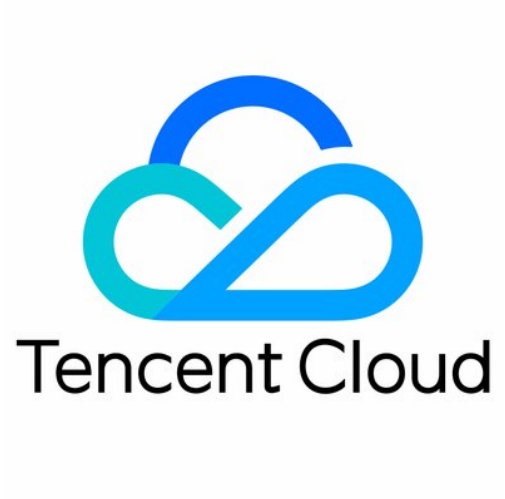
Cloud Virtual Machine

Security Groups

Product Documentation



Contents

Security Groups
- Security Group
- Creating a Security Group
- Adding Security Group Rules
- Associating CVM Instances with Security Groups
- Managing Security Groups
  - Viewing Security Groups
  - Remove from Security Groups
  - Cloning Security Groups
  - Deleting a Security Group
  - Adjusting Security Group Priority
- Managing Security Group Rules
  - Viewing Security Group Rules
  - Modifying Security Group Rules
  - Deleting Security Group Rules
  - Exporting Security Group Rules
  - Importing Security Group Rules
- Security Group Use Cases
- Server Common Port
- Security Group API Overview

Security Groups
Security Group

Last updated：2024-01-08 09:41:35

A security group is a virtual firewall that features stateful data packet filtering. It is used to configure the network access control of CVM, Cloud Load Balancer, TencentDB, and other instances while controlling their outbound and inbound traffic. It is an important means of network security isolation.
You can configure security group rules to allow or reject inbound and outbound traffic of instances within the security group.

Security Group Features

A security group is a logical group. You can add CVM, ENI, TencentDB, and other instances in the same region with the same network security isolation requirements to the same security group.
If a security group has no rules, it will reject all traffic by default, and you need to add rules to it to allow traffic.
Security groups are stateful. Inbound traffic you have allowed can automatically become outbound and vice versa.
You can modify security group rules at any time, and the new rules will take effect immediately.

Usage Limits

For use limits and quotas of security groups, see security group limits in Use Limits Overview.

Security Group Rules

Components

A security group rule consists of:
Source: IP address of the source data (inbound) or target data (outbound)
Protocol type and protocol port: Protocol type such as TCP and UDP
Policy: Allow or reject the access request.

Rule priorities

The rules in a security group are prioritized from top to bottom. The rule at the top of the list has the highest priority and will take effect first, while the rule at the bottom has the lowest priority and will take effect last.
If there is a rule conflict, the rule with the higher priority will prevail by default.

When the traffic goes in to or out from an instance bound to a security group, the security group rules are calculated from top to bottom. If a rule is matched and executed (allow/reject requests), the subsequent rules will not be matched.

Multiple security groups

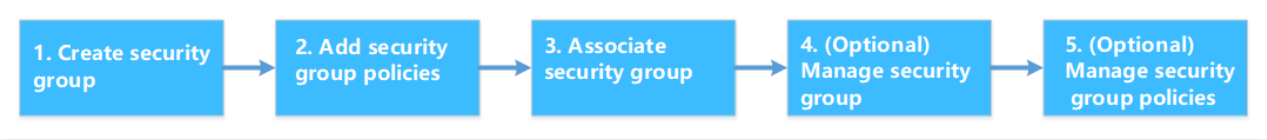
An instance can be bound to one or multiple security groups. When it is bound to multiple security groups, the security group rules are calculated from top to bottom. You can adjust the priorities of security groups at any time.

Security Group Templates

Tencent Cloud provides the following two security group templates:
Open all ports: All inbound and outbound traffic are allowed
Open common ports : It opens port TCP 22 (for Linux SSH login), ports 80 and 443 (for Web service), port 3389 (for Windows remote login), the ICMP protocol (for Ping commands), and allows all traffic from the private network.
Note:
If these templates cannot meet your actual needs, you can create custom security groups. For more information, see Creating a Security Group and Security Group Use Cases.
If you need to protect the application layer (HTTP/HTTPS), please activate Tencent Cloud Web Application Firewall (WAF), which provides web security at the application layer to defend against web vulnerabilities, malicious crawlers, and CC attacks, protecting your websites and web applications security.

Directions

The following figure shows you how to use a security group:



Security Group Best Practices

Creating a security group

We recommend that you specify a security group while you're purchasing a CVM via the API. Otherwise, the default security group will be used. The default security group cannot be deleted, and it adopts the default security rule (i.e.,

allowing all IPv4 addresses). You can modify the security rule after the security group is created.
If you need to change the instance protection policy, we recommend modifying the existing rules rather than creating a new security group.

Managing rules

Export and back up the security group rules before you modify them, so you can import and restore them if an error occurs.
To create multiple security group rules, please use the parameter template.

Associating a security group

You can add instances with the same protection requirements to the same security group, instead of configuring a separate security group for each instance.
It's not recommended to bind one instance to too many security groups, which may cause rule conflicts and result in network disconnection.

