Alibaba Cloud
Smart Access Gateway

Access control list

Issue: 20190814

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.	 Notice: 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]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 What is an access control list?

Smart Access Gateway (SAG) provides the access control list (ACL) function in the form of whitelists and blacklists for different SAG instances.

ACL usage process

The process is described as follows:

1. Create an ACL, and set the ACL name.
2. Set an ACL rule for the ACL.
3. Add an SAG instance to the ACL.
4. You can configure multiple ACL rules for an ACL. You can also add SAG instances to the rules or remove the instances from them.

   Note:
   An SAG instance can be associated with only one ACL, and the quota cannot be adjusted.
5. You can modify or delete existing ACL rules.

ACL configuration recommendations

The recommendations on ACL configuration are as follows:

- Use ACL as a whitelist.
- Follow the minimum authorization principle. For example, you can choose to open a specific port (such as port 80).
- All applications should not be managed with only one ACL, and different layers have different access control requirements.
- Add instances with the same security requirements to the same ACL, and there is no need to configure a separate security group for each instance.

2 Configure an access control list

This topic describes how to configure an access control list (ACL) rule for a target Smart Access Gateway instance to permit or deny access to or from specified IP addresses in the ACL rule.

Procedure

1. Log on to the Smart Access Gateway console.
2. In the left-side navigation pane, click ACL.
3. On the ACL page, click Create ACL.
4. Configure the name of the ACL, and then return to the ACL page.

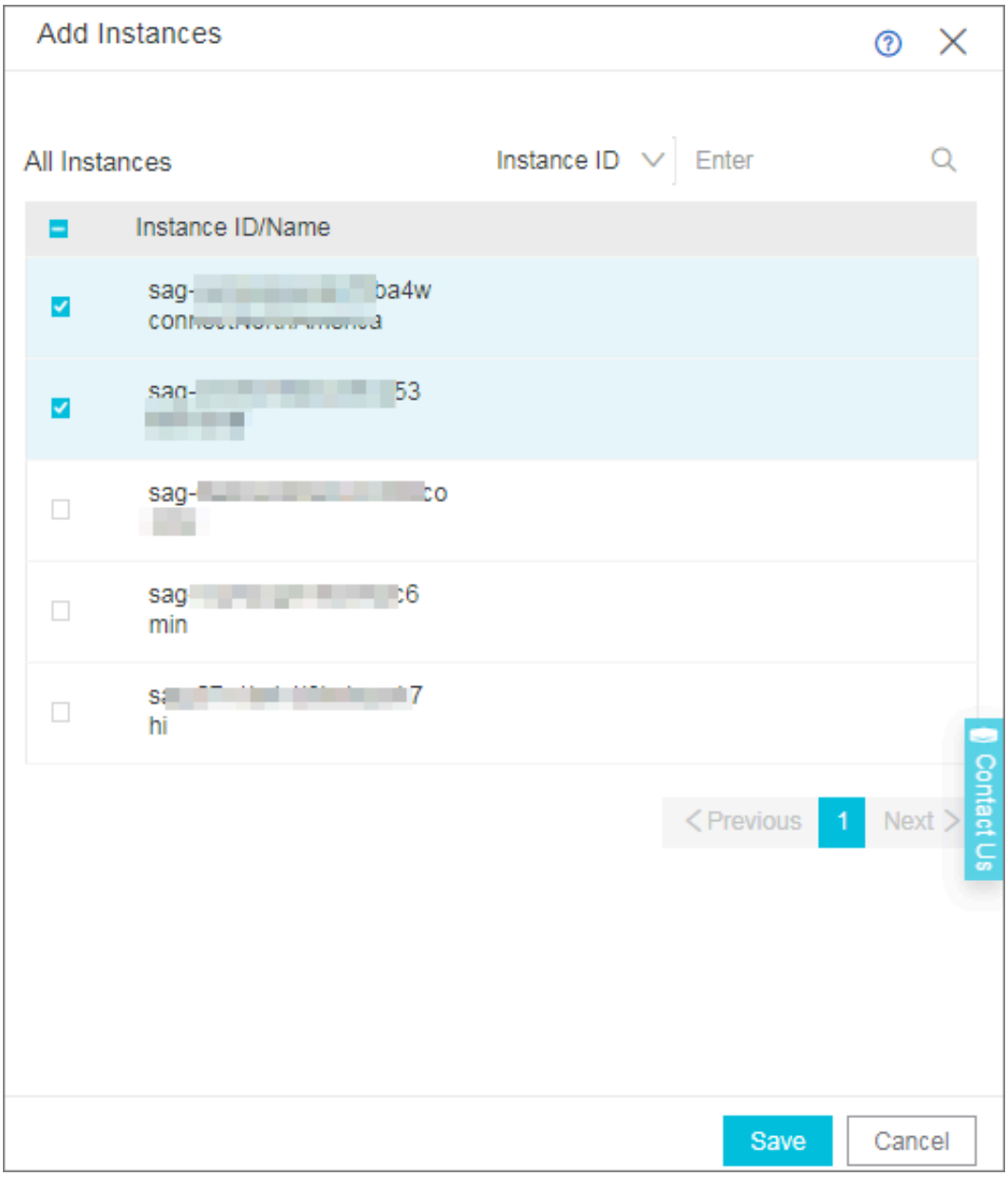
5. Click the ID of the ACL instance or Configure Rules in the Actions column.
6. In the left-side navigation pane, click ACL Rules and then click Add Rule to add an ACL rule to the ACL instance.

Configuration	Description
Direction	· Outbound: Traffic from the local branch connected to Smart Access Gateway to the external environment. · Inbound: Traffic from the external environment to the local branch connected to Smart Access Gateway.
Authorization Policy	Select Allow or Refuse.
Protocol	The transport layer protocol.
Source CIDR	· Outbound: The CIDR block of the local branch that initiates access. · Inbound: The CIDR block that accesses the local branch.
Source Port Range	The source port range of the transport layer. · TCP/UDP protocol: [1, 65535] · ICMP protocol: -1/-1 · All: -1/-1

Configuration	Description
Destination CIDR:	· Outbound: The external destination CIDR block to be accessed. · Inbound: The destination CIDR block of the local branch to access.
Destination Port Range	The destination port range of the transport layer. · TCP/UDP protocol: [1, 65535] · ICMP protocol: -1/-1 · All: -1/-1
Priority	Valid range: 1–100. The smaller the number, the higher the priority. If the priority of two rules is the same, the rule added earlier takes effect.

7. Click OK.

8. After the ACL rule is configured, click Add Instances in the Actions column to add Smart Access Gateway instances that use the ACL rule.



9. Click Save.

   To remove an instance, click the target instance and then click Remove in the Actions column.