Alibaba Cloud
Smart Access Gateway

Best Practices

Issue: 20181025

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⊖	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⊖ **Danger:** Resetting will result in the loss of user configuration data.
⚠	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	⚠ **Warning:** Restarting will cause business interruption. About 10 minutes are required to restore business.
📋	This indicates warning information, supplementary instructions, and other content that the user must understand.	📋 **Note:** Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋 **Note:** You can use **Ctrl** + **A** to select all files.
>	Multi-level menu cascade.	**Settings** > **Network** > **Set network type**
Bold	It is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

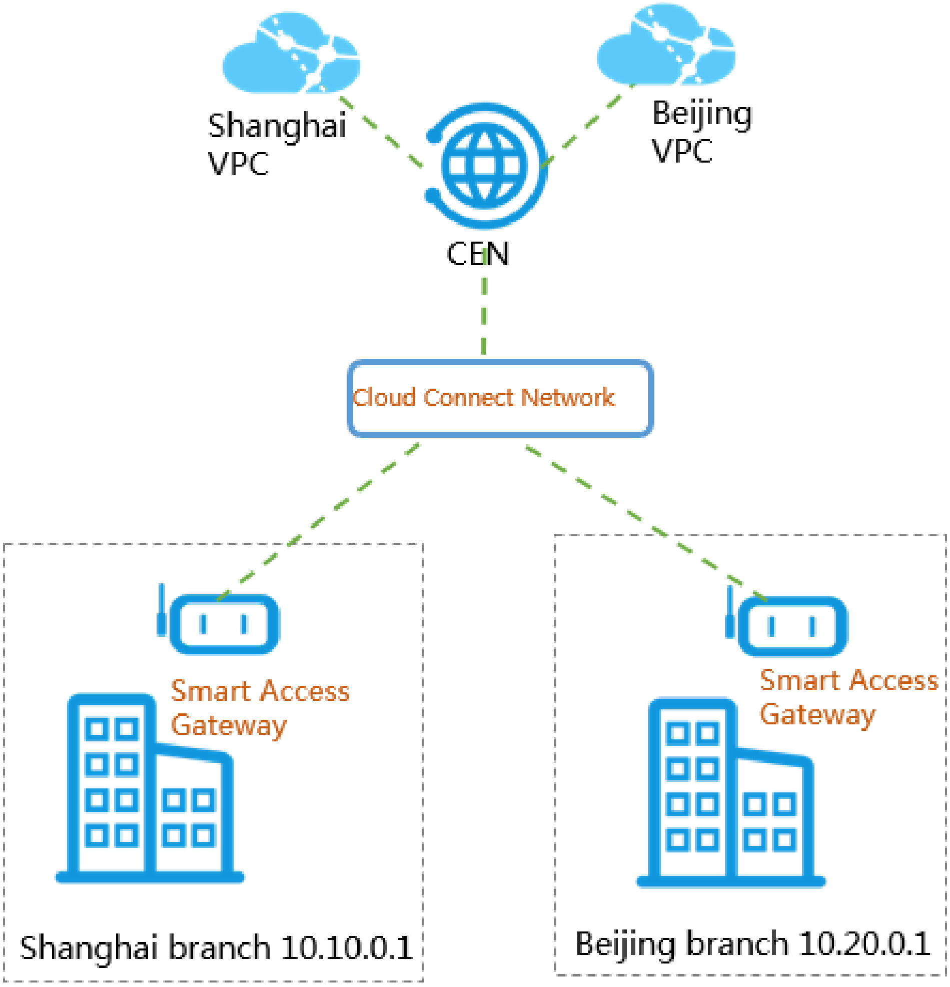
Legal disclaimer..I
Generic conventions.. I
1 Connect local branches to VPCs..1
2 Connect a headquarter network to a VPC.. 7

1 Connect local branches to VPCs

This tutorial explains how to connect two local branches to VPCs hosted in other locations of the same area using Smart Access Gateway. Clients of the local branches can then directly access the VPCs through Smart Access Gateway.

Scenario

In this tutorial, a company wants to connect local branches in Hangzhou and Ningbo to VPCs hosted in Shanghai and Beijing. Since the branches and VPCs are all in the same Smart Access Gateway area, you only need to attach the CCN instance associated with the Smart Access Gateway instances to the CEN instance in the same area.



Step 1. Buy a Smart Access Gateway device

After you buy a Smart Access Gateway device on the console, Alibaba Cloud delivers the device to you and creates a Smart Access Gateway instance for you to manage the network.

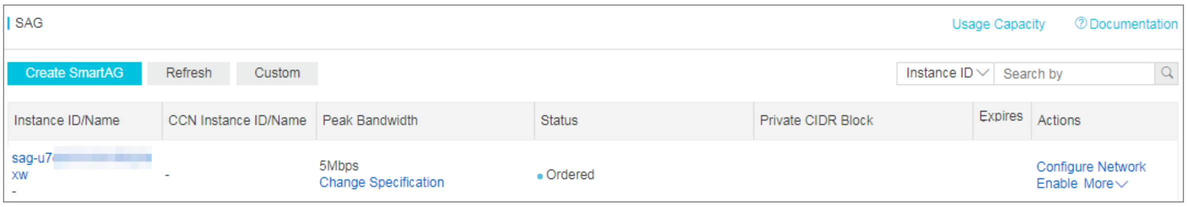
To buy a Smart Access Gateway device, complete these steps:

1. Log on to the *Smart Access Gateway console*.
2. Click **Create SmartAG**.
3. Configure the Smart Access Gateway device according to the following information and click **Buy Now**.

Configuration	Description
Region	Select the area of the Smart Access Gateway. The delivery address of the gateway device must be in the selected area. Each Smart Access Gateway area corresponds to a country. Currently, only the Mainland China area is supported.
Instance	Enter an instance name. The name can contain 2 to 128 characters and must start with an English letter. It can contain numbers and the following special characters: . _- In this tutorial, enter **Hangzhou branch**.
Hardware Specification	Select the hardware specification for the gateway device. The configurations of gateways with different specifications are also different. For more information, see *Specifications of Smart Access Gateway device*. In this tutorial, select **Standard edition**.
Peak Bandwidth	Select the bandwidth of the Smart Access Gateway device. In this tutorial, select **2 Mpbs**.
Procedure	Currently, only the single-device mode is supported, and so a local branch can only buy one Smart Access Gateway device for accessing Alibaba Cloud.
Subscription Duration	Select the purchase duration. In this tutorial, select **1 month**.

