Cloud Firewall

Operation Guide

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Operation Guide
Firewall Switch
Internet Boundary Firewall Switch

Last updated: 2025-05-20 10:31:31

The Cloud Firewall provides an internet boundary switch feature. On the internet boundary switch page, it can automatically detect your public network IP and associated cloud assets, and configure the corresponding firewall switch for you. The Cloud Firewall switch supports one-click protection. You don't need to perform any network access deployment or routing policy configuration, nor install any image files. The Cloud Firewall offers you an out-of-the-box product experience.

Access Mode Description

The current Internet edge firewall supports two deployment modes: serial and bypass. You can choose different modes to enable protection.
Inline Firewall and Bypass Firewall are two different firewall deployment methods. Their positions and working principles in the network vary.

How It Works / Deployment Type	Serial Firewall	Bypass Firewall
deployment path	Inline Firewall is directly deployed on the path of network data flow, and all passing data packets must be checked and processed by the firewall.	Bypass Firewall is not directly deployed on the path of network data flow. Instead, it uses technologies such as mirroring or port replication to obtain copies of network traffic for analysis and detection.
Process data	Since inline firewalls need to process all passing data packets, they have relatively high requirements for performance and processing capability. If the firewall performance is insufficient, it may become a network bottleneck, affecting network speed and stability. Therefore, a serial firewall requires creating a new firewall instance in each region and allocating corresponding bandwidth.	Bypass Firewall only needs to process mirror traffic, with relatively low requirements for performance and processing capability. It can provide security monitoring, interception, and alarm features without affecting network performance.
Security Protection	Inline Firewall can perform deep inspection and processing on data packets, providing relatively high security assurance. It can block malicious data packets from entering the network and protect internal resources from attacks.	The security protection capability of the Bypass Firewall is relatively limited, only able to protect traffic of TCP, HTTP/HTTPS, and TLS/SSL protocols. Moreover, public network mutual access traffic within Tencent Cloud cannot be protected by the Bypass Firewall due to the architecture features of the network. The bypass architecture can indirectly block the connection between the attacker and the target system by sending TCP RST packets through mechanisms such as the preemptive response mechanism.

Notes:
- serial mode supported regions: Chinese mainland, Hong Kong (China), Singapore, Tokyo, Seoul.
- bypass mode supported regions: Chinese mainland.

Support Asset Types

Internet edge firewall supports the following asset types:

Product name		Internet Edge Firewall (Serial Mode)	Internet Edge Firewall (Bypass Mode)
Cloud Virtual Machine (CVM)		Supported	Supported
Lighthouse		Not supported	Supported
Elastic IP	general BGP IP	EIP supports after binding an instance. For details, check whether the firewall switch can be enabled in the console. If you have any questions, you can submit a ticket to contact us.	Supported
	premium BGP IP		Supported
	Accelerated IP		Supported
	static single-line IP		Supported
	High-defense EIP		Supported
	Dedicated internet tunnel	Supported	Supported
Cloud Load Balancer (CLB)	CLB	Not supported	Supported
	Domain-name based CLB	Not supported	Supported
	IPv6 CLB	Not supported	Not supported
	classic CLB	Not supported	Supported
VPN Connections		Not supported	Supported
API Gateway		Not supported	Supported
Bastion Host		Not supported	Not supported

Serial Firewall Preparations

Before using a serial firewall, first perform the following preparations:

Allocate Bandwidth for a Serial Firewall

Since the serial firewall has a region cluster property and has a protection performance upper limit, users are advised to allocate bandwidth for the regions that require the use of the serial firewall.

1. Log in to the CFW console, in the left sidebar, select the **firewall switch** page, and click **Firewall Settings**.

2. Allocate bandwidth for the regions where serial firewalls are required. It is advisable to reasonably estimate based on business peaks. **Bandwidth overage may trigger service degradation**. The cloud firewall will automatically switch the access mode to bypass. For details, see Internet edge firewall bandwidth overage disposal.

Notes:

- General bandwidth: In the current version, allocating bandwidth to a serial firewall consumes general bandwidth, which is shared with the NAT boundary firewall.
- general instance: In the current version, adding a new serial firewall region will consume one general instance quota. General instance quotas are shared with NAT boundary firewalls.
- serial firewall regions: The regions supported in the current version are subject to the regions displayed in the serial firewall settings. More regions are gradually being rolled out in grayscale. Stay tuned.

Confirm That the Asset Is Compliant with the Protection Scope

- Due to network architecture limitations, the current version of the serial firewall only supports protecting Elastic IPs in the latest network architecture. For specifics, refer to the console display. If you have any questions, contact the Elastic IP team for confirmation. Protection for public network CLB types is not currently supported. If protection is needed, switch to the EIP + private network CLB form, which is supported.
- The supported asset types for the current version of the bypass firewall are: Cloud Service CVM, NAT gateway, VPN gateway, Lightweight Server LH, CLB, etc.

Serial Firewall Switch Operation

1. Log in to the CFW console. In the left sidebar, select **Firewall Switch** > **Protected Target** > **Internet Boundary**.
2. On the internet boundary page, locate the assets that need protection, and confirm that the access mode is displayed as **serial**.

3. Click in the firewall switch column to perform boundary protection for this asset.
4. The process of enabling the serial firewall is expected to take 1 minute and has no impact on the network.

Notes:

- Serial mode requires the use of Private Link to connect the VPC to the firewall's network.
- When enabling a serial firewall for the first time for an EIP within the same VPC, you need to create a new private connection endpoint and divert the private IP. The private connection within the serial firewall specification (allocated bandwidth) incurs no additional charge. Exceeding the quota may lead to certain fees. For details, see Private Connection Pricing. Subsequently, the serial firewall switch within the same VPC does not require re-creation of the private connection.

Bypass Firewall Switch Operation

1. Log in to the Cloud Firewall Console. In the left navigation bar, select **Firewall Switch** > **Protected Target** > **Internet Boundary**.
2. On the internet boundary page, locate the assets that need protection, and confirm that the access mode is displayed as **bypass**.

3. Click in the firewall switch column to perform boundary protection for this asset.

Notes:

- Current version supports asset types: Cloud Service CVM, CLB, NAT gateway, VPN gateway, Lightweight Server LH. Currently supports assets in Chinese mainland and Hong Kong (China).
- Turn on the switch: When the switch is turned on, all traffic from this public IP will pass through the cloud firewall, and the access control, intrusion defense, and log audit features will take effect for this public IP.
- – Turn off the switch: When the switch is turned off, all traffic from this public IP will not pass through the cloud firewall.

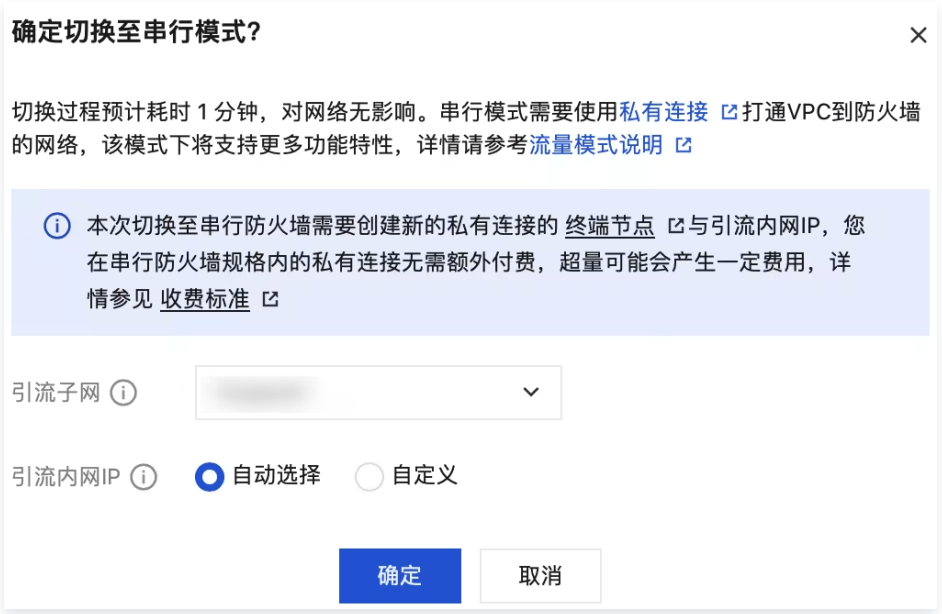
Switching Access Mode

Log in to the Cloud Firewall console. In the left sidebar, select **Firewall Switch** > **Protected Target** > **Internet Boundary**.

Switching the Traffic Mode of a Single Switch

1. On the Internet boundary page, when the firewall switch status is **Off**, simply select the desired access mode to switch. This has no impact on the network.

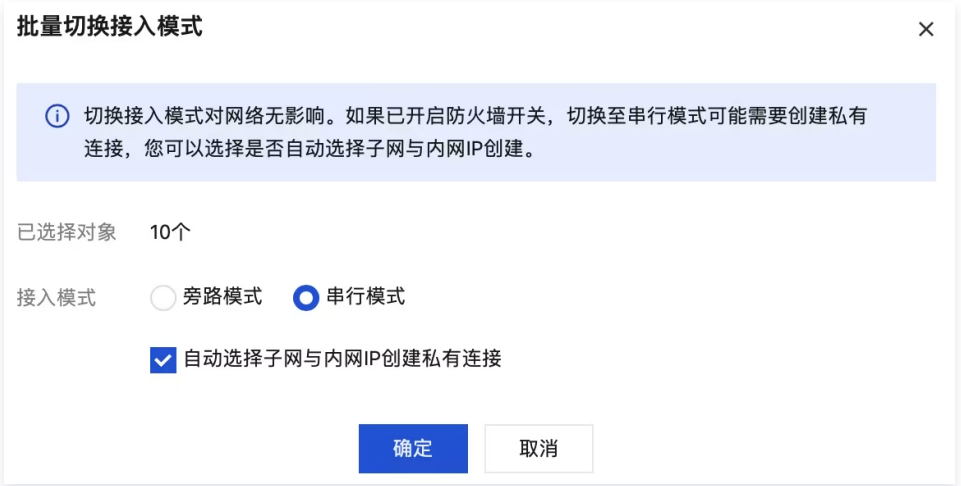
2. If the firewall switch is in the **on** state, switching the access mode will trigger the turn on or off operation of the serial firewall switch. For details, see serial firewall switch operation.



Batch Switch Firewall Switch Access Mode

1. On the internet boundary page, check the firewall switches that need to be switched, and click **Switch Mode**.

2. Confirm that you need to switch the access mode, and click **OK**. If it is serial mode, you can choose whether to automatically select subnets and private IPs to create a private connection.



Firewall Status Monitoring

Users can view and monitor bandwidth status based on public IPs in real time, thereby making timely adjustments such as scaling up or turning off some switches.

1. In the upper-right corner of the status monitoring panel, click the icon.

2. On the status monitoring page, you can view and monitor bandwidth status based on public IPs in real time, and perform operations such as scaling out or turning off some switches.

> **Notes:**
> Peak bandwidth refers to the maximum value of both upstream and downstream. For example, if you purchase 100M bandwidth, the CFW can process 100M upstream and 100M downstream simultaneously.

New Asset Auto On

1. Log in to the CFW console, in the left sidebar, select the **firewall switch** page, and click **firewall setting**.

2. Click **Feature Configuration** > **New Asset Auto-Enable Switch**. When the public IP quota allows protection, the internet boundary switch will be automatically enabled for newly-added public IP assets. Below, you can choose whether to enable serial access mode by default and whether to automatically create a private connection.

Internet Edge Firewall Excess Bypass Weight Setting

- You can customize switch weights. When traffic exceeds the Internet edge firewall specification, we will sequentially Bypass according to the switch weight level you define until the bandwidth in the current region drops within specification.
- Instances with the same weight will be shut down sequentially in descending order of peak bandwidth. The initial weight defaults to 1, with a maximum of 100 and a minimum of 0. A larger weight indicates a higher priority.

Operation Steps

1. Log in to the CFW console, in the left sidebar, select the **firewall switch** page, and click **firewall setting**.

2. In the **Firewall Setting** > **Feature Configuration** page, edit the specified firewall switch weight.

3. Click **Edit Weight** to select the firewall switch, batch edit the switch weight, and click **Confirm** to save.

Sync Assets

- Background periodically polls user asset information every 5 minutes. Therefore, when user asset scale changes within this interval but has not been synchronized by the backend, you can click **Sync Assets** at the top of the list to promptly invoke backend APIs to re-read and synchronize user asset information and data.
- When newly-added assets do not appear in the firewall switch list, you can click **Sync Assets** at the top of the list to attempt asset synchronization.

View Rules, Alarms, or Logs

Except for turning on the firewall switch in the asset list, you can perform some other operations, mainly including viewing rules, alerts, and logs associated with assets.

- View Rules: In the asset list, click **View Rules** in the Action column to navigate to the rules page associated with the asset.

- View alarms: In the asset list, click **More** > **View Alarms** in the Action column, select a specific event type, and navigate to the corresponding event page in the alert center.

- View logs: In the asset list, click **More** > **View Logs** in the Action column, select a specific log type, and navigate to the corresponding log page.

Internet Edge Firewall Bandwidth Overage Handling

Bandwidth overload of the Internet edge firewall will not cause packet loss or affect the traffic rate of customer business traffic, but it will be unable to provide protection features.

Starting from September 25, 2024, when business bandwidth exceeds the internet edge firewall bandwidth by 100%, the following measures will be taken:

- Turn off part of the internet boundary firewall switches, Bypass some traffic, and only protect traffic within the specified bandwidth.
- Serial and bypass mode disposal methods are consistent, turn off some switches to limit traffic.
- Support configuring firewall switch weight, set the priority of automatically closing firewall switches.

For more details, see Common Issues – Bandwidth Related.

Related Information

- If you need to perform traffic control and security protection for internal network assets or conduct network traffic forwarding based on SNAT and DNAT, see NAT boundary firewall switch for operations.
- To automatically detect VPC information and interconnections, and establish CFW switches between each pair of interconnected VPCs, see inter-VPC firewall switch for operations.
- If you encounter internet edge firewall-related issues, please refer to the Firewall document.

NAT Boundary Firewall Switch

Last updated: 2025-05-20 10:33:01

0 The NAT boundary firewall switch supports traffic control and security protection based on private network assets, while also supporting network traffic forwarding based on SNAT and DNAT.

1. Log in to the CFW console, in the left navigation bar, select **firewall switch** > **NAT Boundary Switch**.

> **Notes:**
> When a certain NAT boundary firewall toggle is enabled, the internet traffic of the corresponding subnet will transit through the firewall. At that time, the access control rules and intrusion prevention will take effect on it, and traffic logs will also be generated.

2. On the NAT Boundary Switch page, you can perform the following operations: create an instance, synchronize assets, view and monitor bandwidth status based on NAT boundary.

Creating an instance

1. On the NAT Boundary Switch page, click **Create Instance**.

2. In the pop-up window for creating a NAT Boundary Firewall, you can create a new NAT Boundary Firewall instance for the current account, fill in the relevant fields, and click **Next**.

> **Notes:**
> Create a "NAT boundary firewall" instance, which involves a large amount of backend configuration work. This procedure may last several minutes.

Field Descriptions:

- **Region**: Select the region for creation. Chinese mainland, Hong Kong (China), Taipei (China), and some overseas regions are supported. The selection cannot be changed after the instance is created.

  > **Notes:**
  > Users can select regions in Chinese mainland, Hong Kong (China), Taipei (China), and some overseas regions where they have VPCs. Multiple firewall instances can be created in the same region, but the total bandwidth must not exceed the specified specification.

- **Optional zone**: Select an availability zone according to your needs.
- **Instance name**: Enter the instance name.
- **Instance specification**: Select instance specifications according to needs. Minimum 20Mbps. If more bandwidth is needed, scale out. Instance specifications must match rule count specifications. For details, see Instance specification.

  > **Notes:**
  > The internet bandwidth must be consistent. If multiple NAT firewalls are used, the sum of their bandwidths must be less than or equal to the internet boundary bandwidth.

- **Mode**: Divided into new mode and access mode.
  - **New mode**: If there is no NAT Gateway in the current region, the new mode can use the NAT feature built into the NAT boundary firewall to enable specified instances to access the Internet through the firewall.
  - **Access mode**: If there is an existing NAT Gateway in the current region, or if you want to keep the egress IP for public network access unchanged, access mode can smoothly integrate the NAT boundary firewall between the NAT Gateway and CVM instances.
- **Elastic IP**: In new mode, the cloud firewall supports selecting idle and unused Elastic IPs for binding and also supports quick creation of Elastic IPs; if you choose to create a new Elastic IP, the system will automatically apply for one through CAM for the user.

> **Notes:**
> Note that the bandwidth of the Elastic IP must be greater than or equal to the protection bandwidth of the firewall; otherwise, an excess of protection bandwidth will occur. The cost of the Elastic IP is charged by the EIP product, and no EIP bandwidth fee is collected by the firewall.

3. Select the required VPC or NAT, then configure the firewall network settings and choose **Create a new traffic redirection subnet method**. The ways to establish a traffic redirection subnet include the following three:

> **Notes:**
> - Traffic redirection subnet: The CFW will create a subnet in the 24 network segment within your connected Virtual Private Cloud to redirect traffic to the firewall. You can choose different ways to create the subnet.
> - For NAT firewall instances below 600M: – New mode supports up to 8 VPCs. – Access mode supports up to 4 NAT gateways.
> - For NAT firewall instances above 600M: – New mode supports up to 10 VPCs. – Access mode supports up to 5 NAT gateways.

- Self-owned network range preferred: The cloud firewall will automatically select an available subnet range within the chosen VPC; when there are no subnet quotas available within the VPC, it will use the expansion IP range of the selected VPC.
- Preferred expansion IP range: The cloud firewall will preferentially use idle VPC reserved expansion subnets. In this mode, it does not occupy the subnet quota of the selected VPC.

> **Notes:**
> An expansion subnet refers to a secondary IP range in a private network. See Virtual Private Cloud – Edit IPv4 CIDR.

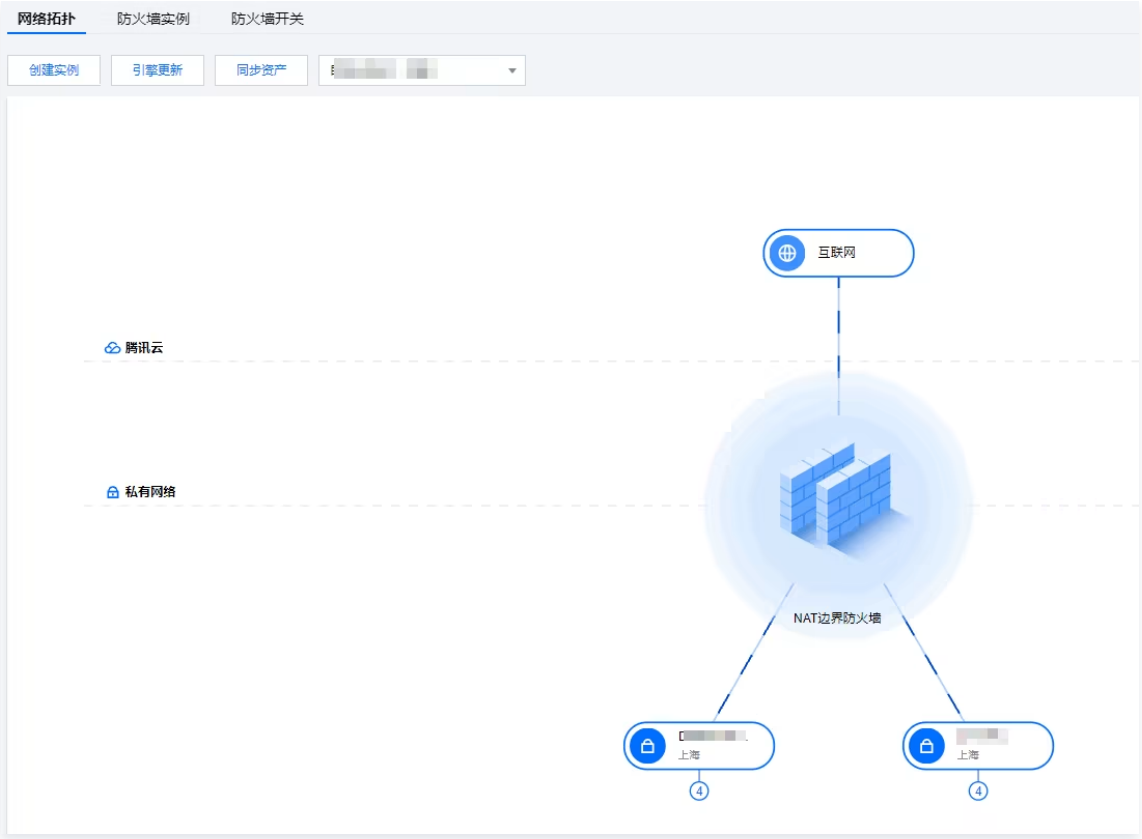
- Custom: Users can customize the subnet range for the firewall. Please note it must be a /24 IP range. The custom IP range must belong to the current VPC's CIDR. Input example: 192.168.0.0/24.

4. After the configuration is complete, click **Create** to successfully create a NAT boundary firewall.

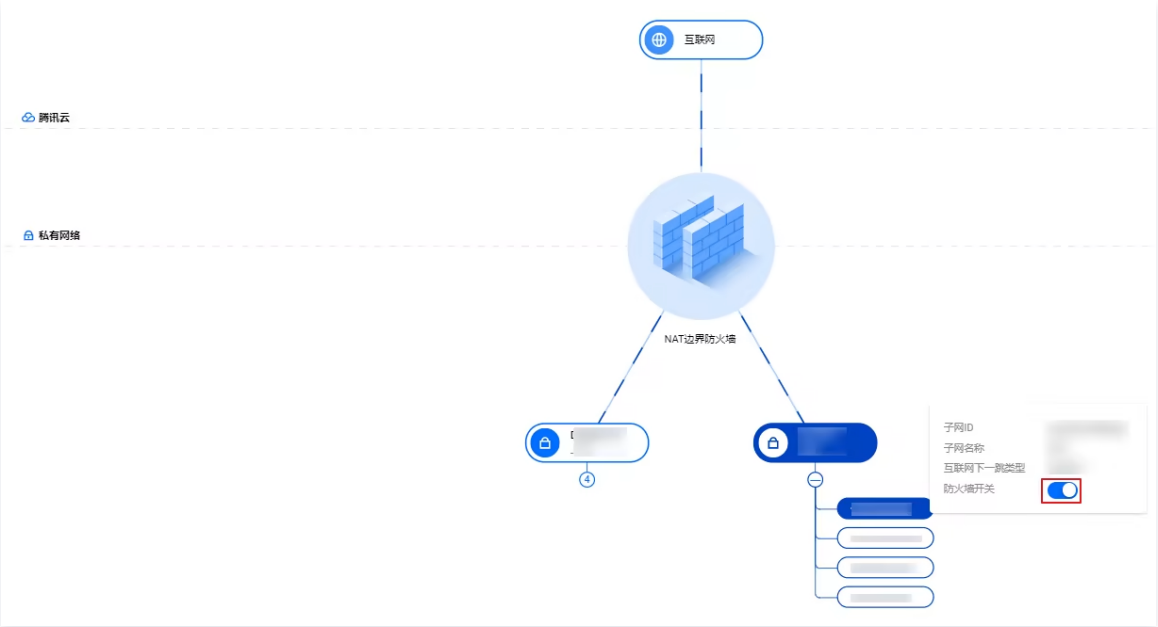
Network Topology

CFW provides a visual view to help you quickly sort out the access relationship at the NAT boundary. In the NAT boundary visual view, the private network displays the VPC instance.

1. On the NAT Boundary Switch page, click **Network Topology** to view the access relationships of the NAT boundary.



2. Click a certain VPC node to view the corresponding subnet list, and you can turn on or off the firewall switch targeting the current subnet.



Firewall Switch

On the Firewall Switch page, you can enable or disable NAT Boundary Protection. CFW will perform scheduled auto sync of cloud assets, so there's no need to worry about firewall configuration after asset changes (for example, if a subnet is modified, the firewall will automatically sync within a short time frame).

- **Enable protection**
  - Above the instance list, click **Enable All**. All NAT boundary firewall switches that are not enabled will be turned on. All routing tables will automatically add routing policies with the next hop type set to NAT boundary firewall. All internet traffic from all subnets will transit through the NAT boundary firewall.

Notes:

- After the switch is turned on, do not manually change the route corresponding to the switch in the VPC console, otherwise it will cause the firewall to lose the route and result in network interruption.
- If users choose to enable all subnets associated with the same route table, the system will automatically add a routing policy in this route table where the next hop points to the NAT boundary firewall and disable the original routing policy for accessing the public internet. Therefore, the internet traffic of all subnets associated with this route table will transit through the NAT boundary firewall.
- If the firewall instance is in access mode, please ensure that the switch at the SNAT rule schematic diagram of the corresponding NAT gateway is closed; otherwise, the firewall's traffic diversion policy will not take effect.

- A firewall switch corresponds to a subnet and is used to control whether traffic transits through the NAT boundary firewall. Subnets associated with the same routing table will be turned on or off simultaneously. After creating a NAT boundary firewall, the firewall will not divert traffic immediately. You need to go to the firewall switch page to manually enable it.

Notes:
After the switch is turned on, the system will automatically modify the routing policy of the subnet-associated routing table and the port forwarding rules corresponding to the subnet. The traffic of this subnet will be diverted to the NAT boundary firewall.

- **Disable protection**
  - **Method 1**: Above the instance list, click **Disable Protection**. All enabled NAT boundary firewall switches will be turned off. The NAT boundary firewall will automatically disable all routing policies with the next hop type set to NAT boundary firewall in all routing tables. All subnets will be disconnected from the Internet. Users need to manually start new routing policies in the VPC console.

Notes:
If users choose to disable all subnets associated with the same route table, the system will automatically disable the routing policy in this route table where the next hop points to the NAT boundary firewall. All subnets associated with

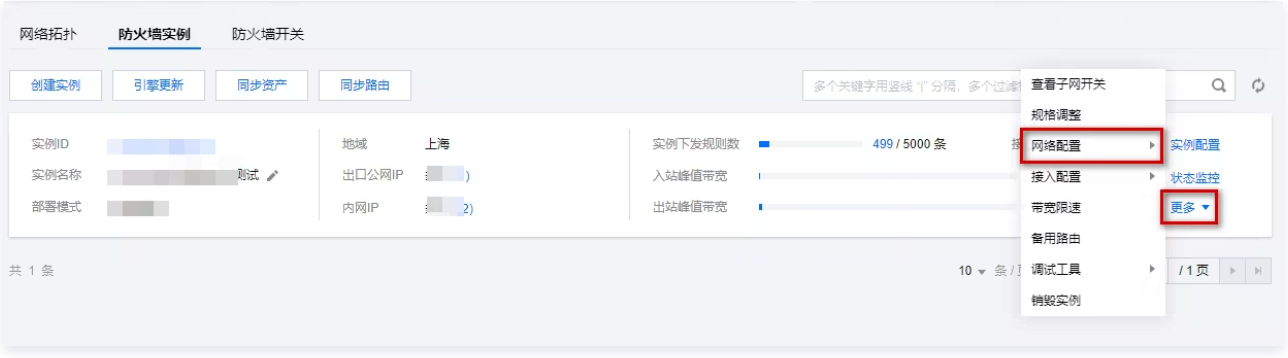
this route table will be disconnected from the Internet.

- **Method 2**: Disable the firewall switch individually.
  To disable a firewall switch individually, click the "Firewall Switch" button for a specific subnet in the firewall switch operation column. Other subnets associated with the same routing table will also be disabled simultaneously.

> **Notes:**
> After the switch is turned off, the system automatically restores the routing policies of the subnet-associated routing table and the port forwarding rules corresponding to the subnet. The traffic of this subnet returns to its original path and does not pass through the NAT boundary firewall.

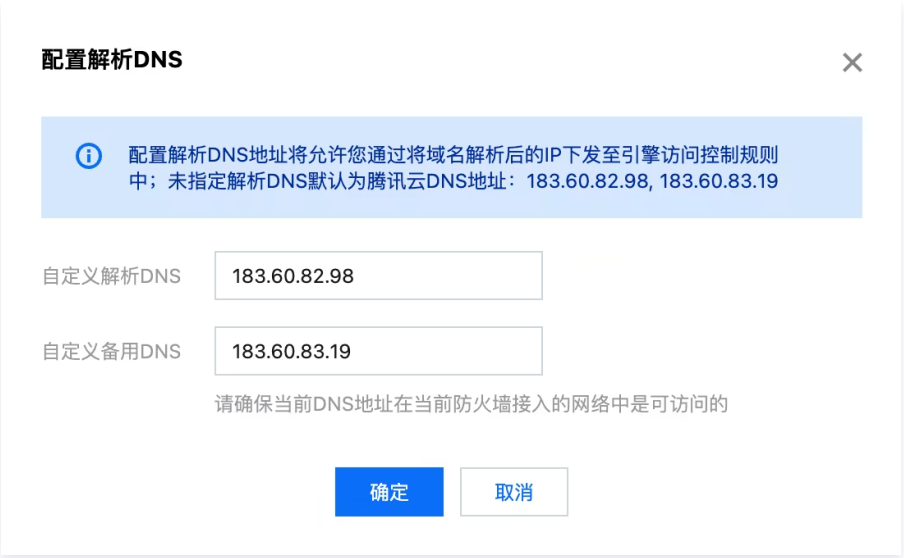
Network Configuration

1. On the NAT Boundary Switch > **Firewall Instance** page, select the required instance, click **More** > **Network Configuration**.



2. Click **Configure DNS Resolution** to set up a custom DNS resolution server address for access control rules related to domain name parsing types.
3. In the Configure DNS Resolution window, fill in relevant parameters, click **OK** to save.

> **Notes:**
> By default, Tencent Cloud's default DNS server addresses will be used, which are 183.60.82.98 and 183.60.83.19. If you need to specify a DNS server for parsing, please fill in below.



Instance configuration

On the NAT Boundary Switch page, click the corresponding **Instance ID**, or click **Instance Configuration** on the right of the firewall instance to enter the instance configuration page.

- **Port forwarding**
  In the right sidebar, you can view the DNAT port forwarding rules added by users based on the NAT boundary firewall instance, as well as the Elastic IPs associated with the instance.

> **Notes:**
> - In access mode, after the switch is turned on for the first time, the NAT boundary firewall will automatically synchronize the existing NAT gateway's port forwarding rules to ensure traffic flow. Subsequent operations for this rule should be performed in the CFW console.
> - Note: For subnets with the firewall switch turned on, their SNAT and DNAT traffic will transit through the firewall. For subnets with the firewall switch turned off, their SNAT and DNAT traffic will follow the original path.
> - Note: Do not go to the VPC console to operate port forwarding rules; otherwise, it may cause network interruption.

1.1 On the port forwarding tab of the instance configuration page, click **Create New Rule**.

1.2 In the "Create Port Forwarding Rule" pop-up box, users can add a DNAT rule for the current NAT Boundary Firewall Instance with an external IP bound to the user's Elastic IP.

> **Notes:**
> - In the drop-down box of the external IP port, the options provided are the Elastic IPs bound to the current NAT boundary firewall instance.
> - When entering an internal IP address, the user must input an available IP within the VPC segment of the local region.

- **Egress binding**

In new mode, when the rule list is empty, all subnets of VPCs will randomly select a NAT Gateway to access the Internet.

> **Notes:**
> Access mode does not support egress binding.

1.1 On the instance configuration page, under the egress binding tab, click **Create Rule**.

1.2 In the "Create Egress Binding Rule" pop-up, provide the firewall instance ID information. Users can add SNAT rules to the current NAT boundary firewall.

> **Notes:**
> - Instance types can be selected from private networks, subnets, and cloud servers. Only instances that are integrated with NAT boundary firewalls and currently have no bound egress NAT rules are supported for selection.
> - The exclusive IP option allows the selected external IP address to serve as the egress IP for the subnet/private network under the exclusive rule, and cannot be used by other subnets/private networks outside the exclusive rule.

- Integrate DNS traffic
  - Due to Tencent Cloud's underlying architecture, PrivateDNS (183.60.83.19, 183.60.82.98) traffic will not pass through firewall, so it cannot be protected by NAT boundary firewall. Other DNS traffic except PrivateDNS can transit firewall.
  - PrivateDNS: Please use DNS firewall protection. For details, see DNS Firewall Switch.
  - Other DNS: The firewall provides default support for protecting this type of traffic, with no need to enable an additional switch.
  - **Application Scenarios**: For other DNS, you can add DNS rules in access control rules to restrict access.
    - On the NAT Boundary Rule page, click **Outbound Rules**.
    - In the outbound rules tab, click **Add Rule**.
    - On the add rule page, fill in the relevant fields, select the DNS protocol, and click **OK**.

- **Associate Elastic IP**

  1.1 On the right side of the instance configuration page, in the "Associate Elastic IP" module, click **+Bind Elastic IP**.

  1.2 In the drop-down list, the user can bind a newly created EIP by the system to the current NAT Boundary Firewall Instance, or select one from all idle EIPs owned in the current region to bind.

  > **Notes:**
  > - Associate Elastic IP functionality currently only supports new mode.
  > - When you disassociate an Elastic IP, the corresponding DNAT rule on the page will also disappear.

- **Bandwidth throttling**

  On the Bandwidth Throttling tab of the instance configuration page, you can perform bandwidth throttling on the IP/CIDR addresses under the current firewall instance.

  > **Notes:**
  > The NAT Gateway rate limiting mechanism is triggered after traffic statistics are completed. Due to the time window between statistics and the speed limit taking effect, data discrepancies may exist in the traffic monitoring data on the NAT Gateway.

- **Add speed limit**

  1.1 Click **Add Rule**, and a pop-up window for adding rate-limiting rules will appear.

1.2 Enter the IP/CIDR address that requires rate limiting and the bandwidth rate to be limited. At least one of the inbound rate or outbound rate must be filled in as a rate limit. Unspecified fields will default to unlimited. Click **OK** to complete the bandwidth rate limiting setup.

> **Notes:**
> Support filling in private IP.

- Edit speed limit

1.1 In the successfully set rate-limiting rules, click **Edit** in the action bar to perform rule editing.

1.2 Re-enter the IP/CIDR address that requires rate limiting and the bandwidth rate to be limited. At least one of the inbound rate or outbound rate must be filled in as a rate limit. Unspecified fields will default to unlimited. Click **OK** to complete the bandwidth rate limiting setup.

- Delete rate limit

In the successfully set rate-limiting rules, click **Delete** in the operation column to delete the bandwidth throttling rule.

Specification Adjustment

1. On the NAT Boundary Switch page, click **scale-out** to navigate to the configuration change page, where you can upgrade bandwidth, version, log storage volume, and other parameters.

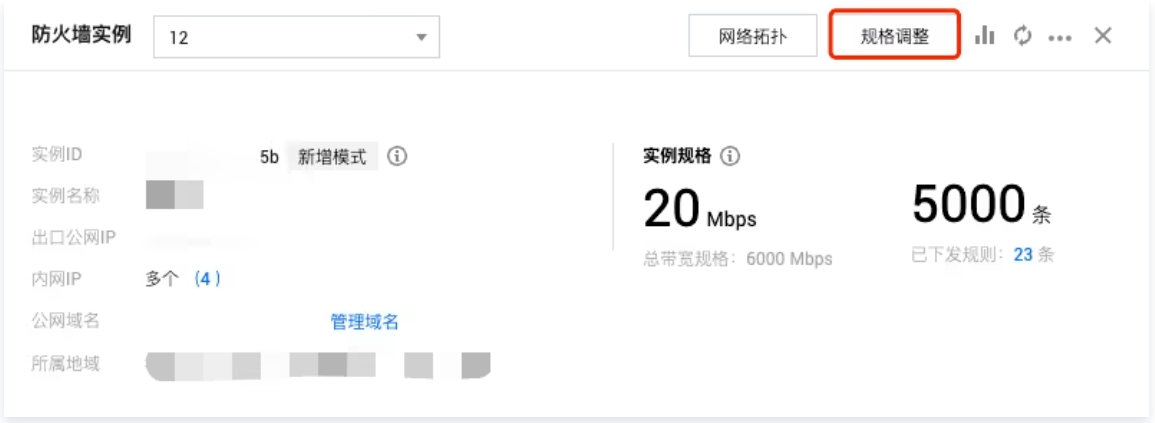
> **Notes:**
> If you only scale out the bandwidth here, this bandwidth refers to the Internet edge bandwidth, which can also be understood as the total bandwidth of the cloud firewall.

2. If you need to expand the bandwidth of a single NAT Boundary Firewall Instance, you can operate according to the following steps:

> **Notes:**
> - The adjustment range must be consistent with the Internet bandwidth. If multiple NAT firewalls are used, their bandwidth sum must be less than or equal to that of the Internet boundary.
> - If the target bandwidth exceeds the currently purchased bandwidth specification, you can click scale-out to adjust the Internet edge bandwidth.
> - For minor bandwidth adjustments, there is no need to switch networks. For larger bandwidth adjustments (involving upgrading instance specification gears, for details, see Instance Specifications), the backend needs to reconfigure the network, which may result in a 3-5 second network interruption.

2.1 On the NAT Boundary Switch > Firewall Instance page, find the instance that needs bandwidth adjustment, click **Instance ID** or the **Instance Configuration** on the right.

2.2 On the firewall instance page, click **specification adjustment** in the upper right corner.



2.3 After allocating the bandwidth, click **Confirm** and wait for the backend adjustment to complete.

Instance Specification

NAT firewall instance specification tier table.

Notes:

- NAT instance specifications and NAT rule list quotas are independent of each other, not involving billing logic, and cannot be expanded separately. The only way is to upgrade instance specifications. For every ACL you configure in the console, we will automatically convert it into specific rules according to the issued formula, auto-identify the access source and destination, and deliver them to the designated NAT firewall instance.
- Issue formula: Number of rules issued = Number of source addresses × Number of destination addresses × Number of ports × Number of protocols.
- The NAT instance specification determines the maximum number of ACL rules that each NAT firewall can handle. When the number of ACLs issued is excessive, it may lead to instability in the engine.
- To avoid disrupting your business, we recommend that you optimize rules reasonably based on each instance's specification and the number of rules issued, reduce the proportion of redundant rules, and enhance engine stability.

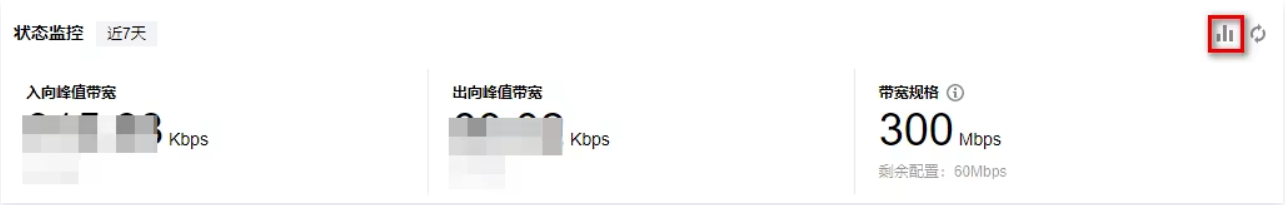
Specification Tiers	Minimum Bandwidth (Mbps)	Maximum Bandwidth/Mbps	Rule Quota (Number)
1	0	299	5,000
2	300	1,300	20,000
3	1,301	4,095	40,000
4	4,096	6,143	60,000

5	6,144	10,239	120,000
6	10,240	102,400	200,000

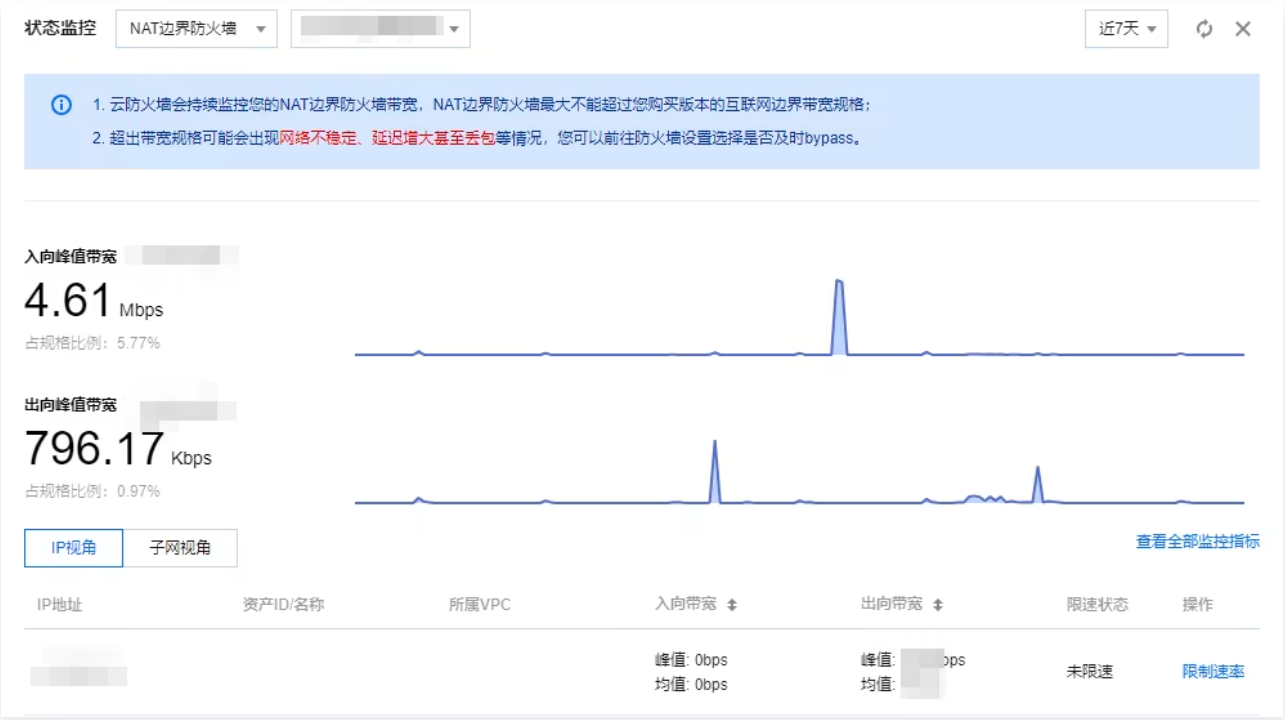
Monitoring Information

On the NAT Boundary Switch page, you can view and monitor bandwidth status based on NAT boundary, sync assets, view network topology, etc.

1. In the upper-right corner of the status monitoring panel, click to enter the firewall status monitoring page.



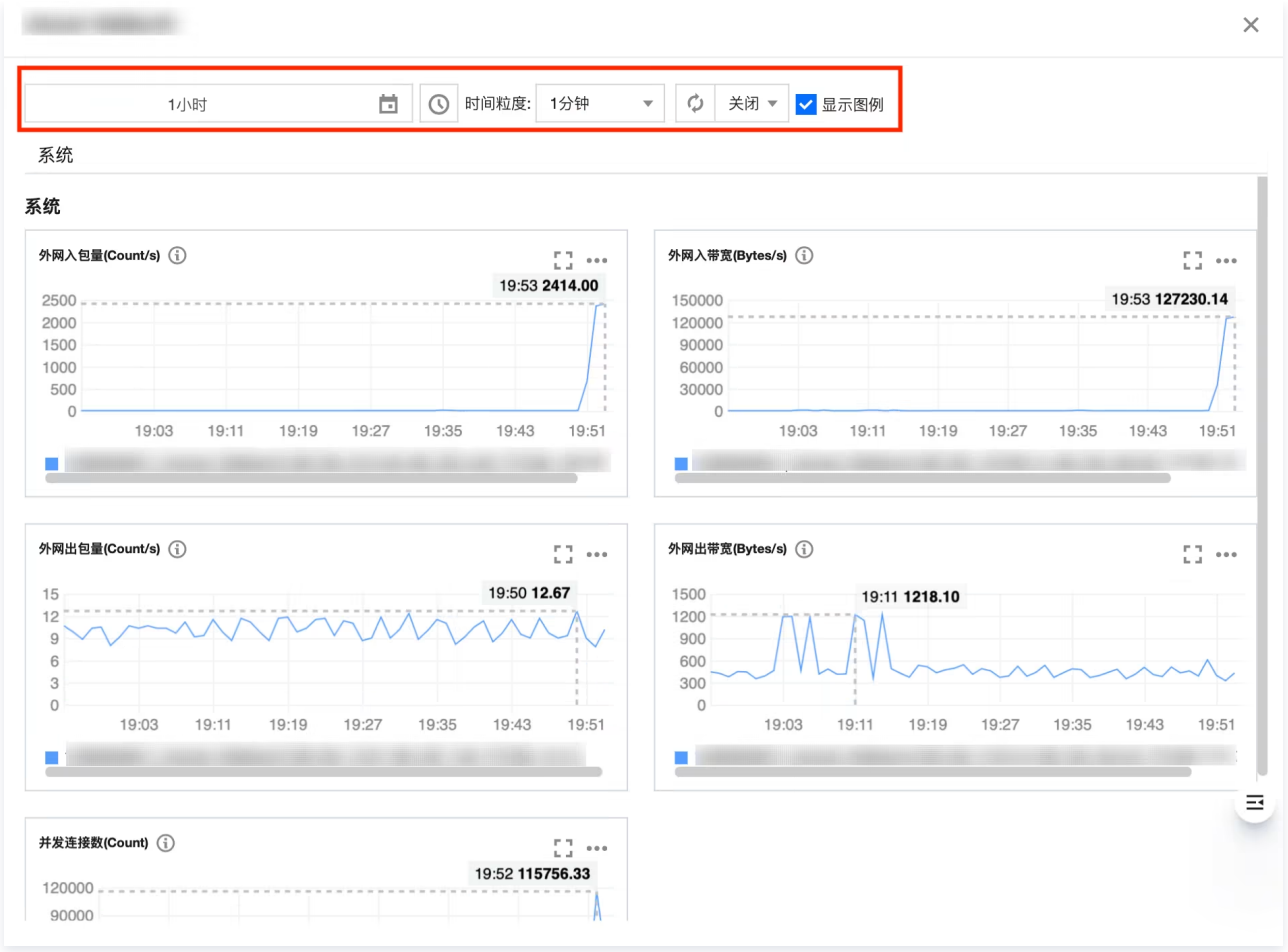
2. On the firewall status monitoring page, you can view and monitor the bandwidth status based on the NAT boundary in real time. This helps prevent network packet loss and fluctuations caused by the NAT boundary firewall bandwidth exceeding the specification, thereby enabling prompt adjustments such as expanding capacity or turning off some switches.



3. On the firewall status monitoring page, you can view the bandwidth status monitoring from the IP perspective or the subnet perspective.
   - IP perspective: Asset information of the IP address, VPC to which the corresponding instance belongs, peak and average values of inbound/outbound bandwidth, rate limiting status, and rate limiting operation.
   - Subnet perspective: Subnet name, IPv4 CIDR address, inbound/outbound peak bandwidth, switch state, view switch operation.

4. Click **View All Monitoring Metrics** to view more monitoring metric data for this instance, including inbound/outbound packet data, etc.; you can also go to Tencent Cloud Observability Platform to view more data content.

5. Settable configuration information such as the time interval for monitoring data, year-on-year/quarter-on-quarter comparison, and refresh time.



Sync Assets

On the NAT Boundary Switch > Firewall Instance Page, click **Synchronize Assets** to proactively invoke backend interfaces to re-read and sync user subnet asset information, avoiding situations where user asset size changes within the backend polling interval but hasn't been synced.

Perform Other Operations on VPC and NAT

Add Access VPC/NAT

- **New mode:**
  1.1 On the NAT Boundary Switch > Firewall Instance page, click **More** > **Access Configuration**, in the dropdown list, click **Add Connected VPC**.

1.2 In the pop-up window for adding a connected VPC, select the required VPC, click **Confirm**, and the configuration will be completed.

> **Notes:**
> - Support VPC ID/name and IPv4 CIDR keyword search.
> - Checkbox: The user's current VPC is selected by default. Selected VPCs cannot be canceled.
> - Click **Add VPC to Connect** to trigger the NAT Edge Firewall Toggle lock for the current region until the reselection is completed. Click **Confirm** to unlock. During the toggle lock period, if another user in the current region requests to enable the switch, a prompt will indicate that another user is reconnecting to the VPC and the switch is locked. Please try again later.

- **Access mode:**

1.1 On the NAT Boundary Switch > Firewall Instance page, click **More** > **Access Configuration**, in the dropdown list, click **Add NAT Connection**.

1.2 In the pop-up window for adding a NAT connection, select the required NAT, click **Confirm**, and the configuration will be completed.

> **Notes:**
> - Support fuzzy keyword search: Support NAT instance ID/name, associated EIP, and VPC ID/name search.

- Checkbox: The NAT Gateway currently connected to the user's NAT firewall instance is selected by default and cannot be canceled.

Re-Select to Access VPC/NAT

- **New mode:**

1.1 On the NAT Boundary Switch > Firewall Instance page, click **More** > **Access Configuration**, in the dropdown list, click **Select Connected VPC Again**.

> **Notes:**
> Disable all subnet switches and DNS traffic toggles under the current firewall instance.

1.2 In the selection of VPCs to connect, you can view the VPCs in the user's current region, select the VPC to connect, click **Confirm**, and the configuration will be completed.

> **Notes:**
> - Support fuzzy keyword search: Support VPC ID/name and IPv4 CIDR keyword search.
> - Checkbox: The current VPC is selected by default. The selected VPC cannot be canceled.

- **Access Mode**

1.1 On the NAT Boundary Switch > Firewall Instance page, click **More** > **Access Configuration**, in the dropdown list, click **Select NAT Connection Again**.

> **Notes:**
> Please first check whether all switches are turned off. Reselect the NAT integration and close all switches (excluding switches that are currently turning off).

1.2 In the selection of NATs to connect, display the NAT instances in the user's current region, and select the NAT to connect.

> **Notes:**
> <Click **Select the NAT to be integrated**, the NAT boundary firewall switch lock in the current region will be triggered until the reselection is complete. Click **Confirm** to unlock it. During the switch lock period, if other users in the current region have a request to turn on the switch, a prompt will indicate that other users are reconnecting to NAT and the switch is locked. Please try again later.</Click>

Terminating an instance.

1. On the NAT Boundary Switch > Firewall Instance page, click **More**, in the dropdown list, click **Destroy Instance**.

> **Notes:**
> - Before terminating the instance, disable all firewall switches.
> - Users may need to autonomously terminate instances due to business changes and can perform the operation on their own through page navigation.
> - After terminating the instance, all configurations of the instance will be deleted, logs will be preserved, and the quota will be returned upon completion. The original route and port forwarding will be automatically restored, the region display status will be updated to show only remaining regions. If no remaining regions are available, the page will return to the initial page for creating instances.

2. In the pop-up confirmation box, click **OK** to delete all configurations of this instance.

Debugging Tool

On the NAT Boundary Switch > **Firewall Instance** page, click **More**, then in the dropdown list, click **Debugging Tool**.

- Enable ByPass: In ByPass mode, all traffic under the current instance will ByPass the firewall, and all firewall configurations will become ineffective. Recommended for debugging. It is expected to take effect within 1 minute after being enabled. After debugging is completed, manually disable the ByPass mode. If you need more help, please submit a ticket.

> **Notes:**
> Enable ByPass mode may have the following effects:
> 1. The route switching process may cause a momentary disconnection for a few seconds.
> 2. Existing long connections will be affected; automatic retry for creating new connections is required.

- Restart instances: We will prioritize restarting the firewall replica. After the restart is complete, we will perform a primary/replica switch and then restart the firewall host. After the host restart is complete, we will perform another primary/replica switch. The entire process is expected to last about 10 minutes. There may be slight network fluctuations. You cannot perform operations or modify firewall configurations. Operate during off-peak business hours.
- Switch primary/replica: The firewall uses a mutual backup solution, where the working instance is the primary instance; you can choose whether to switch to the standby firewall instance. The switching process is expected to take 2–10 seconds, and there may be slight network fluctuations.
- Probe settings: Set the public network probe address.

  The firewall uses periodic checks to detect the liveness status of the NAT boundary firewall bound EIP, therefore needs you to specify a reachable public network IP address for the checks.
  b. You can add up to 5 IP addresses at the same time. When the set bound egress IP becomes unreachable, the firewall will enable high availability mechanism to switch to a standby EIP.

- Enable transparent mode: In transparent mode, the current firewall instance only forwards network traffic, and related access control features or intrusion prevention features will not take effect. Recommended for debugging. It will take effect within 1 minute after enabling. Manually disable transparent mode after debugging is completed. If you need more help, submit a ticket.
- Migrate availability zones: You can choose to migrate the current host or standby host to another availability zone. The migration process is expected to last 2–5 minutes, and operations such as primary/replica switch may occur. Network fluctuations may happen. Operate during off-peak business hours.

Related Information

- If you need to configure the corresponding firewall switch for your public IP addresses and associated cloud assets, see Internet Boundary Firewall Switch for operations.
- If you need to automatically detect VPC information and interconnections, and establish a CFW switch between each pair of interconnected VPCs, see inter-VPC firewall switch for operation.
- Hosts with bound public IPs that need direct access through public IP addresses, please see Adjusting the Priority of NAT Gateway and EIP document.
- For questions about NAT boundary firewall, please refer to the NAT Boundary Firewall document.

VPC Boundary Firewall

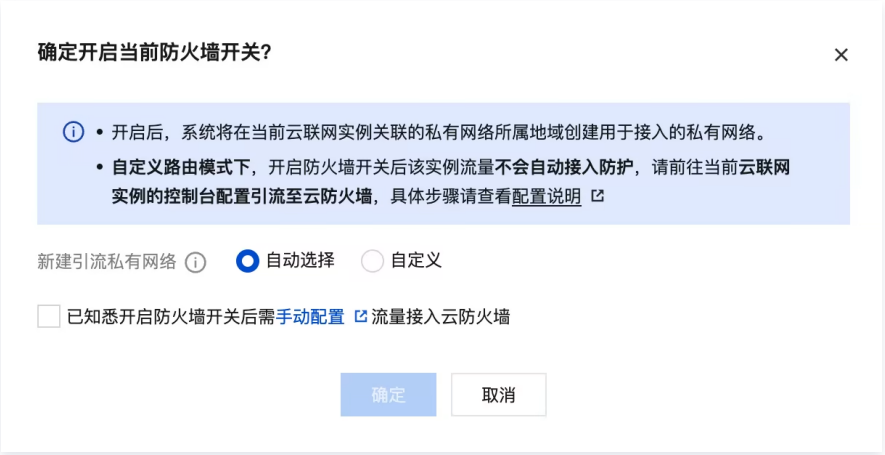
Last updated: 2025-05-21 09:57:04

The Cloud Firewall provides the VPC boundary switch feature in cluster mode. On the VPC boundary switch page, it can automatically detect your Cloud Connect Network instances and configure the corresponding firewall switches for you.
You can log in to the CFW console, select **Firewall Switch** > **Protected Target** > **VPC Boundary** in the left navigation bar, and perform the configuration of the VPC boundary firewall in cluster mode.

> **Notes:**
> The VPC border firewall switch currently **only supports custom routing access mode**. After the firewall switch is turned on, the instance traffic will not automatically access the Cloud Connect Network instance traffic. Please go to the console configuration of the current Cloud Connect Network instance to drain to the Cloud Firewall. For details, see the Custom Routing Configuration Guide. After successful configuration, the traffic of the current Cloud Connect Network instance will pass through the firewall. At that time, the access control rules and intrusion prevention functions will take effect, and traffic logs will be generated.

Firewall Switch

1. Log in to the CFW console. In the left sidebar, select **Firewall Switch** > **Protected Target** > **VPC Boundary**.
2. On the VPC boundary toggle page, find the CCN instance that requires protection in the protected target column.
3. Click in the firewall switch column and select the new traffic diversion private network method.



4. After confirming enablement, the cloud firewall will create a private network for integration in the region where the private network associated with the corresponding CCN instance is located.
5. When the access mode of the current CCN instance is "custom routing", after enabling the firewall toggle, you need to go to the console of the current CCN instance to configure traffic diversion to the CFW. For specific operations, see custom routing configuration guide.

Firewall Status Monitoring

VPC boundary firewall status monitoring supports statistics of the bandwidth of each CCN instance.
1. In the upper-right corner of the bandwidth configuration panel, click to view status monitoring.

2. In the Status Monitoring – VPC Boundary Firewall interface , you can filter bandwidth monitoring dimensions based on Cloud Connect Network (CCN) instance names or select switch to view connection counts . Modify statistical dimensions by choosing a time range . You can observe monitoring curves and access monitoring data from multiple perspectives .

> **Notes:**
> The minimum statistical granularity varies for different time ranges and may result in discrepancies with actual peak values. It is advisable to refer to the data from Tencent Cloud observability platform or the statistics of specific protection units.

DNS Firewall Toggle

Last updated: 2025-05-20 10:33:35

The DNS firewall works in conjunction with Private DNS to provide real-time control, risk alerts, interception, custom policies, and full traffic audit for VPC outbound domain name access. No DNS replacement or proxy deployment is needed; it's out-of-the-box usage.

> **Notes:**
> Feature is currently in beta test. The current version is only supported in partial regions. If you need to apply, please submit a ticket to contact us. The end time of the beta test will be subject to subsequent announcements.

Preparation for Using DNS Firewall

1. The DNS firewall must use the default DNS addresses provided by Private DNS: 183.60.83.19 and 183.60.82.98. If your DNS address is not the above, the DNS firewall cannot be used. It is recommended to use NAT edge firewall for DNS traffic protection integration.
2. The DNS firewall only protects outbound domain name access traffic of VPCs. It does not involve inbound scenarios or Public DNS resolution. Please confirm compliance with business requirement scenarios.

Enable the DNS Firewall Toggle

Log in to the CFW console, in the left navigation bar, select **Firewall Switch** > **DNS Switch** to enter the DNS Firewall Switch page. In the switch list below, you can see the DNS switch list based on your VPC assets. Select the VPC asset you want to enable, click the switch on the right to turn it on. Enabling has no impact on the network.

View DNS Request Frequency Monitoring

1. In the upper-right corner of the status monitoring panel, click the icon.

2. In a new window, you can view the request frequency curve of a specified VPC or specific monitoring metrics of partial IPs.

Custom Routing Configuration Guide

Last updated: 2025-05-21 09:57:32

Integrating a CCN Instance with a Cloud Firewall

Step 1: Create a custom routing pattern instance.

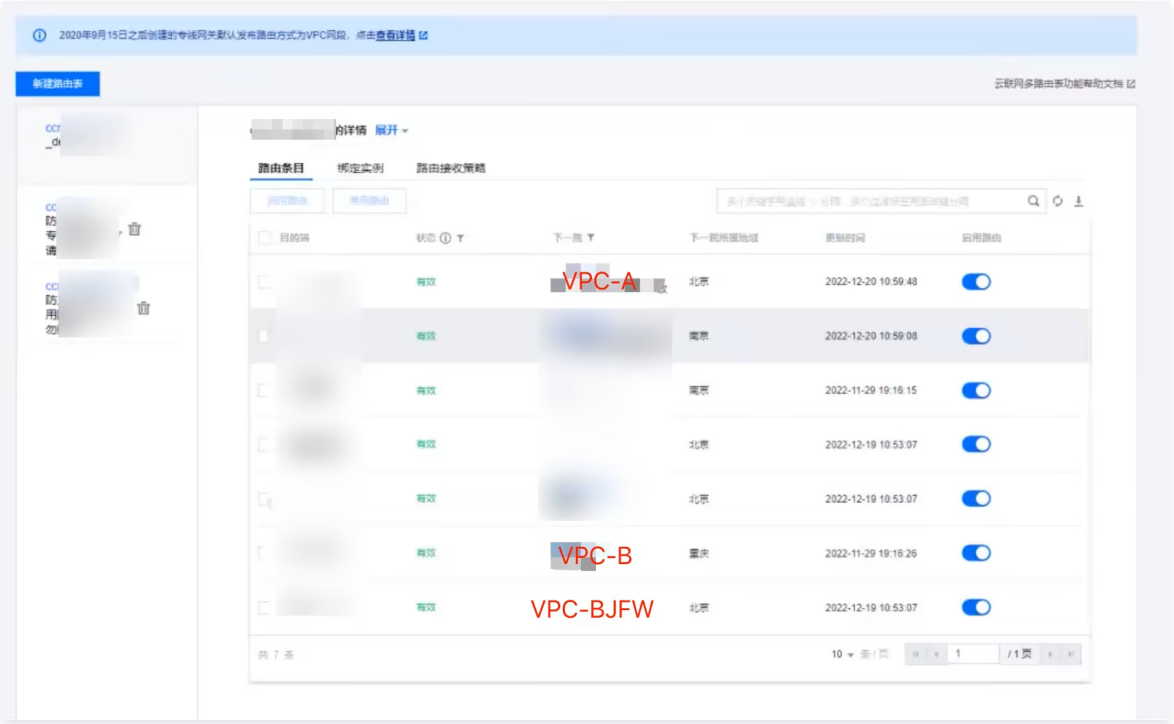
Refer to VPC Boundary Firewall, toggle on the firewall switch of the target CCN instance, where the integration mode selects custom routing.

Step 2: Configure traffic attraction routing.

The current operation aims to divert the user's business that requires protection and the CCN instance to the cloud firewall through the firewall gateway.

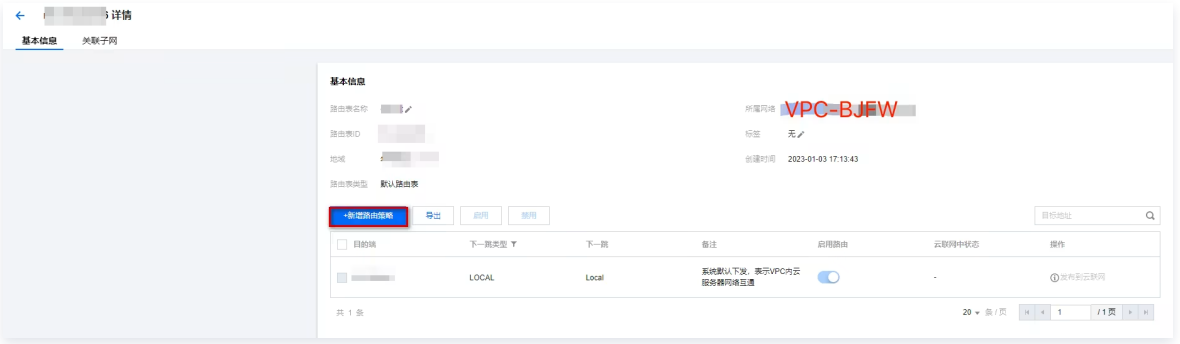
1. Go to the console of the CCN instance selected when opening the VPC boundary firewall, and view the details of the CCN instance associated with the custom routing mode.
2. Confirm that the firewall traffic diversion VPC and related routing table have been created. If not, wait for instance creation to complete or submit a ticket to contact us.
3. View the default route table page, and confirm the business VPC and firewall traffic diversion VPC that need to be connected.

> **Notes:**
> This document uses the following examples to demonstrate how to integrate: Beijing business VPC: VPC-A; Chongqing business VPC: VPC-B; Beijing regional firewall traffic diversion VPC: VPC-BJFW.

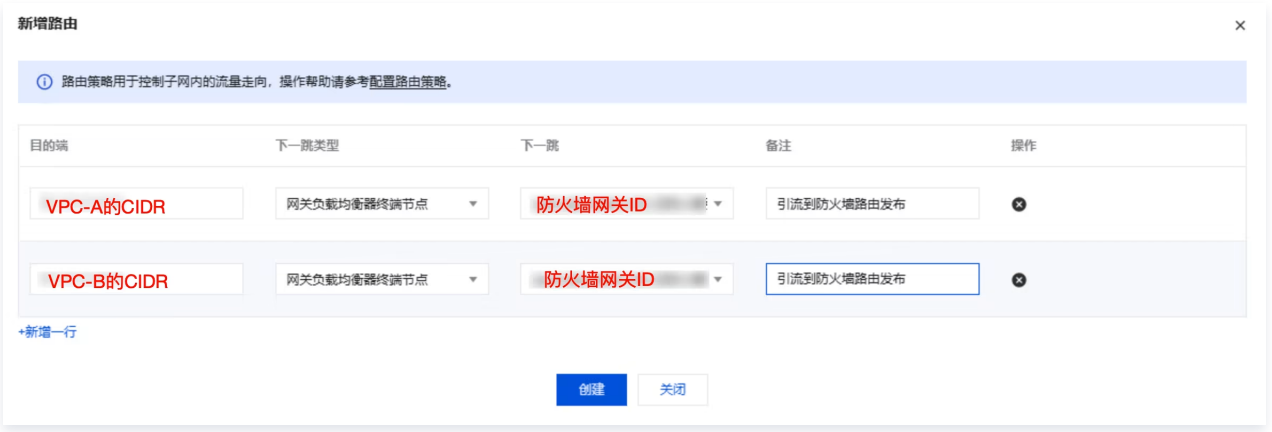


4. Go to the **Virtual Private Cloud** > Route Table page, select the firewall traffic diversion VPC that needs to be connected, and you can see the route tables including "Firewall VPC Dedicated Route Table_Do Not Delete or Modify" and "default". Select the "default" route table and edit the routing strategy.

5. Click **Add Routing Policy** to divert the next hop of the business VPC to the firewall.



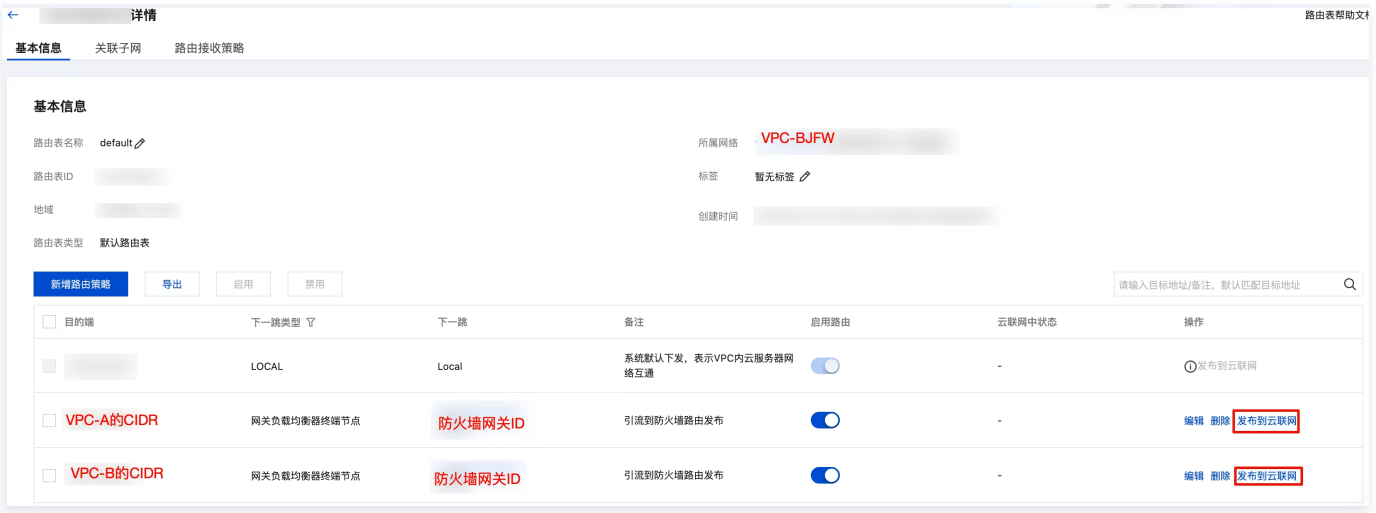
Enter the CIDR of the business VPC as the destination. Select **gateway load balancer terminal node** for the next hop type. Select **firewall gateway ID** for the next hop. The remark can be filled freely.



> **Notes:**
> If there is a prompt indicating "specified CIDR forming ECMP", it is necessary to first disable the related service routes in the default routing table.

6. Add the new route and publish it to the CCN. For details, see Manage Routing Policies. After publication, you can see the specified routing policy in the default route table of the corresponding CCN.

> **Notes:**
> The original route entries will become invalid due to the conflict between the new routing strategy and the original routing strategy, which can be ignored.



Step 3: Create a Route Table to Connect Business VPCs

The purpose of the current operation is to integrate the firewall network with the user's business network to achieve mutual network access.

1. On the CCN page, create a route table for each business VPC diverting traffic to the firewall.

2. Adjust the route reception policy. In the **route reception policy** of the dedicated route table of each VPC, click **add network instance** to add the VPC instance to which the route table itself belongs and the interconnected VPC instances to the route table.

> **Notes:**
> Add a network instance, which must be divided into two steps: first, add your own VPC instance and the VPC instance that does not pass through firewall protection; then, add the VPC instance dedicated for firewall traffic diversion.

For example: Assume VPC-C is a business VPC that does not need to be connected to a firewall instance. In the routing table of VPC-A, first add two instances: VPC-A and VPC-C. Once added successfully, repeat the above operation to add one instance: VPC-BJFW.

3. Check whether the route entries in the route tables of each VPC meet expectations.
4. Bind a network instance. For the **bind instance** of the dedicated route table of each VPC, click **Bind Network Instance** to bind the dedicated route table of each VPC to its corresponding VPC instance. After the operation is completed, traffic will be diverted to the firewall.

> **Notes:**
> Please confirm the route is correct before binding the route table. It will take effect immediately after binding.

Step 4: Verify If the Firewall Is Working Properly

1. Refer to log audit to check whether there are traffic logs.
2. See Log Audit to check whether the intrusion prevention is working properly.
3. Configure private network rules and check whether they are hit normally.

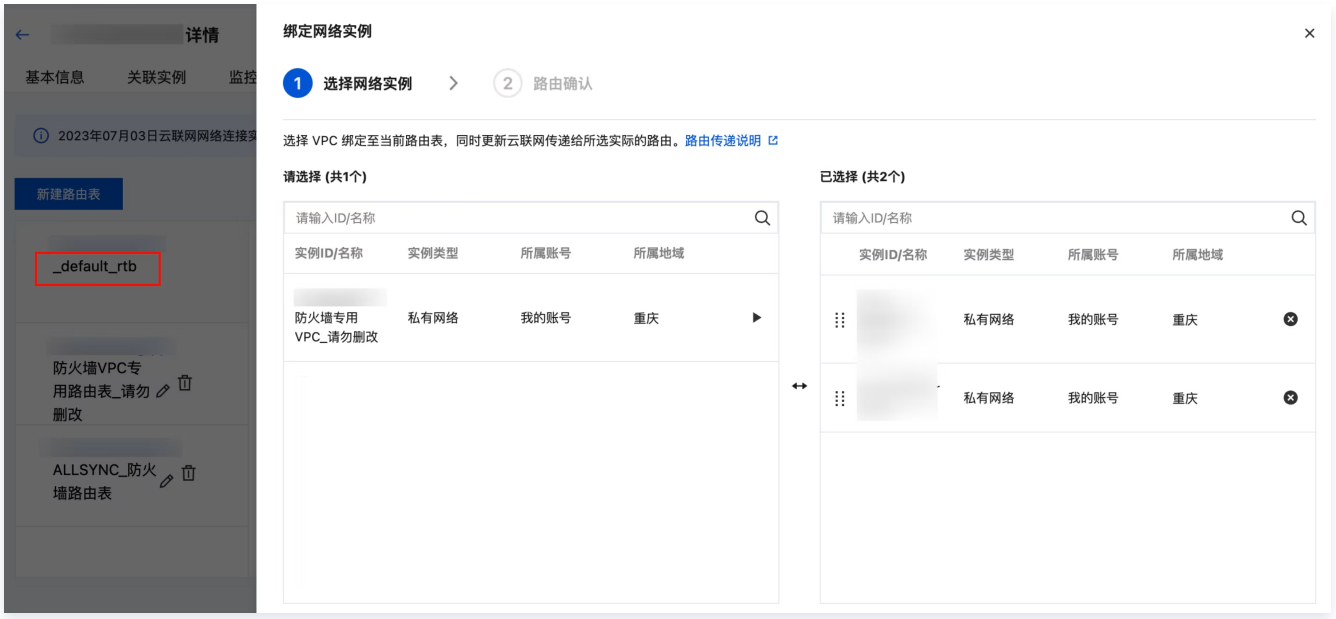
The firewall is now functioning properly. If your network structure is complex or involves a dedicated line scenario, submit a ticket to consult detailed routing configuration solutions. If you have further questions, feel free to submit a ticket to contact us.

Canceling the Integration of a CCN Instance with a Cloud Firewall

> **Notes:**
> Please confirm the CCN instance has been disconnected from the CFW before turning off the corresponding VPC boundary firewall switch; otherwise, it may cause a network interruption.

1. Go to the console of the CCN instance where the VPC boundary firewall needs to be disabled, and view the details of the CCN instance associated with the protection object in the custom routing mode.
2. Bind all network instances, except for the VPC dedicated to the firewall, to the routing table used before integrating with the cloud firewall.
   2.1 Select the route table used before integrating with the cloud firewall, typically the _default_rtb table.

2.2 Select all instances except those dedicated to firewalls.



2.3 Confirm the route, complete the cancellation of integrating the cloud firewall.

3. Check the network status. If it is normal, turn off the firewall switch corresponding to the current CCN instance in the CFW console.

Upgrading the Firewall Engine

Last updated: 2025-05-20 10:42:50

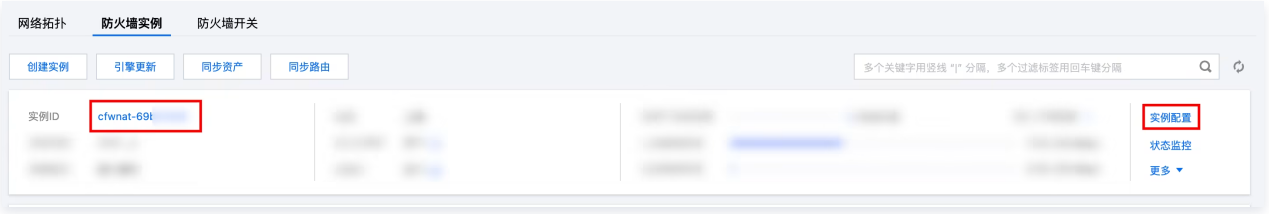
The NAT boundary firewall and inter-VPC firewall are deployed in privatization mode, with their engines exclusively for tenants. Therefore, users are advised to manually update the engines. The following are the upgrade operation guidelines.

Query Upgradeable Firewall Instances

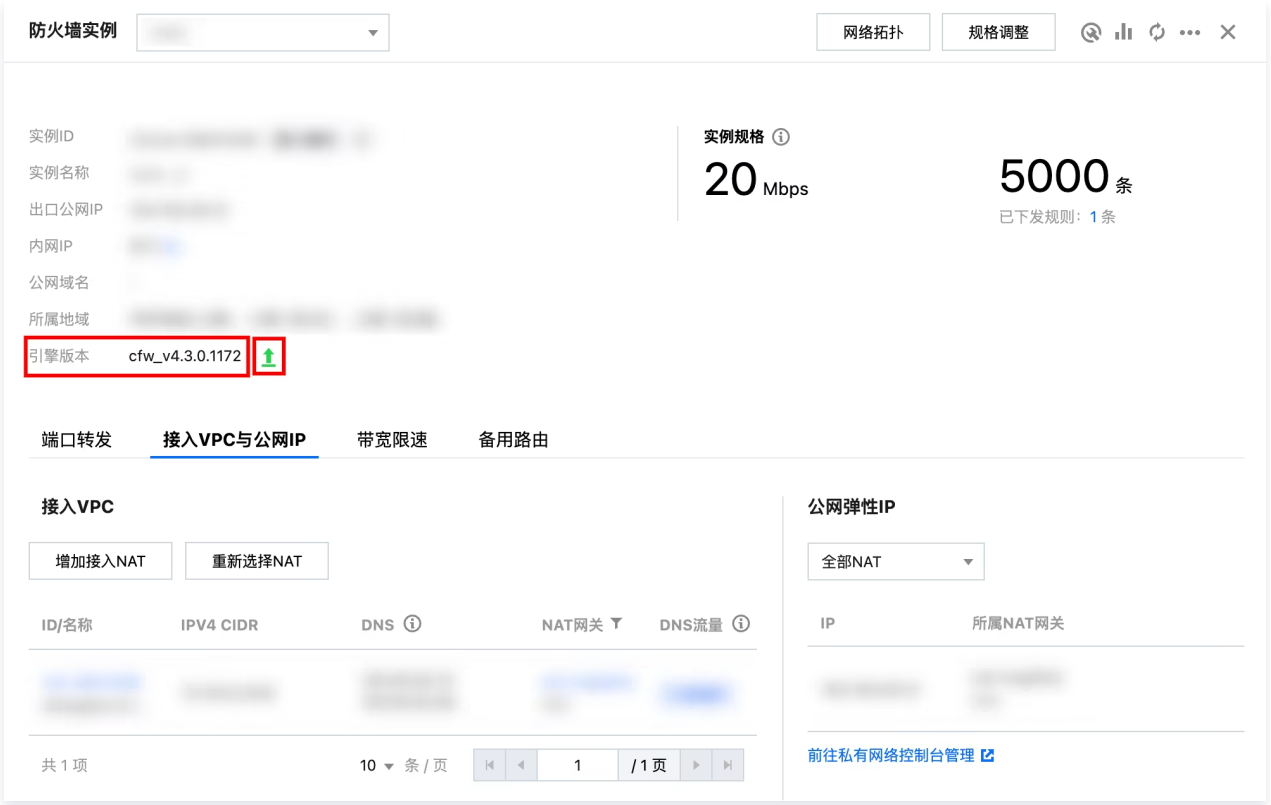
1. Log in to the CFW console. In the left sidebar, select **Firewall Switch** > **NAT Boundary Switch/Inter-VPC Switch**.
2. On the firewall instance page, click **Engine Update** to view the latest version engine and upgradeable instances.

3. We will choose the latest stable version by default. If an upgradable firewall instance exists, the upgrade options below will be selectable.

4. View the engine version and upgradability of a specific instance.
   Click the corresponding firewall instance ID or instance configuration to open the firewall instance details page.



5. Compare the current engine version with the version list provided by engine update dynamics to check if it is upgradable. If the engine version is upgradable, a ⬆ flag will appear on the right side.



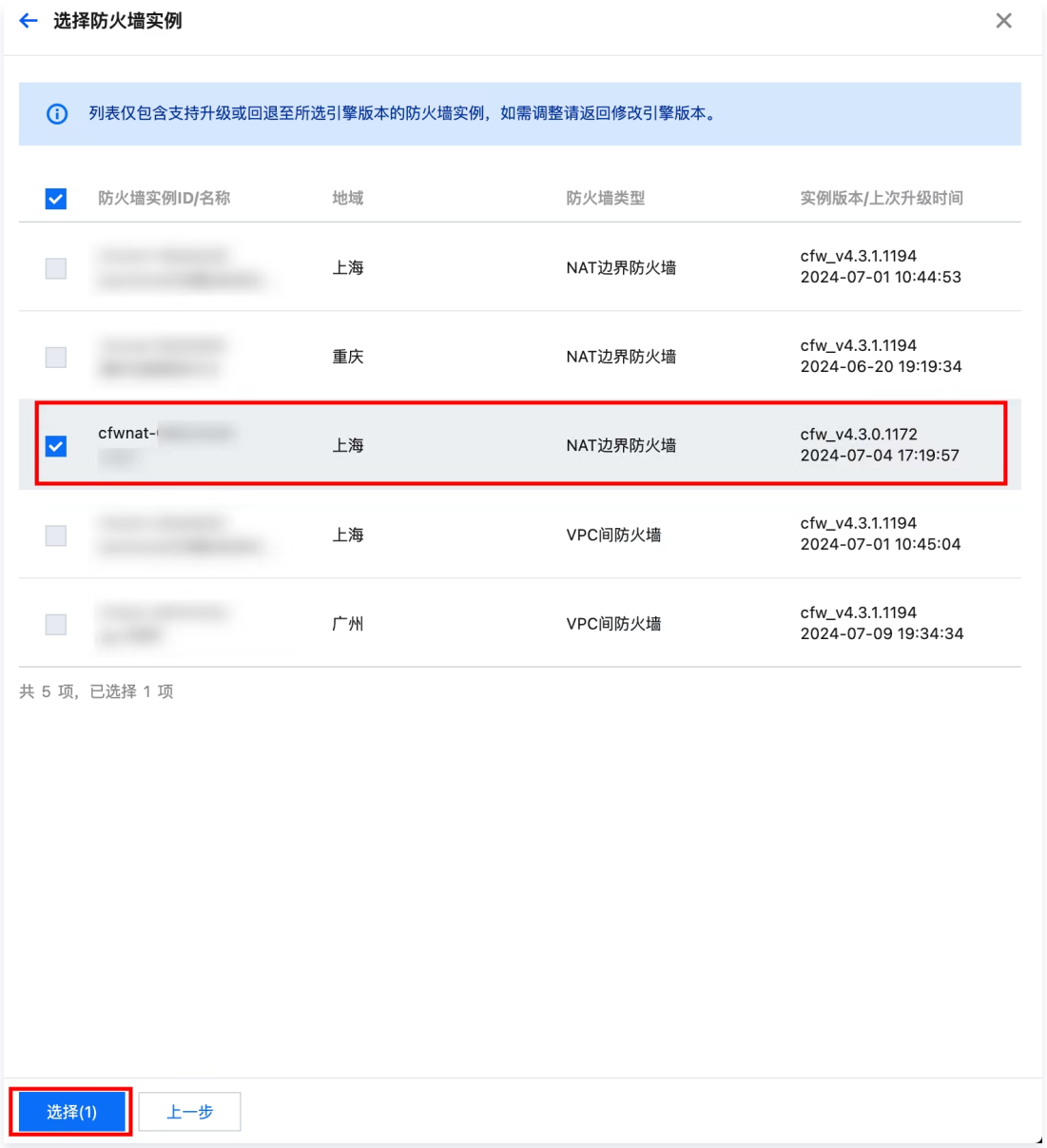
Upgrading the Firewall Engine Version

1. Refer to the above section to enter the engine upgrade page and select the required engine version at the illustrated position.

> **Notes:**
> The preview edition is the latest engine version, containing the latest features and defect fixes; the stable version is a version that has undergone long-term stability verification on the live network, generally lagging behind the preview edition by one major version.
> We recommend you update the engine to the latest stable version promptly. For details, see Engine Update Dynamics.

2. Select the engine instance that requires upgrading.
   - One-click upgrade: After selecting this option, it will automatically identify all firewall engine instances in all regions with the current version and upgrade them to the selected version.
   - Custom upgrade: You can customize the selection of instances for upgrading. Click **Select Instance** to enter the instance selection interface.

