

# Alibaba Cloud

智能接入网关

Product Introduction

Document Version: 20220523

# Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please directly contact Alibaba Cloud for any errors of this document.

# Document conventions

Style	Description	Example
 <b>Danger</b>	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
 <b>Warning</b>	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 <b>Notice</b>	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> If the weight is set to 0, the server no longer receives new requests.
 <b>Note</b>	A note indicates supplemental instructions, best practices, tips, and other content.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click <b>Settings&gt; Network&gt; Set network type</b> .
<b>Bold</b>	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[ ] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

# Table of Contents

1.What is SAG? .....	05
2.Functions and features .....	08
3.Benefits .....	10
4.Terms .....	11
5.Limits .....	12
6.Smart Access Gateway device .....	14
6.1. Deployment modes .....	14
6.2. Network topology .....	15
6.3. HA topology .....	19

# 1. What is SAG?

Smart Access Gateway (SAG) is a one-stop solution for connecting private networks to Alibaba Cloud. You can connect private networks to Alibaba Cloud through SAG in a secure, intelligent, and reliable way.

## Product types

SAG provides the following types:

- **SAG customer-premises equipment (CPE) devices:** applicable to connecting sites to Alibaba Cloud.

After you deploy SAG CPE devices in your data centers and branch offices, you can connect your private networks to Alibaba Cloud. SAG CPE devices provide the following models: SAG-100WM and SAG-1000.

- **SAG-100WM** devices can be placed on desks and in extra-low voltage boxes. You can connect broadband and 4G networks to the WAN ports, and wired and Wi-Fi networks to the LAN ports. The maximum bandwidth of encrypted private networks supported by SAG-100WM devices is 50 Mbit/s (the packet length in the performance test is 512 bytes). SAG-100WM devices are suitable for quickly connecting small branch offices and stores to Alibaba Cloud.
  - **SAG-1000** devices can be placed on server racks. You can connect a hybrid network that consists of Express Connect circuits, broadband networks, and 4G networks to the WAN ports, and wired networks to the LAN ports. The maximum bandwidth of encrypted private networks supported by SAG-1000 devices is 500 Mbit/s (the packet length in the performance test is 512 bytes). SAG-1000 devices are suitable for connecting data centers and large branch offices to Alibaba Cloud.
- **SAG vCPE:** applicable to connecting sites to Alibaba Cloud.

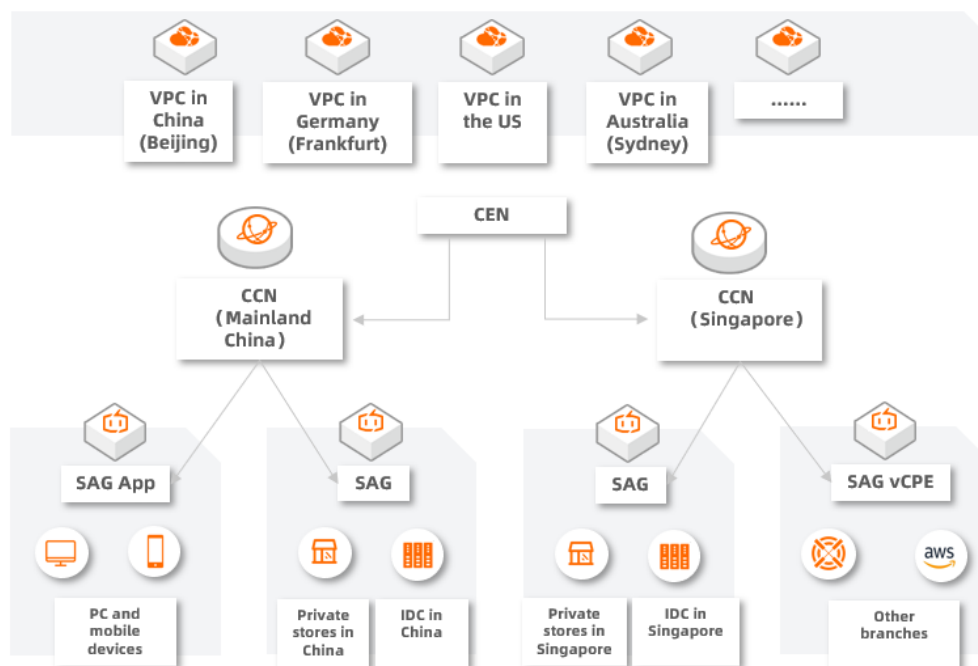
SAG vCPE provides an image that can be deployed on data center servers, Edge Node Service (ENS) instances, Alibaba Cloud instances, Amazon Web Services (AWS) instances, and Microsoft Azure instances. After you deploy the SAG vCPE image on an instance, the instance serves as a vCPE device. The bandwidth of private networks for encrypted connections can reach 300 Mbit/s and higher (the packet length in the performance test is 1,024 bytes). This allows you to connect private networks to Alibaba Cloud in a more flexible way.

