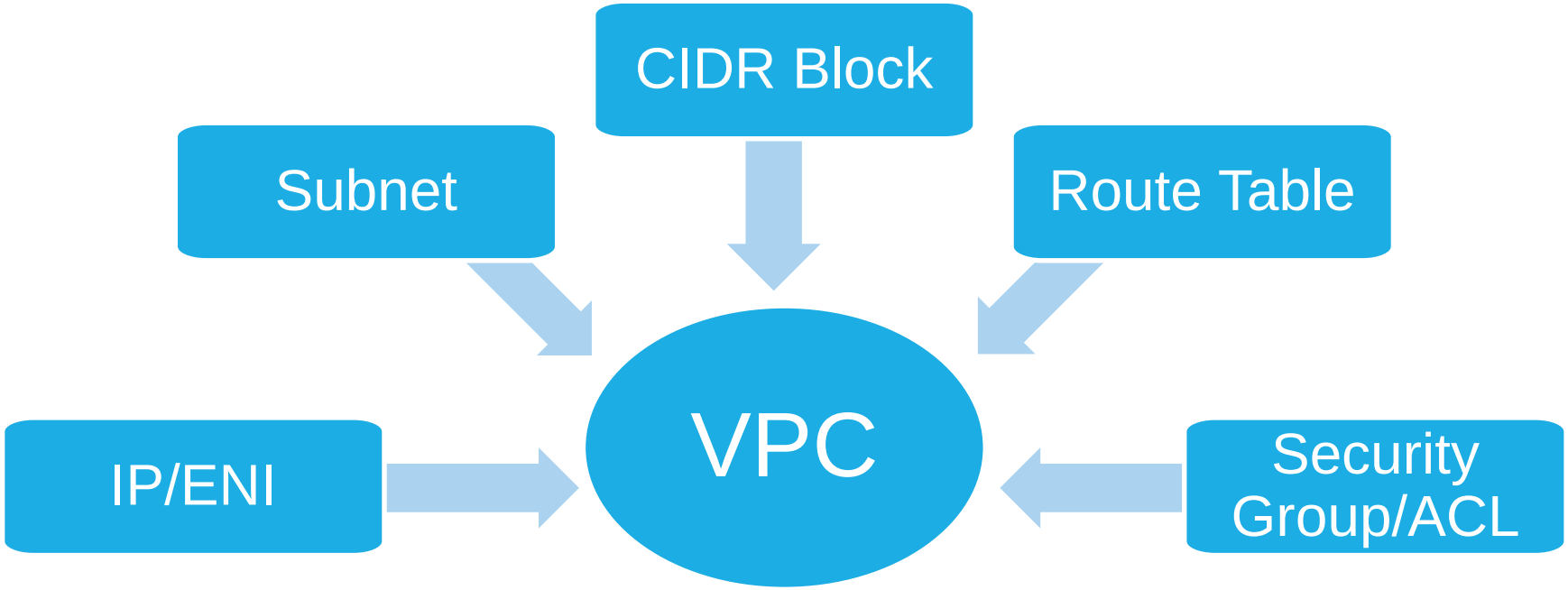
腾讯云

CONTENTS

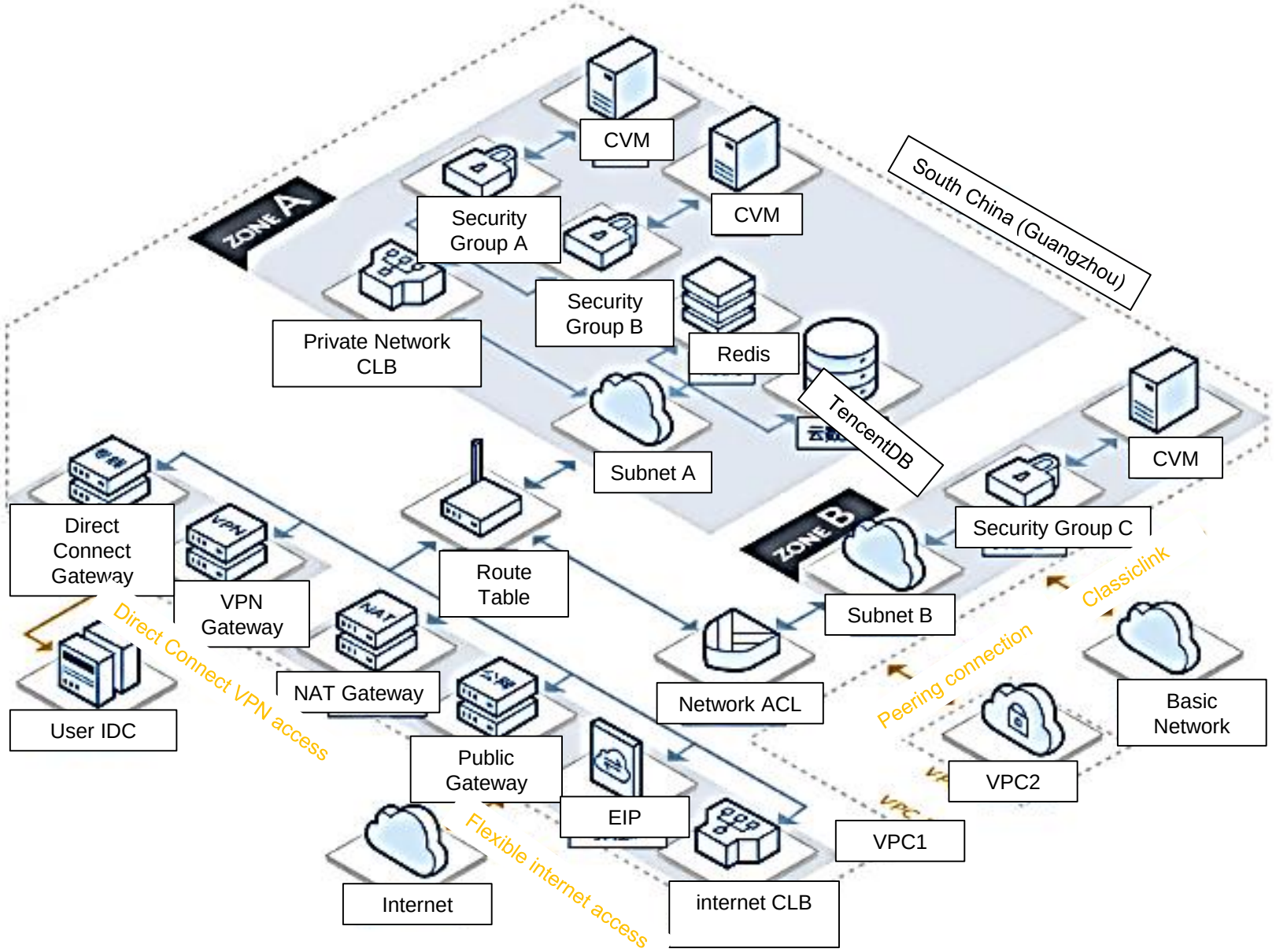
Chapter I Tencent Cloud VPC

1.1 What is a VPC?

- A Virtual Private Cloud (VPC) refers to a user-defined, logically isolated, and dedicated cloud-based network space.

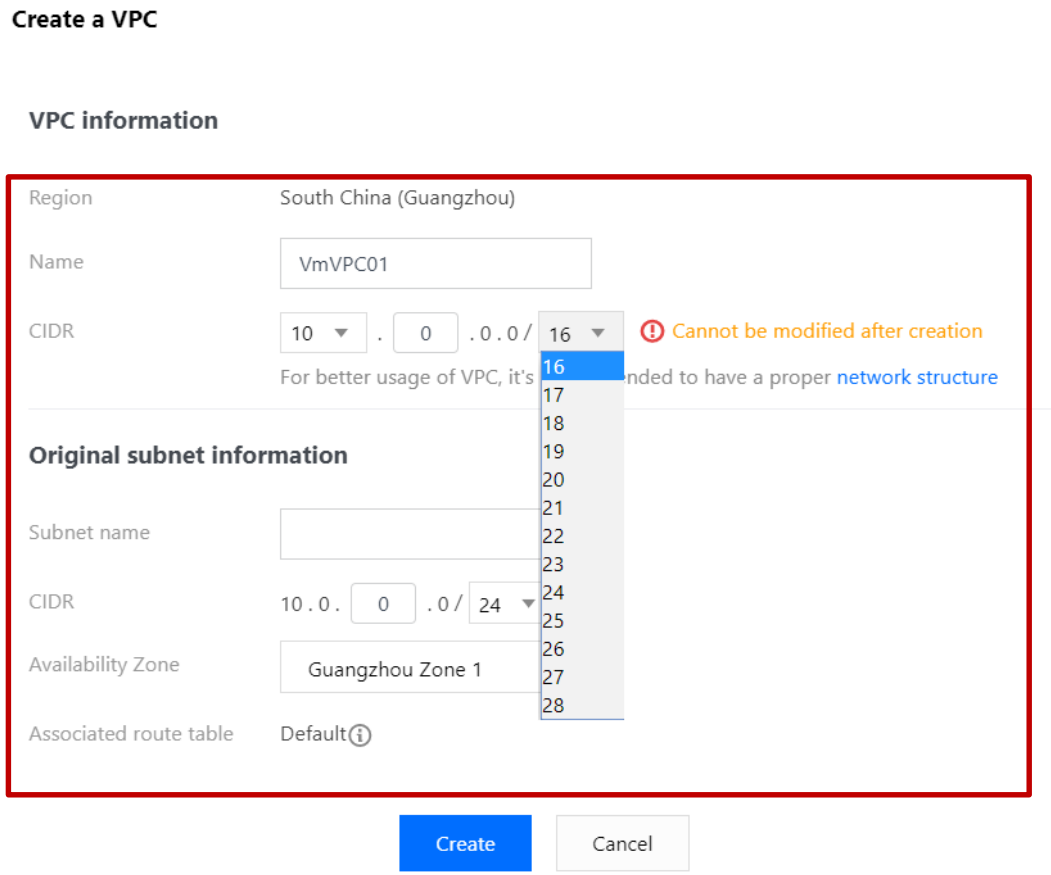


1.1 VPC


South China (Guangzhou)
ZONE A
CVM
CVM
Security Group A
Security Group B
Private Network CLB
Redis
TencentDB
Subnet A
ZONE B
CVM
Security Group C
Subnet B
Direct Connect Gateway
VPN Gateway
Route Table
NAT Gateway
Network ACL
User IDC
Direct Connect VPN access
Classiclink
Peering connection
Basic Network
VPC2
Public Gateway
EIP
VPC1
Flexible internet access
Internet
internet CLB

1.2 VPC CIDR Blocks

- **CIDR blocks:**
  - 10.0.0.0-10.255.255.255 (subnet mask 16-28)
  - 172.16.0.0-172.31.255.255 (subnet mask 16-28)
  - 192.168.0.0-192.168.255.255 (subnet mask 16-28)
- **Subnet:**
  - Cloud resources (e.g. CVM and CDB) need to be deployed on subnets.
  - Private IPs obtained through DHCP are not routable on the public network.
  - The number of available IPs per subnet is 2^n-3 (n is the subnet mask).