3. On the instance selection page, select the instance that needs to be upgraded and click **Select**.



4. Click **Confirm Upgrade** to initiate the upgrade task.

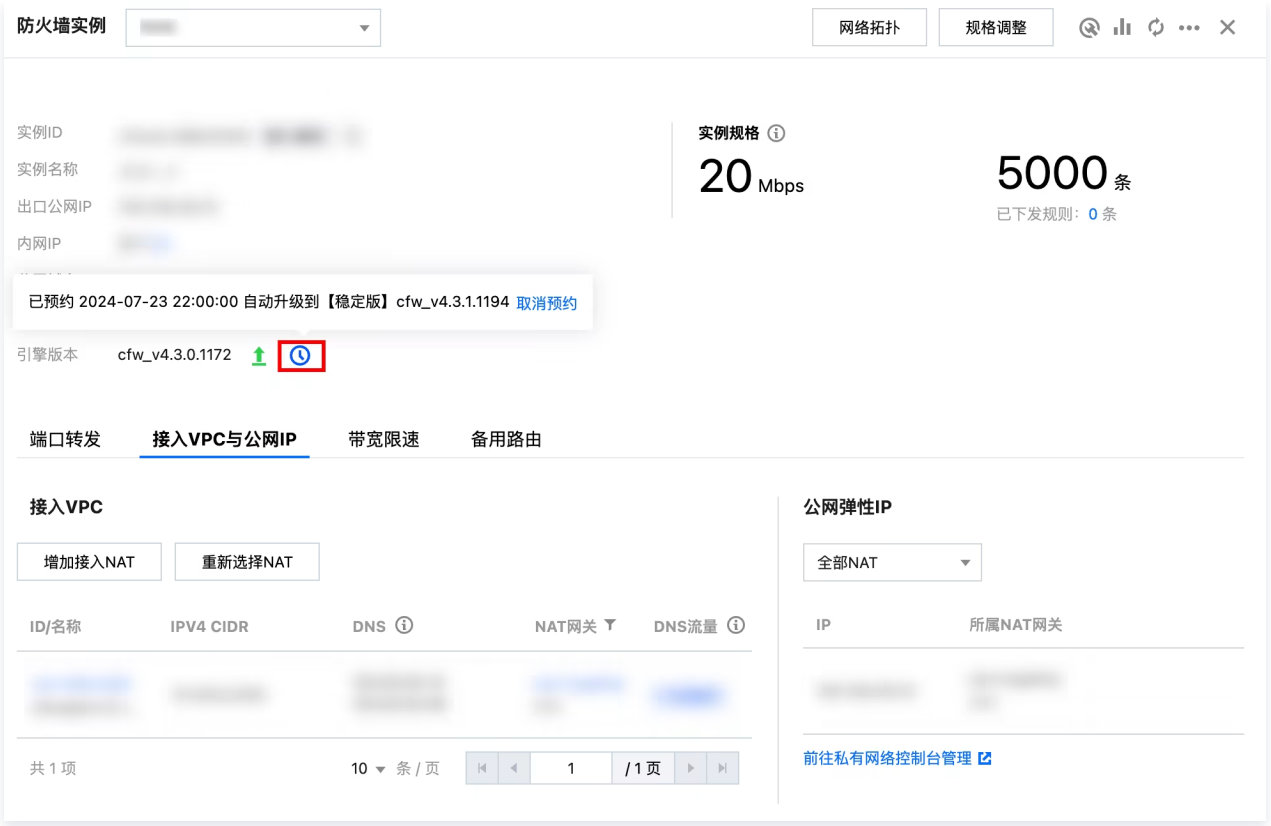
> **Notes:**
> - The upgrade process may take several minutes, during which you are unable to operate the firewall switch and rules; after the upgrade is completed, the switch and rule statuses will be automatically restored.
> - The upgrade process will first upgrade the backup host and then the primary host. During the upgrade, a primary-backup switch operation will be triggered, and the network may experience slight fluctuations, but the business will not be disconnected. It is advisable to perform the upgrade operation during business off-peak hours.

Appointment Time Upgrade

1. After completing steps 1 and 2 above, click **Select Appointment Time** at the illustrated position.

2. Confirm the upgrade task status.

   Access the corresponding firewall instance page. You can see the scheduled upgrade task at the illustrated engine version. You can cancel this reservation by clicking **Cancel Reservation** or re-executing the engine upgrade operation.



Migrating Firewall Engine Region

Last updated: 2025-05-20 10:43:07

1. Log in to the CFW console, and in the left sidebar, select the **firewall switch**.
2. Based on the instance type, switch to **NAT Boundary Switch or Inter-VPC toggle**.

3. In the firewall instance tab, select the engine instance that requires migrating availability zones, click **More** > **Debugging Tool** > **Migrate Availability Zone**.

4. In the migrate availability zone pop-up window, select an availability zone different from the **host** for the **standby host**, click **Confirm**, and complete the operation.

> **Notes:**
> During the migration of hosts to availability zones, an active/standby switch may occur, leading to network jitter. It is advisable to perform host migration during non-business time; the migration of standby hosts will not generate any impact.

VPC Boundary Firewall Switch (Primary/Secondary Mode)
Overview

Last updated: 2025-05-28 10:00:29

Application Scenario

The Cloud Firewall switch provides the firewall switch feature between VPCs. It establishes a firewall to carry the access traffic between different VPCs and provides access control rules and log audit systems.
The current version of the inter-VPC firewall supports protection for Direct Connect gateways. Based on firewall instances, it supports the CCN multi-routing Cloud Connect Network mode. Direct Connect gateways establish connections with cloud-based VPC assets through Cloud Connect Network. Therefore, the inter-VPC firewall supports detecting this traffic.
This document will introduce how to create a firewall, view bandwidth usage and specification information, and view network topology and firewall switches on the VPC switch page.

Architecture Overview

Before using this feature, you need to have a general understanding of the composition of the inter-VPC firewall.
An inter-VPC firewall consists of multiple firewall instances, each responsible for connecting to a different VPC and establishing network connections between the VPCs and the firewall.

The essence of the inter-VPC firewall is to redirect traffic to the firewall by modifying the VPC's routing. Whether firewall instances can communicate with each other depends on whether there **are reachable routing paths between the VPCs they are connected to**. The firewall does not establish connections within the underlying network. The firewall can establish network connections by modifying the next hop in the route table of the Virtual Private Cloud or the multi-route table of the Cloud Connect Network.

Explanation of Abnormal Scenarios for Inter-VPC Firewall

- When the inter-VPC firewall switch is turned on or off, the backend system automatically modifies your routing policies, causing **a momentary network disconnection in a very short time**. To avoid affecting your business, please arrange the operation time of the inter-VPC firewall switch reasonably. If batch or frequent switch operations are required, it is advisable to perform them late at night when business traffic is light.

  > **Notes:**
  > The switch of the Internet edge firewall does not have similar issues.

- The inter-VPC firewall switch is built on the peering connection (or CCN) between VPCs. If you update (or delete) the configuration of the peering connection (or CCN), the firewall switch will also automatically change (or delete). To avoid affecting your business, CFW will only immediately execute changes (or deletions) for switches in the Off status.

  > **Notes:**
  > If your on-cloud assets are modified (or deleted), the internet boundary firewall switch will automatically sync in a short time frame (about 5 minutes).

- If there is no routing enabled between VPCs, the firewall switch cannot be turned on.

  > **Notes:**

> - If you need to configure a peer connection route, see Configure the route pointing to the peer connection.
> - If needed, see Route Overview.

- When the CFW switch is enabled, **manually changing the corresponding VPC routing table in the VPC console is a high-risk operation**. Since CFW cannot synchronize routing changes, it may cause the firewall to fail and result in network disconnection.
- When the Cloud Firewall switch is disabled, you can switch other peering connection (or CCN) routes between VPCs as needed. However, **do not enable routes marked with the note "Firewall"**, as this will cause network connection interruptions and firewall switch failures.

Related Information

- If you need to configure the corresponding firewall switch for your public IP addresses and associated cloud assets, please refer to Internet Boundary Firewall Switch for operations.
- To perform traffic control and security protection for internal network assets or perform network traffic forwarding based on SNAT and DNAT, please refer to NAT Edge Firewall Toggle for operations.
- If you encounter inter-VPC firewall related issues, please refer to the inter-VPC firewall document.

Creating a VPC Boundary Firewall (Primary/Secondary Mode)

Last updated: 2025-05-28 10:02:04

Virtual Private Cloud Mode

1. Log in to the CFW console, in the left navigation bar, select **firewall switch** > **Inter-VPC toggle**.
2. On the Inter-VPC switch page, click **firewall instance**, enter the firewall instance page, and click **create firewall**.

3. In the create inter-VPC firewall pop-up window, enter the instance name, select **Virtual Private Cloud Mode**, and click **Next**.

Parameter description:

- Instance name: The name you customize when creating a firewall instance.
- mode
  - Virtual Private Cloud mode: Select the Virtual Private Cloud VPC to connect to the firewall and implement route redirection by modifying the route table of the Virtual Private Cloud.
  - Cloud Connect Network mode: Select the Cloud Connect Network CCN to integrate with the firewall (multi-route table mode is required), and implement route redirection by changing the Cloud Connect Network route table.
  - SASE mode: The feature is in limited-time beta test. If you need to use it, please submit a ticket.
  - VPC mode (CDC): Consistent with the VPC mode, available only in CDC environment.

4. Fill in the firewall instance name and region, configure disaster recovery information, set the firewall instance bandwidth specification and access network, click **Next**. If the quantity of instances does not meet needs, click on the right ⊕ to create firewall instances.

Parameter description:

- Region: The region to which the protected VPC belongs.
- Remote Disaster Recovery: The inter-VPC firewall supports remote disaster recovery, which can be enabled by checking the box.
- Availability Zone: Select an appropriate availability zone based on your needs.
- Instance bandwidth: Currently, a single instance has a minimum of 1 Gbps and a maximum of 20 Gbps (the console allows configuration with a maximum support of 5 Gbps; for exceeding this, submit a ticket for assessment). Scaling-out is supported. If the maximum bandwidth is not satisfied, multiple firewall instances can be created for traffic diversion. However, note that each firewall instance has its own throughput limit. For multiple firewall instances, ensure that a single instance is within its throughput limit.
- Instance connection: Click **Access Network**, select the required VPC based on the region of the VPC to be connected, and click **Confirm**.

> ⚠ **Notes:**
> - Each VPC can only connect to one instance.
> - The firewall cannot establish connections within the underlying network. Before connecting the network, ensure that peering links or Cloud Connect Networks have been created between the VPCs. If there is no established connection between the VPCs, the connection will not be effective, and the firewall switch will not be available.
> - Each firewall instance can only connect to VPCs within the same region. Each instance can connect to a maximum of 10 VPCs and supports the creation of multiple firewall instances within the same region. It is recommended to plan the VPCs that need to be connected according to their regions in advance. Then, create the firewall instances and proceed with network connections.

5. Configure the traffic redirection subnet, firewall VPC, and routing mode. Once confirmed, click **Create**.

> **Notes:**
> Complete the configuration. The creation process will take several minutes. Wait patiently.

Parameter Name	Description

Traffic Redirection Subnet Configuration	The Cloud Firewall will create subnets of a /24 IP range in the VPC you connect to, which will be used to redirect traffic to the firewall. You can choose different methods for creating this subnet. The traffic redirection subnet cannot be modified after the firewall is created. • Preferred Own IP Range: The Cloud Firewall will automatically select an available subnet range within the chosen VPC. If there are no subnet quotas available within the VPC, we will use the expansion IP range of the selected VPC. • Prefer Extended IP Range: The Cloud Firewall prioritizes using available reserved extended IP ranges within the VPC. In this mode, it does not occupy the subnet quota of the selected VPC. Among them, an extended IP range refers to a secondary IP range in a private network. For more information, see Private Network – Edit IPv4 CIDR. • Custom: You can customize the subnet range for the firewall, ensuring it is a /24 IP range. The custom IP range must belong to the current VPC's CIDR, such as 192.168.0.0/24.
Firewall VPC	It is used to establish network communication between firewall instances. You need to create a new firewall-specific VPC in each region of the selected VPC. • Automatic Selection: The firewall will automatically create a /20 IP range VPC that does not conflict with the connected VPC. • Custom: Enter a /20 VPC that does not conflict with the planned network, such as 192.168.1.0/20.
routing mode	The traffic redirection scheme for the firewall switch. Different methods of network interconnection determine the mode of the firewall switch and routing redirection. It is recommended to choose based on your business network model. • Single-Point Interconnection: Suitable for a small quantity of VPCs with a simple network topology. The switch mode is VPC-to-VPC, and in this mode, a firewall switch will be generated for each reachable path between the VPCs. • Multi-Point Interconnection: Suitable for a larger quantity of VPCs with a simple network topology, such as a star network topology. The switch mode is single VPC, and in this mode, access between VPCs will be controlled by two switches. • Full Interconnection: Suitable for a large quantity of VPCs with a complex network topology, such as a mesh network topology. The switch mode is all VPCs, and in this mode, there will be only one firewall switch used to control the routing of all VPCs. • Custom routing: You can refer to the custom routing configuration guide. After completing the creation of the firewall, you can self-configure the routing. In this mode, there will be no firewall switch. Note: When selecting multiple regions, only custom routing is supported. Please refer to the console to verify the availability of specific routing modes.

CCN Mode

> ⚠ **Notes:**
> Starting from July 1, 2023, the CCN service will charge for network instances and inbound traffic processing. The CFW requires creating a dedicated firewall VPC in your integrated CCN instance for traffic diversion, which may incur certain fees. For details, see CCN Commercialization Announcement.

1. Log in to the CFW console, in the left navigation bar, select **firewall switch** > **Inter-VPC toggle**.
2. On the VPC switch page, click **firewall instance**, enter the firewall instance page, and click **create firewall**.

3. In the create inter-VPC firewall pop-up window, enter the instance name, select **CCN Mode**, and click **Next**.

4. Click **Select**, choose the CCN instance to join the VPC firewall according to the prompts, and click **Confirm**.

> **Notes:**
> - The CCN instance needs to support multi-route table mode. If this requirement is not met, please contact the CCN to enable the multi-route table feature.
> - CCN mode supports creating an inter-VPC firewall in a specified region.
> - CCN mode: A firewall can only bind to one CCN instance.

5. After selecting a CCN instance, the available regions will be automatically generated based on the VPCs connected to the CCN. If you check a region, a firewall instance will be created in the selected region. You can configure the firewall instance name, whether cross-region disaster recovery is required, and the instance bandwidth specification, then click **Next**.

Parameter description:

- Region: The region to which the protected VPC belongs.

> **Notes:**
> - If only one region is selected for deploying a firewall instance, all inter-VPC traffic with the firewall toggle enabled will pass through the firewall instance in that region. Suitable for business networks with a star topology structure.
> - If all regions are selected for deploying firewall instances, the inter-VPC traffic with the firewall toggle enabled will pass through the firewall instance in the local region. This is suitable for business networks with a mesh topology

structure.
- After selecting multiple regions, only custom routing is supported.

- Remote Disaster Recovery: The inter-VPC firewall supports remote disaster recovery, which can be enabled by checking the box.
- Availability Zone: Select an appropriate availability zone based on your needs.
- Instance bandwidth: Currently, a single instance supports a minimum of 1 Gbps and a maximum of 20 Gbps (console allows configuration with a maximum support of 5 Gbps; for exceeding limits, submit a ticket for evaluation). Supports scale-out. If the maximum bandwidth is insufficient, create multiple firewall instances to divert traffic.

> **Notes:**
> Each firewall instance has its own throughput limit. For multiple firewall instances, please confirm that the single instance is within the throughput limit.

6. Configure the new traffic redirection private network and routing mode. Once confirmed, click **Create**.

> **Notes:**
> Complete the configuration. The creation process will take several minutes. Wait patiently.

Parameter Name	Description
Create a traffic redirection private network	The cloud firewall will create a private network in the 20 network segment within your selected CCN instance to redirect traffic to the firewall. You can choose different ways to create the private network. • Automatic selection: The CFW will automatically detect idle /20 VPC IP ranges for traffic diversion. • Custom: You can customize the VPC IP range for the firewall, ensuring it is a /20 IP range. For example, 192.168.1.0/20. Starting from July 1, 2023, the CCN service will charge for network instances and inbound traffic processing. The CFW requires you to create a dedicated firewall VPC in your connected CCN instance for traffic diversion, which may incur certain fees. For details, see CCN Commercialization Announcement.
Routing Mode	The traffic redirection scheme for the firewall switch. Different methods of network interconnection determine the mode of the firewall switch and routing redirection. It is recommended to choose based on your business network model. • Single-Point Interconnection: Suitable for a small quantity of VPCs with a simple network topology. The switch mode is VPC-to-VPC, and in this mode, a firewall switch will be generated for each reachable path between the VPCs. • Multi-Point Interconnection: Suitable for a larger quantity of VPCs with a simple network topology, such as a star network topology. The switch mode is single VPC, and in this mode, access between VPCs will be controlled by two switches.

- Full Interconnection: Suitable for a large quantity of VPCs with a complex network topology, such as a mesh network topology. The switch mode is all VPCs, and in this mode, there will be only one firewall switch used to control the routing of all VPCs.
- Custom Routing: You can refer to the Custom Routing Configuration Guide. After completing the creation of the firewall, you can manually configure the routing. In this mode, there will be no firewall switch.

Note: When selecting multiple regions, only custom routing is supported. Please refer to the console to verify the availability of specific routing modes.

Instance Specification

Instance specification tier table for VCP inter-firewall.

Notes:

- The instance specifications of the inter-VPC firewall and the quota of the intranet rule list are independent of each other, not involving billing logic, and cannot be expanded separately. You can only achieve this by upgrading the instance specifications. For every ACL you configure in the console, we will automatically convert it into specific rules according to the issued formula, automatically identify the access source and access destination, and deliver it to the specified inter-VPC firewall instance.
- Issued formula: Number of rules issued = Number of source addresses × Number of destination addresses × Number of ports × Number of protocols.
- The specification of the inter-VPC firewall instance determines the maximum number of ACL rules that each inter-VPC firewall instance can handle. When the number of ACLs issued is excessive, it may lead to instability in the engine.
- To avoid disrupting your business, we recommend that you reasonably optimize rules based on the specifications of each instance and the number of issued rules, reduce the proportion of redundant rules, and enhance engine stability.

Specification Tiers	Minimum Bandwidth / Mbps	Maximum Bandwidth / Mbps	Rules Quota / Items
1	100	1,023	5,000 (This gear selection does not include intrusion prevention)
2	1,024	1,300	20,000
3	1,301	4,095	40,000
4	4,096	6,143	60,000
5	6,144	10,239	120,000
6	10,240	102,400	200,000

View VPC Boundary Firewall (Primary/Secondary Mode)

Last updated: 2025-05-20 10:45:44

Viewing Status Monitoring

Inter-VPC firewall status monitoring supports the statistics of the overall firewall bandwidth as well as the bandwidth of each instance. These statistics can be queried through multiple entry points.

1. Log in to the CFW console, in the left sidebar, select **Firewall Switch** > **Inter-VPC Switch**.
2. On the VPC switch page, the monitoring panel can be accessed using the following three methods:
   - Click the in the upper-right corner of the status monitoring, or click the **firewall peak bandwidth** and **single instance peak bandwidth** panels to quickly access the monitoring panel.

   - Click **firewall instance**, select the desired firewall, click **Operation** > **Bandwidth Monitoring** to quickly launch the monitoring panel.

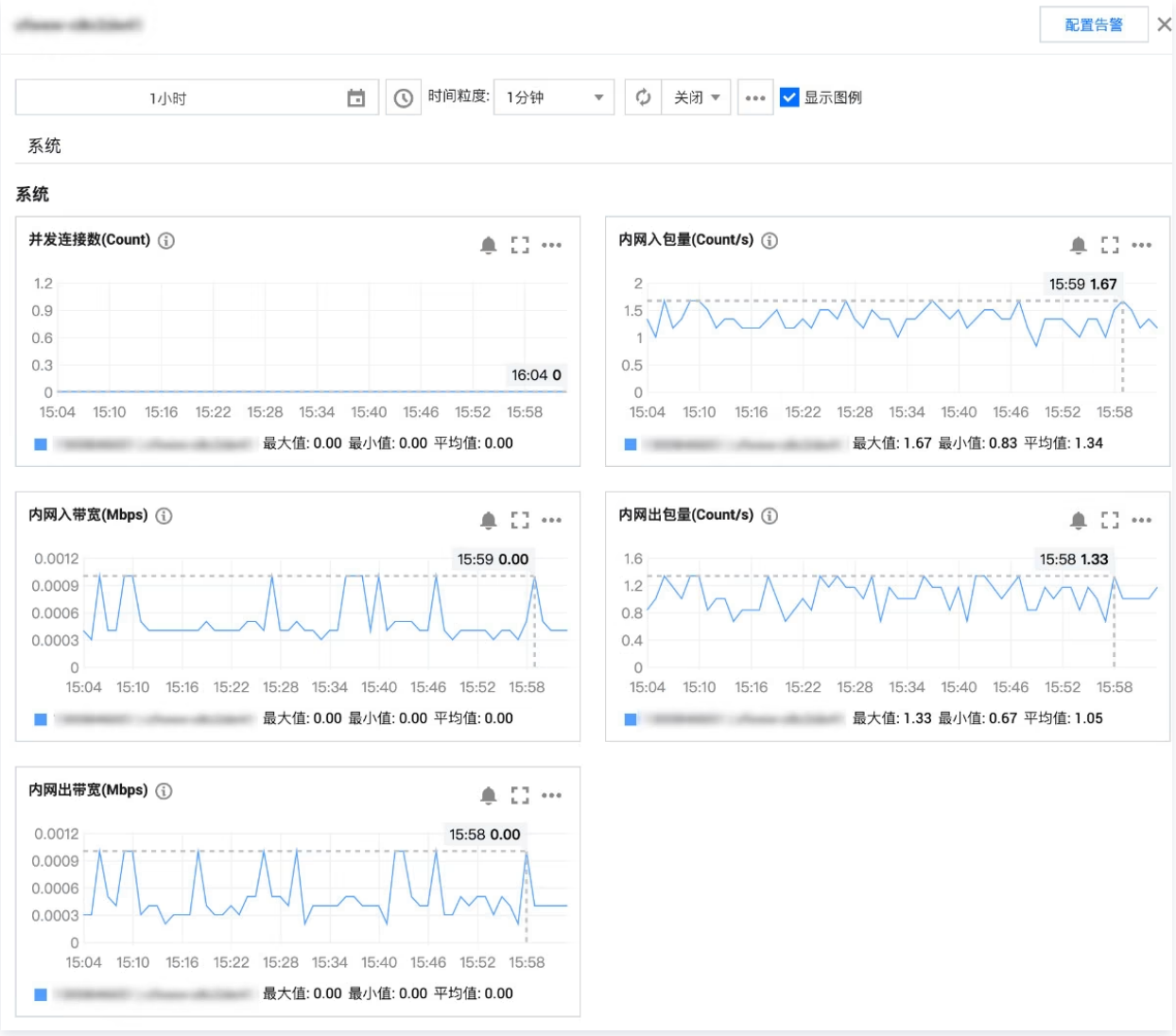
   - Click the **firewall instance**, select the desired firewall instance, and then click **Status Monitoring** to quickly access the monitoring panel.

3. In the monitoring panel, you can filter the monitoring dimensions based on ① firewall name or ② firewall instance name. You can also modify the statistical dimensions by selecting ③ the time range. You can view the ④ monitoring curve of the bandwidth, as well as check the ⑤ peak bandwidth data for the switches associated with the firewall or instance.

> **Notes:**

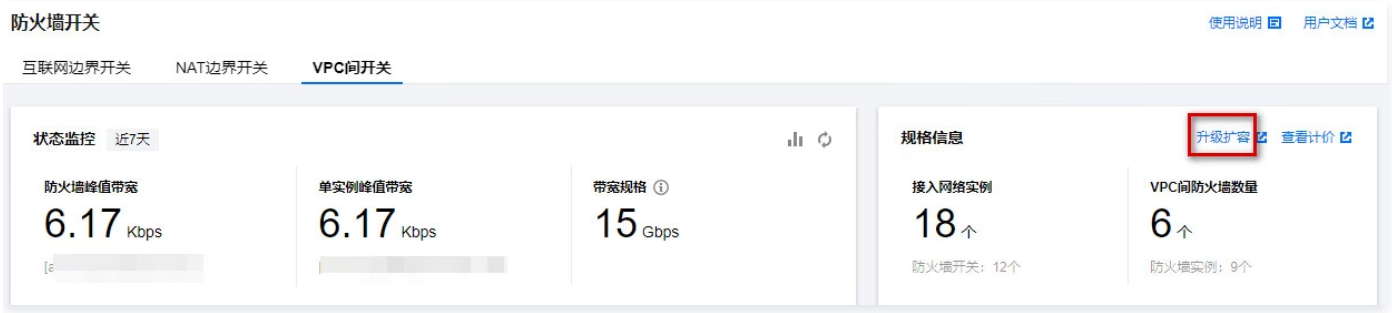
> The minimum statistical granularity for statistics of different time ranges varies and may result in discrepancies with the actual peak values. It is advisable to refer to the data from Tencent Cloud Observability Platform or the statistics of specific protection units as the standard.

4. In the monitoring panel, click **View Monitoring Metrics** to open the sidebar of the Tencent Cloud Observability Platform, view all monitoring metric data of the firewall instance, including concurrent connection number, private network inbound packet volume, private network outbound packet volume, private network outbound bandwidth, and private network inbound bandwidth. Alternatively, you can go to the Tencent Cloud Observability Platform Console to view detailed metrics or configure related alarms.



View Specification Information

In the specification information module on the firewall switch page, you can view specification information, including access network instances and inter-VPC firewall instances. Click **scale-out** in the upper-right corner of the rule information to navigate to the expansion interface. Under the default specification, enterprise edition users can create a maximum of 1 inter-VPC firewall, while flagship edition users can create 3 inter-VPC firewalls. To expand capacity, you can upgrade the version or use expansion resources.



Managing VPC Boundary Firewall (Primary/Secondary Mode)

Last updated: 2025-05-20 10:46:07

After the inter-VPC firewall is created, you can manage the inter-VPC firewall or individual firewall instances.

Viewing Overview

1. Log in to the CFW console, in the left navigation bar, select **firewall toggle** > **Inter-VPC toggle**.
2. On the VPC switch page, click the **firewall instance** to enter the firewall instance page. Here, you can view the already created firewall and its deployed firewall instance information.

> **Notes:**
> Instance Specifications: The current firewall instance's maximum bandwidth and the maximum number of rules that can be deployed. For details, you can refer to Instance Specifications.

Viewing Associated Switches

On the firewall instance page, click **Switch Quantity** to navigate to the firewall switch page. This will automatically filter and display the switches associated with the current firewall.

Configuring Instance

1. On the firewall instance page, hover the mouse over the **Operation** on the right side of the inter-VPC firewall that needs to be configured, select **Configure Instance**.

2. You can adjust the initial configuration made during creation, including the firewall instance name, instance specifications, and the network instances each instance is connected to. Additionally, you can add new inter-VPC firewall instances.

3. If there are newly connected VPCs, the network configuration specified during the creation of the inter-VPC firewall will be automatically applied. If you opt for a custom traffic redirection subnet creation method, you will also need to manually enter the subnet CIDR for the new VPC.

> **Notes:**
> The firewall network configuration cannot be modified.

Terminating the Inter-VPC Firewall

On the firewall instance page, hover the mouse over the **Operation** on the right side of the inter-VPC firewall that needs to be configured, select **Terminate Firewall**, and confirm the operation to proceed.

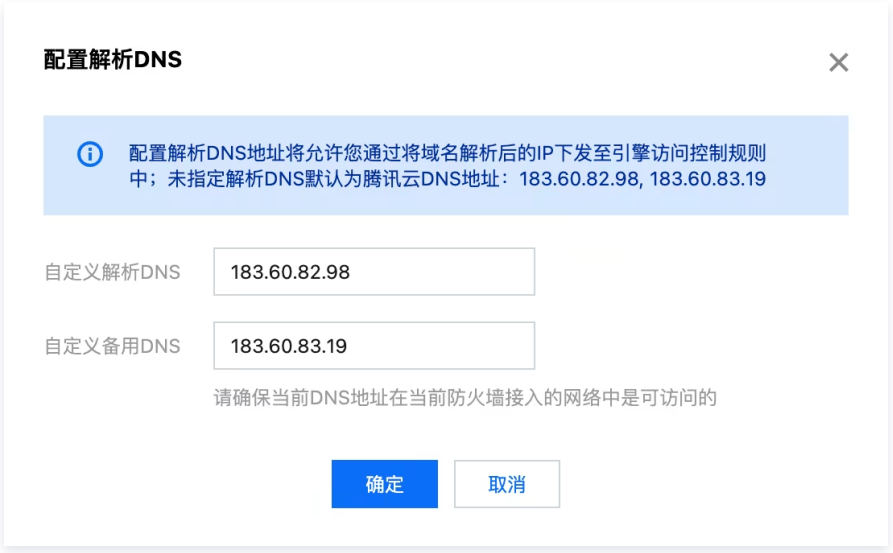
> **Notes:**
> If you chose custom routing, please ensure that you have manually restored the routing.

Configuring DNS Parsing

1. On the firewall instance page, hover over the **Operation** on the right side of the inter-VPC firewall that needs configuration.

2. Click **Configure DNS Resolution** to set up a custom DNS resolution server address for access control rules of domain name resolution type.
3. In the Configure DNS Resolution window, fill in relevant parameters, click **OK** to save.

> **Notes:**
> By default, Tencent Cloud's default DNS server addresses will be used, which are 183.60.82.98 and 183.60.83.19. If you need to specify a DNS server for parsing, please fill in below.



Debugging Tools

On the Inter-VPC toggle > **Firewall instance** page, select the instance as required, click **More**, then in the dropdown list, click **Debugging tool**.

- Enable ByPass: In ByPass mode, all traffic under the current instance will ByPass the firewall, and all firewall configurations will become ineffective. Recommended for debugging. Expected to take effect within 1 minute after enabling. Please manually disable ByPass mode after debugging is completed. For more help, submit a ticket.

> **Notes:**
> Enable ByPass mode may have the following effects:
> 1. Switching routes may cause a brief interruption for a few seconds.
> 2. Existing persistent connections will be affected and automatic retry for creating new connections is required.

- Restart instances: We will prioritize restarting the firewall replica. After the restart is complete, we will perform a primary/replica switch and then restart the firewall host. After the host restart is complete, we will perform another primary/replica switch. The entire process is expected to last about 10 minutes. There may be minor network fluctuations. You cannot perform operations or modify firewall configurations during this time. Operate during off-peak business hours.
- Switch primary/replica: The firewall adopts a mutual backup solution, where the working instance is the primary instance; you can choose whether to switch to the backup firewall instance. The switching process is expected to take 2–10 seconds, and there may be minor network fluctuations.
- Enable transparent mode: In transparent mode, the current firewall instance only forwards network traffic, and related access control features or intrusion prevention features will not take effect. Recommended for debugging. Expected to take effect within 1 minute after enabling. Please manually disable transparent mode after debugging is completed. For more help, submit a ticket.
- Migrate availability zones: You can choose to migrate the current host or replica to another availability zone. The migration process is expected to last 2–5 minutes. Operations such as primary/replica switch may be performed, and network fluctuations may occur. Operate during off-peak business hours.

Manage VPC Boundary Firewall Instances (Primary/Secondary Mode)

Last updated: 2025-05-20 10:46:32

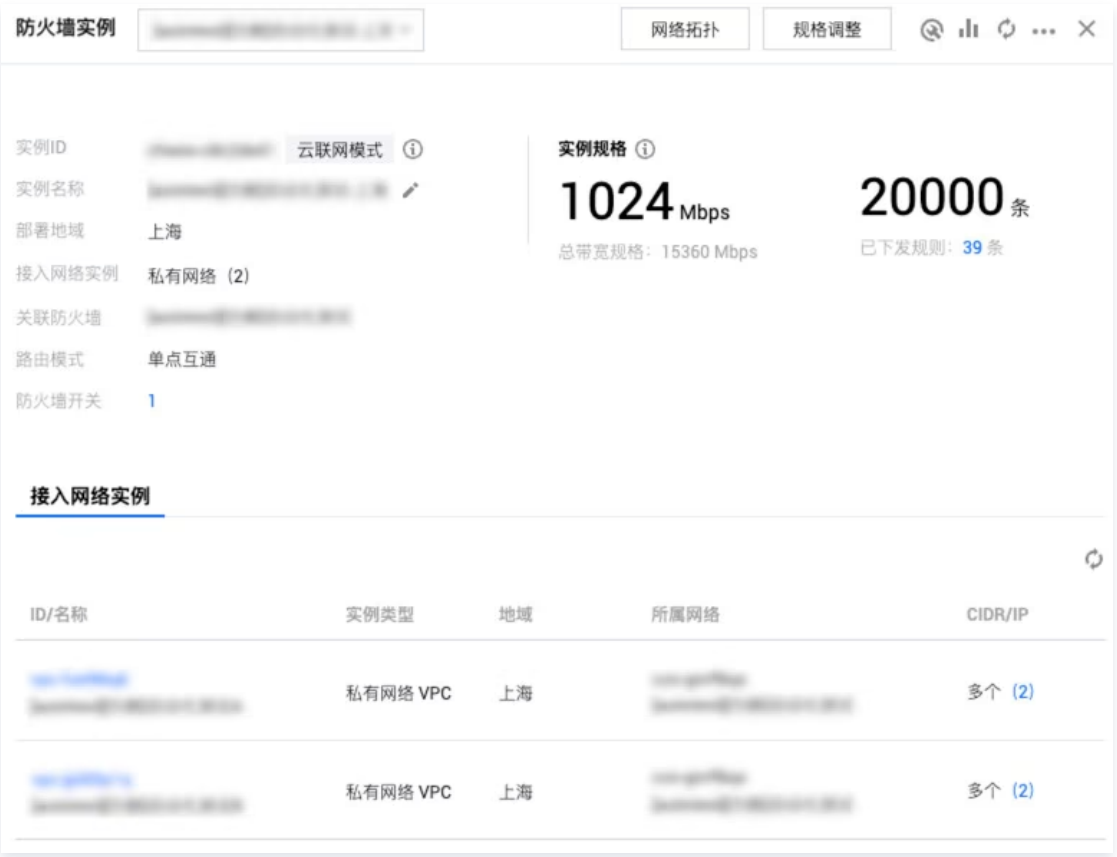
After the inter-VPC firewall is created, you can individually manage the inter-VPC firewall instances.

1. Log in to the CFW console, in the left sidebar, select **Firewall Switch** > **Inter-VPC Switch**.
2. On the VPC switch page, click **firewall instance** to enter the firewall instance page.

Viewing Instance Details

1. On the firewall instance page, click **firewall instance ID** or click on the right **instance details**.

2. On the firewall instance page, you can view the configuration details of the instance.



Viewing Associated Switches

On the firewall instance page, click **More** > **View Firewall Switch** to navigate to the firewall switch page. This will automatically filter and display the switches associated with the current firewall instance.

Notes:
The association of a firewall instance with a switch depends on whether the traffic controlled by the switch will pass through that instance. A switch may be associated with multiple instances.

Terminating Inter-VPC Firewall Instances

Terminating any firewall instance requires turning off all switches associated with the current inter-VPC firewall.

1. On the firewall instance page, click the **quantity of switches** of the inter-VPC firewall.

2. Go to the firewall switch page, then click **All Off** to turn off all switches associated with the current firewall.

3. On the firewall instance page, click **More** > **Terminate Instance**, and the current firewall instance will be terminated after secondary confirmation.

Notes:
After the firewall instance is terminated, the VPC currently connected to the instance will be automatically disconnected, and any used quotas will be returned.

Reconnecting to Instances

To reconnect to an instance, you need to turn off all switches associated with the current inter-VPC firewall.

1. On the firewall instance page, click the **quantity of switches** of the inter-VPC firewall.

2. Go to the firewall switch page, then click **All Off** to turn off all switches associated with the current firewall.

3. On the firewall switch page, click **More** > **Reselect Access Instance** to enter the edit inter-VPC firewall page.

> **Notes:**
> - When integrating with the inter-VPC firewall in Virtual Private Cloud mode, you can select again the connected VPC instance.
> - In CCN mode, all VPC instances within the Cloud Connect Network are accessed, and reselection is not supported.

4. In the pop-up window, select the VPC to reconnect and click **OK**.

ByPass Mode

Manual bypass

The firewall supports manually switching to ByPass mode. In ByPass mode, all traffic from the current instance will ByPass the firewall, and all firewall configurations will become ineffective. **It is recommended for debugging.**
On the firewall instance page, click **More** > **Enable ByPass** / **Disable ByPass**.

> **Notes:**
> After debugging is completed, please manually disable ByPass mode.

Automated bypass

1. On the VPC switch page, click **firewall setting**.

2. On the firewall setting page , modify the maximum duration of firewall full load. The firewall will automatically bypass when the trigger threshold is reached.

> **Notes:**
> Before using, please first upgrade the engine version to the latest. Private network mode with custom routing and traffic diversion does not support automatic bypass. CCN mode with custom routing and traffic diversion automatically enables bypass; backup routes must be prioritized. For details, see View/Edit Backup Routes.

View/Edit Secondary Route

A secondary route refers to the route that a VPC will automatically switch to when the firewall enables bypass mode. You can view the binding relationship of the secondary route in the console.

1. On the VPC switch page, click **firewall instance**, select the desired firewall instance, and click **instance details**.

> **Notes:**
> The current version only supports displaying secondary routes in CCN mode.

2. Click **secondary route**, and you can see the list of all connected Virtual Private Clouds and their bound secondary route relationships below.

3. Click **Edit** to edit the secondary route bound to the VPC. You can select a route table or select firewall not connected. When selecting firewall not connected (bypass), no operation will be performed on this VPC.

> **Notes:**
> Edit operations are only supported in custom routing and traffic diversion mode.

Manage Firewall Switch (Primary/Secondary Mode)

Last updated: 2025-05-28 10:06:34

On the Firewall Switch page, you can enable or disable the inter-VPC firewall switch to control inter-VPC traffic. Meanwhile, the Cloud Firewall automatically synchronizes assets, so you don't need to worry about firewall configuration issues after asset changes. The Cloud Firewall will automatically synchronize within a short time.

> **Notes:**
> Enabling or disabling the firewall involves network and routing switches, which may cause short-term network jitter and momentary disconnection. Please choose an appropriate time for these operations.

Introduction to Firewall Switch Types

There are 4 types of firewall switches: single-point mode, multi-point mode, full interconnection mode, and custom routing.

- Single-Point Mode: In this mode, one firewall switch corresponds to one pair of interconnected VPCs, and one pair of interconnected VPCs corresponds to one peering connection (or Cloud Connect Network) instance.
- Multi-Point Mode: In this mode, one firewall switch corresponds to one VPC, and all traffic entering and exiting this VPC is managed by this switch. Inter-VPC traffic will be controlled independently by two switches for each pair of VPCs.
- Full interconnection mode: In this mode, one firewall switch corresponds to all interconnect routes of a firewall. Enabling the firewall switch will take over all incoming traffic from connected VPCs.
- Custom: The switch has no practical meaning and is only used for showing access to VPC.

If you change the peering connection (or Cloud Connect Network) instance, the firewall switch will correspondingly synchronize the changes. To avoid affecting your business, we will only immediately execute changes for switches that are in the off status. Please ensure that the firewall switch is turned off when you modify the configuration of the peering connection (or Cloud Connect Network) between VPCs.

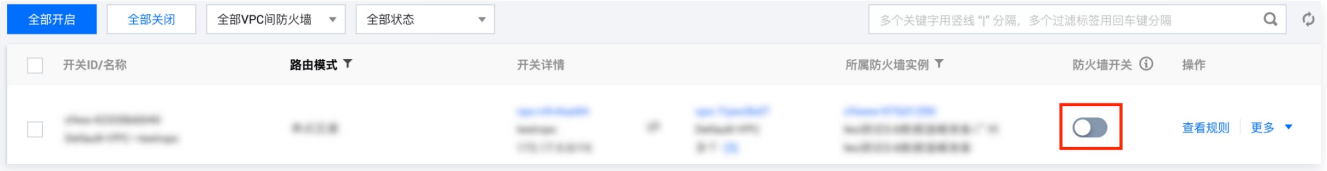
> **Notes:**
> Cloud Firewall does not establish connections with the basic network. The firewall switch is automatically generated based on reachable routes. If no switch exists, check if there is a peering connection or CCN.

Turning on the Switch

After the switch is turned on, the system will automatically modify the routing policies of the relevant route tables, directing all traffic between the local and peer networks corresponding to the firewall switch to the inter-VPC firewall.

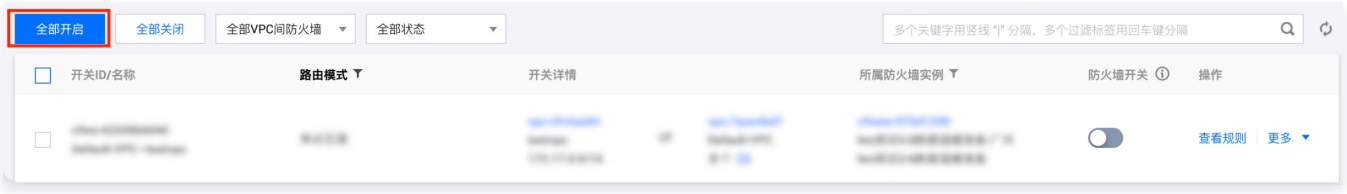
1. On the inter-VPC switch page, click the **firewall switch**, supporting individual, batch, or full firewall activation.

- Select the desired firewall, click the firewall switch's , and a pop-up window to enable it will appear.



- Batch: After selecting the firewall switches, click **Batch Start** in the upper left corner, and a pop-up window to enable it will appear.

- All: When no items are selected, click **Enable All** in the upper left corner, and a pop-up window to enable it will appear.



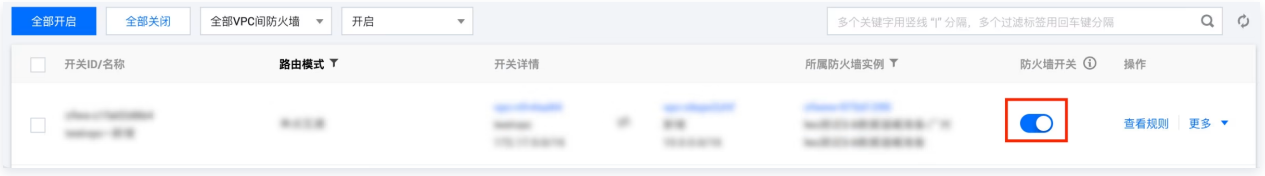
2. In the confirmation pop-up window, click **OK** to enable protection.

> **Notes:**
> - If the peering connection (CCN) route between VPCs is not configured correctly, the firewall cannot be enabled.
> - Once enabled, do not manually change the route corresponding to the switch in the "Virtual Private Cloud" (CCN) console; otherwise, it will cause the firewall to lose the route and result in a network interruption.

Turning Off the Switch

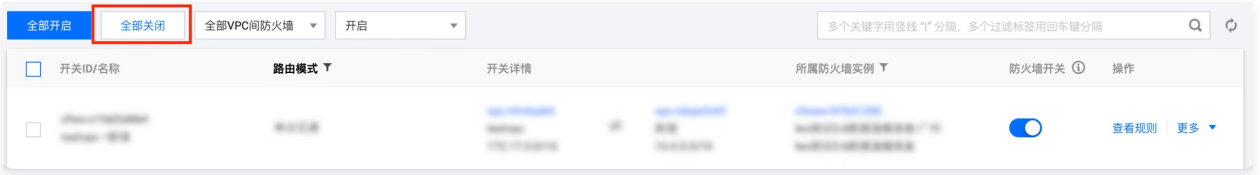
After the switch is turned off, the system will automatically restore the routing policies of the relevant route tables. Traffic between the local and peer networks corresponding to all firewalls will revert to their original paths and will not pass through the inter-VPC firewall.

1. On the inter-VPC switch page, click the **firewall switch**, supporting individual, batch, or full firewall deactivation.
   - Select the desired firewall, click the firewall switch's , and a confirmation close pop-up will appear.



   - Batch: After selecting the firewall switches, click **Batch Shutdown** in the upper left corner, and a confirmation close pop-up will appear.

   - All: When no items are selected, click **Close All** in the upper left corner, and a confirmation close pop-up will appear.



2. In the confirmation pop-up window, click **OK** to disable protection.

> **Notes:**
> After it is turned off, you can switch VPC routes as needed, but do not manually enable firewall routes, as this may cause network interruptions and firewall switch failures.

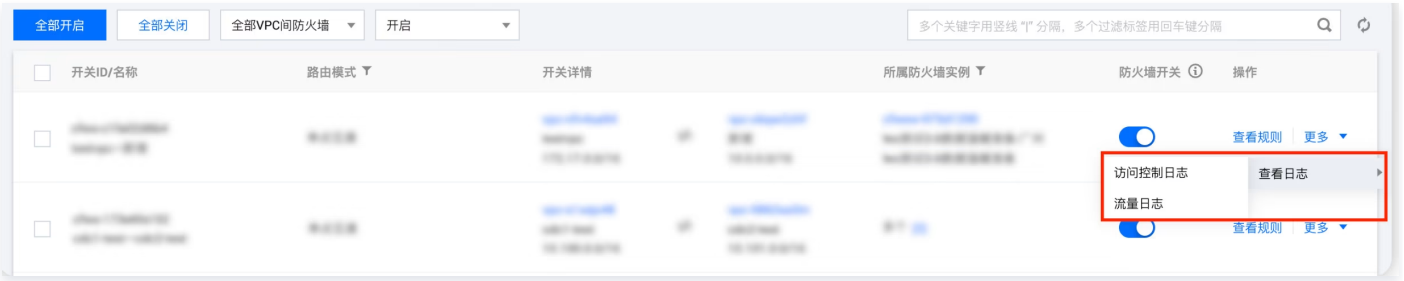
View Rule

1. On the inter-VPC switch page, click the **firewall switch**.
2. On the firewall switch page, select the desired firewall switch, and click **View Rules**.

3. On the private network rules page, you can view and edit rules. For details, see Access Control – Private Network Rules.

Viewing Logs

1. On the inter-VPC switch page, click the **firewall switch**.
2. On the firewall switch page, click **More** > **View Logs**, and you can choose to view traffic access control logs or traffic logs.



Using Network Topology (Primary/Secondary Mode)

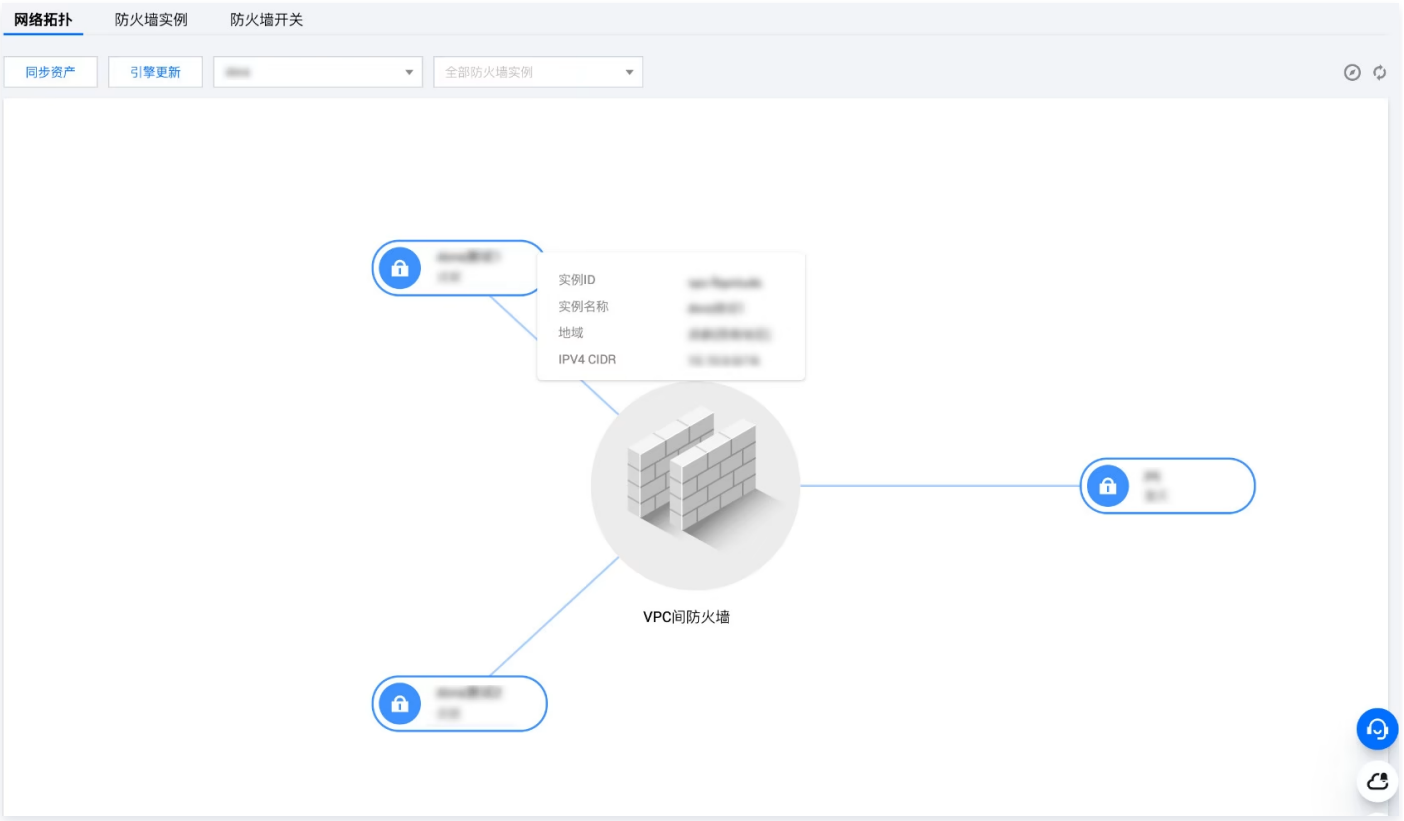
Last updated: 2025-05-28 10:08:10

Viewing Network Topology

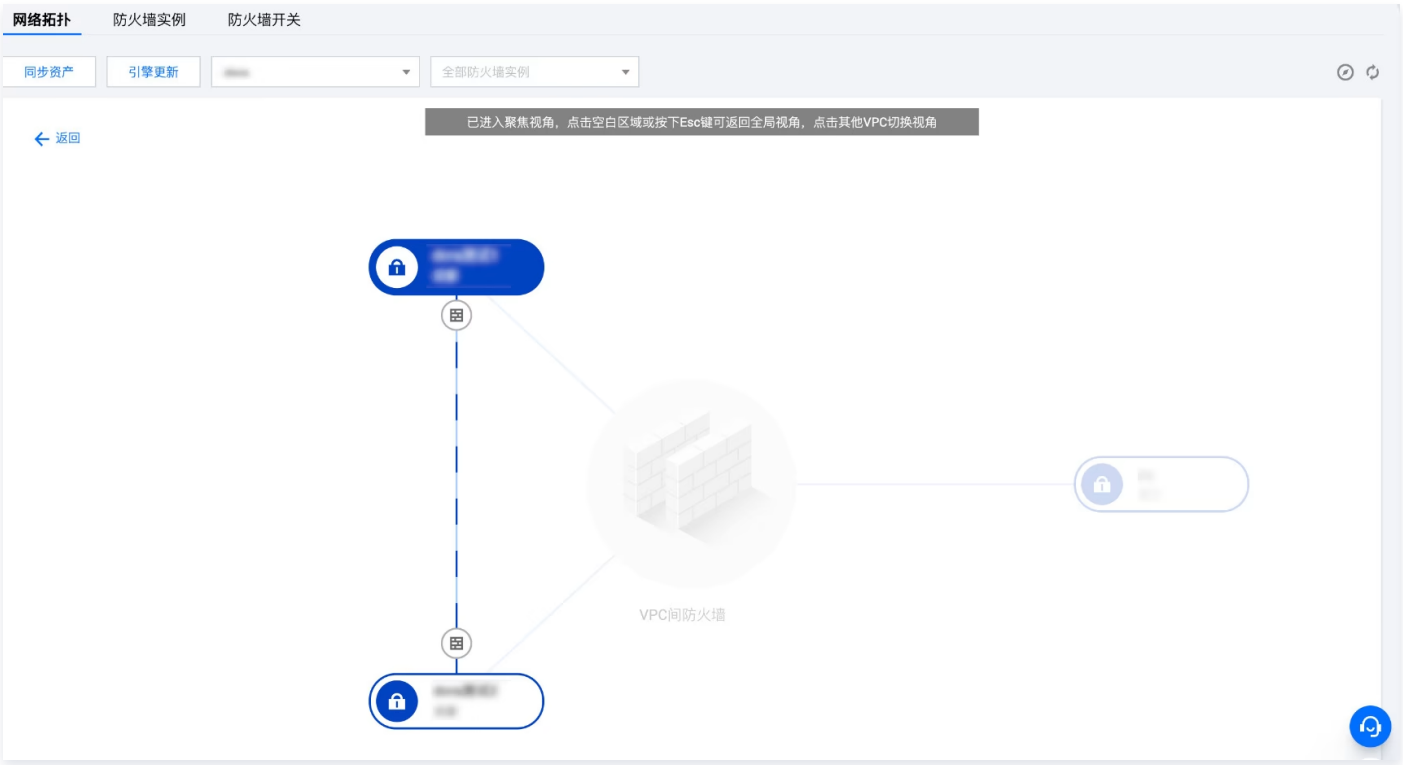
The Cloud Firewall provides a visual view to help you quickly map out the access relationships between assets in VPCs.

> **Notes:**
> No network topology diagram under the custom routing solution.

1. Log in to the CFW console, in the left sidebar, select **firewall toggle** > **Inter-VPC toggle**.
2. On the inter-VPC switch page, click **Network Topology** to view detailed information about the connected VPC network instances.
3. On the network topology page, hover the mouse over a specific VPC instance to view its detailed information.



4. Click an instance to view its connection with other VPC instances and the firewall switch status. If the firewall switch icon is dark blue, it means the switch is on; if it is gray, it means the switch is off.



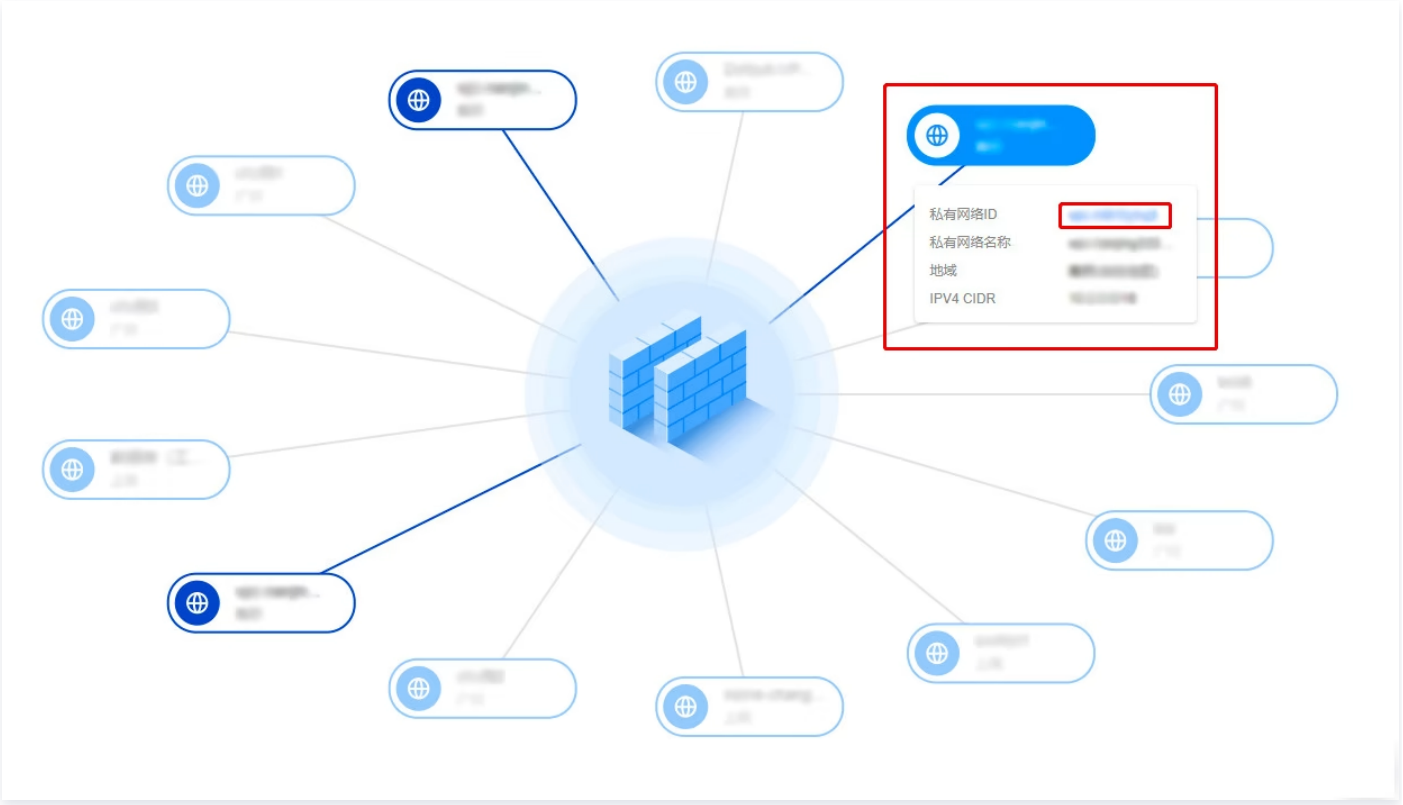
5. On the network topology page, click **Synchronize Assets** to synchronize asset information timely; hover the mouse over the engine update to view version information.

6. On the network topology page, click or in the upper right corner to view operation guide or refresh network topology.

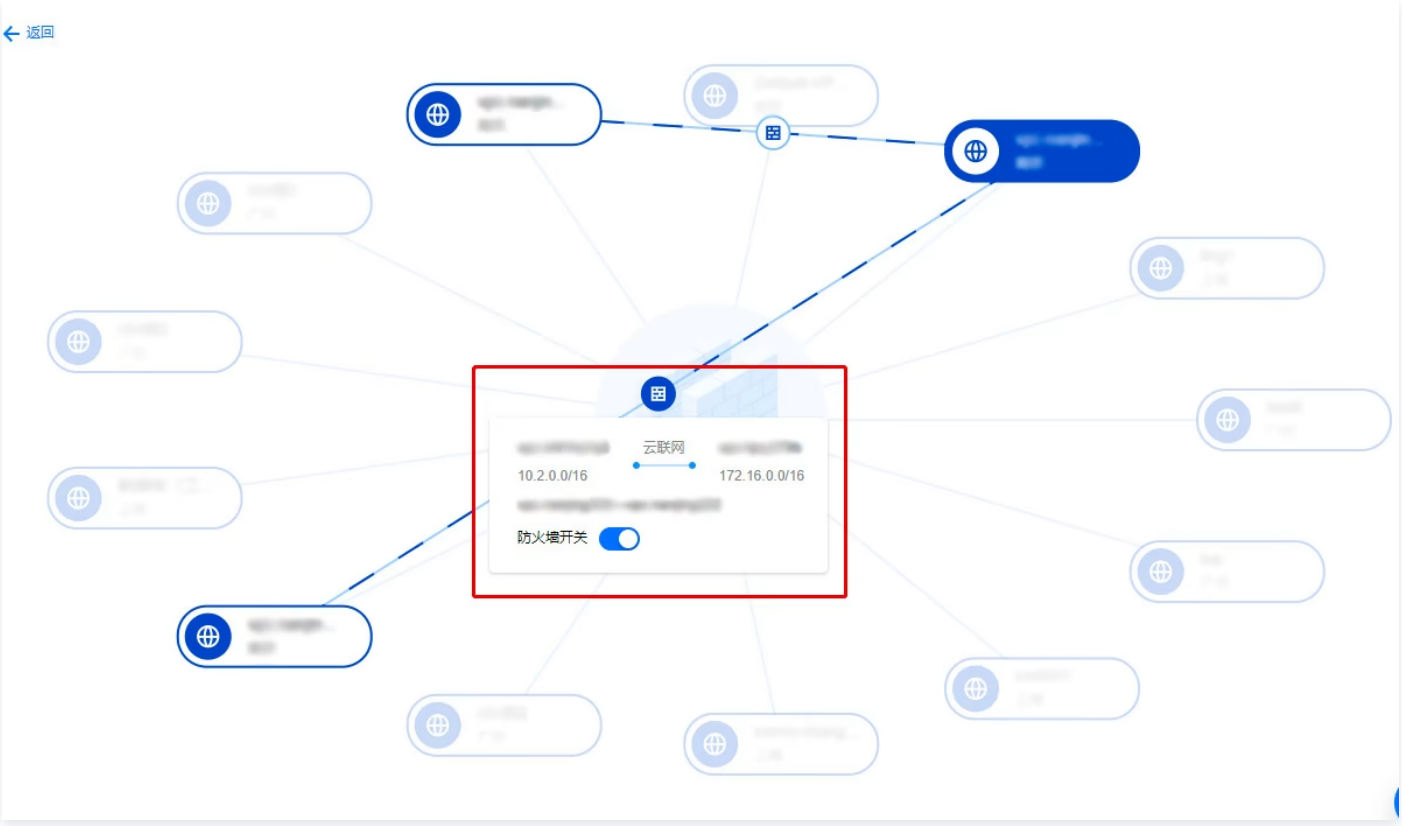
Use VPC view to map out the access relationships between VPCs.

Cloud Firewall provides a visual view to help you quickly sort out the access relationships between VPCs. In the VPC visualization view, each node represents a VPC instance, with the inter-VPC firewall acting as a centralized device. Each switch controls different routes. Once the switch is turned on, the traffic between VPCs will be directed to the firewall for filtering and protection.

1. Log in to the CFW console, in the left navigation bar, select **firewall switch** > **Inter-VPC toggle**.
2. On the inter-VPC switch page, click **Network Topology** to view detailed information about the connected VPC network instances.
3. Hover the mouse over a VPC node to view brief information about the VPC. All VPCs connected to it will also light up. Click the blue font of the Virtual Private Cloud ID to enter the VPC details page to view detailed information about the VPC.



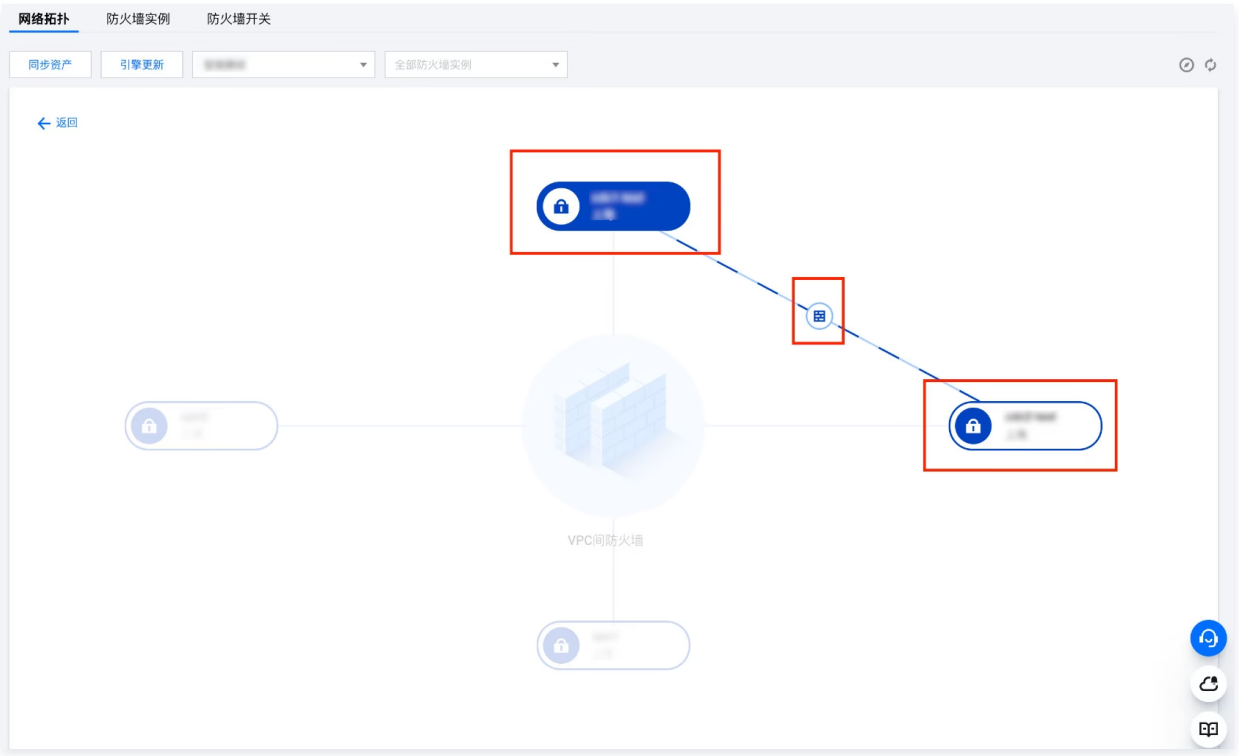
4. You can click **a certain VPC node**, the page enters the focus view, displaying a topology centered on the focused VPC.
5. Interconnected VPCs are connected via lines. You can view or operate the firewall switch during the connection, or click the of the firewall to directly enter the access control rule configuration page.



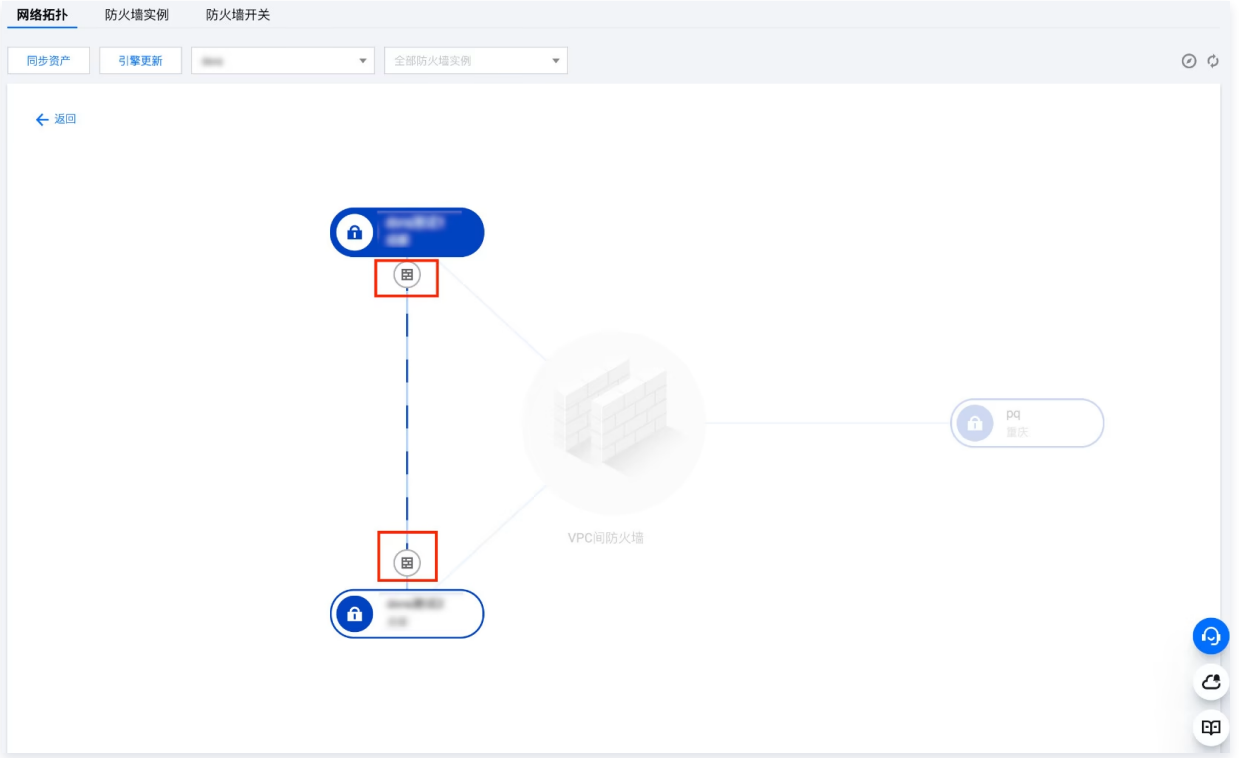
Note

- In the single-point interconnection mode, each pair of mutually accessible VPCs will only display one switch in the diagram.
- In the multi-point interconnection mode, each VPC will display a switch.
- In the full interconnection mode, the inter-VPC firewall will only have one switch.

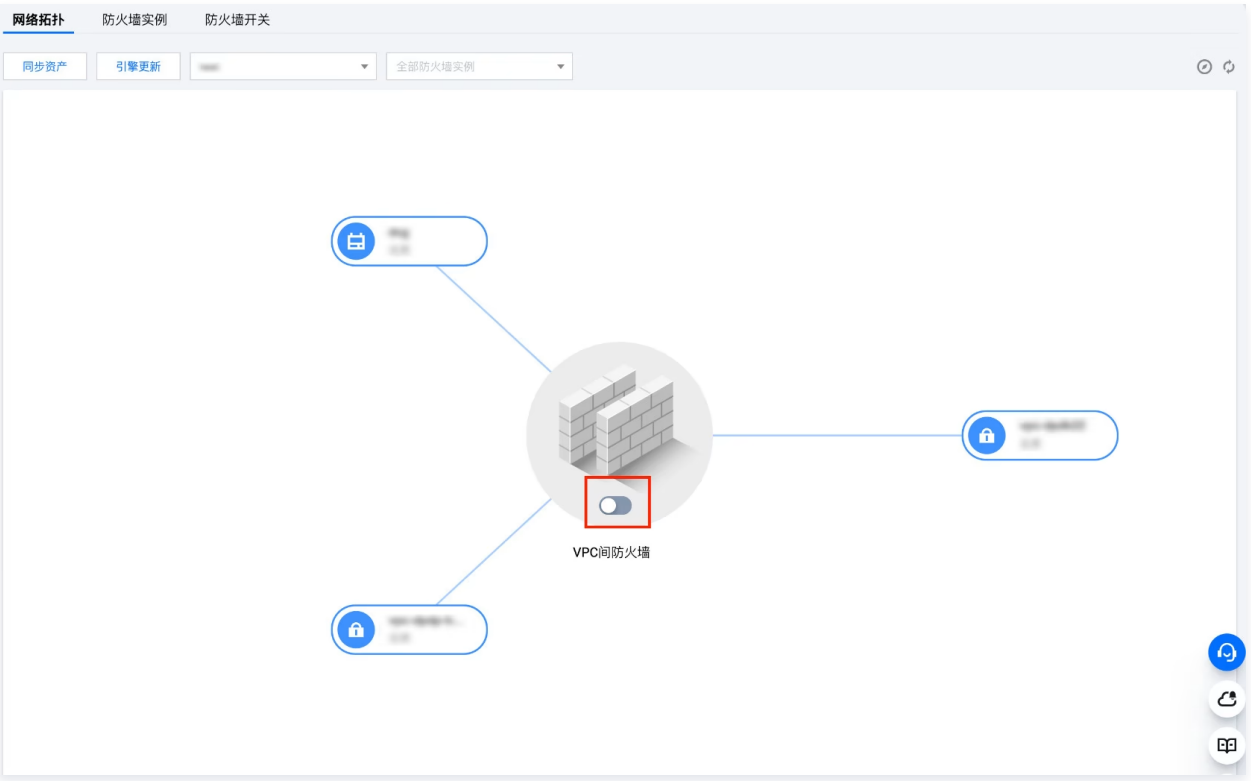
- single point interconnection mode



- multi-point interconnection mode



- full mesh mode



Custom Routing Configuration Guide (Primary/Secondary Mode) Overview

Last updated: 2025-05-20 10:49:56

In the custom routing mode of the inter-VPC firewall, users can customize the routing configuration to implement a personalized traffic diversion and protection solution.

> **Notes:**
> Before using the custom routing mode, please confirm that the basic network has been interconnected (via peering connection or Cloud Connect Network). The cloud firewall cannot perform basic network interconnection.

Basic Concepts

Firewall Instance

A virtualized instance used to host firewall features, similar to a CVM. You can go to the CFW console to view it.

Firewall Traffic Diversion VPC (CCN Mode)

A dedicated VPC created by the firewall in the CCN, used to divert user network traffic through the firewall to the firewall instance, thereby achieving protection effectiveness. Do not delete or modify. It is generally named "Firewall Dedicated VPC_Do not delete or modify". You can go to the CCN instance details console to view it.

> **Notes:**
> The firewall will create different VPCs in each region for traffic diversion of the corresponding region.

Firewall Route Table (CCN Mode)

The route table automatically created by the firewall for traffic distribution. Do not manually modify. It is generally named "Firewall VPC Dedicated Route Table_Do not delete or modify".

> **Notes:**
> A route table is created in each region for the firewall.

Firewall Traffic Diversion VPC

A dedicated VPC created by the firewall in the CCN, used to divert user network traffic through the firewall to the firewall instance, thereby achieving protection effectiveness. Do not delete or modify. It is generally named "Firewall Dedicated VPC_Do Not Delete or Modify". You can go to the CCN instance details console to view.

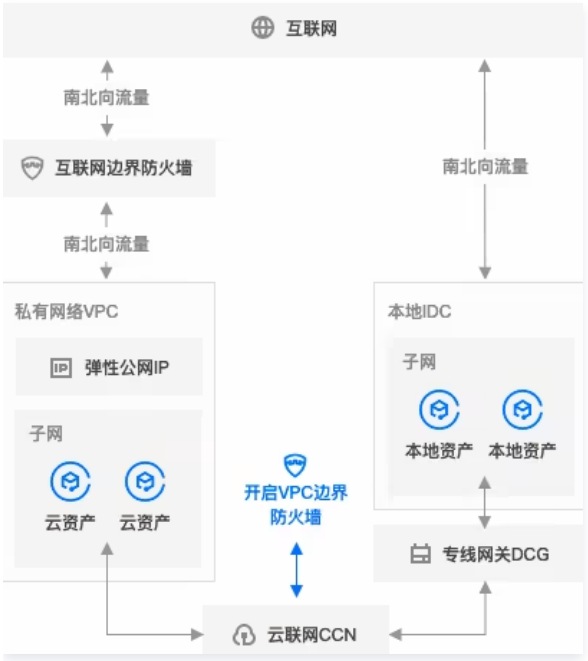
> **Notes:**
> The firewall will create different VPCs separately for each region to divert traffic for the corresponding region.

Working Mode

Virtual Private Cloud Mode

CCN Mode

The inter-VPC firewall and all business VPCs are in the same CCN. A dedicated VPC IP range is established to divert traffic between user VPCs to the firewall.



Virtual Private Cloud Mode

Last updated: 2025-05-28 10:10:14

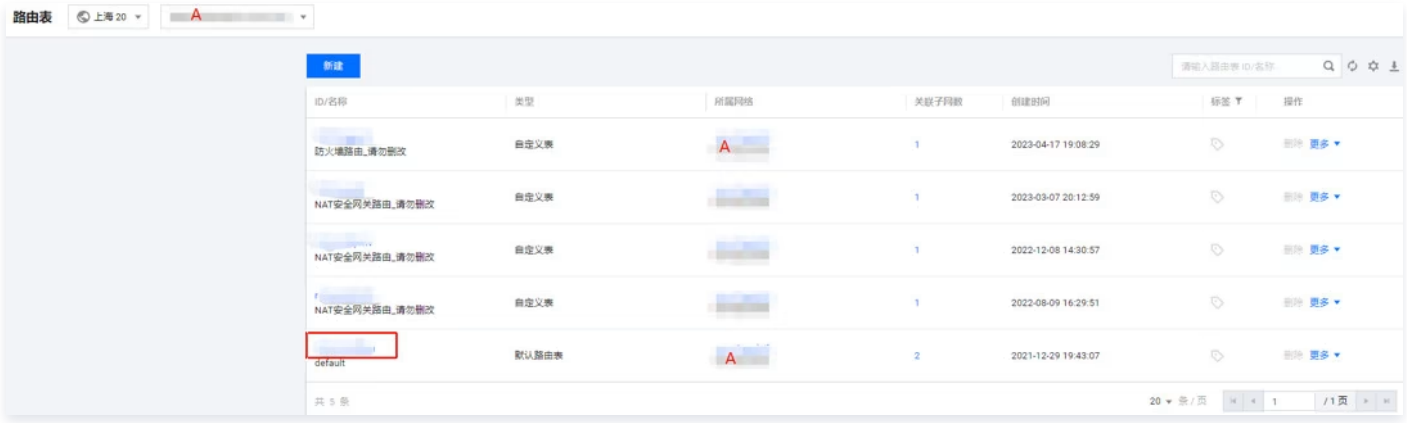
Step 1: Create a custom routing pattern instance.

See Inter-VPC Firewall Switch - Create Inter-VPC Firewall to create a target instance, where the routing mode selects **Custom Routing**.

Step 2: Configure traffic attraction routing.

Check the VPCs at both ends of the peering connection, which are VPC A and VPC B.

1. On the Route Table page, find the route table for VPC A and click the **ID** of that route table. Select the **default routing table**.



2. On the details page, click **add routing policy**.
3. In the Add Routing pop-up window, add a routing policy with the destination as VPC B IP range and the Next Hop as the highly available virtual IP, then click **Create**.

4. On the details page, turn off the routing switch of the original peering connection and immediately enable the routing just configured.

> **Notes:**
> Switching the routing network may cause a momentary disconnection, so it is recommended to operate during the off-peak business period.

5. On the Route Table page, find the route table for VPC B and select the default route table.

6. Repeat the previous steps to add firewall routing entries.

Step 3: Verify that the firewall is working properly.

1. Refer to Log Audit to check whether there are traffic logs.
2. See Log Audit to check whether the intrusion prevention is working properly.
3. Configure private network rules and check whether they are hit normally.

The firewall is now functioning properly. If your network structure is complex or involves a dedicated line scenario, please submit a ticket for detailed routing configuration solutions. If you have further questions, feel free to submit a ticket to contact us.

Using CCN Mode

Last updated: 2025-05-28 10:11:08

Step 1: Create a custom routing pattern instance.

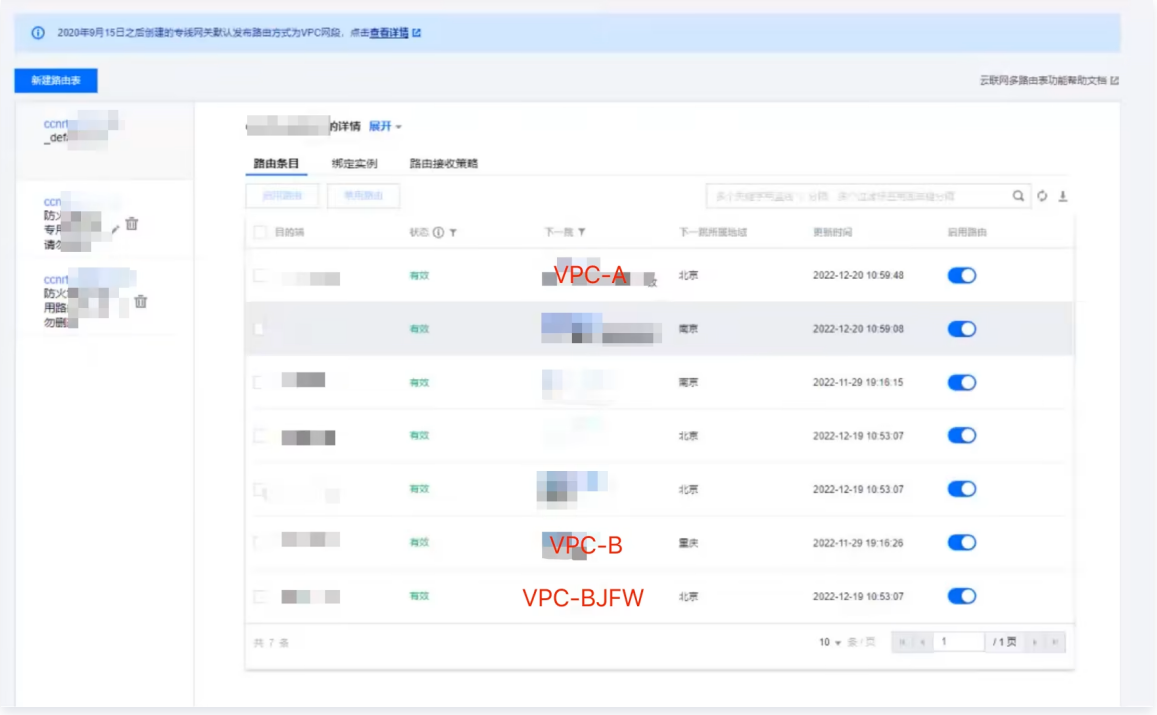
Refer to Create Inter-VPC Firewall to create a target instance, where the mode selects **Custom Routing**.

Step 2: Configure traffic attraction routing.

The current operation aims to divert the business VPC that users need to protect to the firewall instance through the firewall gateway.

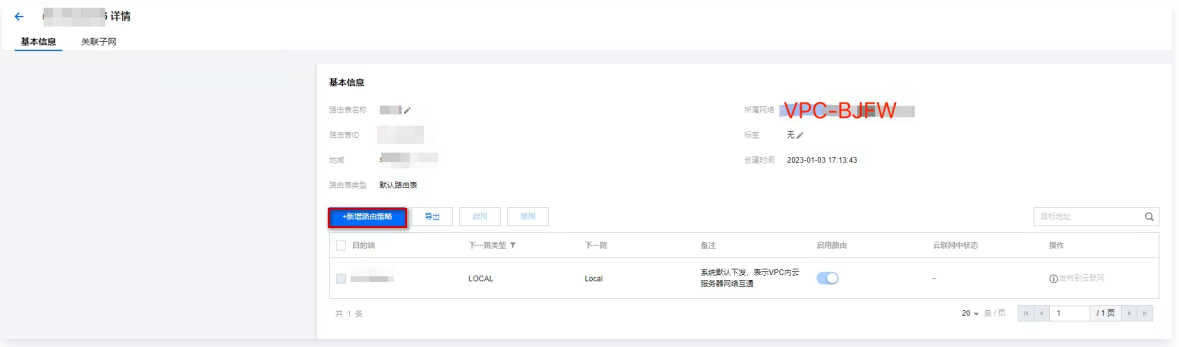
1. Go to the console of the CCN instance selected when Create an Inter-VPC Firewall, and view the detailed information of the associated CCN instance in advanced mode.
2. Confirm that the firewall traffic diversion VPC and related routing tables have been created. If they are not created, wait for the instance creation to complete or submit a ticket to contact us.
3. View the default route table page, and confirm the business VPC and firewall traffic diversion VPC that need to be connected.

> **Notes:**
> This document uses the following examples to demonstrate how to integrate: Beijing business VPC: VPC-A; Chongqing business VPC: VPC-B; Beijing regional firewall traffic diversion VPC: VPC-BJFW.



4. Go to **VPC** > Route Table page, select the firewall diversion VPC that needs to be connected, and you can see the route tables including "Firewall VPC Dedicated Route Table_Do Not Delete or Modify" and "default". Select the "default" route table to edit the routing policy.

5. Click **Add Routing Policy** to divert traffic from the business VPC to the firewall.



Enter the CIDR of the business VPC as the destination, select **HAVIP** for the next hop type, choose **Firewall Gateway ID** for the next hop, and freely fill in the remark.

> **Notes:**
> If there is a prompt "Specify CIDR to form ECMP", you need to first disable the related business routes in the default route table.

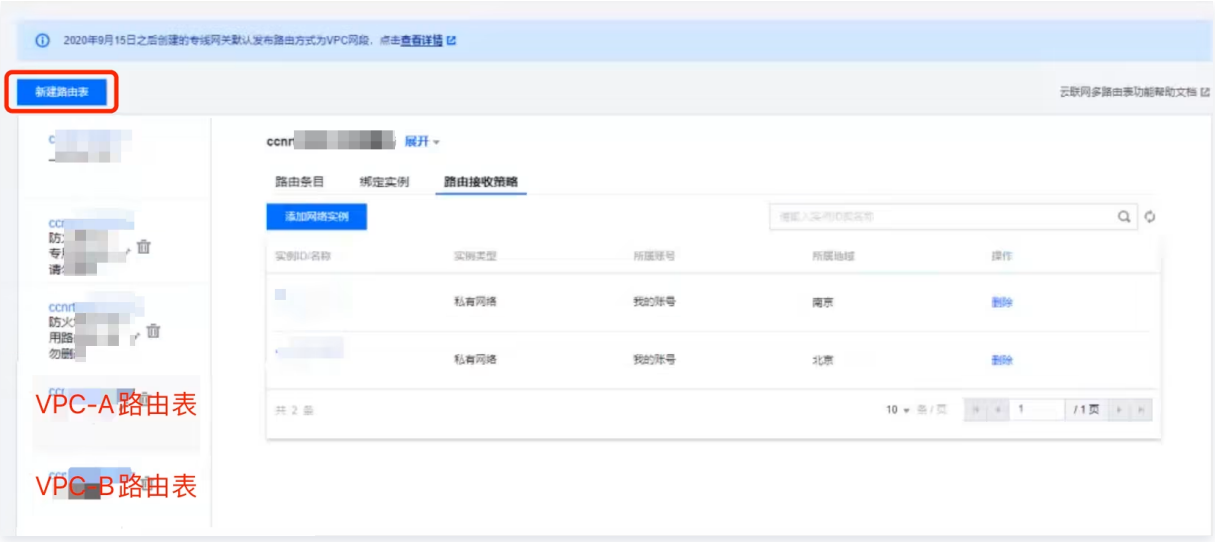
6. Add a new route and publish it to the CCN. For details, see Manage Routing Policies. After publication, you can see the specified routing strategy in the default route table of the corresponding CCN.

> **Notes:**
> The original route entry will become invalid due to the conflict between the new routing strategy and the original routing strategy, which can be ignored.