- **SAG app:** applicable to connecting terminals to Alibaba Cloud.

You can install the SAG app on terminals such as computers and mobile phones to connect them to Alibaba Cloud. The SAG app supports the following operating systems: Windows (Windows 7 SP1 and later), macOS (10.11.1 and later), Android (5.0 to 10.0), and iOS (12.0 and later).

## Components

The following figure shows a use scenario of SAG. In this scenario, data centers and branch offices are connected to Alibaba Cloud through SAG devices. Terminals such as computers and mobile phones are connected to Alibaba Cloud through the SAG app. Other networks are connected to Alibaba Cloud through SAG vCPE. After your networks are connected to Alibaba Cloud, you can use Cloud Enterprise Network (CEN) to connect the following networks in different regions: virtual private clouds (VPCs), data centers, branch offices, mobile clients, and other network nodes on Alibaba Cloud. This forms an enterprise network that is centered on Alibaba Cloud.



Component	Description	Background information
SAG CPE	CPE devices	<a href="#">What is SAG?</a>
SAG vCPE	vCPE devices	<a href="#">What is SAG vCPE?</a>
The SAG app	The SAG app	<a href="#">What is the SAG app?</a>
Cloud Connect Network (CCN)	A matrix of Alibaba Cloud distributed gateways	<a href="#">What is CCN?</a>
CEN	Connect networks across regions	<a href="#">What is CEN?</a>
VPCs	Private networks on Alibaba Cloud	<a href="#">What is a VPC?</a>

## Architecture

SAG uses a Software Defined Wide Area Networks (SD-WAN) architecture based on cloud-native technologies of Alibaba Cloud. Compared with the traditional SD-WAN architecture, SAG offers the following benefits:

- Zero touch provisioning (ZTP) installation and deployment to facilitate management and O&M

Alibaba Cloud provides you with a software-defined method to manage SAG CPE devices by using the SAG console, API, and CloudMonitor. Managing SAG CPE instances is similar to managing VPCs and Elastic Compute Service (ECS) instances.