4. Confirm the order information, and then click **Buy Now**.
5. In the **Delivery address** dialog box, enter the delivery address of the gateway device and click **Place an Order**.

   You can check whether the order is successfully placed on the status page of Smart Access Gateway instances. The system will deliver the device within two days of the order being placed. If you do not receive the device within two days, you can submit a ticket to check the delivery status.



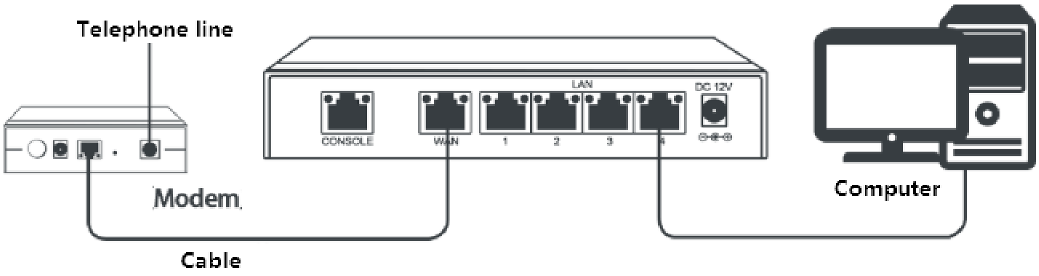
Instance ID/Name	CCN Instance ID/Name	Peak Bandwidth	Status	Private CIDR Block	Expires	Actions
sag-u7[redacted] xw -	-	5Mbps Change Specification	Ordered			Configure Network Enable More

6. Repeat the preceding steps to buy a Smart Access Gateway device for the Ningbo branch.

Step 2. Connect the gateway device

After you receive the gateway device, check you have all of the items listed in the *Gateway device description*. After you start the gateway device, connect the WAN port to the network cable and connect the LAN ports to local clients.

In this tutorial, the gateway device can be directly connected to the clients in the Hangzhou and Ningbo branches, so you can use the default gateway configuration. If you need to configure the WAN port and LAN ports, see *Configure a Smart Access Gateway device*.



Step 3. Activate the gateway

After receiving the gateway device, you need to activate it.

To activate the gateway device, complete these steps:

1. Log on to the *Smart Access Gateway console*.
2. On the **SmartAG** page, find the target gateway instance.
3. Click **Activate** in the **Actions** column.

Step 4. Configure the network connection

After activating the Smart Access Gateway device, you then need to attach it to a CCN instance and then attach the CCN instance to a CEN instance, so that local branches can connect to Alibaba Cloud.

To configure the network, complete these steps:

1. Log on to the *Smart Access Gateway console*.

2. On the **SmartAG** page, find the target gateway instance.
3. Click **Configure Network** in the **Actions** column.
4. On the **Configure Network** page, complete these steps:

    a. **Private CIDR Block**: Configure the private CIDR blocks used by the local clients to access Alibaba Cloud. Make sure none of the private CIDR blocks conflict with each other.

    In this tutorial, enter 172.16.0.0/12. Also use the default gateway configuration, so the IP address used by the local client to access Alibaba Cloud is allocated from the CIDR block 172.16.0.0/12. For more information, see *Network configuration*.

    b. **CCN Instance ID/Name**: Add the gateway instance to the CCN instance. Gateway devices can then communicate with one another.

    In this tutorial, select the default CCN instance. For more information, see *Cloud Connect Network*.

5. **Bind CEN Instance**: Select the CEN instance to attach. After the CCN instance is attached to the CEN instance, all networks (VPCs and VBRs) attached to the CEN instance can communicate with gateway devices in the CCN instance.

    In this tutorial, the CEN instance associated with the Shanghai VPC and Beijing VPC is selected.

    Note:

    Make sure that the CCN instance and the CEN instance are in the same area. For more information, see *CCN areas*.

6. Click **OK**.
7. Repeat the preceding steps to configure network for the gateway instance of the other branch office.

    Make sure the two gateway instances are bound to the same CCN instance and the same CEN instance.

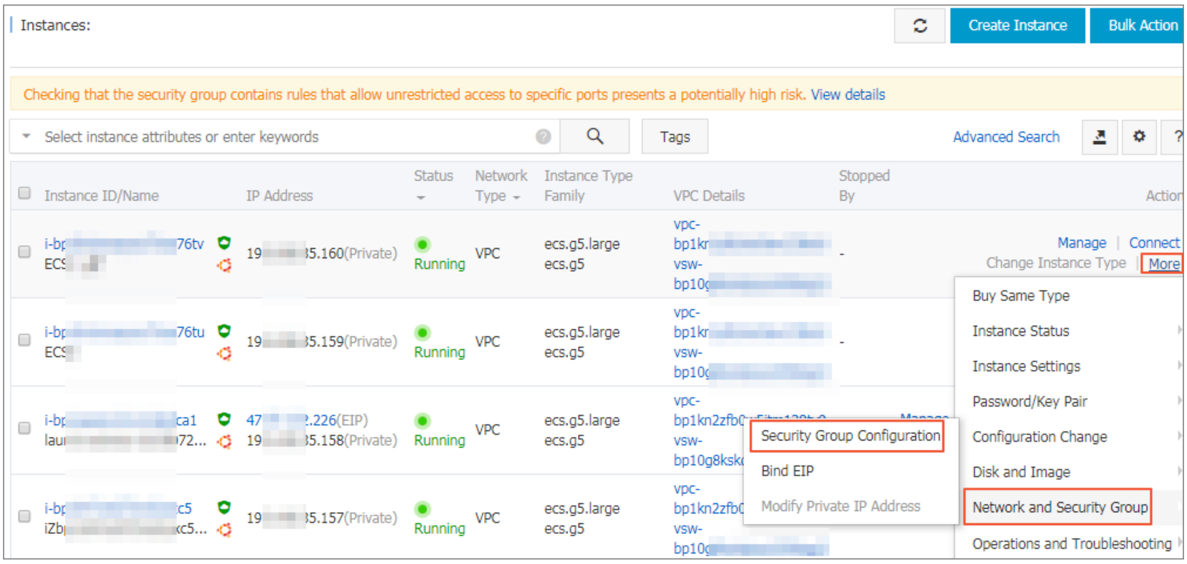
Step 5. Configure security groups

Configure security groups to allow local branches to access VPCs.