Step 3: Create a Route Table for Business VPC Interconnection

The current operation aims to integrate the firewall network with users' business networks to achieve mutual network access.

1. On the CCN page, create a route table for each business VPC that diverts traffic to the firewall.



2. Adjust the route reception policy. In the **route reception policy** of the route table of a service VPC for each VPC, click **Add Network Instance** to add the VPC instance that the routing table itself belongs to and the interconnected VPC instances to the routing table.

> **Notes:**
> Add a network instance, which must consist of two steps: first, add your own VPC instance and the VPC instance that does not pass through firewall protection; then, add the VPC instance dedicated for firewall traffic diversion.

For example: Assuming VPC-C is a business VPC that does not require connection to a firewall instance, then in the routing table of VPC-A, you should first add two instances: VPC-A and VPC-C. Once added successfully, repeat the above operation to add one instance of VPC-BJFW.

3. Check whether the route entries in the route tables of each VPC meet expectations.
4. Bind a network instance. Click **Bind Network Instance** for the **bind instance** of the dedicated route tables of each VPC to bind the dedicated route tables of each VPC to their corresponding VPC instances. After the operation is completed, the network will divert traffic to the firewall.

> **Notes:**
> Please confirm the route is correct before binding the route table. It will take effect immediately after binding.

Step 4: Verify Whether the Firewall Is Working Properly

1. See Log Audit to check whether there are traffic logs.
2. Refer to Log Audit to check whether the intrusion prevention is working properly.

> ⚠ **Notes:**
> In custom routing mode, the intrusion prevention mode follows the main mode and cannot be adjusted independently.

3. Configure private network rules and check whether they are hit normally.

The firewall is now working properly. If your network structure is complex or involves a dedicated line scenario, submit a ticket to consult detailed routing configuration solutions. If you have more questions, feel free to submit a ticket to contact us.

Asset Center Overview

Last updated: 2025-05-20 10:50:48

The Asset Center collects data and information related to users' assets. Through asset grouping, asset classification, etc., it facilitates users to retrieve asset information, helping users better understand the current status of assets, manage assets, and predict and prevent security incidents. Based on different classification logic, the Asset Center is divided into three parts: asset overview, asset list, and service sorting.

- Asset Overview: Contains statistics on the number of assets of all types, traffic statistics, and general overview of attack risk statistics. It also supports user customization grouping and other methods, helping users organize and sort existing assets, making it easier to view asset information.
- Asset List: Classify asset information display and statistics on asset exposure risks by dividing assets into types such as hosts, public IP addresses, and domain names.
- Service Sorting: Statistics of asset information for Web services, including Web traffic and attack risk information.

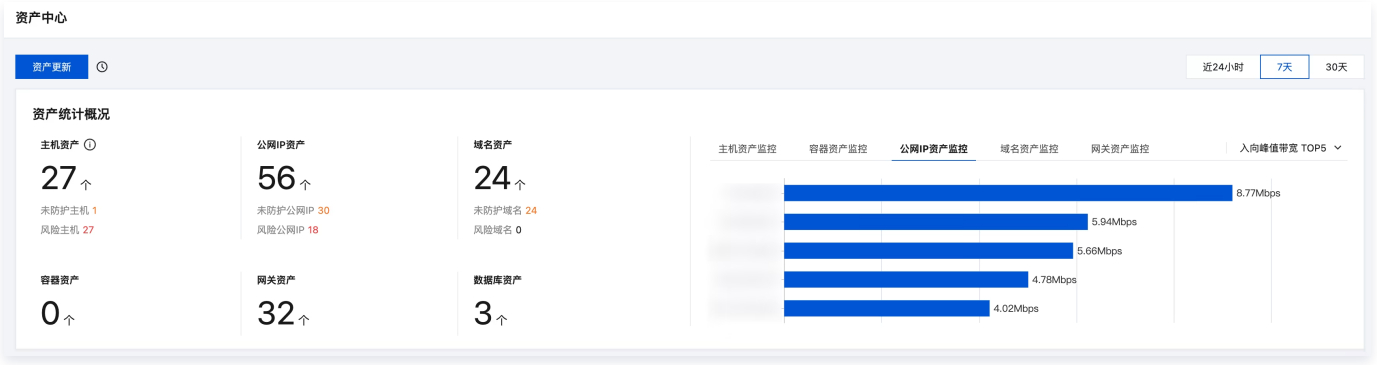
Asset Overview

Last updated: 2025-05-28 10:17:55

Asset Statistical Overview

Through asset statistics overview, you can quickly understand the current number of user assets, as well as the main exposed risks, grasp the asset status, and predict and prevent security incidents.

1. Log in to the Cloud Firewall console, in the left sidebar, click **Asset Center**.



2. On the Asset Center Page, the left side displays the statistical overview of assets and the number of risks. Click **asset number** to navigate to the page of the corresponding **asset type** and view asset details.
3. On the right side of the page, users can select to view asset information from the last 24 hours, 7 days, or 30 days, including TOP5 asset information such as traffic, bandwidth, and asset usage rate.

Update Assets

The backend periodically polls user asset information at intervals of 10 minutes. Therefore, when the user asset size changes within this interval but hasn't been synchronized by the backend, on the Asset Center page, click **Update Assets** to promptly invoke backend APIs to re-read and synchronize user asset information and data.

Asset Group

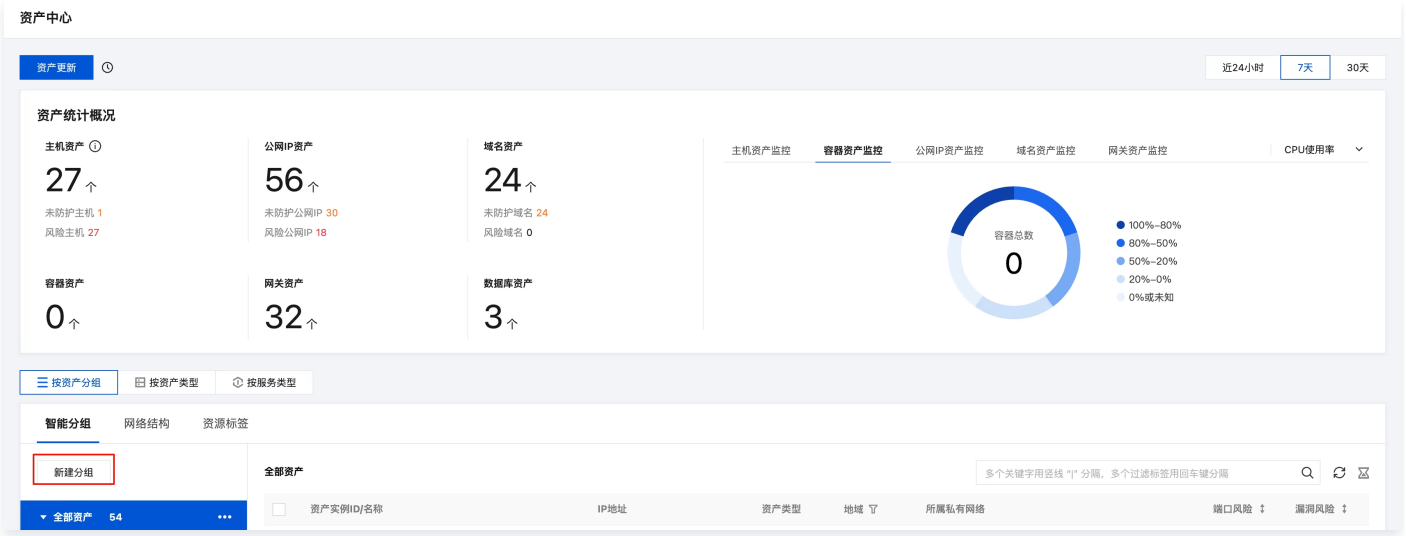
The Asset Center supports users to organize and group-view assets via custom grouping methods, convenient for users to quickly grasp the organization information of current assets.

> **Notes:**
> When used for the first time, the CFW will generate default group information based on the user's resource tags. Users can choose to adjust or reset groups as needed.

Node Group Creation

Method 1

1. On the Asset Center > **Group by Asset** > **Intelligent Grouping** page, click **Create Group** to create a new asset group.



2. In the pop-up window for creating a new asset group, select the method for adding assets to the group:
   - Manually add: Select assets from existing assets to join a group. Choose the parent group for the new group, enter the group name, click **OK**, and complete the creation of the new group.

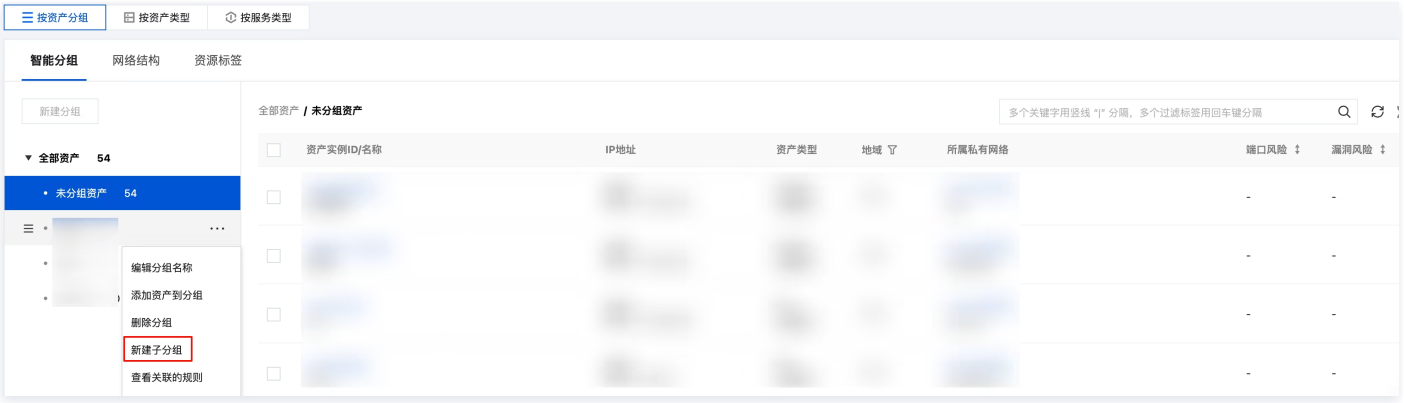
> **Notes:**
> Parent group is an already created group. Add the new group to the asset information under the parent group for layered management.

   - Import from parameter template: Select from existing parameter templates, recognize all IP addresses in the template as assets, and automatically add them to a group.

Notes:
After creating a group, changes to the parameter template will not be synchronized automatically to the group.

Method 2

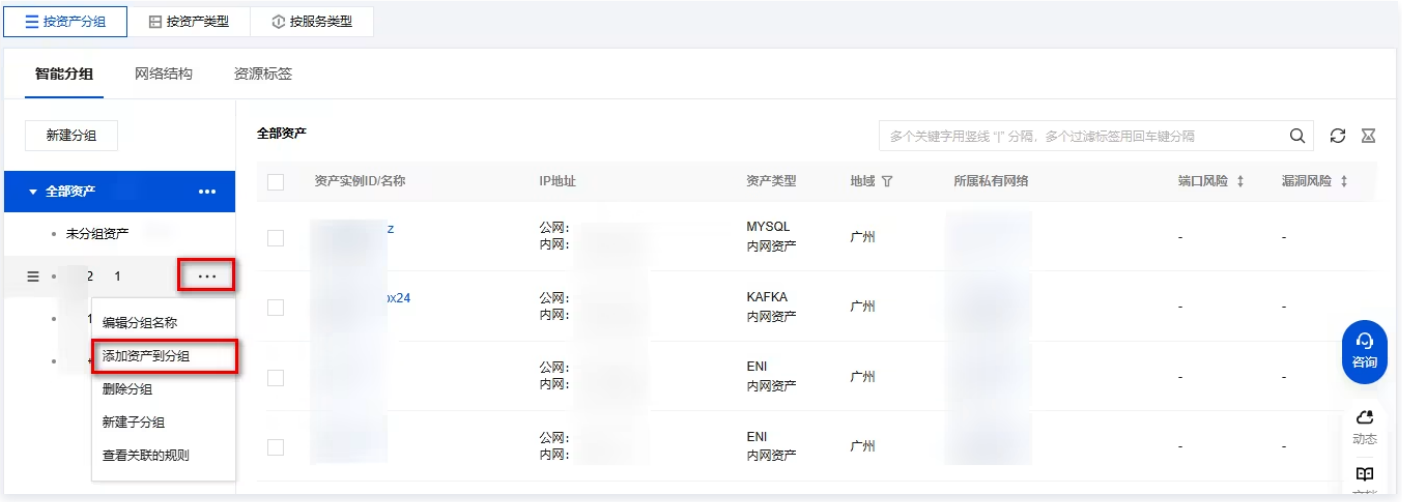
1. On the Asset Center > **Group by Asset** > **Intelligent Grouping** page, click the ... icon of the group, and select **Create New Sub-group** in the dropdown list.



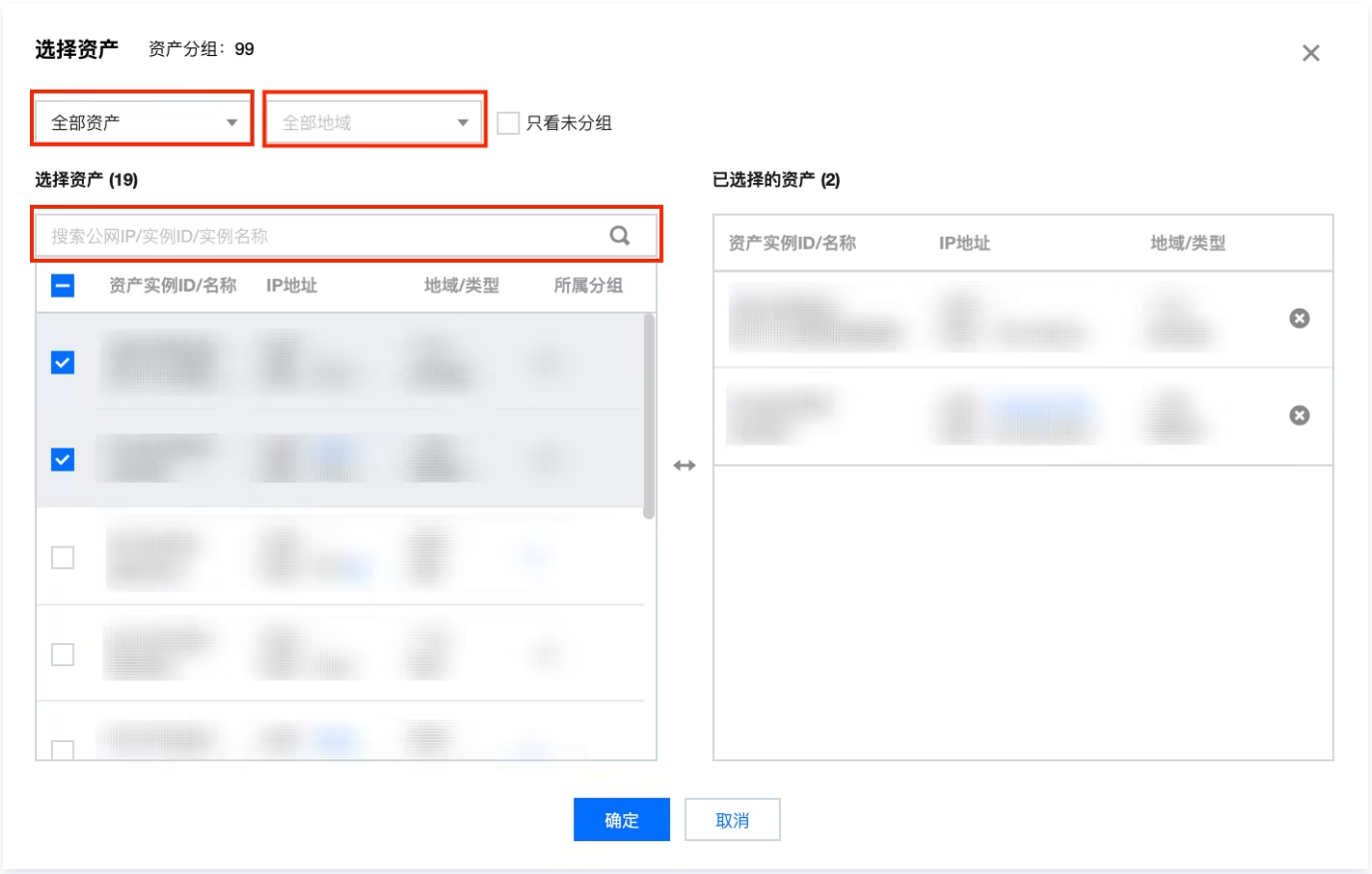
2. In the pop-up window, enter the sub-group name, click **OK**, and complete the creation.

Adding an Asset to a New Group

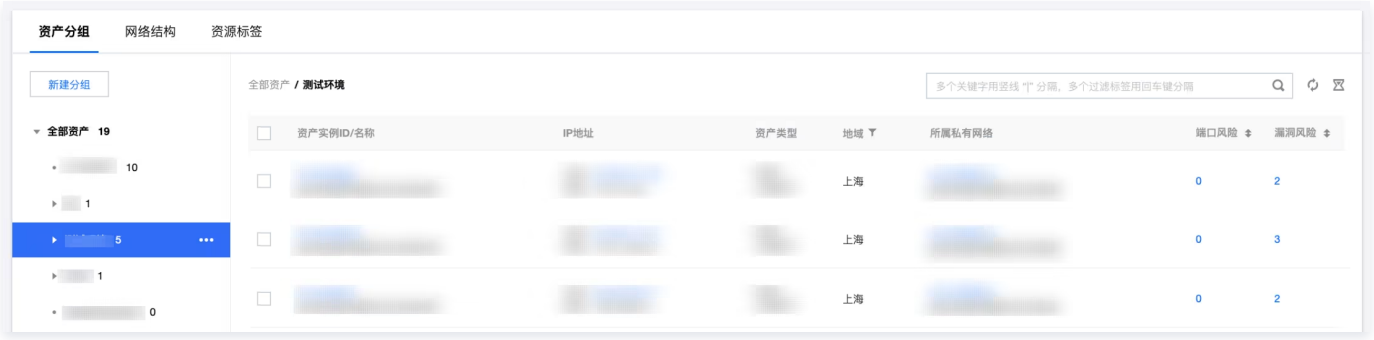
1. On the Asset Center > **Group by Assets** > **Intelligent Grouping** page, click the ... icon of the group and select **Add Assets to a Group** in the dropdown list.



2. In the select asset pop-up, filter assets by asset type, located area, and search for public IP/instance ID/instance name, then select the assets to join the new group.

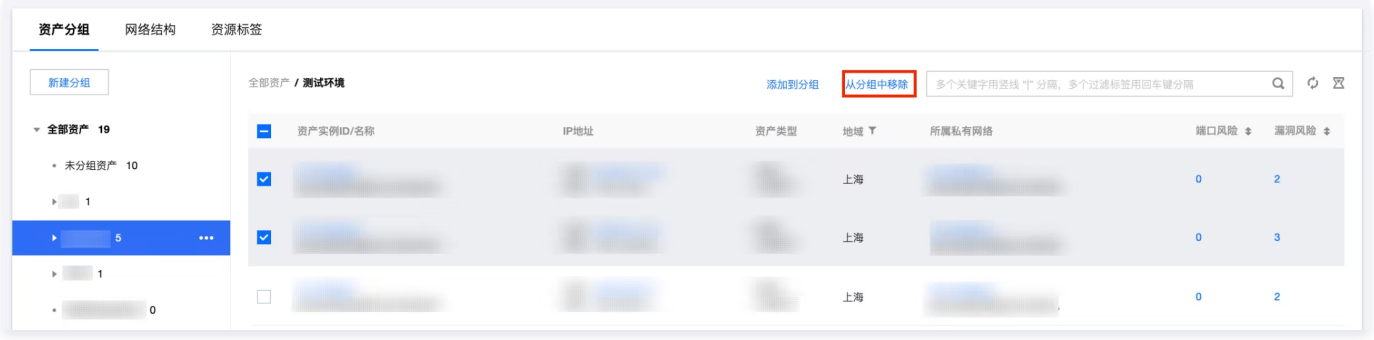


3. After adding assets, the list of assets added to this group appears on the right side of the asset list in this group.



Removing an Asset From a Group

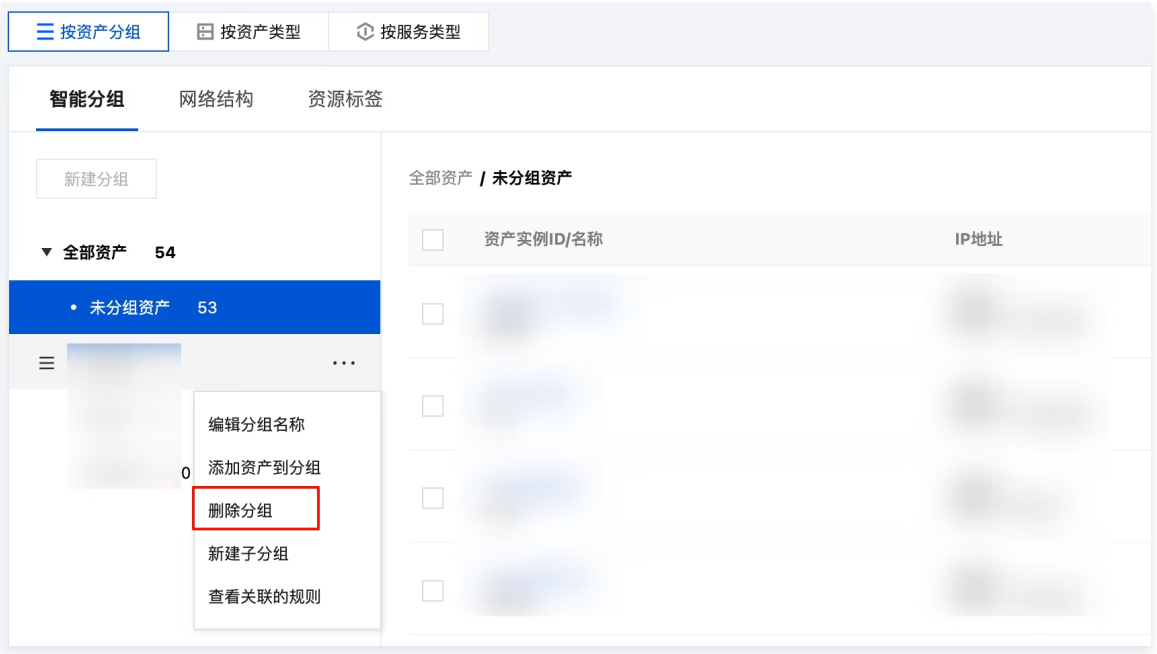
1. On the Asset Center > **Group by Asset** > **Intelligent Grouping** page, check the specified asset and click **Remove from Group**.



2. In the confirmation pop-up, click **Confirm** to complete the removal.

Deleting a Group

1. On the Asset Center > **Group by Asset** > **Intelligent Grouping** page, click the ... icon of the group, then click **Delete Group**.

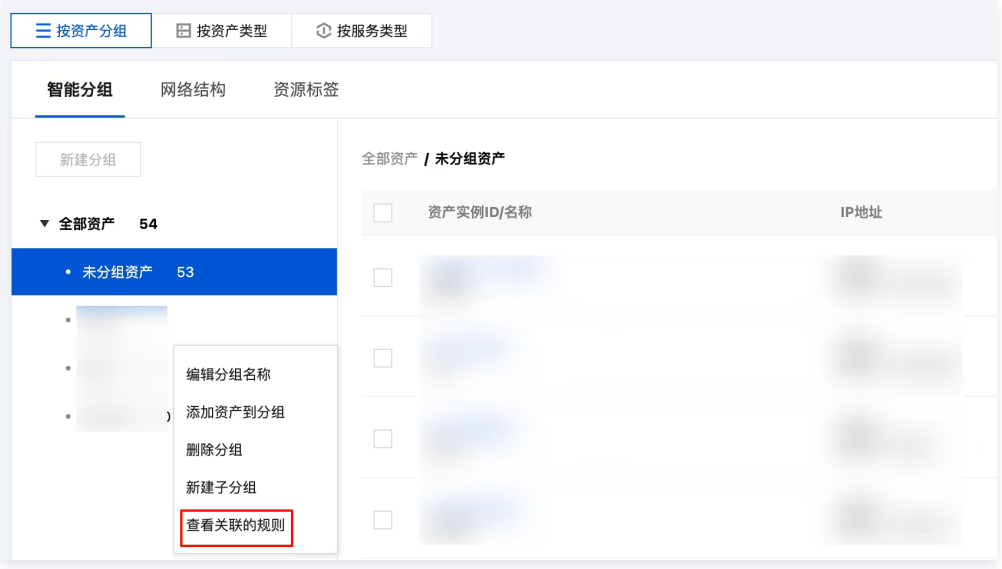


2. In the confirmation pop-up, click **OK** to delete the asset group.

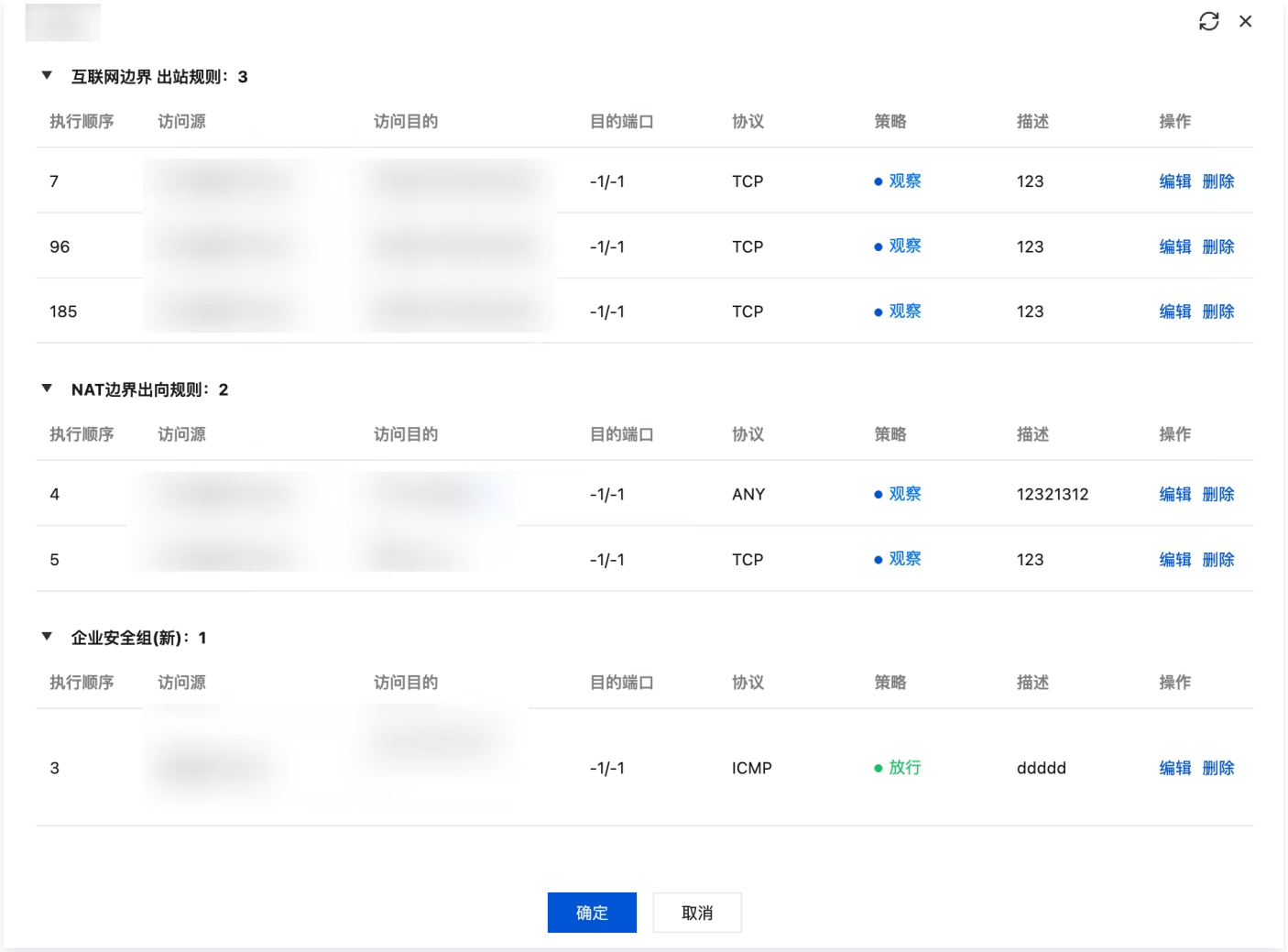
Notes:
If the current asset group is used for the configuration of security policies, it is non-deletable. Manually delete all rules before attempting the operation.

Viewing the Association Rules of a Group

1. On the Asset Center > **Group by Asset** > **Intelligent Grouping** page, click the ... icon of the group, then click **View Associated Rules**.



2. In the pop-up, you can view the rule list associated with this group, and directly perform rule editing and deletion operations in the pop-up.



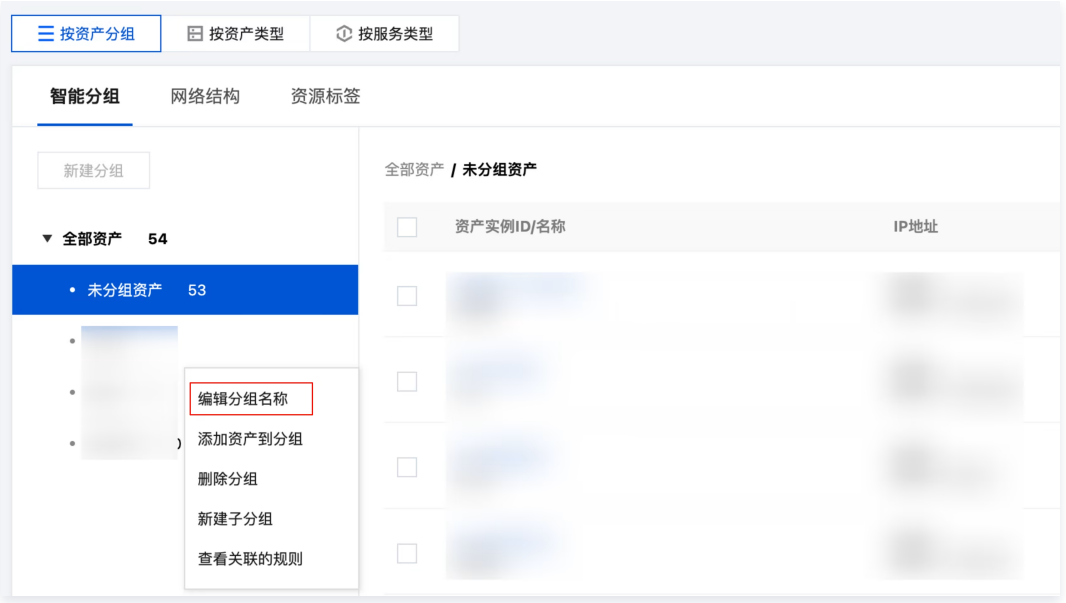
Adjust Group Position

Method 1: Manual Drag and Drop

1. On the Asset Center > **Group by Asset** > **Intelligent Grouping** page, select the group you want to adjust, click on the left ☰, and enter drag state.
2. Drag the group to the desired position and release it.

Method 2: Edit Group Name

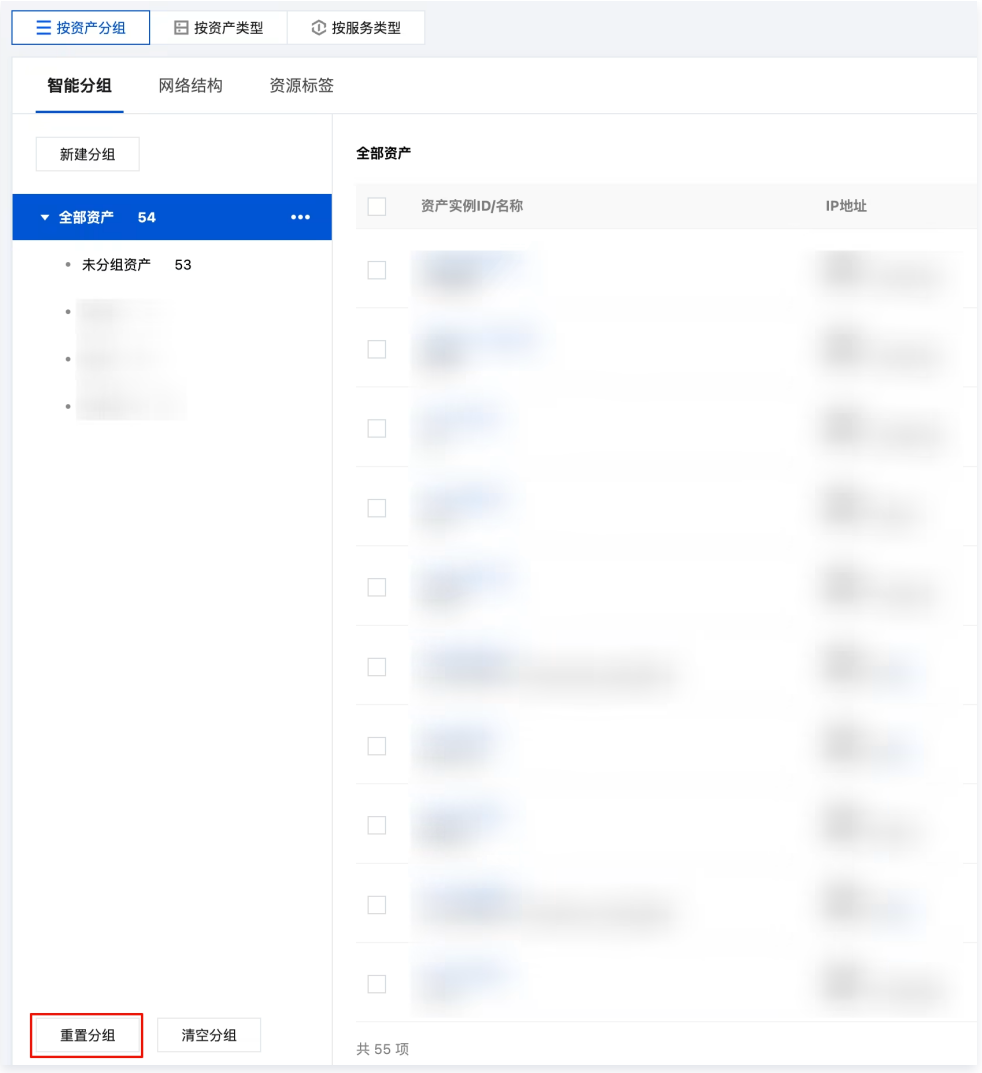
1. On the Asset Center > **Group by Asset** > **Intelligent Grouping** page, click the ... icon of the group, then click **Edit Group Name**.



2. In the edit asset group pop-up window, modify the parent group.
3. You can edit in the group name field, click **Confirm**, and finish editing.

Reset Groups

1. On the Asset Center > **Group by Asset** > **Intelligent Grouping** page, click **Reset Groups** at the bottom left of the page.



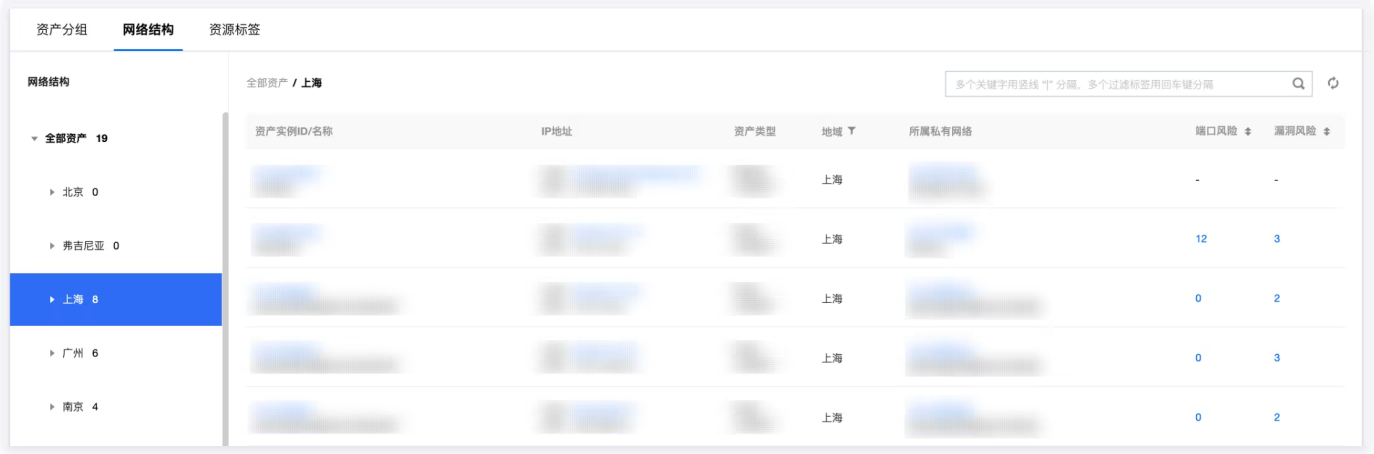
2. In the "Confirm Reset" pop-up window, click **Confirm**, wait for a duration, and the groups will be reset.

> **Note**
> Note: If the current asset group is used for the configuration of security policies, it is non-resettable. Manually delete all rules before attempting the operation.

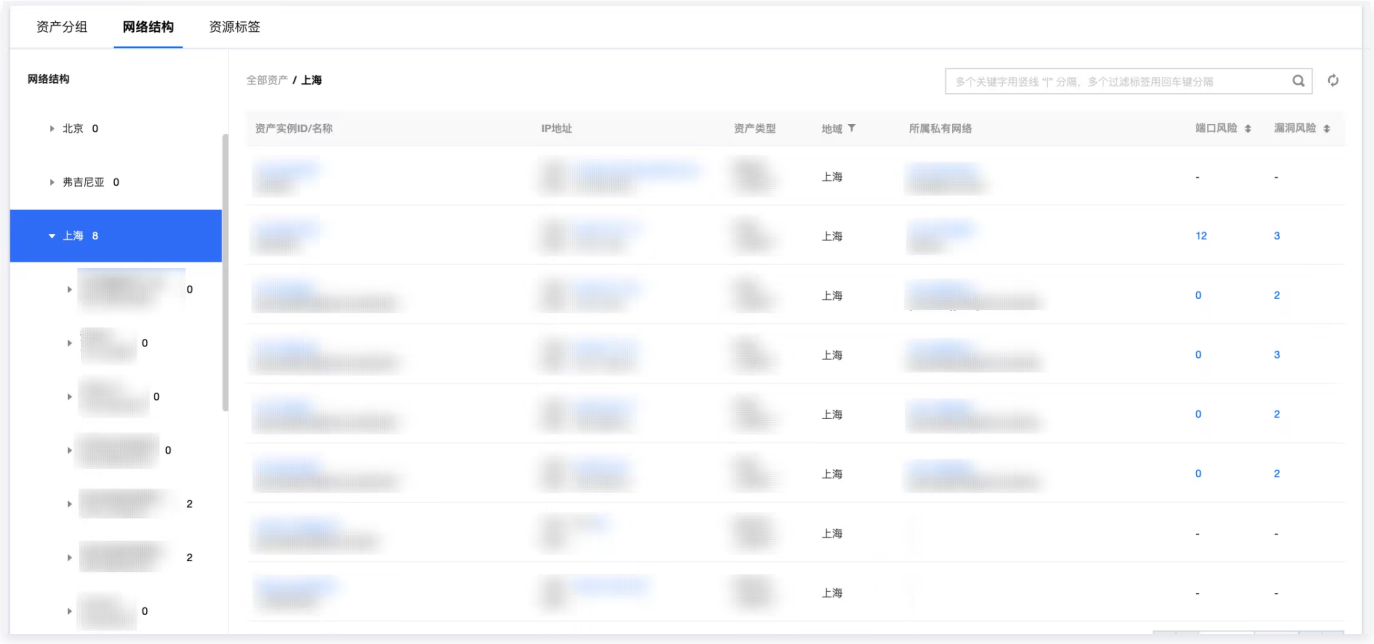
Network Structure

Network Structure page allows users to view assets in different regions. Currently supported regions include all domestic regions and some overseas regions.

1. On the Asset Center > **Group by Asset** > **Network Structure** page, click on the left **Region List** to view all asset information in that region.



2. Click ▸ on the left side of a single region to display all VPC information in that region, with the number of assets under each VPC shown after the VPC. Click **VPC name** to display the asset details under that VPC.



Resource Tag

The asset tag column supports managing assets via tags.

1. On the Asset Center > **By Asset Group** > **Resource Tag** page, click on the left **Tag List** to view all asset information under this tag.

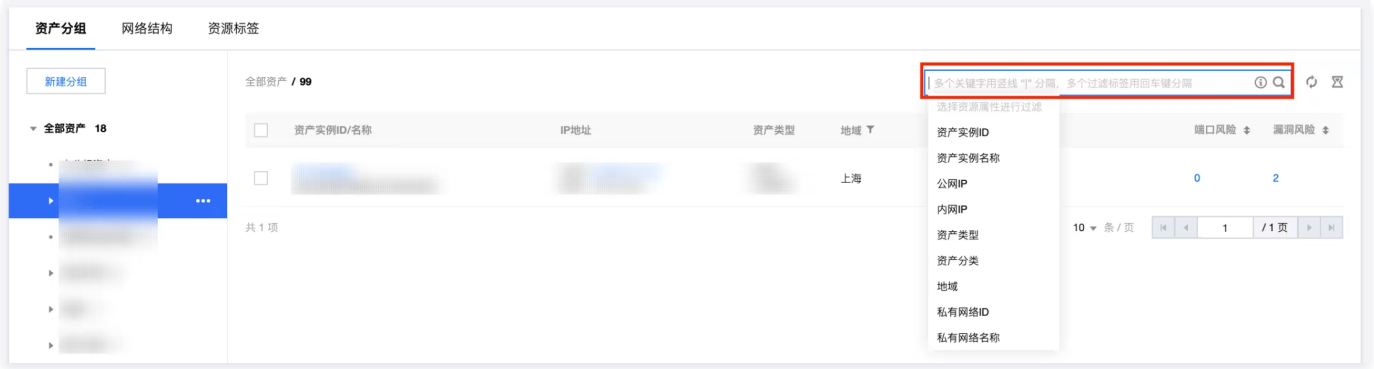
2. Click ▸ on the left side of a single tag key to display all tag value information under that tag key, with the number of assets under each tag value shown after the tag value. Click **tag value** to display the asset details under that tag value.

3. Click **asset name** to go to the asset details page. Click on the asset tag to edit the asset's tag information.

Filter and View Target Assets

1. Users can click on the region in the asset group instance list to perform region filtering of assets according to business needs.
2. Click **Port Risk** or **Vulnerability Risk** to sort assets in ascending or descending order.

3. Click **search box** to search for assets based on keywords.



Asset List

Last updated: 2025-05-20 10:51:52

Log in to the Cloud Firewall console. In the left sidebar, click **Asset Center** > **Asset List** to enter the Asset List Page. The Asset List shows detailed information of six different types of assets, including host assets, public IP assets, domain assets, network assets, and database asset types. See the table below for specific asset classifications.

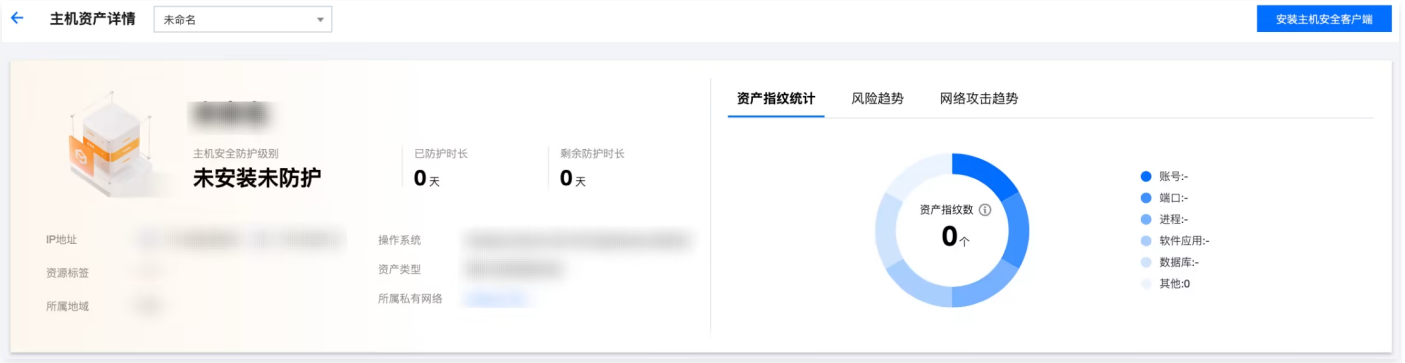
Asset Classification	Subcategory	Monitoring Item	Chinese Name
Host	-	CVM	Cloud Virtual Machine (CVM)
		LH	Lighthouse
		CPM	CBM
		ECM	Edge computing machine
		OTHER	Other
Public network IP address	-	HAVIP	HAVIP
		EIP	EIP
		IP	Public network IP address
Domain name	-	DOMAIN	Domain name
Network	Gateway	NAT	NAT Gateway
		VPN	VPN Gateway
	Network Card	ENI	ENI
	Virtual Private Cloud	VPC	Virtual Private Cloud
	Subnet	SUBNET	Subnet
Database	-	MYSQL	TencentDB for MYSQL
		REDIS	TencentDB for Redis
		MARIADB	TencentDB for MariaDB
		PostgreSQL	TencentDB for PostgreSQL
		MangoDB	TencentDB for MongoDB
Other	-	CLB	Cloud Load Balancer (CLB)
		NATFW	NAT Firewall
		PROBE	probe

View Asset Details

Asset Detail

1. In the asset list, click **target asset instance ID** to navigate to the details page of the asset.

2. Take host asset as an example. On the Host Asset Details Page, on the left side of the page, you can view the detailed information of the asset, including the asset instance name, protection status, IP, resource tag and other information. On the right side of the page, you can view the graphical information of the asset's fingerprint statistics, risk trend and network attack trends.



3. At the bottom of the page, you can view the risk management and network attack information of the host asset.

Asset Risk Management

> **Note**
> Untreated risk information is displayed by default.

Port Risk

1. For unprocessed port risks, click **block ports** in the Action column. It supports issuing Access Control Rules to intercept port access to the target. After blocking, the processing status of the risk is set to blocked.

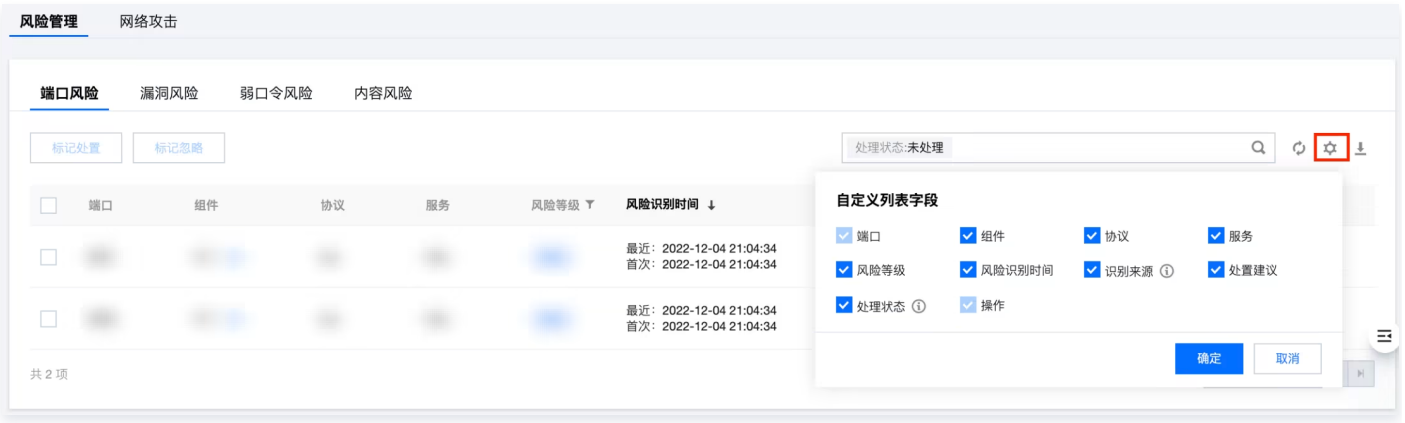
2. Risks after defense disposal can click **More** > **Tag Disposal** in the Action column, indicating that the risk has been processed and the processing status of the risk is set to Tagged as Processed.

> **Note**
> If this risk is still detected in the next scan task, the processing status will revert to unprocessed.

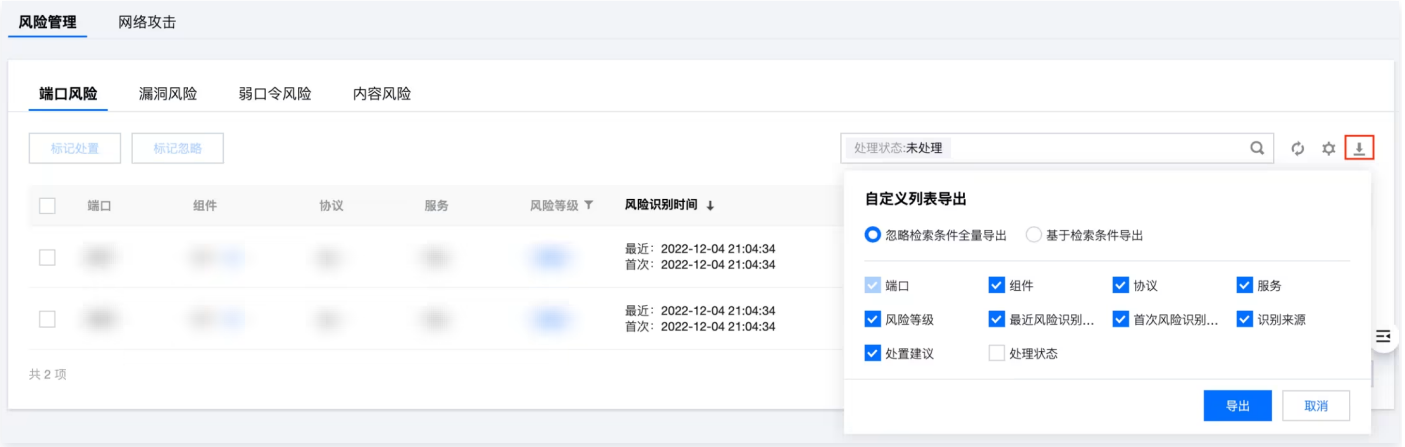
3. When a false positive risk occurs due to a false alarm during scanning or when the risk is considered ignorable, click **More** > **Mark as Ignored** in the Action column to ignore the risk. The risk will be filtered in subsequent scan tasks.

4. Tag disposal and ignoring support batch operations. Select multiple risks and click **Tag Disposal** or **Mark as Ignored** in the upper left corner.

5. Click the icon to customize fields in the Custom Risk List and display user-focused risk information.

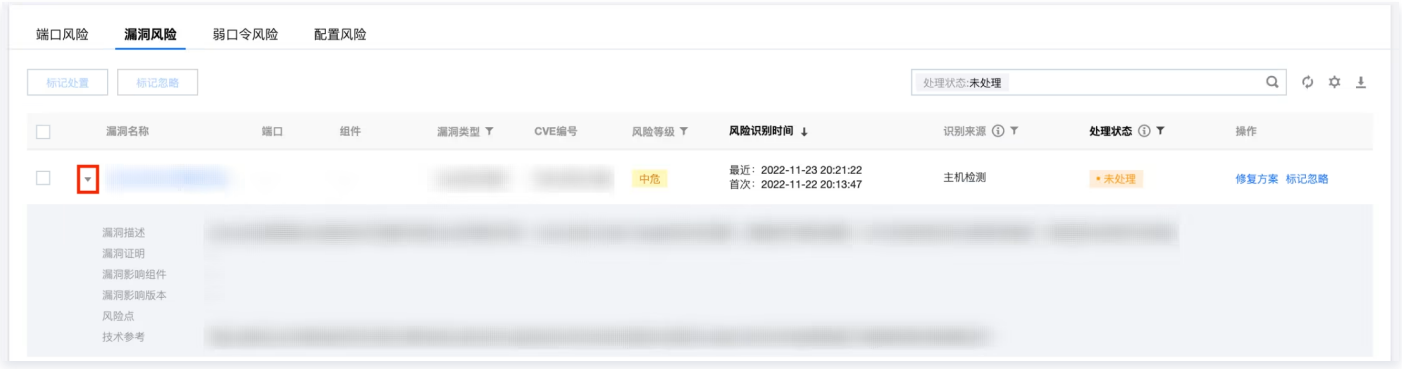


6. Click the icon to export the risk list. It supports custom export fields and retrieval conditions.



Vulnerability Risk

1. In the Vulnerability Risk tab, click to view specific details of vulnerabilities, including vulnerability descriptions.



2. For unaddressed vulnerability risks, click **Fixing solution** in the Action column. It supports viewing the vulnerability remediation plan provided by Tencent Threat Intelligence and the corresponding reference link.

3. Tag disposal and ignore operation, see Port risk.
4. Custom Risk List and export risk list operations, see Port risk.

Weak Password Risk

1. Weak password risks display corresponding weak password types and services. Users can perform tag disposal and ignore operations. See Port risk.
2. Custom Risk List and export risk list operations, see Port risk.

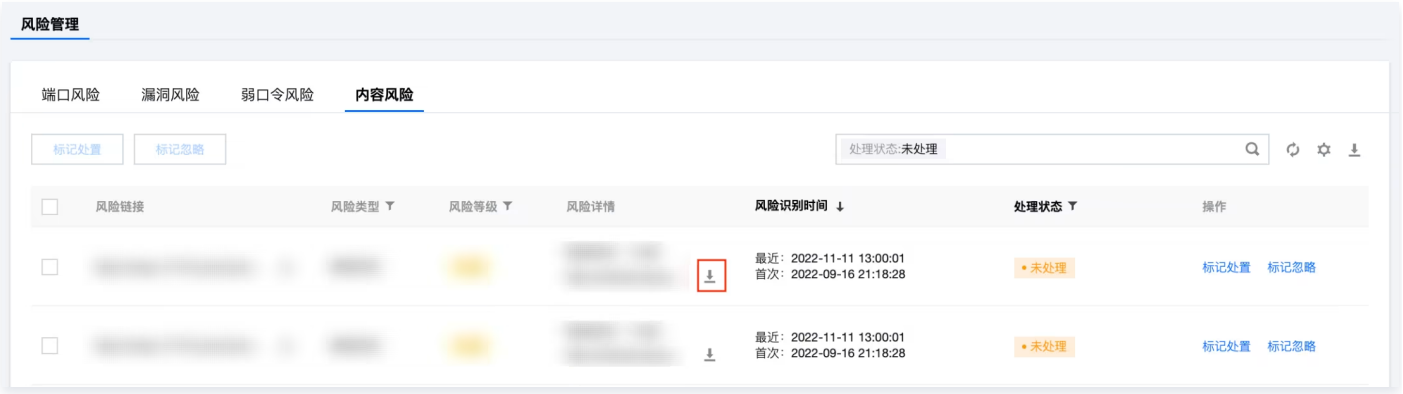
Configuration Risk

1. In the Configuration Risk tab, click ▸ to view detailed information about configuration risks, including risk descriptions.

2. Tag disposal and ignore operation, see Port risk.
3. Custom Risk List and export risk list operations, see Port risk.

Content Risk

1. Website content risks include three types: sensitive information, malicious code and hidden links, and web page tampering, as well as real-world risks where the website link is located. Click ⬇ in the Risk Details column to download and view the html source file content of the website.



> **Note**
> Risk types specific to public IP assets and domain assets, indicating the website content risk under that IP/domain.

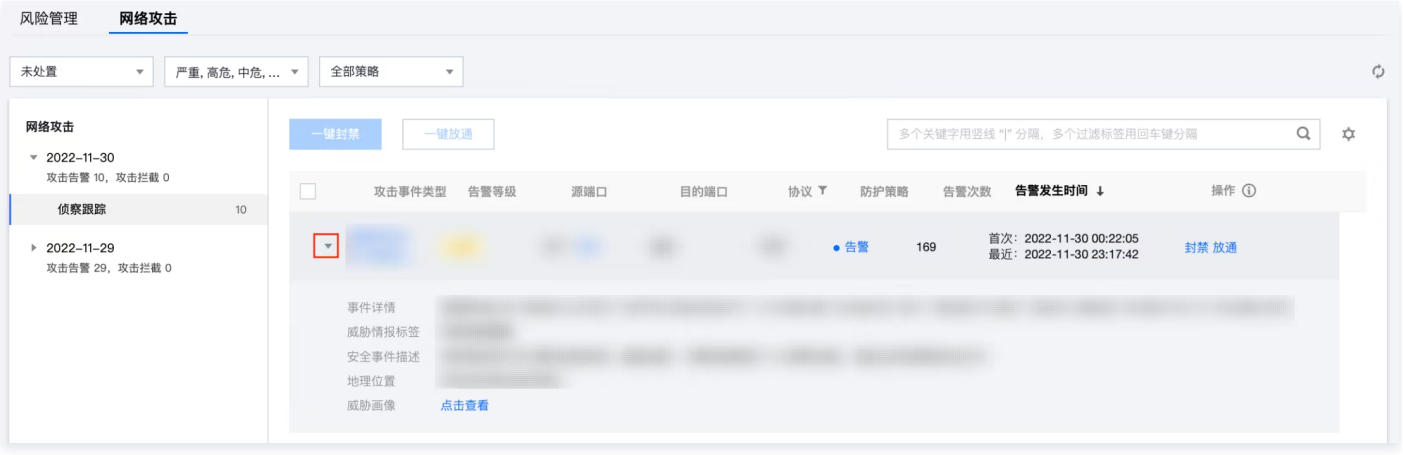
2. Tag disposal and ignore operation, see Port risk.
3. Custom Risk List and export risk list operations, see Port risk.

Asset Network Attack

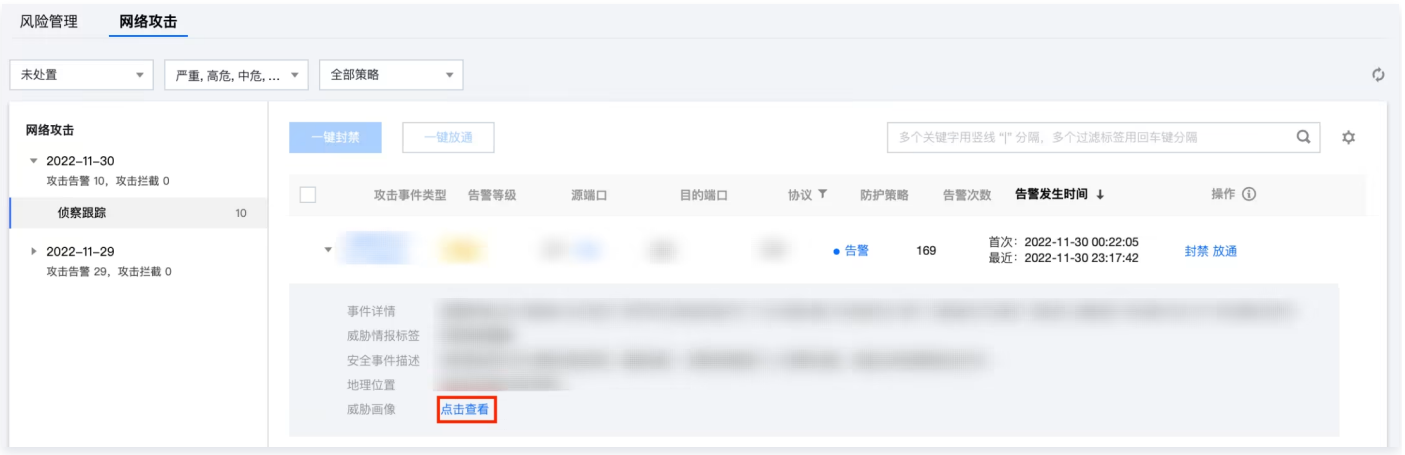
The network attack alerts and interception events of this asset are recorded in chronological order.

1. Users can filter network attack events based on ①**Incident response status (pending by default)**, ②**Alarm level**, ③**Execution policy**, ④**Search box** keywords.

2. Select a specific event and click ▸ to view event details, including event description, TI Tags, etc.



3. 1. Click **Threat Profiling** > **click to view** to view the threat profile information of the attack IP.



4. Support one-click blocking of related IPs of attack events. Click **Block at** ① to intercept a single IP's access to all assets. Select multiple events and click **One-click ban at** ② to block the selected multiple IPs.

5. For potential duplications or misreportings in events, support one-click release for related IPs. Click **Release at** ① to allow the traffic of a single IP. Select multiple events and click **One-click release at** ② to allow the traffic of the selected multiple IPs.

> **Description**
> For operations on blocking and allowing attack IPs, for more information, see alert center document.

6. Click the ⚙ icon to customize fields in the custom event list and display information on focused events.

Host Asset

Host Assets Statistics Overview

1. View the statistical overview of assets. The left side of the page includes the count of host assets, unprotected hosts, risk hosts, public network hosts, and private network hosts. Click **digit**. At the bottom of the page, you can filter the corresponding host asset list for users to view asset details.
2. Users can view the TOP 5 assets of network attack alerts, blocked attacks, exposed ports, and exposed vulnerability statistics within the corresponding time period on the right side of the page.

> **Note**
> Exposed ports and exposure of vulnerability data need to be generated according to scanning results after asset scanning is completed.

View Host Asset List

1. Users can filter corresponding assets by keywords in **①protection status, ②risk status, ③creation time, ④search bar** at the bottom of the page.

Description

The protection status refers to the protection status under the Cloud Workload Protection Platform (CWPP). If the CWP client is not installed, click **Install now** in the Action column to install the CWP client. If the CWP client is installed, click **Protection detail** in the Action column to enter the CWP console and view the protection detail.

2. Click icon to filter corresponding asset information, including IP, asset type, region, and associated VPC.

3. Click the icon to perform asset sorting on corresponding information, including inbound/outbound peak bandwidth, network attacks, exposed ports, exposed vulnerabilities, configuration risks, malicious outgoing requests, scan tasks, and time.

Note

Exposed ports, exposed vulnerabilities, and configuration risk data need to be displayed according to scanning results after asset scanning is completed.

4. Click icon to support user-defined asset list content.

5. Click icon to export asset list. It supports custom list content and search criteria.

Public IP Assets

Statistical Overview of Public IP Assets

1. View the statistical overview of assets. The left side of the page includes public IP assets, unprotected public IPs, risk public IPs, bound CVM assets, bound CLB assets, and bound NAT assets. Click **digit**. At the bottom of the page, you can filter the corresponding public IP asset list for users to view asset details.
2. Users can view the TOP 5 assets of inbound/outbound peak bandwidth, inbound/outbound cumulative traffic, network attack alerts, blocked attacks, exposed ports, and exposed vulnerability statistics within the corresponding time period on the right side of the page.

> **Note:**
> Exposed ports and exposure of vulnerability data need to be generated according to scanning results after asset scanning is completed.

View Public IP Asset List

1. Users can filter corresponding assets by keywords in ①**protection status,** ②**risk status,** ③**creation time,** ④**search bar** at the bottom of the page.

Description

The protection status indicates whether to use CFW for related protection. It includes three corresponding statuses: defended, unprotected, and unknown. If the user has not enabled CFW, click **Enable Protection** in the Action column to turn on the internet boundary firewall switch and provide protection for the access traffic of this public IP asset. If the user has enabled the firewall switch, click **Protection Detail** in the Action column to navigate to the Intrusion Prevention System (IPS) and view the firewall protection mode.

2. Click icon to filter corresponding asset information, including public IP type, asset ownership, and region.

3. Click icon to perform asset sorting for corresponding information, including inbound/outbound peak bandwidth, network access, network attack, port risk, vulnerability risk, weak password risk, content risk, and time.

Note

Exposed ports, exposed vulnerabilities, weak password risks, and content risk data need to be displayed according to scanning results after asset scanning is completed.

4. Customize asset list content and export asset list information. Refer to host asset.

Domain Assets

Domain Name Assets Statistical Overview

1. View the general overview of asset statistics. The left side of the page includes domain assets, unprotected domain assets, risk domain assets, assets bound to CVM, and assets bound to CLB. Click **digit**. At the bottom of the page, you can filter the corresponding domain asset list for users to view asset details.
2. Users can view the TOP 5 assets of the number of network accesses, BOT access count, network attack alerts, attack interceptions, exposed ports, and exposed vulnerability statistics within the corresponding time period on the right side of the page.

> **Note**
> Exposed ports and exposure of vulnerability data need to be generated according to scanning results after asset scanning is completed.

View Domain Asset List

1. Users can filter corresponding assets by keywords in ①**protection status,** ②**risk status,** ③**creation time,** ④**search bar** at the bottom of the page.

> **Note**
> The protection status indicates whether to use the Web Application Firewall (WAF) product for protection, including online and offline statuses. If the user has not enabled WAF protection, click **Enable Protection** in the Action column to enable WAF for the access traffic of domain assets. If the user has enabled WAF protection, click **Protection Detail** in the Action column to navigate to the web application firewall to view the protection details.

2. Click icon to filter corresponding asset information, including asset ownership, region, and type of the associated instance.

3. Click icon to perform asset sorting for corresponding information, including network access, BOT access, network attack, port risk, vulnerability risk, weak password risk, content risk, and scan task.

> **Note**
> Exposed ports, exposed vulnerabilities, weak password risks, and content risk data need to be displayed according to scanning results after asset scanning is completed.

4. Customize asset list content and export asset list information. See host asset.

Network Asset

Network Assets Statistical Overview

1. View the general overview of asset statistics. The left side of the page includes network assets, gateway assets, network interface card assets, private networks, and subnets. Click **digit**. At the bottom of the page, you can filter the corresponding domain asset list for users to view asset details.
2. Users can view the TOP 5 assets of asset type distribution information, inbound/outbound peak bandwidth, inbound/outbound cumulative traffic, network attack alerts, blocked attacks, exposed ports, and exposed vulnerability statistics within the corresponding time period on the right side of the page.

> **Note**
> Exposed ports and exposure of vulnerability data need to be generated according to scanning results after asset scanning is completed.

View Network Asset List

1. Network assets are divided into four types: gateway, network interface card, private network, and subnet. Corresponding assets can be filtered based on ①**risk status,** ②**creation time,** ③**search box** keywords.

> **Note**
> The risk status needs to filter the risk information after asset scanning. VPC assets do not support asset scanning.

2. Click icon to filter corresponding asset information, such as IP, asset type, region, etc.
3. Click icon to perform asset sorting for corresponding information, such as network attack, port risk, etc.

> **Note**
> Risk data need to be displayed according to scanning results after asset scanning is completed.

4. Customize asset list content and export asset list information. See host asset.

Database Assets

Database Asset Statistics Overview

1. View the general overview of asset statistics. The left side of the page includes database assets, unprotected databases, and risk databases. Click **digit**. At the bottom of the page, you can filter the corresponding domain asset list for users to view asset details.

2. Users can view the asset type distribution information and the TOP 5 assets of database access volume statistics within the corresponding time period on the right side of the page.

> **Note**
> Risk data need to be generated according to scanning results after asset scanning is completed.

View Database Asset List

1. Users can filter corresponding assets based on ①**risk status,** ②**creation time,** ③**search box** keywords.

2. Click **Access Domain Management** to go to **Zero Trust Protection** > **Access Domain Name Management**. You can access domain names for database assets and use wechat to scan qr code login functionality to perform asset protection.
3. Click the icon to filter the corresponding asset information, including asset type, region, and associated VPC.

4. Click the icon to perform asset sorting on the corresponding information, including network access, network attack, configuration risk, and scan task.

Note

Risk data need to be displayed according to scanning results after asset scanning is completed.

5. Customize asset list content and export asset list information. See host asset.

Service Sorting

Last updated: 2025-05-28 10:19:34

The Service Sorting page displays the detailed information of Web services.

1. Log in to the CFW console, in the left sidebar, click **Asset Center** > **Service Sorting**.
2. View Web services asset statistical overview. The left side of the page includes the number of Web services, unprotected Web services, and risk Web services. Click **the number**, and at the bottom of the page, you can filter the corresponding Web services asset list for users to view asset details.
3. On the right side of the statistical overview page, you can view the TOP5 assets of Web service traffic and network attack statistics within the corresponding time period.

4. Users can filter corresponding assets at the bottom of the page based on **①protection status, ②risk status, ③creation time, ④search bar** keywords.

> **Notes:**
> Protection status refers to the protection status under the Web application firewall and cloud firewall products.

5. If the user's Web service assets are unprotected, click **Enable Protection** in the Action column, select Connection Protection in the dropdown list, including Web application firewall and cloud firewall, and enter the corresponding product console to perform Web service protection.

6. Click the icon to filter corresponding asset information, including protocol, service type, and region.

7. Click the icon to sort corresponding information by asset, including network access, BOT access, network attack, weak password risk, and content risk. Click the blue **corresponding numbers** to navigate to the corresponding asset flow and asset risk pages.

Notes:
Risk data needs to be displayed based on scan results after asset scanning is completed.

Alert Center Overview

Last updated: 2025-05-20 10:52:30

The alert center collects statistics on network attacks and risk events detected by the intrusion prevention system and network honeypot module. Understand the firewall protection status, thereby giving a timely warning. Support blocking dangerous access sources. According to the actions performed by the firewall, it is divided into attack alert summary, attack interception statistics, and attack deception events.

- Attack alerts summary: all detected cyber attacks and risk events of observation types (users are advised to manually block/release/isolate/ignore the attack IPs).
- Attack interception statistics: contain network attacks and risk events with detected threats and automatically blocked (used for subsequent audit and troubleshooting).
- Attack deception events: contain network attacks and risk events of all detected exposed probes and honeypots (block or pass can be set manually).

Version Support Notes

All versions of CFW support the alert center functionality. For billing details, see Billing Overview.

References

- View and handle alarm events
- View and handle interception events
- Deception event viewing and handling

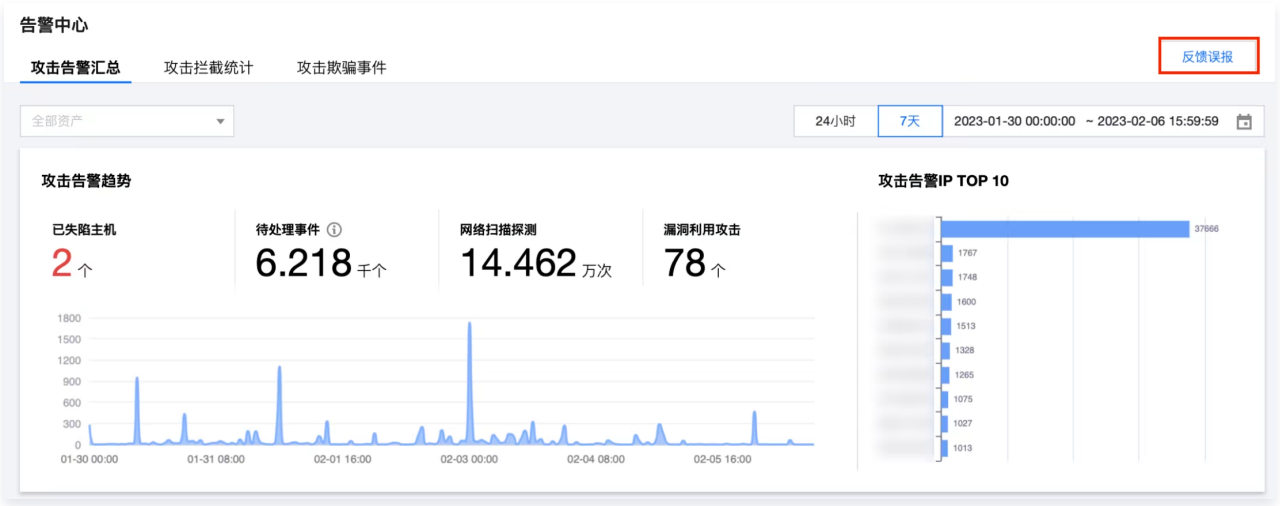
False Alarm Feedback

Last updated: 2025-05-20 10:52:48

When a false alarm occurs in the rule alarm information, users can report false alarms through the false alarm feedback entry in the alert center, thereby submitting feedback from the alarm information in a timely manner.

Method One

1. When a false alarm is detected in the alarm information, click **Submit False Alarm** to submit the false positive information.



2. On the false positive feedback page, select the feedback type and fill in the corresponding false positive information, including:
   2.1 IP/domain name: Enter the false positive IP address or domain name as well as the false positive description.
   2.2 Intrusion prevention rules: Enter the rule ID of the false positive as well as the false positive description.

> **Note:**
> You can view the matched rule details in the event details of the Alarm event, thereby quickly obtaining the rule ID corresponding to the false positive incident.

3. Click **Submit Feedback** to complete the false positive feedback. The false positive feedback records will be displayed at the bottom of the page. The CFW staff will complete the assessment and feedback the processing results within 3 working days.

Method 2

1. When a false alarm is detected in the alarm information, click **Allow** in the action bar to add the false positive IP address to the allowlist of the Intrusion Defense module.

2. Select the reason for releasing as **false positive** in the pop-up, and choose to report the false-positive address/rule. Fill in the false-positive description below, and click **OK** to successfully submit the feedback.

3. The false positive feedback records will be displayed at the bottom of the page. The CFW staff will complete the assessment and feedback the processing results within 3 working days.

Viewing and Handling Alarm Events

Last updated: 2025-05-20 10:53:10

Attack Alert Summary Visualization

Through the visual summary of alarm information, it is easy to perform statistical analysis and operation disposal on the attack events detected by the firewall. Statistical data is updated every 20 minutes.

1. Log in to the CFW console. In the left sidebar, click **Alert Center** > **Attack Alert Summary**.
2. On the attack alert summary page, perform visual analysis on existing security alarm events according to ①**personal assets** and ②**time**.
   a. On the left side of the page is the trend curve of recent security incidents after filtering, showing the number of alarms at different times. And it shows the statistical data of the number of times of compromised hosts, pending events, network scan detections and vulnerability exploitation attacks.
   b. On the right side of the page, the top 10 attack alerts by IP are displayed to provide reference for advance avoidance of Risk IP Attacks.

Quickly Locate Alarm Events

Provide multiple filtering functions, support quick filtering and localization of existing attack alert events.
In the event list of Attack Alert Summary Page, existing attack alert events can be located based on ①**Alarm Event Type**, ②**Conditional Filtering**, and ③**Custom Table Header**.

- Alarm event type: click the button in figure ① to view the alert information details under different categories.

> **Note:**
> The corresponding security event types will be displayed after configuring the required security policies for CFW in the Access Control, Intrusion Defense, and Security Baseline module configurations.

- Conditional filtering: click the button in figure ② to perform conditional filtering on attack alert events.

- Support viewing pending, blocked, allowed, ignored alarm information.
- Support filtering based on alert danger level.
- Support filtering by security event type, protocol, and judgment source.
- Support directly clicking the icon to filter the source IP or destination IP.
- Support sorting and viewing by occurrence time and number of alarms.
- Support keyword search filtering. Include access source, source port, access destination, destination port, danger level, protocol, and judgment source.
- Custom table header: Click the icon in figure ③ to define header fields. You can select up to 10.

View and Locate Event Details

After locating a specific attack alert event, click on the left side of the event to view its detailed information.

Note:
To use the deep detection functionality of host security, you need to purchase Cloud Workload Protection Platform.

- Threat profile: click **click to view** to view the threat profile of this access source. Include IP geo location, whether it belongs to a threat intelligence IP, network information, reverse-check domain information, etc.
- Asset detail: click **click to view**, navigate to **asset center**, view attacked asset details.

Resolve Alert Information Rapidly

Handling a Single Alarm Information

On the Attack Alert Summary Page, you can handle individual alarm information. In the event operation bar, you can perform **block**, **allowlist**, **ignore**, and **isolate** operations on the access source.

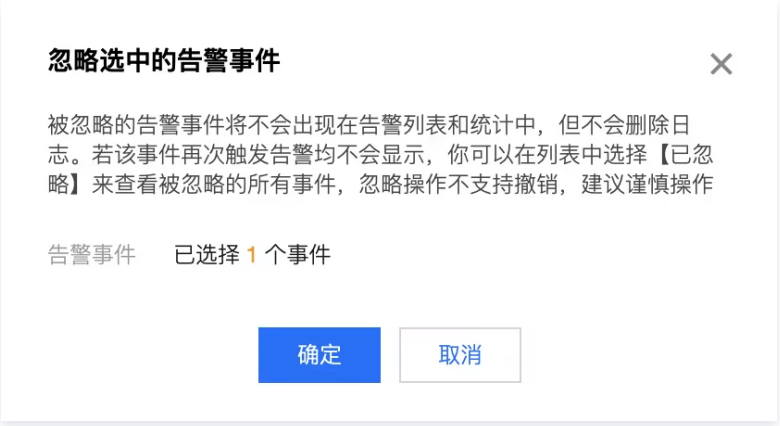
> **Note:**
> The isolation operation is only targeting outbound traffic alert events and isolating compromised hosts to prevent further impact.

- Ban: For security events with a relatively high danger level or a large number of alarms, you can click **Ban** to add the IP address to the blocklist (blocklist) of the Intrusion Defense module, and select the blocking duration, add remarks. CFW will automatically block the IP address from accessing all assets of users within the specified time range.

> **Note:**
> When the alarm IP address may come from the intelligence allowlist, a prompt message will appear. Do not manually block/prohibit. Enable intrusion prevention interception mode. CFW will automatically block attack traffic originating from this address and allow normal traffic.

- Bypass: For repeated or possible false alarms in alarms, you can click **Bypass** to add the IP address to the allowlist (whitelist) of the Intrusion Prevention module, and select the bypass time and bypass reason, and enter remarks. If it is confirmed as a false alarm, you can submit a ticket for feedback on the false alarm content. The cloud firewall will bypass the detection of the intrusion prevention module for the IP address within a certain time range, thereby allowing the traffic of the IP address.

- Ignore: If you don't want to handle alarm information, you can click **Ignore**. The log will not disappear, but you can view the records in the handling status ignored list.



- Isolation: Select the traffic direction and effective time for blocking, click **Isolate**. Asset instance isolation will automatically distribute enterprise security group blocking rules to intercept network access in the specified direction of selected assets within the time range.

Note:
After isolating asset instances, you can use the operation and maintenance allowlist to access assets. You can choose to manually fill in IP or use zero trust protection.
- Only 10 IPs can be manually filled in.
- Zero trust protection supports selecting WeChat or Enterprise WeChat users to allow asset access. How to integrate WeChat or Enterprise WeChat users, please see enterprise security group.

Batch Disposition of Alarm Information

On the Attack Alert Summary Page, you can handle multiple alarm messages. You can select multiple alarm messages and click **one-click interception**, **allowlist**, **isolate**, or **ignore**.

Note:
- The isolation operation is only targeting outbound traffic alert events and isolating compromised hosts to prevent further impact. Mainly for host compromise type alert events, there are isolation operations.
- Users need to perform a modification operation. They can remove the IP in **Intrusion defense** > **blocklist**, **allowlist** or **isolation list** for recovery operations.
- Alarms exceeding 7 days will become invalid and cannot be processed.

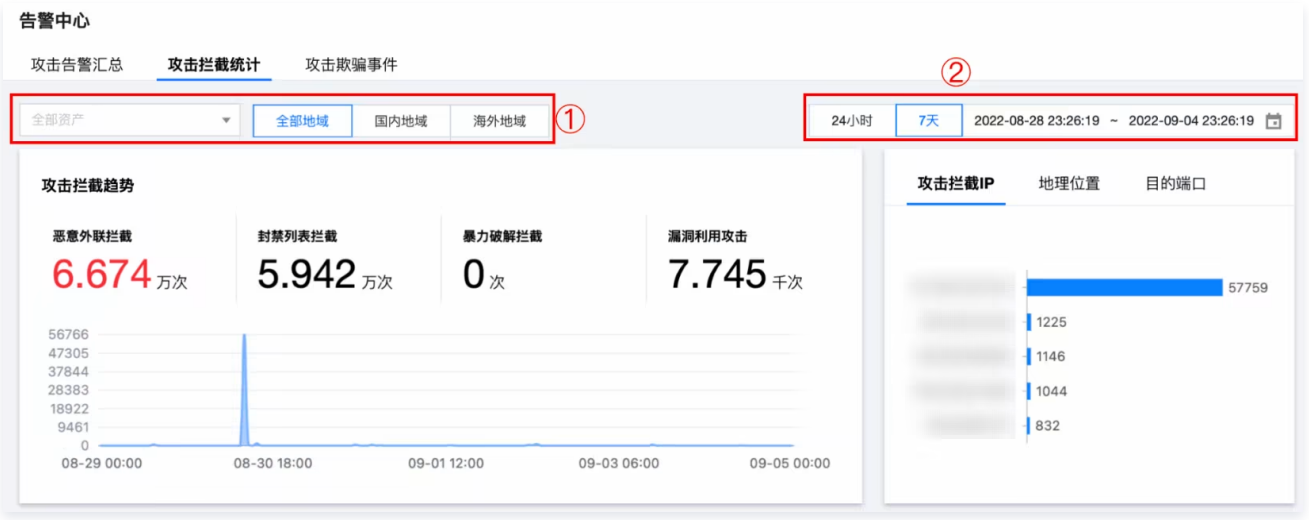
Interception Event View and Handling

Last updated: 2025-05-20 10:53:30

The attack interception statistics module integrates the interception records of the firewall based on all set rules and TI. It can help perform statistical analysis and handling of all intercepted events. Stats are updated every 20 minutes.

Interception Statistics Visualization

1. Log in to the CFW console. In the left sidebar, click **alert center** > **attack interception statistics**.
2. On the attack interception statistics page, you can visualize and analyze existing security alarm events based on ①**personal assets and their regions**, ②**time**.
   2.1 On the left side of the page is the trend curve of the number of filtered recent blocking and interception events, showing the number of interceptions at different times. And it shows the statistics of malicious outgoing access, blocklist interception, blocked brute-force attacks, and vulnerability exploitation attacks.
   2.2 On the right side of the page, based on attack interception IPs, geographical locations, and destination ports, you can view the Interception Event Quantity Ranking.



Quick Location of Interception Information

Provide multiple filtering functions, support quick filtering and localization of existing attack interception information.

1. In the event list of the Attack Interception Statistics Page, two perspectives are provided to display interception information. Click **Asset Perspective** or **Event Perspective** in the figure to switch the perspective.
   1.1 The asset perspective displays interception events with the same access source consolidated and counted from the attacker assets' perspective.
   1.2 The event perspective displays interception events one by one from the perspective of independent interception events.

Note:

> Take the asset perspective as an example. For the event perspective, please refer to the Quickly Locate Alarm Events page.

2. Locate existing attack interception events according to ①**traffic direction** and ②**conditional filtering**.

- Traffic direction: Click the button at position ① in figure to view specific details of interception information under different traffic directions. Including inbound, lateral movement, outbound.
- Conditional filtering: Click the icon at position ② in figure to perform conditional filtering on attack alert events.
  - Supports displaying based on intrusion defense policy, handling status.
  - Supports sorting based on interception time, interception statistics, average blocking frequency.
  - Supports frequency statistics in minutes, hours, days.
  - Supports keyword search filtering. Including access source, access destination, destination port, geographical location.

View Location Information Details

View the information details of the interception information directly in the event list on the attack interception statistics page.

> **Note:**
> Take the asset perspective as an example. For the event perspective, see the View and Locate Event Details page.

- click **access source** to view the threat profile of this access source. including IP geo location, whether it belongs to threat intelligence IP, network information, reverse-check domain information, etc.
- Click **asset name** to navigate to the asset center and view attacked asset details.