Creating a Security Group

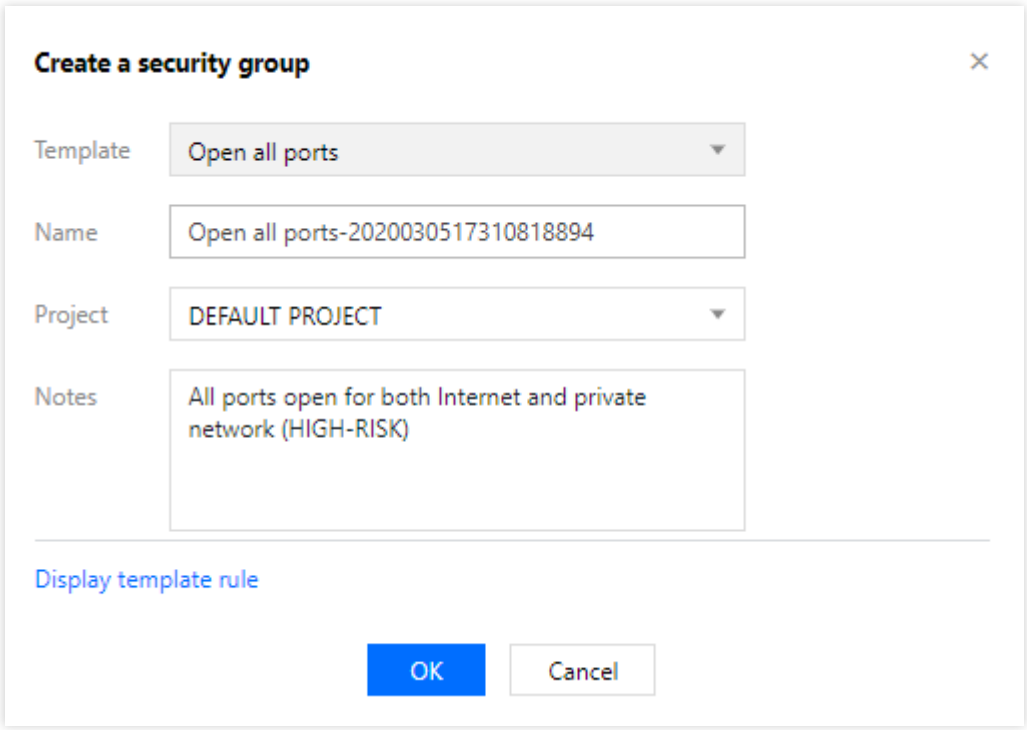
Last updated：2024-01-08 09:41:35

Scenario

Security Groups act as virtual firewalls for CVMs. Each CVM instance must associate with at least one security group. By default, each CVM instance has two templates (**Open all ports** and **Open port 22, 80, 443, 3389 and ICMP protocol**) for creating a default security group. For details, refer to Security Group Overview.
If the default security group does not meet your needs, you can create your own security group as instructed below.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select **Security Group**. The Security Group page then appears.
3. Select a region for the security group. Click **+New**.
4. In the **Create a security group** page, complete the following configurations:



Template: select a template that suits your needs, as shown below:

Template	Description	Notes

Open all ports	All ports are open. May present security issues.	-
Open TCP port 22, 80, 443, 3389 and ICMP	TCP port 22, 80, 443 and 3389, and the ICMP are open. All ports are open internally.	Suitable for instances with web services.
Custom	Creates a blank security group in which rules are added afterwards. For details on how to add rules, refer to this article.	-

Name: name of the security group.

Project: by default, **Default project** is selected. Select a project for better management.

Notes: a short description for the security group.

5. Click **OK** to create the security group.

If you select **Custom** as the template for your security group, click **Add rules now** to add security group rules.

Adding Security Group Rules

Last updated：2024-01-08 09:41:35

Overview

Security groups are used to manage traffic to and from public and private networks. For the sake of security, most inbound traffic is denied by default. If you selected **Open all ports** or **Open ports 22, 80, 443, 3389 and ICMP protocol** as the template when creating a security group, rules are automatically created and added to the security group to allow traffic on those ports. For more information, please see Security Groups.
This document describes how to add security group rules to allow or reject traffic to and from public or private networks.

Notes

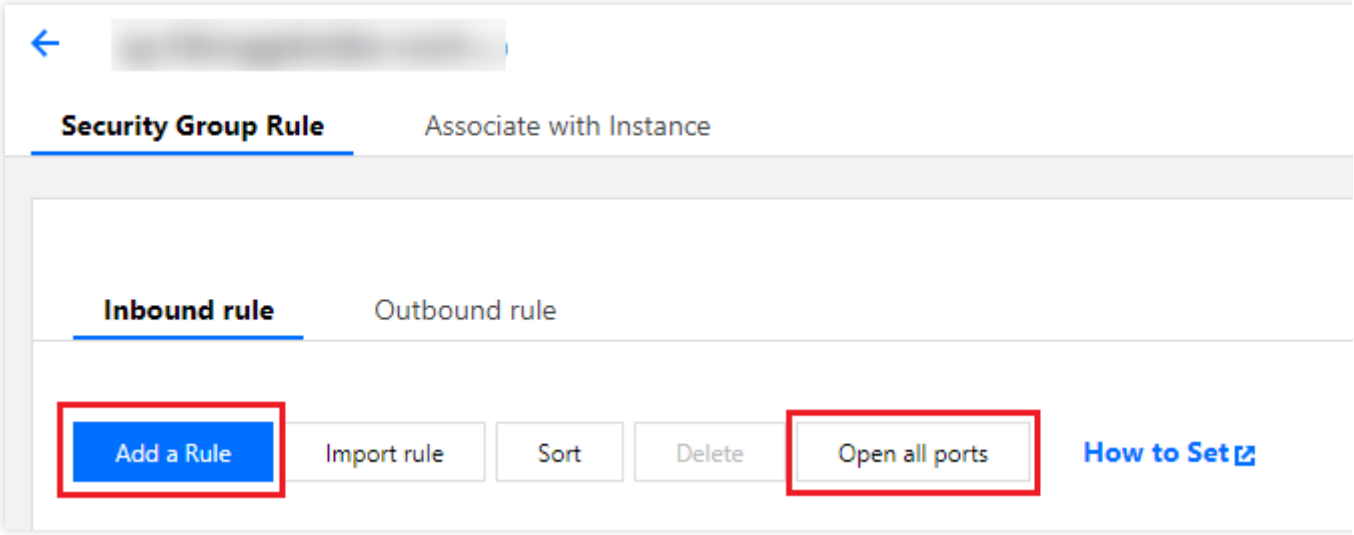
Security group rules support IPv4 and IPv6 rules.
Open all ports allows both IPv4 and IPv6 traffic.

Prerequisites

You should have an existing security group. If you do not, refer to Creating a Security Group for details.
You should know which traffic is allowed or rejected for your CVM instance. For more information on security group rules and their use cases, please see Security Group Use Cases.

Directions

1. Log in to the CVM console.
2. Select **Security Group** on the left sidebar to access the security group management page.
3. Select a region, and locate the security group for which you want to set rules.
4. Click **Modify Rules** in the **Operation** column.
5.
Click **Inbound rules** and choose
either of the following methods to add rules.