To configure the security groups, complete these steps:

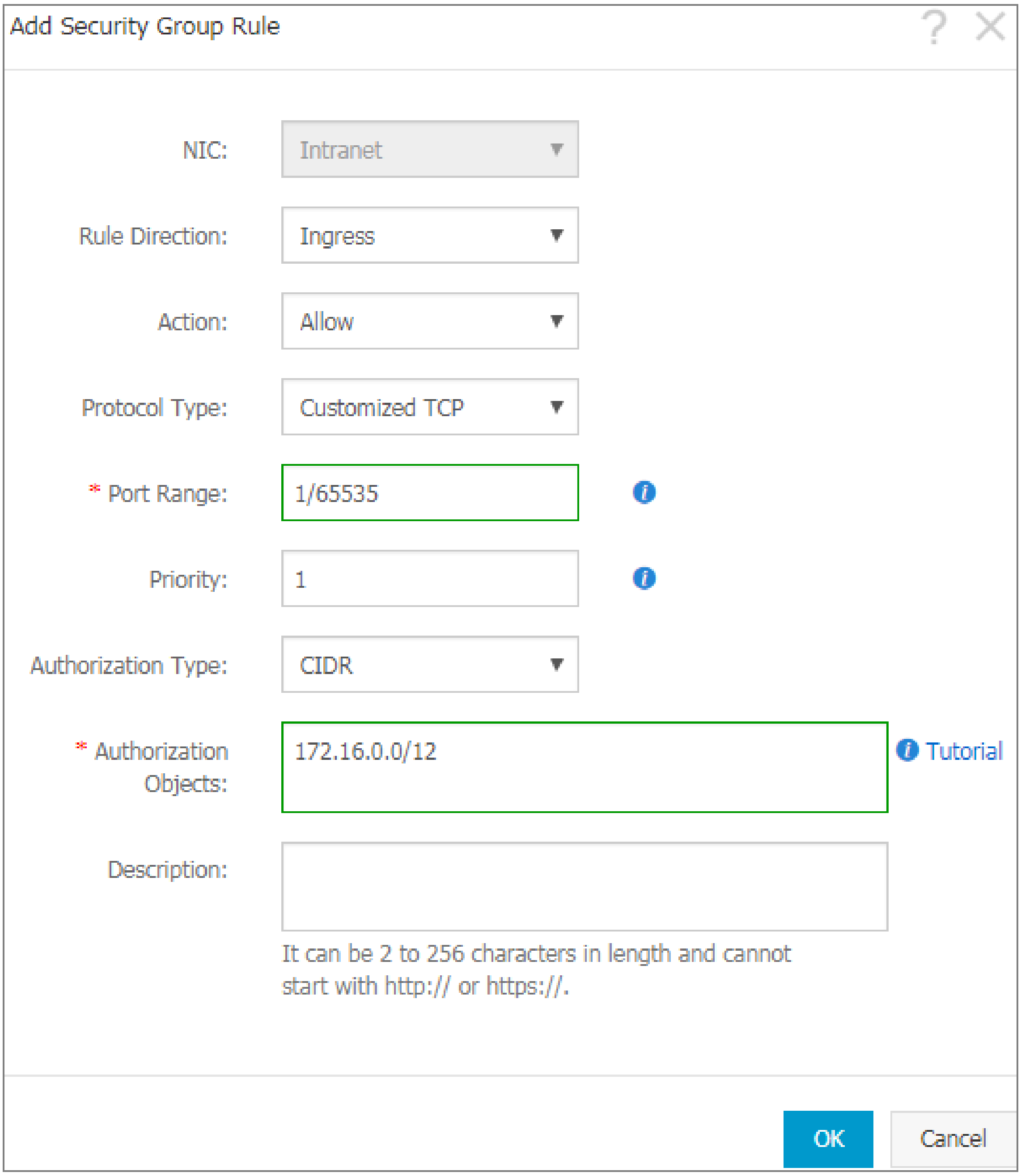
1. Log on to the *ECS console*.
2. In the left-side navigation pane, click **Instances**.

3. Locate the ECS instance in the target VPC, and then click **More** > **Network and Security Group** > **Security Group Configuration**.



4. Click **Security Groups** and click **Add Rules**.
5. Configure a security group rule that allows access from offline branches.

The following figure shows the security group configurations involved. You need set the authorization object as the private CIDR block of the local branch.



Add Security Group Rule

NIC: Intranet

Rule Direction: Ingress

Action: Allow

Protocol Type: Customized TCP

* Port Range: 1/65535

Priority: 1

Authorization Type: CIDR

* Authorization Objects: 172.16.0.0/12

Description:

It can be 2 to 256 characters in length and cannot start with http:// or https://.

Step 6. Test access

After completing the preceding configurations, you can use local clients to access cloud resources deployed in the connected VPCs to check if the new configurations take effect.