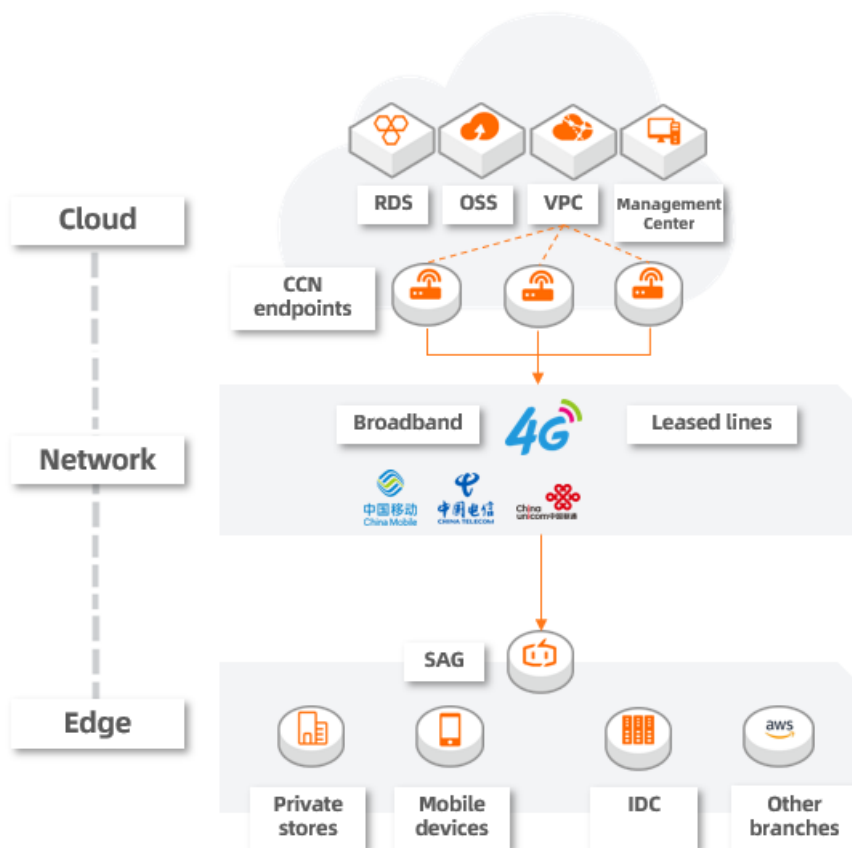
- Hybrid networks

SAG provides a data plane based on private WANs on Alibaba Cloud. You can connect private networks to Alibaba Cloud through a hybrid network that consists of Express Connect circuits, broadband networks, and 4G networks. This increases the utilization of Express Connect circuits and improves network performance.

- Integration of networks and cloud services

An architecture that integrates the cloud, networks, and edge:

- SAG supports automatic protocol negotiation between the on-premises VPN and cloud VPN. No additional configuration is required.
- Quick access from private networks to Alibaba Cloud services.
- End-to-end security policies for both on-premises and cloud workloads.




## 2.Functions and features

Smart Access Gateway (SAG) allows you to connect private networks to Alibaba Cloud over WANs, 4G networks, and Express Connect circuits. SAG also provides various features such as flow logs, access control lists (ACLs), and NAT to facilitate network management.


### Multiple network types

SAG allows you to connect private networks to Alibaba Cloud over WANs, 4G networks, and Express Connect circuits. These network connections support the active-standby mode to ensure high availability.

- Active and standby connections - WAN and 4G: SAG devices can be connected to Alibaba Cloud over WANs and 4G networks. Connections over WANs and 4G networks support the active-standby mode.

 **Note** Each SAG device has a built-in 4G SIM card. However, this card is used only to receive configurations from Alibaba Cloud and does not support data transfer. We recommend that you purchase a 4G SIM card that supports data transfer from an Internet service provider (ISP). After you insert the card into an SAG device, the card can provide a standby network connection. When an error occurs to the WAN connection, the 4G network connection takes over.

- Active and standby connections - SAG and Express Connect: If your private networks are already connected to Alibaba Cloud over an Express Connect circuit, you can use an SAG device to provide a standby connection.
- Active and standby connections - Express Connect and Internet: SAG supports Internet connections and connections over Express Connect circuits as active and standby connections. When the active connection is down, the standby connection takes over.

 **Note** Only SAG-1000 devices support connections over Express Connect circuits. SAG-100WM devices do not support connections over Express Connect circuits. For more information, see [What is Express Connect?](#).

### Routing method

SAG devices support multiple routing methods, including static routing, Border Gateway Protocol (BGP) dynamic routing, and Open Shortest Path First (OSPF) dynamic routing. For more information, see [Add a static route](#).

### Quality of service (QoS)

SAG supports QoS policies that consist of 5-tuples. You can create QoS policies to prioritize your workloads and allocate bandwidth resources based on workload priorities.

You can use QoS policies to allocate bandwidth resources for data transmission and reduce network latency, packet loss, and network jitter. This improves the network performance.

