
HUAWEI
Building a Fully Connected, Intelligent World
Huawei Cloud Landing Zone Workshop

# Why we need Huawei Cloud Landing Zone?

## Security controls

Different controls for different types of application

## Boundary & Isolation

Limit a blast radius and reduce threats to affect others

## Manage multiple developers/teams

Reduce team interferences

## Data isolation

Control and limit access to data. Complying with PDPA & GDPR guideline

## Billing & Quota allocation

Clear visibility on resource spending and able to allocate the right amount of budget per product

# What we often hear from the customer…

I don’t know how many accounts/ VPCs I need

I need to consider isolating production and non-production

I need to validate all services before using them

I need centralized resource sharing

I need separated environment for sandbox purpose

I need dedicated auditor to access multiple accounts

We need charge back or show back capability

I need to understand the spending for each application

I have different business units with different processes.

**5 things to think about…?**

1. **Account Strategy** – How many accounts we need and Why we need them?
2. **VPC & Networking Design** – How many VPCs? How large is CIDR? What about the Connectivity?
3. **User Access Management** – How our team should be accessing the console? Do we need to make any API calls and who needs it (services or human?)?
4. **Security Controls** – What security controls we should put in? What to be restricted, monitored, alerts, and how to collect audit logs? Do we need extra tools?
5. **Governance Controls** – What services are permitted, how are they secured, controlled and audited

# Huawei Cloud Landing Zone

Account Structure & Enterprise Center

# What is an HUAWEI CLOUD (HWC) Account?

## Administrative Boundary

- All access and rights in an account are governed by the permissioned created and managed within the account
- Includes users, groups, applications and other externally federated access methods via roles
- Access is initially managed by the Enterprise Administrator account

## Resource Containment

- Certain resources created within an account are limited to that specific account, they cannot span multiple accounts, e.g. VPC, but may be accessible between accounts
- Resources cannot dynamically migrate from one account to another
- HWC resources have hard and soft limits by account; and within an account can affect each other

## Billing Entity

- Billing and Financial detail, including currency billing country are defined and controlled by account
- Reserved Instances capacity is allocated to an account
- Account balance, Credit Limit and Cash Coupons at an account level

# Understand the business needs and drivers

There are multiple reasons for **segmenting accounts** (or VPCs), including:

## Environmental

- Separation between development, test and production for security, governance or regulatory reason, e.g. PCI Workload

## Financial

- Provide cost visibility, accountability or control on a per account basis; this may also be related to a line of business

## Business

- Delegated control to particular business unit to be able leverage HWC platform within pre-defined governance framework

## Workload

- Segregation of public or private facing services, differing risk profiles, data classification, consumer of service etc.

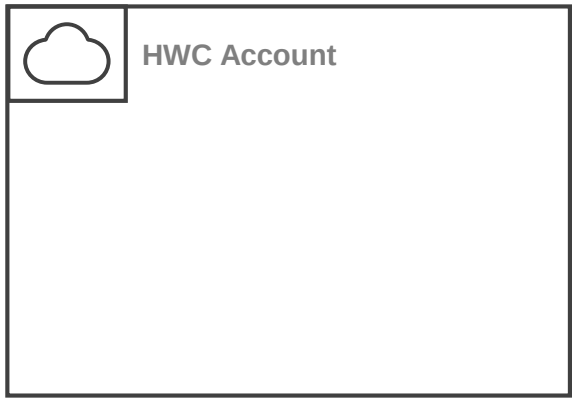
# Consideration points

There are multiple viewpoints to consider when deciding **account structure**:

| Financial | Business | Governance | Operational |
| --- | --- | --- | --- |
| How resource utilisation and consumption is measured, reported and re-charged | Service provider model, M&A possibilities, financial responsibility model, autonomy | What services are permitted, how are they secured, controlled and audited | Operating model, operational integration, networking, HWC quotas |

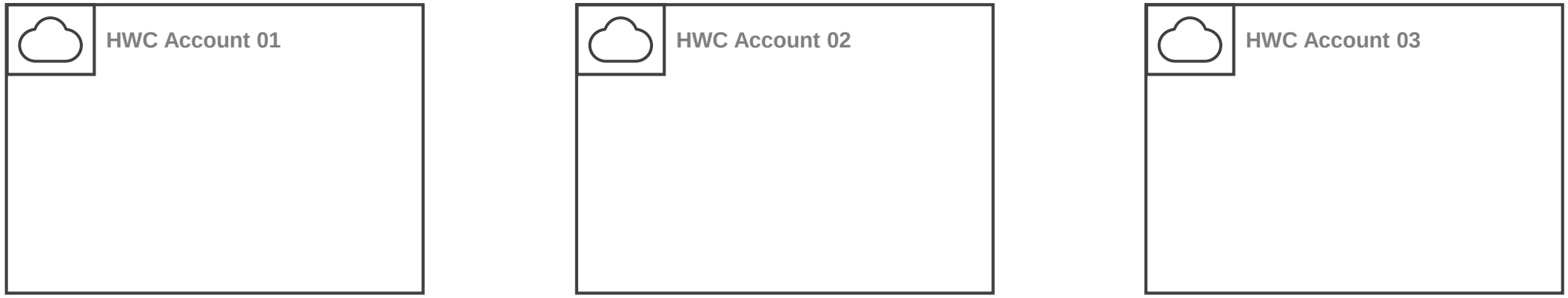
- ✓ Have this conversation in both directions to find the right balance
- ✓ **But, start with a pattern and iterate as customer needs evolve!**

# Account Pattern – Single Account




- Simple operating model, suitable for small operations team only
- Large blast radius for changes, increasing risk, reducing velocity of change
- Drives complex security controls to be effective using complex IAM policies
- Hard to delegate autonomy to multiple businesses, stifles innovation
- Quota limitation of resources being allowed for each account.
- Hard to provide clear financial visibility

# Account Pattern – Multiple Accounts




- Operating model becomes important consideration, multiple service providers, delegated autonomy or requires automation across accounts
- Allows for independent change and innovation
- Allows for more specific security posture, but requires more governance oversight
- Provides financial isolation and reporting, everyone pays what they use
- No way to leverage consolidated billing payment and accounting management

# Account Structure – Master Organization Account

- Only use for managing Organization policies, members and billing
- Required **Enterprise Center** to be enabled on the account
- Enables these below capabilities;
  - Manage multiple accounts
  - Consolidate billing from multiple accounts
  - Allocate quotas to each account members
  - Control resources with policies on the account level
  - Create Enterprise Project to control resources within the account with IAM policy

# Account Structure – Shared Services Account

- Provide common infrastructure or services that shares among workloads
- Host several functions or services that are commonly used by the workloads
  - DNS
  - Active Directory
  - NTP servers
- Leverage VPC peering or VPC Endpoint to connect with different components

# Account Structure – Network Operation Account

- A touch point for all the incoming and outgoing traffic
- Centrally manage all network components
  - 3rd Party Firewall
  - 3rd Party IPS/IDS
  - Cloud Connect
  - Direct Connect
  - VPN
  - NAT Gateway
- Sometime it can be combined with Shared Service account due to small number of people in the team and they wear multiple hats in the same time

# Account Structure – Centralized Identity Access Management Account

- A landing area for IAM user who needs to access another account (Cross-account role)
- Centrally manage other IAM user, user groups, permissions and agency from this account by using Infra-as-Code to assist

# Account Structure – Security Operation Account

- Host several security functions or services that are commonly used by security teams:
  - Collect security logs in centralized location
  - 3rd Party VA Scanning tools
  - 3rd Party Penetration tools
  - Integrates with other SIEMs from a single location

# Account Structure – Product Development Account

- For general product development and hosting
- Separate HUAWEI CLOUD account per environment
- The customer should define account structure based on their requirements
- Security Operation & Logging is separated with specific security user group in the account to give security personal the control over security services
- Below are example;
  - **Scenario 1 – Simple Product Account Structure**
    - Non-Production Account (Dev, QA, Staging)
    - Production Account
  - **Scenario 2 – More control Account Structure**
    - Development Account (Dev/QA)
    - Staging Account (Production-like)
    - Production Account

# Account Structure – Regulated Product Account

- For specific regulated workload that requires a total control to reduce the impact with another products such as PCI-DSS, PCI-3DS, HIPPA workload
- Sometime creates additional requirements for common infrastructure accounts because it has to separate the traffic for auditing with less effort

# Account Structure – Sandbox & Other Account

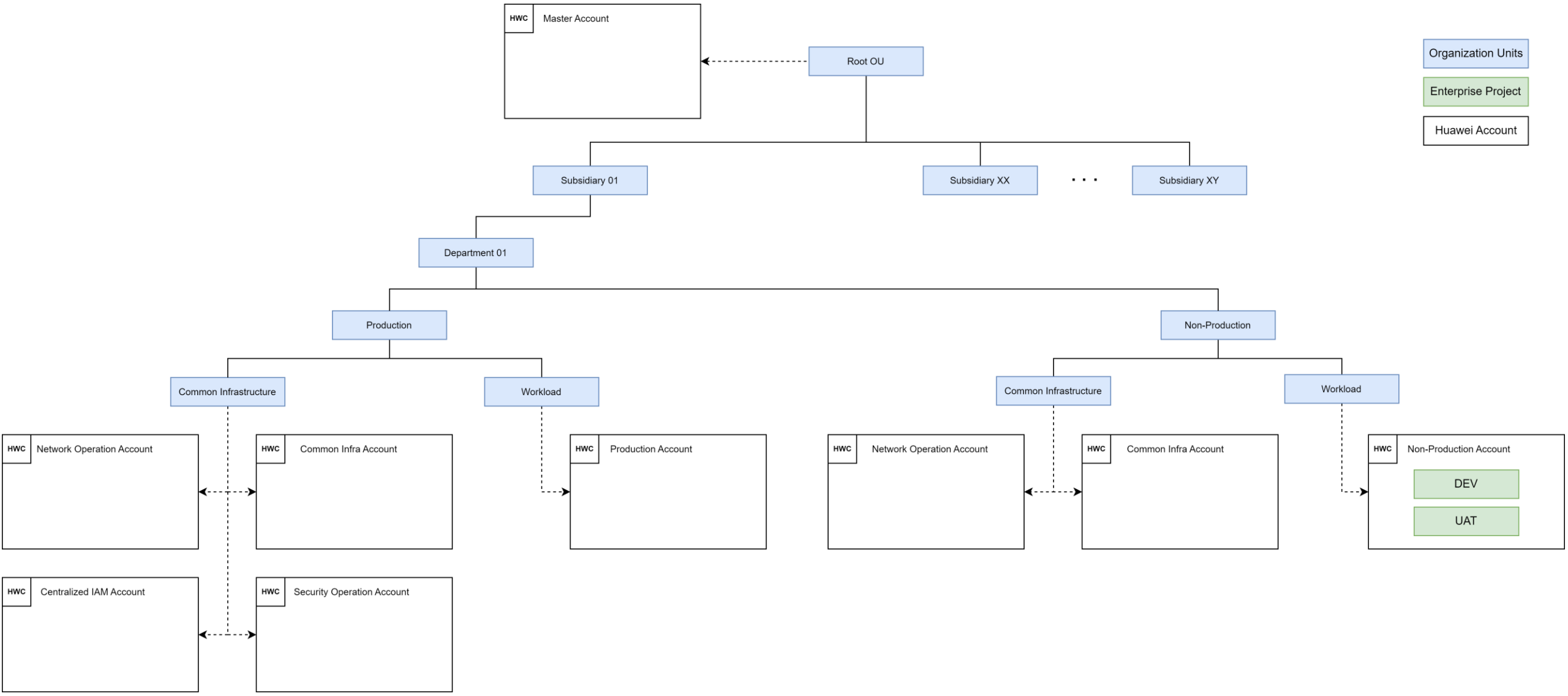
**Sandbox**

- Playground for developers to test new tools
- No need to connect via network to any other accounts
- Should allocate limited budget under Organization

**Others**

- Additional requirements that is not fit in with the existing strategy e.g. Data & Analytics account

# Conceptual Huawei Cloud Account Structure



# Pros & Cons of Conceptual Huawei Cloud Account Strategy

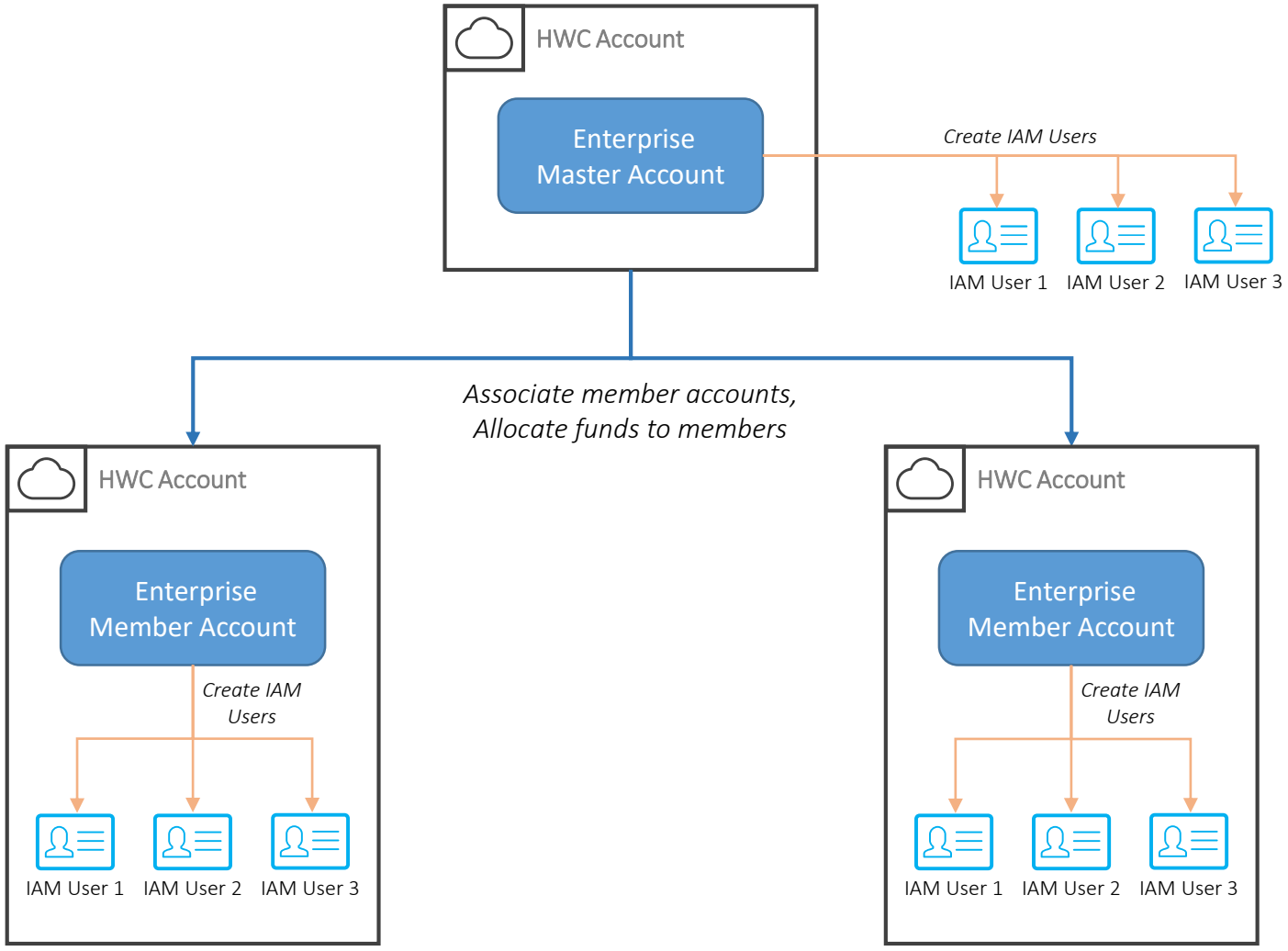
## Pros

- Adaptable Structure
- No impact on environment changes
- Limit blast radius for the application/product
- Create first layer of duty segregation
- Reduce a complexity of writing granular IAM permission in a single account

## Cons

- Overhead in managing IAM in multiple accounts. Needs Infra-as-Code to help
- Not every service in Huawei Cloud supports cross account integration (Still improving!)

# Huawei Cloud Enterprise Center

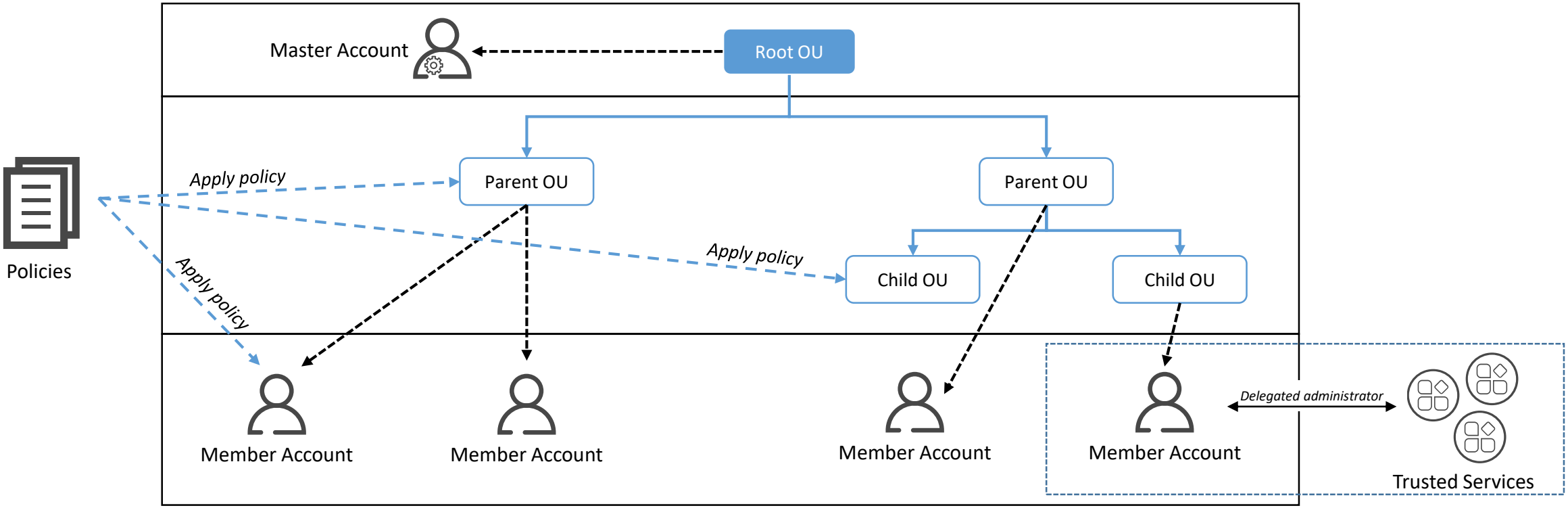



- Enterprise Center allows multiple HUAWEI CLOUD accounts to be associated for accounting purposes
- Enterprise Master Account can allocate funds to member accounts

# Huawei Cloud Organizations

OBT

Organizations service helps govern multiple accounts within an organization. Organization can apply policies to the different accounts to meet security and compliance need of the customer's business

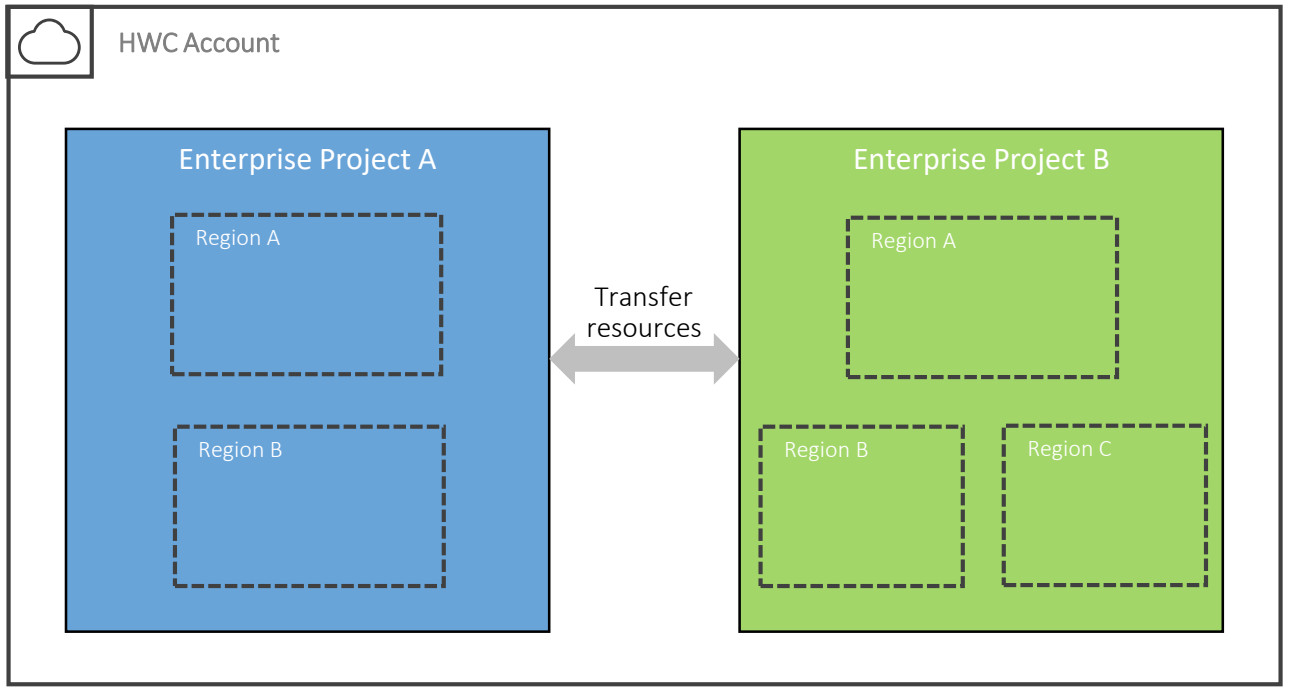



- An organization can have only 1 root OU
- 5 Levels of OU are allowed to be created (exclude root OU)
- 100 of OUs can be created within an organization