2 Connect a headquarter network to a VPC

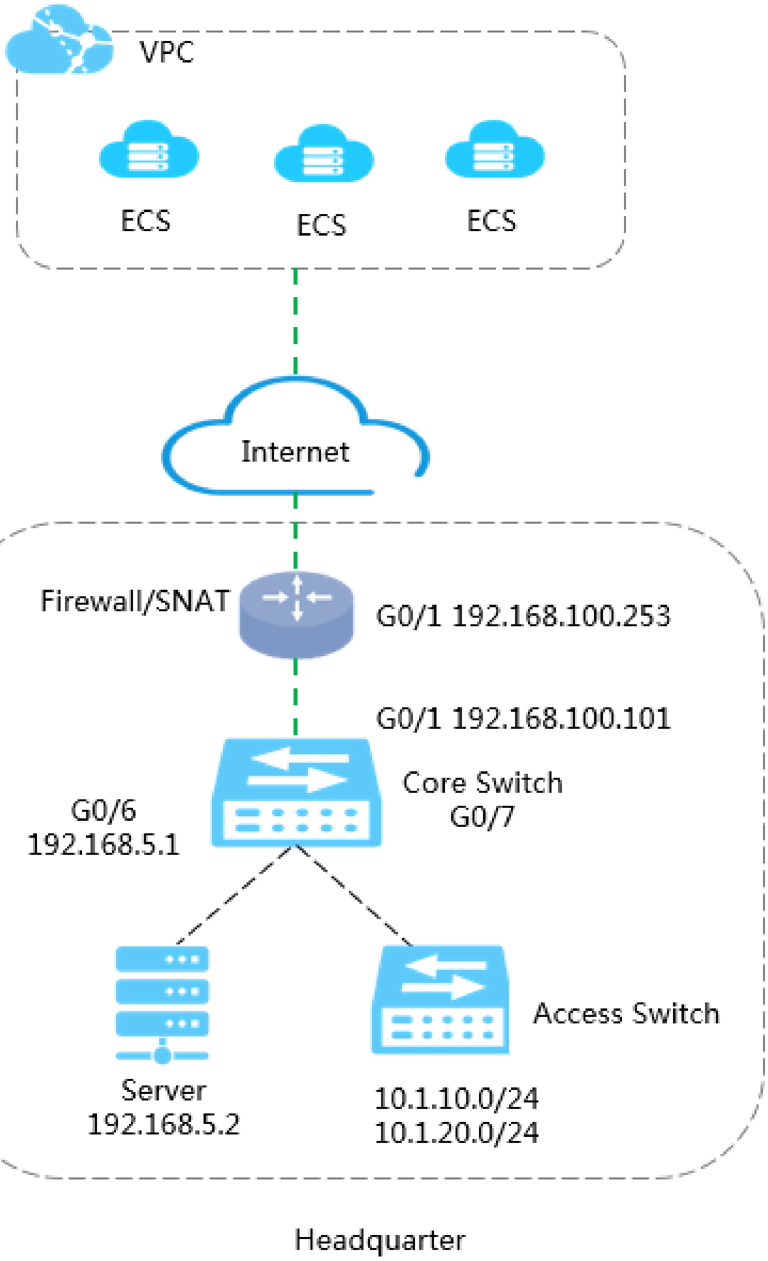
This tutorial explains how to use Smart Access Gateway in single-arm bypass mode to quickly connect a headquarter network to a VPC without making changes to the existing network.

Scenario

A company needs its headquarters to be able to communicate with its business system on the cloud through a carrier broadband. This will allow the headquarters to perform operations and maintenance on cloud resources, and means local data can be synchronized with cloud data.

The network configurations in this tutorial are as follows:

- A VPC has been created in Alibaba Cloud and ECS instances have been created in the VPC and are configured. The CIDR block of the VPC is 192.168.0.0/24.
- An egress router/firewall and a core switch are deployed in the headquarters network. The CIDR block of the local server is 192.168.5.0/24, 172.16.1.0/24, 10.1.1.0/24, and 10.1.20.0/24.



Network architecture

With Smart Access Gateway, the headquarters network has fast access to Alibaba Cloud, as shown in *Figure 2-1: Single-arm bypass routing mode*. In this networking mode, the egress router or firewall device must have SNAT enabled, and Smart Access Gateway must have SNAT disabled.

Note:

If you use the common bypass routing mode as shown in *Figure 2-2: Common bypass routing mode*, you can enable the SNAT function of Smart Access Gateway.