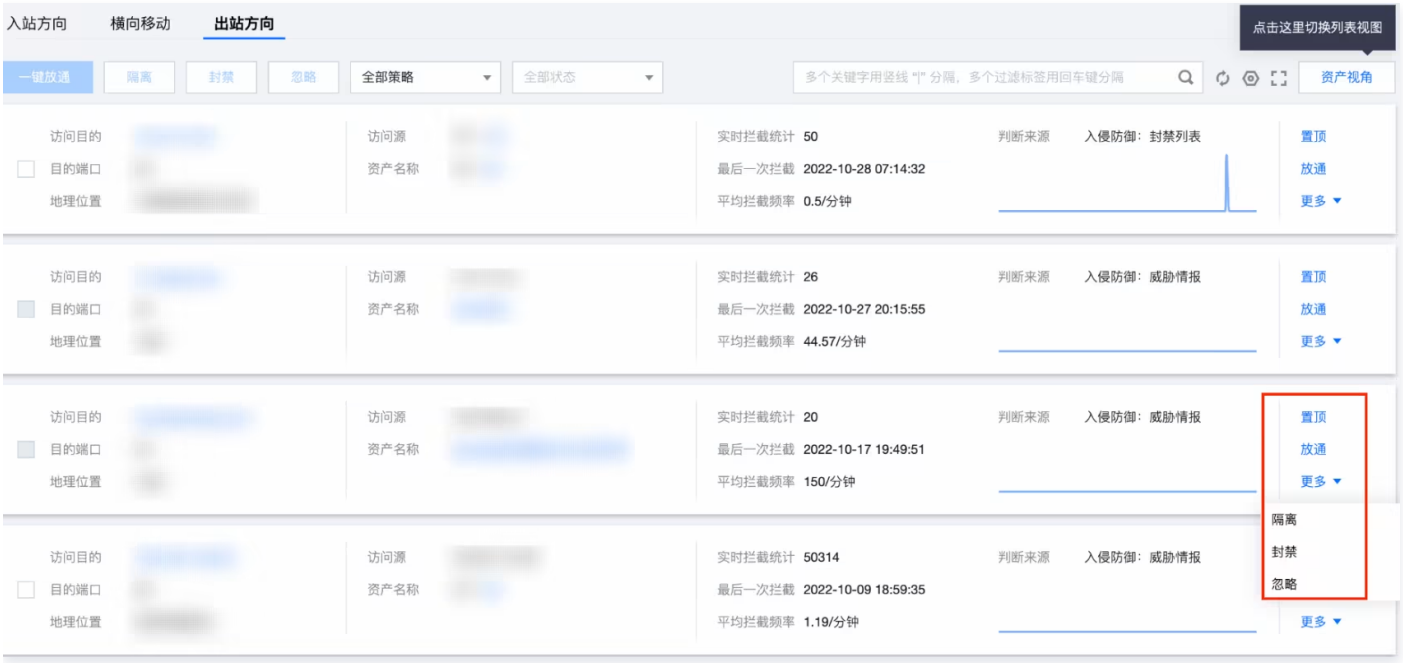
Quick Disposal of Interception Information

> **Note:**
> Take the asset perspective as an example. For the event perspective, refer to the Rapidly Process Alert Information page.

Handle a Single Interception Information

On the attack interception statistics page, you can handle individual interception information. In the right panel of the event, perform **pin to top**, **block**, **release**, **ignore**, **isolate** operations.

> **Note:**
> - Since the states of assets vary, the operable buttons on the right also differ. The isolation operation is only targeting lateral movement and intercepting outbound events, isolating compromised hosts to prevent further expansion of the impact.
> - The following operations are applicable to both batch processing and operations from the event perspective.

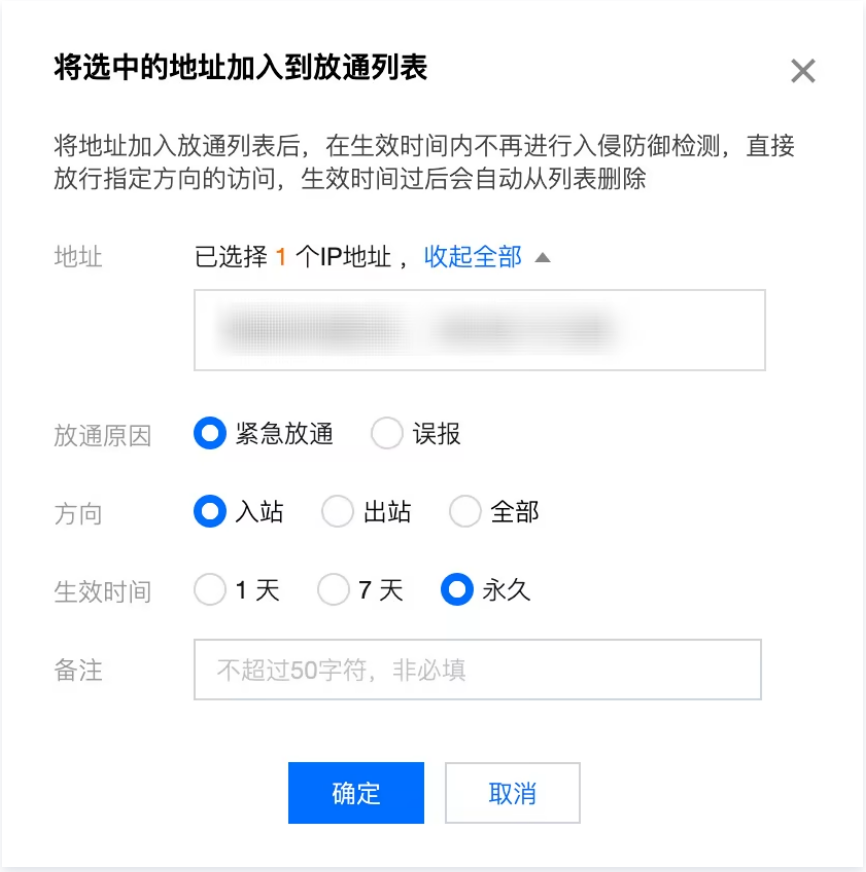


- Pin to top: Under the asset perspective, for risk assets that have interception events, you can pin them to the top with one click to facilitate user attention to the real-time interception situation of the assets.

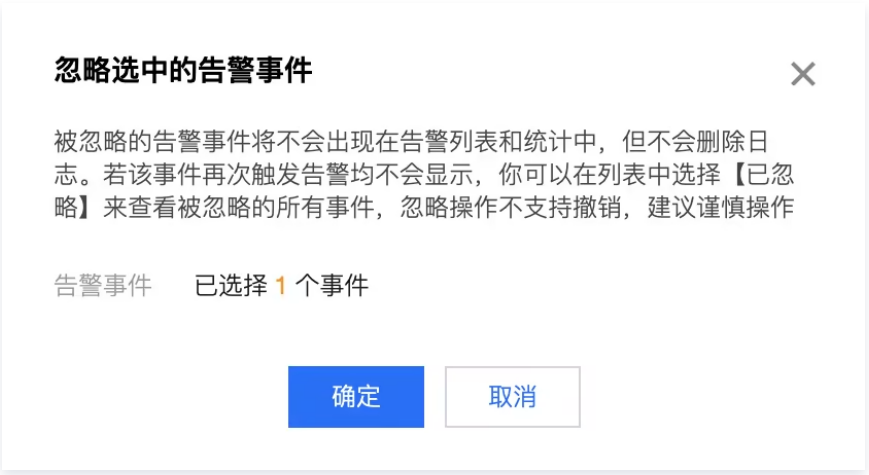
  > **Note:**
  > The maximum quantity of pinned items for a user's inbound and outbound directions must not exceed 5.

- Block: For assets with a relatively high danger level, you can click **Block** to add the IP address to the blocklist (blacklist) of the Intrusion Defense module, select the blocking duration, add remarks, and the cloud firewall will automatically intercept the IP address's access to all of the user's assets within the specified time range.

- Bypass: For IPs that should not be intercepted for user tasks, click **Bypass**. Add this IP address to the allowlist (whitelist) of the Intrusion Prevention System (IPS) module, select the bypass time and bypass reason, and fill in remarks. CFW will bypass the detection of this IP address by the intrusion prevention module within a certain time range and no longer intercept it. If the user is not sure whether the bypass reason is a false alarm, they can preferentially select emergency bypass. If it is confirmed to be a false alarm, feedback on the false alarm content can be submitted, and modifications can be made after clicking **Confirm**.



- Ignore: For duplicate interception events, you can click **Ignore**. The ignored interception events will not appear in the interception list and statistics, but the logs will not be deleted. You can select Ignored in the list to view all ignored events. **The ignore operation cannot be undone. Operate with caution.**



- Isolation: Click **Isolate**. Asset instance isolation will automatically distribute enterprise security group blocking rules, intercept the network access of selected assets in the specified direction, making it easy for subsequent problem localization and troubleshooting, and timely stop loss.

> **Note:**
> After isolating asset instances, you can use the operation and maintenance allowlist to access assets. You can choose to manually fill in IP or use zero trust protection.
> - Only 10 IPs can be manually filled in.
> - Zero trust protection supports selecting WeChat or Enterprise WeChat users to allow asset access. How to integrate WeChat or Enterprise WeChat users, for details, see Enterprise Security Group.

Batch Disposition of Alarm Information

On the attack interception statistics page, you can handle multiple entries of interception information. You can select multiple entries of interception information and click **one-click interception**, **release**, **isolate** or **ignore**.

Note:

- Since the statuses of assets are different, the operable buttons vary. The isolation operation is only targeting lateral movement and intercepting outbound events, isolating compromised hosts to prevent further impact.
- User needs to modify operation, can be recovery operation in **Intrusion defense** > **Blocklist**, **Allowlist** or **Isolation list**. **Ignore operation is not reversible, exercise caution.**.
- Alarms exceeding 7 days will become invalid and cannot be processed.

False Positive Processing

You can add the IP to the allowlist. On the attack interception statistics page, select the desired asset/IP, click **allow**, select false alarm as the bypass reason, and click **confirm**.

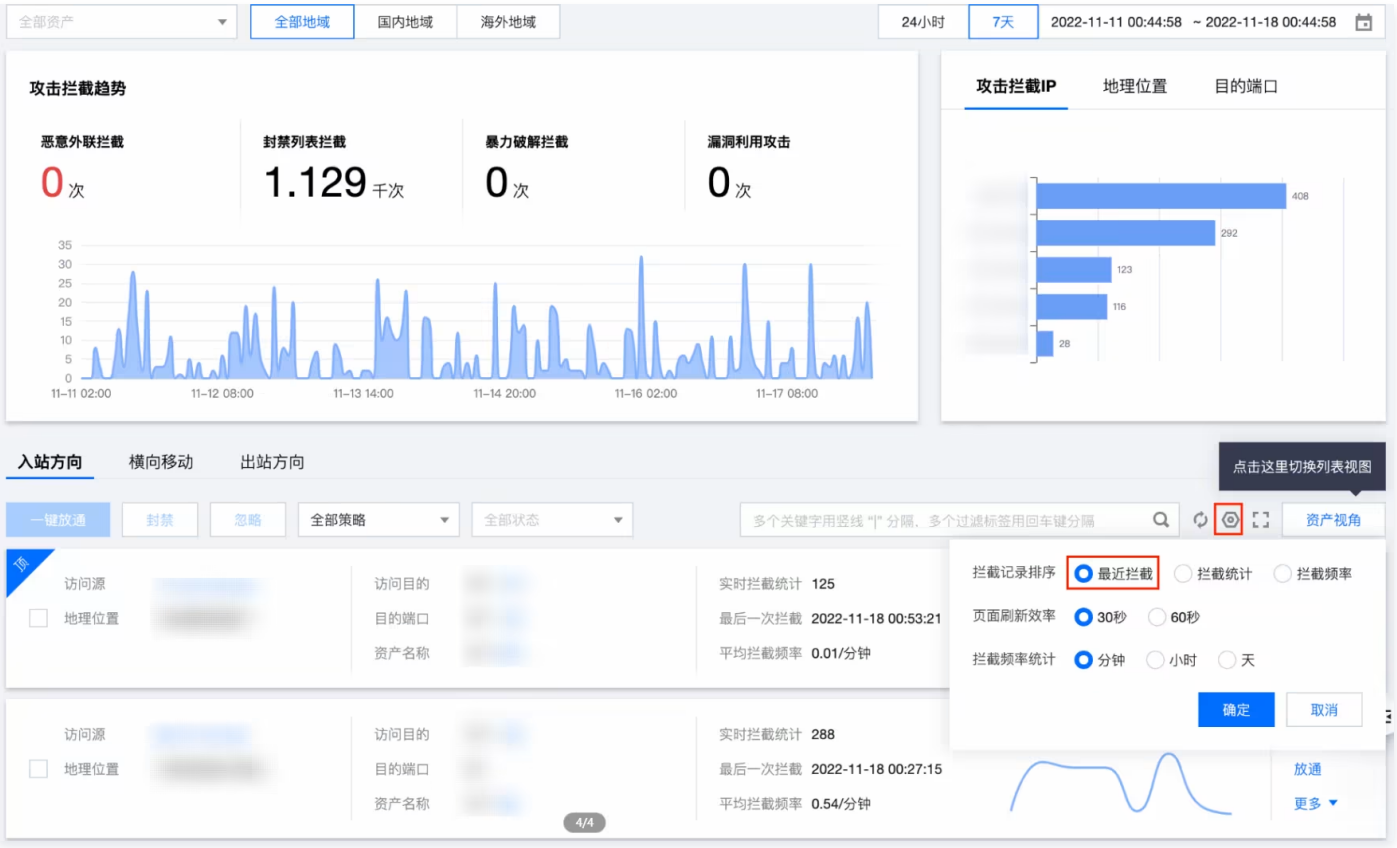
Query an IP'S Attacks on Me

Hover over **Access Destination/Access Source** or **Asset Name** from the asset perspective. Click below **View in Intrusion Prevention Log** to query all attack events.

Note:
In figure, hovering over **access destination/access source** is used as an example.

View the Latest Interception Events

The attack interception statistics page has an auto-refresh function. Click the icon at the top of the page, select "most recent interception" in the interception record sorting, and click **confirm** to monitor the latest interception events in real time.



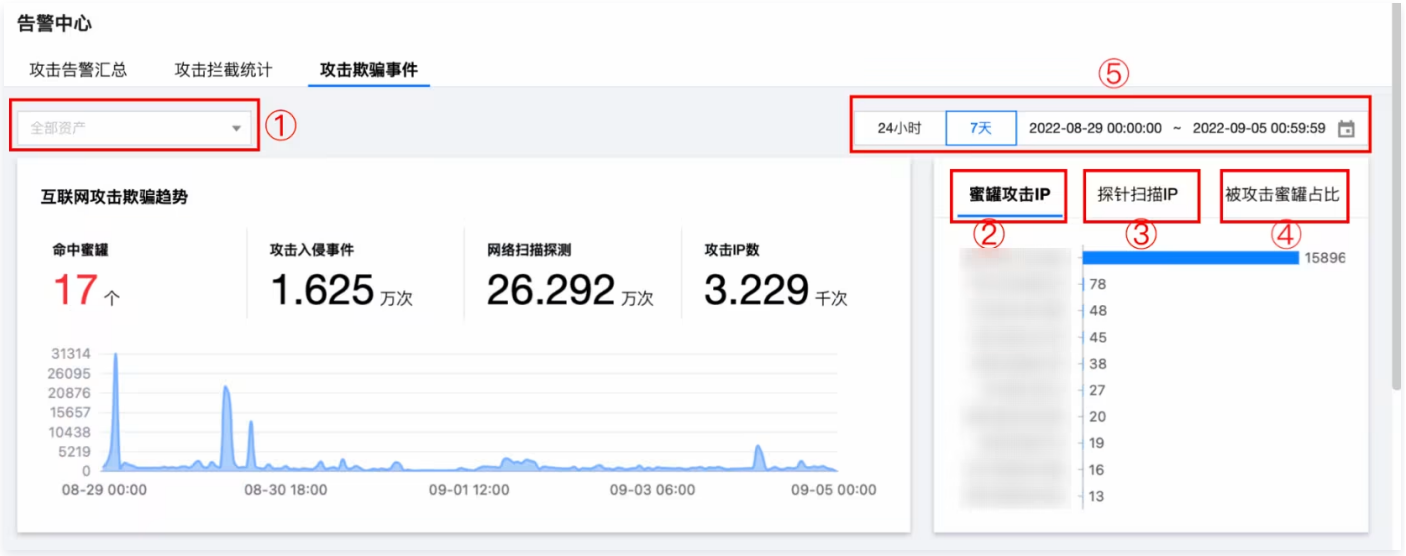
Deception Event Viewing and Handling

Last updated: 2025-05-20 10:53:52

Deception Trend Visualization

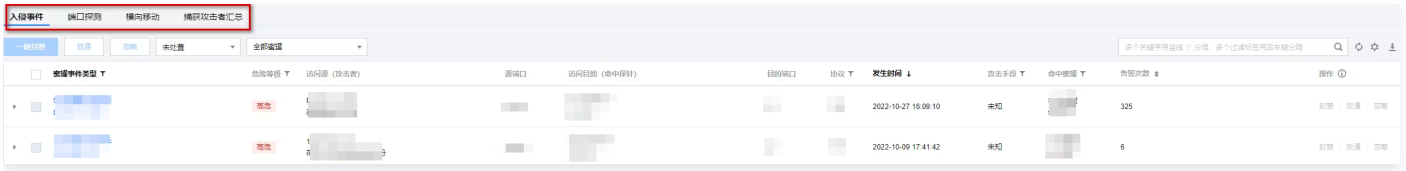
The attack deception event page can record and integrate the scans and attack behaviors of all set exposed probes and network honeypots based on visual statistics and list-based statistics, thereby performing statistical analysis and handling of all intercepted events. Statistical data is updated every 20 minutes.

1. Log in to the CFW console. In the left sidebar, click **Alert Center** > **Attack Deception Events**.
2. On the attack deception event page, you can perform statistical analysis and visualize data based on ①**probe assets**, ②**honeypot attack IPs**, ③**probe scan IPs**, ④**proportion of attacks on honeypots**, and ⑤**time**. On the left side of the page, you can view the number of honeypots hit, the number of attack intrusion events, the number of network scan detections, and the number of attacks on IPs by different probes or all probes at different times.



View Deception Incidents and Attacker Information

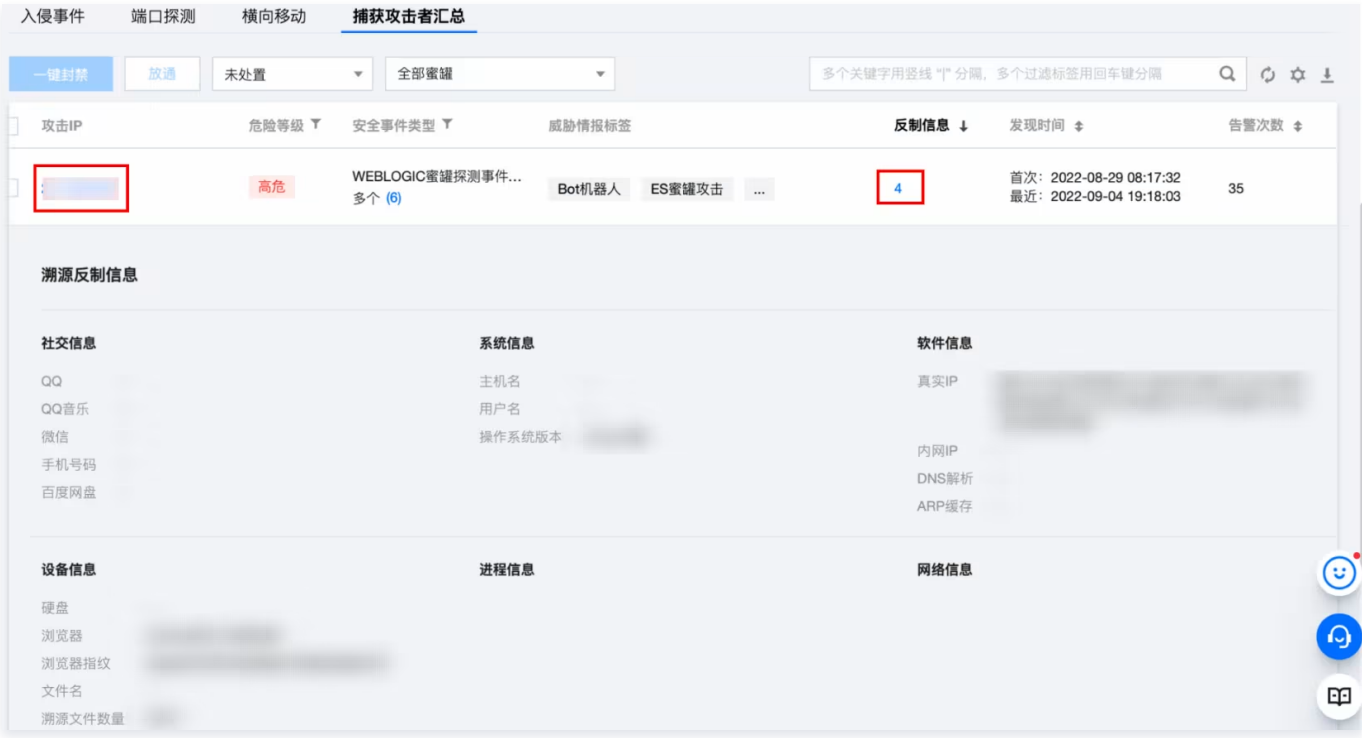
In the event list of the Attack Deception Event Page, there are the following attack deception event types:



- Intrusion events: Attacks can cause host compromise.
- Port detection: A scan attack event performed by an attacker on a honeypot.
- Lateral movement: attack deception events that move laterally between assets.

> **Note:**
> Locate and view deception incidents of intrusion events, port detection, and lateral movement. Support filtering honeypots. For other filter criteria, see Quickly Locate Alarm Events page.

- Summary of attacker capture: Aggregate the attack IP information of deception incidents.
  - Support filtering attackers by threat level and security event type.
  - Support viewing the intelligence tags of attackers, support sorting statistics of countermeasure information, discover events, and number of alarms.
  - Click **attacker IP** or the **number** in the countermeasure information bar to view the traceability and response information of the attack IP.



Quick Disposal of Deceptive Information

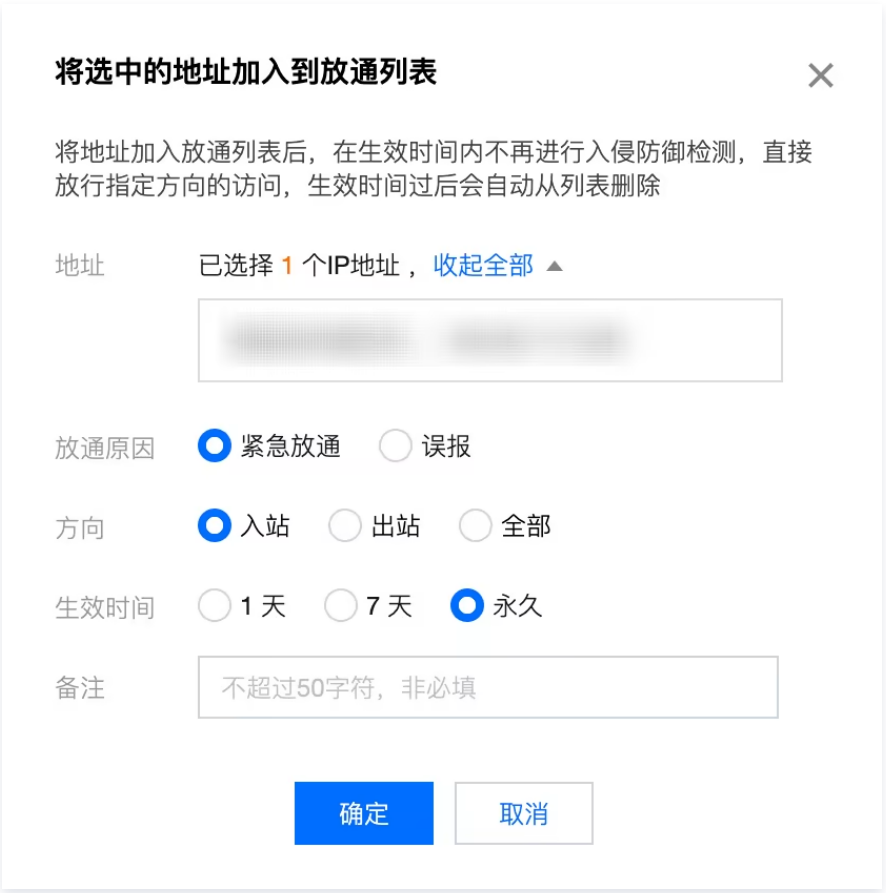
Handle a Single Interception Information

On the Attack Deception Event Page, you can handle individual deception event information. In the right panel of the event, perform **block**, **allowlist**, **ignore**, **isolation** operations.

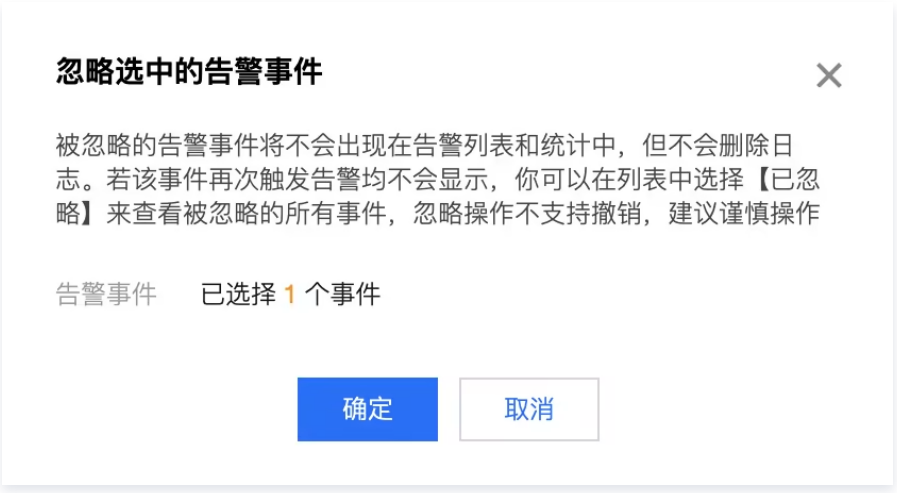
> **Description**
> - Since the status of assets varies, the operable buttons on the right are different. For deception incidents of lateral movement between assets, only isolation and ignore operations are supported.
> - The following operations are also applicable to batch processing operations.
> - Intrusion events and port detections are generally actual attack incidents. It is advisable to block them.
> - Horizontal move events generally mean that your assets have been compromised. It is recommended to isolate them.

- Block: For deception incidents with a relatively high danger level or a considerable number of alarms, you can click **Block**. Add the IP address to the blocklist (blacklist) in the Intrusion Defense module, select the blocking duration, and add remarks. CFW will automatically block the IP address from accessing all of your assets within the specified time range.

- Bypass: For repeated or possible false alarms in deception incident alarms, click **Bypass**. Add the IP address to the allowlist (whitelist) of the Intrusion Prevention module, and select the bypass time and bypass reason, and enter remarks. The cloud firewall will bypass the detection of the intrusion prevention module for the IP address within a certain time range and no longer intercept it. If the user is uncertain whether the bypass reason is a false alarm, they can preferentially select emergency bypass. If it is confirmed as a false alarm, they can submit a ticket for feedback on the false alarm content. Click **Confirm** and modify it.



- Ignore: If you do not want to handle the alarm information, you can click **Ignore**. The log will not disappear, but the record can be viewed in the list of ignored alerts in the handling status. **The ignore operation cannot be undone. Operate with caution.**



- Isolate: Click **Isolate**. Asset instance isolation will automatically distribute enterprise security group blocking rules to intercept network access in the specified direction of the selected assets. It is mainly used for attack deception events of lateral movement between assets, making it easy for subsequent problem localization and troubleshooting, and timely stop loss.

Note:
After isolating asset instances, you can use the operation and maintenance allowlist to access assets. There are two methods: **manually fill in IP** or **use zero trust protection**.
- Only 10 IPs can be manually filled in.
- Zero trust protection supports selecting WeChat or Enterprise WeChat users to allow asset access. How to integrate WeChat or Enterprise WeChat users, for details, see Enterprise Security Group.

Batch Disposition of Alarm Information

On the Attack Deception Event Page, support handling of multiple interception information. Multiple interception information can be selected, click **one-click interception**, **allowlist**, **isolation** or **ignore**.

Note:
- Since the statuses of assets are different, the operable buttons vary. Isolation operations are only targeting deception incidents of lateral movement. Isolate compromised hosts to prevent further impact expansion.
- User needs to modify operations. Recovery operations can be performed in **Intrusion Defense** > **Blocklist**, **Whitelist** or **Isolation List**. **Ignore operation cannot be undone. Operate with caution.**.
- Alarms exceeding 7 days will become invalid and cannot be processed.

Traffic Center

Last updated: 2025-05-20 10:56:22

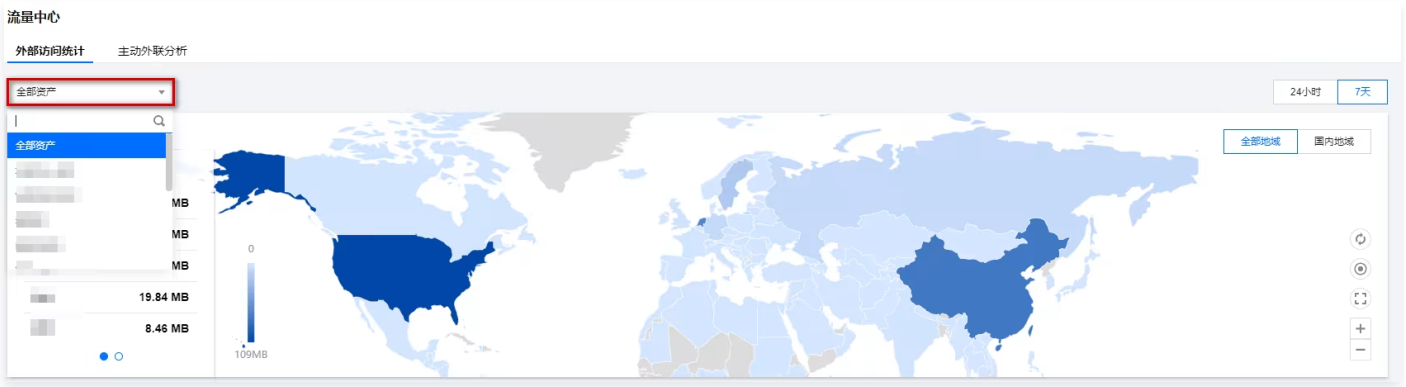
The traffic center's outbound and inbound traffic based on the internet, and the access details of inter-VPC traffic are divided into three pages: incoming access statistics, active outgoing access analysis, and Inter-VPC Activity. This document will guide you on how to view the traffic status of these three pages in the traffic center module and interpret visualization information.

Incoming access statistics

Users can view specific IP addresses, access count, traffic size and other information of inbound traffic on the incoming access statistics page. You can also filter the access details of specific regions to specific assets at different times on the map and view the ranking of traffic in different regions.

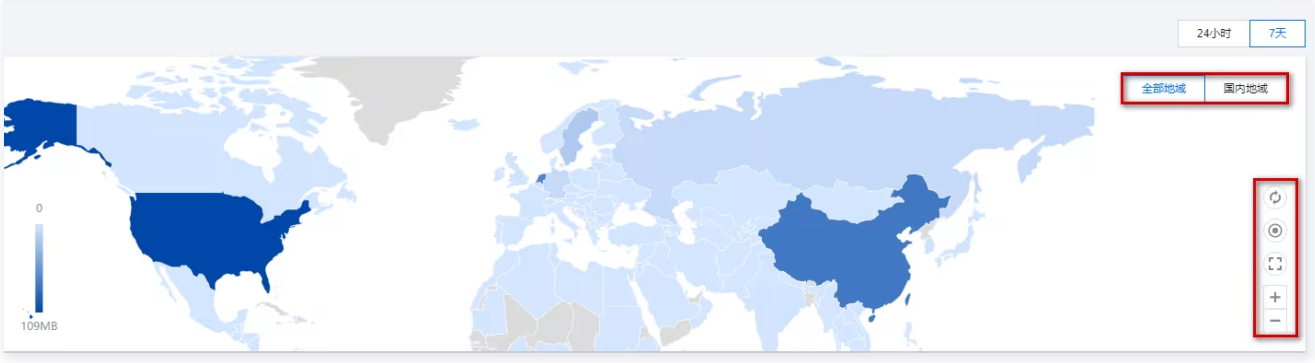
Operation Steps

1. Log in to the CFW console, click **Traffic Center** in the left sidebar, and enter the "Incoming Access Statistics" tab.
2. In the "Incoming Access" module, you can click **All Assets** to view the access status of specific assets in the current region. Meanwhile, you can view the traffic access status in different time periods (last 24 hours or last 7 days).



3. View the access situation of external traffic from two regions, world and China, to assets in the map.
   - Select all regions to view the geographic distribution of traffic access status of countries worldwide.
   - Select a domestic region to view the traffic access status distribution of each province in China.

> **Note:**
> - The left-side carousel slider filters out the top five countries/provinces based on traffic size and access count. You can also move the mouse to the top to view specific IP access details.
> - The depth of color on the map represents the traffic access size of each region (the darker the color, the larger the traffic access). You can also move the mouse to the top of a specific province/country to view specific information.
> - The feature buttons on the right correspond to the following features: update the data in the carousel slider, reset the map to the initial position, unfold the map, and zoom in and out of the map.

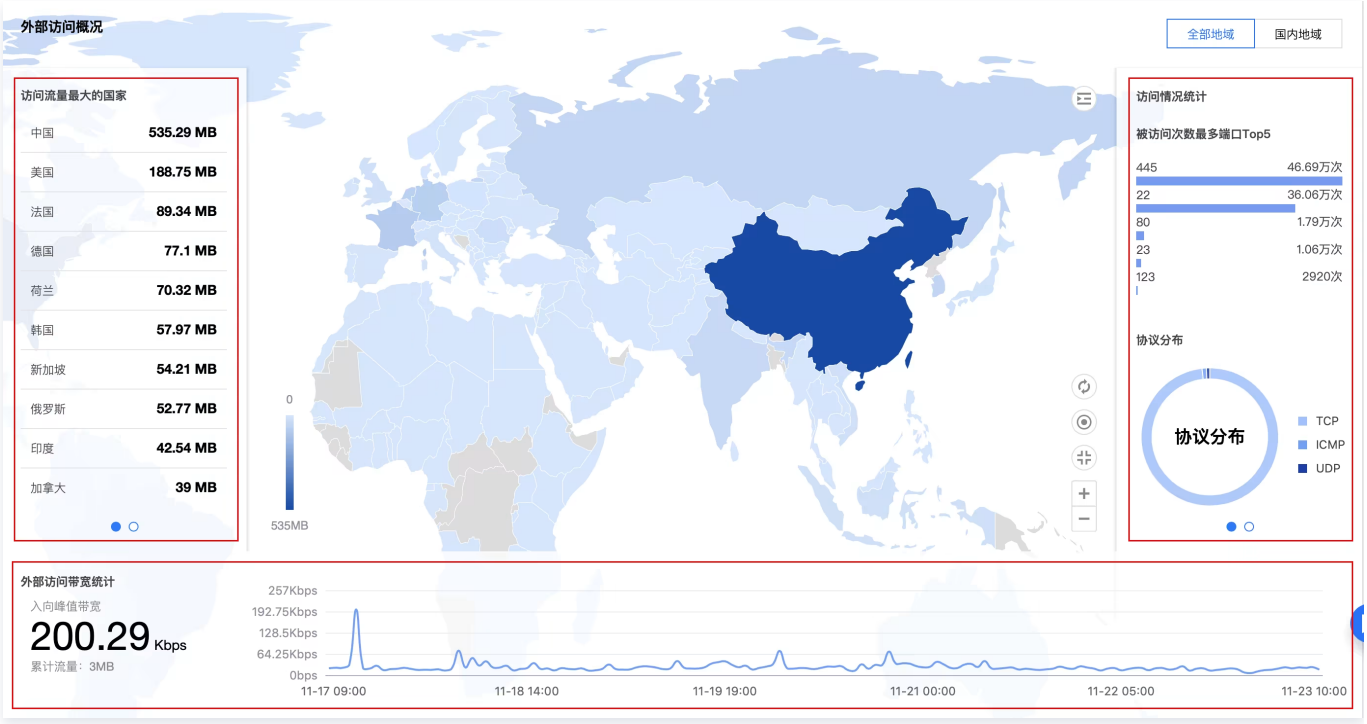


4. On the right side of the map, click  to view the traffic access status in global mode.

5. In global mode, view the rankings in different dimensions.
   - The carousel slider on the left side of the map filters out the top 10 countries/provinces based on access traffic size and access count.
   - The carousel slider on the right side of the map provides viewable information, including the TOP 5 ports with the most accesses, the protocol distribution of external accesses, the TOP 5 assets with the most accesses, and the TOP 5 assets with the largest access traffic.

     Note:
     After selecting a specific asset, the carousel slider on the right will not show the asset ranking.

   - The line statistics chart below the map provides viewable traffic bandwidth rates of external accesses within the current time range, and supports viewing inbound peak bandwidth as well as total traffic size within 7 days or 24 hours.



6. View the specific access IP information of the external access IP list at the bottom of the page.

   Note:
   Since there is considerable traffic information, the list only displays by default the access statistics of the TOP 500 IPs.

   Take the external access list of "Internet access" as an example to provide introduction to the relevant features of the list. The usage of features of other lists is the same as that of it.

   6.1 In the "external address" search bar of the "external access" list, input the **exact** IP address of the access source, in the "destination port" search box, input the **exact** IP address of the asset, or in the "geographical location" search bar, input the **accurate or blurry** place name, then click **start search** to query traffic-related access details.

   6.2 View data details. You can view traffic logs, threat profiles, or asset details in the access list.
   - View traffic logs.

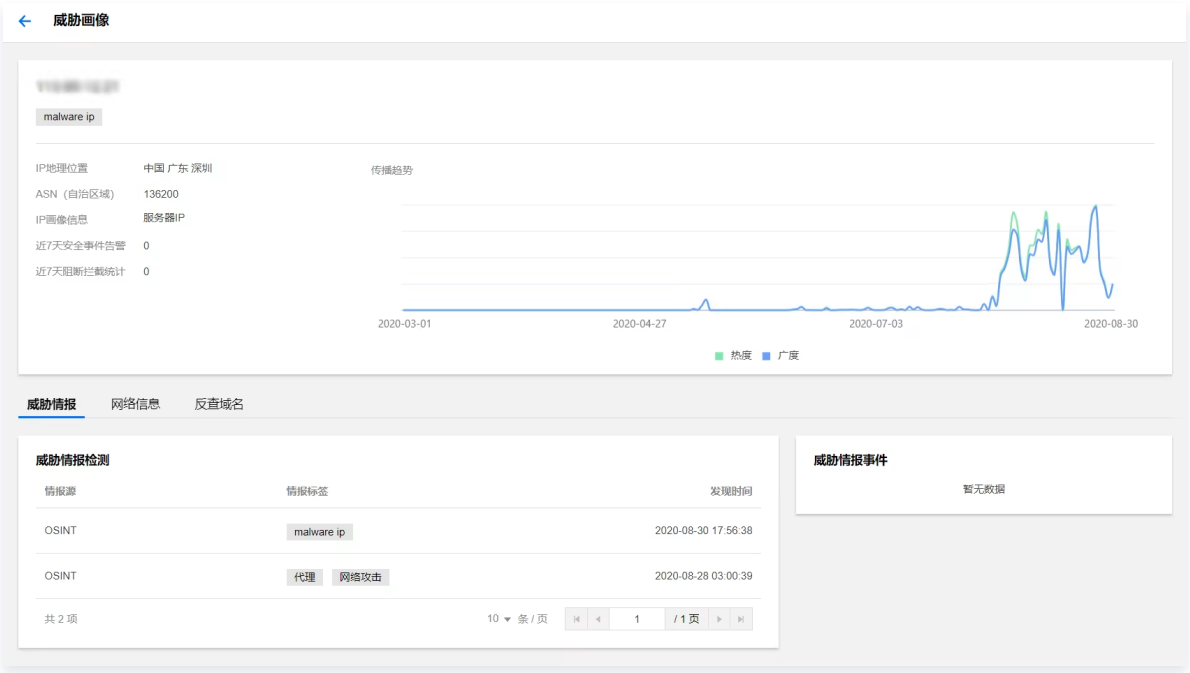
6.2.1.1 In the right operation column of the target data, click **Traffic Log**.

6.2.1.2 On the Traffic Log page, you can view the access details between specified IPs, and present the detailed information of the same access source accessing the same asset by using the access source and access destination as filtering conditions.

- View threat profile

6.2.1.1 In the right operation column of the target data, select **More** > **Threat Profile**.

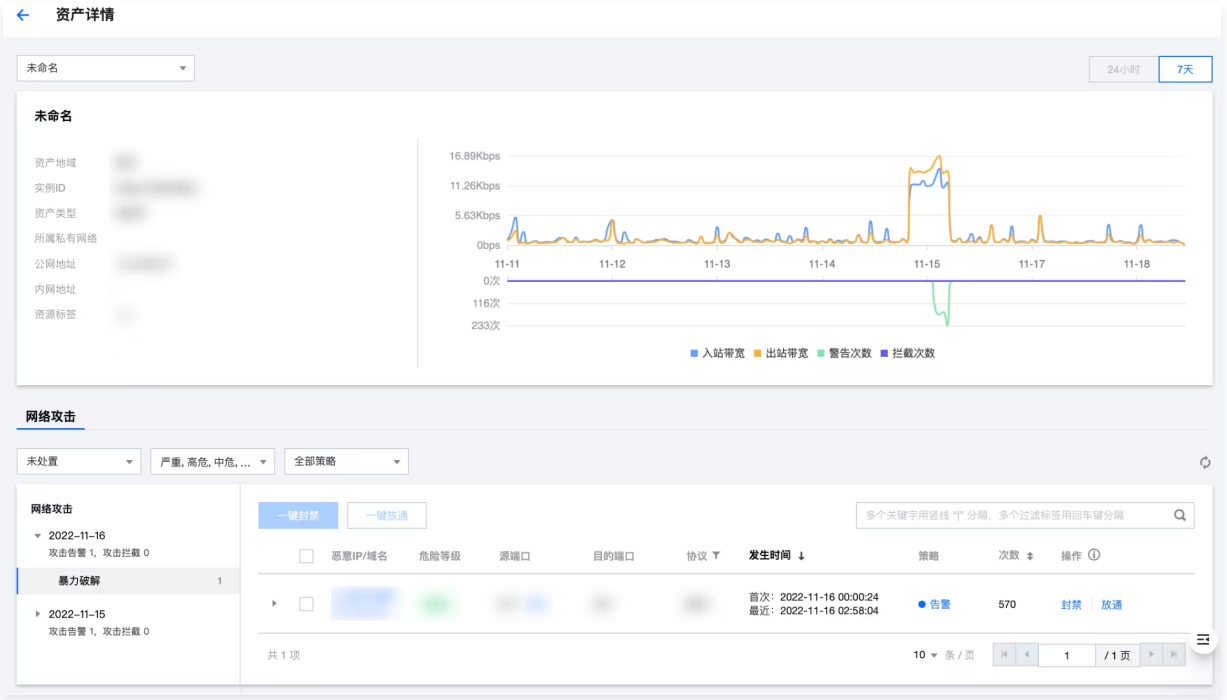
6.2.1.2 On the Threat Profile page, view the threat profile information of the external address and conduct further tracing and auditing.



- view asset details

6.2.1.1 In the right operation column of the target data, select **More** > **Asset Detail**.

6.2.1.2 On the Asset Details Page, view the security events of the asset as well as exposed assets and other information.



Active Outgoing Access Analysis

On the proactive external activities page, you can view the outgoing access details of assets in the last 7 days and understand the specific outbound traffic, external domain names, and external addresses.

Operation Steps

1. Log in to the CFW console, click **Traffic Center** in the left sidebar and enter the "Active Outgoing Access Analysis" page.
   - In the outgoing access overview module, you can view the access details of outbound traffic in the last 7 days or 24 hours. Meanwhile, users can filter the time and assets to view the incoming access statistics of specific assets within a certain time period.
   - On the left side of the Outgoing Access Overview, you can view the external domain names, destination addresses, number of external assets, and alarm counts of assets. Users can view the outgoing access situation of specific assets by filtering the All Assets box.
   - You can view the bandwidth speed in the past 7 days or 24 hours through the line chart below. Hover the mouse over the line chart to view the bandwidth value at a specific time.
   - On the right of the "Outgoing Access Overview", you can view the TOP 5 domains with the most request count, the TOP 5 addresses with the most request count, the address with the maximum access traffic, the TOP 5 assets with the most outbound count, and the TOP 5 assets with the maximum outbound traffic in the past 7 days or within 24 hours.

2. You can view the access status of corresponding outbound traffic, external domain names, external addresses, and external assets in the list below. Among them, details of external domain names, external addresses, and external assets can be viewed.

3. Take the external address as an example for description. The viewing methods of other modules are the same. Click **external address**. In the operation column on the right side of the destination IP, click **access detail** to enter the outgoing destination details page.

4. On the Outgoing destination details page, you can view information such as the access count, traffic size, and IP geo location of the asset to this IP within the last 7 days or 24 hours. You can also view in the list below which assets this IP has accessed. If

you need to learn about traffic log and threat profiling features, please see Incoming access statistics.

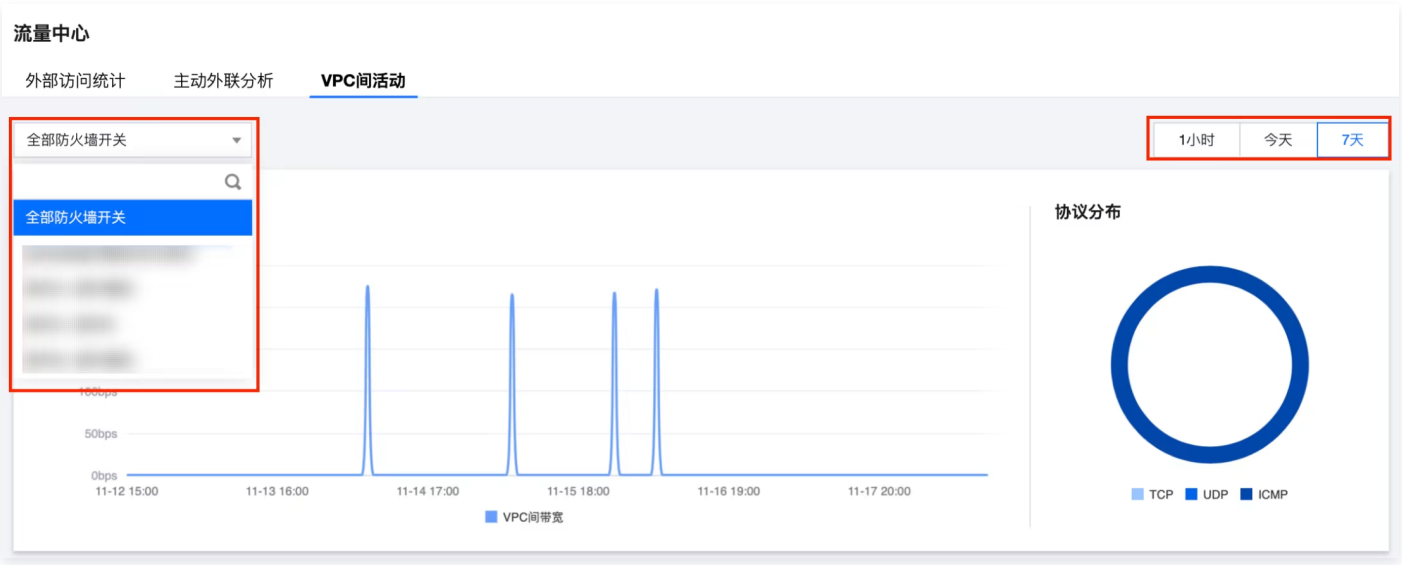
5. If you need to learn more about the outbound situation of a certain asset in the list, you can click **Traffic Log** or **Outgoing Access Details** in the operation column on the right side of the instance list to view the corresponding traffic log or the IPs and domain names that a certain specific asset has accessed in the last 7 days or 24 hours.

Inter-VPC Activity

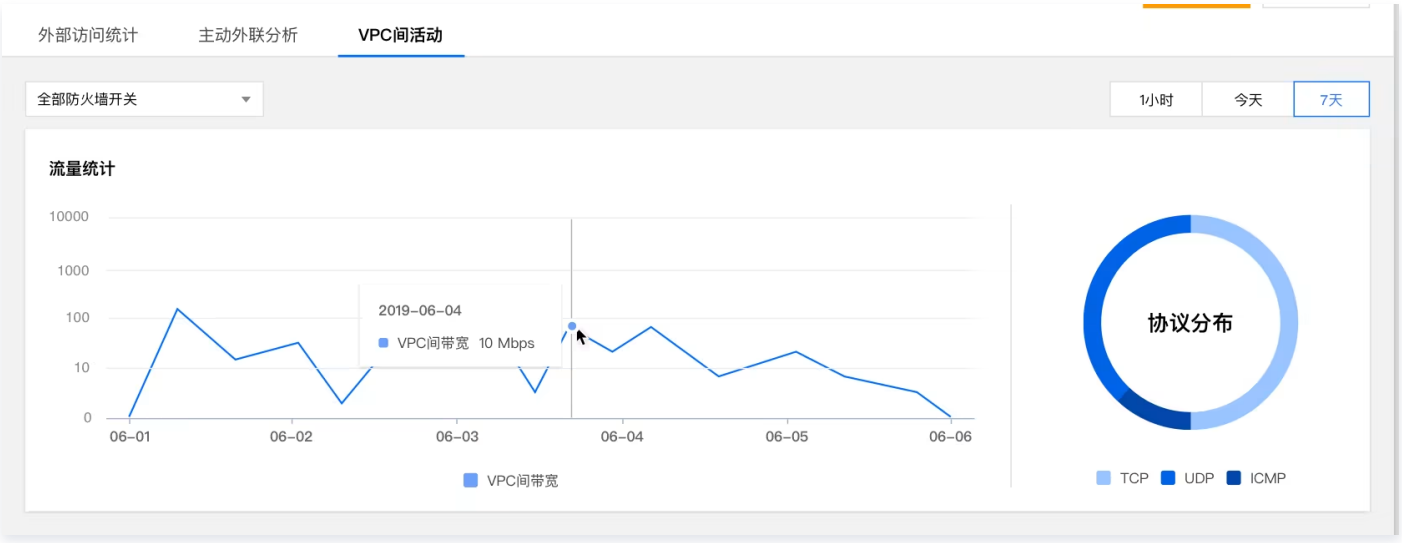
You can view the traffic access and protocol distribution between private clouds on the inter-VPC activity page.

Operation Steps

1. Log in to the CFW console, click **Traffic Center** in the left sidebar and enter the "Inter-VPC Activity" tab.
2. In the filter criterion above the "Inter-VPC Activity" tab, select instances of a specific private cloud and select the time period to view.



3. Hover the mouse over the folding line graph in the traffic statistics to view the bandwidth rate over a fixed period. Meanwhile, hover the mouse over the pie chart of protocol distribution on the right to view the specific distribution percentages of each protocol.



4. View specific IP addresses between VPCs at the bottom of the page. You can also view the IP access destination, access source, and access count on the private cloud. Enter the desired access source, access destination, or destination port in the input box for precise searching. For details, see Incoming Access Statistics.

Information Related To

If you encounter any traffic center-related issues, please refer to the Bandwidth-related document.

Access Control
Access Control Overview

Last updated: 2025-10-31 14:24:43

Access Control Assets

The asset scope protected by CFW covers multiple resource types in cloud environments.

Asset Type	Description
Public network IP address	Including the public network IP bound to CVM instances, Elastic IP (EIP), and the public network egress of Cloud Load Balancer (CLB).
Private IP Address	Including CVM instances, private IP addresses bound to TKE nodes, etc.
Server instance	Including CVM instances, LH instances
Domain name	Including public network domains, private network domains.

Access Control Method

The CFW supports configuring access control rules as follows:

Access Control Method	Description
IP rule	Perform access control based on IPV4 and IPV6, supporting exact matching or CIDR IP range configuration.
Domain name rule	Flexible domain name traffic management based on FQDN, judging whether to allow access based on the requested domain name in the access request, without verifying the IP resolved from the domain name.
Domain name resolution rule	Allow the IP of the actual domain name request according to the protocol and the region where the instance is located.
Resource tag rule	Manage access permissions in batches based on Tencent Cloud resource tags
Address template rule	Use predefined IP address templates for rapid configuration rules
Geolocation rule	Restrict access based on the geographic affiliation (country, region) of the IP address
Cloud provider rule	Control IP ranges or service tags for specific cloud vendors

Rule List Quota Description

Last updated: 2025-05-28 16:08:34

Version Default Quota

The current access control rules include the following types: Internet boundary rules, NAT boundary rules, private network rules, enterprise security groups, and DNS rules. According to the purchased version, the default quotas for different versions are as shown in the table below:

Version	Internet Boundary Rules	NAT Boundary Rules	Private Network Rules	Enterprise Security Group	DNS Rules
Advanced Edition	1000	1000	-	100 entries	-
Enterprise Edition	2000	2000	2000	1000	-
Flagship Edition	5000	5000	5000	2000	-

Occupied Quota Statistical Method

Access control rule quota is divided holistically by firewall type, regardless of region and direction.
Each rule in the list occupies 1 quota. The number of occupied specifications refers to the cumulative sum of all added rules under your corresponding firewall type.

Notes:
For example, if you have 4 inbound rules for NAT boundary rules (Guangzhou), 3 outbound rules for NAT boundary rules (Guangzhou), 2 inbound rules for NAT boundary rules (Shanghai), and 1 outbound rule for NAT boundary rules (Shanghai); then the NAT boundary rule quota usage is 4 + 3 + 2 + 1 = 10 rules.

Expand Rule Description

For rules issued to the firewall, the configured ACL will be split into multiple rules based on the smallest granularity and issued to the engine. Therefore, the number of rules counted by the engine is not the list rule number, but the number of rules issued. The relevant specifications for the number of rules issued can be found in Instance Specifications.
The Rule Expansion Formula is as follows:
Number of rules issued = Number of source addresses × Number of destination addresses × Number of ports × Number of protocols.

Notes:
- For source and destination addresses, 1 IP, CIDR, IP range, or domain/subdomain is considered as 1 minimum expansion unit.
- For ports, a single port, a consecutive port range, and all ports are each considered as 1 minimum expansion unit.
- Note: For protocols, any single protocol except ANY is considered as 1 minimum expansion unit.
  - When both the access source and access destination are IPs, the 4-layer ANY protocol at this point is considered as 1 minimum expansion unit.
  - When the access destination is a domain name, the 7-layer ANY protocol at this point is considered as 6 minimum expansion units.
- Note: For example: The access source 0.0.0.0/0 is 1 CIDR, the access destination is a domain name address template containing 2 domain names, the destination ports are 80, 443/446 (one is a single port and the other is a port range), and the protocol is a 7-layer ANY protocol; therefore, the number of rules issued = 1 * 2 * 2 * 6 = 24.

Number of Rules Issued Limit

When the engine reaches the maximum number of rules issued limit, you will not be able to continue configuring ACL rules. Manage rules appropriately. The specific firewall number of rules issued limit is as follows:

- Internet boundary bypass firewall: Single-tenant supports a maximum of 10,000 issued rules, cannot be expanded, optimize rules appropriately.
- NAT Boundary Firewall: Related to instance specifications. You can expand the number of rules issued limit by upgrading instance specifications. For details, see NAT Boundary Firewall Instance Specifications.
- Inter-VPC Boundary Firewall: Related to instance specifications. You can expand the number of rules issued limit by upgrading instance specifications. For details, see Inter-VPC Firewall Instance Specifications.

Internet Boundary Rules

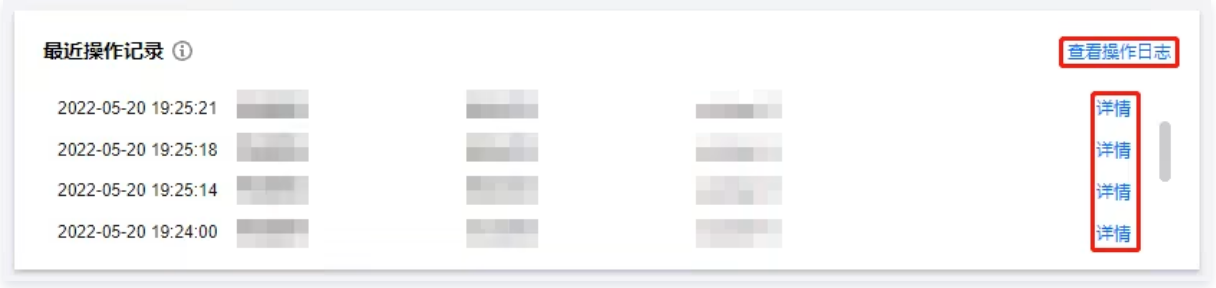
Last updated: 2025-05-20 10:57:42

Access control rules support domain filtering and traffic filtering based on geolocation requirements. Internet boundary rules provide two access control rule lists, which are inbound rules and outbound rules. **Inbound rules**: Control south-north traffic from outside to inside. **Outbound rules**: Control south-north traffic from inside to outside. This document will use "inbound rules" as an example to provide relevant operation instructions. The operation of "outbound rules" is likewise.

Operation Guide

1. Log in to the CFW console. In the left sidebar, select **Access Control** > **Internet Boundary Rules**.
2. On the internet boundary rules page, click **Inbound Rule** to enter the inbound rules page.

3. On the inbound rules page, recent operation records are viewable. Recent operation records show the operations that users have recently performed on the rule list:
   - click **detail** to view this item's operation record detail.



   - click **view operation log** to view detailed operation records.

> **Note:**
> It takes about 1 minute to deliver logs, so recent operation record updates may be slightly delayed.

4. Add rules. On the inbound rules page, you can configure rules.

   4.1 On the inbound rules page, click **Add Rules**, and a "Add Inbound Rule" popup will appear.

   4.2 In the "Add Inbound Rule" popup, you can configure the rule. The access source type can be IP, geographical location, cloud service provider, and address template. The access destination type can be IP, asset instance, resource tag, address template, and asset group. Check the execution order according to the rule importance. After selecting the source and destination types and sequence, fill in the access source, access destination, destination port, protocol, policy, description, and other information. Click **Confirm** to complete the configuration.

> **Note**
> - Inbound rule: When the access source is filled in as 0.0.0.0/0, all public IPs will be automatically associated in the backend. The same applies to filling in a CIDR address; it only takes effect for public IPs within that subnet.
> - Outbound rule: Same as inbound rule.

- **Field Descriptions:**
  - type of access source
    - IP address: any IP or CIDR format address, such as 10.10.10.10 or 10.10.10.10/24.
    - Geographical location: the actual geographical location corresponding to the IP, including each province in Chinese mainland, Hong Kong (China), Macao (China) and Taiwan (China), and each state overseas.

      > **Description**
      > The geolocation function is only supported by the enterprise edition and flagship edition of CFW. If needed, you can upgrade to enterprise edition or flagship edition of CFW.

    - Cloud service provider: the service IP corresponding to each cloud service provider brand.
    - Address template: an IP address template set by users.
  - access purpose type
    - IP address: The access destination of the inbound rule is only applicable to your public IP. If you fill in a CIDR address, the backend will automatically associate it with all your public IPs included in this address range.
    - Asset instance: Select specific instances as the access destination in the inbound direction.
    - Resource tag: Select the access destination according to the resource's tag. The public network IP of the instance in the tag will match the Internet boundary rules.
    - Address template: Select a user-defined IP address template as the access destination.
    - Asset group: Select a user-defined asset group as the access destination.
  - **Rule Priority**: Define the priority of rule execution, the first or last to be executed.
  - Execution order: The execution order of access control rules. The execution orders of outbound rules and inbound rules do not affect each other. Rules with a higher execution order are preferentially matched. After hitting a rule, subsequent rules are no longer matched. When you modify the execution order of a rule, the execution order of the original rule at that position +1, and so on. When you delete a rule, the execution orders of all subsequent rules -1.
  - **Access source**: The inbound rule access source can be set to any IP/CIDR format address. It also supports parameters such as geographic location, cloud service provider, and address template.
  - **Access destination**: The access destination of inbound rules is only effective for public network IPs. It also supports parameters such as asset instances, resource tags, address templates, and asset groups. If it is an outbound rule, the parameters of access source and access destination are swapped.
  - **Destination port**: Support single port number, port range based on '/', and discrete port values separated by commas. For example, "80", "80/80", "-1/-1", "1/65535" or "80,443,3380/3389".
  - **Protocol**: Protocols supported by the serial firewall: TCP, UDP, ICMP, HTTP, HTTPS, HTTP/HTTPS, SMTP, SMTPS, SMTP/SMTPS, TLS/SSL, DNS, and FTP; Protocols supported by the bypass firewall: TCP, HTTP/HTTPS (outbound only), TLS/SSL (outbound only).
  - **Policies**:
    - Allow traffic that hits a rule, record the hit count but not the access control logs, and record traffic logs.
    - Monitor: Allow traffic that hits a rule, record the hit count, access control logs, and traffic logs.
    - Block: Block traffic hitting the rule, record the hit count and access control logs, and the traffic log records information of a request packet of the traffic.
  - Effective firewall range for the current rule: selectable "global rule", "serial firewall", or "bypass firewall".

- **Description**: for description of rules, supports up to 50 characters.

- **Internet Boundary Wildcard Rules:**

Input Field	Input Example	Description
Access Source/Access Destination	0.0.0.0/0	Indicates all IPs.
Domain name (only in outbound rules)	*	Indicates all domain names.
Domain name (only in outbound rules)	*.aa.com	Indicates a second-level domain name starting with *: aa.com.
Destination Port	-1/-1	Indicates all ports.
Destination Port	1/65535	Indicates all ports.
Destination Port	80,443,3389	Indicates that it is effective for ports 80, 443, and 3389.
Destination Port	80/443	Indicates that it is effective for all ports between 80 and 443.
Destination Port	80/443,3389	Indicates that it is effective for all ports between 80 and 443 as well as port 3389.

Note:
- The operations for inputting a domain name are as follows: On the Access Control > **Internet Boundary Rules** > **Outbound Rules** page, click **Add Rule**, select the access destination, input the desired domain name according to the outbound rule, and click **Confirm** to save.
- Outbound rule: The access destination supports any IP address, CIDR address, and domain name. It supports wildcard domain names starting with * as well as all domain names represented by *.

5. Click **Copy** in the right operation column to add multiple rules.

Description
In the pop-up window for adding inbound rules, each row represents a rule. Each time a rule is added, it is inserted at the end of the list by default, which is the position with the highest execution order and the lowest priority.

- **Scenario 1**: Rule list edited locally, need to batch add rules to improve efficiency.

5.1.1 Click **Copy** in the right operation column to add a row of rules below the current position. Supports up to 10 rules at a time.

5.1.2 Complete all fields in the form.

5.1.3 Before submission, check whether the execution order of batch-adding rules meets expectations.

5.1.4 Click **Confirm** to submit the configured rules.

- **Scenario 2**: Need to configure multiple rules for a certain IP simultaneously.

5.1.1 First, edit a rule and only fill in the parts that need to be filled in repeatedly.

5.1.2 Click **Copy** in the right operation column to add a row of rules below the current position and automatically copy the filled content from the previous row. Supports up to 10 rules at a time.

5.1.3 Complete other fields in the form and fill in the parts that do not need to be filled in repeatedly.

5.1.4 Before submission, check whether the execution order of batch-adding rules meets expectations.

5.1.5 Click **Confirm** to submit the configured rules.

6. After rules are added, view related rules in the rule list.
7. Import rules. Click **Import Rules** to select a file from the local system for import. You can specify the import location, download import template, and export existing rules.

8. Rule backup and rollback. Please see Rule Backup document.

Information Related To

- If you need to control inbound and outbound traffic at the NAT boundary in the CFW console, please see NAT Boundary Rules.
- If you need to set private network rules in the CFW console, please see private network rules.
- If you need to learn about the special application scenarios of the access control feature of CFW, please see special application scenarios.
- If you encounter any related issues with the internet boundary rules, please see the Internet Boundary Firewall document.

NAT Boundary Rules

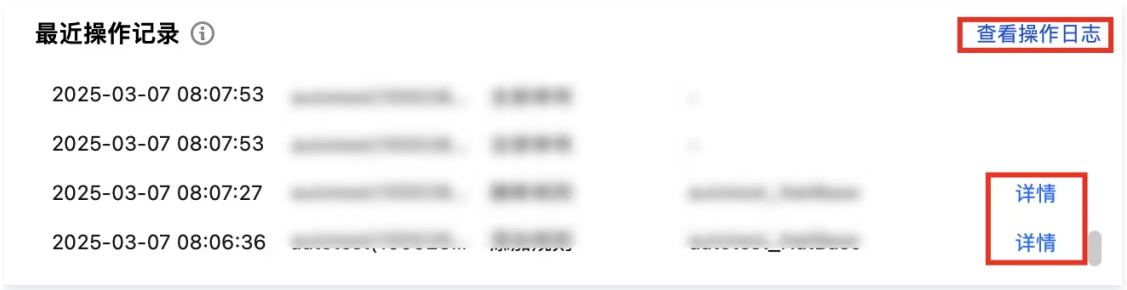
Last updated: 2025-05-20 10:58:03

Access control rules support domain filtering and traffic filtering based on geolocation requirements. NAT boundary rules provide two access control rule lists, namely inbound rules and outbound rules. **Inbound rules**: Manage north-south traffic from outside to inside at the Internet boundaries. **Outbound rules**: Manage north-south traffic from inside to outside at the Internet boundaries. This document will use "inbound rules" as an example to provide relevant operation instructions. The operation of "outbound rules" is likewise.

Operation Guide

1. Log in to the CFW console. In the left sidebar, select **Access Control** > **NAT Boundary Rule**.
2. On the NAT Boundary Rule interface, click **Inbound Rule** to enter the Inbound Rule interface.

3. On the inbound rule interface, you can select different regions to create access control rules, as well as view the rule list (used quota for inbound rules, outbound rules and the total quota of the rule list), recent operation records and details of access control rules. The recent operation records show the operations that users have recently performed on the rule list.
   - Click **detail** to view the operation record detail of this item.
   - Click **View Operation Logs** to view the detailed operation records.



4. Add rules. On the inbound rule page, you can configure rules. Adding inbound rules is used as an example for description.
   4.1 On the inbound rule page, click **Add Rule**, and a pop-up for "Adding Inbound Rules" will appear.
   4.2 In the pop-up for "Adding Inbound Rules", you can configure the rules. For access source type, you can select IP address, geographical location, cloud service provider or address template. For access destination type, you can select IP address, asset instance, resource tag, address template or asset group. Check the first or last to execute according to the importance of the rule. After filling in the access source and access destination, fill in the destination port, select the corresponding protocol and the policy to be executed and other information, make remarks in the description column, and click **OK** to complete the configuration of the rule.

> **Note:**
> - Access destination region: the region where the cloud instance is located.

- type of access source: the type of external access source when adding an inbound rule.

Field Description:

- **Execution order**: The execution order of access control rules. The execution orders of outbound rules and inbound rules do not affect each other. Rules with a higher execution order are preferentially matched. After hitting a rule, subsequent rules will not be matched. When you modify the execution order of a rule, the execution order of the original rule at that position + 1, and so on. When you delete a rule, the execution orders of all subsequent rules − 1.
- **Access source**: Inbound rule access source is effective for all public network IPs. IP addresses, geographical locations, cloud service providers, and address templates are supported.
- **Access destination**: Inbound rule access destination is only applicable to all private network assets in the current region. IP addresses, asset instances, resource tags, address templates, and asset groups are supported. The types supported by outbound rule access source and access destination are just the opposite.
- **Domain Name Rule (Outbound Rule Support)**: Judge whether to allow access based on the requested domain name in the access. No verification of the IP resolved by the domain name.
- **Domain name resolution rule (supported by outbound rules)**: Allow the IP of the actual domain name request according to the protocol and the region where the instance is located.
- **Destination port**: TCP/UDP rules support a single port number, port ranges based on '/', and discrete port values separated by commas. For example, "80", "80/80", "−1/−1", "1/65535", or "80,443,3380/3389". No need to configure ports for ICMP rules.
- **Protocol**: The current version's inbound rules support TCP and UDP protocols; outbound rules support TCP, UDP, ICMP, HTTP, HTTPS, SMTP, SMTPS, DNS, and FTP protocols.
- policy description
  - Allow traffic that hits a rule, record the hit count but not the access control log, and record traffic logs.
  - Monitor: Allow traffic that hits a rule, record the hit count, and log both access control and traffic logs.
  - Block: Block traffic hitting the rule, record the hit count and access control log, and the traffic log records information of a request packet of the traffic.
- **Description**: For describing rules, supports up to 50 characters, inserting rule's special settings via ##, the current version supports settings such as #persistent connection#, suitable for scenarios with persistent connection business.
- **NAT Boundary Wildcard Rule**:
  The firewall provides different rules for wildcard IPs, wildcard ports, and wildcard domain names:

Input Field	Input Example	Description
Access Source/Access Destination	0.0.0.0/0	Indicates all IPs.
Domain name	*	Indicates all domain names.
Domain name	*.aa.com	Indicates a second-level domain name starting with *: aa.com.
Destination Port	−1/−1	Indicates all ports.
Destination Port	1/65535	Indicates all ports.
Destination Port	80,443,3389	Indicates that it is effective for ports 80, 443, and 3389.

Destination Port	80/443	Indicates that it is effective for all ports between 80 and 443.
Destination Port	80/443,3389	Indicates that it is effective for all ports between 80 and 443 as well as port 3389.

5. Click **Copy** in the right operation column to add multiple rules.

> **Note:**
> In the pop-up window for adding inbound rules, each row represents a rule. Each time a rule is added, it is inserted at the end of the list by default, which is the position with the highest execution order and the lowest priority.

- **Scenario 1**: Rule list edited locally, need to batch add rules to improve efficiency.
  5.1.1 Click **Copy** in the right operation column to add a row of rules below the current position. A maximum of 10 rules can be added at a time.

  5.1.2 Complete all fields in the form.
  5.1.3 Before submission, check whether the execution order of batch-adding rules meets expectations.
  5.1.4 Click **Confirm** to submit the configured rules.

- **Scenario 2**: Need to configure multiple rules for a certain IP simultaneously.
  5.1.1 First, edit a rule, and only fill in repeatedly the part that needs to be filled in repeatedly.
  5.1.2 Click **Copy** in the right operation column to add a row of rules below the current position and automatically copy the filled content from the previous row. Supports up to 10 rules in one addition.

  5.1.3 Complete other fields in the form and fill in the parts that do not need to be filled in repeatedly.

5.1.4 Before submission, check whether the execution order of batch-adding rules meets expectations.

5.1.5 Click **Confirm** to submit the configured rules.

6. Import rules. Click **Import Rules** to select a file from the local system for import. You can specify the import location and download the import template.

7. Rule backup and rollback. Please see Rule Backup document.

Related Information

- If you need to control inbound and outbound traffic at the Internet boundary in the CFW console, please see Internet Boundary Rules.
- If you need to set private network rules in the CFW console, please see private network rules.
- If you need to learn about the special application scenarios of the access control feature of CFW, please see special application scenarios.
- If you encounter any NAT boundary rule-related issues, see NAT boundary firewall.

Private Network Rules

Last updated: 2025-05-28 10:31:26

Private network rules provide an access control list. When creating a rule, you can configure the scope of the rule to provide access control for traffic interconnection between different VPCs. This document describes how to set private network rules in the Cloud Firewall console.

Adding Rules

1. Log in to the CFW console, in the left sidebar, select **access control** > **private network rules**.

> **Note:**
> - Different from the internet boundary and NAT boundary access control lists, the private network access control list does not distinguish between direction zones.
> - The local VPC and the peer VPC are equivalent. When configuring rules, you can determine the corresponding VPC based on the CIDR IP range of the access source and access destination, thereby distinguishing the direction.

2. On the private network rules page, click **Add Rule** to enter the Add Rule page.
3. On the add rule page, fill in the source IP, access destination IP, destination port, protocol, policy, effective range, and other information, and click **OK** to complete the rule configuration.

Field Description:

- **Execution Order**: The execution order of access control rules does not affect the execution order of the corresponding rule list in the firewall switch. Rules with a higher execution order are matched first. Once a rule is hit, subsequent rules will no longer be matched. When you modify the execution order of a rule, the original rule at that position will have its execution order increased by 1, and this adjustment applies to all subsequent rules accordingly. When you delete a rule, the execution order of all subsequent rules will be decreased by 1.
- **Access source**: Supports 0.0.0.0/0 as the access source for wildcard rules (only takes effect within the selected scope). Access sources other than this can only be filled with IPs or subnet segments from the local/peer VPC's CIDR, and must not be in the same VPC network segment as the access destination. Click **Details** to view the details of the access source network instance associated with the private network rules.
- **Access destination**: Supports 0.0.0.0/0 as the access destination for wildcard rules (only takes effect within the selected scope). Access destinations other than this can only be filled with IPs or subnet segments from the local or peer VPC's CIDR, and must not be in the same VPC network segment as the access source. Click **Details** to view the access destination network instance details associated with the private network rules.
- **Destination port**: Supports single port numbers, '/'-based port ranges, and discrete port values separated by commas. For example, "80", "80/80", "-1/-1", "1/65535", or "80,443,3380/3389".
- **Protocol**: Supports TCP, UDP, ICMP, HTTP, HTTPS, SMTP, SMTPS, DNS and FTP protocols.
- **Policy description**:
  - Release: Allows traffic that hits a rule, logs the number of hits but does not log access control, and logs traffic.
  - Observe: Allows traffic that hits a rule, logs the number of hits, access control, and traffic.
  - Block: Intercepts traffic that matches the rule, records the number of hits, and records access control logs. The traffic log records information of a single request data packet.

- **Effective scope**:
  - Global Policy: The rule applies to all traffic managed by firewalls between VPCs.
  - Select a VPC firewall switch: The rule only applies to the private network traffic managed by that specific firewall switch.
- **Description**: Used to describe rules. Supports up to 50 characters. Allows inserting special settings for rules via ##. The current version supports the setting #persistent connection#, applicable to long connection business scenarios.
- **Inter-VPC Wildcard Rules**: Support wildcard IP address ranges. For more details, see the Internet Boundary Wildcard Rules in Internet Boundary Rules.

> **Notes**
> - The CIDR IP range of the local VPC and the remote VPC corresponding to the inter-VPC firewall must not be the same or overlap; otherwise, the firewall switch cannot be enabled.
> - In the access control rules for private networks, the access source and access destination can only include IP addresses or CIDR subnet ranges from the CIDR addresses of the local or remote VPC. Since the CIDRs of the local VPC and remote VPC cannot be the same, the "access source" and "access destination" can be used to distinguish the direction of the traffic controlled by the rule.
> - If you enter an address other than the CIDR of the local VPC or the peer VPC, the rule will not take effect.
> - When "access source" and "access destination" are filled with 0.0.0.0/0, they can be used to indicate all addresses of the VPC.

4. Click **Copy** in the right operation column to add multiple rules.

> **Note:**
> In the Add Inbound Rule pop-up window, each row represents a rule. Each time a rule is added, it is inserted at the end of the list by default, that is, the position with the highest execution order and the lowest priority.

- **Scenario 1**: Rule list edited locally, need to batch add rules to improve efficiency.

  4.1.1 Click **Copy** in the right operation column to add a row of rules below the current position. A maximum of 10 rules can be added at a time.

  4.1.2 Complete all fields in the form.

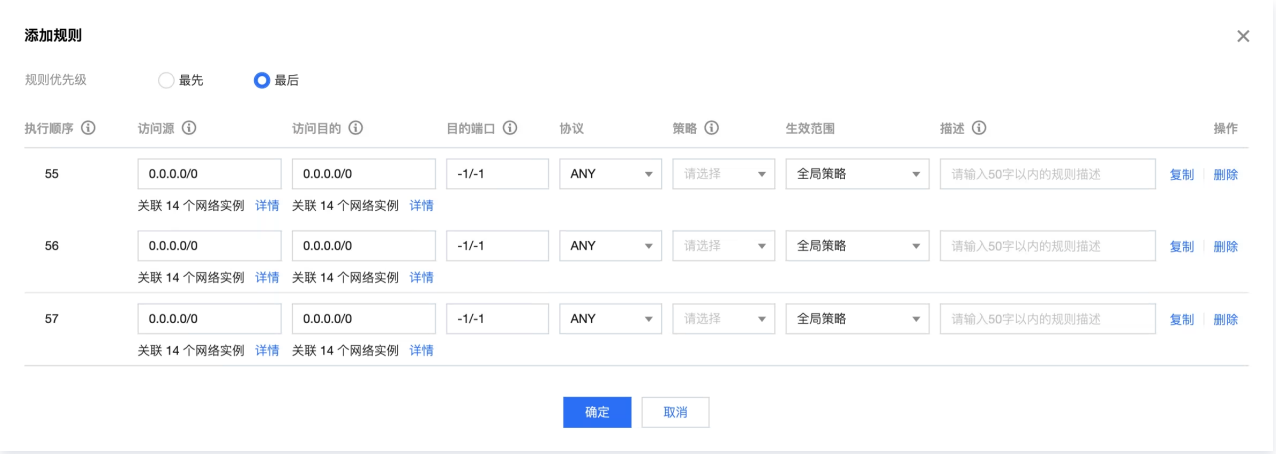
  4.1.3 Before submitting, check whether the execution order of the batch added rules is as expected.

  4.1.4 Click **Confirm** to submit the configured rules.

- **Scenario 2**: Need to configure multiple rules for a certain IP simultaneously.

  4.1.1 Edit a rule to fill in the fields that need to be input repeatedly.

  4.1.2 Click **Copy** in the right operation column to add a row of rules below the current position and automatically copy the filled content from the previous row. A maximum of 10 rules can be added at a time.



4.1.3 Complete other fields in the form and fill in the parts that do not need to be filled in repeatedly.

4.1.4 Before submitting, check whether the execution order of the batch added rules is as expected.

4.1.5 Click **Confirm** to submit the configured rules.

5. After adding the rules, you can view the related rules in the rule list.

Import Rules

On the private network rules page, click **Import Rules** to select a file from your local system for import. You can specify the import location, download an import template, and export existing rules.

Back Up and Roll Back Rules

Rule backup and rollback, please see Rule Backup document.

> **Notes**
> Inter-VPC rules that were backed up before the revision do not support rollback. If needed, submit a ticket to contact us.

Related Information

- For controlling inbound and outbound traffic at the internet boundary on the Cloud Firewall console, please see Internet Boundary Rules.
- To manage inbound and outbound traffic at the NAT boundary in the CFW console, please see NAT Boundary Rules.
- For the special scenarios of the Cloud Firewall access control feature, please see Special Scenarios.

- If you encounter issues related to Inter-VPC Rules, please refer to the inter-VPC firewall document.

Enterprise Security Group Feature Overview

Last updated: 2025-05-20 10:58:57

Enterprise security groups represent a novel control plane for security groups, capable of replacing the security group management interface on the cloud server console. The configuration logic for security groups has been redesigned, maintaining a uniform access control management page, which greatly optimizes the user experience of security groups. The Cloud Firewall offers a rule configuration interface based on quintuples and uses an intelligent conversion algorithm to automatically deliver security group policies, drastically simplifying the configuration operations of security groups.

Note:
CFW has launched a new version of enterprise security group. The new version is improved on the basis of the old version, mainly optimizing configuration items, logic, etc. The rule matching conditions are more fine-grained, and the policies are more intuitive, making it easy to understand and manage. It is recommended that you can use new version of enterprise security group. For specific differences between the old and new versions, please refer to FAQs.

Features of Enterprise Security Group

- Drastically simplify the configuration operation of security groups and retain the usage habits of 5-tuple rules.
- More convenient support for access control between VPCs, between subnets, and for Direct Connect (DC).
- Provide access control logs of security groups to facilitate backtracking of blocking conditions and daily troubleshooting.
- No need to change the network architecture, no impact on network stability, and no additional bottlenecks in terms of network performance.

Enterprise Security Group Limits

Enterprise security groups are developed based on the underlying architecture of CVM security groups, so they are subject to the functional implementation and resource quotas of security groups.

Enterprise Security Group Rules

Rule Composition

- Access source and access destination: It can be an IP, CIDR block, instance, subnet, or Virtual Private Cloud (VPC), depending on the inbound or outbound direction.
- Destination port: Destination port number. This item requires no configuration when the protocol type is ICMP or ANY.
- Protocol type: Currently supports TCP, UDP, and ICMP. ANY represents all supported protocols.
- Policy: The operation executed upon rule hit.
  - Release policy, release the traffic that hits the rule, and do not log access control.
  - Blocking policy, intercept traffic hitting the rule and log access control.

Priority of Rules

Security group rules have priorities. Rule priority is represented by the position of the rule in the list. The rule at the top of the list has the highest priority, and the rule at the bottom has the lowest priority.
The execution order is to perform one-by-one matching from high-priority to low-priority rules. Upon rule hit, subsequent rules will no longer be matched.
Inbound rules and outbound rules belong to different rule lists, and their priorities do not affect each other.
If you need to use the enterprise security group feature, please see Configuration Steps.

Automatically Deploy in Both Directions

To improve the configuration efficiency of security groups, enterprise security groups provide the "automatically deploy in both directions" feature. In scenes where private network-to-private network traffic is blocked or allowed in both directions, there is no longer a need to configure two identical rules in two directions. This feature can automatically perform such operations, reducing the workload of rule configuration.
When the access source address is filled in as an instance, subnet, or private network address, you can use the "automatically deploy in both directions" feature to automatically configure an identical outbound rule (with the highest execution order).

> **Note**
> Applicable only to the communication scenario from private network to private network.

For example, suppose there are two instances. The IP of instance 1 is IP1, and the IP of instance 2 is IP2.
The user has configured a security group with deny all for instance 1 and instance 2 respectively. At this point, if you want to allow one-way access from instance 1 to instance 2, you need to manually configure two security group rules:

- Instance 1, allow outbound traffic to IP2.
- Instance 2: Allow IP1 in the inbound direction.

Use the "automatically deploy in both directions" feature. You only need to manually configure one of the rules. The other one will be automatically generated by the enterprise security group. For details, see Automatically Deploy in Both Directions for Unidirectional Access between Instances to perform the operation.

Logs

Security Group Blocking Log

Security Group Blocking Logs can display all situations where the blocking policies of enterprise security groups take effect. Currently, only a small number of models are supported.

Enterprise Security Group Operation Log

Enterprise Security Group Operation Logs are used to record the operations performed by an account on the enterprise security group page.

Configuration Steps

Last updated: 2025-05-20 11:05:57

This document introduces how to manage quotas and add rules through enterprise security groups.

> **Notes:**
> The Cloud Firewall has launched a new version of the Enterprise Security Group. The new version is improved based on the previous one, with optimizations mainly in configuration items, logic, etc. Rule matching conditions are more granular, and policies are more intuitive, making them easier to understand and manage. We recommend using the New Enterprise Security Group. For specific differences between the old and new versions, please refer to Hotspot Issues.

Prerequisites

- Need to have upgraded the cloud firewall to enterprise edition or flagship edition.
- For first-time use of the Enterprise Security Group, CAM authorization is required. After enabling the Enterprise Security Group, when you first enter the **Access Control** > Enterprise Security Group **page or Access Control Log** > **Enterprise Security Group** page, please perform the authorization operation as prompted.

  > **Notes:**
  > The log delivery feature requires permissions for the cloud firewall service role CFW_QcsRole and the associated policies QcloudAccessForCFWRoleInEnterpriseSecurityGroup and QcloudAccessForCFWRoleInLogService.

- Enable CLS (Cloud Log Service). After completing CAM authorization, network flow logs will be delivered to your Tencent Cloud CLS (Cloud Log Service). If this feature is not yet enabled, follow the console prompt to manually turn it on. Once CLS is enabled, you can refresh the **Access Control Log** > Enterprise Security Group page to view relevant log content.

Operation Steps

Step 1: Quota Management

Enterprise security groups will occupy your security group quota. You can view and manage related security group quotas on the enterprise security group page.

1. Log in to the CFW console, in the left sidebar, select **Access Control** > **Enterprise Security Group**.
2. On the upper-right corner of the rule list overview on the enterprise security group page, click **quota details** to view the security group quota.

3. On the security group quota details page, you can view the security group quota details for each region and check the details of associated instances and security groups as needed.