*As of Jan 01, 2023*

# Huawei Cloud Enterprise Project

- **Recommended** for managing resources under HWC Account
- Logically grouping of resources under the same project
- Cross-region supported
- Once enabled, IAM project are no longer active
- Must be mapped with user group to control access and permission
- Quota can be configured to limit the spending within Enterprise Project and create expenditures to monitor spending within the project



# Huawei Cloud Enterprise Project – Supported Resources

| Product Type | Resource Type |
|---|---|
| Elastic Cloud Server (ECS) | • ECS |
| Bare Metal Server (BMS) | • BMS |
| Auto Scaling (AS) | • AS group |
| Image Management Service (IMS) | • Private image |
| Dedicated Host (DeH) | • Dedicated host |
| FunctionGraph | • Function |
| Object Storage Service (OBS) | • Bucket |
| Elastic Volume Service (EVS) | • Disk |
| Cloud Backup and Recovery (CBR) | • Vault |
| Content Delivery Network (CDN) | • Domain name |
| Scalable File Service (SFS) | • File system<br>• SFS Turbo |

| Product Type | Resource Type |
|---|---|
| Virtual Private Cloud (VPC) | • VPC<br>• Security group |
| Bandwidth | • Shared bandwidth |
| Elastic IP (EIP) | • EIP |
| Elastic Load Balance (ELB) | • Load balancer |
| NAT Gateway | • Public NAT gateway |
| Domain Name Service (DNS) | • Private zone<br>• PTR record<br>• Public zone |
| Cloud Container Engine (CCE) | • Cluster |
| Cloud Container Instance (CCI) | • Namespace |
| GeneContainer Service (GCS) | • Environment |

*As of August 11, 2022*

# Huawei Cloud Enterprise Project – Supported Resources

| Product Type | Resource Type |
|---|---|
| Advanced Anti-DDoS (AAD) | • Instance |
| Web Application Firewall (WAF) | • WAF instance<br>• Web application firewall<br>• Domain expansion package<br>• Bandwidth expansion package |
| Host Security Service (HSS) | • Host security |
| Distributed Cache Service (DCS) | • Instance |
| Distributed Message Service (DMS) | • Kafka instance<br>• RabbitMQ instance |
| Simple Message Notification (SMN) | • Topic |
| Blockchain Service (BCS) | • Blockchain |
| API Gateway | • Dedicated gateway |
| Application Operations Management (AOM) | • Resource group |

| Product Type | Resource Type |
|---|---|
| Application Performance Management (APM) | • Application |
| Log Tank Service (LTS) | • Log stream |
| Cloud Connect (CC) | • Cloud Connect<br>• Bandwidth package |
| Relational Database Service (RDS) | • Instance |
| Document Database Service (DDS) | • Instance |
| Distributed Database Middleware (DDM) | • Instance |
| Data Replication Service (DRS) | • Real-time synchronization task<br>• Real-time migration task<br>• Backup migration task<br>• Data subscription task<br>• Real-time disaster recovery task |

*As of August 11, 2022*

# Huawei Cloud Enterprise Project – Supported Resources

| Product Type | Resource Type |
|---|---|
| GaussDB | • GaussDB instance |
| GaussDB NoSQL | • Instance |
| Cloud Data Migration (CDM) | • Cluster |
| ModelArts | • Workspace |
| MapReduce Service (MRS) | • Cluster |
| Data Lake Insight (DLI) | • Cluster<br>• Queue<br>• Database |
| Cloud Search Service (CSS) | • Cluster |
| Data Warehouse Service (DWS) | • DWS cluster |
| Data Ingestion Service (DIS) | • Stream |

| Product Type | Resource Type |
|---|---|
| CloudTable | • CloudTable cluster |
| Graph Engine Service (GES) | • GES cluster |
| Recommender System (RES) | • Workspace |
| Data Lake Visualization (DLV) | • DLV instance |
| Data Lake Governance Center (DGC) | • DGC instance |
| DevCloud | • Project management |
| ROMA | • ROMA instance<br>• ROMA task |
| SupportPlan | • Support plan |
| PrivateNumber | • Application |

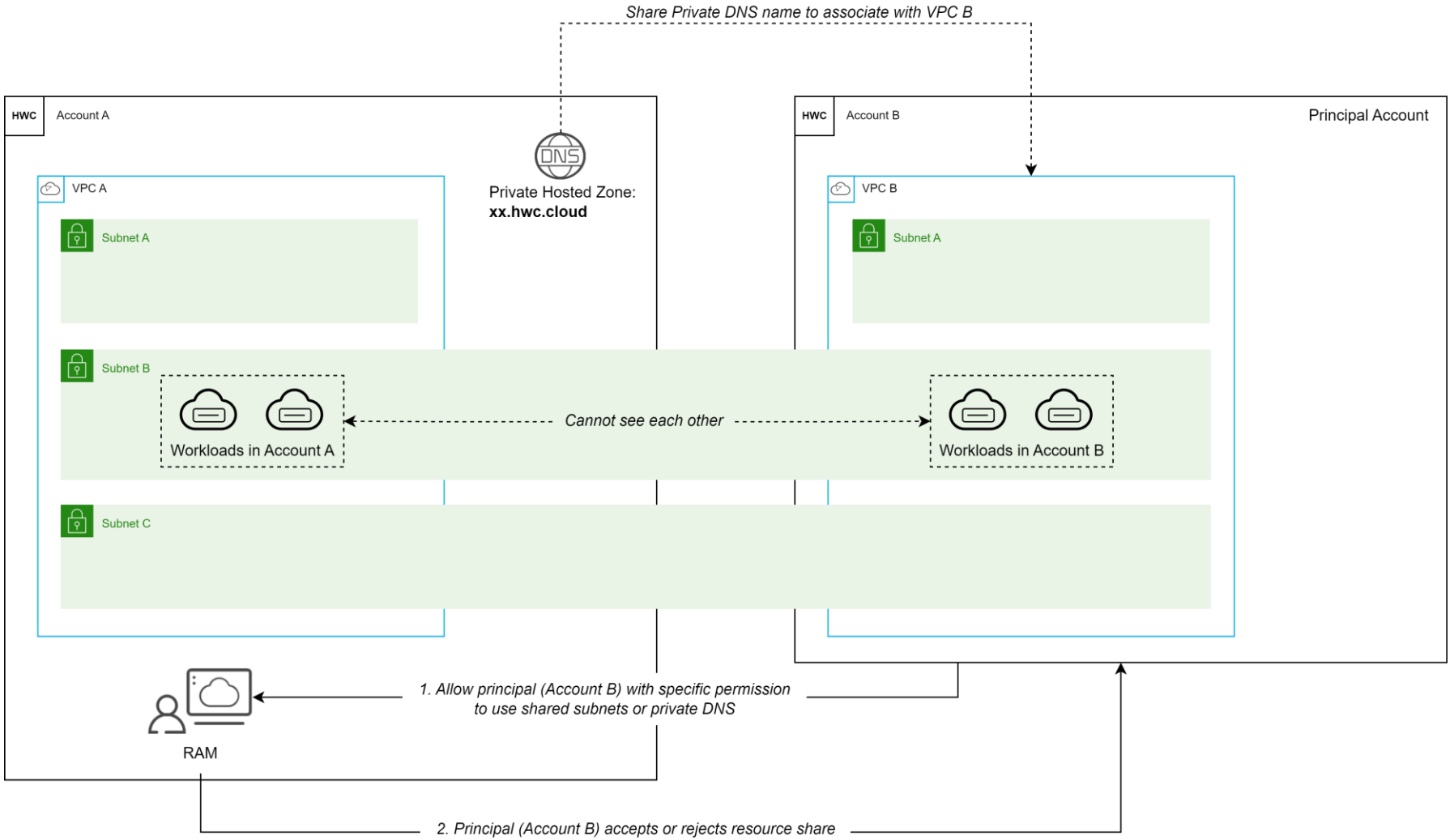
*As of August 11, 2022*

# Huawei Cloud Resource Access Manager (RAM)

OBT

Resource Access Manager (RAM) allows the customer to share resources among Huawei Cloud accounts, OUs, Organization, or IAM roles and users.

Currently, RAM supports 2 services; **VPC (Subnet)** and **DNS (Private Zone, Resolver Rules)**



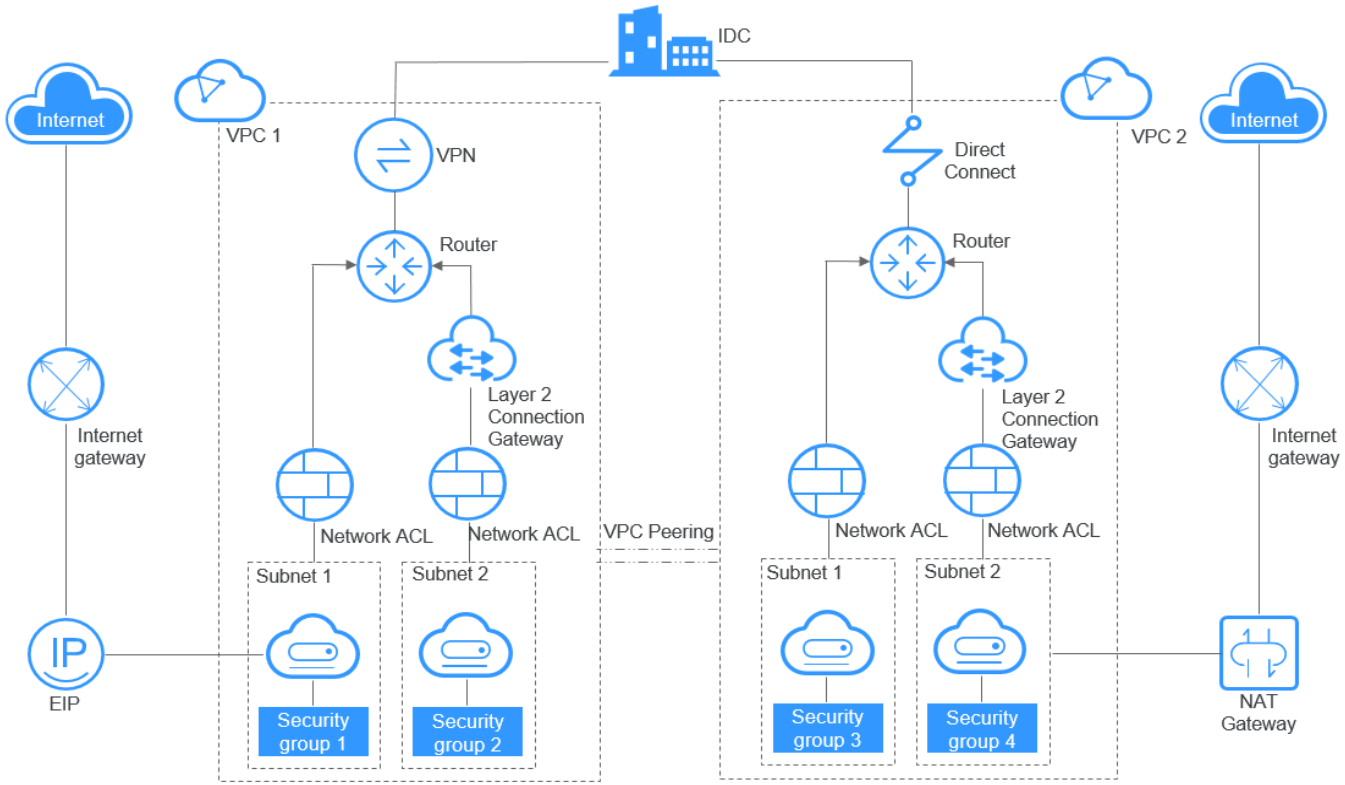

***Remark:*** *Supported compute resources under Shared subnet; VPC, ELB, ECS, CCE Turbo, RDS*

# Huawei Cloud Landing Zone

VPC & Networking Design

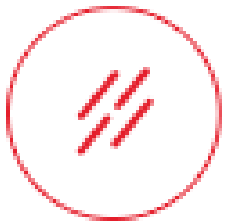
# Understanding VPC

- A logically isolated, configurable, and manageable virtual networks on cloud
- The customer has a complete control over the virtual networking environment
- Customizable networking requirements:
  - User-defined IP address range
  - Bandwidth size
  - Subnets
  - Route Tables
  - Access Control Lists
  - Security Groups
  - Network Gateways



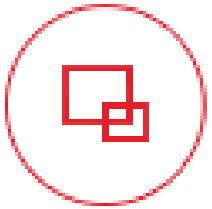

VPC Product Architecture

# VPC Key Benefits



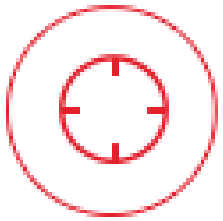
## Flexible Configuration

Self-service network management frees you from routine network configurations and allows flexible network deployment.



## Secure and Reliable

Private networks on the cloud are completely isolated. You can create Elastic Cloud Servers (ECSs) that are in different availability zones, in the same VPC.



## High-Speed Access

Dynamic BGP network connections enable seamless high-speed access to services on the cloud.

## Interconnectivity

VPC peering enables interconnection between VPCs

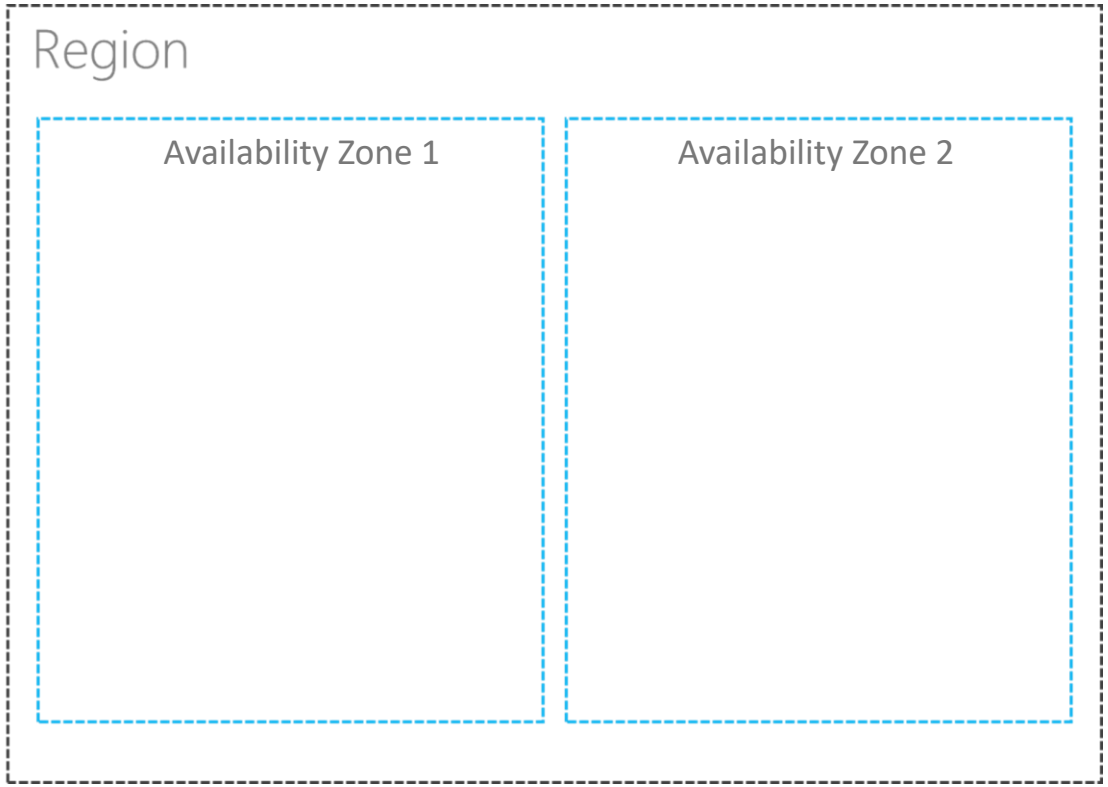
# Regions & Availability Zones

## Region

- Regions are divided based on geographical location and network latency.
- It is recommended that you select the closest region for low network latency and quick access.

## Availability Zones

- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities
- AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability systems.



# Huawei Cloud Network & Region Guideline

**Picking an Huawei region**

- Geographically close to consumers of your services
- Aligned to your regulatory needs
- Use multiple regions if required, but always start with just one

**VPC Guidelines**

- Use address space that is compatible with existing on-premises environment – **No IP overlapping**!
- Plan ahead, allocate a **enough range of IP** for use on Huawei and become self sufficient in allocation
- If your services do not require **network isolation**, a single VPC should be enough.
- Group workloads based on operation, environment, line of business, and dependency.

**Select your Availability Zones (AZ)**

- Make use of multiple AZ's within VPC
- Minimum number is two*
- Leverage more to increase availability of workloads

# Choosing the right CIDR

VPC

1

Allocate any address that is under RFC 1918

2

Avoid conflicts CIDR block with existing network both on premise and on the cloud

3

Recommended CIDR block:

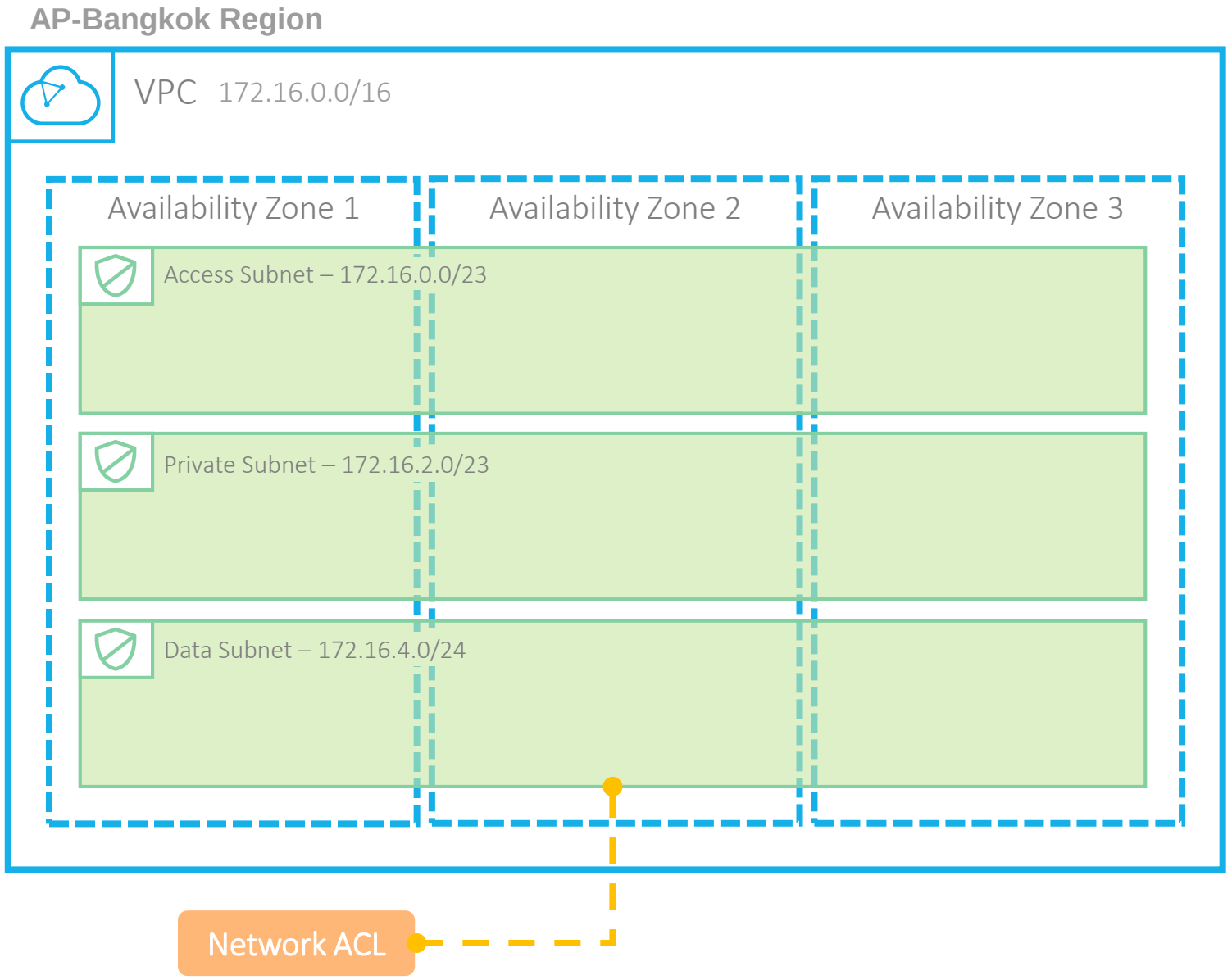
- 10.0.0.0/8-24
- 172.16.0.0/12-24
- 172.31.0.0/12-24
- 192.168.0.0/16-24

***Remark:***

- */28 is the smallest CIDR mask that can be allocated for a single VPC*
- *Adding secondary VPC is now available under Bangkok region*

# Define subnet in VPC

- Default subnet with a default route will be created during VPC creation
- A subnet span across AZs
- Plan ahead on required address per subnet
- Use smaller mask on subnet that requires lesser address e.g. Database Subnet
- Use Route Table to define routes for each subnet
- Network ACL can be configured as a firewall to control traffic in and out on one or more subnets



# The five reserved addresses in a single subnet

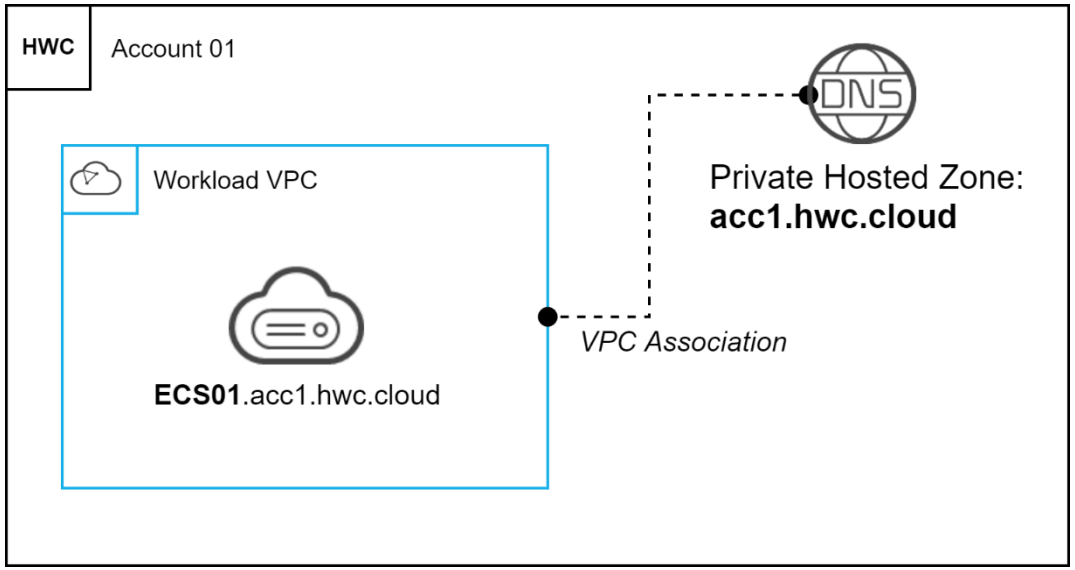
When a subnet is created, there are five reserved IP addresses, which cannot be used.