1.2 VPC CIDR Blocks - Subnetting

- **Subnetting**
  - IP address composition (binary): xxxx xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx

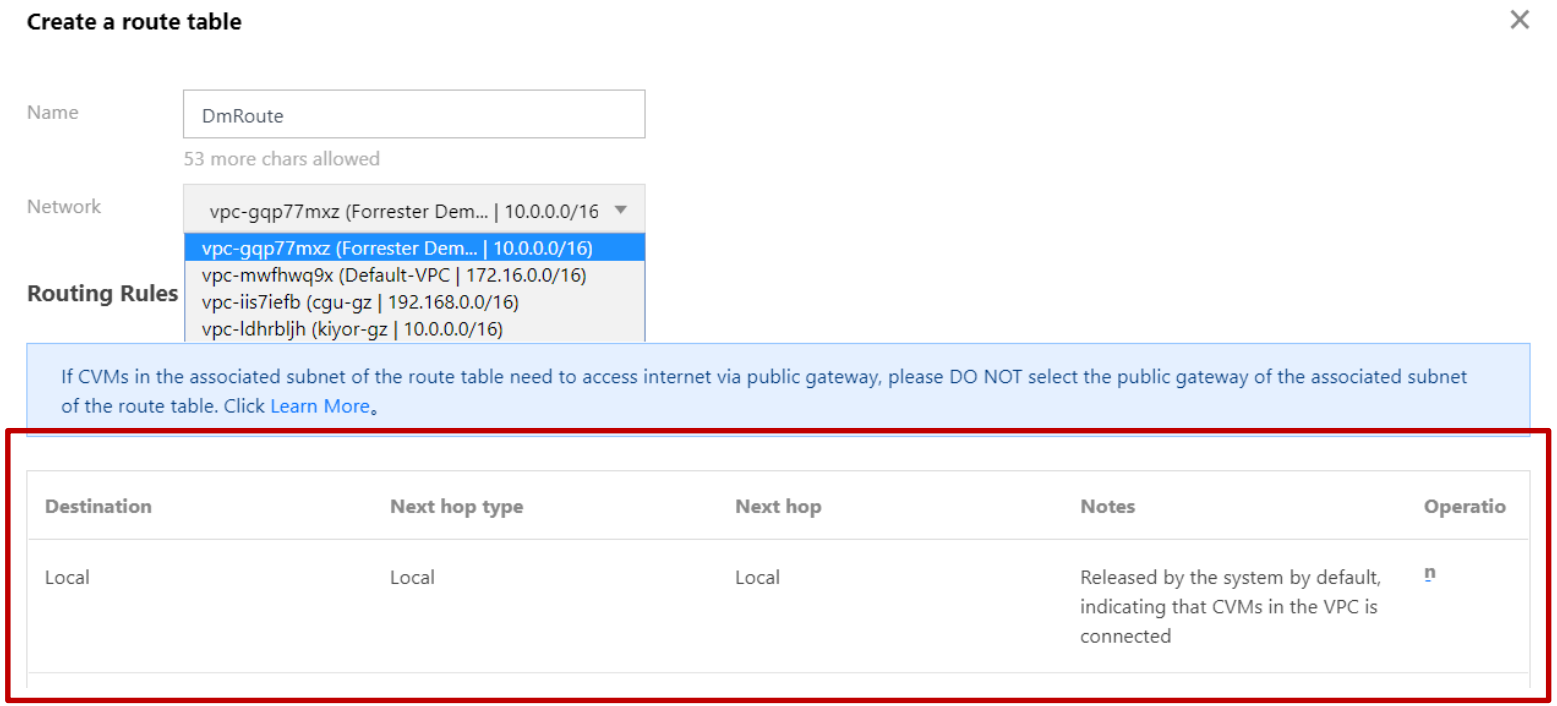
    Subnet location (mask 24) host bit
  - Subnetting: The number of subnet mask bits determines the number of available subnets and the number of host IP addresses. For example, if the subnet mask is n, the number of subnets will be 2^n, and the number of IP will be 2^(32-n)-3.
- **Example: 10.3.5.7/24**
  - Binary: 0000 1010. 0000 0011 . 0000 0101 . 0000 0111
  - Number of subnets: 2^24; number of hosts: 2^(32-24)-3
  - Network address: 10.3.5.0; broadcasting address: 10.3.5.255; gateway address (as configured)

1.3 VPC Route Table

- IP addresses in the same VPC network can communicate by default, but those in different VPC networks cannot communicate unless VPC peering is established and a route table is configured to facilitate traffic among VPCs and between VPCs and public networks.

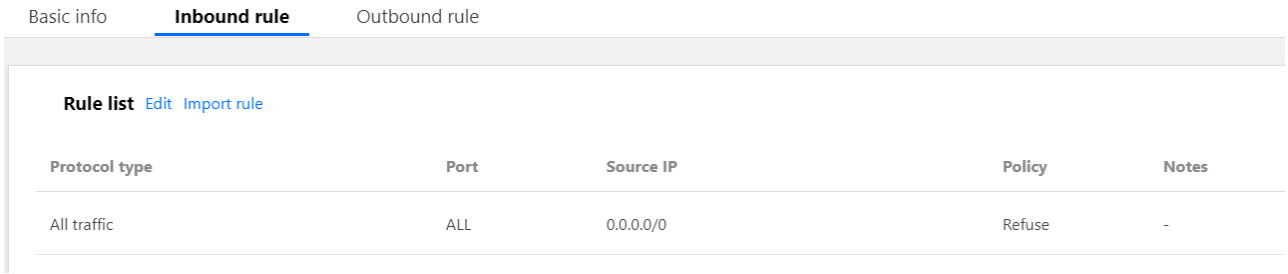
- **Type of route table:**
  - Default route table
  - Customized route tab

- **Routing policies**
  - Destination
  - Next hop type
  - Next hop

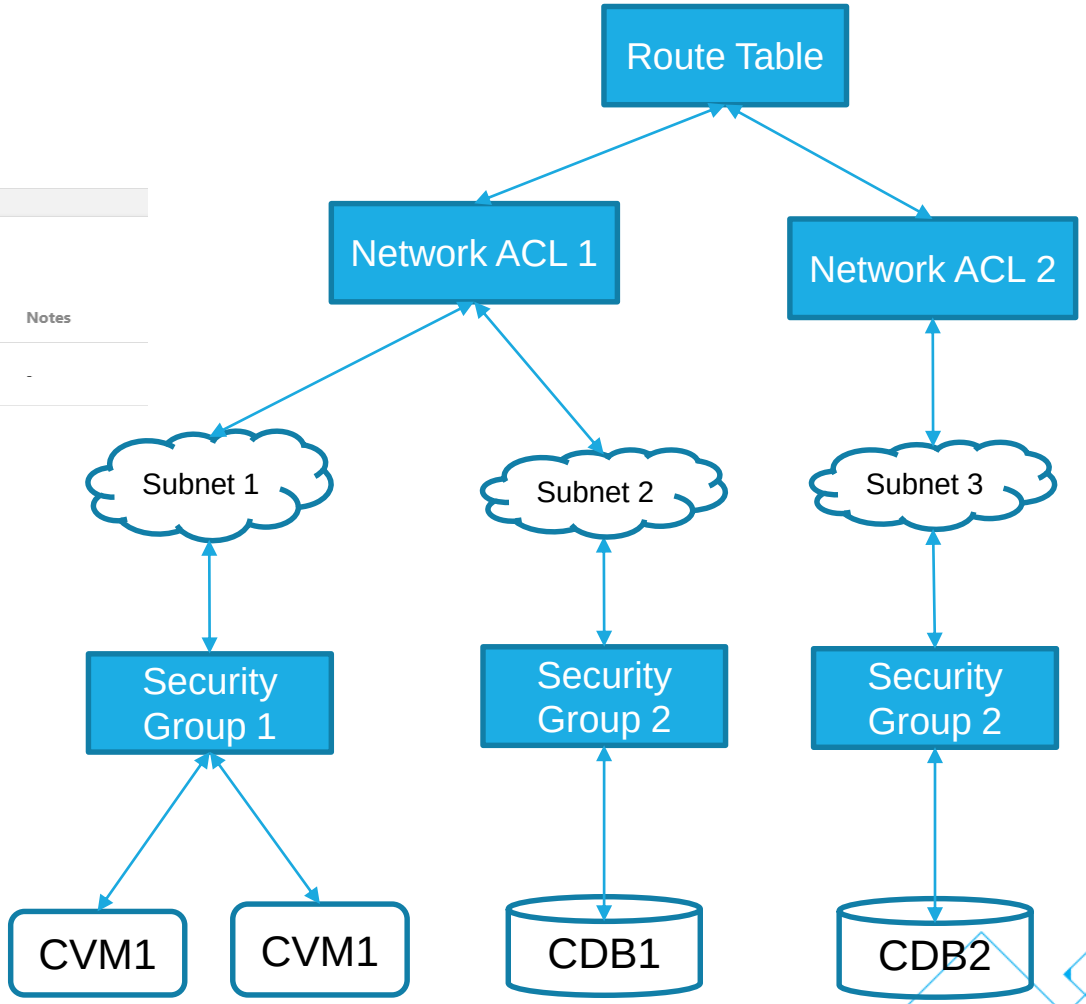


1.4 VPC Access Control

- **Network ACL:** Controls the inbound and outbound traffic of a subnet.



- **Security group**: Decides whether a port/ protocol accepts traffic.

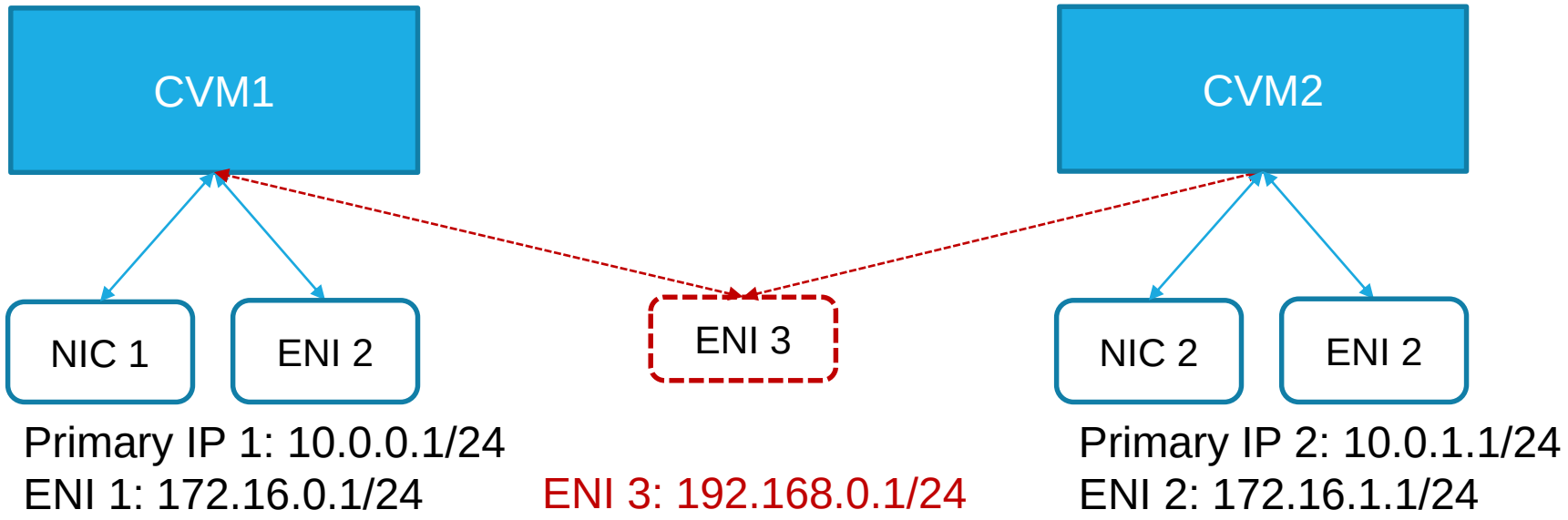


1.4 VPC Access Control - Security Groups and Network ACLs

Security Group	Network ACL
CVM instance-level traffic control (the first layer of defense)	Subnet-level traffic control (the second layer of defense)
Supports Allow and Deny rules	Supports Allow and Deny rules
Stateful: The returned data stream is automatically allowed and is not affected by any rules	Stateless: The returned data stream must be explicitly allowed by rules
Rules only apply to an instance if they are associated with the security group	Rules automatically apply to all CVM instances in the associated subnet. This can act as a backup defense if the instance is already associated with a security group

1.5 ENIs

- **Elastic Network Interface (ENI)**: An elastic network interface is assigned to a CVM instance in a VPC network and can freely migrate between CVM instances.
- **Advantages of ENIs:**
  - Multiple ENIs/ IP addresses
  - Network isolation
  - Flexible migration