Field Descriptions:

- **Number of existing security groups**: The number of configured security groups.
- **Security group quota**: The maximum number of security groups allowed to be created in each region.
- **Number of security group rules**: The number of outbound or inbound rules allowed for each security group.
- **Number of instances bound to a security group**: The number of Cloud Virtual Machines (CVM) associated with a single security group.
- **Number of security groups bound to an instance**: The number of security groups that can be associated with each instance.
- **Associated instances**: A list of associated instances where you can view the details of each instance.
- **Security group list**: A list of existing security groups where you can view the details of each security group.

4. (Optional) The quota for security groups is limited. After you complete an operation such as adding rules, inserting rules, or editing rules, if the security group quota is insufficient, the system will prompt you to adjust the corresponding security group quota. On the upper-right corner of the rule list overview on the enterprise security group page, click **Manage Quota** to apply for relevant security quotas in the ticket system.

Step 2: Adding Rules

Rules are divided into inbound rules and outbound rules. The rule list only allows one user to perform operations at the same time. This document will use inbound rules as an example for explanation (the same applies to outbound rules).

1. On the enterprise security group page, select the region that requires operation in the upper left corner.

> **Notes:**
> Each region has independent inbound and outbound rule lists for enterprise security groups.

2. On the enterprise security group page, select **Inbound Rule** > **Add Rules**.
3. In the pop-up window for adding inbound rules, fill in the relevant fields, and click **Confirm**.
   - Rule priority: "First" inserts the new rule at the front of the rule list with the highest priority. "Last" inserts the new rule at the end of the rule list with the lowest priority.
   - Access purpose type: Includes "CVM", "cloud database", "Elastic Network Interface", and "load balancer". Fill in the relevant fields according to different access purpose types.
   - Automatically deploy in both directions: When the access source address is filled in as an instance, subnet, or private network address, you can automatically deploy in both directions to assign one identical outbound rule (with the highest execution order), which is suitable for bidirectional access scenarios between private networks.

> **Notes:**
> - When an asset is bound to a unique security group, the security group blocks all by default.
> - If there are asset instances in your assets that are not bound to any security group, deploying the corporate security group policy will bind a unique security group to these assets. This poses a relatively high security risk. Proceed with caution.

4. Adding completed, this inbound rule will appear in the inbound rules list.

5. After adding the inbound rule, on the Security Group page in the VPC console, you can view the security groups automatically generated by the enterprise security group, which have automatically configured security group rules and associated instances.

> **Note**
> Please do not manually modify the security groups or route tables maintained by the CFW (such as NAT route tables, CVM security groups, etc.) in other locations. Please perform operations uniformly in the CFW console.

Step 3: Editing Rules

On the Enterprise Security Group page, click **Inbound Rules** to edit, insert, delete, or quickly sort the added rules.

- **Edit Rule:** On the right side of the target rule, click **Edit** to modify the rule configuration. After modification, click **Done** to finish.

- **Deactivate Rule::** In the status bar of the target rule, you can control whether the rule is effective. If you toggle off the switch, the rule will be deactivated and will no longer participate in rule-based matching.

> **Notes:**
> When an Enterprise Security Group Rule is deactivated, the corresponding rule in the security group will be deleted, but this rule will still remain in the rule list of the Enterprise Security Group.

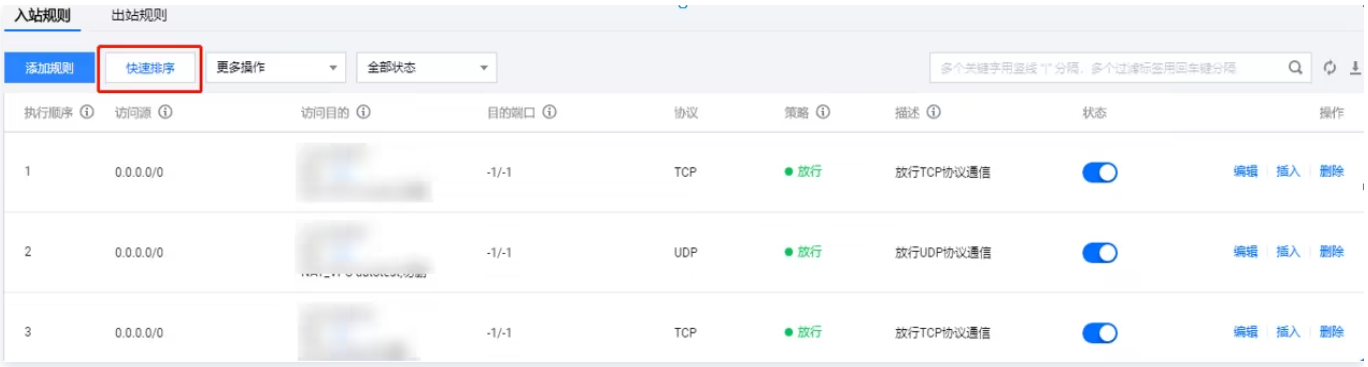
- **Insert Rule:** On the right side of the target rule, click **Insert** to add a new rule in front of the current rule, with a higher priority than the current rule.

- **Delete Rule:** On the right side of the target rule, click **Delete**, then confirm to delete the target rule.

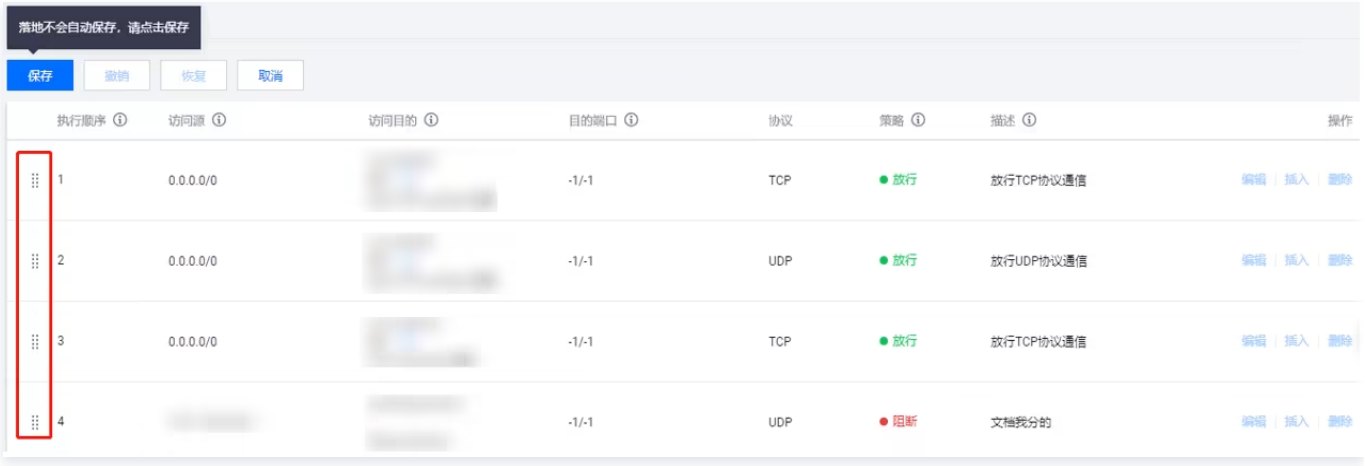
> **Notes:**
> After a rule is deleted, both the Enterprise Security Group and the security group will simultaneously delete this rule, and the operation is irrevocable.

- **Quick Sort**

  1.1 The order of rules in the list determines the execution priority. At the top of the inbound rules list, click **Quick Sort**.



1.2 You can quickly complete the adjustment of rule priorities through the drag-and-drop operation of rules.



1.3 After completing the adjustment, click **Save**, and the adjusted priority will take effect. The enterprise security group will automatically push the new rule priority to the instance.

- **Export rules**: In the upper-right corner of the rule list, click the Export button to export an Excel file containing all inbound or outbound rules.

> **Notes:**
> Note: The rule operation ignores the retrieval criteria and rule switch status.

FAQs

Will the Security Groups Maintained by the CFW Be Deleted after the Enterprise Security Group Expires?

No, the CFW will not purge the security group configuration in the VPC console upon expiration.

Can You Directly Modify the Security Groups Maintained by the CFW in the VPC Console?

No. Manually modified security group rules in the VPC console will not be reflected on the enterprise security group page, which can easily lead to rule management errors, impact network security protection, and meanwhile, when the enterprise security group rules are updated, they will synchronize rules to the security group, and the manually modified security group configuration will be overwritten.
For more enterprise security group related issues, please refer to the security visualization document.

Automatically Deploy Unidirectional Access between Instances in Both Directions

Last updated: 2025-05-20 11:10:35

The automatic two-way deployment feature is used to achieve communication from one private network to another. Taking the one-way access communication between two servers in your private network as an example, this introduces how to use the automatic two-way deployment feature.

> **Note:**
> Cloud Firewall has launched a new version of enterprise security group. The new version is improved on the basis of the old version, mainly optimizing configuration items, logic, etc. The rule matching conditions are more fine-grained, and the policies are more intuitive, making it easy to understand and manage. It is recommended that you can use new version of enterprise security group. For specific differences between the new and old versions, please refer to FAQs.

Prerequisites

- CFW needs to be upgraded to enterprise edition or flagship edition.
- For first-time use of the enterprise security group, CAM authorization is required. After you enable the enterprise security group, when you first enter the **Access Control** > Enterprise Security Group **page or Access Control Log** > Enterprise Security Group page, perform the authorization operation as prompted.

  > **Note:**
  > The log delivery feature requires permissions for the Cloud Firewall service role CFW_QcsRole and the associated policies QcloudAccessForCFWRoleInEnterpriseSecurityGroup and QcloudAccessForCFWRoleInLogService.

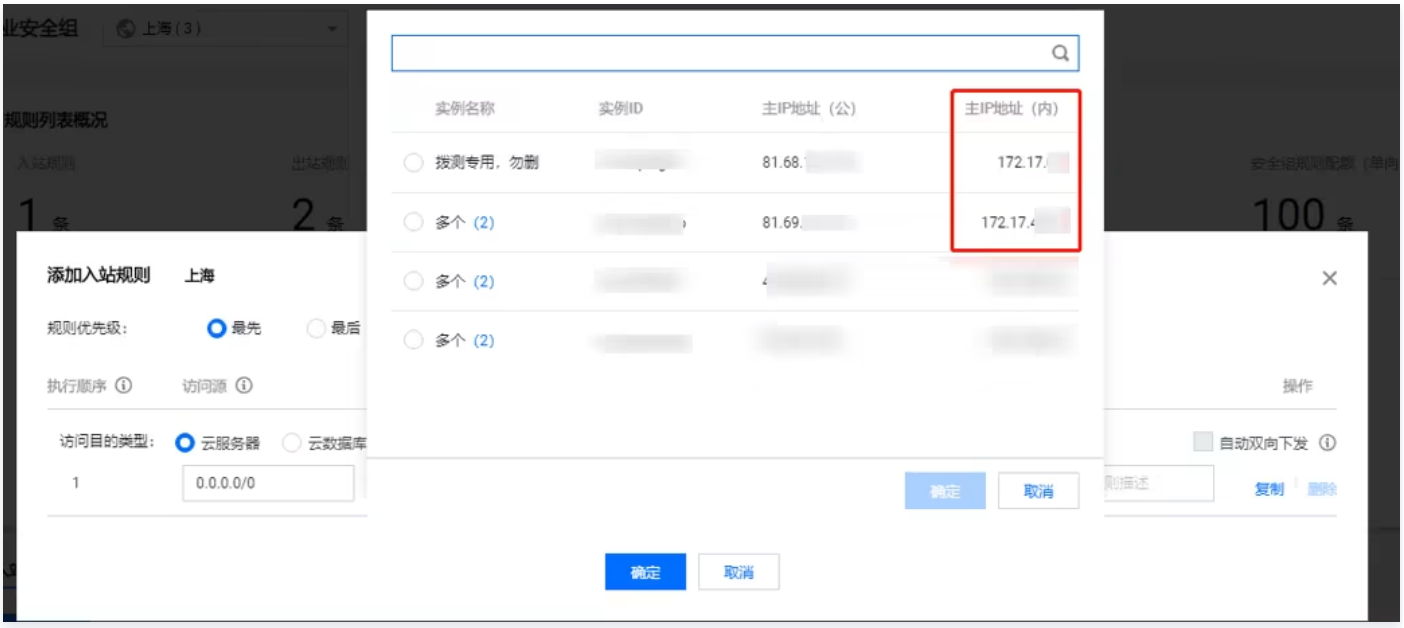
- Enable CLS (Cloud Log Service). After you complete CAM authorization, network flow logs will be sent to your Tencent Cloud CLS (Cloud Log Service). If this feature is not yet activated, please manually enable it according to the console prompt. After enabling CLS, you can view relevant log content by refreshing the CFW's **Access Control Log** > Enterprise Security Group page.

Operation Steps

1. Log in to the CFW console. In the left sidebar, select **Access Control** > **Enterprise Security Group**.
2. On the enterprise security group page, select the region for operation in the top-left corner.

   > **Note:**
   > Each region has independent inbound and outbound rule lists for the enterprise security group.

3. Below the enterprise security group page, select **Inbound Rule** > **Add Rules**.
4. In the pop-up window for adding inbound rules, fill in the relevant fields and choose two server in your private network. For example, a rule that only allows server A (private network IP: 172.17.xx.xx) to access server B (private network IP: 172.17.xx.xx).



5. Configure rules. The first rule allows host A to access host B. The second rule forbids all IPs to access host B. Since the first rule executes first, it will not be affected by the second rule.

6. Check "Automatically deploy in both directions".
   - Since the access source and access destination of rule 1 are both private network IPs, the "automatically deploy in both directions" feature of this rule is enabled, while the access source IP of rule 2 is not a private network IP, so rule 2 cannot "automatically deploy in both directions".
   - When an instance corresponds to multiple IPs, after checking the "automatically deploy in both directions" feature, you need to confirm the number of IPs corresponding to the instance. If an IP corresponds to multiple instances, you need to manually determine the effective instance.
7. After all confirmations, click **Confirm**. You can then view the added rules in the inbound rules list. At the same time, in the outbound rules list, one outbound rule is automatically generated by the enterprise security group.

8. After adding the inbound rules, in the Security Group page of the VPC console, you can view the security groups automatically generated by the enterprise security group. The security group rules and associated instances are automatically configured.

> **Note:**
> Please do not manually modify the security groups or route tables maintained by CFW. Perform operations in the CFW console.

Enterprise Security Group (New) Configuration Steps

Last updated: 2025-05-28 10:32:37

Overview

The new version of enterprise security group has made relatively large adjustments on the basis of the old version, which is mainly reflected in the following aspects:

- Remove the concepts of geographical restrictions and inbound/outbound directions. Just define the access source and access destination to implement the security group distribution.
- Default to automatic bidirectional distribution rules. If unidirectional distribution is not required, it can be achieved by adding a keyword in the description.
- Configuration items added options such as IP/CIDR, region, etc., with symmetric arrangement for each option and allowing any combination.
- When the access source and access destination types are set to IP addresses, automatic synchronization will occur if the IP hits an instance. For example, entering a full-zero IP address in the access source or access destination will synchronize all instances.
- The new version of enterprise security group configuration is simpler than the old version, with a more concise configuration interface and better compliance with access control ACL configuration habits.

> **Note:**
> Enterprise security groups and Internet edge firewalls are independent. Technically, security group settings can be batch deployed to servers or databases. Even if the Internet edge firewall is not enabled or the purchased bandwidth is insufficient, enterprise security groups can still be used normally.

Adding Rules

1. Log in to the CFW console, select **Access Control** > **Enterprise Security Group (New)** in the left navigation.
2. On the New Enterprise Security Group page, click **Add Rule**, and the Add Rule window pops up.
3. In the Add Rule window, configure related parameters and click **Confirm**.

Parameter Description

- Execution order: The execution order of enterprise security group rules. Rules with a higher execution order are preferentially matched. Once matched, subsequent rules are no longer matched. When you modify the execution order of a rule, the execution order of the original rule at that position is increased by 1, and so on. When you delete a rule, the execution order of all subsequent rules is decreased by 1.

- Access source: IPv4 rules support types such as IP/CIDR, parameter template, asset instance, asset group, resource tag, and asset geography.
- Access destination: IPv4 rules support types such as IP/CIDR, parameter template, asset instance, asset group, resource tag, asset geography, and domain name resolution.

> **Note:**
> When you select one type for the access source, you can also select one type for the access destination. However, if the access source or access destination is set to a resource region, the corresponding access destination or access source cannot be set to an asset geography. No such restriction applies to other types.

- Destination port: Supports single port numbers, '/'-based port ranges, and discrete port values separated by commas. Up to 15 discrete ports can be filled in, for example "80", "80/80", "-1/-1", "1/65535".
- Protocol: The current version supports UDP, TCP, and ICMP.
- Policy:
  - Allow: Allow traffic that hits a rule and do not record enterprise security group hit logs.
  - Block: Block traffic that hits a rule and record enterprise security group hit logs.
- Description: Used to describe rules, supports up to 50 characters, allows inserting special settings of rules via ##, currently supported settings include #Only issue access source#, #Only issue access destination#.

> **Note:**
> When the access destination address is an instance, subnet, or private network address, an identical inbound rule can be assigned through automatic bidirectional distribution. If you do not want to achieve the effect of bidirectional distribution, you can add keywords in the description: #Only issue access source# (only apply security group rules to the access source), #Only issue access destination# (only apply security group rules to the access destination).

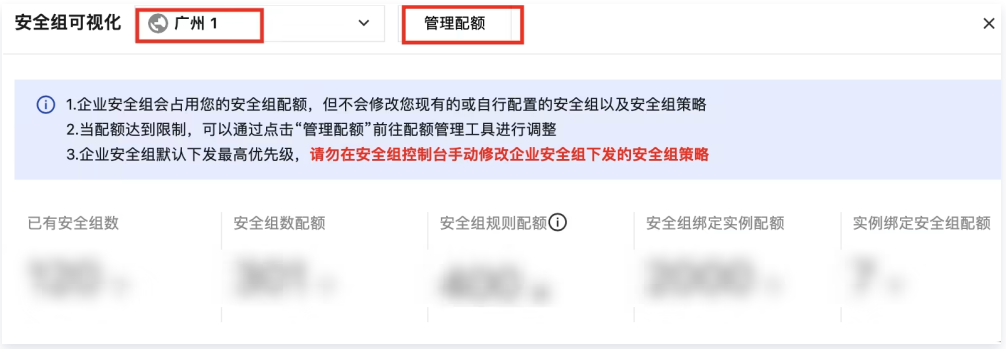
4. After the rule is added, it will be displayed in the rule list.

5. After the rule is added and successfully delivered, you can view the corresponding security group on the security group visualization page of the cloud firewall or in the Security Group Page of the VPC console, and it is automatically associated with instances.

Viewing Security Group Visualization

1. Log in to the Cloud Firewall Console, select **Access Control** > Enterprise Security Group (New) in the left navigation.
2. On the Enterprise Security Group (New) page, click **Security Group Visualization**.

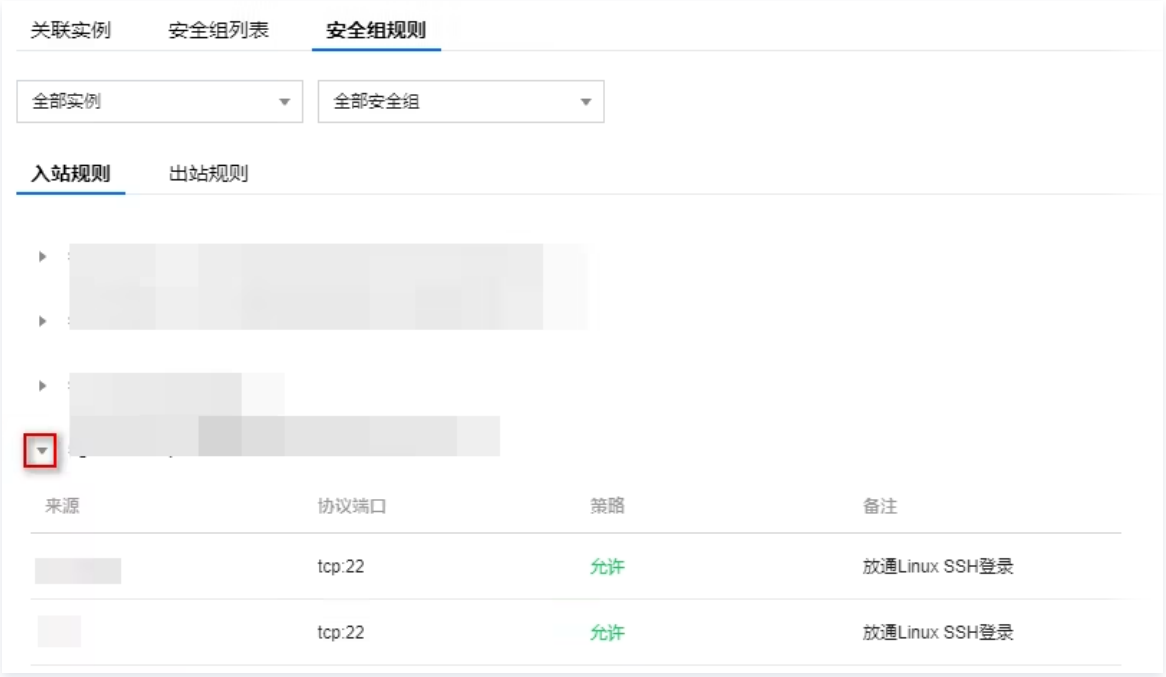
3. On the security group visualization page, you can view the region where the instance is located and various quota information. The security group quota can be expanded according to actual conditions.



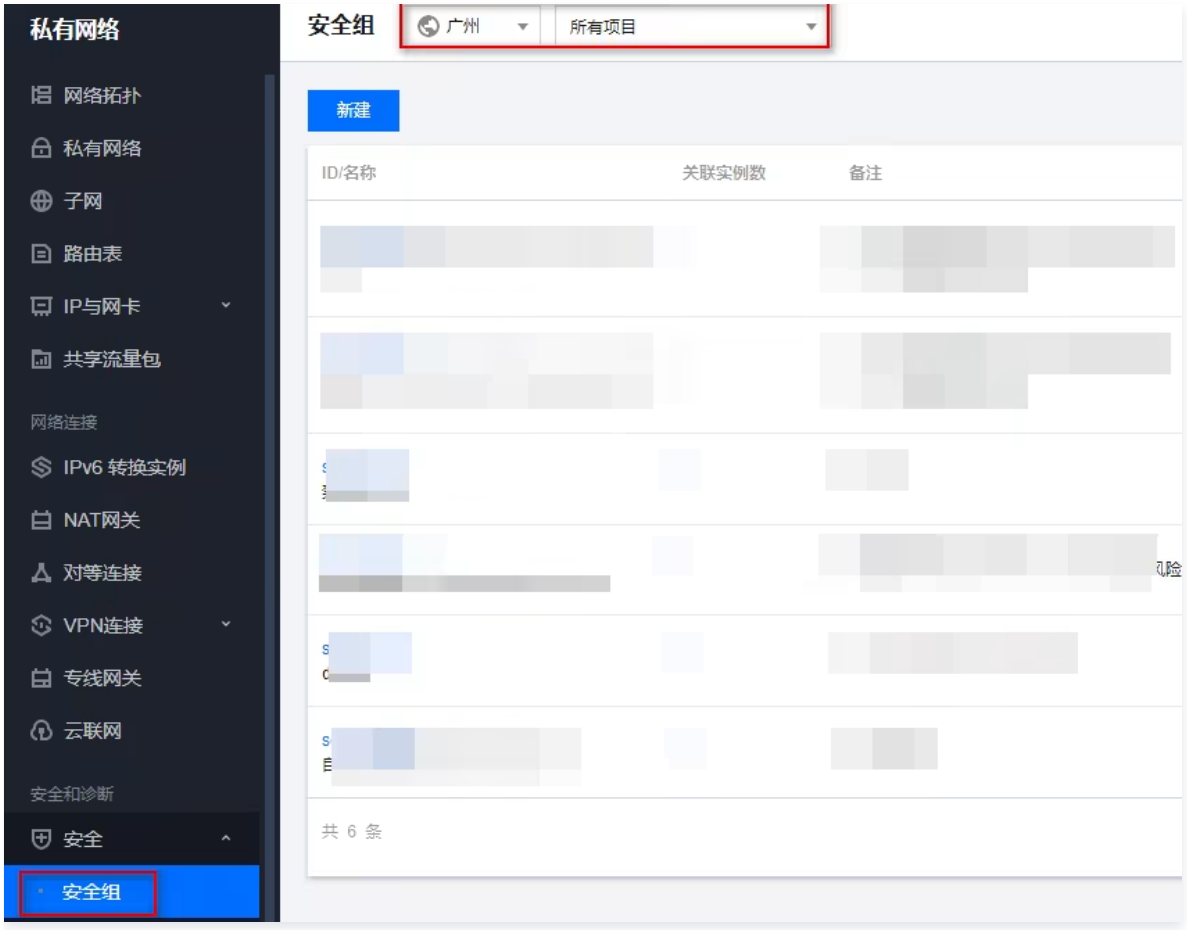
4. Below the security group visualization page, you can view associated instances, security group list, and security group rules.
   - Associated instances: Display all instances in the current region, including instance name, instance type, associated network, IP address, and other information. Click the "number" in the security group or security group rule column to navigate to the security group list or security group rule details page corresponding to a single instance. Click **View Detail** to jump to the instance details page.

   - Security group list: Displays all security groups in the current region, instances associated with each security group, the number of security group rules, creation time, and more. Click the number in the "Associated instance" or "Security group rule" column to navigate to the security group list or rule details page of a single instance. Click **View details** to go to the security group details page in the VPC console.

   - Security group rules: Display all inbound and outbound rules of security groups in the current region. Click ▸ to view rule details or verify whether the enterprise security group has been successfully issued.



5. Log in to the VPC console, click **Security** -> **Security Group** in the left navigation pane, and select the required regions and projects.



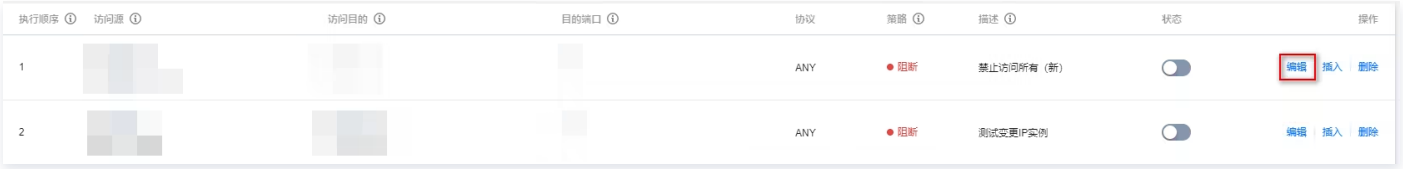
6. Click any security group "ID/name" to view its corresponding inbound rules, outbound rules, and associated instances.

Manage Rules

After completing the setting, you can perform edit, insert, delete, and quick sort operations on rule entries on the Enterprise Security Group (New) page.

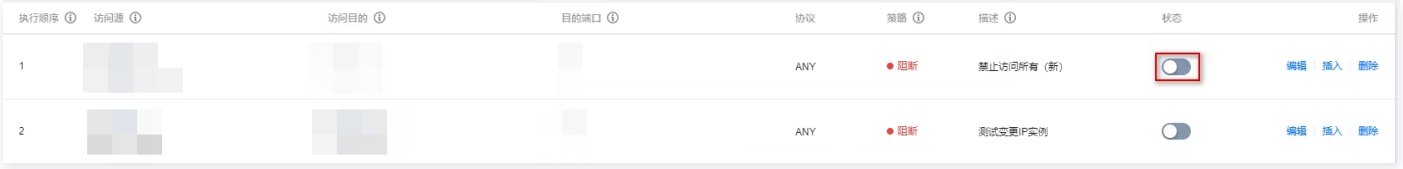
Editing Rules

On the Enterprise Security Group (New) page, select a rule, click **Edit**, modify the relevant parameters, and then click **OK**.



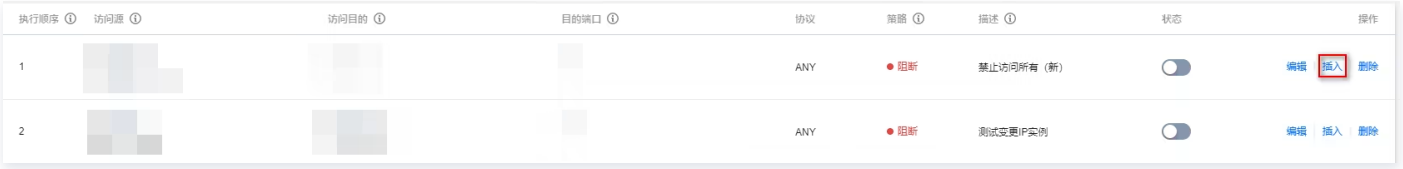
Deactivating Rules

On the Enterprise Security Group (New) page, you can control whether the rule is effective. If you turn off the switch, the rule will be deactivated and will no longer participate in rule-based matching.



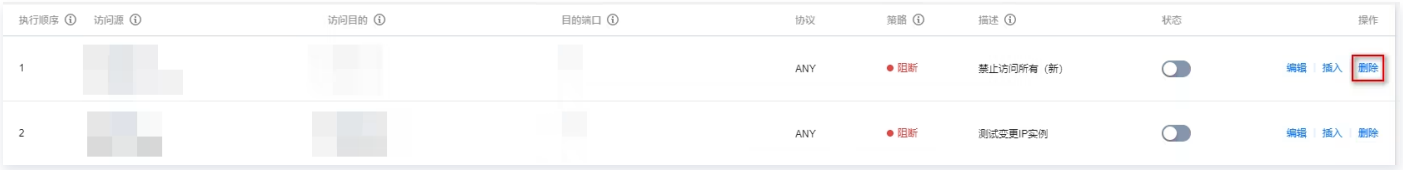
Inserting Rules

On the Enterprise Security Group (New) page, select the desired rule, click **Insert**, enter the relevant parameters, and then click **Done** to add a new rule in front of the current rule with a higher priority than the current rule.



Deleting Rules

On the Enterprise Security Group (New) page, select the desired rule, click **Delete**, confirm the secondary confirmation, and then the target rule can be deleted.



Quick Sort

The order of rules in the list determines the execution priority.

1. On the Enterprise Security Group (New) page, click **Quick Sort**, select the required rule, and drag it to the appropriate position with the left mouse button.

2. After completing the adjustment, click **Save**, and the adjusted priority will take effect. The enterprise security group will automatically push the new rule priority to the instance.

Export a Rule

1. On the Enterprise Security Group (New) page, click ⬇ in the top right corner of the rule list to pop up the custom list export window.

2. In the custom list export window, select to ignore search criteria for full export or export based on search criteria, click **Export** to export the rules.

Enterprise Security Group Flow Log

Last updated: 2025-05-20 11:13:13

Feature Introduction

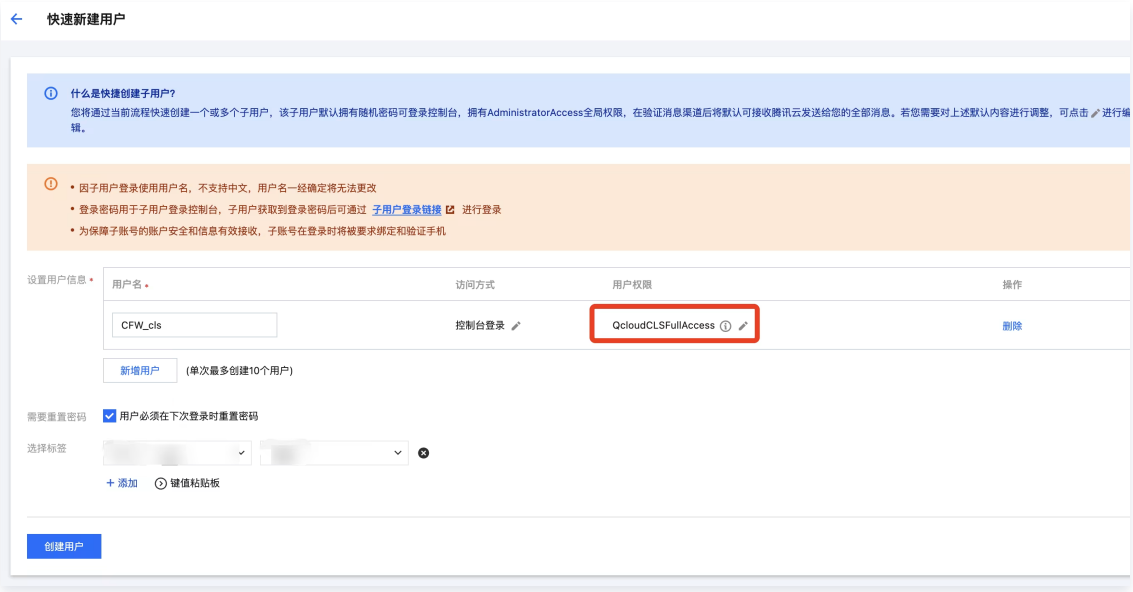
Enterprise security group flow logs will record in real time the traffic status of all security group rules that transit, including blocklist and observation rules. It can cooperate with enterprise security groups to complete cloud isolation and private network traffic audit.

> **Note:**
> Users of editions other than the flagship edition, please submit a ticket to apply for usage of enterprise security group flow logs.

Configuration Guide

Enterprise security group logs depend on network flow logs. It is necessary to collect raw log information from your CLS for processing. So you need to create a role with CLS Permissions and authorize CLS to collect network flow logs.

1. Use **root account** to enter Cloud Access Management - User List Page, create an exclusive API call account for the firewall log delivery task, create a new user and assign full read/write permission (QcloudCLSFullAccess) to CLS. For more details, see Create Sub-users - Quick Creation.

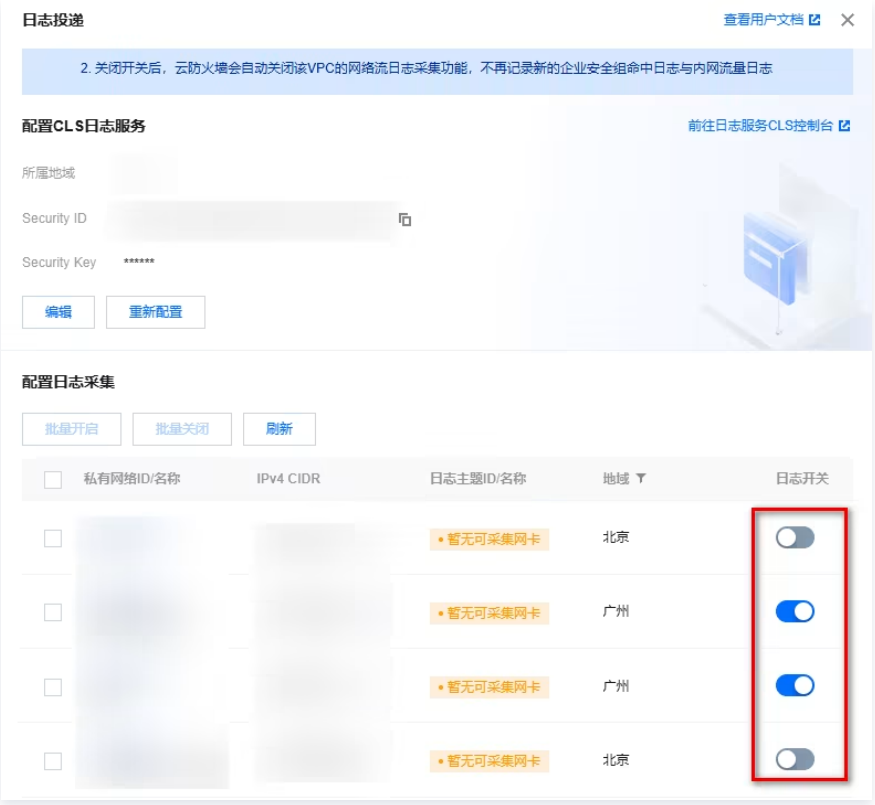


2. 1. On the Access Control - Enterprise Security Group Page, click **Settings Details** of **Enterprise Security Group Logs**.
3. On the page of Enterprise Security Group Log Collection, click **Edit** of **CLS Log Service Configuration**, fill in SecurityID and SecurityKey to perform identity authentication, and click **Save**.

4. Refer to Documentation, go to Role Page to authorize the collection of network flow logs and grant flow log access permissions to CLS with QcloudAccessForVPCRoleInFlowLogAdvanceAnalysis.

5. 1. On the Access Control – Enterprise Security Group Page, click the **Flow Log Switch** of the enterprise security group to enable the flow log feature.

6. Click **settings details** and enable the VPC switch for which inter-private network traffic needs to collect.



Practical Tutorial

Scenario 1: Audit Security Group Intercept Hit

> **Note:**
> Troubleshoot the security group that hits the blocking policy and locate which specific security group rule is blocking traffic.

1. When traffic is blocked by a security group and it is necessary to locate the specific blocking rule.
2. On the Access Control – Enterprise Security Group Page, click **Log Settings** of the enterprise security group and toggle on the corresponding switch of the VPC to be troubleshooted. The enterprise security group will automatically record the hit logs of the security group block.
3. Reproduce the intercepted traffic connection requests. In the access control logs – enterprise security group flow logs, filter by access source/access destination and locate the security group rules that hit the blocking policy.

Scenario 2: Traffic Monitoring Within the VPC (Between Subnets, Within the Subnet)

> **Note:**
> Monitor all traffic within the VPC, including traffic between subnets and within subnets.

1. On the Access Control – Enterprise Security Group Page, click **Log Settings** of the enterprise security group and toggle on the corresponding switch of the VPC to be troubleshooted.
2. The flow log of the enterprise security group will automatically record all traffic conditions in the VPC, including inter-subnet access traffic and intra-subnet traffic.
3. On the Traffic Log – Intranet Traffic Log page, troubleshoot and make records of the traffic between subnets and within the subnet.

Scenario 3: Inter-VPC Traffic Monitoring

> **Note:**
> Monitor all private network traffic entering and exiting the VPC.

1. On the Access Control – Enterprise Security Group Page, click **Log Settings** of the enterprise security group and toggle on the corresponding switch of the VPC to be troubleshooted.
2. The flow log of the enterprise security group will automatically record all traffic entering and exiting the VPC.
3. On the Traffic Log – Intranet Traffic Log page, troubleshoot and make records of the inbound and outbound traffic of this VPC.

Migration Guide

Last updated: 2025-05-20 11:13:36

If you have used a legacy enterprise security group, you can migrate the rules of the legacy enterprise security group to the latest version through the following operations.

Migration Approach

1. Set the rule switch not to auto on.
2. Sort out legacy enterprise security group policies.
3. Migrate configuration to new version of enterprise security group.
4. Enable the new version of enterprise security group switch.
5. Verify whether the policy is successfully delivered and effective.
6. After verification with no problem, delete the earlier version of enterprise security group rules.
7. Complete migration.

> **Note:**
> Migration is at risk. Please confirm carefully whether the verification policy has been successfully issued and made effective.

Step 1: Set the Rule Switch Not to Auto On

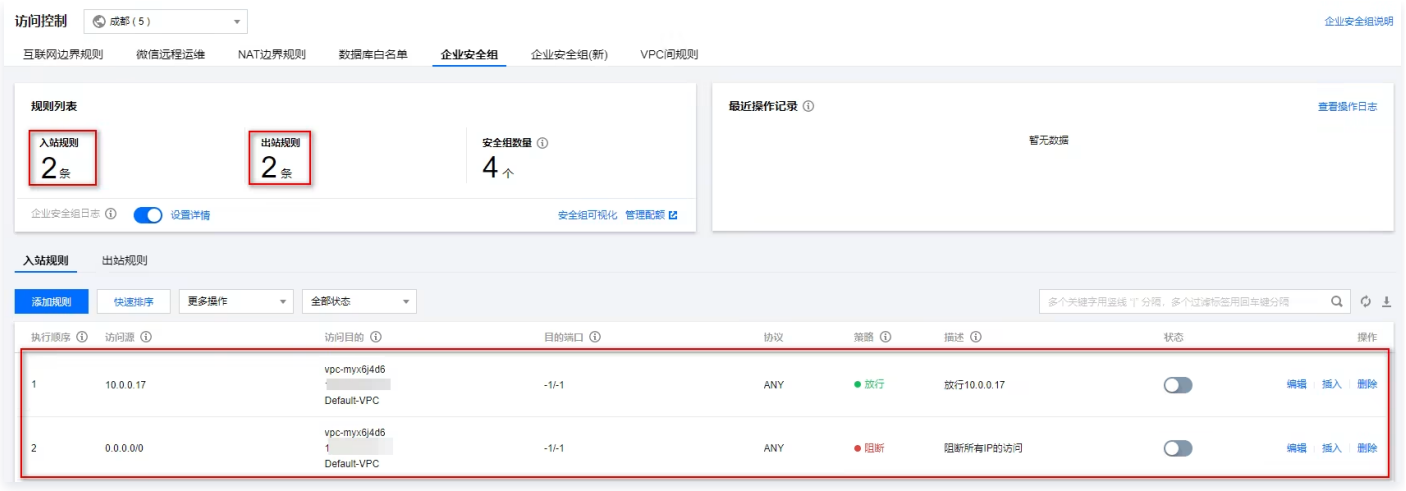
After establishing the new version of enterprise security group rules, the rule switch will not be turned on automatically. You need to turn it on manually, thereby achieving control over the issuance of security group policies, avoiding the impact of rule configuration errors on the business. Specific configuration is as follows:

1. Log in to the CFW console. In the left sidebar, click **General Settings** to enter the General Settings page.
2. On the General Settings page, scroll down to find the Access Control Rule setting item and select **not enabled by default**.

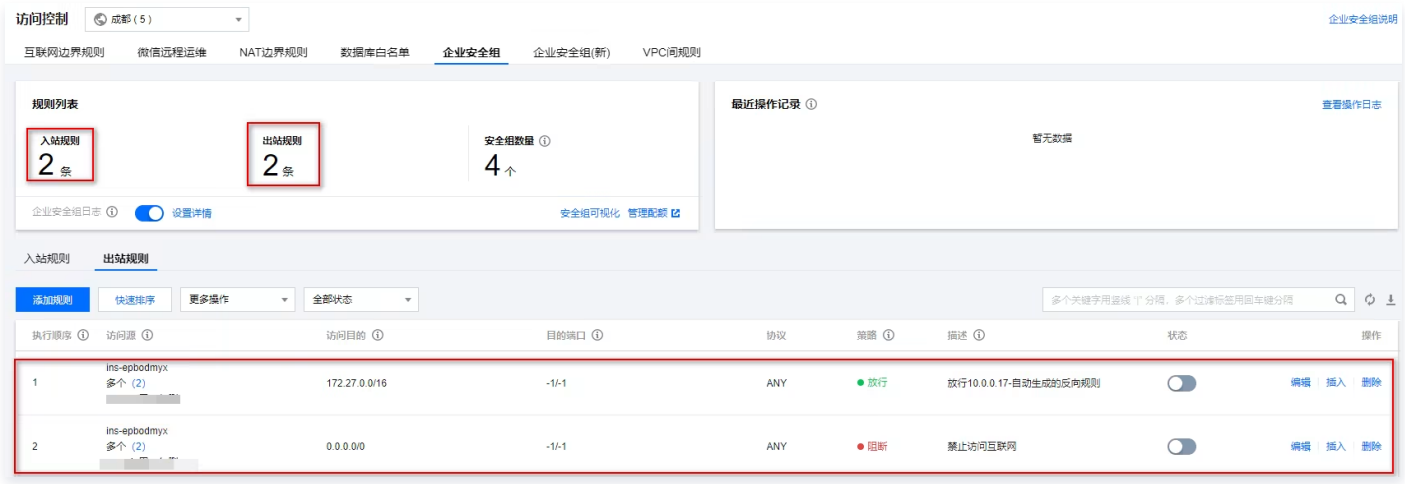
Step 2: Sort Out Legacy Enterprise Security Group Policies

Clarify the inbound and outbound rules of the legacy enterprise security group, which rules are two-way, one-way, and how they are configured, to prepare for the development of new version enterprise security group rules. An example will be used to demonstrate the steps of rule migration. Details as follows:

1. On the Enterprise Security Group > **Inbound Rules** page, it shows that 2 inbound rules and 2 outbound rules are configured for the Chengdu region. Among them, the first inbound rule targets the instance `vpc-myx6j4d6` and sets one inbound policy to allow `10.0.0.17` to access. The second one also sets one inbound policy to forbid all other IPs from accessing.



2. Click **Outbound Rules** to switch page. Obviously, the first rule is an inbound creation rule with bidirectional distribution automatically generated when checked. That is, an outbound rule is automatically generated targeting `ins-epbodmyx` this access source, allowing access to `vpc-myx6j4d6` this instance. The second rule is a manually set rule prohibiting `ins-epbodmyx` from accessing other IPs.



3. The above is an example of rule analysis for the legacy enterprise security group. Specifically, each environment needs to be analyzed according to actual conditions. After the analysis is completed, the rules need to be migrated to the new version of enterprise security group.

Step 3. Migrate to New Version of Enterprise Security Group

Introduce how to configure the new version of enterprise security group to achieve the same effect.

1. First, let me introduce what changes have been made to the configuration interface of the new version of the enterprise security group. As shown below, the new version has added configuration items such as IP and region. It can achieve access control between two IP ranges as well as two-way access control from IP, asset instance, and asset group to region.

2. After introducing the configuration rules of the new version, let's see how to configure the above two inbound and outbound scenario rules. There are two key points for inbound policy configuration: one allows `10.0.0.17` to access `vpc-myx6j4d6`; one forbids all IPs to access `vpc-myx6j4d6`. The specific configuration is as shown in the figure below:

   2.1 On the Enterprise Security Group (New) page, click **Add Rules**, and the Add Rules window pops up.

   2.2 In the Add Rules window, configure the related parameters and click **OK**.

Parameter Name	First Rule	Second Rule

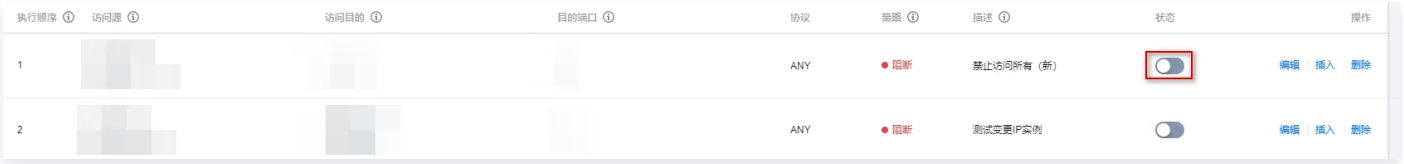
Access source type	IP/CIDR	IP/CIDR
Access destination type	Select asset instances	Select asset instances
Port protocol type	Custom	Custom
Rule Priority	Custom	Custom
Access source	10.0.0.17	0.0.0.0/0
Access Destination	vpc-myx6j4d6	vpc-myx6j4d6
Destination Port	ALL	ALL
Protocol	All	ALL
Policy	Allow/Release/Pass (select according to specific scenarios)	Block
Description	Custom	Custom

3. Wait a few seconds for it to be distributed to the security group of the asset, and then you can migrate the legacy enterprise security group policy to the new version of enterprise security group.

Step 4. Enable the New Version of Enterprise Security Group Switch

Enable the rule switch of the new version of security group rules to make the rule effective.

1. On the Enterprise Security Group (New) page, select the required rule, click under the status column, in the "Confirm Enable" pop-up window, click **OK**, and the rule takes effect.

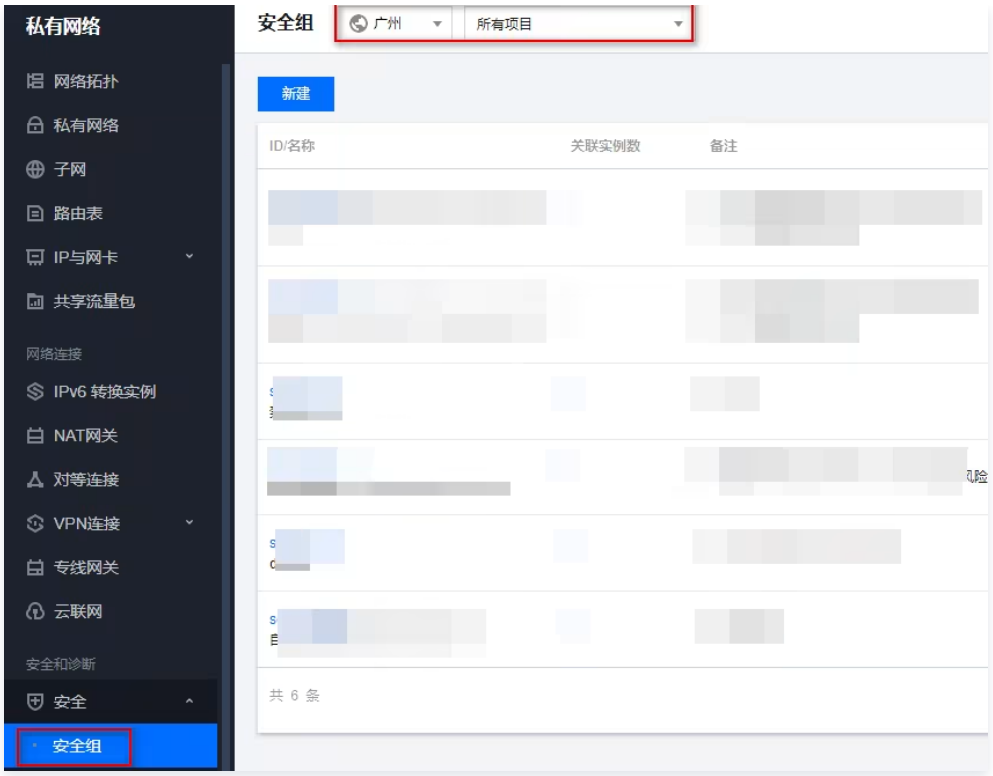


2. In the "Confirm Enable" pop-up window, click **OK**, and the rule takes effect.

Step 5: Verify Whether the Policy Is Successfully Delivered and Effective

After enabling the rule, you need to take a look at the security group of the instance to see whether the policy has been successfully issued.

1. Log in to the VPC console. In the left sidebar, select **Security** > **Security Group**, and select the desired region and project.



2. On the security group page, the security group policy highlighted in the red box is issued by the enterprise security group. The annotation with the text "cfwsg" below also indicates that this rule is created by CFW.

3. Click any one of the security group "ID/Name", verify whether the above rules are successfully issued, as shown below, two inbound rules are successfully issued.

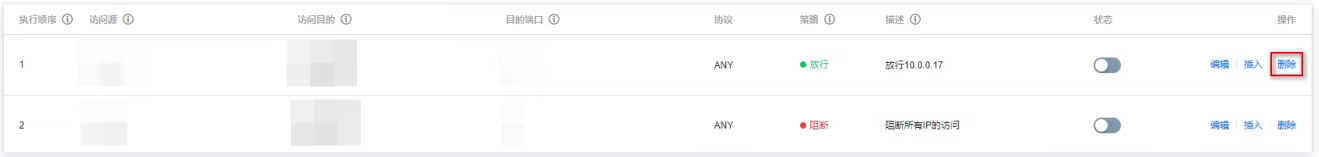
4. Click **Outbound Rule** to switch page. As shown below, the outbound rule is also delivered successfully.

> **Note:**
> Article 1 rule is automatically generated in both directions. That is, a rule allowing `10.0.0.17` to access is created in the inbound direction of `vpc-myx6j4d6 (172.27.0.0/16)`. Correspondingly, for `10.0.0.17`, an outbound rule allowing access to `vpc-myx6j4d6 (172.27.0.0/16)` will be automatically generated in its outbound direction. Article 3 rule prohibiting all access has also been successfully issued.

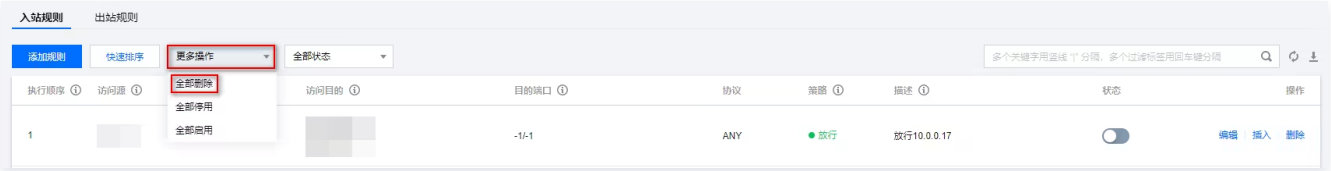
Step 6: Delete Legacy Enterprise Security Group Rules

After the above verification that there is no problem with the issuance of the new version of rules, you can delete the old version of rules.

1. On the Enterprise Security Group > **Inbound Rules** page, support deleting each or all rules. The specific operations are as follows.
   - Select the desired rule, click **Delete** in the Action column. A "Confirm Deletion" window pops up.



   - All: click **More Operations** > **Delete All**, and a "Confirm Deletion" window pops up.



2. In the "Confirm Deletion" window, click **Confirm** to delete the rule.

Step 7: Complete the Migration

The above is an introduction to the method of migrating enterprise security groups from the old version to the new version. Subsequently, you can add security group rules on the Enterprise Security Group (New) page. For detailed operations, see Configuration Steps.

Hotspot Issues

Last updated: 2025-05-20 11:13:55

Why Launch a New Version of Enterprise Security Group?

Legacy enterprise security groups are relatively cumbersome in terms of configuration and management. The new version of enterprise security group has made some improvements on the basis of the earlier version, mainly optimizing in aspects such as configuration items and logic. Rule matching conditions are more fine-grained, and policies are more intuitive, making it easy to understand and manage.

What Are the Strengths of the New Version of Enterprise Security Group Compared with the Legacy Enterprise Security Group?

The new version of enterprise security group has following characteristics:

- The bidirectional delivery button is removed. When configuring rules, one inbound rule and one outbound rule will be automatically generated.
- The direction concept of inbound rules and outbound rules is removed. Only need to define the access source and access destination to complete the rule configuration.
- The region limit is removed. All rules are displayed on the same interface, making it easier for Ops management.
- A configuration item addition includes options such as IP/CIDR, region. The options are symmetrically arranged and can be combined in any way.
- When adding a new access source or access destination and the configuration is an IP address, it will automatically hit the corresponding instance of the IP.

Can Two Versions of Enterprise Security Groups Coexist?

The features of new and old versions of enterprise security groups can be used together. However, the priority of the new version of enterprise security group is higher than that of the old version. If a policy of the new version of enterprise security group is configured, the matching order of the policy will be to match the new version first and then the old version.

Can the Legacy Enterprise Group Still Be Used?

After launching the new version of enterprise security group functionality, the old version will continue providing services and can still be used.

How to Migrate the Rules of the Legacy Enterprise Group to the New Version of Enterprise Security Group?

For detailed operations on migrating legacy enterprise group rules to the new version of enterprise security group, for details, see Migration Guide.

Special Use Cases

Last updated: 2025-05-20 11:14:14

This document will introduce the special use cases of the access control feature of the Cloud Firewall.

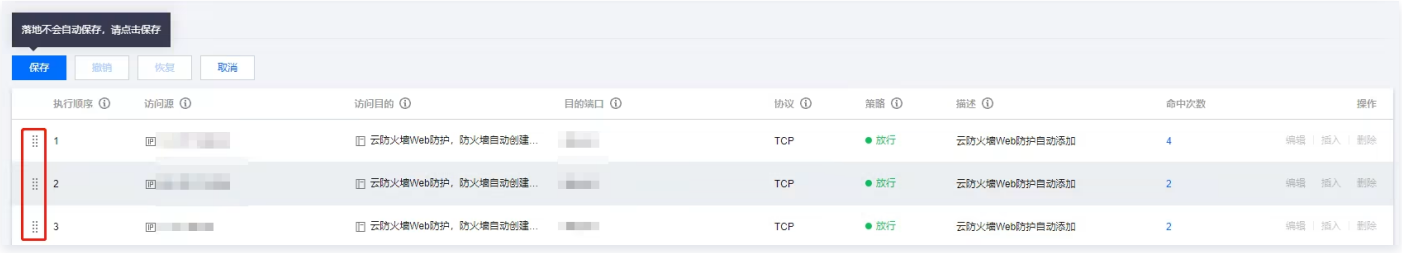
Execution Order of Management Rule List

Internet boundary rules, NAT boundary rules, and Inter-VPC rules all support managing the execution order of the rule list. Next, "Internet boundary rules" will be used as an example for illustration.

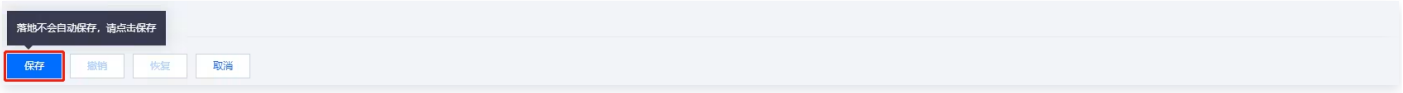
Scenario 1: Perform Quick Sort on Rules Within the List

1. Log in to the CFW console. In the left sidebar, select **Access Control** > **Internet Boundary Rules**.
2. At the top of the rule list on the internet boundary rules page, click **Quick Sort** to enter edit mode for the list.

3. User can batch move the location and sequence of rules within the current page range and sort the rules by dragging the icon in front of the rule.



4. Once the moving is completed, click **Save** to take effect.



Sorting operation instructions:

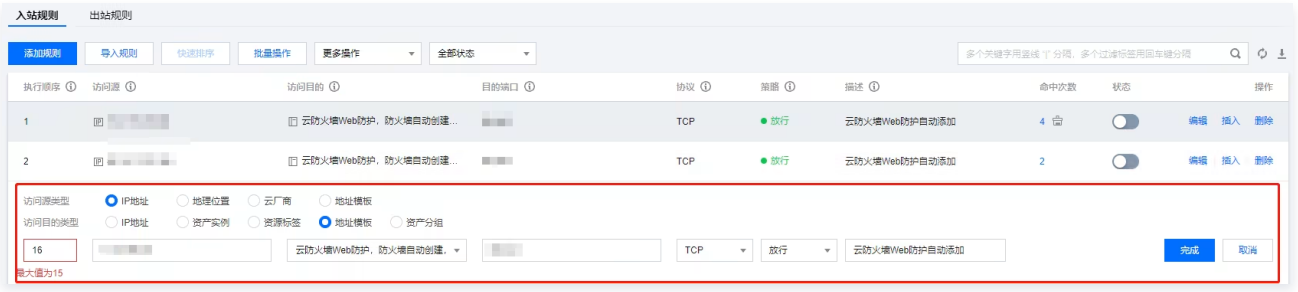
- Each time you release the mouse, the rule that causes the **position** to change is implemented, which is considered a sorting operation.
- If the **position** does not change after you release the mouse, it is not a sorting operation.
- After a sorting operation has occurred, the **undo** button lights up.
- Click **restore** once, and the list returns to the state after the last sorting operation.
- Click **Save**. Once completed, a sorting **completion** prompt will appear at the top of the page.
- Click **cancel**, and the list will return to its initial status, and all sorting operations will be invalid.

Scenario 2: Move the Rule to a Specified Location by Editing

When you need to move a rule over a large range, the quick sort feature may not efficiently perform this operation. Therefore, you can use the edit feature to quickly move the current rule to a specified position. Unlike quick sort, the edit feature allows you to modify the execution order of one rule at a time.

1. Log in to the CFW console. In the left sidebar, select **Access Control** > **Internet Boundary Rules** to enter the internet boundary rules page.
2. In the rule list on the internet boundary rules page, locate the rule to be moved and determine the desired position for the movement.
3. On the right side of the rule, click **Edit** to enter rule editing mode.
4. Modify the value in the execution order field to the desired position's execution order value.

> **Note:**
> Due to the principles of non-repetition and continuity of execution order, when moving a rule via editing, the minimum value for reasonable input of the execution order is 1, and the maximum value is the current quantity of rules in the list.



5. Click **Complete** and check whether the order of rules in the list is as expected.

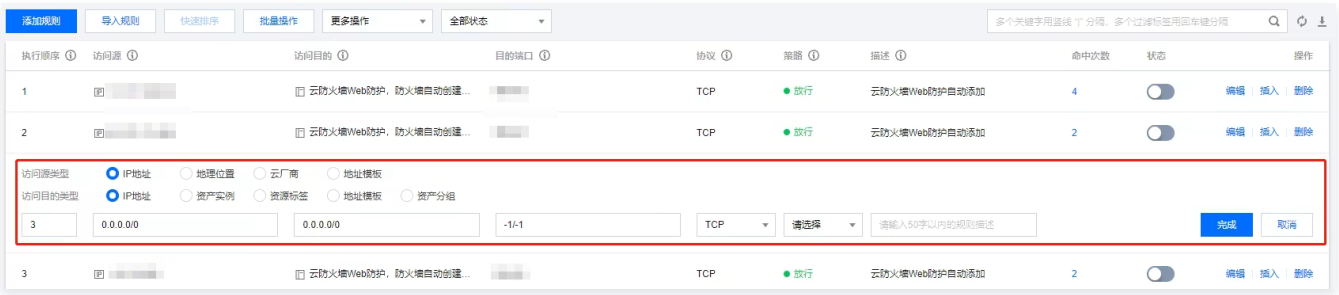
> **Note:**
> By editing a rule, you can change its position in the list, thereby directly adjusting its execution order to the desired position. Automatic movement and adjustment of all other rules will also occur.

Scenario 3: Insert a Rule at a Specified Position in the Existing List

The Cloud Firewall supports inserting a rule between any two rules. The execution order of the inserted rule is the current insertion position.
Rules are inserted in a pre-insertion manner. If you need to insert a new rule between rules with execution orders "2" and "3":

1. Log in to the CFW console. In the left sidebar, select **Access Control** > **Internet Boundary Rules** to enter the internet boundary rules page.
2. In the rule list on the internet boundary rules page, find the rule with an execution order of "3" and click **Insert** on the right side of the rule.
3. Pop up the rule editing box above the rule with an execution order of "3".
4. In the rule editing box, fill in rule fields and click **Complete** to complete rule insertion.

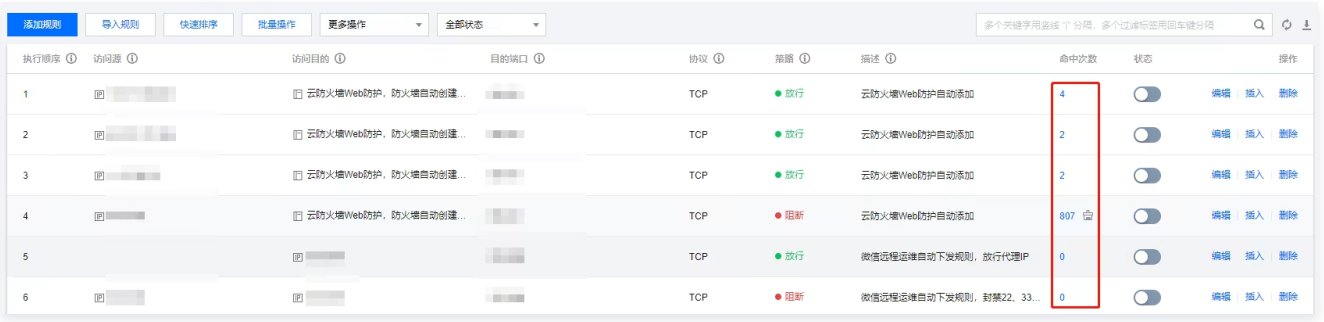
> **Note:**
> After completing the insertion operation, the execution order of the inserted rule replaces the execution order of the rule below it, and the execution orders of all rules below the inserted rule are incremented by "1".



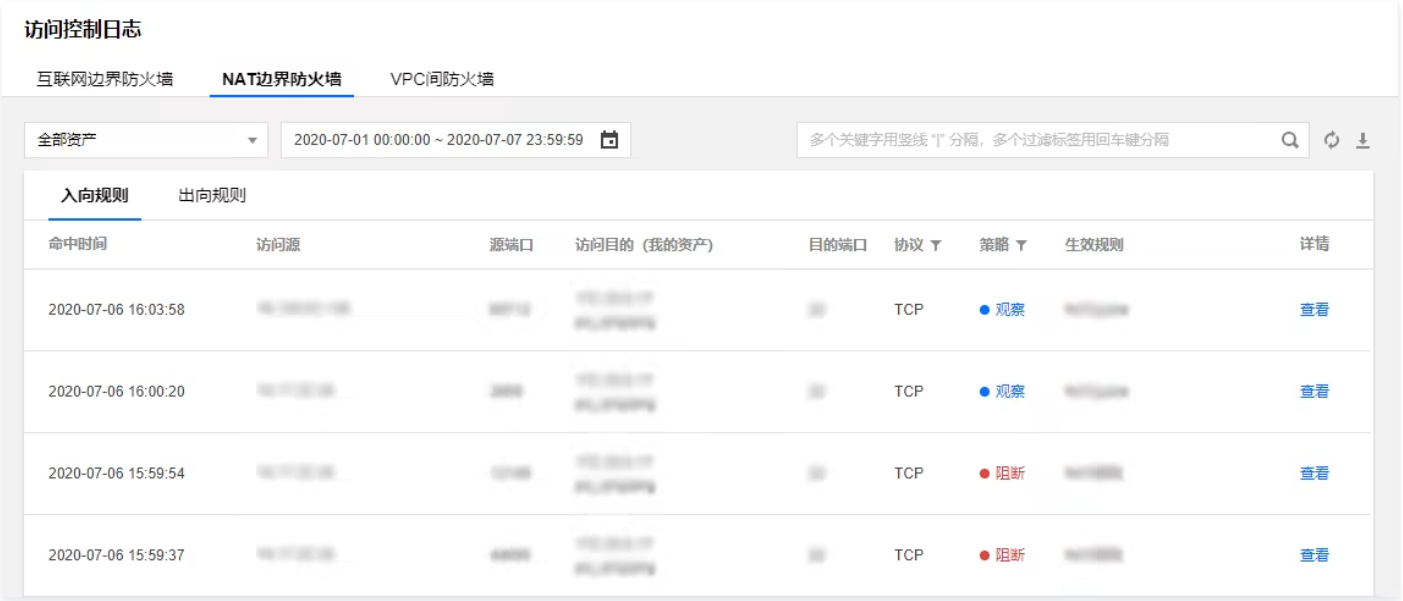
View Whether the Rule Is Effective

- **Method 1:** Check the hit count in the access control list. If there is a hit count, the rule is effective.

> **Note:**
> If the number of rule hits is zero, it only indicates that the rule has not been hit yet. It can be understood as not taking effect temporarily, but does not necessarily mean that the rule is configured incorrectly.



- **Method 2:** In the left sidebar, select **Log Audit** > Access Control Log to view the access control log (rule hit log). If you see relevant rules in the access control log, it means that the rule is effective.



Operation Lock

For the same access control list of the same AppID (VPC uses firewall ID to distinguish), only one user is allowed to perform any one of the following operations: Add Rules, Import Rules, Quick Sort, Edit, or Insert at the same time.
When a user sees the prompt "The list may be currently in use by someone else and is locked. Please try again later" at the top of the page while performing operations on the list, it means that another user is currently working on the same list.

> **Note:**
> The validity period of the operation lock is 5 minutes and it will be automatically released after that time.

Information Related To

If you encounter any access control-related issues, see Access Control document.

Intrusion Prevention
Enabling Threat Intelligence

Last updated: 2025-05-20 14:18:35

After the threat intelligence is enabled, the CFW will connect internet boundary traffic to the threat intelligence detection and analysis engine to identify unknown risks beyond access control rules. For important period guarantee scenarios, the prioritized protection package feature has been introduced to enhance the risk resistance capability.

Operation Steps

1. Log in to the CFW console, and click **Intrusion Prevention** in the left sidebar to enter the intrusion prevention page.
2. On the intrusion prevention page, click  under Threat Intelligence to enable threat intelligence.

> **Note**
> The threat intelligence switch and Internet boundary firewall switch are combination logic switches. Only when the Internet boundary firewall switch is enabled for a certain public IP and the threat intelligence switch is enabled, will CFW monitor and analyze the threat intelligence of the north-south traffic of this public IP.

3. After the threat intelligence is enabled, the CFW will connect internet boundary traffic to the threat intelligence detection and analysis engine to identify unknown risks beyond access control rules:
   - Monitor and identify malicious IPs and threat samples such as malicious scans from external sources, brute force cracking, mining trojans, ransomware, and remote control that initiate access to cloud assets.
   - Proactive external activities: Monitor and identify proactive external activities initiated by cloud assets to external malicious IP addresses or domain names, and determine the possible occurrence of host compromise risks based on big data comparative analysis provided by threat intelligence.
4. Enable the Prioritized Protection special intelligence package functionality. The Prioritized Protection special intelligence package is formed via crowdsourcing by the attack-defense team during the critical maintenance period. On the Intrusion Prevention Page, click **View Details** at the threat intelligence section. Click  to enable the Prioritized Protection special intelligence package switch. Once enabled, IPs in the intelligence package will automatically be added to the blocklist, intercepting all access behavior.

> **Description**
> The special intelligence package feature for major events protection is only available for CFW flagship edition users to purchase and use.

Information Related To

If you encounter any intrusion prevention related issues, see Intrusion Prevention document.

Enabling Basic Defense

Last updated: 2025-05-20 14:18:55

After enabling basic defense, intrusion prevention rule testing can be performed on the north-south traffic of public network IPs.

Operation Steps

1. Log in to the CFW console. In the left sidebar, click **Intrusion Prevention** to enter the intrusion prevention page.
2. On the intrusion prevention page, find the "Basic Defense" module and click **View Rules**. The basic defense rule list pop-up will appear.

3. In the basic defense rule list pop-up, you can view the Tencent Cloud IPS rule list. Click **rule ID** to view the corresponding rule description.

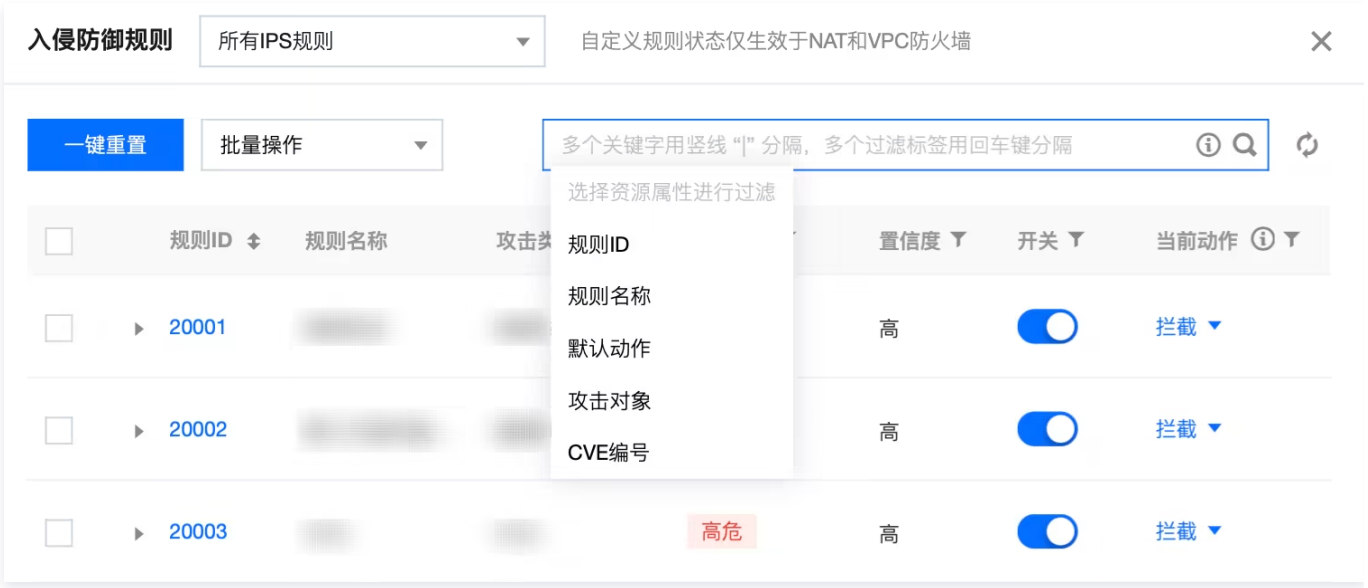
4. Click the switch to specify whether the rules take effect for NAT and VPC firewalls.

> **Note:**
> If the version of some firewall engines is too low, the corresponding firewall will not take effect.

5. In the current action column, you can select the rule action after rule match. Rule action is only effective for assets whose protection mode is interception mode.

Note:
The custom intrusion prevention rule feature only takes effect for customers of the Enterprise Edition or higher, and only takes effect on the NAT boundary firewall and the VPC boundary firewall. If the version of some firewall engines is too low, the corresponding firewall will not take effect.

6. For all IPS rules, support keyword search, one-click reset, and batch operation.
   - Keyword search: Support querying corresponding rules based on rule attributes, thereby enabling the setting of switch status and disposition actions.



   - One-click reset: Supports one-click restoration of the switch status of all rules and switches the action to the default action, taking effect immediately.

- Batch operation: Supports selecting multiple rules for batch enabling, disabling, or toggling disposal actions.

7. Learn about the rules. In the "Basic Defense" module, click  at the basic defense to enable basic defense.

> **Note:**
> - After the Basic Defense switch is disabled, all basic defense rules will no longer take effect.
> - The basic defense switch and Internet Boundary Firewall switch are composite logic switches. Only when a certain public IP address enables both the Internet Boundary Firewall switch and the basic defense switch, will CFW perform intrusion prevention rule testing on the north-south traffic of this public IP address.
> - In interception mode, some high-confidence rules support automatic interception, while other rules still generate security event alarms.

Information Related To

If you encounter any intrusion prevention-related issues, please refer to the Intrusion Prevention document.

Enabling Virtual Patch

Last updated: 2025-05-28 10:34:57

After enabling virtual patch, CFW will automatically identify and intercept all exploitable and attack traffic in the north-south traffic, thereby avoiding exposure of vulnerabilities in CVM to the Internet.

Operation Steps

1. Log in to the Cloud Firewall console, and click **Intrusion Prevention** in the left sidebar to enter the intrusion prevention page.
2. On the intrusion prevention page, find the "Virtual patch" module and click **View rules**. A virtual patch rule list pop-up will appear.

3. In the virtual patch rule list pop-up, you can see all applied patch rules. Click **rule ID** to view the application description of the patch rule.

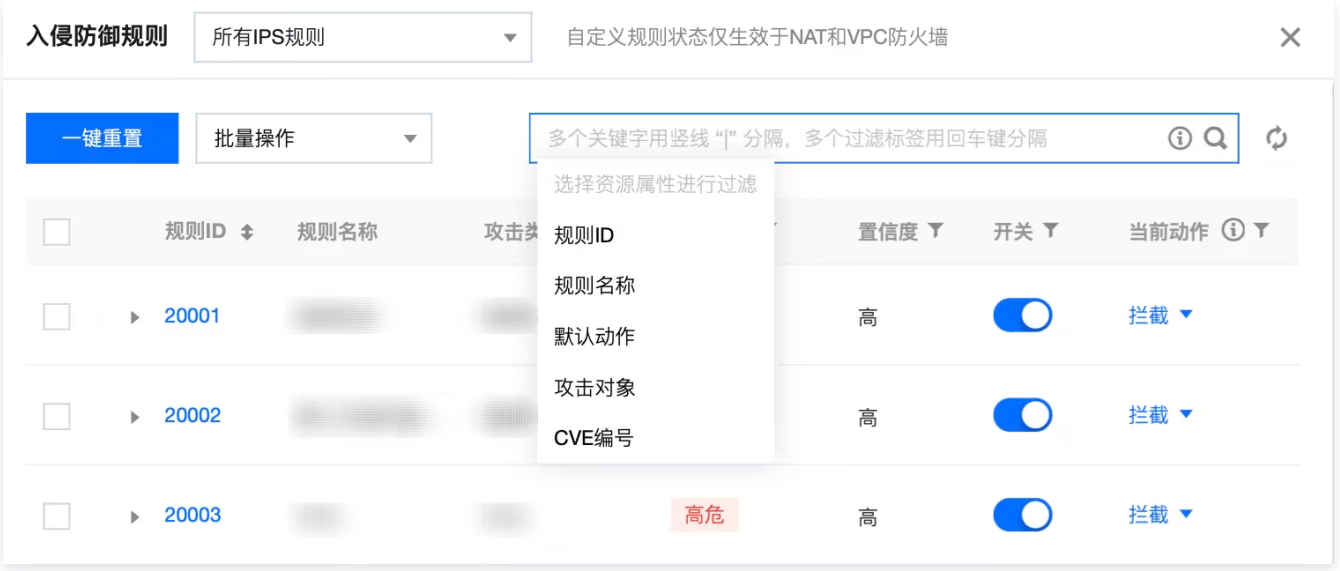
4. Click the switch to specify whether the rule takes effect for NAT and VPC firewalls.

> **Note:**
> If version of some firewall engines is too low, corresponding firewall will not take effect.

5. In the current action column, you can choose the rule action after hitting the patch rule. The rule action is only effective for assets whose protection mode is interception mode.

Note:
Custom intrusion prevention rule feature **only takes effect on enterprise edition and above customers**, and only takes effect on NAT boundary firewall and VPC boundary firewall. If the version of some firewall engines of yours is too low, the corresponding firewall will not take effect.

6. For all IPS rules, support keyword search, one-click reset, and batch operation.
   - Keyword search: Support querying corresponding rules based on rule attributes, thereby enabling the setting of switch status and disposition actions.



   - One-click reset: Supports one-click restoration of the switch status of all rules and switches the action to the default action, taking effect immediately.

- Batch operation: Support selecting multiple rules to enable, disable in batch, or switch the handling actions.

7. After viewing the patch rules, in the "Virtual patch" module, click  at the virtual patch to enable virtual patching.

> **Note:**
> - When the virtual patch switch is enabled, the corresponding rule of the virtual patch takes effect on the public IP where the switch is turned on.
> - The corresponding rule of the virtual patch does not take effect when the virtual patch switch is set to "Off".
> - In the interception mode, all intrusion activities are automatically blocked.

Information Related

If you encounter any intrusion prevention related issues, see Intrusion Prevention document.

Using a Security Baseline

Last updated: 2025-05-20 14:19:54

this document guides you through the basic concepts and running processes of CFW security baseline, and how to use the security baseline feature through the CFW console to maintain product health and stability.

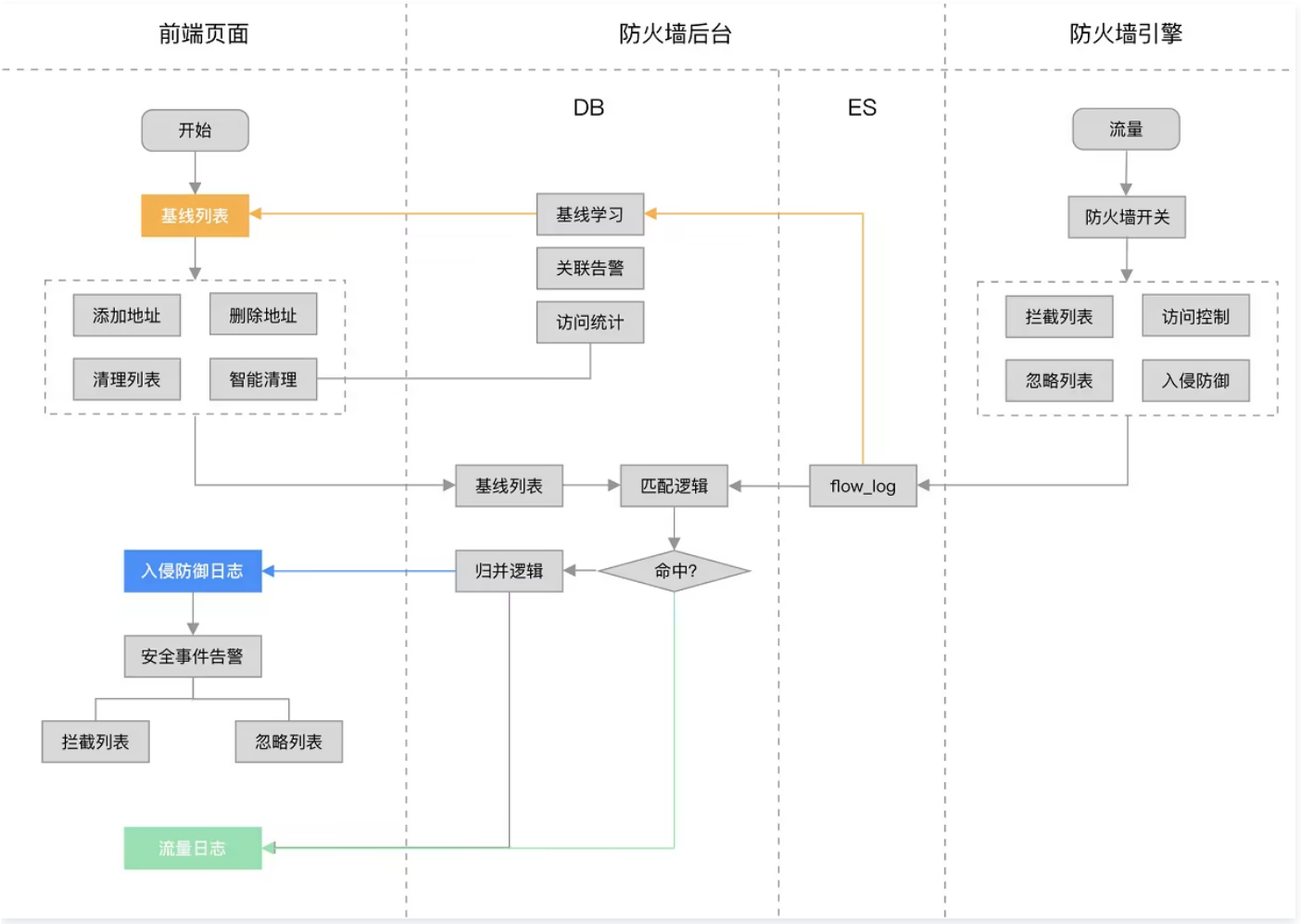
Background Information

What Is the Security Baseline of CFW

A security baseline refers to a preliminary IP address or domain name access list that the Cloud Firewall forms by observing traffic access within a certain time frame. Users can maintain the baseline list by adding or deleting IP addresses or domain names based on security scores, associated security events, and network access conditions, thereby forming the final **security baseline**.
After the security baseline is set, any newly-added IP address or domain name access outside the baseline will trigger a security alarm. Users can handle IP addresses or domain names in the alarm list. The security baseline is applicable to traffic baseline protection during the critical maintenance period.

Operating Principle of Security Baseline

The operating principle of the security baseline is illustrated in the figure below:



The security baseline generates a preliminary security baseline list by learning traffic logs, combining access details and associating alarm records. Users can maintain the baseline list in this list by using features such as smart cleanup, adding addresses, deleting addresses, and clearing the baseline to enhance the baseline score and generate the final IP access allowlist (i.e., the security baseline list).
Once the security baseline is established, for subsequent accessed IP addresses that belong to the security baseline, they will be deemed Trusted IPs and merged into the Traffic Log for log audit. If they are outside the baseline, they will all be determined as

malicious addresses to trigger alarms and merged into the alert center. Users can "blocklist" or "ignore" the IP addresses of security baseline alarms on the security event alert page in the Alert Center to complete event handling.

Prerequisites

The security baseline is available only for flagship users. Please ensure that you upgrade to flagship edition user before starting configuration.

Operation Steps

Procedure 1: Configure safety baseline rules.

1. Log in to the Cloud Firewall console, and click **Intrusion Prevention** in the left sidebar to enter the intrusion prevention page.
2. On the intrusion prevention page, find the **Security Baseline module**, click **View Rules** to go to the Security Baseline page.

3. The first time you enter the security baseline page, you need to configure the safety baseline rules.

Field Description:

- **Start time**: The time when the security baseline starts traffic observation. Click "calendar" to set a custom start time. The earliest option is 00:00, 30 days ago.
- **End time**: The time when the security baseline completes traffic observation. Click "Calendar" to customize the termination time. You can choose a time up to 23:59:59 30 days later at the latest.

> **Note:**
> The analyzable time range is from the date of use of the firewall to the data of the next 30 days.

- **Traffic type**: Select the traffic direction for establishing the security baseline.

  > **Note:**
  > The traffic type only selects the outbound direction by default. If there are special requirements, please submit a ticket to contact us.

- **Remove asset**: The related traffic under the removed asset will not be counted into the analysis object of the security baseline.