For example, in a subnet with CIDR block *192.168.0.0/24*, the following IP addresses are reserved:

| | |
|---|---|
| *192.168.0.0* | Network ID. This address is the beginning of the private IP address range and will not be assigned to any instance. |
| *192.168.0.1* | Gateway address. |
| *192.168.0.253* | Reserved for the system interface. This IP address is used by the VPC for external communication. |
| *192.168.0.254* | DHCP service address. |
| *192.168.0.255* | Network broadcast address. |

# VPC, Subnet and DNS Service

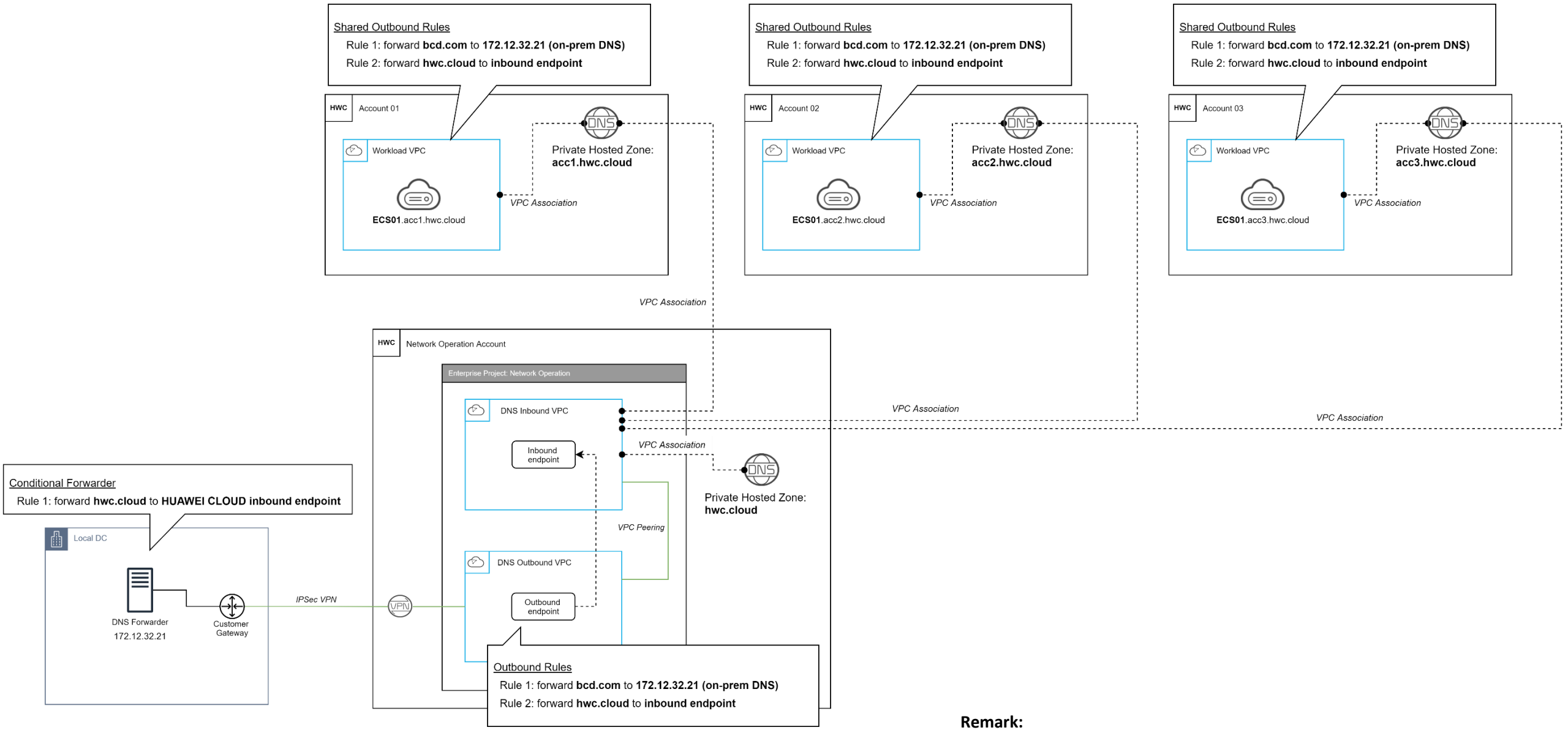
- Subnets are automatically configured with 2 DNS server IP addresses that are provided from HUAWEI CLOUD DNS Service
  - For AP-Bangkok, **100.125.1.250** and **100.125.1.251** are default DNS Servers
- DNS Server IP Address can be configured to external DNS server (Both on-premise or Public DNS Server)
  - If public DNS server is configured, all the query will be routed over the internet which may incur additional traffic fees
- Each subnet can configured with different DNS servers




*Full list of DNS Server IP Address for each region: here*

# Huawei Cloud DNS Resolver

OBT




**Remark:**

- Require RAM (Resource Access Manager)
- Inbound VPC and Outbound VPC require VPC peering as their next hop

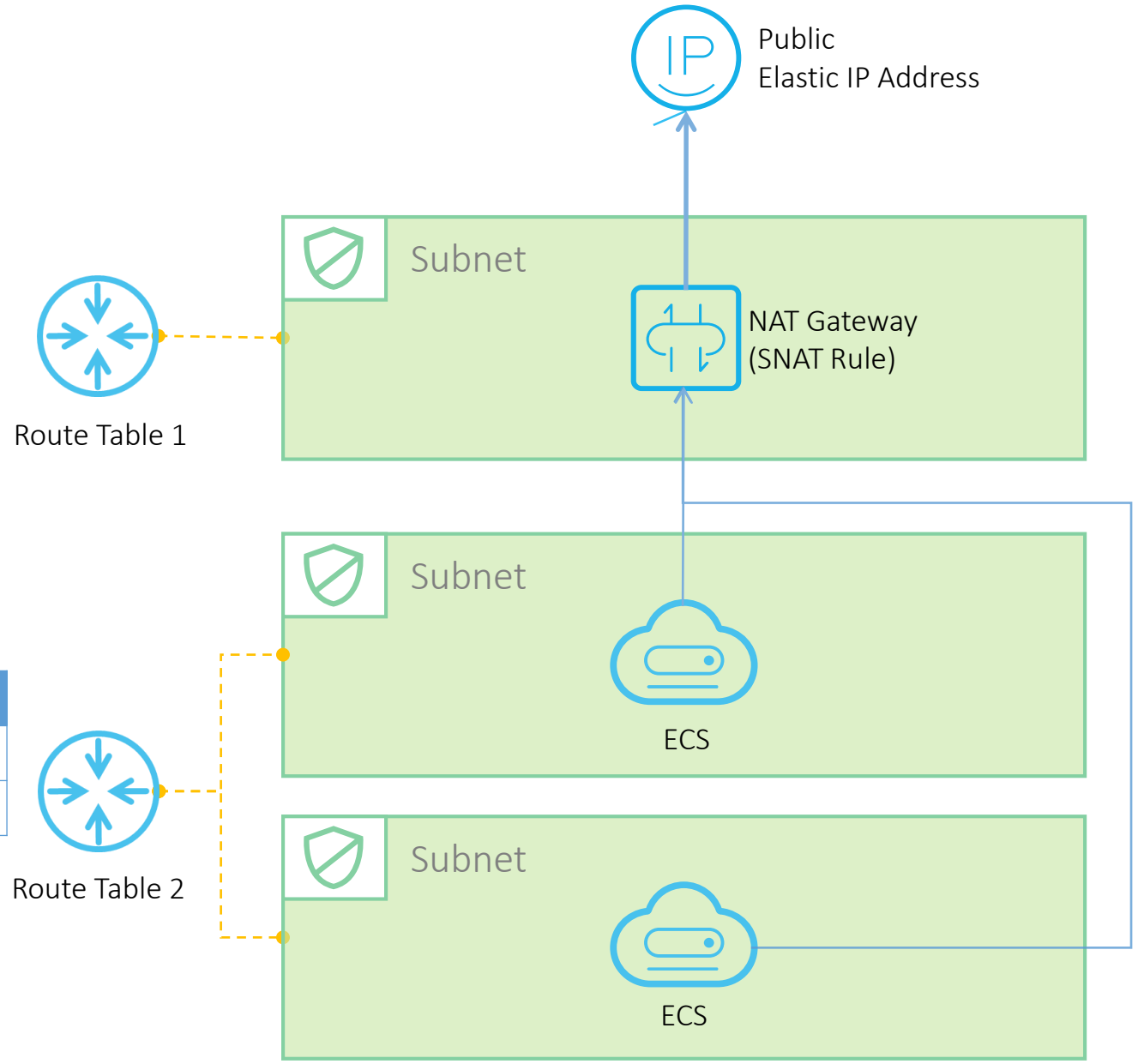
# Route Table

**System route** – Added by the system and cannot be modified or deleted

| Destination | Next Hop Type | Next Hop | Type |
|---|---|---|---|
| Local | Local | Local | System |

| Destination | Next Hop Type | Next Hop | Type |
|---|---|---|---|
| Local | Local | Local | System |
| 0.0.0.0/0 | NAT Gateway | natgw-instance | Custom |

**Custom route** – A route that can be modified and deleted. The destination of a custom route cannot overlap with the system route




**Remark:**

- The **custom route table** associated with a subnet affects only the **outbound traffic**. The **default route table** determines the **inbound traffic**

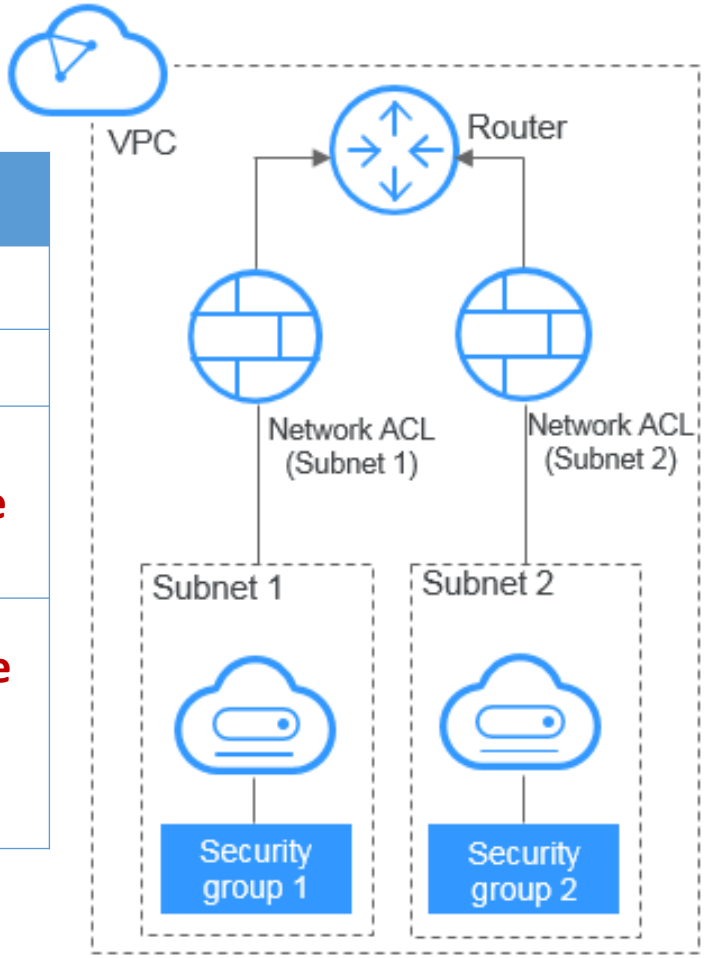
# Route Table – Next Hope Type

| Next Hop Type | Description | Supported Route Table |
|---|---|---|
| Server | Traffic intended for the destination is forwarded to an ECS in the VPC. | • Default route table<br>• Custom route table |
| Extension NIC | Traffic intended for the destination is forwarded to the extension NIC of an ECS in the VPC. | • Default route table<br>• Custom route table |
| BMS user-defined network | Traffic intended for the destination is forwarded to a BMS user-defined network. | • Default route table<br>• Custom route table |
| VPN gateway | Traffic intended for the destination is forwarded to a VPN gateway. | • Custom route table |
| Direct Connect gateway | Traffic intended for the destination is forwarded to a Direct Connect gateway. | • Custom route table |
| Cloud connection | Traffic intended for the destination is forwarded to a cloud connection. | • Custom route table |
| Supplementary network interface | Traffic intended for the destination is forwarded to the supplementary network interface of an ECS in the VPC. | • Default route table<br>• Custom route table |
| NAT gateway | Traffic intended for the destination is forwarded to a NAT gateway. | • Default route table<br>• Custom route table |
| VPC peering connection | Traffic intended for the destination is forwarded to a VPC peering connection. | • Default route table<br>• Custom route table |
| Virtual IP address | Traffic intended for the destination is forwarded to a virtual IP address and then sent to active and standby ECSs to which the virtual IP address is bound. | • Default route table<br>• Custom route table |
| Cloud container | Traffic intended for the destination is forwarded to a cloud container. | • Default route table<br>• Custom route table |
| Enterprise router | Traffic intended for the destination is forwarded to an enterprise router. | • Default route table<br>• Custom route table |
| Cloud firewall | Traffic intended for the destination is forwarded to a cloud firewall. | • Default route table<br>• Custom route table |

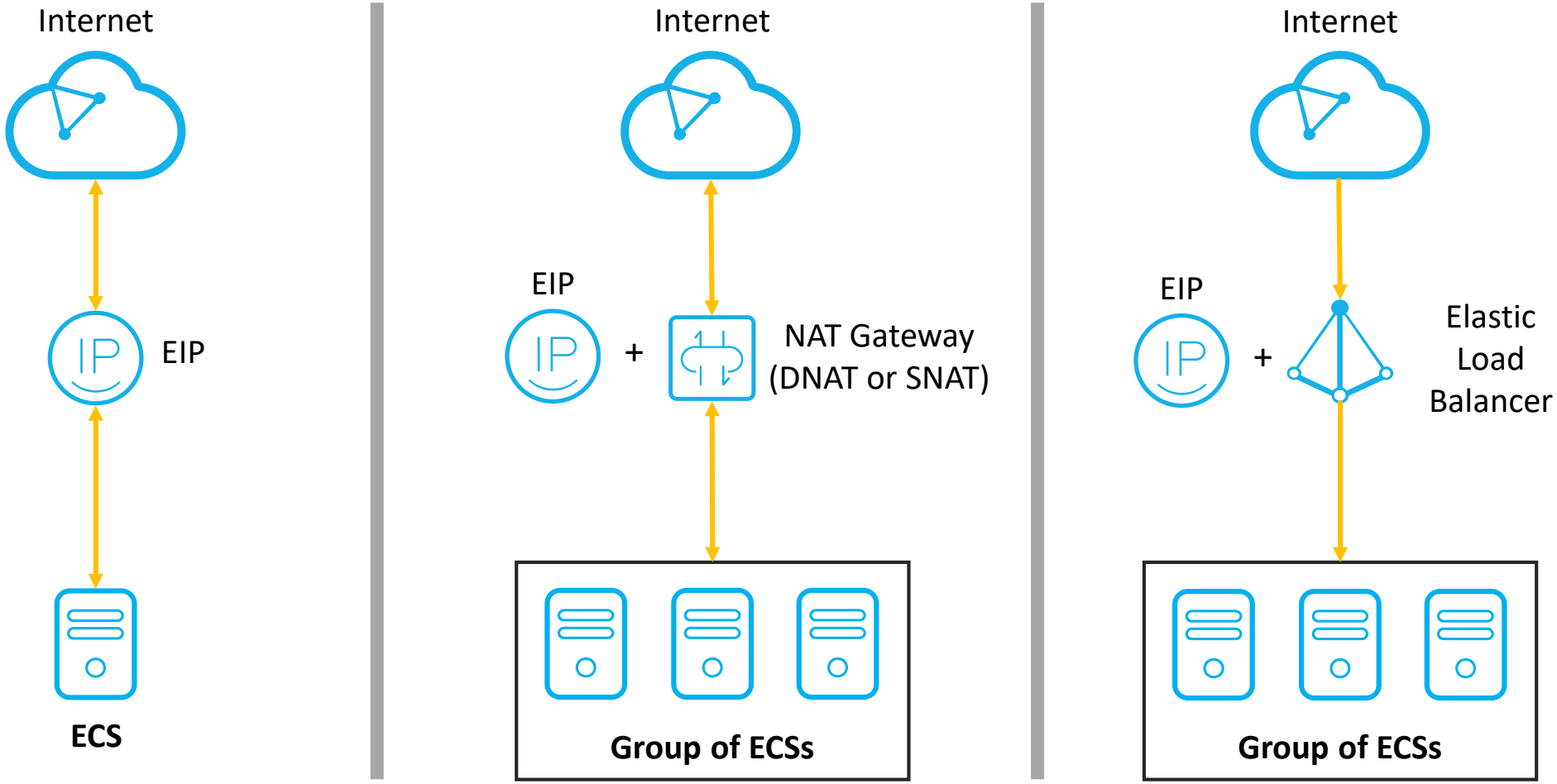
*As of April, 26th 2023*
*Reference: here*

# Network Access Control List (NACL) vs Security Group

| NACL | Security Group |
| --- | --- |
| At **subnet** level | At **ECS** level |
| Support **ALLOW** and **DENY** rules | Support only **ALLOW** rules |
| If network ACL rule conflicts, the rule with **higher priority wins** | If security group rules conflict, the **overlapping elements of these rules take effect**. |
| Only packet filtering based on the **5-tuple** (protocol, source port, destination port, source IP address, and destination IP address) is supported. | Only packet filtering based on the **3-tuple** (protocol, port, and peer IP address) is supported. |