Figure 2-1: Single-arm bypass routing mode

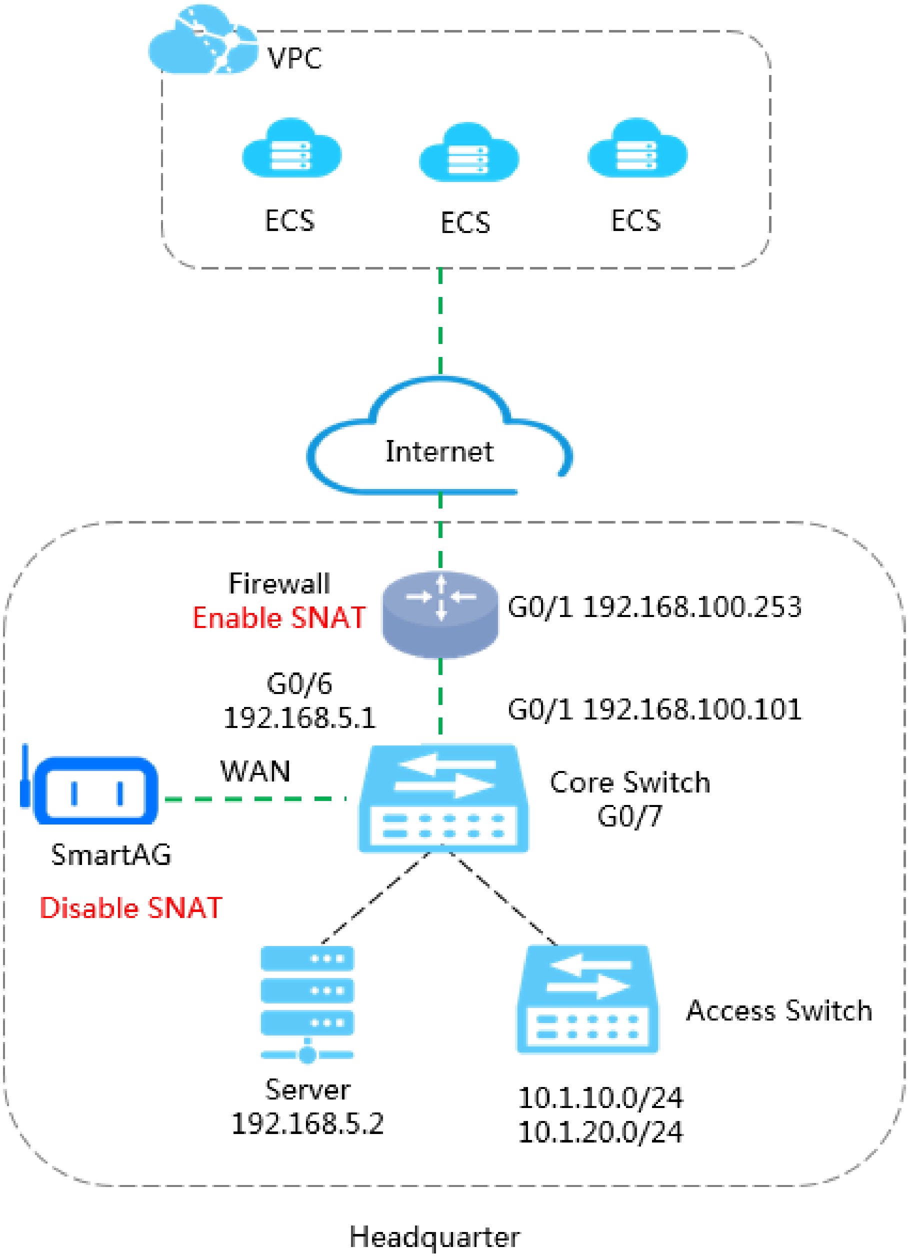
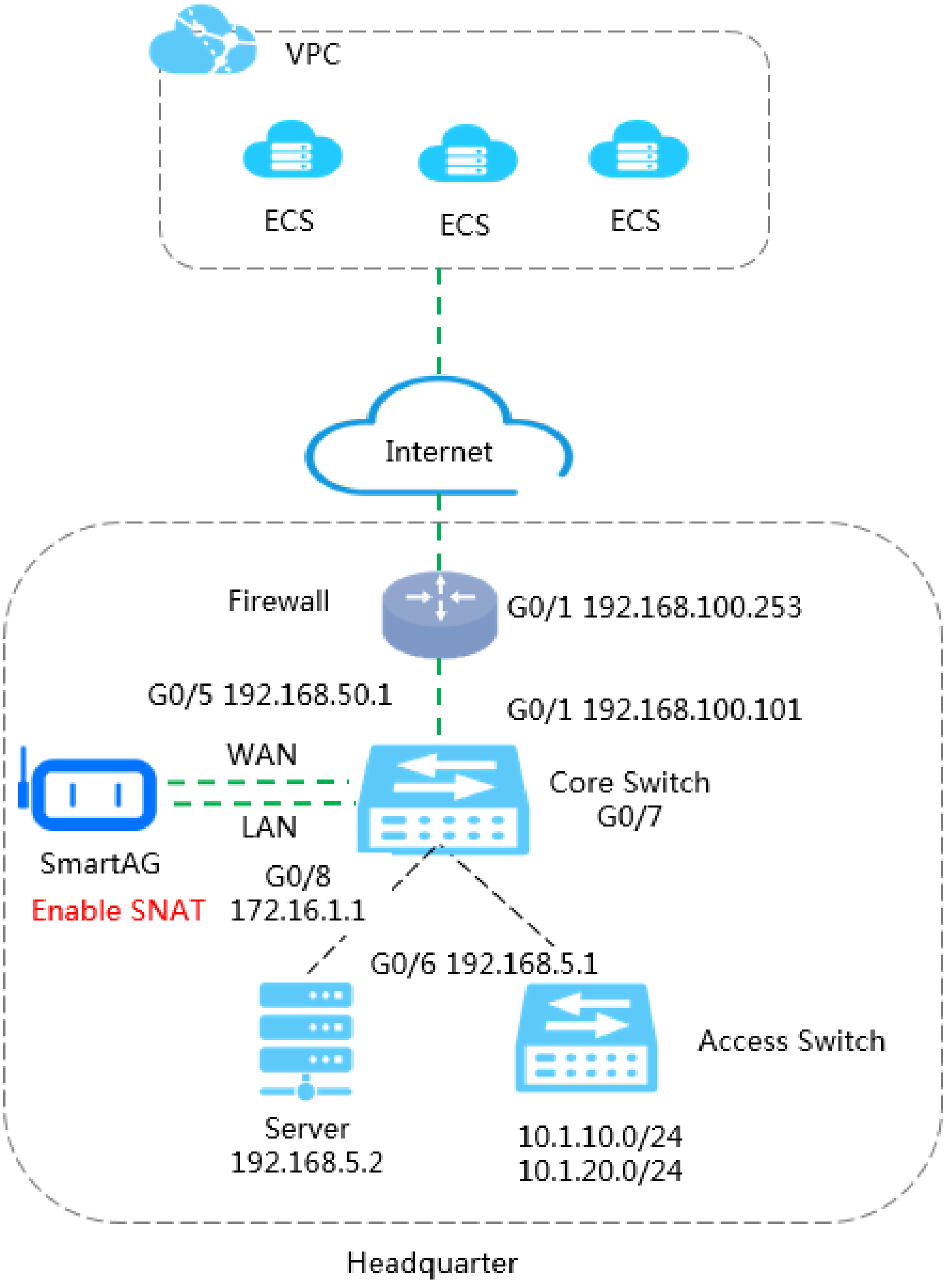


Figure 2-2: Common bypass routing mode



Step 1. Buy a Smart Access Gateway device

After you buy a Smart Access Gateway device on the console, Alibaba Cloud delivers the device to you and creates a Smart Access Gateway instance for you to manage the network.

To buy a Smart Access Gateway device, complete these steps:

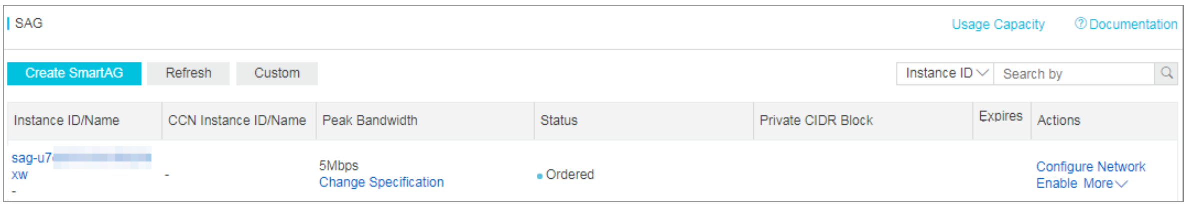
1. Log on to the *Smart Access Gateway console*.
2. Click **Create SmartAG**.