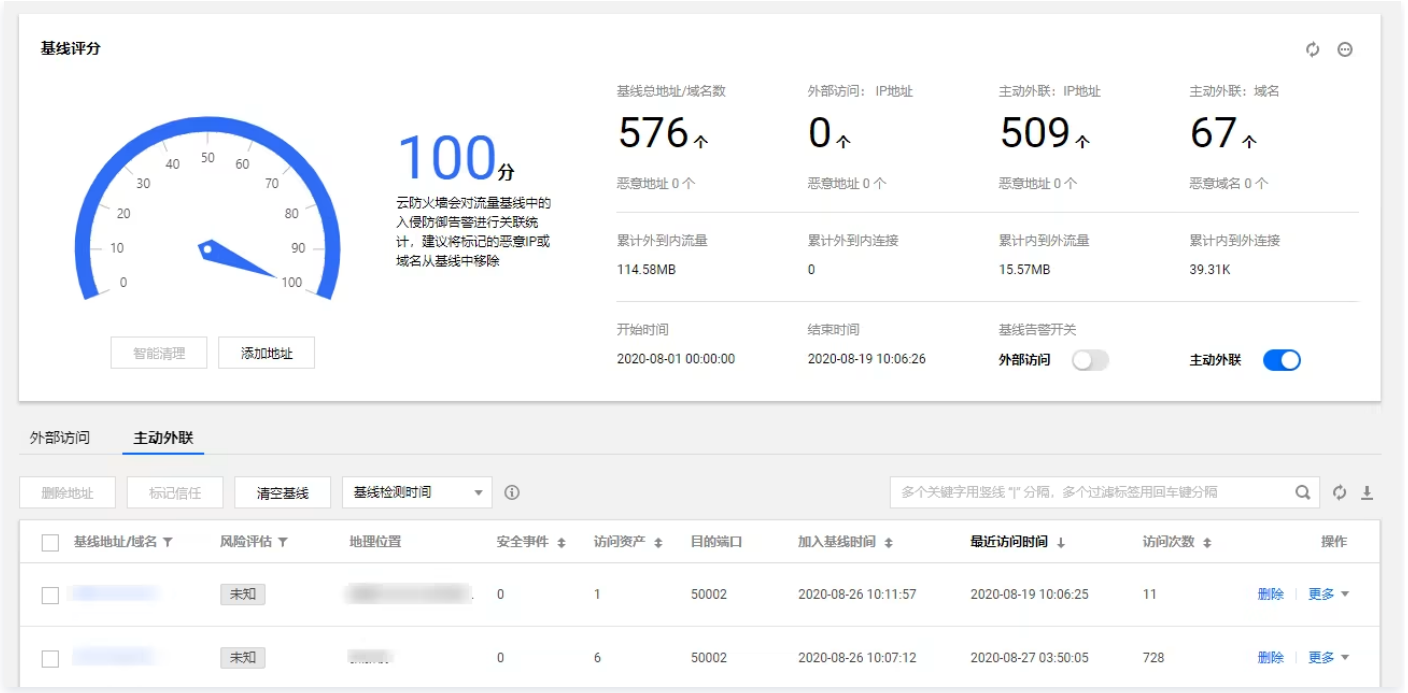
4. Click **Confirm** to configure successfully.

Procedure 2: Execute Security Baseline Learning Tasks

1. After configuring the security baseline rules, the page will automatically start baseline learning. Users can view the learning progress in the bottom-right corner.

> **Note:**
> - The backend will perform baseline learning based on the assets after removal, and subsequently only trigger warnings targeting the assets within the baseline.
> - Analysis tasks take some time (depending on network conditions). You can view the progress through the task status in the bottom-right corner.
> - Click **End Task** to force terminate the security baseline analysis and use the analyzed list as the security baseline.

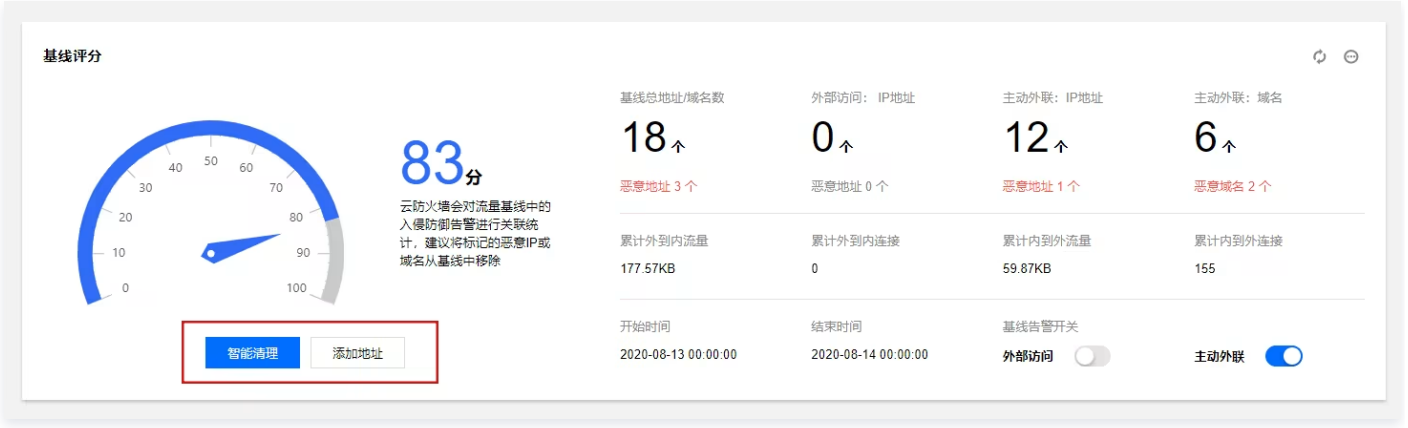
2. After learning is finished, the security baseline will learn the traffic of the selected time period according to the user, extract information, generate statistical results for the user, and create an access details list at the bottom of the current page.
   - **Baseline score**: An assessment of the current access environment based on the proportion of malicious IP addresses in the list. It provides a reference metric for users' subsequent security baseline maintenance and guides users to continuously improve baseline security.
   - **Access details list**: It contains IPs/domains in two orientations: external access and proactive external activities. Users can choose the baseline learning time/baseline check time to view the IP information in the security baseline within different time ranges.
     - **Baseline learning time**: Statistical data within the time range from the baseline start time to the baseline end time.
     - **Baseline inspection time**: Add statistical data from the baseline time to within the current time range.



Procedure 3: Edit and Maintain Security Baseline

After the learning process is finished, users can, based on the **baseline score**, use smart cleanup and manually add or delete to **improve** the current baseline list's **security index**. The security baseline can be maintained in the following two ways:

- Users can click **Smart cleanup** or **Add address** on the security baseline page to automatically or manually edit the security baseline list.



- In the security baseline list, select a baseline address or domain name, and click **Clear baseline** or **Delete** to delete the IP address or domain name in the security baseline list.

The following is a detailed introduction on how to use smart cleanup, add address, remove address and clear baseline features:

Smart cleanup

Perform one-click cleaning of malicious addresses in the baseline list. The CFW will automatically perform statistics on associated tags for intrusion prevention alerts in the traffic baseline and remove malicious IPs or domain names marked as "untrusted" from the baseline. Subsequent access will trigger a warning.

> ⚠ **Note:**

> When all addresses or domain names in the external access and proactive external activities lists have the **trust** tag, the **smart cleanup** functionality will not be available.

1. Log in to the CFW console. In the left sidebar, click **Intrusion Prevention** to enter the intrusion prevention page.
2. On the intrusion prevention page, find the **Security Baseline module**, click **View Rules** to go to the Security Baseline page.

3. In the "Baseline score" module, click **Smart cleanup**. The "Smart cleanup security baseline" popup will appear.
4. In the "Smart cleanup security baseline" pop-up window, select the baseline type and the number of IPs detected by the system.

5. Click **OK**. The system will start to automatically clear the "untrusted" IP or domain name in the baseline list.

Add address

Customize the security baseline allowlist. If there are specific trusted IPs or domain names, you can manually add the IP or domain name to the security baseline list. Subsequent access to the IP will be directly included in the Traffic Log of log audit.

1. Log in to the CFW console, and click **Intrusion Prevention** in the left sidebar to enter the intrusion prevention page.
2. On the intrusion prevention page, find the **Security Baseline module**, click **View Rules** to go to the Security Baseline page.

3. In the "Baseline score" module, click **Add address**. The "Add baseline address/domain name" popup will appear.
4. In the "Add baseline address/domain name" pop-up window, select to add the IP address to the security baseline list of all, external access, or proactive external activities, and manually enter the trusted IP or domain name.

> **Note:**
> Since only the outbound direction is selected by default for the traffic type when configuring safety baseline rules, the baseline type only supports selecting "active external connections". If there are special requirements, please submit a ticket to contact us.

- All: this address will be added to the security baseline list for external access and proactive external activities at the same time.
- External access: this address will only be added to the following external access list.
- Proactive external activities: this address will only be added to the following proactive external activities list.

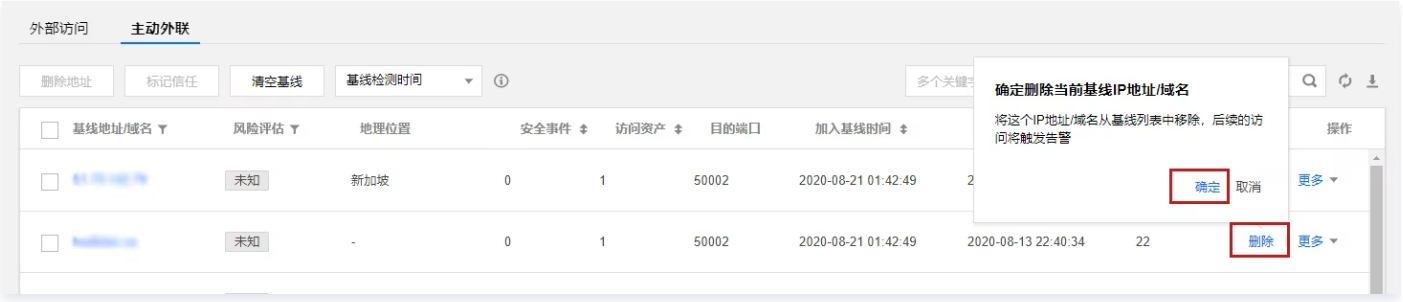
5. Click **Confirm**, and the IP will be automatically added to the selected baseline type list.

Remove address

Users can manually delete the IP address considered to have abnormal access directly from the security baseline list. If the address needs to be restored subsequently, you can select to ignore the address in the alert center, and the address will return to the baseline list.

1. Log in to the CFW console, click **Intrusion Prevention** in the left sidebar, and enter the intrusion prevention page.
2. On the intrusion prevention page, find the **Security Baseline module**, click **View Rules** to go to the Security Baseline page.

3. Below the Security Baseline page, click **External Access** or **Proactive External Activities**.
4. Select an untrusted IP address. In the right operation column, click **Delete**.



5. In the deletion confirmation box, click **Confirm**. The IP address will be removed from the security baseline list. Subsequently, IP address access will trigger a warning.

Clear Baseline

If you need to disable the security baseline feature and clear all IP addresses or domain names in the external access or proactive outbound list, you can use the clear baseline feature to remove all IP addresses and domain names in the security baseline.

1. Log in to the CFW console, and click **Intrusion Prevention** in the left sidebar to enter the intrusion prevention page.

2. On the intrusion prevention page, find the **Security Baseline module**, click **View Rules** to go to the Security Baseline page.

3. Below the Security Baseline page, click **External Access** or **Proactive External Activities**.
4. At the top of the list, click **Clear Baseline**. A confirmation pop-up will appear.

5. Click **Confirm**. All IPs and domain names in the security baseline will be cleared, and the warning baseline switch will be closed simultaneously.

> **Note:**
> Clearing the baseline will not delete the original IP addresses or DNS records in logs, but only delete the selected security baseline list.

Step 4: Start Security Baseline Control

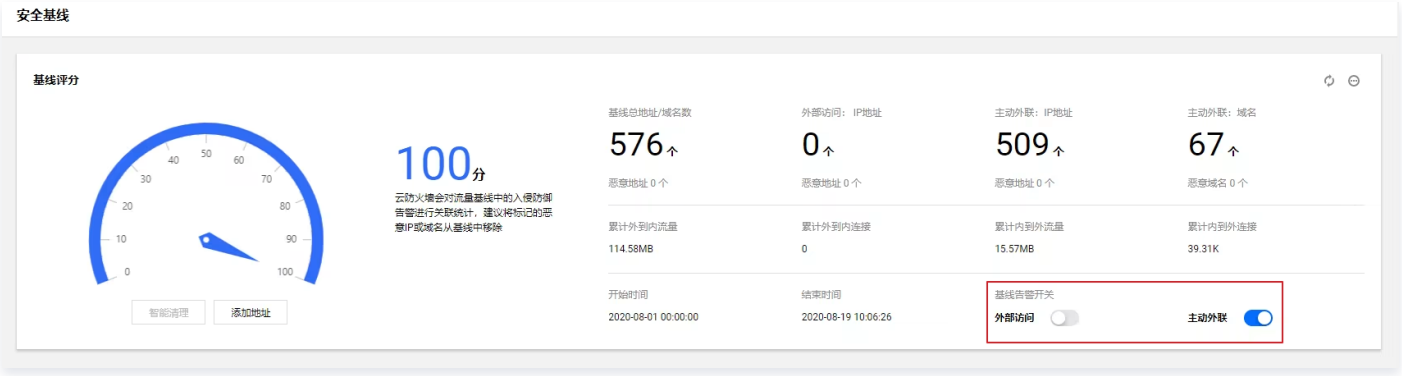
Turn on the Baseline Warning Switch

After the security baseline is established, users need to enable the baseline alarm switch. Subsequently, for IP or domain name access not in the security baseline, an alarm will be triggered.

1. Log in to the CFW console, and click **Intrusion Prevention** in the left sidebar to enter the intrusion prevention page.

2. On the intrusion prevention page, find the **Security Baseline module**, click **View Rules** to go to the Security Baseline page.

3. In the "Baseline score" module, select the traffic direction for warnings.



- When enabling **external access**: For inbound traffic, if there is access NOT_IN the baseline, a security alarm will be triggered.
- When enabling **proactive external activities**: For outbound traffic, if there is access NOT_IN the baseline, a security alarm will be triggered.

View Security Alarms and Trace Traffic Records

After the baseline warning switch is turned on, CFW will classify traffic into trusted IPs and untrusted IPs based on the security baseline list, and merge them into Traffic Log and Alert Center respectively. Users can search for corresponding IP information on the corresponding page.

View Security Alarms

1. Log in to the CFW console. In the left sidebar, click **Alert center** to enter the alert center page.
2. On the attack alert summary page, click **Security Baseline** to enter this page. You can see the alarm information of all security baseline types. Users can choose to block, allow, or ignore, and process this address or domain name.

- Click **Block**, and the IP address will be added to the blocklist. Subsequent access will be blocked and can be viewed in the attack interception statistics page in the Alarm Center.
- Click **Allow**, and the IP will be added to the baseline list. Access in the specified direction will no longer be subject to security baseline testing.
- Click **Ignore**, and the alarm events of this IP will not appear in the alarm list and statistics. Subsequent traffic will not be detected either. You can select **Ignored** in the list to view all ignored events.

Trace Traffic Records

IP addresses or domain names listed in the security baseline can be queried in the traffic center or traffic logs.

- Method 1: Log in to the CFW console. In the left sidebar, select **Log audit** > **Traffic log** to view the specific information of IP or domain name of inbound or outbound traffic.
- Method 2: Log in to the CFW console. In the left sidebar, click **Traffic center** and search for approved IP or domain name.

Step 5. Reset the Security Baseline (Optional)

After the baseline has been established for a period of time, if updates are required to the baseline list, the subsequent IP situation can be re-learned through the "Reset Security Baseline" feature.

1. Log in to the CFW console. In the left sidebar, click **Intrusion Prevention** to enter the intrusion prevention page.
2. On the intrusion prevention page, find the **Security Baseline module**, click **View Rules** to go to the Security Baseline page.

3. In the "Baseline Score" module, select > **Reset Baseline** from the top right corner. The baseline rules will be reset.

> **Note**
> Once the baseline is reset, the manually added addresses and manually added tags will be cleared.

4. After resetting the baseline, you can reconfigure the safety baseline rules as needed. For details, see Configure Safety Baseline Rules.

Manage Defense Operations

Last updated: 2025-05-20 14:20:18

This document will guide you through the intrusion prevention feature to identify unknown risks beyond access control rules and perform intrusion prevention rule detection on the north-south traffic of public network IP addresses while preventing vulnerabilities in CVM from being exposed to the internet.

Select a Protection Mode

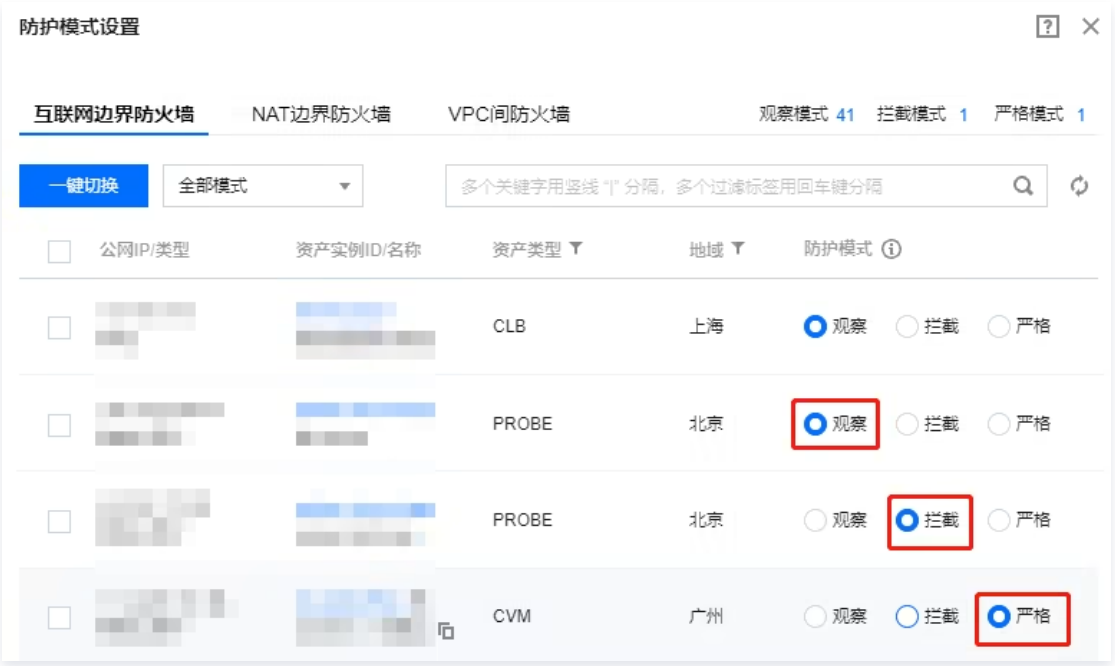
1. Log in to the CFW console. In the left sidebar, click **Intrusion Prevention** to enter the intrusion prevention page.
2. On the intrusion prevention page, find the "Protection Mode" module and perform protection mode settings.
   The protection mode is divided into three modes: **Observation Mode**, **Interception Mode** and **Strict Mode**.

> **Note:**
> The system's default selection for the protection mode is observation mode.

- Select "Observation Mode" to set threat intelligence, basic defense, and virtual patching in detection mode. For detected malicious access or cyber attack behavior, only alarms will be generated, and connections will not be automatically blocked.
- Select "interception mode" to automatically intercept high-confidence network attacks or malicious access. Threat intelligence supports automatic interception of outbound malicious access. Basic defense supports automatic interception of high-confidence rule alarms. Virtual patch supports automatic interception of traffic detected as vulnerability exploits.
- Select "strict mode". TI (except outbound domain name threat intelligence detection), basic defense and virtual patching are all in global interception mode. For any detected alarm, automatically block connection. False alarms may occur. Suitable for critical period guarantee or attack and defense scenarios.

3. On the right side of the protection mode, click **Advanced Setting** to enter the advanced settings popup.
4. In the advanced settings popup, users can select a single asset at the Internet boundaries, NAT boundary, or inter-VPC firewall to change its mode. For example: some assets can be set to observation mode, some assets to interception mode, and some

assets to strict mode.



Intrusion Prevention Feature Description

1. Log in to the CFW console. In the left sidebar, click **Intrusion Prevention** to enter the intrusion prevention page.
2. On the intrusion prevention page right side, you can view feature dynamics and feature descriptions:
   - **Feature dynamics**: In the feature dynamics module, you can view the features of the intrusion prevention system.

   - Intelligence Center

     2.1.1 In the top right of feature dynamics, click **Intelligence Center** to view threat intelligence information.

     2.1.2 In the intelligence center pop-up window, you can click the specific intelligence title to view specific vulnerability descriptions, threat levels and other specific information on the secondary page. At the same time, users can also target specific vulnerability intelligence and use the scanning feature to check whether their assets are threatened.

Management List

1. Log in to the CFW console. In the left sidebar, click **Intrusion Prevention** to enter the intrusion prevention page.
2. You can view the "Blocklist", "Allowlist" and "Isolation list" at the bottom of the intrusion prevention page.

Blocklist

View the Blocklist

1. Click **Blocklist** to enter the blocklist page.

2. Under the blocklist, you can view the IPs with the handling status of "block" and their relevant information in Alert Center > **Attack Alert Summary**, or you can manually add IPs to the blocklist.

Disable Blocklist

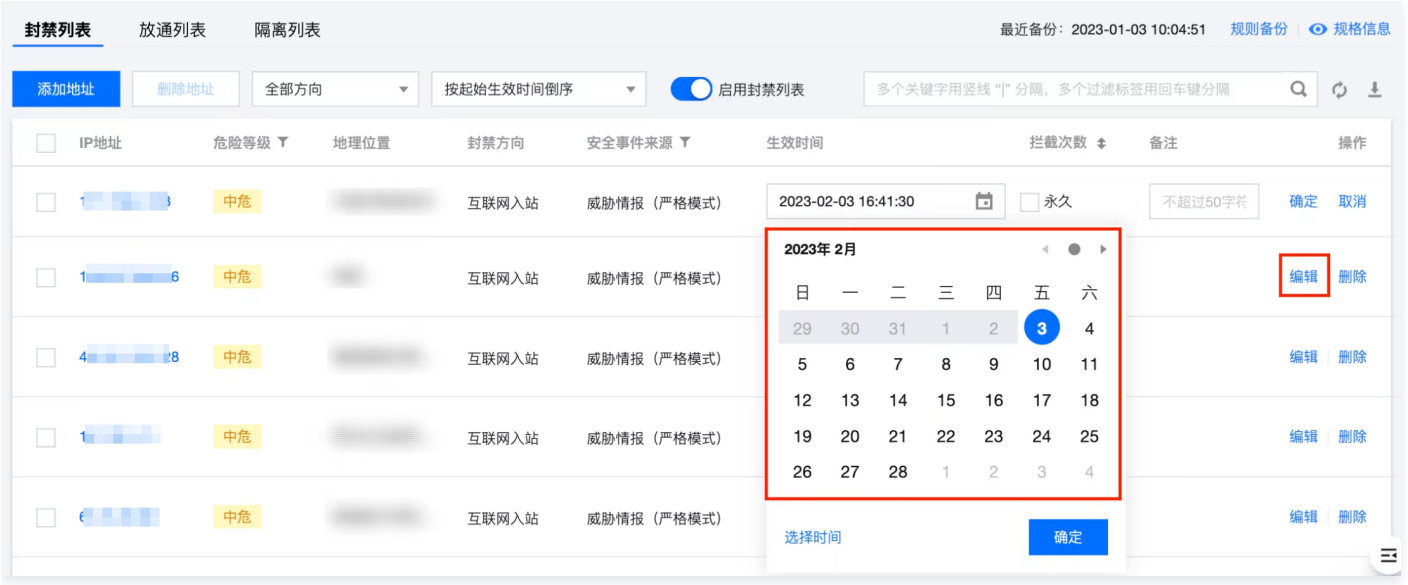
1. When encountering an emergency, you can click to disable "Enable Blocklist", disable the blocklist, and enter Alert Center > **Attack Interception Statistics** to view all blocklist statistics and troubleshoot and locate the blocklist source.

2. After locating and fixing the fault cause, you can click to turn on the "Enable Blocklist" switch and re-enable this feature.

Manage the Effective Time of the Blocklist

In the blocklist, when the effective time of an IP expires, the list will automatically delete the IP. At this point, the subsequent traffic access of the IP will not be blocked by the firewall. Therefore, to avoid the blocklist automatically removing IPs that pose security risks, you can click **Edit** in the operation column on the right side of the list to modify the expiration time and date of the IP to be operated.

> **Note:**
> IP addresses in the blocklist will block all traffic transiting through CFW in outbound or inbound direction and record it in **log audit** > ** invasion prevention log **.



Manage the Specification Information of the Blocklist

1. Click **specification information** to view the currently available total list quota and remaining quota information.

2. When the remaining quota is insufficient, you can click **scale-out** to purchase blocklist quota.

Allowlist

View the Allowlist

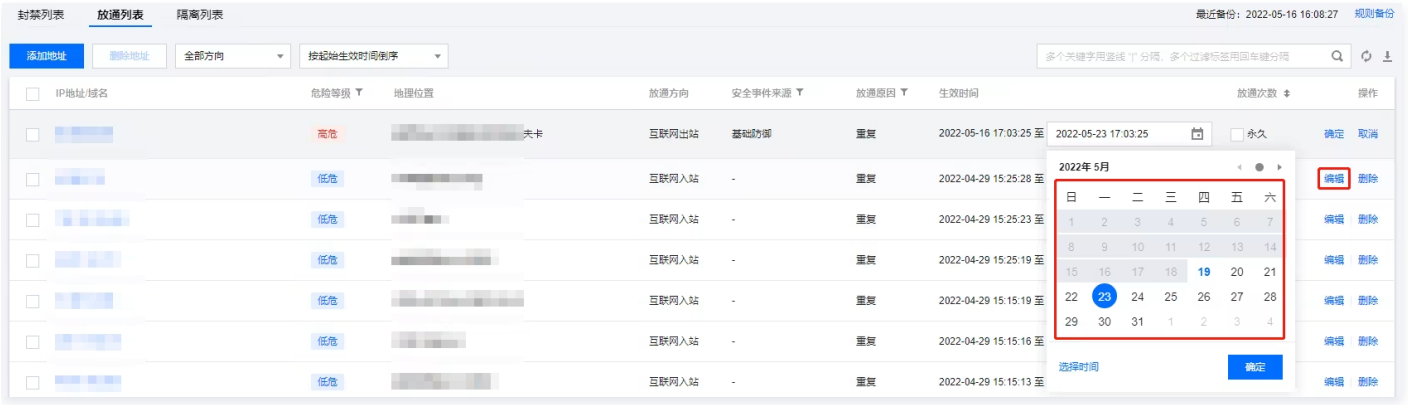
1. Click **allowlist** to enter the allowlist (whitelist) page.

2. Under the allowlist, you can view the IPs with the handling status of "allow" and their relevant information in Alert Center > **Attack Alert Summary**, or you can manually add addresses to the allowlist.

> **Note:**
> - IP addresses in the allowlist will directly bypass the IDPS feature.
> - The blocklist and allowlist have a cap on the number of rules. The number of items in the blocklist and allowlist is the same.
> - The maximum number of each version is shown in the purchase guide.

Managing the Effective Time of the Allowlist

In the allowlist, when the effective time of an IP expires, the list will automatically delete the IP. At this time, subsequent access by the IP will not bypass the firewall's IDPS. Therefore, to avoid the trusted IP being automatically removed from the allowlist, you can click **Edit** in the operation column on the right side of the list to modify the expiration time and date of the IP to be operated.

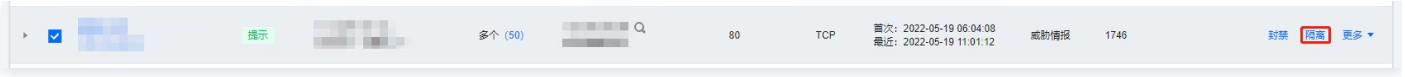


Isolation List

View the Isolation List

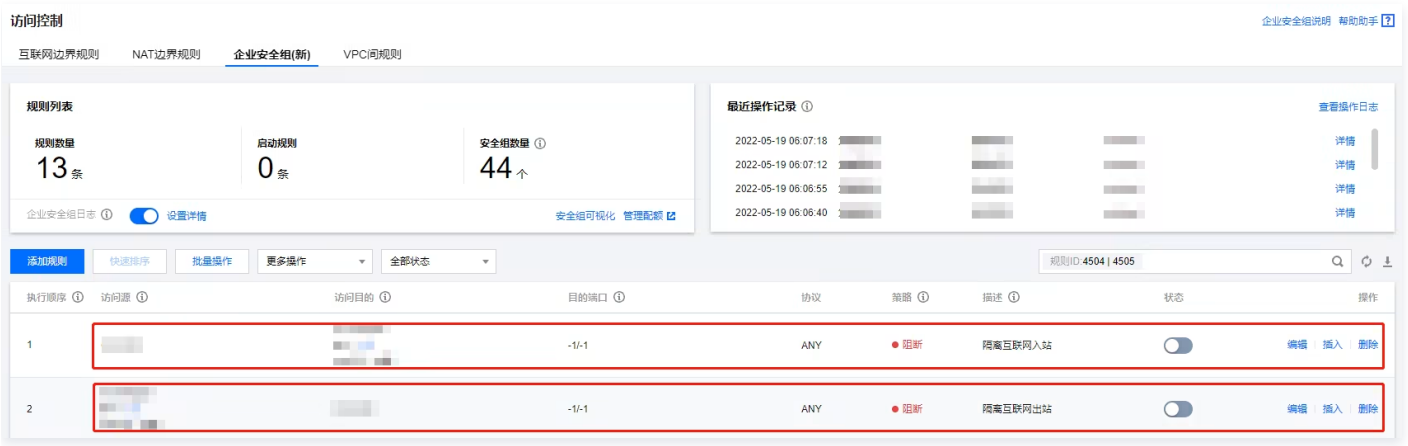
1. Click **Quarantined list** to enter the quarantined list page.

2. In the isolation list, you can see the IPs with the handling status of isolation and their relevant information in Alert Center > Attack Alert Summary > Host Compromise.



View Rules

The isolation of compromised host IPs is achieved by security groups. Click **View Rules** to navigate to the enterprise security group page and view detailed rule information.

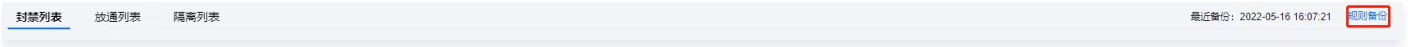


Managing the Effective Time of the Isolation List

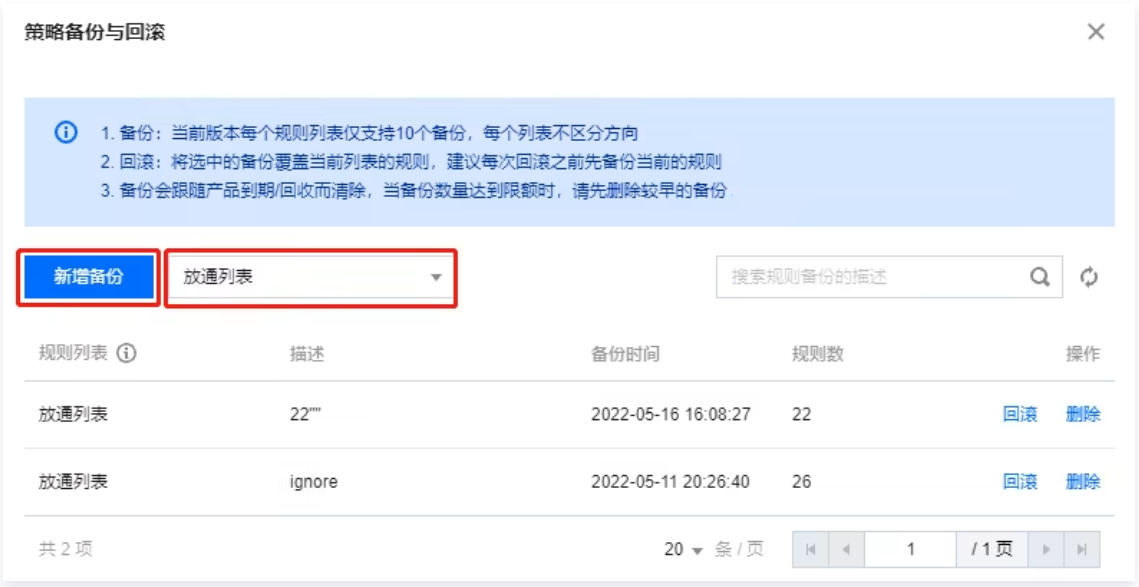
In the isolation list, when the effective time of an IP expires, the list will automatically delete the IP. At this time, the security group rules of the IP will also be deleted. Therefore, to avoid the compromised IP being automatically removed from the isolation list, you can click **Edit** in the operation column on the right side of the list to modify the expiration time and date of the IP to be operated.

Rule Backup and Rollback

Click **Rule Backup** to back up existing blocklist and allowlist rules. Meanwhile, when the rules have changed significantly, click **Rollback** on the right side of the backup file to restore the rules.



1. On the rule backup and rollback page, click **create backup**, select blocklist or allowlist from the drop-down selection next to it, enter description, and click **confirm** to complete the rule backup.



2. Perform rule rollback. Click **Rollback** on the far right of the backup list to restore the rule.

Related Information

If you encounter intrusion prevention related issues, see Intrusion Prevention document.

Zero Trust Operations and Maintenance Overview

Last updated: 2025-05-20 11:15:00

During daily operations, enterprises often face scenarios where they need to access servers, databases, internal OA systems, etc., from the office network to the production network. How to achieve secure and efficient operations and maintenance is a challenge that enterprises have been trying to solve. When assets such as SSH, RDP, internal OA systems, and database public IP addresses are directly exposed to the Internet, the resulting attacks are particularly evident during the critical maintenance period. Therefore, CFW provides a zero-trust-based security operations and maintenance solution for the above scenarios.

Module Overview

The usage of zero trust operations and maintenance, following the thought process of access management and identity before events, permission configuration during events, and post-event auditing, can be divided into four modules, which are access management, asset management, permission management, and Zero Trust Operations Log.

- Access management: Responsible for preparations such as creating zero trust operations and maintenance instances, integrating the network of operation and maintenance assets, integrating the identity system of iOA or WeChat, and integrating the website domain names of Web services.
- Asset management: Responsible for Ops configuration of server assets, Web service assets, and database assets, including server log-in credentials, Web service ports, related domain name configurations, etc.
- Permission Management: Responsible for allocating Ops permissions based on the identity system and Ops assets that have been integrated, according to the dimensions of people and assets. Supports adding permissions from the identity perspective or rule perspective.

Using Zero Trust Protection

1. Zero trust operations and maintenance supports intranet endpoint operations and maintenance based on iOA. Cloud resources can be accessed and controlled without a password through iOA identity. For details, see Endpoint Operations and Maintenance with iOA.
2. Zero trust operations and maintenance supports public network terminal-free operations and maintenance based on WeChat or iOA. Access control to cloud resources can be performed via WeChat or iOA QR code scanning. For details, see Terminal-free Operations and Maintenance via WeChat or iOA.

Logs

Zero Trust Operations Log

Zero Trust Operations Log can display access details of servers, Web services, and databases in the database by asset dimension, audit and analyze logs such as successful login or illegal access, and support operation replay.

Zero Trust Ops Log

On the Operation Log page, select **Zero Trust Operations** to view the operation details of the Zero Trust Protection feature and the corresponding account.

Version Description

The zero trust operations and maintenance feature of CFW requires additional purchase. For specific billing and specification information, please refer to Purchase Guide.

Practical Tutorial
Performing On-Premises Ops through iOA

Last updated: 2025-05-20 11:16:11

Background Information

Accessing the production network in the cloud from the offline office network is a difficulty in network isolation and permission control. How to minimize security risks while enhancing daily Ops experience is a pain point that every company tries to solve. Now, via the joint use of iOA and CFW, complex network interconnection and configurations between the cloud and offline environments are avoided, achieving a convenient out-of-the-box access experience. And it supports identity-based access control and audit at the same time.

Overview

For on-premises Ops, users are advised to log in to the iOA account on their client devices. Controlled assets include servers, Web services, and databases.

Step 1: Access Preparations

Prerequisite

Please confirm that you have completed the configuration of relevant features in the iOA console. For details, see Client-to-site Connections - Out-of-the-Box Guide.

Procedure 1: Enable a Zero Trust Operations and Maintenance Instance

The Zero Trust Operations and Maintenance Instance (hereinafter referred to as the operations instance) is responsible for providing the connector integrated with iOA to communicate with the zero trust gateway and connecting the network communication between assets and the operations instance. Before enabling the operations instance, you need to plan according to the purchased quota and the region where the assets belong, and confirm the region where the operations instance to be enabled is located. After determining the region, for details, see Enable Zero Trust Operations and Maintenance Instance.

> ⚠ **Note:**
> Use iOA client-side Ops. Ensure to bind the Ops IP. Otherwise, all client-side Ops features will be unavailable.

Procedure 2: Connect to the Asset Network

After enabling the Zero Trust Operations and Maintenance Instance, you still need to integrate the network between the instance and the asset to match the network flow direction. CFW provides a shortcut operation for accessing with VPC granularity. You only need to enable the VPC switch in the corresponding region to complete the access. For details, see Asset Access with VPC Granularity.

> ⚠ **Note:**
> Due to instance specification limits, each instance only supports access to 9 VPCs.

Step 3: Integrate Identity Information

You have completed the basic network connectivity. Now you need to connect the identity information that requires Ops. Please import the iOA organizational directory as needed. For details, see Identity Connection.

> ⚠ **Note:**
> iOA directory integration only supports integration in organizational dimensions. Permissions will not be allocated by default after access. Operate with confidence.

Step Two: Asset Configuration Work

In the access preparation work, you have completed the network connection and identity access. Next, you need to configure the operation and maintenance parameters related to the connected assets.

Server Type Assets

Server type assets support remote Ops for Linux and Windows. The default ops ports are 22 and 3389. If you need to modify the ops ports, please refer to Configure Ops Ports.
The server supports the password/key of the hosted server, thereby avoiding the leakage of the password/key by employees, realizing identity-based password-free login. For details, see Password/Key Hosting.

> **Note:**
> In the asset list, only assets in the VPC enabled in the aforementioned connected asset network can perform remote ops.

Web Service Type Assets

If you need to perform Ops on web-based business such as OA via the public network, you can first manually add a web service. For details, see Add Web Service.

> **Note:**
> After adding the Web service, you can use the private network port O&M without the need to bind a domain name. Please use the real service address to access.

Database Type Assets

Database Assets will automatically pull relevant PaaS services you own on the cloud. The existing supported types include five kinds of database types: MySQL, MariaDB, Redis, CKafka, and ElasticSearch. Based on the situation, you can click Sync Assets to re-pull Database Assets for synchronization. For details, see Database Management Center (DMC).

> **Note:**
> CFW does not need to configure database ops information. All information is subject to the corresponding product console. After configuring permissions, you can directly connect through the database address.

Step Three: Permission Configuration Work

Permission is essentially a triplet allowlist based on identity and asset. Therefore, permissions can be managed and added from the perspective of the permission rule itself, the asset perspective, or the identity perspective.

- Perform permission management or add permission from the perspective of the permission rule itself. For details, see Rule Perspective.
- Manage or edit assets with permission from the identity perspective. For details, see Identity Perspective.
- Manage or edit users or organizations with permissions from the asset perspective. Please visit the management page of each asset type.

Step Four: Verify Whether Login Is Normal

For agent-based Ops via iOA, you can refer to iOA User's Private Network Access to Ops Assets.

Perform Terminal-Free Ops Via WeChat or iOA

Last updated: 2025-05-20 11:16:32

Background Information

Recently, security events such as Web attacks, mining, and extortion on the cloud have been rampant. Tencent Security Engineers have followed up on source tracing analysis from a large number of security ticket feedback and found that most users have many edge business websites or internal core business websites such as OA mistakenly opened to the public network, causing websites to be penetrated; and since the backend servers directly expose remote ops ports 22 and 3389 to the Internet, and use relatively weak login credentials, it has led to CVM being very easy to brute force crack login, affecting business stability and even system crash.
Port 22 and port 3389 are the fourth largest traffic ports on the cloud, second only to ports 80, 443 and 8080. They are also important ports for remote Ops and login. Before that, users could set an access control policy for the IP allowlist in CFW to limit external access to their important ports. However, since non-office work has become the new normal, the IP allowlist cannot handle scenarios of remote work and Ops. Therefore, Tencent Cloud Firewall has designed an identity-based access control feature, which manages and controls remote logins to websites and CVMs in the form of Weixin QR code authentication or iOA system authentication, preventing servers from being brute-force logged in from the source.

Overview

The asset protection currently targeted by terminal-free Ops includes two types: servers and Web services.

Feature Introduction

CFW zero trust operations and maintenance support remote access implemented based on WeChat or iOA authentication, including servers represented by two types of protocols such as public network or private network Web services, SSH and RDP.
Ops asset protection plan

- This feature addresses the issue that traditional static IP allowlist security policies are not suitable for IP changes in remote office scenarios. It also avoids the risks of CVM ops ports being brute-forced or suffering from credential stuffing attacks. The zero trust operations and maintenance feature of CFW requires no deployment of instances or agents, and no client installation (client installation may be required for iOA identity), achieving a seamless experience of "zero deployment, agentless, and clientless".

The protection plan for Web provides two protection modes: basic protection and advanced protection. Among them:

- Basic protection: Automatically filter humans and attackers. For users who have not purchased WAF, this feature can be used to protect Web businesses.
- Advanced protection: Scan the WeChat QR code or authenticate with iOA. Adds identity-based access control for Web services using the HTTPS encryption protocol. Identity verification is required for all users accessing network services. Recommended feature for protection during important periods and penetration prevention.

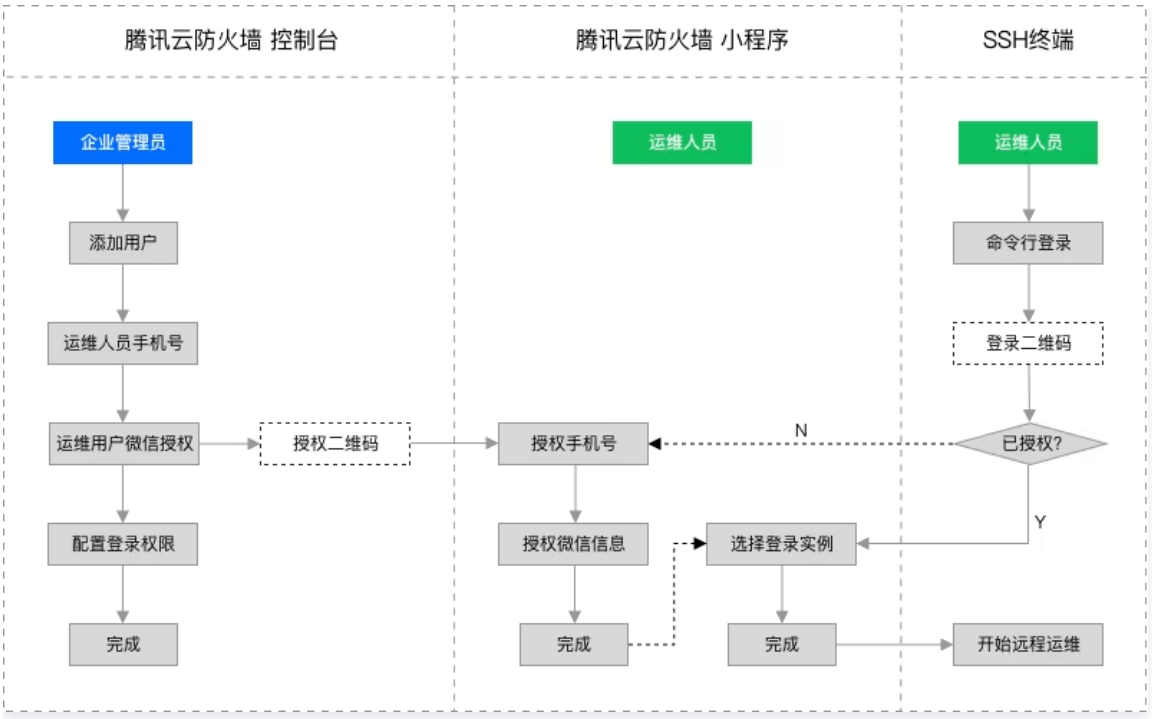
Web service management can be used to handle 0day vulnerabilities and network attacks. Web protection can be used to protect key systems of an enterprise such as OA system, email system, corporate VPN, backend, etc. It supports protecting private network, public network, IP-based and domain name-based web services.

Functional Characteristics

- Based on the zero trust principle, supports quick authentication via WeChat or iOA, which is safe and convenient.
- Can block management ports and hide the origin server at the Internet boundaries.
- Zero deployment, agentless, clientless.
- Automatically filter Web attacks, vulnerability exploitation attacks; avoid brute force attacks and credential stuffing.
- Access Web services within WeChat without scanning codes. One-click authentication.
- End-to-end, full-user audit, automatically record login logs.

Feature Process

The system usage of CFW zero trust operations and maintenance can be generally divided into four processes: access preparation, asset configuration, permission configuration, and login verification. Taking SSH log-in to the server operation and maintenance with WeChat identity as an example, the following is the process overview:



Step 1: Access Preparations

Access preparation work can be divided into four steps, which are enabling zero trust operations and maintenance instance, integrating access assets network, integrating identity information, and integrating Web domain.

Procedure 1: Enable Zero Trust Operations and Maintenance Instance

The zero trust operations and maintenance instance (hereinafter referred to as the operations instance) is responsible for providing public network reverse proxy and establishing network communication with assets. Before enabling the operations instance, you need to plan according to the purchased quota and the region where the asset is located. Confirm the region where the operations instance to be enabled is located. After determining the region, see Enable Zero Trust Operations and Maintenance Instance.

> **Note:**
> If you only need to operate and maintain public network assets, you do not need to bind an operation and maintenance IP and can perform operation and maintenance through the public domain name `cfw.tencentcs.com`; if you need to operate and maintain private network assets, please bind an operation and maintenance IP.

Step 2. Connect the Asset Network

After enabling the zero trust operations and maintenance instance, you also need to establish network connectivity between the instance and the asset to achieve reverse proxy. CFW provides a shortcut operation for accessing with VPC granularity. You just need to enable the VPC switch in the corresponding region to complete the access. For details, see Asset Access with VPC Granularity.

> **Note:**
> Due to specification limits of the instance, each instance only supports access to 9 VPCs.

Procedure 3: Integrate Identity Information

So far, you have completed the basic network interconnection. Now you need to integrate the identity information that requires operations and maintenance. Unauthorized public network operations and maintenance only support WeChat identity. Or you can log in to the page callback to iOA for authorized access with a client. Now, according to your needs, select to integrate WeChat identity or import the iOA organizational directory. For details, see Identity Connection.

> **Note:**

WeChat identity is associated with mobile number. Please ensure that the added WeChat account is associated with the correct mobile number.

Procedure 4: Configure Access Domain

Domain name access is necessary in untargeted public network ops, because untargeted public network ops requires the zero trust operations and maintenance instance of the firewall to provide a reverse proxy and access via domain name. If you need to use this feature, ensure to connect a domain name.
Domain names are divided into Ops domain names and web domains. Ops domain names are primarily responsible for remote ops of servers. Web domains are primarily responsible for reverse access to web services. For the method of integration, please see Domain Name Access.

Note:
Please ensure that the domain name connected has been filed; otherwise, normal access may be intercepted by Tencent Cloud.

Step Two: Asset Configuration Work

In the access preparation work, you have completed the connection of the network, the access of the identity, and the access of the domain. Next, you need to configure relevant operation and maintenance parameters for the connected assets.

Server Type Asset

Server type assets support remote ops for Linux and Windows. The default ops ports are 22 and 3389. If you need to modify the ops port, please see Configure Ops Port.
The server supports the password/key of the hosted server, thereby avoiding the leakage of the password/key by employees, and realizing identity-based password-free login. For details, see Password/Key Hosting.

Note:
In the asset list, only assets enabled under VPC in the aforementioned connected assets network can perform remote ops.

Web Service Type Asset

If you need to perform ops on web services such as OA via the public network, you can manually add a web service first. For details, see Add Web Service.
After adding, if you need to perform Ops over the public network, ensure you perform domain binding. For details, see Bind Domain Name.

Note:
- The current step highly depends on the preparations for access. Make sure that you have completed the enablement of the instance, access of the asset, and hosting of the domain name and certificate.
- It is recommended to adopt an advanced protection plan for binding a domain name to facilitate the configuration of identity-based access control rules.

Step 3: Permission Configuration Work

Permission is essentially a triplet allowlist based on identity and asset. Therefore, whether from the perspective of the permission rule itself, or the asset perspective, or the identity perspective, permissions can be managed and added.
- Perform permission management or add permission from the perspective of the permission rule itself. For details, see Rule Perspective.
- Manage or edit assets with permission from the identity perspective. For details, see Identity Perspective.
- Manage or edit users or organizations with permissions from the perspective of assets. Please go to the management page of each asset type.

Step Four: Verify Whether Login Is Normal

- For logging in to server-type assets, you can refer to WeChat user public network remote server login.

- For accessing Web service type assets, you can refer to WeChat or iOA users accessing Web services from the public network.

Connection Management Overview

Last updated: 2025-05-20 11:21:28

The access management module is primarily responsible for the preliminary preparations for using zero trust operations and maintenance. It includes the creation of zero trust operations and maintenance instances, VPC network access for operations and maintenance assets, access of iOA identity and WeChat identity, and access of Public Network Ops domain names and Web service domain names.

Operation Steps

CFW creates a zero trust operations and maintenance instance in each region and is responsible for establishing network communication to the VPC of the corresponding operations and maintenance asset.

1. You need to enable the operations instance switch in the corresponding region in the Instance Management module.
2. You need to integrate the VPC under the operations instance of the region enabled in the previous step in the asset access module.
3. 1. You need to integrate the identity system that includes O&M personnel in the Identity Connection module, which can be done via iOA import or WeChat addition.
4. If you need to use Public Network Ops, you need to integrate the Public Network Ops domain name or public network Web service domain name in domain name access.

Instance Management

Last updated: 2025-05-20 11:21:57

1. Log in to the CFW console. In the left sidebar, select **Zero Trust Operations and Maintenance** > **Access Management**.
2. On the instance management page, you can manage zero trust operations and maintenance instances for future asset access and operations and maintenance.

Enabling Zero Trust Operations and Maintenance Instance

The current version has 1 zero trust operations and maintenance instance per region. Based on your quota, you can choose whether to enable the instance switch in the specified region.

1. Find the region where the required operations assets are located. Click on the right  to use the operations instance in the current region.

> **Note:**
> If your asset's located area is not in the list, please go to Asset Center and click **Asset Update**.

2. If you have not bound the operations IP yet, in the current region, assets can only be operated through public domain names for public network assets. iOA authentication is not supported, and the operations of internal network assets are not supported.

> **Note:**
> How to integrate the domain name for Public Network Ops, refer to domain access.

3. If you have already bound the operations IP, after the switch is turned on, the current region simultaneously supports the operations and maintenance of public network assets and private network assets. You can use iOA identity or WeChat identity to configure access control permissions.

4. After successful completion, you can go to Asset Access to proceed to the next step.

> **Note:**
> After enabling a zero trust operations and maintenance instance, the assets under the current regional instance will not be immediately integrated into the zero trust network. You need to go to Asset Access and manually select the Virtual Private Cloud network to be integrated.

Bind Ops IP

Binding the Ops IP can let the zero trust operations and maintenance instance have the ability of public network access and communication with the iOA gateway. Therefore, it can support iOA-based identity access control and also support remote Ops of private network assets under the corresponding instance.

1. Find the region where the required operations and maintenance assets are located. Click on the right of the operations and maintenance IP below.

2. You can select an existing idle EIP or create a new EIP and bind it to the current instance. Click **Save** to take effect.

> **Note:**
> When the regional instance switch is not enabled, selecting the Ops IP will not immediately bind the EIP to the instance, **which may incur certain idle fees**. Please enable the switch as soon as possible after binding or bind the EIP when the regional instance is enabled. If you have confirmed that this instance is no longer in use, please adjust the EIP binding relationship to No Selection.

3. Click on the right of Ops IP-2. You can bind multiple ops IPs.

> **Note:**
> The current version can support binding up to 2 ops IPs, achieving high availability and dynamic load balancing of the instance. Binding the second ops IP requires purchasing the advanced edition of zero trust operations and maintenance.

Query Zero Trust Operations and Maintenance Instance Quota

In the specification information of Access Management, you can view the number of authorized operations instances and the remaining quota.

Asset Access

Last updated: 2025-05-20 11:22:20

Asset access refers to connecting the network where the asset resides with the instance network of zero trust operations and maintenance, thereby achieving subsequent access control and other features. On the **Access Management** > Asset Access page, you can enable the VPC where the operation and maintenance assets are located and integrate the operation and maintenance assets into the zero trust operations and maintenance instance.

Perform Asset Access at VPC Granularity

Select the VPC where the assets to be integrated are located, and click on the right to integrate zero trust operations and maintenance. After the switch is turned on, the assets under the current VPC can be operated and maintained through the access network of zero trust operations and maintenance.

Note:

- Please confirm that the zero trust operations and maintenance instance in the region where the Virtual Private Cloud to be accessed is located has been enabled; otherwise, it will not appear in the list of accessible Virtual Private Clouds.
- If the region where the Virtual Private Cloud to be accessed is not bound to an operation and maintenance public IP address, only public network assets of the current Virtual Private Cloud can be maintained. For details, see Instance Management.
- Turning on will create a /29 subnet under the enabled VPC for traffic diversion.

Identity Connection

Last updated: 2025-05-20 11:22:50

1. Log in to the CFW console. In the left sidebar, select **zero trust operations and maintenance** > **access management**.
2. On the **Access Management** > **Identity Management** page, you can import an existing identity system from iOA for terminal-based Ops, or manually add a WeChat identity for non-terminal-based Ops.

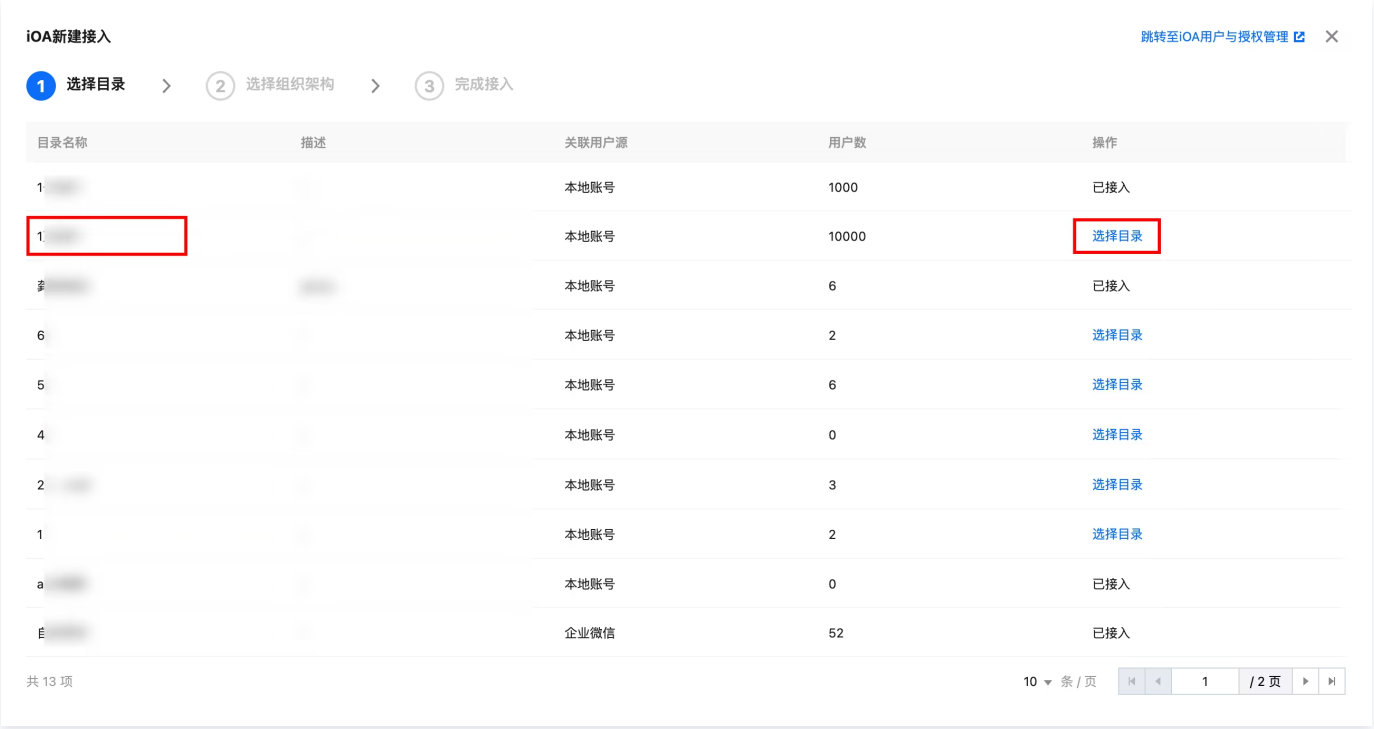
Integrating iOA Identity Directory

Before integrating iOA identity, ensure that you have purchased the zero trust operations and maintenance expansion package and completed the configuration and deployment of iOA Zero Trust Security Management System.

1. CFW will obtain your identity directory information through role authorization. You need to click **Start Authorization** to perform role authorization.

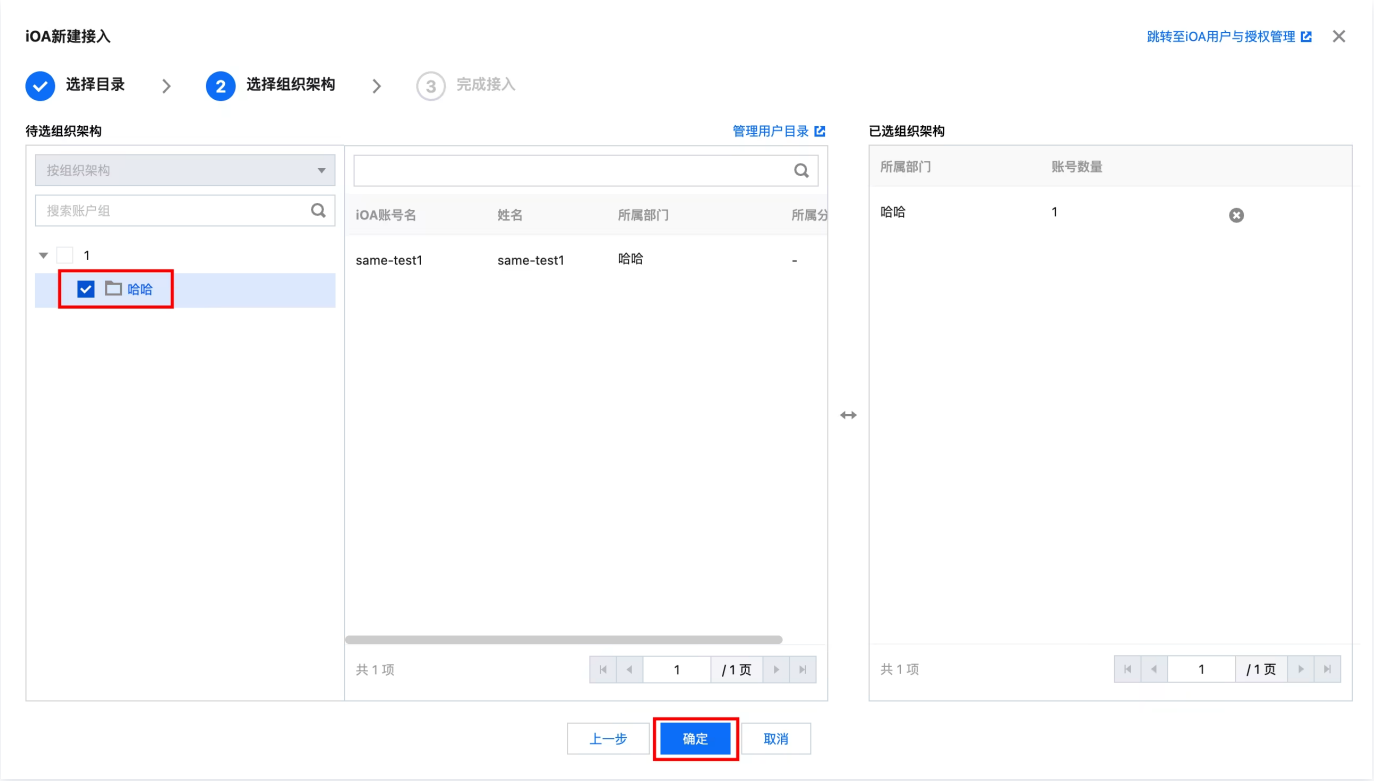
2. 1. Click **Add access** to initiate the access process for the iOA directory.

3. Select the directory you need to integrate and click on the right **Select Directory**.



4. Select the organizational structure you need to integrate in the current directory, verify the account information it contains, and click **Confirm** after verification.

> **Note:**
> - Only support importing identity information by organizational structure. Support selecting subdirectories.
> - New identities or organizations added under the selected directory will be automatically synchronized.

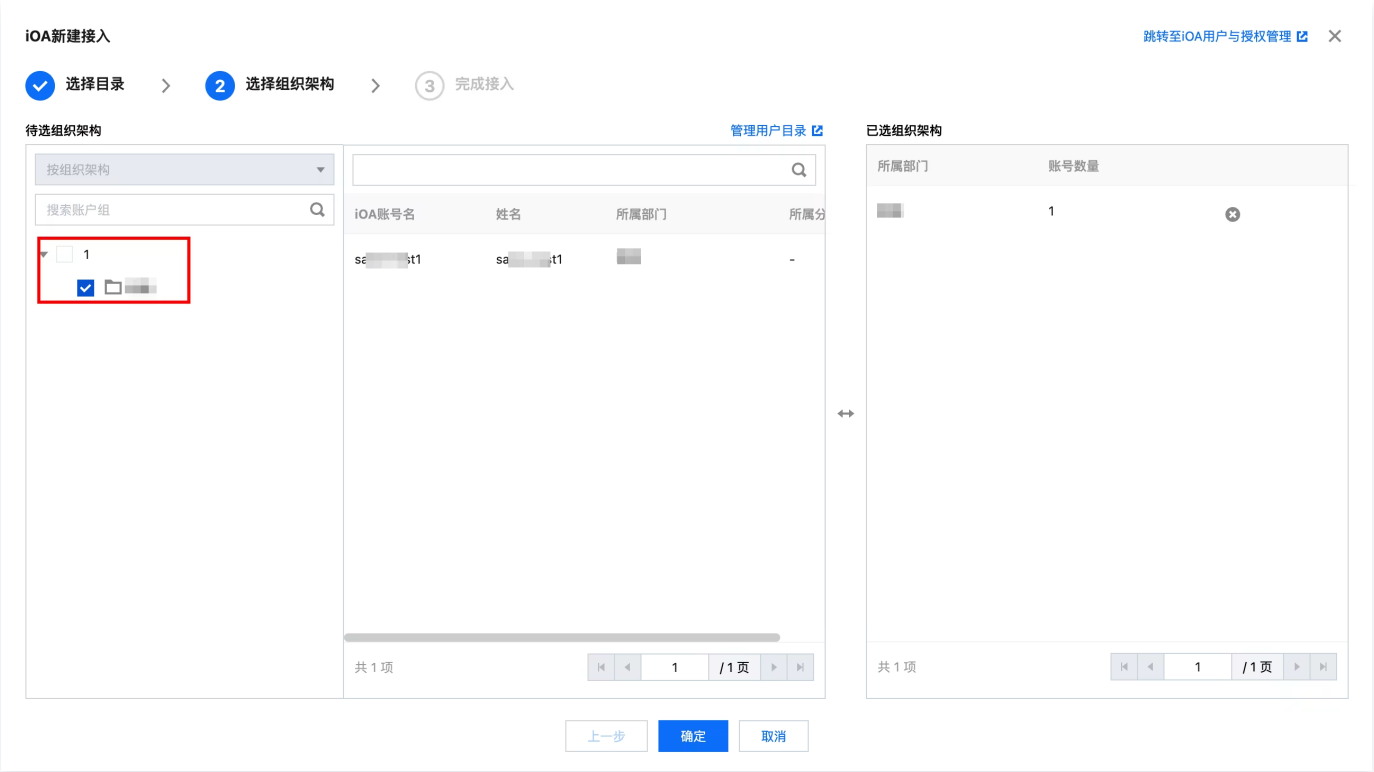


5. After the service access is completed, you can configure Ops permissions for the identity information just imported through the button for quickly configuring permissions. For details, see Identity Perspective – Add New Permissions.

Editing the Integrated iOA Identity Directory

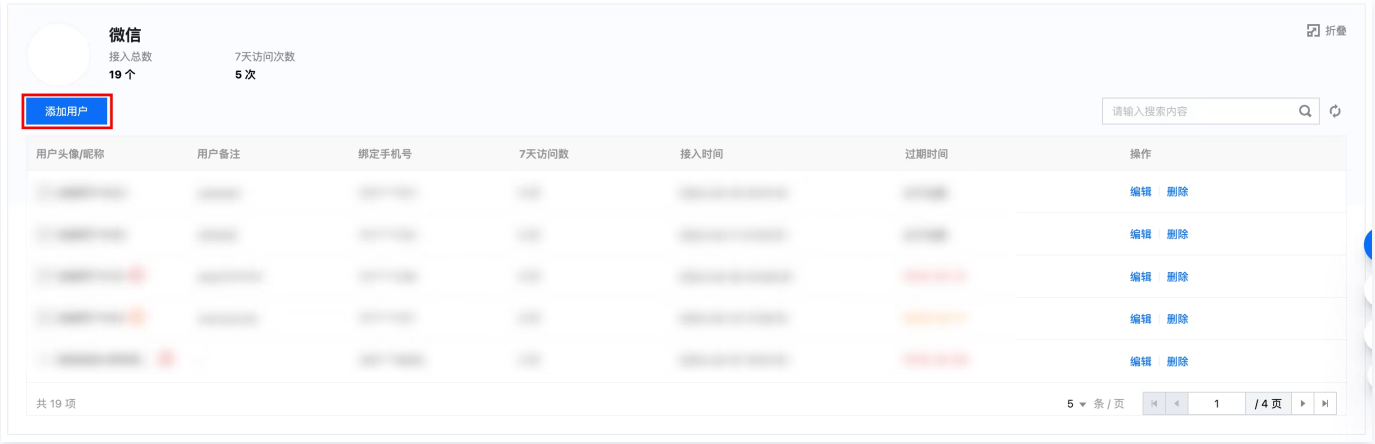
1. Select the directory to be edited and click on **Modify Configuration** on the right.

2. You can modify the organizational structure you want to integrate in the current directory and click **Confirm** to save.



Adding WeChat User

1. In the WeChat Identity Management section, click **Add User**.



2. In the pop-up window for configuring the WeChat account, input the mobile number bound to the ops user's WeChat and click **Next**.

3. In the pop-up window for editing user information, click **click to obtain authorization** to scan the QR code to obtain Weixin authorization, input user remark, set account expiration time, and click **submit**.

> **Note:**
> If unable to obtain authorization on the spot, you can skip obtaining the WeChat nickname and profile photo information and preset the user's permission information in advance; wait for the user to log in by scanning QR code with WeChat, and the system will automatically obtain the user's mobile number, profile photo and nickname and match them.

4. After submission, the WeChat user is added. You can configure Ops permissions for the newly-added WeChat user through the button for quickly configuring permissions. For details, see Identity Perspective – Add New Permissions.

Editing WeChat User

1. Select the WeChat user to be edited and click on the right **Edit**.

2. You can modify the remark and expiration time of the current WeChat user.

Domain Name Access

Last updated: 2025-05-20 11:23:17

1. Log in to the CFW console. In the left sidebar, select **Zero Trust Operations and Maintenance** > **Access Management**.
2. In the **Access Management** > **Domain Name Access** page, you can add Ops domain names and Web service domain names for terminal-free ops for public network access.

Access Ops Domain Name

The operation and maintenance domain name is used for public network remote login and operation and maintenance of assets SSH, RDP, and databases in the specified region. It is only accessible via Layer-4 protocol. After access, it can achieve access to the public access domain name through proxy.

1. Click **Access Domain Name**, select **Ops Domain Name**.

2. You can bind the ops domain name through **self-owned public network domain**.

   Bind your own domain name: Please ensure that the entered domain name has been filed; otherwise, it may not be able to integrate normally.
   Operation steps: Select the **self-owned public network domain** option, select the region to be associated with the domain name, fill in the self-owned domain name address, and click **Confirm**.

3. Access completed.

After access completion, modify the resolution address of your self-owned public network domain to the cname provided in the list.

Integrate Web Domain

The Web domain is a domain name used for accessing the Web assets. Please ensure that the domain name has been filed. After access, reverse proxy access via the public network can be achieved, with support for public network protection and identity access control.

1. 1. Click **Access Domain Name**, select **Web Domain**.

2. The Web domain supports the integration of self-owned public network domains and private network domains. Please ensure that the entered domain name has been filed; otherwise, it may not be able to integrate normally. According to the prompts, select the region to be associated with the domain name and fill in the custom sub-domain prefix.

3. Associate an SSL certificate.

After a Tencent Cloud-managed certificate is hosted, it can be used for HTTPS access in zero-trust Web protection. You need to select from Tencent Cloud-managed certificates. If you have not hosted yet, please visit SSL certificate console to manage.

> **Notes:**
> If you need to perform headless Ops on public network Web services, please ensure that the associated domain name has a hosted certificate; otherwise, integration will not be possible.

4. Click **Confirm** to complete the service access.
   Please modify the resolution address of your own domain name to the cname provided in the list as soon as possible after completion.

> **Notes:**
> The Web domain can only be accessed via public network. If you have previously mounted a Web service on the domain name, please switch the resolution address after completing domain name binding; otherwise, the real service address may not be found, causing access failure.

Asset Management Overview

Last updated: 2025-05-20 11:28:24

The Asset Management Module is primarily responsible for the asset configuration work of ops assets using zero trust operations and maintenance. Ops assets are divided into three types: servers, Web services, and databases. In this module, you can specify the ops port of the server, manage the server password key, add Web services, bind Web domains, perform public network protection and terminal-free operations, and manage database assets.

- Server: CVM server resources in the cloud, supporting Windows or Linux.
- Web service: Web service resources in the cloud, whose backend address needs to be on Tencent Cloud.
- Database: Asset of database type in the cloud. For supported types, please see Database Management Center (DMC).

Server Management

Last updated: 2025-05-20 11:31:51

1. Log in to the CFW console. In the left sidebar, select **Zero Trust Operations and Maintenance** > **Asset Management**.
2. On the **Asset Management** > **Servers** page, you can configure operational parameters for all CVM servers. You can manage access permissions for connected users, making it easy to view authorized personnel and organizations from the server perspective.

Configure Operation and Maintenance Parameters

CFW supports remote Ops for servers of Windows and Linux types. It supports configuration of the following operation and maintenance parameters.

Configure Ops Port

CFW zero-trust remote Ops supports modification of non-standard ops ports, thereby achieving reverse proxy Ops connections on the public network.

> **Notes:**
> When performing remote Ops using the public network without a terminal, please ensure that the ops port is configured correctly; otherwise, normal connection will not be possible. Using iOA for intranet operation and maintenance is not affected by this parameter. Please manually input the corresponding port and directly perform the connection during operation and maintenance.

1. On the server page, select the corresponding server and click **Edit** on the right of the **Protocol Port** column.

2. In the protocol port, modify the ops port and click **Confirm**.

Password/Key Managed

CFW zero-trust remote Ops supports password/key of hosted servers, thereby avoiding password/key leakage from employees and achieving identity-based password-free login.

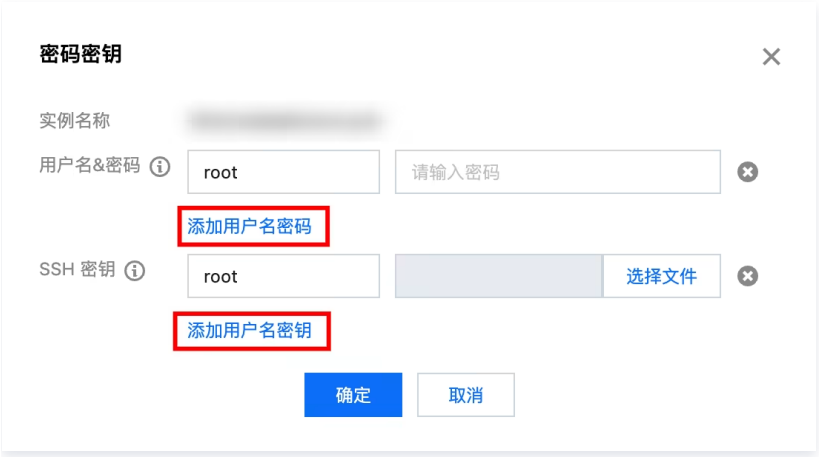
> **Notes:**
> SSH log-in supports managed username/password or key, while RDP log-in only supports managed username and password.

1. On the server page, select the corresponding server and click **Edit** on the right of the **Password/Key** column.

> **Notes:**
>
> The asset key type is divided into three types: unhosted, hosted, and password exception. Click of the password/key to make appropriate modifications.

- Unhosted: The login password of the instance is not managed by CFW. You need to enter the password when performing remote ops.
- Hosted: Instances that have been managed by CFW.
- Password exception: Instance of with password exception.

2. In the password/key window, click **Add Username and Password** to fill in the username and password, or click **Add Username and Key** to fill in the username and upload the key.



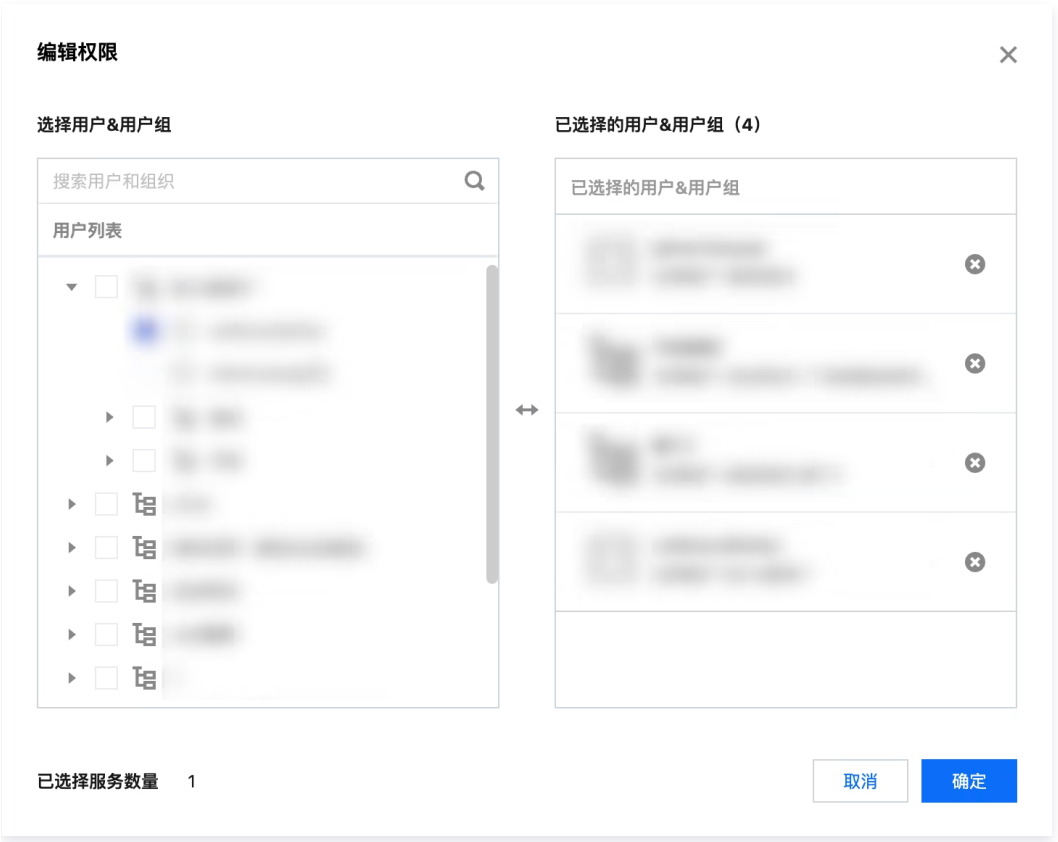
3. Click **Confirm** to complete the editing.

Management Permission

1. On the server page, you can view the list of all types of server assets and authorized users.
2. Click **Management Permission** to manage authorized ops users of the instance. It supports unbinding users and adding new users.

3. In the Edit Permission pop-up window, you can add or delete permissions. Check the users and organizations on the left side to add permissions. Click on the right side to delete permissions.

Notes:
The Edit Permissions page can only edit the rule permissions added from the identity perspective. If you need to edit inherited permissions, please go to the rule perspective of Permission Management to edit the rules.



4.

View Login Logs

Zero Trust Operation and Maintenance Logs record the ops records of server asset instances, making it easy for subsequent audits.

On the Server Page, click **Login Log** to navigate to **Zero Trust Operations Log** > **Server Login** page, showing the user's login logs of the current server instance. The feature of supporting login replay makes it easy to trace the user's operation behavior.

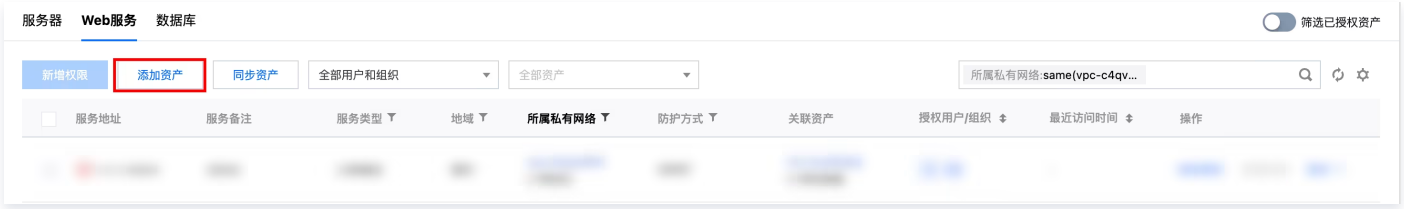
Web Service Management

Last updated: 2025-05-20 11:32:33

1. Log in to the CFW console. In the left sidebar, select **Zero Trust Operations and Maintenance** > **Asset Management**.
2. On the **Asset Management** > **Web Service** page, you can add a web service and configure the service address. It supports binding domain name to access the public network through reverse proxy to achieve advanced protection. It supports configuring access permissions for the private network with terminals and the public network without terminals. It provides viewing of authorized personnel and organizations from the perspective of the web service.

Adding a Web Service

1. On the Web service page, click **Add Asset** to add the Web asset address you need to connect.



2. In the pop-up window for adding assets, configure the information of the Web service and click **Confirm**.
   - Associated instance: the server where the Web service deployment location is located, used for integrating into the zero trust operations and maintenance network.
   - Service address: the IP address and port bound to the Web service, support through public network connection or private network connection.
   - Service remark: remark information used to manage Web services, for future unified maintenance and display.

> **Note:**
> Please confirm that the asset access switch of the server asset associated with the Web service in the VPC location has been enabled. Otherwise, it may not be associated with the corresponding asset.

Deleting a Web Service

1. On the Web service page, click **More** > **Delete Service**.

2. In the confirm deletion window, click **Confirm** to delete the current Web service.

> **Note:**

> Deletion will automatically disconnect protection, and associated permissions will be deleted. Proceed with caution.

Bind Domain Name

Bind a domain name can connect Web services to zero trust operations and maintenance instances, hide the actual service address in the form of public network reverse proxy, filter accesses of different identities, thereby avoiding service exposure on the Internet to Web attacks. It is a lightweight Web operations and maintenance solution without terminal.

Usage Scenarios

- Application object: Web services that need to expose public network access addresses, which might be public network services or private network services.
- Application scenario: need to perform identity access restriction on Web services and intercept Web attacks. Hope to hide the actual service address and access through domain name.

Operation Steps

1. Complete adding asset. On the Web service page, click **domain name binding** on the right side of the Web service.

2. In the domain name binding pop-up window, select **a connected Web domain**.

> **Note:**
> If you have not completed domain name access, you cannot select the corresponding domain name. See domain name access.

3. After selecting the domain name, you can choose whether to enable HTTPS access and configure the default access port.

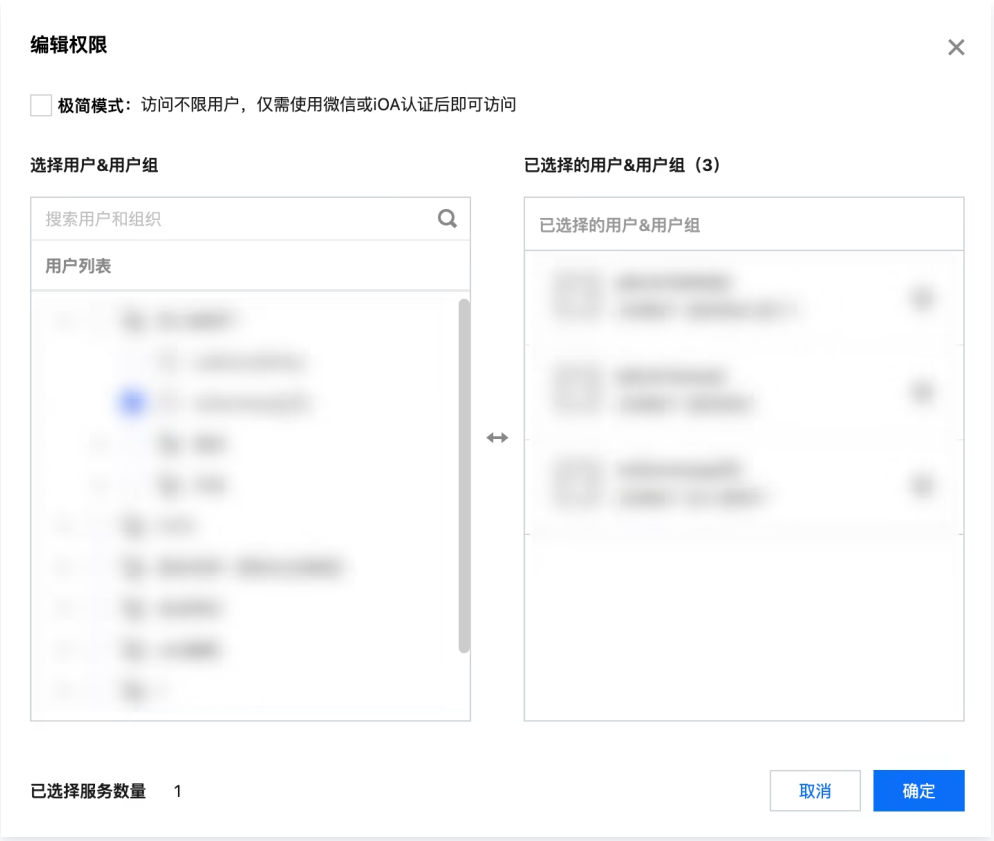
Note:
- If you do not host a certificate during domain name access, HTTPS access is not supported.
- If you need to perform Public Network Ops and configure identity-based Access Control Rules, please select to enable HTTPS.

4. Select a public network protection solution.
   - Basic protection: Provide basic protection based on frontend confrontation and frontend challenges, effectively filter humans, attackers, etc., and can be directly accessed through the domain name. **Public network access control is not supported.**
   - Advanced protection: It includes basic protection features. Perform identity authentication through WeChat or iOA before accessing the service. Advanced protection only supports HTTPS protocol.

Note:
Public network protection allows only the public network to access the Web service through the bound domain names. For direct client access to iOA, please use the actual service address to connect directly.

5. Click **next** to configure permissions for the current Web service.
   - If the protection method selects **Basic Protection**, **permission control will only take effect on iOA's client access**, and public network access will remain unrestricted.
   - If the protection method selects **advanced protection**, it is necessary to select bound users and click **confirm** to generate configuration.