# VPC Connectivity – Internet Connection

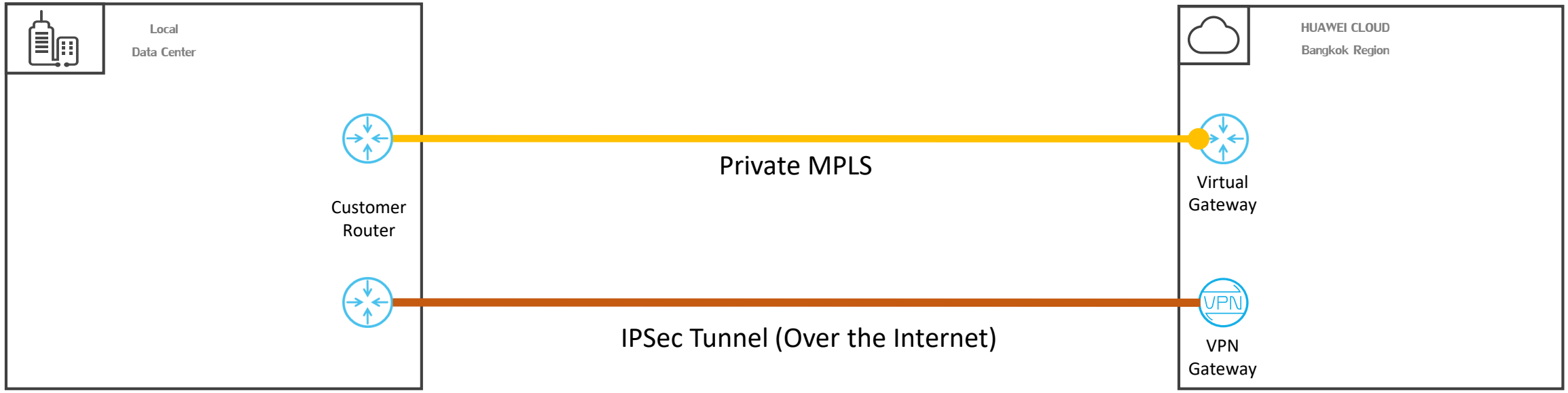



| | | | |
|---|---|---|---|
| **Traffic direction:** | Incoming & Outgoing | Incoming **AND/OR** Outgoing | Incoming **ONLY** |
| **Route configuration:** | Not require | Require | Require |

# VPC Connectivity – Hybrid Connection

There are **two ways** to connect between Local Data center and HUAWEI CLOUD

1. **VPN (Virtual Private Network)** – Encrypted connection over the internet
2. **Direct Connect** – Dedicated and Private link with guarantee latency

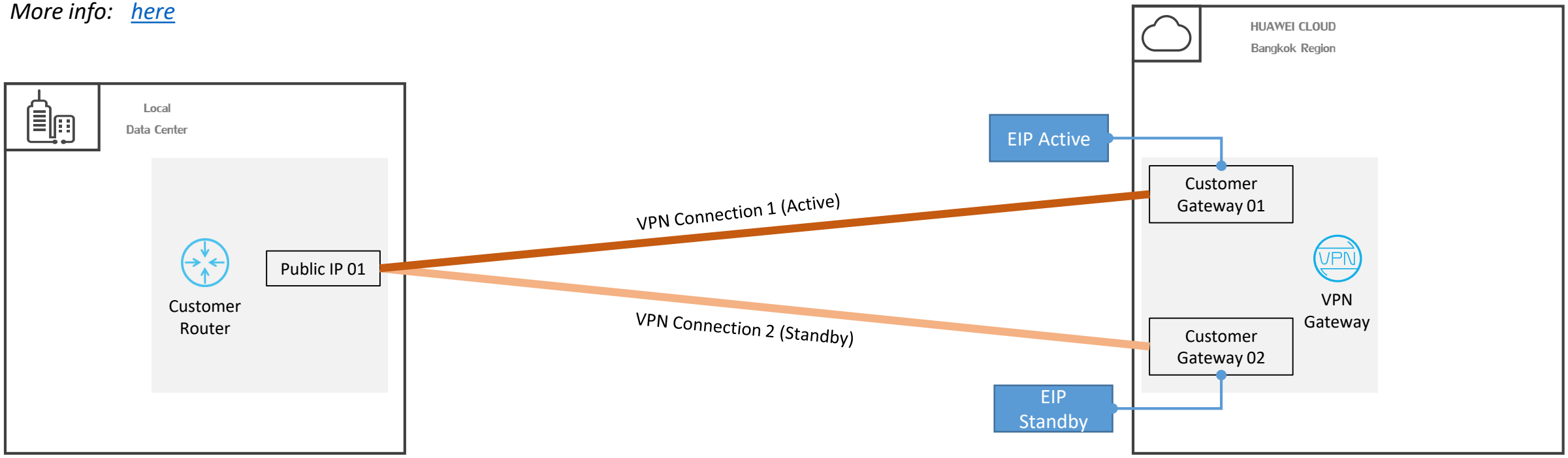


# Hybrid Connection – Virtual Private Network (VPN)

**Two** VPN editions are available;

1. Classic VPN – Traditional VPN with shared gateway. Single AZ deployment.
2. Enterprise edition VPN – Dedicated gateway with BGP supported. Multi-AZ deployment.

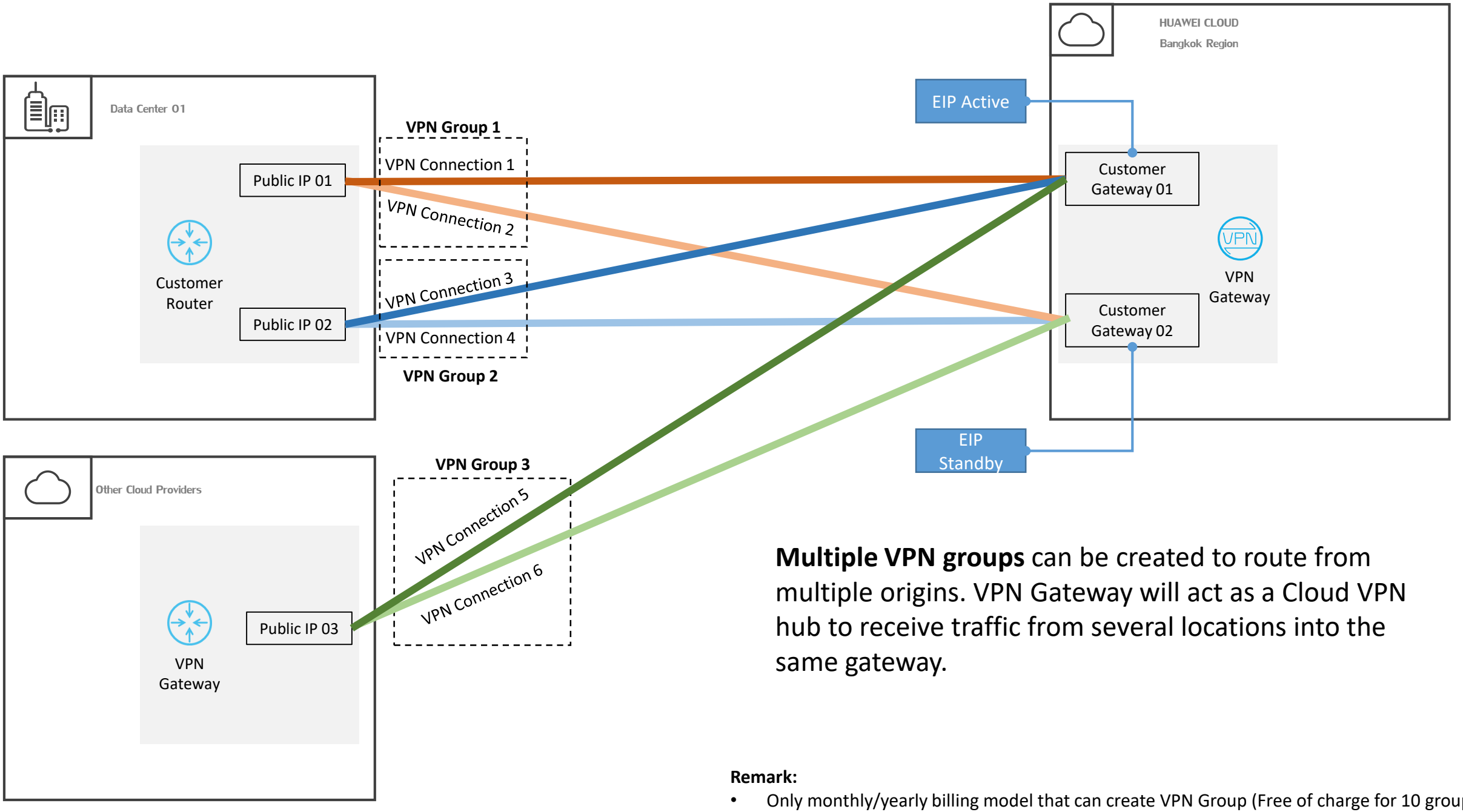
*More info:* *here*




VPN connection are available in 3 IPsec connection modes:

- **Static routing:** Determines the data that enters the IPsec VPN tunnel based on the route configuration (local subnet and customer subnet). The BGP protocol is supported.
- **BGP routing:** The customer gateway can advertise a maximum of 100 BGP routes to the VPN gateway.
- **Policy-based:** Determines the data that enters the IPsec VPN tunnel based on the policy (between the customer network and VPC). Data flows to be encrypted can be customized.

# Hybrid Connection – Virtual Private Network (VPN)



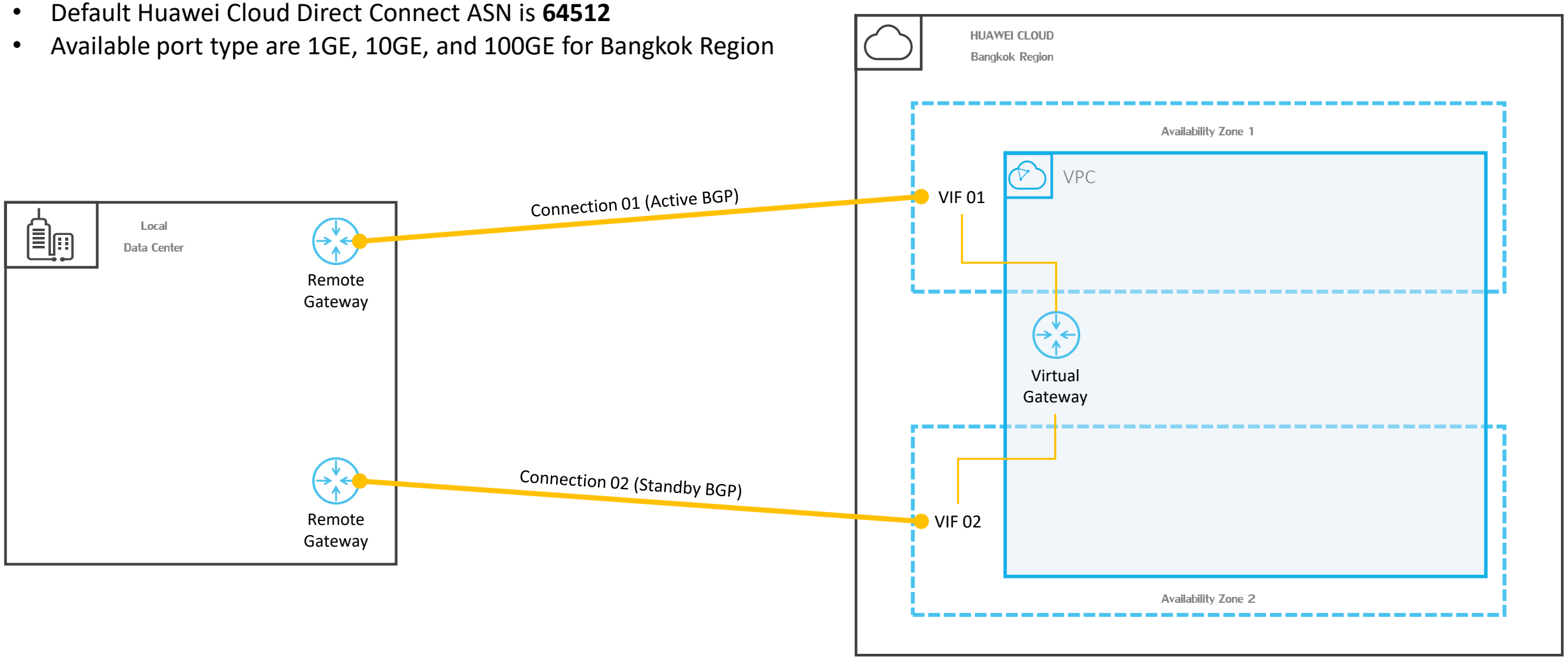

**Multiple VPN groups** can be created to route from multiple origins. VPN Gateway will act as a Cloud VPN hub to receive traffic from several locations into the same gateway.

**Remark:**

- Only monthly/yearly billing model that can create VPN Group (Free of charge for 10 groups)

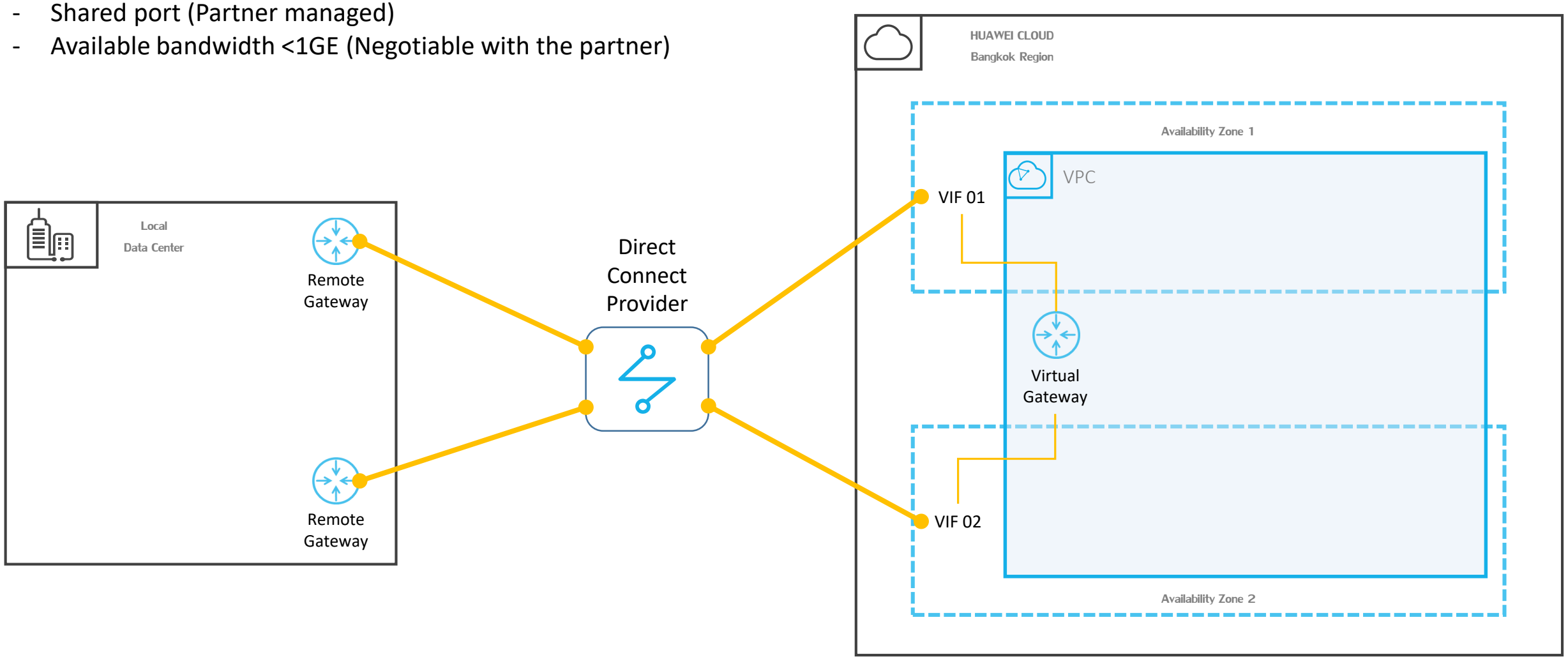
# Hybrid Connection – Direct Connect (DC) with standard connection

- Lease line connection with multiple local MPLS available
- Exclusive port (Dedicated to the customer)
- Default Huawei Cloud Direct Connect ASN is **64512**
- Available port type are 1GE, 10GE, and 100GE for Bangkok Region



# Hybrid Connection – Direct Connect (DC) with hosted connection

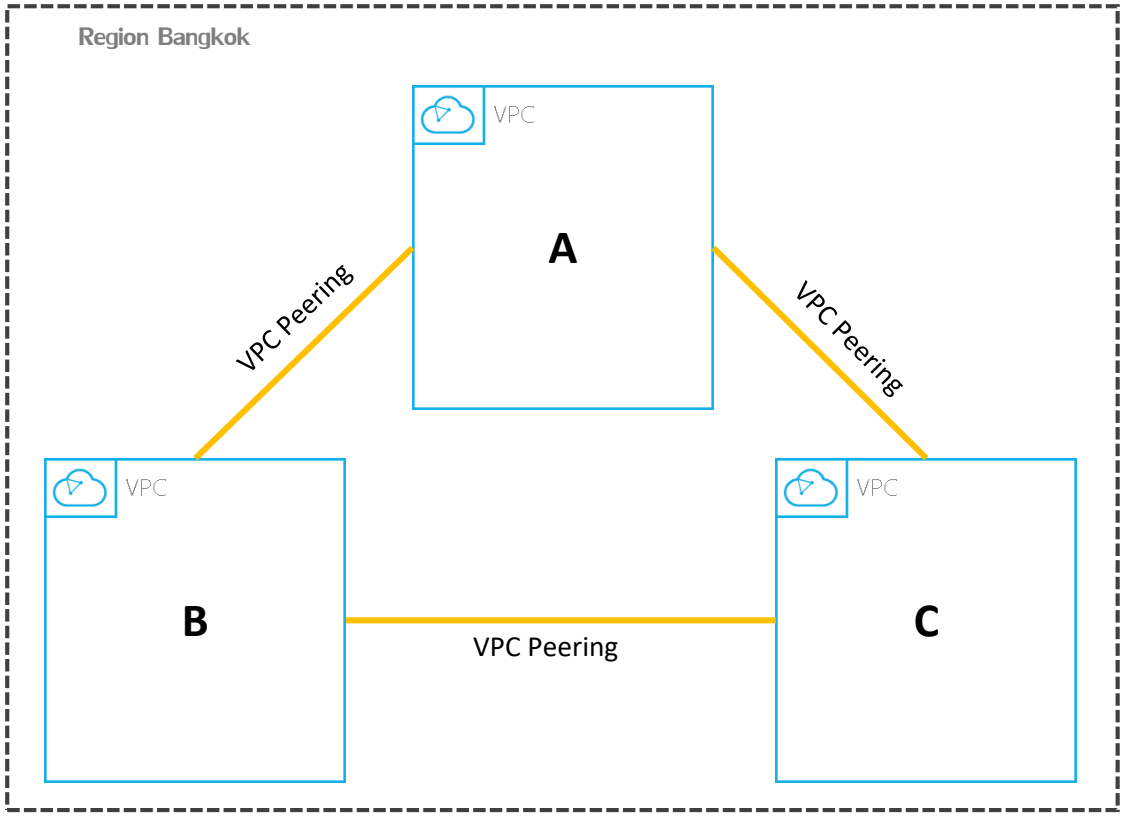
- Lease line connection. Only certified local MPLS partner can provide the service
- Shared port (Partner managed)
- Available bandwidth <1GE (Negotiable with the partner)



# VPC Connectivity – Connect multiple VPCs in the SAME region

## VPC Peering

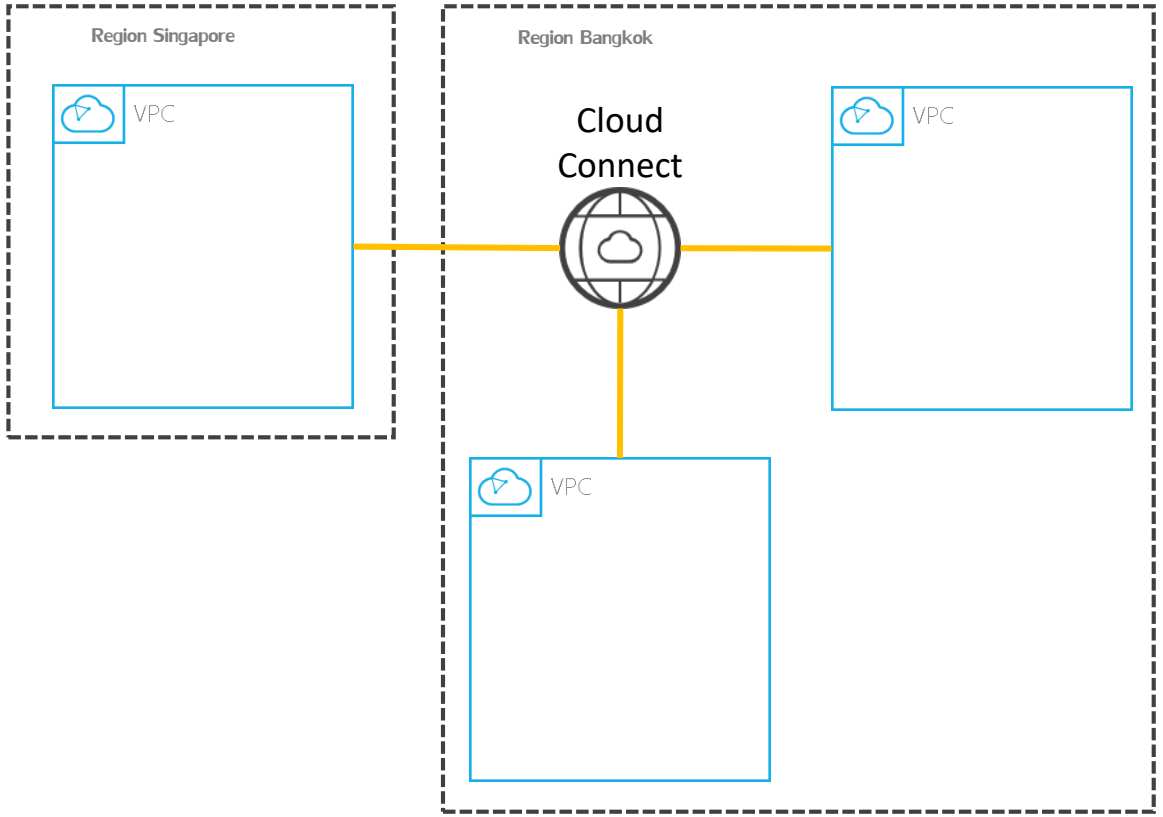
- Traffic is routed under **private network**
- Cross-account is supported
- Overlapped CIDR is not supported
- Maximum 50 VPC Peering can be created in one region per account
- Manual routing configuration (Static route)
- It’s free!