If you use different service systems such as enterprise resource planning (ERP), office automation (OA), and order management, these systems may compete for bandwidth resources. As a result, business-critical services may have insufficient bandwidth resources, which causes packet loss.

In this case, you can create QoS policies to properly allocate bandwidth resources based on the priorities of your services. This ensures that your business-critical services have sufficient bandwidth resources. For more information, see [What is a QoS policy?](#).



## NAT

SAG supports NAT. You can use NAT to hide private IP addresses, resolve IP conflicts in private networks, and improve network security.

- SNAT: hides private IP addresses and resolves IP conflicts in private networks. You can use SNAT to translate private IP addresses to public IP addresses. This way, you can use the SAG device to access external networks over the Internet. However, your private networks cannot be accessed over the Internet. For more information, see [Configure an SNAT rule](#).
- DNAT: maps private IP addresses to public IP addresses. Your private networks can provide services over the Internet. For more information, see [Add a DNAT rule](#).

## ACLs

SAG supports ACLs that allow you to configure whitelists and blacklists for different SAG instances. For more information, see [Overview](#).

## Flow logs

SAG supports flow logs that can record information about inbound and outbound traffic of SAG instances. Flow logs help you monitor network traffic and troubleshoot network errors. You can also analyze workloads and make informed business decisions based on flow logs. For more information, see [Overview](#).

## Health checks

SAG supports health checks. You can create a health check to test the network connectivity between an SAG device and the destination. For more information, see [Create a health check instance](#).

## 3. Benefits

SAG is intelligent, secure, and reliable. It provides a management platform to help you facilitate gateway management.

### Intelligence

An out-of-the-box service that supports automatic configurations and dynamically adjusts network settings to adapt to network topology changes.

### Reliability

Private networks are connected to the nearest Alibaba Cloud infrastructure through the Internet. Device-based and link-based high availability (HA) ensure reliable connections between private networks and Alibaba Cloud.

- Device-based HA

SAG devices support active-standby mode. When an error occurs to the active device, network connections are switched to the standby device.

- Link-based HA

Each SAG device provides two encrypted links to implement automatic optimal link selection and real-time link failover when errors occur.

### Security

SAG provides encrypted connections among private networks. Data transmitted over the Internet is encrypted and authenticated.

- Data encryption

You can use the IKE and IPsec protocols to encrypt data to ensure secure and reliable data transmission.

- Anti-replay

SAG authenticates data sources to prevent replay attacks.

- Tamper-proofing

SAG provides multiple methods to authenticate data.

### Centralized management

The SAG console allows you to perform management operations centrally.

## 4.Terms

This topic describes the terms of Smart Access Gateway (SAG).

Term	Description
Smart Access Gateway	<p>Smart Access Gateway is a one-stop solution for connecting private networks to Alibaba Cloud.</p> <p>SAG allows enterprises to connect to the nearest VPC network through encrypted connections over the Internet. This is a more intelligent, secure, and reliable approach to migrate workloads to Alibaba Cloud.</p>
Smart Access Gateway device	<p>Smart Access Gateway devices are customer-premises equipment (CPE) devices that connect private networks to Alibaba Cloud.</p> <p>To purchase an SAG device, create an SAG instance in the SAG console. Alibaba Cloud will deliver an SAG device to the specified address. You can also query the shipping status and configure SAG devices in the SAG console.</p>
Cloud Connect Network (CCN)	<p>CCN is a device matrix that consists of Alibaba Cloud distributed gateways.</p> <p>You can associate multiple SAG devices with a CCN instance and then associate the CCN instance with a Cloud Enterprise Network (CEN) instance to establish connections between private networks and Alibaba Cloud.</p>

## 5.Limits

This topic describes the limits on Smart Access Gateway (SAG).