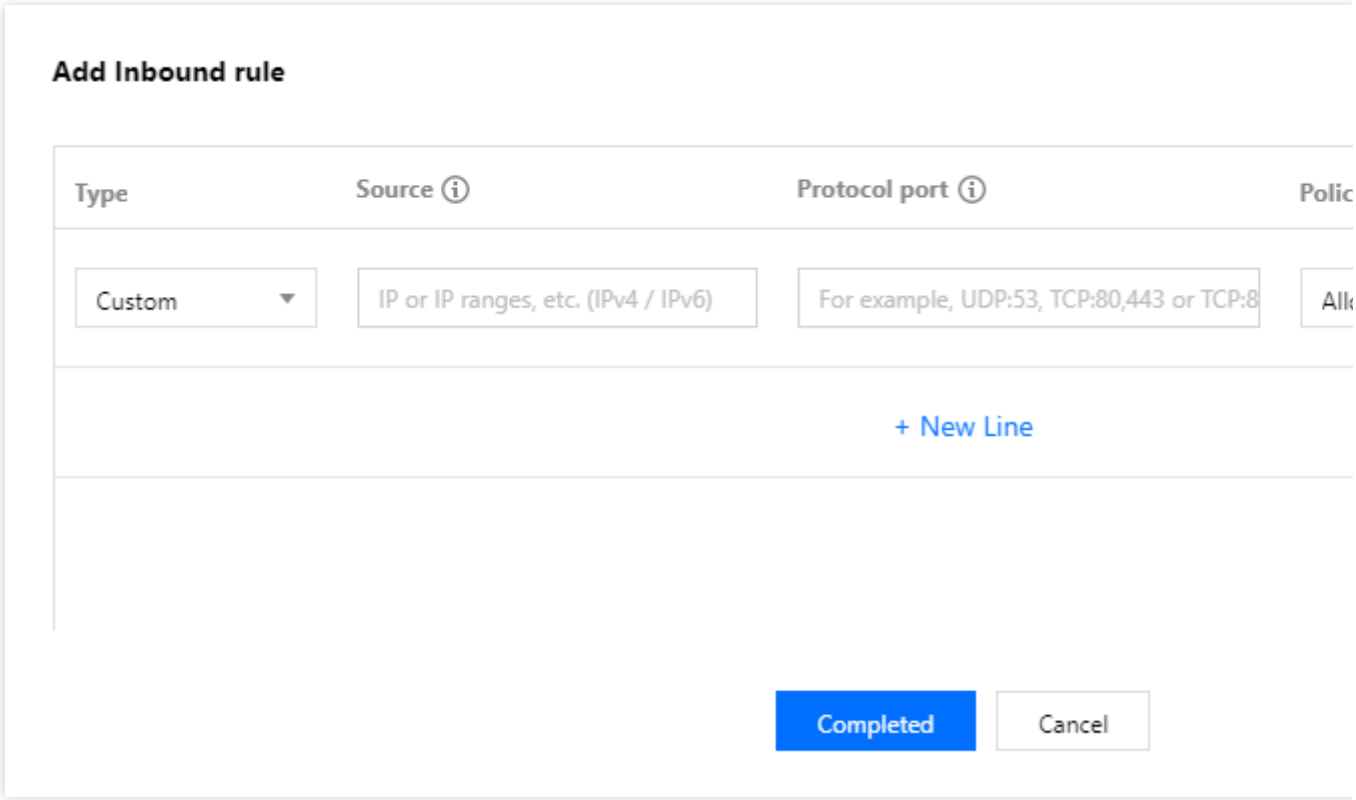
Note:

The following instructions use **Add a Rule** as an example.

Open all ports: this method is ideal if you do not need custom ICMP rules and all traffic goes through ports 20, 21, 22, 80, 443, and 3389 and the ICMP protocol.

Add a Rule: this method is ideal if you need to use multiple protocols and ports other than those mentioned above.

6. In the pop-up window, set rules.



Configure the following parameters:

Type: **Custom** is selected by default. You can also choose another system rule template including **Login Windows CVMs (3389)**, **Login Linux CVMs (22)**, **Ping**, **HTTP (80)**, **HTTPS (443)**, **MySQL (3306)**, and **SQL Server (1433)**.
Source or **Destination**: traffic source (inbound rules) or destination (outbound rules). You need to specify one of the following options:

Source or Destination	Description
A single IPv4 address or an IPv4 range	In CIDR notation, such as 203.0.113.0, 203.0.113.0/24 or 0.0.0.0/0, where 0.0.0.0/0 indicates all IPv4 addresses will be matched.
A single IPv6 address or an IPv6 range	In CIDR notation, such as FF05::B5, FF05:B5::/60, ::/0 or 0::0/0, where ::/0 or 0::0/0 indicates all IPv6 addresses will be matched.
ID of the referenced security group. You can reference the ID of: Current security group Other security group	To reference the current security group, please enter the ID of security group associated with the CVM. You can also reference another security group in the same region and belongs to the same project by entering the security group ID. **Note:** The referenced security group is available to you as an advanced feature. The rules of the referenced security group are not added to the current security group. If you enter the security group ID in Source/Destination when configuring security group rules, the private IP addresses of the CVM instances and the ENIs that are associated with this security group ID are used as the source/destination. This does not include public IP addresses.
Reference an IP address object or IP address group object in a parameter template.	-

Protocol port: enter the protocol type and port range or reference a protocol/port or protocol/port group in a parameter template. The supported protocol type includes TCP, UDP, ICMP, ICMPv6 and GRE in the following formats.
Single port: such as `TCP:80` .
Multiple ports: such as `TCP:80,443` .
Port range: such as `TCP:3306-20000` .
All ports: such as `TCP:ALL` .
Policy: **Allow** or **Refuse**. **Allow** is selected by default.
Allow: traffic to this port is allowed.
Refuse: data packets will be discarded without any response.
Notes: a short description of the rule for easier management.
7.

Click **Complete** to finish adding the rule.

8. To add an outbound rule, click **Outbound rule** and refer to Step 5 to Step 7.

Associating CVM Instances with Security Groups

Last updated：2024-01-08 09:41:35

Note:
Security groups can be associated with CVMs, ENIs, TencentDB for MySQL, and CLBs. This topic describes how to associate a security group with a CVM.

Overview

Security groups can be associated with one or more CVMs for network access control. They are an important part of CVM network security measures. You can associate your CVM with one or more security groups if necessary. The following are detailed instructions.

Prerequisites

You should already have a CVM instance created before starting.

Directions

1. Log in to the CVM console.
2. On the left sidebar, choose **Security Group** to go to the **Security Group** page.
3. On the **Security Group** page, select a region and locate the security group for which you want to set rules.
4. In the row of the target security group, click **Manage Instances** in the **Operation** column of the target security group. The **Associated Instances** page then appears.
5. On the **Associates Instances** page, click **Add Instance**.
6. In the pop-up **Add Instance** window, select the instances to bind and click **OK**.