3. Configure the Smart Access Gateway device according to the following information and click **Buy Now**.

Configuration	Description
Area	Select the area of the Smart Access Gateway. The delivery address of the gateway device must be in the selected area. Each Smart Access Gateway area corresponds to a country. Currently only the Mainland China area is supported.
Instance	Enter an instance name. The name can contain 2 to 128 characters and must start with an English letter. It can contain numbers and the following special characters: . _- In this tutorial, enter **Hangzhou branch**.
Hardware Specification	Select the hardware specification for the gateway device. The configurations of gateways with different specifications are also different. For more information, see *Specifications of Smart Access Gateway device*. In this tutorial, select **Standard edition**.
Peak Bandwidth	Select the bandwidth of the Smart Access Gateway device. In this tutorial, select **2 Mpbs**.
Use Method	Currently, only the single-device mode is supported, and so an on-premises organization can only buy one Smart Access Gateway device for accessing Alibaba Cloud.
Subscription Duration	Select the purchase duration. In this tutorial, select **1 month**.

4. Confirm the order information, and then click **Buy Now**.
5. On the **Delivery address** dialog box, enter the delivery address of the gateway device and click **Place an Order**.

   You can check whether the order is successfully placed on the page of Smart Access Gateway instances. The system will deliver the device within two days of the order being placed. If you do not receive the device within two days, you can submit a ticket to check the delivery status.



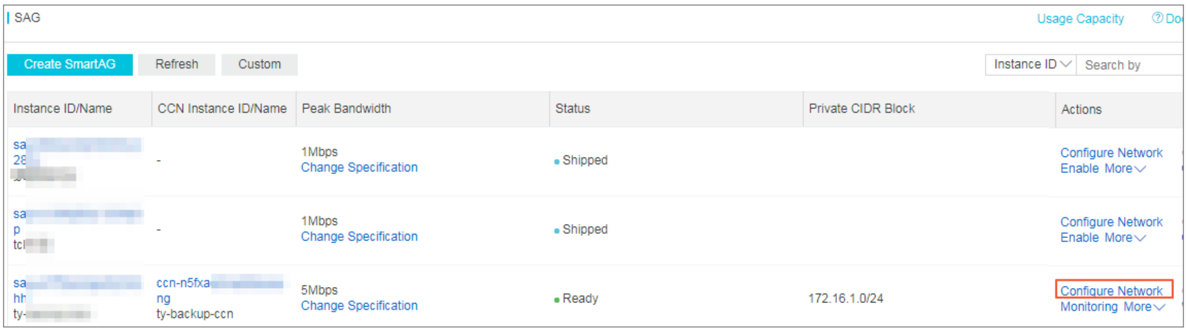
Instance ID/Name	CCN Instance ID/Name	Peak Bandwidth	Status	Private CIDR Block	Expires	Actions
sag-u7[redacted] xw -	-	5Mbps Change Specification	Ordered			Configure Network Enable More

Step 2. Configure the network connection

After activating the Smart Access Gateway device, you then need to attach it to a CCN instance and then attach the CCN instance to a CEN instance, so that local branches can connect to Alibaba Cloud.

To configure the network, complete these steps:

1. Log on to the *Smart Access Gateway console*.
2. On the **SmartAG** page, find the target gateway instance.
3. Click **Configure Network** in the **Actions** column.



Instance ID/Name	CCN Instance ID/Name	Peak Bandwidth	Status	Private CIDR Block	Actions
sa[redacted] 28[redacted] [redacted]	-	1Mbps Change Specification	Shipped		Configure Network Enable More
sa[redacted] p tcl[redacted]	-	1Mbps Change Specification	Shipped		Configure Network Enable More
sa[redacted] hh ty-[redacted]	ccn-n5fxa[redacted] ng ty-backup-ccn	5Mbps Change Specification	Ready	172.16.1.0/24	Configure Network Monitoring More

4. On the **Configure Network** page, complete these steps:
   a. **Private CIDR Block**: Configure the private CIDR blocks used by the local clients to access Alibaba Cloud. Make sure none of the private CIDR blocks conflict with each other.

      In this tutorial, enter 172.16.1.0/24, 192.168.5.0/24, 10.1.10.0/24, and 10.1.20.0/24. For more information, see *Network configuration*.
   b. **CCN Instance ID/Name**: Add the gateway instance to the CCN instance. Gateway devices can then communicate with one another.

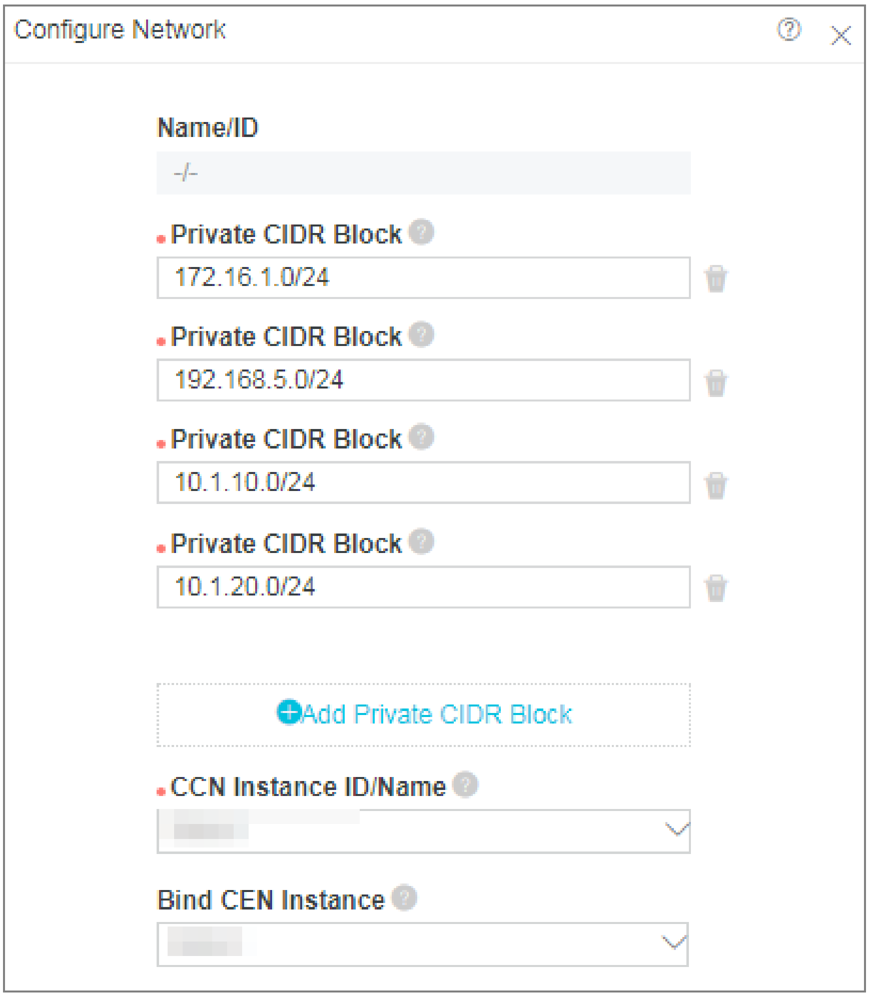
      In this tutorial, select the default CCN instance. For more information, see *Cloud Connect Network*.
5. **Bind CEN Instance**: Select the CEN instance to attach. After the CCN instance is attached to the CEN instance, all networks (VPCs and VBRs) attached to the CEN instance can communicate with gateway devices in the CCN instance.