### Limits on SAG instances


Resource	Limit	Adjustable
The maximum number of SAG instances that can be created by an Alibaba Cloud account	500	<a href="#">Submit a ticket</a>
The maximum number of private CIDR blocks that can be associated with an SAG instance	10	<a href="#">Submit a ticket</a>

### Limits on CCN

Resource	Limit	Adjustable
The maximum number of Cloud Connect Network (CCN) instances that can be created by an Alibaba Cloud account	10	<a href="#">Submit a ticket</a>
The maximum number of CCN instances that can be attached to an SAG instance	1	Not supported
The maximum number of Cloud Enterprise Network (CEN) instances that can be attached to a CCN instance	1	Not supported
The maximum number of private CIDR blocks that can be added to a CCN instance	5	<a href="#">Submit a ticket</a>
The maximum subnet length supported by CCN instances	24	Not supported

### Limits on QoS policies

Resource	Limit	Adjustable
The maximum number of quality of service (QoS) policies that can be created by an Alibaba Cloud account	10	<a href="#">Submit a ticket</a>
The maximum number of QoS policies that can be applied to an SAG instance	1	Not supported

Resource	Limit	Adjustable
The maximum number of traffic throttling rules that can be created in a QoS policy	3	<a href="#">Submit a ticket</a> <div>  <b>Note</b> The upper limit is 4.         </div>
The maximum number of traffic classification rules that can be created for a traffic throttling rule	50	<a href="#">Submit a ticket</a>

## Limits on ACLs

Resource	Limit	Adjustable
The number of access control lists (ACLs) that can be created by an Alibaba Cloud account	10	<a href="#">Submit a ticket</a>
The maximum number of ACLs that can be associated with an SAG instance	1	Not supported
The number of ACL rules that can be created in an ACL	50	<a href="#">Submit a ticket</a>

## Limits on SAG devices

Resource	Limit	Adjustable
The maximum number of terminals that can connect to an SAG-100WM device over Wi-Fi	20	Not supported

## Limits on the SAG app

Resource	Limit	Adjustable
The maximum bandwidth supported by the SAG app, in Kbit/s	20000	Not supported

## Limits on enterprise codes

Resource	Limit	Adjustable
The maximum number of enterprise codes that can be created by an Alibaba Cloud account	5	Not supported
The maximum number of characters supported by an enterprise code	5	Not supported

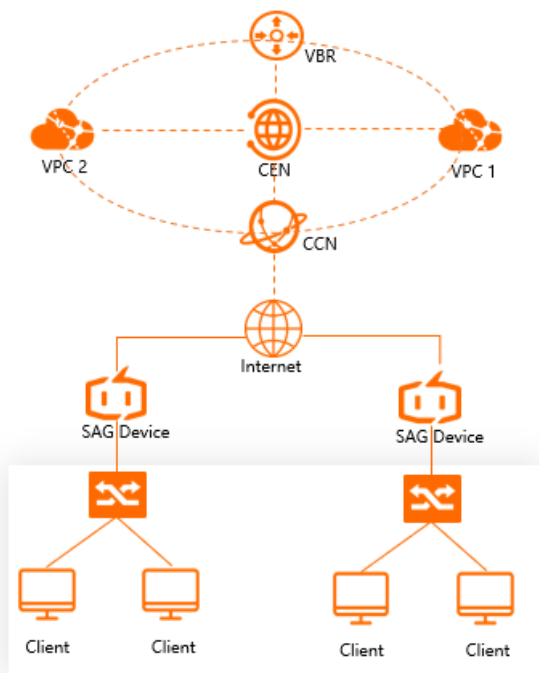
## 6.Smart Access Gateway device

### 6.1. Deployment modes

Smart Access Gateway (SAG) supports two deployment modes: inline mode and one-arm mode.