Note:
After multiple security groups are bound to an instance, they are executed based on their priorities, which are consistent with their binding sequence. To adjust the priorities of the security groups, see Adjusting Security Group Priority.

Subsequent Operations

You can check all security groups in a specific region.

For operation details, see Viewing Security Groups.

If you want to disassociate a CVM instance from one or more security groups, you can remove it from the security group.

For operation details, see Remove from Security Groups.

If you no longer need a security group, you can delete it. Once a security group is deleted, all rules within it are also deleted.

For operation details, see Deleting a Security Group.

Managing Security Groups
Viewing Security Groups

Last updated：2024-01-08 09:41:35

Scenario

This article describes how to view all security groups of a region.

Directions

View security groups

1. Log in to the CVM Console.
2. In the left sidebar, select **Security Group**. The Security Group page then appears.
3. Select a region to see a list of security groups under that region.

Search for a security group

You can also use the search bar on the Security Group page to quickly find a specific security group.
1. Log in to the CVM Console.
2. In the left sidebar, select **Security Group**. The Security Group page then appears.
3. On the Security Group Management page, select **Regions**.
4. Click the search bar and use one of the following fields to search for a security group.
Security Group ID: input the desired ID and click

to see the corresponding security group.
Security Group Name: input the desired name and click

to see the corresponding security group.
Tag: input a tag and click

to see a list of all security groups with that tag.

Other Operations

To learn more about how to search for a security group, click

.

Remove from Security Groups

Last updated：2024-01-08 09:41:35

Scenario

You can remove a CVM instance from a security group if necessary.

Prerequisites

The instance is associated with two or more security groups.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select **Security Group**. The Security Group page then appears.
3. Select the desired region and find the desired security group.
4. Click the corresponding **Manage Instances** button to go to the **Bind with Instance** page.
5. Select the instances to be removed and click **Remove Selected**.
6. In the pop-up window, click **OK**.

Cloning Security Groups

Last updated：2024-01-08 09:41:35

Scenario

You might need to clone a security group if you:
Have created a security group sg-A in region A and you want to apply the same rules to an instance in region B. You can clone sg-A to region B, instead of creating a new security group from scratch.
Need a new security group for your service but want to clone the old security group as a backup.

Notes

By default, when you clone a security group, only the rules are cloned, not the association with instances.
You can clone a security group across projects and regions.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select **Security Group**. The Security Group page then appears.
3. Select desired region. A list of security groups under the region then appears.
4. Locate the desired security group and click **More**. Then click **Clone**. The **Clone security group** page then appears.
5. Select a **Target region** and **Target project** and input a **New name** for the new security group. Click **OK**.

Deleting a Security Group

Last updated：2024-01-08 09:41:35

Scenario

If you no longer need a security group, you can delete it. Once a security group is deleted, all rules within it are also deleted.

Prerequisites

Before deleting a security group, you must remove all associated CVM instances. Otherwise, the operation will fail. For details, refer to Removing From Security Group.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select **Security Group**. The Security Group page then appears.
3. Select the desired region and find the security group to be deleted.
4. Locate the desired security group and click **Delete**.
5. In the pop-up window, click **OK**.

Adjusting Security Group Priority

Last updated：2024-01-08 09:41:35

Overview

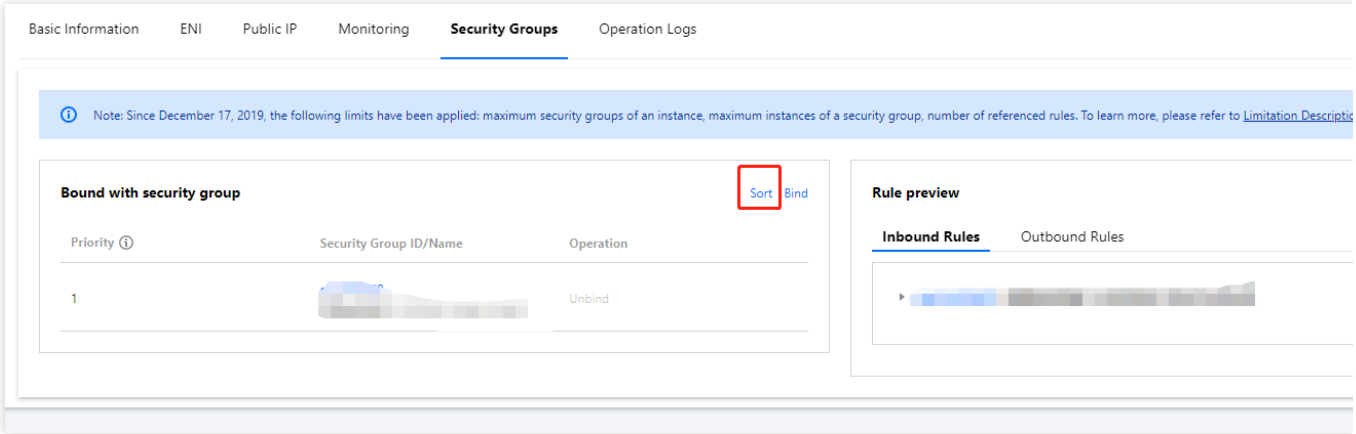
You can bind one or more security groups to a CVM. If you have bound multiple security groups, these security groups are executed based on their priorities. You can adjust the priorities as follows.