   In this tutorial, select the CEN instance associated with the VPC.

Note:

Make sure that the CCN instance and the CEN instance are in the same area. For more information, see *CCN areas*.

6. Click **OK**.



Configure Network

Name/ID

-/-

* Private CIDR Block

172.16.1.0/24

* Private CIDR Block

192.168.5.0/24

* Private CIDR Block

10.1.10.0/24

* Private CIDR Block

10.1.20.0/24

* CCN Instance ID/Name

[redacted]

Bind CEN Instance

[redacted]

Step 3. Connect and activate the gateway device

After you receive the gateway device, check you have all of the items according to the *Gateway device description*, and then activate the device.

To activate the gateway device, complete these steps:

1. Log on to the *Smart Access Gateway console*.
2. On the **SmartAG** page, find the target gateway instance.
3. Click **Activate** in the **Actions** column.

Step 4. Configure the gateway device

After you start the gateway device, connect the WAN port to the network cable and connect the LAN ports to a local client.

Note:

> You cannot log on to the web configuration page through the WAN port of the Smart Access Gateway device. To modify configurations, connect a local client to a LAN port of the gateway device, then go to the web configuration page and log on.

To configure the gateway device, complete these steps:

1. Enter https://192.168.0.1 in the browser of the local client and set the initial password.

   By default, the local client can obtain addresses in the CIDR block 192.168.0.0/24.
2. Configure the WAN port.

   In this tutorial, the gateway address is the IP address of the peer port on the core switch. Disable the SNAT function to enable SNAT on the egress router/firewall.
3. Configure the LAN ports.
4. Connect the WAN port of the Smart Access Gateway device to G 0/5 of the core switch to connect local clients with the core switch. The NIC of the local client uses a static IP address and the core switch serves as the gateway.

Step 5. Configure the core switch and the egress router

To configure the core switch, complete these steps:

1. Configure the interface connected to the Smart Access Gateway device and configure the IP address:

   ```
   interface GigabitEthernet 0/5———//In the bypass mode, connect it to
   the WAN port of Smart Access Gateway
   no switchport
   ip address 192.168.50.1 255.255.255.0
   ```
2. Configure the route to forward traffic from the headquarters to Alibaba Cloud:

   ```
   ip route 192.168.0.0 255.255.255.0 192.168.50.2———// Route traffic
   from local clients to Smart Access Gateway
   ```
3. Configure a route to Smart Access Gateway in the egress router:

   ```
   ip route 192.168.50.0 255.255.255.0 192.168.100.101——// Forward
   traffic from Alibaba Cloud to the core switch
   ```

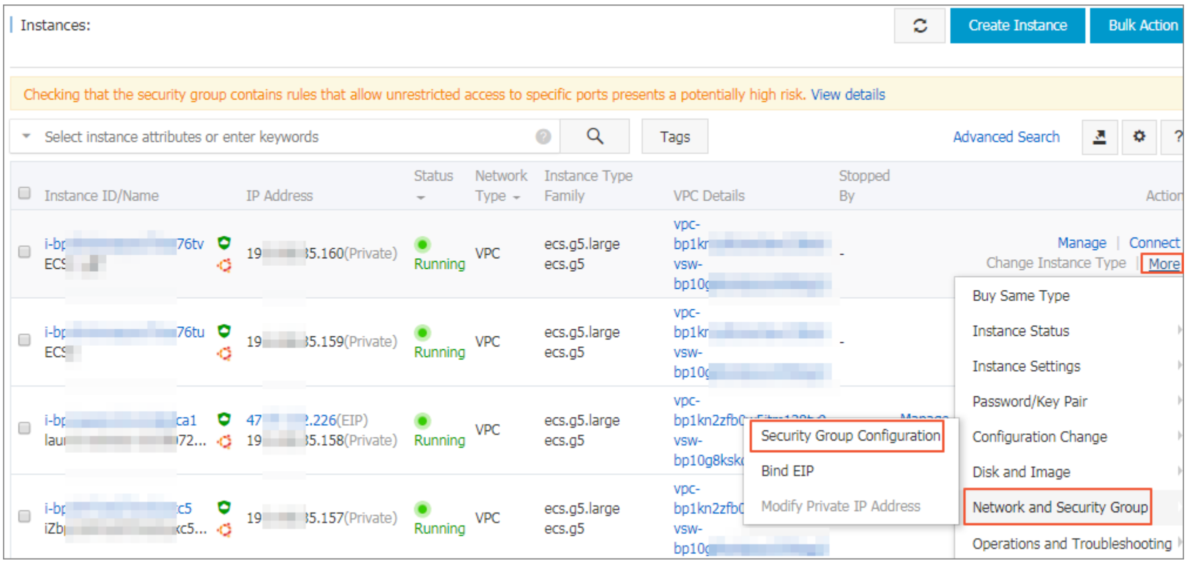
Step 6. Configure security groups

Configure security groups to allow local branches to access a VPC.