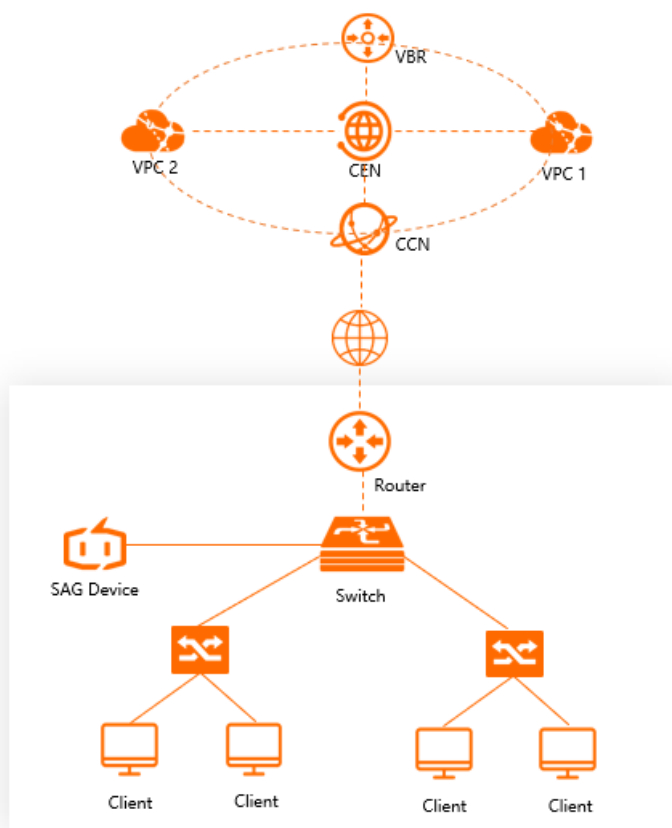
#### Inline mode

SAG devices can connect small office branches and organizations to Alibaba Cloud. In inline mode, all local network traffic must be transmitted through SAG devices.



#### One-arm mode

You can deploy SAG devices in one-arm mode, which avoids networking changes. In one-arm mode, traffic within the private network is transmitted through SAG devices. Network traffic destined for the Internet is transmitted through your Internet-facing device.

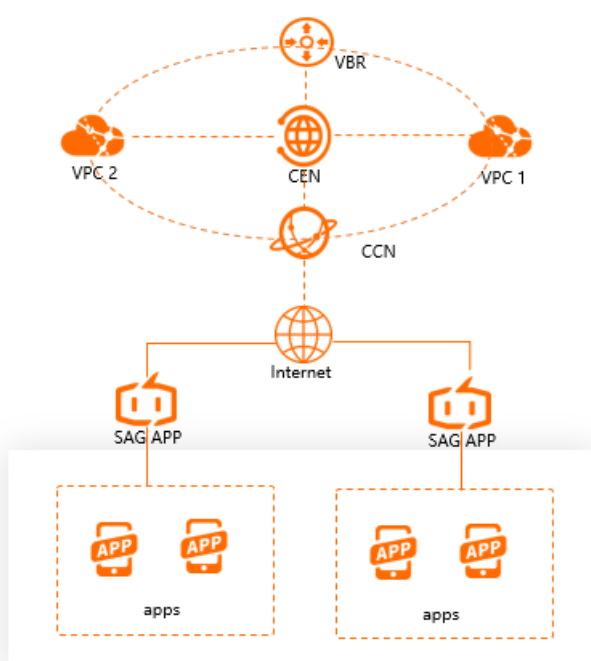


## 6.2. Network topology

Smart Access Gateway (SAG) provides different scenarios with solutions to migrate workloads to the cloud. You can choose a suitable network topology based on your actual requirements.

### Connect mobile devices to Alibaba Cloud

To connect mobile devices or remote devices to Alibaba Cloud, you can use SAG APP. SAG APP supports dial-up access from client devices such as PCs and mobile phones to Alibaba Cloud. Network connections between private networks and Alibaba Cloud are encrypted. SAG APP is suitable for office automation and remote operations and maintenance.