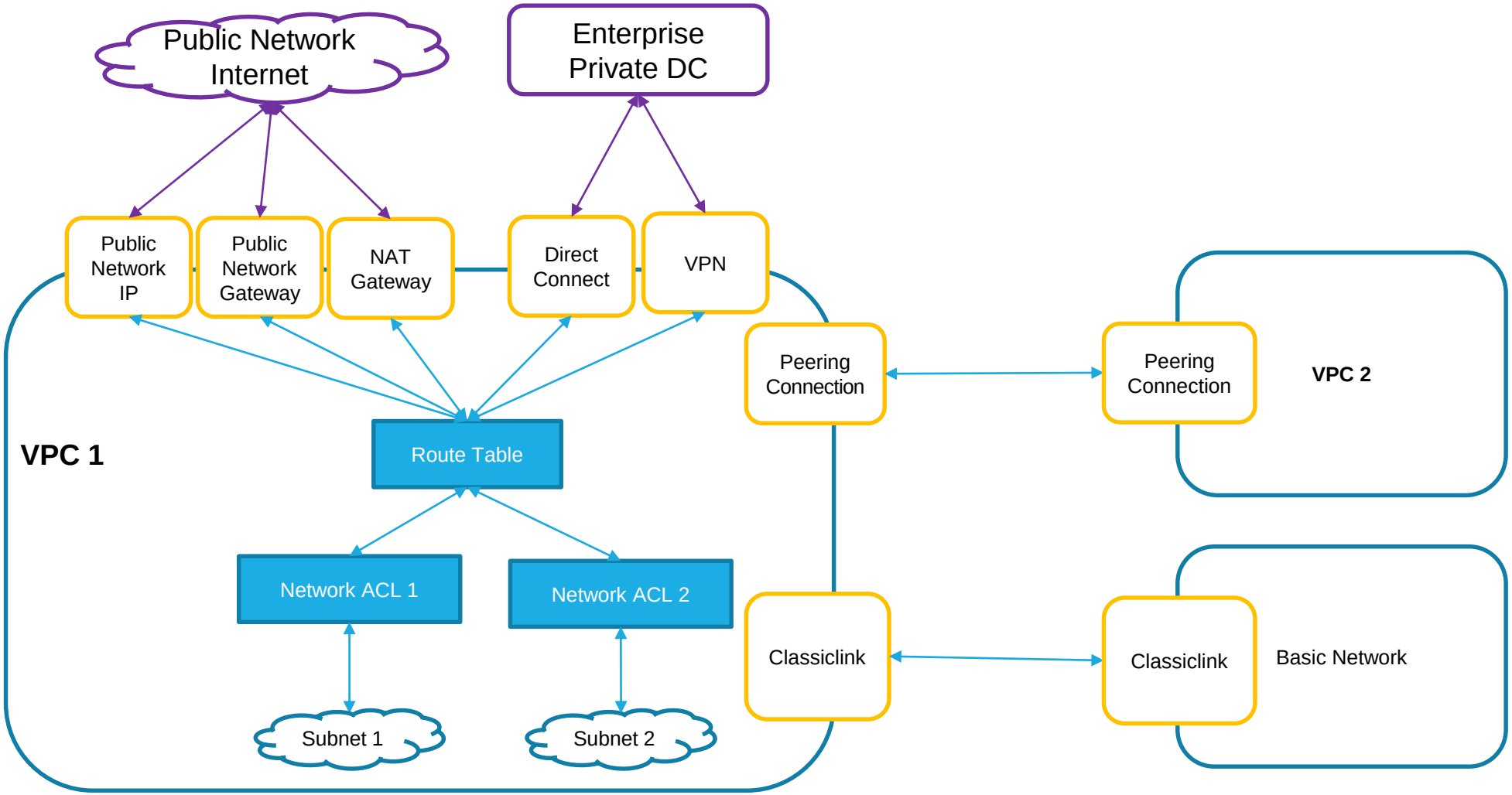


腾讯云

CONTENTS

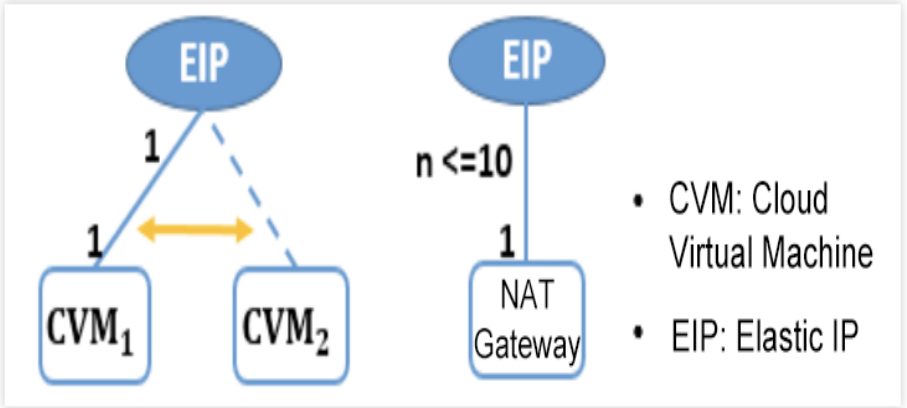
Chapter II Tencent Cloud Networking

2.1 Networking Products



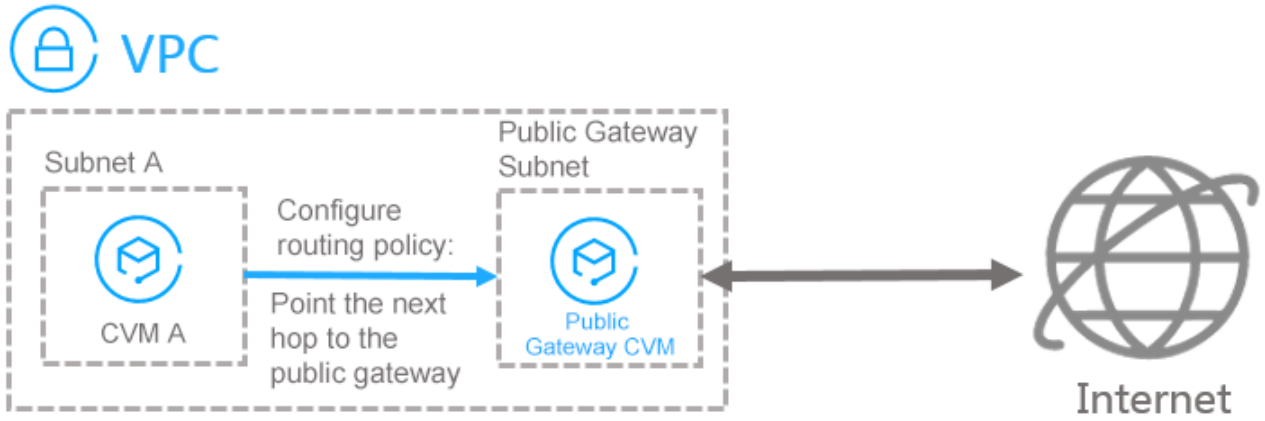
2.2 Public Network Access: EIP

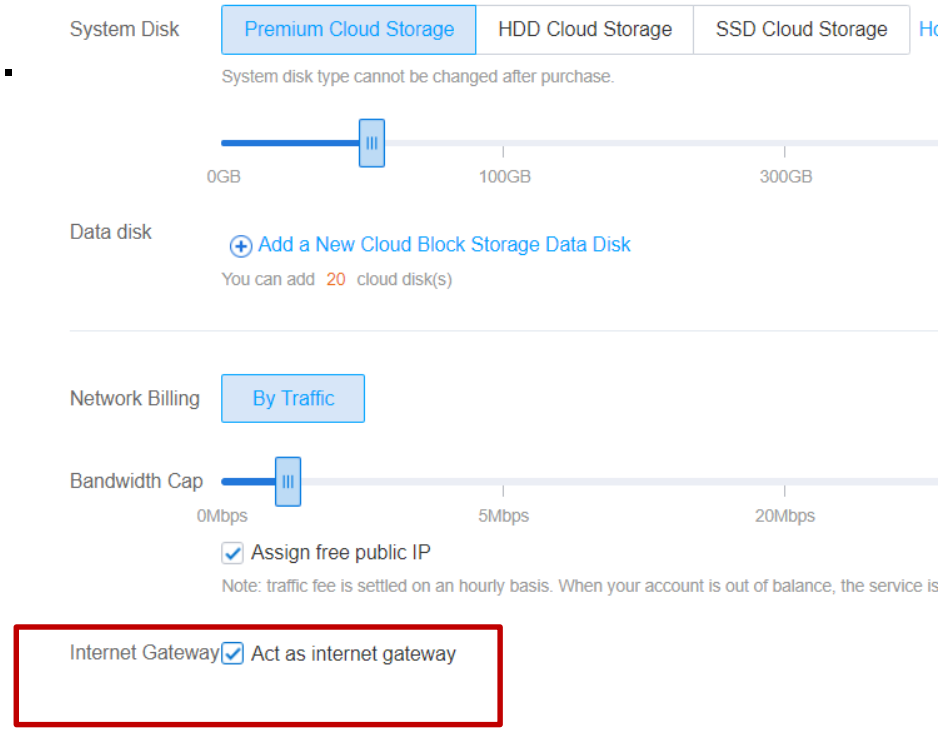
- A VPC network has private IP address in a range of your choice, For internet traffic, a public IP address must be assigned to the network.
  - **Classic public network IP:** This type of IP address is bound to a CVM instance and is not associated with an account. It is released immediately after unbinding and cannot be recovered.
  - **Elastic Public Network IP:** (Elastic IP, EIP)
    - ✓ An EIP is bound to the CVM or NAT Gateway.
    - ✓ It is associated with an account and therefore can be recovered and re-bound after unbinding.
    - ✓ It can be released via API/console or automatically released if the account becomes delinquent.



2.2 Public Network Access: Public Gateways

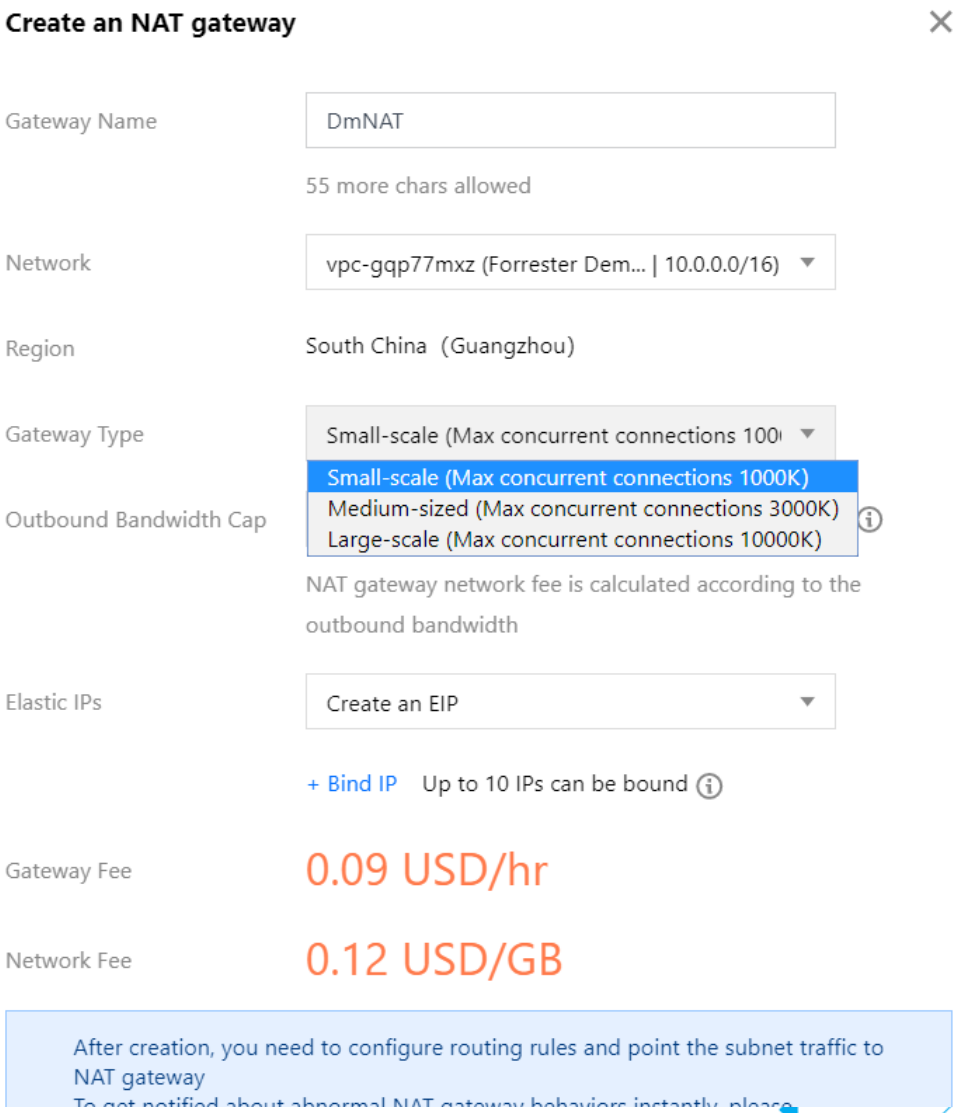
- A CVM instance can also use the internet gateway in a different subnets to access the public network, instead of an EIP.
- A internet gateway is a CVM instance that forwards traffic to and from the public network.
- The internet gateway must be designated as such when the CVM instance is purchased.
- A separate subnet gateway needs to be created.