Prerequisite

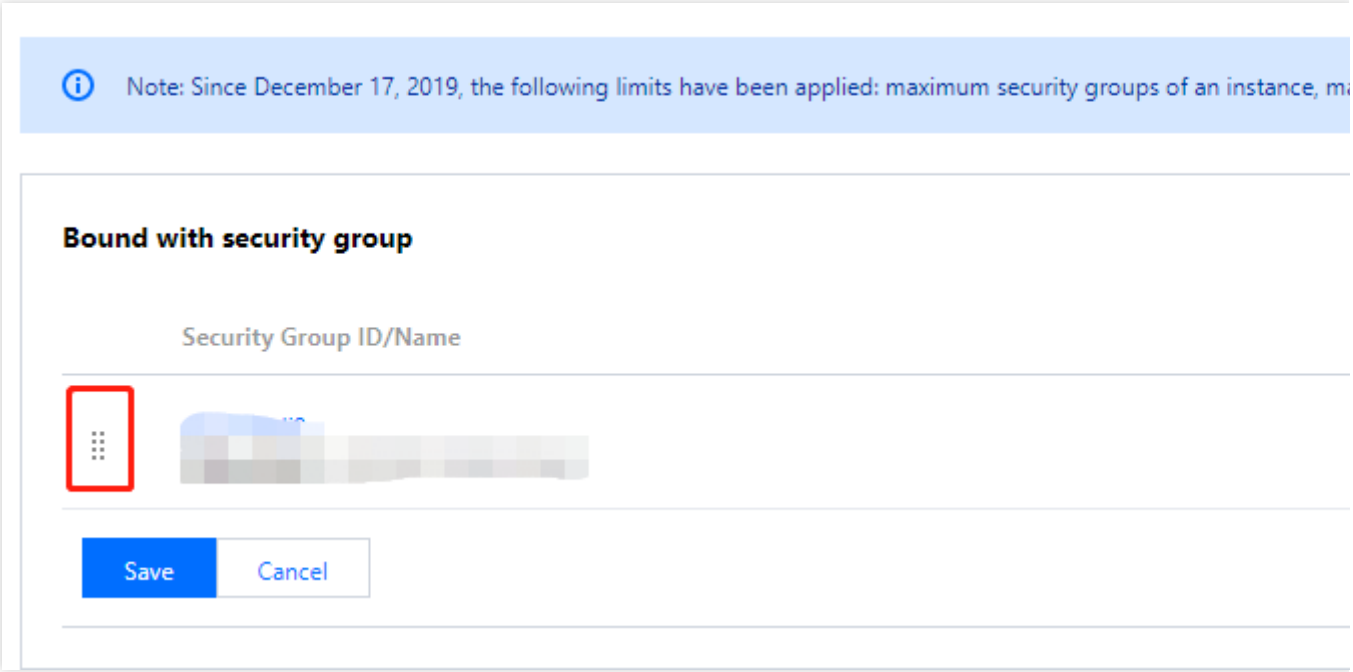
The CVM instance is bound to two or more security groups.

Directions

1. Log in to the CVM console.
2. On the instance management page, click the ID of the CVM instance to go to the details page.
3. Click the **Security Groups** tab to enter the security group management page.
4. In the **Bound Security Groups** module, click **Sort**.



5. Click the following icon and drag it up/down to adjust the priority of the security group. The higher the position is, the higher the priority of the security group becomes.



6. After completing the adjustment, click **Save**.

Managing Security Group Rules
Viewing Security Group Rules

Last updated：2024-01-08 09:41:35

Scenario

After adding a security group rule, you can view its details in the console.

Prerequisites

You have created a security group and added at least one rule.
For information on how to create a security group and a security group rule, refer to Creating a Security Group and Adding Security Group Rules.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select **Security Group**. The Security Group page then appears.
3. On the **Security Group** page, select a region, and find the security group for which you want to view rules.
4. Click the ID or the desired security group to go to the details page.
5. Select **Inbound rule** or **Outbound rule** to view all inbound or outbound security group rules.

Modifying Security Group Rules

Last updated：2024-01-08 09:41:35

Scenario

This article describes how to modify a security group rule. Rules are important because they protect you CVM instance from malicious attacks. For example, they can protect certain ports from being abused.

Prerequisites

Make sure you have created a security group with rules.
Refer to Creating Security Groups and Adding Security Group Rules.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select **Security Group**. The Security Group page then appears.
3. Select the desired region and find the security group.
4. Locate desired security group and click **Modify Rules**. The Security Group Rule page then appears.
5. Use **Inbound rule** and **Outbound rule** to switch between inbound and outbound security group rules.
6. Locate the desired rule and click **Edit** to modify it.

Note:
You don’t need to reboot the CVM for the rule changes to take effect.

Deleting Security Group Rules

Last updated：2024-01-08 09:41:35

Scenario

If you no longer need a security group rule, you can delete it.

Prerequisites

You have created a security group and added at least one rule to it.
For information on how to create a security group and add security group rules to it, see Creating a Security Group and Adding Security Group Rules.
You have confirmed that your CVM instance does not need to permit or forbid Internet access or private network access.

Directions

1. Log in to the CVM console.
2. In the left sidebar, click **Security Group**. The "Security Group" page then appears.
3. On the security group management page, select **Region** and locate the security group whose rules you want to delete.
4. In the action column, click **Modify Rule** to go to the security group rule page.
5. Select inbound or outbound rules by clicking **Inbound Rules** or **Outbound Rules**.
6. Locate the security group rule to delete and click **Delete** in the action column.
7. In the window that appears, click **OK**.