# VPC Connectivity – Connect multiple VPCs in the SAME or DIFFERENT region

## Cloud Connect (CC)

- Traffic is routed under **private network of HUAWEI CLOUD network backbone (at least two physical links are leveraged)**
- Average latency around 30 – 40 ms* cross-region (North-Beijing4 and Hongkong)
- Cross-account and cross-region are supported
- Overlapped CIDR is not supported
- Maximum 10 network instances can be loaded in each region
- Route will be automatically assigned (Cannot manage route)
- To connect with Chinese mainland, a cross-border permit needs to be applied
- It's free for the same region, but charge bandwidth package for cross-region

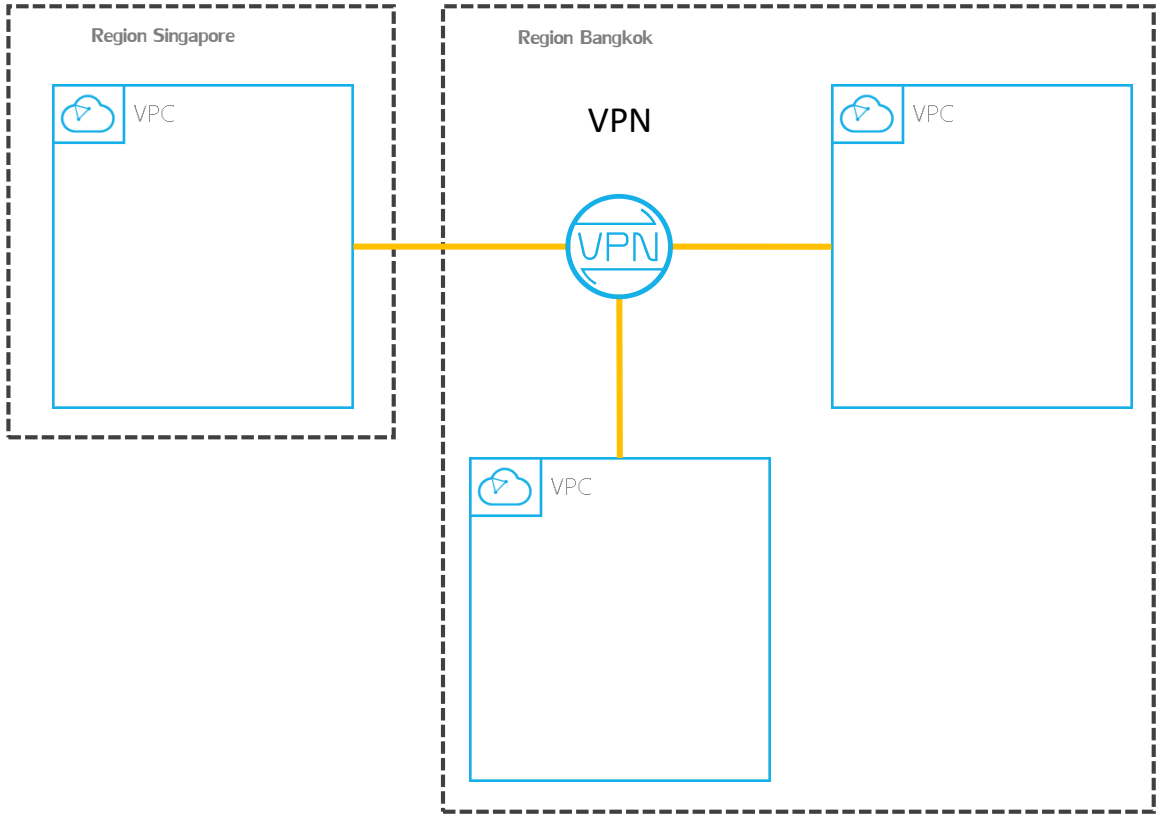



*Reference: here

# VPC Connectivity – Connect multiple VPCs in the SAME or DIFFERENT region

## Virtual Private Network (VPN)

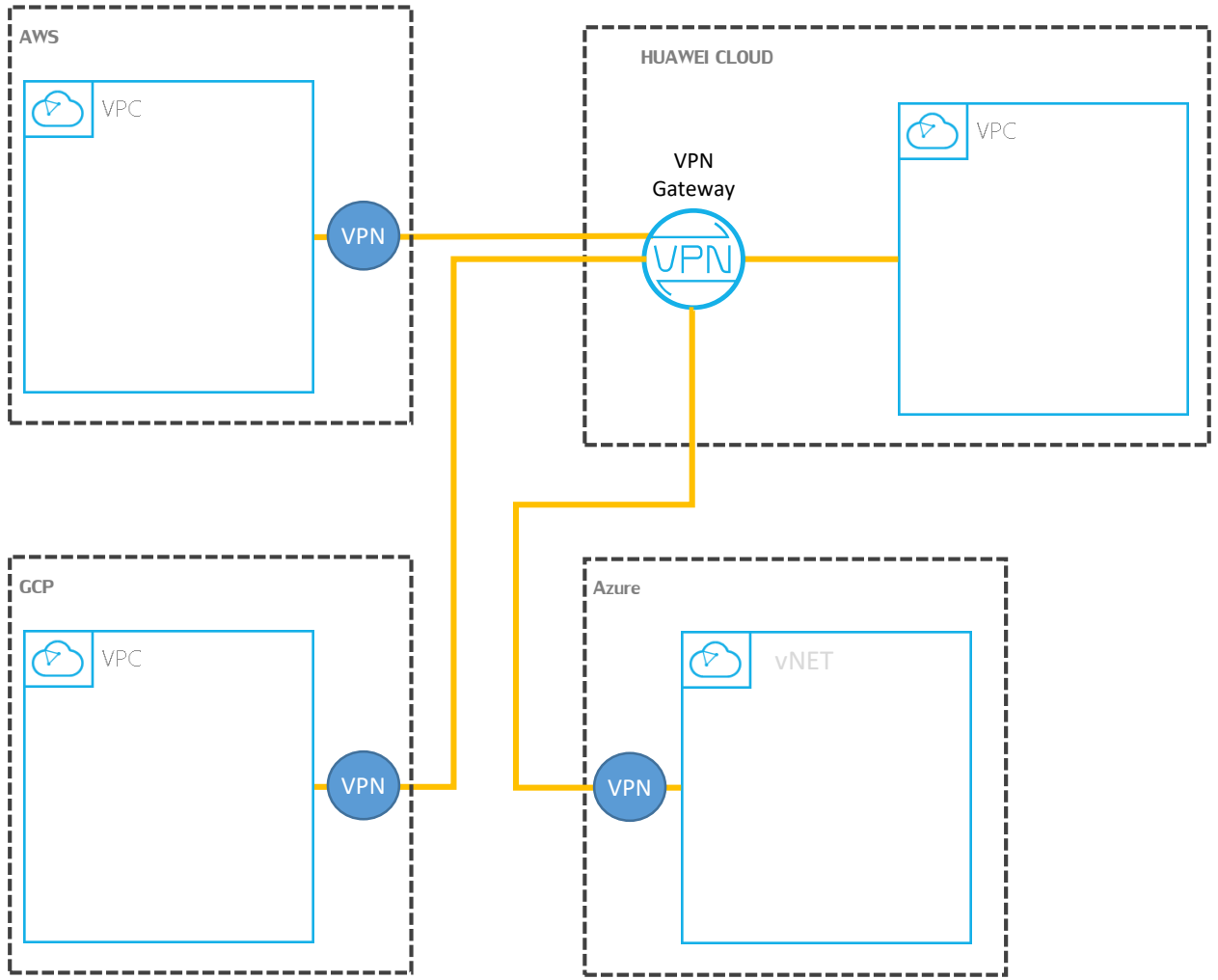
- Traffic is routed over **public network with encrypted tunnel**
- Cross-account and cross-region are supported
- Overlapped CIDR is not supported
- Maximum 12 connections per region
- Incur charges



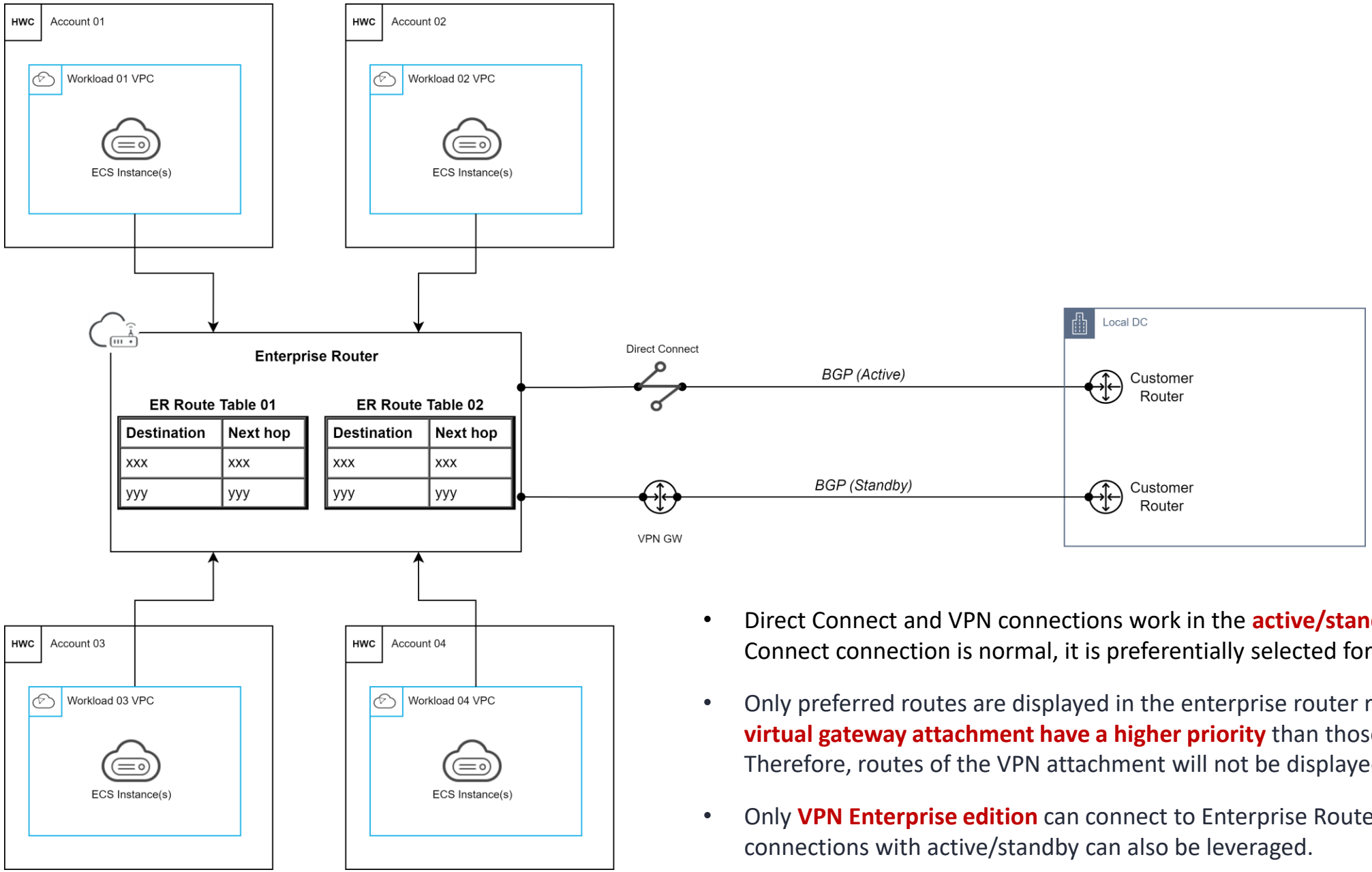
# VPC Connectivity – Connect to other Public Cloud Providers (AWS, Azure, GCP)

## Virtual Private Network (VPN)

- Traffic is routed over **public network with encrypted tunnel**
- Cross-account and cross-region are supported
- Overlapped CIDR is not supported
- Maximum 12 connections per region
- Initiate negotiation from HUAWEI CLOUD
- Incur charges on both sides



# VPC Connectivity – Connect between VPC(s), VPN and Direct Connect




- Direct Connect and VPN connections work in the **active/standby mode**. If the Direct Connect connection is normal, it is preferentially selected for traffic forwarding.
- Only preferred routes are displayed in the enterprise router route table. The **routes of a virtual gateway attachment have a higher priority** than those of a VPN attachment. Therefore, routes of the VPN attachment will not be displayed in the route table.
- Only **VPN Enterprise edition** can connect to Enterprise Router. Multiple VPN connections with active/standby can also be leveraged.

# Introducing Huawei Cloud Firewall

## Cloud Firewall (CFW)

A next-generation cloud-native firewall. It protects Internet and VPC borders on the cloud by real-time intrusion detection and prevention, global unified access control, full traffic analysis, log audit, and tracing. CFW employs AI for intelligent defense, and can be elastically scaled to meet changing business needs and easily handle security threats.

### Intelligent Defense

- Integrated Huawei Cloud/security capabilities and Huawei network threat intelligence
- AI intrusion prevention engine can detect and block malicious traffic in real time
- defend against Trojans, worms, injection attacks, vulnerabilities, phishing, and brute-force attacks

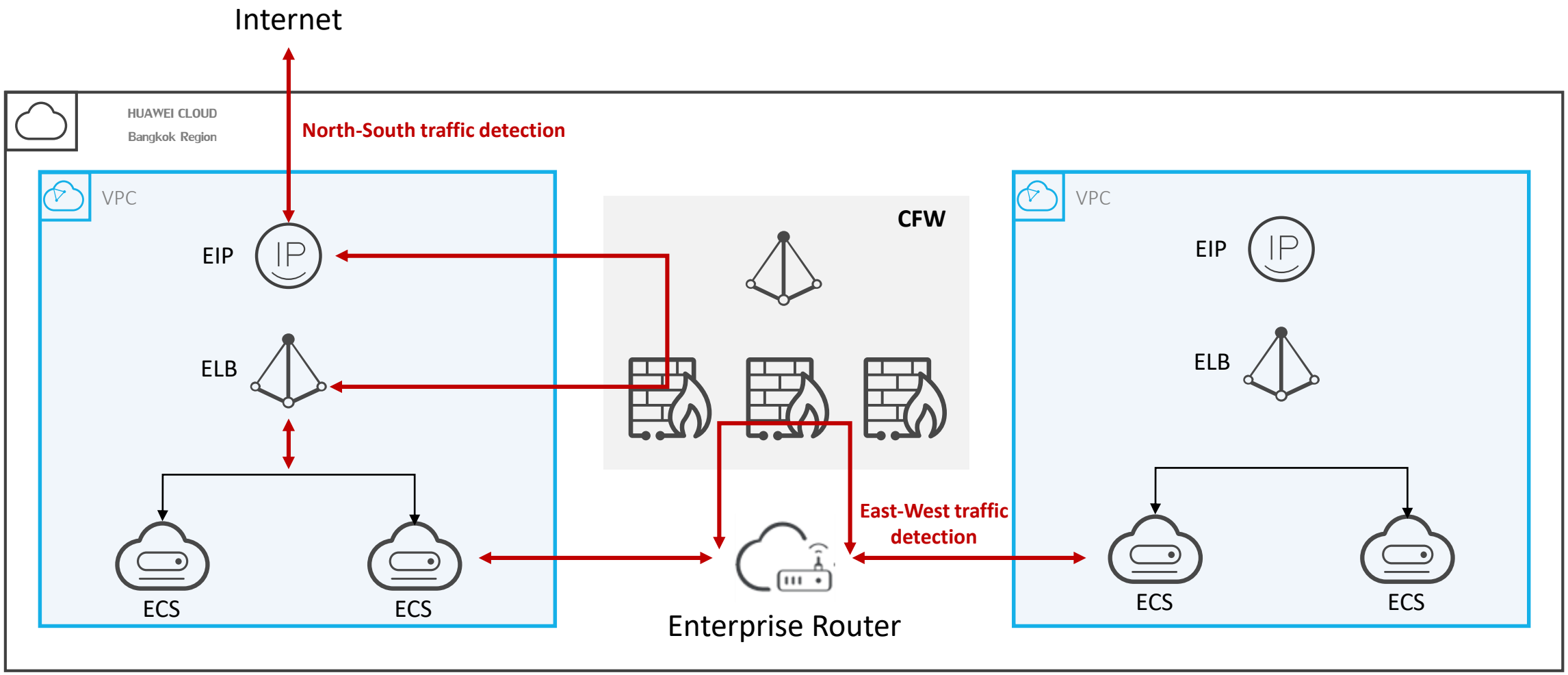
### High Scalability

- CFW cluster is deployed in high availability
- Bandwidth, EIPs, and security policies can be increased without limit

### Easy-to-Use Application

- Import multi-engine security policies with a few clicks
- Automatically check assets within seconds

# Cloud-native CFW  protects all traffic in all scenarios




**Remark:**

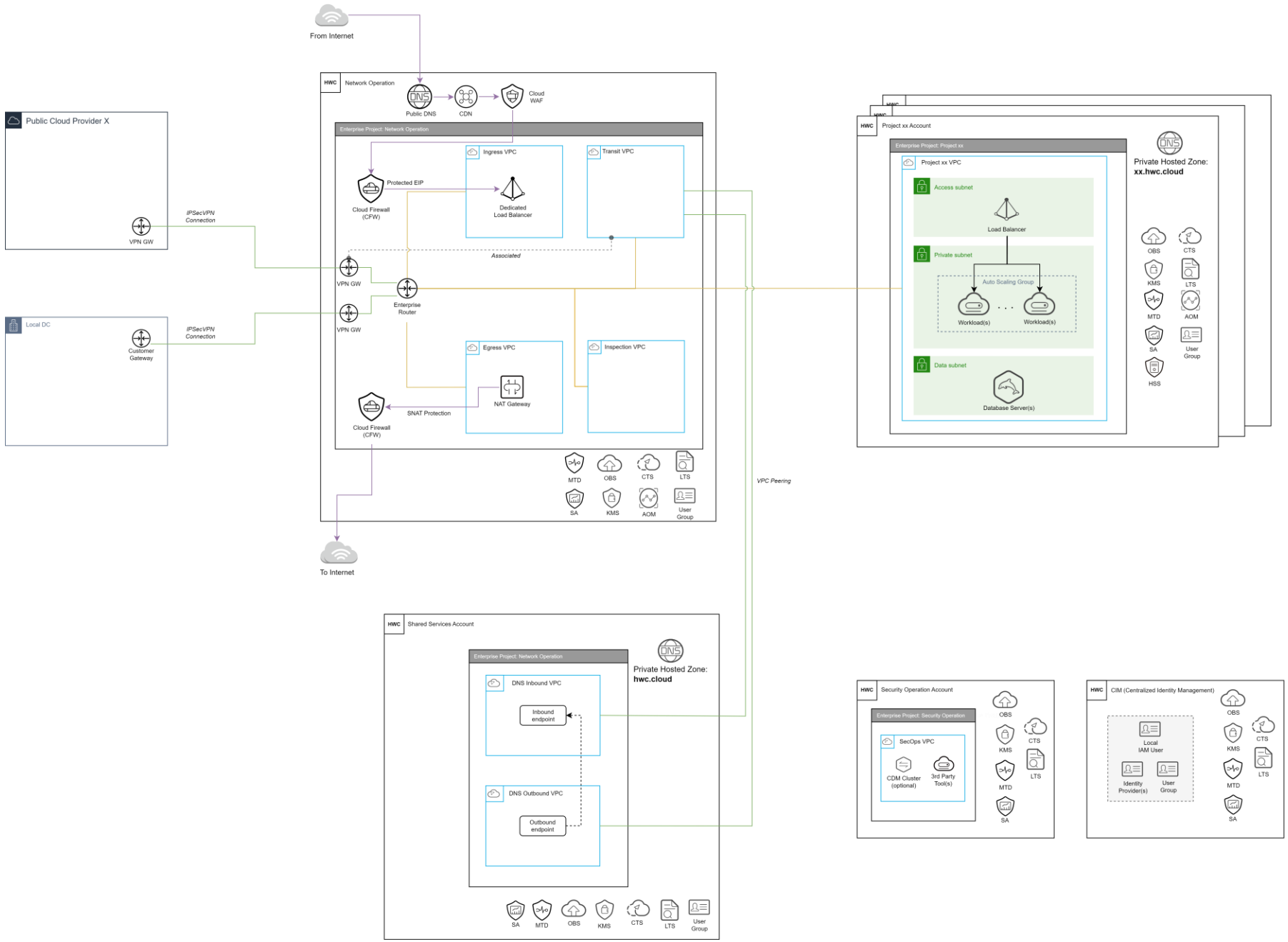
- VPN is considered as East-West traffic
- NAT Gateway protection can be enabled with East-West traffic protection