2.2 Public Network Access: NAT Gateways

- **NAT Gateways**
  - Provides Internet access through IP address translation
  - SNAT (source network address translation)
  - DNAT (destination network address translation)
  - Gateway traffic control, traffic alerts, and shared bandwidth packages
- **Types of NAT Gateways**
  - Small (maximum concurrent connections: 1 million)
  - Medium (maximum concurrent connections: 3 million)
  - Large (maximum concurrent connections: 10 million)

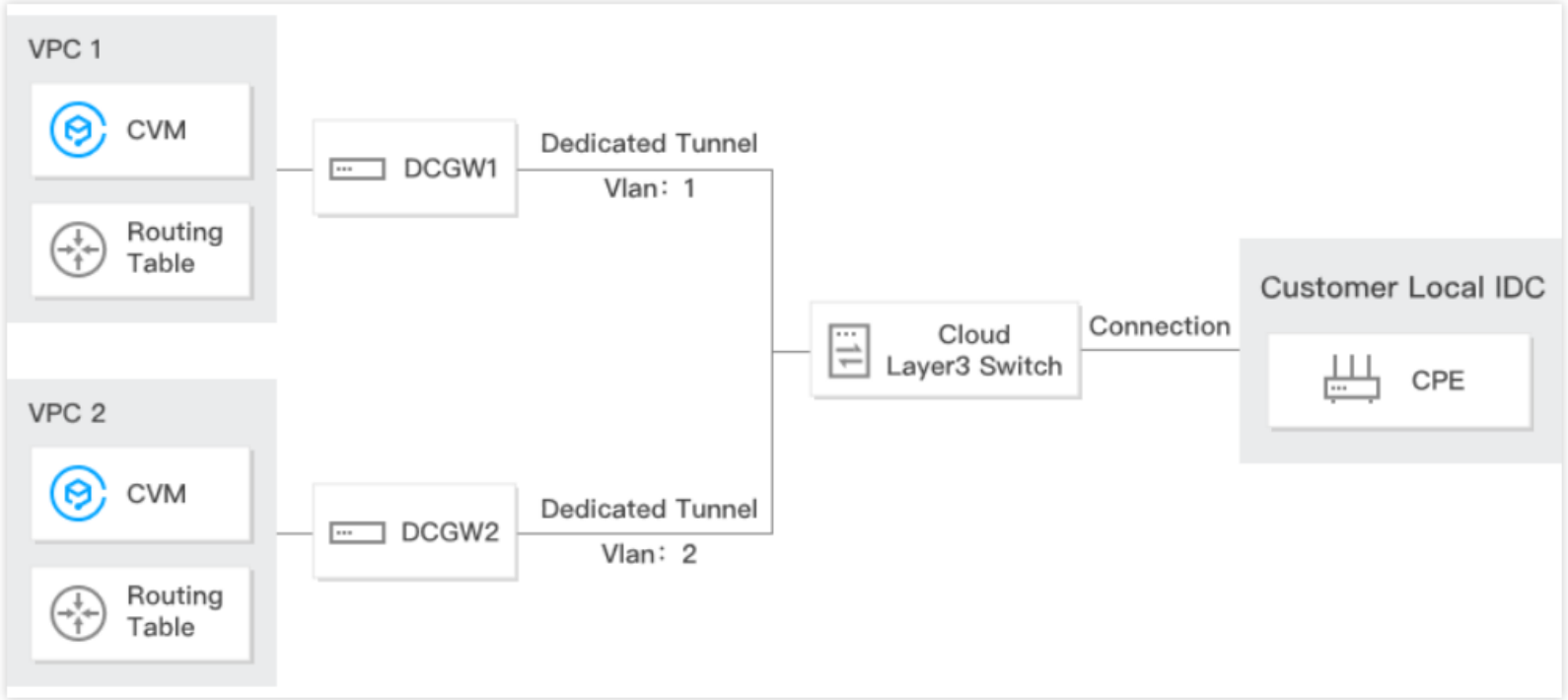


2.2 NAT Gateway vs. Public Gateway

Feature	NAT Gateway	Public Gateway
Availability	Dual-host hot backup and auto hot failover	Manual switching
Public network bandwidth	Up to 5 Gbps	Depends on CVM bandwidth
Public network IP	Up to 10 EIPs can be bound	One EIP or public IP
Public network speed limit	None	Depends on CVM speed limit
Maximum connections	10 million	500,000
Private IP	A private IP that does not occupy users' IP address quota	Occupies IP addresses in the subnet
Security groups	Not supported	Supported

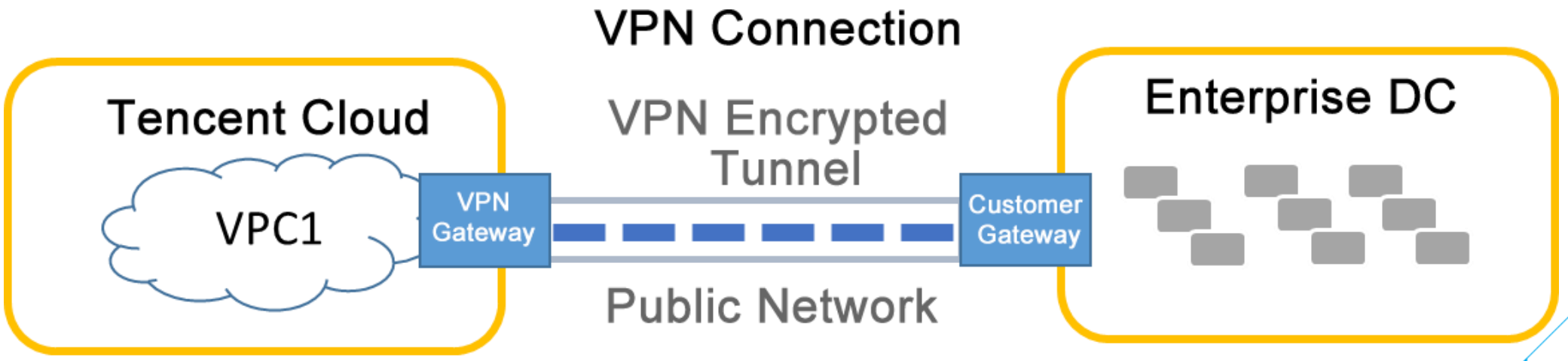
2.3 EDC: Direct Connect

- Direct Connect (DC) provides a physical connection completely isolated from the public network to connect an Enterprise Data Center (EDC) and Tencent Cloud.
- **Products**: Physical connection, Direct Connect, and Direct Connect Gateway
- **Product advantages:**
  - High network quality
  - Multi-region access
  - Multi-port, multi-protocol
  - Master/Slave access
- **Use cases:**
  - Hybrid clouds
  - Data center disaster recovery



2.3 EDC: VPN Connection

- VPN connections build secure and encrypted network tunnels over the Internet to allow traffic between EDCs and Tencent Cloud.
  - **Products:** VPN gateway, customer gateway, and VPN tunnel
  - **Product advantages:** Secure and reliable, rapid and elastic deployment, traffic monitoring, and traffic control
  - **Encrypted protocol:** IKE and IPsec

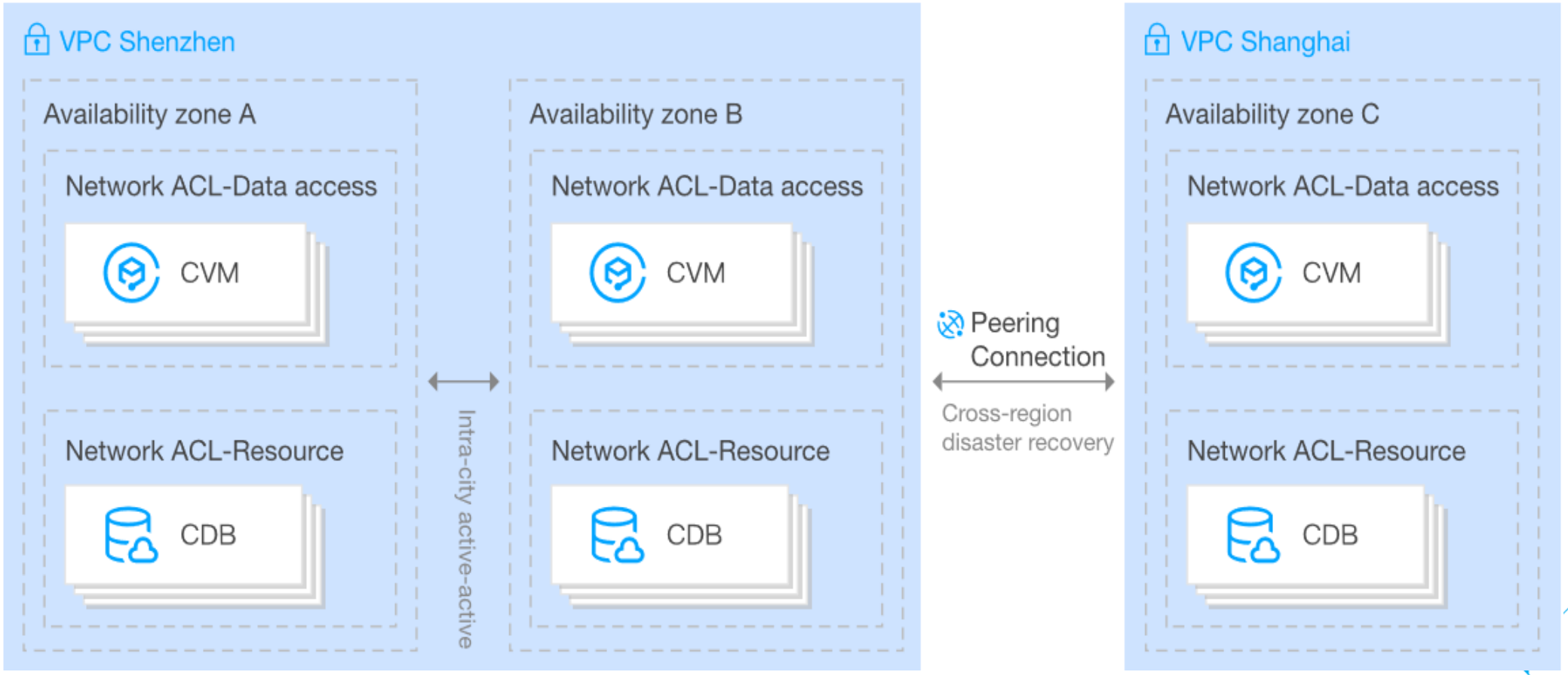


2.3 EDC: Direct Connect vs. VPN Connection

Properties	Direct Connect	VPN connection
Network quality	Latency: 99.5% assurance, fixed route configuration to avoid congestion or detours Bandwidth: Up to 10 Gbps/line, link redundancy	Latency: During peak Internet hours, detour paths may be used to avoid congestion Bandwidth: 100 Mbps/gateway, multiple VPN gateways can be configured
High reliability	Access and forwarding devices are deployed in distributed clusters with dual-link access for 99.95% availability	Dual-gateway hot backup; the gateway layer is highly available, but the Internet link is unreliable
Security	Dedicated connection for high security and no risk of data leaks Complies with security requirements for finance, government, and enterprises	IPsec and IKE-based encrypted transmission meet the security requirements for most network transmission scenarios
NAT support	Supported	Not supported currently
Deployment time	Weeks	Real-time

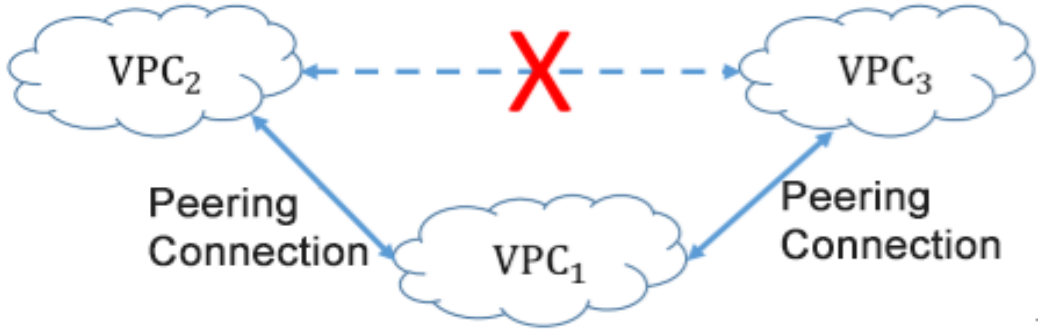
2.4 Peering Connection

- Peering Connection (PC) is a high-bandwidth and high-quality service for the interconnection of resources on cloud. It can connect multiple VPC networks, zones, accounts, and heterogeneous networks. Peering Connection is not transitive.