Exporting Security Group Rules

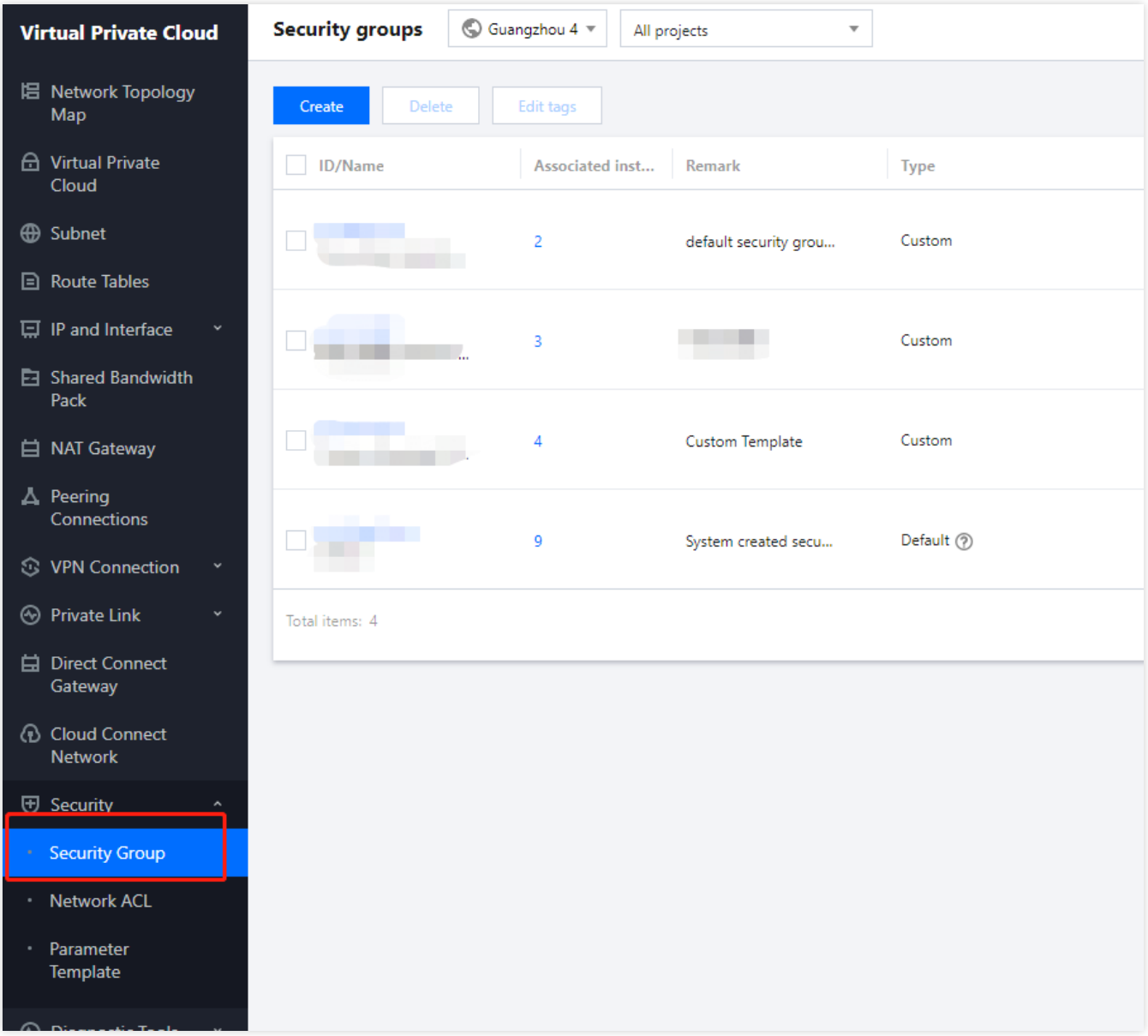
Last updated：2024-01-08 09:41:35

Scenarios

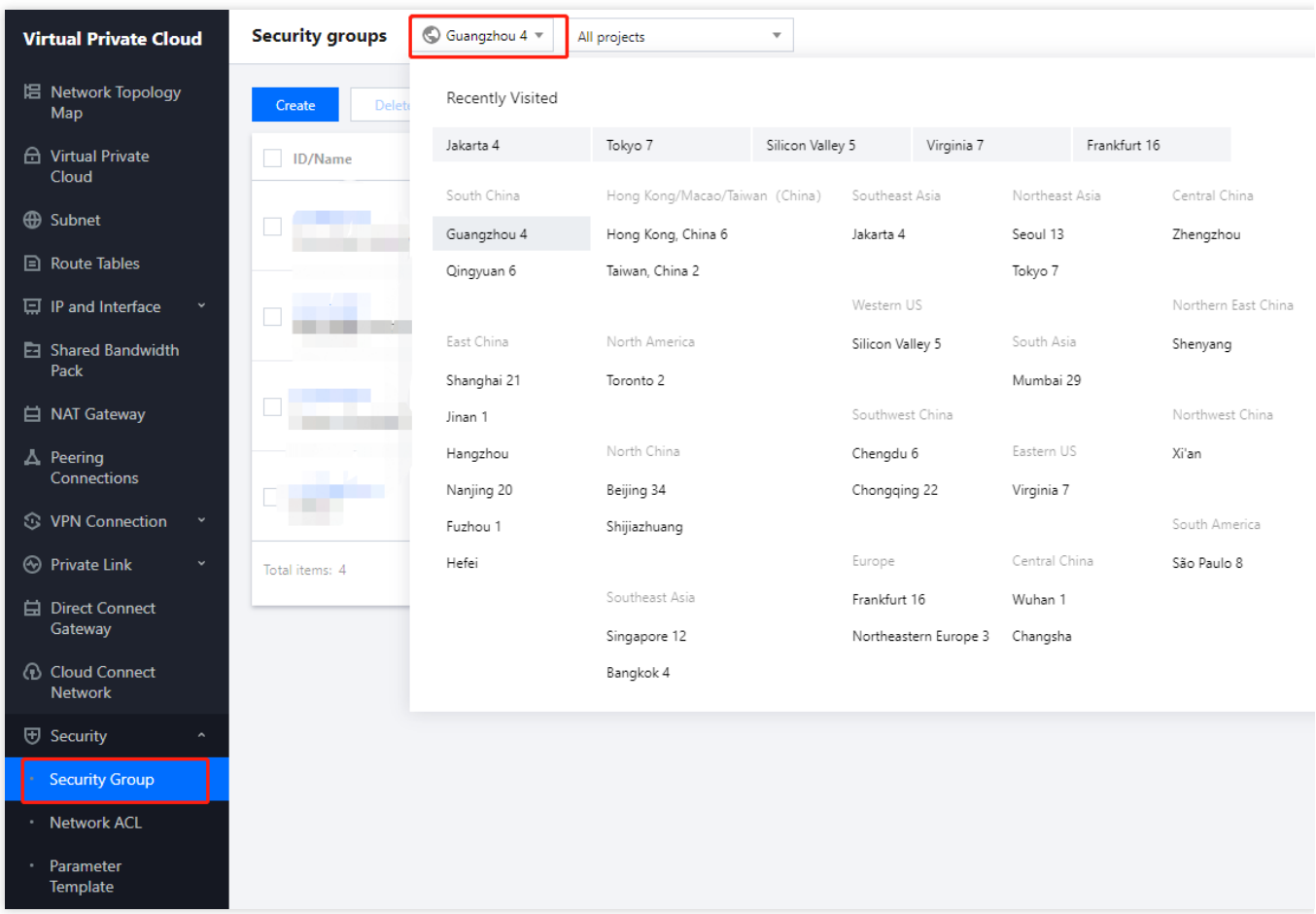
You can export security group rules and save them locally for backup.