> **Note:**
> In minimalist mode, there is no longer a limit on users accessing the selected service. After identity authentication, real-name authentication access can be proceed with. In this mode, the user information of all visiting users will be recorded.



6. Click **OK** to complete domain binding and permission configuration operations.

> **Note:**
> After completing the domain name binding, you can still access through the actual service address. This kind of access will bypass the firewall's permission control. It is recommended to use the firewall to block the actual service access address.

Cancel Domain Name Binding

1. On the Web service page, select the Web service that needs to cancel the binding and click on the right **Modify Binding**.

2. In the Modify Binding window, click **Unbind** to complete the unbinding operation.

Management Permission

1. On the Web services page, you can view the list of added web services and authorized users.
2. Click **Management Permission** to manage the authorized ops users of the Web service. User unbinding and addition are supported.

3. In the Edit Permission pop-up window, you can add or delete permissions. Check the users and organizations on the left to add permissions. Click ⊗ on the right to delete permissions.

> **Note:**
> The edit permissions page can only edit the permissions configured by the rule under the identity perspective. If necessary, please go to Permission Management and edit the rules from the rule perspective.

4. Click **Confirm** to save the configuration.

Database Management

Last updated: 2025-05-20 11:32:52

1. Log in to the CFW console. In the left sidebar, select **Zero Trust Operations and Maintenance** > **Asset Management**.
2. In the **Asset Management** > **Database Page**, you can perform unified viewing of database assets, overview the access permissions of integrated accesses, and conveniently view authorized personnel and organizations from a database perspective.

> **Note:**
> The current version only supports five database types: MySQL, MariaDB, Redis, CKafka, and ElasticSearch. Editing permissions through the database perspective is not supported yet.

View Authorized Users/Organizations

You can hover over the **Authorized User/Organization** column in the list to view authorized users or organizations.

View Access Logs

You can click **Access Log** in the operations area on the right side of the list, and navigate to Zero Trust Operations Log to view all access records of the current database.

Permission Management Overview

Last updated: 2025-05-20 11:34:49

The permission management module is primarily responsible for issuing and managing permissions for integrated identity information and asset information. Overall, it can be divided into two parts: identity perspective and rule perspective.

- Identity perspective: View the permission information of assets owned from the perspective of individuals or organizations.
- Rule perspective: Manage access control permissions from the perspective of allowlist rules.

The identity perspective provides more intuitive and precise permission configuration; the rule perspective tends to issue permissions on a large scale or in batches, making it more suitable for users with a larger number of personnel or assets and faster changes.

Identity Perspective

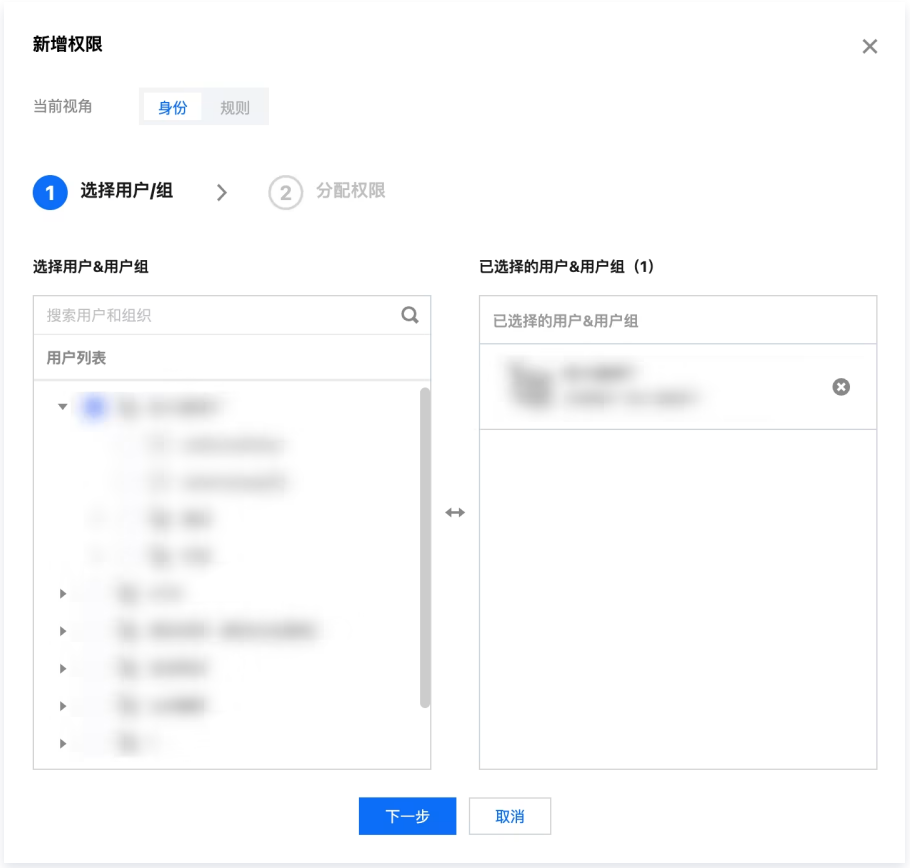
Last updated: 2025-05-20 11:35:09

View the permission information of assets owned from the perspective of a person or an organization.

New Permissions

1. Log in to the CFW console. In the left sidebar, select **Zero Trust Operations and Maintenance** > **Permission Management**.
2. In Permission Management, click **Add New Permissions**.

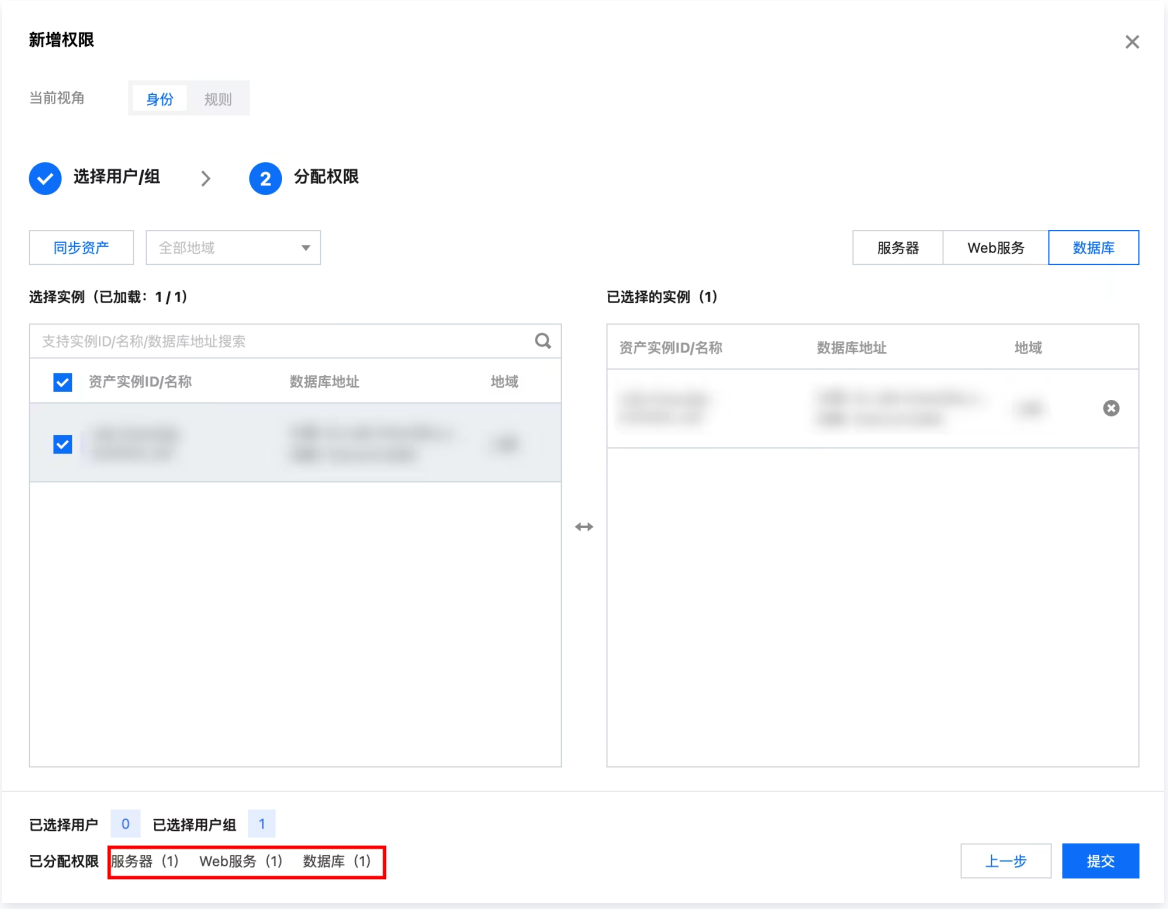
3. Select the identity perspective, select user/user group. After checking, confirm the selected authorized users among the selected users/user groups. Click **Next**.



> **Note:**
> When a user group is selected, permissions are granted to the organizational structure. Even if the organizational user members change subsequently, all users under the organization will have access privileges.

4. For the selected user/user group, assign asset permissions, including server assets, Web services, and database assets.

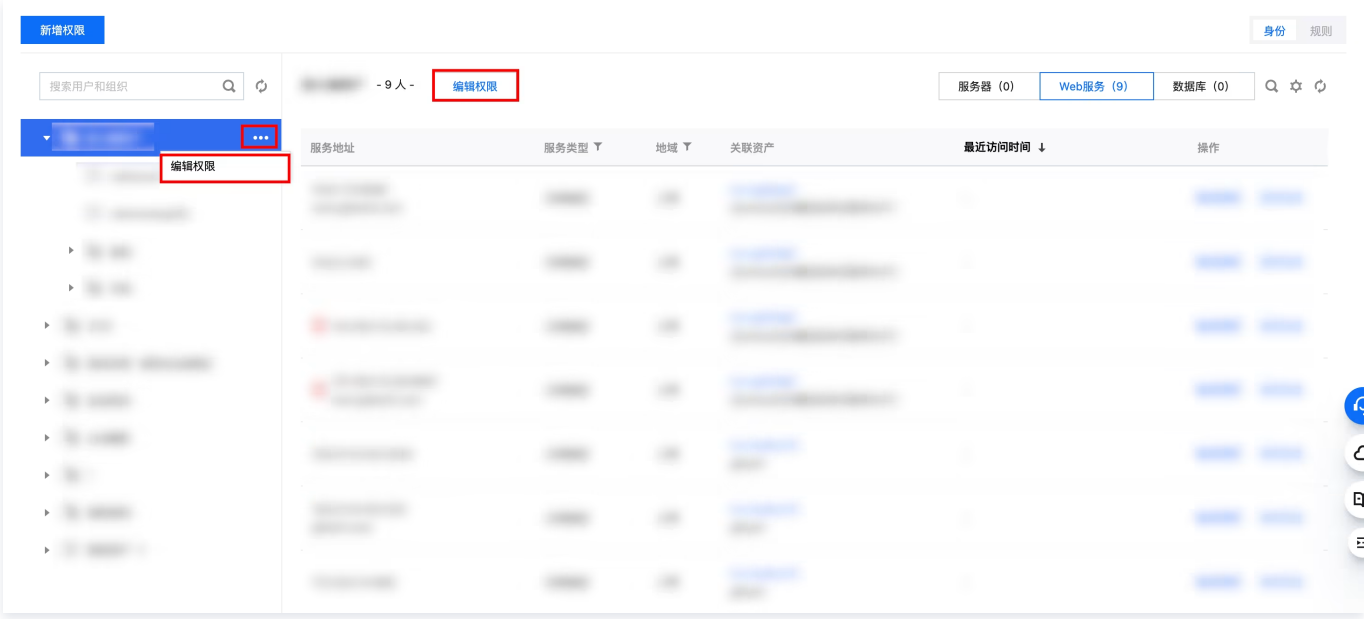
Support filtering assets by region and asset type for selection. After selecting allocated assets, the current number of selected users and user groups, as well as the number of allocated operations instances and Web services, will be displayed below the pop-up. Confirm that everything is correct, then click **Submit** to complete the addition of permissions.



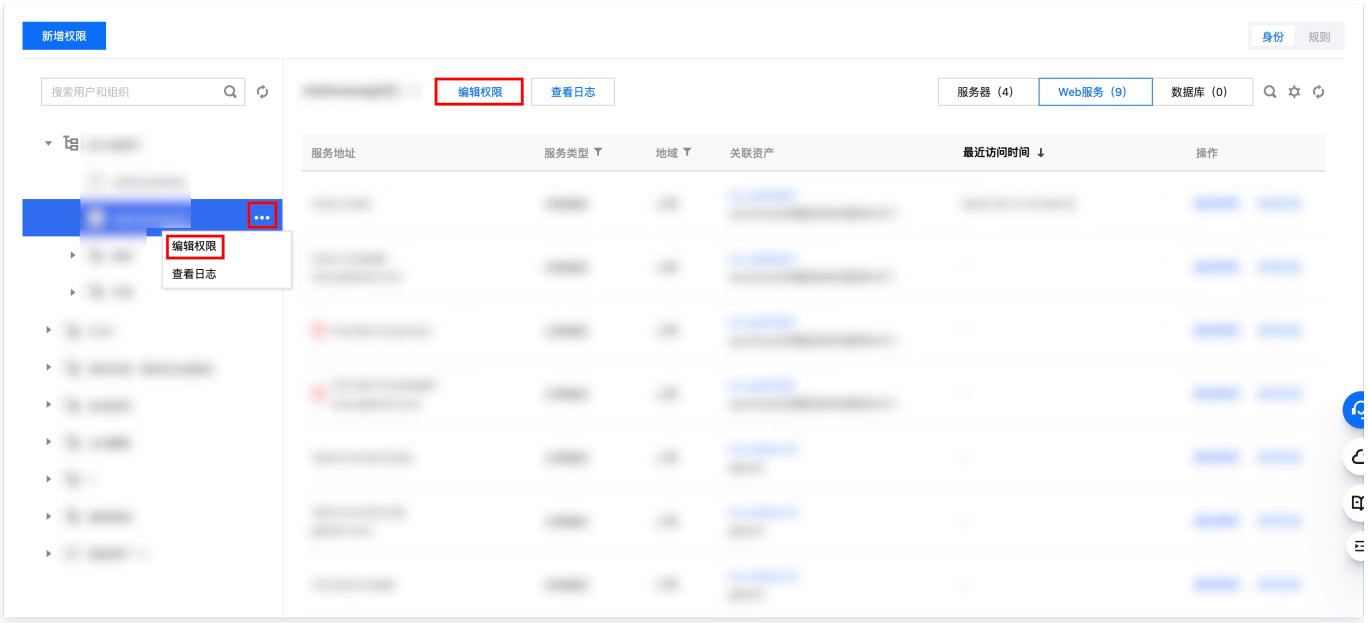
Edit Permission

Support editing permissions for each user or user group.

1. On the Permission Management Page, select the identity perspective and select the user/user group whose permissions need to be edited. The accessible assets corresponding to the permissions of this user/user group appear on the right side of the page.
2. Click ••• on the right of the avatar. The user identity operation options appear. Click **Edit Permission**. Editing user/user group identity privileges is supported.
   - Organization



- User

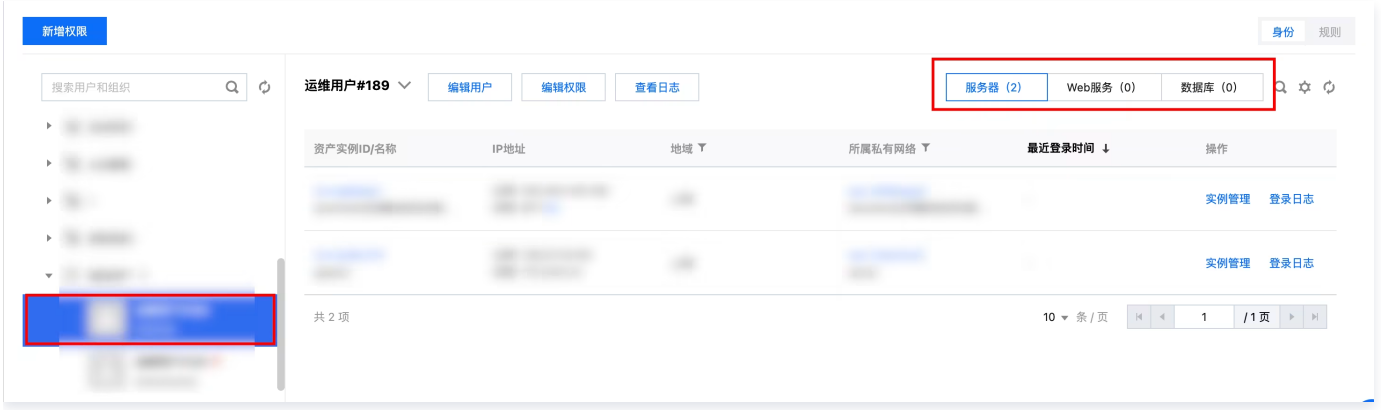


3. In the pop-up window for editing user permissions, reselect the assets that this user/user group is authorized to access. The number of asset permissions currently allocated to this user/user group will be displayed below the pop-up window. Confirm that everything is correct, and click **Confirm** to complete the permission editing.

> **Note:**
> The Edit Permissions page can only edit rule permissions added from the identity perspective. If you need to edit inherited permissions, please go to the rule perspective of Permission Management to edit the rules.

View Permissions

On the Permission Management page, select the user/user group whose permissions you want to view. The accessible assets corresponding to the permissions of this user/user group will appear on the right side of the page, including servers, Web services, database types. It supports viewing asset instance names/IDs, IP addresses, regions, associated VPCs, latest log-in times, etc.



Rule Perspective

Last updated: 2025-05-20 11:35:31

The rule perspective is to manage access control permissions from the perspective of allowlist rules.

New Permissions

1. Log in to the CFW console. In the left sidebar, select **Zero Trust Operations and Maintenance** > **Permission Management**.
2. In Permission Management, click **Add New Permissions**.

3. Select the selection rule perspective, fill in the source, access destination and description.

Parameter Name	Description
Access source type	• Personal: Once selected, you can choose an individual user or WeChat user in iOA. • Organization: You can select an organizational unit in iOA or all WeChat users.
Access destination type	• Server: Select server type assets. • Web service: Select web service type assets. **Note:** When the identity information selects the iOA identity, the Web service type is unlimited; if the identity information selects the WeChat identity, the Web service can only select assets that have a bound domain name and the protection type is advanced protection. • Database: Select database type assets. **Note:**

> WeChat identity is not supported. Only iOA private network on-premises Ops is allowed.

- Asset group: Select an asset group. CFW will automatically distribute permissions to server type and database type assets under the asset group.
- Tag: Select a resource tag. CFW will automatically distribute permissions to server type and database type assets associated with the resource tag.

4. **Click Confirm**. The CFW will automatically grant access permissions based on the filled-in identity information and authorized assets. You can also view the corresponding permissions from the identity perspective or the corresponding assets. There may be a delay in permission deployment. Wait patiently.

Edit Permission

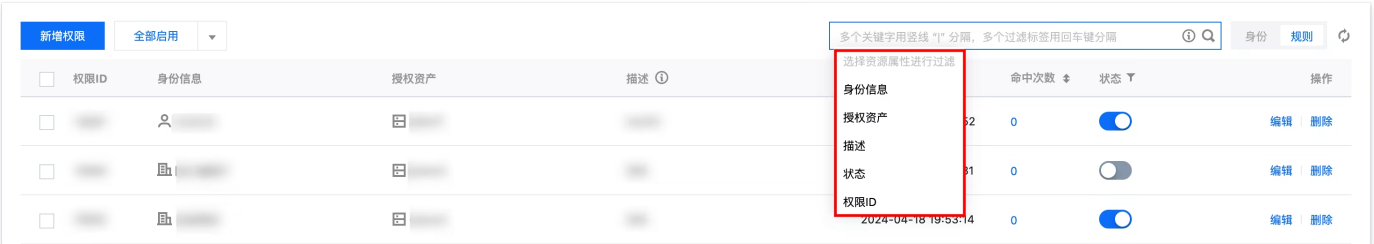
1. Find the permission you want to modify and click on the right **Edit**.

2. You can modify identity information, authorized assets, or description in the permission editing status. For specific fields, refer to adding new permissions.

Permission to View

1. Log in to the CFW console. In the left sidebar, select **Zero Trust Operations and Maintenance** > **Permission Management**.
2. In permission management, click on the rule to switch to the rule viewing angle.

3. You can view all rule contents with permissions in the permission list below.
4. Support retrieving permissions based on permission ID, identity information, authorized assets, and description.



Log-In Methods
WeChat User Remote Server Login Via Public Network

Last updated: 2025-05-20 11:36:03

After configuring the login permission of the user who integrates zero trust operations and maintenance, verify whether the configuration takes effect by logging in remotely using the domain name.

Quick Start

This video introduces how to quickly start WeChat remote ops.
Watch video

Login Method of Type SSH

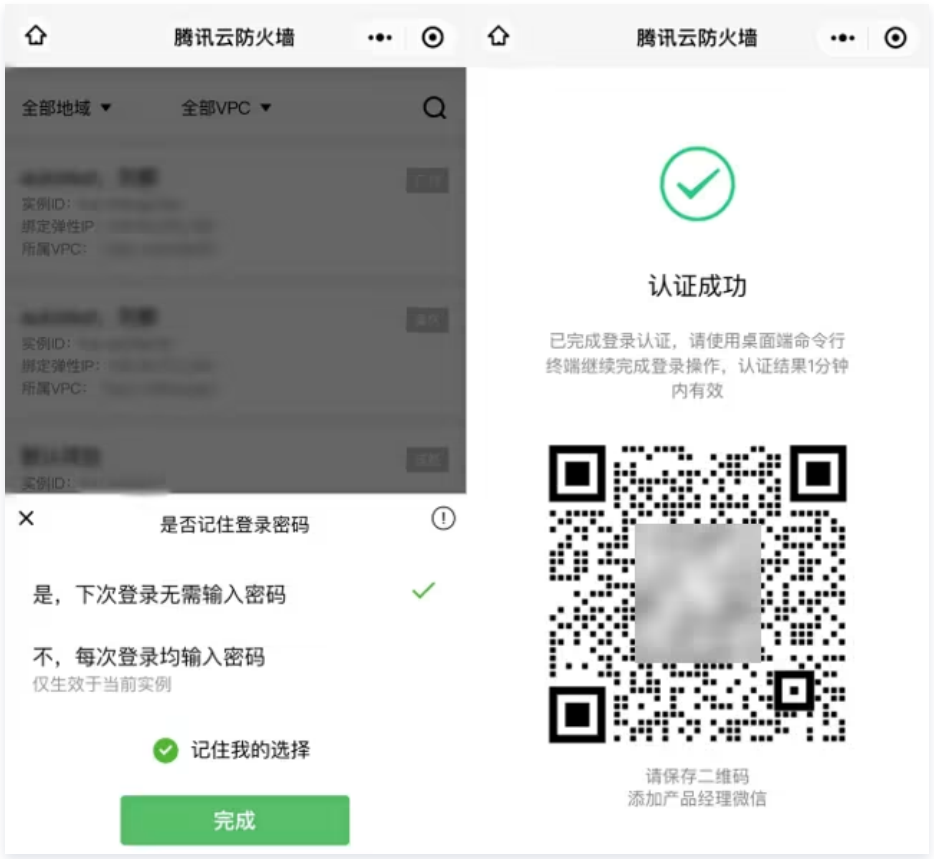
1. Enter the command in the command line:
   - Method 1: Use username login. Execute the command ssh username `@cfw.tencentcs.com`, for example `ssh abc123@cfw.tencentcs.com`.
   - Method 2: Use the root user to log in. Execute the command `ssh root@cfw.tencentcs.com`.
2. CFW will return a QR code in command line. WeChat Scan this QR code with the WeChat identity privilege bound in Access on the console before using.

> **Note:**
> If the QR code is not displayed normally, there will be a URL at the end. Accessing this URL can also show the QR code.

3. In WeChat, select the Tencent Cloud account and instance to perform authorization login.

4. After authorization-based login, please complete the log-in operation within 1 minute; otherwise, reauthorization is required. If you choose to remember the login password, the cloud firewall will record the user's password for command line log-in. Subsequent log-ins will no longer require manual log-in. Even if the password is changed, the firewall will automatically record

the new password.

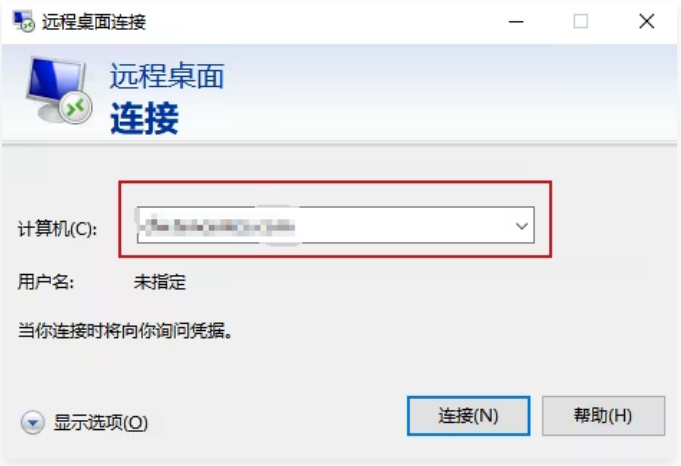


Note:

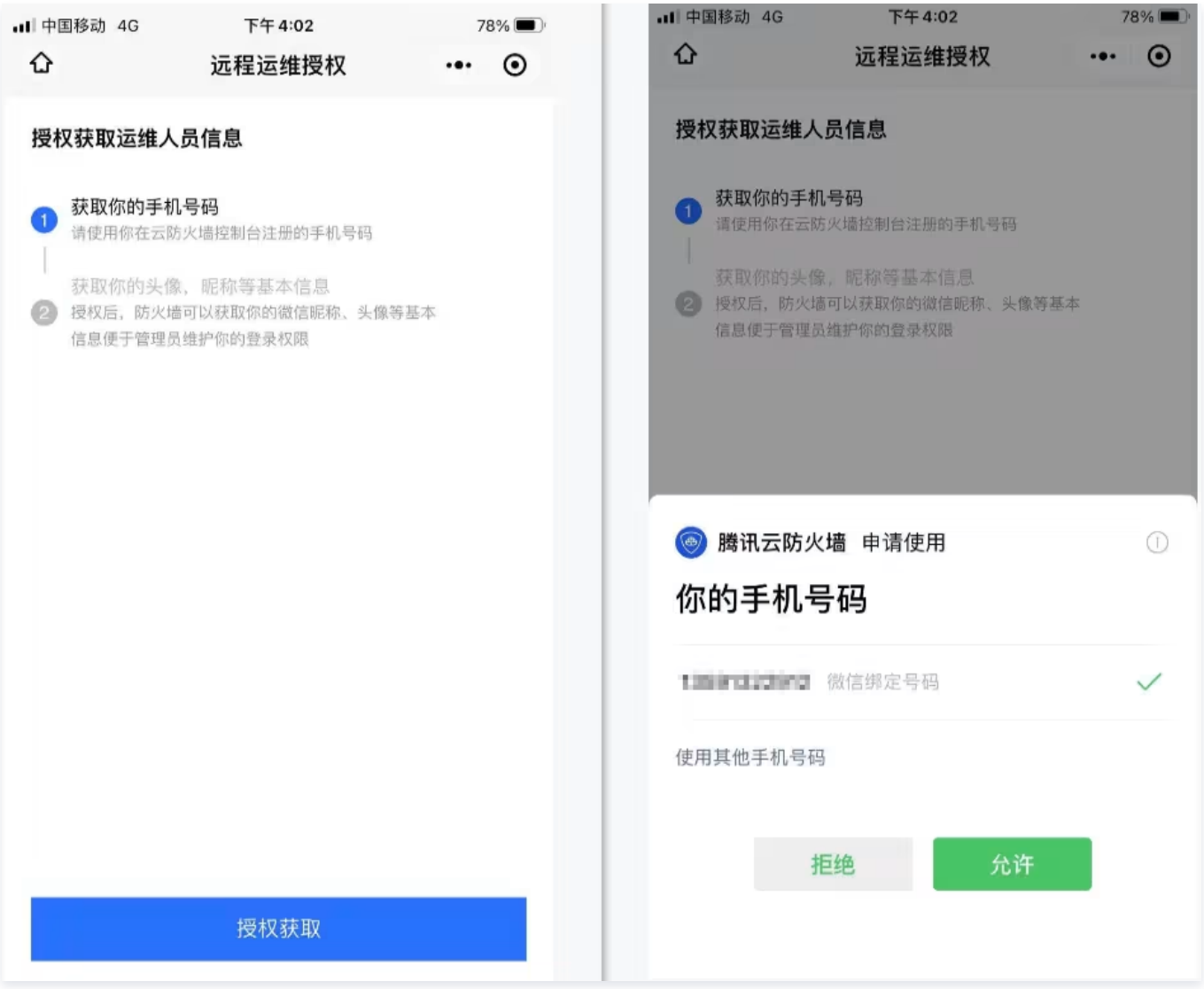
- If the operating system is Windows, the type is RDP and the port is 3389.
- Note: If the operating system is another, the type is SSH and the port is 22.
- If the QR code of SSH is scanned, only display the instance list of SSH.
- If the QR code of RDP is scanned, only display the instance list of RDP.

Login Method of Type RDP

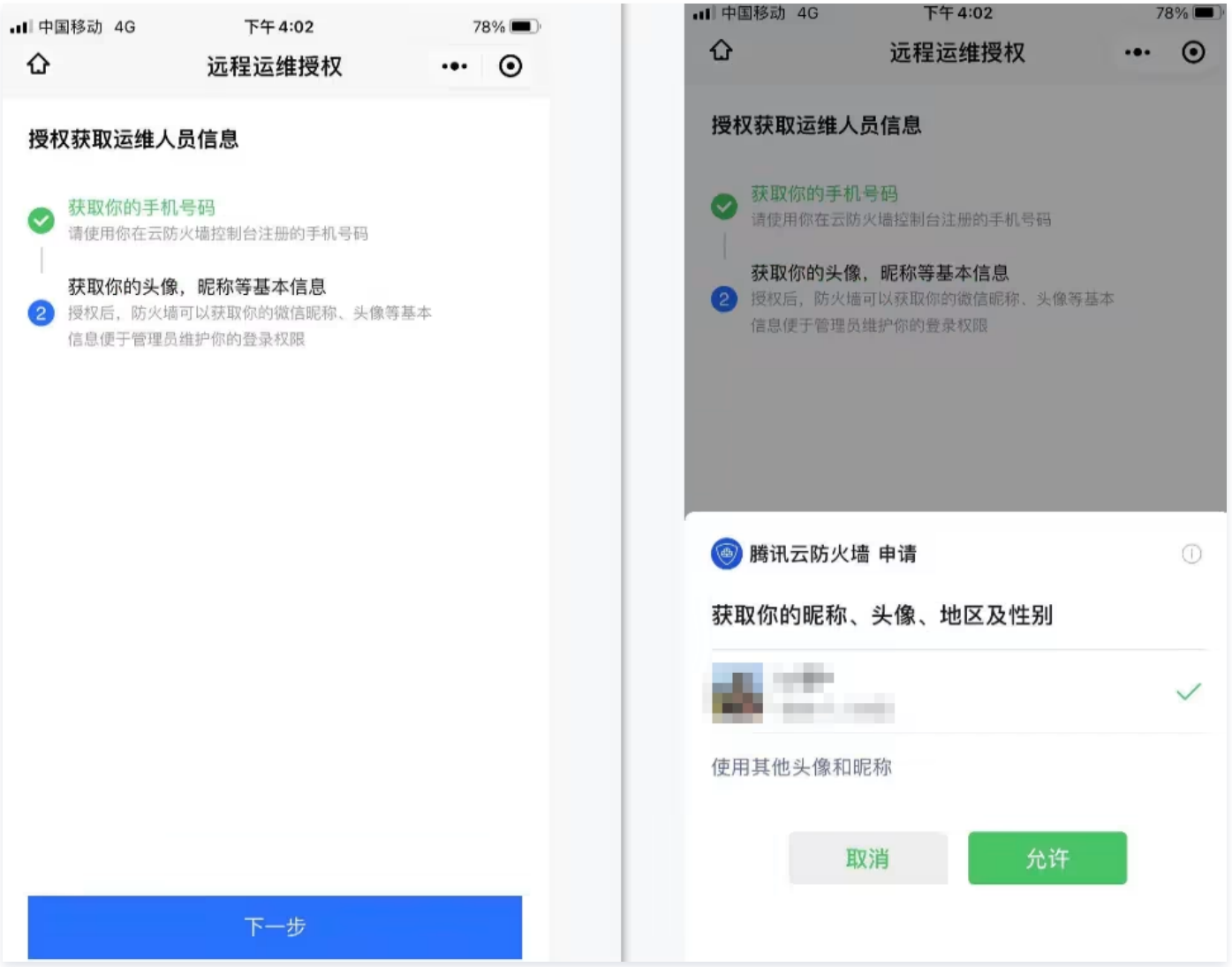
1. O&M personnel open the remote ops desktop feature on the machine, input the domain specified by the console, click **Connect**, and return to the page of the QR code.



2. O&M personnel scan the authorization QR code to obtain the mobile number.



3. Retrieve WeChat profile photo and Nickname, click **Allow** to complete successful authorization.



4. Select the instance that needs login. After verification is complete, remote ops can be performed. After authorization-based login, please complete the login operation within 1 minute, otherwise reauthorization is required.

> **Note:**
> - If the operating system is Windows, the type is RDP and the port is 3389.
> - If the operating system is another, the type is SSH and the port is 22.
> - If the QR code of SSH is scanned, only display the instance list of SSH.
> - If you scan the QR code of RDP, only the instance list of RDP will be displayed.

iOA User'S Intranet Access to Ops Assets

Last updated: 2025-05-20 11:36:21

Prerequisites

1. Completed iOA identity directory integration.
2. Configure user permissions has been done.
3. Logged in to iOA terminal device.
4. Access operation and maintenance assets through iOA proxy intranet access.

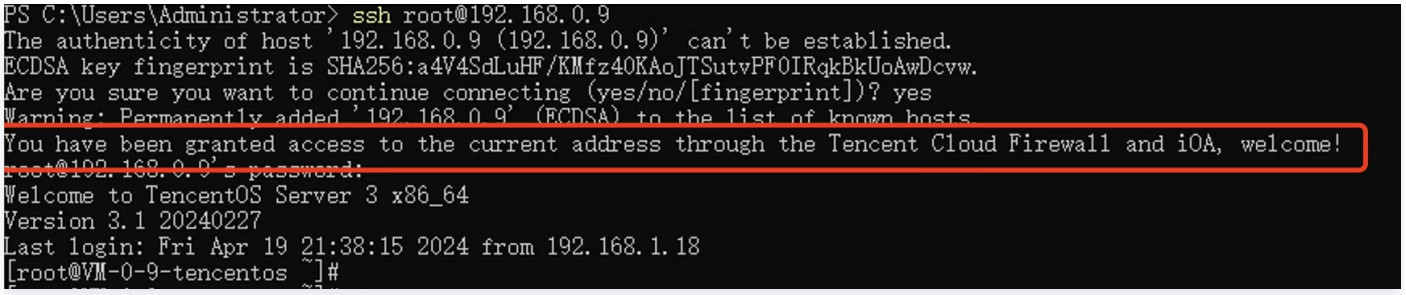
Access Method

iOA user support can directly access operation and maintenance assets of server type, Web service type, and database type through private network.

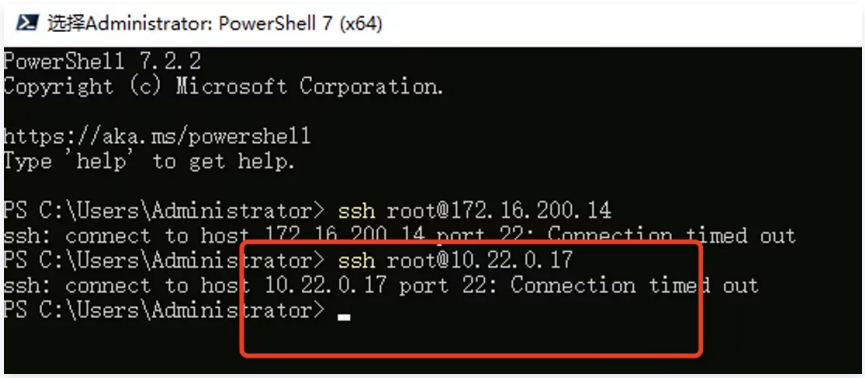
> **Note:**
> Directly access the asset through its real address. If you access it through the bound domain name, the private network direct connection will not be used to operate and maintain the asset.

Server Asset Login

1. Enter username, password and server address directly on the command line to connect. For example: `ssh root@192.168.0.9 -p 2222`.
2. If you have the permission of the corresponding server, you can directly continue with the next operation.



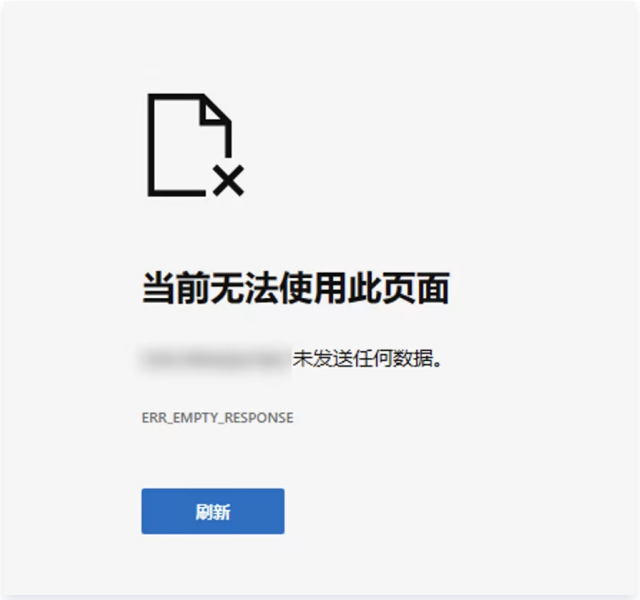
3. If you don't have access, it may prompt a connection timeout.



Access to Web Services Assets

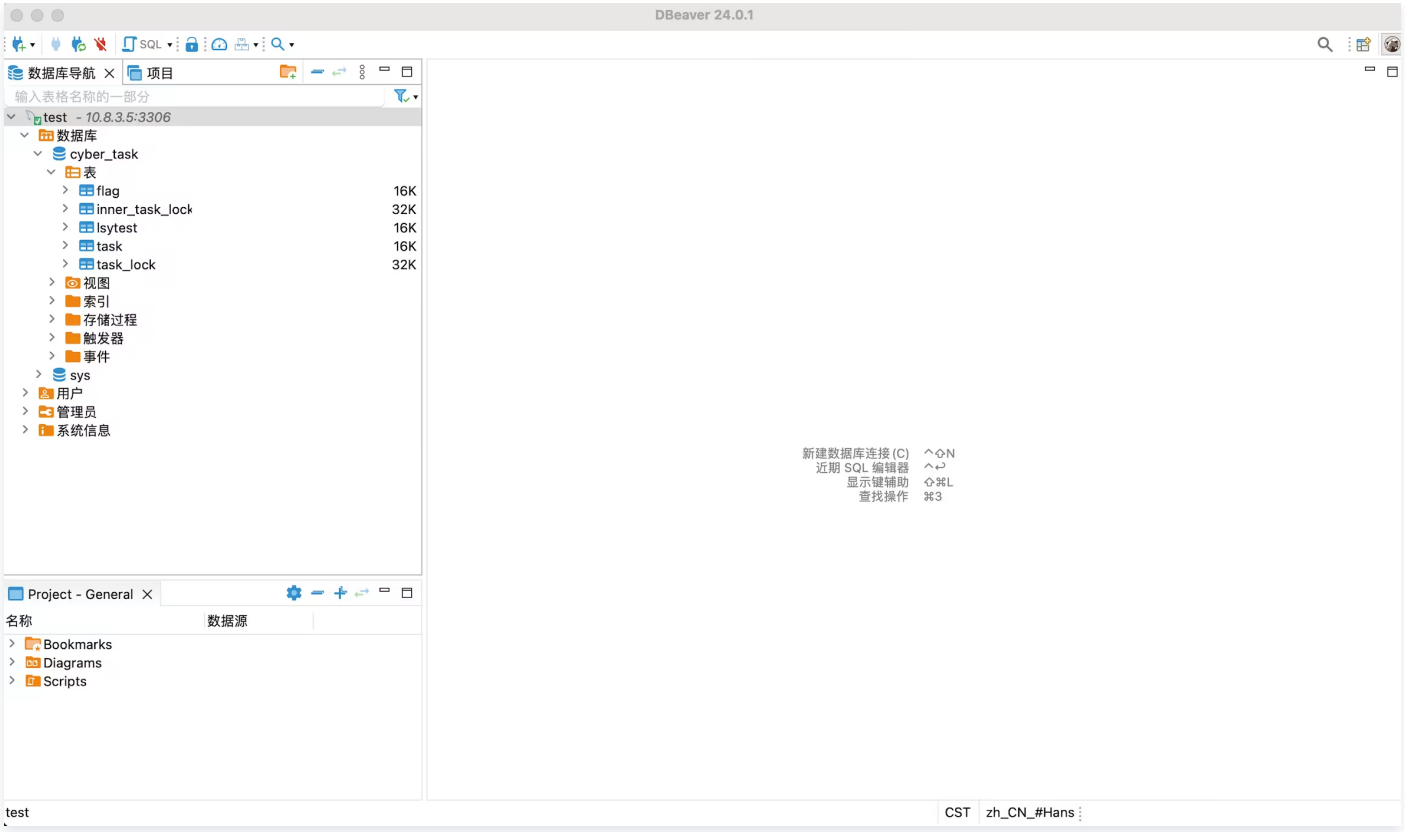
1. Enter the actual service address directly in the browser to connect. For example: `https://192.168.0.9/`.
2. If you have the permission of the corresponding server, you can directly continue with the next operation.

3. If you have no permission, it may prompt no response.



Database Asset Login

1. You can connect to the corresponding database through the database's self-owned protocol or command line.
2. If you have the permission of the corresponding database, you can directly continue with the next operation. Otherwise, it will result in a connection timeout and inability to access.



3. If you don't have access, it may prompt a connection timeout.

WeChat or iOA User Public Network Access to Web Service

Last updated: 2025-05-20 11:36:42

Access Prerequisites

1. Completed domain name binding.
2. Modified the domain name resolution address.
3. Configured user permissions.
4. Access Web service via public network.

Access Method

1. Directly enter the bound domain name in a browser to access, and a QR code for identity verification will pop up.
2. Please use a WeChat account with permissions to scan the QR code to confirm your identity.

3. If you are an iOA user, you can also click below **other login methods** to go to iOA for identity verification.

4. After authentication, the Web service can be accessed.

Network Honeypot Overview

Last updated: 2025-05-28 10:39:02

A network honeypot is a simulated business system running on the Internet that does not actually handle any real business. The network honeypot exposes probes in the user's network. For example, if an attacker triggers it, it will actively record attacker information and track attack methods, providing accurate attacker intelligence and counter-tracing capability for the defense of real business. Meanwhile, in critical protection scenarios, the network honeypot buys sufficient time for real business operations to achieve a successful defense.
The honeypot service of Tencent Cloud Firewall is deployed in Tencent Cloud honeyfarm, without occupying users' network space, and achieves mutual isolation by deploying different VPCs. Even if an attacker gains access, it will not cause lateral movement. The exposed probe of the honeypot is deployed in the user's network, which can be an IP or domain name, and forwards traffic of specified ports/paths to different honeypot services, achieving the deployment of "traps" in the business system.

Using Network Honeypots

1. Create a new probe, and enable it.
2. Manage probes.
3. Create a honeypot service, bind a probe.
4. Manage honeypot services.
5. Defense and source tracing, view network honeypot alarms and logs.

Main Feature

Honeypot service based on Tencent Cloud Firewall has the following three main features:

- High simulation degree and cannot be easily detected by attackers.
- Collects attacker information to provide to the defender.
- Delays attackers and provides time assurance for network security protection.

The security of the business system is directly proportional to the probe count and does not excessively occupy the user's network resource. By using high-authenticity simulation services in the honeynet, it achieves the purpose of deceiving attackers.

Alarm and Log

Attack Deception Event Alarm

On the **Alert Center** > Attack Deception Events page, you can view detailed information about attack deception events detected by network honeypots.

Network Honeypot Deception Logs

On the **Log Audit** > **Intrusion Prevention Log** > Network Honeypot page, you can view log information about attack deception events detected by network honeypots.
Network Honeypot Operation Logs
On the **Log Audit** > **Operation Log** > Network Honeypot Operations page, you can view operation details of the network honeypot feature and corresponding accounts.

Version Support Notes

CFW Advanced Edition, Enterprise Edition, and Flagship Edition all support purchasing honeypot service quotas. For details, see Purchase Guide.

Create a Probe

Last updated: 2025-05-28 10:40:01

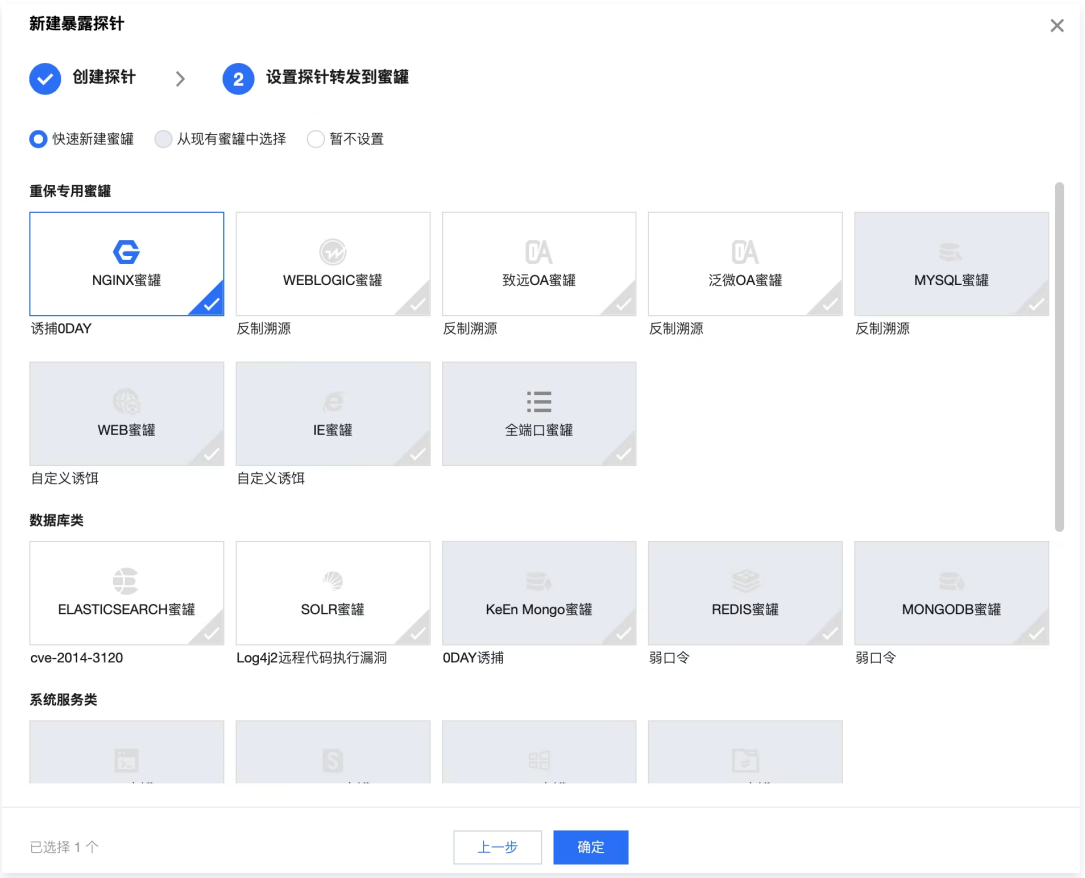
An exposure probe is a "trap" deployed in a user's business system. It can be an IP or domain name, forwarding traffic from specified ports/paths to a designated honeypot service. This enables recording attacker information and tracing attack methods. Therefore, the network honeypot service must be associated with the exposure probe to run properly.
When entering the network honeypot console, users will default to the **probe exposure** page. It is recommended that users first create a new probe, then create a honeypot and associate it with the corresponding probe.

1. Log in to the CFW console, in the left sidebar, click **network honeypot** > **probe exposure**.
2. On the probe exposure page, click **Create Probe**.

3. In the pop-up window for creating a probe exposure, select the region, instance name, deployment mode, and Elastic IP, then click **Next**.

Parameter	Description
Region	Supports domestic partial regions (specific regions can log in to the CFW console > **network honeypot** > **create a new probe** > **region** to view). Cannot be changed after the instance is created.
Instance name	Custom instance name.
Deployment mode	• private IP: Select a subnet, and we will automatically create an ENI and a private IP. The designated port of this IP can be configured to forward to the honeypot service. • public IP: Select an existing public IP to deploy a probe. The traffic on the designated port of this IP will be forwarded to the honeypot service. • Load balancing: Select an existing load balancing instance to deploy a probe. The traffic on the path of the specified domain name will be forwarded to the honeypot service.
Select a subnet	When the deployment mode is private IP, this content requires configuration.
IP Address	This content requires configuration when the deployment mode is private IP.
EIP	This content requires configuration when the deployment mode is public IP. Select create EIP.
Deployed instance	This content requires configuration when the deployment mode is CLB. Configure according to actual needs.
Domain name	This should be set when the deployment mode is load balancer. Set this as needed.
forwarder	When the deployment mode is CLB, this content requires configuration. Please select a CVM instance from the VPC where the current CLB instance belongs as the backend service of the current listener. Only CVM instances supporting Linux systems are allowed.
Honeypot service	Support rapid creation of honeypots, selection from existing honeypots, or not setting yet.

4. Set up the honeypot service, click **OK** to complete the creation.



- Quick create honeypot: Click **Quick create honeypot**, select the desired honeypot services, and multiple selections are allowed.

  > **Notes:**
  > Since the WEB honeypot requires using existing SSH/MySQL honeypots as bait, it will not automatically associate with bait after quick selection. When a user clicks Quick Select Honeypot and selects the WEB honeypot while creating a new probe, the honeypot service does not start working. The user needs to find the corresponding WEB honeypot in the honeypot service, edit it, and associate it with the corresponding SSH/MySQL honeypot before the honeypot service starts working.

- Select from existing honeypots: Click **Select from existing honeypots**, choose the desired honeypot services (multiple selections allowed), and modify the listening port or input path as required.

  > **Notes:**
  > - When the deployment mode is public IP, the listening port can be modified.
  > - When the deployment mode is load balancing, some honeypots support customizable paths. Details are based on the console.

5. Enable probes individually or in batches.
   - Select a target probe, click  in the switch column, then click **OK** in the "Confirm Enable" pop-up window to enable a single probe.

- Select one or more probes, click **Enable Probe**, click **Confirm** in the "Confirm Enable" pop-up window to enable multiple probes.

Managing Probes

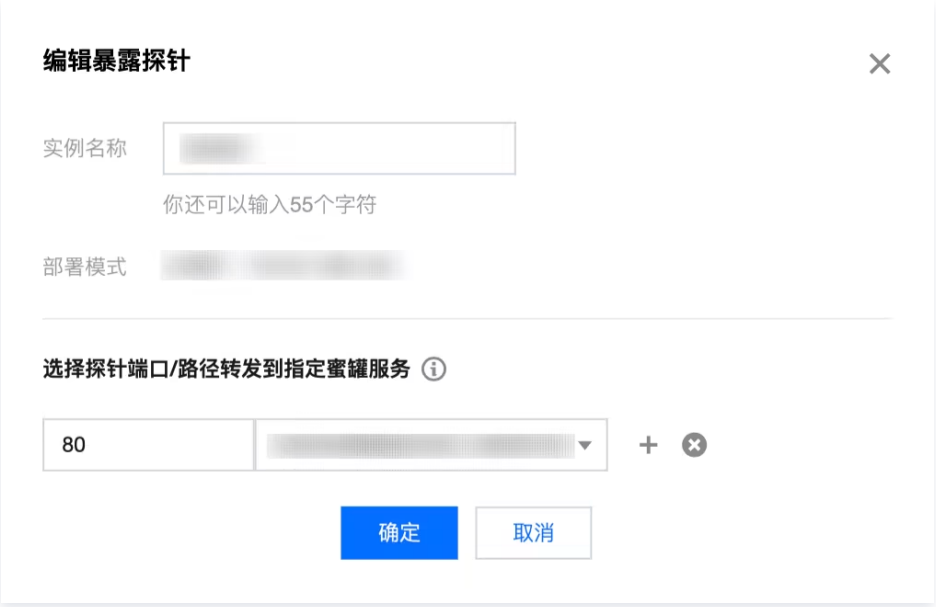
Last updated: 2025-05-20 14:22:02

Perform operations such as editing, deleting, filtering, and sorting on the established exposure probes.

Editing Configuration

1. Log in to the CFW console. In the left sidebar, click **Network Honeypot** > **Probe Exposure Page**.
2. On the Probe Exposure Page, select a target probe and click **Edit** in the Action column.

3. In the Edit Probe Exposure pop-up window, you can modify the instance name and the probe port/path forwarded to the honeypot service. Click **Confirm** to save changes.



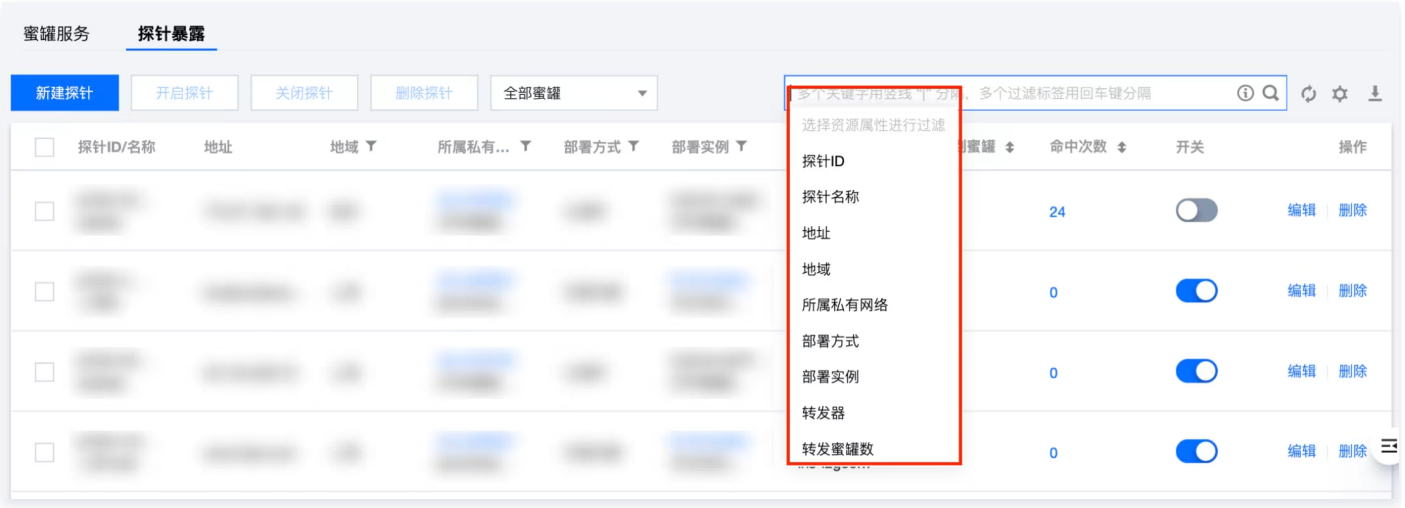
Deleting Probe

1. On the Probe Exposure Page, you can enable individually or delete probes in batches.
   - Select a target probe, click **Delete** in the Action column, click **Confirm** in the "Confirm deletion" pop-up window to delete a probe.

- Batch: Select one or more probes, click **Delete**, click **Confirm** in the "Confirm deletion" pop-up window to delete the selected probes.

Filtering/Sorting

- On the Probe Exposure Page, click the search box, support filtering probe exposure events by keywords such as "Probe ID, Probe Name".



- Click the headers "Region", "Belonging to Virtual Private Cloud", "Deployment Method", "Deployment Instance" and "Forwarder" in the probe exposure list in figure to filter probe exposure events.

- Click the headers "Forward to Honeypot" and "Number of Hits" in the probe exposure list in figure to display probe exposure events in ascending or descending order.

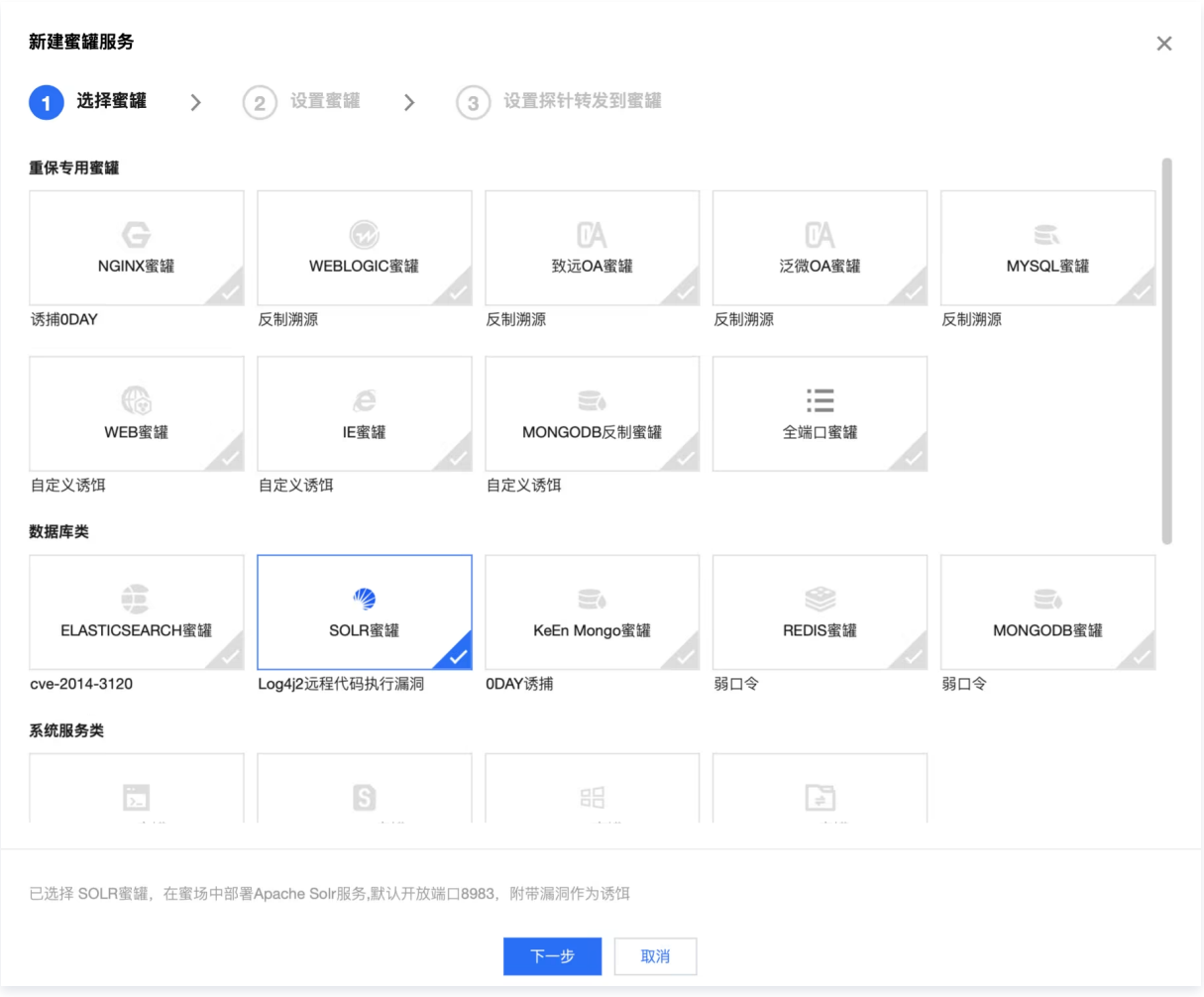
Creating a Honeypot Service

Last updated: 2025-05-20 14:22:19

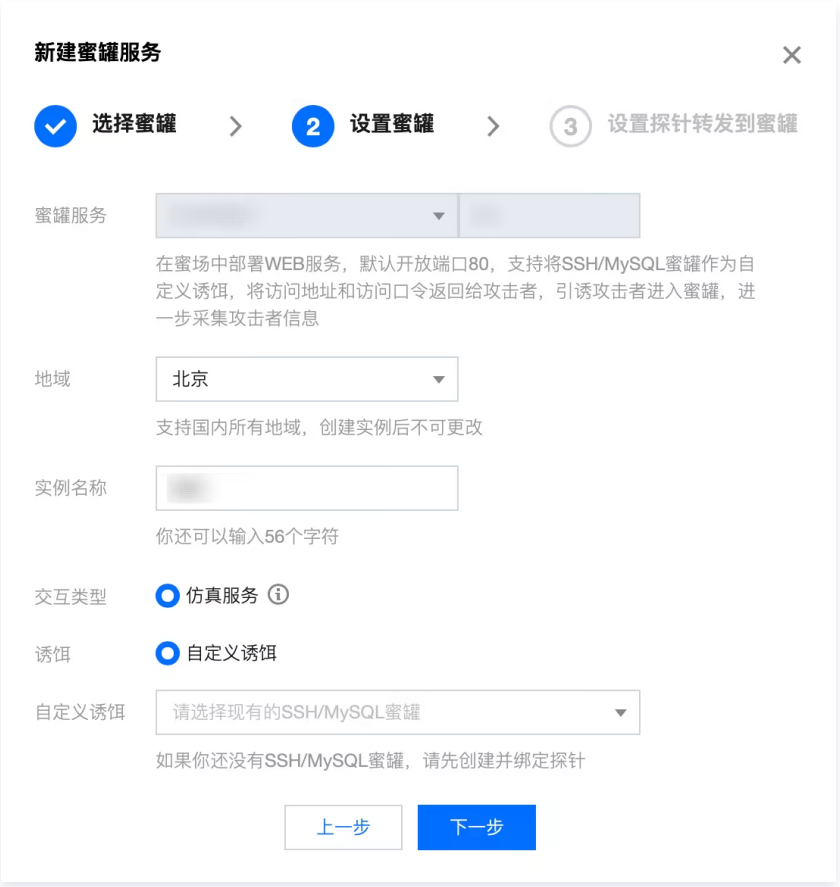
The network honeypot service and exposure probe can only run properly after association. After creating an exposure probe, it is required to create a honeypot service associated with it.

1. Log in to the CFW console. In the left sidebar, click **Network Honeypot** > **Honeypot Services**.
2. On the honeypot service page, click **Create Honeypot**.

3. In the window for creating a new honeypot service, select the required honeypot service type and click **Next**.



4. Set relevant parameters for the honeypot. Then, click **Next** to set the forwarding of probes to the honeypot.



Parameter	Description
Region	Supports all domestic regions and cannot be changed after the instance is created.
Instance Name	Customize the instance name.
Honeypot Service	Including ELASTICSEARCH honeypot, MYSQL honeypot, NGINX honeypot, SALTSTACK honeypot, SSH honeypot, STRUTS honeypot, WEBLOGIC honeypot and web honeypot. Among them, except for the web honeypot, all other types of honeypots have built-in bait and vulnerabilities.
Interaction type	• Real service: high interaction type, running real services and bait on the backend, will fully respond to each request from attackers, thereby fully deceiving attackers and buying time for real protection. • Simulation service: medium interaction type, running simulated services and bait on the backend, can generate corresponding response information according to some requests from attackers and induce attackers to continue execution, thereby buying time for real protection.
Bait	• ELASTICSEARCH honeypot: cve-2014-3120. • SALTSTACK honeypot: cve-2020-11651. • SSH honeypot: weak password. • STRUTS honeypot: cve-2017-12611. • WEBLOGIC honeypot: cve-2017-10271. • Other honeypots: none.
Custom bait	• MYSQL honeypot, SSH honeypot: selectable login password, and set password. • WEB honeypot: available existing SSH/MySQL honeypots can be used as custom bait. If there is not yet an SSH/MySQL honeypot, please first create and bind a probe. • Other honeypots: none.
Set the probe.	• Select from existing probes: Select from existing probes, and then select the required probe instance and port number.

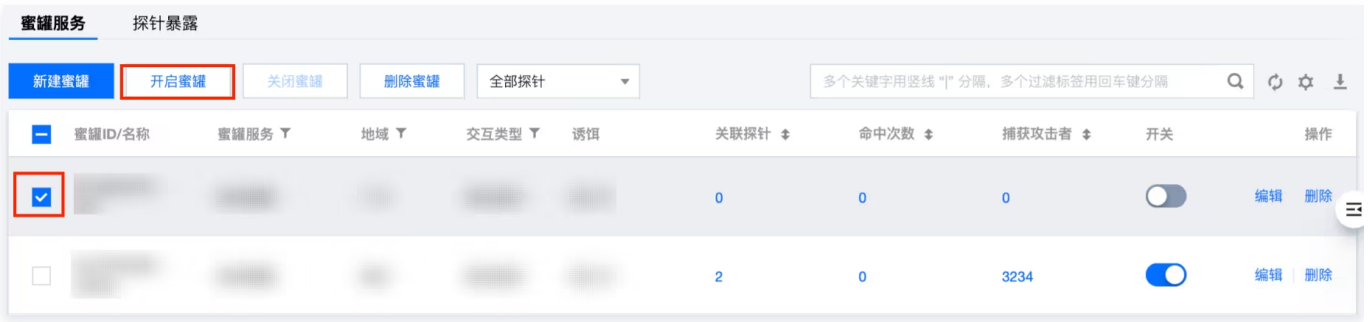
- Not set yet: do not bind a probe.

5. Bind the exposed probe.
   - Select from existing probes: select, choose the required probe instance and port number, and click **Confirm**.
   - No probe or not set yet: bind probe later, click **Confirm**.

> **Note:**
> The honeypot service must be bound to a probe to be effective. If you select not to set it for now, users can rebind the probe by editing the honeypot after the honeypot is created or complete the binding with the honeypot in the probe interface.

6. Enable honeypots individually or in batches.
   - Individually: Select a target honeypot, click  in the switch column, and in the "Enable" pop-up window, click **Confirm** to enable the current honeypot service.

   - Batch: Select one or more honeypots, click **Enable Honeypots**, and in the "Confirm Enable" pop-up window, click **Confirm** to enable the selected honeypot services.



Managing Honeypots

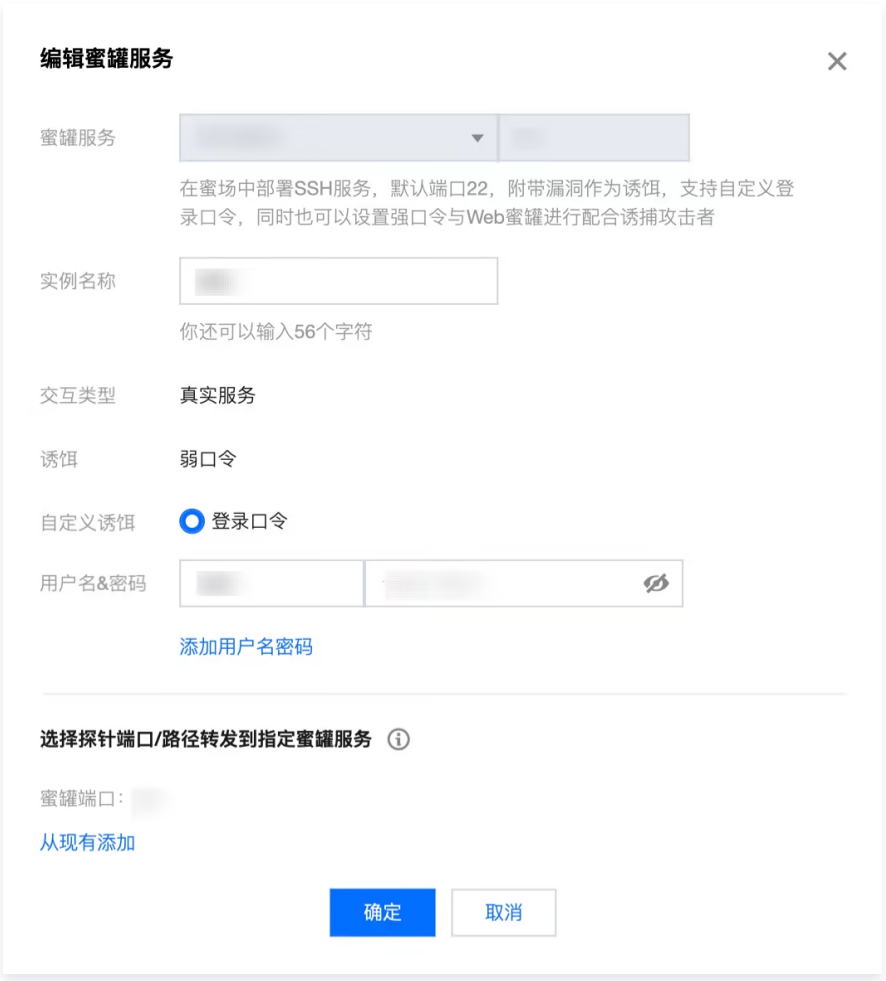
Last updated: 2025-05-20 14:22:37

Perform operations such as editing, deleting, filtering, and sorting on the established honeypot services.

Editing Configuration

1. Log in to the CFW console. In the left sidebar, click **Network Honeypot** > **Honeypot Services**.
2. On the honeypot service page, select a honeypot service and click **Edit** in the Action column.

3. In the pop-up window for editing the honeypot service, you can modify the instance name and associate exposed probes. Click **Confirm** to save changes.



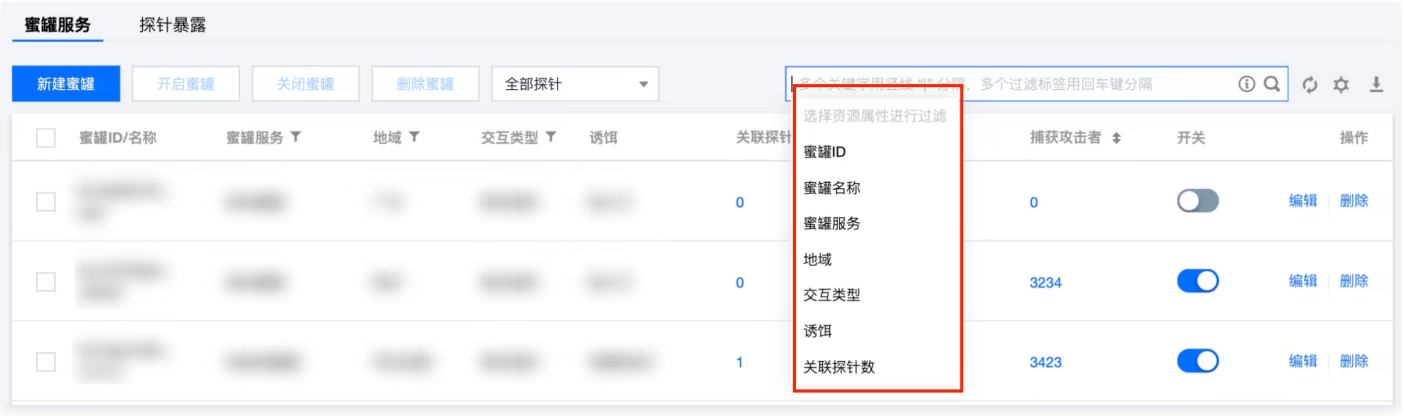
Deleting Honeypots

1. On the Honeypot Service Page, you can delete honeypots individually or in batches.
   - Select a target honeypot, click **Delete** in the Action column. In the "Confirm deletion" pop-up window, click **OK** to delete a honeypot.

- Batch: Select one or more honeypots, click **Delete**. In the "Confirm deletion" pop-up window, click **OK** to delete the selected honeypots.

Filtering/Sorting

- On the Honeypot Service Page, click the search box and filter honeypot service events by keywords such as "Honeypot ID, Honeypot Name".



- Click the headers "Honeypot Service", "Region" and "Interaction Type" in the honeypot service list to filter honeypot service events.

- Click the headers "Associated Probe" and "Number of Hits" in the honeypot service list to display honeypot service events in ascending or descending order.

Defending and Tracing the Source

Last updated: 2025-05-20 14:22:54

View Alarms

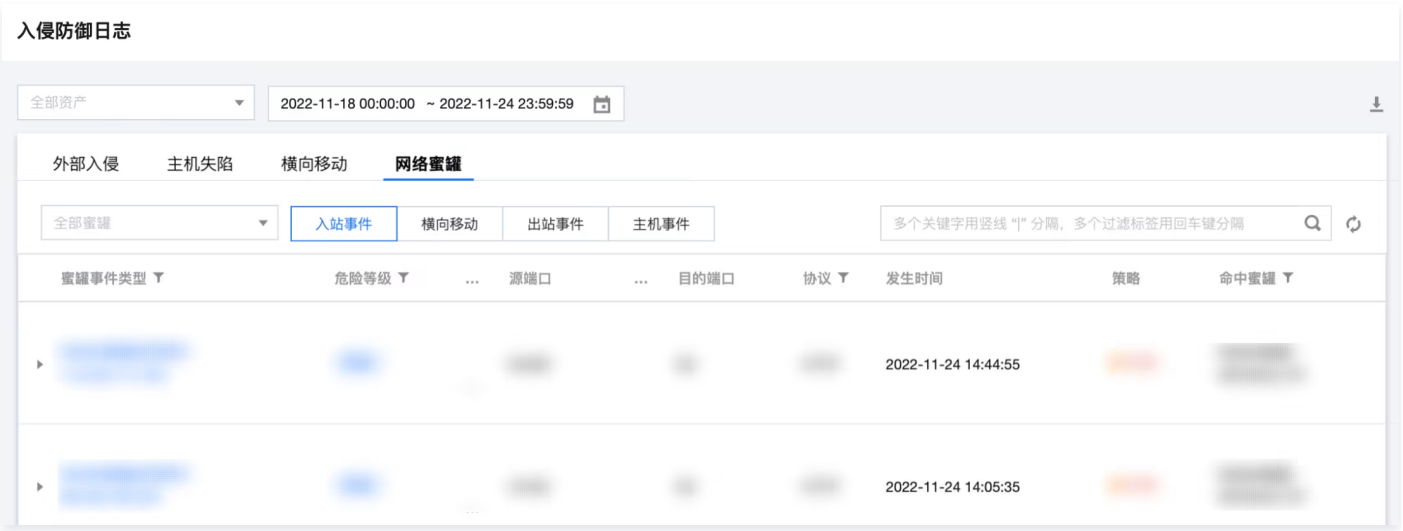
1. Log in to the CFW console. In the left sidebar, click **Network Honeypot** > **Honeypot Services**.
2. On the honeypot service page, click to view alarms, navigate to **Alert Center** > **Attack Deception Events**, and view detailed information on attack deception events detected by the network honeypot.

> **Note:**
> Support operations such as blocking, allowing, and ignoring dangerous IPs that generate network honeypot alarms. See Deception Event Viewing and Handling.

View Logs

1. On the Honeypot Service Page, click **View Logs**, navigate to **Log Audit** > **Intrusion Prevention Log** > Network Honeypot.

2. On the Network Honeypot tab, you can view the log information of attack deception events detected by the network honeypot.



Defense Overview

1. On the Honeypot Service Page, support quick check of the quantities of honeypot services, probe exposures, hit honeypots, scanned probes, attack IPs and scan IPs.
2. The quota for network honeypots can be expanded according to actual conditions. Click **Purchase Quota** to perform quota purchase.

Honeypot Policy Visualization

The honeypot strategy diagram includes a policy list and a policy view, which show different paths corresponding to different probe addresses, different honeypot service types, and different bait types in the form of a table and a line chart, respectively.

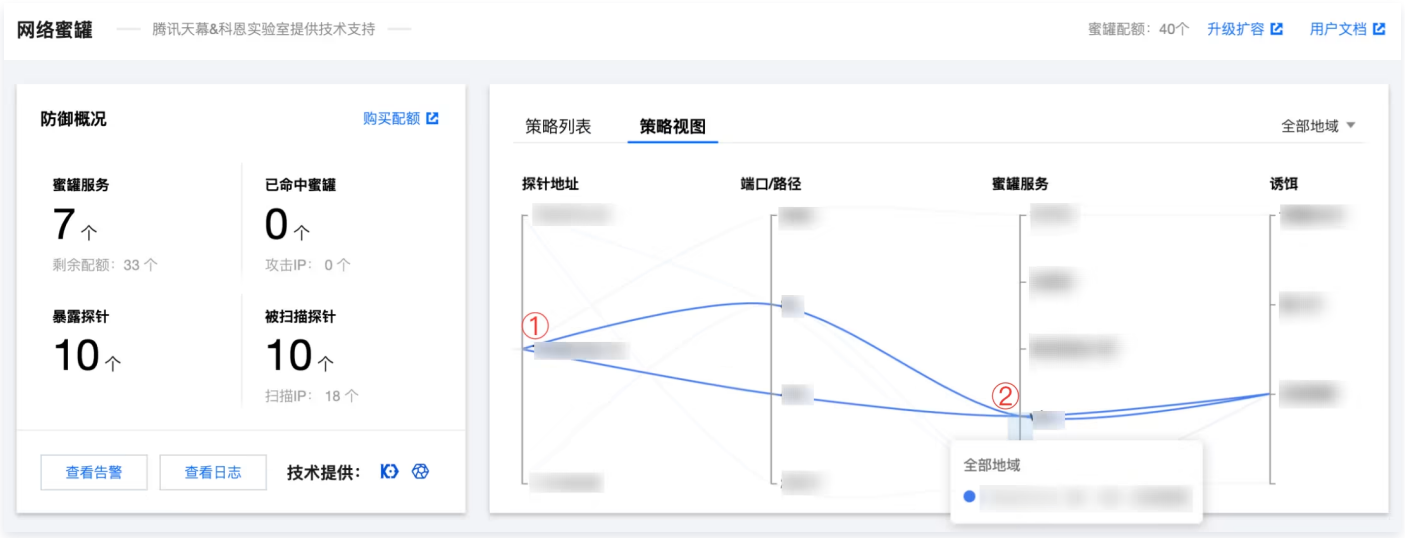
Policy List

The policy list shows the corresponding honeypot information for different probe addresses in detail in the form of a table.

Policy View

- The policy view uses a line chart to intuitively and clearly show the honeypot information corresponding to different probe addresses in different regions.

- The view supports querying specific probe addresses through honeypot filtering conditions. For example, you can click ①**Probe address** and ②**Honeypot service** to find the corresponding probe and bait of the honeypot service. If you hover over the specific strategy connection line, it can also display the region, port/path, corresponding honeypot service, and bait information of the probe deployment.



Log Audit

Last updated: 2025-05-28 10:41:54

This document guides you to view CFW-related logs.

View Access Control Log

1. Log in to the CFW console, in the left navigation bar, select **log audit** > **access control log**.
2. On the access control log page, you can view the rule hit logs generated by the cloud firewall based on the access control rules configured by users on the internet edge firewall, NAT boundary firewall, inter-VPC firewall, and enterprise security groups.
3. Meanwhile, on the internet edge firewall and NAT boundary firewall pages, the access control log will generate two rule hit lists based on inbound and outbound directions, convenient for users to distinguish and view.

4. In the right operation column of the rule hit list, click **View**.

5. On the Hit Rule Details page, you can view the details of the hits against the rule.

> **Notes:**
> - If a rule was deleted by the user after the log was generated, the status will be Deleted.
> - If a rule was edited by the user after the log was generated, the status will be Edited.
> - If a rule was not edited or deleted from the time the log was generated up to now, the status will be Added.

6. To further speed up the retrieval and filtering of access control logs, you can click the 🔍 on the right of the access source or access destination to view all rule hits between the two IP addresses.

7. Click on the right side of the page to manually download logs ⬇. Pages can be filtered by conditions. Each download is limited to 60,000 records.

Viewing Zero Trust Operations Log

1. Sign in to the CFW console, in the left sidebar, select **log audit** > **Zero Trust Operations Log**.
2. On the zero trust protection log page, you can view the zero trust operations logs under the four modules of server access, Web service access, database access, and behavior audit for users, including login and access service details.

View Intrusion Prevention Log

1. Log in to the CFW console, in the left navigation bar, select **log audit** > **intrusion prevention log**.
2. On the intrusion prevention log page, you can view all security events generated and recorded by the cloud firewall based on "observation mode" and "interception mode". There are four lists: "external intrusion", "host compromise", "lateral movement", and "network honeypot". View the details of inbound and outbound security events separately.

View Traffic Log

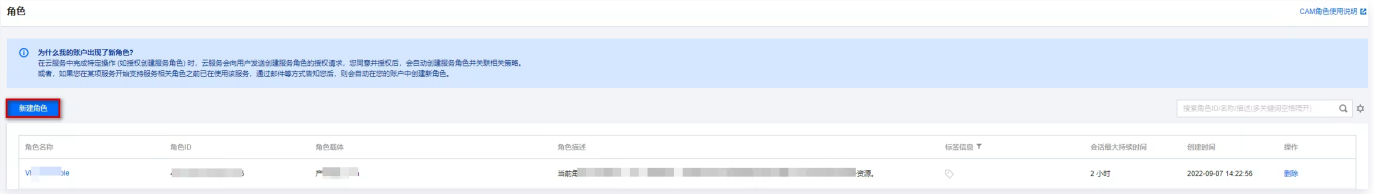
1. Log in to the CFW console, select **Log Audit** > **Traffic Log** in the left sidebar.
2. On the Traffic Log page, you can view the 10-tuple information of north-south traffic generated by Internet edge firewalls and NAT edge firewalls for outbound and inbound traffic, as well as the east-west traffic between VPCs.

3. Use the asset instance name to query and filter logs. To facilitate a comprehensive view of traffic based on the granularity and perspective of assets, click **All Assets** at the upper left corner of the Traffic Log page, filter the logs using an asset instance name in the search dropdown, and query all traffic logs for the asset.

4. To further speed up the retrieval and filtering of logs, click the 🔍 on the right of the access source or access destination to view all traffic between the two IP addresses.

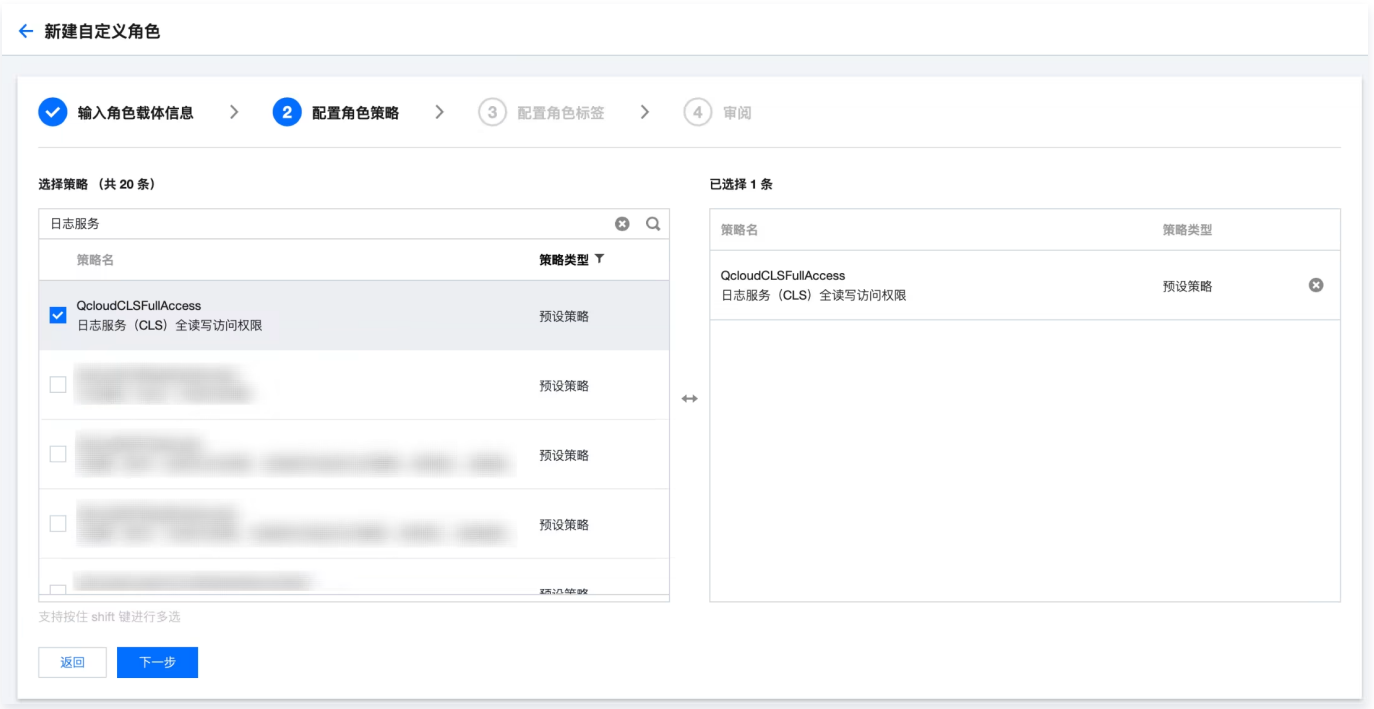
Authorizing Private Network Traffic Logs

1. Log in to the CAM console. In the left sidebar, select **role**.
2. On the role page, click **Create Role**, select Tencent Cloud account, and enter the Create Custom Role page.