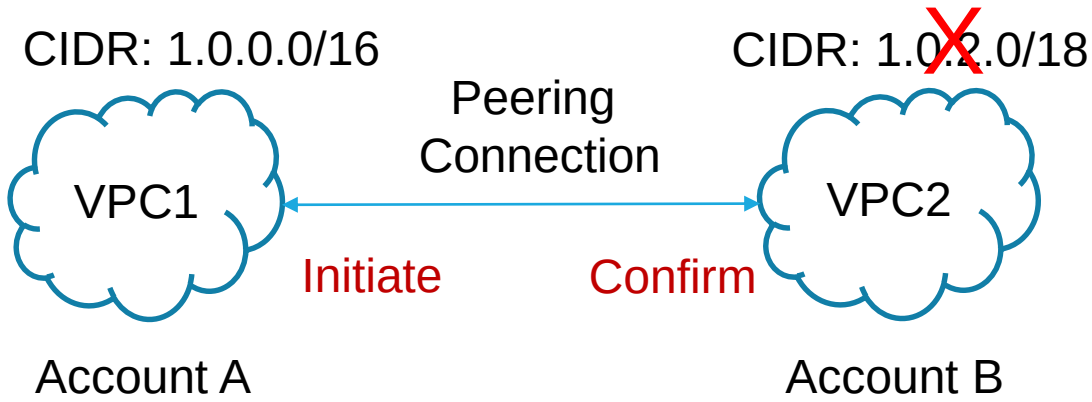
2.4 Limitations of Peering Connection

- VPC peering is not transitive.



- Cross-account peering connection requires confirmation from the receiving end.

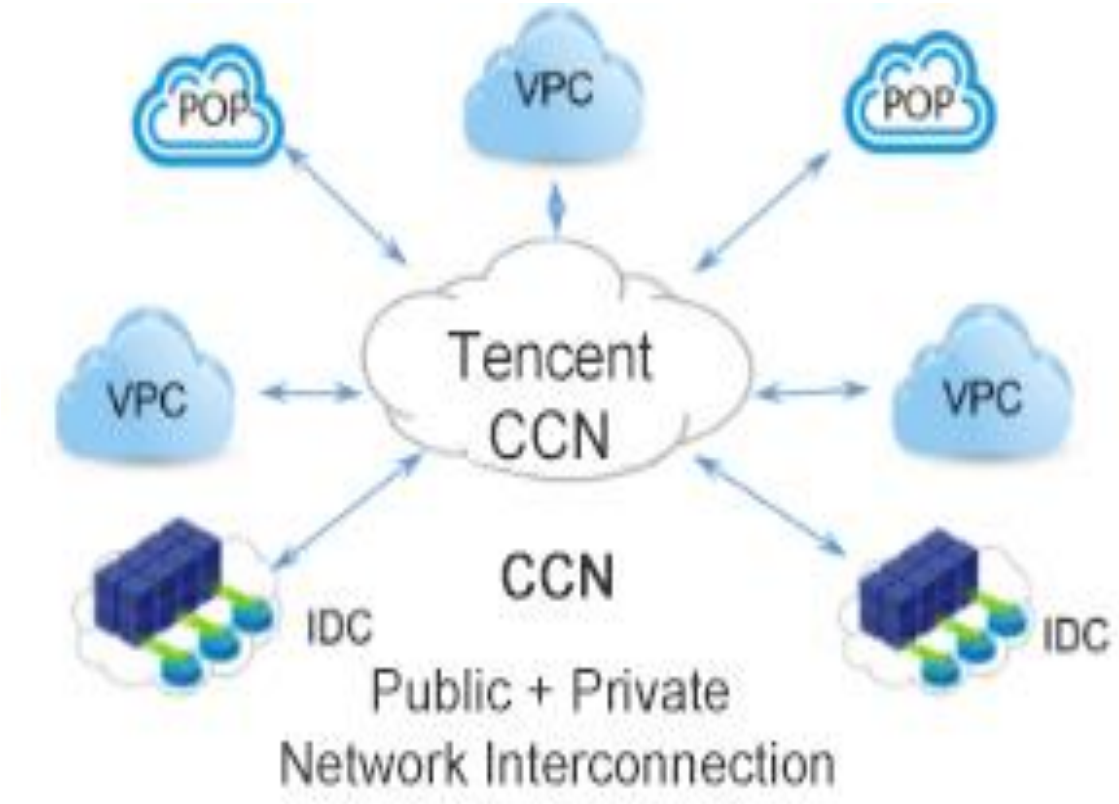
- The VPC CIDR blocks on both ends of the peering connection cannot overlap.



2.4 Peering Connection Comparison

Feature	Intra-region Peering Connection	Cross-region Peering Connection
Architecture	Based on the local private network of the Tencent Cloud region	Based on the internal cross-region MPLS network of Tencent Cloud
Maximum bandwidth	5 Gbps; BM: 1 Gbps	Up to 1 Gbps
Billing	Free	Daily network bandwidth charges
Link availability	99.50%	Platinum: 99.95%; gold: 99.50%; silver: 99.00%
Cross-account connection	Supported	Supported
Access permission	Access to all resources	Access to all resources
Limitations	CIDR blocks of both ends of a VPC peering connection cannot overlap. Peering connections is not transitive	CIDR blocks of both ends of a VPC peering connection cannot overlap. Connects one VPC to multiple VPCs (IP ranges cannot overlap)
Use case	VPC interconnection	Cross-region VPC interconnection 2-region 3-data center disaster recovery

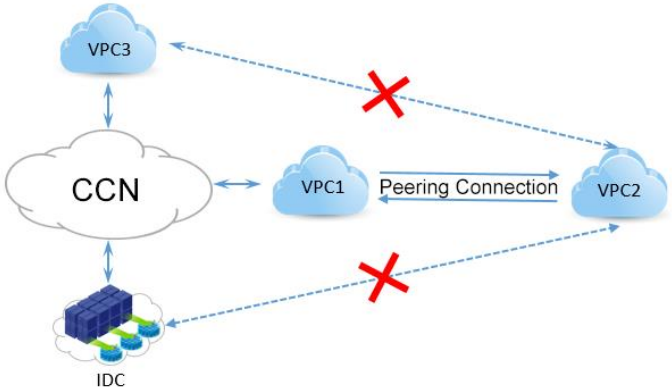
2.5 Cloud Connect Network (CCN)



- Public + Private network interconnection
- Smart learning and scheduling
- Auto routing delivery

2.5 Limitations of Cloud Connect Network

- Non-transitive Peering connection still applies, after joining CCN.

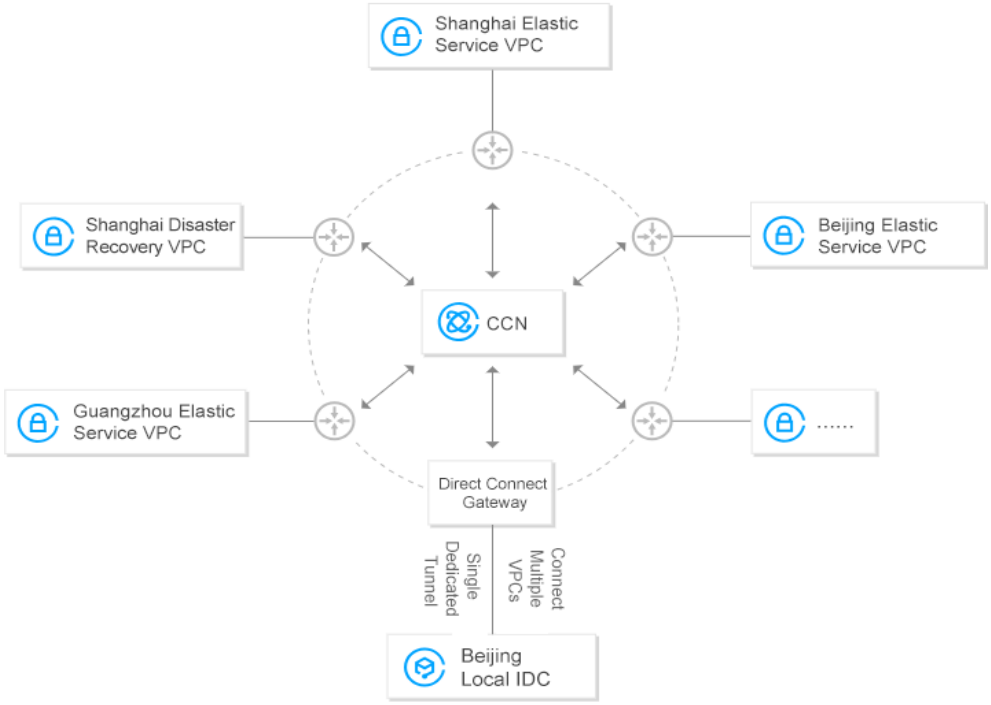


- **Limitations:**
  - Subnets with the same CIDR block in different VPC networks cannot interconnect.
  - If different VPC networks have overlapping CIDR block, their subnets can still interconnect, as long as these subnets do not have the same CIDR block.
  - If the CIDR blocks overlap, the routing entries of the VPC instance associated with Cloud Connect Network (CCN) first will take effect, while those associated later with CCN will be ignored.

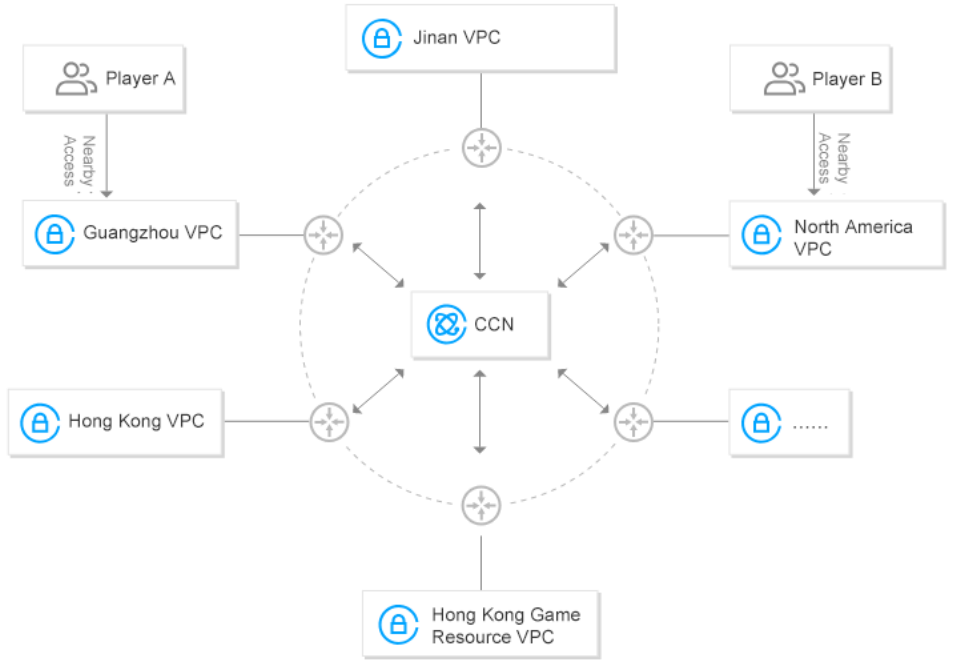
Resources	Limitations (quantity)
Number of CCN instances can create each account	5
Number of VPC instances can be bound to each CCN instance	25
Number of routing entries of each CCN instance	Unlimited