Directions

1. Log into the CVM Console.
2. On the left sidebar, choose **Security Group** to go to the **Security Group** page.

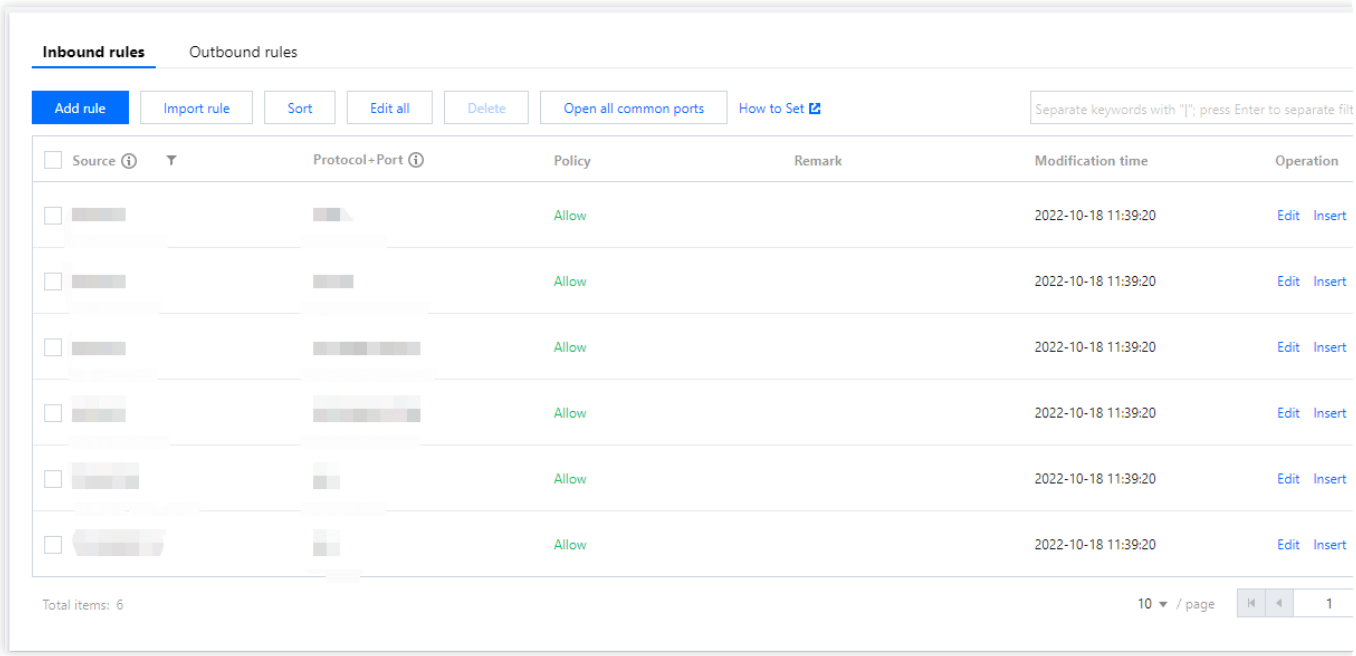


3. Select a region and locate the target security group.



4. Click the name or ID of the desired security group. The details page of the selected security group appears.
5. Use **Inbound Rule** and **Outbound Rule** to switch between inbound and outbound security group rules.
6. Click

to export security group rules to a file and save it to your local device.



Importing Security Group Rules

Last updated：2024-01-08 09:41:35

Scenario

Security group rules can be imported from a file. You can use this feature to quickly restore or create security group rules.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select **Security Group**. The Security Group page then appears.
3. Select desired region to see a list of security groups.
4. Locate desired security group and click its name. Security Group Rule page appears.
5. Select inbound or outbound rules by clicking **Inbound rule** or **Outbound rule**.
6. Click **Import rules**. The **Batch import - Inbound/Outbound Rules** page appears.
7. Click **Browse** and select a rule template file. Click **Import**.

Note:
If there are existing rules in the security group, export them before importing new rules. Existing rules are overwritten after importing.
If there is no existing rules in the security group, download the template first. Use it as a start to modify rules to your liking. Import them once you are finished.

Security Group Use Cases

Last updated：2024-01-08 09:41:35

Security groups can manage the access to CVMs. You can configure inbound and outbound rules for security groups to specify whether your server can be accessed by or can access other network resources.
The default inbound and outbound rules for security groups are as follows:
To ensure data security, the inbound rule for a security group is a rejection policy that forbids remote access from external networks. To enable public access to your CVM, you need to open the corresponding port to the Internet in the inbound rule.
The outbound rule for a security group specifies whether your CVM can access external network resources. If you select **Open all ports** or **Open ports 22, 80, 443, and 3389 and the ICMP protocol**, the outbound rule for the security group opens all ports to the Internet. If you select a custom security group rule, the outbound rule blocks all ports by default, and you need to configure the outbound rule to open the corresponding port to the Internet.

Common Use Cases

This document provides several common use cases of security groups. You can directly use its recommended security group configurations if a use case meets your requirements.

Scenario 1: remotely connecting to a Linux CVM via SSH

Case: you have created a Linux CVM and want to remotely connect to it via SSH.
Solution: when adding a security group rule, set **Type** to **Login Linux CVMs(22)**, enter WebShell proxy IP address for **Source**, and open TCP port 22 to the Internet to enable Linux login via SSH.
You can open all IP addresses or a specified IP address (or IP range) to the Internet as required. This allows you to configure the source IP addresses of the CVMs that can be remotely connected to through SSH.

Direction	Type	Source	Protocol Port	Policy
Inbound	Linux login	All IP addresses: 0.0.0.0/0 WebShell proxy IP addresses: as detailed in Orcaterm Proxy IP Addresses Updates Specified IP address: enter your specified IP address or IP range	TCP:22	Allow

Scenario 2: remotely connecting to a Windows CVM through RDP

Case: you have created a Windows CVM and want to remotely connect to it by using Remote Desktop (RDP).
Solution: when adding a security group rule, set **Type** to **Login Windows CVMs(3389)**, enter the WebRDP proxy IP

addresses for **Source**, and open TCP port 3389 to the Internet to enable remote login to Windows.
You can open all IP addresses or a specified IP address (or IP range) to the Internet as required. This enables you to configure the source IP addresses of the CVMs that can be remotely connected to via RDP.

Direction	Type	Source	Protocol Port	Policy
Inbound	Windows login	All IP addresses: 0.0.0.0/0 WebRDP proxy IP addresses: 81.69.102.0/24 106.55.203.0/24 101.33.121.0/24 101.32.250.0/24 Specified IP address: enter your specified IP address or IP range	TCP:3389	Allow

Scenario 3: pinging a CVM on the Internet

Case: you have created a CVM and want to test whether its communication with other CVMs is normal.
Solution: test the connection by using the `ping` command. Specifically, when adding a security group rule, set **Type** to **Ping** and open Internet Control Message Protocol (ICMP) ports to the Internet to enable other CVMs to access this CVM through ICMP.
You can open all IP addresses or a specified IP address (or IP range) to the Internet as required. This allows you to configure the source IP addresses of the CVMs that can access this CVM through ICMP.