# CFW Editions

| Feature | Standard | Professional |
| --- | --- | --- |
| Protected EIPs at Internet boundary | 20 (expandable) | 50 (expandable) |
| Peak protection traffic at Internet boundary | 10 Mbit/s (expandable) | 50 Mbit/s (expandable) |
| Protected VPCs | × | 2 (expandable) |
| Max. peak protection traffic between VPCs | × | 200 Mbit/s |
| Northbound and southbound traffic audit and attack log query | √ | √ |
| Northbound and southbound traffic protection and cloud resources (including EIPs) protection against risks on the Internet | √ | √ |
| ACL management for public network resources based on IP addresses, domain names, or applications | √ | √ |
| Network traffic analysis and abnormal inbound and outbound traffic detection | √ | √ |
| Network intrusion prevention system | √ | √ |
| **Eastbound and westbound traffic protection**, resource protection between VPCs, access control, traffic analysis, and intrusion prevention | × | √ |

*Reference: here*

# Overall VPC and Networking Design (Sample Idea)

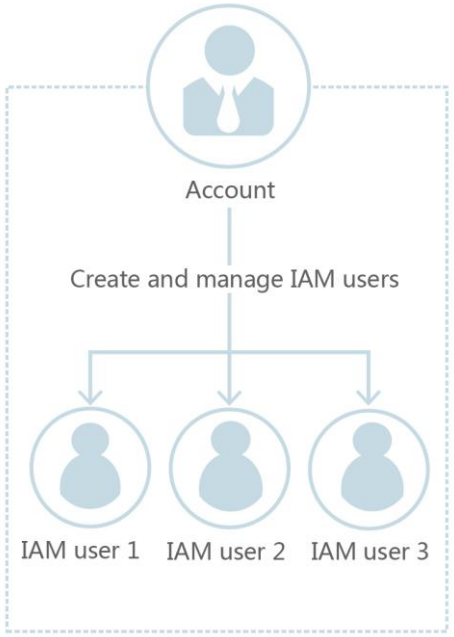


# Huawei Cloud Landing Zone

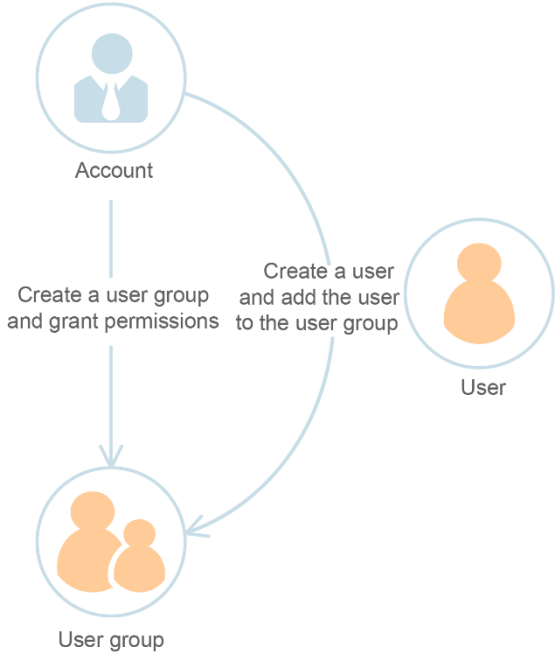
User Access Management & IAM

# Identity Access Management

**Identity and Access Management (IAM)** enables the customer to manage users and control the access to HUAWEI CLOUD services and resources




Account vs IAM Users




User groups

# Identity Access Management – Terminology

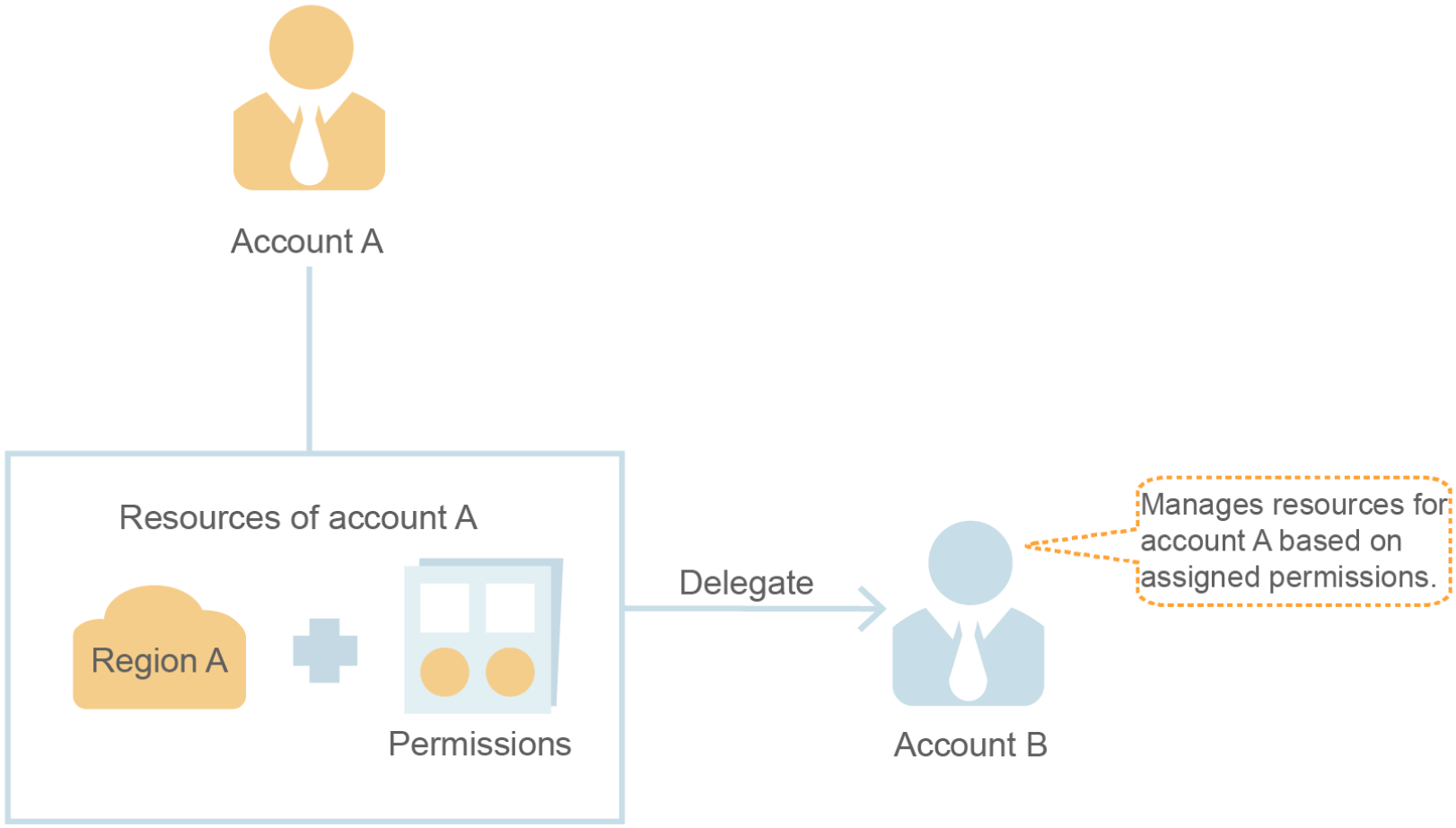
*HUAWEI CLOUD Account* == *Enterprise Administrator* == *Root Account*

- An actual account
- Getting this by register HUAWEI CLOUD with email address

- 1st user under IAM system after the account is created
- Act as the account owner
- Administrator access (under admin user group)
- Cannot be controlled by IAM
- Cannot revoke permission

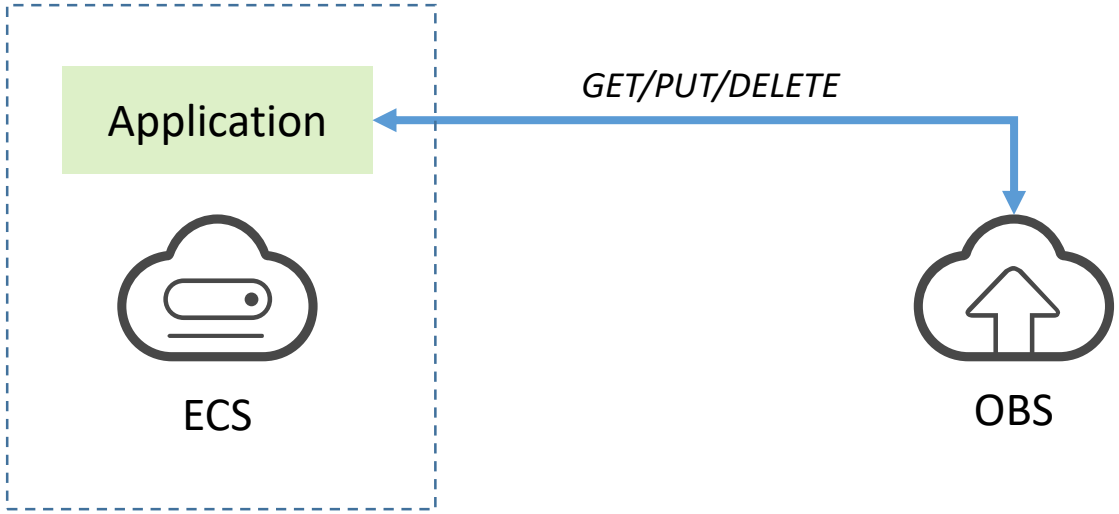
- AWS terminology

# IAM Agency – Delegating resource access to another account



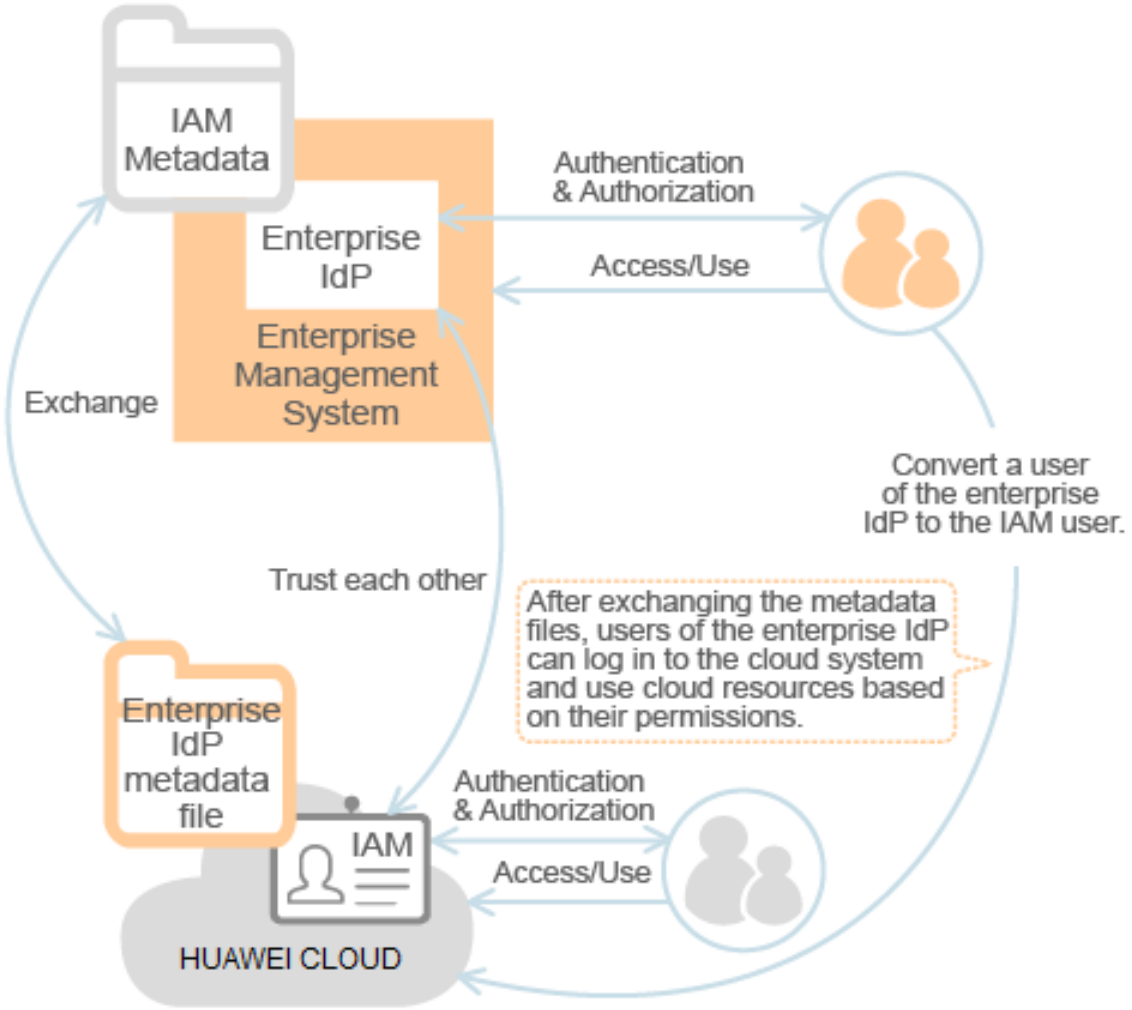
# IAM Agency – Delegating for HUAWEI CLOUD Services

This will allow application to reach OBS without the need for putting any credential in the code

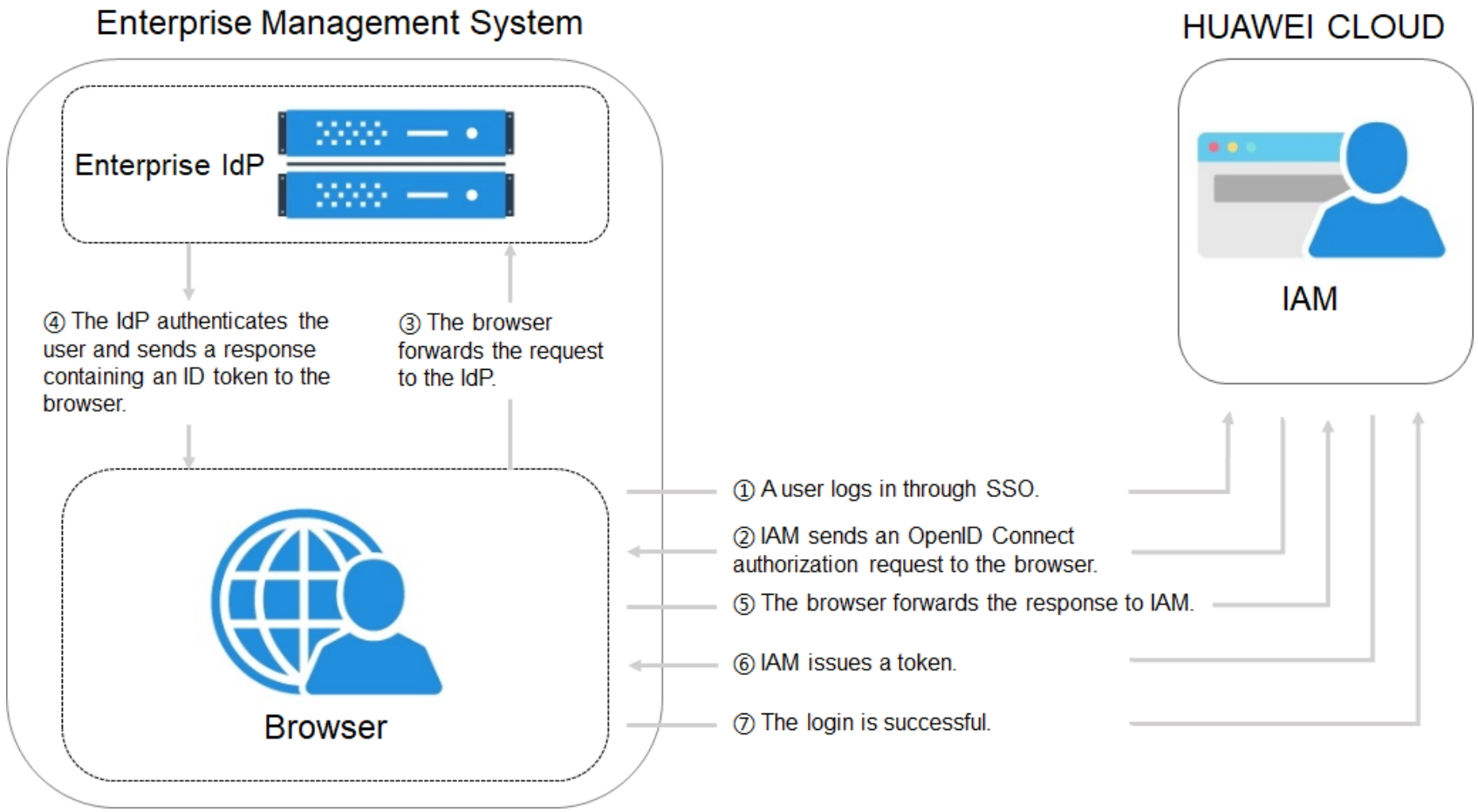



IAM Agency with OBS permission

# SAML-based federated identity authentication



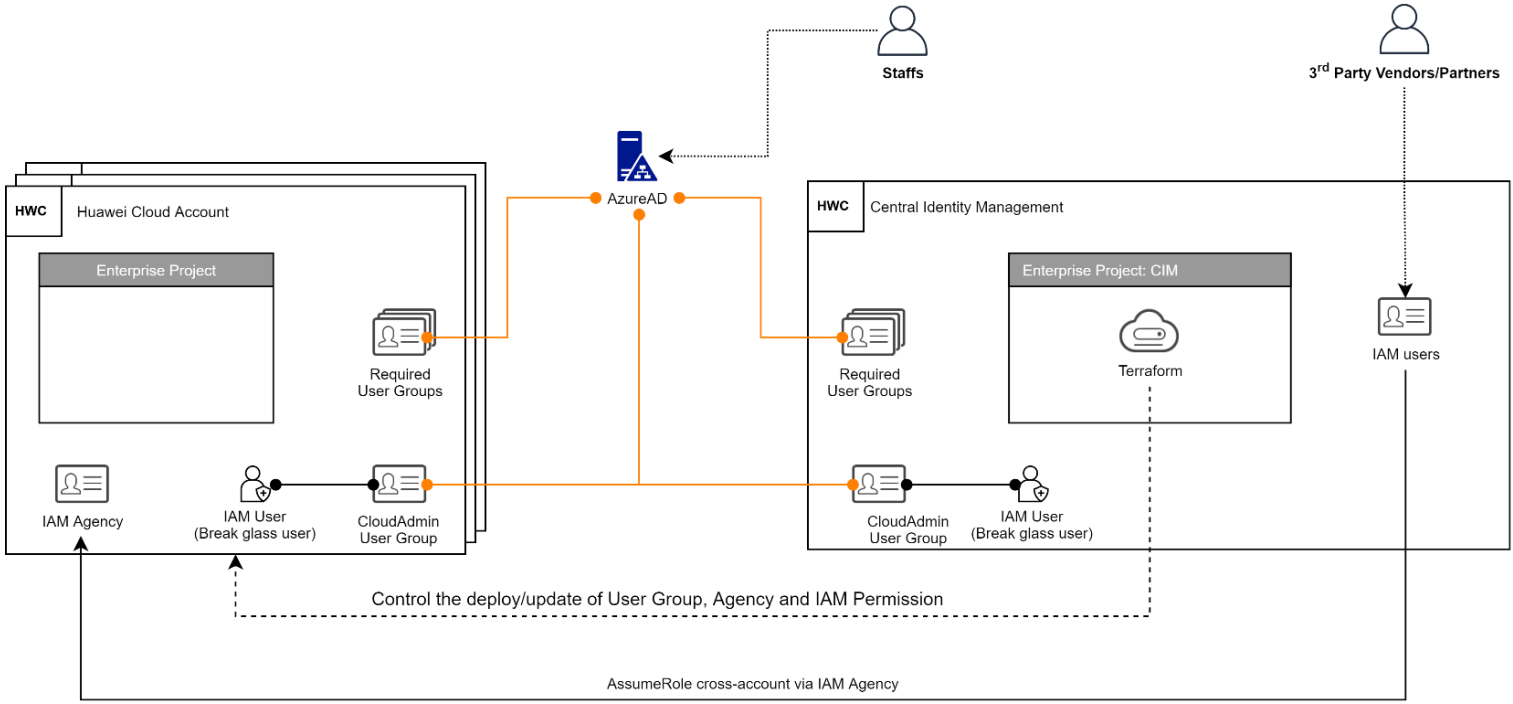
# OpenID Connect–based Federated Identity Authentication