2.5 Cloud Connect Network: Hybrid Cloud

- Hybrid cloud: One-time integration, universal network interconnection



- Game acceleration: Global deployment, nearby access



腾讯云

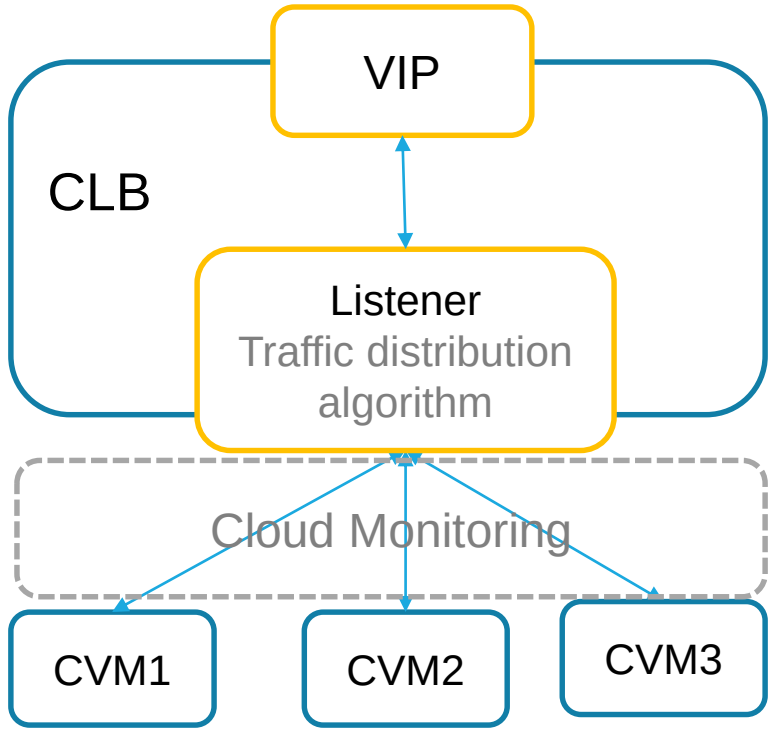
CONTENTS

Chapter III Tencent Cloud CLB

3.1 Cloud Load Balancer (CLB)

- **Cloud Load Balancer (CLB)** provides a secure and fast traffic distribution service.

- **How it works:**
  - **VIP:** a single IP address that handle requests
  - **CLB instances:** Monitor requests and distribute traffic through a listener
  - **Backend CVMs:** Process requests and return results
  - **Cloud Monitoring:** Monitors CVMs and synchronizes data to the listener



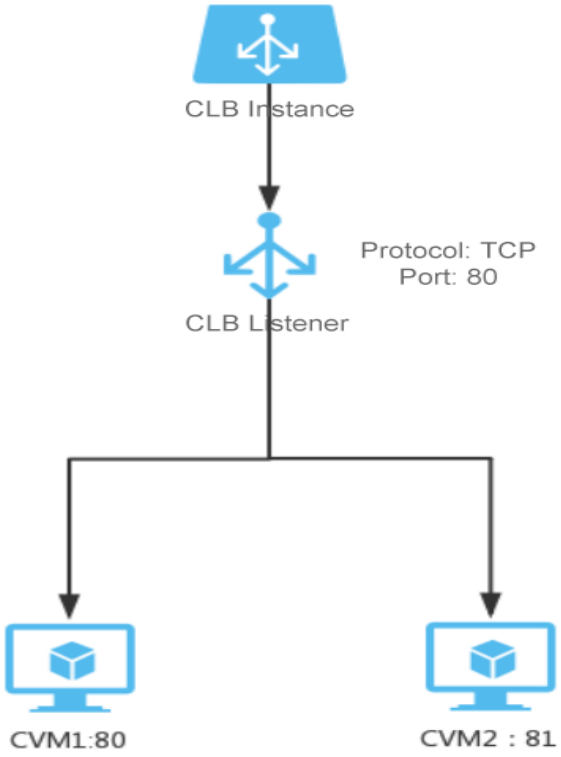
3.1 Advantages of CLB

- **High performance and high throughput**
  - A single cluster supports up to 120 million connections
  - Single cluster maximum bandwidth of 40Gb/s; processing capacity per second: 6 million
- **High availability:** 99.95%
  - Node health check and automatic switching
  - Cross-availability zone deployment and data center-level disaster recovery
- **Security**
  - Strictly isolates the traffic of each tenant
  - Provides active DDoS protection

3.2 Multi-protocol Forwarding

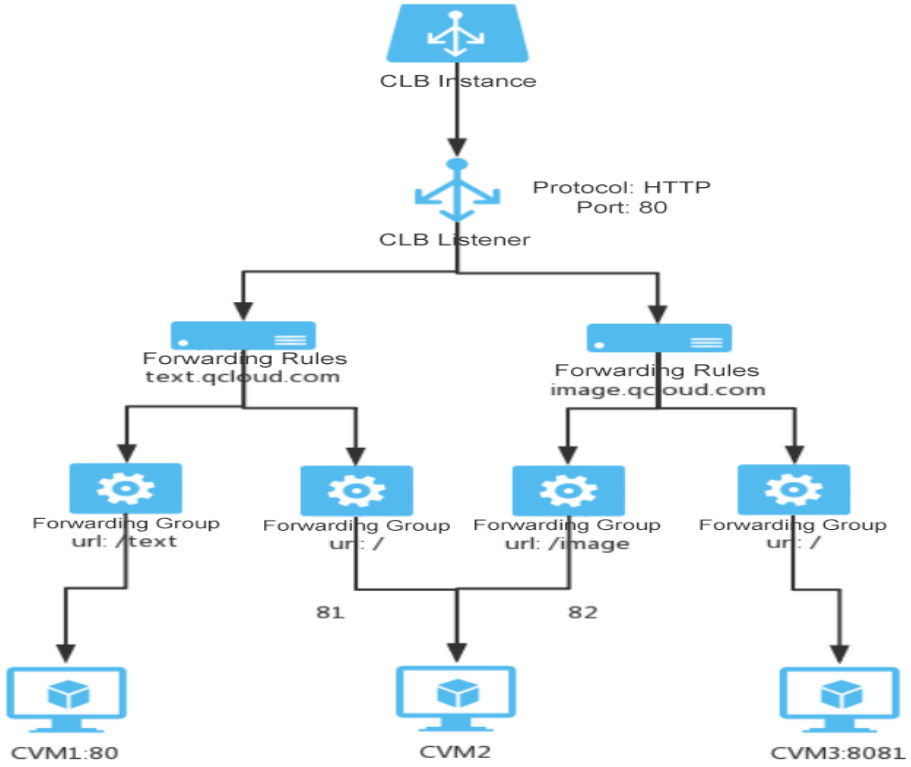
Layer-4 Cloud Load Balancer

Monitors TCP and UDP traffic, forwarding is based on port and VIP



Layer-7 Cloud Load Balancer

Monitors HTTP and HTTPS requests, distribution is based on content (domain name/URL)

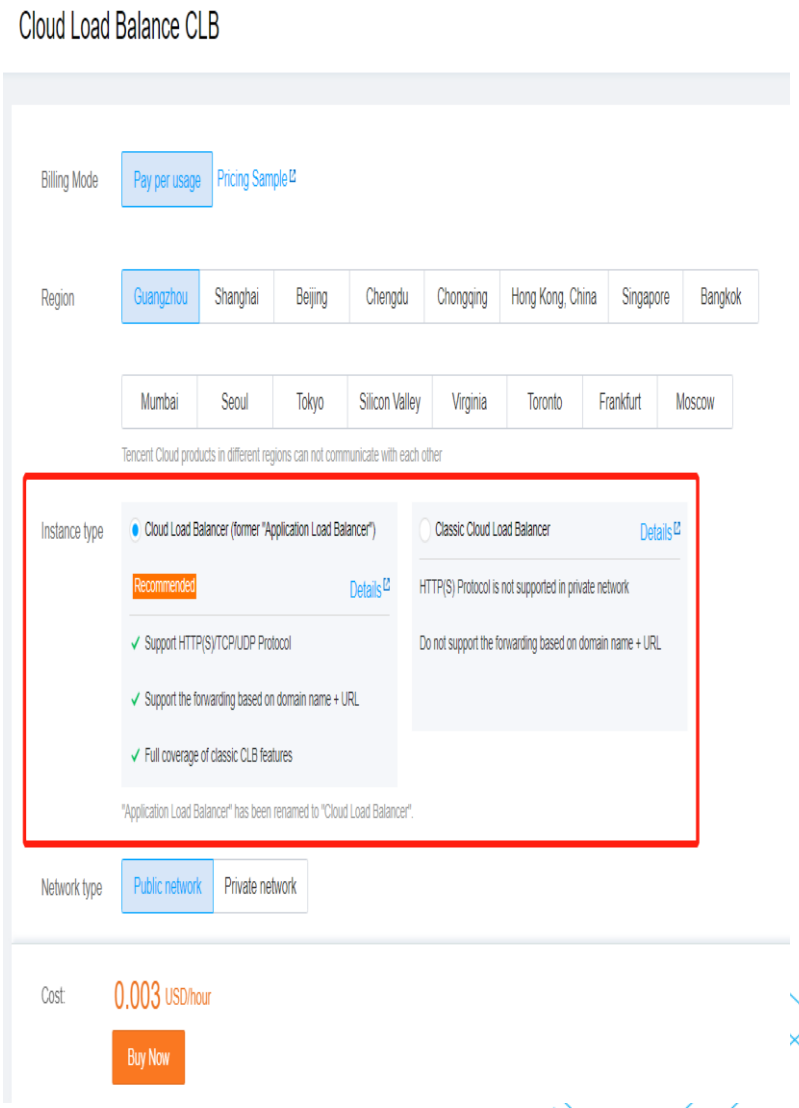


3.2 Traffic Distribution Algorithms

	Weighted Round Robin Scheduling	Weighted Least-Connection Scheduling	Source Hashing Scheduling
Notes	Schedules according to the number of new connections. Connections are assigned to the CVM with a higher weight first. Additional connections are processed by sequential polling.	Sets weights (wi) and the number of current connections (ci). Traffic is assigned to the CVM with the smallest ci/wi value.	Assigns network connections to the CVMs by looking up a statically assigned hash table by their source IP addresses.
Use cases	Suitable for short connections (HTTP) with similar service times.	Suitable for long connections with variable service times, e.g., FTP. A backend server is added.	Suitable for fixed assignment, session persistence, and TCP protocol without cookies.
Limitations	Not suitable for connections with highly variable service times.	Minimum connections and session persistence functions cannot be enabled at the same time.	Availability is affected if the number of CVMs changes or when a CVM is unavailable.