Direction	Type	Source	Protocol Port	Policy
Inbound	Ping	All IP addresses: 0.0.0.0/0 Specified IP address: enter your specified IP address or IP range	ICMP	Allow

Scenario 4: remotely logging in to a CVM through Telnet

Case: you want to remotely log in to a CVM by using Telnet.
Solution: when adding a security group rule, configure the following security group rule:

Direction	Type	Source	Protocol Port	Policy
Inbound	Custom	All IP addresses: 0.0.0.0/0 Specified IP address: enter your specified IP address or IP range	TCP: 23	Allow

Scenario 5: allowing access to a web service through HTTP or HTTPS

Case: you have built a website and want to allow access to your website through HTTP or HTTPS.
Solution: when adding a security group rule, configure the following security group rules as required:
Allow all public IP addresses to access this website

Direction	Type	Source	Protocol Port	Policy
Inbound	HTTP (80)	0.0.0.0/0	TCP: 80	Allow
Inbound	HTTPS (443)	0.0.0.0/0	TCP: 443	Allow

Allow some public IP addresses to visit this website.

Direction	Type	Source	Protocol Port	Policy
Inbound	HTTP (80)	IP address or IP range that is allowed to access your website	TCP: 80	Allow
Inbound	HTTPS (443)	IP address or IP range that is allowed to access your website	TCP: 443	Allow

Scenario 6: allowing an external IP address to access a specified port

Case: you have deployed a service and want the specified service port (such as port 1101) to be externally accessible.
Solution: when adding a security group rule, set **Type** to **Custom** and open TCP port 1101 to the Internet to allow external access to the specified service port.
You can open all IP addresses or a specified IP address (or IP range) to the Internet as required. This allows the source IP address to access the specified service port.

Direction	Type	Source	Protocol Port	Policy
Inbound	Custom	All IP addresses: 0.0.0.0/0 Specified IP address: enter your specified IP address or IP range	TCP: 1101	Allow

Scenario 7: rejecting an external IP address to access a specified port

Case: you have deployed a service and want to prevent external access to a specified service port (such as port 1102).
Solution: when adding a security group rule, set **Type** to **Custom**, configure the TCP port 1102, and set **Policy** to **Reject**, so that external services cannot access the specified service port.

Direction	Type	Source	Protocol Port	Policy
Inbound	Custom	All IP addresses: 0.0.0.0/0	TCP: 1102	Reject

		Specified IP address: enter your specified IP address or IP range		

Scenario 8: allowing a CVM to access only a specified external IP address

Case: you want your CVM to access only a specified external IP address.

Solution: add two outbound security group rules as follows.

Allow the CVM instance to access a specified external IP address.

Forbid the CVM instance from accessing any public IP addresses via any protocol.

Note:

The first rule takes priority over the second.

Direction	Type	Source	Protocol Port	Policy
Outbound	Custom	Specified public IP address that the CVM can access	Required protocol and port number	Allow
Outbound	Custom	0.0.0.0/0	All	Reject

Scenario 9: prohibiting a CVM from accessing a specified external IP address

Case: you do not want your CVM to access a specified external IP address.

Solution: add a security group rule as follows.

Direction	Type	Source	Protocol Port	Policy
Outbound	Custom	Specified public IP address that your CVM instance cannot access	All	Reject

Scenario 10: uploading or downloading a file from a CVM through FTP

Case: you want to allow uploads and downloads over FTP.

Solution: add a security group rule as follows.

Direction	Type	Source	Protocol Port	Policy
Inbound	Custom	0.0.0.0/0	TCP: 20 to 21	Allow

Multi-scenario Configurations

You can configure multiple security group rules to meet your business requirements. For example, both inbound and outbound runes can be simultaneously configured. A CVM instance can be bound to one or multiple security groups. When it is bound to multiple security groups, the security group rules will be matched sequentially from top to bottom.

You can adjust the priorities of security groups at any time. For more information about the priorities, see Rule Priorities.

Server Common Port

Last updated：2024-01-08 09:41:35

This document describes common server ports. For more information on service application ports for Windows, see Service Overview and Network Port Requirements for Windows.

Port	Service	Description
21	FTP	An open FTP server port for uploading and downloading.
22	SSH	An SSH port for remotely connecting to Linux servers in CLI mode.
25	SMTP	An open SMTP server port for sending emails.
80	HTTP	A port for web services, such as IIS, Apache, and Nginx, to provide external access.
110	POP3	A port for the POP3 (email protocol 3) service.
137, 138, 139	NetBIOS protocol	Ports 137 and 138 are UDP ports for transferring files through My Network Places. Port 139: connections established through port 139 attempt to access the NetBIOS/SMB service. This protocol is used for file and printer sharing on Windows and SAMBA.
143	IMAP	A port for Internet Message Access Protocol (IMAP) v2, which is a protocol for receiving emails like POP3.
443	HTTPS	A port for web browsing. HTTPS is a variant of HTTP that provides encryption and transmission over secure ports.
1433	SQL Server	Default port for SQL Server. The SQL Server service uses two ports: TCP-1433 and UDP-1434. Port 1433 is used to provide external services, and port 1434 is used to return a response to the requester to indicate the TCP/IP port used by SQL Server.
3306	MySQL	Default port for MySQL databases, which is used by MySQL to provide external services.
3389	Windows Server Remote Desktop Services	Service port for the Windows Server remote desktop, through which you can connect to a remote server by using the "Remote Desktop" connection tool.
8080	Proxy port	Similar to port 80, port 8080 is used in the WWW proxy service for web

		browsing. The port number ":8080" is often appended to the URL when you visit a website or use a proxy. In addition, after the Apache Tomcat web server is installed, its default service port is port 8080.

Security Group API Overview

Last updated：2024-01-08 09:41:35

API Name	Description
CreateSecurityGroup	Create security groups
CreateSecurityGroupPolicies	Create security group rules
DeleteSecurityGroup	Delete security groups
DeleteSecurityGroupPolicies	Delete security group rules
DescribeSecurityGroupAssociationStatistics	Query the statistics of the instances associated with a security group
DescribeSecurityGroupPolicies	Query security group rules
DescribeSecurityGroups	Query security groups
ModifySecurityGroupAttribute	Modify security group attributes
ModifySecurityGroupPolicies	Modify the inbound and outbound rules of a security group
ReplaceSecurityGroupPolicy	Replace a single security group rule