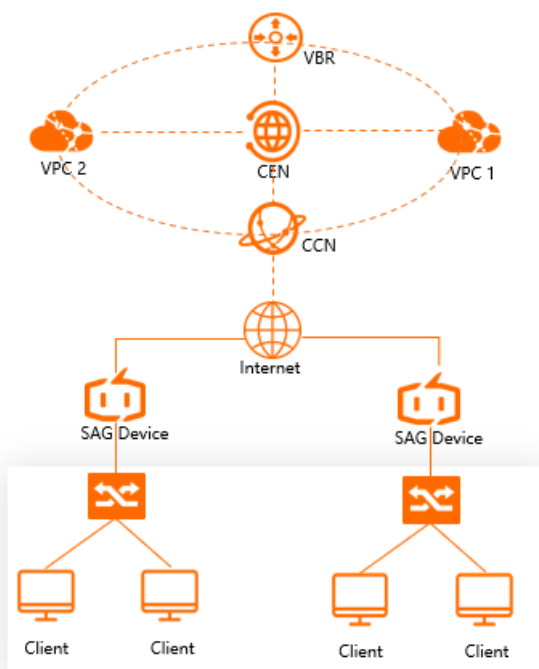


## Connect small-scale networks to Alibaba Cloud

To connect small office branches or stores to Alibaba Cloud, you can deploy SAG devices in inline mode.



Before you deploy an SAG device to connect a small-scale network to Alibaba Cloud, we recommend that you purchase a 4G subscriber identity module (SIM) card and insert it into the device. The 4G SIM card provides standby network connections. When an error occurs to the active network connection, data transmission is automatically switched to the standby connection. This improves network reliability.



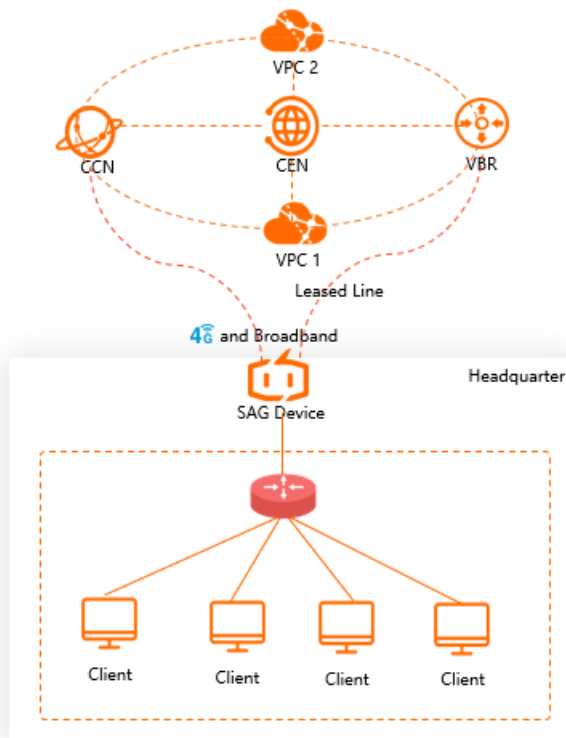
## Connect large-scale networks to Alibaba Cloud

To connect large-scale networks to Alibaba Cloud, you can deploy SAG devices in one-arm mode.

Before you deploy an SAG device to connect a large-scale network to Alibaba Cloud, we recommend that you purchase a SIM card and leased line. In this way, the broadband network, 4G network, and leased line are deployed in active-standby mode. This improves network reliability.

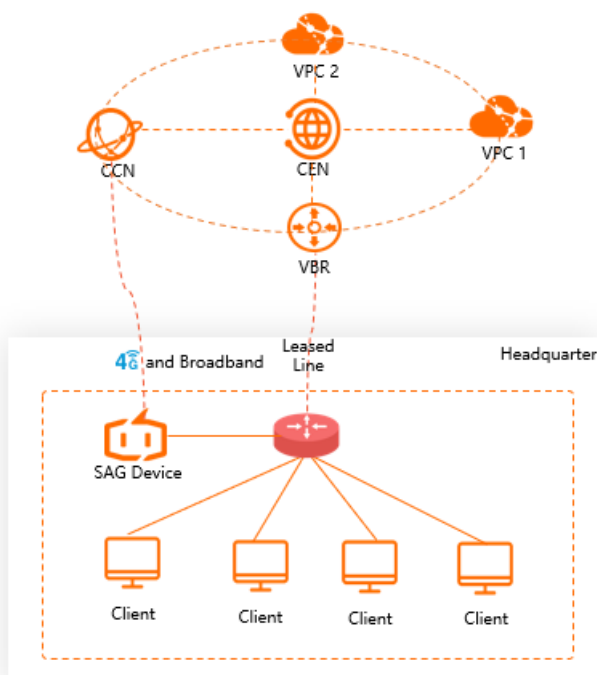
- Deploy a leased line (connected to an SAG device) to set up standby network connections