3.3 Types of CLB

Product type	Application CLB		Traditional CLB	
	inernet	Private Network	internet	Private Network
Layer-7 HTTP/HTTPS forwarding	✔	✔	✔	✘
Layer-4 TCP/UDP forwarding	✔	✔	✔	✔
HTTP/2 support	✔	✔	✔	✘
Algorithms	SHS (Layer-7) WRRS WLCS	SHS (Layer-7) WRRS WLCS	SHS (Layer-7) WRRS WLCS	WRRS
Session persistence	✔	✔	✔	✔
Health check	✔	✔	✔	✔
Custom forwarding: Domain name/URL	✔	✔	✘	✘
Forwarding to different backend ports	✔	✔	✘	✘
Rewrite support	✔	✘	✘	✘
Cross-region binding support	✔	✘	✘	✘
COS log storage	✔ (Layer-7)	✘	✔ (Layer-7)	✘



3.3 Public Network CLB vs. Private Network CLB

腾讯云

internet CLB
(public network access point)

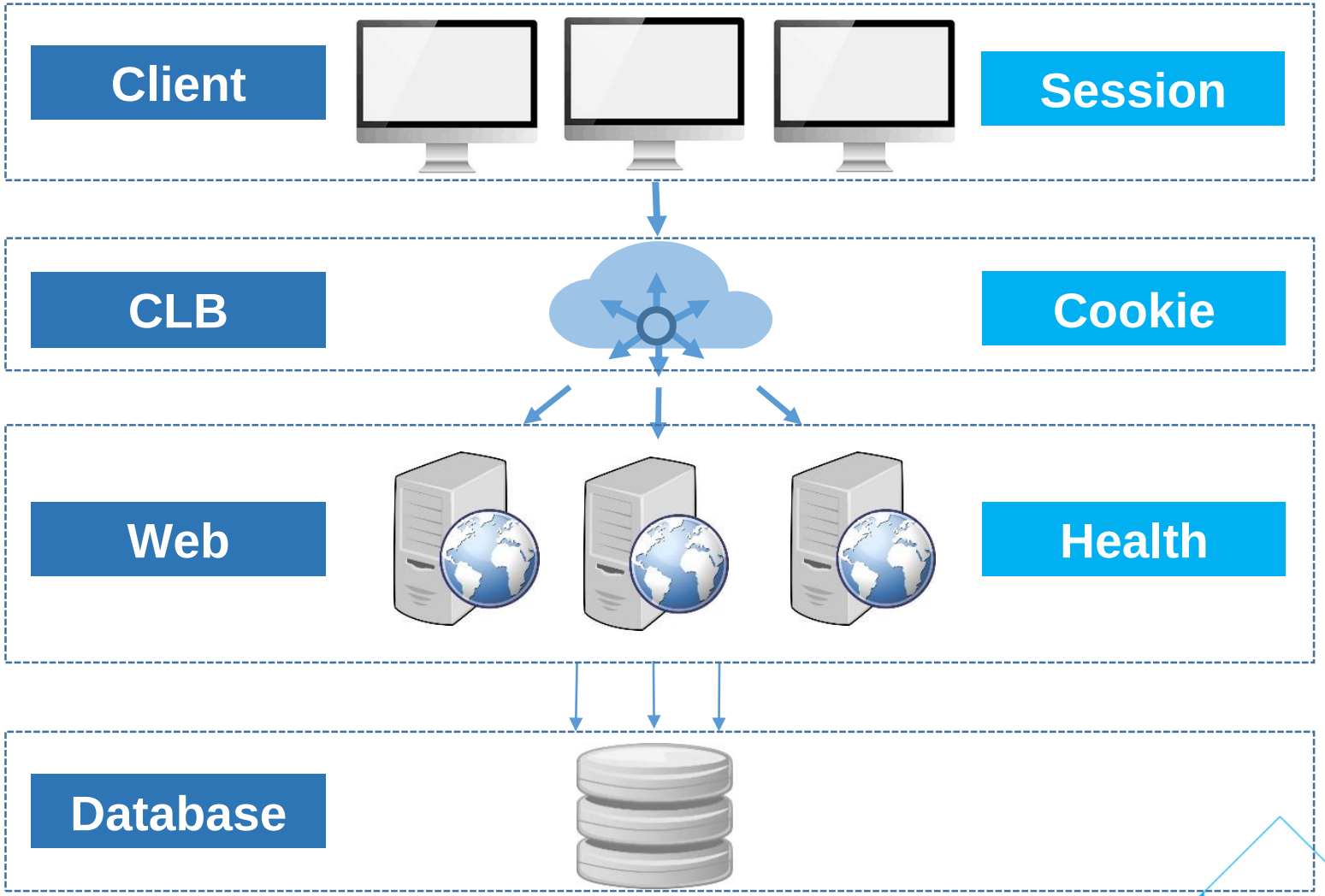
- Provides a unified public network access point
- Server fault tolerance and recovery
- Access to any ISPs nearby

Private Network CLB
(private network distribution)

- Distribution of private network access traffic
- Server fault tolerance and recovery
- IP blocking and transparent service

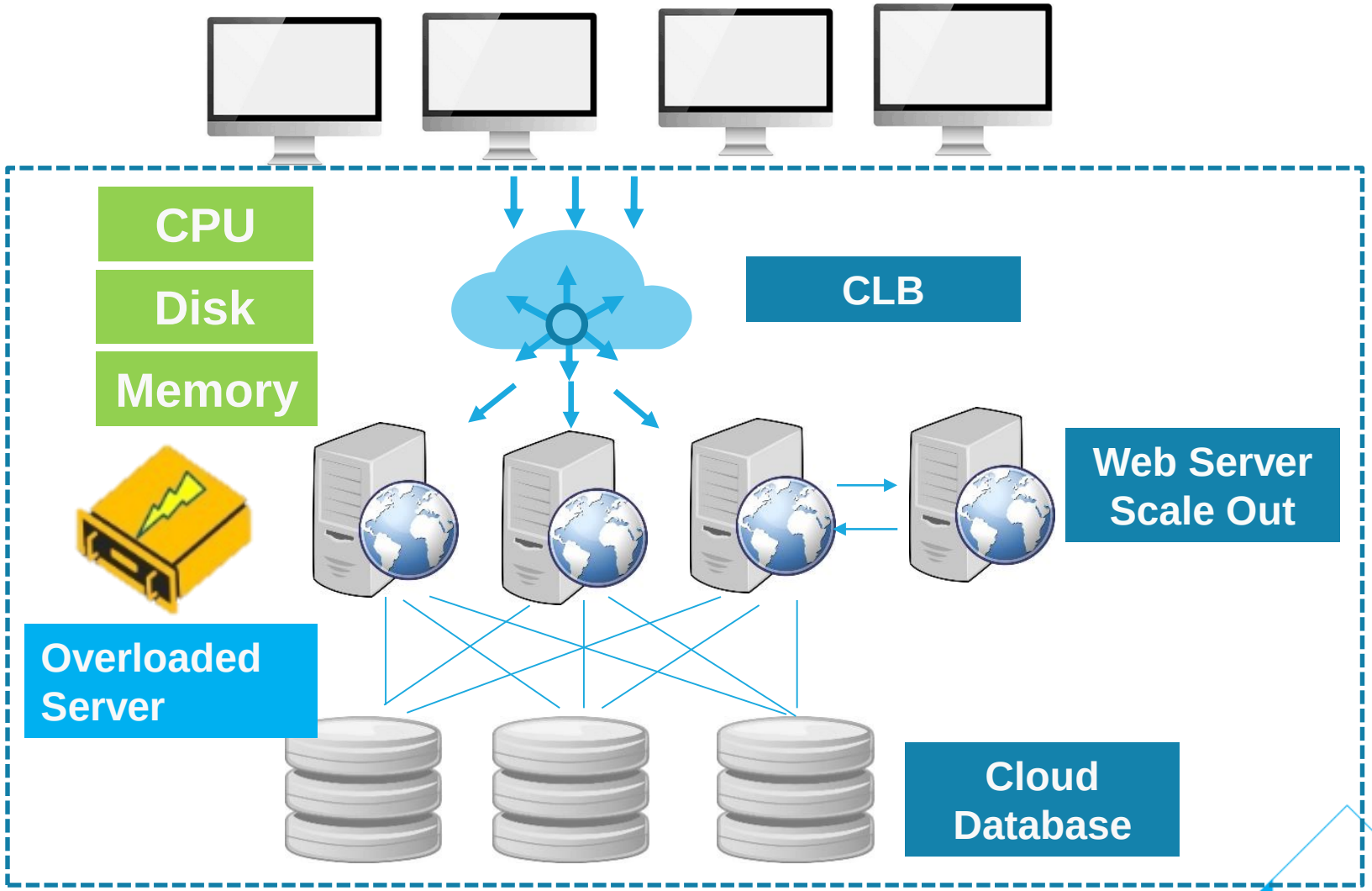
3.4 Use Case: Traffic Distribution

- Multiple access-layer web servers are virtualized into a high-performance and highly available access-layer service pool.



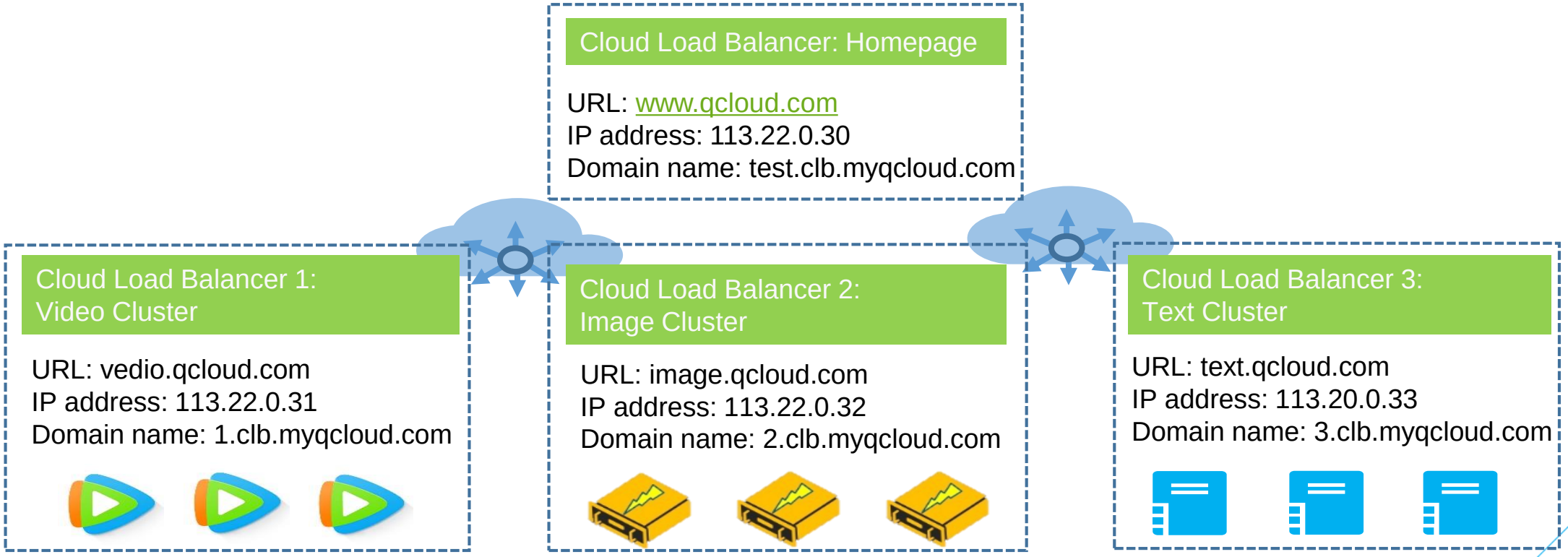
3.4 Use Case: Scaling Out

- An access-layer web server can scale in or out according to traffic volume.