To configure security groups, complete these steps:

1. Log on to the *ECS console*.

2. In the left-side navigation pane, click **Instances**.
3. Find the ECS instance in the target VPC, and click **More** > **Network and Security Group** > **Security Group Configuration**.

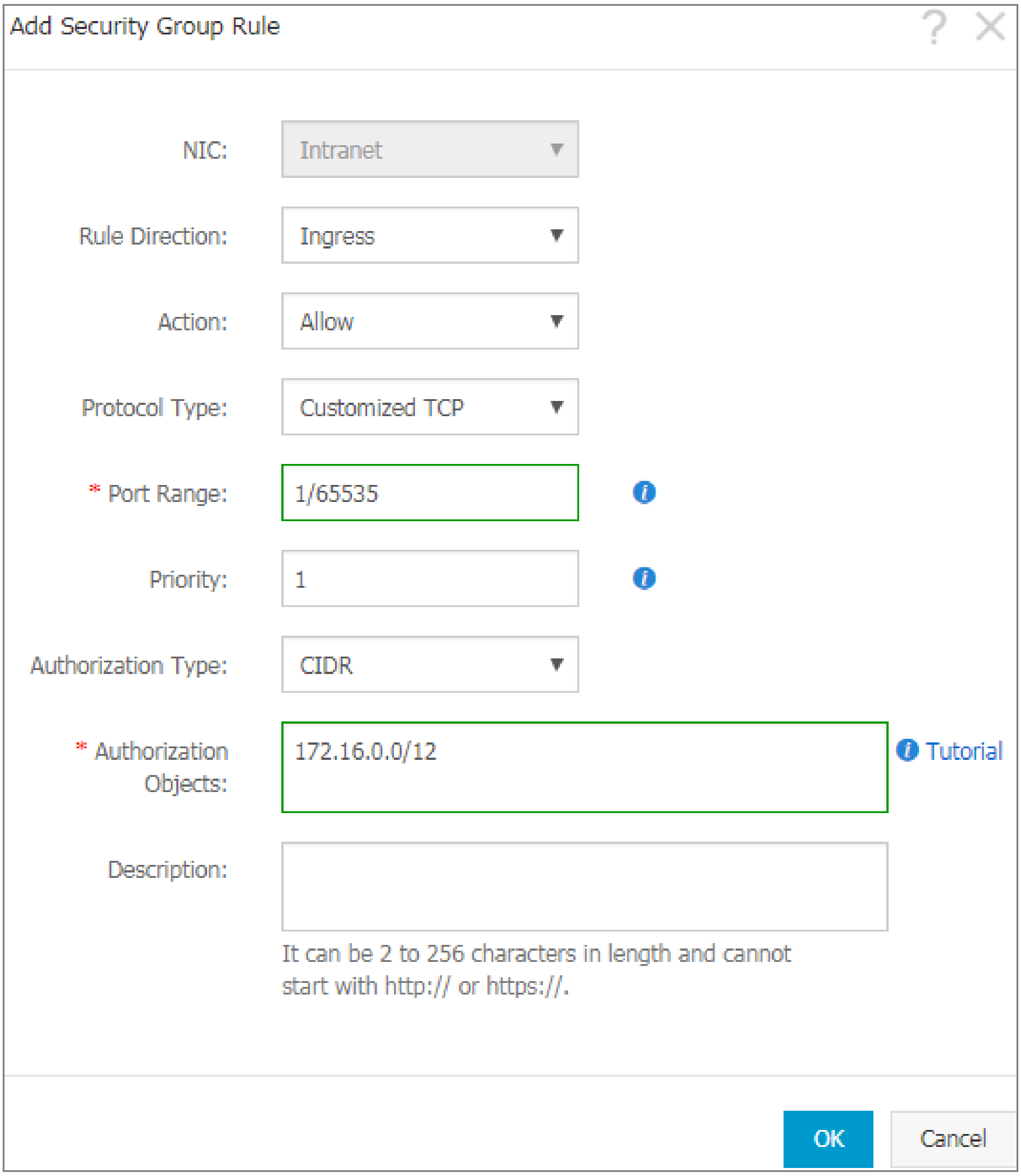


Checking that the security group contains rules that allow unrestricted access to specific ports presents a potentially high risk. View details

Instance ID/Name	IP Address	Status	Network Type	Instance Type Family	VPC Details	Stopped By	Action
i-bp[redacted]76tv ECS[redacted]	19[redacted]5.160(Private)	Running	VPC	ecs.g5.large ecs.g5	vpc-bp1kr[redacted] vsw-bp10[redacted]	-	Manage | Connect Change Instance Type | More
i-bp[redacted]76tu ECS[redacted]	19[redacted]5.159(Private)	Running	VPC	ecs.g5.large ecs.g5	vpc-bp1kr[redacted] vsw-bp10[redacted]	-	
i-bp[redacted]ca1 lau[redacted]72...	47[redacted].226(EIP) 19[redacted]5.158(Private)	Running	VPC	ecs.g5.large ecs.g5	vpc-bp1kn2zfb0 vsw-bp10g8ksk		
i-bp[redacted]c5 iZb[redacted]xc5...	19[redacted]5.157(Private)	Running	VPC	ecs.g5.large ecs.g5	vpc-bp1kn2zfb0 vsw-bp10[redacted]		

4. Click **Add Rules** and then click **Add Security Group Rule**.
5. Configure a security group rule that allows VPC access from offline branches.

   The following figure shows the security group configuration in this tutorial. The authorization object must be the private CIDR block of the local branch.



Add Security Group Rule

NIC: Intranet

Rule Direction: Ingress

Action: Allow

Protocol Type: Customized TCP

* Port Range: 1/65535

Priority: 1

Authorization Type: CIDR

* Authorization Objects: 172.16.0.0/12

Description:

It can be 2 to 256 characters in length and cannot start with http:// or https://.

Step 7. Test access

After completing the preceding configurations, you can use local clients to access cloud resources deployed in the connected VPC to check if the new configurations take effect.