If you connect a leased line to the SAG device deployed in your network, local network traffic is transmitted through the leased line preferentially.



- Deploy a leased line (connected to a local Internet-facing device) to set up standby network connections

If you connect a leased line to a local Internet-facing device, you can prioritize the use of SAG and local devices for data transmission.



## 6.3. HA topology

If your workloads require high availability (HA), you can use two Smart Access Gateway (SAG) devices when you design the network topology.

### Background information

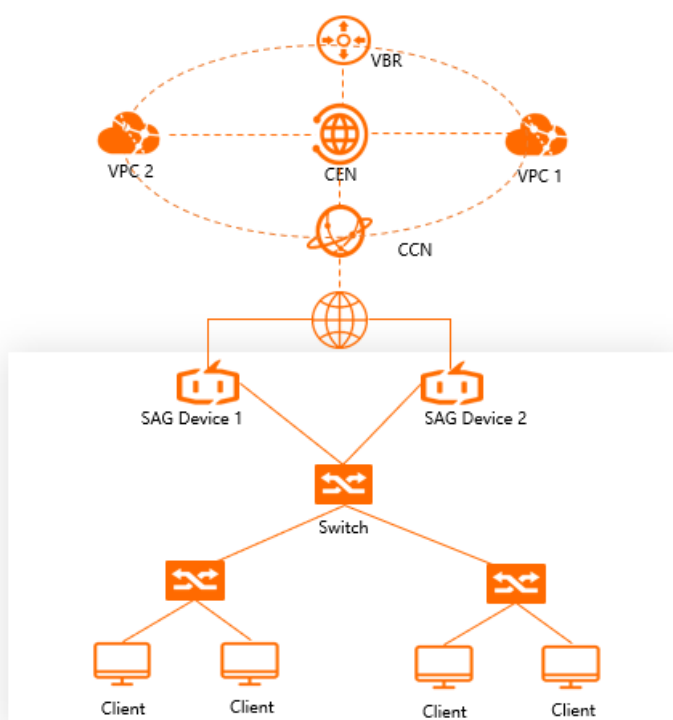
You can purchase two SAG devices to enable network HA when you connect a private network to Alibaba Cloud. The two SAG devices can be deployed in active-standby or active-active mode.

- Active-standby: One active device and one standby device. When an error occurs to the active device, you can switch network connections to the standby device. You must manually switch the standby device to the new active device in the console.
- Active-active: Two active devices. When an error occurs to one device, network connections are automatically switched to the other device.

SAG-100WM adopts active-standby mode by default. To request active-active mode, [submit a ticket](#). SAG-1000 supports active-active mode only.

### Device-based HA in inline mode

When you connect a private network to Alibaba Cloud, you can deploy two SAG devices in inline mode in your network and enable device-based HA. When an error occurs to one SAG device, network connections are automatically switched to the other device to avoid single point of failures (SPOFs). This improves network reliability.



### Device-based HA in one-arm mode

To connect a private network to Alibaba Cloud, you can deploy two SAG devices in one-arm mode in your network and enable dynamic routing. This reduces system latency and improves network reliability.

After dynamic routing is enabled, SAG automatically learns and selects the optimal routes to local devices. Dynamic routing satisfies the needs of large-scale networks that require frequent networking changes and reduces operations and maintenance expenses.