# HUAWEI CLOUD User Access Management with AzureAD and Local IAM Users

## EPS, IAM User Groups & IAM Agency

- Manually mapping Azure AD vs IAM User Groups via Claim Rules
- Requires additional script to use AK/SK with federated user
- IAM IdP has to be configured in every account
- Local IAM users will be created for 3rd Party Vendors or Partners to use IAM Agency for cross-account access
- Recommend to use Terraform for CUD (Create, Update, Delete) IAM User Groups and IAM Permission on every account




*Remark: Restricted Console/API access via IP Addresses are available only for IAM Users*

# Huawei Cloud Landing Zone

Account Security Baseline

# HUAWEI CLOUD Account Security Baseline

## Access Control

**Identity and Access Management (IAM)**
Control user access and permission on Huawei Cloud

## Audit and Governance

**Resource Compliance**
Enable to record/track configuration changes of resources on Huawei Cloud. Define rules to audit the resource compliance violation

**Cloud Trace Service (CTS)**
Collect audit logs for events on Huawei Cloud.

# HUAWEI CLOUD Account Security Baseline

## Security Notifications

**Key Event Notification on CTS**
Configure Key Event Notification based on monitored event.

**Alarm Rules on Cloud Eyes**
Create Event Monitoring in Alarm Rules to monitor and trigger alarm based on supported resource type event

**Metric Filter on CTS System Event via LTS**
Create a metric filter on Log Stream to monitor specific CTS parameter and configure alarm rules based on the metric filter

# HUAWEI CLOUD Account Security Baseline

## IAM Baseline

- Reduce the permanent credential usage as much as possible. Rely on temporary tokenize with validity expiration period
- Configure password policy to enforce a strong password
- Bind MFA for IAM users, root account
- Lock down root and protect root account at all cost
- Create and document a process for adding/removing IAM users and integrate with employee provisioning/de-provisioning process
- Leverage managed permission roles/policies

# HUAWEI CLOUD Account Security Baseline

## CTS Baseline

- Enable 1 system tracker and store log in OBS bucket
- Enable verification check to ensure log integrity
- To get OBS log, enable data tracker

## Resource Compliance Baseline

- Enable the recorder
- Try leveraging default Resource Rule or follow CIS rules

# Huawei Cloud Landing Zone

Logging & Alerting

# HUAWEI CLOUD Logging & Monitoring Services

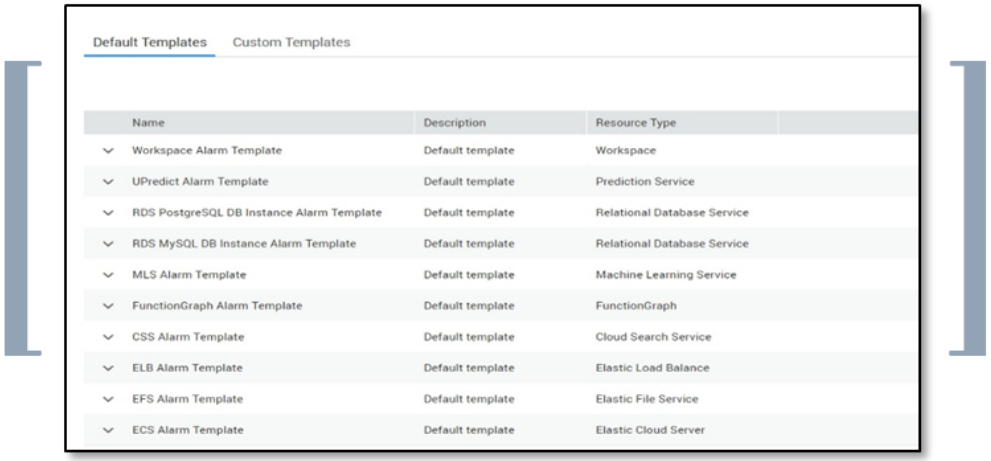
- ✓ Real-time log collection
- ✓ Real-time log query
- ✓ Unified log storage



- ✓ Automated service provisioning
- ✓ Real-time data collection
- ✓ Comprehensive monitoring screen

- ✓ User behavior analysis
- ✓ Fault locating and troubleshooting
- ✓ Security compliance audit

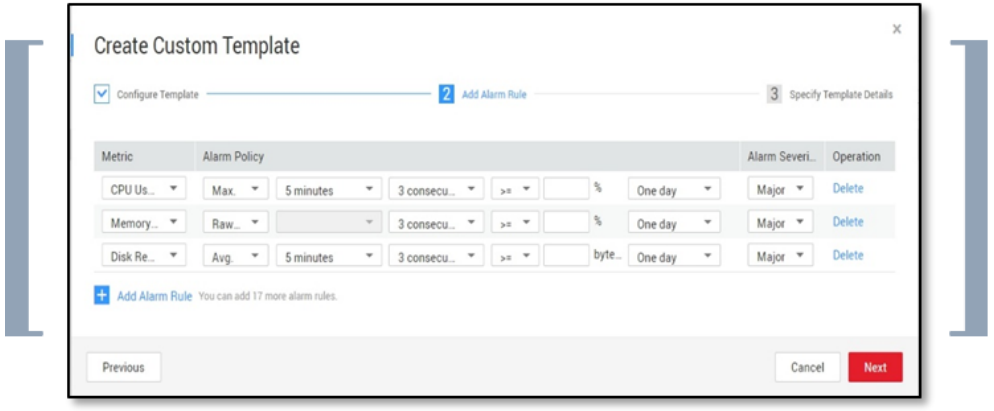
# HUAWEI CLOUD Cloud Eye Alarm Rules




## Alarm rules

Notifications of three status changes
(Alarm, insufficient data, and recovery)

Four alarm notification modes
(SMS, email, HTTP, and HTTPS)



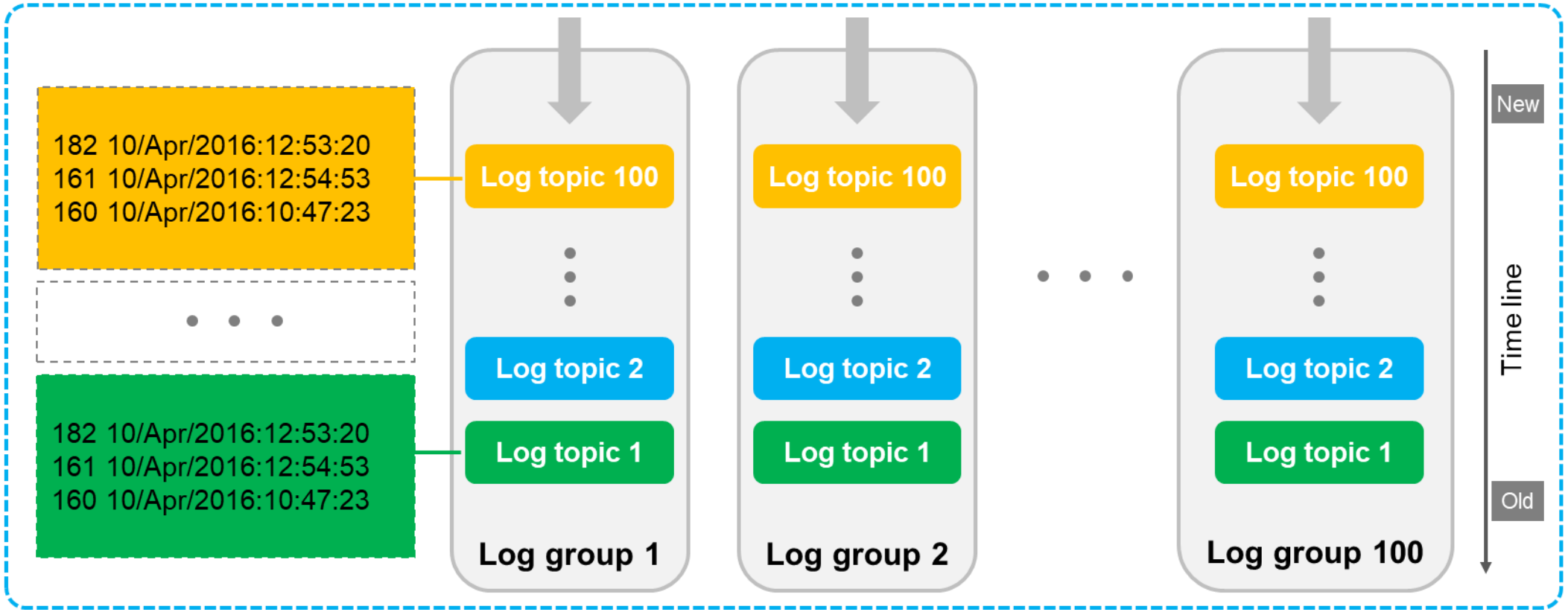

## Alarm template

Quick and batch creation of alarm rules

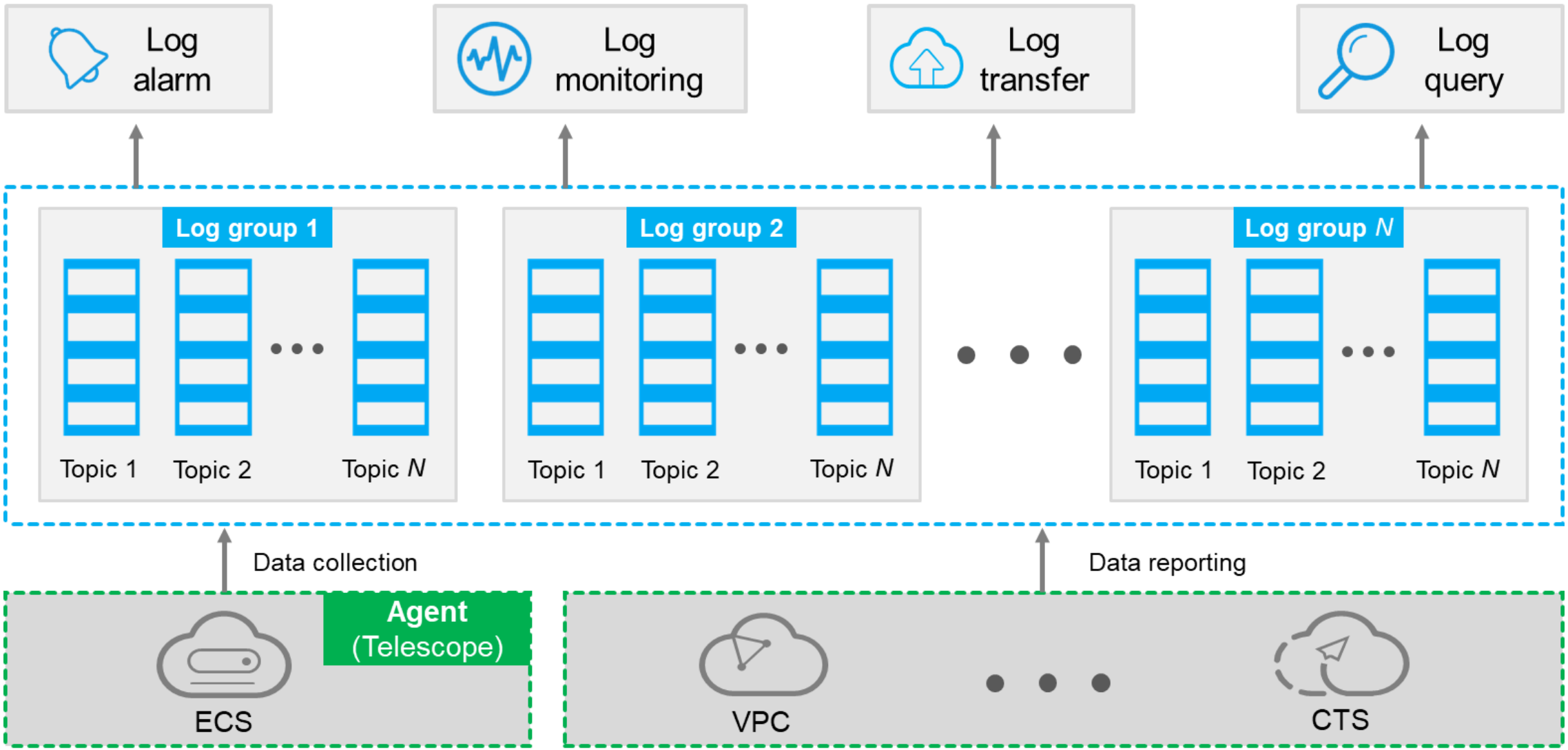
Efficient creation of alarm rules with preset alarm templates

# HUAWEI CLOUD Log Tank Service

- A log group is a collection of logs and a basic unit for log management. You can transfer logs to log groups for storage to facilitate log queries.
- A log topic is the basic unit of a log group. Each log group contains a maximum of 100 log topics.



# HUAWEI CLOUD Log Tank Capabilities

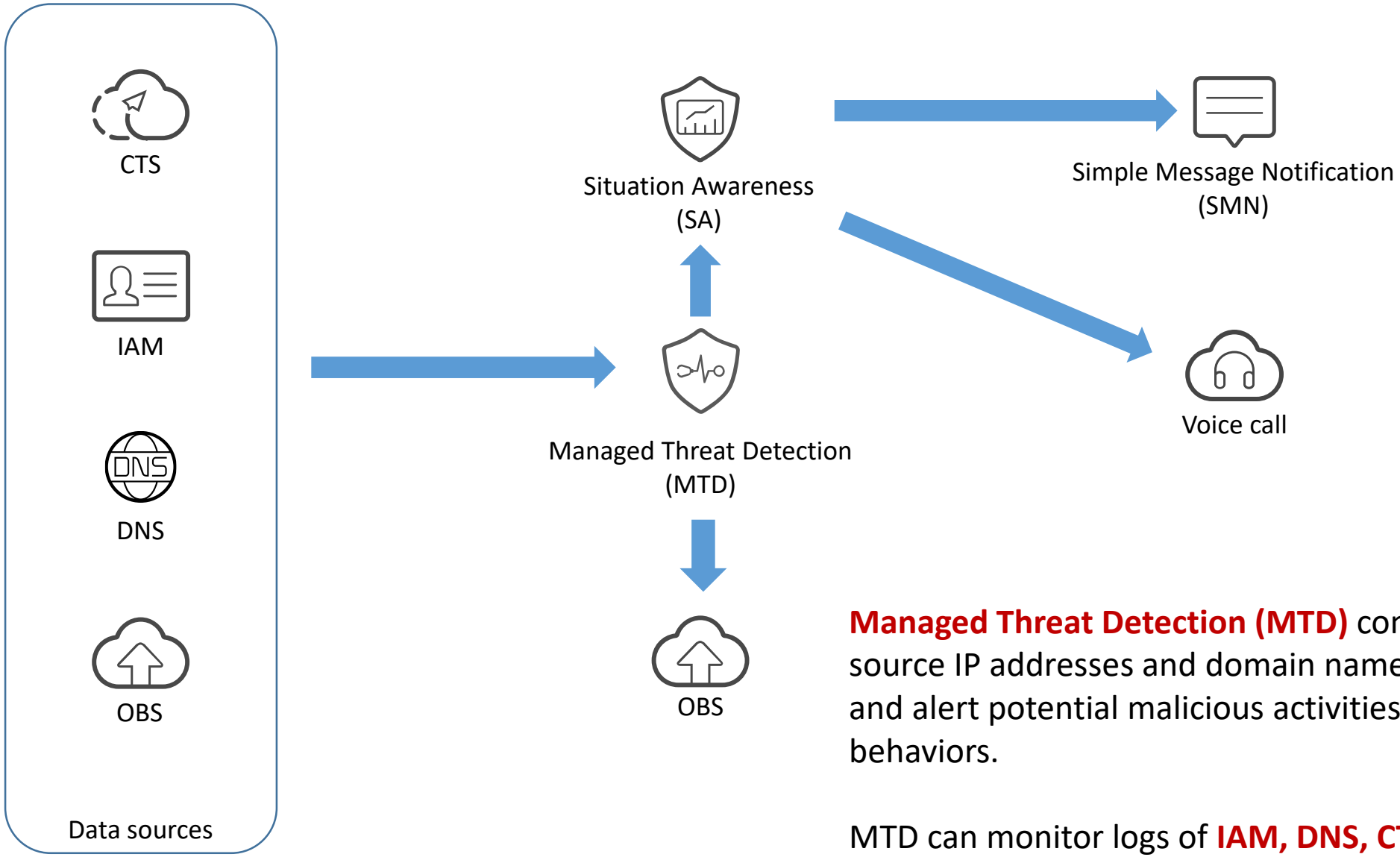


# HUAWEI CLOUD Sample Event Monitoring

## Event Monitoring with Cloud Trace Key Event Notification

| Event Name | Description |
| --- | --- |
| Root Login | Send notification when there is a login event of Enterprise administrator |
| CTS Change | Send notification when there is a change on CTS tracker |
| KMS Change | Send notification when there is a schedule for key deletion or disable KMS key |
| Bucket Policy Change | Send notification when there is a change on OBS bucket policy |
| VPC Change | Send notification when there is a change on the VPC |
| Password Policy Change | Send notification when there is a change on password policy |
| Security Group Change | Send notification when there is a change on security group |

# HUAWEI CLOUD Managed Threat Detection (MTD)




**Managed Threat Detection (MTD)** continuously checks source IP addresses and domain names in cloud service logs and alert potential malicious activities and unauthorized behaviors.

MTD can monitor logs of **IAM, DNS, CTS, OBS and VPC**, all of which are global services in the customer account.

# MTD Detection Scenario – IAM

| Service | Type | Finding |
|---|---|---|
| IAM | Risk password | Weak password |
| | | Password shared by multiple accounts |
| | Credential AK/SK Disclosure | Voucher leakage |
| | | Credential usage exception |
| | Token Utilization | Token disclosure |
| | | Token invoking exception |
| | Abnormal Delegation | Malicious entrustment |
| | | Entrusted account exception |
| | Brute Force Cracking | One-on-one break |
| | | A pair of multi-bursts |
| | | Many-to-one break |
| | | Many-to-multi-break |
| | Unknown Threat | Floating IP port attack |
| | | Distributed attack |
| | Abnormal IP Address Access | Abnormal, Suspicious, Blacklist |
| | | Detection, Vulnerability, Breach |
| | | CNC, DDoS, Sinkhole, Botnet |
| | | Agent, mining, mining pool |
| | | Spam, phishing, fraud, onion network |
| | | Malicious scanning, website, crawler |

*Detail IAM Alarm type:* *here*

# MTD Detection Scenario – DNS

| Service | Type | Finding |
|---|---|---|
| DNS | DGA Domain Name | Remote control botnet trojans periodically access the C&C server through the DGA domain name |
| | | Hosts are controlled by hackers to send spam |
| | DNS tunnel communication | A large number of frequently accessed tunnel domain names |
| | | Hackers use DNS tunnels to remotely control victim hosts |
| | | Hackers use DNS tunneling to transfer data files |
| | Mining behavior | A large number of frequent accesses to mine pool domain names and actual communication |
| | | Mining trojan horse consumes a large amount of computing resources of the victim host for mining |
| | Extortion | The ransomware uses the DGA domain name to access a specific C&C server, uploads local information, downloads the encrypted private key and public key, and uses the private key and public key to encrypt the file |
| | | Important files are encrypted by ransomware |
| | Malicious domain name access | Adware |
| | | CNC Server |
| | | Vulnerability exploit domain name |
| | | Malicious websites, malware |
| | | Mine machine, pool |
| | | Spam, phishing, payment domain name |
| | | Suspicious domain name |

*Detail DNS Alarm type:* *here*

# MTD Detection Scenario – OBS

| Service | Type | Finding |
|---|---|---|
| OBS | User first access | User first access |
| | | IP first access |
| | | Client first appearance |
| | | First cross-domain access |
| | Abnormal access frequency | User access frequency |
| | | IP access frequency |
| | | User + IP access frequency |
| | | IP address switchover exception |
| | Operation sequence exception | User operation exception |
| | | IP operation exception |
| | | The sequence of user + IP access operation is abnormal |
| | The download operation is abnormal | The number of IP address is abnormal |
| | | The number of accounts are abnormal |
| | | Abnormal download volume |
| | | Abnormal user + IP download volume |
| | Location physical logic | Geographical location anomaly |
| | | Network area exception |
| | | Common read/write exception |
| | | Unauthorized access exception |
| | Other exceptions | Access status code conversation |
| | | Off-working hours access |
| | | Non-working time operation |
| | | IP address switchover exception |