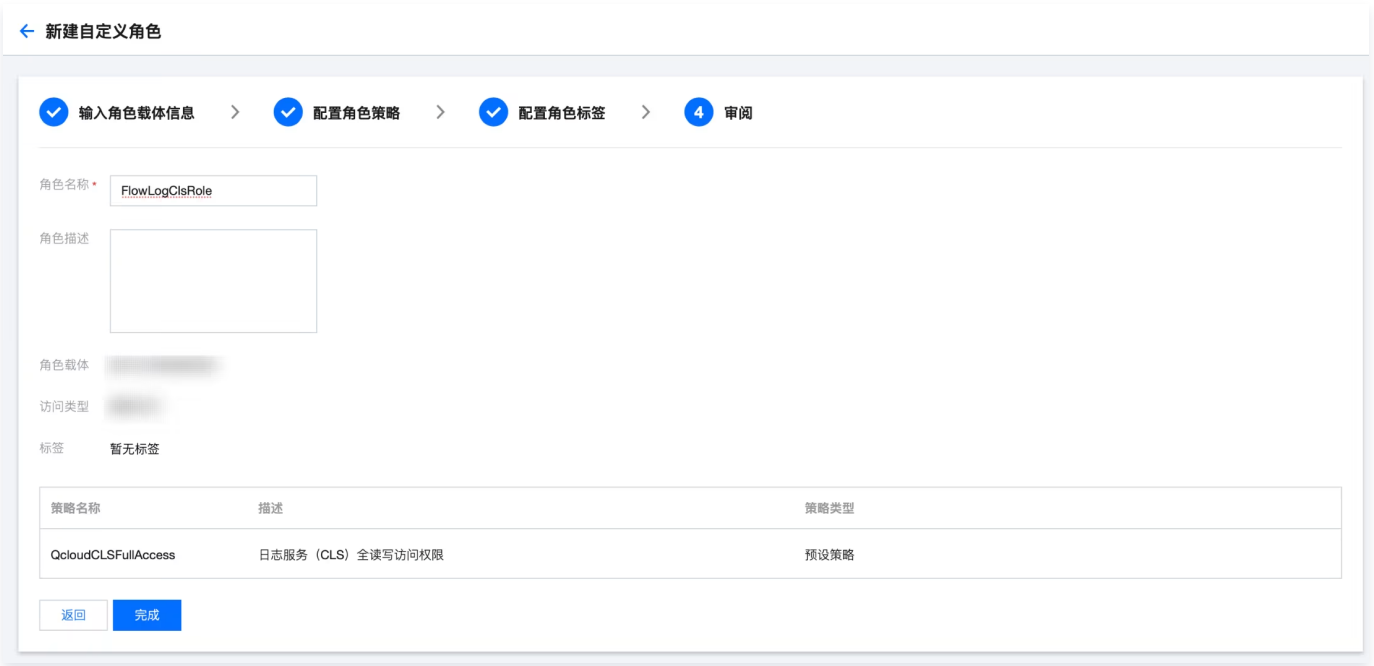
3. On the Create Custom Role page, select another root account and enter the traffic log public account 91000000202, then click **Next**.

4. Enter a search keyword "Cloud Log Service", grant full read/write permission QcloudCLSFullAccess to the Cloud Log Service, then click **Next**.



5. Configure role tags. You can set different dimensional tags for sub-users or skip this step without configuring. Click **Next**.

6. Enter the role name FlowLogClsRole, click **Done**, and complete the role creation.



View operation logs

1. Log in to the CFW console, in the left navigation bar, select **log audit** > **operation log**.
2. On the operation log page, you can view all operational activities and operation details performed by users within the account against security policies and switch pages.

Tag Name	Tag Description
Firewall Switch	Logs the status of the firewall switch and the details of user-configured instance operations.
Perform operations in the asset center	Record user operations on the Asset Center Module.
Access control operation	Log the user's operations on access control rules, including addition, edit, and deletion.
Zero trust protection operation	Record user operations on the zero trust protection module.
Intrusion prevention operation	Logs the user's detailed operations on the intrusion prevention module.
Address template operation	User documentation on row operations for address templates.
Network honeypot operation	Logs the user's operations on the honeypot service and exposed probe.
Log delivery operation	Log the user's log delivery operation details.
Login log	Log the login situation of all accounts of the user.

Related Information

If you encounter log audit-related issues, please refer to the log-related document.

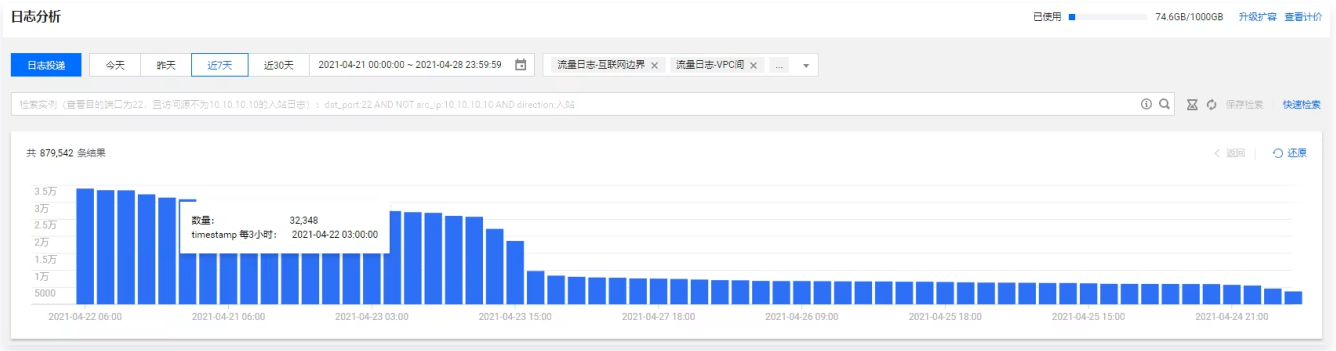
Log Analysis

Last updated: 2025-05-20 14:23:50

Log analysis allows you to view the detailed information of all logs stored by CFW based on your login account in the past 6 months. Meanwhile, log analysis supports log retrieval and querying based on search statements, and provides reports and statistical analysis services. This document guides you on how to use the log analysis feature.

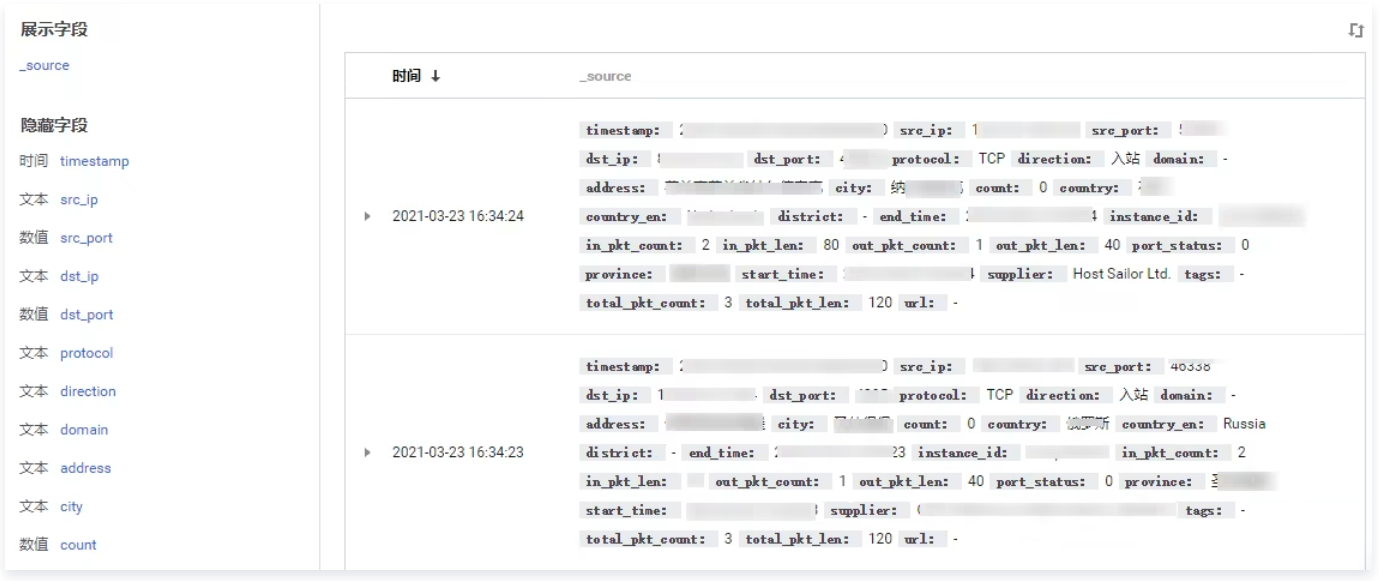
Operation Steps

1. Log in to the CFW console. In the left sidebar, click **Log Analysis** to enter the Log Analysis page.
2. To facilitate the retrieval of logs within a specified time range, you can slide the mouse pointer on the blue log quantity bar chart on the page, quickly select a time range, and click the blue log quantity bar chart to zoom in on the logs for searching.
   - Restore: Click **Restore** in the upper right corner of the bar chart, and the time selector will return to the initial time range (today).
   - Operations such as switching the options of the time selector, switching log type and re-inputting the search box to re-initiate retrieval will all make the bar chart regress to the initial time (today) of the current time selector range.



> **Note:**
> - Logs will no longer be written when the log storage capacity is full. If needed, expand the log storage capacity by clicking the scale-out button in the top right corner of the page to perform a capacity purchase.
> - Users who perform log analysis are supported with 4 chances to manually clear logs each calendar month. Operate in **Universal Setting** > **Log Storage Settings** > **Clear Count** > **Manual Clearing**.
> - Enterprise edition and above users can customize the storage duration. Operate in **Universal Setting** > **Log Storage Settings** > **Log Storage Duration** > **Edit**.

3. The log list will display the field details of each traffic log in the order from top to bottom according to the content of the "fields to display" module. When there is only the source field in the "fields to display", the order of fields displayed in the log list will be the order of the "hidden field".



   - **Display**: Move the mouse pointer over the hidden field. On the right side of the hidden field, click **Display**. The hidden field will appear in the display field. The corresponding log list on the right displays the content of that field.

- **Hide**: Move the mouse pointer over the display field. On the right side of the display field, click **Hide**. The hidden field will be removed from the display field, and the corresponding log list on the right will no longer display the content of that field.

Log Delivery

Last updated: 2025-05-28 10:43:12

Shipping to CLS

With the log delivery feature, you can automatically deliver Cloud Firewall logs to a designated CLS instance for efficient storage and analysis. Below is a detailed introduction on how to use the log delivery feature in log analytics to CLS.

> **Notes:**
> Use shipping to CLS. Activating Tencent Cloud log service is required first. Understand the usage and pricing model of the log service.

Background

- The log delivery feature can precisely send different types of cloud firewall logs to designated CLS log topics (Log Topic) based on their types, convenient for you to perform targeted management and analysis according to log categories.
- The log delivery feature supports two network access methods: public network access and Tencent Cloud VPC internal network access.
  - Deliver Cloud Firewall logs to CLS via public network, suitable for scenarios where direct access to Tencent Cloud private network is not possible.
  - Deliver logs through Tencent Cloud's internal private network, offering advantages in security and transmission performance, effectively ensuring data transmission stability and efficiency.

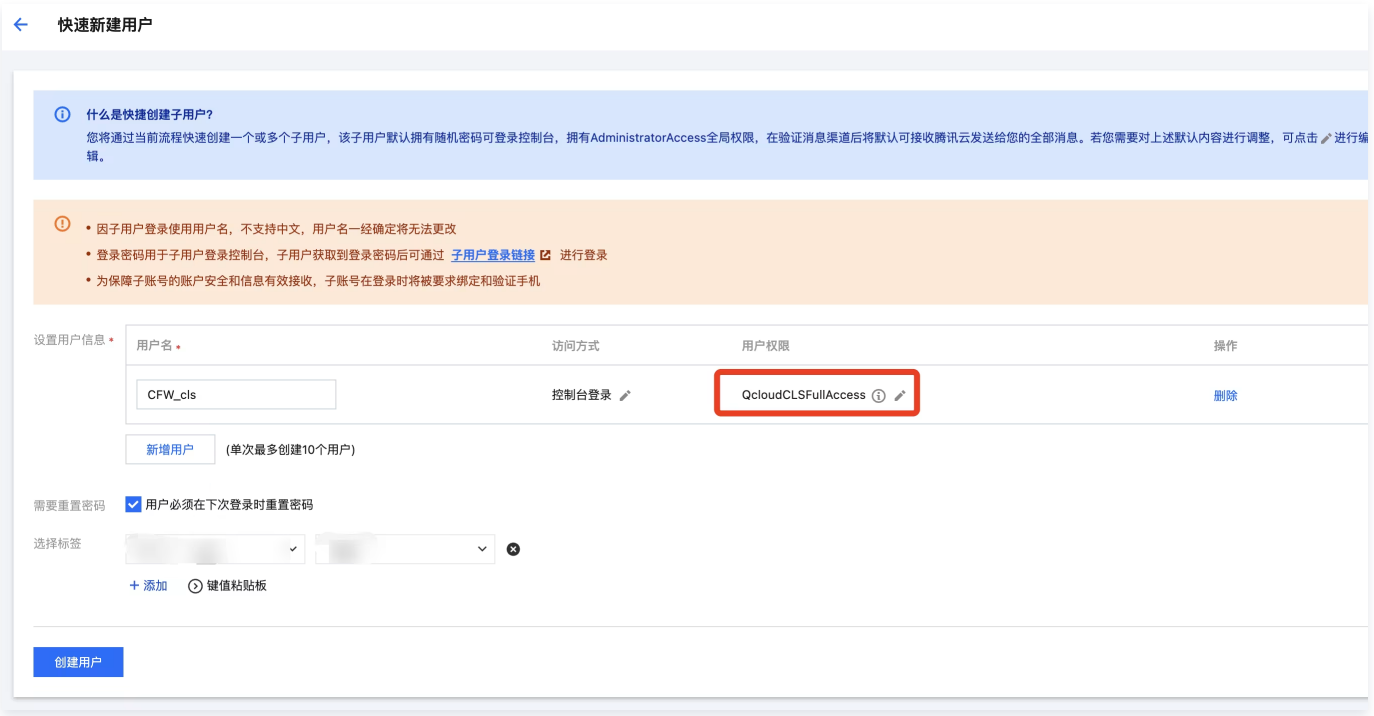
Prerequisites

Tencent Cloud CLS service and Cloud Firewall Log Analysis need to be activated.

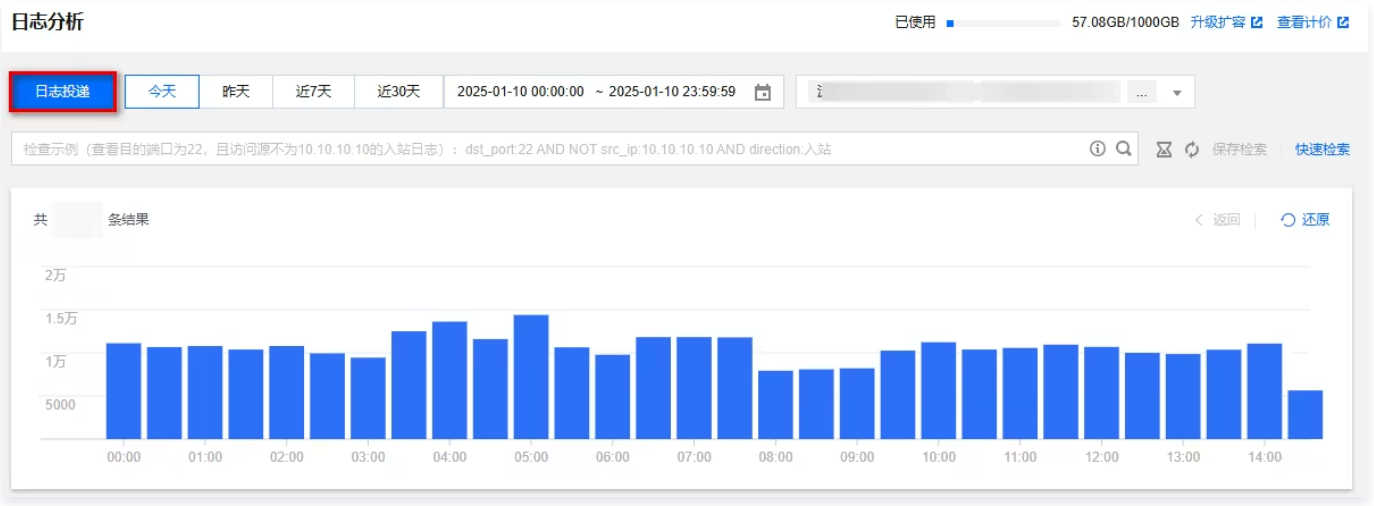
Configuration Steps

1. Recommend creating a new sub-account for log shipping. Use the root account to enter the Access Management - User List page, create an exclusive API call account for firewall log delivery tasks, and assign full read/write access `QcloudCLSFullAccess` to CLS.

   > **Notes:**
   > Use the root account or an existing sub-account to configure cloud firewall log delivery. If using a sub-account, ensure it has the `QcloudCLSFullAccess` permission. If not, you can authorize the sub-account with `QcloudCLSFullAccess` on the Access Management - User List Page.



2. Log in to the CFW console, in the left navigation bar, click **log analysis**.
3. On the log analysis page, click **Log delivery** > **Ship to CLS**.



4. On the CLS delivery page, click **Edit** to configure CLS delivery, fill in SecurityID and SecurityKey for identity authentication, click Save, and complete the CLS delivery configuration.

Notes:
Security ID can be retrieved in Access Control – API Key Management, and Security Key is obtained when creating an account.

5. On the ship to CLS page, find the **delivery switch** option, and switch the switch button from **off** status to **on** status.

After completing the above steps, the logs of Tencent Cloud Firewall will be successfully delivered to CLS. You can further manage and analyze the received log data in the CLS console to better monitor network security status and perform related OPS operations.

Shipping to Ckafka

With the log delivery feature, you can automatically deliver Cloud Firewall logs to a designated Ckafka instance. Next, we'll introduce how to use the log delivery feature in log analytics.

Background

- The log delivery feature can deliver different types of CFW logs to specified Ckafka topics respectively.
- Log delivery supports two network access methods: public domain name access and environment access support.
  - Access via public domain name is actually for log shipping through the public network.
  - Support environment access delivers logs through Tencent Cloud private network with higher performance.

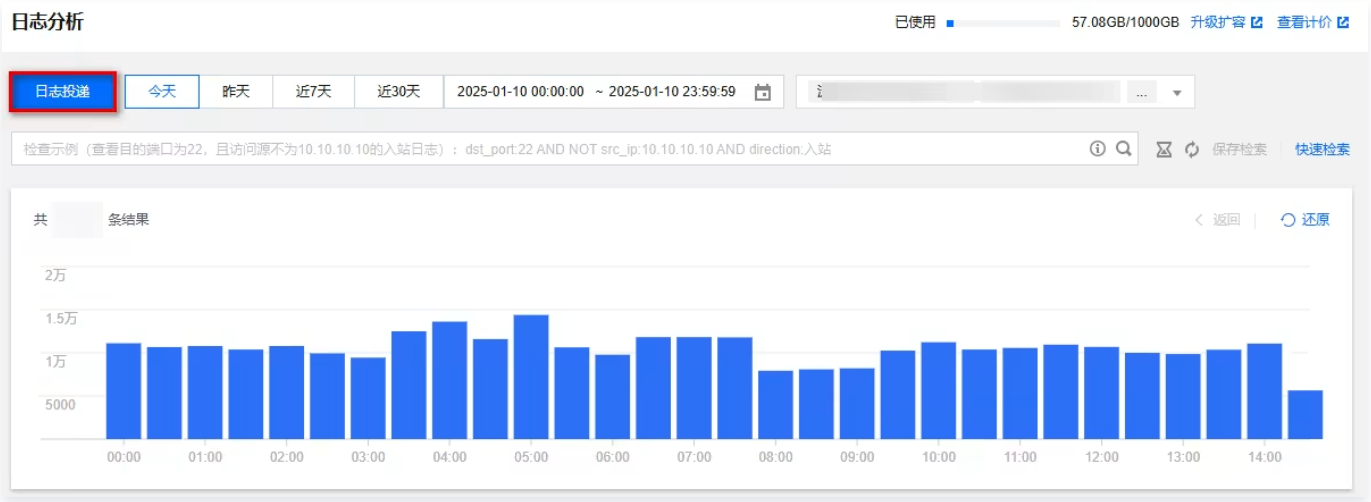
Prerequisites

- Need to have purchased a Tencent Cloud message queue Ckafka instance and cloud firewall log analytics, and configure the bandwidth specification of the Ckafka instance according to the cloud firewall bandwidth.
- According to the message queue Ckafka documentation guide, contact Tencent Cloud customer service to enable "public domain name access" or "support environment access" allowlist.

- Only supports using one message queue Ckafka account for log shipping.

Configuration Steps

1. log in to CFW console, in the left navigation bar, click **Log Analysis**.
2. On the upper left corner of the log analysis page, click **Log Delivery**, and by default enter the page for shipping to Kafka.



3. On the page for shipping to Kafka, perform the initial configuration.

3.1 Select the network access method: public domain name access or supported environment access.

- **Method 1**: Select public domain name access, choose a message queue instance and a public domain name, and enter the username and password of the selected message queue instance.

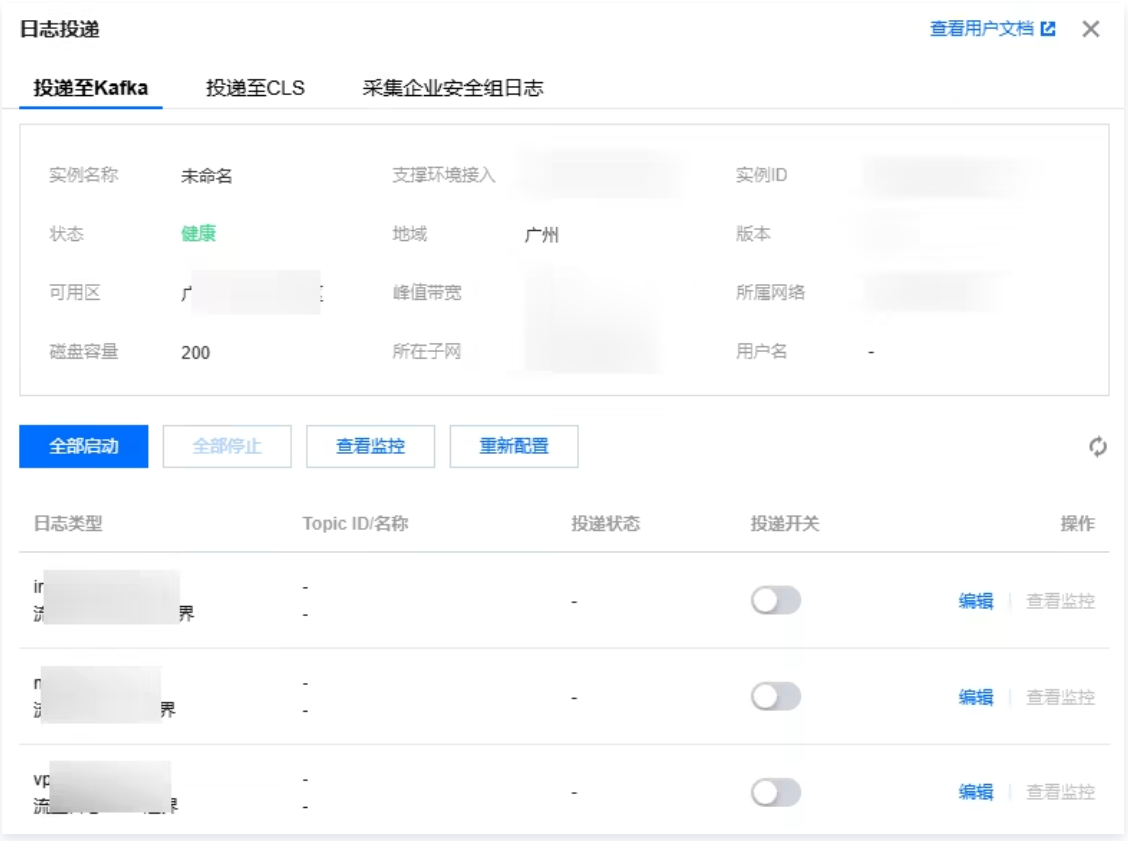
- **Method 2**: Select environment access support, which refers to the products you have purchased in Tencent Cloud that can be used in conjunction with Ckafka, and then choose a Message Queue Instance and IP ports.

3.2 After selecting the network access method, you can bind a Ckafka topic on the log delivery page.

> **Notes:**
> The log delivery feature supports delivery of various CFW log types. Different types of logs need to be delivered to different Ckafka topics. Each Ckafka topic can only be bound to one CFW log type.

3.3 After the configuration is complete, click **OK**, and you will be prompted that the log delivery configuration is successful, indicating that the log delivery has been successfully configured.

4. After initial configuration is complete, you can view the log delivery details.



- **Basic information**: Shows the basic information of a Ckafka instance.

> **Notes:**
> You need to pay attention to the "health status" field. When prompted with "unhealthy", click **view monitoring** to check whether the Ckafka service is abnormal or if the quota is insufficient.

- **Log delivery switch**: Used to control specified log types, start or stop log delivery tasks.
  - Method 1: You can individually control log delivery tasks by using the "Switch" button in the "Delivery Switch" column on the right side of each log type.
  - Method 2: Use batch operations. Currently supports **start all** and **stop all** two operations.
- **Rebind Ckafka topic**: In the operation column on the right side of the log type, click **Edit** for individual configuration. You can reselect a Ckafka topic from the specified Ckafka instance that is not bound by other firewall log types.

> **Notes:**
> Each Ckafka topic can only be bound to one CFW log type.

- **View monitoring**: In the operation column on the right side of the log type, click **View monitoring** to navigate to the monitoring page of the Message Queue Ckafka console. You can view network traffic, peak bandwidth, message count, disk usage, and

other conditions.

- **Reconfigure**: At the top of the log type list, click **Reconfigure** to allow you to reselect the message queue instance for delivery, network access method, and username/password.

> **Notes:**
> Reconfigure, which will interrupt the current shipping process.

Log Field
Log Subfield

Last updated: 2025-05-20 14:24:35

Log Type ID	Log Type Name
CFWRuleAcl	Access control log – Internet boundary
CFWRuleVpcAcl	Access control log – NAT, VPC firewall
HoneyPotHost	Intrusion prevention log – Network honeypot – Host log
HoneyPotNetwork	Intrusion prevention log – Network honeypot – Network log
BlockList	Intrusion prevention log – Interception list log
IdsLog	Intrusion prevention log – Virtual patch, Basic defense log
TiLog	Intrusion prevention log – Threat intelligence log
BaseLineLog	Intrusion prevention log – Security baseline log
CFWOnline	Traffic log – Internet boundary
CFWNetflowVpc	Traffic log – VPC
CFWNetflowNat	Traffic log – NAT
CFWNetflowFI	Traffic log – Private network traffic
CFWOperateLogAll	Operation Log
CFWOperateRemoteOM	Zero trust protection log – Remote operation and maintenance login
CFWOperateWebAccess	Zero trust protection log – Web service access

Access Control Types

Last updated: 2025-05-28 10:43:57

Field Identifier	Field Type	Field Name	Field Description	Reference Value	Subcategory	Remarks
src_ip	string	Source IP	-	192.168.0.1	CFWRuleAcl,CFWRuleVpcAcl	-
dst_ip	string	Destination IP	-	192.168.0.1	CFWRuleAcl,CFWRuleVpcAcl	-
src_port	uint16	Source Port	-	22	CFWRuleAcl,CFWRuleVpcAcl	-
dst_port	uint16	Destination Port	-	22	CFWRuleAcl,CFWRuleVpcAcl	-
protocol	string	Protocol	-	tcp	CFWRuleAcl,CFWRuleVpcAcl	-
info	string	URL information	Hit log URL for HTTP	domain/test php	CFWRuleAcl	-
direction	int8	Direction	Set rules for traffic direction	Outbound	CFWRuleAcl,CFWRuleVpcAcl	-
detail	string	Alarm rule description (attach rule description)	View the alarm details.	-	CFWRuleAcl,CFWRuleVpcAcl	-
rule_info	string	Rule alarm details (used for association rules)	-	-	CFWRuleAcl	-
strategy	string	Policies	Action policy for rule execution		CFWRuleAcl,CFWRuleVpcAcl	-
time	int64	Event	The time when a rule is hit	-	CFWRuleAcl,CFWRuleVpcAcl	-
appid	string	appid	Account appid	-	CFWRuleAcl	-
instance_id	string	victim-related asset ID	victim-related asset ID	-	CFWRuleAcl,CFWRuleVpcAcl	-
uuid	string	unique original alarm log ID	unique original alarm log ID	-	CFWRuleAcl	-
uid	int64	unique rule ID	Unique ID of the rule (internal use)	-	CFWRuleAcl	-

insert_time	int64	Log Insertion Time	Time when this log is recorded	–	CFWRuleAcl,CFWRuleVpcAcl	–
mode	uint8	Firewall property	0: Bypass 1: Serial	–	CFWRuleAcl	–
type	uint8	Protocol TYPE	Protocol TYPE: 1:TCP 3:HTTP	–	CFWRuleAcl	–
fw_type	string	Firewall type	Rule Ownership firewall type	NAT Boundary Firewall	CFWRuleAcl,CFWRuleVpcAcl	–
timestamp	string	Timestamp	Current Time	–	CFWRuleAcl,CFWRuleVpcAcl	–
fws_id	string	Engine instance ID		cfwnat-fd7f678e	CFWRuleVpcAcl	–
nat_ins_name	string	Instance name of NAT	–	–	CFWRuleVpcAcl	–
log_type	uint8	Internal Use Log Type	Current log type fixed value: 5	–	CFWRuleVpcAcl	–
dst_vpc	string	victim asset VPCID	–	–	CFWRuleVpcAcl	When the current log field is empty, the current field is hidden by default.
fws_name	string	Instance engine name	–	–	CFWRuleVpcAcl	–
src_vpc	string	Attacker asset VPC ID	–	–	CFWRuleVpcAcl	When the current log field is empty, the current field is hidden by default.
region	string	Region	–	–	CFWRuleVpcAcl	–
dst_domain	string	External domain name	External domain information	–	CFWRuleVpcAcl	–
l7proto	string	layer 7 protocol name	–	DNS,SMTP,HTTP	CFWRuleVpcAcl	–
src_vpc_name	string	access source VPC name	–	–	CFWRuleVpcAcl	When the current log field is empty, the current field is hidden by default.
dst_vpc_name	string	access destination VPC name	–	–	CFWRuleVpcAcl	When the current log field is empty, the current field is hidden by default.
ew_ins_id	string	VPC wall instance ID	–	–	CFWRuleVpcAcl	–

ew_ins_name	string	VPC wall instance name	–	–	CFWRuleVpcAcl	–
src_ins_id	string	Access the source asset ID	–	–	CFWRuleVpcAcl	When the current log field is empty, the current field is hidden by default.
dst_ins_id	string	Access the target asset ID	–	–	CFWRuleVpcAcl	When the current log field is empty, the current field is hidden by default.
src_ins_name	string	Access the source instance name.	–	–	CFWRuleVpcAcl	When the current log field is empty, the current field is hidden by default.
dst_ins_name	string	Access the destination instance name	–	–	CFWRuleVpcAcl	When the current log field is empty, the current field is hidden by default.

Zero Trust Protection Log

Last updated: 2025-05-20 14:30:31

Field Identifier	Field Type	Field Name	Field Description	Subcategory
service	string	Service type for Ops	SSH/RDP, etc.	CFWOperateRemoteOM,CFWOperateWebAccess
src_ip	string	Source IP	-	CFWOperateRemoteOM,CFWOperateWebAccess
src_port	uint16	Source Port	-	CFWOperateRemoteOM,CFWOperateWebAccess
dst_ip	string	Destination IP	-	CFWOperateRemoteOM,CFWOperateWebAccess
dst_port	uint16	Destination Port	-	CFWOperateRemoteOM,CFWOperateWebAccess
appid	string	appid	-	CFWOperateRemoteOM
user	string	Ops user name	When ywid exists, use the corresponding name, otherwise empty	CFWOperateRemoteOM
corp_id	string	Enterprise WeChat for Business ID	Enterprise ID when an enterprise user logs in	CFWOperateRemoteOM
msg	string	Login status	Successful login, etc.	CFWOperateRemoteOM
session	string	Session ID	Session ID	CFWOperateRemoteOM
ywid	int64	Ops user ID	Ops table Ops ID	CFWOperateRemoteOM
filename	string	Playback File Name	Playback File Name	CFWOperateRemoteOM
login_type	int64	Login Status Codes	Login Status Codes, corresponding to msg, represent the login status.	CFWOperateRemoteOM
start_time	int64	Start time of the session	-	CFWOperateRemoteOM,CFWOperateWebAccess
end_time	int64	End time of the session	-	CFWOperateRemoteOM,CFWOperateWebAccess
login_failed_type	int64	Reason for login failure	-	CFWOperateRemoteOM
address_en	string	Default access address	-	CFWOperateRemoteOM
req_uri	string	URL for session access	-	CFWOperateWebAccess
pay_load	string	Session request payload	-	CFWOperateWebAccess
access_type	int64	Login status	-	CFWOperateWebAccess
access_time	string	Log-in time	-	CFWOperateWebAccess

request_time	string	Request duration of the session	–	CFWOperateWebAccess
user_id	string	User ID of the logged-in user	Ops ID	CFWOperateWebAccess
user_corp_id	string	Logged-in Enterprise WeChat for Business ID	Enterprise ID when an enterprise user logs in	CFWOperateWebAccess
user_type	string	User Type	Enterprise WeChat user, Ordinary user	CFWOperateWebAccess
wx_name	string	WeChat name	WeChat Name	CFWOperateWebAccess
openid	string	WeChat openid	–	CFWOperateWebAccess
src_region	string	source region	–	CFWOperateWebAccess
dst_instance_id	string	Instance ID of the accessed instance	–	CFWOperateWebAccess
http_cookie	string	Request cookie Information	session cookie	CFWOperateWebAccess

Intrusion Prevention Log

Last updated: 2025-05-20 14:31:02

Field Identifier	Field Type	Field Name	Field Description	Reference Value	Subcategory
instance_id	string	Victim-related asset ID	-	-	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
time	int64	Alarm occurrence time	-	-	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
src_ip	string	Source IP	-	192.168.0.1	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
dst_ip	string	Destination IP	-	192.168.0.1	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
src_port	int64/int	Source Port	-	-	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
dst_port	int64/int	Destination Port	-	-	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
direction	int64	Direction	• Outbound • 1: Inbound • TCP protocol alarm: for session direction • Non-session protocol: for traffic direction	-	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
protocol	string	Protocol	-	TCP	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
strategy	string	alarm action	Handling actions of an alarm • Observe • Block • 2: Allow • 3: Deception	0	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
strategy_res	string	Alarm action identifier ID	-	strage_alert	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog
event_name	string	Attack event type	-	Exploitation of Log4j2 Vulnerability	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
eventname_res(event_name_res)	string	Attack event type identification ID	-	log4j2_exploit	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog

dst_domain	string	External domain name	–	–	HoneyPotHost,HoneyPotNetwork,BlockList,TiLog,BaseLineLog
level	string	Alarm Severity	Severity of the Alarm	Critical	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
level_res	string	Alert level identification ID	–	level_serious	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog
level_int	int	Alarm level number	–	5	HoneyPotHost,HoneyPotNetwork
address	string	The city where the attack IP is located	–	Tokyo, Tokyo, Japan	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
address_en	string	The city where the attack IP is located	–	Tokyo,Japan	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog
insert_time	int64	Alarm storage time	–	2023/1/1 0:00:00	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
service_id	string	Network honeypot ID	–	–	HoneyPotHost,HoneyPotNetwork
type	string	alert subtype identifier	–	ti	HoneyPotHost,HoneyPotNetwork,TiLog,BaseLineLog
sub_source_type	string	Alert Subtype	alarm category, including: virtual patch, basic defense, blocklist, network honeypot	Virtual Patch	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
sub_source_type_res	string	alert subtype identifier ID	alert subtype identifier ID, source_virtualpatch, source_basicrule	source_virtualpatch	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog
payload	string	attack payload	Payload information of attack traffic	–	HoneyPotHost,HoneyPotNetwork,IdsLog,TiLog
cmdline	string	Execute command	Network honeypot host event, sensitive command executed in the honeypot	bash –c ifconfig execve /bin/bash|m=100755|o=0:0	HoneyPotHost
template_id	string	Network honeypot template ID	–	–	HoneyPotHost
docker_id	string	Network honeypot Unique ID	–	–	HoneyPotHost,HoneyPotNetwork
proc_chan	string	Process Tree	Network honeypot host event process	bashP{	HoneyPotHost

			tree		
kill_chain	string	Attack chain	Attack chain, attack stage where the warning event occurs	Exploitation	HoneyPotHost,HoneyPotNetwork
kill_chain_res	string	Attack chain identification ID	–	kill_chain_exploit	HoneyPotHost,HoneyPotNetwork
event_id	string	Alarm ID	–	–	HoneyPotHost,HoneyPotNetwork
exe	string	Execute file path	–	/sbin/ifconfig	HoneyPotHost
probe_id	string	Probe ID	–	probe-id	HoneyPotHost,HoneyPotNetwork
service_type	string	Network honeypot type	Network honeypot type	SSH honeypot	HoneyPotHost,HoneyPotNetwork
service_type_res	string	Network honeypot type identifier ID	–	ssh_honeypot	HoneyPotHost,HoneyPotNetwork
script_name	string	Network honeypot script name	–	–	HoneyPotHost,HoneyPotNetwork
log_source	string	Data source	Alarms of the inter-VPC firewall and alarm values of the intranet honeypot are move. Honeypot host alarm value is host. Honeypot public network alarm value is network.	move	HoneyPotHost,HoneyPotNetwork,IdsLog
login_user	string	Attack login user	–	[root, 1qaz!QAZ]	HoneyPotHost,HoneyPotNetwork
visible_tag	int	Visibility	–	–	HoneyPotHost,HoneyPotNetwork
timestamp	string	Alarm timestamp	–	2023-01-01T00:00:00+08:00	HoneyPotHost,HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
ti_type	string	Correlated intelligence threat type tags (built-in in alarming)	–	SSH honeypot attack Conventional Network Brute Force brute force cracking	HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
ti_type_en	string	Correlated intelligence threat type tag (built-in in alarming)	–	["SSH honeypot attack","General network cracking","Brute force"]	HoneyPotNetwork,BlockList,IdsLog,TiLog

ti_white	string	Allowlist tag (built-in in Alarming)	-	Intelligence allowlist	HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
ti_white_res	string	Allowlist tag (built-in in Alarming) identifier ID	-	intelligence_allowlist	HoneyPotNetwork,BlockList,IdsLog,TiLog,BaseLineLog
src_country	string	Source country	Country where the source IP is located	United States	BlockList,IdsLog,TiLog,BaseLineLog
src_country_en	string	Source country - English	Country where the source IP is located - English	United States of America	BlockList,IdsLog,TiLog
dst_country	string	Destination country	Country where the destination IP is located	United States	BlockList,IdsLog,TiLog,BaseLineLog
dst_country_en	string	Destination country - English	Country where the destination IP is located	United States of America	BlockList,IdsLog,TiLog
attack_vector	string	Attack exploitation methods	-	code-exec	IdsLog
attack_count	int	Alarm quantity	-	-	IdsLog
nat_ip	string	NAT IP	Public network IP address of NAT	8.8.8.8	IdsLog,TiLog,BaseLineLog
nat_port	int	The port of NAT	Public network port of NAT	-	IdsLog,TiLog,BaseLineLog
fws_id	string	Firewall ID	-	-	IdsLog
fw_type	string	Firewall type	Firewall type, including: • vpc: Inter-vpc firewall • nat: NAT firewall • sg: enterprise security group • Internet boundary	nat	IdsLog
src_vpc	string	Attacker asset VPCID	-	-	IdsLog
dst_vpc	string	Victim asset VPCID	-	-	IdsLog
src_ins_id	string	Attacker-related asset ID	-	-	IdsLog
dst_ins_id	string	Victim-related asset ID	-	-	IdsLog
nat_ins_id	string	NAT Instance ID	-	-	TiLog,BaseLineLog

nat_ins_name	string	NAT Instance Name	-	-	TiLog

Traffic Log

Last updated: 2025-05-20 14:32:26

Field Identifier	Field Type	Field Name	Field Description	Reference Value	Subcategory	Notes
appid	string	appid	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
instance_id	string	Asset Instance ID	-	-	CFWOnline,CFWNetflowNat	-
src_ip	string	Source IP	-	192.168.0.1	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
dst_ip	string	Destination IP	-	192.168.0.1	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
src_port	uint16	Source Port	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
dst_port	uint16	Destination Port	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
protocol	string	Protocol	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
direction	int8	Direction	Traffic Direction	Outbound	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	sd-wan
dst_domain	string	Access destination domain name	-	-	CFWOnline,CFWNetflowNat	-
in_pkt_count	uint64	Number of inbound packets	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
in_pkt_len	uint64	Inbound package size	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
out_pkt_count	uint64	Number of outbound packets	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
out_pkt_len	uint64	Outbound package size	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
total_pkt_count	uint64	Total packet count	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
total_pkt_len	uint64	Total package size	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
ti_tag	string	Association intelligence tag	-	-	CFWOnline,CFWNetflowNat	-

		(built-in in alarming)				
start_time	int64	Session start time	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
end_time	int64	Session end time	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	-
supplier	string	Carrier	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
supplier_en	string	Carrier (when referring to an enterprise operator)	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
src_country	string	Source country	Country where the source IP is located	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
src_country_en	string	Source country - English	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
dst_country	string	Destination country	Country where the destination IP is located	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
dst_country_en	string	Destination country - English	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
src_province	string	Source province	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
src_province_en	string	Source province - English	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
dst_province	string	Destination province	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
dst_province_en	string	Destination province - English	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
src_city	string	Source city	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
dst_city	string	Destination city	-	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
district	string	Region	-	-	CFWOnline,CFWNetflowNat	-
address	string	Detailed address	• Inbound source detailed address • Outbound target detailed address	-	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan

address_en	string	Detailed address in English	• Inbound source detailed address – English • Outbound target detailed address – English	–	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
src_lat	float32	Source dimension	–	–	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
dst_lat	float32	Target dimension	–	–	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
src_lon	float32	source longitude	–	–	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
dst_lon	float32	destination longitude	–	–	CFWOnline,CFWNetflowVpc,CFWNetflowNat	sd-wan
insert_time	int64	log storage time	–	–	CFWOnline,CFWNetflowNat	–
count	uint64	alarm quantity	–	–	CFWOnline	–
url	string	Layer-7 URL	–	–	CFWOnline	–
domain_flag	uint8	Existence of domain name	• Existence • Not found	–	CFWOnline	–
port_status	uint8	Port status	• Turn on • 0: Disable	–	CFWOnline	–
bot_flag	uint8	reserved field	–	–	CFWOnline	–
mode	uint8	Firewall properties	• 1: Serial • Bypass	–	CFWOnline	–
argus_ip	uint32	reserved field	–	–	CFWOnline	–
tcp_flag	uint8	TCP tag	• 1:OUTSyn • 2:OUTRst • 3:OutSynAck • 4:OUTFin • 5:INSyn • 6:INRst • 7:INSynAck • 8:InFin	–	CFWOnline	–
timestamp	string	Unified Timestamp	–	–	CFWOnline,CFWNetflowVpc,CFWNetflowNat,CFWNetflowFl	sd-wan
cvm_id	string	reserved field	–	–	CFWNetflowVpc	–

ew_ins_id	string	VPC firewall instance ID	–	–	CFWNetflowVpc	–
fws_id	string	VPC Firewall Edge ID	–	–	CFWNetflowVpc,CFWNetflowNat	–
fws_name	string	VPC Firewall Name	–	–	CFWNetflowVpc	–
log_type	uint8	Log Type (Internal Use)	Current Log Type Fixed Value: 2	–	CFWNetflowVpc	–
if_pair_key	string	reserved field	–	–	CFWNetflowVpc	–
uuid	int64	unique original alarm log ID	–	–	CFWNetflowVpc	–
flow_id	int64	internal field	–	–	CFWNetflowVpc	–
src_vpc	string	attacker asset VPCID	–	–	CFWNetflowVpc	–
dst_vpc	string	victim asset VPCID	–	–	CFWNetflowVpc	–
dst_vpc_name	string	target VPC name	–	–	CFWNetflowVpc	–
src_vpc_name	string	source VPC name	–	–	CFWNetflowVpc	–
retans	int8	Whether there is retransmission	• 1: Retransmission • 0: No retransmission	–	CFWNetflowVpc,CFWNetflowNat	–
timeout	int64	Session duration	–	–	CFWNetflowVpc,CFWNetflowNat	–
src_ins_id	string	Attacker-related asset ID	–	–	CFWNetflowVpc,CFWNetflowFl	–
dst_ins_id	string	Victim-related asset ID	–	–	CFWNetflowVpc,CFWNetflowFl	–
src_ins_name	string	Source asset name	–	–	CFWNetflowVpc	–
dst_ins_name	string	Destination asset	–	–	CFWNetflowVpc	–

		name				
is_out	int8	SDWAN firewall access to public network marking	• 1: Access the public network • 0: Normal access	–	CFWNetflowVpc	sd-wan
ti_tag_en	string	Attacker IP intelligence tag – English	–	–	CFWNetflowNat	–
fw_type	string	Alert Subtype	–	–	CFWNetflowNat	–
fw_region	string	Firewall located area	–	–	CFWNetflowNat	–
nat_ip	string	NAT IP	NAT IP address	–	CFWNetflowNat	–
nat_port	uint16	NAT port	–	–	CFWNetflowNat	–
if_id	string	Network Interface Card ID	–	–	CFWNetflowFl	–
action	string	alarm action	Alarm handling actions	Interception; Allow	CFWNetflowFl	–

Operation Log

Last updated: 2025-05-20 14:32:46

Field Identifier	Field Type	Field Name	Subcategory	Notes
level	string	Danger Level	CFWOperateLogAll	The current log field is empty. The current field is hidden by default.
operator	string	Operator	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
result	string	Operation Result	CFWOperateLogAll	The current log field is empty. The current field is hidden by default.
fw_type	string	Firewall type	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
action	string	Firewall switch – operation behavior Asset Center operation – operation behavior Access Control operation – operation behavior Zero trust protection operation – operation behavior Intrusion Prevention operation – operation category Address template operation – operation behavior Network honeypot operation – operation behavior Universal setting operation – operation behavior	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
opt_type	string	Major Category of Operation Logs	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
detail	string	Firewall switch – operation details Asset Center operation – operation details Access Control operation – operation details Zero trust protection operation – operation details Intrusion Prevention operation – operation behavior Address template operation – template description Network honeypot operation – operation details	CFWOperateLogAll,CFWOperateWebAccess	When the current log field is null, the current field is hidden by default.

		General Setting Operation – Operation Detail		
time	string	Occurred At	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
app_id	string	Tenant Unique ID	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
info	string	Access Control operation – rule description Intrusion prevention operation – Operation details Address template operation – operation detail	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
longitude	float32	source longitude	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
address	string	source city	CFWOperateLogAll,CFWOperateRemoteOM	When the current log field is null, the current field is hidden by default.
district	string	source city district	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
more_info	string	Supplementary information	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
rule	string	Rule list	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
instance_region	string	Asset instance region	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
public_ip	string	Honeypot public IP	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
remote_type	string	Operation Type General Setting Operation – Log Type	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
services	string	Honeypot detailed information	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
template_id	string	Honeypot template ID	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
region	string	Asset region	CFWOperateLogAll,CFWOperateWebAccess	When the current log field is null, the current field is hidden by default.
instance_id	string	Related asset ID	CFWOperateLogAll,CFWOperateRemoteOM	The current log field is empty. The current field is hidden by default.

asset_type	string	Asset classification	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
addr_name	string	Template Name	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
base_type	string	Baseline type	CFWOperateLogAll	When the current log field is null, the current field is hidden by default.
timestamp	string	Alarm Timestamp	CFWOperateLogAll,CFWOperateRemoteOM,CFWOperateWebAccess	When the current log field is null, the current field is hidden by default.
level_res	string	Danger Level Identifier ID	CFWOperateLogAll	When the current log field is null, the current field is hidden by default; the current field is only shown on the international site.
action_res	string	Operation Behavior Identifier ID	CFWOperateLogAll	When the current log field is null, the current field is hidden by default; the current field is only shown on the international site.
detail_res	string	Operation detail identifier ID	CFWOperateLogAll	When the current log field is null, the current field is hidden by default; the current field is only shown on the international site.
rulelist	string	Rule list	CFWOperateLogAll	When the current log field is null, the current field is hidden by default; the current field is only shown on the international site.
appid	string	appid	CFWOperateLogAll,CFWOperateWebAccess	When the current log field is null, the current field is hidden by default; the current field is only shown on the international site.
instance_region_res	string	Asset Instance Region Identifier ID	CFWOperateLogAll	When the current log field is null, the current field is hidden by default; the current field is only shown on the international site.
rule_res	string	Rule List Identifier ID	CFWOperateLogAll	When the current log field is null, the current field is hidden by default; the current field is only shown on the international site.
natinsid	string	Instance ID of NAT instance	CFWOperateLogAll	When the current log field is null, the current field is hidden by default; the current field is only shown on the international site.

remote_type_res	string	Operation Type Identifier ID	CFWOperateLogAll	When the current log field is null, the current field is hidden by default; the current field is only shown on the international site.
detail_id	string	Operation details Asset ID	CFWOperateLogAll	When the current log field is null, the current field is hidden by default; the current field is only shown on the international site.
base_type_res	string	Security baseline type	CFWOperateLogAll	When the current log field is null, the current field is hidden by default; the current field is only shown on the international site.

Notifications and Settings-Related

Last updated: 2025-05-20 14:33:04

Subscription Message Center

CFW defaults to non-subscription push method. The notified account refers to the account configuration in notification settings. CFW will automatically identify accounts that have logged in to the CFW console and add them to the optional list.

1. 1. Log in to the CFW console. In the left sidebar, click **notification settings**.
2. On the Notification Settings Page, configure push notifications for the firewall. If you need to adjust to subscription-based push or enable the configuration of the message center, click **Message Center Subscription Settings** and toggle the **switch**.

Note:

After the message center is enabled, the alarm objects of **all alarm types in the notification settings will become invalid**. For details, see the settings of Message Center.

Configuring Notification Settings

On the Notification Settings Page, you can configure some common firewall alarms and notifications.

Notification Type	Notification Content	Supported Configuration Items
Security alarm notification	CFW supports sending SMS, Message Center notifications, and WeChat notifications for security event alerts in the alert center. On the console, you can configure the configuration object and alarm source.	• Supports configuration of WeChat Service Account Alerts for Tencent Cloud security. • Support triggering notifications based on alarm type
Bandwidth Alarm Notification	We offer you a three-tier bandwidth alert. When the firewall bandwidth reaches the threshold percentage you set, it will trigger alarm notifications via SMS, Message Center, and WeChat to the selected account.	Supports distinguishing different cascaded alarms based on firewall type
Storage Alarm Notification	We offer you a two-tier storage alarm. When the firewall storage reaches the threshold percentage you set, it will trigger alarm notifications via SMS, Message Center, and WeChat to the selected account.	Configurable cascaded alerts
Disaster recovery alarm notification	When your NAT boundary firewall or VPC firewall triggers BYPASS, alarm notifications via SMS, Message	-

	Center, and email will be sent to the selected account.	
Newly-added exposure surface alert notification	When newly-selected exposure surface types are detected in your account, alarm notifications via SMS, Message Center, and email will be triggered for the selected account.	Support triggering notifications by exposure surface type.
Enterprise security group change notification	When changes are detected in the enterprise security group of your account, we will push relevant notifications to you regardless of whether automatic distribution is enabled.	-
Automation task exception notification	If exceptions in your automation task are detected, we will push relevant notifications to you.	-
System Log Push Notifications	When you generate new system logs, we will notify you as per your settings.	Support triggering notifications by system log event type.

Universal Setting

On the General Settings page, universal settings integrate some commonly used configurations.

Setting Item Name	Setting Item Description	Must-Knows
Cloud IP Blocking Setting	When CFW blocks an IP, it can automatically deliver corresponding enterprise security group rules to the DMZ zone based on malicious IP type. Do not manually modify the corresponding parameter template and enterprise security group rules.	The Internet Bypass Firewall is unable to block cloud internal IPs. Serial and NAT firewalls support this feature. It is recommended to prioritize their use.
Log storage settings	Enterprise edition and above users can modify the log storage type and storage duration, and can only modify it once every 2 months. We will automatically delete your expired logs for you. You can also manually clear the logs, but note that each user only has 4 chances per calendar month.	Existing logs will not be affected after log settings are modified. Only new logs created after the edit will be affected. For example, if you change the log storage duration from 180 days to 90 days, existing logs will still be stored for 180 days, while new logs will be stored for 90 days.
Access Control Rule Settings	In the access control rule list, set the enable status of the rule each time you add, insert, or import a control rule.	-
Automatic Reconstruction Settings of Honeypot	In a network honeypot, if a honeypot breach occurs, you can choose whether to automatically reconstruct the honeypot and set the interval time.	-
Tag Settings	CFW has no resource attributes. Adding tags is only supported for billing resources of the account. You can modify the tag value here.	-

Common Tools
Address Template

Last updated: 2025-05-20 14:33:29

Address templates provide users with a more convenient and faster way to batch manage commonly used addresses. Users can create IP templates, domain name templates, or protocol port templates in address templates; these templates can be applied to access control rules to facilitate management and operations. This document introduces how to batch manage addresses in address templates, while users can match established templates with relevant rules in access control for easier management.

Feature Entrance

1. Log in to the Cloud Firewall console, then in the left navigation, click **Common Tools**.
2. On the common tools page, click **Go to Configuration** for **Address Template**.

3. On the address template page, users can create and edit templates, and can directly call templates when adding rules on the access control page to reduce operation frequency.

Create a template

1. On the address template page, click **Create a template**.
2. In the create new address template popup, select **template type**.
   - IP address template: contains only IP addresses or CIDR, and supports IP address ranges.
   - domain name template: contains only domain name addresses, and supports wildcard domain names.
   - Protocol port template: A combination of protocols and ports, distinguished by Layer-4 and Layer-7 protocols, supporting single ports, combined ports, or port ranges.

3. Enter the address template name, IP address, and description, click **Confirm** to complete creating a new address template.

> **Note:**
> - When entering a single address, use a line break.
> - When entering multiple addresses simultaneously, ensure the address format is separated by commas before pasting so that the system can recognize them.
> - Note: Inputting duplicate addresses will be automatically merged at the backend.
> - A single address template supports adding up to 500 addresses simultaneously. For completion specifications and content details, refer to the console.

Edit a Template

After the address template is created, you can query it in the left-side address template list; users can add, delete, and modify addresses in the corresponding category within the established template list.

1. On the address template page, click **Edit** in the right operation column of the target address template.
2. In the edit address template popup, select the IP address that needs to be edited for modification or deletion, or search for the IP address that needs to be modified in the search box, perform the operation, and click **Confirm** to save.

> **Notes:**
> Template type cannot be edited. If modification is needed, delete the template and create a new one.

Delete a message template.

1. On the address template page, click **Delete** in the right operation column of the target address template.

> **Note:**
> - <Warning>If there are associated rules, please go to the Access Control Page and delete the corresponding contact rules.</Warning>
> - Deletion is irreversible. It is advisable to back up the current template first.

2. In the confirmation deletion popup, click **Confirm** to delete the rule.

Using Address Templates

On the Access Control Page, you can click **Add Rule** or find the rule that needs to be modified and click **Edit** on the right to choose to use an address template.

> **Notes:**
> - Access rules configured with address templates take effect for all addresses within the template.
> - Address templates only support configuring Internet boundary rules, NAT boundary rules, private network rules, and DNS rules, and do not support configuring enterprise security groups.

- The number of address templates is limited. Plan reasonably and make full use of them.

IP Address Template or Domain Name Template

In access control rules, you can select **address templates** from **access source** or **access destination**. The list pull-down menu will display configurable IP address templates or domain name templates.

> **Notes:**
> The selection of template type is related to the protocol. Please fill in according to the prompt of the corresponding access control rule.

Protocol Port Templates

In the access control rule, you can select **protocol port templates** from the **port protocol type**. The list pull-down menu will display the configurable protocol port templates.

> **Notes:**
> The selection of template type is related to the configuration form of the access source or access destination. Please fill in according to the prompt of the corresponding access control rule.

Rule Backup

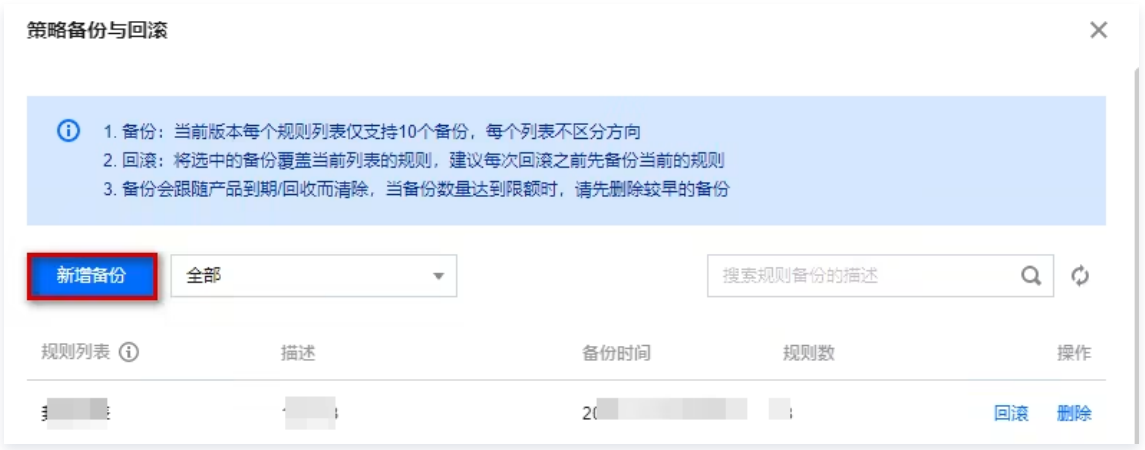
Last updated：2025-05-20 14:33:46

Support backing up existing rules when modifying access control rules, as well as supporting rule rollback for different defense statuses.

Creating a New Backup

1. Log in to the CFW console. In the left sidebar, click **Access Control**.
2. On the access control page, click **Rule Backup** in the upper right corner. The policy backup and rollback popup pops up.

3. In the policy backup and rollback window, click **Create Backup**.



4. Select the rule list for backup, enter remarks, and click **Confirm** to complete adding rule backup.

Rollback Backup

1. On the Access Control Page, click **Rule Backup** in the upper right corner. The Policy Backup and Rollback Popup pops up.
2. Select a backed-up rule and click **Roll Back**.

3. In the "Confirm to Use Backup Rollback Rule List" pop-up window, click **Confirm** to roll back the backed-up rules and overwrite the current rule list.

> **Note**
> The rule rollback operation will override the corresponding rule list. The existing policies will be deleted. To ensure data security, it is recommended to back up the current list first.

Deleting a Backup

1. On the Access Control Page, click **Rule Backup** in the upper right corner. The Policy Backup and Rollback Popup pops up.
2. Select a backed-up rule and click **Delete**.

3. In the "Confirm Deletion" popup, click **Confirm** to delete the backed-up rules.

> **Note**
> Backup deletion of rules cannot be retrieved/restored. Operate with caution.

Automation Assistant

Last updated：2025-05-20 14:34:06

The Automation Assistant is an operation and maintenance tool that provides automatic commands and scheduled commands for users of the Enterprise Edition and above. Users can manually orchestrate commands to achieve automated operation and maintenance.

Feature Entrance

1. Log in to the CFW console. In the left sidebar, click **common tool**.
2. On the common tools page, click **automation assistant go to configuration**.

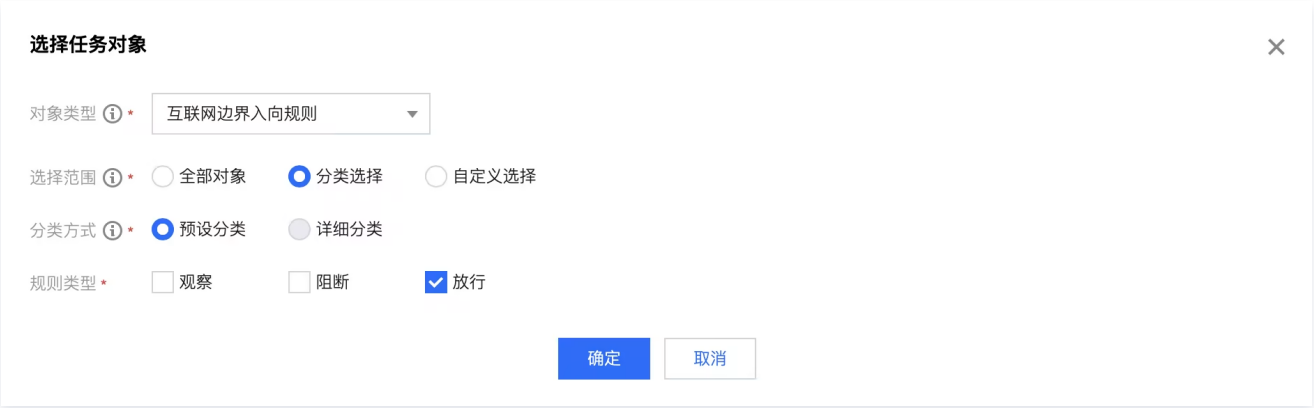
3. On the automation assistant page, users can create and orchestrate automated tasks to implement scheduled start/stop of access control rules, scheduled ignoring of categorized alerts, and other features.

Adding Automation Task

1. On the automation assistant page, click **Add task**.
2. In the new automation task popup, fill in the name of the automated task.

3. Click **click to select** on the right of the task object. You can select the task object that the automation task wants to associate through **category selection** or **custom selection**. Click **confirm**.

> **Note:**
> The current version supports selecting object types including **All Access Control Rule Lists** and **Pending Intrusion Defense Alerts.**



4. **Click [Add Action]** to add the task actions you want to execute. Temporary tasks or periodic tasks and execution time can be set. Multiple actions will be executed in execution order and time sequence; **click [Copy]** to add the number of actions executed. A maximum of 10 actions can be added.

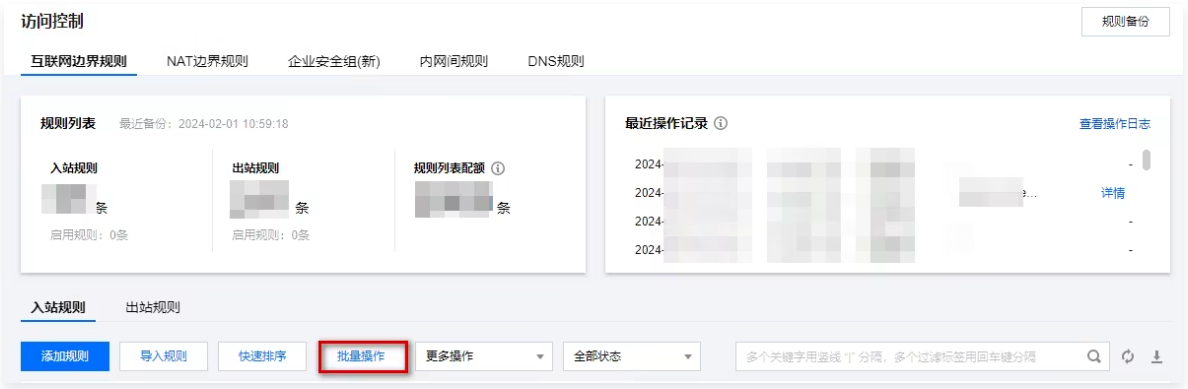
> **Note:**
> The actions supported by the current version are as follows:
> - Access control rule type: Enable Rule, Deactivate Rule.
> - Pending intrusion defense alert: Ignore alerts.

5. Click **Submit** to query configured automation tasks and task status in the task list.

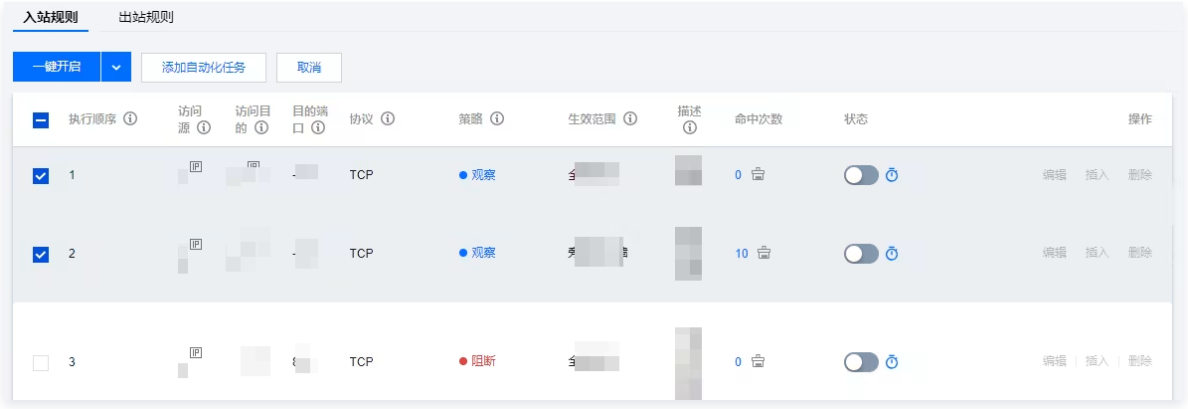
Quickly Add Automation Task

You can quickly add tasks from the access control rule list. Below is an example of an Internet boundary rule.

1. Log in to the CFW console. In the left sidebar, click **Access Control** > **Internet Boundary Rules**.
2. On the internet boundary rules page, click **Bulk Operation**.



3. Check the rules for the automation task you want to execute, and click **Add Automation Task**.



4. In the Create Automation Task window, enter the task name, **click Add Action**, configure other parameters, and **click Submit**.

Editing Automation Task

1. On the common tools page, click **go to configuration** of **automation assistant**.

2. On the Automation Assistant page, locate the task you want to edit and click **Edit**.

3. In the Edit Automation Task popup, you can edit the task name, task type, task action, and execution time. You can also copy or delete a task. Click **Submit** to save.

> **Note:**
> Please note that the automated task will no longer execute after the task object is updated (such as editing, deleting).

Delete Task

1. On the Common Tools Page, click **Go to Configuration** of **Automation Assistant**.

2. On the automation assistant page, find the task you want to delete and click **Delete**.

3. In the confirm deletion window, click **Confirm** to delete the task.

Query Execution Records

In the Operation Log of the associated object of the automated task, you can view the operation records of the account named "Automation Task".

Network Packet Capture Tool

Last updated: 2025-05-20 14:34:26

The network packet capture tool provides users of the Enterprise Edition and above with a tool to obtain network data packets of specified IPs and ports and analyze packet content, helping you locate network faults and analyze attack behaviors, so as to identify security risks in network communication.

Feature Entrance

1. Log in to the CFW console. In the left sidebar, click **common tool**.
2. On the common tools page, click **Go to Configuration** of **Network Packet Capture Tool**.

3. On the network packet capture tool page, users can capture packets and perform download analysis for the traffic of the NAT edge firewall and inter-VPC firewall.

Create Packet Capture Task

1. On the network packet capture tool page, click **Create Packet Capture Task**.

2. In the pop-up window for creating a packet capture task, configure related parameters and click **Start Packet Capture**.

> **Note:**
> Please confirm that your packet capture object has the corresponding firewall switch enabled, otherwise the corresponding traffic will not be able to be captured.

3. Wait until the packet capture task is completed, and then click **Download** to download the packet capture results.

> **Note:**
> Download the packet capture file promptly after completion, with a validity of 3 days.

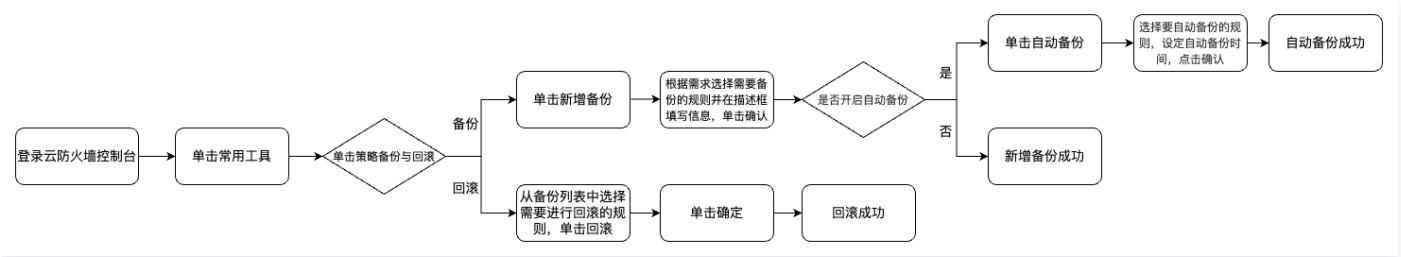
4. The packet capture results can be opened using network packet capture software such as Wireshark for further analysis.

Rule Backup and Rollback

Last updated: 2025-05-20 14:34:53

To respond to possible mis - operations, policy change requirements or emergency fault recovery scenarios, the rule backup and rollback functionality is provided to ensure that your network protection policies are stable and reliable.
Through rule backup and rollback, you can quickly undo recent modifications and return the policy configurations of the Internet edge firewall, NAT edge firewall, VPC boundary firewall, and enterprise security group to the previously saved state.

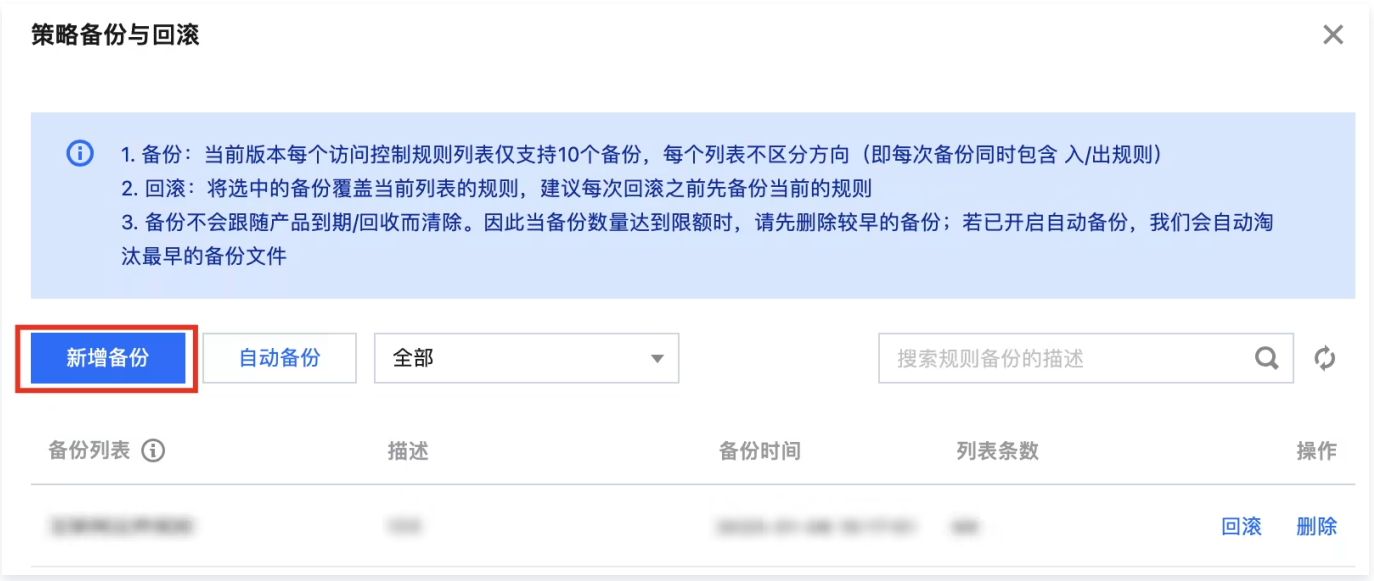
Process Flow Diagram



Policy Backup

1. Log in to the CFW console. In the left sidebar, click **common tool**.
2. On the common tools page, click **Go to Configuration** of **Rule Backup and Rollback**.

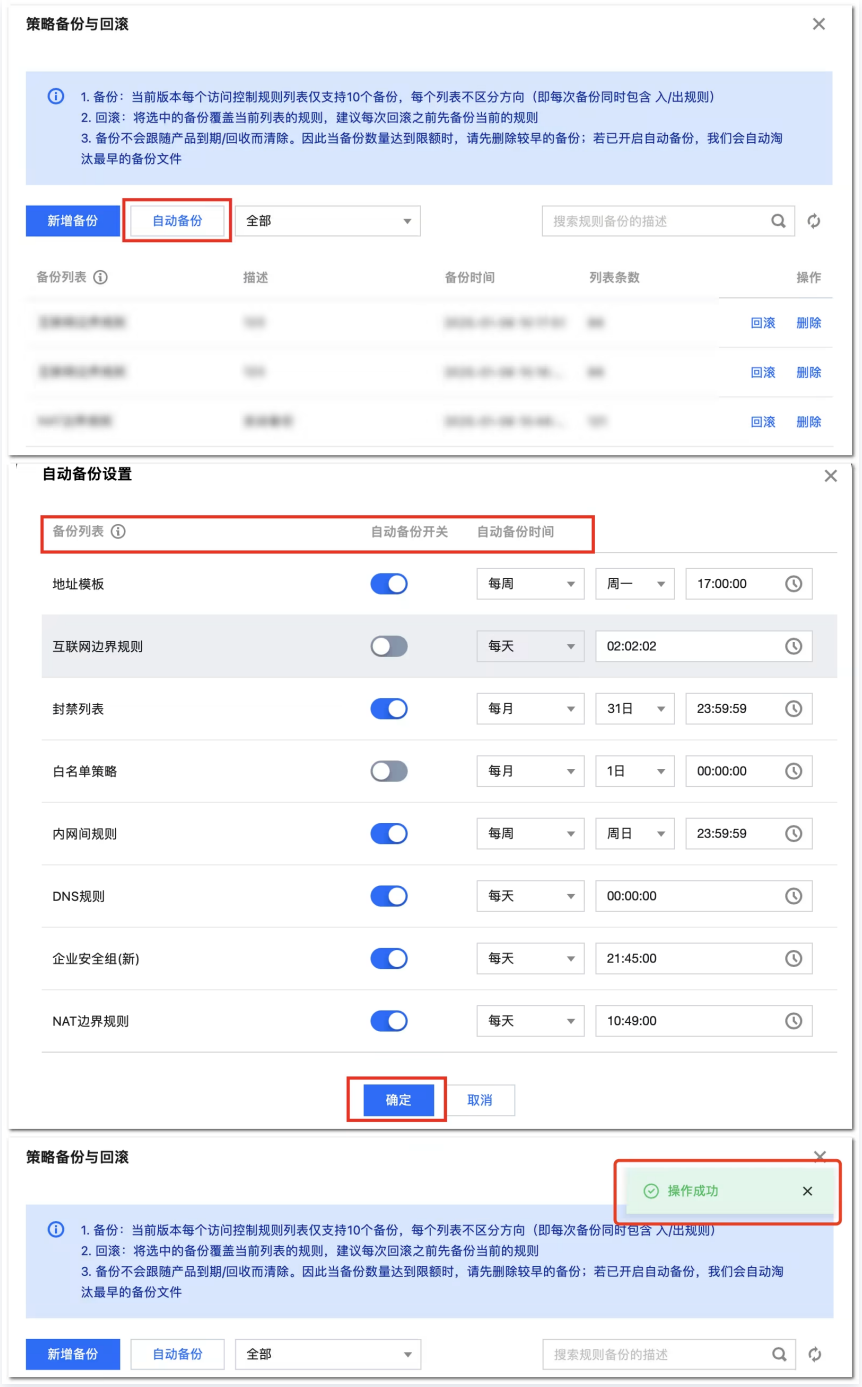
3. On the rule backup and rollback page, click **create backup**.



4. Expand the backup list Options. The system will list the current available rule list for backup. You can choose according to your needs. Meanwhile, for easy identification of the backup purpose later, please fill in a clear and concise description in the **Description** column.

5. After completing the above rule selection and description information filling, click **Confirm**. The system will start the backup program immediately. After backup completion, there will be a 'backup successful' prompt message, informing you that this backup has been smoothly completed and properly stored.

6. The system can also perform **automatic backup** of your selected rules on a scheduled basis as needed. Click **Automatic Backup**. The system will list the available rules for backup. Select the rules that require automatic backup configuration and set a suitable time for automatic backup. After completing the selection of rules and time, verify that the information is correct, and click **Confirm**. The system will start the automatic backup task based on your settings.



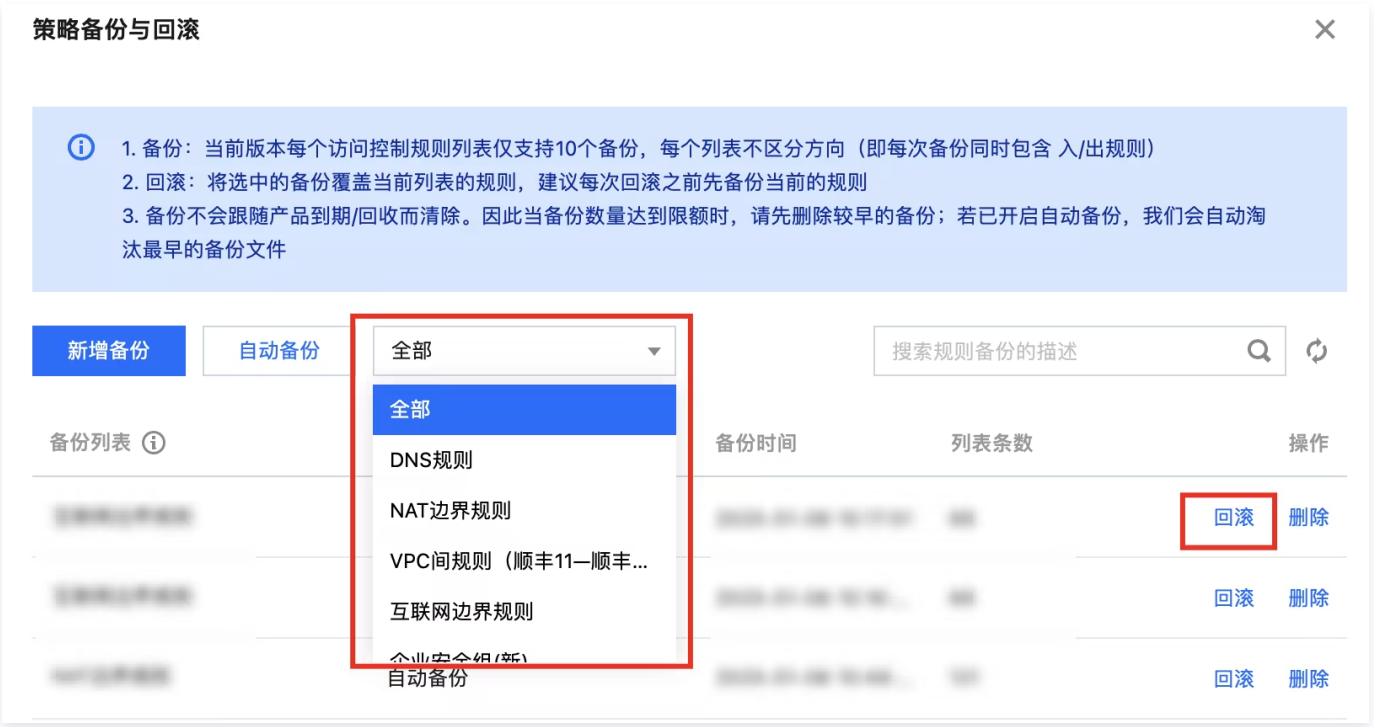
Policy Rollback

> **Note:**
> Using the selected policy backup to perform a rollback operation will overwrite the corresponding policy list. The existing policies will be deleted. To ensure data security, it is recommended to back up the current list first.

1. Log in to the CFW console. In the left sidebar, click **common tool**.
2. On the common tools page, click **Go to Configuration** of **Rule Backup and Rollback**.

3. On the rule backup and rollback webpage, the popup includes all backed-up rule resources, descriptions, and backup times.

4. Scroll down the **Options** to find the rule that needs to be rolled back and click **Roll Back**.



5. **Click Confirm**, and the system will immediately start to overwrite the current rule list with the backed-up rules.

Application Scenario

Scenario Type		Policy Details
Policy Backup	Scheduled Backup	Regularly back up the firewall policy based on a fixed cycle, helping retain the phase status of the network protection policy. Subsequently, when tracing the evolution of the policy, compliance auditing, or comparing the pros and cons of policies at different stages, materials can be quickly obtained as a basis. For example: In the quarterly internal network security review of an enterprise, relying on regular backups can clearly display the adjustment direction and focus of the firewall policy between quarters.
	Before significant business change	Before launching a new business system, scaling out network zones, or making large-scale adjustments to server architecture, businesses must perform policy backup. If the implementation of new policies causes issues such as impact on existing business access, network delay, or exposure of security vulnerabilities, backup policies can be

		quickly restored to avoid prolonged business disruption and damage. For example, e-commerce enterprises scale out servers and adjust firewall policies before the "Double 11" shopping carnival. If backed up in advance, even if new policies encounter problems, fast rollback can be performed to guarantee smooth online transactions during the festival.
	Personnel handover scenario	Back up policies in advance when there is a personnel change in the network security management team. This can reduce work delays and risks caused by personnel changes. Meanwhile, backup policies can be used as a benchmark for subsequent policy adjustments by new members, ensuring the consistency and rationality of policy modifications.
Policy rollback	After an operation error	Due to operation errors, such as accidentally deleting important rules or misconfiguring access permissions, some services may be unable to access properly or potential security risks may occur. In this case, the policy rollback function can immediately restore the policy to the correct state before the operation error, ensuring the normal operation of the business. For example, if an administrator accidentally deletes an access rule for a key business in use while cleaning up expiration rules, rolling back the backup policy from the previous day can quickly fix it.
	Policy adjustment test failure	Enterprises adjust and optimize firewall policies due to business development or to cope with new security threats. If in testing, there are situations such as incompatibility with the existing network architecture, inability to block new type attacks, or impact on business performance, use the rollback feature to restore to the stable state before adjustment, reevaluate the test solution, and avoid losses caused by unsuccessful adjustments. For example, after a financial enterprise tests a new intrusion detection policy and finds a high false positive rate affecting efficiency, it rolls back the original policy and then further studies and improves it.
	After suffering a network attack or failure	When an enterprise network suffers a malicious attack that tampers with the firewall policy, or due to system failures (such as hard disk damage, software crash) resulting in the loss or damage of policy files, the rollback feature can help enterprises quickly restore to the previous reliable policy configuration, reduce losses, and buy time for troubleshooting and repair. For example, an enterprise suffers a DDoS attack late at night, and the policy is maliciously modified. Roll back the backup policy of the previous day to quickly restore protection, and at the same time, technical staff respond urgently to investigate and repair the source.