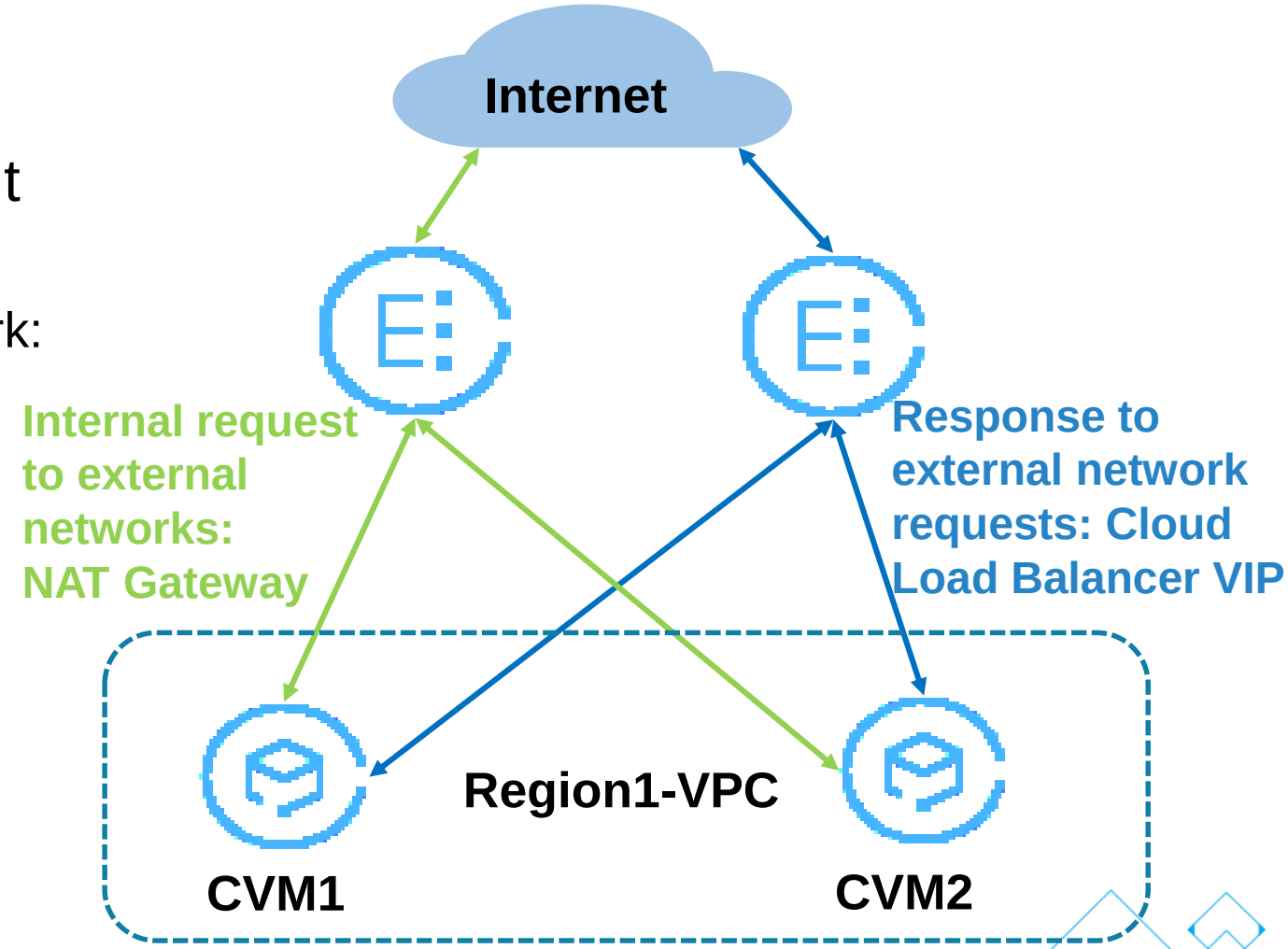
3.4 Use Case: Request Distribution

- Different types of traffic is distributed to the corresponding clusters through CLB and CDN according to requested resource types (text, image, or video) to achieve optimal performance and cost savings.



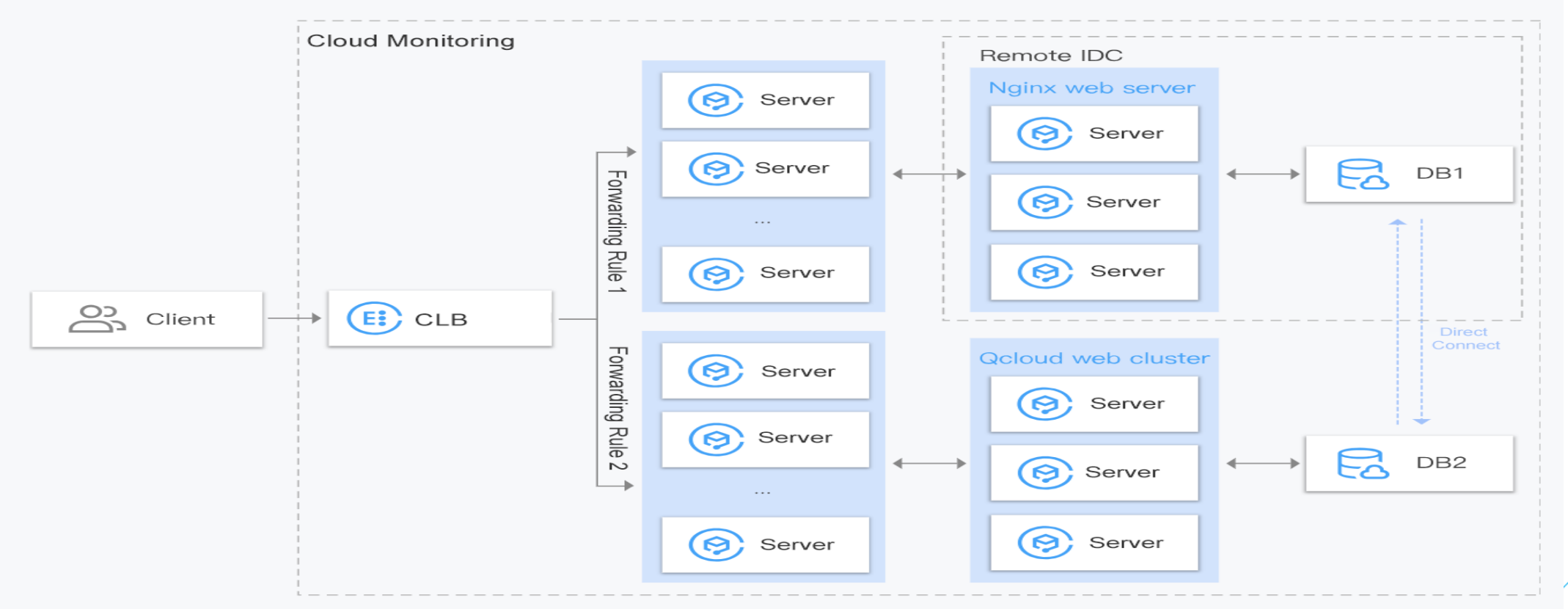
3.4 Use Case: Separation of Inbound and Outbound Traffic

- Requests that are initiated internally and external are handled differently and different rules apply.
  - Internal request to a public network: The NAT Gateway translates between private and public IP addresses.
  - Response to external network requests: CLB distributes traffic through and hides the backend servers.

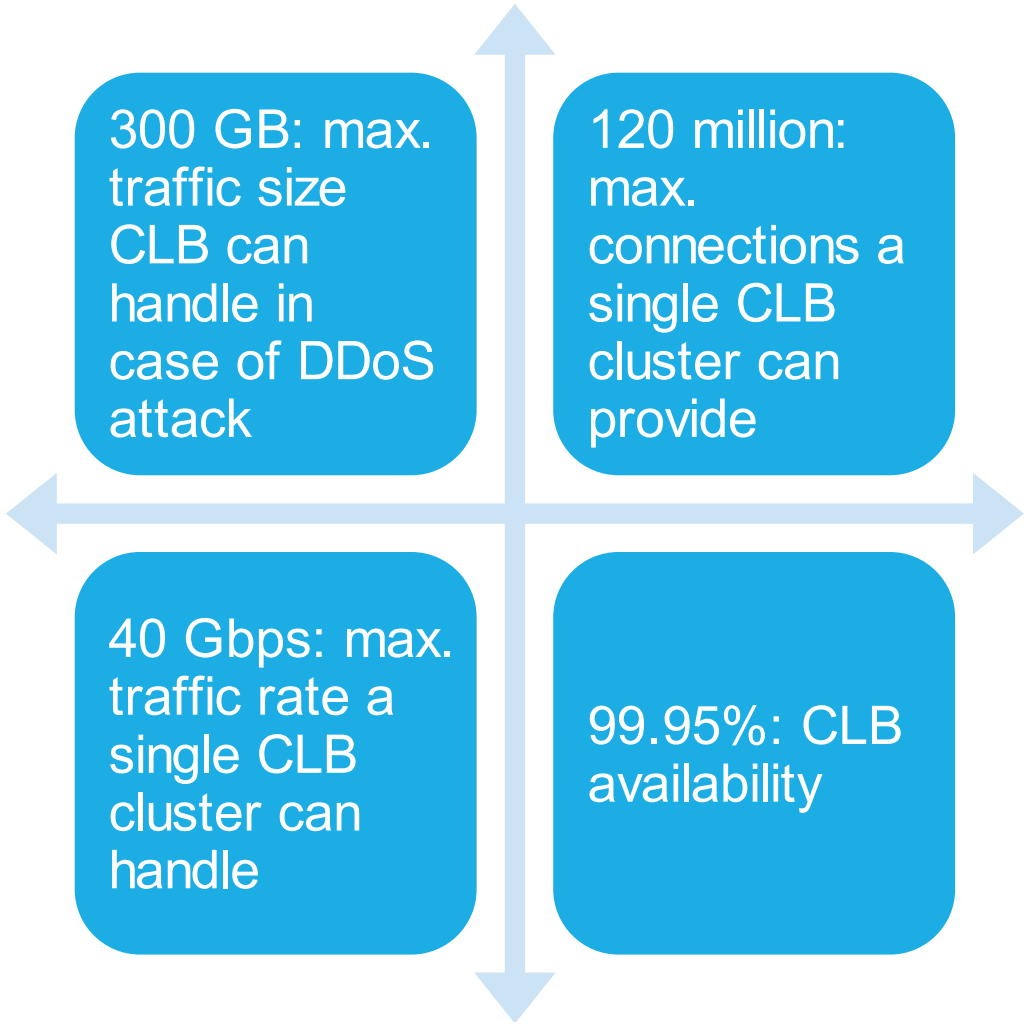


3.4 Use Case: Hybrid Cloud

- CLB distributes traffic to an EDC or public cloud.



3.5 CLB Indicators



CONTENTS

4.1 Billing Plans for Tencent Cloud Networking Products

Free Products:

- VPCs, subnets, routing tables, high-availability virtual IPs, network ACLs, security groups, Direct Connect gateways, VPN tunnels, peer gateways and network detection are free of charge.
- Intra-region communication over private network is free of charge. This
- means that communication among instances in different subnets does not incur bandwidth fees, and intra-region peering connections are free of charge too
- Tencent Cloud service prices in VPC and basic networks are the same. There are no surcharges such as CVM and TencentDB.
- Private network-based Cloud Load Balance (CLB) is free of charge.

Paid Products:

- Communication over public network incurs fees. For more information, see Public Network Billing Methods.
- NAT gateways, VPN gateways, CLB, and cross-region peering connections are paid services. See following slides for more information.

4.2 NAT Gateway Pricing

腾讯云

NAT Gateway fees consists of the gateway usage (billed hourly) and the Internet access traffic. See the table below for gateway fees. For details of traffic fees (in USD/hour), see the "Bill-by-traffic" section in Public Network Billing Methods.

Type	Mainland China	Singapore, Silicon Valley, Virginia, Frankfurt, Hong Kong (China), Korea, Russia & Japan	Mumbai	Toronto & Bangkok
Small (up to 1 million connections)	0.089	0.13	0.14	0.18
Medium (up to 3 million connections)	0.28	0.39	0.42	0.54
Large (up to 10 million connections)	0.89	1.3	0.14	0.18

For more information, please visit NAT Gateway Pricing Page.

4.3 VPN Connection Pricing

VPN tunnels and peer gateways are **free of charge**. VPN Gateway is pay-as-you-go.

Pay-as-you-go fees consists of the public network access traffic fees and an hourly gateway fee.

For detailed traffic fees, see "Bill-by-traffic" section in Public Network Billing Methods.

See the table below for gateway fees in USD/hour:

Region	Mainland China	Silicon Valley, Virginia, Frankfurt, Hong Kong (China), Korea & India	Toronto, Singapore & Thailand
Price	0.078	0.088	0.12

For more information, please visit VPN Connection Pricing Page.

4.4 Peering Connection Pricing

Intra-region peering connections are free of charge.

Cross-region peering connections incur fees that should be paid by the connection initiator.

Two billing methods are supported:

Billed by the daily peak*.

Billed by the monthly 95th percentile peak**.

***Billed by Daily Peak**

Calculation formula: Daily fees = bandwidth peak of the day * tiered unit price.

****Billed by the Monthly 95th Percentile Peak**

Calculation method: Monthly fees = the monthly 95th percentile bandwidth peak * valid day proportion * tiered unit price

For more information, please visit Peering Connection Pricing Page.

Course Summary

- This course covered the following topics:
  - Tencent Cloud VPC: CIDR blocks, route tables, security groups, network ACLs, and ENIs
  - Tencent Cloud networking: EIP, public gateways, NAT gateways, Direct Connect, VPN connection, Peering Connection, and Cloud Connect Network
  - Tencent Cloud CLB: Forwarding mechanism, traffic distribution, CLB types, and use cases
  - Billing plans for Tencent Cloud networking products

Thank you