*Detail OBS Alarm type:* *here*

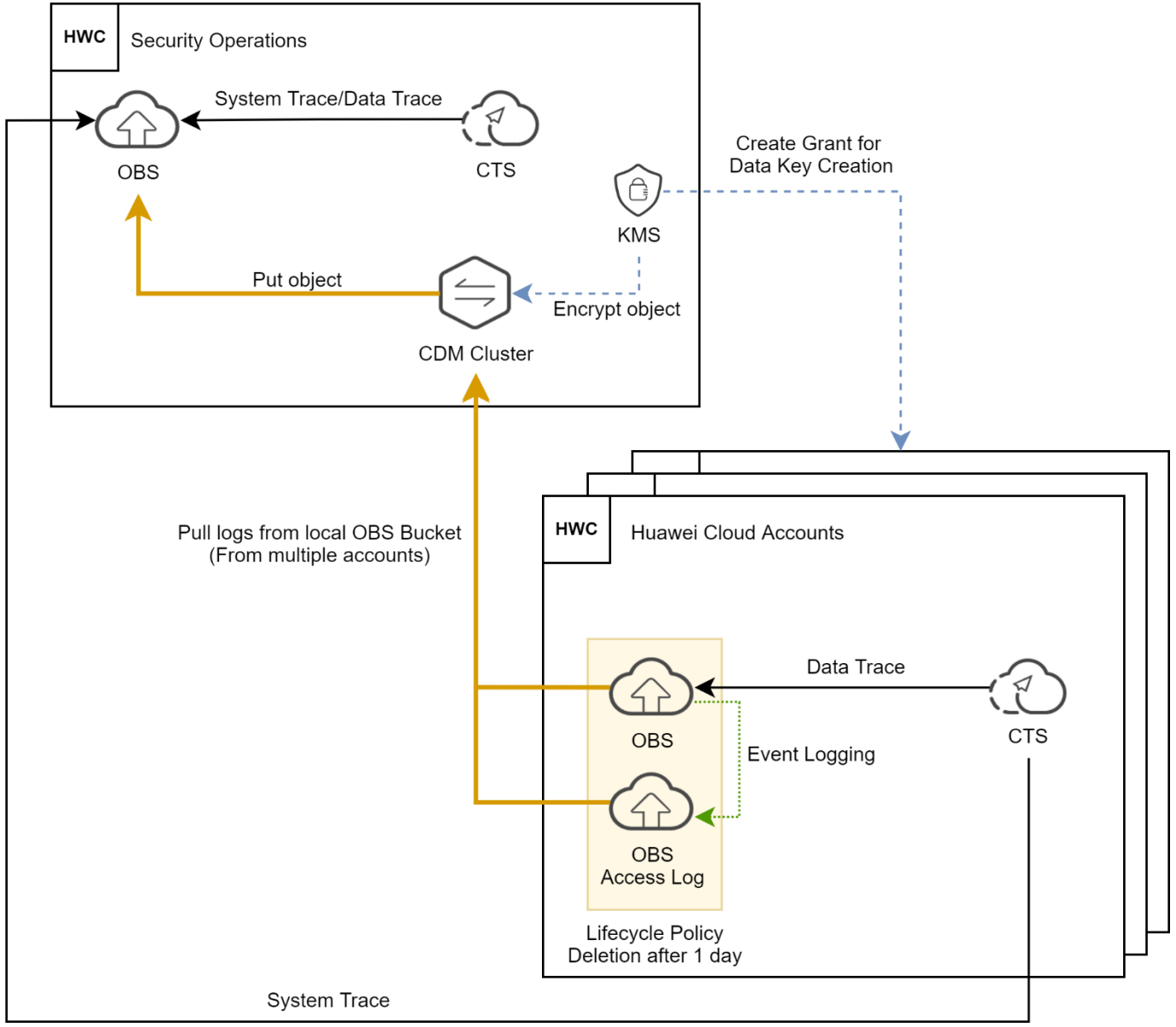
# MTD Detection Scenario – CTS

| Service | Type | Finding |
| --- | --- | --- |
| CTS | Modifying network permissions | Modifying a security group |
| | | Modifying a route |
| | | Modifying an ACL |
| | Modifying a resource policy | Modifying a resource security access policy |
| | Modifying an account policy | Add user |
| | | Delete user |
| | | Add user policy |
| | Starting computing resources | Starting ECS resources |
| | | Abnormal OBS usage |
| | Changing the password policy | Changing the password |
| | | Modify associated mobile number |
| | Dark network access | IP call API of the Tor Network egress |

*Detail CTS Alarm type:* *here*

# HUAWEI CLOUD Centralized Logging

- CTS System Trace will deliver log directly from CTS to OBS Bucket in Security Operation
- Required CDM Cluster to configure a job for pulling data trace log and OBS access log from each OBS bucket in several accounts
- Minimum leased time is at least 5 mins
- **CTS System Trace:** 1 OBS Bucket for 1 Account
- **CTS Data Trace and OBS Access Log:** 1 OBS Bucket for every account and separated by account name
- OBS Bucket is encrypted with specific CMK-KMS
  - KMS-Obs
- OBS event logging is enabled for OBS Buckets
- Lifecycle Policy is set for OBS bucket at the origin to delete the log after 1 day of creation



# Huawei Cloud Landing Zone

Data Protection & Encryption

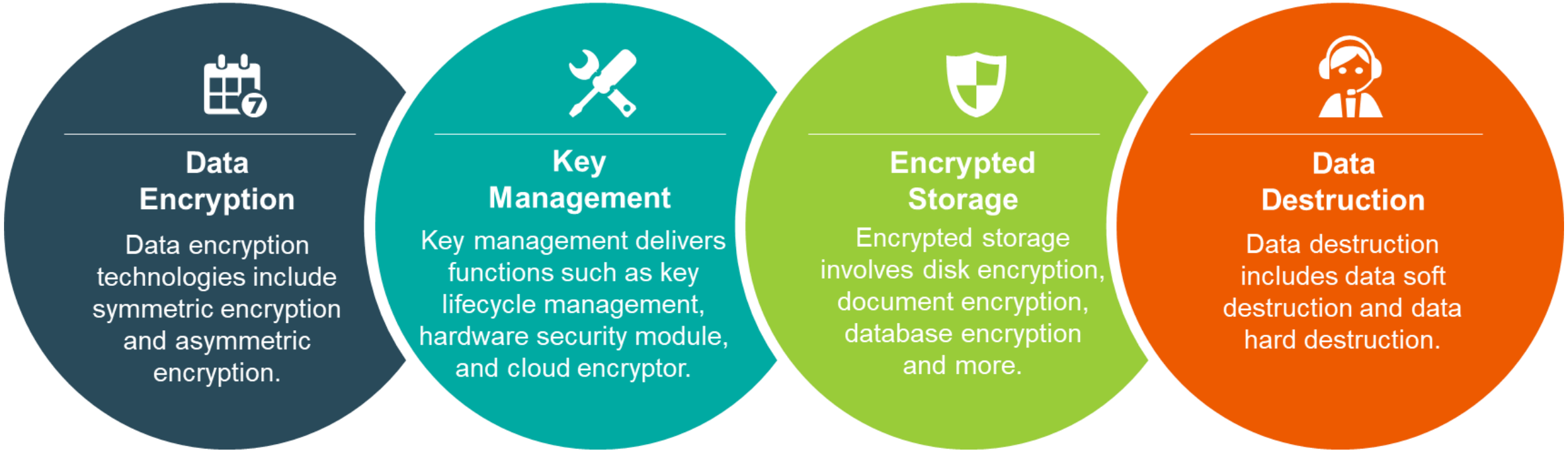
# HUAWEI CLOUD Data Privacy consideration

- Customers select where to store the data
- Data will not be replicated to other region unless the customer said do
- Customers always own the data, ability to encrypt, move and delete

HUAWEI CLOUD Customer Agreement

Privacy Statement_HUAWEI CLOUD

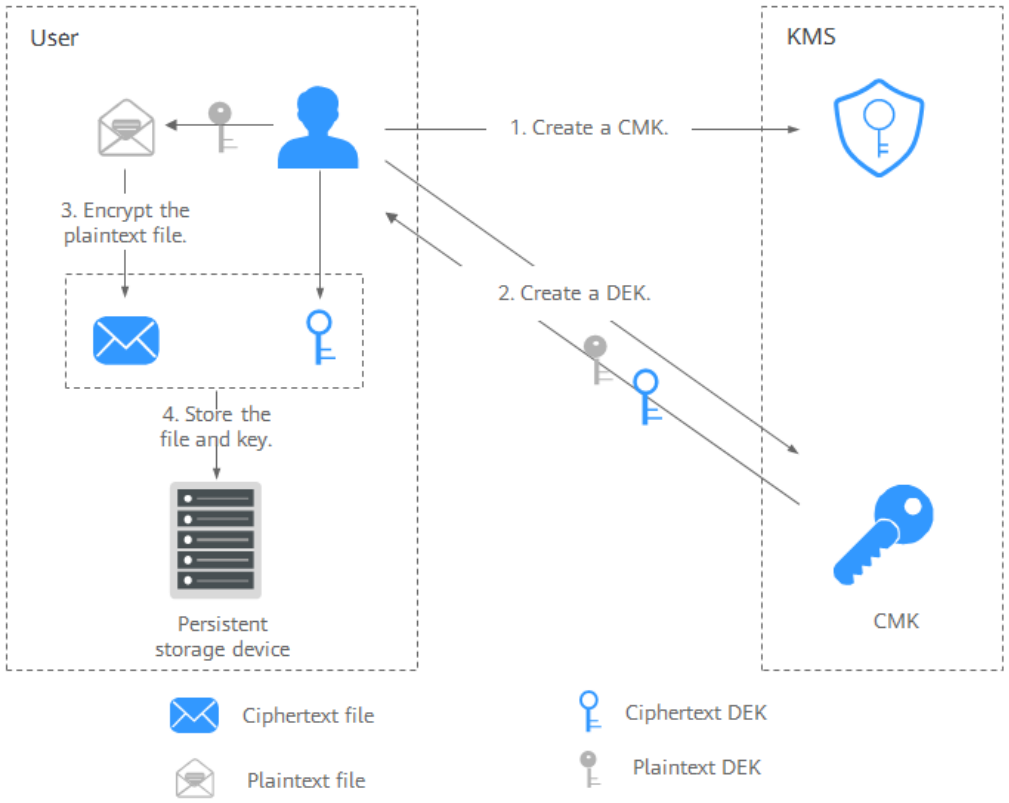
# HUAWEI CLOUD Data Storage Security Technologies



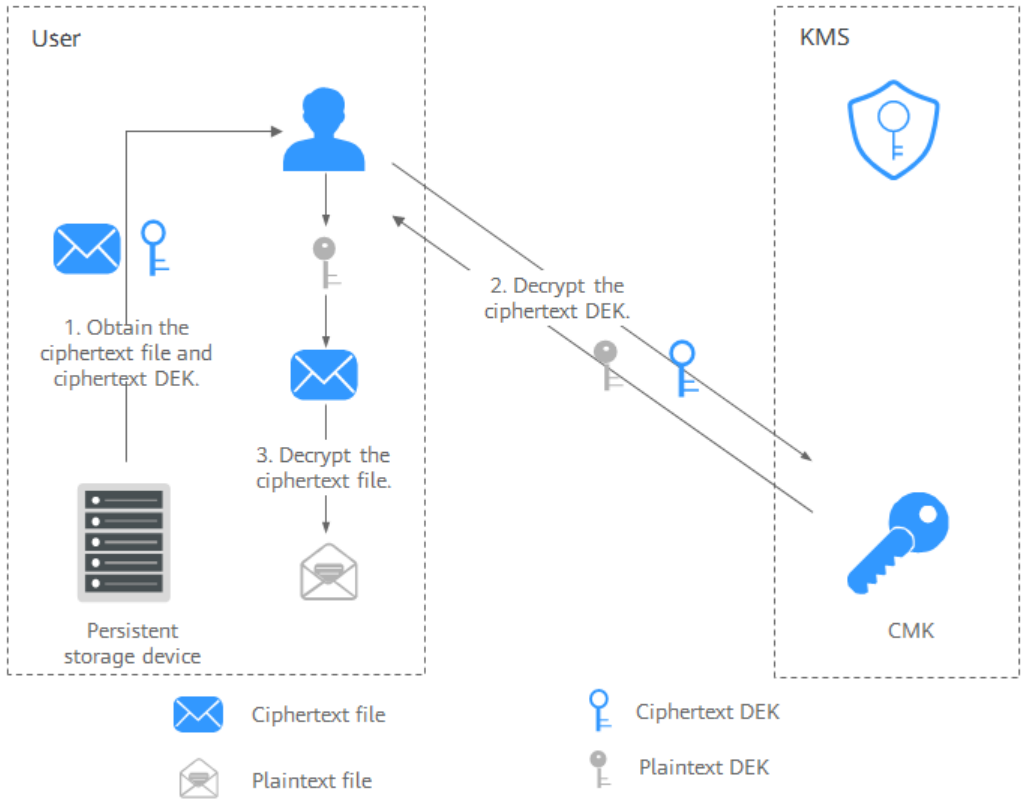
# HUAWEI CLOUD KMS – Data Keys and CMKs

A Customer Master Key (CMK) is created by user on KMS. It is used to encrypt and protect Data Encryption Key (DEKs). One CMK can be used to encrypt one or multiple DEKs.

A data key is used by users to encrypt data and is protected by CMD. To encrypt or decrypt data, decrypt the DEK using the CMK first

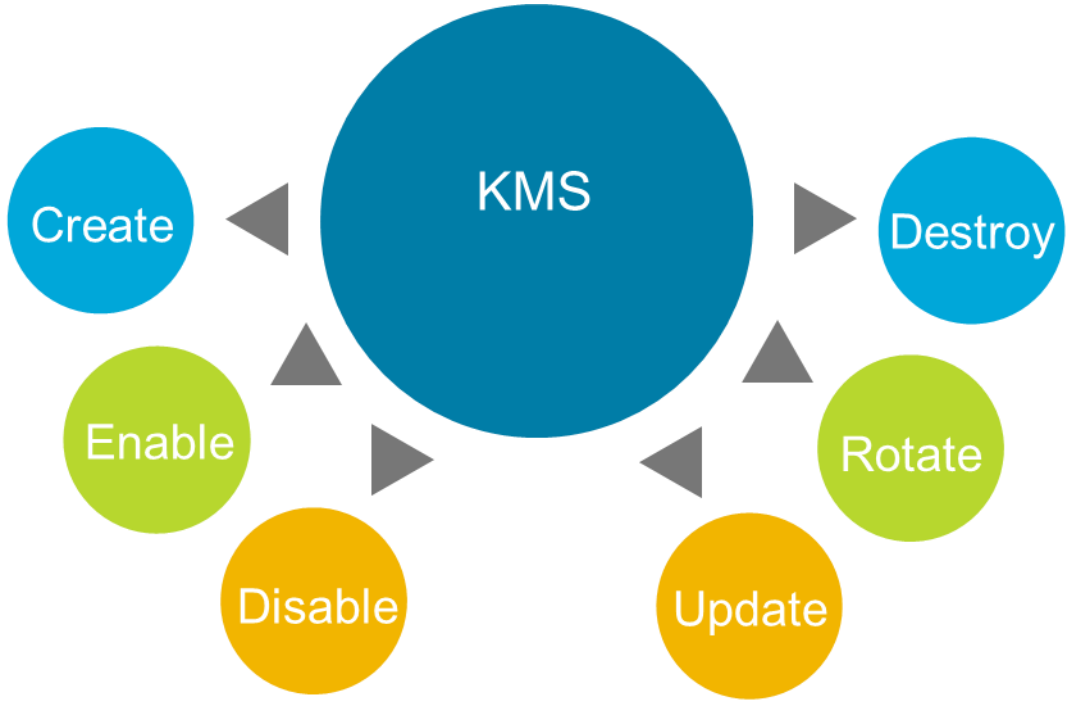



Encrypting data



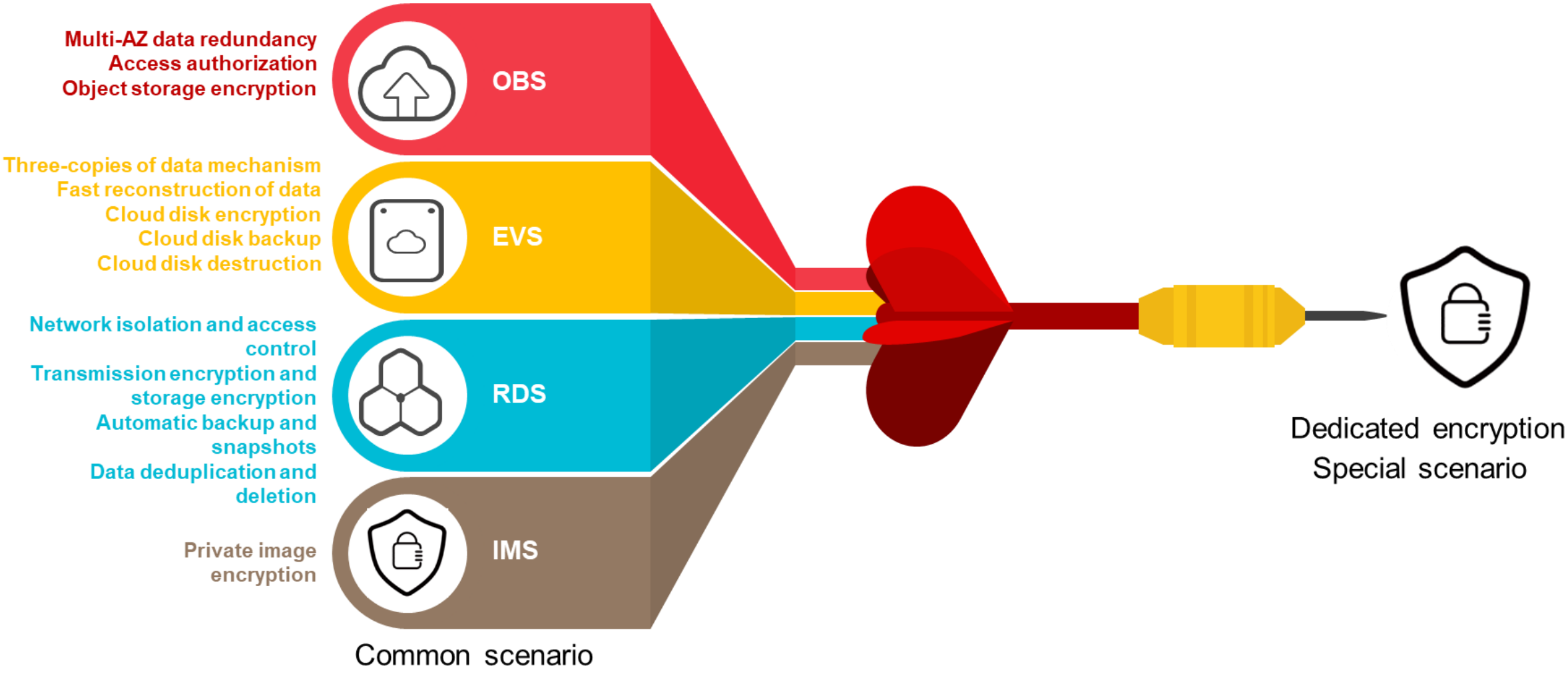

Decrypting data

# HUAWEI CLOUD KMS Key Lifecycle




Key Management Service (KMS) is a secure, reliable, and easy-to-use key hosting service. It helps manage keys and keep keys properly. It uses Hardware Security Module (HSM) to create and manage keys, preventing plaintext keys from being exposed outside the HSM, thus ensuring key security.

# HUAWEI CLOUD Data Storage Overview



# HUAWEI CLOUD Sample Scenarios

| Storage Type | Confidentiality | Reliability |
| --- | --- | --- |
| EVS | KMS provides keys. A customer master key (CMK) is generated, managed, and destroyed by KMS and used to encrypt and decrypt data encryption keys. HUAWEI CLOUD offers the volume encryption function. | Three-copies of data mechanism ensure 99.99995% availability.<br>VBS backs up, restores, and creates EVS disks. |
| VBS | KMS provides keys. A customer master key (CMK) is generated, managed, and destroyed by KMS and used to encrypt and decrypt data encryption keys. HUAWEI CLOUD offers the volume encryption function. | Data durability reaches 99.999999999%. |
| OBS | OBS offers two key management modes:<br>• SSE-C mode. If a key is provided by the customer, the customer needs to provide the key, hash value of the key, and AES256 encryption algorithm. Requests should be sent using HTTPS.<br>• SSE-KMS mode. KMS provides and manages keys. When a user uploads an object encrypted using SSE-KMS to a bucket in a region, OBS automatically creates a CMK used to encrypt and decrypt the keys. | Data reliability is 99.999999999% and service availability is 99.99%.<br>Data consistency is checked before the storage to ensure that data to be stored is the data uploaded.<br>Data shard redundancy: Data shards are stored redundantly on different disks. The system checks data consistency and recovers damaged data automatically at the backend. |
| RDS | RDS offers data confidentiality from the following two aspects:<br>• Encrypt database files through the database management system. In this case, it is difficult to decode the data when it is disclosed or lost.<br>• Recommend customers to encrypt the data to be uploaded and store the data in the database. | Three-copies backup ensures 99.99995% data durability; active and standby RDS instances can be quickly switched over when a fault occurs. The service availability reaches 99.95%.<br>Automatic backup and snapshot creation are available. Data can be restored to a point in time. |
| IMS | KMS provides keys. A CMK is generated, managed, and destroyed by KMS and used to encrypt and decrypt data encryption keys. You can create an encrypted image using an encrypted ECS or an external image file. | Multiple redundant copies of private images are used, reaching 99.999999999% durability. |

# Thank you